



USER GUIDE

cnMaestro On-Premises



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.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”).

This product is not restricted in the EU. Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

Contents

Contents	3
Introduction	14
Supported Devices and Features	14
cnMaestro shared features	14
Differences with cnMaestro Cloud	18
Supported browsers	20
Supported Virtualization Infrastructures	20
Device software	22
Quick Start	26
Installation	26
Virtualization	26
Desktop virtualization	26
Bare metal hypervisor	26
cnMaestro deployment	26
Onboard devices	37
DHCP Options (Linux)	43
UI Navigation	47
Account View	47
Access and Backhaul View	48
Enterprise View	48
Industrial Internet View	48
Home page	48
Page structure	49
Page navigation	51
Access and Backhaul View	51
Overview	51
Enterprise View	57
Overview	57
System	57
Devices	57
AP groups and WLANs	58
Sites	58
Side menu	59
Section tabs	59

System status	60
Logout	60
Architecture	62
Overview	62
Networking	62
Device Onboarding	64
Overview	64
60 GHz E2E Controller Onboarding	64
Pre-Configuration and Approval of Devices (Optional)	64
Device Authentication	65
Claiming the Wi-Fi Devices from AP Group	65
Claiming the Wi-Fi Devices from Site Dashboard	66
60 GHz E2E Controller Onboarding	68
Overview	68
High Availability (HA)	72
Overview	72
Primary vs Secondary	72
Shared (Floating) IP Address	72
Network Ports	72
Recommendations	73
Dual Interfaces	73
Add eth1 Network Adapter	73
HA Cluster Setup	75
Bootstrap (Primary)	75
Accept (Primary)	75
Join (Secondary)	75
Basic HA Cluster Creation Flow	76
Secondary Server	77
HA Menu	78
High Availability Cluster Menu (Pre-Bootstrap)	78
High Availability Menu (Post-Bootstrap)	79
New Cluster	79
Accept Join Requests	80
Join Existing Cluster	80
Validate SSH Fingerprints	80
HA Cluster Status	81

Delete Node	83
Leave Cluster	83
Information	83
Behaviour of cnMaestro features when HA is Enabled	84
Monitoring	86
Network Monitoring	86
Dashboard	86
KPI (Key Performance Indicators)	86
Device Health	86
Connection Health	87
Charts and Graphs	87
Notifications	88
Overview	88
Events	88
Alarms	90
Statistics and Details	91
Performance	99
Maps	111
Geolocation Map Settings	112
Map Navigation	113
Mode	113
Tools	115
60 GHz cnWave Tools	116
cnMatrix Tools	116
cnPilot Home Tools	121
cnRanger Tools	122
cnReach Tools	123
cnVision Tools	124
Enterprise Wi-Fi Tools	126
ePMP Tools	133
Machfu	137
PMP Tools	137
Tower-to-Edge view	139
WIDS	140
Detecting Rogue APs	140
cnPilot Dashboards	144

Device Dashboard	144
Overview	144
Clients	144
Dashboard	147
Network Info	150
Mesh Peers	152
Neighbors	153
Site Dashboard	153
Wi-Fi Devices Availability (Total and Offline)	154
Wireless	154
Throughput	154
RF Quality	154
AP Types	155
Top Wi-Fi APs	155
Channel Distribution by Band	155
Radio/WLAN Distribution by Band	156
Clients by SNR	156
Clients by Performance	156
Clients Graph	157
Throughput Graph	157
Statistics	157
Wireless Clients	158
Floor Plan	158
Inventory	160
Inventory Export	160
Bulk Delete	160
Bulk Reboot	161
Schedule Reboot	162
CSV Configuration Import	162
Sample Configuration File	163
Sample Configuration File (60 GHz cnWave)	163
Uploading a Configuration File	164
Reports	167
Generating Reports	167
Device Report	167
Performance Report	173

Active Alarms Report	179
Alarms History Report	179
Events Report	179
Clients Report	180
Mesh Peers Report	181
Guest Access Login Events	181
Remote Upload	182
Report Jobs	183
Provisioning	184
Software Update	184
Software Update Overview	184
Create Software Update Job	185
Software Update while Onboarding	187
Software Update through Managed Devices	188
Viewing Running Jobs in Header	192
cnReach Bulk Software Upgrade	192
Fixed Wireless Configuration	194
Overview	194
Configuration Templates	194
Configuration Variables	195
Macros	195
Variable Caching	196
Device Type-Specific Configurations	196
Variable Validation	196
Sample Templates	196
Template File Creation	196
Template	196
Configuration Update	198
Device Selection	198
Device Type	198
Device Table	198
Configuration Update Steps	200
Configuration Backup	200
Jobs	203
Configuration Update	204
Wireless LAN Configuration	205

cnPilot Home and Enterprise Wi-Fi	205
Configure cnPilot using cnMaestro	205
Create an AP Group	211
Pre-Defined Overrides	216
User-Defined Overrides	216
User-Defined Variables	216
Bulk Overrides	217
Synchronize (Sync) Configuration	223
Configuration Job Status	224
Factory Reset	224
Association ACL	225
Overview	226
Configuring Association ACL	226
cnMatrix Switches	227
Switch Groups Configuration	227
Synchronize (Sync) Configuration	233
Policy Based Automation(PBA)	235
Switches	237
Switch Ports	242
Device Details	249
60 GHz cnWave Network Configuration	253
Managing E2E Network	253
Site Configuration	291
Node Configuration	295
PoP Node	303
DN/CN Node	323
Auto-Provisioning	334
Creating Auto-Provisioning Rule	334
Services	336
Managed Service Provider (MSP)	336
Overview	336
Managed Accounts	336
Managed Service	337
Managed Service Provider (MSP)	338
Managed Service Users (Administrators)	339
Configuring Managed Services	341

Enable Managed Service Provider (MSP)	341
Create Managed Services	342
Create Managed Account	344
Validate Managed Account Administrators	345
Managed Services Administration	348
Overview	348
System Dashboard	349
Managed Account Administration	350
Device Management	351
Disabling Managed Service Provider Feature	353
API Client	354
Overview	354
API Clients	354
RESTful API Specification	355
Authentication	355
Swagger API	356
Introduction	356
Sample Swagger UI Screenshot	357
Client ID and Client Secret Generation	357
cnMaestro User Interface	357
API Session	358
Introduction	358
Retrieve Access Token	358
Access Resources	360
API Details	360
HTTP Protocol	360
REST Protocol	361
Parameters	363
Access API	368
Token (basic request)	368
Token (alternate request)	369
Validate Token	370
Selected APIs	371
Overview	371
cnMaestro v2 API	371
Devices API Response (v2 Format)	372

Statistics API Response (v2 format)	374
Performance API Response (v2 format)	386
External Guest Access Login API	394
60 GHz cnWave RESTful API	396
cnPilot Guest Access	399
Configuration	399
Create the Guest Access Portal in cnMaestro	399
Mapping the Device to Guest Access Portal in cnMaestro	409
Access Types	411
Guest Access using Social Login	411
SMS Authentication	422
Generic SMS Gateway Configuration	422
cnPilot GRE Tunnels	429
Overview	429
Typical Deployment Model (Two Port Solution)	429
Multicast/Broadcast Handling with Multiple APs on Tunnel Concentrator	430
Inter AP Wireless Client Communication (through Concentrator)	430
Access Control List (ACL) Configuration	430
MAC Layer ACL	431
IP Layer ACL	431
Transport Layer ACL	432
SNMP	433
Overview	433
Enable SNMP	433
Configure SNMP Parameters	433
cnMaestro MIB (Management Information Base)	434
RADIUS Proxy	435
Overview	435
Minimum cnMaestro On-Premises Version Requirements	435
RADIUS Proxy Configuration	435
Citizen Broadband Radio Service (CBRS)	437
Enabling CBRS in Cloud	437
Enabling CBRS in On-Premises	442
Share CBRS Configuration to the On-Premises Instance	443
CBRS HTTP Proxy Configuration Options	444
Management Tool	446

Using a HTTP Proxy Server for CBRS Connectivity	468
Proxy Suggestions for CBRS Connectivity	468
External Proxy Requirements	468
Squid as External Proxy	468
HA for Squid external proxy	469
LTE	470
Adding SIM Cards	470
cnArcher Installation Summary	472
Configuration	474
Photos and Location	474
Link Test Result	474
AP Scan Result	475
Administration	476
User Management	476
Authentication	476
Local Users	476
Creating Users and Configuring User Roles	481
Changing Password	482
Authentication Servers	483
Session Management	492
Server Management	493
Monitoring	493
Settings	493
Operations	499
Update cnMaestro Software	500
System Backup	500
In-System Upgrade	502
Diagnostics	504
SSL Certificate	505
Certificate Management	506
Manage Software Images	509
Webhooks	514
Integrations	514
Limits	515
cnMaestro Webhooks Configuration	515
Types of Variables	518

Error and Retransmission	519
Viewing Configured Webhooks	519
Status Check	520
Custom Template Examples	520
Audit Logs	535
Syslog	538
Cloud Connectivity	542
Overview	542
Connecting cnMaestro On-Premises to Anchor Account	543
Software Images	544
cnMaestro System Update	545
Appendix	547
Maintenance	547
Command Line Alternatives	547
Export cnMaestro Data	547
Import cnMaestro Data	547
Technical Support Dump	548
Apply OVA Upgrade	548
Apply Package Update	548
SSH Access	548
Enabling SSH Access	548
Data Backup	551
Overview	551
cnMaestro backups	551
Full Backups	551
Virtualization System specific Backup Methods	552
Extending the Data Disk	553
VMware Workstation Disk Expansion	553
VirtualBox Disk Expansion	554
Partition and File System Updates	554
Account Recovery	554
Virtual Machine (Console) Account Recovery	554
cnMaestro Application Account Recovery	556
Application Account Recovery	556
Configure Network Time Protocol (NTP)	558
Disabling NTP Support	558

Statistics API Response (v1 Format)	559
Performance API Response (v1 Format)	570
Deployments	579
VMware ESXi Installation	579
cnMaestro VM Deployment	579
Oracle VirtualBox 5 Installation	582
VMWare Workstation	583
KVM Installation	585
Deployment	585
Windows DHCP	589
Configuring Option 60	589
Windows DHCP Server Configuration	589
Configuring Option 43	590
Windows DHCP Server Configuration	590
Configuring Option 15	590
Windows DHCP Server Configuration	591
Configuring Vendor Class Identifiers	591
Configuring the Policies at the SCOPE Level	592
Citrix Hypervisor Installation	596
Overview	596
Import using Citrix Hypervisor	596
Access cnMaestro	600
SSH Access	600
HTTPS Access	601
Advanced Options	601
Expand the Data Disk	601
Expand the volume through Citrix Hypervisor	601
Expand the file system within cnMaestro	602
Network Requirements	603
Inbound Ports	603
Outbound Ports	603
Custom Network Scripts	604
Contact Cambium Networks	605

Introduction

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

This section covers the following topics:

- [Supported Devices and Features](#)
- [Quick Start](#)
- [UI Navigation](#)
- [Architecture](#)
- [Device Onboarding](#)
- [High Availability](#)

Supported Devices and Features

cnMaestro shared features

Table 1 lists the features shared between the on-premises and cloud deployments.

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
✓	✓	60 GHz cnWave	Manage 60 GHz cnWave Networks.
✓	✓	Advanced Troubleshooting	Display tower-to-edge status in a single graphic, which is used to: <ul style="list-style-type: none">• Troubleshoot client connectivity directly on the AP.• View Wi-Fi client details and health.
✓	✓	AP Group Configuration	Configure Enterprise Wi-Fi and cnPilot Home devices.
✓	✓	AP Group Dashboard	Display aggregate Wi-Fi AP statistics for the configured AP Group.
	✓	Audit Logs	Record administrator activities.
	✓	Auto Manage Routes	Support automated IPv6 routes for cnWave 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.

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
✓	✓	Bulk Image Upgrade	Schedule software image upgrades across sectors or device groups.
✓	✓	Citizen Broadband Radio Service Subscription (CBRS)	Support CBRS-compliant devices in the 3.6 GHz band (from 3550 MHz to 3700 MHz).
	✓	Client Dashboard	Allows methods to control, or block applications or terminate based on consumption of applications.
✓	✓	Cloud Connectivity	Automatically download device software from the cloud.
	✓	cnArcher Installation Summary	It displays installation summary of PMP SMs.
	✓	Data Reports	Export device, performance, alarm, and event statistics data in CSV formats.
✓	✓	Device Inventory	Aggregate inventory data at the System, Network, Tower, Sector, or Site level. It supports data export in PDF or CSV formats.
✓	✓	Email Notifications	Send email alerts when the alarm status changes.
✓	✓	Enterprise View	Display a simplified UI tailored for Enterprise Wi-Fi devices.
✓	✓	Guest Access Portal	Allow Wi-Fi Clients to access wireless service using a free model or vouchers.
	✓	Guest Access Portal (Paid Access)	Allow Wi-Fi Clients to connect to wireless service through paid access.
✓	✓	Hierarchical Dashboards	Visualize devices from tower-to-edge through customized dashboards for each device type.
✓	✓	IPv6 Support	Provide IPv6 support for cnPilot Enterprise devices.
	✓	Long Term Historical Data	Display long-term performance graphs for the following: <ul style="list-style-type: none"> • Fixed Wireless Broadband up to 2 years. • Wi-Fi APs, IIoT, and cnMatrix up to 1 year.

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
✓	✓	LTE	Manage cnRanger LTE devices.
	✓	Managed Server Provider (MSP)	Split an installation into separate Managed Accounts with independent administration and configuration.
✓	✓	Maps and Map Modes	Position devices and visualize their health and connectivity on the map. Also, change the map mode to display wireless key performance indicators.
✓		Mesh Peers	Display the details of available Mesh clients.
✓	✓	Multiple UI View	<p>Support the following tailored views in the cnMaestro UI:</p> <ul style="list-style-type: none"> ● Access and Backhaul View: Used for managing Fixed Wireless and Wi-Fi deployments, including the following: <ul style="list-style-type: none"> ● 60 GHz cnWave ● cnMatrix ● cnPilot Home (cnPilot R-Series) ● cnRanger ● cnVision ● Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) ● ePMP ● PMP ● PTP ● Enterprise View: Used for managing Enterprise Wi-Fi (E-Series and XV-Series), cnPilot Enterprise (ePMP 1000 Hotspot), and cnMatrix. ● Industrial Internet View: Used for managing Fixed Wireless, Wi-Fi, and IIoT deployments, including the following: <ul style="list-style-type: none"> ● 60 GHz cnWave ● cnMatrix ● cnPilot Home (cnPilot R-Series)

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
			<ul style="list-style-type: none"> • cnRanger • cnReach • cnVision • Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) • ePMP • Machfu • PMP • PTP
✓	✓	Notifications	Communicate immediate status with stateful alarms and events. Notifications help troubleshoot customer issues.
	✓	RADIUS Proxy	Proxy RADIUS packets are sent through cnMaestro (On-Premises) instead of directly to the RADIUS server from the AP.
	✓	RESTful API	Support HTTPS RESTful API for inventory, monitoring, performance, notification, and basic provisioning.
✓	✓	Role-Based Access	Assign the following roles to users: <ul style="list-style-type: none"> • Super Administrator • Administrator • Operator • Monitor • CPI
✓	✓	Scheduled Configuration Update	Specify a time to configure devices.
✓	✓	Scheduled Software Update	Specify a time to install device software.
✓	✓	Site Dashboard	Aggregate Wireless LAN AP statistics by location.
✓	✓	Statistics and Trending	Present historical radio and network statistics.

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
✓	✓	Switch Groups	Share configuration across cnMatrix switches.
✓	✓	Syslog	Forward audit and event logs to a configured external Syslog server.
✓	✓	Template-Based Configuration	Schedule configuration of single devices or a group of devices across the network using templates for cnMatrix, cnPilot Home Series, cnReach, cnVision, ePMP, and PMP devices.
	✓	User Session Management	Track current cnMaestro users and support forced logoff.
✓	✓	Zero Touch Onboarding	Enable cnVision Client, PMP SMs, and ePMP SMs to automatically appear in the onboarding queue if the parent AP is already onboarded.

Differences with cnMaestro Cloud

The majority of features in cnMaestro On-Premises are identical to cnMaestro Cloud, but there are some differences.

Table 2 lists the feature differences between Cloud and On-Premises supported by cnMaestro.

Table 2: Differences with Cloud

Essentials	X	Feature	Description
✓	✓	Account Recovery	Password and account recovery issues are resolved locally.
	✓	Auto-Provisioning	New devices, such as cnPilot, cnVision, ePMP, and PMP, can automatically be approved and onboarded using the subnet.
✓	✓	Certificate Management	SSL certificate management is available for the UI and Guest Access Portal.
✓	✓	cnMaestro Software Upgrade	Enable three types of software upgrade: <ul style="list-style-type: none"> • Virtual machine upgrade requires the customer to replace the entire virtual machine with a new instance. The configuration and the data are exported from the old instance and imported to the new. • Package upgrade only updates the cnMaestro software. It does not require a virtual machine reinstallation.

Table 2: Differences with Cloud

Essentials	X	Feature	Description
			<ul style="list-style-type: none"> ● OVA upgrade only overwrites the OS partition. For more information, refer to OVA Image.
✓	✓	Configuration Backup	Backup configuration from fixed wireless devices (cnVision, PMP and ePMP) and cnReach devices that are currently online.
✓	✓	Deployment	<ul style="list-style-type: none"> ● The Cloud version is fully hosted and maintained by Cambium Networks at https://cloud.cambiumnetworks.com. ● The On-Premises version is released as an OVA (Open Virtualization Archive) file that needs to be installed on either VMware or VirtualBox.
✓	✓	Device Connectivity	<ul style="list-style-type: none"> ● In the Cloud version, all devices can be accessed through https://cloud.cambiumnetworks.com. ● In the On-Premises, version, 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	<ul style="list-style-type: none"> ● In the Cloud, device images are automatically available. ● In On-Premises, new images need to be downloaded from Support Center and added to the cnMaestro server.
✓	✓	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+, RADIUS, LDAP, and Active Directory).
✓	✓	Onboarding	<ul style="list-style-type: none"> ● 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 On-Premises version, all devices contacting cnMaestro are added to the Onboarding Queue, where they are approved and managed.

Table 2: Differences with Cloud

Essentials	X	Feature	Description
✓	✓	On-Premises Console	Configure networking parameters and update the system password using the CLI available through the virtual machine console.
✓	✓	Server Management	Monitor virtual machine parameters such as disk, memory, and CPU utilization through the UI.
	✓	SNMP	Basic SNMP for inventory and alarms.
✓	✓	System Events	System events for On-Premises server instance.
✓	✓	System Log	Forward events to a remote system log server.
	✓	Webhooks	Send alarm notifications to the external servers.
✓	✓	Wireless LAN Speed Test	Test the speed between the wireless LAN APs and cnMaestro.

Supported browsers

Table 3 lists the 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

Supported Virtualization Infrastructures

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

**NOTE:**

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

Table 4 lists the platforms supported by cnMaestro:

Table 4: Supported virtualization infrastructures

Platform	Version
VMware ESXi	Version 6.0.0 Update 3 (Build 7967664) or higher (this is the preferred platform)
VMware Workstation/Player	Version 16

Hardware requirements

cnMaestro On-Premises is preconfigured with two virtual drives of approximately 120 GB total size. The image supports up to 10,000 devices, including cnMatrix, cnReach, cnPilot, ePMP, PMP, and PTP.

**NOTE:**

Virtual hardware is different than physical hardware. Virtual hardware executes the cnMaestro application, and physical hardware executes the VMware virtualization infrastructure and the cnMaestro application (and other independent applications).

**NOTE:**

- Cambium Networks recommends using a recent Intel Core i7 or Xeon CPU with the following Geekbench Multi-Core score:
 - 4,500 for 100 devices
 - 8,000 for 4,000 devices
 - 13,400 for 10,000 devices.
- If RADIUS Proxy is enabled, system resources like vCPUs and RAM must double the requirements in [Table 5](#).
- If a user enables NBI APIs and generates multiple performance reports, system resources like vCPUs and RAM must increase by 1.5 times the requirements in [Table 5](#).
- Cambium Networks recommends using a SSD drive to improve performance.

Table 5 lists the hardware requirements supported by cnMaestro.

Table 5: Hardware requirements

Number of Devices	Wireless Clients	Number of vCPUs	RAM Size (GB)	Hard Disk (GB)
1 - 100	Up to 1500	2	4	80
101 - 1,000	Up to 15,000	4	4	100
1,001 - 4,000	Up to 60,000	4	8	150
4,001 - 10,000	Up to 150,000	8	16	250

Device software

The cnMaestro OVA contains the latest versions of device software. Download new device software to your local computer using the steps described in the [Supported Devices and Features](#) section.

Device software is available from Cambium Support Center at: <https://support.cambiumnetworks.com/files>.

Table 6 lists the device model and the minimum software version supported by cnMaestro (not the recommended version).

Table 6: Supported devices and minimum software versions

Device	Minimum Software Version
60 GHz cnWave V1000	1.1
60 GHz cnWave V3000	1.1
60 GHz cnWave V5000	1.1
cnMatrix	2.0.4-r1
cnPilot e400/e500	3.2.1-r6
cnPilot e425H/e505	4.0
cnPilot e430W/e410/e600	3.5.2-r4
cnPilot e501S	3.2.1-r6
cnPilot e502S	3.2.1-r6
cnPilot e510	3.11.4-r9
cnPilot e700	3.7-r9
cnPilot r190	4.4.2-R2

Table 6: Supported devices and minimum software versions

Device	Minimum Software Version
cnPilot r195P	4.7
cnPilot r195W	4.5.2
cnPilot r200/r201	4.4.2-R2
cnPilot XE3-4	6.4
cnPilot XV2-2	6.1
cnPilot XV2-2	6.4
cnPilot XV2-2T0	6.3.5-r4
cnPilot XV3-8	6.0
cnRanger Sierra 800	1.0.1.0-r1
cnRanger Tyndall 101	1.0.1.0-r1
cnRanger Tyndall 201	2.0-r1
cnReach N500	5.2.17e
cnVision Client	4.6
cnVision Hub	4.6
E2E Controller	1.0.1-r2
ePMP 1000	2.6.2
ePMP 1000 Hotspot	3.2.1-r6
ePMP 2000	3.0.1
ePMP 3000	4.4.1
ePMP Elevate	3.2
ePMP Elevate SXGLIT5/LHG5	4.3.2.1
ePMP Elevate XM/XW	3.2
ePMP Force 130 2.4 GHz	4.4
ePMP Force 130 5 GHz	4.3.2

Table 6: Supported devices and minimum software versions

Device	Minimum Software Version
ePMP Force 180/200	2.6.2
ePMP Force 190	3.5
ePMP Force 200L	4.7.0
ePMP Force 300	4.1
ePMP Force 300-13	4.4
ePMP Force 300-13L	4.5.2
ePMP Force 300-13LC	4.6
ePMP Force 300-19	4.4
ePMP Force 300-19R	4.4
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 MP 3000	4.5
ePMP PTP 550	4.1
ePMP PTP 550E	4.4.2
Machfu	7.1.2-11.0.5
PMP	15.0.1
PMP 450 MicroPoP Omni	16.2.1
PMP 450 MicroPoP Sector	16.2.1
PMP 450b Retro	16.2.2
PTP 650	01-47
PTP 670 (650 Emulation)	01-47
PTP 670, PTP 700	02-67



NOTE:

By default, Cambium Networks does not update device builds during OVA or package upgrades. The user must upload device software by clicking the **Add** button in **Administration > Server > Software Images > Manage Software Images**. Software can also be downloaded through an Anchor account.

For further information, refer to [Manage Software Images](#).

Quick Start

Installation

The default passwords for cnMaestro are:

Table 7: Default passwords

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



NOTE:

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

Virtualization

On-Premises supports two types of virtualization:

- [Desktop virtualization](#)
- [Bare metal hypervisor](#)

Desktop virtualization

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

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

Bare metal hypervisor

A bare metal hypervisor takes over the entire physical machine and uses it to host virtual instances. This type of virtualization is best for production environments, but takes time to set up correctly. VMware vSphere ESXi is an example of this type of virtualization, and it is discussed in detail in the [Appendix](#). You can download ESXi [here](#).

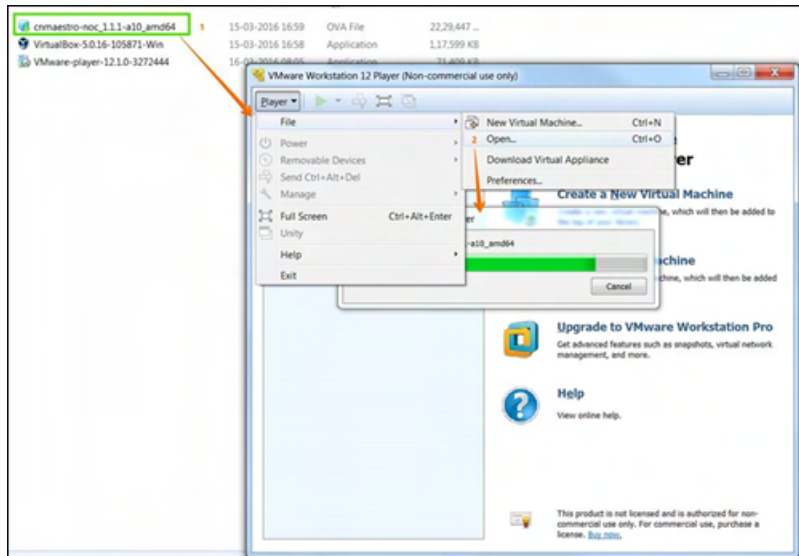
cnMaestro deployment

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

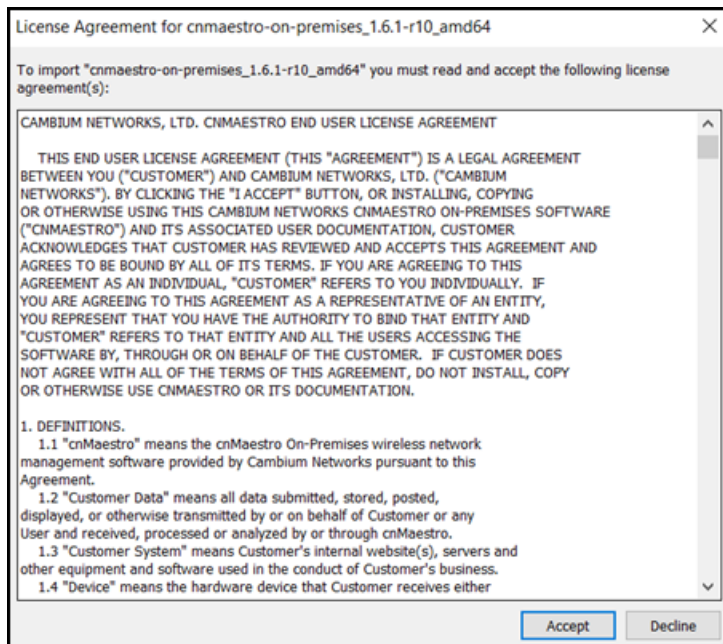
VMware Workstation Player

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

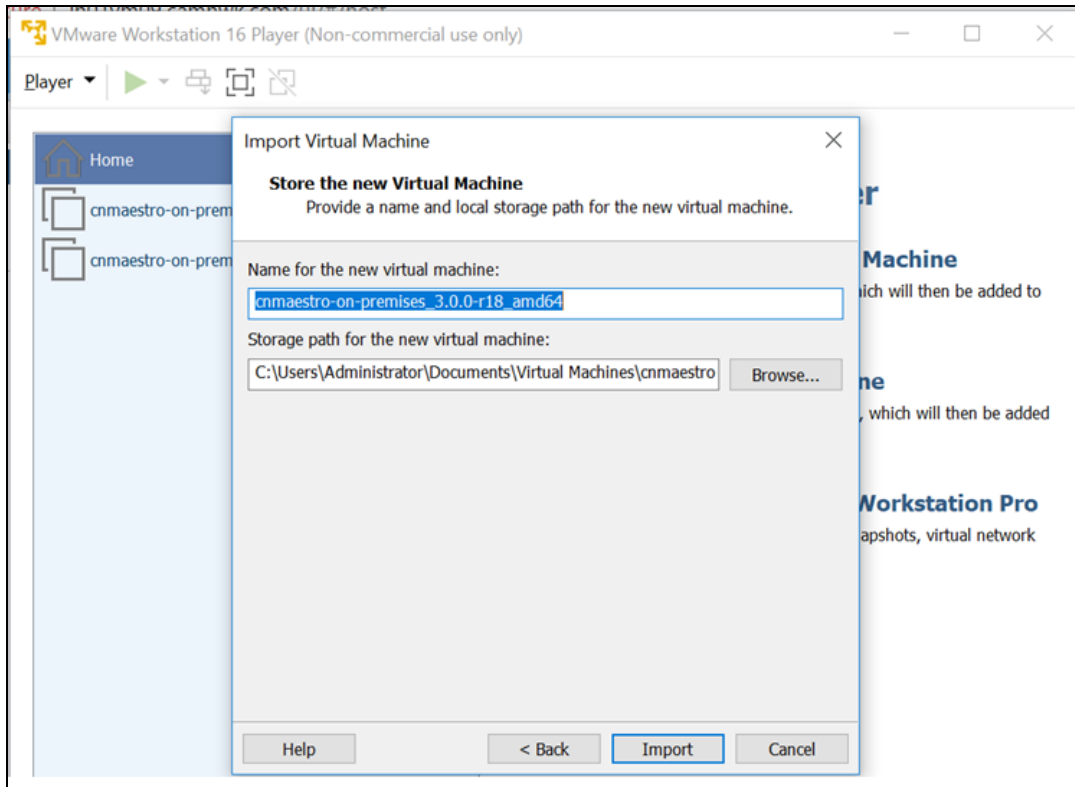
1. Download the cnMaestro On-Premises OVA file from Cambium Support Center.
2. Open VMware Workstation Player and navigate to **Player > File > Open**. Import the cnMaestro OVA.



3. **Accept** the cnMaestro EULA.



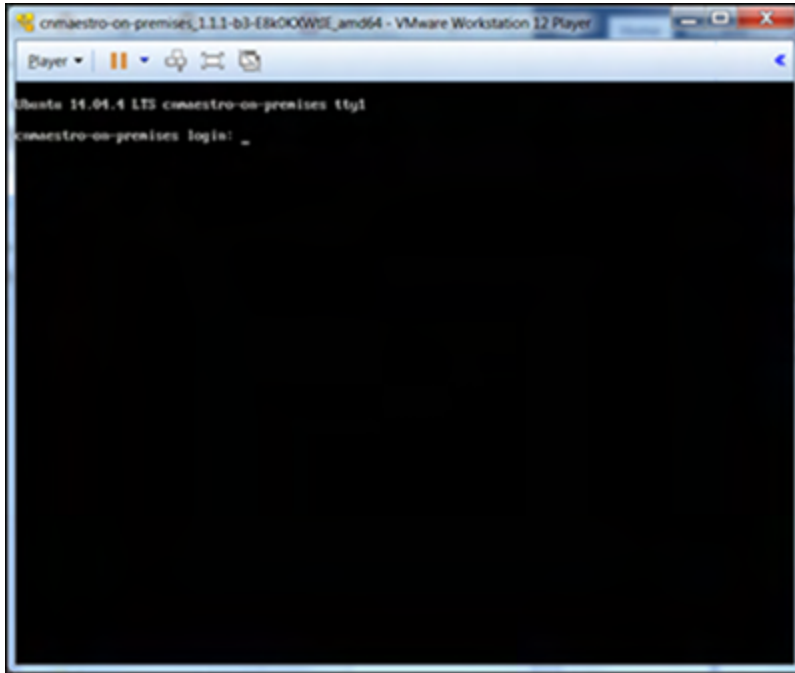
4. Click **Import** to start the deployment. This process could take a couple of minutes.



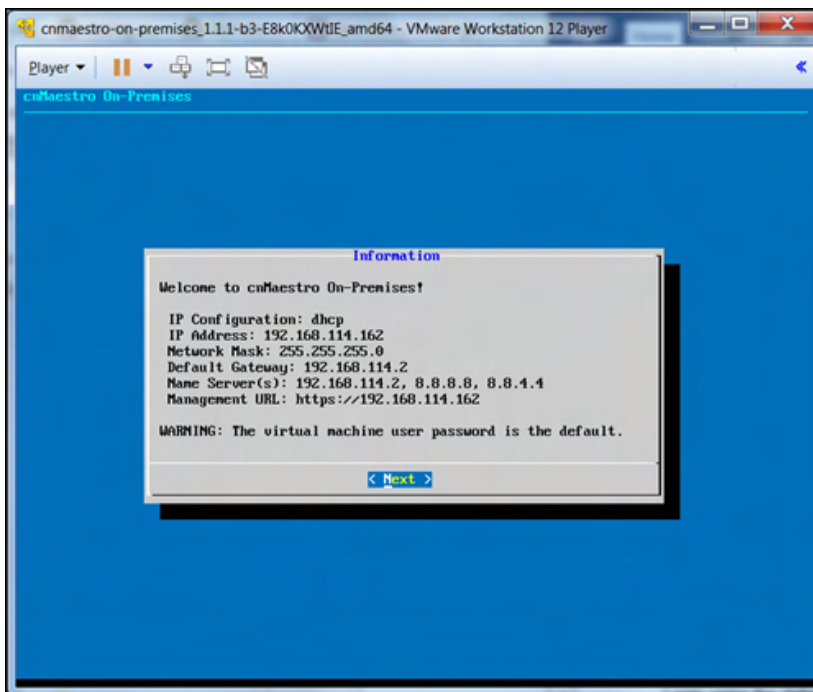
5. Click **Play** to start the Virtual Machine.



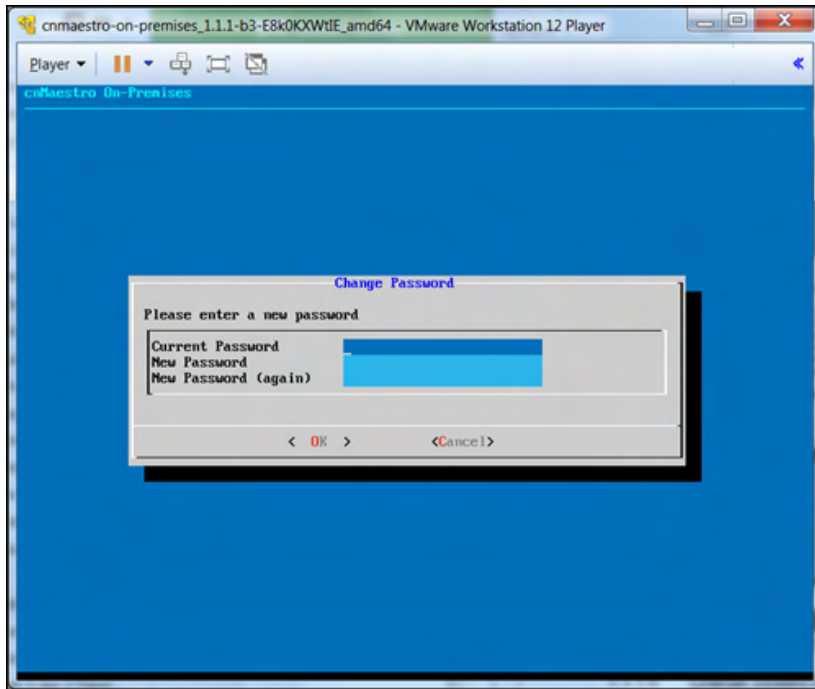
6. Login to the cnMaestro Console using the default username/password (cambium/cnmaestro). The Console is the primary way to access the cnMaestro CLI (Command Line Interface).



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



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



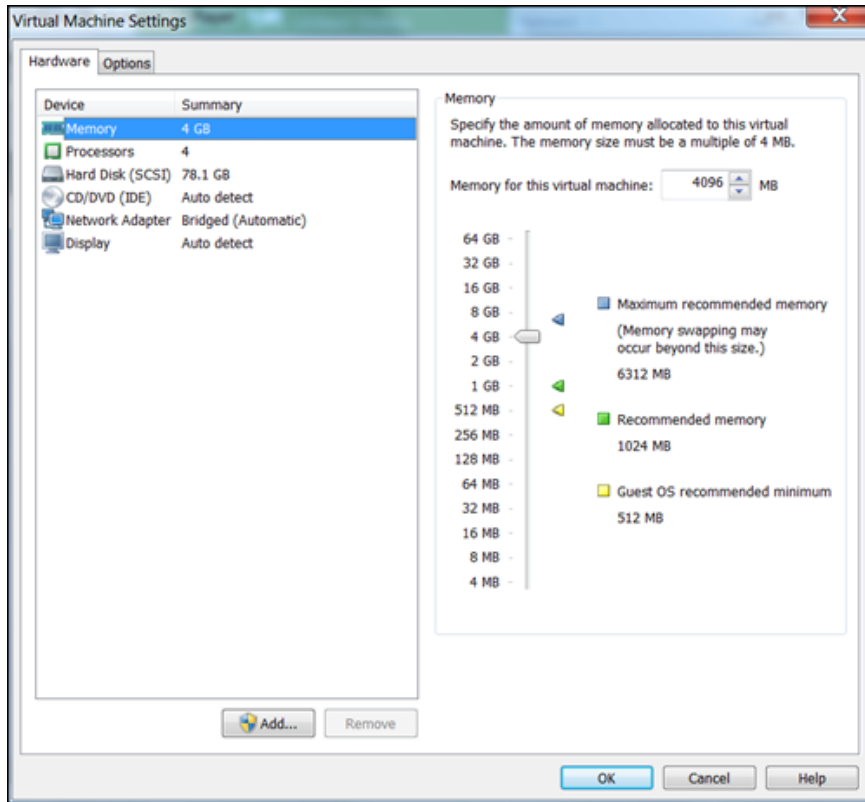
Update virtual machine hardware

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



NOTE:

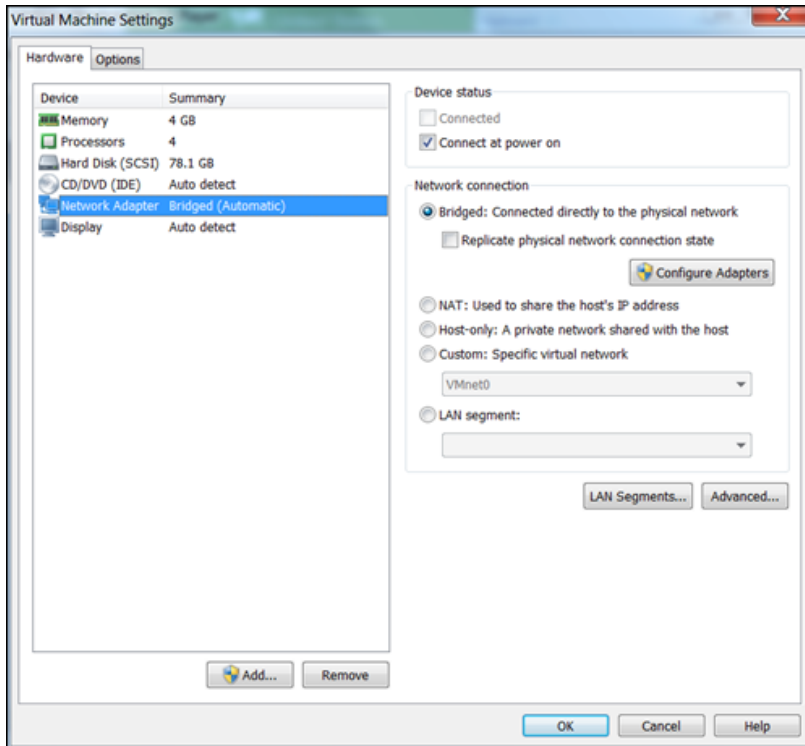
If you are evaluating more than 100 devices, we recommend to use at least 4 GB of memory and 4 processors.



Configure network adapter

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

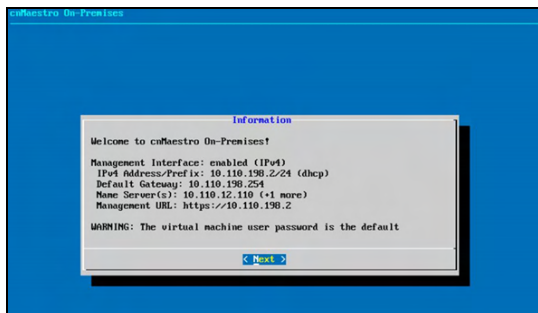
1. In the VMware settings, select **Bridged** for the Network Adapter state and select the **Network Adapter > Configure Adapter** to choose the external LAN adapter.



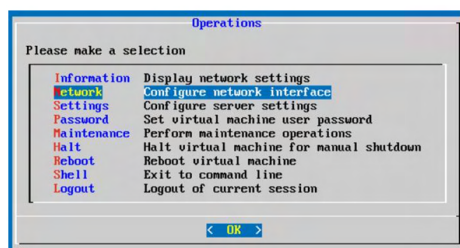
2. Restart cnMaestro.

Configure cnMaestro networking

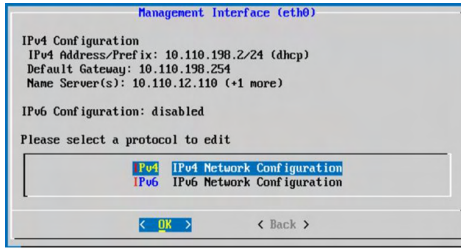
1. After logging back in, the **Information** page displays the IP address from the LAN instead of the private network.



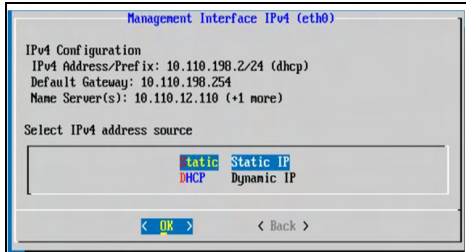
2. Click **Next** to view the **Operations** menu and select **Network**.



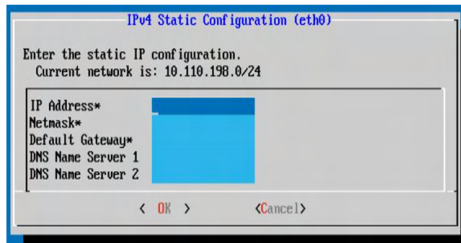
3. The **Management Interface (eth0)** window appears.



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



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



Network configuration

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

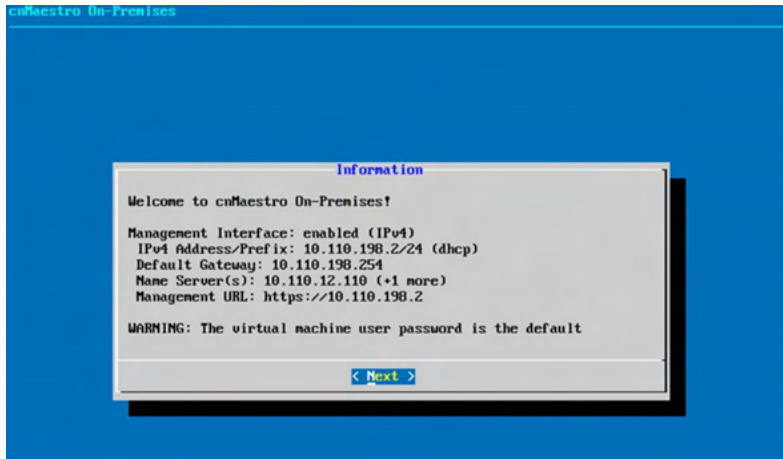
Single interface (eth0)

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

Protocols (IPv4, IPv6)

cnMaestro supports both IPv4 and IPv6. The eth0 interface requires IPv4 (for the system IP address and clustering configuration) and optionally supports IPv6.


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

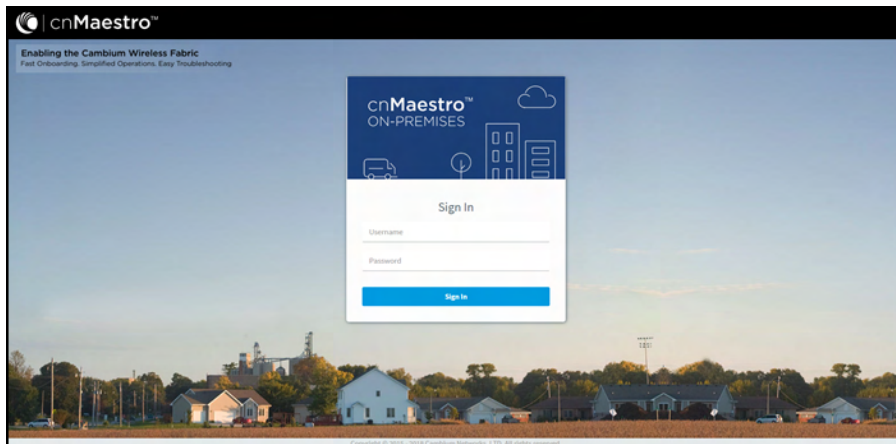


cnMaestro UI access

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

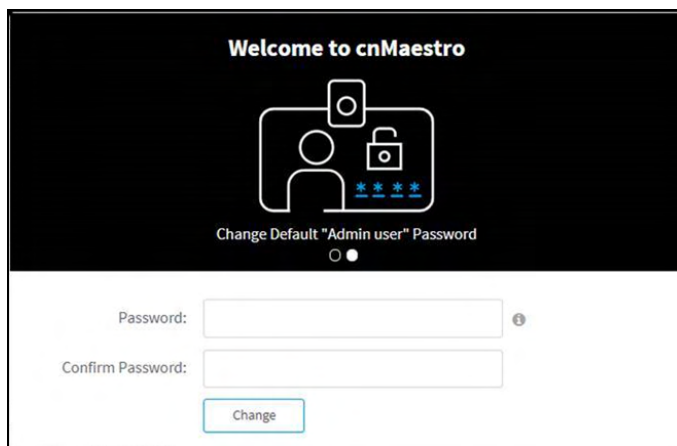
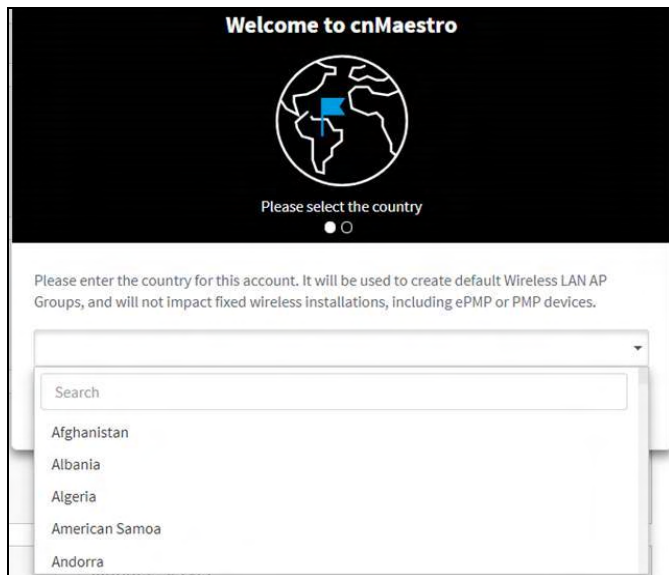
The default username/password are admin/admin.

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




First login

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



User can connect to Cloud account using Enforce Anchor account.

	<p>NOTE: Enforce Anchor account connectivity is available only for new 3.1.0 installations.</p>
---	--

Perform the following steps to connect to the Cloud account.

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

Welcome to cnMaestro

cnMaestro

Connect to cnMaestro Cloud

cnMaestro On-Premises must be connected to a Cloud Anchor account in order to complete installation. Please see the [Cloud Connectivity](#) section of the online help for additional direction.

Cambium ID

Onboarding Key

HTTP Proxy

Configure HTTP Proxy to connect to cnMaestro Cloud

Connect [Login to Cloud Account](#)

Configure HTTP Proxy to connect to cnMaestro Cloud.

2. Select **HTTP Proxy**.
3. Enter **IP or Hostname**.
4. Enter **Port** number and click **Connect**.

Welcome to cnMaestro

cnMaestro

Connect to cnMaestro Cloud

cnMaestro On-Premises must be connected to a Cloud Anchor account in order to complete installation. Please see the [Cloud Connectivity](#) section of the online help for additional direction.

Cambium ID

QA_ANCHOR

Onboarding Key

.....

HTTP Proxy

Configure HTTP Proxy to connect to cnMaestro Cloud

IP or Hostname

cnssquid.cnmww.com

Port

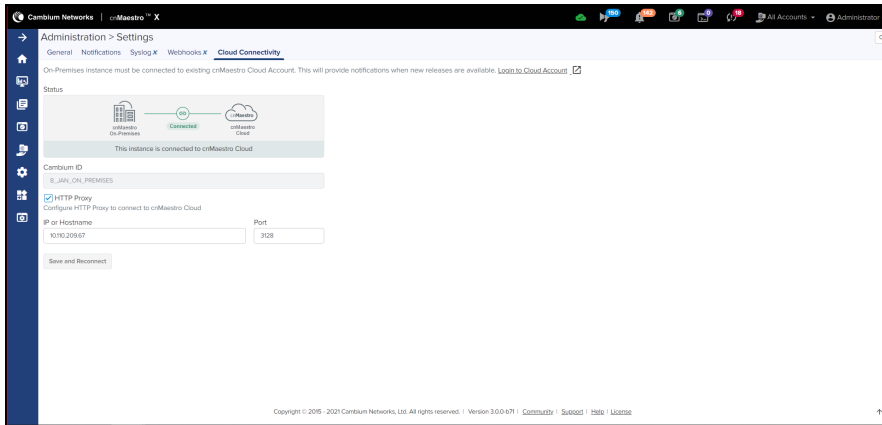
2

Connect [Login to Cloud Account](#)

For more details to connect with Cloud Anchor account, refer to [Cloud Connectivity](#).

Once the initial configuration is complete, you will have access to the entire UI.

5. Navigate to **Administration > Settings > Cloud Connectivity** to connect the Cloud Anchor account with On-Premises.



6. Navigate to **Administration > Server** to monitor and manage cnMaestro On-Premises.

Onboard devices

Devices must have the correct software installed in order to access cnMaestro. These images are hosted on the Cambium Networks website, and they can also be downloaded directly from cnMaestro On-Premises. The minimum software requirements are listed in the Release Notes. The cnMaestro OVA contains the latest software versions at the time of build.


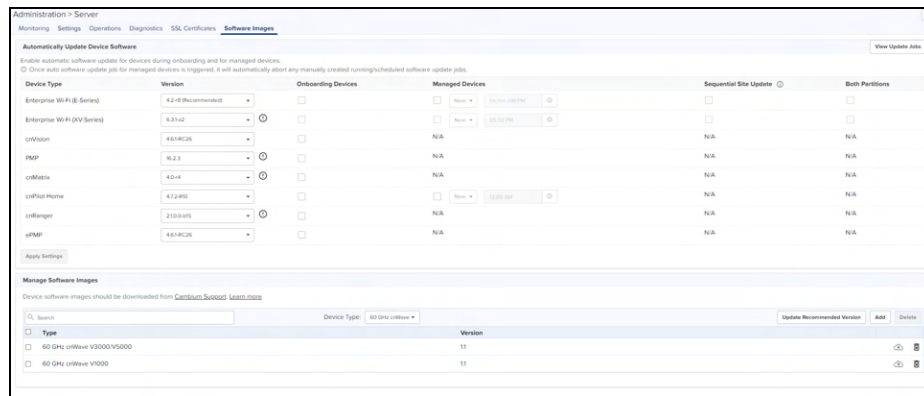
Navigate to **Administration > Server > Software Images**. Select your device type to display the available images, and then click the download icon ().

Figure 1 Device software



Once the device is updated with the correct software version, it can be onboarded.

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

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

If none of these are present, the default action on the device is to access the cnMaestro Cloud URL:

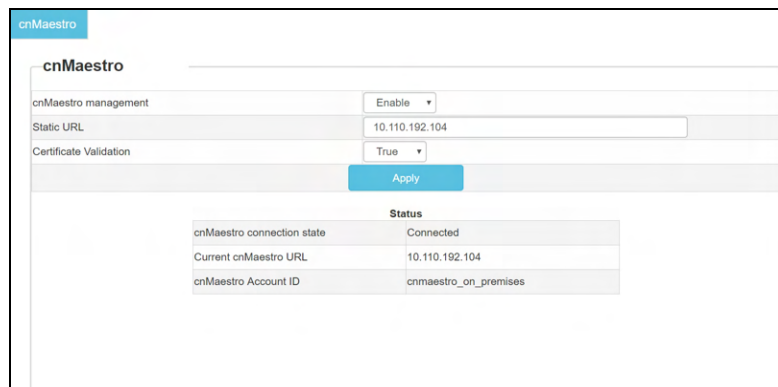
<https://cloud.cambiumnetworks.com>.

Static URL

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

cnMatrix

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

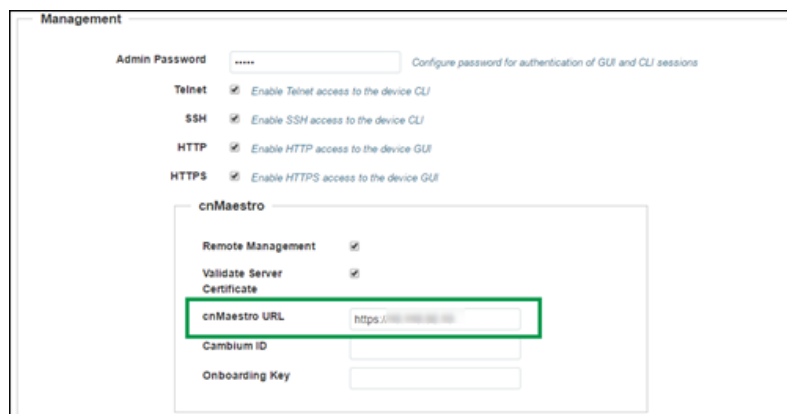


The screenshot shows the 'cnMaestro' configuration page. At the top, there is a 'cnMaestro management' dropdown menu set to 'Enable'. Below it, the 'Static URL' field is populated with '10.110.192.104'. The 'Certificate Validation' dropdown is set to 'True'. An 'Apply' button is visible. Below the configuration fields, a 'Status' section displays the following information:

Status	
cnMaestro connection state	Connected
Current cnMaestro URL	10.110.192.104
cnMaestro Account ID	cnmaestro_on_premises

cnPilot Enterprise

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



The screenshot shows the 'Management' configuration page. Under the 'cnMaestro' section, the 'cnMaestro URL' field is highlighted with a green box and contains the value 'https://10.110.192.104'. Other fields include 'Remote Management', 'Validate Server', 'Cambium ID', and 'Onboarding Key', all with checkboxes or input fields.

cnPilot Home

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

cnMaestro Configuration

Configuration

Remote Management Disable Enable

IPv6 Preferred Disable Enable

Use Management Interface Disable Enable

cnMaestro URL

Connection Status Connected to 10.110.209.84

Credentials

Cambium ID

Onboarding Key

AccountID cnmaestro_on_premises

cnRanger

Setting static URL for cnMaestro on Sierra 800

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

Setting static URL for cnMaestro on Tyndall 101

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

cnReach

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

cnMaestro Remote Management Settings

Status

Remote Management Status: Enabled

cnMaestro URL: https:// 192.168.1.14

State: Connected Force Reconnect

Account ID: cnmaestro_on_premises

Settings

cnMaestro Management:

cnMaestro URL: https:// 192.168.1.14

Cambium ID: cnmaestro_on_premises

Onboarding Key:

2. Click **cnMaestro Management** check box.
3. Enter **cnMaestro URL**.

cnVision Client

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

Cambium Networks | cnVision Client_MICRO Client 192.168.1.14

cnMaestro

Remote Management: Disabled Enabled

cnMaestro URL: qa.cloud.cambiumnetworks.com

Cambium ID: Cambium ID

Onboarding Key:

Account Management

Administrator Account: Disabled Enabled

Installer Account: Disabled Enabled

Home User Account: Disabled Enabled

Read-Only Account: Disabled Enabled

Administrator Account: Username: admin Password:

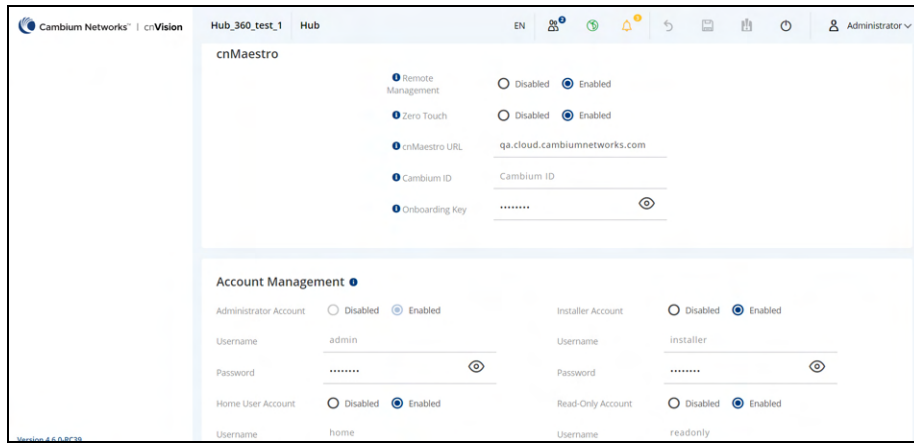
Installer Account: Username: installer Password:

Home User Account: Username: home Password:

Read-Only Account: Username: readonly Password:

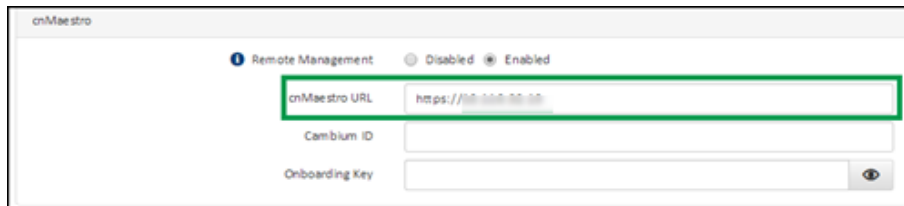
cnVision Hub

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



ePMP 1000 AP/SM

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



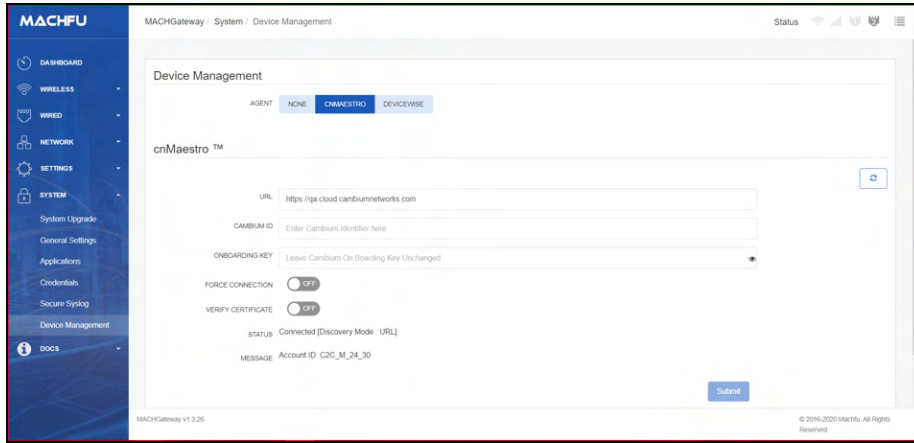
ePMP 1000 Hotspot

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



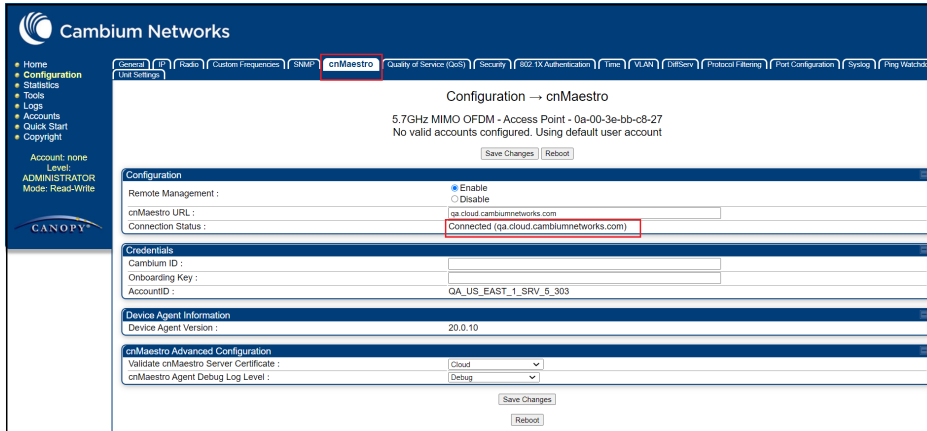
Machfu

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



PMP

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



PMP configuration prerequisites

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

SM (not using NAT)

- LAN 1 network interface should have 'public' accessibility.
- IP address should be public IP address: either static IP address or obtained via DHCP.
- DNS server configuration should be filled: either static IP address or obtained via DHCP.

SM using NAT

- Remote Management interface with standalone config should be enabled.
- Remote Management IP address should be public IP address.
- DNS server should be configured.

AP

- IP address should be public.
- DNS server should be configured.

PTP

1. Navigate to **Installation** and click **run Installation wizard** button.

- In the **Management Configuration** window, under cnMaestro, select **Enabled**.

Management Configuration

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

Management configuration data entry

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

◀ Back
Next ▶

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

Management Configuration

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

Management configuration data entry

Attributes	Value	Units
cnMaestro	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
cnMaestro Server	<input type="radio"/> cnMaestro Cloud <input checked="" type="radio"/> cnMaestro On-Premises	
cnMaestro Server Internet Address	10.110.32.102	
cnMaestro Server Port	443	
Onboarding Method	<input type="radio"/> MAC Address <input checked="" type="radio"/> Cambium ID <input type="radio"/> Auto	
Cambium ID	<input type="text"/>	
Onboarding Key	<input type="text"/>	

◀ Back
Next ▶

DHCP Options (Linux)

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

The following configuration is for Linux-based systems. Refer to [Appendix: Windows DHCP Options Configuration](#) for configuring DHCP options for Windows.

**NOTE:**

DHCP Options are available from the following builds:

- cnMatrix: 2.0.4-r1
- cnPilot e400/e500/e502S/e501S: 3.2.1-r6
- cnPilot e425H/e505: 4.0
- cnPilot e430W/e410/e600: 3.5.2-r4
- cnPilot e510: 3.11.4-r9
- cnPilot e700: 3.7-r9
- cnPilot r190: 4.4.2-R2
- cnPilot r195P: 4.7
- cnPilot r195W: 4.5.2
- cnPilot r200P/r201P: 4.4.2-R2
- cnReach: 5.2.17e
- ePMP 1000, ePMP Force 180/200: 3.1
- ePMP 1000 Hotspot: 3.2.1-r6
- ePMP 2000: 3.0
- ePMP 3000: 4.5
- ePMP Elevate: 3.2
- ePMP Force 190: 3.5
- ePMP Force 300: 4.1
- ePMP PTP 550: 4.1
- Machfu 7.1.2-1.1.0.5
- PMP: 15.0.1
- PTP 650, PTP 670 (650 Emulation): 02-67

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

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

**NOTE:**

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

Using DHCP Option 43

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

The VCI for the individual Cambium products is listed below:

Table 8: VCI (DHCP Option 60)

Product	VCI (DHCP Option 60)
cnMatrix	Cambium-cnMatrix-EX2K
cnPilot r190	Cambium-cnPilot r190
cnPilot r195	Cambium-cnPilot r195
cnPilot r200P	Cambium-cnPilot r200P
cnPilot r201P	Cambium-cnPilot r201P
cnPilot e400/e410/e430W cnPilot e425H/e505 cnPilot e500/e501S/e502S/e510 cnPilot e700/e600	Cambium-WiFi-AP
ePMP	Cambium
ePMP 1000 Hotspot	Cambium-WiFi-AP
PMP 430 SM	Cambium PMP 430 SM
PMP 450 AP	Cambium PMP 450 AP
PTP 450 BHM	Cambium PTP 450 BHM
PMP 450 BHS	Cambium PTP 450 BHS
PMP 450 SM	Cambium PMP 450 SM
PMP 450b SM	Cambium PMP 450b SM
PMP 450i AP	Cambium PMP 450i AP
PMP 450i BHM	Cambium PTP 450i BHM
PTP 450i BHS	Cambium PTP 450i BHS
PMP 450i SM	Cambium PMP 450i SM
PMP 450m APs	Cambium PMP 450m AP

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

```

option option-43 code 43 = string;

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

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

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

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

```

Using DHCP Option 15

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

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

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

UI Navigation

cnMaestro On-Premises provides a number of ways to navigate its content.

This section includes the following topics:

- [Account View](#)
- [Home page](#)
- [Page structure](#)
- [UI Navigation](#)
- [Access and Backhaul View](#)
- [Enterprise View](#)
- [Side menu](#)
- [Section tabs](#)
- [System status](#)
- [Logout](#)



NOTE:

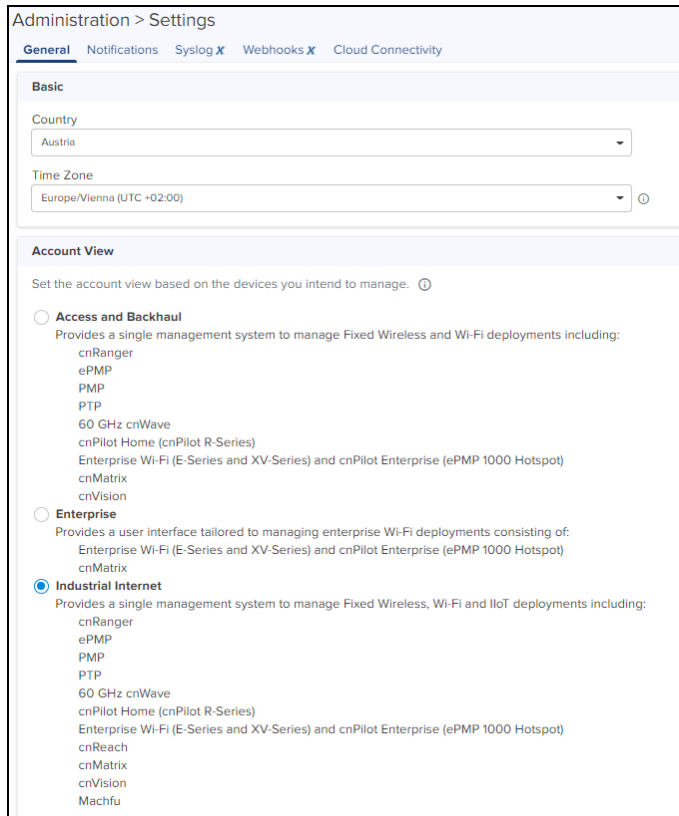
- Only Super Administrator and Administrator can change the Time Zone.
- The Time Zone setting is applicable only for Email Notifications, Webhooks, and RESTful APIs only.

Account View

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

- [Access and Backhaul view](#)
- [Enterprise view](#)
- [Industrial Internet view](#)

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



Access and Backhaul View

The Access and Backhaul View supports all Fixed wireless and Wi-Fi devices. The device types include 60 GHz cnWave, cnMatrix, cnPilot Enterprise (ePMP 1000 Hotspot), cnPilot Home, cnRanger, cnVision, Enterprise Wi-Fi (E-Series and XV-Series), ePMP, PMP, and PTP.

Enterprise View

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

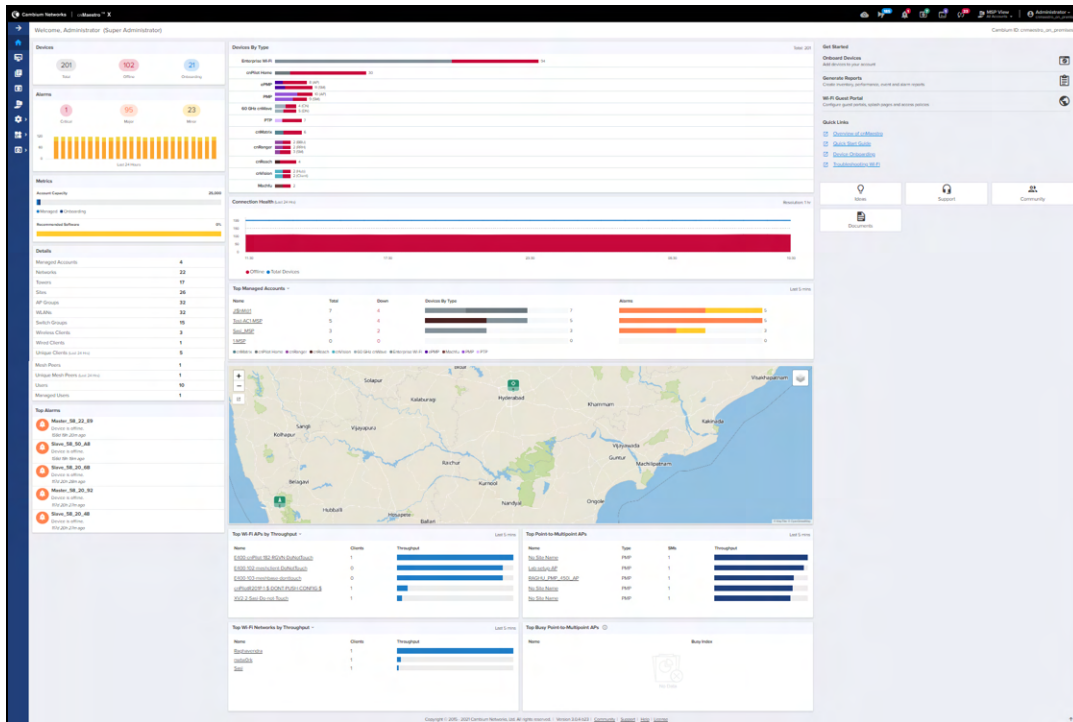
Industrial Internet View

Industrial Internet View provides a interface for Fixed Wireless, Wi-Fi, and cnReach deployments. The device types include 60 GHz cnWave, cnMatrix, cnPilot Home (cnPilot R-Series), cnRanger, cnReach, cnVision, Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) and ePMP.

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**.

Figure 2 cnMaestro On-Premises - Home page



Page structure

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

Figure 3 cnMaestro On-Premises - page structure

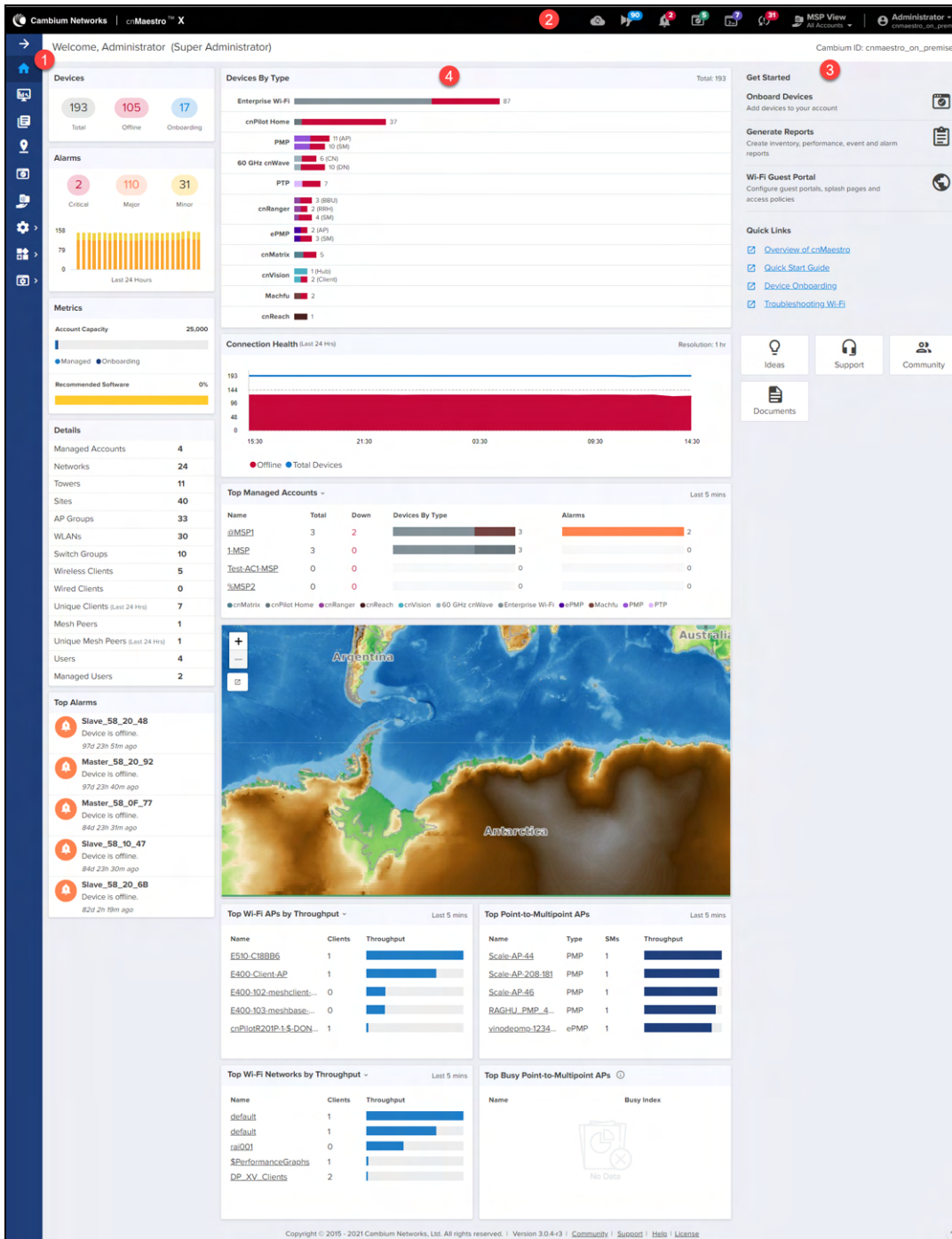


Table 9: UI description

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 Synch Devices.
3	Right menu	Provides links to Cambium Ideas, Support, Community, Documents, and Licensing .
4	Functional area	Shows the detailed view of the section selected in the left menu.

Page navigation

The cnMaestro pages include items such as **Dashboard, Notifications, Configuration, Statistics, Report, Software Update, Map, Clients, and, Mesh Peers.** 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 below.

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.

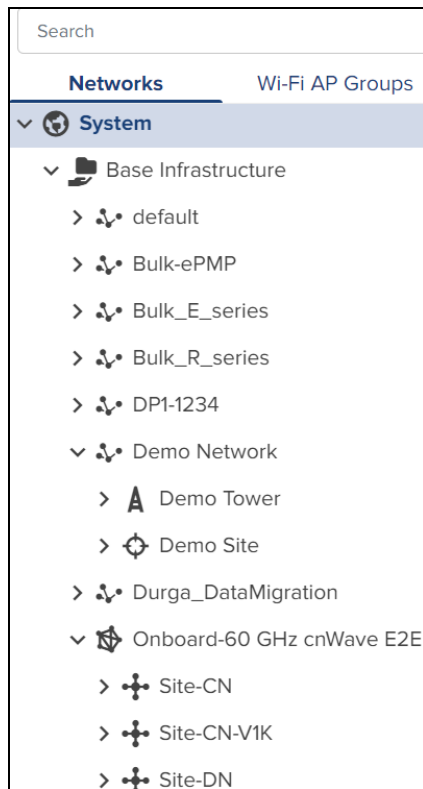
Selecting an arrow icon will expand the node and display the next level of hierarchy.



NOTE:

Opening the node does not automatically select a node in the new hierarchy, instead the desired node needs to be clicked.

Figure 4 Device tree navigation



The structured hierarchy has the following devices:

Table 10: Structured hierarchy nodes

Icon	Name	Description
	60 GHz cnWave CN	CN is mapped to a Site in E2E Network.
	60 GHz cnWave DN	DN is mapped to a Site in E2E Network.
	60 GHz cnWave External E2E Network	60 GHz cnWave devices are located within a Network deployed through the external E2E controller.
	60 GHz cnWave Onboard E2E Network	60 GHz cnWave devices are located within a Network deployed through the Onboard 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 Site	Sites are located within E2E Networks. A site maps to a single area and represents a location on a map that has 60 GHz cnWave devices.

Table 10: Structured hierarchy nodes















Icon	Name	Description
	cnMatrix	cnMatrix devices are located within a Network . Optionally they can also be mapped standalone to a Tower or to a Site .
	cnPilot Home	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 .
	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.
	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 .
	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 .
	Machfu	Machfu devices are located within a Network . Optionally they can also be mapped standalone to a Network or to a Tower .
	Network	All devices are placed within Networks . Networks represents the geographical regions or collections of devices with a shared responsibility. Accounts can have one network or many networks. Networks allow one to provide structure to accounts with many devices and also provides aggregation buckets for cnMaestro On-Premises statistics (essentially the system pre-calculates statistics, so they are displayed quickly).
	PMP AP	Point-to-Multipoint access points are located in a Network and are optionally mapped to a Tower .
	PMP SM	Point-to-Multipoint Subscriber Modules (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.
	PTP Master	Point-to-Point (PTP) Master device located in a network and optionally mapped to a Tower.

Table 10: Structured hierarchy nodes

Icon	Name	Description
	PTP Slave	Point-to-Point (PTP) Slave device located in a network and optionally mapped to a Tower.
	Site	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 show), 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, PTP devices 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.

Default network

cnMaestro On-Premises 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, but it can be renamed.

Tree menu

Each node in the device tree has a menu icon () that supports node-specific actions. For example, the system node lets you **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
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.
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.

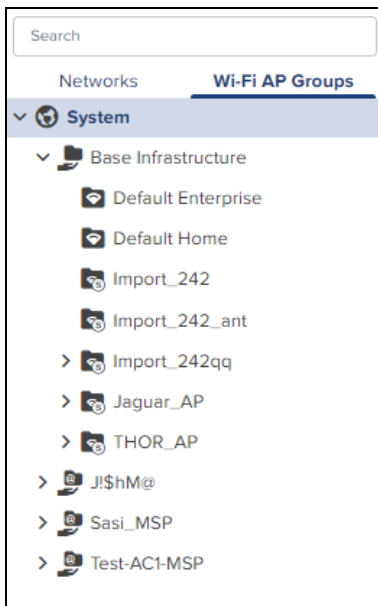
Table 11: Tree menu

Action	Node	Description
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.
60 GHz cnWave Network		
Add Link	Network and Most Nodes	Add a new link to the System.
Add Node	Site	Add a new Node as a child to the Site.
Download PoP (s) Onboarding Config	Network and PoP Nodes	Download PoP(s) Onboarding Configuration data.
Hide or Show Sites		It allows to hide or show sites in E2E Controller Network tree menu.
Replace Node	CN/DN Nodes	Replace Node by changing the MAC address of th faulty node.
Sync Topology	Network	To sync the Topology of E2E Network.
Update Software	Network and Nodes	Allows the user to update the 60 GHz cnWave nodes software.

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 one 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 5 Wi-Fi AP Groups



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.

Figure 6 Map navigation

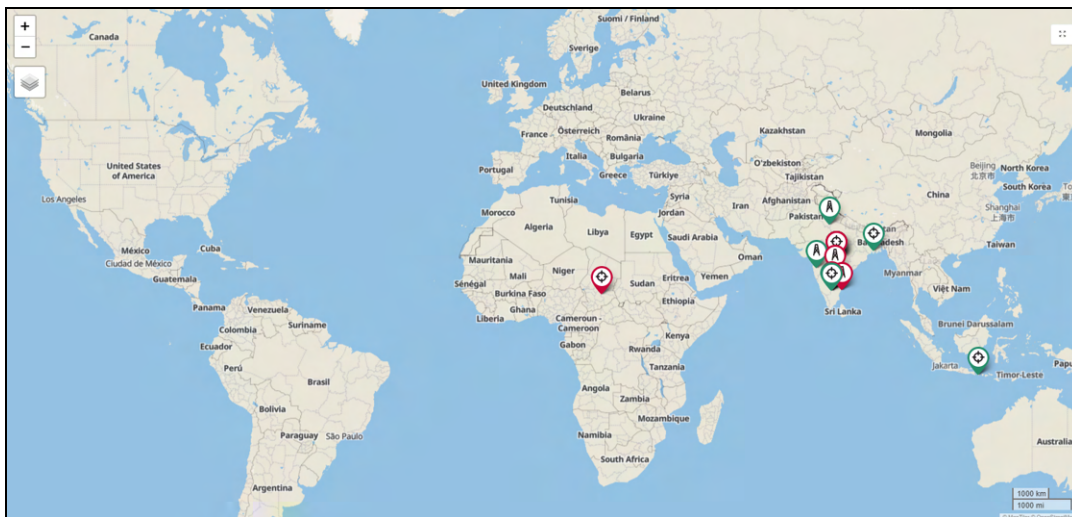


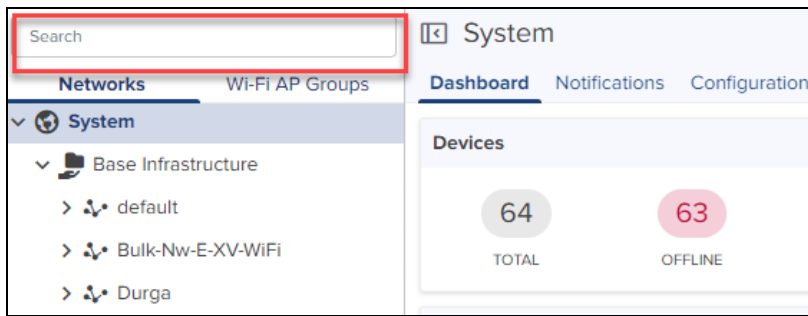
Table navigation

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 7 Node search



Enterprise 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.

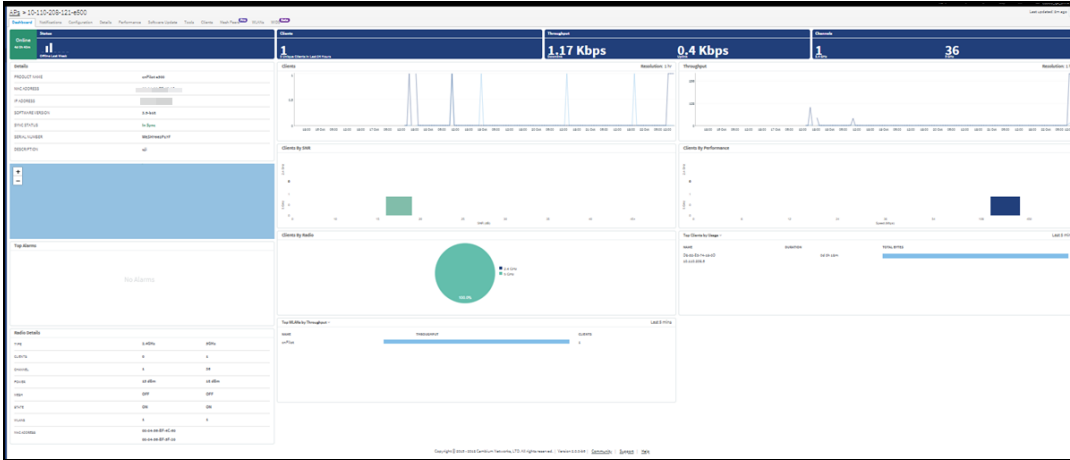
Devices

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

A screenshot of the 'Devices' table in the network management interface. The table has a search bar at the top left and several columns: Device, Health, Onboarding Status, Serial Number, IP Address, Type, AP Group, Tower/Site, and Client Count. The table lists various devices with their respective details. At the bottom right, it shows 'Showing 1 - 10 Total: 12' and navigation buttons for 'Previous', 'Next', and page numbers '1' and '2'.

Device	Health	Onboarding Status	Serial Number	IP Address	Type	AP Group	Tower/Site	Client Count
AP-XV2-2	Offline	Onboarded 77d 9h 50m		10.100.240.48	XV2-2	Jaguar_WLAN_Clients	Jaguar_Clients	1
E800-AF0346	Offline	Onboarded 73d 10h 34m		10.100.202.7	cnPilot e400	Default Enterprise		0
E800-9B8A97	Offline	Onboarded 73d 10h 34m		10.100.202.8	cnPilot e410	Default Enterprise		0
E425H-Edted	Offline	Onboarded 84d 3h 12m		10.100.240.65	cnPilot e425h	N/A	site	0
E500-B14C00	Offline	Onboarded 46d 9h 0m		10.100.240.42	cnPilot e500	N/A	option43-15	0
E500-BE47BC	Offline	Onboarded 89d 3h 21m		10.100.202.21	cnPilot e500	Default Enterprise	E-series	0
E500-cnMaestro1	Offline	Onboarded 84d 3h 12m		10.100.240.36	cnPilot e505	N/A	site	0
E600-027888	Offline	Onboarded 46d 9h 0m		10.100.240.67	cnPilot e600	N/A	option43-15	0
E200-D290C6	Offline	Onboarded 89d 3h 21m		10.100.202.25	cnPilot e700	Default Enterprise	E-series	0
Nisa	Offline	Onboarded 14d 6h 13m		10.100.223.55	cnPilot e400	Rogue-APgroup	usaplle	0

Selecting a device launches its management page.



AP groups and WLANs

AP Groups and WLANs 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 8 AP groups

Name	Type	AP Status	Scope	Clients Now	Clients 24 HR	Throughput (DL/UL)	WLANs	Auto Sync
Leopard_2	Enterprise Wi-Fi	0 of 0 offline	Base Infrastructure	0	0	0 Kbps / 0 Kbps	Z_Leopard	ON
Permanen_Scale_Client_15_70	Enterprise Wi-Fi	0 of 1 offline	Base Infrastructure	0	0	0 Kbps / 0 Kbps	Permanen_Scale_Client	ON
Thor07	cnPilot Home (R-Series)	0 of 1 offline	Base Infrastructure	0	0	0 Kbps / 0 Kbps	Default_Home	OFF
BSeries_1	cnPilot Home (R-Series)	3 of 3 offline	Shared	0	0	0 Kbps / 0 Kbps	BSeries_1	ON
III_ga_wth_load	cnPilot Home (R-Series)	0 of 0 offline	Shared	0	0	0 Kbps / 0 Kbps	III_ga_wth_load	ON
THOR_AP_GAP	Enterprise Wi-Fi	0 of 0 offline	Base Infrastructure	0	0	0 Kbps / 0 Kbps	Thor_wlan_GAP	ON
Jaguar_AP	Enterprise Wi-Fi	1 of 1 offline	Base Infrastructure	0	0	0 Kbps / 0 Kbps	Jaguar_wlan_data_wlan	ON
ABGROUP_210_rs	Enterprise Wi-Fi	0 of 0 offline	Shared	0	0	0 Kbps / 0 Kbps	WLAN_210_rs_Jaguar_wlan...	ON
ABGROUP_200_rs	Enterprise Wi-Fi	2 of 2 offline	Shared	0	0	0 Kbps / 0 Kbps	WLAN_200_rs	ON
data_atc	Enterprise Wi-Fi	1 of 1 offline	Shared	0	0	0 Kbps / 0 Kbps	data_wlan	ON

Figure 9 WLANs

Name	Scope	Type	AP Status	Clients Now	Clients 24 HR	Throughput (DL/UL)
Z_Leopard	Base Infrastructure	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps
Default_Enterprise	Rgwn	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps
Permanen_Scale_Client	Base Infrastructure	Enterprise Wi-Fi	0 of 1 offline	0	0	0 Kbps / 0 Kbps
BSeries_1	Shared	cnPilot Home (R-Series)	3 of 3 offline	0	0	0 Kbps / 0 Kbps
III_ga_wth_load	Shared	cnPilot Home (R-Series)	0 of 0 offline	0	0	0 Kbps / 0 Kbps
Thor_wlan_GAP	Base Infrastructure	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps
Jaguar_wlan	Shared	Enterprise Wi-Fi	1 of 1 offline	0	0	0 Kbps / 0 Kbps
Thor_wlan	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps
WLAN_200_rs	Shared	Enterprise Wi-Fi	2 of 2 offline	0	0	0 Kbps / 0 Kbps
WLAN_210_rs	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps

Sites

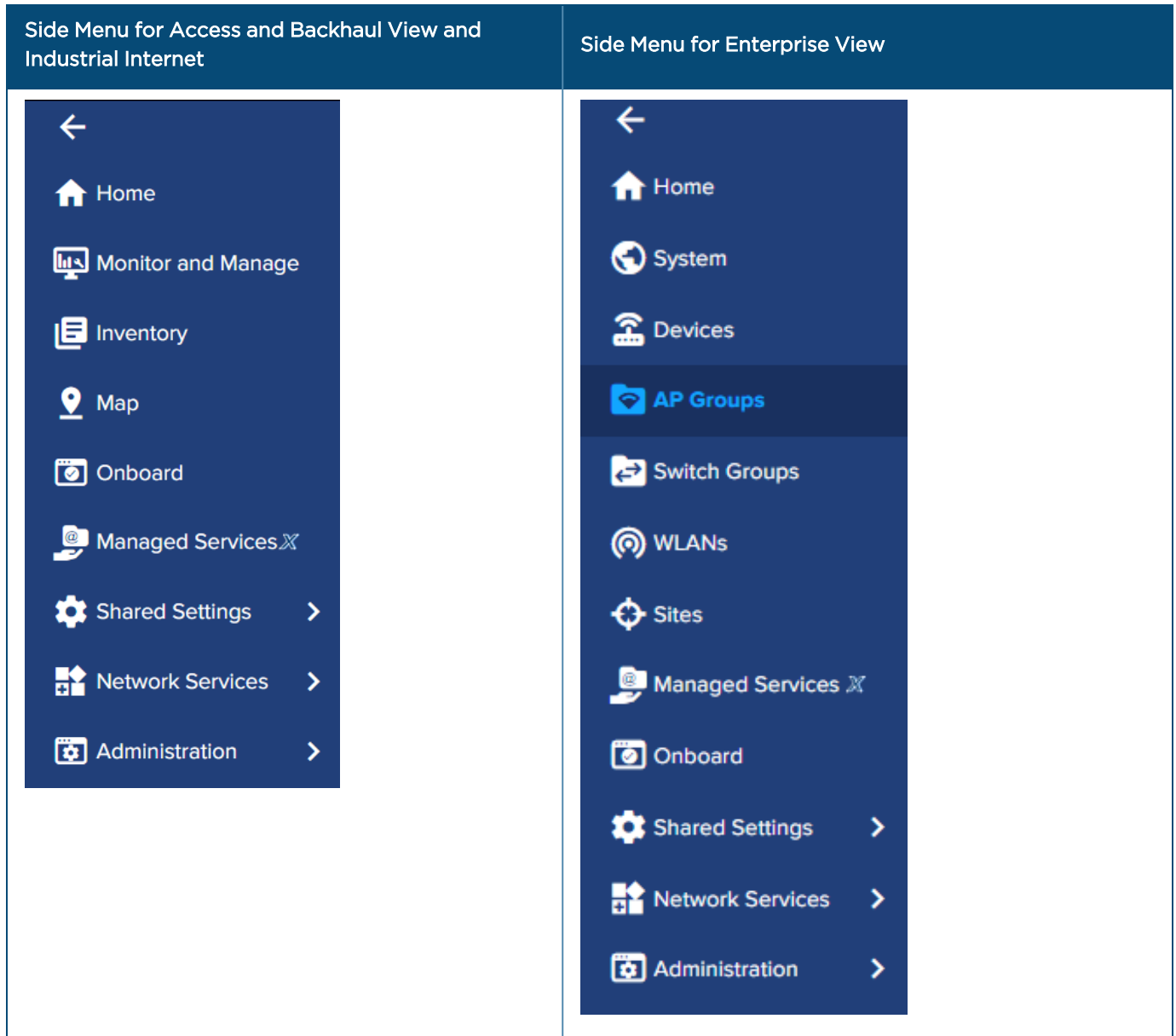
Sites are similar to AP Groups in that they aggregate statistics from many APs. The difference is a site represents APs installed at a single physical location (and mapped to a Floor Plan). Sites also have their own dashboard and aggregation pages.

Side menu

The side menu provides high-level navigation through the cnMaestro UI. You can expand or collapse the menu bar by clicking the arrow icon at the top.

The side menu for the **Access and Backhaul View** and **Industrial Internet** and **Enterprise View** is shown below:

Figure 10 Side menu



Section tabs

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

Table 12: Section tabs

Page	Tabs
System	Dashboard Notifications Configuration Statistics Report Software Update Clients Map Mesh Peers
Site	Dashboard Notifications Configuration Statistics Report Floor Plan APs Clients WIDS Mesh Peers

System status

The UI header has the following System status icons.

Table 13: System status icons

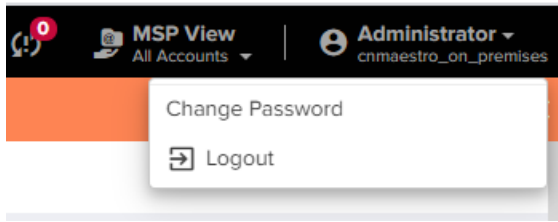
Icon	Name	Description
	Active Software Upgrade Jobs	The number of devices in the onboarding queue that are registered to the account but which need to be manually accepted prior to completing their onboarding.
	Announcements	If cnMaestro Cloud is synced with the On-Premises announcement notifies the latest Device Software images, Package, or OVA to upload from Cloud.
	Cloud Connectivity Status	It notifies that cnMaestro Cloud is Synced or not with the On-Premises.
	Critical Alarms	The count of critical alarms currently raised in the system (if no critical alarms are raised, then the major alarm count will be displayed).
	Devices Waiting for Approval	The count of jobs in the queue. It includes both running and pending jobs.
	Major Alarms	The count of major alarms currently raised in the system.
	Out-of-Sync Devices	The number of Wi-Fi devices with unsynchronized configuration (which can occur when automatic synchronization is disabled in the AP Group, or the configuration is changed directly on the device).

Clicking the icons directs the user to the relevant management page.

Logout

Log out of cnMaestro by clicking on the user icon in the upper-right corner and selecting **Logout**.

Figure 11 Logout



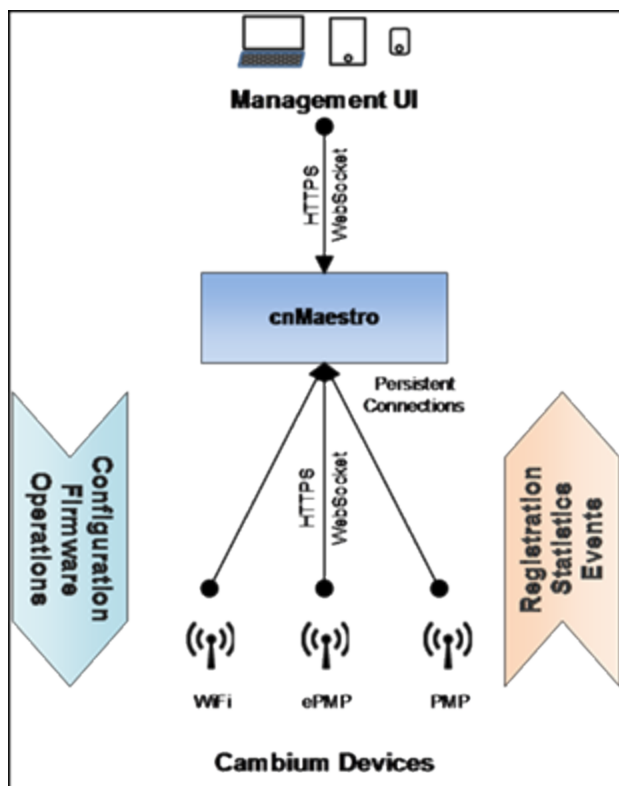
Architecture

Overview

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

In cnMaestro On-Premises, devices must be configured to contact the cnMaestro instance (by default, they access cloud.cambiumnetworks.com). This can be done either by configuring the device through its UI, or by setting DHCP Options (described in the [Appendix](#)).

Figure 12 On-Premises architecture



Networking

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

**NOTE:**

1. Devices must have a route to the cnMaestro On-Premises server.
2. A static IP address or hostname for cnMaestro server, so it will persist over time.
3. An outbound connection from the device must be allowed for port 443.
4. An outbound connection will also be required for port 80 for legacy software on some devices. If your devices are running an image older than the one listed below, outbound connectivity over port 80 is needed for software update. The versions listed (and later) support port 443.
 - 60 GHz cnWave (External Controller) 1.0.1
 - 60 GHz cnWave (Onboard Controller) 1.0.1
 - cnPilot E-Series / ePMP 1000 Hotspot: 3.2.1-r6
 - cnPilot R-Series: 4.4.2-R2
 - cnRanger 1.0.1.0-r1
 - cnReach: All versions
 - Enterprises Wi-Fi 6 APs: 6.0
 - ePMP: 3.2
 - PMP: 15.0.1
 - PTP: All versions

Device Onboarding

Overview

By default, all devices contacting cnMaestro On-Premises will be placed in the Onboarding Queue, where they persist until Approved (after which they become Managed). The Onboarding Queue (**Onboard > Devices**) is shown below.

Figure 13 Onboarding Devices

Type	Serial Number	Device	Managed Account	IP Address	Managed Account	Added By	Status	Duration	Configure
cnReach BHS		cnReach_PTP_EP		10.10.208.38	Base Infrastructure	Unspecified	Waiting for Device	5d 13h 57m	Approve Delete
cnPilot e500		Sesi-E500-BBB484		10.10.208.16	Base Infrastructure	Unspecified	Waiting for Device	8d 21h 51m	Approve Delete
#PMP Force 300-19 AP		F300-LinkS-AP123		10.10.212.60	Base Infrastructure	Administrator Using Cambium ID	Waiting for Appro...	2d 20h 18m	Approve Delete

Onboarding devices is different between On-Premises and Cloud.

- In On-Premises, when a device contacts cnMaestro, it is placed in the Onboarding Queue by default, from which it can be approved into the account.
- In Cloud, the user needs to enter the serial number (MSN) of the device to claim it through the **cnMaestro UI**, or enter the Cambium ID and the Onboarding Key to claim it through the **Device UI**.

60 GHz E2E Controller Onboarding

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

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

Network Name	Management Address	IPv6 Address	Deployment	E2E Controller Version	Status
Onboard-60 GHz cnWave E2E	10.110.178.11	fd00:ba5e:0088:30ff:88:30ff	Running Onboard	1.0.1-dev171	Onboarded



NOTE:

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

Refer [60 GHz E2E Controller Onboarding](#) chapter for details on how to onboard E2E devices.

Pre-Configuration and Approval of Devices (Optional)

To preemptively configure and approve devices when they access cnMaestro, add the MAC address of the device to the **Onboard > Settings**. Adding devices here places them in the Onboarding Queue, where they can be pre-configured and/or pre-approved.

If this step is not done, the devices automatically show up in the Onboarding Queue, where they can be approved.

Figure 14 Pre-Configuration and Approval of Devices

Type	Serial Number	Device	MAC	IP Address	Managed Account	Added By	Status	Duration	Configure
cnReach BHS		cnReach_PTP_EP		10.10.208.38	Base Infrastructure	Unsolicted	Waiting for Device	5d 13h 57m	Force Onboard
cnPilot e500		Sasi-E500-88B484		10.10.208.16	Base Infrastructure	Unsolicted	Waiting for Device	8d 21h 51m	Force Onboard
ePMP Force 300-19 AP		F300-Link5-API23		10.10.212.60	Base Infrastructure	Administrator Using Cambium ID	Waiting for Appro...	2d 20h 18m	Force Onboard

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

Type	Serial Number	Device	MAC	IP Address	Managed Account	Added By	Status	Duration	Configure
cnPilot e600		E600-A65E28			MSP-Account-User	Administrator	Updating	0d 0h 6m	Force Onboard

Device Authentication

To require devices to authenticate with cnMaestro before they are added to the Onboarding Queue, enable Cambium ID based authentication at **Onboard > Settings**. During configuration, the Onboarding Key must also be created. Each user can have their own Onboarding Key. The Onboarding Key needs to be entered into the Device UI before cnMaestro allows it into the Onboarding Queue.

NOTE: When Cambium ID authentication is enabled, the Device UI requires both a Cambium ID and an Onboarding Key. For cnMaestro On-Premises, the Cambium ID is ignored. This mechanism is optional, and it should only be used to force device authentication before adding to the Onboarding Queue.

Figure 15 Device Authentication

Cambium ID: cnmaestro_on_premises

Enable Cambium ID based authentication to onboard devices

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

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

User: Administrator	Onboarding Key:	Delete
User: super user	Onboarding Key:	Delete

Save Cancel Add New

Claiming the Wi-Fi Devices from AP Group

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

1. Navigate to the **Wi-Fi AP Groups** tree view and click the drop-down menu for the selected **AP Group**.
2. Click the **Claim Devices** option.

3. Select the **Device Type**, **Network** and **Site** under which these devices should be placed. By default, the devices claimed will have the configuration settings as the AP Group.

Claim Enterprise Wi-Fi Devices

Enter the ESN (Ethernet MAC) of the devices you would like to add to your account (comma-separated or one per line).

Managed Account: Base Infrastructure

Device Type: Enterprise Wi-Fi

Network: default

Site: None

Enterprise AP Group: Default Enterprise

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

Import .csv

Claim Devices Cancel Clear



NOTE:
In Network and Site the **Search** option is enabled.

4. Specify the MAC Address of the devices line-by-line or comma-separated, or click **Import .csv** to import the MAC addresses of the device from a file.
5. Click **Claim Devices** to add to the selected AP Group with the configuration applied.

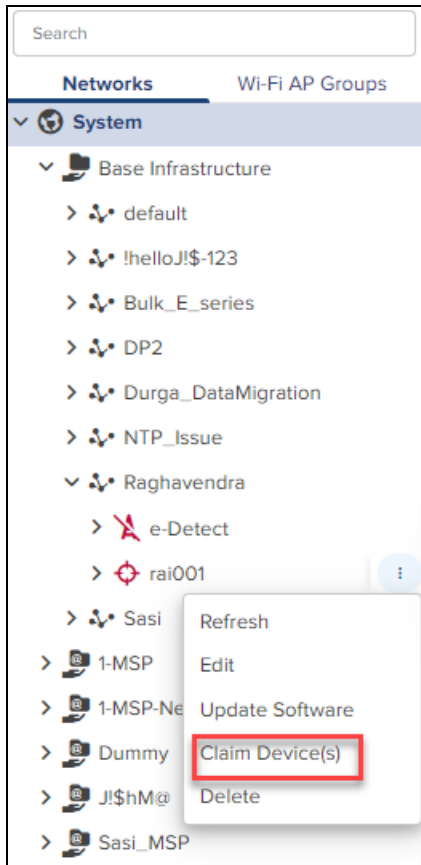


NOTE:
In cnMaestro Cloud the procedure is same as On-Premises, but instead of MAC Address, the user enters the MSN of the device.

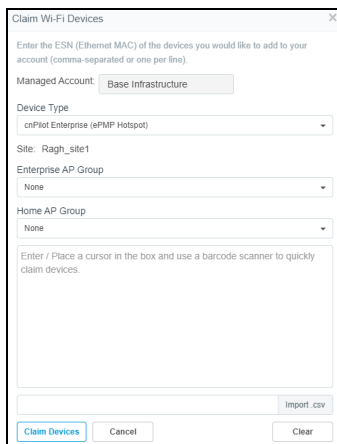
Claiming the Wi-Fi Devices from Site Dashboard

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


1. Navigate to **Manage > Networks** tree view and select the drop-down menu for the Site.
2. Click **Claim Devices** from the drop-down.



3. Select the AP Group that should be applied for cnPilot E (Enterprise) and R (Home) devices. The devices claimed under the Site will have the configuration settings from the selected AP Group.



4. Specify the MAC Address of the devices line-by-line or comma-separated, or use the **Import .csv** option to import the MAC of the devices from a file.
5. Click **Claim Devices** to add the devices to the selected AP Group and **Apply Configuration**.

	<p>NOTE: In cnMaestro Cloud, the procedure is the same as On-Premises, but instead of MAC Address the user should use the MSN of the device.</p>
---	---

60 GHz E2E Controller Onboarding

Overview

There are two ways to deploy 60 GHz E2E Controller:

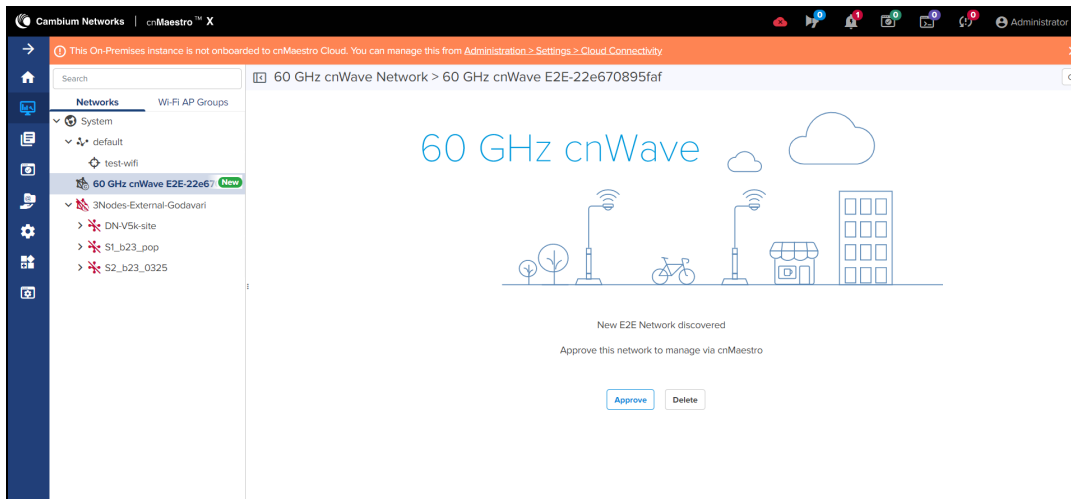
- External E2E Controller
- Onboard E2E Controller

External E2E Controller

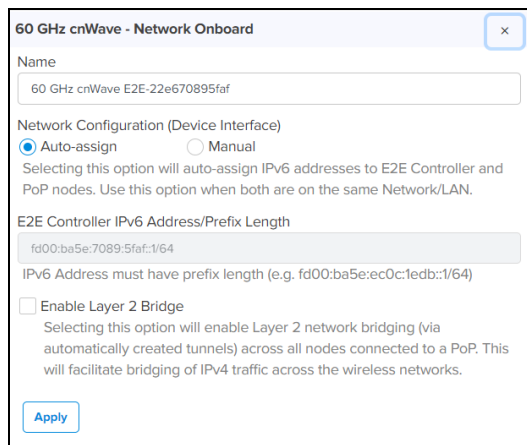
External E2E Controller is an OVA file which can be deployed in ESXi or VMware. The External E2E Controller discovers cnMaestro after it is deployed and ready.

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

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

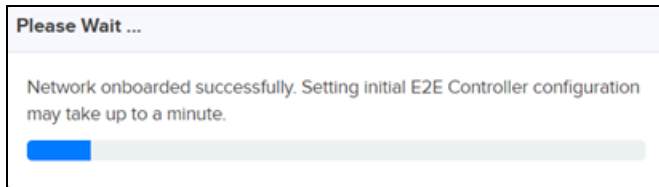


60 GHz cnWave – Network Onboard window pops up.

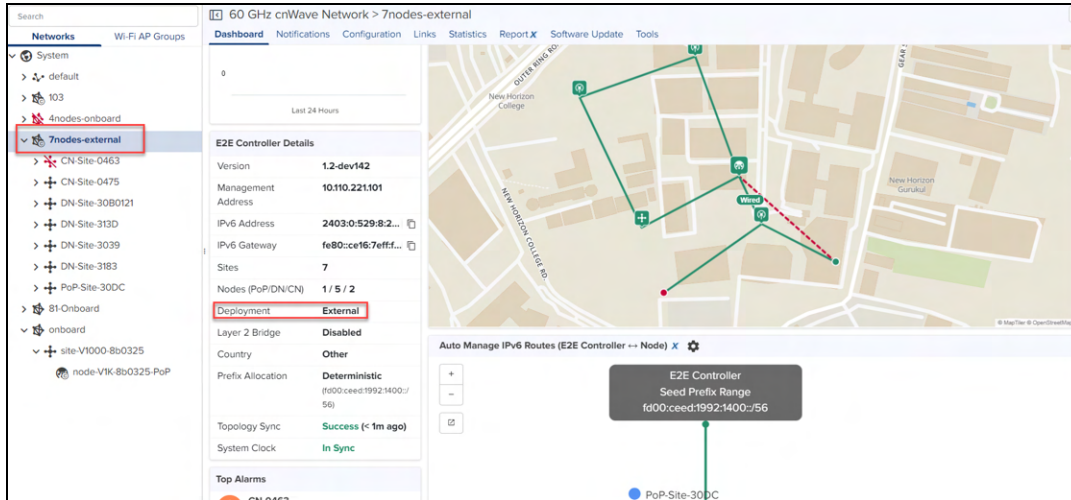


3. By default **Auto-assign** is selected however, the user can select **Auto-assign** or **Manual** to update the IPv6 address in the E2E Network. It takes a while for the IPv6 address to update (after which, the user can optionally **Enable Layer 2 Bridge**).
4. Click **Apply**.

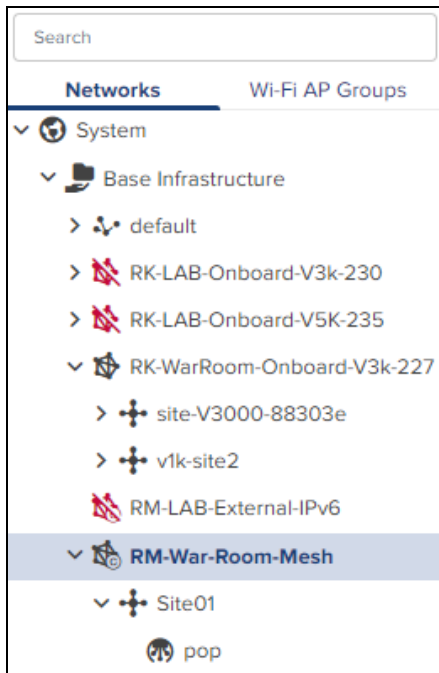
5. Wait until the network onboard completes.



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



External E2E Controller network icon will be displayed .

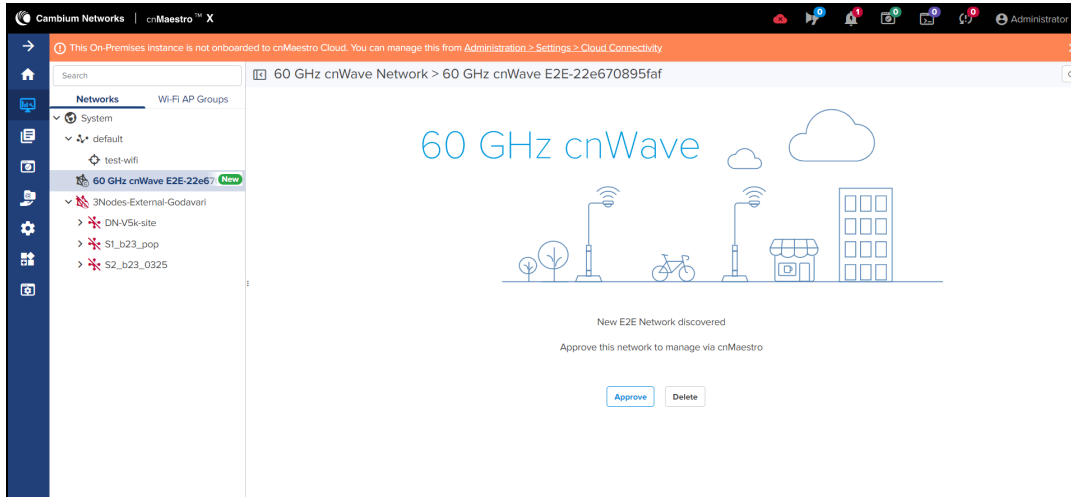


Onboarding E2E Controller

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

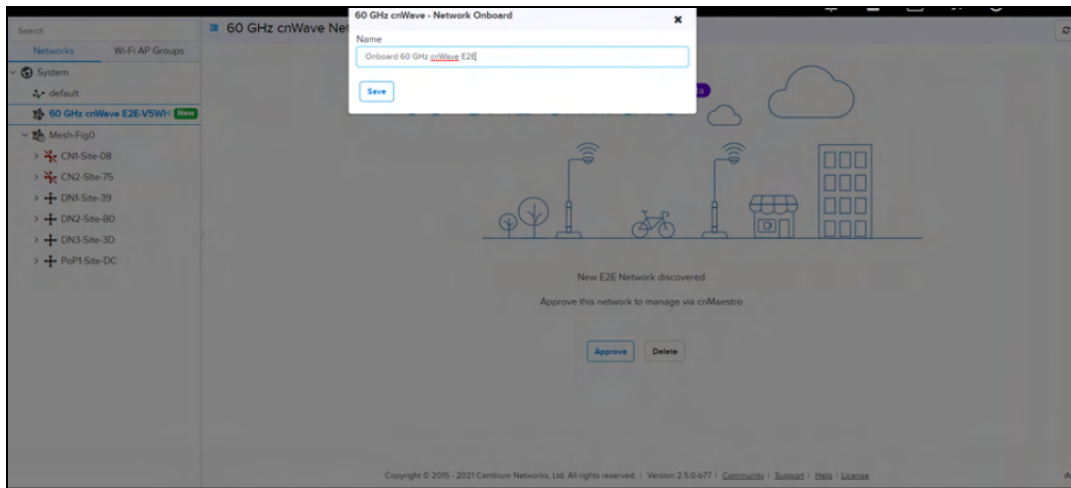
To approve, proceed as follows:

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

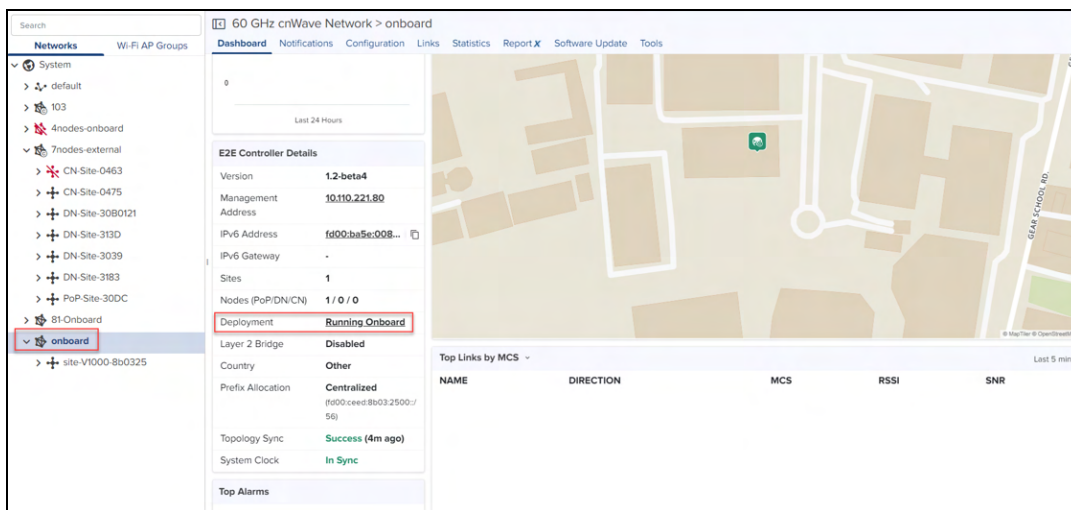



60 GHz cnWave-Network Onboard window pops up and provides option to **Edit** Network name.

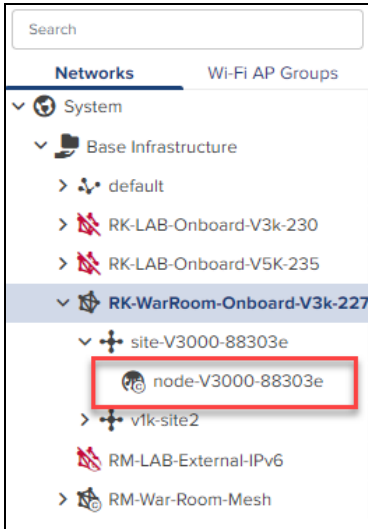
3. Click **Save**.



4. After the successful Onboard E2E Network, it can be managed through cnMaestro. The E2E Network **Dashboard** for an Onboard Controller is shown below:



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



High Availability (HA)

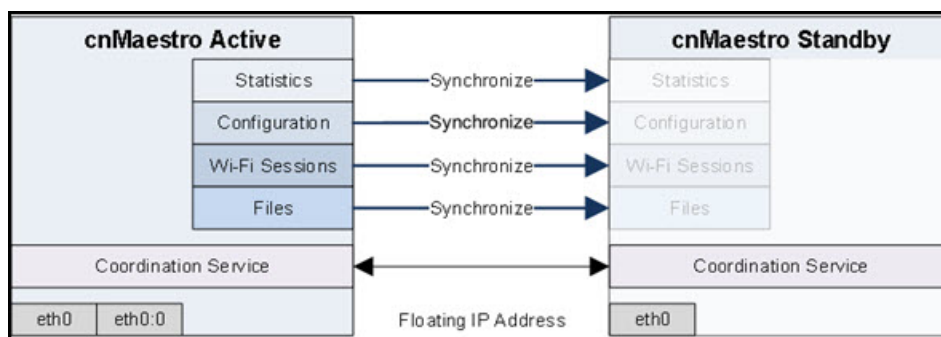
This section includes the following topics:

- [Overview](#)
- [HA Cluster Setup](#)
- [HA Menu](#)

Overview

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

Figure 16 Overview of High Availability



Primary vs Secondary

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

Shared (Floating) IP Address

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

Network Ports

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

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

Recommendations

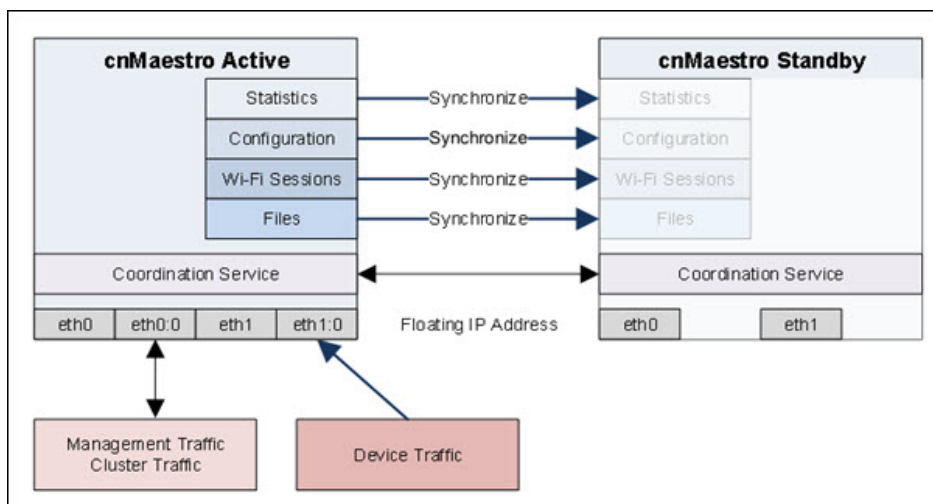
Cambium Networks recommends backing up virtual machines prior to starting HA. To take daily automated backups of cnMaestro configuration, navigate to **Administration > Server > System Backup and Restore**. For larger installations, and to backup statistics, refer section on backing up the data disk.

Dual Interfaces

cnMaestro can be configured with two interfaces, eth0 and eth1, on VMware workstation and ESXi. This allows traffic to be segmented into Management/Cluster and Device/Control. Starting with 3.1.0 release, this traffic separation will be strictly enforced. The implementation allows deployments with separate management and control subnets to integrate more easily with cnMaestro.

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

A high-level overview of the separation is below:



Add eth1 Network Adapter

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

Network Interface PCI Ordering

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

VMware Workstation

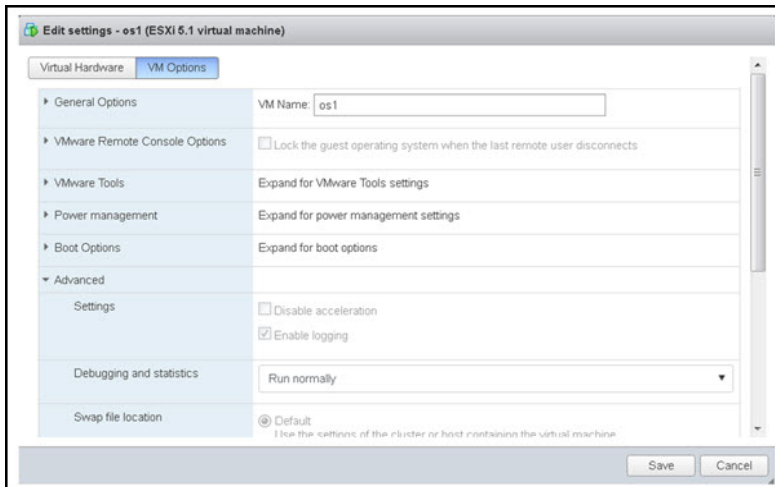
In VMware Workstation, edit the configuration file (ending in .vmx) in the virtual machine home directory. After shutting down the VM, change the following two entries, so the eth0 PCI number is lower than eth1.

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

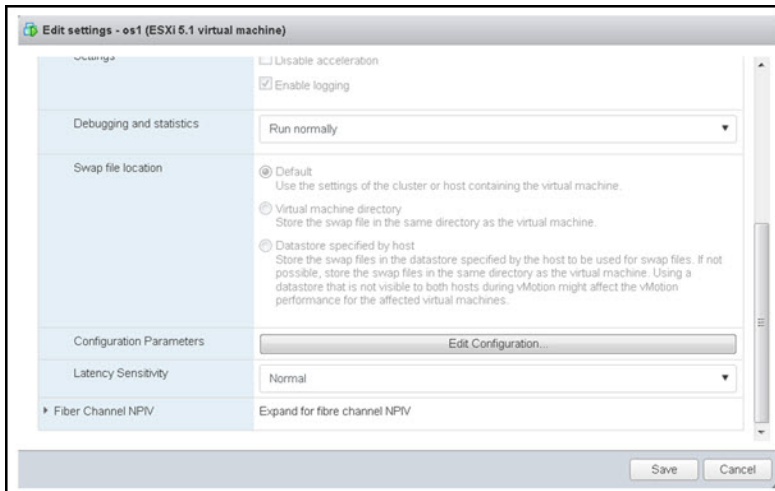
VMware ESXi

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

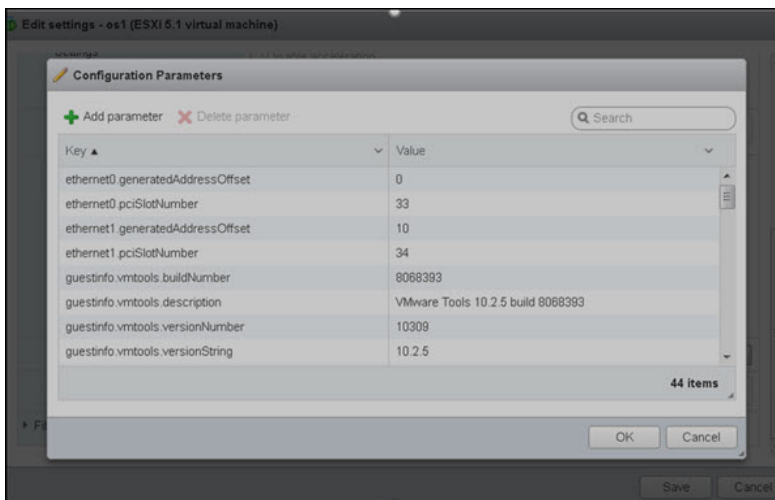
1. Select **Edit Settings** of the VM and choose **VM Options > Advanced**.



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



This launches a screen that allows updating the PCI numbers.



HA Cluster Setup

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

Bootstrap (Primary)

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

Accept (Primary)

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

Join (Secondary)

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



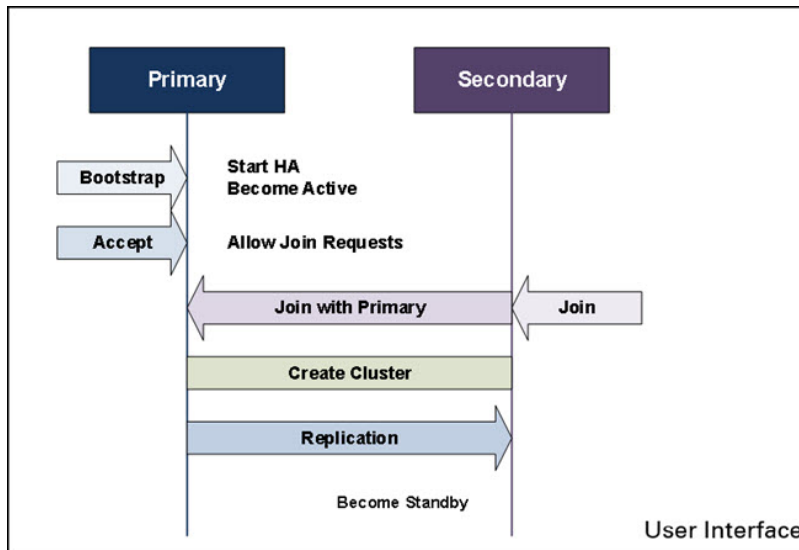
	<p>NOTE: The Join process uses SSH (port 22) to connect to the Primary. It is important to review the fingerprint displayed during the Accept and Join operations, to make sure they are the same (and protect against man-in-the-middle attacks).</p>
	<p>WARNING: All data on the Secondary will be overwritten during the operation.</p>

Figure 17 Accept Join

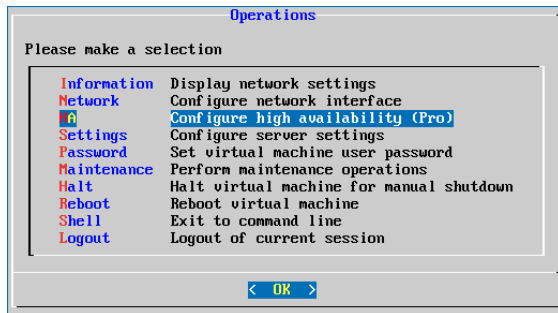


Basic HA Cluster Creation Flow

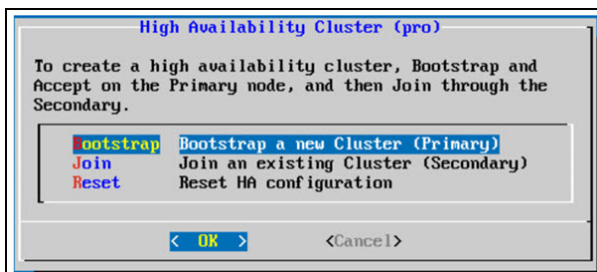
A general HA configuration flow is presented below. Each page will be discussed independently in later sections.

Primary Server

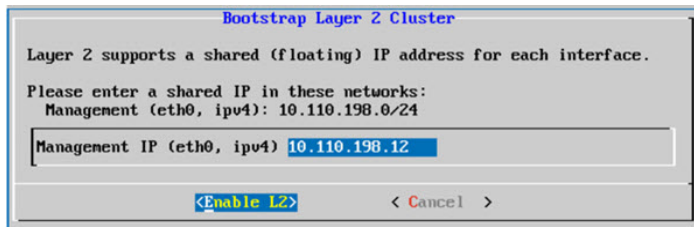
1. After logging into cnMaestro console, from **Operations** tab, select **HA** and click **OK**.



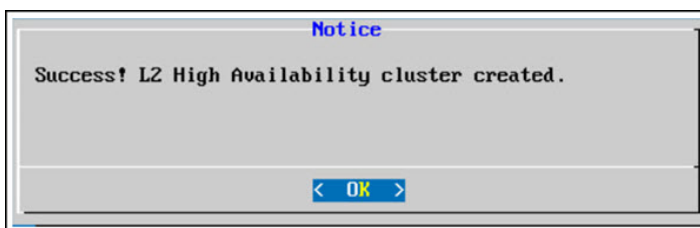
2. From **High Availability Cluster** tab, select **Bootstrap** and click **OK**.



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



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



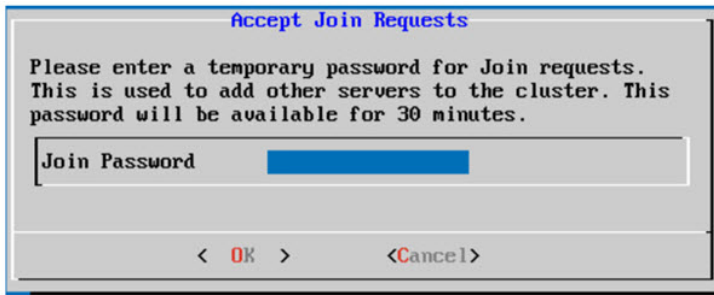
The Primary Bootstrap is successfully completed.

4. Click **OK**.

Accept Join Requests page displays.

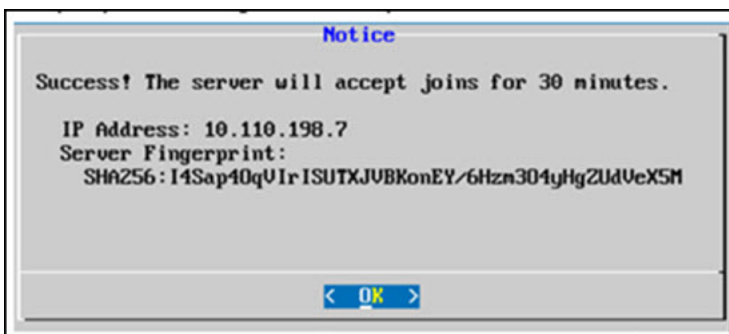
5. Enter a temporary password for Join requests.

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



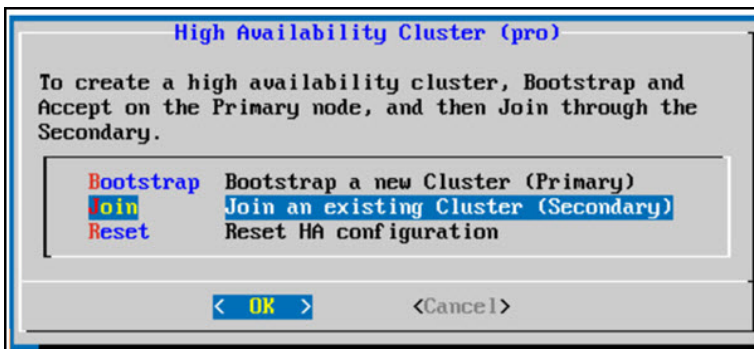
6. After the **Join Password** is set, click **OK** to initialize the system for 30 minutes.

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

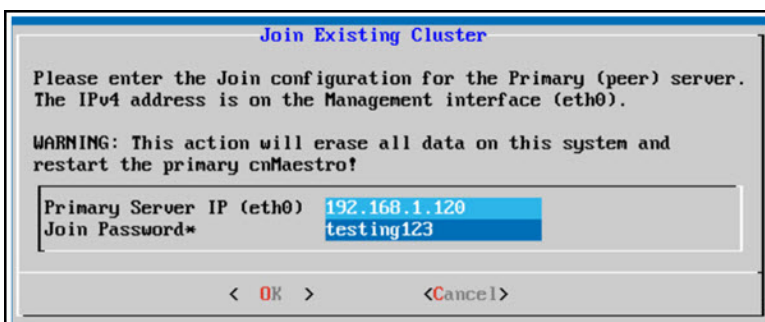


Secondary Server

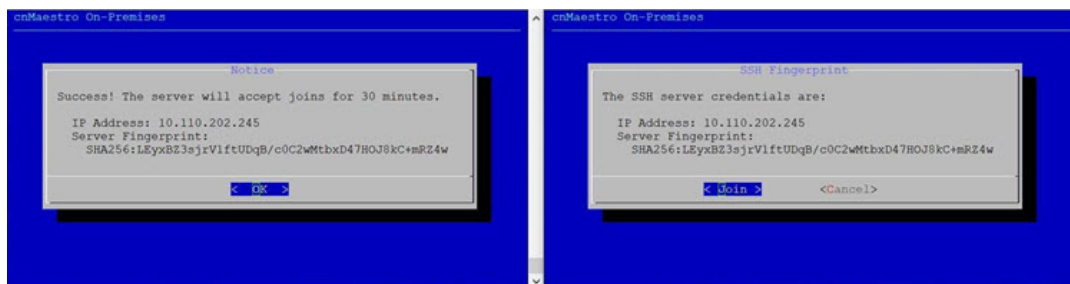
1. On the Secondary cnMaestro server, from the **High Availability Cluster** menu, select **Join** and click **OK**.



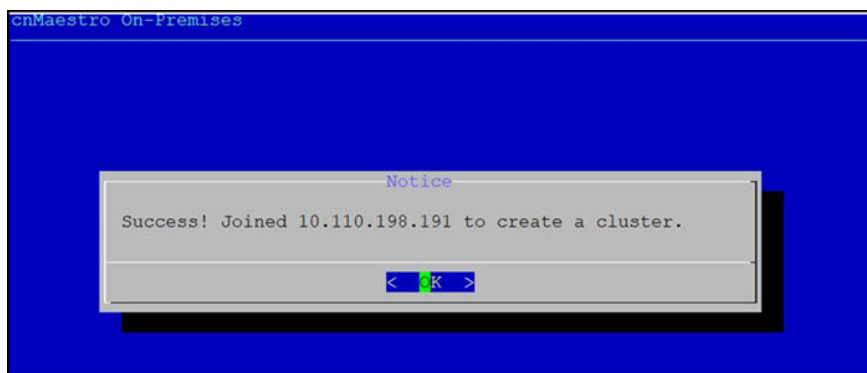
2. **Join Existing Cluster** window appears. Enter the **Primary Server IP (eth0)** and the **Join Password**, click **OK**.



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



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

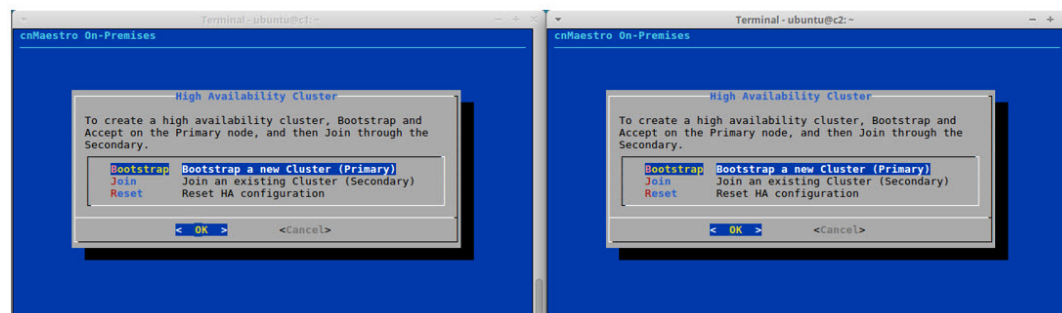


HA Menu

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

High Availability Cluster Menu (Pre-Bootstrap)

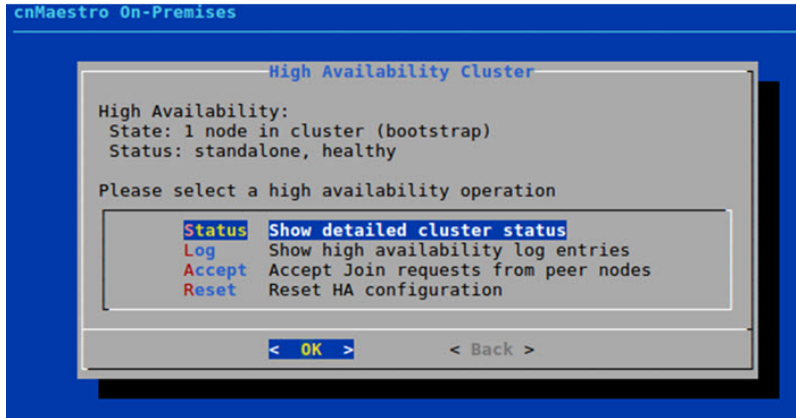
This menu is available before HA is enabled and the cluster has been created.



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

High Availability Menu (Post-Bootstrap)

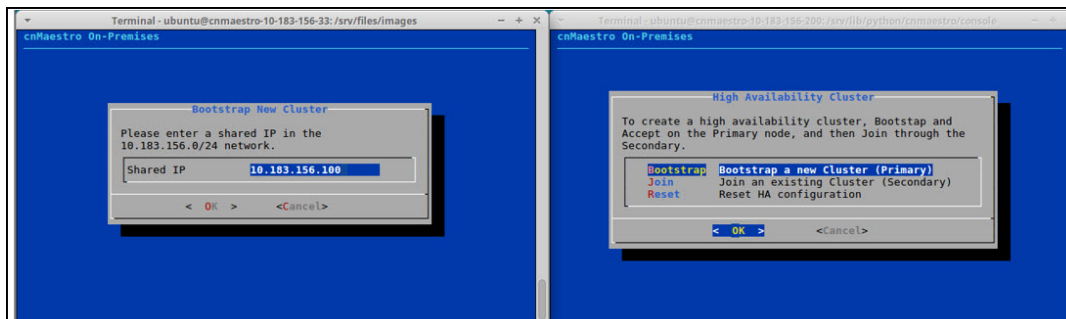
This menu is available after a successful Bootstrap.



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

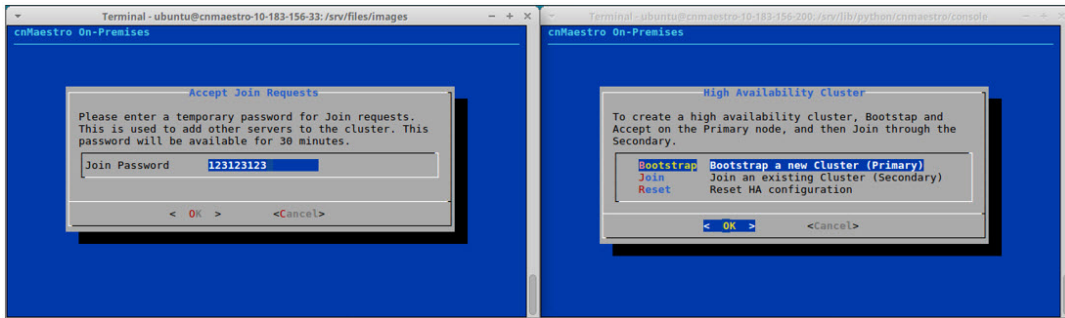
New Cluster

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



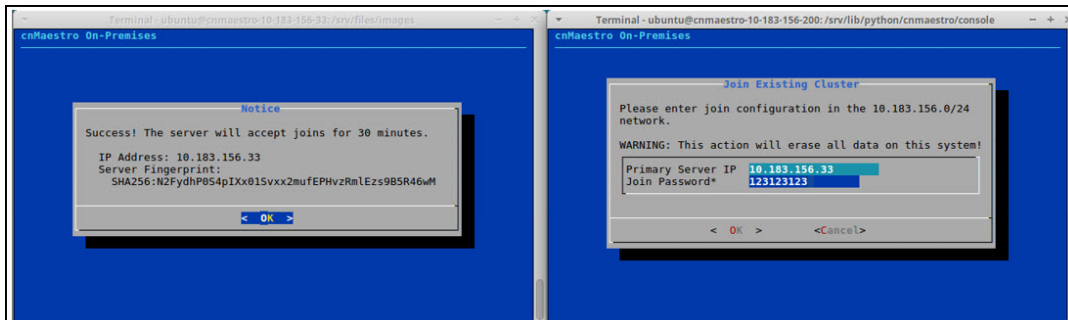
Accept Join Requests

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



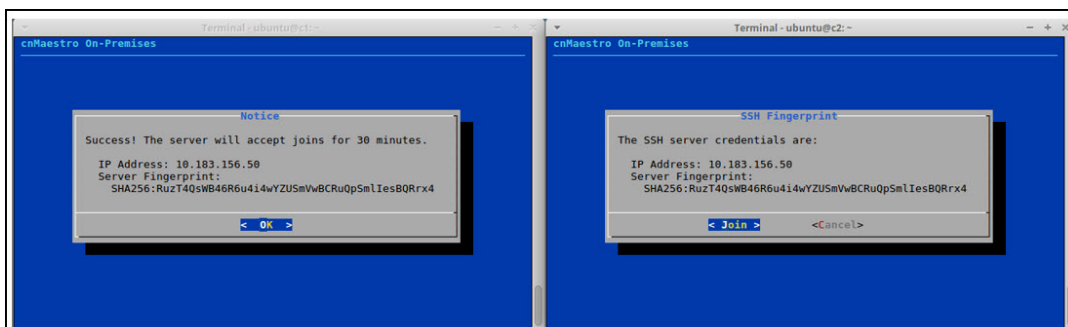
Join Existing Cluster

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



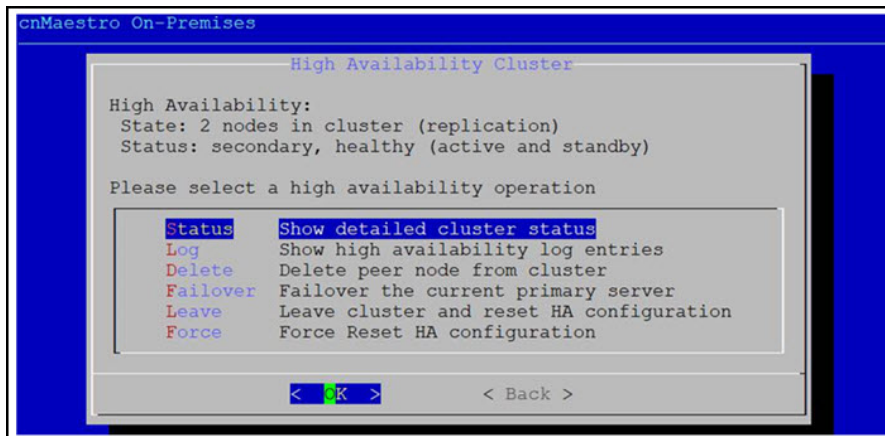
Validate SSH Fingerprints

Customers should validate the fingerprint before joining. If the fingerprint on the Primary is different than the fingerprint displayed at the Secondary, the Join should be cancelled, because the Primary server is incorrect. In the graphic below, the Primary server is on the left, and the Secondary server is on the right.



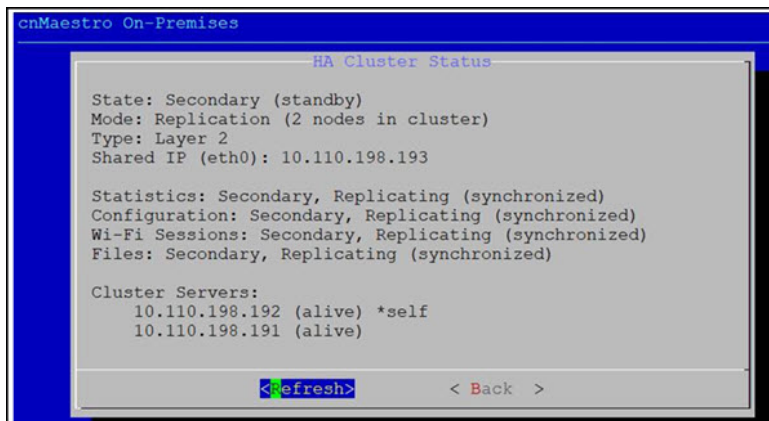
HA Cluster Status

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



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

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



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

```

HA Cluster Status

State: Primary (active)
Mode: Replication (2 nodes in cluster)
Shared IP: 10.110.134.227

Statistics: Primary, Replicating (lag: 0 seconds)
Configuration: Primary, Replicating (lag: 0 bytes)
Wi-Fi Sessions: Primary, Replicating (lag: 0 bytes)
Files: Primary, Replicating (lag: 0 files)

-- --
HA Cluster Status


State: Secondary (standby)
Mode: Replication (2 nodes in cluster)
Shared IP: 10.110.134.227

Statistics: Secondary, Replicating (lag: 0 seconds)
Configuration: Secondary, Replicating (lag: 0 seconds)
Wi-Fi Sessions: Secondary, Replicating (lag: 0 bytes)
Files: Secondary

Cluster Servers:
 10.110.134.226 (alive) *self
 10.110.134.225 (alive)

<Reload> <Cancel>

```

	<p>NOTE: There may be discrepancy in the Primary and Secondary lag values it may display the results in bytes or seconds.</p>
---	--

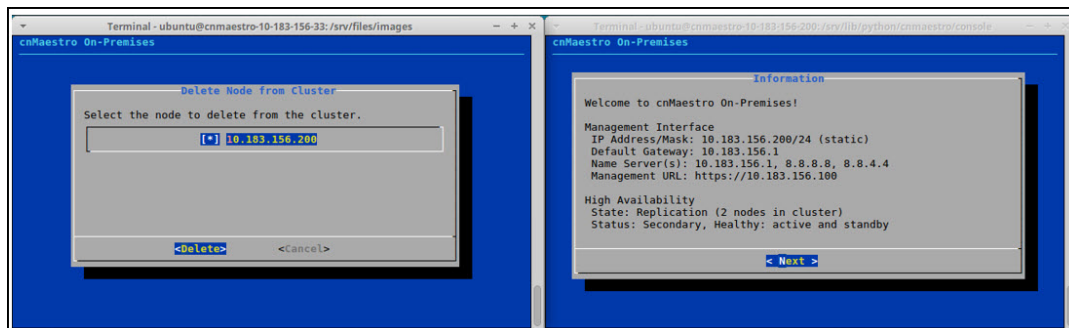
Delete Node

Delete from Cluster

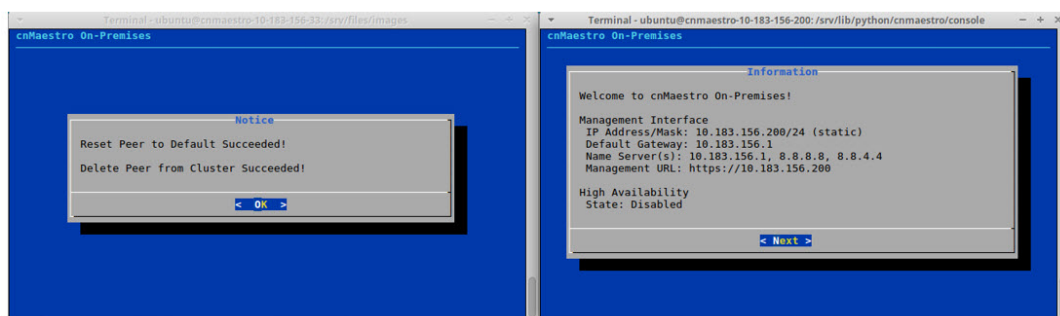
Deleting removes the peer node from the cluster. Navigate to **Operations > HA**, select **Delete** and click **OK**.

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

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



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



NOTE:

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

Leave Cluster

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

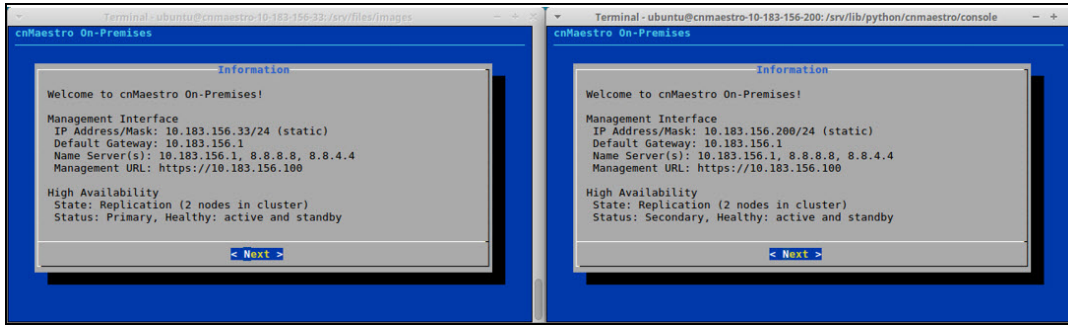


NOTE:

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

Information

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



Behaviour of cnMaestro features when HA is Enabled

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

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

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

Monitoring

This section includes the following topics:

- Network Monitoring
- cnPilot Dashboard
- Inventory
- Reports

Network Monitoring

The Monitoring tab displays the monitoring panel for cnMaestro On-Premises. This includes the following sections:

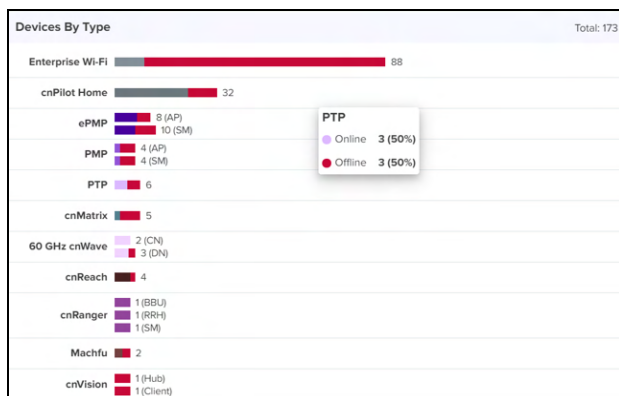
- Dashboard
- Notifications
- Statistics and Details
- Performance
- Maps
- Tools
- WIDS

Dashboard

Dashboard pages are 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 aggregates dashboard data for the devices they contain.

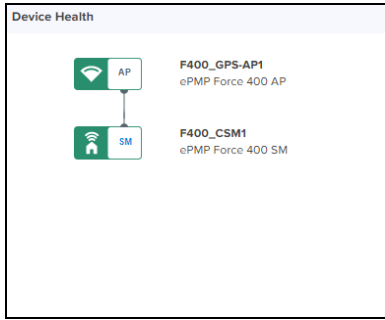
KPI (Key Performance Indicators)

Each page has a set of KPIs tailored to the node type. These displays a current value and often historical trend data.



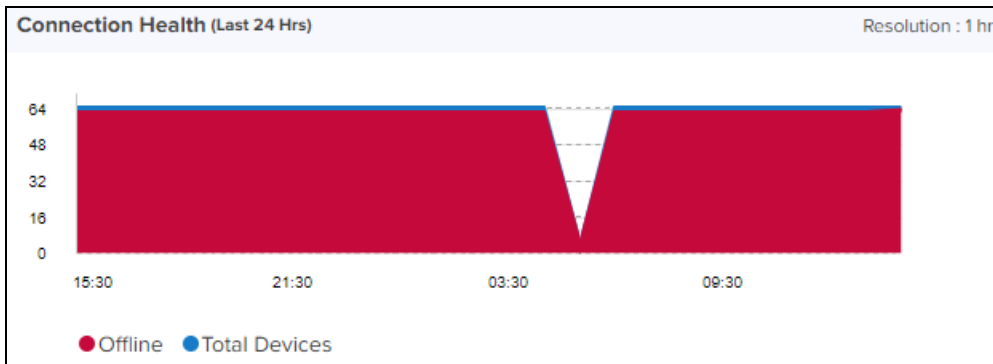
Device Health

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



Connection Health

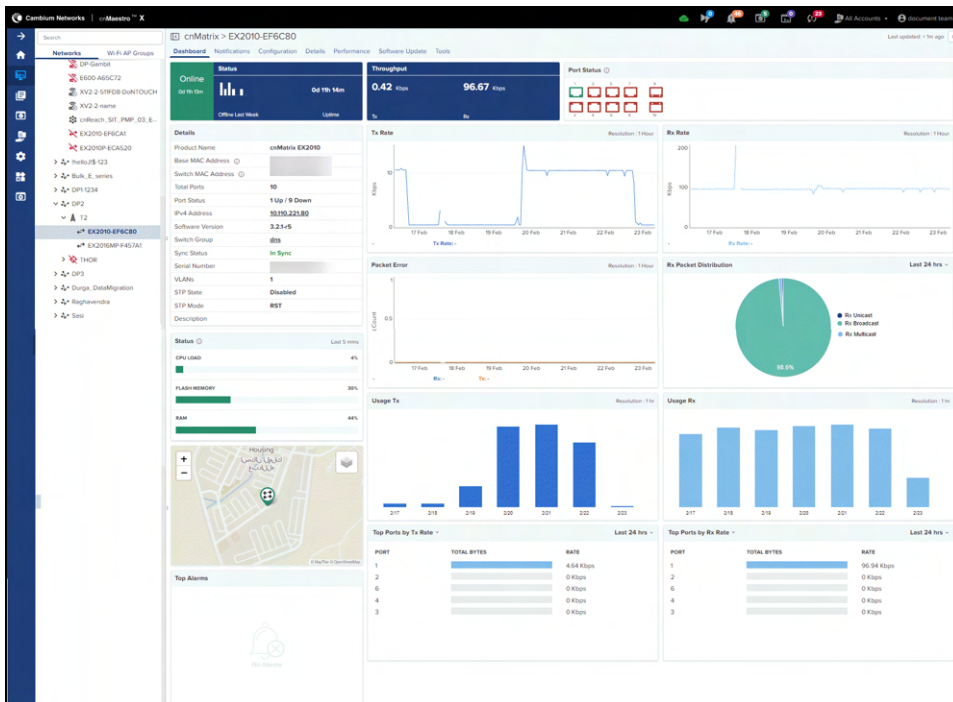
Connection Health displays the health of the devices connected to the network.



Charts and Graphs

Contextual charts and graphs provides details on important dashboard metrics.

Figure 18 Charts and Graphs




Notifications

Overview

Notifications consist of Events, Alarm History, and Alarms. They are asynchronous messages that provides real-time system status.

Table 14: Notification Overview

Type	Description
Alarms	<p>Alarms have state and persist as long as the problematic activity continues; they reflect the current health of the devices in the network.</p> <div style="border: 1px solid black; padding: 5px;"><p>NOTE:</p><p>After every server reboot or restart, alarm displays as shown below:</p><ul style="list-style-type: none">• cnMaestro takes up to 10 minutes to reflect the alarm count.• Email Notification subscribers status up and down major alarms is blocked for 30 minutes.• Webhooks will not send the device status up and down major alarms for next 30 minutes.</div>
Alarm History	<p>Expired Alarms are added to the Alarm History. The Alarm History displays historical active alarm counts.</p>
Events	<p>Events are stateless, transient messages that occur in response to an input or action, such as 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.</p>

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 for each across the account surpasses 1,000 multiplied by the number of devices in the account. The oldest entries will be 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 15: 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 notification which includes type of reboot of cnPilot Wi-Fi devices.

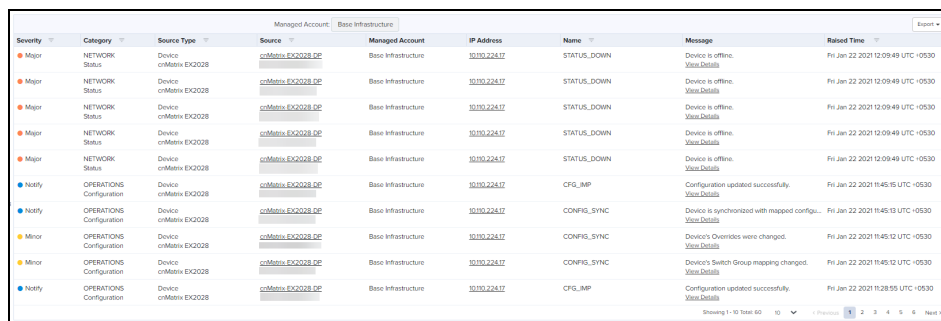
Event Export

The event data in a table can be exported in a CSV or PDF file format.

Support for System Events

The source type can be System, Device, or Client. Events generated by the application will be filtered using the source type **System**.

Figure 19 System Events



Severity	Category	Source Type	Source	Managed Account	IP Address	Name	Message	Raised Time
Major	NETWORK Status	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	STATUS_DOWN	Device is offline. View Details	Fri Jan 22 2021 12:09:49 UTC +0530
Major	NETWORK Status	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	STATUS_DOWN	Device is offline. View Details	Fri Jan 22 2021 12:09:49 UTC +0530
Major	NETWORK Status	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	STATUS_DOWN	Device is offline. View Details	Fri Jan 22 2021 12:09:49 UTC +0530
Major	NETWORK Status	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	STATUS_DOWN	Device is offline. View Details	Fri Jan 22 2021 12:09:49 UTC +0530
Major	NETWORK Status	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	STATUS_DOWN	Device is offline. View Details	Fri Jan 22 2021 12:09:49 UTC +0530
Notify	OPERATIONS Configuration	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	CFG_IMP	Configuration updated successfully. View Details	Fri Jan 22 2021 11:45:15 UTC +0530
Notify	OPERATIONS Configuration	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	CONFIG_SYNC	Device is synchronized with mapped config... View Details	Fri Jan 22 2021 11:45:13 UTC +0530
Minor	OPERATIONS Configuration	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	CONFIG_SYNC	Device's Overrides were changed. View Details	Fri Jan 22 2021 11:45:12 UTC +0530
Minor	OPERATIONS Configuration	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	CONFIG_SYNC	Device's Switch Group mapping changed. View Details	Fri Jan 22 2021 11:45:12 UTC +0530
Notify	OPERATIONS Configuration	Device	cnMaestro-EX2028-DE	Base Infrastructure	10.100.224.17	CFG_IMP	Configuration updated successfully. View Details	Fri Jan 22 2021 11:28:55 UTC +0530

The following table describes the different types of event categories and their descriptions.

Table 16: Event Types and Definitions

Event Category	Description
Infrastructure	Events related to infrastructure management – such as HA state, System resources (e.g CPU, Disk, Memory), etc. Source: cnMaestro
Network	Events related to networking issues, such as link up/down. Source: Device
Operations	Events related to system-level processes, such as pushing configuration, installing images, etc. Source: Device
Other	Events unrelated to the above categories. Source: Device
Registration	Events related to managing/unmanaging devices. Source: Device

Table 16: Event Types and Definitions

Event Category	Description
Security	Events related to logging into the devices and establishing secure links. Source: cnMaestro, Device and Client
Services	Events related to additional services added to the product. Source: cnMaestro and Device
Wireless	Events related to issues/notifications with the PTP/PMP radio connectivity, Wi-Fi Clients, etc. Source: Device and Client

Alarms

Alarm Life Cycle

The basic alarm life cycle has the following states:





Table 17: Alarm Life Cycle

State	Description
Acknowledged	Active alarms can be acknowledged, which signifies they are known and being handled. Acknowledgment alarms are not included in the total alarm count.
Active	The alarm remains active until the combination of inputs that generated it are cleared.
Expired	Expired Alarms are placed in the Alarm History.
Inactive	Inactive alarms remain visible in the active alarm table for 10 minutes, then 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 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 18: 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.
	Notify	It represents clear and is used for inactive alarms.

Alarm Types

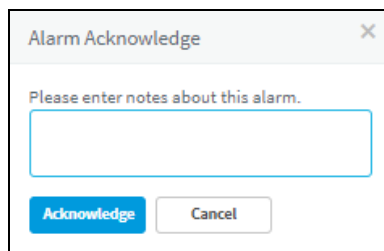
Table 19: Alarm Types

Alarm Type	Definition
Configuration	Tracks issues encountered during a device configuration update.
DFS State	Tracks issues related to DFS operational status.
GPS State	Tracks issues related to GPS synchronization.
Link State	Tracks issues related to the status of device interfaces.
Status	Tracks when connectivity between cnMaestro On-Premises and a device is lost.
Upgrade	Tracks 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.

Figure 20 Alarm Acknowledge



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 one to view which alarms were active at a specific time in the past.

Figure 21 Alarm History



Statistics and Details

Statistics provide a tabular aggregation of data, including general information on the devices monitored, as well as Wireless, Network, and Traffic metrics. Details pages provide information on a single device, generally in a page format.

The table below highlights the type of information generally found in cnMaestro Statistics and Details sections (separated by Device Type).

Table 20: Device Statistics

Device Statistics	Fields
60 GHz cnWave Nodes	<p>General</p> <ul style="list-style-type: none"> ● Device ● IPv6 Address ● Main Aux SFP ● Mode ● Model ● Network ● PoP Node ● Radio Channel ● Serial Number ● Site ● Software Version ● Status ● Status Time ● Sync Mode ● Zone <p>GPS</p> <ul style="list-style-type: none"> ● Fix Type ● Height ● Latitude ● Longitude ● Satellites Tracked
cnMatrix	<p>General</p> <ul style="list-style-type: none"> ● Device ● IP Address ● Product Name ● Serial Number ● Status <p>Traffic</p> <ul style="list-style-type: none"> ● Throughput (DL) ● Throughput (Rx)
cnPilot Home	<p>General</p> <ul style="list-style-type: none"> ● Device ● IP Address ● Product Name ● Serial Number ● Status <p>Wireless</p> <ul style="list-style-type: none"> ● Radios (Channel)
cnRanger BBU	<p>General</p> <ul style="list-style-type: none"> ● Device ● IP Address ● Registered SM Count ● Serial Number ● Status <p>Traffic</p>

Table 20: Device Statistics

Device Statistics	Fields
	<ul style="list-style-type: none"> ● Throughput (DL) ● Throughput (UL)
cnRanger SM	<p>General</p> <ul style="list-style-type: none"> ● Device ● IMSI ● IP Address ● Serial Number ● Status <p>Traffic</p> <ul style="list-style-type: none"> ● Throughput (DL) ● Throughput (UL) <p>Wireless</p> <ul style="list-style-type: none"> ● Bandwidth ● Frequency ● MCS (DL) ● MCS (UL) ● RSRP ● RSRQ ● RSSI
cnReach	<p>General</p> <ul style="list-style-type: none"> ● Device ● IP Address ● Neighbors ● Radio ● Role ● Status <p>Radio</p> <ul style="list-style-type: none"> ● Average Noise ● Radio Temperature ● RSSI ● SNR ● Tx Power <p>Traffic</p> <ul style="list-style-type: none"> ● Throughput (DL) ● Throughput (UL)
cnReach XIO	<p>General</p> <ul style="list-style-type: none"> ● Active S/W Version ● Device ● IP Address ● Product Name ● Serial Number ● Status
cnVision Client	<p>General</p> <ul style="list-style-type: none"> ● Device ● DFS Status

Table 20: Device Statistics

Device Statistics	Fields
	<ul style="list-style-type: none"> ● Distance ● IP Address ● Serial Number ● Session Time ● Status <p>Network</p> <ul style="list-style-type: none"> ● LAN Interface ● LAN Interface 2 ● WAN IP Address <p>Traffic</p> <ul style="list-style-type: none"> ● Retransmission Rate (DL) ● Retransmission Rate (UL) ● Throughput (DL) ● Throughput (UL) <p>Wireless</p> <ul style="list-style-type: none"> ● Antenna Gain ● Connected AP ● MCS (DL) ● MCS (UL) ● Quality Capacity ● RSSI (DL) ● RSSI (UL) ● SSID ● Tx Power ● Wireless MAC
cnVision Hub	<p>General</p> <ul style="list-style-type: none"> ● Device ● DFS Status ● IP Address ● Registered SM Count ● Reregistration Count ● Serial Number ● Status <p>Network</p> <ul style="list-style-type: none"> ● LAN Interface ● LAN Interface 2 <p>Traffic</p> <ul style="list-style-type: none"> ● Throughput (DL) ● Throughput (UL) <p>Wireless</p> <ul style="list-style-type: none"> ● Antenna Gain ● Bandwidth ● DL/UL Ratio ● Max Range ● Frequency ● SSID ● Tx Power

Table 20: Device Statistics

Device Statistics	Fields
Enterprise WiFi	<p>General</p> <ul style="list-style-type: none"> ● Device ● IP Address ● Product Name ● Serial Number ● Status <p>Wireless</p> <ul style="list-style-type: none"> ● Radios (Channel)
ePMP AP	<p>General</p> <ul style="list-style-type: none"> ● Device ● DFS Status ● IP Address ● Registered SM Count ● Reregistration Count ● Serial Number ● Status <p>Network</p> <ul style="list-style-type: none"> ● LAN Interface ● LAN Interface 2 <p>Traffic</p> <ul style="list-style-type: none"> ● Throughput (DL) ● Throughput (UL) <p>Wireless</p> <ul style="list-style-type: none"> ● Antenna Gain ● Bandwidth ● DL/UL Ratio ● Frequency ● Maximum Range ● SSID ● Tx Power
ePMP SM	<p>General</p> <ul style="list-style-type: none"> ● Device ● DFS Status ● Distance ● IP Address ● Serial Number ● Session Time ● Status <p>Network</p> <ul style="list-style-type: none"> ● LAN Interface ● LAN Interface 2 ● WAN IP Address <p>Traffic</p> <ul style="list-style-type: none"> ● Retransmission Rate (DL) ● Retransmission Rate (UL)

Table 20: Device Statistics

Device Statistics	Fields
	<ul style="list-style-type: none"> ● Throughput (DL) ● Throughput (UL) <p>Wireless</p> <ul style="list-style-type: none"> ● Antenna Gain ● Capacity ● Connected AP ● MCS (DL) ● MCS (UL) ● Quality ● RSSI (DL) ● RSSI (UL) ● SSID ● Tx Power ● Wireless MAC
Machfu	<p>Cell</p> <ul style="list-style-type: none"> ● Cell Enabled ● Cell ICCID ● Cell IMEI ● Cell IMSI ● Cell IP ● Cell Link ● Cell Manufacturer ● Cell Network Type ● Cell RSSI ● Cell Rx Rate ● Cell Sw Version ● Cell Tx Rate <p>Ethernet</p> <ul style="list-style-type: none"> ● Ethernet ● Ethernet Enabled ● Ethernet Gateway ● Ethernet IP Address ● Ethernet Link ● Ethernet Link Speed ● Ethernet MAC ● Ethernet Mask ● Ethernet Mode ● Ethernet Rx Rate ● Ethernet Tx Rate <p>General</p> <ul style="list-style-type: none"> ● Device ● IP Address ● Status <p>GPS</p> <ul style="list-style-type: none"> ● GPS Accuracy ● GPS Altitude ● GPS Fix Time ● GPS Satellites in use ● GPS Status

Table 20: Device Statistics

Device Statistics	Fields
	<ul style="list-style-type: none"> ● GPS Time <p>VPN</p> <ul style="list-style-type: none"> ● VPN IP ● VPN Link ● VPN Server ● VPN Type <p>Wireless Client</p> <ul style="list-style-type: none"> ● WC Enabled ● WC Gateway ● WC IP ● WC Link ● WC MAC ● WC Mask ● WC RSSI ● WC Rx Rate ● WC SSID ● WC Tx Rate <p>Wireless Access Point</p> <ul style="list-style-type: none"> ● WAP Enabled ● WAP IP ● WAP Link ● WAP MAC ● WAP Mask ● WAP Mode ● WAP Rx Rate ● WAP SSID ● WAP Tx Rate
PMP AP	<p>General</p> <ul style="list-style-type: none"> ● Device ● DFS Status ● IP Address ● Registered SM Count ● Reregistration Count ● Serial Number ● Status <p>Network</p> <ul style="list-style-type: none"> ● LAN Interface <p>Traffic</p> <ul style="list-style-type: none"> ● Busy Index (DL) ● Busy Index (UL) ● Frame Utilization (DL) ● Frame Utilization (UL) ● Throughput (DL) ● Throughput (UL) <p>Wireless</p> <ul style="list-style-type: none"> ● Antenna Gain ● Bandwidth

Table 20: Device Statistics

Device Statistics	Fields
	<ul style="list-style-type: none"> ● Color code ● DL/UL Ratio ● Frequency ● Maximum Range ● Tx Power
PMP SM	<p>General</p> <ul style="list-style-type: none"> ● Device ● DFS Status ● Distance ● IP Address ● Serial Number ● Session Time ● Status <p>Network</p> <ul style="list-style-type: none"> ● LAN Interface ● WAN IP Address <p>Traffic</p> <ul style="list-style-type: none"> ● Packet Loss (DL) ● Packet Loss (Error Drop) (DL) ● Packet Loss (Overcapacity) (DL) ● Packet Loss (UL) ● Packet Loss (Overcapacity) (UL) ● Packet Loss (Error Drop) (UL) ● Throughput (DL) ● Throughput (UL) <p>Wireless</p> <ul style="list-style-type: none"> ● Antenna Gain ● Color Code ● Connected AP ● Horizontal SNR (DL) ● Horizontal SNR (UL) ● LQI (DL) ● LQI (UL) ● Modulation (DL) ● Modulation (UL) ● RSSI (DL) ● RSSI Imbalance ● Tx Power ● Vertical SNR (DL) ● Vertical SNR (UL)
PTP	<p>General</p> <ul style="list-style-type: none"> ● Device ● IP Address ● Product Name ● Status <p>Network</p> <ul style="list-style-type: none"> ● Aux Interface ● Main PSU Interface

Table 20: Device Statistics

Device Statistics	Fields
	<ul style="list-style-type: none">● SFP Interface <p>Wireless</p> <ul style="list-style-type: none">● Antenna Gain● Bandwidth● Errored Seconds● Licensed Country● Maximum Transmit Power● Receive Frequency● Severely Errored Seconds● Transmit Frequency● Unavailable Seconds

Performance

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

The following images represents the sample performance graphs for 60 GHz cnWave, cnMatrix, cnPilot Enterprise, cnPilot Home, cnRanger, cnReach, ePMP AP, ePMP SM, PMP AP, PMP SM, and PTP.

Table 21: Performance Graph

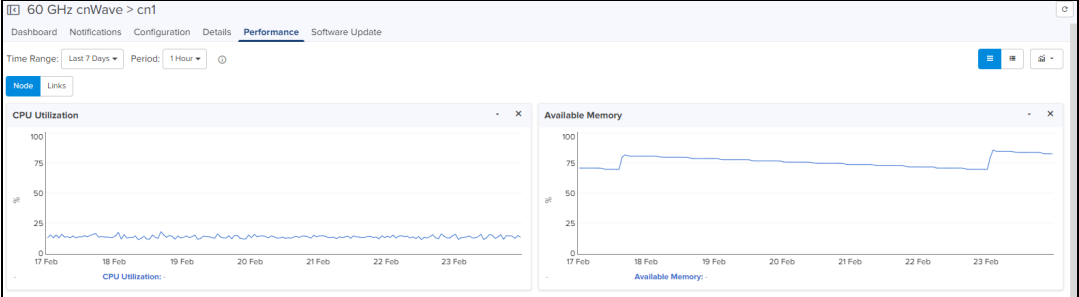
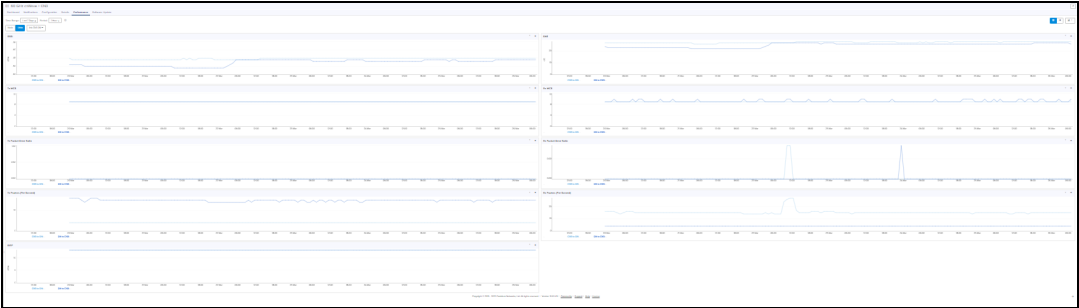
Device	Fields
<p>60 GHz cnWave (Node)</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Available Memory ● CPU Utilization 
<p>60 GHz cnWave (Links)</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● EIRP ● RSSI ● Rx Frames (Per Second) ● Rx MCS ● Rx Packet Error Ratio ● SNR ● Tx Frames (Per Second) ● Tx MCS ● Tx Packet Error Ratio 
<p>cnMatrix</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● CPU ● Packet Error ● Rx Packets ● Throughput ● Tx Packets

Table 21: Performance Graph

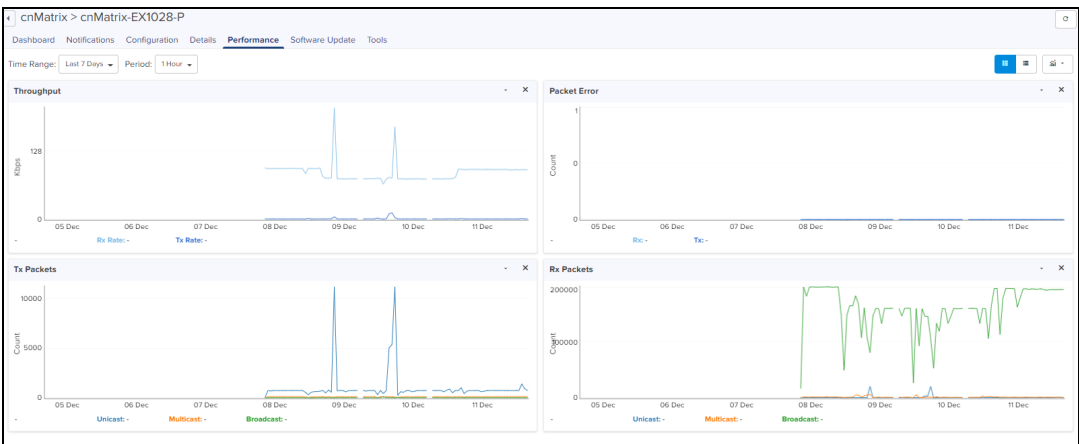
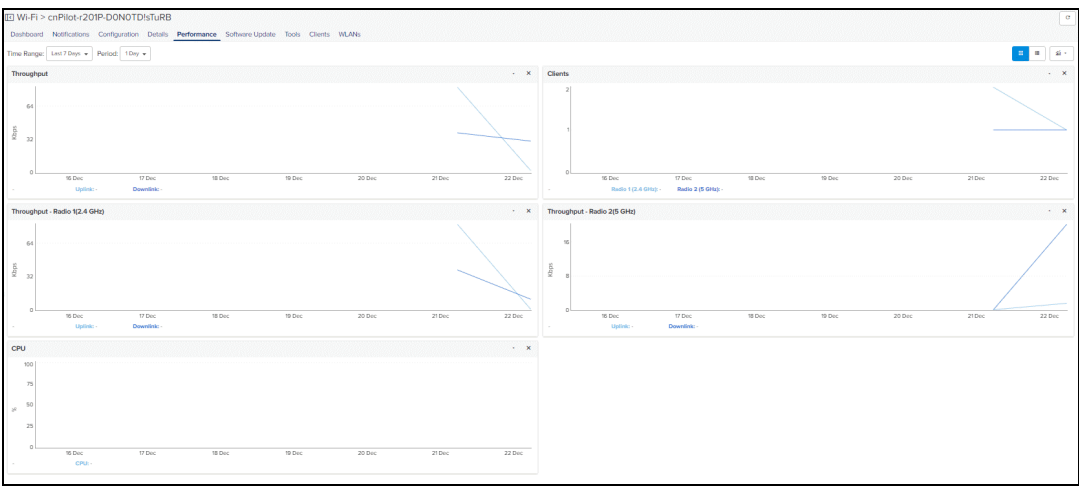
Device	Fields
	 <p>The screenshot shows the Performance page for device cnMatrix-EX1028-P. It features four line graphs: Throughput (Mbps), Packet Error (Count), Tx Packets (Count), and Rx Packets (Count). The x-axis for all graphs represents time from Dec 05 to Dec 11. The Throughput graph shows a peak around Dec 09. The Packet Error graph shows a low, stable count. The Tx Packets graph shows a significant spike on Dec 09. The Rx Packets graph shows a high, fluctuating count.</p>
<p>cnPilot Home</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Clients ● CPU ● Throughput ● Throughput - Radio 1 (2.4 GHz) ● Throughput - Radio 2 (5 GHz)  <p>The screenshot shows the Performance page for a Wi-Fi device. It features five line graphs: Clients, CPU, Throughput, Throughput - Radio 1 (2.4 GHz), and Throughput - Radio 2 (5 GHz). The x-axis for all graphs represents time from Dec 16 to Dec 22. The Clients graph shows a steady increase. The CPU graph shows a steady increase. The Throughput graph shows a steady increase. The Throughput - Radio 1 (2.4 GHz) graph shows a steady increase. The Throughput - Radio 2 (5 GHz) graph shows a steady increase.</p>
<p>cnReach</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Neighbors ● Noise ● RSSI ● Throughput ● Transmit Power

Table 21: Performance Graph

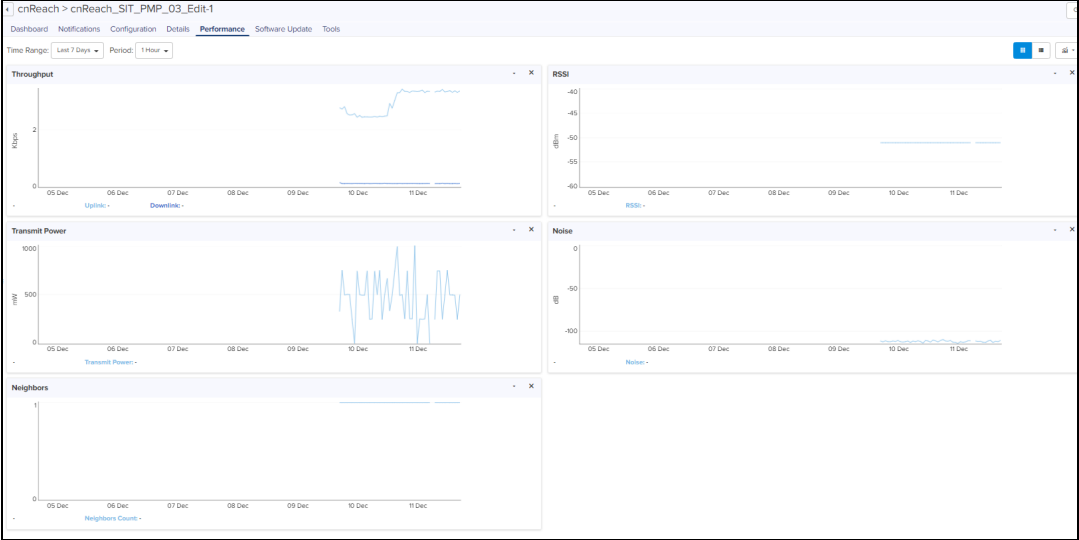
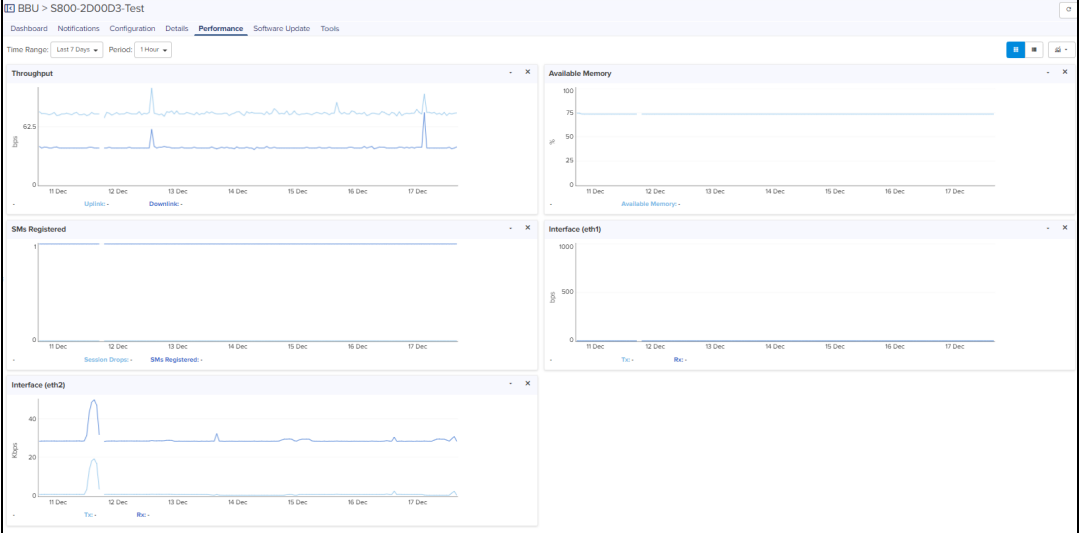
Device	Fields
	 <p>The screenshot shows a performance dashboard for a device named 'cnReach'. It features five line graphs: 'Throughput' (Mbps) showing a spike on Dec 10; 'RSSI' (dBm) showing a constant level around -60; 'Transmit Power' (mW) showing a spike on Dec 10; 'Noise' (dB) showing a constant level around -100; and 'Neighbors' (Neighbors Count) showing a constant level around 1. The interface includes a 'Time Range' dropdown set to 'Last 7 Days' and a 'Period' dropdown set to '1 Hour'.</p>
<p>cnRanger BBU</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Available Memory ● Interface (eth1) ● Interface (eth2) ● SMs Registered ● Temperature ● Throughput  <p>The screenshot shows a performance dashboard for a device named 'cnRanger BBU'. It features five line graphs: 'Throughput' (Mbps) showing a spike on Dec 12; 'Available Memory' (MB) showing a constant level around 75; 'SMs Registered' showing a constant level around 1; 'Interface (eth1)' showing Tx and Rx rates near 0; and 'Interface (eth2)' showing Tx and Rx rates with a spike on Dec 12. The interface includes a 'Time Range' dropdown set to 'Last 7 Days' and a 'Period' dropdown set to '1 Hour'.</p>
<p>cnRanger RRH</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Ambient Temperature ● CPU ● Die Temperature ● Frame Utilization ● SMs Registered ● Throughput

Table 21: Performance Graph

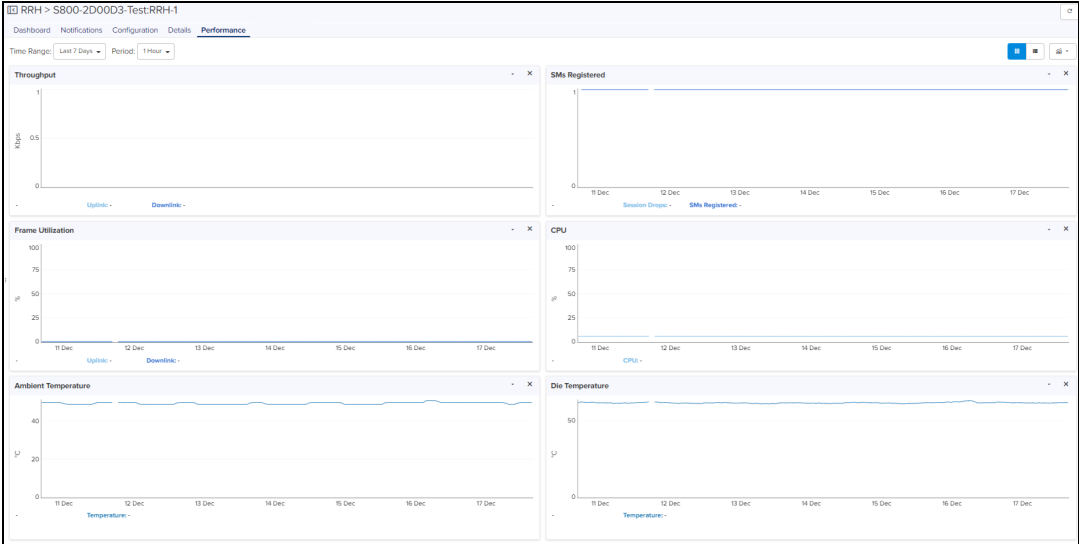
Device	Fields
	 <p>The screenshot displays a performance dashboard for a device identified as 'RRH - S800-2D00D3-TestRRH-1'. The dashboard is titled 'Performance' and includes a navigation menu with 'Dashboard', 'Notifications', 'Configuration', and 'Details'. The time range is set to 'Last 7 Days' and the period is '1 Hour'. The dashboard contains six line graphs arranged in a 3x2 grid:</p> <ul style="list-style-type: none"> Throughput: Shows Mbps on the y-axis (0 to 1) over time. It includes sub-graphs for 'Upload' and 'Download'. SMS Registered: Shows the number of SMS registered on the y-axis (0 to 1) over time. It includes sub-graphs for 'Session Drops' and 'SMS Registered'. Frame Utilization: Shows percentage utilization on the y-axis (0 to 100) over time. CPU: Shows percentage CPU utilization on the y-axis (0 to 100) over time. Ambient Temperature: Shows temperature in degrees Celsius on the y-axis (0 to 40) over time. Die Temperature: Shows temperature in degrees Celsius on the y-axis (0 to 50) over time.
cnRanger SM	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Available Memory ● CPU ● MCS ● RSRP ● RSRQ ● RSSI ● SINR ● Throughput

Table 21: Performance Graph

Device	Fields
	<p>cnRanger SM > T101-2D3E86</p> <p>Dashboard Notifications Configuration Details Performance Software Update Tools</p> <p>Time Range: Last 7 Days Period: 1 Hour</p> <p>Throughput (Kbps), RSRP (dBm), SINR (dB), RSSI (dBm), RSRQ (dBm), MCS, CPU (%), Available Memory (%)</p>
<p>cnVision Client</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● CPU ● MCS ● Retransmission ● RSSI ● Session Drops ● SNR ● Throughput <p>Clients > Client_MCR0</p> <p>Dashboard Notifications Configuration Details Performance Software Update Tools</p> <p>Time Range: Last 7 Days Period: 1 Hour</p> <p>Throughput (Kbps), Retransmission (%), MCS, RSSI (dBm), Session Drops, CPU (%)</p>

Table 21: Performance Graph

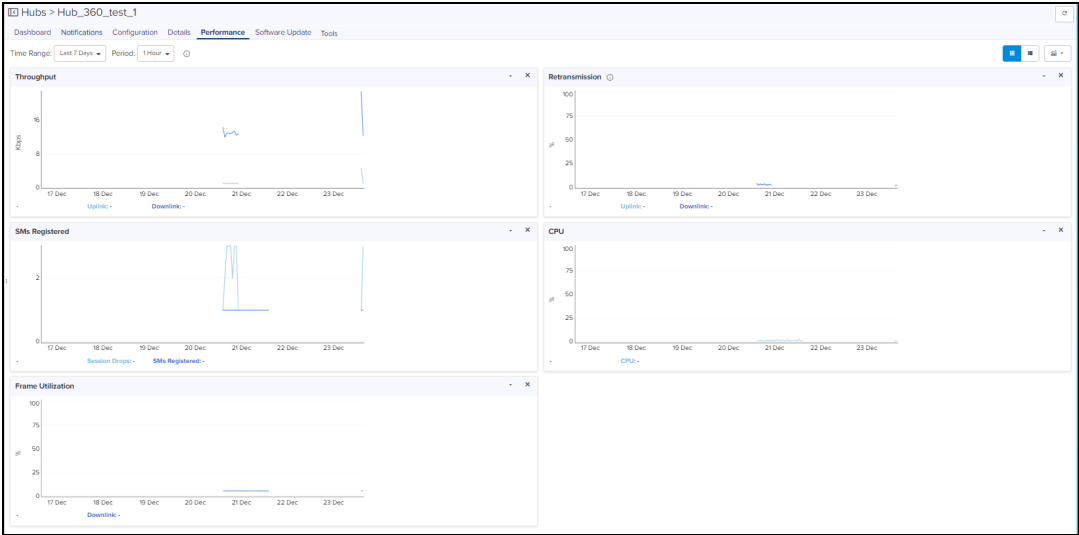
Device	Fields
<p>cnVision Hub</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● CPU ● Frame Utilization ● Retransmission ● SMs Registered ● Throughput 
<p>Enterprise Wi-Fi</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Airtime (2.4 GHz) ● Airtime (5 GHz) ● Available Memory ● Clients ● CPU ● Interference ● Noise Floor ● Packet Rate ● Throughput ● Throughput - Radio 1 (2.4 GHz) ● Throughput - Radio 2 (5 GHz)

Table 21: Performance Graph

Device	Fields
	
<p>ePMP AP</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● CPU ● Frame Utilization ● Retransmission ● SMs Registered ● Throughput 
<p>ePMP SM</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● CPU ● MCS ● Retransmission ● RSSI ● Session Drops ● SNR ● Throughput

Table 21: Performance Graph

Device	Fields
Machfu	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Cellular RSSI ● Cellular Throughput ● CPU Load ● Disk Storage ● Ethernet 1 Throughput ● Ethernet 2 Throughput ● Flash Memory ● Wi-Fi Access Point Throughput ● Wi-Fi Client RSSI ● Wi-Fi Client Throughput

Table 21: Performance Graph

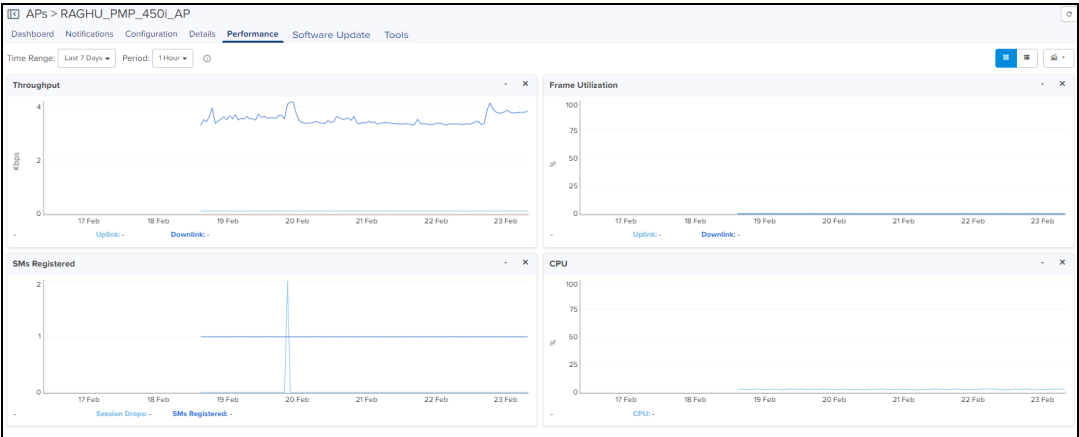
Device	Fields
	
<p>PMP AP</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● CPU ● Frame Utilization ● SMs Registered ● Throughput 
<p>PMP SM</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● CPU

Table 21: Performance Graph

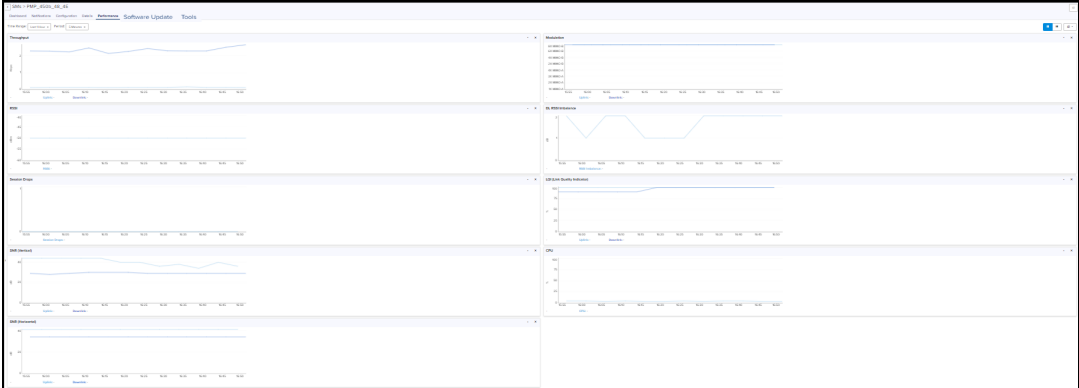
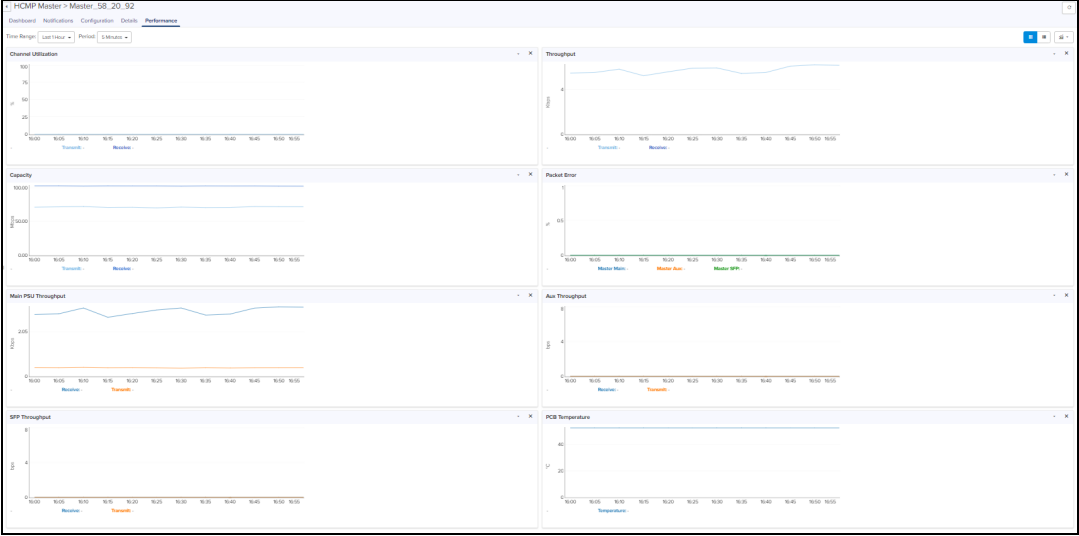
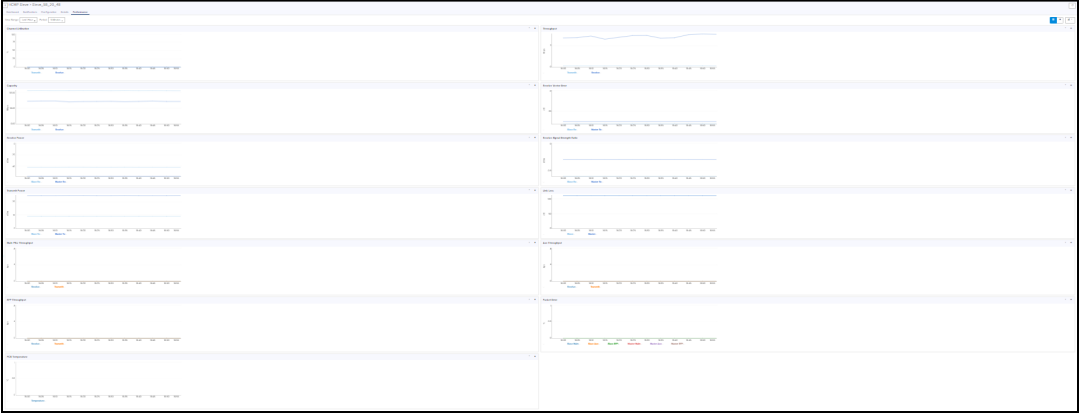
Device	Fields
	<ul style="list-style-type: none"> ● DL RSSI Imbalance ● LQI (Link Quality Indicator) ● Modulation ● RSSI ● Session Drops ● SNR (Horizontal) ● SNR (Vertical) ● Throughput 
<p>PTP and HCMP Masters</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Aux Throughput ● 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

Table 21: Performance Graph

Device	Fields
	
<p>PTP and HCMP Slaves</p>	<p>Displays the following graphs:</p> <ul style="list-style-type: none"> ● Aux Throughput ● Channel Utilization ● Capacity ● Main PSU Throughput ● Link Loss ● Packet Error ● PCB Temperature ● Receive Vector Error ● Receive Power ● Receive Signal Strength Ratio ● SFP Throughput ● Throughput ● Transmit Power 

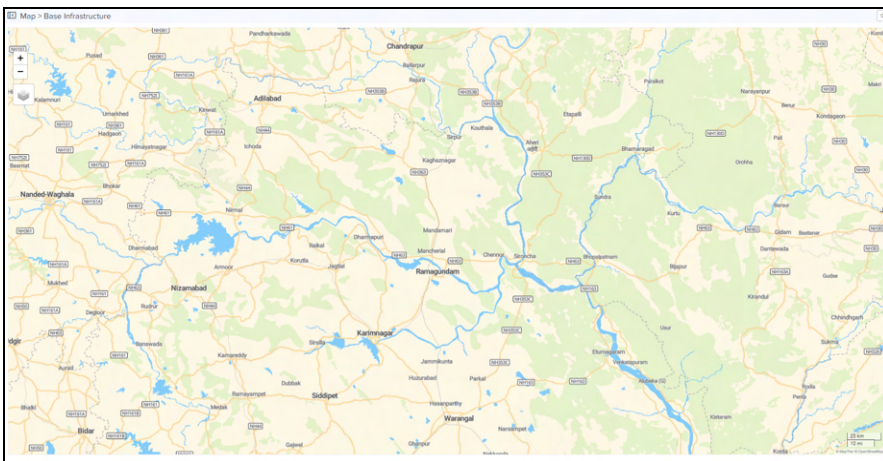
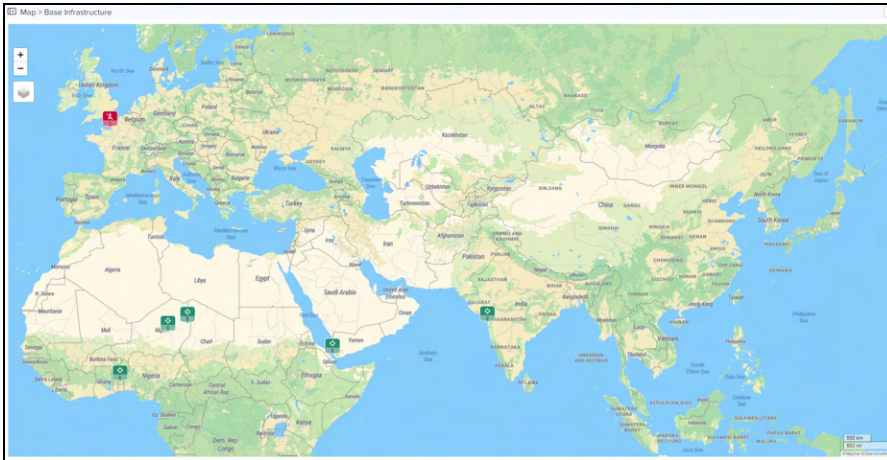
Maps

Maps provide a 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.

Two views are supported in System Maps and Network/Tower Dashboard Map:

- Street view
- Satellite view

Figure 22 Map Street View



To enable Satellite View, perform the following steps:

1. Navigate to **Administration > Settings > Advanced Features**.
2. Click **Satellite View** checkbox.

Advanced Features

Instantaneous Offline Alarm Send offline alarms immediately, instead of waiting 5 minutes. This may generate many false alarms due to slow or unstable connections.

Lock Wi-Fi AP/cnMatrix device Configuration Overwrite Wi-Fi AP and cnMatrix configuration changes made outside of a mapped AP Group or Switch Group (such as through the Device UI).

RADIUS Proxy Enable the "Proxy RADIUS through cnMaestro" feature in WLAN policies (configured at Enterprise WLAN Policy > AAA Servers).

NAS IP:

WiFiPerf Daemon Enable Wi-Fi Performance tests between the Wi-Fi AP or CPE and cnMaestro (configured at Wi-Fi Device > Tools > Wi-Fi Performance)

Geolocation Map Settings

Satellite View Enable satellite view in maps.

Custom Map Server Enable third-party WMS GeoLocation Map Server (replacing the default map tile service). [Learn more](#)

WMS Map Server URL

Layer Name

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

Figure 23 Map Satellite View



Geolocation Map Settings

Geolocation Map Settings allows you to customize the Map using a Web Map Service (WMS) map server. Map can be customized using the WMS map server URL and the Layer Name provided by the service provider.

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

Advanced Features

Instantaneous Offline Alarm Send offline alarms immediately, instead of waiting 5 minutes. This may generate many false alarms due to slow or unstable connections.

Lock Wi-Fi AP/cnMatrix device Configuration **X** Overwrite Wi-Fi AP and cnMatrix configuration changes made outside of a mapped AP Group or Switch Group (such as through the Device UI).

RADIUS Proxy **X** Enable the "Proxy RADIUS through cnMaestro" feature in WLAN policies (configured at Enterprise WLAN Policy > AAA Servers).

NAS IP:

Wi-Fi Perf Daemon **X** Enable Wi-Fi Performance tests between the Wi-Fi AP or CPE and cnMaestro (configured at Wi-Fi Device > Tools > Wi-Fi Performance)

Geolocation Map Settings

Satellite View Enable satellite view in maps.

Custom Map Server **X** Enable third-party WMS Geolocation Map Server (replacing the default map tile service). [Learn more](#)

WMS Map Server URL

Layer Name

Optional Features

To enable Geolocation Map Settings, perform the following steps:

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

Advanced Features

Instantaneous Offline Alarm Send offline alarms immediately, instead of waiting 5 minutes. This may generate many false alarms due to slow or unstable connections.

Lock Wi-Fi AP/cnMatrix device Configuration **X** Overwrite Wi-Fi AP and cnMatrix configuration changes made outside of a mapped AP Group or Switch Group (such as through the Device UI).

RADIUS Proxy **X** Enable the "Proxy RADIUS through cnMaestro" feature in WLAN policies (configured at Enterprise WLAN Policy > AAA Servers).

NAS IP:

Wi-Fi Perf Daemon **X** Enable Wi-Fi Performance tests between the Wi-Fi AP or CPE and cnMaestro (configured at Wi-Fi Device > Tools > Wi-Fi Performance)

Geolocation Map Settings

Satellite View Enable satellite view in maps.

Custom Map Server **X** Enable third-party WMS Geolocation Map Server (replacing the default map tile service). [Learn more](#)

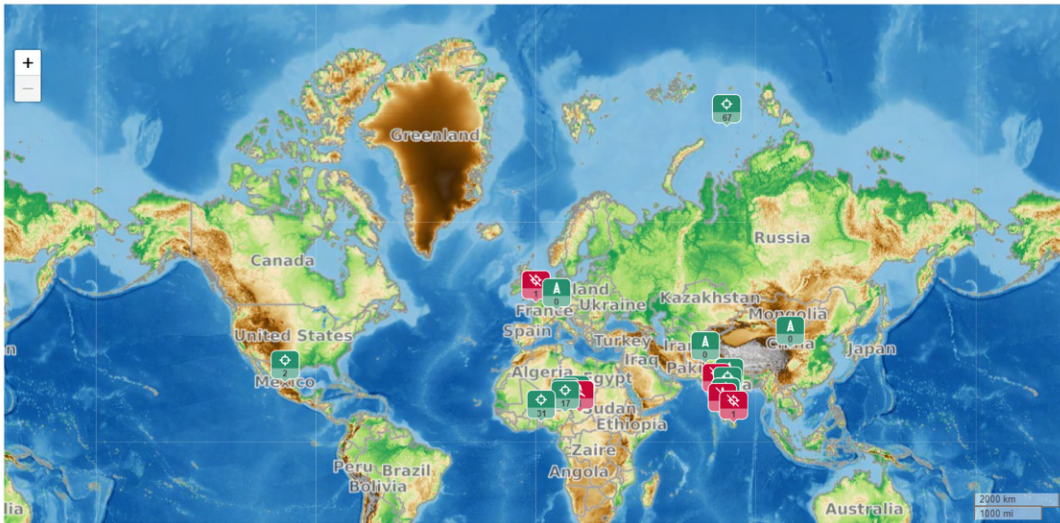
WMS Map Server URL

Layer Name

Optional Features

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

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



Map Navigation

There are a various ways to navigate through the map display.

Action	Description
Double-Click	Double-Click on the following items on the Map, the UI will auto-navigate to the Dashboard of that item: <ul style="list-style-type: none"> ● ePMP SM ● Site ● Tower
Hover	Hovering over a tower or device will pop-up a tool tip that provides basic status information. Hovering over an RF link will display status on the link.
Click	Click the following items on the Map, auto-select the same item in the Tree: <ul style="list-style-type: none"> ● ePMP SM ● Tower
Standard Components	In the upper-left corner are generic map navigation components that allow one to zoom in and out. User can also use the mouse to drag and reposition the view as well as turn on satellite display.

Mode

The map can be placed in a number of different modes for the devices of PMP/ePMP SMs only, which define how the device status is presented.

Table 22: Mode

Mode	Details
Alarm Status	Highlights devices based upon alarm count (Critical, Major, Minor).
Average MCS (ePMP only)	Displays the Uplink or Downlink average MCS per device.
Device Status	Displays whether a device is Up (Green) or Down (Red).
Frequency	Displays the sector frequency.
Link Quality Indicator (PMP only)	Displays the Uplink or Downlink average indicator per device.
Reregistration Count	Displays the nodes based upon the number of reregistrations in the last 24 hours. The more reregistration, the larger the node is displayed.
Retransmission Percentage (ePMP only)	Displays the percentage of packets retransmitted between ePMP SM and AP on the wireless link.

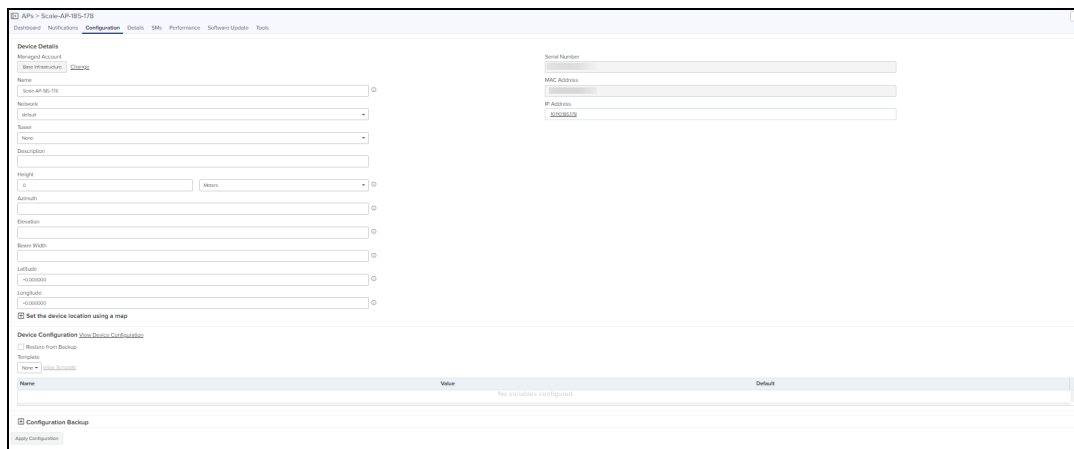
Embedded Maps

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

Sector Visualization

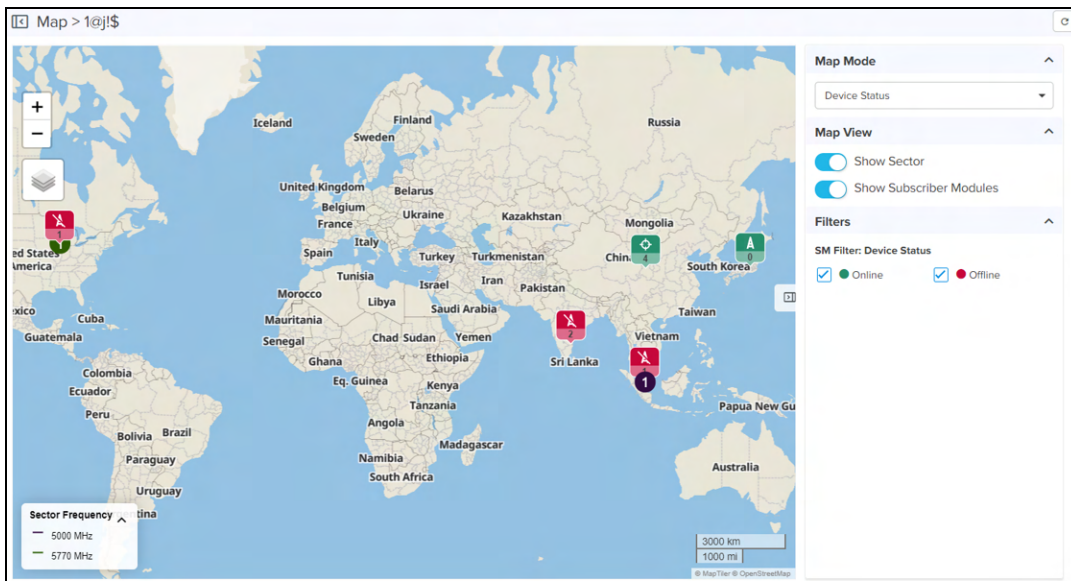
cnMaestro is able to present a basic sector View for ePMP and PMP fixed wireless devices. This requires configuration of Height, Azimuth, Elevation and Beam Width under ePMP/PMP AP configuration. This configured data is used to generate the Sector View. The presentation is not based upon link planning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

Figure 24 AP Configuration Page



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

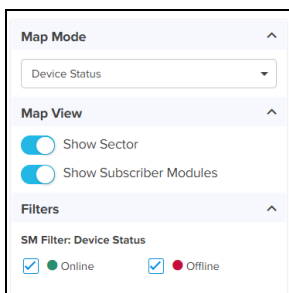
Figure 25 Sector Visualization



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/Offline status.



NOTE:
By default **Show Subscriber Modules** is disabled.



Tools

This section provides the following details:

- 60 GHz cnWave Tools
- cnMatrix Tools
- cnPilot Home Tools
- cnRanger Tools
- cnReach Tools
- cnVision Tools
- ePMP Tools
- Enterprise Wi-Fi
- Machfu
- PMP Tools
- Tower-to-Edge View

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 and you can reboot the device.

Table 23: cnMatrixTools

Field	Description
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Remote CLI	Remote CLI mode is enabled for Super Administrator and Administrator only. But only Show commands can be executed by the Operator. The user can provide the CLI command in the Command text box. The output will be displayed in the output window.
Status	Displays the Status and Port Status.

In **Status** tab, user can view the status of the device either Online or Offline, you can reboot the device.



In **Port Status**, user can view the following port status 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:

The screenshot shows the 'Port Status - Port 1' section of the network management interface. It displays a grid of port status indicators for ports 1 through 28. Below the grid are buttons for 'Cable Diagnostic', 'Port Enable', 'Port Disable', 'PoE Enable', 'PoE Disable', and 'PoE Toggle'. The 'Cable Diagnostic' button is highlighted, and the 'Output' window is open, showing the following text:

```

Complete
Device->config terminal; cable-diagnostics test inter gi 0/1 force
%Cable diagnostics test has started for interface Gi0/1
Device->show cable-diagnostics inter gi 0/1;
Cable Diagnostics Port Status
-----
Port      Pair  Status      Distance  Date of
          Pair  (OK/Err)    to Fault   Last Valid Test
-----
Gi0/1    Pair 1  OK          0 m       Tue Jul 13 15:57:15 2021
          Pair 2  OK          0 m
          Pair 3  OK          0 m
          Pair 4  OK          0 m
  
```

- You can download the generated output by clicking the download  icon.
- You can clear the generated output by clicking the delete  icon.



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:

The screenshot shows the 'Port Status - Port 9' section of the network management interface. It displays a grid of port status indicators for ports 1 through 28. Below the grid are buttons for 'Cable Diagnostic', 'Port Enable', 'Port Disable', 'PoE Enable', 'PoE Disable', and 'PoE Toggle'. The 'Port Disable' button is highlighted, and the 'Output' window is open, showing the following text:

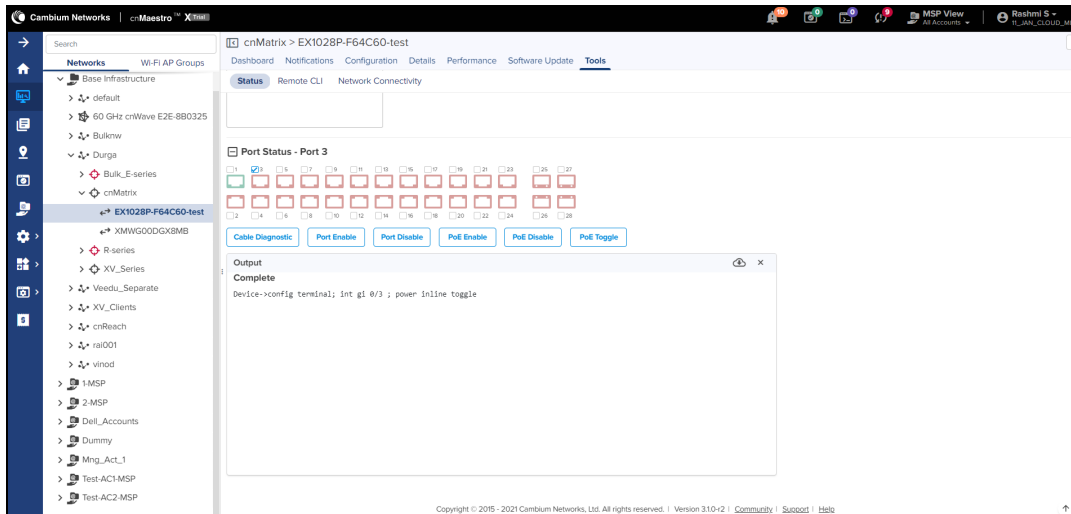
```



Complete
Device->config terminal; int gi 0/1; no shutdown
  
```

- You can download the generated output by clicking the download  icon.
- You can clear the generated output by clicking the delete  icon.

PoE Toggle

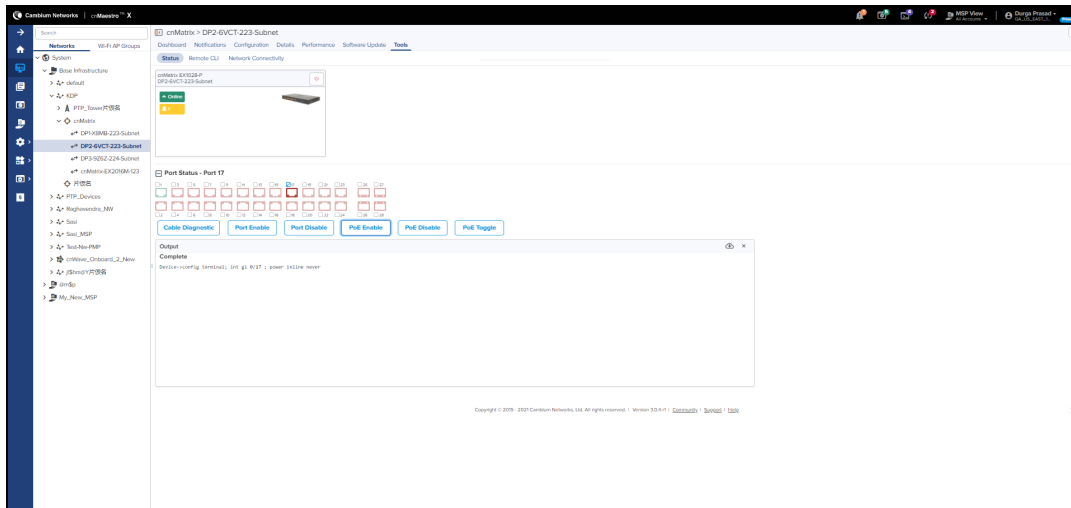
Navigate to **Tools > Status > Port Status**, select the Port and click **PoE Toggle**, the following output is displayed:



- You can download the generated output by clicking the download  icon.
- You can clear the generated output by clicking the delete  icon.

PoE Enable or PoE Disable

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



In **Port Status**, user can view the following port status for the **non-PoE Switches**:

- Cable Diagnostic
- Port Enable
- Port Disable

cnMatrix > XMWG00DGX8MB

Dashboard Notifications Configuration Details Performance Software Update **Tools**

Status Remote CLI Network Connectivity

Online

Port Status - Port 5

1 3 5 7 9 11 13 15 17 19 21 23 25 27
 2 4 6 8 10 12 14 16 18 20 22 24 26 28

Output

Complete

```

Device->config terminal; cable-diagnostics test inter gi 0/5 force
%Cable diagnostics test has started for inter-face Gi0/5
Device->show cable-diagnostics inter gi 0/5;
Cable Diagnostics Port Status
-----
Port      Pair  Status      Distance  Date of
         Pair  to Fault   to Fault  Last Valid Test
-----
Gi0/5    Pair 1  Test in Progress  0 m      Tue Nov 9 08:31:55 2021
         Pair 2  Test in Progress  0 m
         Pair 3  Test in Progress  0 m
         Pair 4  Test in Progress  0 m
  
```

Remote CLI

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

cnMatrix > EX1028P-F61240

Dashboard Notifications Configuration Details Performance Software Update **Tools**

Status **Remote CLI** Network Connectivity

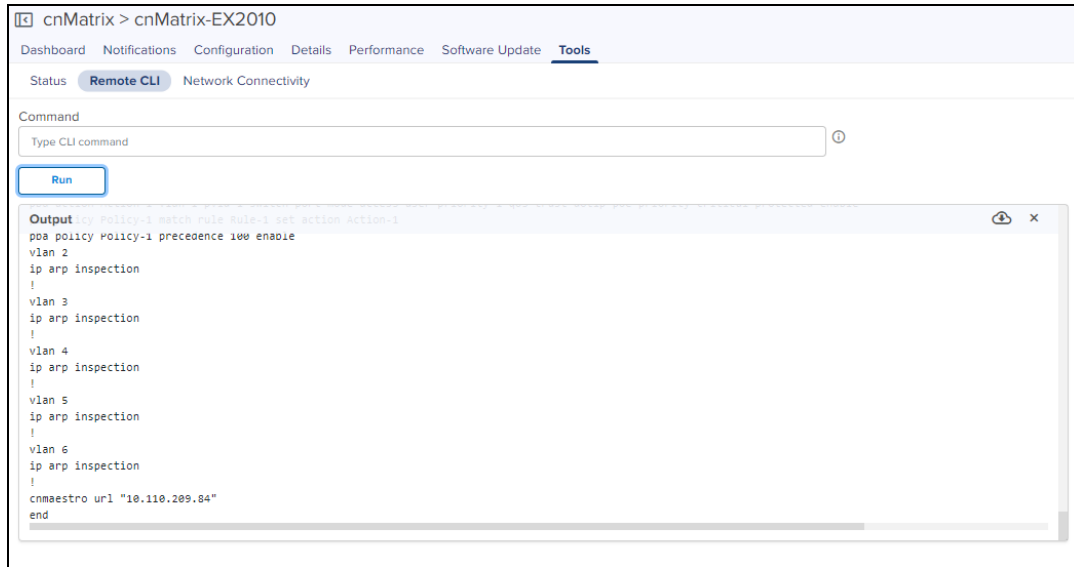
Command



Type CLI command

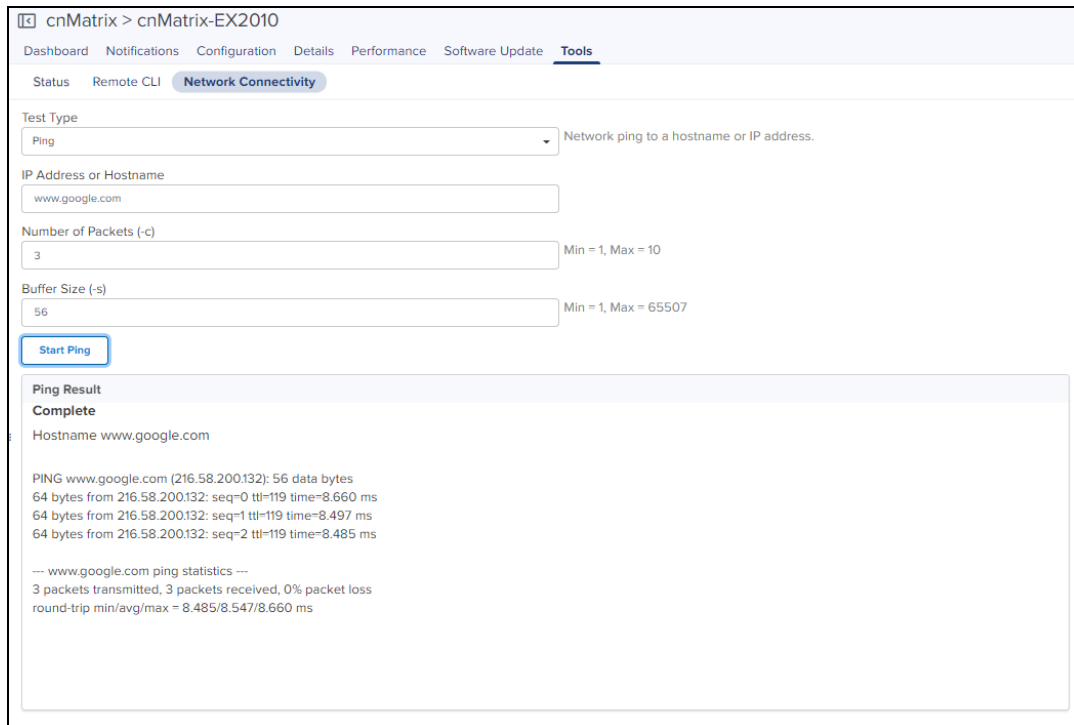
Output

Table 24: cnMatrix Tools

Tools	Description
Remote CLI	<p>Remote CLI mode is enabled for super admin and admin users only. But only show commands can be executed by operator.</p> <p>The user can provide the CLI command in the Command textbox. The output will be displayed in the output window.</p>



- You can download the generated output by clicking the download  icon.
- You can 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 is listed below:

Table 25: 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 26 cnPilot Tools Enterprise WiFi

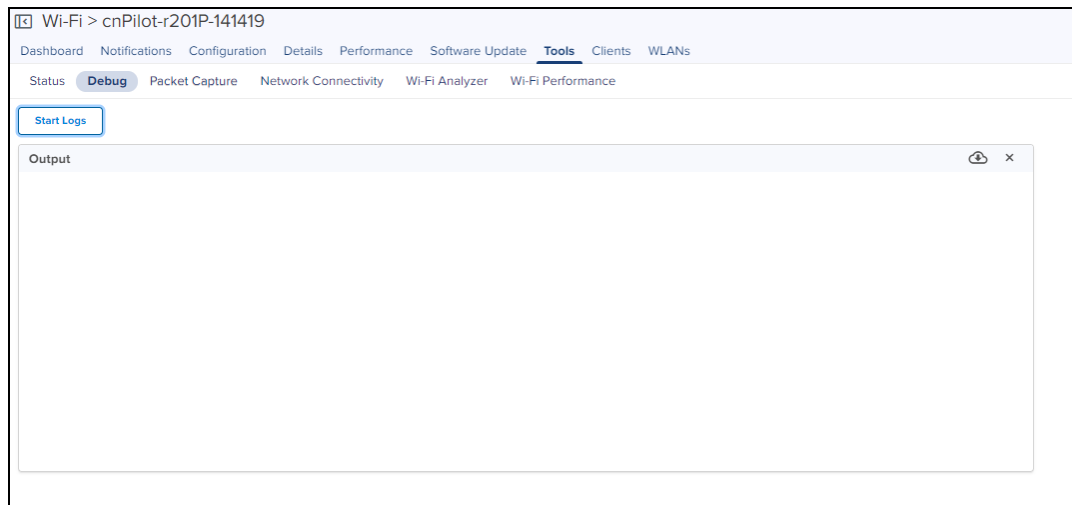


Figure 27 cnPilot Tools Status



cnRanger Tools

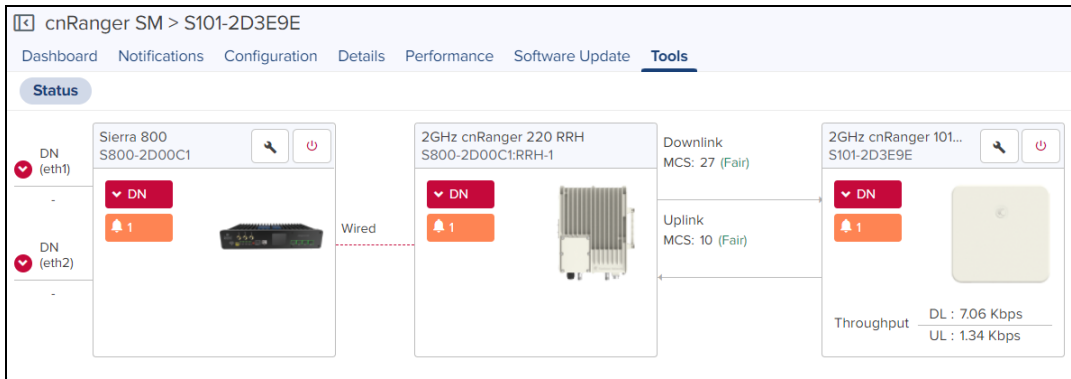
cnRanger BBU

In **Status** tab you can view the status of the device either Online or Offline, allows to download Tech Support File and can reboot the device.



cnRanger SM

In **Status** tab you can view the status of the device either Online or Offline, allows to download Tech Support File, displays the wired connectivity status, and can reboot the device.



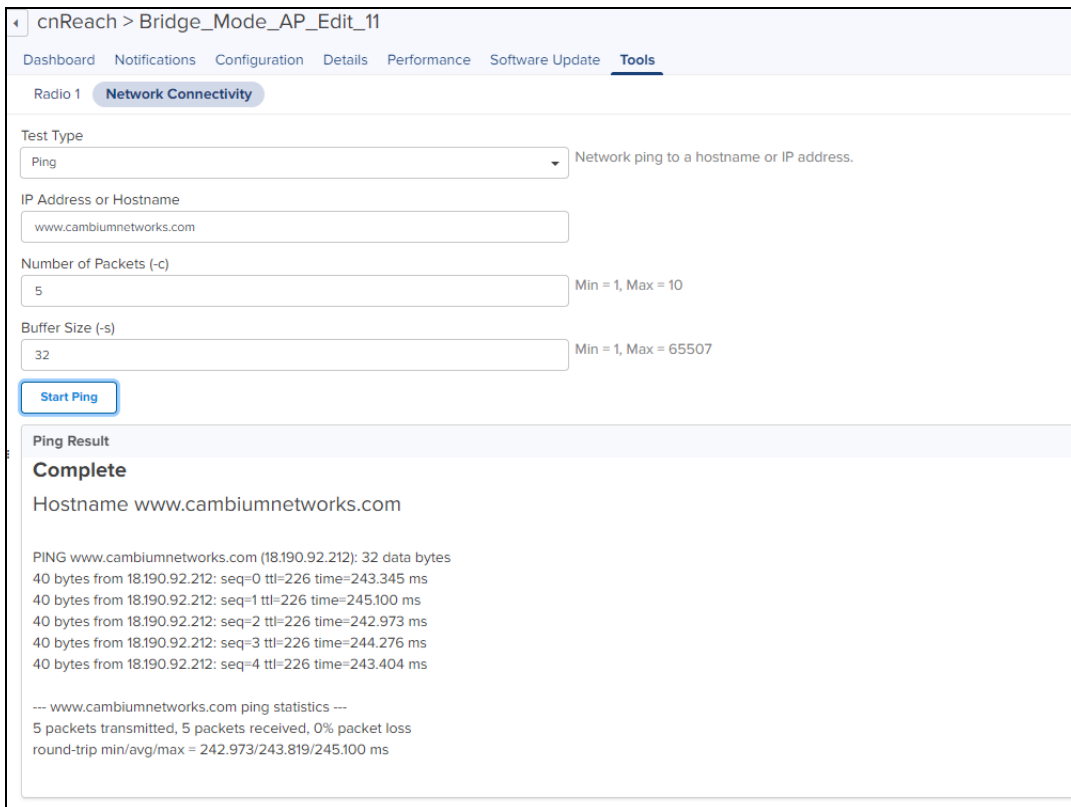
cnReach Tools

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

Table 26: 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 28 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 27: cnVision Tools

Field	Description
Debug	Displays the log details.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the Status.

Table 27: cnVision Tools

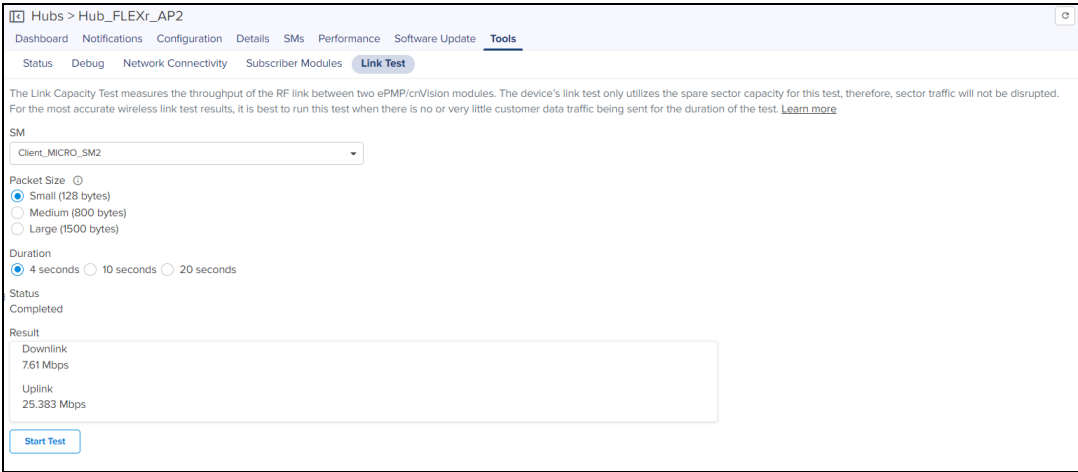
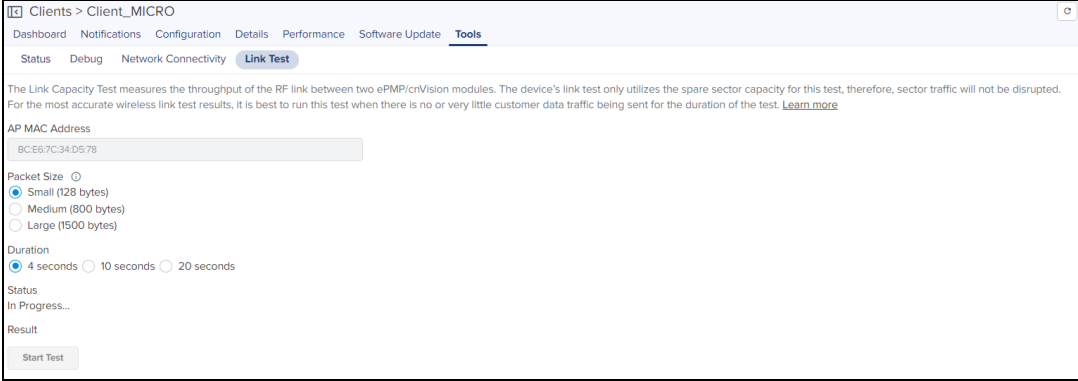
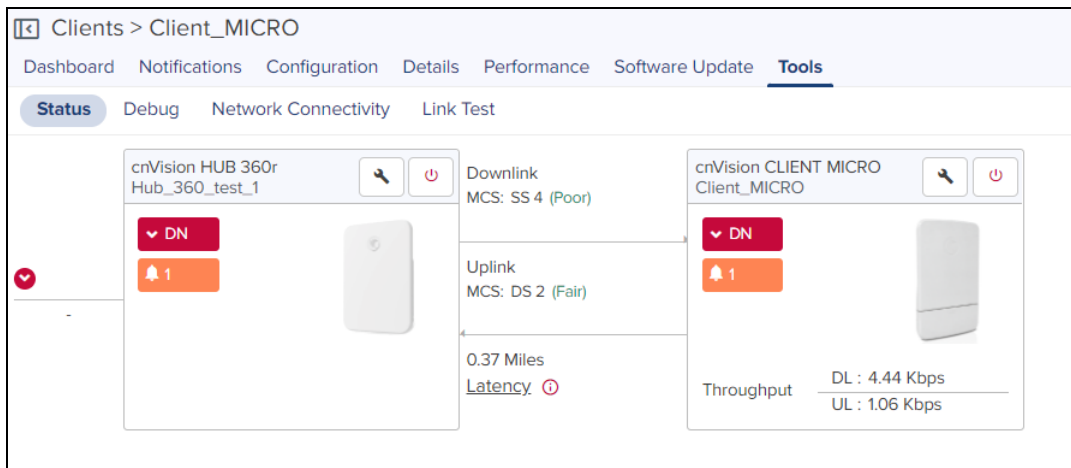
Field	Description
Subscriber Modules	Displays the SM linked to the Hub and allows to reboot and download the tech support file.
Link Test	<p>The Link Capacity Test measures the throughput of the RF link between two cnVision modules. cnVision link test only utilizes the spare sector capacity for this test, therefore, sector traffic will not be disrupted. For the most accurate wireless link test results, it is best to run this test when there is no or very little customer data traffic being sent for the duration of the test.</p> <p>Displays the link related test result with respect to Throughput. Link Test can be performed on the cnVision Hub and its SM link. In order to run this operation, select the device and then the Tools tab.</p> <ul style="list-style-type: none"> • If an cnVisiosn Hub is selected you can choose the SM from the list and start the test.  <p>Displays the following fields:</p> <ul style="list-style-type: none"> • Packet Size: Choose the Packet Size to use for the throughput test. • Duration: Choose the time duration in seconds to use for the throughput test. • If an cnVision Client is selected, click Start Test to run the link test.  <p>Displays the following fields:</p> <ul style="list-style-type: none"> • Packet Size: Choose the packet size to use for the throughput test. • Duration: Choose the time duration in seconds to use for the throughput test.

Figure 29 cnVision Tools



Enterprise Wi-Fi Tools

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

The operations of Enterprise Wi-Fi are listed below:

Table 28: Enterprise Wi-Fi Tools

Tools	Description
Debug	Displays the log details.
Flash LEDs (Only for E Series Device)	The LEDs of the device enables to identify and locate the device.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Packet Capture	Lists packet capture details.
Remote CLI	Remote CLI mode is enabled for super admin and admin users only. But only show commands can be executed by operator. The user can provide the CLI command in the Command textbox. The output will be displayed in the output window.
Status	Displays the status of device.
Wi-Fi Analyzer	Displays radio traffic and signal.
Wi-Fi Performance (wifiperf)	Wi-Fi performance measures the backhaul speed across devices with respect to cnMaestro.

Figure 30 Enterprise Wi-Fi Tools

The screenshot shows the 'Wi-Fi > E500-BB15702' interface. The 'Tools' tab is active, and the 'Debug' sub-tab is selected. A 'Stop Logs' button is visible. An 'Output' window is open, displaying a log of system events:

```
2021-05-25 07:05:27 749 device-agent.c:667:PING_DATA: len=28 msg [{"Pid": "749", "PLoss": "0"}]
May 25 07:05:27: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2871)
May 25 07:05:30: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2871)
May 25 07:05:33: scmd : prev_tx 150983395 curr_tx 0 (stats.c:1052)
May 25 07:05:33: scmd : prev_rx 1034060344 curr_rx 0 eth index 0 (stats.c:1053)
May 25 07:05:34: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2871)
May 25 07:05:40: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2871)
May 25 07:05:43: wifid : lldp frame:dmac 01-80-C2-00-00-0E smac B0-B9-8A-6E-F1-03 type 88cc (lldp.c:89)
May 25 07:05:46: scmd : stats timer at 1621926346 (stats.c:196)
2021-05-25 07:05:52 749 device-agent.c:667:PING_DATA: len=28 msg [{"Pid": "749", "PLoss": "0"}]
2021-05-25 07:11:09 749 log.c:207:start_cns_logging: Send log history (10 lines)
May 25 07:05:54: scmd : Device IP 10.110.208.137 (stats.c:346)
2021-05-25 07:05:54 749 wifi.c:948:Stats read successfully cleanup g_scm_fd
```

Figure 31 Enterprise Wi-Fi Remote CLI Tools

The screenshot shows the 'Wi-Fi > E500-BB15702' interface. The 'Tools' tab is active, and the 'Remote CLI' sub-tab is selected. A 'Command' input field is present with the placeholder text 'Type CLI command'. A 'Run' button is visible. An 'Output' window is open, displaying the output of the 'show config' command:

```
Device >
Device > show config
!
management user admin password $crypt$1$bC50U7LVxFK9C5sE5ZpFOgYl7ssnFRYm
no management radius-auth
management cambium-remote
management cambium-remote url 10.110.209.84
management cambium-remote validate-server-cert
no management telnet
management ssh
management ssh idle-timeout 300
management http
management http port 80
management https
management https port 443
```

Figure 32 Enterprise Wi-Fi Packet Capture

Interface	Packets	Duration	Size	Filter	Start Time	Expires In	Status
Tunnel (bcp0)	241	2m/2m	28.3 KB/10 MB	-	07 Oct 2021 21:47	0d 0h 0m	Uploaded
Radio1	28565	1m 45s/2m	10.0 MB/10 MB	-	07 Oct 2021 21:47	0d 0h 0m	Uploaded
Vlan 1	5296	1m 59s/2m	4.3 MB/10 MB	-	07 Oct 2021 21:47	0d 0h 0m	Uploaded
Eth1	5475	2m/2m	4.3 MB/10 MB	-	07 Oct 2021 21:47	0d 0h 0m	Uploaded
Radio3 (Channel: 2)	874	4s/2m	348.1 KB/10 MB	(type mgt subtype beacon)	07 Oct 2021 21:42	0d 0h 0m	Uploaded
Radio1	0	2m	10 MB	-	07 Oct 2021 21:40	-	Failed
SSID (diva_pact)	986	1m 59s/2m	83.2 KB/10 MB	-	07 Oct 2021 21:38	0d 0h 0m	Uploaded
Vlan 50	29	2m/2m	2.4 KB/10 MB	-	07 Oct 2021 21:35	0d 0h 0m	Uploaded
Vlan 215	0	2m	10 MB	-	11 Oct 2021 13:17	-	Failed
Vlan 115	6	51s/2m	2.1 KB/10 MB	-	07 Oct 2021 21:34	0d 0h 0m	Uploaded

Packet Capture

The Packet Capture allows the user to capture all packets on a specified interface simultaneously. The user can trigger packet capture on an interface (or multiple interfaces simultaneously). The main input for packet capture is by selecting type of interface and filter options.



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**.

Interface	Packets	Duration	Size	Filter	Start Time	Expires In	Status
Radio1	227	9s/2m	84.2 KB/10 MB	-	19 Oct 2021 11:38	0d 15h 51m	Uploaded
Eth1	0	2m	10 MB	-	-	-	Not Started

Table 29: Packet Capture field

Field	Description
Duration	Represents packet capture running duration in seconds versus maximum duration configured.
Expires In	Expiry time of packet capture. By default the packets captured expires in 24 hours.
Filter	Type of filter option opted by user.
Interface	The following interfaces supports the packet capture: <ul style="list-style-type: none"> • Ethernet • Radio • Wireless LAN • VLAN • SSID • TUNNEL • BRIDGE • PPPoE
Packets	Represents number of packets captured versus maximum limit of packet count configured.
Size	Current packet capture size versus maximum packet capture size configured.
Start Time	Start time of the capture.
Status	Status of packet captured is as follows: <ul style="list-style-type: none"> • Queued • Failed • Skipped • Aborted

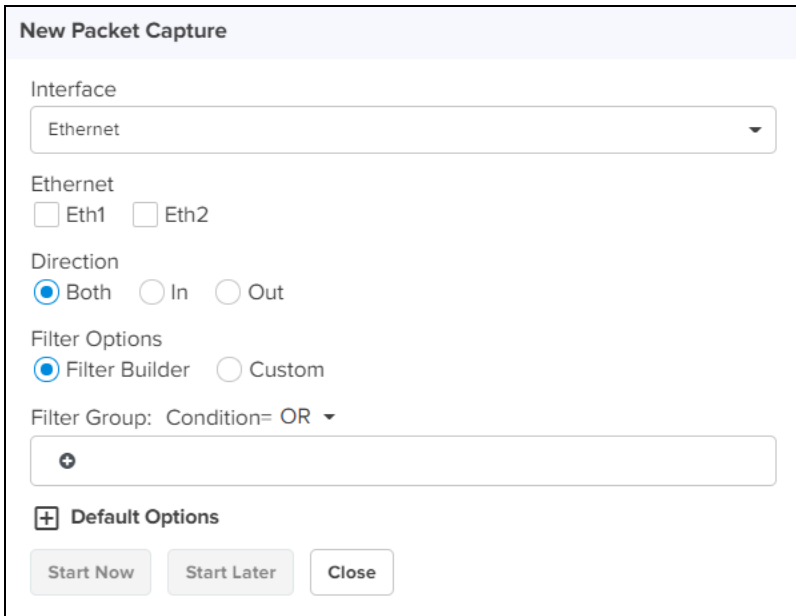
New Packet Capture

Perform the following steps to start a new packet capture:

**NOTE:**

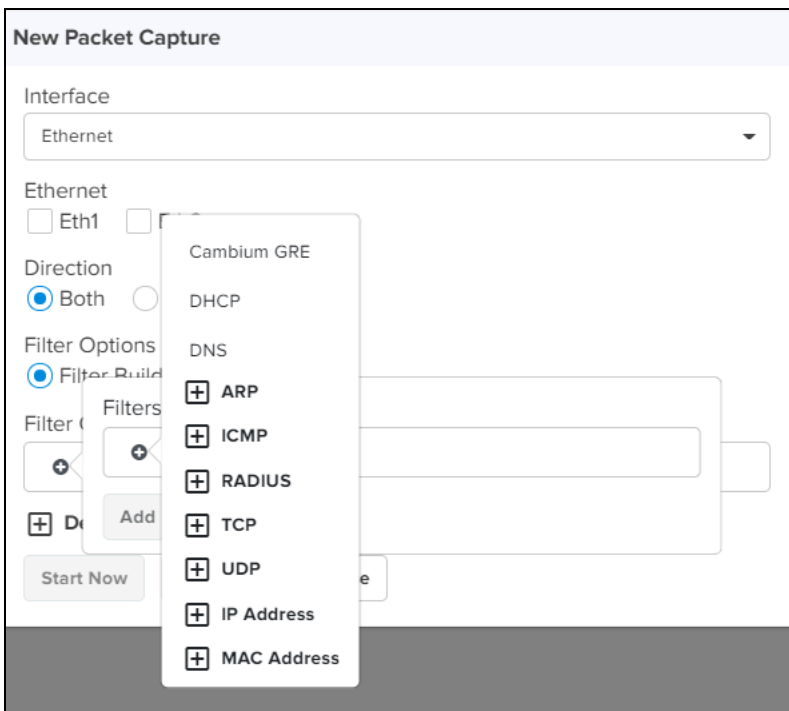
- Filter options vary for different interfaces (Radio, Wireless LAN, VLAN, SSID, TUNNEL, BRIDGE, and PPPoE. Radio, SSID has wireless 802.11 filters, other interfaces has wired 802.3 filters).
- User can also add custom filters if needed.

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



2. Select the **Interface** type from the drop-down list.
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**.

New Packet Capture

Interface: Ethernet

Ethernet
 Eth1 Eth2

Direction
 Both In Out

Filter Options
 Filter Builder Custom

Filter Group: Condition= OR

+ [Empty Filter Field]

Default Options


Packets: 0
 0 to 65535 (default 0 indicates unlimited)


Duration: 120
 1 to 600 (default 120) seconds

Packet Length: 0
 0 to 1500 (default 0 indicates full packet length)

File Size: 10
 1 to 50 (default is 10 MB on 11ax APs)

Start Now Start Later Close

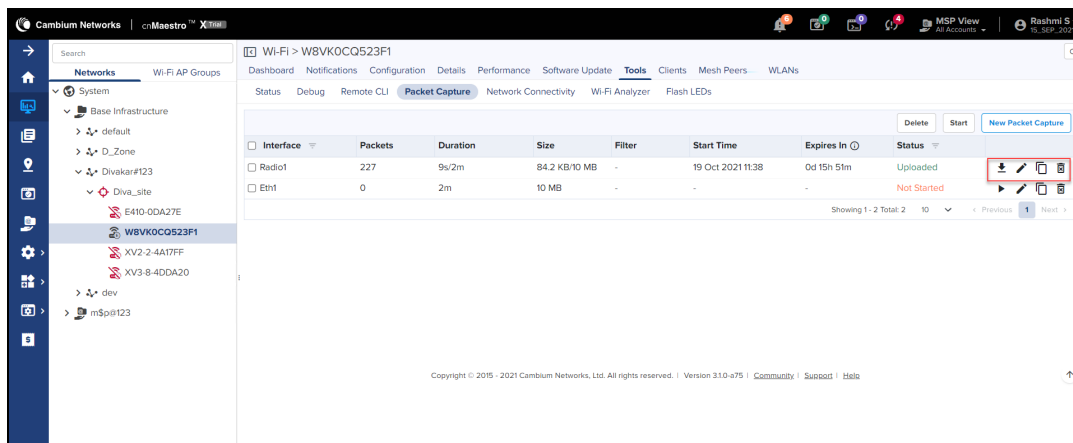
- Click **Start Now** to capture the packets immediately or start the capture later by selecting **Start Later** option. The progress of packets captured can be seen in **Status** field.
- Click download  icon to download the packets post completion in **PCAP** file format.



NOTE:

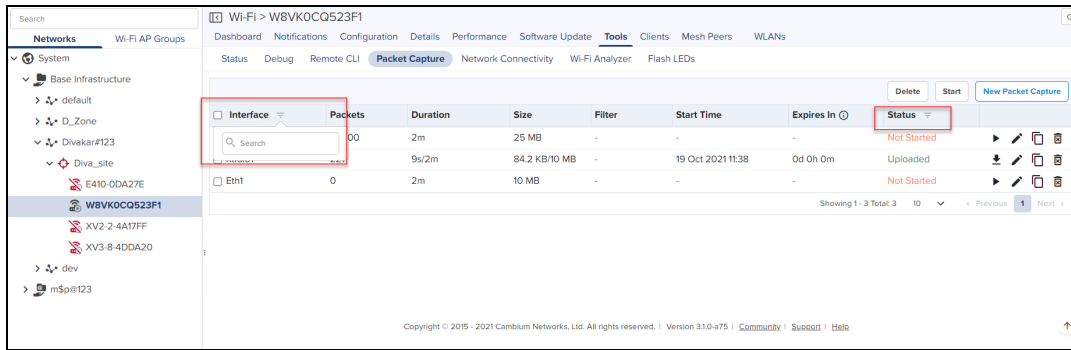
For cnMaestro X, a maximum of four sessions of packet capture is supported whereas for cnMaestro Essentials a maximum of two sessions of packet capture is supported.

The user can **Edit**, **Clone**, and **Delete** the packets captured. Packets captured can be cloned depending on the type of interface opted during the start of the capture.



Interface	Packets	Duration	Size	Filter	Start Time	Expires In	Status
Radio1	227	9s/2m	84.2 KB/10 MB	-	19 Oct 2021 11:38	0d 15h 51m	Uploaded
Eth1	0	2m	10 MB	-	-	-	Not Started

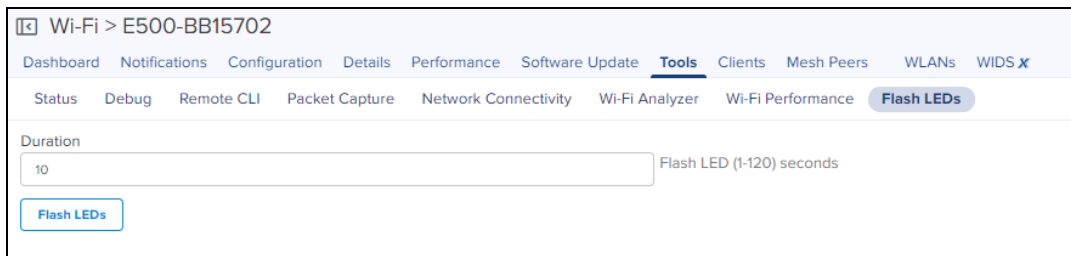
The user can search the packet capture by **Interface** type and **Status**.



NOTE:

- User can start packet capture by clicking **Play** button for packet capture stopped at **Not Started/Failed/ Expired**.
- **Bulk Start** and **Bulk Delete** can be done by selecting multiple packet capture settings.
- Expired packet capture is deleted from cnMaestro after 7 days.
- Packet capture is removed immediately, when device(AP) is deleted from cnMaestro.
- Packet capture cannot be started on same interface simultaneously.
- Only **Show** command works for user like Operator.

Figure 33 Flash LEDs

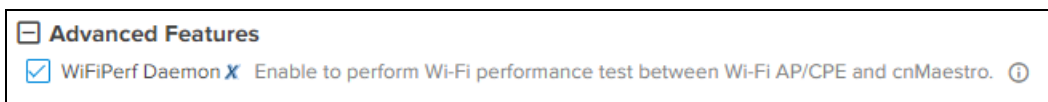


Wi-Fi Performance Test

Currently, Wi-Fi performance test feature is supported only on cnPilot devices. Wi-Fi performance test will be triggered between the AP and Wi-FiPerf Endpoint.

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

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



- **Locally installed Wi-Fi Performance Server** : Wifiperf performance inter-operates with the open source zapwireless tool.

(<https://code.google.com/archive/p/zapwireless/>). So install zap on the local host on the site. This is especially helpful in the scenarios to troubleshoot connectivity/performance issues related to Wi-Fi AP/Client in a site.



To configure locally installed site level speed test server on cnMaestro, navigate to **Site > Configuration > Wi-FiPerf Server** page.

WiFiPerf Server Pro

This option allows you to configure WiFiPerf daemon at a site level in order to perform wireless performance test between Wi-Fi AP/Client and this daemon. This is especially helpful in the scenarios to troubleshoot connectivity/performance issues related to Wi-Fi AP/Client in a site, where cnMaestro instance is remote and not really part of the site network. Please ensure that open source zapd is running on below host before initiating the WiFiPerf test.

WiFiPerf ⓘ

Host:

	<p>NOTE: The Wifiperf manager running on cnMaestro establishes control session with AP (and other endpoint-local host) using TCP port number 18301. So it is mandatory that both the AP and the other endpoint is reachable from cnMaestro. Make sure that the NAT/firewall does not block the wifiperf traffic from cnMaestro to any endpoint or AP (also between the endpoints and AP). Ensure that the port number 18301 is not blocked in the network for TCP and UDP.</p>
	<p>NOTE: For more details on Wi-Fi performance (wifiperf) feature, refer here.</p>

Performing the Test:

To run the Wi-Fi performance test, navigate to **Tools > Wi-Fi Performance** page.

It can be used to measure the following parameters with intervals of 10, 20 and 30 seconds:

Traffic Types

- TCP
- UDP

Traffic Direction

- Downlink
- Uplink

WiFiPerf Endpoint

- cnMaestro
- WiFi Perf Local Host

ePMP Tools

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

The operations are listed below:

Table 30: ePMP Tools

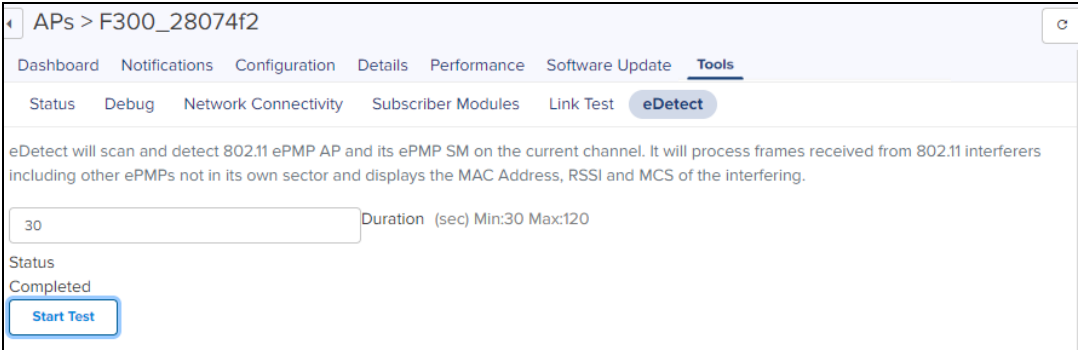
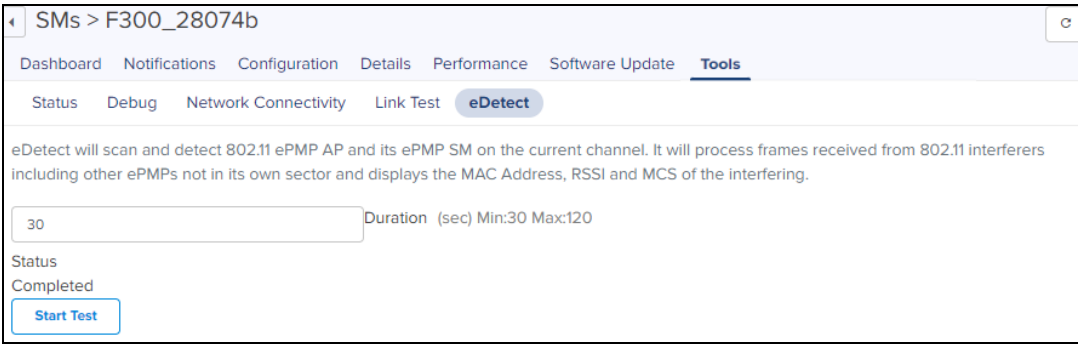
Tools	Description
Debug	Displays the log details.
eDetect	<p>eDetect is supported on the ePMP AP or SM. It is also launched from the Tools tab.</p> <p>The eDetect tool (not available in ePMP Master/Slave mode) is used to measure the 802.11 interference at the ePMP radio or system when run from the AP or the SM, on the current operating channel. When the tool is run, the ePMP device processes all frames received from devices not connected to the ePMP system and collects the interfering frame's information such as MAC Address, RSSI, and MCS.</p> <p>Configure the duration for which the AP scans for interference.</p>  <p>Configure the duration for which the SM scans for interference.</p> 
Link Test	<p>The Link Capacity Test measures the throughput of the RF link between two ePMP modules. ePMP's 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 no or very little customer data traffic being sent for the duration of the test..</p> <p>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.</p> <ul style="list-style-type: none"> ● If an ePMP AP is selected you can choose the SM from the list and start the test.

Table 30: ePMP Tools

Tools	Description
	<div data-bbox="397 226 1469 970" style="border: 1px solid #ccc; padding: 10px;"> <p>APs > F300_28074f2 c</p> <p>Dashboard Notifications Configuration Details Performance Software Update Tools</p> <p>Status Debug Network Connectivity Subscriber Modules Link Test eDetect</p> <p>The Link Capacity Test measures the throughput of the RF link between two ePMP modules. ePMP's 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 no or very little customer data traffic being sent for the duration of the test. Learn more</p> <p>SM</p> <p>F300_28074b</p> <p>Packet Size ⓘ</p> <p><input checked="" type="radio"/> Small (128 bytes)</p> <p><input type="radio"/> Medium (800 bytes)</p> <p><input type="radio"/> Large (1500 bytes)</p> <p>Duration</p> <p><input checked="" type="radio"/> 4 seconds <input type="radio"/> 10 seconds <input type="radio"/> 20 seconds</p> <p>Status</p> <p>Completed</p> <p>Result</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>Downlink</p> <p>32.635 Mbps</p> <p>Uplink</p> <p>32.104 Mbps</p> </div> <p>Start Test</p> </div> <p>Displays the following fields:</p> <ul style="list-style-type: none"> ● Packet Size: Choose the packet size to use for the throughput test. ● Duration: Choose the time duration in seconds to use for the throughput test. ● If an ePMP SM is selected, click Start Test to run the link test.

Table 30: ePMP Tools

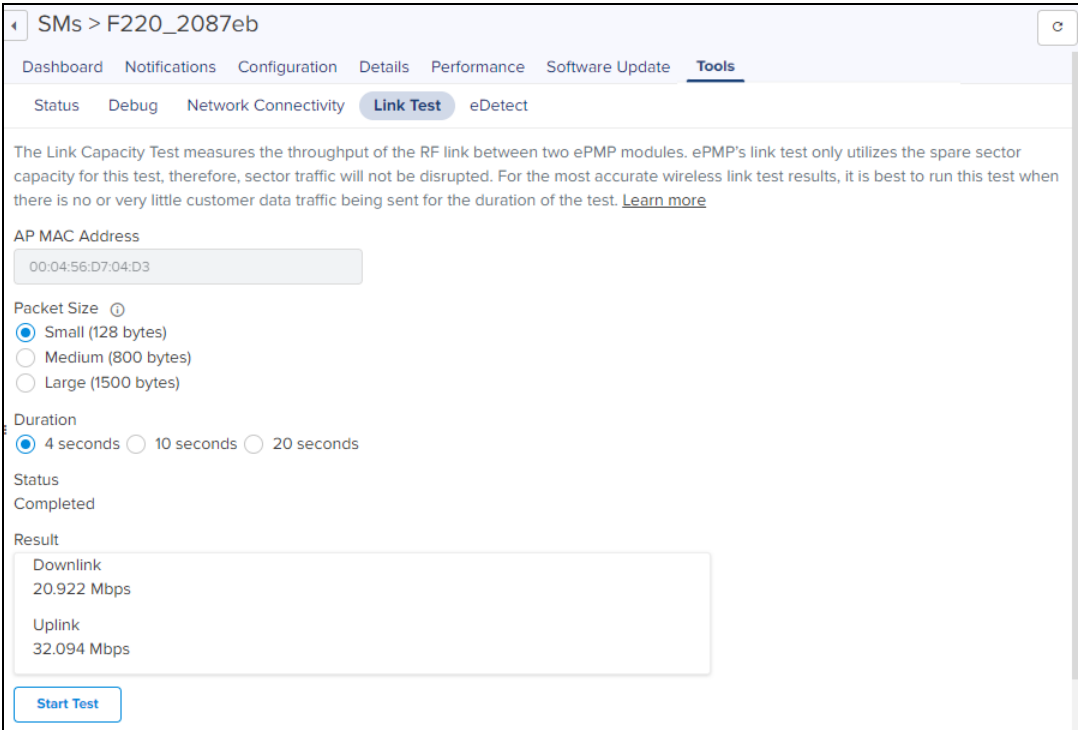
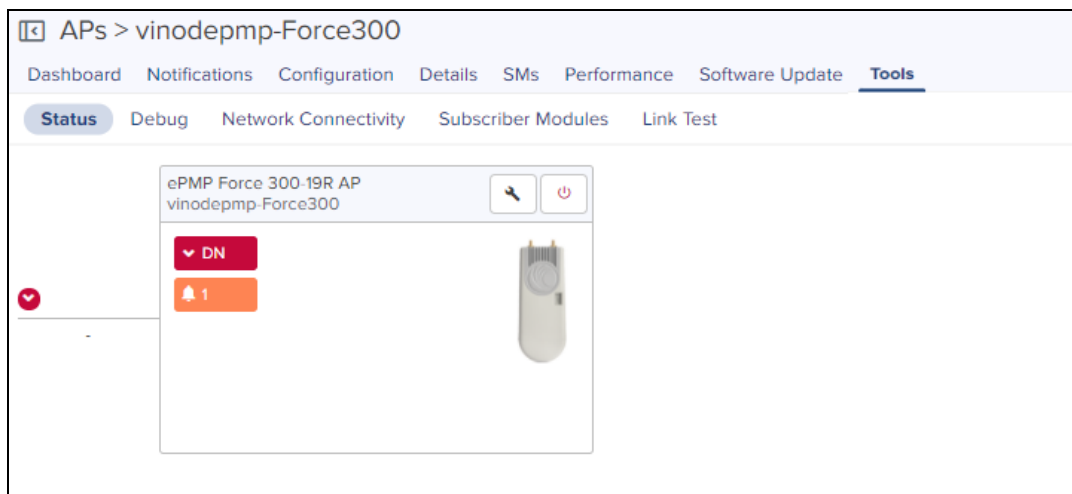
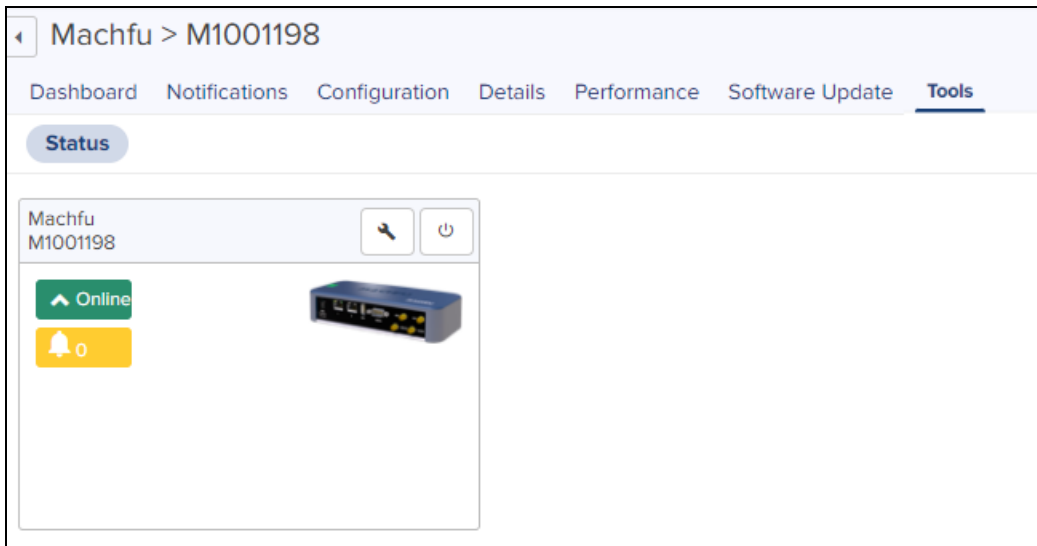
Tools	Description
	 <p>Displays the following fields:</p> <ul style="list-style-type: none"> ● Packet Size: Choose the Packet Size to use for the throughput test. ● Duration: Choose the time duration in seconds to use for the throughput test.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the status.

Figure 34 ePMP Tools



Machfu

In **Status** tab you can view the status of the device either Online or Offline, allows to download Tech Support File and can reboot the device.



PMP Tools

The Tools page for PMP devices consolidates a number of operations into a single troubleshooting interface.

The operations are listed below:

Table 31: PMP Tools

Tools	Description
Debug	Displays the log details.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the status.

Table 31: PMP Tools

Tools	Description		
Subscriber Modules	Lists all the SMs connected to the selected AP. This is available for PMP APs only.		
Link Test	<p>The Link Capacity Test measures the throughput and efficiency of the RF link between two PMP modules. Many factors, including packet length, affect throughput. Packets are added to one or more queues in the AP in order to fill the frame. Throughput and efficiency are then calculated during the test</p> <p>The Link Capacity Test tool has following modes:</p> <ul style="list-style-type: none"> • Link Test without Bridging - Tests radio-to-radio communication, but does not bridge traffic. • Link Test with Bridging - Bridges traffic to “simulated” Ethernet ports, providing a status of the bridged link. • Link Test with Bridging and MIR - Bridges the traffic during test and also adheres to any MIR (Maximum Information Rate) settings for the link. • Extrapolated Link Test: Estimates the link capacity by sending few packets and measuring link quality. <p>Displays the link related test result with respect to Throughput and Interference. Link Test can be performed on the PMP AP and its SM link. In order to run this operation, select the device and then the Tools tab.</p> <ul style="list-style-type: none"> • If a PMP AP is selected you can choose the SM from the list and start the test. <div data-bbox="402 995 1479 1764" style="border: 1px solid black; padding: 10px;"> <p>APs > PMP 450i-BBC827</p> <p>Dashboard Notifications Configuration Details Performance Software Update Tools</p> <p>Status Debug Network Connectivity Subscriber Modules Link Test</p> <p>The Link Capacity Test measures the throughput and efficiency of the RF link between two PMP modules. Many factors, including packet length, affect throughput. Flood Link test is available for cnMedusa AP with software version of 15.2 or higher. Learn more</p> <p>Link Test Mode</p> <p>Link Test with Bridging ⓘ</p> <p>ⓘ Sector traffic will be disrupted for 2 seconds.</p> <p>Current SM</p> <p>450b SM1</p> <p>Packet Length</p> <p>1714 ⓘ Bytes (64 — 1714 Bytes)</p> <p>Re-Test</p> <p>Result</p> <table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 50%;"> <p>Downlink</p> <p>442.37 Kbps</p> <p>99% Efficient</p> <p>Signal to Noise Ratio: 36 dB V, 35 dB H</p> </td> <td style="width: 50%;"> <p>Uplink</p> <p>442.37 Kbps</p> <p>100% Efficient</p> <p>Signal to Noise Ratio: 41 dB V, 43 dB H</p> </td> </tr> </table> </div> <ul style="list-style-type: none"> • If a PMP SM is selected, click Start Test to run the link test. 	<p>Downlink</p> <p>442.37 Kbps</p> <p>99% Efficient</p> <p>Signal to Noise Ratio: 36 dB V, 35 dB H</p>	<p>Uplink</p> <p>442.37 Kbps</p> <p>100% Efficient</p> <p>Signal to Noise Ratio: 41 dB V, 43 dB H</p>
<p>Downlink</p> <p>442.37 Kbps</p> <p>99% Efficient</p> <p>Signal to Noise Ratio: 36 dB V, 35 dB H</p>	<p>Uplink</p> <p>442.37 Kbps</p> <p>100% Efficient</p> <p>Signal to Noise Ratio: 41 dB V, 43 dB H</p>		

Table 31: PMP Tools

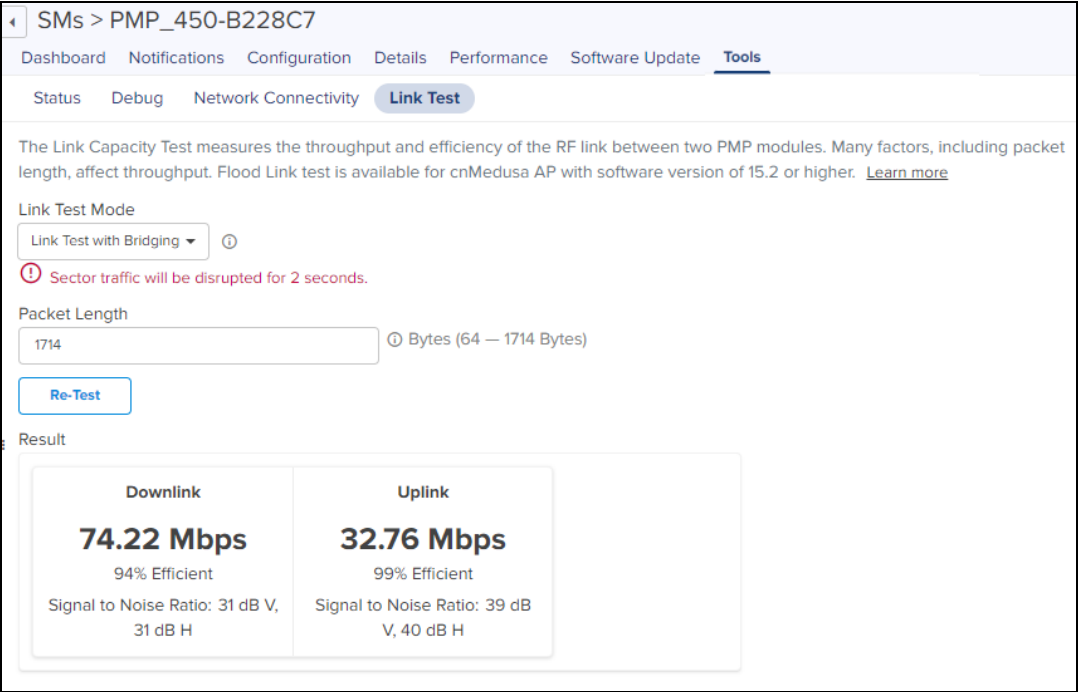
Tools	Description								
	 <p>SMS > PMP_450-B228C7</p> <p>Dashboard Notifications Configuration Details Performance Software Update Tools</p> <p>Status Debug Network Connectivity Link Test</p> <p>The Link Capacity Test measures the throughput and efficiency of the RF link between two PMP modules. Many factors, including packet length, affect throughput. Flood Link test is available for cnMedusa AP with software version of 15.2 or higher. Learn more</p> <p>Link Test Mode</p> <p>Link Test with Bridging ⓘ</p> <p>ⓘ Sector traffic will be disrupted for 2 seconds.</p> <p>Packet Length</p> <p>1714 ⓘ Bytes (64 – 1714 Bytes)</p> <p>Re-Test</p> <p>Result</p> <table border="1"> <thead> <tr> <th>Downlink</th> <th>Uplink</th> </tr> </thead> <tbody> <tr> <td>74.22 Mbps</td> <td>32.76 Mbps</td> </tr> <tr> <td>94% Efficient</td> <td>99% Efficient</td> </tr> <tr> <td>Signal to Noise Ratio: 31 dB V, 31 dB H</td> <td>Signal to Noise Ratio: 39 dB V, 40 dB H</td> </tr> </tbody> </table>	Downlink	Uplink	74.22 Mbps	32.76 Mbps	94% Efficient	99% Efficient	Signal to Noise Ratio: 31 dB V, 31 dB H	Signal to Noise Ratio: 39 dB V, 40 dB H
Downlink	Uplink								
74.22 Mbps	32.76 Mbps								
94% Efficient	99% Efficient								
Signal to Noise Ratio: 31 dB V, 31 dB H	Signal to Noise Ratio: 39 dB V, 40 dB H								

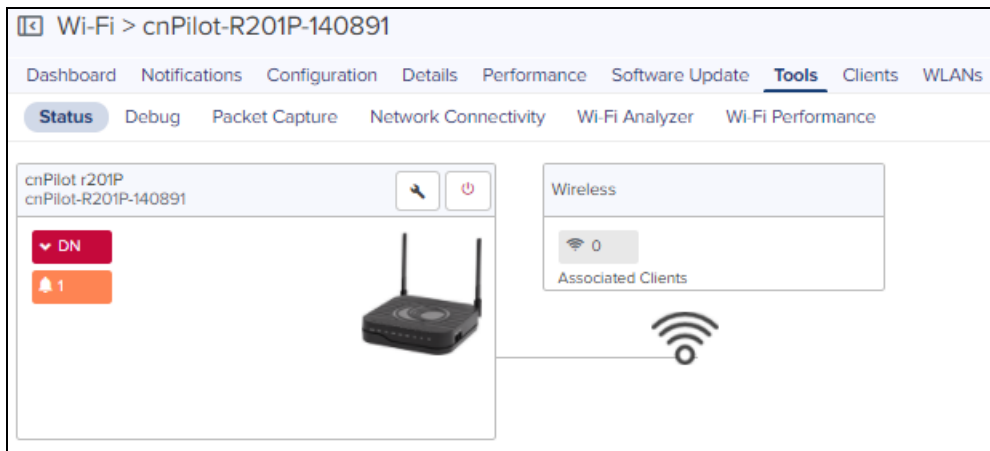
Figure 35 PMP Tools



Tower-to-Edge view

This component displays the network from the Point-to-Multipoint AP to the edge Enterprises devices.

Figure 36 Tower-to-Edge view



WIDS

This section provides details on Rogue APs.

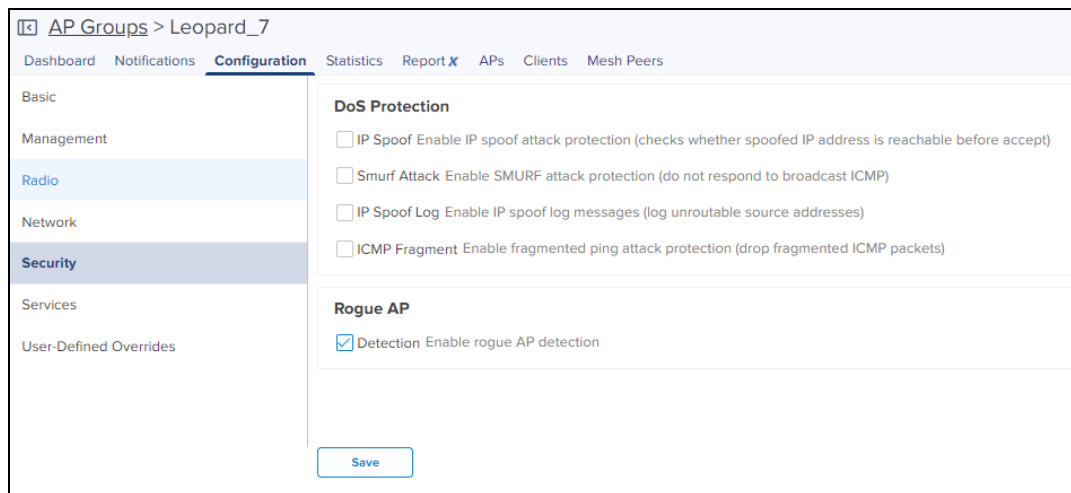
Detecting Rogue APs

A rogue AP is an unsanctioned AP, which is not onboarded to cnMaestro. The AP scans the channels, collects the details about the neighbor APs and sends them to cnMaestro.

Configuring Rogue AP

To enable Rogue AP feature:

1. Navigate to **AP Groups > Configuration > Security** page.
2. Select **Rogue AP Detection** checkbox.



To enable OCS (Off Channel Scan):

1. Navigate to **AP Groups > Configuration > Radio** (Available on both radio 2.4 GHz and 5 GHz) page.
2. Select the **Enable OCS** checkbox under **OCS** tab.

Off-Channel Scan

Enable **Enable OCS**

Dwell-time
 Configure Off-Channel-Scan dwelltime in milliseconds (50-300)

Auto RF

Save

You can grant valid APs to provide secure access to the network by adding them to the Whitelist by providing their MAC address and SSID.

To add Rogue APs to whitelist:

1. Navigate to **APs > WIDS** page.
2. Click **Add Whitelist** under **Site Whitelist** tab.
3. Enter **MAC** and **SSID** of the device to be whitelisted.
4. Click **Save**.

Site Whitelist

These values are shared across all APs at the Site.

Add Whitelist **Delete All**

SSID	BSSID	Manufacturer
Requires placement in Site		

Showing 0 of 0 entries

The whitelisted Rogue AP WLAN will be grayed out in Rogue AP list and it will be removed after 24 hours.

Rogue APs (Last 24 Hours)

Whitelist 0 devices

SSID	MAC	Channel	First Seen	Last Seen	Signal (dBm)	Manufacturer
CambiumMobile	88:8E:8E:8E:8E:8E	6	Thu Apr 11 2019 15:37	Wed Apr 24 2019 11:03	-36	Cambium Networks Limited
CambiumGuest	88:8E:8E:8E:8E:8E	6	Tue Apr 23 2019 14:38	Wed Apr 24 2019 11:03	-37	Cambium Networks Limited
Cambium	88:8E:8E:8E:8E:8E	6	Thu Apr 11 2019 15:37	Wed Apr 24 2019 11:03	-38	Cambium Networks Limited
1 NAT Test	88:8E:8E:8E:8E:8E	11	Wed Apr 17 2019 15:26	Wed Apr 24 2019 11:03	-38	Cambium Networks Limited
Auto_pilot_3	88:8E:8E:8E:8E:8E	1	Mon Apr 22 2019 16:06	Tue Apr 23 2019 11:21	-39	Cambium Networks Limited
Auto_pilot_1	88:8E:8E:8E:8E:8E	6	Mon Apr 22 2019 16:06	Tue Apr 23 2019 11:16	-40	Cambium Networks Limited
Auto_pilot_4	88:8E:8E:8E:8E:8E	1	Mon Apr 22 2019 16:21	Tue Apr 23 2019 11:21	-40	Cambium Networks Limited
EPSK-Test2	88:8E:8E:8E:8E:8E	6	Thu Apr 11 2019 15:37	Wed Apr 24 2019 11:03	-40	Cambium Networks Limited
BugVerification2.4GHz_2_4_1	88:8E:8E:8E:8E:8E	1	Tue Apr 23 2019 17:08	Tue Apr 23 2019 17:58	-41	Cambium Networks Limited
BugVerification2.4GHz_2_4_2	88:8E:8E:8E:8E:8E	1	Tue Apr 23 2019 17:03	Tue Apr 23 2019 17:58	-41	Cambium Networks Limited

Showing 1 - 10 Total: 501

To whitelist multiple Rogue APs:

1. Select the Rogue APs in the list.
2. Click **Whitelist Devices**.

Rogue APs (Last 24 Hours)

Search [] Whitelist 2 devices

SSID	MAC	Channel	First Seen	Last Seen	Signal (dBm)	Manufacturer
CambiumMobile	88:88:88:88:88:88	6	Thu Apr 11 2019 15:37	Wed Apr 24 2019 11:03	-36	Cambium Networks Limited
CambiumGuest	88:88:88:88:88:88	6	Tue Apr 23 2019 14:38	Wed Apr 24 2019 11:03	-37	Cambium Networks Limited
Cambium	88:88:88:88:88:88	6	Thu Apr 11 2019 15:37	Wed Apr 24 2019 11:03	-38	Cambium Networks Limited
1 NAT Test	88:88:88:88:88:88	11	Wed Apr 17 2019 15:26	Wed Apr 24 2019 11:03	-38	Cambium Networks Limited
Auto_pilot_3	88:88:88:88:88:88	1	Mon Apr 22 2019 16:06	Tue Apr 23 2019 11:21	-39	Cambium Networks Limited
Auto_pilot_1	88:88:88:88:88:88	6	Mon Apr 22 2019 16:06	Tue Apr 23 2019 11:16	-40	Cambium Networks Limited
Auto_pilot_4	88:88:88:88:88:88	1	Mon Apr 22 2019 16:21	Tue Apr 23 2019 11:21	-40	Cambium Networks Limited
EPSC-Test2	88:88:88:88:88:88	6	Thu Apr 11 2019 15:37	Wed Apr 24 2019 11:03	-40	Cambium Networks Limited
BugVerification2.4GHz_2_4_1	88:88:88:88:88:88	1	Tue Apr 23 2019 17:08	Tue Apr 23 2019 17:58	-41	Cambium Networks Limited
BugVerification2.4GHz_2_4_2	88:88:88:88:88:88	1	Tue Apr 23 2019 17:03	Tue Apr 23 2019 17:58	-41	Cambium Networks Limited

Showing 1 - 10 Total: 501

The following pop-up is displayed after successfully adding the Rogue APs to the whitelist.

Success
Whitelist added Successfully. The device(s) will be removed from the Rogue APs list within 5 minutes.

Wi-Fi > E510-C18B5F

Last Seen: Apr 23 11:04 AM

Rogue APs (Last 24 Hours)

Search [] Whitelist 0 devices

SSID	MAC	Channel	First Seen	Last Seen	Signal (dBm)	Manufacturer
CambiumMobile	88:88:88:88:88:88	6	Thu Apr 11 2019 15:37	Wed Apr 24 2019 11:03	-36	Cambium Networks Limited
CambiumGuest	88:88:88:88:88:88	6	Tue Apr 23 2019 14:38	Wed Apr 24 2019 11:03	-37	Cambium Networks Limited
Cambium	88:88:88:88:88:88	6	Thu Apr 11 2019 15:37	Wed Apr 24 2019 11:03	-38	Cambium Networks Limited
1 NAT Test	88:88:88:88:88:88	11	Wed Apr 17 2019 15:26	Wed Apr 24 2019 11:03	-38	Cambium Networks Limited
Auto_pilot_3	88:88:88:88:88:88	1	Mon Apr 22 2019 16:06	Tue Apr 23 2019 11:21	-39	Cambium Networks Limited
Auto_pilot_1	88:88:88:88:88:88	6	Mon Apr 22 2019 16:06	Tue Apr 23 2019 11:16	-40	Cambium Networks Limited
Auto_pilot_4	88:88:88:88:88:88	1	Mon Apr 22 2019 16:21	Tue Apr 23 2019 11:21	-40	Cambium Networks Limited
EPSC-Test2	88:88:88:88:88:88	6	Thu Apr 11 2019 15:37	Wed Apr 24 2019 11:03	-40	Cambium Networks Limited

View List of Rogue APs

The user can view list of Rogue APs at the device level in the Monitor page:

Rogue APs (Last 24 Hours)

Search [] Whitelist 0 devices

SSID	MAC	Channel	First Seen	Last Seen	Signal (dBm)	Manufacturer
CambiumGuest		1	Mon Apr 15 2019 07:01	Tue Apr 16 2019 12:26	-31	Cambium Networks Limited
Ha test		11	Thu Apr 04 2019 17:01	Tue Apr 16 2019 12:26	-33	Cambium Networks Limited
Cambium		1	Thu Apr 04 2019 17:01	Tue Apr 16 2019 12:26	-34	Cambium Networks Limited
ASUS-2.4G		10	Thu Apr 11 2019 15:51	Tue Apr 16 2019 12:26	-34	ASUSTek Computer Inc.
CambiumMobile		1	Thu Apr 04 2019 17:01	Tue Apr 16 2019 12:26	-35	Cambium Networks Limited
e410_dhcp		9	Thu Apr 04 2019 17:01	Tue Apr 16 2019 12:26	-37	Cambium Networks Limited
Dns acl test		1	Fri Apr 12 2019 12:36	Tue Apr 16 2019 12:26	-39	Cambium Networks Limited
200_Test123_12		2	Mon Apr 15 2019 16:56	Tue Apr 16 2019 12:26	-41	Cambium Networks Limited
Jaggu+WLAN		11	Mon Apr 15 2019 17:56	Tue Apr 16 2019 12:26	-47	Cambium Networks Limited
WiFiChoupal		1	Tue Apr 09 2019 19:16	Tue Apr 16 2019 12:26	-49	Cambium Networks Limited

Showing 1 - 10 Total: 301

The following parameters are displayed:

- **SSID:** SSID of the Rogue AP.
- **MAC:** MAC address of the Rogue AP.
- **Channel:** Channel in which the Rogue AP operates.
- **First Seen:** Time at which the Rogue AP is detected for the first time.

- **Last Seen:** Time at which the Rogue AP is detected last.
- **Signal:** Signal strength of the Rogue AP detected by the device.
- **Manufacturer:** Manufacturer of the Rogue AP (Cambium, Cisco, Aruba, etc).

The user can view list of Rogue APs at the Site level in the Monitor page:

SSID	MAC	Channel	First Seen	Last Seen	Strongest RSSI	Detecting APs	Manufacturer
WiFiChoupal	08:00:2E:00:00:00	36	Thu Apr 11 2019 15:42	Mon Apr 22 2019 15:31	58:C1:7A:C1:8B:5F (-37 dBm)	1	Cambium Networks Limited
	08:00:2E:00:00:00	36	Thu Apr 11 2019 15:42	Mon Apr 22 2019 15:31	58:C1:7A:C1:8B:5F (-37 dBm)	1	Cambium Networks Limited
	08:00:2E:00:00:00	36	Thu Apr 11 2019 15:42	Mon Apr 22 2019 15:31	58:C1:7A:C1:8B:5F (-38 dBm)	1	Cambium Networks Limited
E400-220R33HA	08:00:2E:00:00:00	157	Thu Apr 11 2019 15:42	Mon Apr 22 2019 15:31	58:C1:7A:C1:8B:5F (-39 dBm)	1	Cambium Networks Limited
Auto_pilot_3	08:00:2E:00:00:00	1	Mon Apr 22 2019 16:06	Tue Apr 23 2019 11:21	58:C1:7A:C1:8B:5F (-39 dBm)	1	Cambium Networks Limited
CAMBUIUM_2.4GHz_1...	08:00:2E:00:00:00	6	Mon Apr 15 2019 12:27	Mon Apr 22 2019 16:16	58:C1:7A:C1:8B:5F (-40 dBm)	1	Cambium Networks Limited
Auto_pilot_1	08:00:2E:00:00:00	6	Mon Apr 22 2019 16:06	Tue Apr 23 2019 11:16	58:C1:7A:C1:8B:5F (-40 dBm)	1	Cambium Networks Limited
Auto_pilot_4	08:00:2E:00:00:00	1	Mon Apr 22 2019 16:21	Tue Apr 23 2019 11:21	58:C1:7A:C1:8B:5F (-40 dBm)	1	Cambium Networks Limited
CAMBUIUM_2.4GHz_1...	08:00:2E:00:00:00	11	Mon Apr 22 2019 16:26	Mon Apr 22 2019 16:31	58:C1:7A:C1:8B:5F (-41 dBm)	1	Cambium Networks Limited
Ha test	08:00:2E:00:00:00	149	Thu Apr 11 2019 15:42	Mon Apr 22 2019 15:31	58:C1:7A:C1:8B:5F (-43 dBm)	1	Cambium Networks Limited

The following parameters are displayed:

- **SSID:** SSID of the Rogue AP.
- **MAC:** MAC address of the Rogue AP.
- **Channel:** Channel in which the Rogue AP operates.
- **First Seen:** Time at which the Rogue AP is detected for the first time.
- **Last Seen:** Time at which the Rogue AP is detected last.
- **Strongest RSSI:** Rogue AP RSSI which is detected strongest RSSI by AP.
- **Detecting AP:** Number of APs detecting the same Rogue AP.
- **Manufacturer:** Manufacturer of the Rogue AP (Cambium, Cisco, Aruba, etc).

You can search for a specific Rogue AP based on the MAC, SSID, Channel, and the Manufacturer by using the search option.

SSID	MAC	Channel	Manufacturer
Auto_pilot_3	08:00:2E:00:00:00	1	Cambium Networks Limited
Auto_pilot_3	08:00:2E:00:00:00	6	Cambium Networks Limited
Auto_pilot_3	08:00:2E:00:00:00	11	Cambium Networks Limited



NOTE:

1. OCS (on both 2.4 GHz and 5 GHz) and Rogue AP detection should be enabled for WIDS option to work at site and device level in cnMaestro.
2. It takes 5 minutes to detect Rogue AP on AP boot up.

cnPilot Dashboards

Device Dashboard

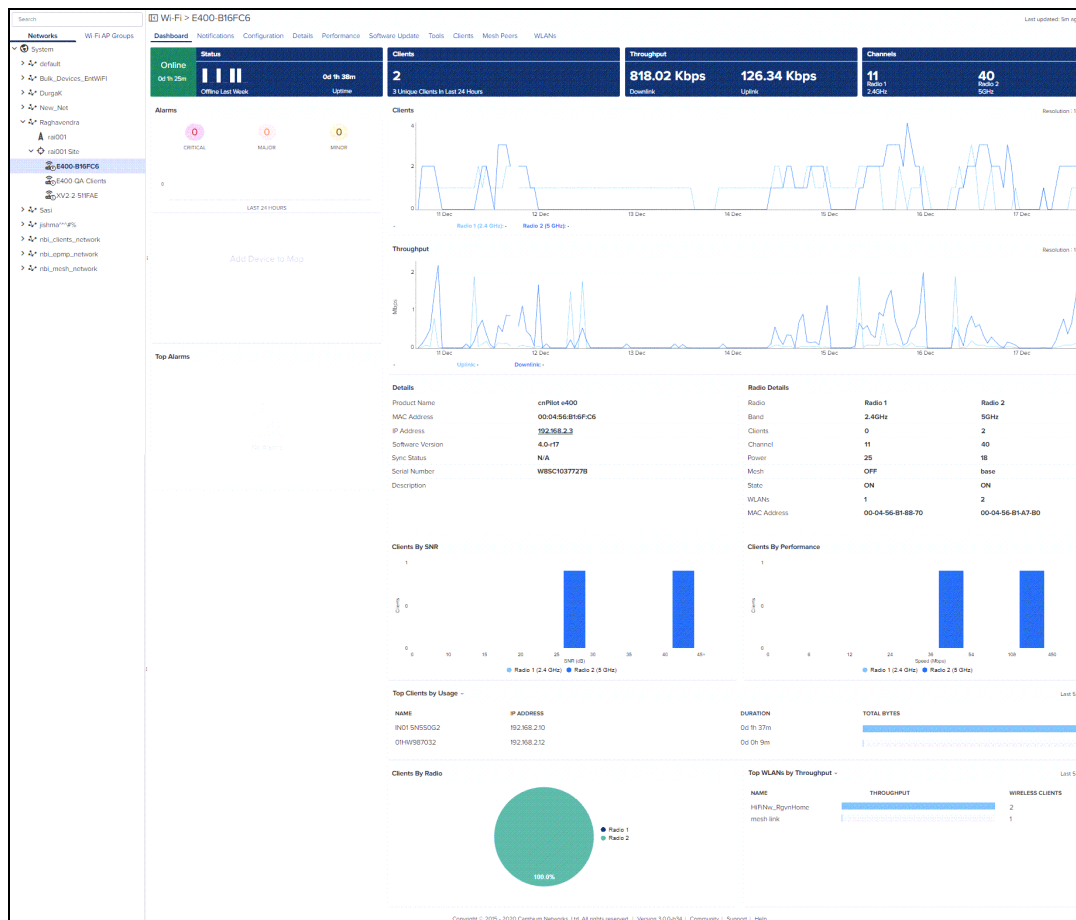
The Device Dashboard page displays details of all the Wi-Fi devices in cnMaestro. It mainly focuses on the following parameters:

- Overview
- Clients
- Network Info
- Mesh Peers
- Neighbors

Overview

The overview section displays the radio **Details**, **Clients**, **Throughput**, **Channels**, **Top Alarms**, **Clients by SNR**, **Clients by Performance**, **Clients by Radio**, **Top Clients by Usage**, and **Top WLANs by Throughput**.

Figure 37 Device Dashboard > Overview Page



Clients

The **Clients** section displays the details of all the wireless and wired clients.

Following parameters are displayed for wired clients for cnPilot Home Series:

- Address Type

- Expires
- Interface
- IP Address
- MAC Address
- Name
- Status

Figure 38 cnPilot Home: Device Dashboard > Wired Clients Page

Name	IP Address	MAC	Address Type	Expires	Interface	Status
IN01-H35G152	192.168.11.207	34:E6:D7:69:0E:2A	DHCP	65740s	LAN3	Active

Following parameters displays for Wireless Clients of R-Series:

- Band
- Download
- Host Name
- IP Address
- MAC
- Manufacturer
- RSSI
- WLAN
- Upload

Figure 39 cnPilot Home: Device Dashboard > Wireless Clients Page

Host Name	IP Address	MAC	Manufacturer	SSID	Band	Radio ID	Managed Account	RSSI	Download	Upload
Windows:Phone	192.168.11.209		Nokia Corporation	11L_RGVN_Home...	2.4Ghz	1	Base Infrastructure	-39 dBm	1.9 MB	321.9 KB

Following parameters displays for Wireless Clients of E-Series:

- Actions
- Authentication
- Band
- Client Type
- Download
- Download Quota
- Download Quota Balance
- GA Mode
- Guest Access Type
- Host Name
- IP Address
- MAC
- Manufacturer

- Managed Account
- Mode
- OS
- RSSI
- SNR
- Session Expiry
- Type
- User
- Upload
- Upload Quota
- Upload Quota Balance
- VLAN
- WLAN

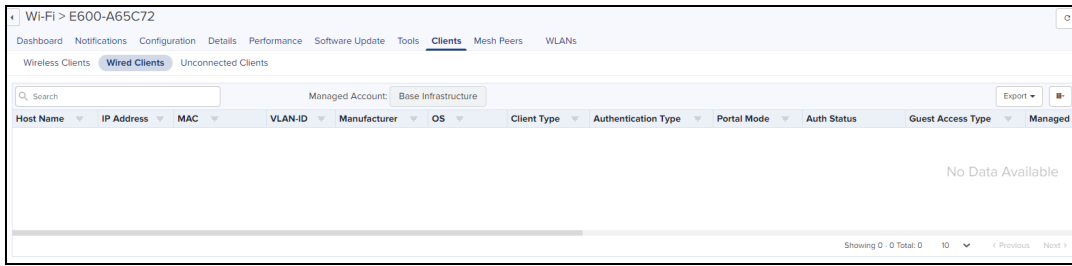
Figure 40 Enterprise Wi-Fi: Device Dashboard > Wireless Clients Page

Host Na...	User	AP	IP Address	MAC	VLAN-ID	Manufacturer	OS	SSID	Band	Radio ID	Radio Mode	RSSI	SNR	Client Type
iPhone	XV3-8-Sasi-Do-no...	XV3-8-Sasi-Do-no...	10.110.240.73	A8:5C:2C:E2:F3:BA	1	Apple	iPhone/iPad	THOR_PER...	5GHz	2	ec	-44 dBm	51 dB	Client

Following parameters displays for Wired Clients of E-Series:

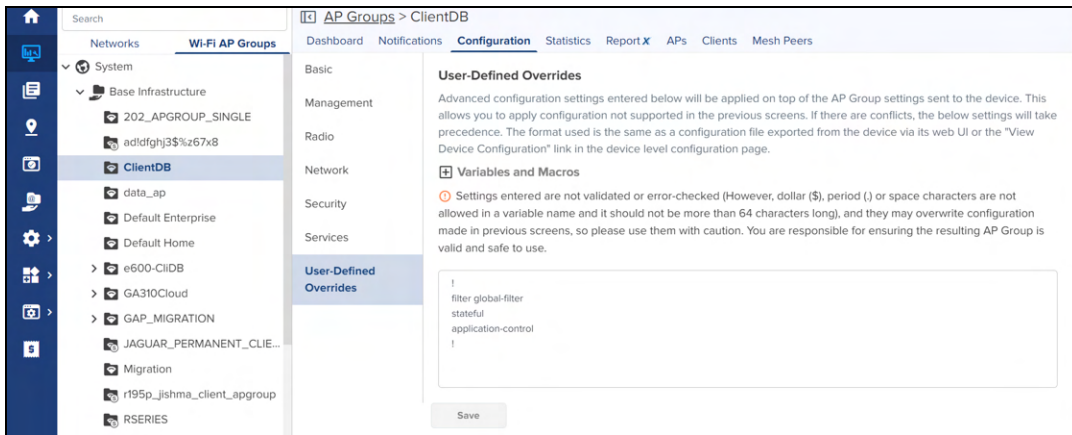
- Authentication
- Auth Status
- Client Type
- Download
- Download Quota
- Download Quota Balance
- Guest Access Type
- Host Name
- IP Address
- MAC
- Manufacturer
- OS
- Portal Mode
- Total Quota
- Total Quota Balance
- User
- Upload
- Upload Quota
- Upload Quota Balance
- VLAN

Figure 41 Enterprise Wi-Fi: Device Dashboard > Wired Clients Page



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.

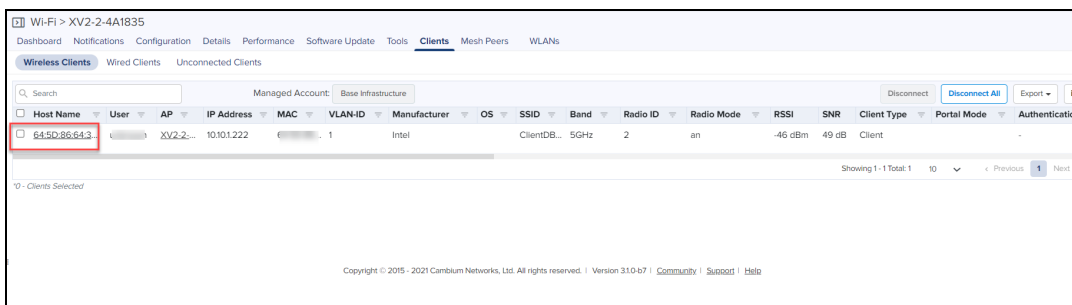
NOTE:

- Enable the Application Visibility feature to view **Application** page and supported only for XV-series devices.
- Dashboard is supported for all cnPilot devices.

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

It navigates to detailed client **Dashboard** as shown below:

Figure 42 XVseries: Device Dashboard > Wireless Client Page



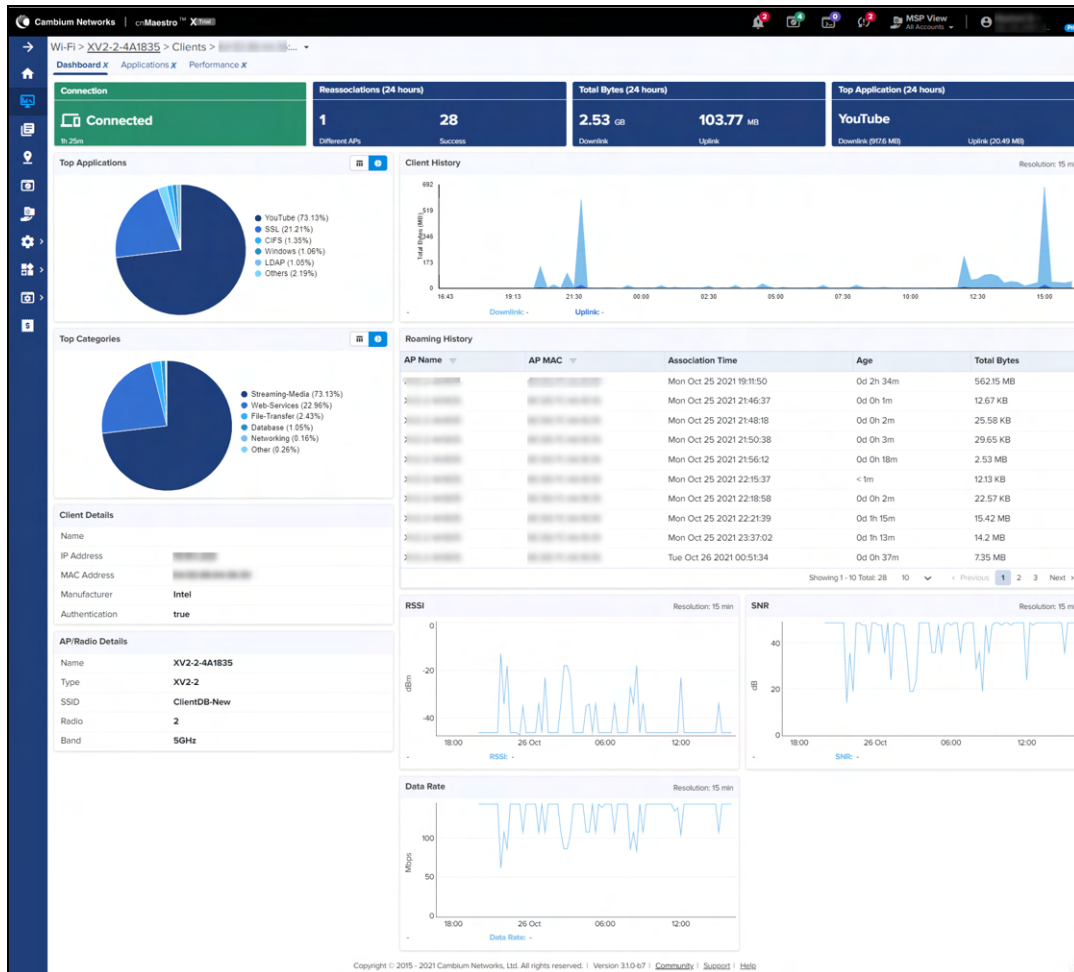
The following parameters are displayed for wireless clients for XV-series:

- AP/Radio Details
- Client Details
- Client History
- Connection

- Reassociations
- Roaming History
- Top Applications
- Top Application (24 hours)
- Total Bytes (24 hours)
- Top Categories

The client traffic distribution in Uplink and Downlink direction during last 24 hours is buffered every 5 minutes granularly.

User can hover over the piechart to view specific application usage and in linear graph to view date, timings, Downlink, and Uplink data statistics.



Application

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

The Application data is displayed for 24 hours or 7 days.

- **Total Bytes** - represents the Uplink and Downlink of the client data usage across applications.
- **Top Application** - represent top application.
- **Top Category** - represent single category specific to the top application.

**NOTE:**

- Advance Client Dashboard is applicable for cnMaestro X.
- Application usage data is applicable for only XV series of devices.

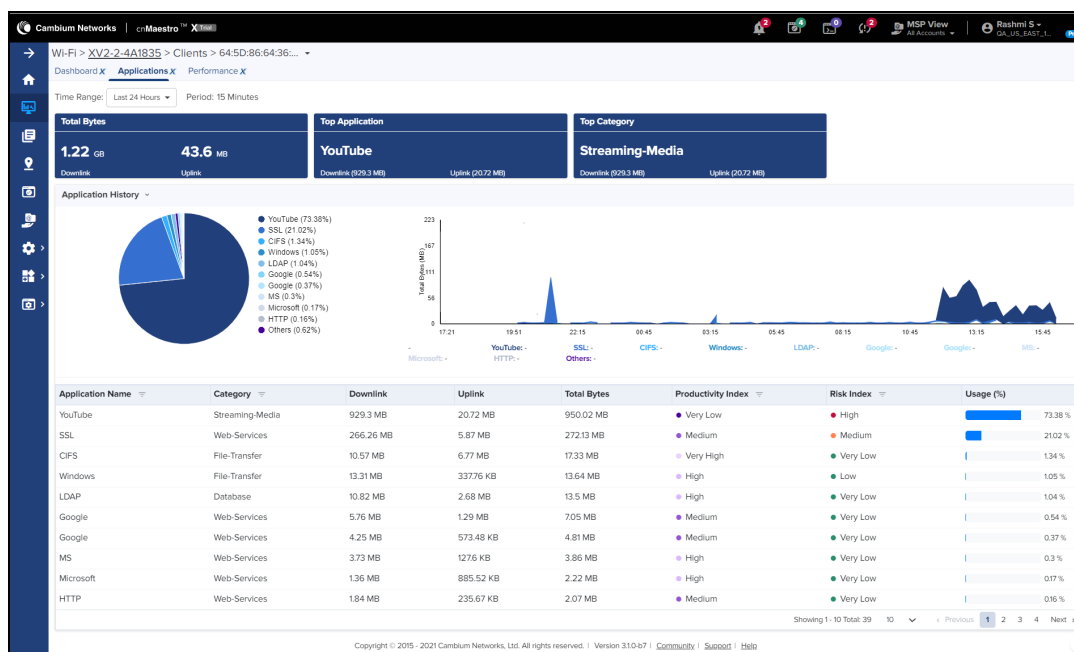
User can view the data usage in single format (pie chart). You can select type of history from the drop-down.

- **Application History** - displays data usage of top 10 and others applications in pie and linear graph format.
- **Category History** - displays data usage for list of categories in pie and linear graph format.

The following parameters are shown:

Table 32: Application fields

Field	Description
Application Name	Name of the application.
Category	Category of the application.
Downlink	Downlink of application data.
Productive Index	Index label for each application to reflect the overall productivity of network users.
Risk Index	Index label for each application to reflect undesirable content onto network.
Total Bytes	Total number of application data in bytes.
Uplink	Uplink of application data.
Usage	Percentage of data usage by application.



Performance

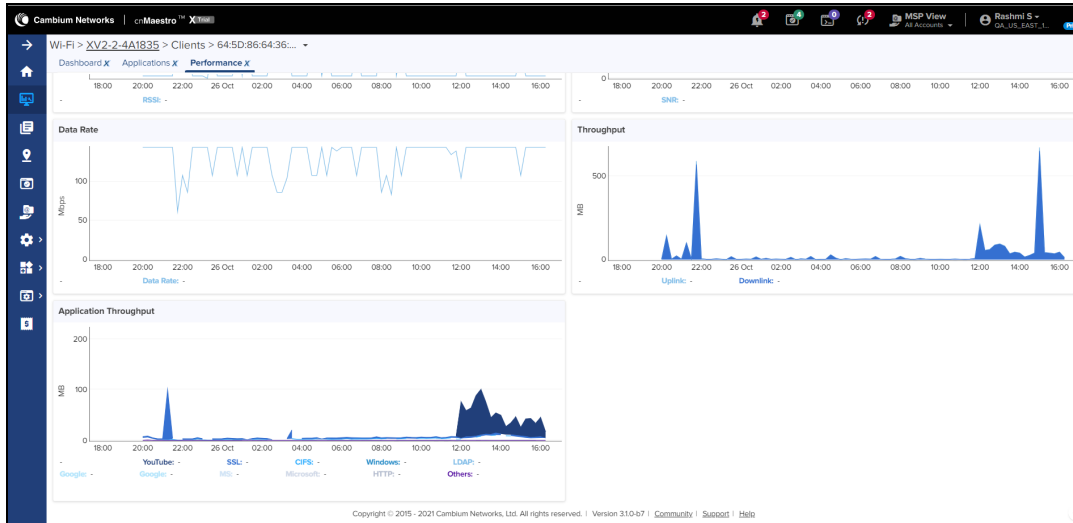
The **Performance** tab displays a synchronized view of time-series data which includes parameters for client's connection health, application usage.

The client data usage can be viewed based upon on **Time Range** which is shown in **four different quadrants**.

- User can select the Time Range by **Last 24 Hours** or **Last 7 Days**.
- User can hover over the pie chart to view specific application usage and in linear graph to view date, timings, Downlink, and Uplink values.

The following client data parameters are shown:

- Application Throughput
- Data Rage
- RSSI
- SNR
- Throughput



Network Info

The Network Info section displays the details of the Network.

Following parameters are displayed for cnPilot Home router:

- Ethernet Ports
 - Type
 - Tx Bytes
 - Rx Bytes
 - Tx Packets
 - Rx Packets
 - Tx Error Bytes
 - Rx Error Bytes
- FXS Ports
 - Type
 - SIP Account Status
 - Phone Number
 - Hook State

Figure 43 cnPilot Home: Device Dashboard > Network Info Page

Wi-Fi > cnPilot-r201P-DON0TDIsTuRB						
Dashboard Notifications Configuration Details Performance Software Update Tools Clients WLANs						
Overview Network Info						
Ethernet Ports						
Type	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Tx Error Bytes	Rx Error Bytes
WAN	4518147	18211803	28696	54061	0	0
LAN 1	0	0	0	0	0	0
LAN 2	0	0	0	0	0	0
LAN 3	0	0	0	0	0	0
LAN 4	0	0	0	0	0	0
FXS Ports						
Type	SIP Account Status	Phone Number	Hook State			
FXS 1	Unregistered	-	On			
FXS 2	Unregistered	-	On			

Following parameter details are displayed in E-Series:

- VLAN
- Routes
- DNS Server(s)
- Domain Name
- Ethernet Ports
- Tunnels
- PPPoE

Figure 44 Enterprise Wi-Fi: Device Dashboard > Network Info Page

Wi-Fi > E700-DD9052													
Dashboard Notifications Configuration Details Performance Software Update Tools Clients Multi Ports WLANs													
Overview Network Info Neighbors List													
VLAN													
Interface Name	IP Address	IP Address	Source	Tx Bytes	Rx Bytes	Tx Avg	Tx Max	Tx Min	Rx Avg	Rx Max	Rx Min	Tx Drops	Rx Drops
PORT-CHANNEL1	0.0.0.0	N/A	0	0	0	0	0	0	0	0	0	0	0
VLAN1	10.10.12.25	10.10.12.25/24	28805	2321084								0	0
E111	0.0.0.0	N/A	30329	3487113	0	0	0	0	16	20	0	0	362
E112	0.0.0.0	N/A	0	0	0	0	0	0	0	0	0	0	0
IPv4 Routes													
Destination	Mask	Gateway	Flags	Metric	Refs	Use	Interface						
0.0.0.0	0.0.0.0	10.10.12.254	UG	0	0	0	VLAN1						
10.10.12.0	255.255.255.0	0.0.0.0	U	0	0	0	VLAN1						
192.168.0.0	255.255.0.0	0.0.0.0	U	0	0	0	VLAN1						
IPv6 Routes													
Destination	Gateway	Flags	Metric	Refs	Use	Interface							
No Routes Configured													
DNS Server(s)													
IP Address	Interface												
10.10.12.110	VLAN1												
10.10.12.111	VLAN1												
Domain Name													
Domain Name	CAMBIO.COM												
Ethernet Ports													
Type	Status	Mode	Access VLAN	Native VLAN	Native Tag	Allowed VLAN	Port Speed	Duplex	MAC				
E111	N/A	access	1	1	None		1000M						
E112	N/A	access	1	1	None								

IPv6 Routes

IPv6 Routes						
Destination	Gateway	Flags	Metric	Refs	Use	Interface
2006:cafe:0:15c::/64	::	UAe	256	0	0	VLAN1
:::0	fe80::529a:4cf: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

Following parameter details are displayed in E-Series:

- Port
- Tx Octets
- Rx Octets
- Tx Frames
- Rx Frames
- Rx Frames with Error
- Tx Broadcasts
- Rx Broadcasts
- Rx Frames Undersize
- Rx Frames Oversize

Figure 45 PTP: Device Dashboard > Network Info Page

Type	Status	Mode	Access VLAN	Native VLAN	Native Tag	Allowed VLAN	Port Speed	Duplex	MAC
ETH1	N/A	access	1	1	false		1000M		
ETH2	N/A	access	1	1	false				

Mesh Peers

The **Mesh Peers** tab displays information related to mesh clients and respective RF parameters such as SNR, RSSI, and Band. This tab helps the user to trigger Wi-Fi performance between the Mesh Client and Mesh Base.

Figure 46 Device Dashboard > Mesh Peers Page

Base AP	Mesh Base	Mesh Client	SSID	End Hosts	Host Name	Managed Account	IP Address	Band	WLAN	WLAN	Uptime	SNR	RSSI	Authorized	Actions
E500MeshBase_B...	00:04:56:88:D6...	00:04:56:88:7F...	cnmaestromesh...	View End Hosts	E500MeshClient	Base Infrastructure	0.0.0.0	5GHz	1	1	1d 22h 28m	83	-12	Yes	

You can also perform the Wi-Fi performance test by clicking the icon in the **Action** field.

Roaming History for Mesh Peers

The roaming history provides details of the mesh clients such as **Connected AP**, **AP MAC**, **Duration**, number of packets transferred and received by the clients (Tx and Rx), duration etc during roaming from one mesh base to a different mesh base.

Figure 47 Roaming History for Mesh Peers

Mesh Base	Mesh Client	End Hosts	Host Name	Managed Account	IP Address	IPv6 Address	Band	WLAN	WLAN	Uptime	SNR	RSSI	Authorized	Actions
00:04:56:88:D6:A0	00:04:56:88:7F:A0	View End Ho...	E500MeshC	J\$HMi@	10.10.208.201		5GHz	1	1	1d 3h 56m	76	-19	Yes	

Connected AP	AP MAC	Connected	Duration	Tx + Rx
No Data Available				

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

Neighbors

Displays the BSSID, SSID, Channel, RSSI details of neighboring 2.4 GHz and 5 GHz radios.

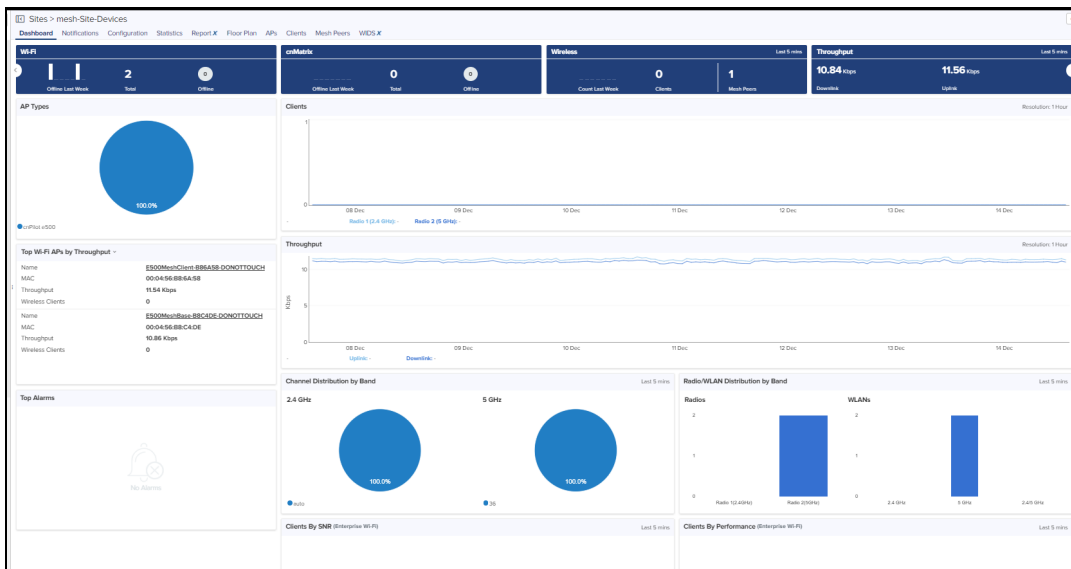
Figure 48 Device Dashboard > Neighbors Page

BSSID	SSID	Channel	SNR
No Neighbors			

Site Dashboard

The Site dashboard page provides the overview of site related parameters and devices as shown below:

Figure 49 Site Dashboard



The Site Dashboard displays the following parameters:

- AP Types
- Channel Distribution by Band
- Clients by SNR

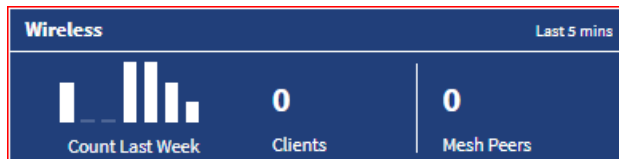
- Clients by Performance
- Floor Plan
- Radio/WLAN Distribution by Band
- RF Quality
- Throughput
- Top Wi-Fi APs
- Throughput Graph
- Wi-Fi Devices Availability (Total and Offline)
- Clients Graph
- Statistics
- Wireless Clients

Wi-Fi Devices Availability (Total and Offline)

Displays total number of access points in the site and the devices that are offline.

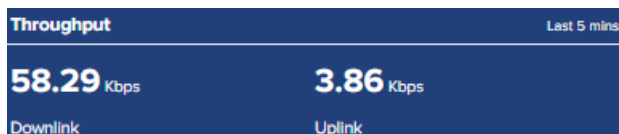


Wireless

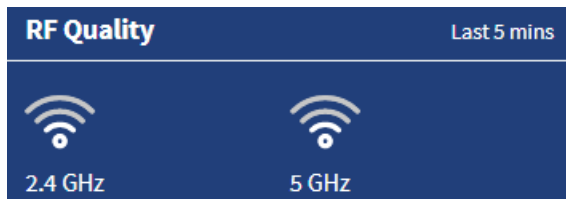


Throughput

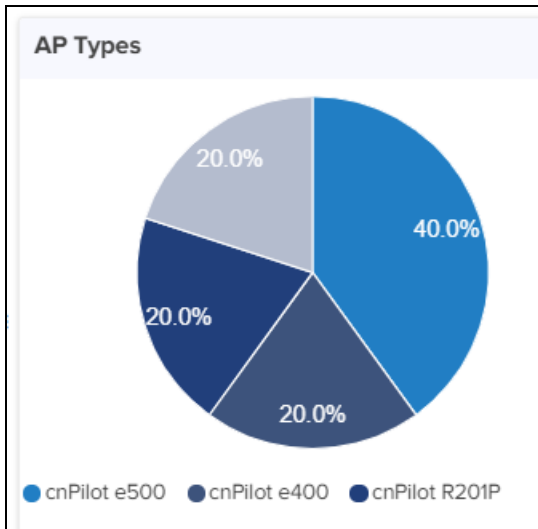
Displays aggregated throughput for all the clients.



RF Quality



AP Types

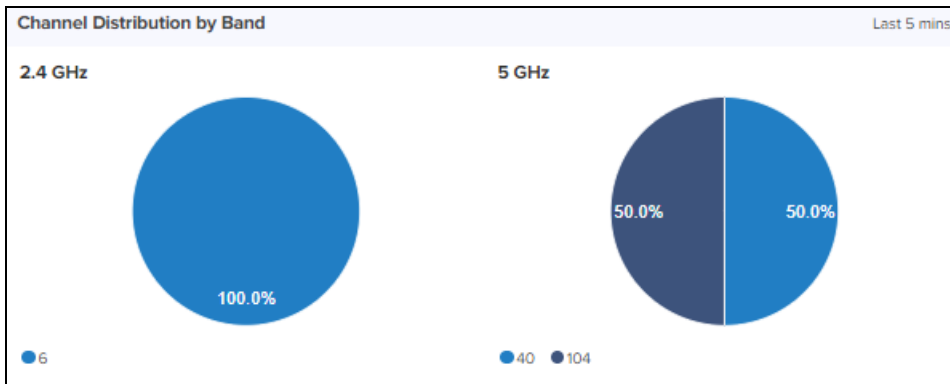


Top Wi-Fi APs

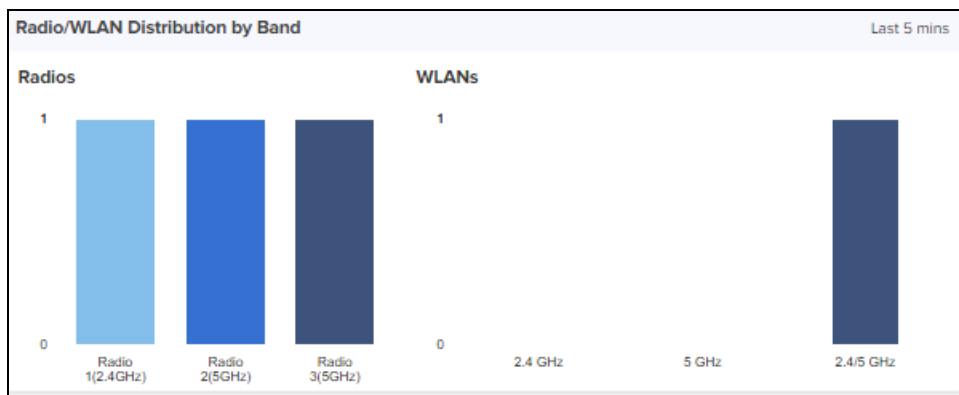
Top Wi-Fi APs by Throughput	
NAME	MAC
XV3-8-Sasi-Do-not-Touch	BC:E6:7C:4D:DA:C4
THROUGHPUT	WIRELESS CLIENTS
30.94 Kbps	2

Channel Distribution by Band

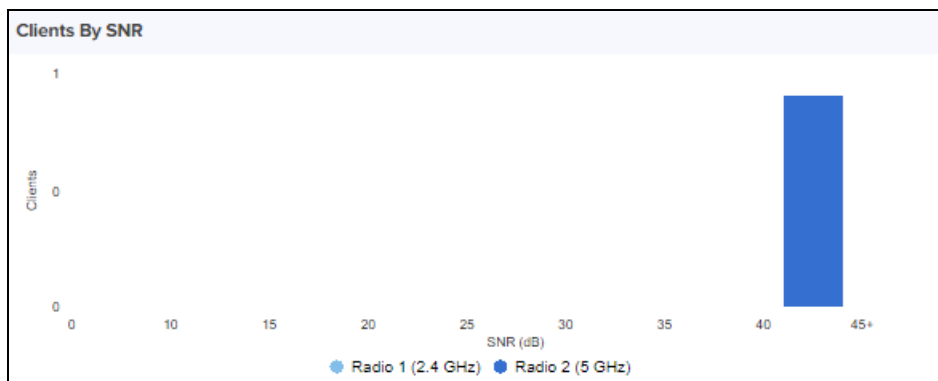
Channel Distribution by AP displays usage of channels in 2.4 GHz and 5 GHz. This helps users in planning and implementing WLANs within a high-density environment.



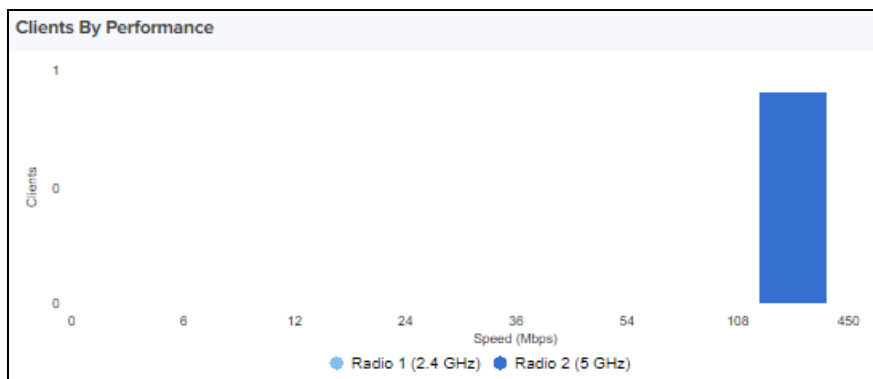
Radio/WLAN Distribution by Band



Clients by SNR



Clients by Performance

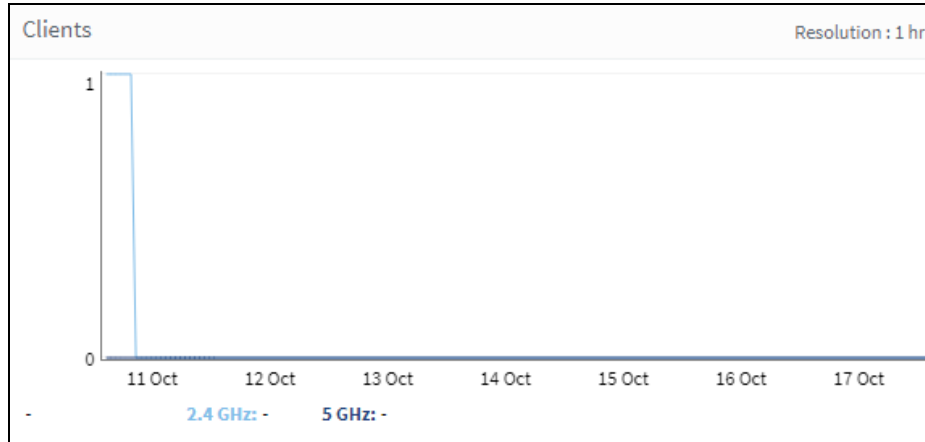


Clients By Performance (For XV3-8)



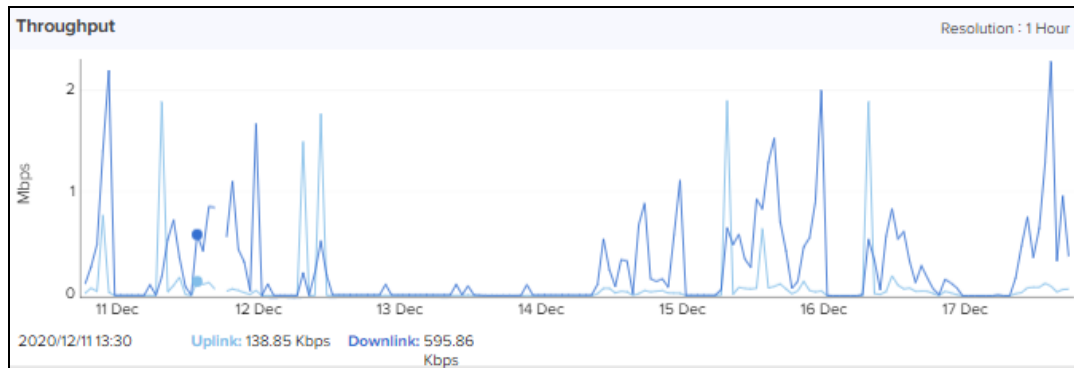
Clients Graph

Clients Graph displays clients that are connected in 2.4 GHz and 5 GHz for the last week.



Throughput Graph

Throughput Graph displays client traffic for the last week.



Statistics

Statistics displays following parameters:

- Channel
- Device
- IP Address
- Managed Account
- Power
- Product Name
- Status
- Throughput (DL)
- Throughput (UL)
- Type

User can **Export Statistics** data to PDF or CSV.

Device	Managed Account	IP Address	Status	Frequency	Bandwidth	DL/UL Ratio	Max Range	DFS Status	Throughput (UL)	Throughput (DL)	Registered SM Count
P1P550-AP 00:04:56:28:BD:06	Base Infrastructure	10.110.224.217	Online 17d 0h 5m	5500 MHz	20 MHz	50/50	3 Miles	N/A	0.2 Kbps	2.67 Kbps	1

Wireless Clients

Wireless Clients displays following parameters:

- Auth Status
- Authentication Type
- Band
- Client Type
- Host Name
- IP Address
- MAC
- Manufacturer
- Mode
- OS
- Portal Mode
- RSSI
- SNR
- Session Expiry
- User
- VLAN-ID
- WLAN

The table can be exported as PDF or CSV.

Host Name	IP Address	MAC	Manufactur...	SSID	Band	Radio ID	Managed Account	RSSI	Download	Upload
iPad	192.168.11.156	CE:5C:31:0D:09:47	[Local MAC]	11_r_client...	5Ghz	2	JJ\$M@	-72 dBm	20.7 MB	3.2 MB

Floor Plan

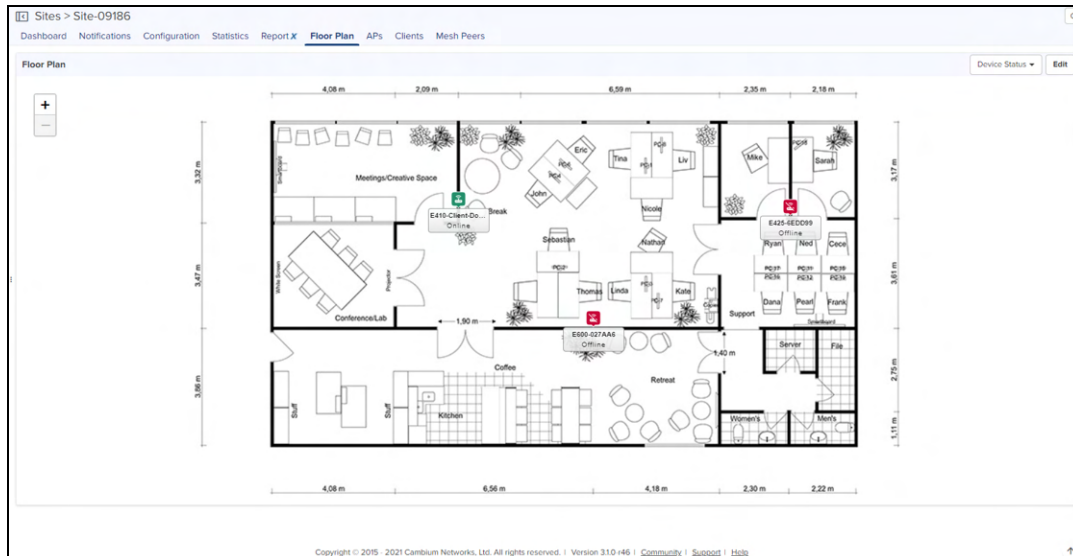
Floor Plan is used to locate all APs on the map (and present device status, connected clients, and Tx power). This is done by uploading the map in **Site > Floor Plan > Edit > Upload** or floor map can be uploaded when site is created. Placing the APs on the floor map is done by clicking full-screen option and then click edit; then place the APs on the map and click **Save**.



NOTE:

While uploading the floor plan follow the recommended specifications such as:

- Resolution: 1024 px X 800 px
- Supported file types: jpeg, jpg, png, and gif
- File size: not more than 5 mb.

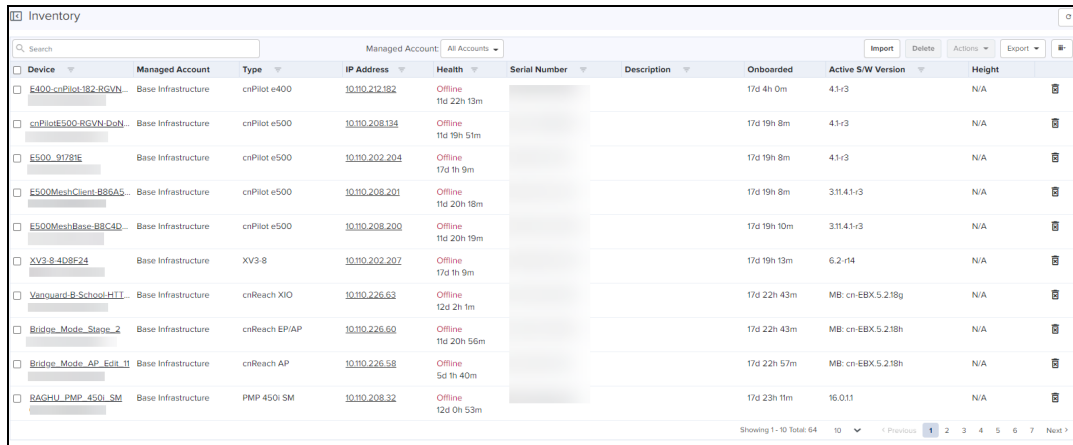


Inventory

The Inventory displays a list of devices under the selected node. It presents health and maintenance information that can be toggled through a button bar at the top. It aggregates children devices and provides a tabular view that allows for sorting and filtering. When selected for a single device, it presents a detailed page tailored to that device.

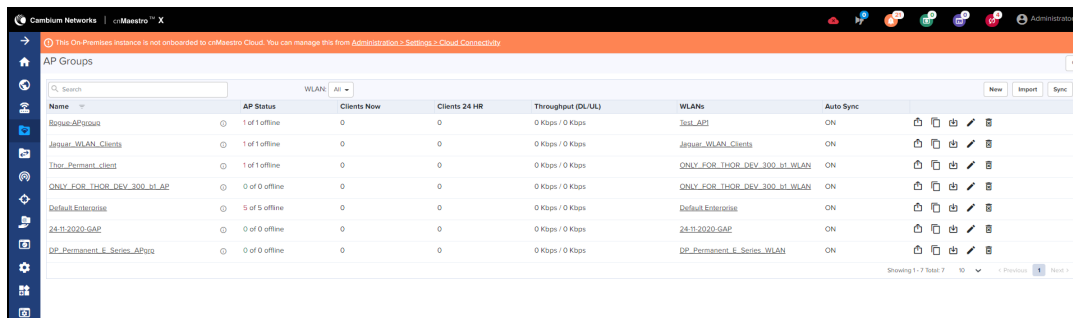
Navigate to [Inventory](#).

Figure 50 Inventory - Access and Backhaul and Industrial Internet View



Device	Managed Account	Type	IP Address	Health	Serial Number	Description	Onboarded	Active S/W Version	Height
E400-cnPilot-182-BGVN	Base Infrastructure	cnPilot e400	10.110.212.182	Offline 11d 22h 13m			17d 4h 0m	4.1-r3	N/A
cnPilotE500-BGVN-DeN	Base Infrastructure	cnPilot e500	10.110.208.134	Offline 11d 19h 51m			17d 19h 8m	4.1-r3	N/A
E500_91281E	Base Infrastructure	cnPilot e500	10.110.202.204	Offline 17d 1h 9m			17d 19h 8m	4.1-r3	N/A
E500MeshClient-B86A5	Base Infrastructure	cnPilot e500	10.110.208.201	Offline 11d 20h 18m			17d 19h 8m	3.11.4.1-r3	N/A
E500MeshBase-B8C4D	Base Infrastructure	cnPilot e500	10.110.208.200	Offline 11d 20h 19m			17d 19h 10m	3.11.4.1-r3	N/A
XV3-9-4D9F24	Base Infrastructure	XV3-8	10.110.202.207	Offline 17d 1h 9m			17d 19h 13m	6.2-r14	N/A
Vanguard-B-School-HTT	Base Infrastructure	cnReach XIQ	10.110.226.63	Offline 12d 2h 1m			17d 22h 43m	MB: cn-EBX.5.2.18g	N/A
Bridge_Mode_Stage_2	Base Infrastructure	cnReach EPI/AP	10.110.226.60	Offline 11d 20h 56m			17d 22h 43m	MB: cn-EBX.5.2.18h	N/A
Bridge_Mode_AP_Edit_11	Base Infrastructure	cnReach AP	10.110.226.68	Offline 5d 1h 40m			17d 22h 57m	MB: cn-EBX.5.2.18h	N/A
BAGHU_PMP_4501_SM	Base Infrastructure	PMP 4501 SM	10.110.208.32	Offline 12d 0h 53m			17d 23h 11m	16.0.11	N/A

Figure 51 Inventory - Enterprise View



Name	AP Status	Clients Now	Clients 24 HR	Throughput (DL/UL)	WLANs	Auto Sync
ReverseAPNetwork	1 of 1 offline	0	0	0 Kbps / 0 Kbps	3rd_APS	CN
Januar_WLAN_Clients	1 of 1 offline	0	0	0 Kbps / 0 Kbps	Januar_WLAN_Clients	CN
110r_Perment_client	1 of 1 offline	0	0	0 Kbps / 0 Kbps	ONLY_FOR_110R_DEV_300_bt_WLAN	CN
ONLY_FOR_110R_DEV_300_bt_AP	0 of 0 offline	0	0	0 Kbps / 0 Kbps	ONLY_FOR_110R_DEV_300_bt_WLAN	CN
Default Enterprise	5 of 5 offline	0	0	0 Kbps / 0 Kbps	Default Enterprise	CN
24-11-2020-GAP	0 of 0 offline	0	0	0 Kbps / 0 Kbps	24-11-2020-GAP	CN
OP_Perment_E_Series_APNet	0 of 0 offline	0	0	0 Kbps / 0 Kbps	OP_Perment_E_Series_WLAN	CN

Inventory Export

The inventory can be exported in either CSV or PDF 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** is available in the inventory page of System/Network/Tower/Site in cnMaestro On-Premises. This feature helps the users in bulk deletion of devices from System/Network/Tower/Site.

Figure 52 Bulk Delete

Device	Managed Account	Type	IP Address	Health	Serial Number	Description	Onboarded	Active S/W Version	Height
<input checked="" type="checkbox"/> 190V_Test	J\$H-M@	cnPilot r190V	10.110.224.11	Offline 17d 0h 55m			19d 3h 31m	4.7.2-R8	
<input checked="" type="checkbox"/> Bridge_Mode_AP_Edit_11	Base Infrastructure	cnReach AP	10.110.226.58	Offline 5d 1h 43m			17d 23h 1m	MB: cn-EBX.5.2.18h	N/A
<input checked="" type="checkbox"/> Bridge_Mode_Stage_2	Base Infrastructure	cnReach EPIAP	10.110.226.60	Offline 11d 2h 0m			17d 22h 46m	MB: cn-EBX.5.2.18h	N/A
<input checked="" type="checkbox"/> Cambium_123	J\$H-M@	cnPilot r190V	10.110.224.3	Offline 17d 0h 58m			19d 3h 30m	4.6.1-R1	N/A
<input checked="" type="checkbox"/> Client_MICRO	Base Infrastructure	cnVision CLIENT MICRO	10.120.155.32	Offline 12d 2h 51m			17d 23h 59m	4.6-RC40	N/A
<input checked="" type="checkbox"/> cnMatrix-EX2028-DP	Base Infrastructure	cnMatrix EX2028	10.110.224.17	Offline 17d 2h 28m		durga	20d 3h 39m	3.21-r5	N/A
<input checked="" type="checkbox"/> cnMatrixEX1028-P-123	Base Infrastructure	cnMatrix EX1028-P	10.110.221.11	Offline 28d 3h 31m		test	32d 23h 46m	3.21-r5	N/A
<input checked="" type="checkbox"/> cnPilot_r200_080121	J\$H-M@	cnPilot r200P	10.110.224.10	Offline 11d 20h 18m			19d 2h 45m	4.4.2-R2	N/A
<input checked="" type="checkbox"/> cnPilot_080DA1	J\$H-M@	cnPilot r200P	10.110.224.21	Offline 17d 0h 56m			19d 3h 27m	4.4.2-R2	N/A
<input checked="" type="checkbox"/> cnPilot-R190V_DP	J\$H-M@	cnPilot r190V	10.110.224.76	Offline 17d 0h 8m			19d 3h 34m	4.7.2-R6	N/A

To delete devices using Bulk Delete, perform the following steps:

1. Navigate to **Inventory** page of System/Network/Tower/Site.
2. Select one or multiple devices as per the requirement.
3. Click **Delete**.

NOTE:
In Wi-Fi view, Bulk Delete can also delete the devices that are in waiting for approval state.

Bulk Reboot

The **Bulk Reboot** is available in the inventory page of Network/Tower/Site in cnMaestro On-Premises.

This feature helps the users in bulk reboot of devices.

When the devices are moved using the Bulk Reboot option, all the **Network/Tower/Site Dashboards, Graphs, Clients, Reports, and Mesh Peers** will also get updated accordingly.

Figure 53 Bulk Reboot

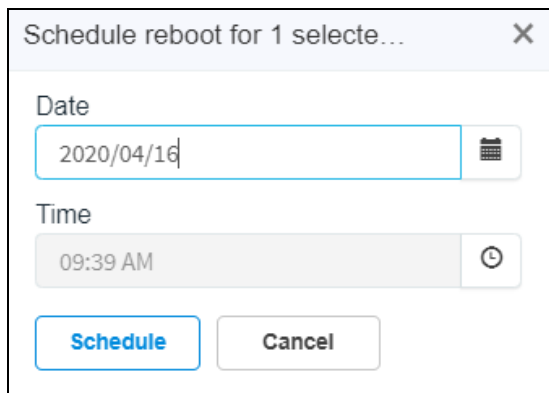
Device	Managed Account	Type	IP Address	Health	Serial Number	Description	Onboarded	Active S/W Version	Height
<input checked="" type="checkbox"/> 190V_Test	J\$H-M@	cnPilot r190V	10.110.224.11	Offline 17d 0h 55m			19d 3h 31m	4.7.2-R8	
<input checked="" type="checkbox"/> Bridge_Mode_AP_Edit_11	Base Infrastructure	cnReach AP	10.110.226.58	Offline 5d 1h 43m			17d 23h 1m	MB: cn-EBX.5.2.18h	N/A
<input checked="" type="checkbox"/> Bridge_Mode_Stage_2	Base Infrastructure	cnReach EPIAP	10.110.226.60	Offline 11d 2h 0m			17d 22h 46m	MB: cn-EBX.5.2.18h	N/A
<input checked="" type="checkbox"/> Cambium_123	J\$H-M@	cnPilot r190V	10.110.224.3	Offline 17d 0h 58m			19d 3h 30m	4.6.1-R1	N/A
<input checked="" type="checkbox"/> Client_MICRO	Base Infrastructure	cnVision CLIENT MICRO	10.120.155.32	Offline 12d 2h 51m			17d 23h 59m	4.6-RC40	N/A
<input checked="" type="checkbox"/> cnMatrix-EX2028-DP	Base Infrastructure	cnMatrix EX2028	10.110.224.17	Offline 17d 2h 28m		durga	20d 3h 39m	3.21-r5	N/A
<input checked="" type="checkbox"/> cnMatrixEX1028-P-123	Base Infrastructure	cnMatrix EX1028-P	10.110.221.11	Offline 28d 3h 31m		test	32d 23h 46m	3.21-r5	N/A
<input checked="" type="checkbox"/> cnPilot_r200_080121	J\$H-M@	cnPilot r200P	10.110.224.10	Offline 11d 20h 18m			19d 2h 45m	4.4.2-R2	N/A
<input checked="" type="checkbox"/> cnPilot_080DA1	J\$H-M@	cnPilot r200P	10.110.224.21	Offline 17d 0h 56m			19d 3h 27m	4.4.2-R2	N/A
<input checked="" type="checkbox"/> cnPilot-R190V_DP	J\$H-M@	cnPilot r190V	10.110.224.76	Offline 17d 0h 8m			19d 3h 34m	4.7.2-R6	N/A

To reboot devices using Bulk Reboot:

1. Navigate to **Inventory** page of Network/Tower/Site.
2. Select one or multiple devices as per the requirement.
3. Click **Actions** and choose **Reboot Now**.

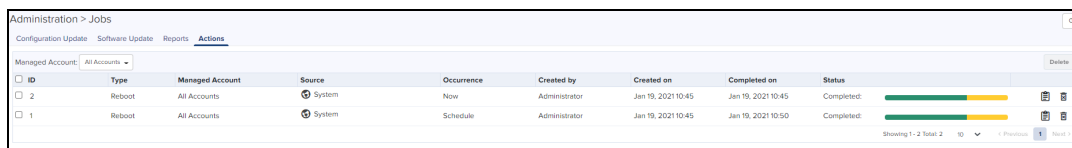
Schedule Reboot

You can also schedule reboot of the device/device(s) by selecting **Schedule reboot** from **Actions** drop-down list, and by providing the **Date** and **Time**.



Screenshot of the "Schedule reboot for 1 selecte..." dialog box. The dialog has a title bar with a close button. It contains two input fields: "Date" with the value "2020/04/16" and a calendar icon, and "Time" with the value "09:39 AM" and a clock icon. At the bottom, there are two buttons: "Schedule" (highlighted in blue) and "Cancel".

After creating a scheduled reboot job, you can view the status in the **Administration > Jobs > Actions** page.




Screenshot of the "Administration > Jobs > Actions" page. The page shows a table of actions. The table has columns: ID, Type, Managed Account, Source, Occurrence, Created by, Created on, Completed on, and Status. Two rows are visible, both showing "Reboot" jobs with a "Completed" status. The first row has ID 2, and the second row has ID 1. The status column shows a progress bar and a "Completed" label.

ID	Type	Managed Account	Source	Occurrence	Created by	Created on	Completed on	Status
2	Reboot	All Accounts	System	Now	Administrator	Jan 19, 2021 10:45	Jan 19, 2021 10:45	Completed
1	Reboot	All Accounts	System	Schedule	Administrator	Jan 19, 2021 10:45	Jan 19, 2021 10:50	Completed

CSV Configuration Import

Import device(s) configuration is available from 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:

- Azimuth
- Beam Width
- Elevation
- Height
- Latitude
- Longitude

The following parameters are supported for ePMP/PMP SM is in the CSV file:

- Latitude
- Longitude

Figure 54 Import Device Configuration

Device ID	Managed Account	Type	IP Address	Health	Serial Number	Description	Onboarded	Active SW Version	Height
190V_Test	JIS-M@	cnPilot r190V	10.110.224.11	Offline 17d 1h 2m			19d 3h 37m	4.7.2-R8	N/A
Bridge_Mode_AP_Edit_11	Base Infrastructure	cnReach AP	10.110.226.58	Offline 5d 1h 49m			17d 23h 7m	MB: cn-EBX.5.2.18h	N/A
Bridge_Mode_Stage_2	Base Infrastructure	cnReach EPIAP	10.110.226.60	Offline 11d 2h 6m			17d 22h 52m	MB: cn-EBX.5.2.18h	N/A
Cambium-123	JIS-M@	cnPilot r190V	10.110.224.3	Offline 17d 1h 5m			19d 3h 36m	4.6.1-R1	N/A
Client_MICRO	Base Infrastructure	cnVision CLIENT MICRO	10.120.155.32	Offline 12d 2h 57m			18d 0h 6m	4.6-RC40	N/A
cnMatrix-EX2028-DP	Base Infrastructure	cnMatrix EX2028	10.110.224.17	Offline 17d 2h 34m		durga	20d 3h 45m	3.21-r5	N/A
cnMatrixEX1028-P-123	Base Infrastructure	cnMatrix EX1028-P	10.110.224.11	Offline 28d 3h 38m		test	32d 23h 52m	3.21-r5	N/A
cnPilot_r200.08D121	JIS-M@	cnPilot r200P	10.110.224.10	Offline 11d 20h 24m			19d 2h 51m	4.4.2-R2	N/A
cnPilot_08DDA1	JIS-M@	cnPilot r200P	10.110.224.21	Offline 17d 1h 2m			19d 3h 33m	4.4.2-R2	N/A
cnPilot-R190V_DP	JIS-M@	cnPilot r190V	10.110.224.76	Offline 17d 0h 15m			19d 3h 40m	4.7.2-R6	N/A

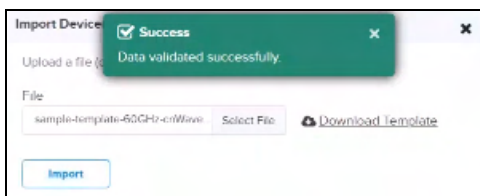
Sample Configuration File

MAC	LATITUDE	LONGITUDE	AZIMUTH	ELEVATION	BEAM WIDTH	HEIGHT	HEIGHT UNIT
Supports formats with ':', '-', 'no space', upper and lower case.	Signed degrees format (DDD.ddd).	Signed degrees format (DDD.ddd).	Degrees from North (0 to 360)	Degrees from horizon (-90 to 90)	Degrees from 1 to 360	Min=0, Max=5 Meters/Feet	
	16	19	17	130	1500	Feet	
	-90	119.0123	190	64	120	1000	feet
	79.0123	11	111	74	112	110	Meters
	-44	-12.78	124	67	177	190	meters

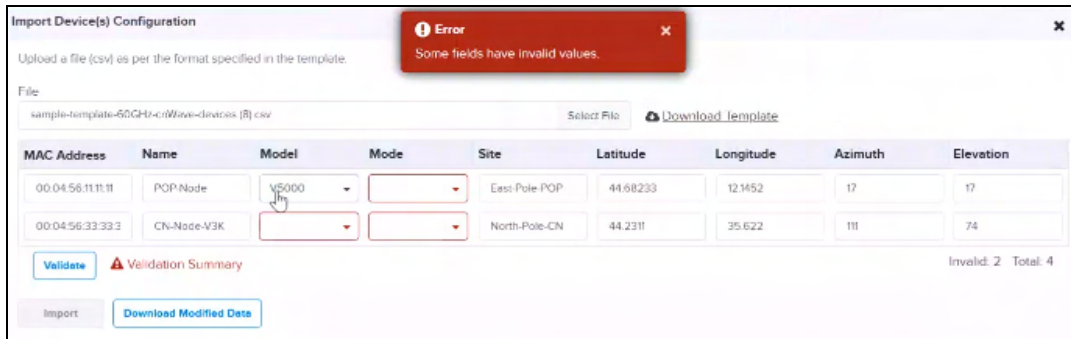
Sample Configuration File (60 GHz cnWave)

MAC	Serial Nun	Device Na	Model	Device McPoP	Node	Site	Latitude	Longitude	Azimuth	Elevation	Description
Supports	Serial Nun	Name of t	V5000/V3000	DN/CN	Yes/No	Name of t	Signed de	Signed de	Degrees fr	Degrees from horizon (-90 to 90)	
		POP-Node	V5000	DN	Yes	East-Pole-	44.68233	12.1452	17	17	
		DN-Node	V5000	DN	No	West-Pole	-12.5425	119.0123		190	64
		CN-Node-	V3000	CN	No	North-Pole	44.2311	35.622	111	74	
		CN-Node-	V1000	CN	No	South-Pole	22.6533	-12.78	124	67	

While importing the file it automatically validates the data as shown below.



If any invalid fields are found while validating it pops-up an error window as shown below:



Uploading a Configuration File

To upload a configuration file (CSV) as per the format specified in the sample template:

1. Download Sample Template or prepare a sheet in CSV file format with necessary column details.
2. Upload a configuration file (CSV) as per the format specified in the sample template.

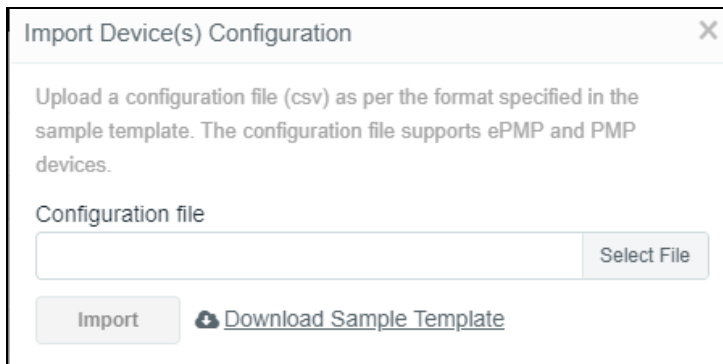


NOTE:

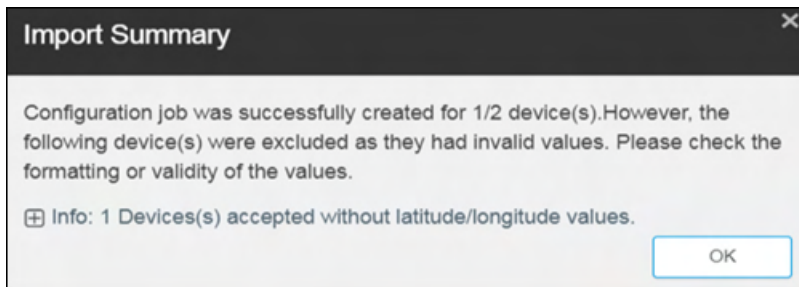
You must know the MAC address of the device to push the configuration.

3. Click **Import**.

Figure 55 Uploading Configuration File



4. A configuration job will be created in the tower page.



5. You can view the completed status of import device (s) configuration in the Managed Account page.

ID	Details	Occurrence	Target	Created by	Created on	Completed on	Parallel	Stop on Error	Sector Priority	Status
43	2 device(s)	Now		Auto-Sync	Jan 22, 2021 18:07	Jan 22, 2021 18:07	15	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>
42	1 XV3-8 device(s)	Now	import_24200	Administrator	Jan 22, 2021 16:52	Jan 22, 2021 16:53	-	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>
41	1 device(s)	Now		Auto-Sync	Jan 22, 2021 16:52	Jan 22, 2021 16:52	15	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>
40	1 XV3-8 device(s)	Now	import_24200	Administrator	Jan 22, 2021 16:46	Jan 22, 2021 16:46	-	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>
39	1 XV3-8 device(s)	Now	import_242_anc	Administrator	Jan 22, 2021 16:42	Jan 22, 2021 16:42	-	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>
38	1 XV3-8 device(s)	Now	TRIGB_AP	Administrator	Jan 22, 2021 16:41	Jan 22, 2021 16:42	-	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>
37	1 device(s)	Now		Auto-Sync	Jan 22, 2021 16:40	Jan 22, 2021 16:41	15	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>
36	1 XV3-8 device(s)	Now	import_242_anc	Administrator	Jan 22, 2021 16:38	Jan 22, 2021 16:39	-	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>
35	1 device(s)	Now		Auto-Sync	Jan 22, 2021 16:34	Jan 22, 2021 16:34	15	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>
34	1 device(s)	Now		Auto-Sync	Jan 22, 2021 15:45	Jan 22, 2021 15:45	15	false	N/A	Completed: <div style="width: 100%; height: 10px; background-color: green;"></div>

The following table provides details on different errors that might occur while importing a CSV file:

Table 33: CSV Importing Error

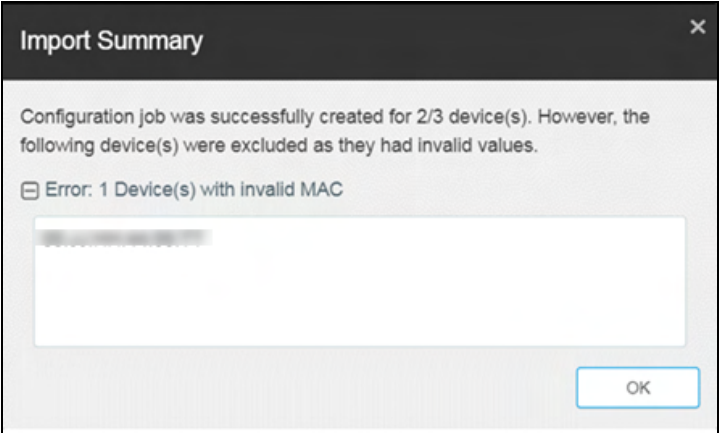
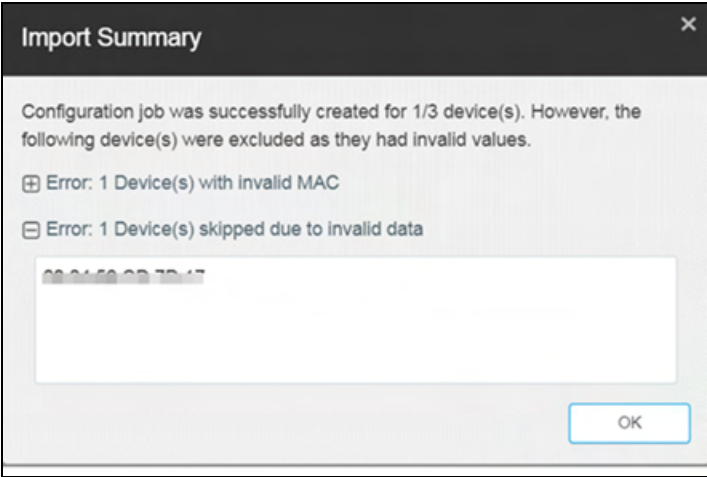
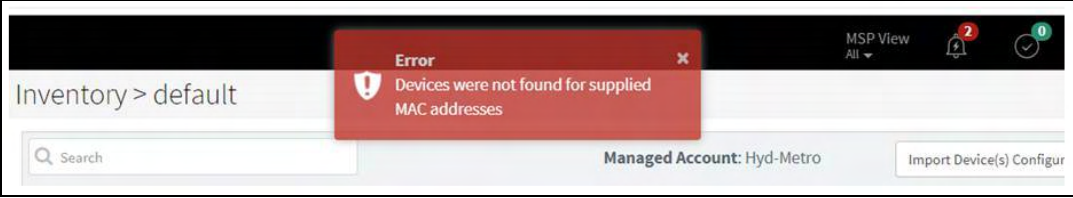
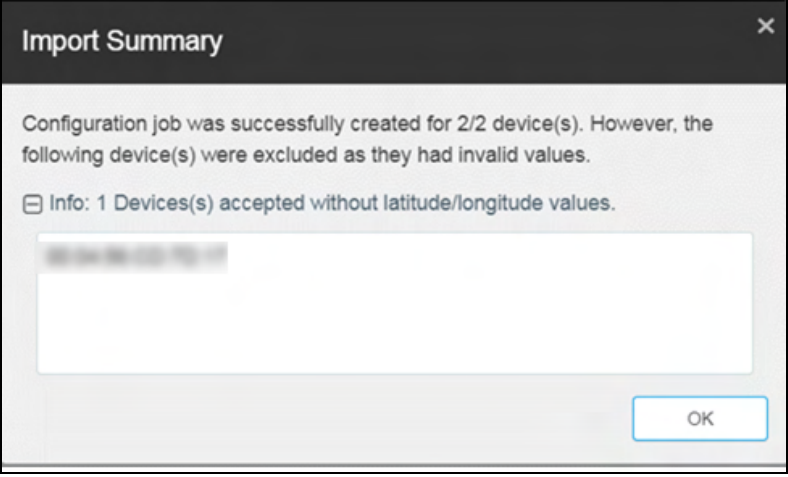
Error	Description
<p>Error1: Error: {Count of Devices} Device(s) with invalid MAC</p>	<p>This error is displayed if the uploaded CSV file contains invalid MAC Address.</p> 
<p>Error2: {Count of Devices} Device(s) skipped due to invalid data</p>	<p>This error is displayed if the uploaded CSV file contains invalid Data or data not relevant for Latitude, Longitude, Azimuth, Height and Elevation.</p> 
<p>Error3: Devices were not found for supplied MAC Address</p>	<p>This error message is displayed if the devices were not found with supplied MAC address in the CSV file.</p>

Table 33: CSV Importing Error

Error	Description
	 <p>The screenshot shows a web application interface with a dark header. A red error dialog box is centered on the screen, displaying a shield icon with an exclamation mark and the text: "Error: Devices were not found for supplied MAC addresses". The background interface includes a search bar, a "Managed Account: Hyd-Metro" label, and an "Import Device(s) Configur" button. The top right corner shows "MSP View" and notification icons.</p>
<p>Error4: Info: 1 Device(s) accepted without latitude/longitude values</p>	<p>This error is displayed when the latitude and longitude values are tried to push on to ePMP AP or PMP AP which are under a Tower.</p>  <p>The screenshot shows an "Import Summary" dialog box with a close button (X) in the top right. The text inside reads: "Configuration job was successfully created for 2/2 device(s). However, the following device(s) were excluded as they had invalid values." Below this, there is an expandable section with a minus sign icon and the text: "Info: 1 Device(s) accepted without latitude/longitude values." A blurred area follows, and an "OK" button is located at the bottom right.</p>

Reports

This section provides details on how to schedule and generate different types of data reports in cnMaestro On-Premises.

- [Generating Reports](#)
- [Remote Upload](#)
- [Report Jobs](#)

Generating Reports

The following reports can be generated such as:

- [Device Report](#)
- [Reports](#)
- [Active Alarms Report](#)
- [Alarms History Report](#)
- [Events Report](#)
- [Clients Report](#)
- [Mesh Peers Report](#)
- [Guest Access Login Events Report](#)

Device Report

To generate device reports:

1. Navigate to **Report > Devices** tab.
2. Select the device type for which the user wants to generate the report or select **ALL** for generating the report for All device types.
3. Select data to include in report.
4. Click **Start Job** to generate report **Now** or you can **Schedule** based on schedule type (**Daily**, **Weekly** or **Monthly**).

Based on the device type selection the Data Export parameters will change.

- If 60 GHz cnWave with enabling CN or DN or both is selected as the **Device Type**, then Basic, Radio, GPS, and Ethernet Data of CN or DN will be exported.

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices Performance Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for device parameters as a comma-separated value (CSV) file. All devices under the tree node selected will be included in the export. Select all parameters that should be included.

Schedule
 Now Daily Weekly Monthly (30 days)

Device Type
 60 GHz cnWave

Mode
 CN DN

Select data to include in report

Basic

<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Mode	<input checked="" type="checkbox"/> Model	<input checked="" type="checkbox"/> Network
<input checked="" type="checkbox"/> Onboard Status	<input checked="" type="checkbox"/> PoP Node	<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Serial Number
<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Status Time
<input checked="" type="checkbox"/> Sync Mode			

Radio

<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Packets	<input checked="" type="checkbox"/> Radio Channel	<input checked="" type="checkbox"/> Throughput
---	---	---	--

GPS

<input checked="" type="checkbox"/> Fix Type	<input checked="" type="checkbox"/> GPS Coordinates	<input checked="" type="checkbox"/> GPS Satellites Tracked	<input checked="" type="checkbox"/> Height
--	---	--	--

Ethernet

<input checked="" type="checkbox"/> Errors	<input checked="" type="checkbox"/> Packet Drops	<input checked="" type="checkbox"/> Packets	<input checked="" type="checkbox"/> Status
<input checked="" type="checkbox"/> Throughput			

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

- If **ALL** is selected as the **Device Type**, the Basic Data Export parameters will be exported.

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices Performance Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for device parameters as a comma-separated value (CSV) file. All devices under the tree node selected will be included in the export. Select all parameters that should be included.

Schedule
 Now Daily Weekly Monthly (30 days)

Device Type
 All

Select data to include in report

Basic

<input checked="" type="checkbox"/> Country	<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Location	<input checked="" type="checkbox"/> Device Name
<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> Hardware	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> Last Update Message	<input checked="" type="checkbox"/> Last Update Status	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Network
<input checked="" type="checkbox"/> Onboard Date	<input checked="" type="checkbox"/> Onboard Status	<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Serial Number
<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Status Time	<input checked="" type="checkbox"/> Tower/Site

Location

<input checked="" type="checkbox"/> GPS Coordinates			
---	--	--	--

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

- If cnMatrix is selected as the **Device Type**, then Basic data will be exported.

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices Performance Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for device parameters as a comma-separated value (CSV) file. All devices under the tree node selected will be included in the export. Select all parameters that should be included.

Schedule
 Now Daily Weekly Monthly (30 days)

Device Type
 cnMatrix

Select data to include in report

Basic

<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Location	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type
<input checked="" type="checkbox"/> Hardware	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> Last Update Message	<input checked="" type="checkbox"/> Last Update Status
<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Onboard Date	<input checked="" type="checkbox"/> Onboard Status
<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Serial Number	<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Software Version
<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Status Time	<input checked="" type="checkbox"/> Tower	

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

- If cnPilot Home (R-Series) is selected as the **Device Type**, then Basic, Network and Radio Data will be exported.

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices Performance Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for device parameters as a comma-separated value (CSV) file. All devices under the tree node selected will be included in the export. Select all parameters that should be included.

Schedule
 Now Daily Weekly Monthly (30 days)

Device Type
 cnPilot Home (R Series)

Select data to include in report

Basic

<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Location	<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name
<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> Hardware	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> Last Update Message	<input checked="" type="checkbox"/> Last Update Status	<input checked="" type="checkbox"/> Last Updated Time	<input checked="" type="checkbox"/> MAC
<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Onboard Date	<input checked="" type="checkbox"/> Onboard Status	<input checked="" type="checkbox"/> Product Name
<input checked="" type="checkbox"/> Serial Number	<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status
<input checked="" type="checkbox"/> Status Time	<input checked="" type="checkbox"/> Sync Status		

Network

<input checked="" type="checkbox"/> Default Gateway	<input checked="" type="checkbox"/> Ethernet	<input checked="" type="checkbox"/> WAN IP Address
---	--	--

Radio

<input checked="" type="checkbox"/> End Hosts	<input checked="" type="checkbox"/> Radios Band	<input checked="" type="checkbox"/> Radios Channel	<input checked="" type="checkbox"/> Radios Client Count
<input checked="" type="checkbox"/> Radios MAC	<input checked="" type="checkbox"/> Radios Power	<input checked="" type="checkbox"/> Radios State	<input checked="" type="checkbox"/> Radios Throughput
<input checked="" type="checkbox"/> Radios WLANs			

Location

<input checked="" type="checkbox"/> GPS Coordinates

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

- If cnReach is selected as the **Device Type**, then Basic, Radio and Network Data will be exported.

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices Performance Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for device parameters as a comma-separated value (CSV) file. All devices under the tree node selected will be included in the export. Select all parameters that should be included.

Schedule
 Now Daily Weekly Monthly (30 days)

Device Type
 cnReach

Select data to include in report

Basic

<input checked="" type="checkbox"/> DA Version	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> Last Update Message
<input checked="" type="checkbox"/> Last Update Status	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Software Version

Network

<input checked="" type="checkbox"/> DNS	<input checked="" type="checkbox"/> Default Gateway	<input checked="" type="checkbox"/> Netmask
---	---	---

Radio

<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Neighbors	<input checked="" type="checkbox"/> RSSI	<input checked="" type="checkbox"/> Radio Temperature
<input checked="" type="checkbox"/> Role	<input checked="" type="checkbox"/> SNR	<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> TxPower

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

- If cnReach XIO is selected as the **Device Type**, then Basic, Radio and Network Data will be exported.

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices Performance Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for device parameters as a comma-separated value (CSV) file. All devices under the tree node selected will be included in the export. Select all parameters that should be included.

Schedule
 Now Daily Weekly Monthly (30 days)

Device Type
 cnReach XIO

Select data to include in report

Basic

<input checked="" type="checkbox"/> DA Version	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> Last Update Message
<input checked="" type="checkbox"/> Last Update Status	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Software Version

Network

<input checked="" type="checkbox"/> DNS	<input checked="" type="checkbox"/> Default Gateway	<input checked="" type="checkbox"/> Netmask
---	---	---

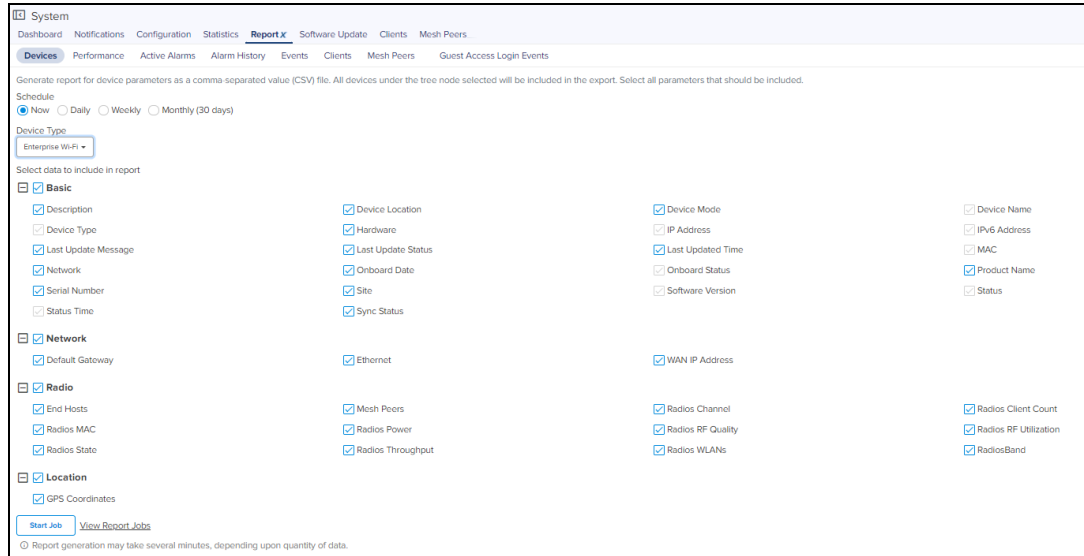
[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

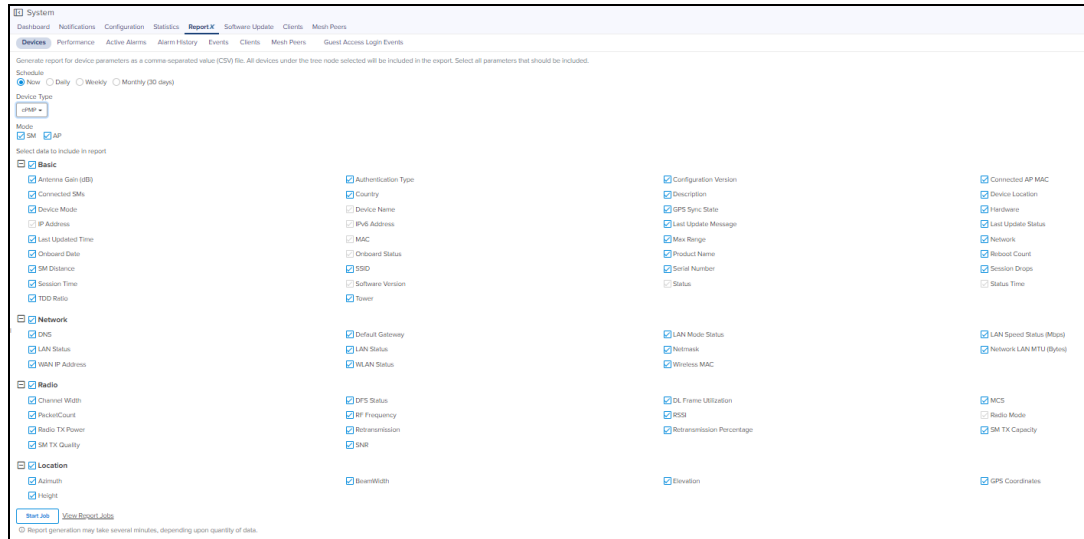
- If cnRanger is selected as the **Device Type**, then Basic, Radio, Location, CBRS, and Network Data will be exported.

- If cnVision is selected as the **Device Type**, then Basic, Network, Location and Radio Data will be exported.

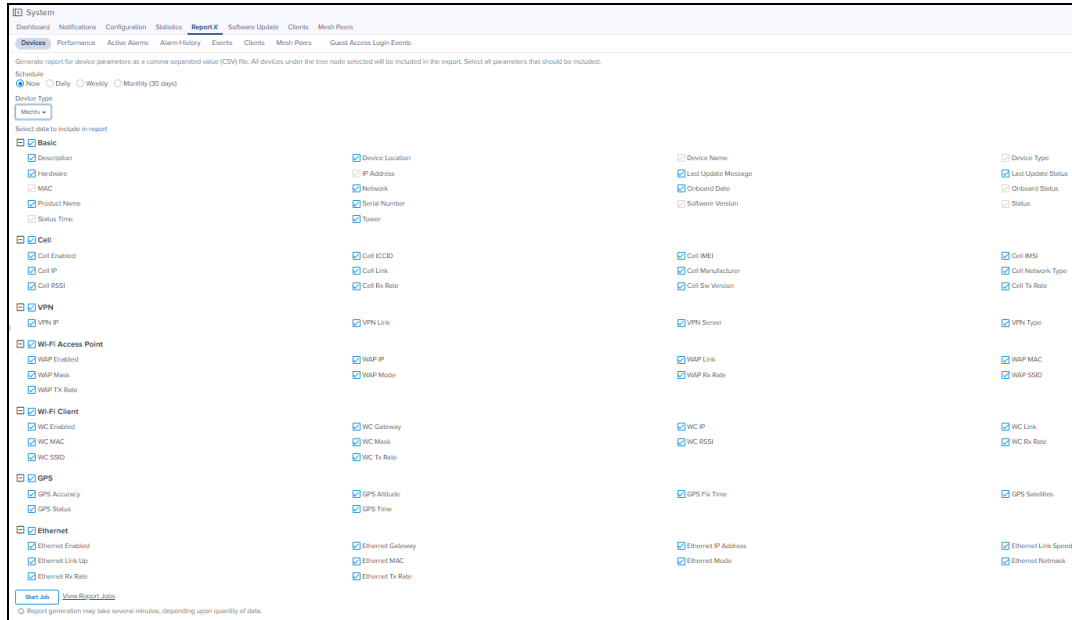
- If Enterprise Wi-Fi is selected as the **Device Type**, then Basic, Network, Location, and Radio Data will be exported.



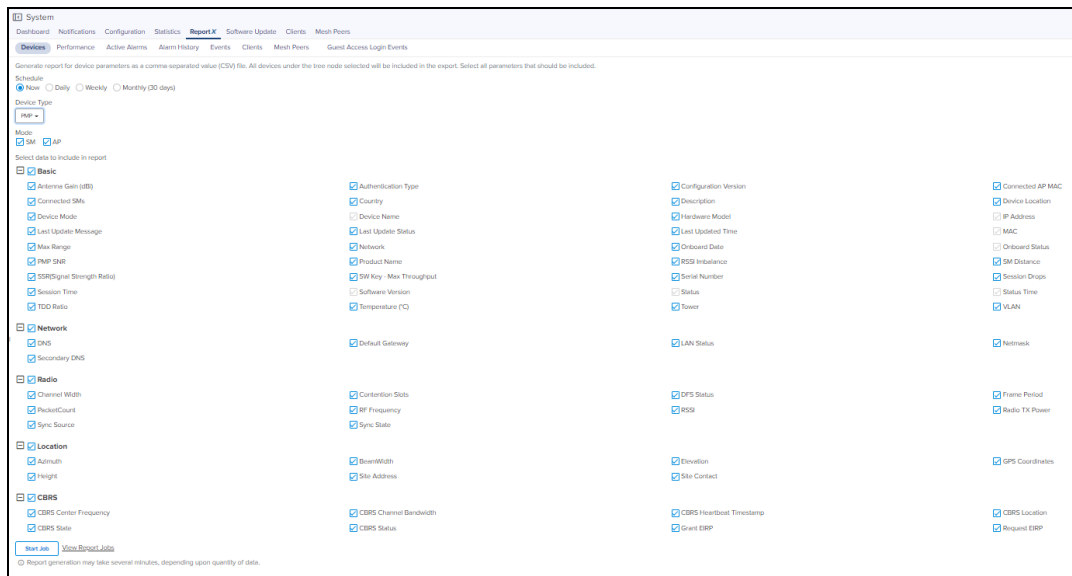
- If eMP is selected as the **Device Type**, then Basic, Network, Location and Radio data will be exported. User can select to generate the report for either AP or SM or both. Based on the AP or SM selection, the data related to AP or SM will be exported.



- If Machfu is selected as the Device Type, then Basic, Cell, VPN, Wi-fi Access Point, Wi-Fi Client, GPS and Ethernet data will be exported.



- If PMP is selected as the **Device Type**, then Basic, Network, Location and Radio data will be exported. User can select to generate the report for either AP or SM or both. Based on the AP or SM selection, the data related to AP or SM will be exported.



- If PTP is selected as the **Device Type**, then Basic, Network, Location and Radio data will be exported.

System

Dashboard Notifications Configuration Statistics **Report** Software Update Clients Mesh Peers

Devices Performance Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for device parameters as a comma-separated value (CSV) file. All devices under the tree node selected will be included in the export. Select all parameters that should be included.

Schedule
 Now Daily Weekly Monthly (30 days)

Device Type
 PTP

Select data to include in report

Basic

<input checked="" type="checkbox"/> Antenna Gain (dBi)	<input checked="" type="checkbox"/> Color Code	<input checked="" type="checkbox"/> DA Version	<input checked="" type="checkbox"/> Description
<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Hardware	<input type="checkbox"/> IP Address	<input type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> License Country	<input checked="" type="checkbox"/> Link Name	<input type="checkbox"/> MAC	<input checked="" type="checkbox"/> Max Range
<input checked="" type="checkbox"/> Maximum Number Of Slaves	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Receive Frequency
<input type="checkbox"/> Remote MAC Address	<input type="checkbox"/> Remote Unit Name	<input checked="" type="checkbox"/> Software Version	<input type="checkbox"/> Status Time
<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Topology	<input checked="" type="checkbox"/> Tower	<input checked="" type="checkbox"/> Transmit Frequency
<input checked="" type="checkbox"/> Unit MSN	<input checked="" type="checkbox"/> Unit Name		

Network

<input checked="" type="checkbox"/> Default Gateway	<input type="checkbox"/> IP Version		
---	-------------------------------------	--	--

Radio

<input checked="" type="checkbox"/> Antenna Type	<input checked="" type="checkbox"/> Cable Loss	<input checked="" type="checkbox"/> Channel Width	<input checked="" type="checkbox"/> Data Bridging Availability
<input checked="" type="checkbox"/> Dual Payload	<input checked="" type="checkbox"/> Highest Mod Mode	<input checked="" type="checkbox"/> Link Capacity (Mbps)	<input checked="" type="checkbox"/> Link Capacity Variant
<input checked="" type="checkbox"/> Link Optimization (IP / TDM)	<input checked="" type="checkbox"/> Link Status	<input checked="" type="checkbox"/> Link Symmetry	<input checked="" type="checkbox"/> Link Up/Time
<input checked="" type="checkbox"/> Lower Centre Frequency (MHz)	<input checked="" type="checkbox"/> Lowest Ethernet Modulation Mode	<input checked="" type="checkbox"/> Maximum Transmit Power (dBm)	<input checked="" type="checkbox"/> QoS Data Priority Scheme
<input checked="" type="checkbox"/> Receive DataRate (Mbps)	<input checked="" type="checkbox"/> Signal Strength Ratio (dB)	<input checked="" type="checkbox"/> Spectrum Management Control	<input checked="" type="checkbox"/> TDD Sync Device
<input checked="" type="checkbox"/> TDD Synchronization Mode	<input checked="" type="checkbox"/> Transmit DataRate (Mbps)	<input checked="" type="checkbox"/> Wireless Link Availability	<input checked="" type="checkbox"/> Wireless Link Encryption

Location

<input checked="" type="checkbox"/> GPS Coordinates			
---	--	--	--

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.



NOTE:

The data will be exported for the devices which are under the System/Managed Account/Network/Tower/Site/AP Group based on the selection made by the user in the LHS Tree.

Performance Report

To generate performance reports:

1. Navigate to **Report > Performance** tab.
2. Select **Time Range** based on which the report can be generated for **Last Day** or **Last Week** or **Custom Time Range**.
3. Select **Period** to report at either **5 Minutes** or **1 Hour** or **1 Day**.
4. Select **Device Type**.
5. Select data to include in report.
6. Click **Start Job** to generate report **Now** or you can **Schedule** based on schedule type (**Daily**, **Weekly** or **Monthly**).



NOTE:

Custom Interval is currently supported only for one week and in future releases it will be expanded for Monthly data.

60 GHz cnWave Performance Report

Figure 56 60 GHz cnWave Performance Report (Node Type)

The screenshot shows the 'Report X' configuration page for a 60 GHz cnWave performance report. The 'Type' is set to 'Nodes'. Under 'Select data to include in report', the 'Basic' section is expanded, showing a grid of checkboxes for various metrics: CPU, MAC, Site, Device Mode, Memory, Device Name, Network, Device Type, and Timestamp. All these checkboxes are checked. The 'Start Job' button is visible at the bottom left.

Figure 57 60 GHz cnWave Performance Report (Links Type)

The screenshot shows the 'Report X' configuration page for a 60 GHz cnWave performance report. The 'Type' is set to 'Links'. Under 'Select data to include in report', the 'Basic' section is expanded, showing a grid of checkboxes for various metrics: Timestamp, RSSI, Frame Rate, Link Name, SNR, PER, A-Node Sector MAC, MCS, and Z-Node Sector MAC. All these checkboxes are checked. The 'Start Job' button is visible at the bottom left.

cnMatrix Performance Report

Figure 58 cnMatrix Performance Report

The screenshot shows the 'Report X' configuration page for a cnMatrix performance report. The 'Device Type' is set to 'cnMatrix'. Under 'Select data to include in report', the 'Basic' section is expanded, showing a grid of checkboxes for various metrics: CPUs, Packet Error, Packets Count (Tx), Device Name, Packets Count (Rx), Device Type, Throughput, and MAC. All these checkboxes are checked. The 'Start Job' button is visible at the bottom left.

cnPilot Home (R-Series) Performance Report

Figure 59 cnPilot Home (R-Series) Performance Report

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices **Performance** Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export. Select all parameters that should be included. Note: This feature may generate a large file if many devices are selected.

Schedule
 Now Daily Weekly Monthly (30 days)

Time Range
 Last Day Last Week Last Month Custom Time Range

Period
 5 Minutes 1 Hour 1 Day

Device Type
cnPilot Home (R Series)

Select data to include in report

Basic

<input checked="" type="checkbox"/> Avg No. Of Mesh Peers	<input checked="" type="checkbox"/> Avg Receive Rate	<input checked="" type="checkbox"/> Avg Send Rate	<input checked="" type="checkbox"/> Avg Usage
<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> MAC
<input checked="" type="checkbox"/> Max Receive Rate	<input checked="" type="checkbox"/> Max Send Rate	<input checked="" type="checkbox"/> Max Usage	<input checked="" type="checkbox"/> Min Receive Rate
<input checked="" type="checkbox"/> Min Send Rate	<input checked="" type="checkbox"/> Min Usage	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> No. of Clients
<input checked="" type="checkbox"/> Received Bytes (2.4 GHz)	<input checked="" type="checkbox"/> Received Bytes (5 GHz)	<input checked="" type="checkbox"/> Sent Bytes (2.4 GHz)	<input checked="" type="checkbox"/> Sent Bytes (5 GHz)
<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Total Received Bytes	<input checked="" type="checkbox"/> Total Sent Bytes

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

cnReach Performance Report

Figure 60 cnReach Performance Report

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices **Performance** Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export. Select all parameters that should be included. Note: This feature may generate a large file if many devices are selected.

Schedule
 Now Daily Weekly Monthly (30 days)

Time Range
 Last Day Last Week Last Month Custom Time Range

Period
 5 Minutes 1 Hour 1 Day

Device Type
cnReach

Select data to include in report

Basic

<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Neighbors
<input checked="" type="checkbox"/> Noise	<input checked="" type="checkbox"/> RSSI	<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Timestamp

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

cnRanger Performance Report

Figure 61 cnRanger Performance Report

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices **Performance** Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export. Select all parameters that should be included. Note: This feature may generate a large file if many devices are selected.

Schedule
 Now Daily Weekly Monthly (30 days)

Time Range
 Last Day Last Week Last Month Custom Time Range

Period 5 Minutes 1 Hour 1 Day

Device Type
cnRanger

Mode
 BBU RRH SM

Select data to include in report

Basic

<input checked="" type="checkbox"/> CPU	<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type
<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> MCS	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> RSRP
<input checked="" type="checkbox"/> RSRQ	<input checked="" type="checkbox"/> RSSI	<input checked="" type="checkbox"/> Session Drops	<input checked="" type="checkbox"/> SINR
<input checked="" type="checkbox"/> SM Count	<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Tower

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

cnVision Performance Report

Figure 62 cnVision Performance Report

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices **Performance** Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export. Select all parameters that should be included. Note: This feature may generate a large file if many devices are selected.

Schedule
 Now Daily Weekly Monthly (30 days)

Time Range
 Last Day Last Week Last Month Custom Time Range

Period 5 Minutes 1 Hour 1 Day

Device Type
cnVision

Mode
 Hub Client

Select data to include in report

Basic

<input checked="" type="checkbox"/> CPUs	<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type
<input checked="" type="checkbox"/> DL Frame Utilization	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> MCS	<input checked="" type="checkbox"/> Network
<input checked="" type="checkbox"/> Usage (Packet Count)	<input checked="" type="checkbox"/> Retransmission	<input checked="" type="checkbox"/> RSSI	<input checked="" type="checkbox"/> Session Drops
<input checked="" type="checkbox"/> SM Count	<input checked="" type="checkbox"/> SNR	<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Timestamp
<input checked="" type="checkbox"/> Tower			

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

Enterprise Wi-Fi Performance Report

Figure 63 Enterprise Performance Report

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices **Performance** Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export. Select all parameters that should be included. Note: This feature may generate a large file if many devices are selected.

Schedule
 Now Daily Weekly Monthly (30 days)

Time Range
 Last Day Last Week Last Month Custom Time Range

Period
 5 Minutes 1 Hour 1 Day

Device Type
Enterprise Wi-Fi

Select data to include in report

Basic

<input checked="" type="checkbox"/> Airtime (2.4 GHz)	<input checked="" type="checkbox"/> Airtime (5 GHz)	<input checked="" type="checkbox"/> Avg No. Of Mesh Peers	<input checked="" type="checkbox"/> Avg Receive Rate
<input checked="" type="checkbox"/> Avg Send Rate	<input checked="" type="checkbox"/> Avg Usage	<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name
<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> Interference (2.4 GHz)	<input checked="" type="checkbox"/> Interference (5 GHz)	<input checked="" type="checkbox"/> MAC
<input checked="" type="checkbox"/> Max Receive Rate	<input checked="" type="checkbox"/> Max Send Rate	<input checked="" type="checkbox"/> Max Usage	<input checked="" type="checkbox"/> Min Receive Rate
<input checked="" type="checkbox"/> Min Send Rate	<input checked="" type="checkbox"/> Min Usage	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Noise Floor (2.4 GHz)
<input checked="" type="checkbox"/> Noise Floor (5 GHz)	<input checked="" type="checkbox"/> No. of Clients	<input checked="" type="checkbox"/> Received Bytes (2.4 GHz)	<input checked="" type="checkbox"/> Received Bytes (5 GHz)
<input checked="" type="checkbox"/> Sent Bytes (2.4 GHz)	<input checked="" type="checkbox"/> Sent Bytes (5 GHz)	<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Timestamp
<input checked="" type="checkbox"/> Total Received Bytes	<input checked="" type="checkbox"/> Total Sent Bytes		

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

ePMP Performance Report

Figure 64 ePMP Performance Report

System

Dashboard Notifications Configuration Statistics **Report X** Software Update Clients Mesh Peers

Devices **Performance** Active Alarms Alarm History Events Clients Mesh Peers Guest Access Login Events

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export. Select all parameters that should be included. Note: This feature may generate a large file if many devices are selected.

Schedule
 Now Daily Weekly Monthly (30 days)

Time Range
 Last Day Last Week Last Month Custom Time Range

Period
 5 Minutes 1 Hour 1 Day

Device Type
ePMP

Mode
 AP SM

Select data to include in report

Basic

<input checked="" type="checkbox"/> CPUs	<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type
<input checked="" type="checkbox"/> DL Frame Utilization	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> MCS	<input checked="" type="checkbox"/> Network
<input checked="" type="checkbox"/> Usage (Packet Count)	<input checked="" type="checkbox"/> Retransmission	<input checked="" type="checkbox"/> RSSI	<input checked="" type="checkbox"/> Session Drops
<input checked="" type="checkbox"/> SM Count	<input checked="" type="checkbox"/> SNR	<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Timestamp
<input checked="" type="checkbox"/> Tower			

[Start Job](#) [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

Machfu Performance Report

Figure 65 Machfu Performance Report

The screenshot shows the 'Report X' configuration page for Machfu. The 'Performance' tab is active. The 'Device Type' is set to 'Machfu'. Under 'Select data to include in report', the 'Basic' category is expanded, and the following parameters are checked: Cellular RSSI, Cellular Throughput, CPU Load, Device Name, Device Type, Disk Storage, Flash Memory, MAC, Timestamp, and Wi-Fi Client RSSI. The 'Start Job' button is visible at the bottom.

PMP Performance Report

Figure 66 PMP Performance Report

The screenshot shows the 'Report X' configuration page for PMP. The 'Performance' tab is active. The 'Device Type' is set to 'PMP'. Under 'Select data to include in report', the 'Basic' category is expanded, and the following parameters are checked: LQI (DL), LQI (UL), CPU, Device Mode, Device Name, Device Type, Frame Utilization, MAC, Modulation, Network, RSSI, RSI Imbalance, Session Drops, SM Count, SNR, and Tower. The 'Start Job' button is visible at the bottom.

PTP Performance Report

Figure 67 PTP Performance Report

The screenshot shows the 'Report X' configuration page for PTP. The 'Performance' tab is active. The 'Device Type' is set to 'PTP'. Under 'Select data to include in report', the 'Basic' category is expanded, and the following parameters are checked: Capacity, Device Name, Device Type, Link Loss, MAC, Power, Receive SSI, and Throughput. The 'Start Job' button is visible at the bottom.

Active Alarms Report

To generate the Active Alarms reports, navigate to **Report > Active Alarms** tab.

This report will export the data for the Alarms which are currently active at the report generation time.

Figure 68 Active Alarms Report

The screenshot shows the 'Active Alarms' report configuration page. The breadcrumb trail is 'System > Report X > Active Alarms'. The page title is 'Active Alarms'. Below the title, there is a description: 'Generate report for active alarms as a comma-separated value (CSV) file. Active alarms for all devices under the tree node will be included in the export.' The 'Schedule' section has radio buttons for 'Now' (selected), 'Daily', 'Weekly', and 'Monthly (30 days)'. The 'Select data to include in report' section has a 'Basic' checkbox checked, and a grid of checkboxes for various fields: Acknowledged By, Duration, IP Address, IPv6 Address, MAC, Message, Name, Raised Time, Severity, Source, Source Type, and Status. At the bottom, there are 'Start Job' and 'View Report Jobs' buttons, and a note: 'Report generation may take several minutes, depending upon quantity of data.'

Alarms History Report

To generate the Active Alarms reports, navigate to **Report > Alarm History** tab.

This report will export the data for the Alarms which are currently active at the report generation time and the historical alarms for the specified time period and interval.

Figure 69 Alarms History Report

The screenshot shows the 'Alarm History' report configuration page. The breadcrumb trail is 'System > Report X > Alarm History'. The page title is 'Alarm History'. Below the title, there is a description: 'Generate report for all alarms that were active at any time within the time period selected. Alarms for all devices under the tree node selected will be included in the export.' The 'Schedule' section has radio buttons for 'Now' (selected), 'Daily', 'Weekly', and 'Monthly (30 days)'. The 'Interval' section has buttons for 'Last Day' (selected), 'Last Week', 'Last Month', and 'Custom Time Range'. The 'Select data to include in report' section has a 'Basic' checkbox checked, and a grid of checkboxes for various fields: Acknowledged By, Clear Time, Duration, IP Address, IPv6 Address, MAC, Message, Name, Raised Time, Severity, Source, Source Type, and Status. At the bottom, there are 'Start Job' and 'View Report Jobs' buttons, and a note: 'Report generation may take several minutes, depending upon quantity of data.'

Events Report

To generate the Events reports:


1. Navigate to **Report > Events** tab.
2. Select **Schedule** as **Now**, **Daily**, **Weekly**, or **Monthly**.
3. Select **Interval** on which the report can be generated for **Last Day**, **Last Week**, **Last Month**, or **Custom Time Range**.
4. Select data to include in report.
5. Click **Start Job** to generate report **Now** or you can **Schedule** based on schedule type (**Daily**, **Weekly** or **Monthly**).

Figure 70 Events Report

The screenshot shows the 'Events' report configuration page. At the top, there are navigation tabs: Dashboard, Notifications, Configuration, Statistics, **Report x**, Software Update, Clients, and Mesh Peers. Below these are sub-tabs: Devices, Performance, Active Alarms, Alarm History, **Events**, Clients, Mesh Peers, and Guest Access Login Events. The main heading is 'Generate report for all events raised during the time period selected. Events for devices under the tree node will be included in the export.' The 'Schedule' section has radio buttons for 'Now' (selected), 'Daily', 'Weekly', and 'Monthly (30 days)'. The 'Interval' section has buttons for 'Last Day' (selected), 'Last Week', 'Last Month', and 'Custom Time Range'. The 'Select data to include in report' section has a 'Basic' checkbox checked and a list of 10 items with checkboxes: Category, Message, Source, IP Address, Name, Source Type, IPv6 Address, Raised Time, Sub Category, MAC, and Severity. At the bottom, there are 'Start Job' and 'View Report Jobs' buttons, and a note: 'Report generation may take several minutes, depending upon quantity of data.'

The Events report will export the data for the events for the specified Time Period and Interval.

Clients Report



NOTE:
Clients Data is available for last day, last 24 Hrs and last week.

To generate the E-Series device reports of Client report:

1. Navigate to **Report > Clients** tab.
2. Select **Schedule** as **Now**, **Daily**, or **Weekly**. You can generate report based on schedule type (**Daily** or **Weekly**).
3. Select **Interval** on which the report can be generated. for **Last Day** or **Last Week**.
4. Select data to include in report.
5. Click **Start Job** to generate report **Now** and click **View Jobs** to view the Reports.

Figure 71 Clients Report

The screenshot shows the 'Clients' report configuration page. At the top, there are navigation tabs: Dashboard, Notifications, Configuration, Statistics, **Report x**, Software Update, Clients, and Mesh Peers. Below these are sub-tabs: Devices, Performance, Active Alarms, Alarm History, Events, **Clients**, Mesh Peers, and Guest Access Login Events. The main heading is 'Generate report for clients data'. The 'Schedule' section has radio buttons for 'Now' (selected), 'Daily', and 'Weekly'. The 'Time Range' section has radio buttons for 'Last Day' (selected) and 'Last Week'. The 'Select data to include in report' section has a 'Basic' checkbox checked and a list of 16 items with checkboxes: Average Signal, Avg Transmit Rate (Kbps), Client Username, Max Usage (Kbps), Min Usage (Kbps), Average Signal Quality, Client Class, Duration, Manufacturer, Total Receive Traffic, Average Usage, Client MAC, Max Receive Rate (Kbps), Min Receive Rate (Kbps), Total Traffic, Avg Receive Rate (Kbps), Client Type, Max Transmit Rate (Kbps), Min Transmit Rate (Kbps), and Total Transmit Traffic. At the bottom, there are 'Start Job' and 'View Report Jobs' buttons, and a note: 'Report generation may take several minutes, depending upon quantity of data.'

The **Clients** report exports the data for the clients for the specified Time Period and Interval.

Mesh Peers Report



NOTE:

Mesh Peers report is available for last 24 Hrs and last week.

To generate the Mesh Peers report:

1. Navigate to **Report > Mesh Peers** tab.
2. Select **Schedule** as **Now**, **Daily**, or **Weekly**. You can generate report based on schedule type (**Daily** or **Weekly**).
3. Select **Interval** on which the report can be generated. for **Last Day** or **Last Week**.
4. Select data to include in report.
5. Click **Start Job** to generate report **Now** and click **View Jobs** to view the Reports.

Figure 72 Mesh Peers Report

The screenshot shows the 'Mesh Peers' report configuration page. At the top, there are navigation tabs: Dashboard, Notifications, Configuration, Statistics, Report X (selected), Software Update, Clients, and Mesh Peers. Below these are sub-tabs: Devices, Performance, Active Alarms, Alarm History, Events, Clients, Mesh Peers (selected), and Guest Access Login Events. The main content area is titled 'Generate report for mesh peers data'. It includes a 'Schedule' section with radio buttons for 'Now' (selected), 'Daily', and 'Weekly'. Below that is a 'Time Range' section with a radio button for 'Last Day'. The 'Select data to include in report' section has a 'Basic' checkbox checked and a list of 20 data fields, each with a checked checkbox: AP MAC, AP Name, Association Time, Avg RSSI, Avg Receive Rate, Avg SNR, Avg Send Rate, Avg Throughput, Band, Base MAC Address, Client IPv6, Dissociation Time, Hostname, IP Address, Last Data Rate, MAC Address, Max Data Rate, Min Data Rate, Network, Total Received Bytes, Total Sent Bytes, Session Duration, and Site. At the bottom left, there are 'Start Job' and 'View Report Jobs' buttons. A note at the bottom states: 'Report generation may take several minutes, depending upon quantity of data.'



NOTE:

1. Every report page has a **View Report Jobs** link that directs the user to the **Report Jobs** page under **Administration > Jobs > Reports**.
2. To schedule a report **Now**, click **Start Job** under the respective report section. cnMaestro downloads the report immediately for the current system time.

Daily report will generate reports on a daily basis depending upon the start and the end time. The weekly report generates report on seven days interval depending upon the start and the end time. Click **Schedule** button and configure start and end time to schedule daily or weekly reports under the respective Reports section.

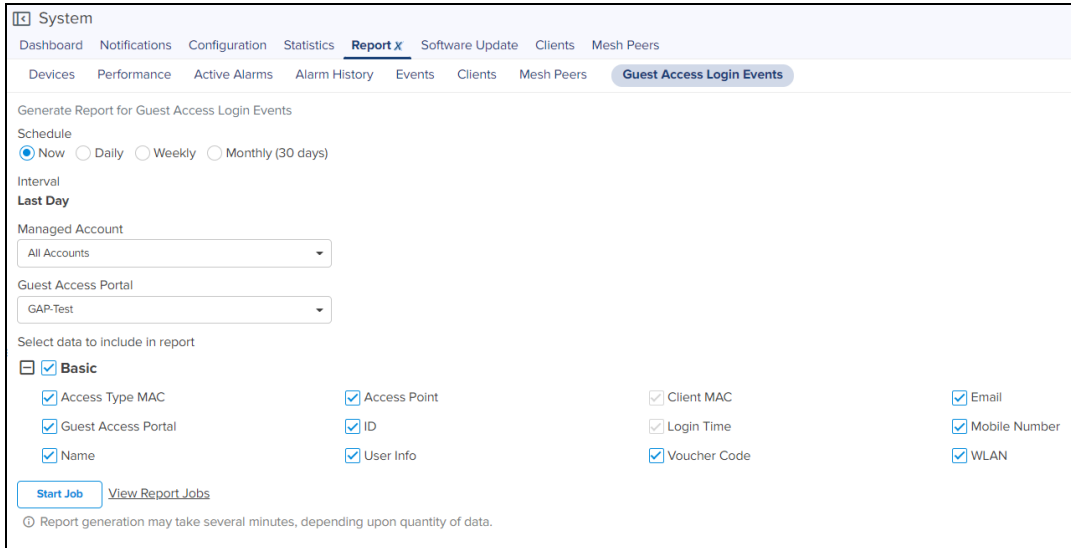
3. Export now option helps the user to create no of export jobs and these will be stored under **Administration > Jobs > Report** tab in the export page and can be downloaded with in seven days from the day of generation. This saves user's local memory from downloading each and every export report.

Guest Access Login Events

To generate the Guest Access Login Events reports:

1. Navigate to **Report > Guest Access Login Events** tab.

2. Select **Schedule** as **Now**, **Daily**, or **Weekly**. You can generate report based on schedule type (**Daily**, **Weekly**, or **Monthly**).
3. Select **Interval** the report can be generated for **Last Day**. By default Interval will be **Last Day**.
4. Select **Managed Account** and **Guest Access Portal** from drop-down.
5. Select data to include in report.
6. Click **Start Job** to generate report and click **View Jobs** to view the reports.



System

Dashboard Notifications Configuration Statistics **Report x** Software Update Clients Mesh Peers

Devices Performance Active Alarms Alarm History Events Clients Mesh Peers **Guest Access Login Events**

Generate Report for Guest Access Login Events

Schedule

Now Daily Weekly Monthly (30 days)

Interval

Last Day

Managed Account

All Accounts

Guest Access Portal

GAP-Test

Select data to include in report

Basic

<input checked="" type="checkbox"/> Access Type MAC	<input checked="" type="checkbox"/> Access Point	<input checked="" type="checkbox"/> Client MAC	<input checked="" type="checkbox"/> Email
<input checked="" type="checkbox"/> Guest Access Portal	<input checked="" type="checkbox"/> ID	<input checked="" type="checkbox"/> Login Time	<input checked="" type="checkbox"/> Mobile Number
<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> User Info	<input checked="" type="checkbox"/> Voucher Code	<input checked="" type="checkbox"/> WLAN

Start Job [View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

Remote Upload

Reports scheduled for **Now**, **Daily** or **Weekly** can be downloaded directly through the UI, or from an FTP or SFTP server.

To transfer reports to FTP or SFTP server:

1. Navigate to **Administration > Settings** page and select **Optional Features** tab.
2. Select the **Report Scheduler** check box to enable scheduling feature for data reports.
3. Select **Remote Upload** check box to upload the generated reports to the configured file server by FTP or SFTP.
4. Enter the **Remote Host**.
5. Enter the **Port Number**.
6. Enter the **Username**.
7. Enter the **Password**.
8. Enter the **File Path**.
9. Click **Save**.

Figure 73 Scheduling Reports

Optional Features

SNMP

Enable SNMP ✘ This feature requires configuration

Scheduled Jobs

Configure a remote file server (FTP/SFTP) to upload Reports and System Backups generated through scheduled jobs. [Learn more](#)

Remote Upload Upload data reports to below configured server.

Protocol

FTP SFTP

Remote Host

Port Number

Username

Password

 Show

File Path

 📁

Save
Discard

Report Jobs

Displays the list of scheduled report job created by different users.

Figure 74 Report Jobs

ID	Type	Managed Account	Source	Schedule	Starts At	Ends After	Created by	Created on	Status	Last Report	
70	Devices	All Accounts	System	Now	May 21, 2021 15:41	May 21, 2021 15:41	Administrator	May 21, 2021 15:41	Completed	May 21, 2021 15:42	
69	Devices	All Accounts	System	Now	May 21, 2021 14:56	May 21, 2021 14:56	Administrator	May 21, 2021 14:56	Completed	May 21, 2021 14:57	
68	Devices	All Accounts	System	Now	May 21, 2021 14:43	May 21, 2021 14:43	Administrator	May 21, 2021 14:43	Completed	May 21, 2021 14:44	
67	Devices	All Accounts	System	Now	May 21, 2021 13:17	May 21, 2021 13:17	Administrator	May 21, 2021 13:17	Completed	May 21, 2021 13:18	
66	Devices	All Accounts	System	Now	May 21, 2021 13:16	May 21, 2021 13:16	Administrator	May 21, 2021 13:16	Completed	May 21, 2021 13:16	
65	Performance	All Accounts	System	Monthly	Apr 29, 2021 16:28	Dec 25, 2021 16:28	Administrator	Apr 29, 2021 16:22	Scheduled (May 29, 2021 16:28)	Apr 29, 2021 16:28	
64	Performance	All Accounts	System	Monthly	Apr 29, 2021 16:28	Dec 25, 2021 16:28	Administrator	Apr 29, 2021 16:22	Scheduled (May 29, 2021 16:28)	Apr 29, 2021 16:28	
63	Performance	All Accounts	System	Daily	Apr 29, 2021 16:28	Jun 22, 2021 16:28	Administrator	Apr 29, 2021 16:22	Scheduled (May 23, 2021 16:28)	May 22, 2021 16:28	
62	Performance	All Accounts	System	Now	Apr 29, 2021 16:22	Apr 29, 2021 16:22	Administrator	Apr 29, 2021 16:22	Completed	Apr 29, 2021 16:22	
61	Devices	All Accounts	System	Now	Apr 29, 2021 16:22	Apr 29, 2021 16:22	Administrator	Apr 29, 2021 16:22	Completed	Apr 29, 2021 16:22	

A scheduled report job displays the following action buttons:

- **Edit:** Visible only for the active Jobs which are not yet run once. With this option, you can reschedule a job.
- **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:** User can instantly download the latest report directly once the download is complete without checking the show history.

Provisioning

This section includes the following topics:

- [Software Update](#)
- [Fixed Wireless Configuration](#)
- [Wireless LAN Configuration](#)
- [Auto-Provisioning](#)

Software Update

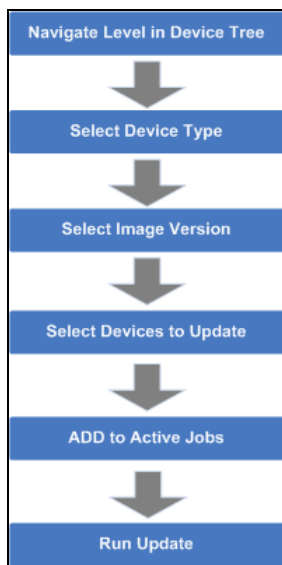
The **Software Update** tab displays the device update details for cnMaestro On-Premises. This section includes the following:

- [Software Update Overview](#)
- [Create Software Update Job](#)
- [Viewing Running Jobs in Header](#)
- [cnReach Bulk Software Upgrade](#)

Software Update Overview

The Software Update feature allows users to deploy the latest software images to devices. Software updates can be started at any level in the Device Tree, and individual devices can be selected for update. Updates are created as Jobs and placed into the jobs queue. When the update is ready to run, it can be started. The basic flow is the following:

Figure 75 Software Update Overview



When a Job finishes, it is placed in the completed Jobs table, where it remains for a week before it is deleted.

Create Software Update Job

Device Selection

Navigate the Device Tree to an appropriate level for the devices to be updated. For example, selecting an AP will filter the selectable devices to include itself and its children.

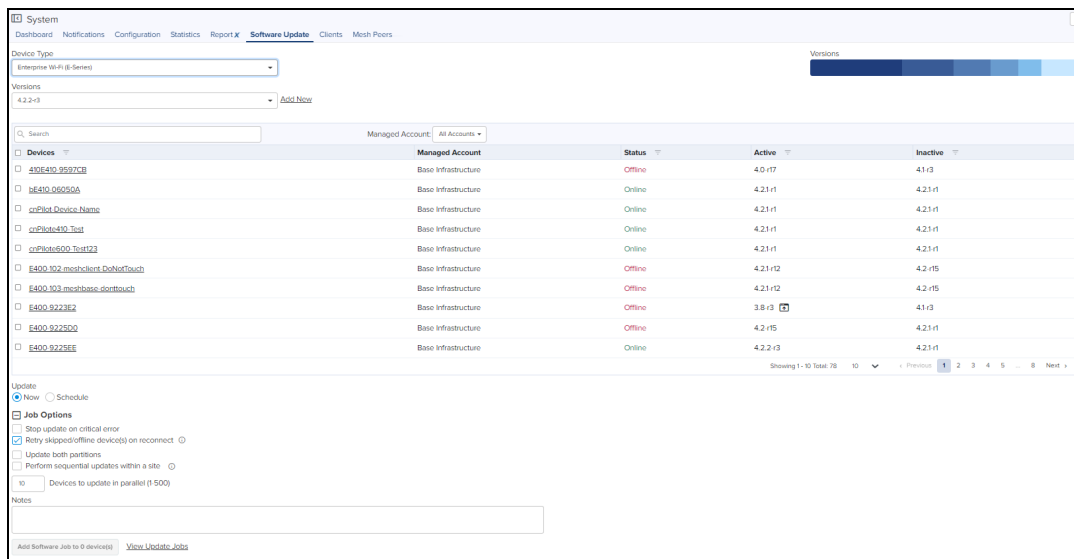
Device Type

Software Updates are executed on one device-type at a time. The type includes the specific hardware (Backhaul and Wi-Fi devices).

Software Update Dashboard

Once device type is chosen, the Software Update Dashboard 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 in the upgrade view.

Figure 76 Software Update Dashboard Enterprise Wi-Fi (E-Series)



NOTE:

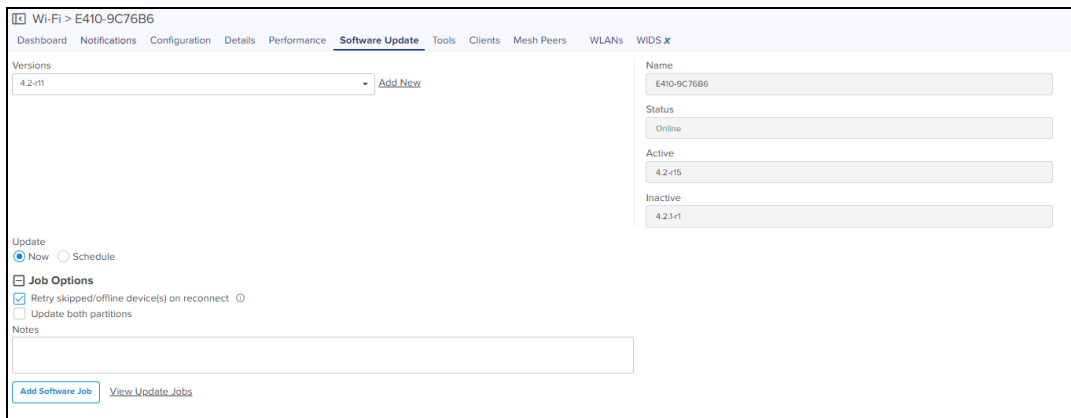
Update both partition option is available at System/Managed Account/Network/Site/Device levels.

Perform sequential updates within a site option is available at System/Managed Account/Network/Site level except the device level.

If the **Update both partition** is enabled/disabled. In the device level of the software update will be displayed as follows:

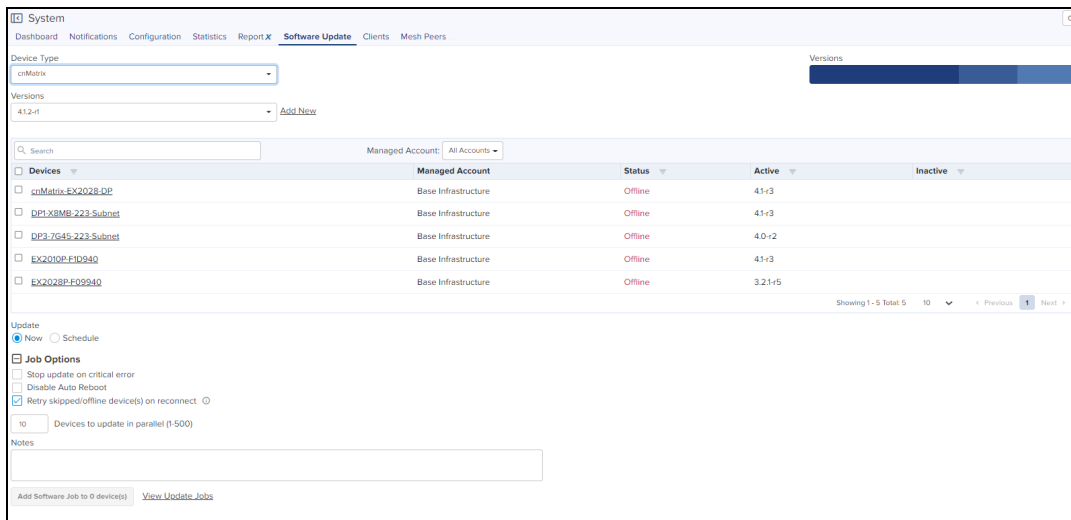
- **Enable:** The selected target image will be upgraded in both active and inactive portions of the device.
- **Disable:** The selected target image will be upgraded in only active portion of the device.

Figure 77 Software Update Dashboard Device level



If **Perform sequential updates within a site** is enabled the image upgrade will happen only on one device at a time in that particular site or upgrade will happen on all the devices.

Figure 78 Software Update Dashboard (cnMatrix)



Disable Auto Reboot option disables reboot after applying the new software image. User has to manually reboot the switch to complete the software update and boot with new version.

Figure 79 Software Update Dashboard (cnRanger)

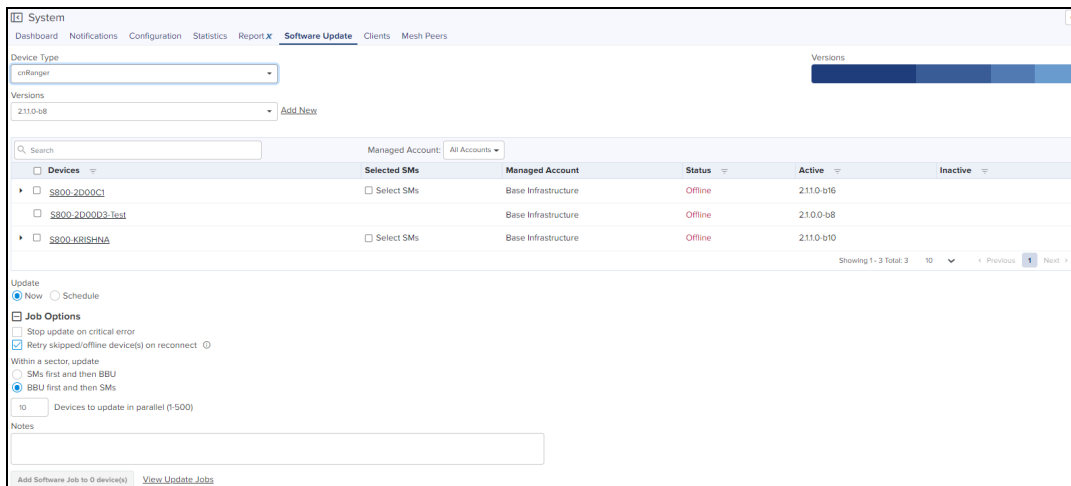
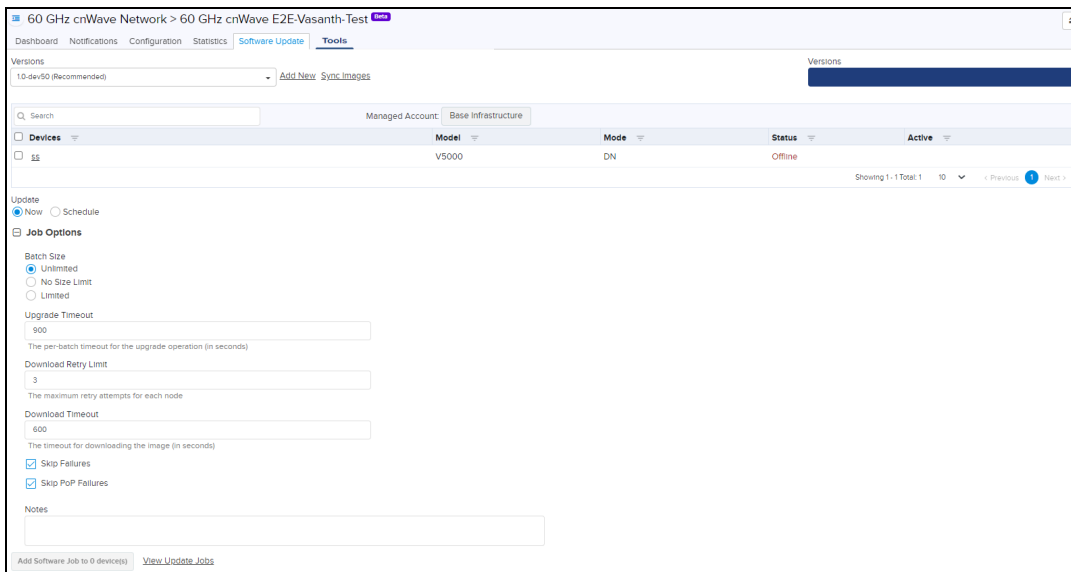


Figure 80 Software Update Dashboard (60 GHz cnWave)



Scheduling Software Update Job

You can now schedule a software update job on the devices by selecting **Schedule** radio button and providing the **Start Date** and **Start Time**.

Figure 81 Scheduling Software Update Job



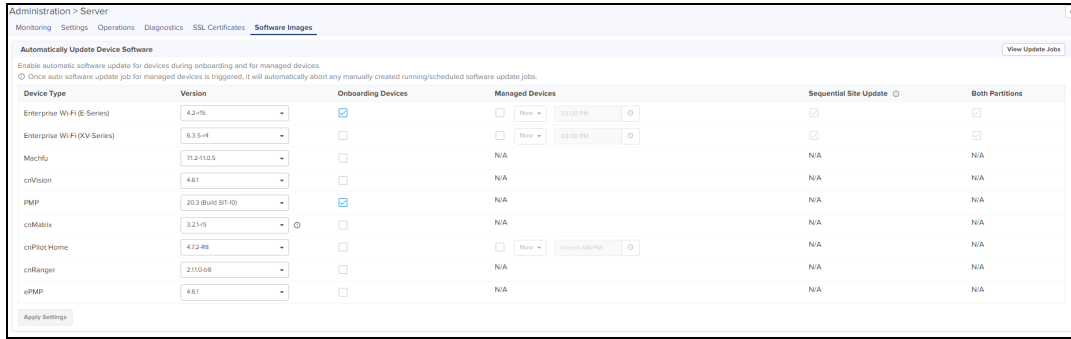
You can view the status of software update job in **Administration > Jobs > Software Update > Manual or Auto** page.

Software Update while Onboarding

The software version on the devices can be auto updated to the preferred version when the device first contacts cnMaestro.

To enable the device software feature update feature perform as follows:

1. Navigate to **Administration > Server > Software Images**.
2. Click the **Onboarding** checkbox for the particular device version.
3. Click **Apply Settings**.



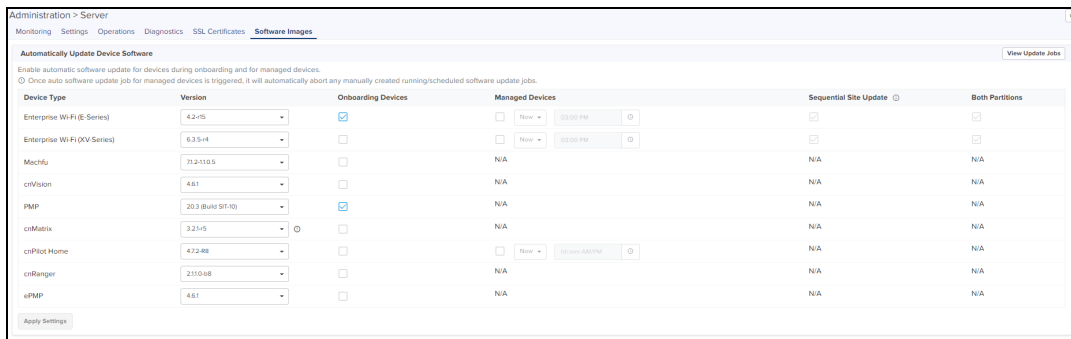
The device will get automatically upgraded based on the software selected while Onboarding.

Software Update through Managed Devices

The software version on the devices can be auto updated to the preferred version through the Managed Devices.

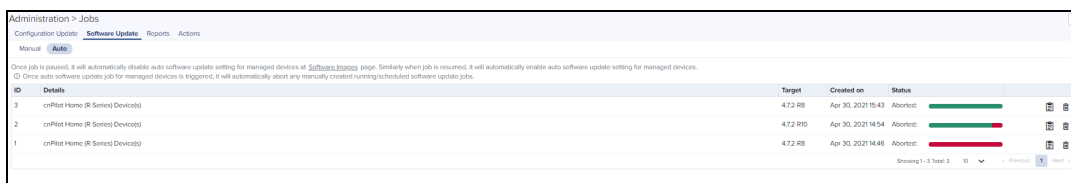
To enable the device software feature update feature perform as follows:

1. Navigate to **Administration > Server > Software Images**.
2. Click the **Managed Devices** checkbox for the particular device version.
3. Click **Apply Settings**.



Once the Setting is applied user can view the Jobs in **Administration > Jobs > Software Update > Auto** page.

Figure 82 Auto Update Page



NOTE

Auto update can be aborted during job is in-progress or idle state.

Device Table

Select the devices to upgrade in the Devices Table.



NOTE:

You can upgrade a device only when its status is Up. If you try to upgrade a device when it is Down, The selected device is down message is displayed in the UI.

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 34: Parameters Displayed 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 and cannot have images pushed to them.

Retry Software Update

The **Retry Software Update** option is available in every **Software Update** tab, and it is enabled by default.

Figure 83 Retry Software Update

Job Options

Update

Now Schedule

Stop update on critical error


Disable Auto Reboot

Retry skipped/offline device(s) on reconnect ⓘ

Devices to update in parallel (1-500)

If the software update job was skipped for a device as it was offline, an icon (⏪) appears next to the active software version of the device. This indicates that the software update for the device will be done with the **Target** device version in the Job, whenever it reconnects to cnMaestro.

If the software update job was skipped while upgrading with the same version as the device active version, then the icon will not be displayed and the device will not update when it reconnects.

	<p>NOTE: The device which undergoes Retry Software Update, does not create a new Job.</p>
---	---

Options

Stop Updates on Critical Error

If one of the 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, if desired.

Sector Upgrade Order

The recommended update ordering for devices within a sector will be pre-configured according to the recommendations for the device. It can be changed if desired.

**NOTE:**

Device updates 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 upgrade an ePMP (Sectors) device:

1. Navigate to **System** or **Network** or **Tower** or **Device** level. From the list, select the system or network or tower or device to which the device belongs.
2. Navigate to **Manage > Software Update > Select Devices** page.
3. Select **ePMP (Sectors)** from the following **Select Device Type** drop-down list:
 - a. 60 GHz cnWave
 - b. cnMatrix
 - c. cnReach
 - d. cnRanger
 - e. cnPilot Home (R-Series)
 - f. cnPilot Enterprise (ePMP Hotspot)
 - g. cnVision
 - h. Enterprise Wi-Fi (E-Series)
 - i. Enterprise Wi-Fi (XV-Series)
 - j. ePMP (Sectors)
 - k. Machfu
 - l. PMP (Sectors)
 - m. PTP
4. Select the software image to update from the **Select Image Version** drop-down list.
5. Select the devices to update by clicking the **tick** icon.
6. Set desired **Job Options**.
7. Click **Add Software Job** button.

Software Update Parameters

The Software Update Jobs table lists all currently running, queued, and completed jobs. The jobs can be triggered immediately or can be run later.

(**Administration > Jobs > Software Update** tab)

The following table displays the list of parameters displayed in the **Software Update Jobs** tab:

Table 35: Parameters displayed in Software Update Jobs tab

Parameter	Description
Created By	The user who has created this job.
Created On	Date and time on which the job is created.
Completed On	Date and time on which the job is
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Image Type	Displays the type of image selected for the device.
Occurrence	Displays the occurrence of the update like now, scheduled, etc.
Status	Status of update.
Target	Target software version to upgrade.
Managed Account	Displays the Managed Account Name.

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 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 84 Abort Software Job


ID	Details	Image Type	Occurrence	Target	Created by	Created on	Completed on	Status
6	1 cnMaestro Device(s)	Device	Now	3.11-r3	Administrator	Jan 21, 2021 14:06	Jan 21, 2021 14:10	Completed:
4	1 cnMaestro Device(s)	Device	Schedule	3.2-r4	Administrator	Jan 19, 2021 11:31	Jan 19, 2021 11:37	Completed:
3	1 cnMaestro Device(s)	Device	Now	3.2-r5	Administrator	Jan 11, 2021 13:18	Jan 11, 2021 13:22	Aborted:
2	1 cnMaestro Device(s)	Device	Now	3.2-r5	Administrator	Jan 07, 2021 18:29	Jan 07, 2021 18:33	Completed:
1	1 Enterprise Wi-Fi Device(s)	Device	Schedule	3.11.4-r3	Administrator	Jan 07, 2021 15:55	Jan 07, 2021 16:04	Completed:



NOTE:

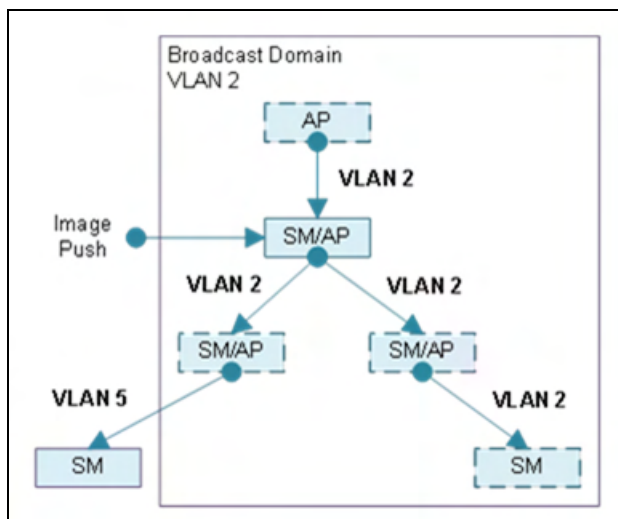
1. Devices which are already completed display as **Completed** with a message update complete along with the status as **Completed**.
2. Devices which are ongoing display as **Aborted** with a message **Manually Aborted** with the status as **Aborted**.
3. Devices which have not yet started display as "skipped" with a message "job was aborted" with the status as **Skipped**.
4. Software update jobs can be scheduled in parallel irrespective of other running Jobs as PRO account supports Parallel Jobs also If same devcie is used for config/ software job at a time only one operation will be done as the Job locks the device until it finishes.

Viewing Running Jobs in Header

Click the  icon at the top right corner of the UI. This directs you to the **Jobs** page of the Software Update tab. For more information, see [Software Update Parameters](#).

cnReach Bulk Software Upgrade

Distributing software to cnReach devices can take many hours, due to the relatively low RF bandwidth. In order to minimize wireless traffic, cnMaestro supports the cnReach mechanism by which a single AP coordinates the broadcast distribution of firmware to every cnReach device within its VLAN. In the below figure, the bulk upgrade operation transfers an image to the middle AP, which then distributes it to all APs with VLAN 2. The APs are not updated in this process; the firmware is just pushed into their storage, where it can be applied later (once the distribution completes). cnReach has a mechanism to handle offline devices during the distribution (which can take upwards of a day), or devices added midway through the transfer. Often this means the process repeats a second time, to handle any updates.



The **Bulk Software Upgrade** is optional, and meant to be used for efficiency. One can still use the standard Software Update mechanism to transfer images to cnReach devices one-at-a-time, though the distribution could be many hours or days.

Firmware Versions (OS and Radio)

cnReach devices have two versions of software: one for the Motherboard OS, and another for the Radio. Each Radio can have a different version of firmware. When selecting software to distribute, one should choose either OS or Radio. During the Apply phase, when the image is updated, one or both Radios can be selected.

Bulk Upgrade

The Bulk Upgrade tab is accessed by selecting a cnReach AP then **Software Update > Bulk Upgrade**. The Motherboard (OS) or Radio software is available, and the distribution started and stopped. Once the bulk upgrade is started, the distribution continues until stopped, so be sure to manually stop the process when complete.

Figure 85 : Bulk Upgrade

cnReach > Vanguard-B-School-HTTPS

Dashboard Notifications Configuration Details **Software Update**

Device

Image Type
OS

Versions
cn-EBX.5.2.17e (Recommended) [Release Notes](#) [Add New](#)

Update
 Now Schedule

Job Options

Notes

[Add Software Job](#) [View Update Jobs](#)

Name
Vanguard-B-School-HTTPS

Status
Offline

Active
cn-EBX.5.2.18g

Inactive
cn-EBX.5.2.18c



NOTE:

You must start the distribution on a single AP in a cnReach VLAN, and only run it from that AP. Executing Bulk Software Upgrade on more than one AP in a VLAN will not be prevented by cnReach devices, and it could lead to distribution failures.

Upgrade Tracking

The following page is displayed when an AP is actively distributing software. One can view other devices in the VLAN (and their current software versions), and the distribution status. Distribution can be stopped at any time, and images can be applied directly to the devices in the list.

Device **Bulk Upgrade**

Distribute a software image across the cnReach deployment using the native cnReach Bulk Upgrade. The image is efficiently copied from this AP to all cnReach devices on the same VLAN. The process could take many hours, depending upon available bandwidth.

Distribution Status

Started on: Oct 18 2019 16:13:15 0 of 2 (0.00%)

Distribution Version: cn-EBX.5.2.17e

Apply Status

Not Started

[Abort Job](#) [View Update Jobs](#)

View Affected Devices

Device	Mode	IP Address	OS Version	Radio 1 Version	Radio 2 Version	Distribution Status	Apply Status
cnReach_SIT_PMP_02_HTTPS	AP/EP	10.110.208.191	cn-EBX.5.2.18c	1.52.19110	1.51.18494		
cnReach_SIT_PMP_03_Edited	EP	10.110.208.192	cn-EBX.5.2.18c	1.48.17487			

Showing 1 - 2 Total: 2

Fixed Wireless Configuration

This chapter provides the following information:

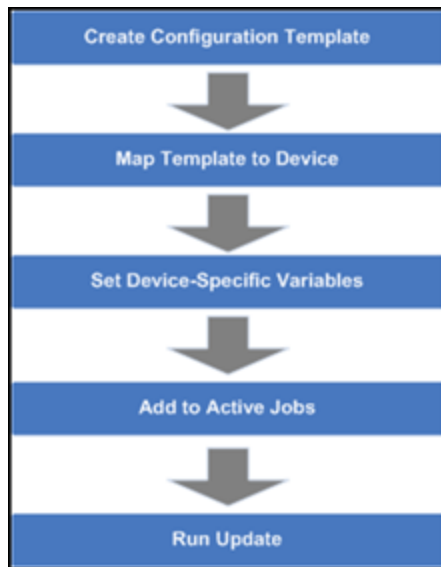
- [Overview](#)
- [Configuration Templates](#)
- [Configuration Variables](#)
- [Configuration Update](#)

Overview

Template configuration is supported for cnMatrix, cnPilot Home, ePMP, PMP, Machfu, cnVision and cnReach devices. Templates are textual representations of device settings that contain a full configuration or partial configuration. When a template is applied to a device, the only parameters changed are those in the template.

The below figure presents the basic template configuration flow:

Figure 86 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.

Sample ePMP Template

The ePMP template uses the exported ePMP configuration format, which is JSON-encoded.

Figure 87 Sample ePMP Template

```

"device_props": {
  "acsEnable": "0",
  "acsScanMinDwellTime": "200",
  "acsScanMaxDwellTime": "300",
  "acsControl": "0",
  "bcPriority": "0",
  "cambiumInternetConnectionServerIP": "",
  "centerFrequency": "5670",
  "dataVLANEnable": "0",
  "dataVLANVID": "",
  ...,
  "snmpTrapTable": [{
    "snmpTrapEntryIP": "10.120.143.176",
    "snmpTrapEntryPort": "162"
  }],
  ...
}

```

Configuration Variables

Administrators can embed variables into templates that will be replaced when the template is applied to a device. This allows one to leverage a shared, generic template, but to tailor it to individual devices when it is pushed. Template variables are added to a configuration file by replacing an existing parameter with a customer-defined string of the format `${VARIABLE}`. An example configuration line with a single variable replacement is shown below:

`"networkLanIPAddr": $ {IP ADDRESS}`

The above variable is named `IP_ADDRESS`. When the template is pushed to a device, this variable will be replaced with a value specific to the device. This value needs to be set for the device prior to the template application, else the configuration will not be pushed. Default values can also be specified for variables, as shown below:

`"networkLanIPAddr": $ {IP ADDRESS="10.1.1.254"},`

The default value is `"10.1.1.254"`. In this case if the variable is not set for a device, the default value is used.

Variable Usage

The figure below highlights how **Templates** and **Variables** are merged to create the final configuration that is pushed to the device.

Figure 88 Variable Usage



Macros

Macros can be used in templates similar to configuration variables except they automatically take 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 re-used later. This means the next time you apply a template that leverages a variable with the same name as one used previously, its 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 one type of device will 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, executes in AP and SM modes. The ePMP templates can be configured so they can only be applied 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 that have default settings will 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. See the documentation for your devices for full details.

Template File Creation

The typical process taken for creating your own configuration template text from scratch are below.

1. On a test device configure the parameters you are interested in pushing to devices with values that will be easy to search for. This can be done directly on the device web UI .
2. Export the device configuration. Via cnMaestro this is done by navigating to **Configuration > Templates**, selecting the device in the left-hand tree and then clicking 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 you entered in step 1. You can also search for the parameter name to try 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 **Shared Settings > Templates** in the main menu.
2. Click the **Add Template**.
3. Choose a **Device Type**, **Name**, and **Description** for the template. For ePMP templates, you should select a **Device Mode**.

4. Either upload your template into the UI or paste the 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 mode match the device selected.
6. By selecting **Custom** option under **Template** type filter. All Default templates will be hidden.



NOTE:

When you navigate to the **Template** default template type filter will be custom. User needs to select **All** or **Default** in order to view other templates.

Figure 89 Template configuration (ePMP/PMP)

System Configuration page for ePMP/PMP. The interface includes a navigation bar with 'Configuration' selected. A 'Device Type' dropdown is set to 'ePMP (Sector)'. The 'Managed Account' is 'All Accounts'. A 'Template' dropdown is set to 'Example ePMP AP GPS - Quick Start Template'. A search bar is present above a table of devices. The table has columns: Device, Selected SMs, Managed Account, Status, and Network > Tower. Two devices are listed:

Device	Selected SMs	Managed Account	Status	Network > Tower
E400_2003a7	Select SMs	Base Infrastructure	Offline	default
vinodecmn1234567890123456789012	Select SMs	Base Infrastructure	Offline	1qj5 > ePMP_tower

Below the table, there are 'Update' options (Now or Schedule) and 'Job Options' (SMs first or AP first). A 'Notes' field is also present.

Figure 90 Template configuration (cnPilot Home R-Series)

System Configuration page for cnPilot Home R-Series. The interface includes a navigation bar with 'Configuration' selected. A 'Device Type' dropdown is set to 'cnPilot Home (R-Series)'. The 'Managed Account' is 'All Accounts'. A search bar is present above a table of devices. The table has columns: Device, Managed Account, AP Group, Status, Sync Status, Network, and Tower/Site. Multiple devices are listed:

Device	Managed Account	AP Group	Status	Sync Status	Network	Tower/Site
190V_Test	Base Infrastructure	Default Home	Offline	In Sync	default	R5SERIES
Cambium123	Base Infrastructure	Default Home	Offline	Not In Sync	default	R5SERIES
cnP_Home_Bsym_06_9f	Base Infrastructure	N/A	Offline	N/A	1qj5	ePMP_tower
cnPilot_R190W-10C2D1	Base Infrastructure	N/A	Offline	N/A	default	
cnPilot_R201P_changed	Base Infrastructure	Default Home	Offline	Not In Sync	default	R5SERIES
cnPilot_r200-08072f	Base Infrastructure	N/A	Offline	N/A	default	R5SERIES
cnPilot_08B0A1	Base Infrastructure	Default Home	Offline	Not In Sync	default	R5SERIES
cnPilot_R190V_DP	Base Infrastructure	Default Home	Offline	Not In Sync	default	R5SERIES
cnPilot_r190V-14BDc1	Base Infrastructure	N/A	Offline	N/A	j\$hm0stet[あ-う]ア-ヴ[あ-...	Site
cnPilot_r190V-14EF49	Base Infrastructure	Default Home	Offline	Not In Sync	default	R5SERIES

At the bottom right of the table, it says 'Showing 1-10 Total: 38'.

Figure 91 Template configuration (cnVision)

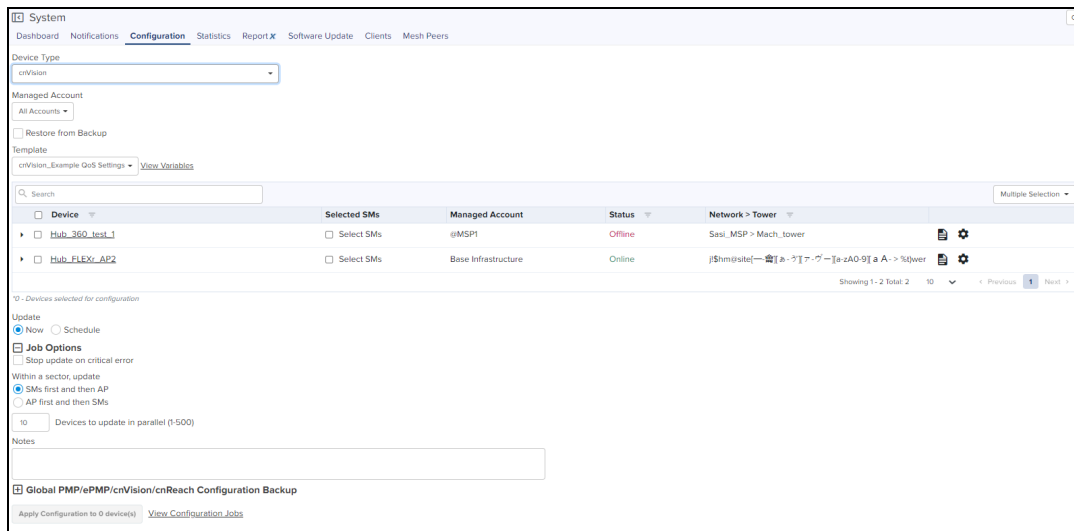
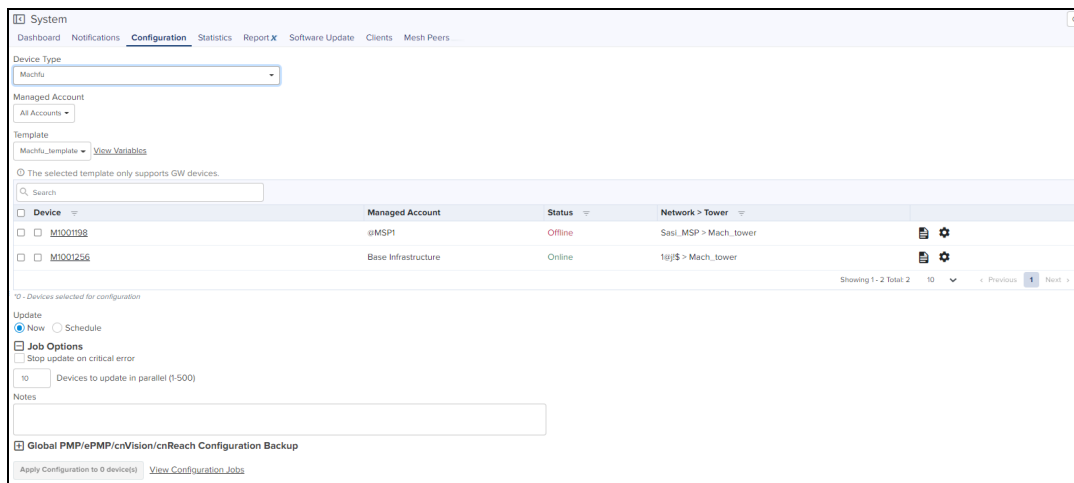


Figure 92 Template configuration (Machfu)



Configuration Update

Device Selection

First navigate to the **Configuration Update** tab, then navigate the Device Tree to the appropriate level for device selection. For example, selecting an 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 36: Parameters Displayed in the Device Table

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” cannot have images pushed to them.



NOTE:

You can save and download the existing device configuration as template by clicking **View Device Configuration** link.

Options

Stop all Configuration on a Critical Error

If one of the configuration updates fails, then do not start any additional updates and instead pause the update job. All existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off.

Parallel Upgrades

Define how many configuration updates to perform in parallel.

Start Job Now

If enabled, attempts to automatically start the configuration job immediately after creation.

Update Ordering

Allows you to specify update ordering within a 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 that are 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 93 Abort Configuration

ID	Details	Image Type	Occurrence	Target	Created by	Created on	Completed on	Status
6	1 cnMaestro Device(s)	Device	Now	3.15-r3	Administrator	Jan 21, 2021 14:06	Jan 21, 2021 14:10	Completed:
4	1 cnMaestro Device(s)	Device	Schedule	3.2-44	Administrator	Jan 19, 2021 11:31	Jan 19, 2021 11:37	Completed:
3	1 cnMaestro Device(s)	Device	Now	3.2.1-5	Administrator	Jan 11, 2021 13:18	Jan 11, 2021 13:22	Aborted:
2	1 cnMaestro Device(s)	Device	Now	3.2.1-5	Administrator	Jan 07, 2021 18:29	Jan 07, 2021 18:33	Completed:
1	1 Enterprise Wi-Fi Device(s)	Device	Schedule	3.11.43-r3	Administrator	Jan 07, 2021 15:55	Jan 07, 2021 16:04	Completed:

**NOTE:**

1. Devices which are already completed 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:

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 following **Device Type** drop-down list:
 - a. cnMatrix
 - b. cnPilot Enterprise (ePMP Hotspot)
 - c. cnPilot Home (R-Series)
 - d. cnReach
 - e. cnVision
 - f. Enterprise Wi-Fi (E-Series, XV-Series)
 - g. ePMP (Sectors)
 - h. Machfu
 - i. PMP (Sectors)
 - j. PTP
4. Select the configuration template to upgrade from the **Template** drop-down list.
5. Select the device(s) to upgrade by clicking the tick icon.
6. Set any variables that are required for selected devices by clicking the gear icon under the "Configure" column on the right side of the table. The configuration upgrade cannot proceed until all required variables (those without default parameters) are set. 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.
7. Click **Apply Configuration**.

**NOTE:**

You can save and download the existing device configuration as template by clicking **View Device Configuration** link.

Configuration Backup

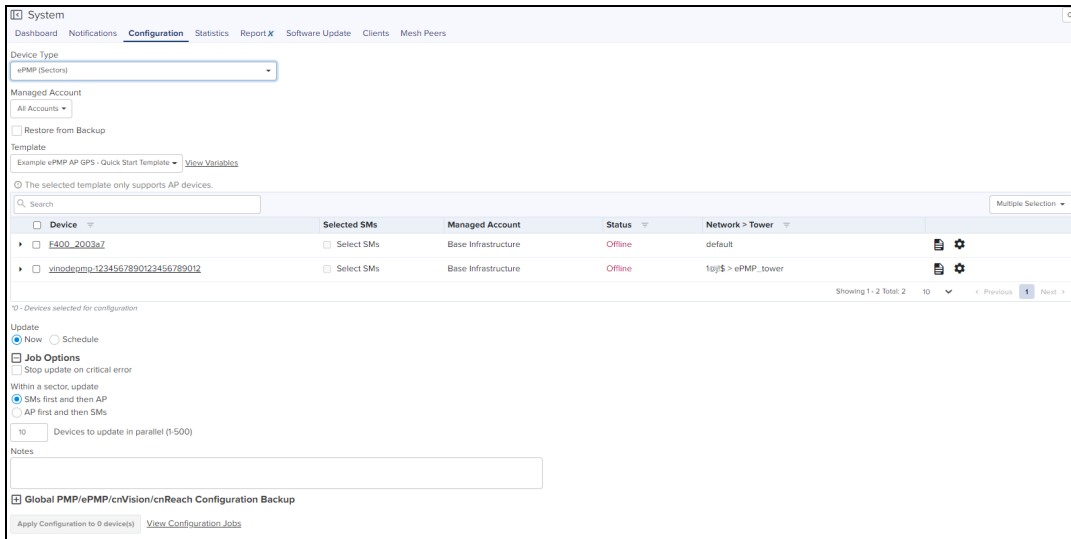
Configuration Backup pulls and stores configuration from Fixed Wireless devices (PMP and ePMP) and cnReach devices which are currently online.

The backup operations log can be done through:

- System level
- Device level

System Level

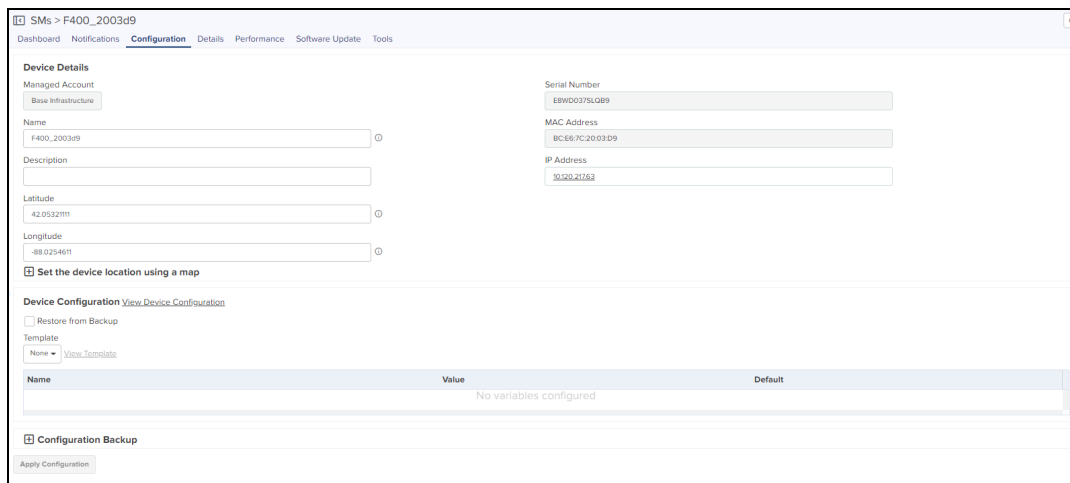
1. Navigate to **Manage > Configuration**.
2. Select cnReach/cnVision/PMP/ePMP (Sectors) from the following **Device Type** drop-down list:
3. In **Global cnReach/PMP/ePMP Configuration Backup** click **Backup Now**.



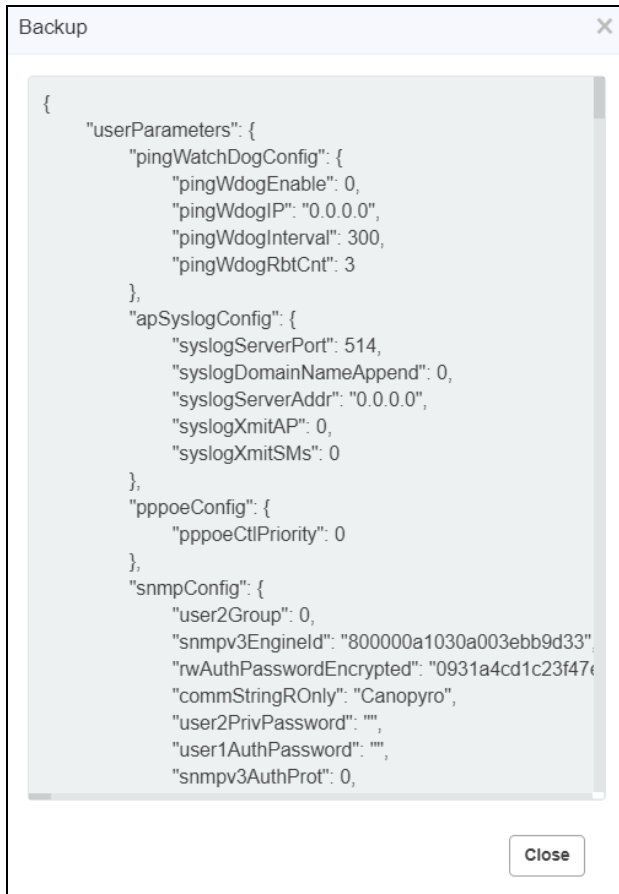
4. Last backup displays in the **Log from Last Execution** tab with the date and time.
5. Click **Export** to export the backup in **.json** format.

Device Level

1. Navigate to **Manage > System**, select cnReach/cnVision/PMP/ePMP **Network** in the Device Tree.
2. Navigate to **Configuration > Configuration Backup** click **Backup Now**.



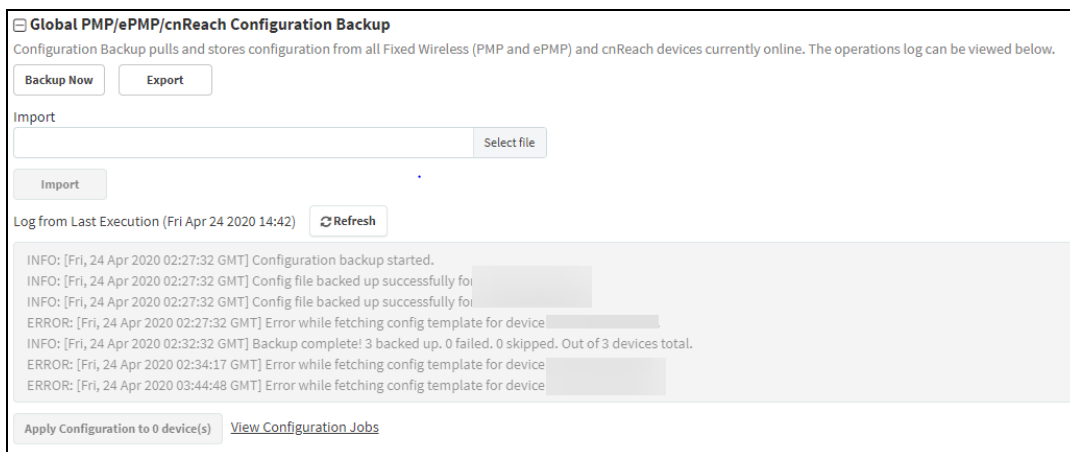
3. Click **View** to view the backup data.



Import Configuration Backup

Perform as follows to import the configuration backup of the device.

1. Navigate to **Manage > Configuration > Device Details** in the main menu.
2. Select cnReach/cnVision/PMP/ePMP (Sectors) from the following **Device Type** drop-down list:
3. In **Global cnReach/cnVision/PMP/ePMP Configuration Backup**, click **Select File** in import tab.



4. Once selected the file click **Import**.

Restore from Backup

Restore from backup operations can be done through:

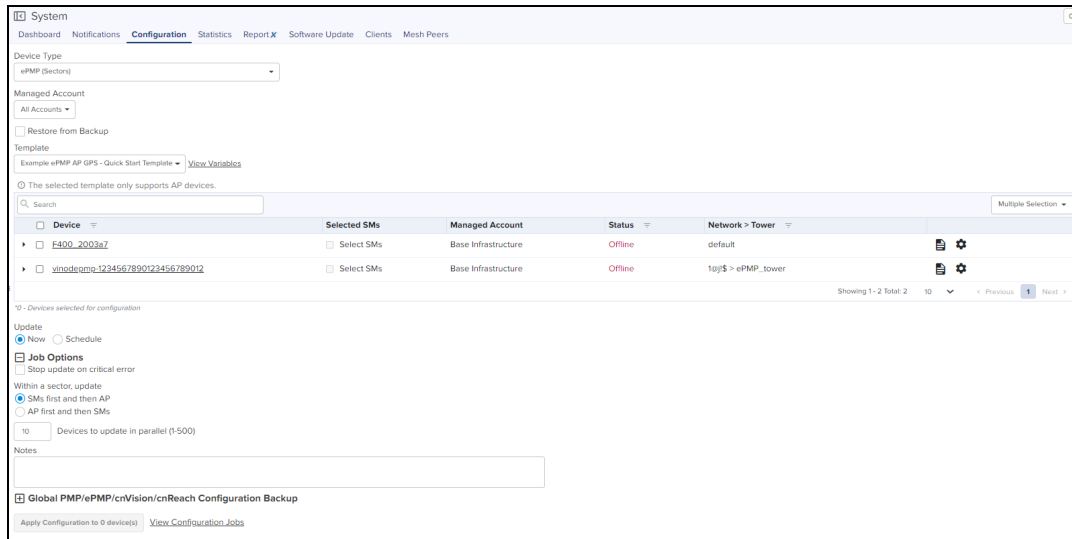
- System level

- Device level

System Level

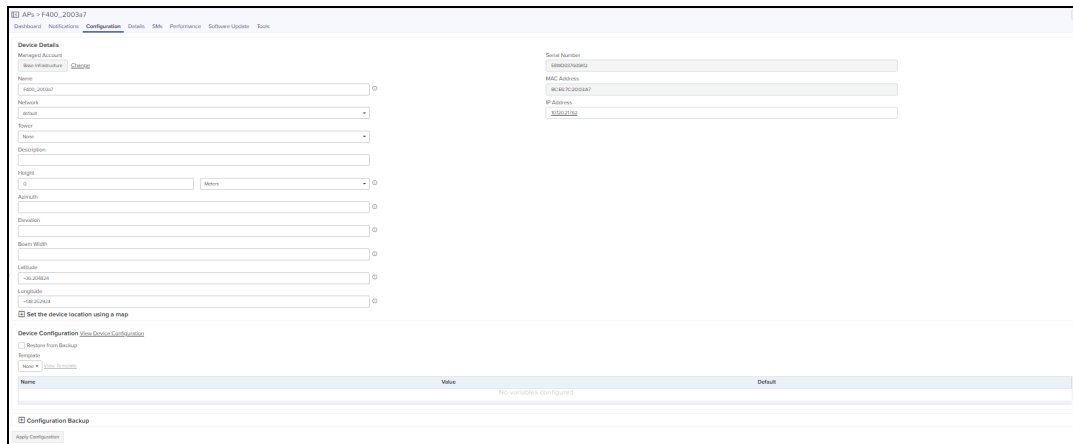
Perform as follows to restore the configuration backup of the device.

1. Navigate to **Manage**, select **System/Managed Account/ Network/Tower > Configuration** in the main menu.
2. Select cnReach/cnVision/PMP/ePMP (Sectors) from the following **Device Type** drop-down list.
3. Enable the **Restore from Backup**.
4. Select the Device from the list.
5. Click **Apply Configuration to devices**.



Device Level

1. Navigate to **Manage > System**, select **cnReach/cnVision/PMP/ePMP Network** in the Device Tree.
2. Navigate to **Configuration > Device Configuration > click Restore from Backup**.
3. Click **Apply Configuration to devices**.



Jobs

Administration > Jobs > Configuration Update tab lists all currently running, queued and completed jobs. The jobs can be triggered immediately or run later.

The following table displays the list of parameters in the **Jobs** tab:

Table 37: Parameters displayed in Configuration Update tab

Parameter	Description
Action	Use the Start or Delete button to manage the upgrade process. After upgrade has started, the Pause button will stop new upgrades from beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the Resume button.
Created By	The user who has created this job.
Created On	Date and time on which the job is created.
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Parallel	Number of device to start in parallel.
Stop on Error	Stop the job, if any device in middle finds any error.
Sector Priority	For ePMP/PMP, cnVision Client/Hub, the priority of AP/SM to start.
Status	Status of 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 displayed after the update.
Result	The upgrade status of the device.
Status	Status of the device.

Configuration Update

Administrators can apply 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](#).

Wireless LAN Configuration

Wi-Fi configuration is handled through AP Groups (Fixed Wireless devices, such as cnMatrix, ePMP and PMP, use Templates).

This chapter provides the following details:

- [cnPilot Home and Enterprise Wi-Fi](#)
- [Factory Reset](#)
- [cnMatrix Switches](#)

cnPilot Home and Enterprise Wi-Fi

This section provides the following details:

- [Configure cnPilot using cnMaestro](#)
- [Pre-Defined Overrides](#)
- [User-Defined Overrides](#)
- [User-Defined Variables](#)
- [Synchronize \(Sync\) Configuration](#)
- [Configuration Job Status](#)

There are two types of cnPilot devices:

1. Enterprise Wi-Fi by Enterprise Wi-Fi (E-Series), Enterprise Wi-Fi (XV-Series) and cnPilot Enterprise (ePMP hotspot)
2. cnPilot Home by cnPilot R-Series devices.

Each WLAN or AP Group, prior to creation, is mapped to one of these device categories and can only be used with supported device types. Two categories are required, because the features available in Enterprise and Home are different.

Configure cnPilot using cnMaestro

cnPilot devices are configured by creating an AP Group, mapping it to shared WLANs, and then assigning it to a particular device through the **Configuration** tab. Once assigned, the configuration is pushed automatically if Auto Sync is enabled, or manually if disabled (this requires a manual sync).

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 will be placed in an unsynchronized state until it is manually synchronized. This can be done by navigating to the device Configuration page and clicking the **Sync Now** button, or by navigating to the **Sync Configuration** page (**Administration > Sync Configuration**).

The process for creating a Wi-Fi device configuration is as follows:

1. Navigate to **Shared Settings > AP Groups and WLANs**.
2. Create an AP Group.

3. Select an AP Group Type. The choices are cnPilot Home (which represents the R-Series) and cnPilot Enterprise (which maps to the E-Series and ePMP Hotspot). The configuration options depend upon the AP Group Type.



NOTE:

The Wireless LAN view supports cnPilot Enterprise devices, so the cnPilot Home device type is not available.

4. Assign WLANs to the AP Group (you may want to update WLAN SSID and security parameters during this step).
5. Map devices to an AP Group by selecting the AP Group in the device **Configuration** tab.

AP Groups support all Wi-Fi devices, including: cnPilot R190/200/201, cnPilot E400/E410/E500, and ePMP 1000 Hotspot.

Creating a WLAN

To create a WLAN, navigate to **Shared Settings > AP Groups and WLANs** (or the WLAN page in the Wireless LAN View) and select **New WLAN**. As with AP Groups, WLANs are separated into cnPilot Home and cnPilot Enterprise types. cnPilot Enterprise WLANs are able to configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters. cnPilot Home WLANs 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-Z0-9_- *&#@!<>.[]^~`\$). The user can also rename them if required.

Steps to create WLAN policy:

1. From homepage navigate to **WLANs**.
2. Click **New WLAN**, provide basic parameters to WLAN, and ensure **WPA2 Pre-Shared keys** is enabled in Security drop-down.

Basic Information

Type: Enterprise WLAN

Name:

Scope:

Description:

Basic Settings

SSID: Enable

SSID: The SSID of this WLAN (up to 32 characters)

Mode: Match Basic/Client/Recovery mode

Security: Default VLAN assigned to clients on this WLAN (0-4094)

Security: Set authentication and encryption type

Radio: Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported

Client Isolation: When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

cnMaestro Managed Roaming: Enable centralized Guest Access Session management of roaming for wireless clients through cnMaestro

Hide SSID: Do not broadcast SSID in beacons

Advanced Settings

Max Clients: Default maximum client assigned to this WLAN (0-255)

LAN Pinning: Configure VLAN Pinning

Session Timeout: Session time in seconds (60 to 604800)

Reconnect Timeout: Reconnect time in seconds (60 to 28800)

Drop Multicast Traffic: Drop the send/receive of multicast traffic

LAMPSD: Enable LAMPSD

QoS: Enable QoS load element

DTIM Interval: Configure Delivery Traffic Indication Message (0-255 beacon count)

Monitored Host

Host: IP Address or Hostname that should be reachable for this WLAN to be active

Interval: Duration in seconds (60-3600)

Attempts: Number of attempts to check the reachability of monitored host (0-25)

DNS Logging List: Types server where all client DNS requests will be logged

Connection Logging List: Types server where all client connection requests will be logged

Band Steering: Steer dual-band capable clients towards 5GHz radio

Proxy ARP: Respond to ARP requests automatically on behalf of clients

Proxy ND: Respond to IPv6 ND requests automatically on behalf of clients

Unicast DHCP: Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients

Insert DHCP Option 82: Enable DHCP Option 82

Tunnel Mode: Enable tunneling of WLAN traffic over configured tunnel

Host Backing Protocol: CMC_SSD In

RRM (802.11k): Enable Radio Resource Measurements (802.11k)

3. Click **Save**.

Creating a ePSK WLAN

To create a WLAN, navigate to **Shared Settings > AP Groups and WLANs** (or the WLAN page in the Wireless LAN View) and select **New WLAN**. As with AP Groups, WLANs are separated into cnPilot Home and cnPilot Enterprise types. cnPilot Enterprise WLANs are able to configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters. cnPilot Home WLANs 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-Z0-9_-*&%#@!<>.[\]^~`\$). The user can also rename them if required.
- In cnMaestro X pro user allowed to create 1024 espk per Wlan.
- By default password will not be configured. User has to configure the password for WLAN.

Steps to create WLAN policy:

1. From homepage navigate to **WLANs**.
2. Click **New WLAN**, provide basic parameters to WLAN, and ensure **WPA2 Pre-Shared keys** is enabled in Security drop-down.

Basic Information

Type:

Name:

Scale:

Description:

Basic Settings

Enable

SSID: The SSID of this WLAN (up to 32 characters)

Mode: WPA (WPA2/TKIP/CCMP) mode

VLAN: Default VLAN assigned to clients on this WLAN (0-4094)

Security: Set authentication and encryption type

Radio: Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported

Client Isolation: When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same WLAN

cnMaestro Managed Security: Enable centralized Guest Access Session management of roaming for wireless clients through cnMaestro

Hide SSID: Do not broadcast SSID in beacons

Advanced Settings

Max Clients: Default maximum client assigned to this WLAN (0-255)

VLAN Pruning: Configure VLAN Pruning

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

Inactivity Timeout: Inactivity time in seconds (60 to 3600)

Drop Multicast Traffic: Drop the send/receive of multicast traffic

L2MSD: Enable L2MSD

QoS: Enable QoS load sharing

QoS Interval: Configure Delivery Traffic Indication Message (0-255 beacon count)

Monitored Host

Host: IP Address or hostname that should be reachable for this WLAN to be active

Interval: Duration in seconds (60-3000)

Attempts: Number of attempts to check the reachability of monitored host (0-25)

DNS Logging Host

Port: Port

Server: Routing server where all client DNS requests will be logged

Connection Logging Host

Port: Port

Server: Routing server where all client connection requests will be logged

Roam Steering

Enable: Clear dual-band capable clients towards 5GHz radio

Proxy AP: Respond to AP request automatically on behalf of clients

Proxy ND: Respond to IPv6 ND requests automatically on behalf of clients

Unicast DHCP: Convert DHCP OFFER and DHCP ACK to unicast before forwarding to clients

Invert DHCP Option 82: Enable DHCP Option 82

Tunnel Mode: Enable tunneling of WLAN traffic over configured tunnel

Fast Roaming Protocol: Enable/Disable/Force/No

RRM (802.11k): Enable Radio Resource Measurements (802.11k)

3. Click **Save**.

4. Navigate to **ePSK** tab. Select the **Passphrase Strength** as **Easy** or **Strong** or **Number**.

WLANs > Import_242

Configuration: **ePSK**

Passphrase Strength: Easy Strong Number This allows Alphanumeric and Special Characters (up to 16 Characters)

User Name	MAC Address	Passphrase	Creation Date	VLAN
No Data Available				

Showing 0 - 0 Total: 0 |

5. Click **Add New**. The Add PSK window pops-up where you can select the **Mode** as either **Single** or **Bulk**.

6. In Single Mode **User Name** is mandatory and rest of the entries are optional.

Add PSK
✕

Mode

Single Bulk

User Name *

The number of characters allowed is between 1 and 24

Passphrase

The number of characters allowed is between 8 and 16

MAC Address

XX:XX:XX:XX:XX:XX OF XX-XX-XX-XX-XX-XX

VLAN

VLAN ID should be in between 1 and 4094



NOTE:

Passphrase is optional and it will be automatically generated based on the selected passphrase strength.

6. In **Single** Mode we can see single entry only.

WLANs > Add New
✕

Passphrase Strength:

Easy Strong Number This allows Alphanumeric characters (up to 8 Characters)

User Name	MAC Address	Passphrase	Creation Date	VLAN	
User-1	N/A	dVND10Y	Mon, Jun 17, 2019	N/A	✕

[Add New](#) [Import](#) [Export](#) [Delete](#)

Showing 1 - 1 Total: 1 | 10 | [Previous](#) [Next](#)

7. In **Bulk** Mode, **Count** and **User Name Prefix** are mandatory fields. Enter the **Count** and **User Name Prefix**.

Add PSK ✕

Mode
 Single Bulk

Count*

This allows values between 2 and 1024

User Name Prefix*

Username and Passphrase will be auto generated i.e prefix-1

VLANs

Use comma "," separated VLANs. To provide a range use "-".

Save

8. In **Bulk Mode** we can see many entries.

MLANs ~ |@#%&*(0_Divya

Configuration | APs

Passphrase Strength
 Easy Strong Number This allows Alphanumeric characters (up to 8 Characters)

User Name	MAC Address	Passphrase	Creation Date	VLAN	
D-1	N/A	3#NM3pWFA*Mrv,T	Wed, Oct 16, 2019	1	✕
D-2	N/A	YU14n@GHEJZUS	Wed, Oct 16, 2019	1	✕
D-3	N/A	8*mvfp0upZUZYEJ	Wed, Oct 16, 2019	1	✕
D-4	N/A	ACC65q#JCTwv	Wed, Oct 16, 2019	1	✕
D-5	N/A	DE%4chpm6*KO5>	Wed, Oct 16, 2019	1	✕

Showing 1 - 5 Total: 5 10 1 Previous Next

Save

Import ePSK

1. Click **Import**. A dialogue box appears.
2. Select **import.csv** and import the file.

Add PSK ✕

CSV File
 Import .csv

Import **Cancel** [Download Sample File](#)

3. When you click **Download Sample File**, you can see Sample ePSK excel sheet.

	A	B	C	D	E	F	G	H	I
1	username	mac	passphrase	vlan					
2	Unique na	MAC address of the client,if any (optional)	The Passphrase (Pre Shared Key) to be used in the WPA2 handshake	The VLAN to which the client traffic should be mapped (optional)					
3	Lounge-1	6-46)hj6ab;AB([;	6-46)hj6ab;AB([;	9					
4	Lounge-2	9jdf];qj*38GU53%	9jdf];qj*38GU53%	10					
5	Lounge-3	*{;mQg=UdeM2ErR	*{;mQg=UdeM2ErR	1					
6	Lounge-4]jzam4F1)xJzgg%]jzam4F1)xJzgg%	2					
7									
8									
9									
10									
11									
12									

Export ePSK

1. Click **Export**. A dialogue box appears.
2. Select **export.csv** and export the file.

WLANs > 000111_Portal_Hostname_Oct17

Configuration | APs

Passphrase Strength
 Easy Strong Number This allows Alphanumeric and Special Characters (up to 16 Characters)

Buttons: Add New, Import, **Export**, Delete

User Name	MAC Address	Passphrase	Creation Date	VLAN	
Number-1	N/A	29129397	Thu, Oct 17, 2019	N/A	✕
Number-10	N/A	37619639	Thu, Oct 17, 2019	N/A	✕
Number-100	N/A	99426899	Thu, Oct 17, 2019	N/A	✕
Number-11	N/A	65484534	Thu, Oct 17, 2019	N/A	✕
Number-12	N/A	82132899	Thu, Oct 17, 2019	N/A	✕
Number-13	N/A	82161516	Thu, Oct 17, 2019	N/A	✕
Number-14	N/A	18245656	Thu, Oct 17, 2019	N/A	✕
Number-15	N/A	48344748	Thu, Oct 17, 2019	N/A	✕
Number-16	N/A	75175229	Thu, Oct 17, 2019	N/A	✕
Number-17	N/A	38662187	Thu, Oct 17, 2019	N/A	✕

Showing 1 - 10 Total: 100 | 10 | Previous 1 2 3 4 5 10 Next >

3. When you click **Download Sample File**, you can see Sample ePSK excel sheet.

	A	B	C	D	E	F	G	H	I
1	username	mac	passphrase	vlan					
2	Unique name	MAC address	The Passphrase	The VLAN to which the client traffic should be mapped (optional)					
3	Room-1		WVghr8SmY_a;;Q(e						
4	Room-2		a{n5&HepkI~=Qt%,						
5	Room-3		6q@Qk#WU8JzC.Br)						
6	Room-4		eX~g!n!sjj)tZw[j						
7	Room-5		y\$Cqds{!YAw5gJ;p						
8	Room-6		j;Ag]EBKk8kNRS*c						
9	Room-7		8H(\$F)u;m9C4_MQ=						
10	Room-8		_(hgH7;dzb]Ys~9w						
11	Room-9		7%{C5bqDMpt^()2]						
12	Room-10		3mq=xY~zg&fn!mN%						

Delete ePSK

To delete ePSK, select the ePSK and click **Delete**.

WLANs > |@#5%^&*(0_Divya

Configuration | APs

Passphrase Strength
 Easy Strong Number This allows Alphanumeric and Special Characters (up to 16 Characters)

Buttons: Add New, Import, Export, **Delete**

User Name	MAC Address	Passphrase	Creation Date	VLAN	
<input checked="" type="checkbox"/> D-1	N/A	3*Nm<3pW^A^Mw^T	Wed, Oct 16, 2019	1	✕
<input checked="" type="checkbox"/> D-2	N/A	2UJ]4n@GHE]UUS	Wed, Oct 16, 2019	1	✕
<input checked="" type="checkbox"/> D-3	N/A	@^mVp]OpZuZDREJ	Wed, Oct 16, 2019	1	✕
<input checked="" type="checkbox"/> D-4	N/A	AcC6S]rK]C]Twc	Wed, Oct 16, 2019	1	✕
<input checked="" type="checkbox"/> D-5	N/A	DB;%4chpmR^X9S>	Wed, Oct 16, 2019	1	✕

Showing 1 - 5 Total: 5 | 10 | Previous 1 Next >



NOTE:

- You can group select or individually select ePSK entry and delete the same.
- ePSK feature is supported in cnPilot from System Release 3.11.1 onwards.

Create an AP Group

To create an AP Group, perform the following steps:

1. Navigate to **Configuration > AP Groups and WLANs** page > **AP Group** tab.
2. Click **New AP Group** tab.
3. Enter values of **AP Group name**, **Country name**, and **WLAN** parameters.
4. Click **Add WLAN** and select **WLAN** from the list.
5. Enter the **Administrator** password in the Management tab.
6. Click **Save**.

Map WLANs to AP Groups

WLANs are added to AP Groups in the AP Group configuration. Ensure that the WLANs are ordered correctly if Mesh mode is used.



NOTE:

Maximum of 16 WLAN policies are supported for E-Series and XV-Series devices and 8 WLAN policies are supported for ePMP 1000 Hotspot and Only one WLAN for cnPilot Home AP Group.

Lock cnPilot/cnMatrix device Configuration

This feature supports automatically restoring the configuration of devices to their mapped AP Group if their configuration is changed outside of cnMaestro. When this feature is enabled in cnMaestro, the configurations changed from the UI or CLI of the device are reverted back by pushing the existing AP Group configuration. The configuration will get pushed only if the device is in sync status.

Advanced Features

- Instantaneous Offline Alarm Send offline alarms immediately, instead of waiting 5 minutes. This may generate many false alarms due to slow or unstable connections.
- Lock Wi-Fi AP/cnMatrix device Configuration **X** Overwrite Wi-Fi AP and cnMatrix configuration changes made outside of a mapped AP Group or Switch Group (such as through the Device UI).
- RADIUS Proxy **X** Enable the "Proxy RADIUS through cnMaestro" feature in WLAN policies (configured at Enterprise WLAN Policy > AAA Servers).
- WiFiPerf Daemon **X** Enable Wi-Fi Performance tests between the Wi-Fi AP or CPE and cnMaestro (configured at Wi-Fi Device > Tools > Wi-Fi Performance)

To enable this feature:

1. Navigate to **Administration > Settings > Advanced Features** page.
2. Enable the **Lock cnPilot/cnMatrix device Configuration** check box.
3. Click **Save**.

When a configuration change is made on the device via its UI or CLI, cnMaestro detects the change as **Device's configuration changed outside of cnMaestro** and the device is marked as **Not In Sync**. In this scenario, an Auto-Sync job is triggered automatically by cnMaestro to revert back the changes.

The Auto-Sync job can be viewed in **Administration > Jobs > Configuration Update** page.

ID	Details	Managed Account	Occurrence	Target	Created by	Created on	Completed on	Parallel	Stop on Error	Sector Priority	Status
44	1 cnPilot-200P device(s)	J&M	Now	Default_Hotspot	Administrator	Jan 27, 2021 18:15	Jan 27, 2021 18:15	-	false	N/A	Completed
43	2 device(s)	Base Infrastructure	Now		Auto Sync	Jan 27, 2021 18:07	Jan 27, 2021 18:07	15	false	N/A	Completed
42	1 XV3 8 device(s)	Base Infrastructure	Now	Hotspot_2430g	Administrator	Jan 22, 2021 16:52	Jan 22, 2021 16:53	-	false	N/A	Completed
41	1 device(s)	Base Infrastructure	Now		Auto Sync	Jan 22, 2021 16:52	Jan 22, 2021 16:52	15	false	N/A	Completed
40	1 XV3 8 device(s)	Base Infrastructure	Now	Hotspot_2430g	Administrator	Jan 22, 2021 16:46	Jan 22, 2021 16:46	-	false	N/A	Completed
39	1 XV3 8 device(s)	Base Infrastructure	Now	Hotspot_2430g	Administrator	Jan 22, 2021 16:42	Jan 22, 2021 16:42	-	false	N/A	Completed
38	1 XV3 8 device(s)	Base Infrastructure	Now	Hotspot_2430g	Administrator	Jan 22, 2021 16:41	Jan 22, 2021 16:42	-	false	N/A	Completed
37	1 device(s)	Base Infrastructure	Now		Auto Sync	Jan 22, 2021 16:40	Jan 22, 2021 16:41	15	false	N/A	Completed
36	1 XV3 8 device(s)	Base Infrastructure	Now	Hotspot_2430g	Administrator	Jan 22, 2021 16:38	Jan 22, 2021 16:39	-	false	N/A	Completed
35	1 device(s)	Base Infrastructure	Now		Auto Sync	Jan 22, 2021 16:34	Jan 22, 2021 16:34	15	false	N/A	Completed

Retry Configure

When the user tries to apply any AP Group on the device and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as "Device was offline", in the **Jobs** page. In this case, when device comes up and connects to cnMaestro, then cnMaestro will create an Auto-sync job for that device and pushes the AP group. (It will not apply the AP group if the **Auto-Sync** was disabled in the AP group).



NOTE:

The config update (Auto-Sync) will happen only when the "Auto-Sync" option was enabled in the AP 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.

AP Groups > Add New

Basic Information

Type: cnPilot Home (R-Series)

Name*: ewew

Scope: Shared

Auto Sync: Automatically push configuration changes to devices sharing this AP Group

Country*: NONE (For appropriate regulatory configuration)

Description:

Order	WLAN	Delete
No WLAN selected		

[Add WLAN](#) [Create WLAN](#)

Default password: **admin** of cnPilot R-series should be changed before upgrading to the build 4.6-RX.

AP Groups > Add New

Administrator Access

User Type: Admin User (Choose the user type from admin user and normal user and basic user)

New User Name: admin

New Password: [masked] (Configure password for authentication of GUI and CLI sessions (max 25 characters))

Once after the upgradation of build 4.6-RX, default password; **admin** becomes invalid and password needs to be reset through the WAN.



NOTE:

Default User Name: **admin** can be used after the upgradation.

Import/Export of AP Groups and WLANs

The AP Groups and WLANs are created for cnPilot Home and Enterprise devices. The configurations created for each AP Groups and WLANs in a server can be exported and imported to different servers. This will help the users reduce the effort of manually creating the WLAN and AP Group each time.

Shared Settings > AP Groups and WLANs

AP Groups **WLANs**

Search [] Device Type: All Scope: All Accounts

Name	Scope	Type	AP Status	Clients Now	Clients 24 HR	Throughput (DL/UL)			
2Access	Basic Infrastructure	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps			
Default Enterprise	Any	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps			
Permanent_Scale_Client	Basic Infrastructure	Enterprise Wi-Fi	0 of 1 offline	0	0	0 Kbps / 0 Kbps			
SSIDs_1	Shared	cnPilot Home (R Series)	3 of 3 offline	0	0	0 Kbps / 0 Kbps			
WLAN_200_05	Shared	cnPilot Home (R Series)	0 of 0 offline	0	0	0 Kbps / 0 Kbps			
WLAN_200_08	Basic Infrastructure	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps			
WLAN_200_09	Shared	Enterprise Wi-Fi	1 of 1 offline	0	0	0 Kbps / 0 Kbps			
WLAN_200_10	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps			
WLAN_200_15	Shared	Enterprise Wi-Fi	2 of 2 offline	0	0	0 Kbps / 0 Kbps			
WLAN_200_18	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps			

Showing 1 - 10 Total 16

Shared Settings > AP Groups and WLANs

AP Groups **WLANs**


Search [] Device Type: All Scope: All Accounts **WLAN** All

Name	Type	AP Status	Scope	Clients Now	Clients 24 HR	Throughput (DL/UL)	WLANs	Auto Sync			
2Access	Enterprise Wi-Fi	0 of 0 offline	Basic Infrastructure	0	0	0 Kbps / 0 Kbps	2Access	ON			
Permanent_Scale_Client_15_20	Enterprise Wi-Fi	0 of 1 offline	Basic Infrastructure	0	0	0 Kbps / 0 Kbps	Permanent_Scale_Client	ON			
Test987	cnPilot Home (R Series)	0 of 1 offline	Basic Infrastructure	0	0	0 Kbps / 0 Kbps	Default Home	OFF			
SSIDs_1	cnPilot Home (R Series)	3 of 3 offline	Shared	0	0	0 Kbps / 0 Kbps	SSIDs_1	ON			
WLAN_200_05	cnPilot Home (R Series)	0 of 0 offline	Shared	0	0	0 Kbps / 0 Kbps	WLAN_200_05	ON			
WLAN_200_08	Enterprise Wi-Fi	0 of 0 offline	Basic Infrastructure	0	0	0 Kbps / 0 Kbps	WLAN_200_08	ON			
WLAN_200_09	Enterprise Wi-Fi	1 of 1 offline	Basic Infrastructure	0	0	0 Kbps / 0 Kbps	WLAN_200_09	ON			
WLAN_200_10	Enterprise Wi-Fi	0 of 0 offline	Shared	0	0	0 Kbps / 0 Kbps	WLAN_200_10	ON			
WLAN_200_15	Enterprise Wi-Fi	2 of 2 offline	Shared	0	0	0 Kbps / 0 Kbps	WLAN_200_15	ON			
WLAN_200_18	Enterprise Wi-Fi	1 of 1 offline	Shared	0	0	0 Kbps / 0 Kbps	WLAN_200_18	ON			

Showing 1 - 10 Total 17

To export WLAN and AP Group,

1. Navigate to **Shared Settings > AP Groups and WLANs page > WLAN or AP Group** tab (according to the choice).
2. Click **Export**.



NOTE:

- The AP Groups and WLANs should be exported separately as the associated WLANs are not exported while exporting an AP Group.
- The AP Groups and WLANs will be exported with proper name and time stamp.

To import WLAN and AP Group,

1. Navigate to **Shared Settings > AP Groups and WLANs page > WLAN or AP Group** tab (according to the choice).
2. Click **Import WLAN**.

Import WLAN ✕

Name*

Scope
 Shared

Configuration file Import .json

Import

3. Enter the **Name**.
4. Select the **Configuration file** in Json format.
5. Click **Import**.



NOTE:

- To import an AP Group, ensure that all the associated WLANs in that AP Group are already imported. If the WLAN associated with the AP Group is unavailable, an error message will be displayed during AP Group import.
- If the name is not provided for WLAN or AP Group while importing, it will take the name of the file that is to be imported, automatically.
- If the name provided for the AP Group/WLAN while importing matches with the existing list of WLAN or AP Group in the system, an error " **The specified policy name already exists**" will be displayed.
- Importing WLAN and AP group type R-series are not allowed in Wi-Fi mode.

Create a Configuration Job

Configuration job can be created from **Monitor and Manage > System > Configuration**. Select a device type and a set of devices along with AP groups to which they will be mapped. This can be done in three steps:

The screenshot shows the 'System Configuration' page. The 'Device Type' is set to 'ePMP (Sector)'. The 'Managed Account' is 'All Accounts'. A search bar is present above a table of devices. Two devices are selected: 'F400_2003a7' and 'yinosdome-1234567890123456789012'. The table columns include Device, Selected SMs, Managed Account, Status, and Network. Below the table, there are options for 'Update' (Now or Schedule), 'Job Options' (Stop update on critical error, Within a sector, update), and 'Notes'. A 'Global PMP/ePMP/cnVision/cnReach Configuration Backup' section is also visible.

1. Select the **AP Group**.
2. Select the list of Wi-Fi Devices.
3. Click **Apply Configuration**.

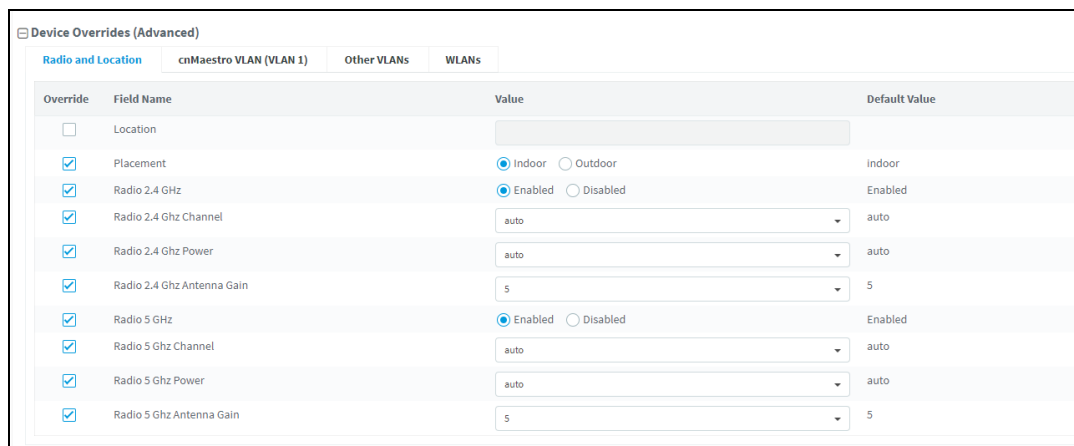
The screenshot shows the 'System Configuration' page with a list of devices. The 'Device Type' is 'cnPilot Home (R-Series)'. The 'Managed Account' is 'All Accounts'. The table columns include Device, Managed Account, AP Group, Status, Sync Status, Network, and Tower/Site. The table lists various devices like '190V_Test', 'Cambium-123', 'cnP_Home_Bryn_05_91', etc., with their respective AP Groups and Sync Status.

Pre-Defined Overrides

Some device configuration is generally specific to an individual device, and hence not easily shared through an AP Group. This includes IP Address, Radio Channel Settings, and WLAN details such as SSID, Enabling/Disabling SSID, Enabling/Disabling Radio 2.4 GHz and 5 GHz, and Passphrase. These items can be configured in the device Configuration tab, navigate to **Manage > Configuration** and select a device in the tree to update.

You can 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.

By default, Enterprise Wi-Fi devices will 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.



Override	Field Name	Value	Default Value
<input type="checkbox"/>	Location		
<input checked="" type="checkbox"/>	Placement	<input checked="" type="radio"/> Indoor <input type="radio"/> Outdoor	Indoor
<input checked="" type="checkbox"/>	Radio 2.4 GHz	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Enabled
<input checked="" type="checkbox"/>	Radio 2.4 GHz Channel	auto	auto
<input checked="" type="checkbox"/>	Radio 2.4 GHz Power	auto	auto
<input checked="" type="checkbox"/>	Radio 2.4 GHz Antenna Gain	5	5
<input checked="" type="checkbox"/>	Radio 5 GHz	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Enabled
<input checked="" type="checkbox"/>	Radio 5 GHz Channel	auto	auto
<input checked="" type="checkbox"/>	Radio 5 GHz Power	auto	auto
<input checked="" type="checkbox"/>	Radio 5 GHz Antenna Gain	5	5

User-Defined Overrides

User-Defined Overrides can be entered into the end of an AP Group configuration. They will be merged into or appended to the AP Groups before the configuration is applied to the device. This allows setting configuration parameters which are not supported by GUI, and they are considered as advanced operation that should rarely be used. The format of the commands would be same as with the device CLI.

For example, if a new version of the software had a feature unsupported in cnMaestro, it could be pushed to the device using CLI commands through the User-Defined Override mechanism

This can be explained with the following example, in which country-code and hostname are appended to the end of the configuration, and will override any settings in the UI

```
country-code IN
hostname Wi-Fi_Device
```

User-Defined Variables

Override configuration also supports a programmatic concept called user-defined variables (which are also used with Fixed Wireless 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 the 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 they automatically take values provided by the device itself.

- `%{ESN}` will be replaced with the MAC address of devices.
- `%{MSN}` will be replaced with the Serial Number of devices.

Bulk Overrides

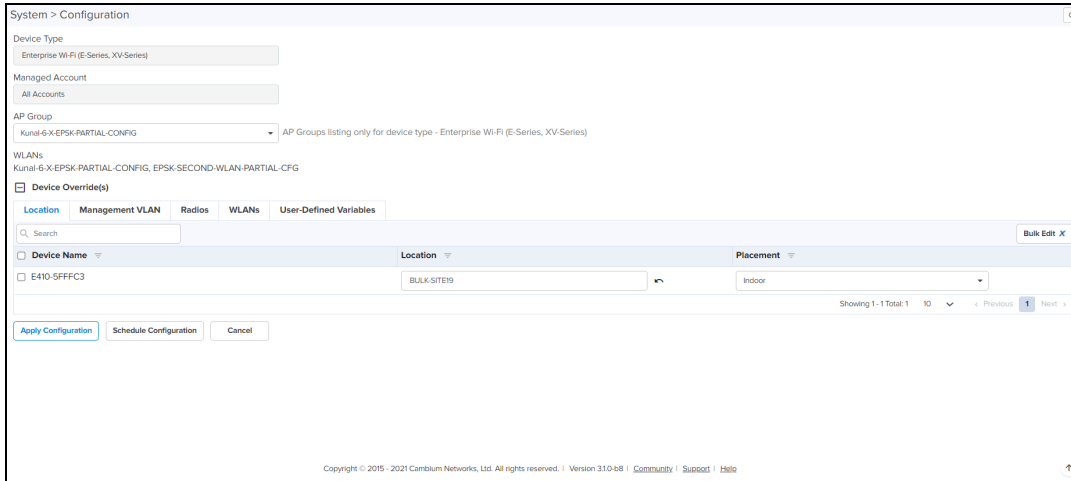
Bulk Overrides allows the user to edit the multiple configurations shared through an AP Group for one or more devices.

**NOTE:**

Bulk Edit option under **Configuration > Devices Overrides** is supported only for cnMaestro X.

The user can override for the following configurations:

- Location
- Management VLAN
- Radios
- WLANs
- User-Defined Variables

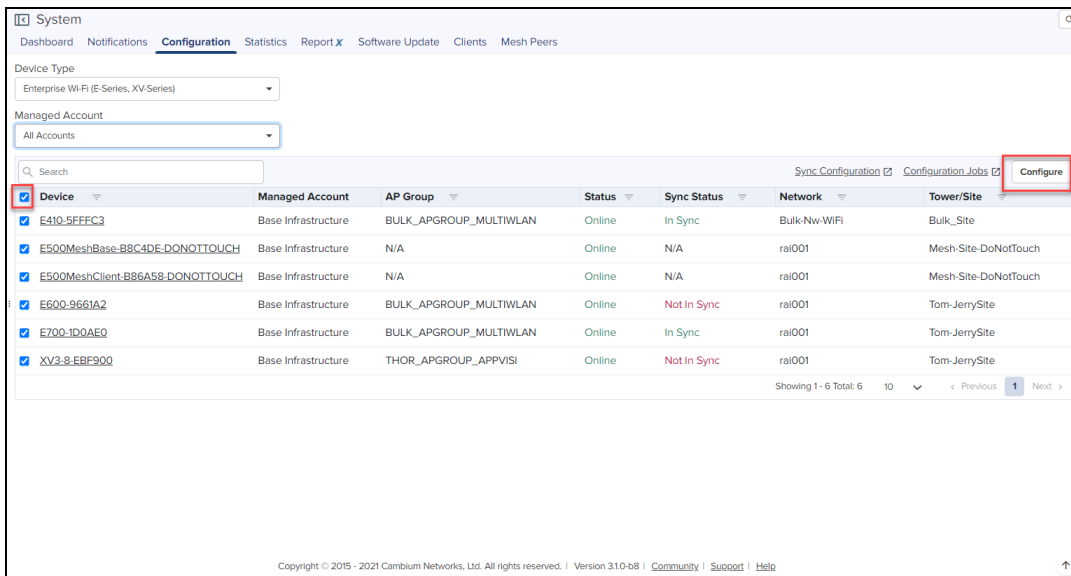


Perform the following steps to configure Bulk Overrides for the devices.

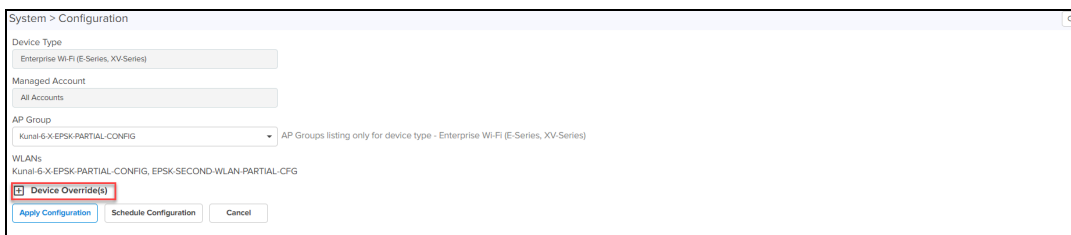
NOTE:

Configuration tab will be available from other container levels like Network/Site and also from AP group level..

1. Navigate to **Manage > System > Configuration**.
2. Select the **Device Type** from the drop-down.
3. Select **Device** from the list and click **Configure**.

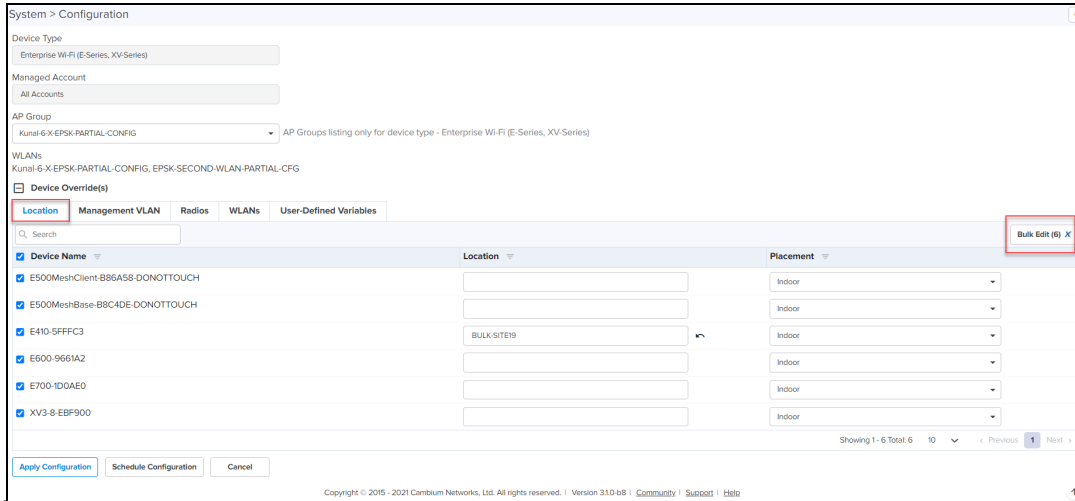


The bulk device configuration is displayed as shown below. Click (+) next to **Device Override(s)** to view the list of devices.

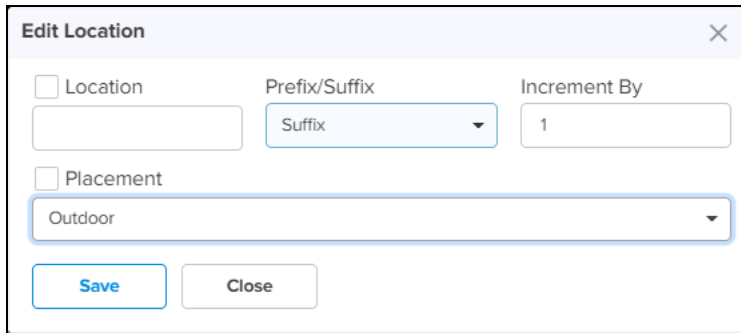


Location

1. In **Location** tab, select the devices from the list.
2. Click **Bulk Edit**. **Edit Location** window appears.

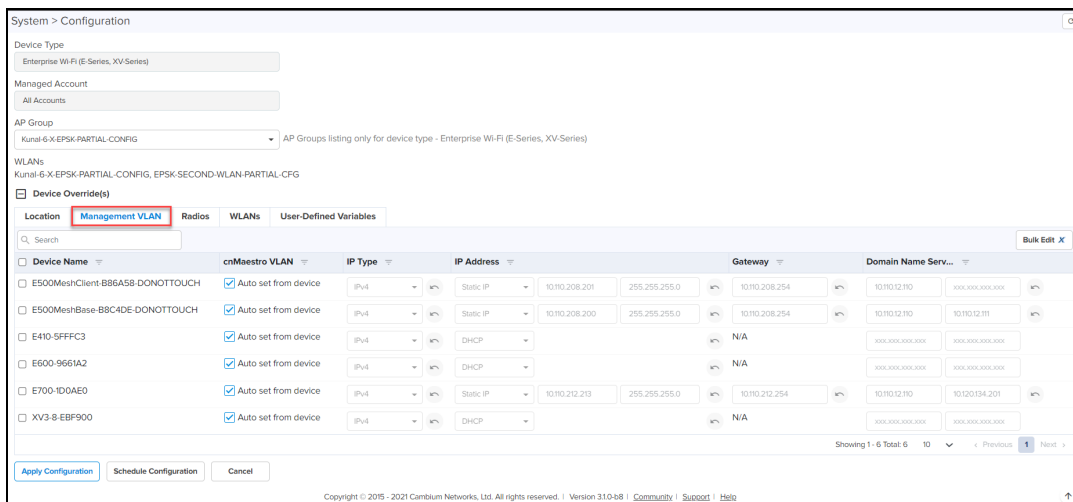


3. Edit the configuration details and click **Save**.



Management VLAN

1. In **Management VLAN** tab, select the **VLAN** of the device from the list.



2. Click **Bulk Edit**. **Edit Management VLAN** window appears

System > Configuration

Device Type
Enterprise Wi-Fi (E-Series, XV-Series)

Managed Account
All Accounts

AP Group
Kunal-6-X-EPSK-PARTIAL-CONFIG

WLANs
Kunal-6-X-EPSK-PARTIAL-CONFIG, EPSK-SECOND-WLAN-PARTIAL-CFG

Device Override(s)

Location Management VLAN Radios WLANs User-Defined Variables

Search

Device Name Bulk Edit (6) X

Device Name	cnMaestro VLAN	IP Type	IP Address	Gateway	Domain Name Serv...
<input checked="" type="checkbox"/> E500MeshClient-B86A58-DONOTTOUCH	<input checked="" type="checkbox"/> Auto set from device	IPv4	Static IP 10.110.208.201	255.255.255.0 10.110.208.254	10.110.12.110 800.000.000.000
<input checked="" type="checkbox"/> E500MeshBase-B8C4DE-DONOTTOUCH	<input checked="" type="checkbox"/> Auto set from device	IPv4	Static IP 10.110.208.200	255.255.255.0 10.110.208.254	10.110.12.110 10.110.12.111
<input checked="" type="checkbox"/> E410-5FFFC3	<input checked="" type="checkbox"/> Auto set from device	IPv4	DHCP	N/A	800.000.000.000 800.000.000.000
<input checked="" type="checkbox"/> E600-9661A2	<input checked="" type="checkbox"/> Auto set from device	IPv4	DHCP	N/A	800.000.000.000 800.000.000.000
<input checked="" type="checkbox"/> E700-ID0AE0	<input checked="" type="checkbox"/> Auto set from device	IPv4	Static IP 10.110.212.213	255.255.255.0 10.110.212.254	10.110.12.110 10.120134.201
<input checked="" type="checkbox"/> XV3-8-EBF900	<input checked="" type="checkbox"/> Auto set from device	IPv4	DHCP	N/A	800.000.000.000 800.000.000.000

Showing 1 - 6 Total: 6 10 < Previous 1 Next >

Apply Configuration Schedule Configuration Cancel

Copyright © 2015 - 2021 Cambium Networks, Ltd. All rights reserved. | Version 3.10-b8 | Community | Support | Help

3. Edit the changes and click **Save**.

Edit Management VLAN X

Auto set from device

Type
IPv4

IP Mode
DHCP

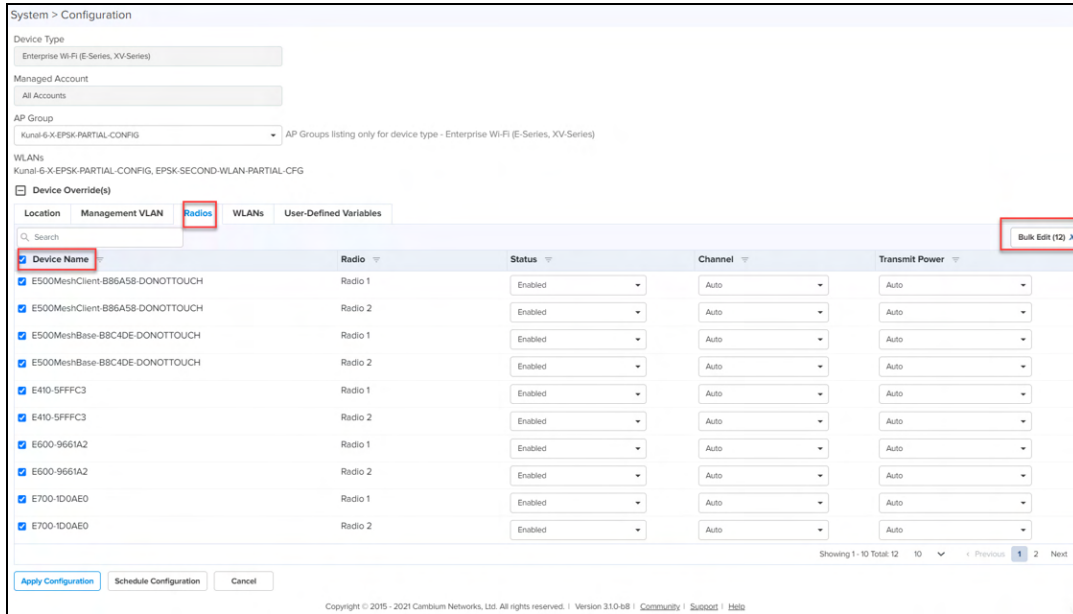
DNS1
xxx.xxx.xxx.xxx

DNS2
xxx.xxx.xxx.xxx

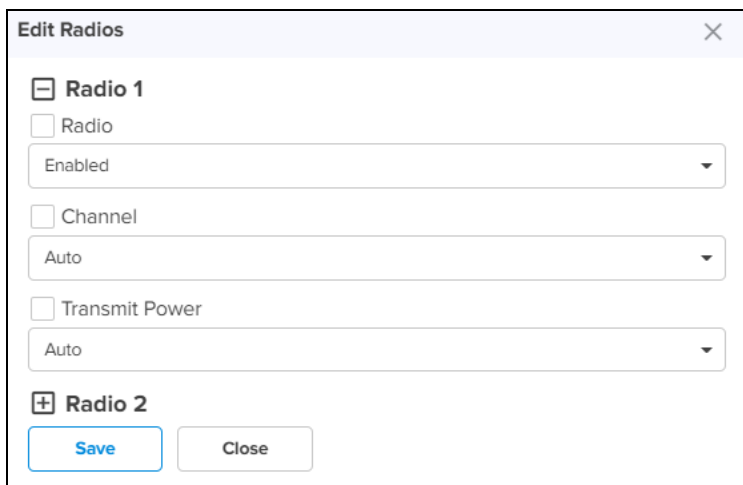
Save Close

Radios

1. In **Radio** tab, select the radios from the device list.

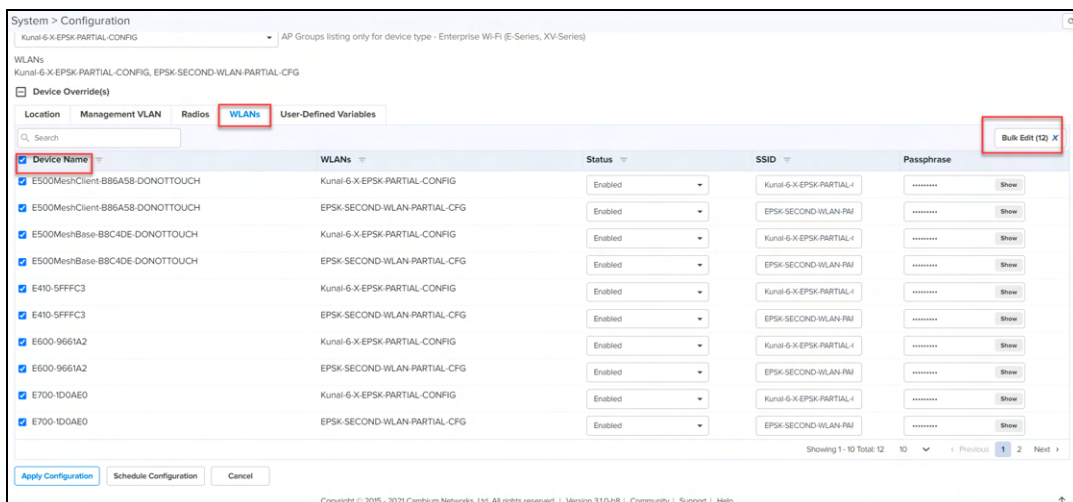


2. Click **Bulk Edit**. **Edit Radios** window appears.
3. Edit the configuration details and click **Save**.



WLANs

1. In **WLANs** tab, select the WLAN of the devices from the list.



2. Click **Bulk Edit. Edit WLANs** window appears.
3. Edit the configuration details and click **Save**.

User-Defined Variables

1. In **User-Defined Variables** tab, select the devices from the list.

Device Name	logging_level	syslog_host_ip
XV3-8-EBF900	2	1111
E500MeshClient-B86A58-DONOTTOUCH	2	1111
E500MeshBase-B8C4DE-DONOTTOUCH	2	1111
E410-5FFFC3	5	5.79.0
E600-9661A2	2	1111
E700-1D0AEO	2	1111

2. Click **Bulk Edit. Edit User Defined Variables** window appears.

3. Edit the configuration details and click **Save**.



NOTE:

For Bulk overrides to enable in **User Defined Overrides** tab, user has to define overrides in User Defined Overrides section of AP groups. For more details, refer to [User-Defined Overrides](#)

- 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 found in the AP Group configuration.

- 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).
- cnPilot Home AP Groups** by default synchronize manually. Updates to them (or the WLANs to which they map) need manual synchronization to push configuration to the devices.

Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately. Navigate to **Administration > Sync Configuration**.

Sync Configuration only displays devices currently out-of-sync with a mapped AP Group .

Sync Configuration has the following fields:

- AP Group (AP Group to which device is mapped)
- Device (Hostname)
- Device Type
- Network (Network in which device is present)
- Status (Up/Down)
- Site (Site under which device is present)
- Sync Status (Sync status will tell whether job is completed or failed)

Steps to do Sync Configuration:

- Click the **Sync Configuration** in the top right of the **Configuration > WLAN and AP Groups** or **Manage > Configuration > Device Details** or **Jobs** tab.
- Select devices you wish to synchronize.

Device	Type	Status	Managed Account	Network	Site	AP Group/Switch Group	Sync Status
EX020-ETSC80-000000	cnMaestro EX200	Offline	Base Infrastructure	Durga	cnMaestro	6-1-2021	Not in Sync: Configuration failed: Device was offline
EX020B-ET0940	cnMaestro EX200B P	Offline	Base Infrastructure	Durga	cnMaestro	6-1-2021	Not in Sync: Configuration failed: Device was offline
cnPilot-R900V-01	cnPilot r900v	Offline	J59M8	default	Default Home	default	Not in Sync: Device's configuration changed outside of cnMaestro
cnPilotR200P	cnPilot r200P	Offline	J59M8	default	Default Home	default	Not in Sync: Device's configuration changed outside of cnMaestro
cnPilot-R200P-M0889	cnPilot r200P	Offline	J59M8	default	Default Home	default	Not in Sync: Device's configuration changed outside of cnMaestro
200P	cnPilot r200P	Offline	J59M8	default	Default Home	default	Not in Sync: Device's configuration changed outside of cnMaestro
cnPilotR200P-442-adv-1886	cnPilot r200P	Offline	J59M8	default	Default Home	default	Not in Sync: Device's configuration changed outside of cnMaestro
R90V-Test	cnPilot r900v	Offline	J59M8	default	Default Home	default	Not in Sync: Device's configuration changed outside of cnMaestro
cnPilot-R900V-ES-23	cnPilot r900v	Offline	J59M8	default	Default Home	default	Not in Sync: Device's configuration changed outside of cnMaestro
cnPilot-r200P-080123	cnPilot r200P	Offline	J59M8	default	Default Home	default	Not in Sync: Device's configuration changed outside of cnMaestro

- Click **Sync Now**.



NOTE:

Sync configuration can only be used if a AP Group is already mapped to the device. Software update jobs can be scheduled in parallel irrespective of other running Jobs as PRO account supports Parallel Jobs also If same devcie is used for config/ software job at a time only one operation will be done as the Job locks the device until it finishes.

Configuration Job Status

After applying configuration, navigate to **Administration > Jobs** to view configuration jobs (for Wireless LAN devices). When configuration is pushed from Sync Configuration, a Configuration job will be created in the background.

ID	Details	Managed Account	Occurrence	Target	Created by	Created on	Completed on	Parallel	Stop on Error	Sector Priority	Status
44	1 cnMaestro (200P device(s))	JSMIS	Now	Default Hosts	Administrator	Jan 27, 2021 18:15	Jan 27, 2021 18:15	-	false	N/A	Completed
43	2 device(s)	Base Infrastructure	Now		Auto Sync	Jan 27, 2021 18:07	Jan 27, 2021 18:07	15	false	N/A	Completed
42	1 XV3 8 device(s)	Base Infrastructure	Now	impost_24200	Administrator	Jan 22, 2021 16:52	Jan 22, 2021 16:53	-	false	N/A	Completed
41	1 device(s)	Base Infrastructure	Now		Auto Sync	Jan 22, 2021 16:52	Jan 22, 2021 16:52	15	false	N/A	Completed
40	1 XV3 8 device(s)	Base Infrastructure	Now	impost_24200	Administrator	Jan 22, 2021 16:46	Jan 22, 2021 16:46	-	false	N/A	Completed
39	1 XV3 8 device(s)	Base Infrastructure	Now	impost_242_apt	Administrator	Jan 22, 2021 16:42	Jan 22, 2021 16:42	-	false	N/A	Completed
38	1 XV3 8 device(s)	Base Infrastructure	Now	TruOC_Ap	Administrator	Jan 22, 2021 16:41	Jan 22, 2021 16:42	-	false	N/A	Completed
37	1 device(s)	Base Infrastructure	Now		Auto Sync	Jan 22, 2021 16:40	Jan 22, 2021 16:41	15	false	N/A	Completed
36	1 XV3 8 device(s)	Base Infrastructure	Now	impost_242_apt	Administrator	Jan 22, 2021 16:38	Jan 22, 2021 16:39	-	false	N/A	Completed
35	1 device(s)	Base Infrastructure	Now		Auto Sync	Jan 22, 2021 16:34	Jan 22, 2021 16:34	15	false	N/A	Completed



NOTE:

1. Configuration jobs will skip devices which are offline. With manual synchronization, they need to be synchronized by the administrator.

For more information on Wi-Fi AP configuration, refer 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](#)

2. cnMaestro X account user can run any number of jobs in parallel.

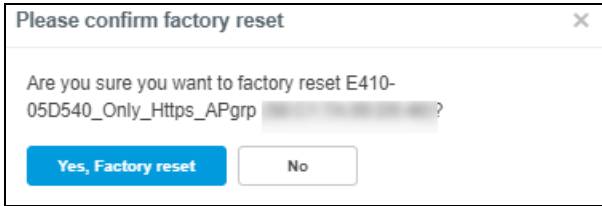
Factory Reset

A factory reset erases all the data on the device. Factory reset is supported for two device models, Enterprise Wi-Fi with greater than 3.10-R6 version and cnMatrix with greater than 4.0 version.

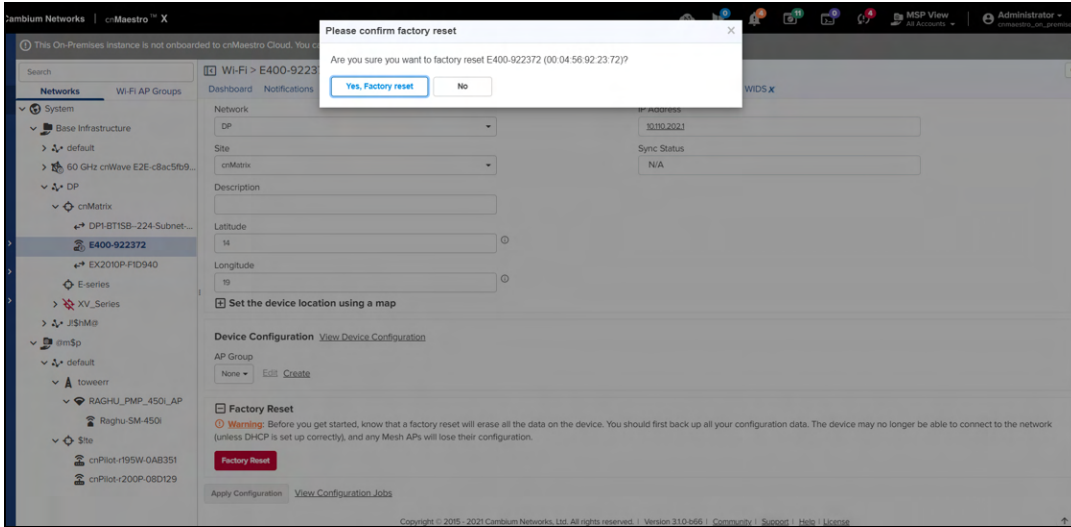
To factory reset the device from cnMaestro:

1. Navigate to the **Configuration** tab of the device.
2. Select **Factory Reset**.

3. Click **Factory Reset**.



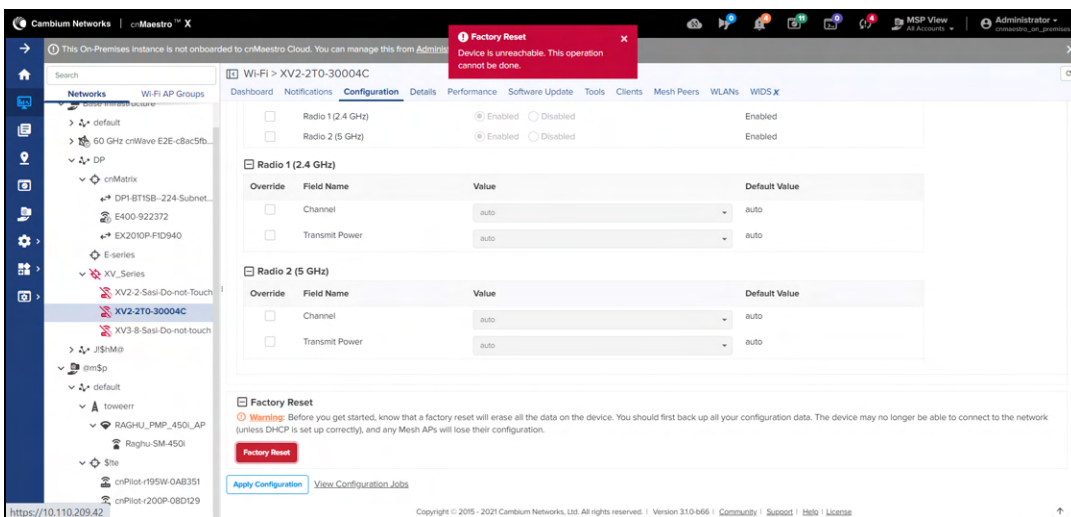
The following window pops-up if you click **Yes, Factory reset** option.



Once the Factory Reset is successful, the following message is displayed in the **Notifications** tab.

Severity	Device Type	Device	Managed Account	IPv4/IPv6 Address	Category	Message	Raised Time
Major	cnPilot e600	E600-665E26	MSP-Account-User	10.110.224.35	STATUS	Device is offline View Details	Wed Apr 17 2019 14:33:08 GMT+0530
Notify	cnPilot e600	E600-665E26	MSP-Account-User	10.110.224.35	SYSTEM_CONFIG_DEFAULTED	System configuration was reset to default: View Details	Wed Apr 17 2019 14:33:07 GMT+0530

If the user does Factory Reset on an offline device it displays 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 MAC association list on the controller.

Overview

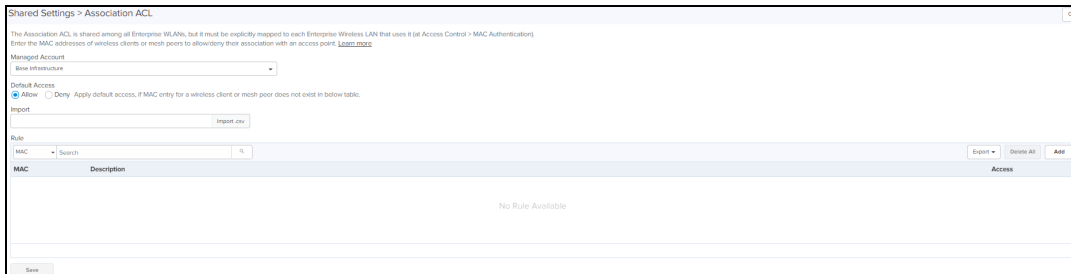
When a client requests to get connected to an AP,

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.

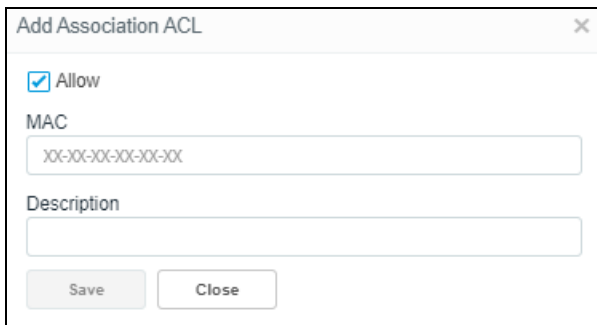
Configuring Association ACL

To configure the Access Control List (ACL) in cnMaestro:

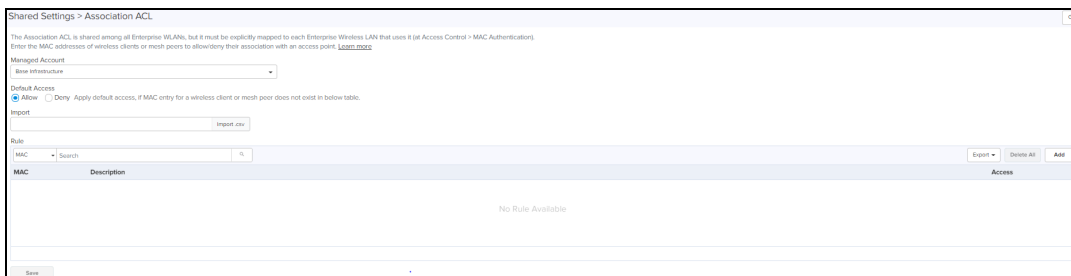
1. Navigate to **Shared Settings > Association ACL** page.
2. Click **Add**.



3. Enter the **MAC**.
4. Click the **Allow** check box.
5. Enter the **Description**.
6. Click **Save**.

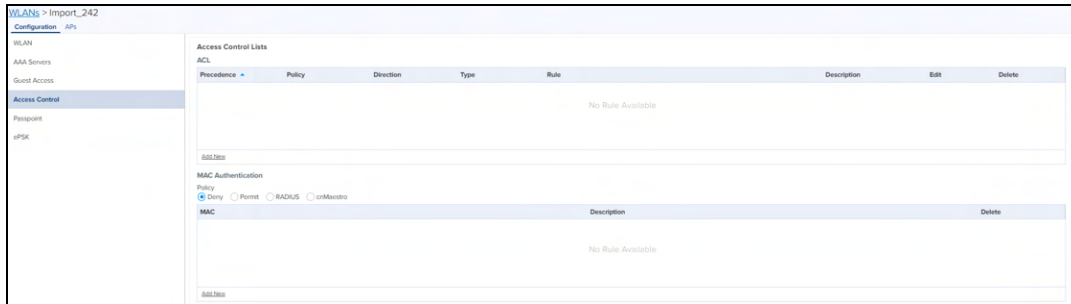


4. Once the MAC is successfully configured, a pop-up **Association ACL default action** is saved successfully is displayed and lists the configured MAC in **Shared Settings > Association ACL** tab.



5. 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/deny), the default action will be applied.
- To **edit/delete** Association ACL, click the respective icons.
- You can import Association ACL, by clicking **Import.csv** and export using the **Export**.

cnMatrix Switches

cnMatrix switches simplify the network deployment and operation. cnMaestro provides management, configuration and control, and security services for cnMatrix with deployment options such as policy-based automation (PBA) to streamline core operations and improve network security. Central to cnMaestro’s orchestration of cnMatrix devices is the concept of Switch Groups.

Switch Groups Configuration

A Switch Group can also be considered a Virtual Stack. The Switch Group functionality enables the users to manage multiple switches with the same configurations.

Configuration is common to all switches belonging to a Switch Group:

- Configuration changes are synchronized and applied for all the switches in a Switch Group.
- A subset of configuration attributes can be overruled for an individual switch.
- Switch ports across all physical switches are associated with a Switch Group and can be simultaneously bulk edited.

From the Switch Groups tab, the administrator can navigate to the Switches and the Switch Ports tabs for configuration. The Dashboard tab is used to monitor the health condition of the virtual stack.

The process for creating a new Switch Group configuration is as follows:

1. Navigate to **Shared Settings > Switch Groups**.
2. Click **New Switch Group**.



**NOTE:**

To Edit the Configuration of existing Switch group, click **Edit** icon > navigates to **Configuration** page.

3. Configure the following tab parameters to create a Switch groups:

- Basic
- Management
- Network
- Security
- User-Defined Overrides

**NOTE:**

- Click **Show Advanced** to view the advanced options of the Switch Groups.
- Click **Save** on individual tab parameters or click once after entering all the four tab parameters.

Basic

The Basic tab provides options to the user to configure the device name as well as other standard values used to identify a switch.

1. Navigate to **Configuration > Switch Groups > Basic**.
2. On the **Basic** page enter device identification data such as:
 - Name
 - Scope
 - Contact
 - Description
 - WISP Configuration

**Note:**

The special characters can be used to create names of Switch Groups (Eg: a-zA-Z_-*&%#@!<>.[() []^~`\$1234567890).

Switch Groups > Add New

Basic

Management
Network
Security
User Defined Overrides

Show Advanced

Basic Information

Name*

Scope Shared Scope means the Switch Group is accessible to all Managed Accounts

Auto Sync Automatically push configuration changes to devices sharing this Switch Group. Note: Lock Wi-Fi AP/cnMatrix device Configuration checkbox should be enabled at Administration > Settings - Advanced Features section

Contact Contact information for the device (max 64 characters)

Description

WISP Configuration

PoE Auto-Detect - cnMedusa

Cambium Sync

Antenna Administration Status

cnPulse Administration Status

cnPulse Power

Save

3. Click **Save**.

Management

1. Navigate to **Management** page.
2. Enable the **Daylight Saving Time** and enter the details.

Administrator Access

Telnet
 HTTP

Change your passwords, do not use default passwords!

Username	Password	Privilege
admin	<small>Set new password</small>	Root
guest	<small>Set new password</small>	Guest

Add New Showing 1 - 2 Total: 2 10 Previous 1 Next

Time Settings

SNTP Server Address Name or IP Address of Network Time Protocol Server

Time Zone

Daylight Saving Time
 Disabled Enabled

Start Week of Month

Start Day of Week

Start Month

Start Hour of Day

Stop Week of Month

Stop Day of Week

Stop Month

Stop Hour of Day

DNS

DNS Server 1

DNS Server 2

SNMP

Enable Controls SNMP support on the device

SNMPv2c RO Community SNMPv2c read-only community string (max 32 characters)

SNMPv2c RW Community SNMPv2c read-write community string (max 32 characters)

Trap Receiver IP SNMP trap server IPv4 address

SNMPv3 Username SNMPv3 user name (max 32 characters)

SNMPv3 Authentication Key Show SNMPv3 Authentication Key (0, 8 to max 32 characters)

SNMPv3 Privacy Key Show SNMPv3 Privacy Key (0, 8 to max 32 characters)

Access
 Read Only Read Write

Authentication

Encryption

Event Logging

Minimum Syslog Level

Server Address Port

Save

Copyright © 2015 - 2021 Cambium Networks, Ltd. All rights reserved. | Version 3.10-r2 | [Community](#) | [Support](#) | [Help](#)

3. Click **Add New** to add **Administrator Access**, enter the details and click **Add**.

Administrator Access ✕

Username*

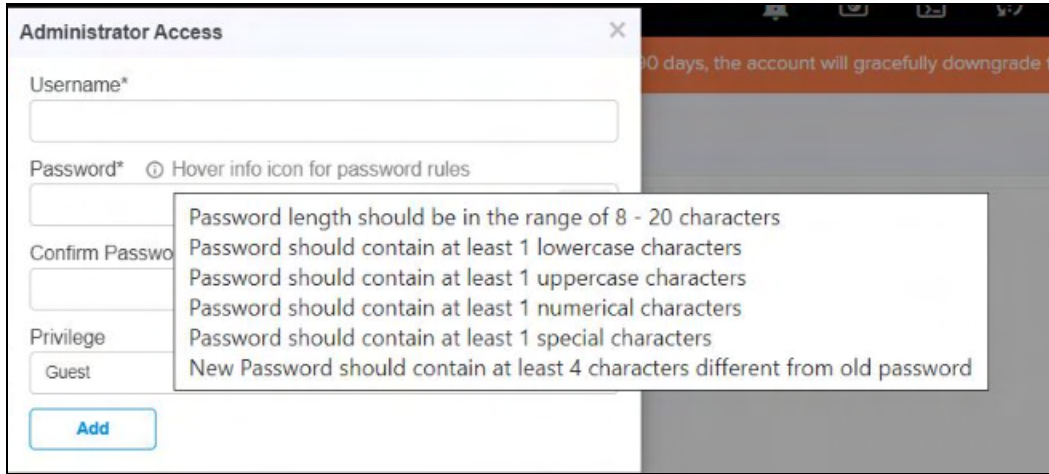
Password* Hover info icon for password rules Show

Confirm Password* Show

Privilege

Add

4. Password should match the special characters as shown below:

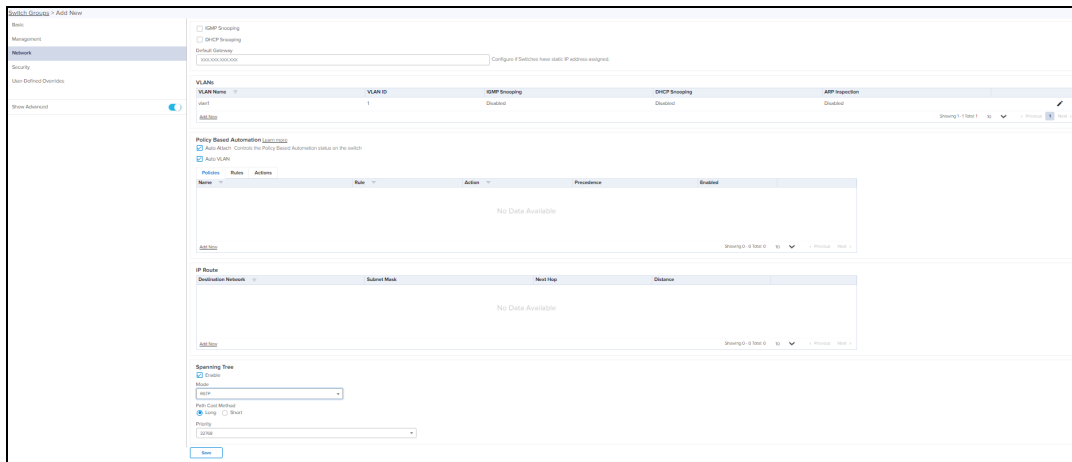


5. Click **Save**.

Network

The **Network** page allows the user to configure VLANs, PBA, IP Route, and Spanning Tree details.

1. Navigate to **Network**, enter the details of VLANs, Policy Based Automation, IP route, and Spanning Tree.

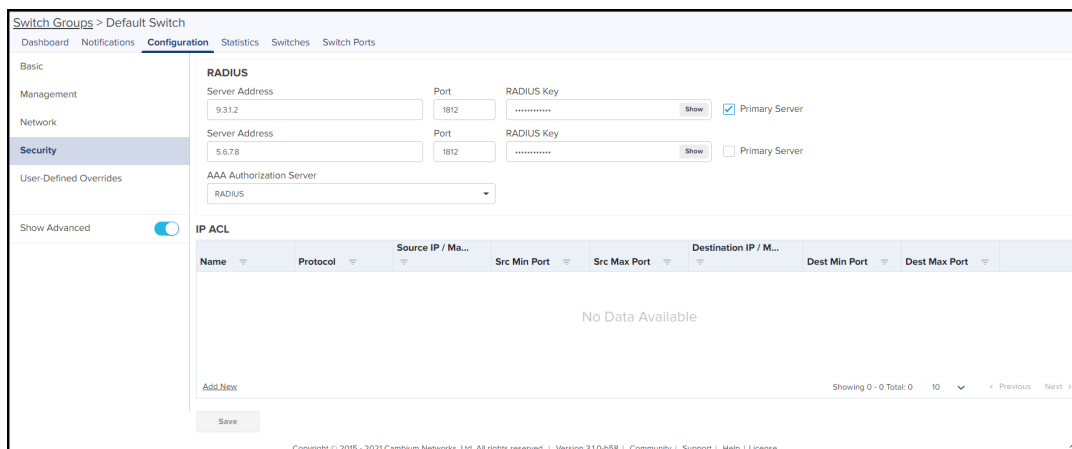


2. Click **Save**.

Security


The Security page allows the user to configure RADIUS and Access Control List (ACL) details.

1. Navigate to **Security** page and enter the details of **RADIUS** and **ACL IP**.



- Click **Save**.

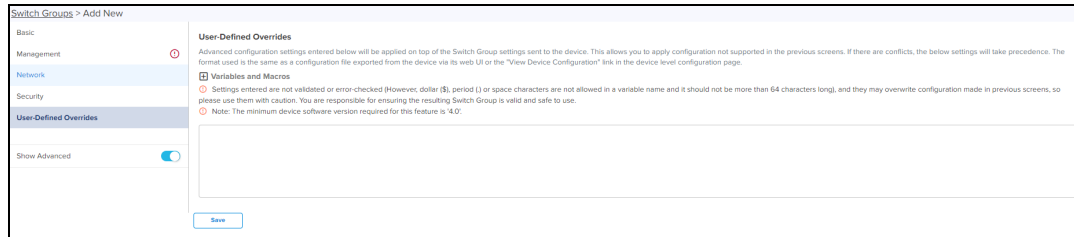
User-Defined Overrides



NOTE:

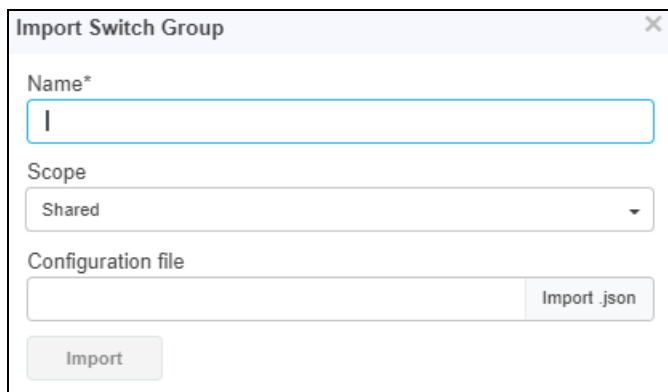
The minimum device software version required for this feature is 4.0.

User-Defined Overrides allows you to apply configuration in cnMatrix switches. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.



Import Switch Group

- Click **Import Switch Group**. A dialogue box appears.
- Select **import.json** and import the file.



- When you click **Download Sample File**, you can see Sample excel sheet.
- Click **Import**

Delete Switch Group

To delete Switch Group from the list click **Delete** icon of the specific device row.



Name	Offline Switches	Scope	Ports Up	VLANs	Active PoE Ports	Auto Sync	Last Edited
8-2-2021	0 of 0	Base Infrastructure	0 of 0	1	0	Off	Feb 08 2021 10:20:53
8-2-2021	0 of 0	Base Infrastructure	0 of 0	1	0	Off	Feb 04 2021 10:37:23
helloworld	0 of 0	Shared	0 of 0	1	0	Off	Feb 03 2021 18:08:39
test2	0 of 1	Base Infrastructure	1 of 10	1	0	Off	Feb 03 2021 18:01:42
Default_Switch	0 of 0	Test-AC1-MSP	0 of 0	1	0	On	Feb 01 2021 16:01:40
Default_Switch	0 of 0	JSP-MSP	0 of 0	1	0	On	Feb 01 2021 08:08:01
Default_Switch	0 of 0	Sau_MSP	0 of 0	1	0	On	Jan 29 2021 15:33:00
HouseE	0 of 0	Base Infrastructure	0 of 0	1,2,201	0	On	Jan 29 2021 14:43:39
Complete_Confound	0 of 0	Base Infrastructure	0 of 0	1-4066	0	On	Jan 29 2021 13:03:55
test	0 of 0	Base Infrastructure	0 of 0	1	0	On	Jul 22 2020 10:47:51

Retry Configure

When the user tries to apply any Switch Group on the device and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as "Device was offline", in the Jobs page. In this case, when device comes Up and connects to cnMaestro, then cnMaestro will create an Auto-sync job for that device and pushes the Switch Group. (It will not apply 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. Select update **Now/Schedule**.
4. Click **Apply Configuration**.

The screenshot shows the 'Configuration' page in the cnMaestro interface. It includes a search bar, a table of devices, and configuration options. The table has columns for Device, Managed Account, Switch Group, Status, Sync Status, Network, and Tower/Site. Below the table are options for 'Update' (Now or Schedule) and 'Job Options' (Stop update on critical error, Devices to update in parallel (1-500)).

Device	Managed Account	Switch Group	Status	Sync Status	Network	Tower/Site
cnMatrix-EC2028-0P	Base Infrastructure	N/A	Offline	N/A	!%&-%. DuRgA<	!%&-%. DuRgA<
DP1-X8MB-223-Subnet	Base Infrastructure	Complete, Configured	Offline	In Sync	!%&-%. DuRgA<	!%&-%. DuRgA<
DP3-7G45-223-Subnet	Base Infrastructure	N/A	Offline	N/A	default	
EX2020P-FID940	Base Infrastructure	N/A	Offline	N/A	!%&-%. DuRgA<	Monitor
EX2028P-F09940	Base Infrastructure	N/A	Offline	N/A	cnMatrix	Durga

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 > SyncConfiguration**.

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)
- AP Group/Switch Group (AP Group/Switch Group to which device is mapped)
- Sync Status (Sync status will tell whether job is completed or failed)

Steps to do Sync Configuration:

Navigate to **Manage > Network > Configuration > Device Details or Jobs** tab.

1. Select devices to synchronize and click the **Sync Configuration**.

The screenshot shows the 'System' configuration page. At the top, there are navigation tabs: Dashboard, Notifications, Configuration (selected), Statistics, Report X, Software Update, Clients, Mesh Peers. Below these are filters for Device Type (cnMaestro), Managed Account (All Accounts), and Configuration Method (Switch Group selected, Template unselected). A 'Switch Group' dropdown is set to 'None'. A search bar is present. The main table has columns: Device, Managed Account, Switch Group, Status, Sync Status, Network, Tower/Site, and a gear icon. A red box highlights the 'Sync Configuration' link above the table. Below the table are 'Update' options (Now, Schedule) and 'Job Options' (Stop update on critical error, 10 Devices to update in parallel (1-500)).


Device	Managed Account	Switch Group	Status	Sync Status	Network	Tower/Site
cnMaestro-EX2028-DP	Base Infrastructure	N/A	Offline	N/A	!["&"; DuRqA<[]	![";cnMatrix132F#
DP1X3MR-223-Subnet	Base Infrastructure	Complete, Configured	Offline	In Sync	!["&"; DuRqA<[]	![";cnMatrix132F#
DP2-7G15-223-Subnet	Base Infrastructure	N/A	Offline	N/A	default	
EX2028P-F1D940	Base Infrastructure	N/A	Offline	N/A	!["&"; DuRqA<[]	Monitor
EX2028P-F09940	Base Infrastructure	N/A	Offline	N/A	cnMatrix	Durga

2. Automatically it navigates to **Administration > Sync Configuration** and select devices to synchronize.

The screenshot shows the 'Administration > Sync Configuration' page. It includes a search bar and filters for AP Groups, Managed Account (All Accounts), and Device Type (All). The table has columns: Device, Type, Status, Managed Account, Network, Site, AP Group/Switch Group, and Sync Status. Below the table are 'Job Options' (Stop update on critical error, 10 Devices to update in parallel (1-500)) and a 'Sync Now' button.

Device	Type	Status	Managed Account	Network	Site	AP Group/Switch Group	Sync Status
EX2028P-F1D940	cnMatrix EX2028	Offline	Base Infrastructure	Durga_DataMigration	cnmatrix-tower	Test12	Not In Sync; Device's configuration changed outside of console
E400-307_Htra_From_ABreg	crPilot e400	Offline	Base Infrastructure	DP1 1234	Clients	E400_Appro	Not In Sync; Configuration failed: Device was offline
E400H-Edred	crPilot e425h	Offline	Base Infrastructure	DP2	THOR	E400_Appro	Not In Sync; Configuration failed: Device was offline
DE-Sage	crPilot e410	Offline	Base Infrastructure	default	adminuser	E400_Appro	Not In Sync; Configuration failed: Device was offline
DE-Gambel	crPilot e500	Offline	Base Infrastructure	default		E400_Appro	Not In Sync; Configuration failed: Device was offline
40E400-9527CB	crPilot e410	Offline	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not In Sync; Configuration failed: Device was offline
E400-5225EE	crPilot e400	Offline	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not In Sync; Configuration failed: Device was offline
E400-ASD4E6	crPilot e600	Offline	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not In Sync; Configuration failed: Device was offline
E400-522372	crPilot e400	Online	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not In Sync; Configuration failed: key not in the table
E400-5223E2	crPilot e400	Online	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not In Sync; Configuration failed: key not in the table

3. Click **Sync Now**.



NOTE:
Sync configuration can only be used if a Switch Group is already mapped to the device.

Policy Based Automation(PBA)

Cambium Networks PBA functionality fully automates certain 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 currently connected to the port. These dynamic PBA settings remain in-use for the duration of the device connection and are automatically cleared when the device disconnects from the switch.

PBA configuration is common to all switches within a switch group.

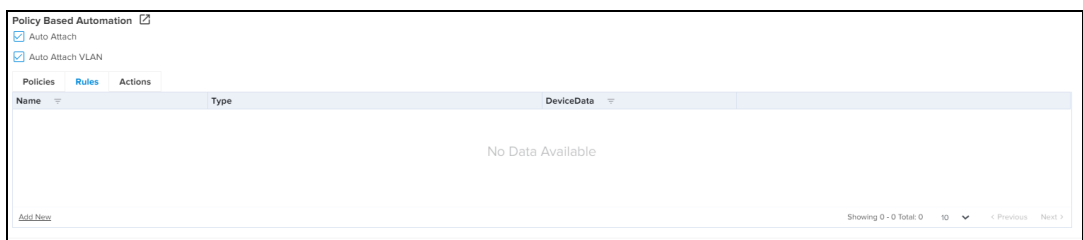


NOTE:

Dynamic PBA updates are indicated by asterisk * on the Switch Dashboard and on the Switch Ports pages.

Configure the PBA as follows:

1. Navigate to **Switch Groups > Configuration > Network > Policy Based Automation.**
2. Navigate to **Rules tab.**



3. Click **Add New** to set the rules.

Add New Rule

A PBA Rule specifies the criteria that is used to identify connected devices for PBA policies. Devices are identified based on generated traffic (LLDP) or MAC address.

Name*

Type*

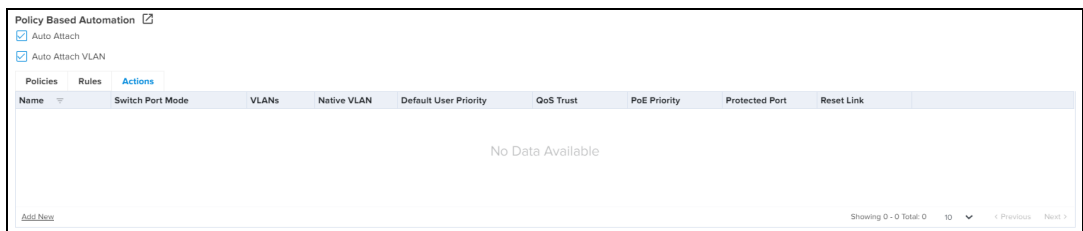
LLDP-ANY

Match LLDP System Name, System Description, Chassis ID

Device Data*

Add

4. Click **Add.**
5. Navigate to **Actions** tab.



6. Click **Add New** to set the actions.

Add New Action ✕

A PBA Action specifies a collection of port-based settings that are updated when a PBA Policy (that references the action) is applied to a port. Updated settings are reset once the policy is no longer applicable.

Name*

Switch Port Mode

VLANs

Native VLAN

Default User Priority

QoS Trust

PoE Priority

Protected Port

Reset Link
Toggle the port link state when native VLAN is updated.

[Add](#)

7. Click **Add**.
8. Navigate to **Policies**.

Policy Based Automation ✕

Auto Attach

Auto Attach VLAN

Policies Rules Actions

Name	Rule	Action	Precedence	Enabled
No Data Available				

[Add New](#)
Showing 0 - 0 Total: 0 10 < Previous Next >

9. Click **Add New** to set the policies.

Add New Policy ✕

Enable

PBA Policies are an ordered list of PBA Rules(filters) and PBA Actions(configuration) that allow automatic configuration of ports based upon traffic. The policies are applied in increasing order of precedence until there is a positive match.

Name*

Enter alphanumeric string without spaces (max 20 chars).

Rule*

Criteria to detect connecting device by PBA. It is created in Rules tab.

Action*

Configuration to be updated when PBA is applied to a port. It is created in Actions tab.

Precedence

50

Evaluation order 1 (first) - 100 (last).

Add

10. The VLANs Action which is set with the Device Data rules and policies is displayed in the System Dashboard Port Status under each port.

Port	Administrative State	Operational State	MAC Address	Description	Speed / Mode / Duplex	MIRROR	Port Group	Type	VLANs	PVID/Native VLANs	STP Mode	STP State	STP Status	QoS Trust	User Priority
4	Enabled	Down			1 Gbps / Auto / Full		desc-4	Hybrid	N/A	1	BST	Discarding	Authorized	Untrusted	0

Switches

The Switches page is accessed by selecting the **Switch Groups > Switches** tab lists all of the physical switches assigned to the Switch Group. The switch dashboard and switch override configurations settings are accessible through this page.

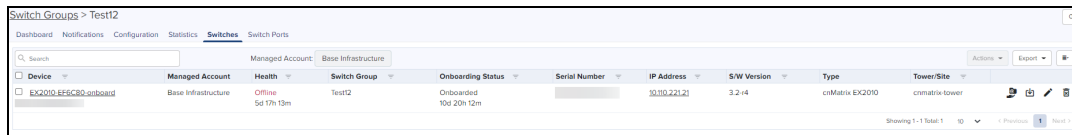
Switch overrides allow certain attributes for each switch to be configured individually.

NOTE:

For configuration, a switch must belong to a Switch Group.

Configure the Switch Group as follows:

- Navigate to **Switch Groups** > select the switch from the list and click **Switches** page to view and edit the onboarded switches.

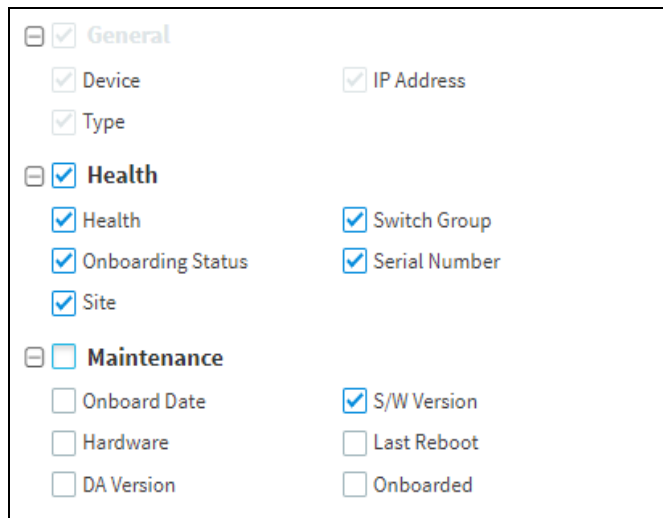


The Switches details view displays following fields by default:

- Device, Health, Onboarding Status, Serial Number, IP Address, Switch Group, Type, Site and Action tab.

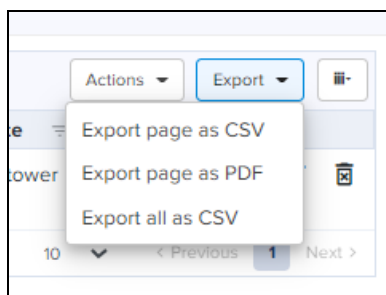
Action column can be used to edit or delete any device of the Switches.

User can click on top bar to include additional fields in Switches Detail view.



Export Switches

1. Click **Export**. A dialogue box appears.

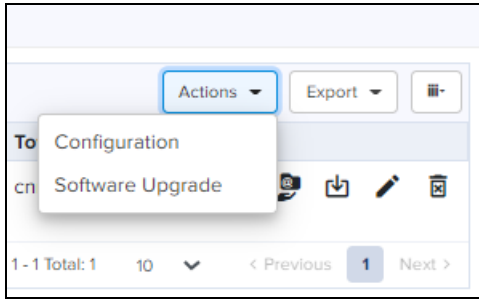





2. Select **Export page as CSV/PDF/all as CSV** and export the file.

Action

Action column can be used to edit or delete any device of the Switches.

1. Click **Action**. A dialogue box appears.

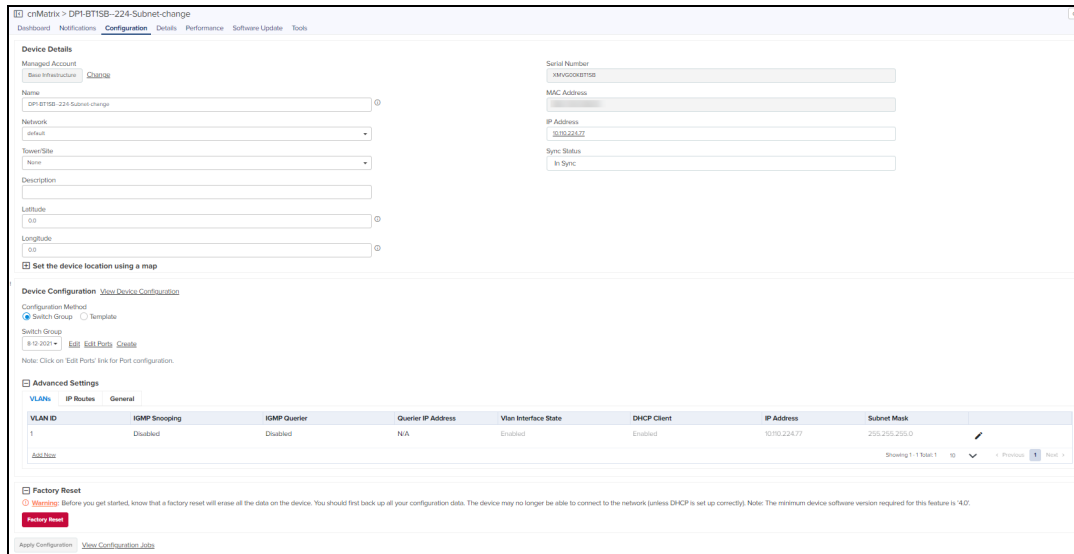


2. Select **Configuration** to edit the device details or click Edit icon 
3. Select **Software Upgrade** to update the device software or click 
4. Click  to delete the selected device from the list.

Switch Configuration

To edit or configure the switches, click the **Edit** or **Configuration** from the **Action** drop-down. Navigates to the Device **Configuration** page.

1. Enter the **Device Details**, **Set the service location** and **Device Configuration**.



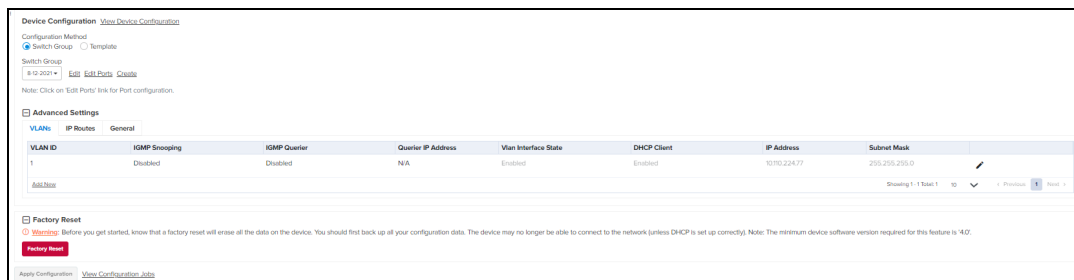
2. Click **Apply Configuration**.

Device Configuration

Device Configuration allows the customer to configure the Configuration Method as Switch Group.

Switch Group Configuration Method

Enable the **Switch Group** and select a device from the **Switch Group** drop-down.



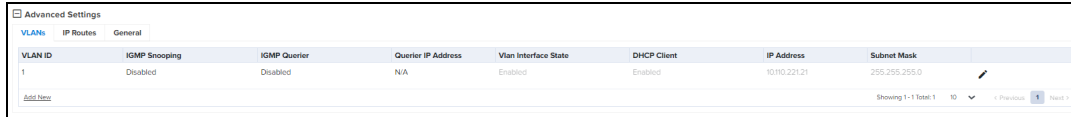
To Edit or Create a Switch Group, refer to the [Switch Groups Configuration](#).

Navigate to the **Advanced Settings** and configure the following parameters:


Vlan Interface

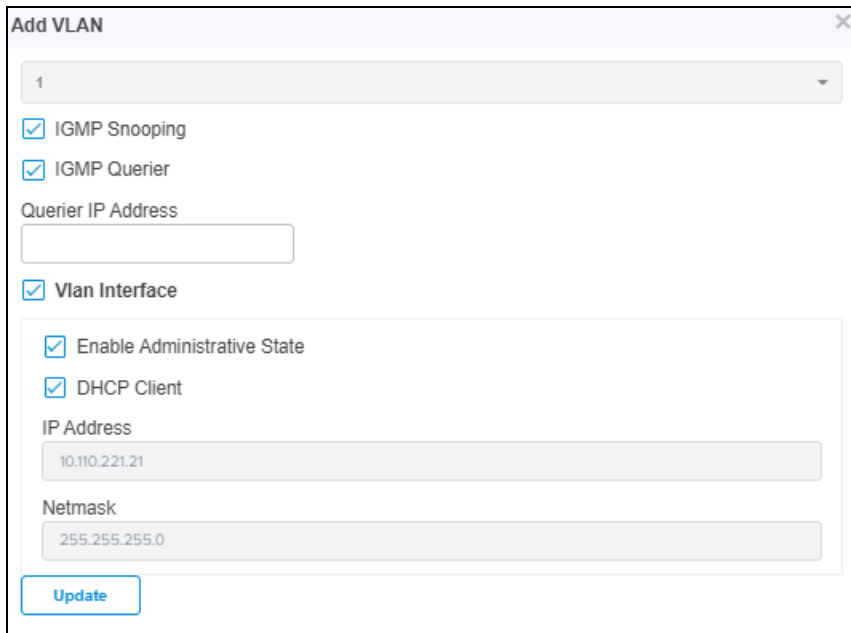
VLAN Interface allows the user to edit/Add the VLAN details such as **Vlan ID**, **IGMP Snooping**, **IGMP Querier**, **Querier IP Address**, **DHCP Client**, **IP Address**, and **Subnet Mask**.

1. Click **Advanced Settings** in **Configuration** page and navigate to **Vlan Interface** tab.



VLAN ID	IGMP Snooping	IGMP Querier	Querier IP Address	Vlan Interface State	DHCP Client	IP Address	Subnet Mask
1	Disabled	Disabled	N/A	Enabled	Enabled	10.110.221.21	255.255.255.0

2. Click Edit Icon  or Add New.
3. Enter the required details and click **Add**



Add VLAN

1

IGMP Snooping

IGMP Querier

Querier IP Address

Vlan Interface

Enable Administrative State

DHCP Client

IP Address

10.110.221.21

Netmask

255.255.255.0

Update

General

Certain configurations are different for each Switch, and these are highlighted within cnMaestro as overrides.

Configure the Overrides as follows:

1. Click **Advanced Settings** in **Configuration** page and navigate to **General** tab.
2. Click **Enable Spanning Tree Overrides**.
3. Select the **Spanning Tree** parameters.

Advanced Settings

- VLANs
- IP Routes
- General**

Enable Spanning Tree Overrides

Spanning Tree


Enable To configure Spanning Tree to override the Switch Group settings.

Mode

Priority

PBA Uplink Ports
 No Configured PBA Actions

Note: Port configuration can be done from Switch Groups -> Switch Ports tab.



NOTE:
 If Spanning Tree is disabled the overrides feature will be disabled on the Switch configuration.

IP Routes

IP Routes allows the user to configure the Default Gateway and IP Routes to override the Switch Group.

- Configure the IP Route as follows:
- Enable the **IP Routes Override** and enter the **Default Gateway**.

Advanced Settings

- VLANs
- IP Routes**
- General

IP Routes Override Enable to configure Default Gateway and IP Routes below to override the Switch Group settings.

Default Gateway

Destination	Subnet Mask	Next Hop	Distance
10.110.10.20	255.255.255.0	10.110.10.30	1

[Add New](#) Showing 1 - 1 Total: 10 < Previous 1 Next >

Note: Port configuration can be done from Switch Groups -> Switch Ports tab.

Factory Reset

[Apply Configuration](#) [View Configuration Jobs](#)

1. Click **Add New**.
2. Enter the parameters such as Destination Network, Subnet Mask, Next Hop, and Distance.
3. Click **Add**.

Add New IP Route

Destination Network

Subnet Mask

Next Hop

Distance
 Integer between 1 and 255.

[Add](#)

Default gateway IP will override the all IP's of the Switch Groups.

Switch Ports

Switch Ports tab displays the list of the Ports and the port channel assigned to the specific switch.

The Switch Ports tab allows the administrators to configure the port settings by port ID for all ports within the switch group. By default, a port ID identifies the switch (by switch name) and port number, example., EX2028P-EC9541: 1.

It supports bulk editing of switch port settings across all physical switches.

To view the Switch Ports, navigate to **Shared Settings > Switch Groups > Switch Ports**.

Ports

cnMaestro **Switch Ports Configuration** tab allows the user to configure the following parameters:

- General
- Physical
- Network
- Security

General Tab

Port	Tags	Description	Interface	Administrative State	Operational State	PoE Capable	
EX2028P-EC9541:1	N/A	DP-Domestic-EX2028-Monag...	RJ-45	Enabled	Up	No	✎
EX2028P-EC9541:2	N/A	27.11	RJ-45	Enabled	Down	No	✎
EX2028P-EC9541:3	N/A	27.13	RJ-45	Enabled	Down	No	✎
EX2028P-EC9541:4	N/A	desc-4	RJ-45	Enabled	Down	No	✎
EX2028P-EC9541:5	N/A	27.15	RJ-45	Enabled	Down	No	✎
EX2028P-EC9541:6	N/A		RJ-45	Enabled	Down	No	✎
EX2028P-EC9541:7	N/A		RJ-45	Enabled	Down	No	✎
EX2028P-EC9541:8	N/A	27.18	RJ-45	Enabled	Down	No	✎
EX2028P-EC9541:9	N/A		SFP	Enabled	Down	No	✎
EX2028P-EC9541:10	N/A	27.10	SFP	Enabled	Down	No	✎


Channel ID	Switch	Tags	Description	VLAN	Native VLAN	Type	Administrative State	Mode	Ports	STP State	STP Priority
No Data Available											

The **Ports General** details view displays following fields by default:

- Port, Tags, Description, Interface, Administrative State, Operational State, PoE Capable, and Edit.

User can click  on top bar to include additional fields in **Ports** General Detail view.

<input checked="" type="checkbox"/> General	<input checked="" type="checkbox"/> Interface	<input checked="" type="checkbox"/> Administrative State
	<input checked="" type="checkbox"/> Operational State	<input checked="" type="checkbox"/> PoE Capable
<input type="checkbox"/> Physical	<input type="checkbox"/> PoE State	<input type="checkbox"/> PoE Priority
	<input type="checkbox"/> PoE Mode	<input type="checkbox"/> Output signal
	<input type="checkbox"/> Speed	<input type="checkbox"/> Duplex
	<input type="checkbox"/> MTU	
<input type="checkbox"/> Network	<input type="checkbox"/> Type	<input type="checkbox"/> VLANs
	<input type="checkbox"/> Native VLAN	<input type="checkbox"/> Channel ID
	<input type="checkbox"/> PBA Policy	<input type="checkbox"/> PBA State
	<input type="checkbox"/> STP State	<input type="checkbox"/> STP Priority
	<input type="checkbox"/> STP BPDU Guard	<input type="checkbox"/> Broadcast
	<input type="checkbox"/> Unknown Unicast	<input type="checkbox"/> Multicast
	<input type="checkbox"/> Suppression Rate	
<input type="checkbox"/> Security	<input type="checkbox"/> QoS Trust	<input type="checkbox"/> User Priority
	<input type="checkbox"/> Dot1x port-control	<input type="checkbox"/> Protected Port
	<input type="checkbox"/> DHCP Snooping Trust	<input type="checkbox"/> ACL Name

1. Click Edit  icon or Port device in the list to edit the **Ports Configuration** General tab details.
2. Navigates to **Switch Groups > Switches > Port Configuration**.

Switch Groups > Complete Configured > Port Configuration

<p>Basic ></p> <p>Physical</p> <p>Network</p> <p>Security</p>	<p>Switch Port(s) Configuration</p> <p>EX2010-EF6CA1: [1]</p> <p>Tags</p> <p>Enter alphanumeric string for port identification and filtering.</p> <p>Description</p> <p>Enter string with max 32 characters.</p> <p>Save</p>
---	--

3. Enter the **Tags** and **Description** details.
4. Click **Save**.

Physical Tab

The **Ports Physical** details view displays following fields by default:

- Port, Tags, Operational State, PoE State, PoE Priority, Speed, Duplex, MTU, and Edit.

Switch Groups > Test12

Dashboard Notifications Configuration Statistics Switches **Switch Ports**

Configuration Statistics

Ports


Port	Tags	Description	Port State	Port Priority	Port Mode	Speed	Duplex	MTU
EX2000_EF6C80_ onboard_1	NA	DP-Don'tLias EX2000 Management	Enabled	Low		1 Gbps	Full	1500
EX2000_EF6C80_ onboard_2	NA	27.1.1	Enabled	Low		1 Gbps	Full	1500
EX2000_EF6C80_ onboard_3	NA	27.1.3	Enabled	Low		1 Gbps	Full	1500
EX2000_EF6C80_ onboard_4	NA	disc 4	Enabled	Low		1 Gbps	Full	1500
EX2000_EF6C80_ onboard_5	NA	27.1.5	Enabled	Low		1 Gbps	Full	1500
EX2000_EF6C80_ onboard_6	NA		Enabled	Low		1 Gbps	Full	1500
EX2000_EF6C80_ onboard_7	NA		Enabled	Low		1 Gbps	Full	1500
EX2000_EF6C80_ onboard_8	NA	27.1.8	Enabled	Low		1 Gbps	Full	1500
EX2000_EF6C80_ onboard_9	NA		Disabled	Low		1 Gbps	Full	1500
EX2000_EF6C80_ onboard_10	NA	27.1.10	Disabled	Low		1 Gbps	Full	1500

Showing 1 - 10 Total 10 10 Previous Next


Port Channel

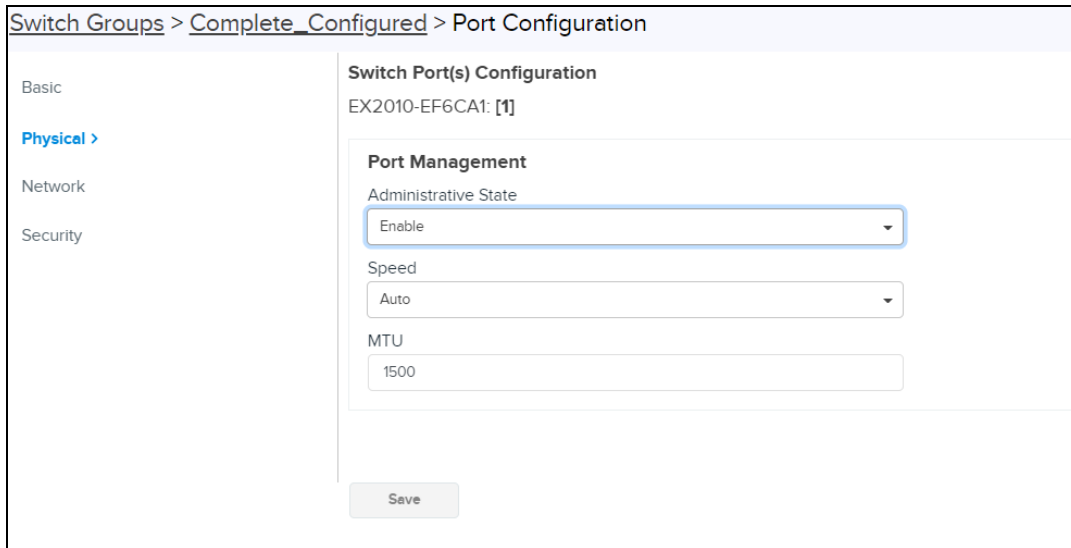
Channel ID	Switch	Tags	Description	VLAN	Native VLAN	Type	Administrative State	Mode	Ports	STP State	STP Priority
No Data Available											

Showing 0 - 0 Total 0 10 Previous Next

User can click  on top bar to include additional fields in **Ports Physical** Detail view.

<input checked="" type="checkbox"/>	General		
<input checked="" type="checkbox"/>	Interface	<input checked="" type="checkbox"/>	Administrative State
<input checked="" type="checkbox"/>	Operational State	<input checked="" type="checkbox"/>	PoE Capable
<input type="checkbox"/>	Physical		
<input type="checkbox"/>	PoE State	<input type="checkbox"/>	PoE Priority
<input type="checkbox"/>	PoE Mode	<input type="checkbox"/>	Output signal
<input type="checkbox"/>	Speed	<input type="checkbox"/>	Duplex
<input type="checkbox"/>	MTU		
<input type="checkbox"/>	Network		
<input type="checkbox"/>	Type	<input type="checkbox"/>	VLANs
<input type="checkbox"/>	Native VLAN	<input type="checkbox"/>	Channel ID
<input type="checkbox"/>	PBA Policy	<input type="checkbox"/>	PBA State
<input type="checkbox"/>	STP State	<input type="checkbox"/>	STP Priority
<input type="checkbox"/>	STP BPDU Guard	<input type="checkbox"/>	Broadcast
<input type="checkbox"/>	Unknown Unicast	<input type="checkbox"/>	Multicast
<input type="checkbox"/>	Suppression Rate		
<input type="checkbox"/>	Security		
<input type="checkbox"/>	QoS Trust	<input type="checkbox"/>	User Priority
<input type="checkbox"/>	Dot1x port-control	<input type="checkbox"/>	Protected Port
<input type="checkbox"/>	DHCP Snooping Trust	<input type="checkbox"/>	ACL Name

1. Click Edit  icon or Port device in the list to edit the **Ports Configuration** Physical tab details.

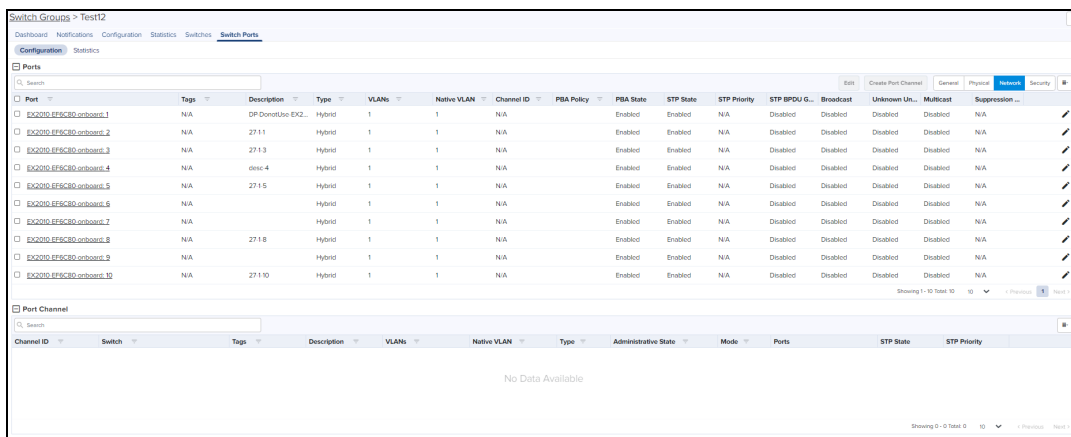


2. Enter the **Port Management** and **PoE** details.
3. Click **Save**.

Network Tab


The **Ports Network** details view displays following fields by default:

- Port, Tags, Type, VLANs, Native VLAN, Channel ID, PBA Policy, PBA State, STP State, STP Priority, and Edit.



User can click  on top bar to include additional fields in **Ports Network** Detail view.

<input checked="" type="checkbox"/> General	<input checked="" type="checkbox"/> Interface	<input checked="" type="checkbox"/> Administrative State
	<input checked="" type="checkbox"/> Operational State	<input checked="" type="checkbox"/> PoE Capable
<input type="checkbox"/> Physical	<input type="checkbox"/> PoE State	<input type="checkbox"/> PoE Priority
	<input type="checkbox"/> PoE Mode	<input type="checkbox"/> Output signal
	<input type="checkbox"/> Speed	<input type="checkbox"/> Duplex
	<input type="checkbox"/> MTU	
<input type="checkbox"/> Network	<input type="checkbox"/> Type	<input type="checkbox"/> VLANs
	<input checked="" type="checkbox"/> Native VLAN	<input type="checkbox"/> Channel ID
	<input type="checkbox"/> PBA Policy	<input type="checkbox"/> PBA State
	<input type="checkbox"/> STP State	<input type="checkbox"/> STP Priority
	<input type="checkbox"/> STP BPDU Guard	<input type="checkbox"/> Broadcast
	<input type="checkbox"/> Unknown Unicast	<input type="checkbox"/> Multicast
	<input type="checkbox"/> Suppression Rate	
<input type="checkbox"/> Security	<input type="checkbox"/> QoS Trust	<input type="checkbox"/> User Priority
	<input type="checkbox"/> Dot1x port-control	<input type="checkbox"/> Protected Port
	<input type="checkbox"/> DHCP Snooping Trust	<input type="checkbox"/> ACL Name

1. Click Edit icon  or Port device in the list to edit the **Ports Configuration** Network tab details.

Switch Groups > 27-10-2021 > Port Configuration

Basic

Physical

Network

Security

Switch Port(s) Configuration
XMWG00DGX8MB: [1]

VLANs

Type
Hybrid

VLANs
1 Available VLANs - 1

Native VLAN
1 Tagged

STP

BPDU Guard
Disable

Policy Based Automation

PBA port status
Enable

LLDP Actions

Expiration Reset
Disable

Automatic LLDP-MED Voice
Enable

Storm Control

Suppression Rate
1-262143

Broadcast
Disable

Multicast
Disable

Unknown Unicast
Disable

Save

2. Enter **VLANs**, **STP**, **Policy Based Automation**, and **Strom Control** details.


3. Click **Save**.

Security Tab

The **Ports Security** details view displays following fields by default:

- Port, Tags, QoS Trust, User Priority, Dot1x port-control, Protected Port, DHCP Snooping Trust, ACL Name, and Edit.

Port	Tags	Description	QoS Trust	User Priority	Dot1x port-control	Protected Port	DHCP Snooping Trust	ACL Name
EX2010_EF5C80_ onboard_1	N/A	DP DonorLine-EX2010 Mana...	Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2010_EF5C80_ onboard_2	N/A	27 11	Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2010_EF5C80_ onboard_3	N/A	27 13	Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2010_EF5C80_ onboard_4	N/A	desc 4	Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2010_EF5C80_ onboard_5	N/A	27 15	Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2010_EF5C80_ onboard_6	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2010_EF5C80_ onboard_7	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2010_EF5C80_ onboard_8	N/A	27 16	Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2010_EF5C80_ onboard_9	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2010_EF5C80_ onboard_10	N/A	27 10	Untrust	0	forceAuthorized	Disabled	Untrusted	

User can click  on top bar to include additional fields in **Ports Network Detail** view.

General

Interface Administrative State

Operational State PoE Capable

Physical

PoE State PoE Priority

PoE Mode Output signal

Speed Duplex

MTU

Network

Type VLANs

Native VLAN Channel ID

PBA Policy PBA State

STP State STP Priority

STP BPDU Guard Broadcast

Unknown Unicast Multicast


Suppression Rate

Security

QoS Trust User Priority

Dot1x port-control Protected Port

DHCP Snooping Trust ACL Name

1. Click Edit  icon or Port device in the list to edit the Ports Configuration Security tab details.

Switch Groups > Default Switch > Port Configuration

Basic

Physical

Network

Security >

Switch Port(s) Configuration

["Harshit-151:1"]

802.1x Port Control

Port Control
Force-Authorized

DHCP Snooping Trusted State

Port Trusted State
Untrusted

QoS

Trust
Untrust

User Priority
1

Protected Port

State
Disable

Access Control List

ACL Name
Select or search ACL...

Save

2. Enter **802.1x Port Control**, **DHCP Snooping Trusted State**, **QoS**, **Protected Port**, **Access Control List** details.
3. Click **Save**.

Port Channel

1. To create a Port Channel, select a **Port** from the list under the specific parameters and click **Create Port Channel**.
2. **Create Port Channel** window pops-up, enter details.
3. Click **Create**.

Create Port Channel

Channel ID

Mode
Active

Ports
1

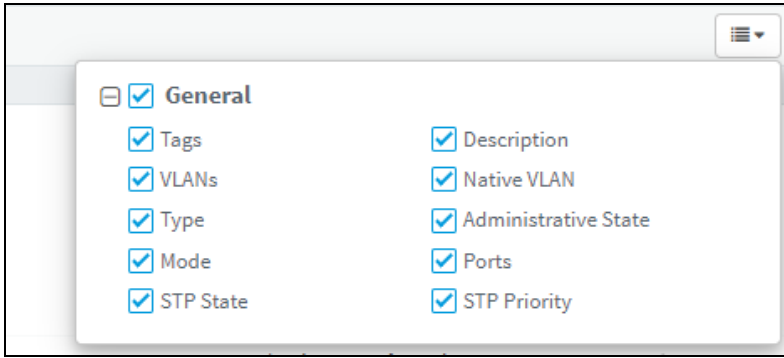
Create

The **PortChannel** details view displays following fields by default:

- Channel ID, Switch, Tags, Description, VLANs, Native VLAN, Type, Administrative State, Mode, Ports, STP State, and STP Priority.

Channel ID	Switch	Tags	Description	VLANs	Native VLAN	Type	Administrative State	Mode	Ports	STP State	STP Priority
1	EX2010MP F453A1	Tag 123	hello 123	1	1	Access	Enabled	Manual	2,3	Disabled	128
2	EX2010MP F453A1	Tag 456	hello 456	1	1	Hybrid	Enabled	Manual	4,5	Enabled	128
10	EX2010MP F453A1	N/A	N/A	1	1	Hybrid	Enabled	Active	10	Enabled	128
30	EX2010MP F453A1	port3	hello 3	14006	1	Trunk	Disabled	Passive	6	Disabled	128

User can click on top bar to include additional fields in **Port Channel** Detail view.



Statistics

The **Statistics** page displays the latest data and statistics of each Port. Port statistics match the Client statistics and generate the Client View.

To view the Switch Ports Statics navigate to **Shared Settings > Switch Groups > Switch Ports > Statistics**.

Switch Groups > Test12


Dashboard Notifications Configuration Statistics Switches **Switch Ports**

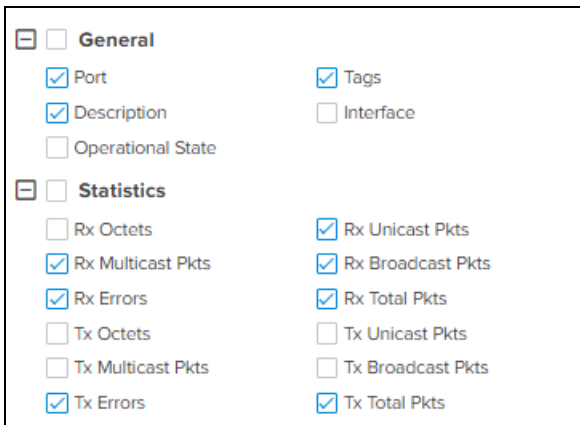
Configuration **Statistics**

Search

Port	Tags	Description	Rx Unicast Pkts	Rx Multicast Pkts	Rx Broadcast Pkts	Rx Errors	Rx Total Pkts	Tx Errors	Tx Total Pkts
EX2010-EP6C30-orboard-1	N/A	DP-DonorUse-EX2010-Management-183	1227	10702	0	0	12212	0	350
EX2010-EP6C30-orboard-2	N/A	2711	0	0	0	0	0	0	0
EX2010-EP6C30-orboard-3	N/A	2713	0	0	0	0	0	0	0
EX2010-EP6C30-orboard-4	N/A	disc-4	0	0	0	0	0	0	0
EX2010-EP6C30-orboard-5	N/A	2715	0	0	0	0	0	0	0
EX2010-EP6C30-orboard-6	N/A		0	0	0	0	0	0	0
EX2010-EP6C30-orboard-7	N/A		0	0	0	0	0	0	0
EX2010-EP6C30-orboard-8	N/A	2718	0	0	0	0	0	0	0
EX2010-EP6C30-orboard-9	N/A		0	0	0	0	0	0	0
EX2010-EP6C30-orboard-10	N/A	2710	0	0	0	0	0	0	0

Showing 1-10 Total 10 10 10

User can click  on top bar to include additional fields in **Statistics** Detail view.



Device Details

Details page provide the information about the switches **Overview**, **Topology**, and **Port Statistics**.

cnMatrix > EX2010-EF6C80-onboard

Dashboard Notifications Configuration **Details** Performance Software Update Tools

Overview Topology Port Statistics

System

Name	EX2010-EF6C80-onboard
Device Type	cnMatrix EX2010
System Uptime	5d 19h 5m
Coordinates	[78.96, 20.59]
Description	
Hardware	Ethernet switch 8 copper 1G ports, 2 SFP 1G ports
Hardware Version	01
DA Version	4.9
Manufacture Date	2019-04-06
Onboard Date	Jan 29 2021 16:12:35

Software Update

Active Software Version 3.2-r4

History

Date	Status	Version
Wed Feb 03 2021 18:40:41 UTC +0530	Success	3.2-r4
Wed Feb 03 2021 16:34:08 UTC +0530	Success	3.2.1-r5
Wed Feb 03 2021 13:58:55 UTC +0530	Success	3.1.1-r3

Configuration Update

History

Date	Status	Template
Wed Feb 03 2021 18:02:00 UTC +0530	Success	Test12
Wed Feb 03 2021 17:59:57 UTC +0530	Success	Default Switch
Wed Feb 03 2021 17:59:27 UTC +0530	Success	Default Switch

Details Overview

To view the details of the overview page, navigate to the **Details > Overview** tab.

cnMatrix > EX2010-EF6C80-onboard

Dashboard Notifications Configuration **Details** Performance Software Update Tools

Overview Topology Port Statistics

System

Name	EX2010-EF6C80-onboard
Device Type	cnMatrix EX2010
System Uptime	5d 19h 5m
Coordinates	[78.96, 20.59]
Description	
Hardware	Ethernet switch 8 copper 1G ports, 2 SFP 1G ports
Hardware Version	01
DA Version	4.9
Manufacture Date	2019-04-06
Onboard Date	Jan 29 2021 16:12:35

Software Update

Active Software Version **3.2-r4**

History

Date	Status	Version
Wed Feb 03 2021 18:40:41 UTC +0530	Success	3.2-r4
Wed Feb 03 2021 16:34:08 UTC +0530	Success	3.2.1-r5
Wed Feb 03 2021 13:58:55 UTC +0530	Success	3.1.1-r3

Configuration Update

History

Date	Status	Template
Wed Feb 03 2021 18:02:00 UTC +0530	Success	Test12
Wed Feb 03 2021 17:59:57 UTC +0530	Success	Default Switch
Wed Feb 03 2021 17:59:27 UTC +0530	Success	Default Switch

Topology

To view the details of the Topology page, navigate to the **Details > Topology** tab.

cnMatrix > EX2010-EF6C80

Dashboard Notifications Configuration **Details** Performance Software Update Tools

Overview **Topology** Port Statistics

Chassis ID: Search

ID	Name	Chassis ID	Description	MAC	IP Address
GD1	DP DonotUse EX2010 Management	58c17aef6ca1	Cambium Networks cnMatrix EX2010 Ethernet Switch HW...	58c17aef6ca3	

Showing 1-1 Total 1 | Previous 1 Next

Port Statistics

To view the details of the Port Statistics page, navigate to the **Details > Port Statistics** tab.

cnMatrix > EX2010-EF6C80-onboard

Dashboard Notifications Configuration **Details** Performance Software Update Tools

Overview Topology **Port Statistics**

Search

Port	Tags	Description	Rx Unicast Pkts	Rx Multicast Pkts	Rx Broadcast Pkts	Rx Errors	Rx Total Pkts	Tx Errors	Tx Total Pkts
EX2010-EF6C80-onboard:1	N/A	DP-DonotUse-EX2010-Mana... 183	1227	110702	0	0	112112	0	350
EX2010-EF6C80-onboard:2	N/A	27:1:1	0	0	0	0	0	0	0
EX2010-EF6C80-onboard:3	N/A	27:1:3	0	0	0	0	0	0	0
EX2010-EF6C80-onboard:4	N/A	desc:4	0	0	0	0	0	0	0
EX2010-EF6C80-onboard:5	N/A	27:1:5	0	0	0	0	0	0	0
EX2010-EF6C80-onboard:6	N/A		0	0	0	0	0	0	0
EX2010-EF6C80-onboard:7	N/A		0	0	0	0	0	0	0
EX2010-EF6C80-onboard:8	N/A	27:1:8	0	0	0	0	0	0	0
EX2010-EF6C80-onboard:9	N/A		0	0	0	0	0	0	0
EX2010-EF6C80-onboard:10	N/A	27:1:10	0	0	0	0	0	0	0

Showing 1 - 10 Total 10 10 < Previous Next >

60 GHz cnWave Network Configuration

60 GHz cnWave 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.

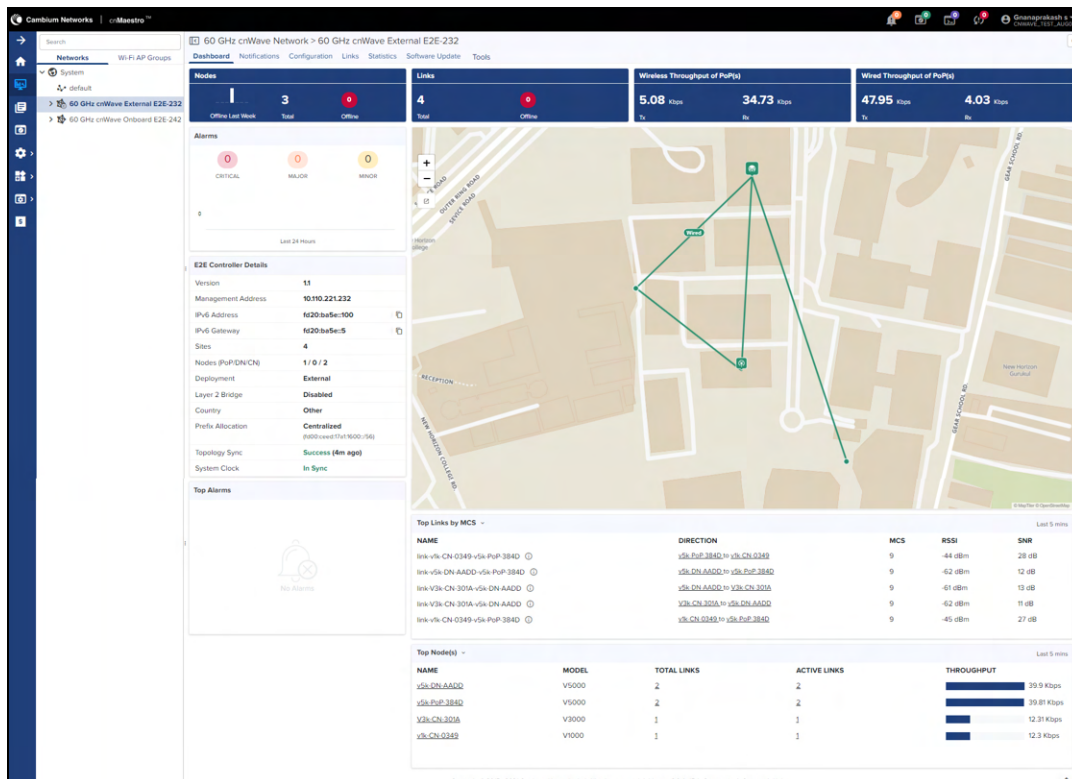
Managing E2E Network

The Monitoring tab displays the monitoring panel of 60 GHz cnWave for cnMaestro On-Premises. This section includes the following:

- Dashboard
- Notifications
- Configuration
- Links
- Statistics
- Software Update
- Reports
- Map
- Tools

Dashboard

Dashboard pages are customized for each device type and aggregation level (such as E2E Network, Node, and Site). The dashboard section displays the **Nodes**, **Links**, **Auto Manage IPv6 Routes**, **Wireless Throughput of PoP(s)**, **Wired Throughput of PoP(s)**, **Alarms**, **E2E Controller Details**, **Top Alarms**, **Map**, **Top Links by MCS**, **Top Links by RSSI**, **Top Links by SNR**, **Top Node(s)**, **Top PoP(s)**, **Top DN(s)**, and **Top CN(s)**.



Auto Manage IPv6 Routes (E2E Controller ↔ Node)

The E2E Controller 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.

The screenshot displays the E2E Controller Network dashboard. The top navigation bar shows 'Auto Manage IPv6 Routes (E2E Controller ↔ Node)' as the active tab. The main area is divided into three sections:


- Map:** A map showing the physical layout of the network with nodes and connections.
- E2E Controller Details:** A configuration panel for the E2E Controller. Key details include:
 - Version: 1.2.0-01
 - Management Address: 10.10.10.1
 - IPv6 Address: 2001:db8:1:1::1
 - IPv6 Gateway: 2001:db8:1:1::1
 - Sites: 1
 - Nodes: 1
 - Deployment: External
 - Layer 2 Bridge: Disabled
 - Country: Australia
 - Prefix Allocation: Deterministic (Hierarchical)
 - Topology Sync: Success (Mn app)
 - System Clock: In Sync
- Auto Manage IPv6 Routes (E2E Controller ↔ Node):** A diagram showing the E2E Controller connected to a PoP node, which is in turn connected to a CN. Below this is a table of routes managed by the system:

NAME	DIRECTION	MCS	RIS	DIR
10.10.10.1/24	2001:db8:1:1::1/32	10	10	10
10.10.10.1/24	2001:db8:1:1::1/32	10	10	10
10.10.10.1/24	2001:db8:1:1::1/32	10	10	10
10.10.10.1/24	2001:db8:1:1::1/32	10	10	10



E2E Controller Details

E2E Controller Details displays the details such as **Version, Management Address, IPv6 Address, IPv6 Gateway, Sites, Nodes, Deployment, Layer 2 Bridge, Country, Prefix Allocation, Topology Sync, and System Clock**

- If Onboard E2E controller is enabled in device and managed by cnMaestro, it displays deployment as **Running Onboard**.

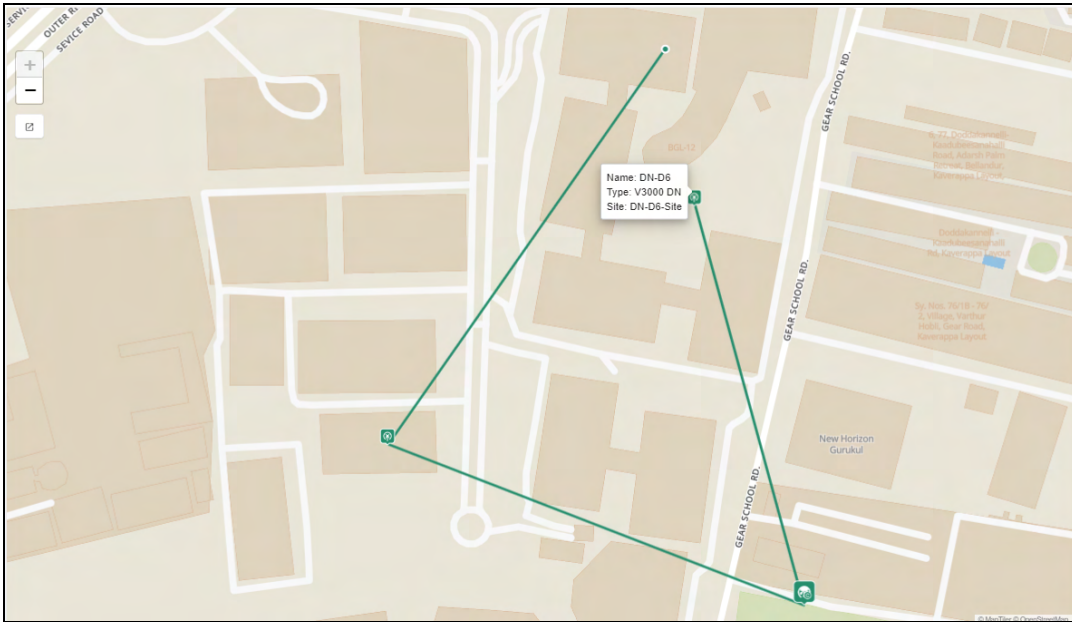
E2E Controller Details	
Version	1.1
Management Address	10.110.221.242
IPv6 Address	fd00:ba5e:88:3083::88:3... 
IPv6 Gateway	-
Sites	4
Nodes (PoP/DN/CN)	1 / 0 / 1
Deployment	Running Onboard
Layer 2 Bridge	Disabled
Country	Belgium
Prefix Allocation	Deterministic (fd00:ceed:8830:8300::/56)
Topology Sync	Success (6m ago)
System Clock	In Sync

- If External E2E controller is managed by cnMaestro, it displays deployment as **External**.

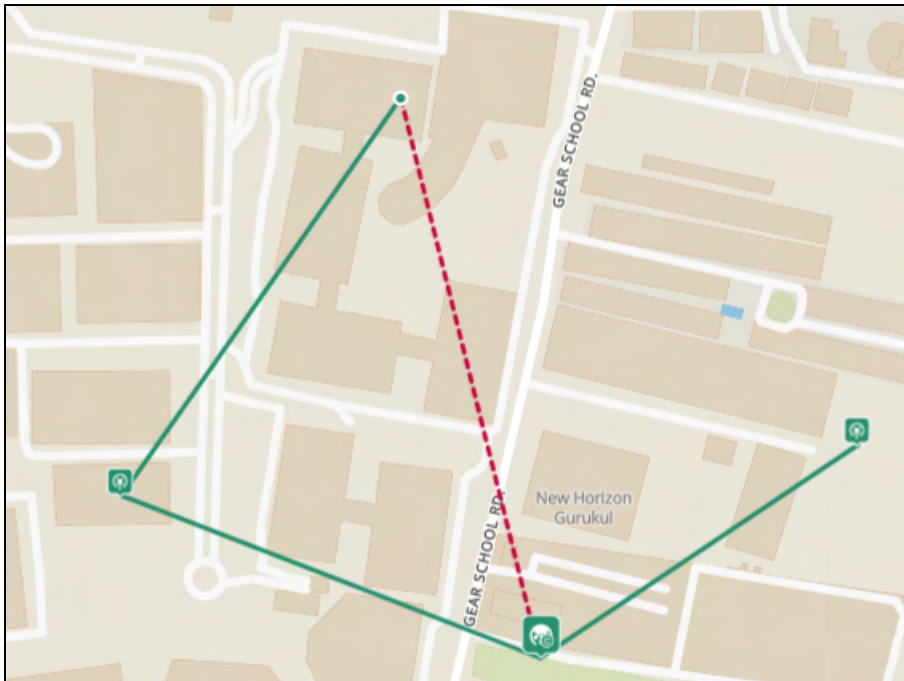
E2E Controller Details	
Version	1.1
Management Address	10.110.221.232
IPv6 Address	fd20:ba5e::100 
IPv6 Gateway	fd20:ba5e::5 
Sites	4
Nodes (PoP/DN/CN)	1 / 0 / 2
Deployment	External
Layer 2 Bridge	Disabled
Country	Other
Prefix Allocation	Centralized (fd00:ceed:17a1:1600::/56)
Topology Sync	Success (4m ago)
System Clock	In Sync

Dashboard Maps

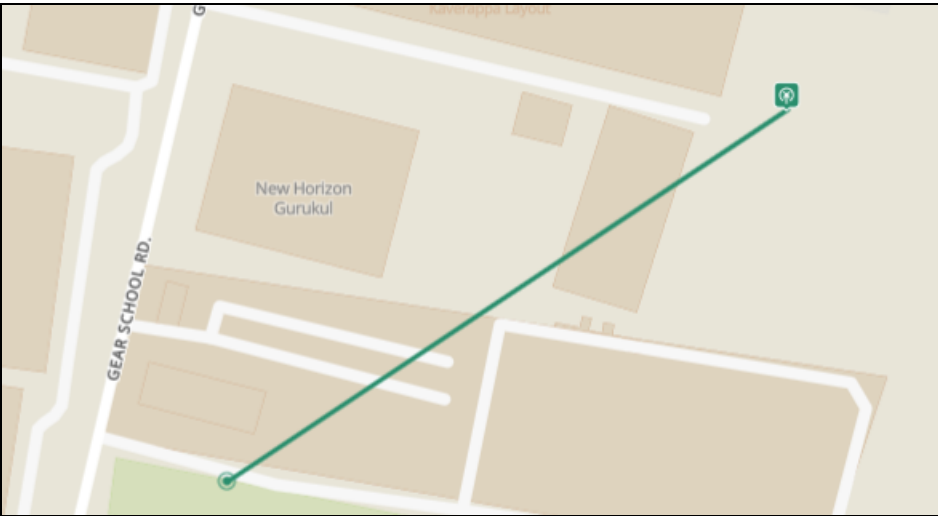
In the dashboard map, when user hover on particular link or node, it pops-up link or node basic details.



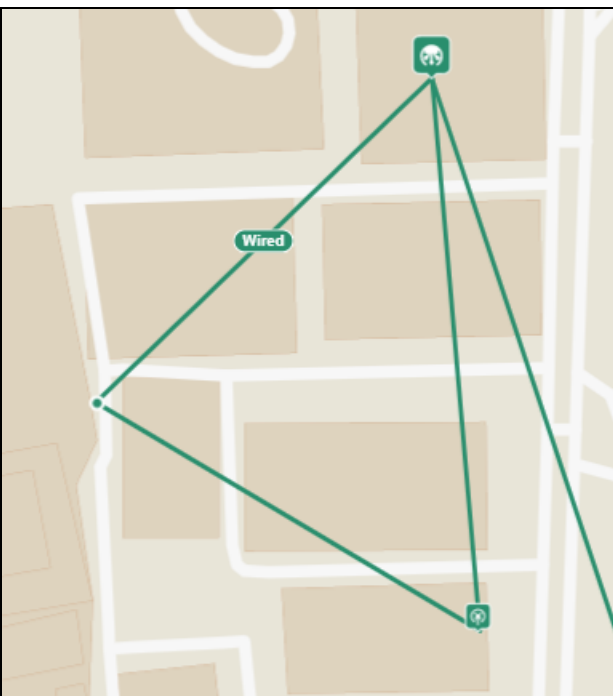
- Dotted line displays the Backup CN link between the DN and CN.



- Continuous line displays the wireless link between PoP, DN or CN.



- Continuous line with **Wired** tag displays the wired link between PoP, DN or CN.



To navigate to the Maps page click the Map view  .

Notifications

Notifications are same as shown above for other devices, refer [Notification](#) for more details.

Configuration

Configure the following after onboarding the 60 GHz cnWave E2E controller:

- [Basic](#)
- [Management](#)
- [Security](#)
- [Advanced](#)
- [E2E Controller](#)

60 GHz cnWave Network > 7Nodes-external

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Security Advanced E2E Controller

Seed Prefix: 1600:0ae4d:1992:1400::56 IPv6 'seed prefix' in CIDR format from which subnet prefixes are allocated to all DNs and CNs (e.g. fdcc:b00c:cafe:ba00::56)

Prefix Length: 64 Length of per-node allocated prefixes

Layer 2 Bridge

Enable Selecting this option will enable Layer 2 network bridging (via automatically created tunnels) across all nodes connected to a PoP. This will facilitate bridging of IPv4 traffic across the wireless networks.

IP-v6 Layer3 CPE Address

SLAAC DHCPv6 Relay

CPE Prefix Zoning

Summarized CPE Prefix: Prefix summarizing network wide customized CPE Prefixes/Prefixed allocated by DHCPv6 Relay (that fall outside Seed Prefix range).

Country: Other

Enabled Radio Channels: 2 List of enabled transmission channels for topology. Comma separated values from 1 to 4 (subject to regulatory). This configuration is used by the controller for auto config override. Channels set manually ignore this configuration.

DNS Servers: DNS server list, comma separated. IPv4 is only supported when Layer 2 bridge is enabled.

NTP Server: NTP Server hostnames or IP addresses, comma separated. IPv4 address is only supported when Layer 2 Bridge is enabled. Note: NTP should be enabled from E2E Network -> Tools -> Settings page.

Time Zone: Africa/Cairo

Wireless Scans

Scheduled Beam Adjustment: Enabled Disabled

Scan Interval: 14400 Interval between wireless scans in seconds



NOTE:

Once user selects the **Auto-assign** IPv6 Addresses while configuring E2E Controller and PoP node. Uses the same IPv6 during the prefix allocation.

Basic Configuration

1. Navigate to **Configuration > Basic** to configure basic settings of E2E Controller.

60 GHz cnWave Network > 7Nodes-external

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Security Advanced E2E Controller

Seed Prefix: 1600:0ae4d:1992:1400::56 IPv6 'seed prefix' in CIDR format from which subnet prefixes are allocated to all DNs and CNs (e.g. fdcc:b00c:cafe:ba00::56)

Prefix Length: 64 Length of per-node allocated prefixes

Layer 2 Bridge

Enable Selecting this option will enable Layer 2 network bridging (via automatically created tunnels) across all nodes connected to a PoP. This will facilitate bridging of IPv4 traffic across the wireless networks.

IP-v6 Layer3 CPE Address

SLAAC DHCPv6 Relay

CPE Prefix Zoning

Summarized CPE Prefix: Prefix summarizing network wide customized CPE Prefixes/Prefixed allocated by DHCPv6 Relay (that fall outside Seed Prefix range).

Country: Other

Enabled Radio Channels: 2 List of enabled transmission channels for topology. Comma separated values from 1 to 4 (subject to regulatory). This configuration is used by the controller for auto config override. Channels set manually ignore this configuration.

DNS Servers: DNS server list, comma separated. IPv4 is only supported when Layer 2 bridge is enabled.

NTP Server: NTP Server hostnames or IP addresses, comma separated. IPv4 address is only supported when Layer 2 Bridge is enabled. Note: NTP should be enabled from E2E Network -> Tools -> Settings page.

Time Zone: Africa/Cairo

Wireless Scans

Scheduled Beam Adjustment: Enabled Disabled

Scan Interval: 14400 Interval between wireless scans in seconds



NOTE:

Prefix allocation automatically gets updated, when E2E Controller is managed by cnMaestro.

2. In the **Prefix Allocation**, select **Centralized** or **Deterministic** to allocate the IP for the nodes.

60 GHz cnWave Network > 7Nodes-external

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Security Advanced EZE Controller

Prefix Allocation

Centralized Deterministic

Seed Prefix: IPv6 'seed prefix' in CIDR format from which subnet prefixes are allocated to all DNs and Cns (e.g. f00c:300c:cafe:5a00::56)

Prefix Length: Length of per-node allocated prefixes

Layer 2 Bridge

Enable: Selecting this option will enable Layer 2 network bridging (via automatically created tunnels) across all nodes connected to a PoP. This will facilitate bridging of IPv4 traffic across the wireless networks.

IPv6 Layer3 CPE Address

SLAAC DHCPv6 Relay

DHCPv6 Server Address:

CPE Prefix Zoning

Summarized CPE Prefix: Prefix summarizing network wide customized CPE Prefixes/Prefixes allocated by DHCPv6 Relay (that fall outside Seed Prefix range)

Country:

Enabled Radio Channels: List of enabled transmission channels for topology. Comma separated values from 1 to 4 (subject to regulatory). This configuration is used by the controller for auto config override. Channels set manually ignore this configuration.

DNS Servers: DNS server list, comma separated. IPv4 is only supported when Layer 2 bridge is enabled.

NTP Server: NTP Server hostnames or IP addresses, comma separated. IPv4 address is only supported when Layer 2 Bridge is enabled. Note: NTP should be enabled from EZE Network -> Tools -> Settings page.

Time Zone:

Wireless Scans

Scheduled Scan Adjustment: Enabled Disabled

Scan Interval: Interval between wireless scans in seconds

Copyright © 2015 - 2021 Cambium Networks, Ltd. All rights reserved. | Version 3.0.4-1 | [Connect](#) | [Support](#) | [FAQ](#) | [License](#)

3. Enter the **Seed Prefix** and **Prefix Length**.

60 GHz cnWave Network > 7Nodes-external

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Security Advanced EZE Controller

Prefix Allocation

Centralized Deterministic

Seed Prefix: IPv6 'seed prefix' in CIDR format from which subnet prefixes are allocated to all DNs and Cns (e.g. f00c:300c:cafe:5a00::56)

Prefix Length: Length of per-node allocated prefixes

Layer 2 Bridge

Enable: Selecting this option will enable Layer 2 network bridging (via automatically created tunnels) across all nodes connected to a PoP. This will facilitate bridging of IPv4 traffic across the wireless networks.

IPv6 Layer3 CPE Address

SLAAC DHCPv6 Relay

DHCPv6 Server Address:

CPE Prefix Zoning

Summarized CPE Prefix: Prefix summarizing network wide customized CPE Prefixes/Prefixes allocated by DHCPv6 Relay (that fall outside Seed Prefix range)

Country:

Enabled Radio Channels: List of enabled transmission channels for topology. Comma separated values from 1 to 4 (subject to regulatory). This configuration is used by the controller for auto config override. Channels set manually ignore this configuration.

DNS Servers: DNS server list, comma separated. IPv4 is only supported when Layer 2 bridge is enabled.

NTP Server: NTP Server hostnames or IP addresses, comma separated. IPv4 address is only supported when Layer 2 Bridge is enabled. Note: NTP should be enabled from EZE Network -> Tools -> Settings page.

Time Zone:

Wireless Scans

Scheduled Scan Adjustment: Enabled Disabled

Scan Interval: Interval between wireless scans in seconds

Copyright © 2015 - 2021 Cambium Networks, Ltd. All rights reserved. | Version 3.0.4-1 | [Connect](#) | [Support](#) | [FAQ](#) | [License](#)

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 check box to enable Layer2 Network Bridging, choose **Tunnel Concentrator** as **Best PoP** or **Static**.

The screenshot shows the configuration page for a 60 GHz cnWave Network. The 'Layer 2 Bridge' section is expanded, and the 'Tunnel Concentrator' is set to 'Static'. Other sections include 'Prefix Allocation', 'IPv6 Layer3 CPE Address', 'CPE Prefix Zoning', and 'Wireless Scans'.

- If user selects **Tunnel Concentrator as Static**.
- Enter the Concentrator can be an external switch/router when static is selected.

This screenshot is similar to the previous one, but the 'IPv6 Address' field under the 'Layer 2 Bridge' section is now visible and empty. The 'Tunnel Concentrator' remains set to 'Static'.



NOTE:

IPv6 Layer3 CPE Address can be enabled when E2E Controller is running 1.1 version and Layer 2 Bridge is disabled.


5. Select the **IPv6 Layer3 CPE Address** as **SLAAC** or **DHCPv6 Relay**.

CPE sends a DHCP request. DHCPv6 server assigns address and the CN node uses the Address and Prefix from the corresponding DHCP pool.

The screenshot shows the configuration page for a 60 GHz cnWave Network. The 'IPv6 Layer3 CPE Address' section is selected, with 'DHCPv6 Relay' chosen. Other visible settings include 'Prefix Allocation' (Centralized), 'Seed Prefix' (192.168.100.0/24), 'Prefix Length' (24), 'Layer 2 Bridge' (disabled), 'CPE Prefix Zoning' (Summarized CPE Prefix), 'Country' (Other), 'Enabled Radio Channels' (2), 'DNS Servers', 'NTP Server', 'Time Zone', and 'Wireless Scans' (disabled).

- If user selects **IPv6 Layer3 CPE Address as DHCPv6 Relay**, User can configure the DHCPv6 server address.

This screenshot is similar to the previous one but shows the 'DHCPv6 Server Address' field in the 'IPv6 Layer3 CPE Address' section, which is currently empty. The 'DHCPv6 Relay' option remains selected.

	<p>NOTE:</p> <ul style="list-style-type: none"> ● By default Country is Other, user can configure it. ● By default Enabled Radio Channels is 2, user can configure channel if required. ● Enter the Hostnames or IP address of NTP server
---	--

6. In **CPE Prefix Zoning** enter **Summarized CPE Prefix**.
7. Select the **Country** from the drop-down.
8. Enter the channel number in **Enable Radio Channels** and **DNS Servers**.
9. Enter **NTP Server**.
10. Select the **Time Zone** from the drop-down.

	<p>NOTE:</p> <p>By default Wireless Scans will be disabled.</p>
---	---

11. In **Wireless Scans** enable the **Scheduled Beam Adjustment** and configure **Scan Interval** as required.

The screenshot shows the configuration page for a 60 GHz cnWave Network. The 'Wireless Scans' section is expanded, showing 'Scheduled Beam Adjustment' set to 'Enabled' and 'Scan Interval' set to 18000. Other sections include 'Prefix Allocation', 'Layer 2 Bridge', 'IPv6 Layer 2 CPE Address', 'CPE Prefix Zoning', and 'Time Zone'.

12. Click **Save**.

Management

Management configuration allows user to configure and manage the credentials of the administrator and it allows enable **SNMP**.

1. Navigate to **Configuration > Management** to set the **Device GUI Passwords** and to enable the **SNMP**.

60 GHz cnWave Network > 4-Nodes-Onboard-Godavari

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic **Management** Security Advanced E2E Controller

Device GUI Users

Admin User Password

Installer User Password

Monitor User Password

SNMP

Enable SNMP

System Contact

No Contact

System Location

No Location

Community

SNMP community string

Address

Allowed IPv6 source address or prefix

SNMPv3 User

SNMPv3 Security Level

None Authentication Only Authentication & Privacy

Authentication type

MD5 SHA SHA-512 SHA-384 SHA-256 SHA-224

Authorization Key

Privacy Protocol

DES AES

Privacy Key

Privacy (encryption) passphrase

Save Reset

2. Click **Save**.

Security

Security page allows the user to enable the wireless security **PSK** or **802.1x**. Disabling option unsecure the devices.

To Enable PSK :

1. Navigate to **Configuration > Security** tab.
2. Select **PSK** in **Wireless Security**.

60 GHz cnWave Network > 4-Nodes-Onboard-Godavari

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management **Security** Advanced E2E Controller

Wireless Security

Disabled PSK 802.1x Enable wireless security and set the method

Passphrase

..... WPA pre-shared key, in ASCII passphrase format (8-63 characters). If blank, default psk key will be used.

Save Reset

3. Enter the **Passphrase**.

**NOTE:**

If passphrase is left blank, default psk_key will be used.

4. Click **Save**.**To Enable 802.1x**

1. Navigate to **Configuration > Security**.
2. Select **802.1x** in **Wireless Security**.

60 GHz cnWave Network > 4-Nodes-Onboard-Godavari

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management **Security** Advanced E2E Controller

Wireless Security

Disabled PSK 802.1x Enable wireless security and set the method

Radius server IP IP address of auth (i.e, radius) server

Radius server port Auth server port

Radius server shared secret

3. Enter the **Radius server IP**.
4. Enter the **Radius server port**.
5. Enter the **Radius server shared secret**.
6. Click **Save**.

Advanced

Advanced tab allows the advanced user to edit the settings of the **Table** and **JSON** format of the E2E Controller.

It also allows to optimize the network using the following options:

- Optimize Control Superframe Allocation
- Optimize DPA Zone Allocation
- Clear Node Auto Configuration

60 GHz cnWave Network > 60 GHz cnWave External E2E-232

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Security **Advanced** E2E Controller

All the settings below are for advanced users only.

Base: default Firmware: 13.9.0 Hardware: v1000

Field	Description	Status	
logTailParams.sources.terragraph_opem_logs.enabled	Enable tailing from this source.	set	✓
logTailParams.sources.terragraph_opem_logs.filename	The log file name.	set	✓
logTailParams.sources.terragraph_minion_logs.filename	The log file name.	set	✓
logTailParams.sources.terragraph_minion_logs.enabled	Enable tailing from this source.	set	✓
logTailParams.sources.terragraph_kern_logs.filename	The log file name.	set	✓
logTailParams.sources.terragraph_kern_logs.enabled	Enable tailing from this source.	set	✓
popParams.NAT64_POP_ENABLED	Enable NAT64 on POP interface for IPv6 <-> IPv4 NAT.	set	✓
popParams.NAT64_IPV6_PREFIX	NAT64 IPv6 prefix. Can use 64:95b::96 (well known prefix).	unset	✓
popParams.NAT64_IPV4_ADDR	IPv4 Address for NAT64 interface.	unset	✓
snmpConfig.location	System location.	set	✓
snmpConfig.contact	System contact.	set	✓

Device Logs

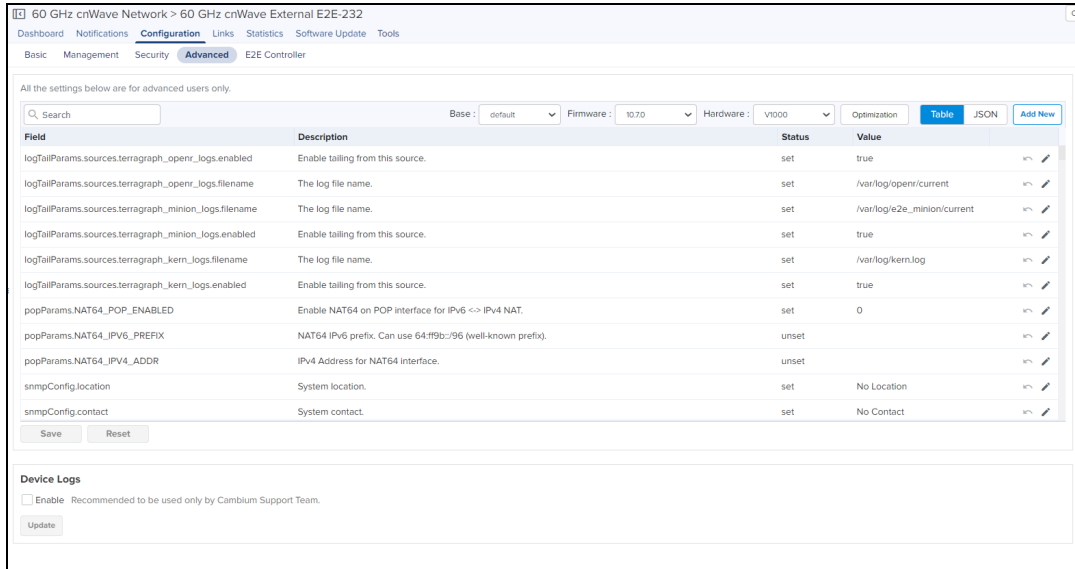
Enable Recommended to be used only by Cambium Support Team.

Table

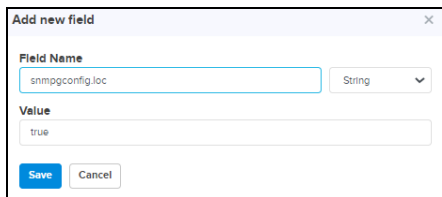
In the **Table** advanced user can able to view, add, and edit **Field Name** and **Value**.

To add a field:

1. Navigate to **Configuration > Advanced**.
2. Click **Add New**.



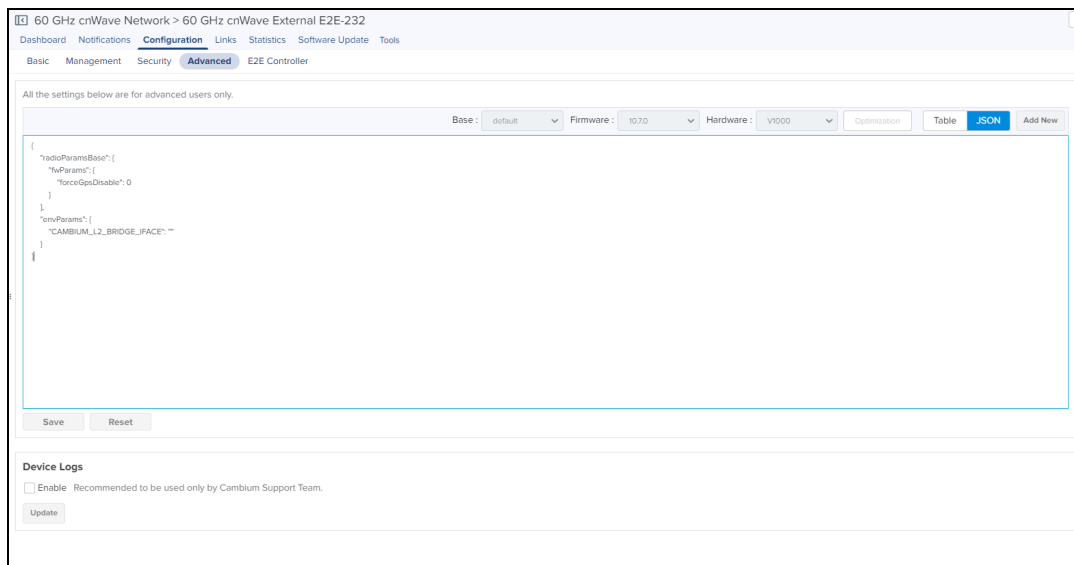
3. Enter the **Field Name** and **Value**.



4. Click **Save**.

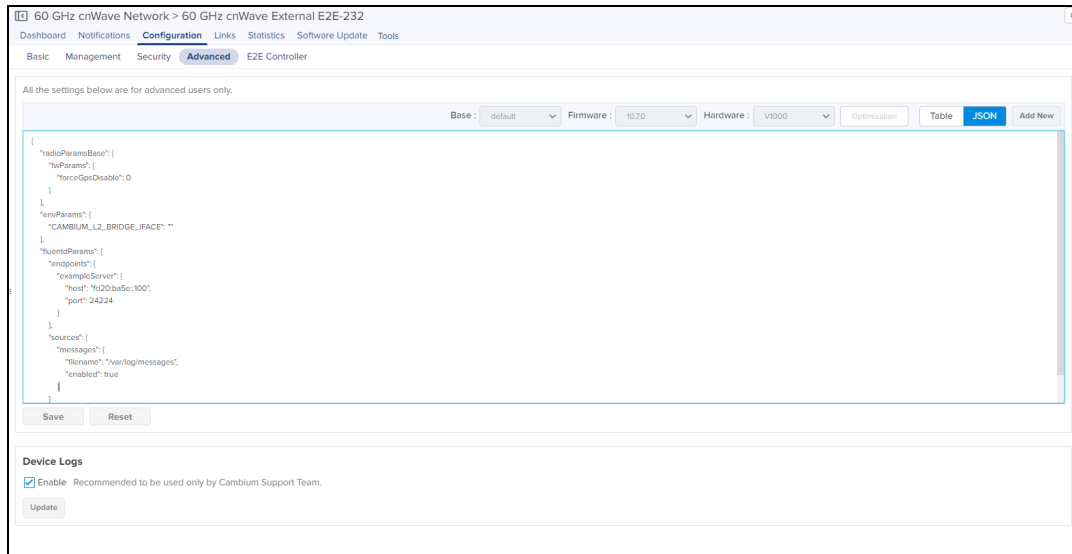
JSON

JSON allows Advanced user can view and edit 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 can view the logs.

2. Enable **Device Logs**.
3. Click **Update**.

E2E Controller

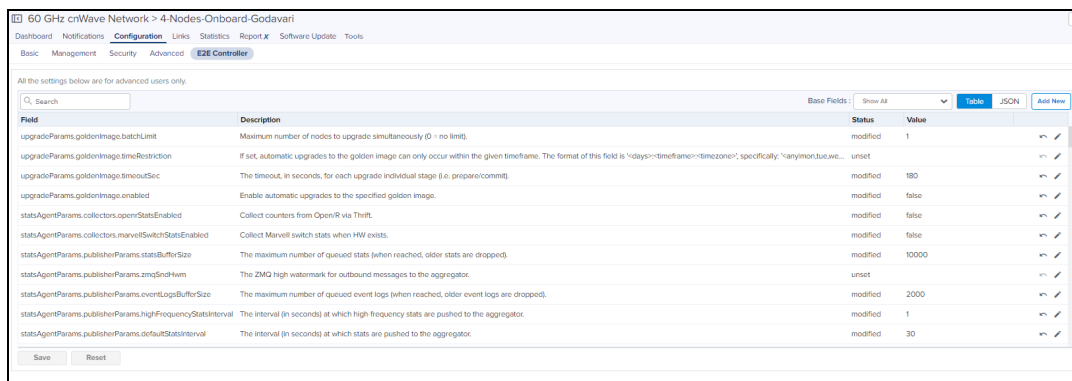
E2E Controller allows the advanced user to set the **Table** and download the **JSON** file.

Table

In **E2E Controller Table** user can view, edit and 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**.



Add new field [X]

Field Name String [v]

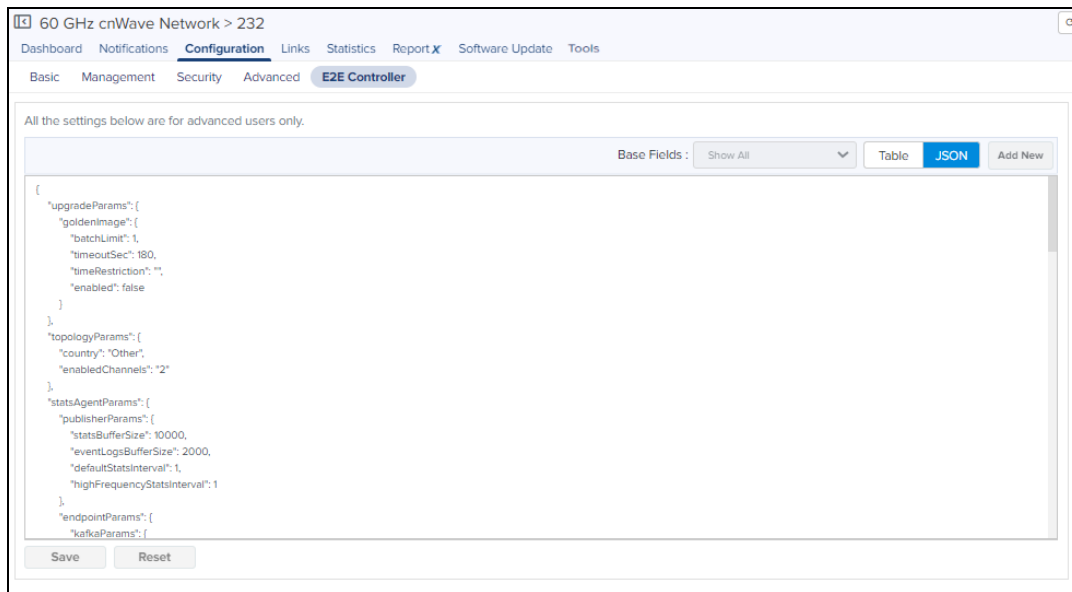
Value

[Save] [Cancel]

4. Click **Save**.

JSON

JSON allows Advanced user to view and edit json format.



60 GHz cnWave Network > 232

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Security Advanced **E2E Controller**

All the settings below are for advanced users only.

Base Fields: Show All [v] Table **JSON** Add New

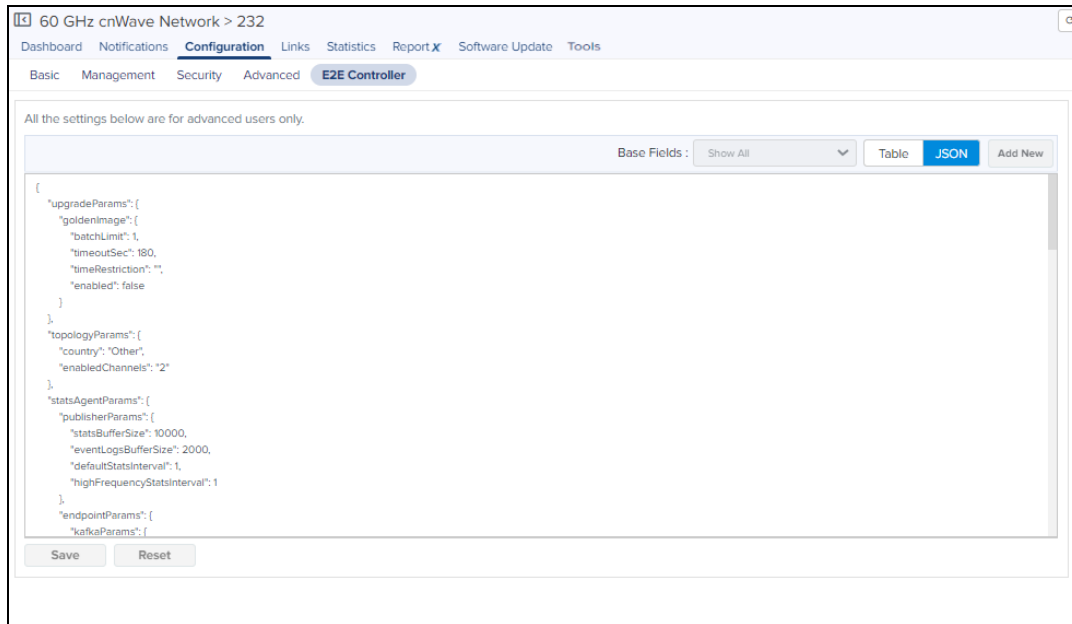
```
{
  "upgradeParams": {
    "goldenImage": {
      "batchLimit": 1,
      "timeoutSec": 180,
      "timeRestriction": "",
      "enabled": false
    }
  },
  "topologyParams": {
    "country": "Other",
    "enabledChannels": "2"
  },
  "statsAgentParams": {
    "publisherParams": {
      "statsBufferSize": 10000,
      "eventLogBufferSize": 2000,
      "defaultStatsInterval": 1,
      "highFrequencyStatsInterval": 1
    }
  },
  "endpointParams": {
    "kafkaParams": {

```

[Save] [Reset]

To view or edit the JSON file:

1. Navigate to **Configuration > E2E Controller > JSON**



Links



NOTE:

Backup CN Link option gets enabled when E2E controller is running on Version 1.1.

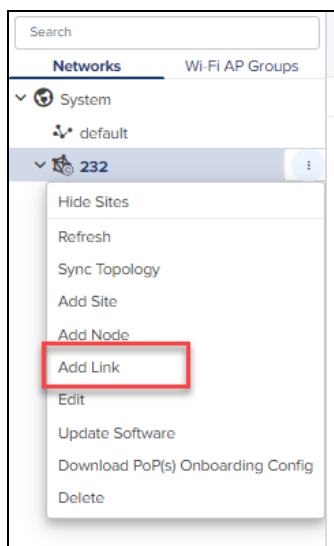
Links provide the details about the link established between the nodes and also provides the option to create a new Wireless, Statistics, Events, Wired and CN backup link.

- [List](#)
- [Statistics](#)
- [Events](#)

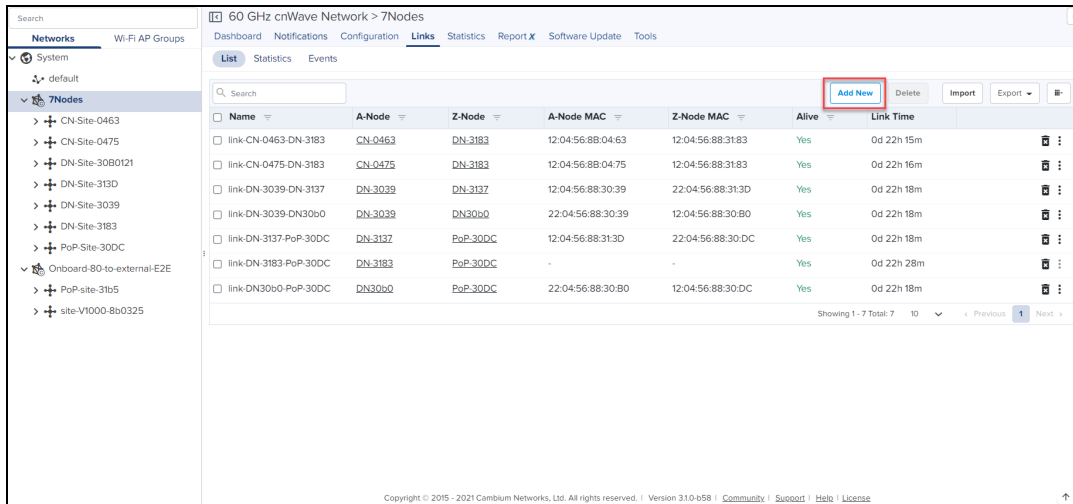
List

To add a link:

1. Navigate to the E2E Network tree menu click  icon and select **Add Link** or

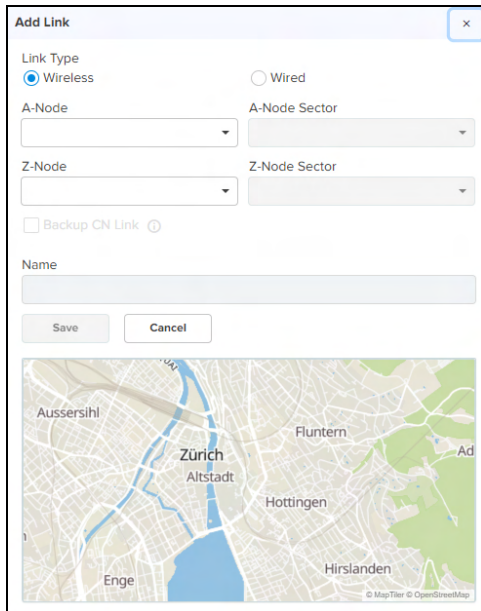


Navigate to **Network > Links > List > Add New.**



Add Link window pops-up.

Figure 94 Wireless

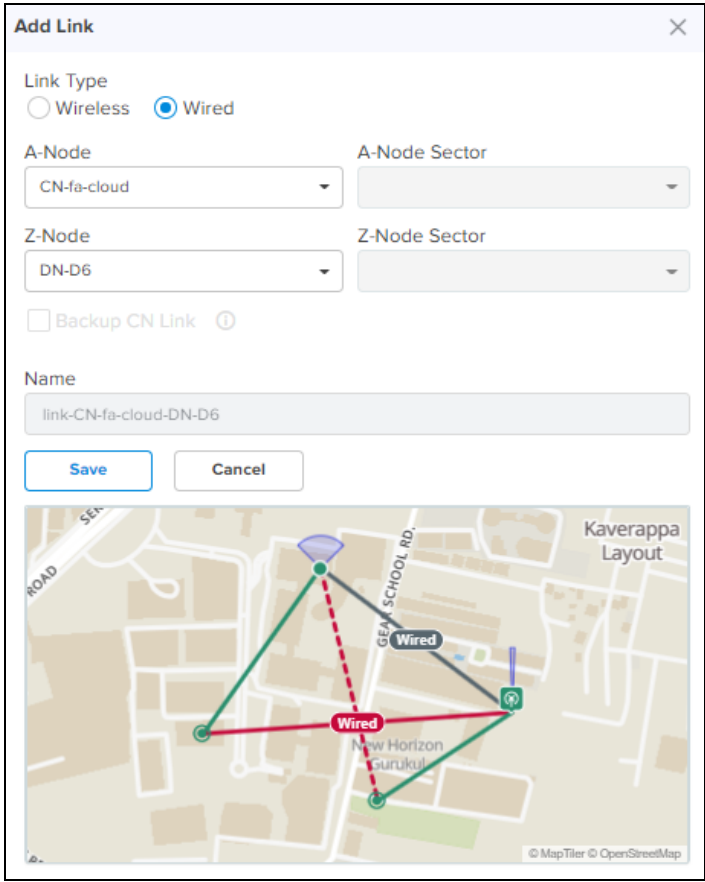


2. Select **Link Type** Wireless or Wired.

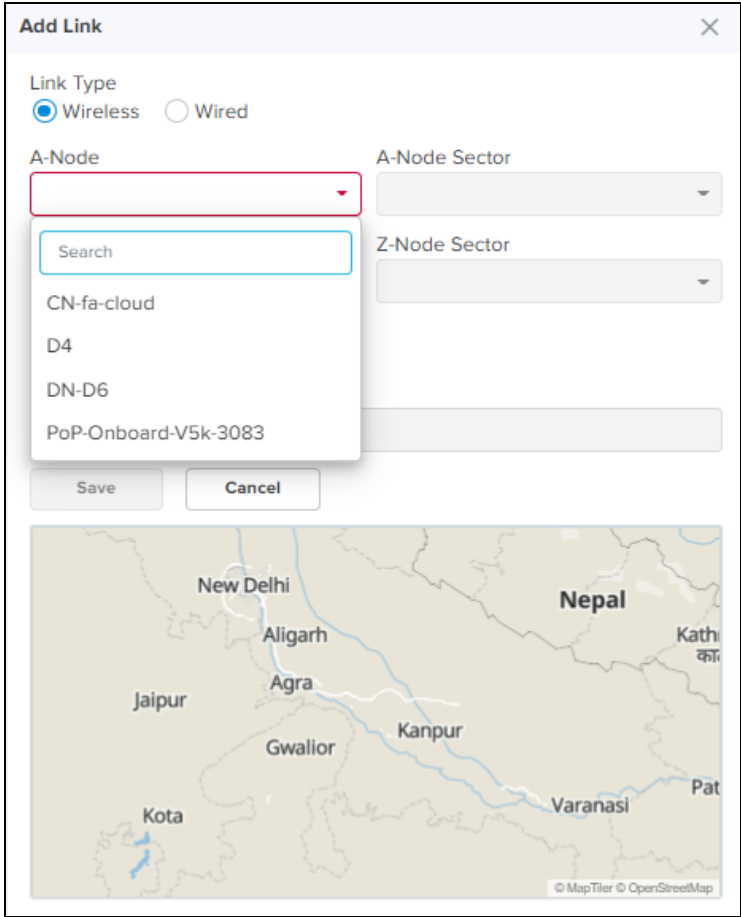
Figure 95 Wired

NOTE:

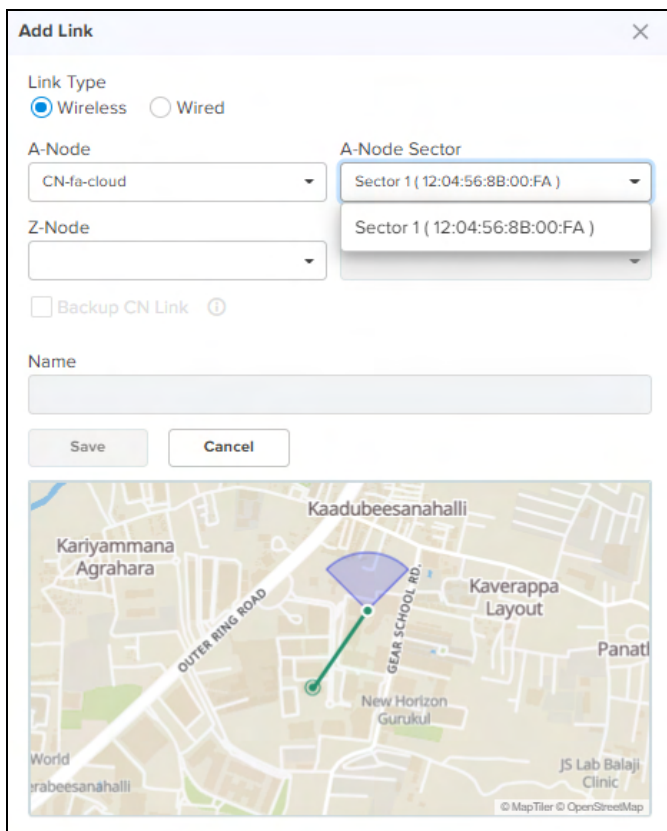
In Wired Link Type Sector will be disabled.



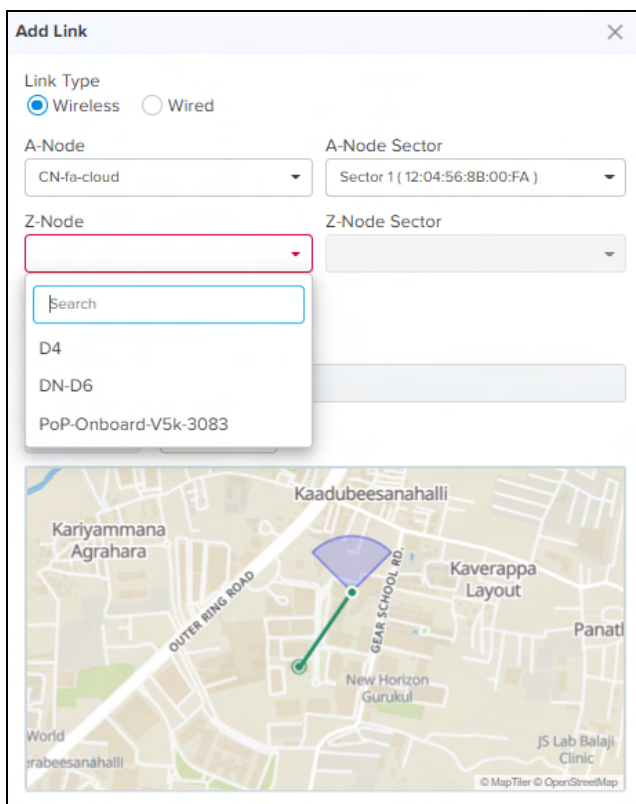
3. Select the **Node** from the drop-down in **A-Node**.



4. Select the **Sector** of the node from the drop-down in **A-Node Sector**.



5. Select the **Node** from the drop-down in **Z-Node**.



6. Select the **Sector** of the node from the drop-down in **Z-Node Sector**.

Add Link ✕

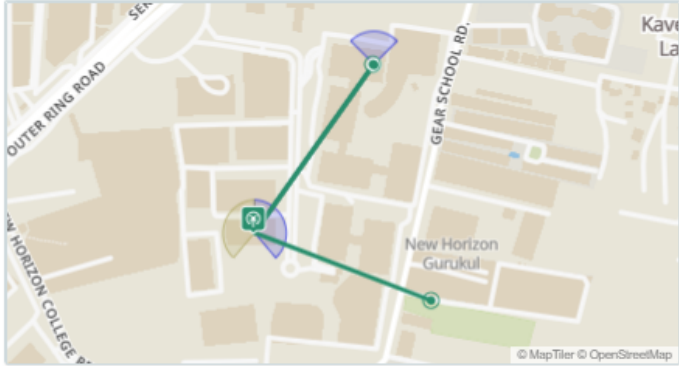
Link Type
 Wireless Wired

A-Node: CN-fa-cloud A-Node Sector: Sector 1 (12:04:56:8B:00:FA)

Z-Node: D4 Z-Node Sector: Sector 1 (12:04:56:88:38:D4)

Backup CN Link ⓘ

Name
 link-CN-fa-cloud-D4



NOTE:

. Backup CN link is optional.

7. Enable the **Backup CN Link**.

- If the link between PoP or DN and CN gets disconnected. This Backup CN link provides the backup connectivity from DN or PoP to particular CN.

Add Link ✕

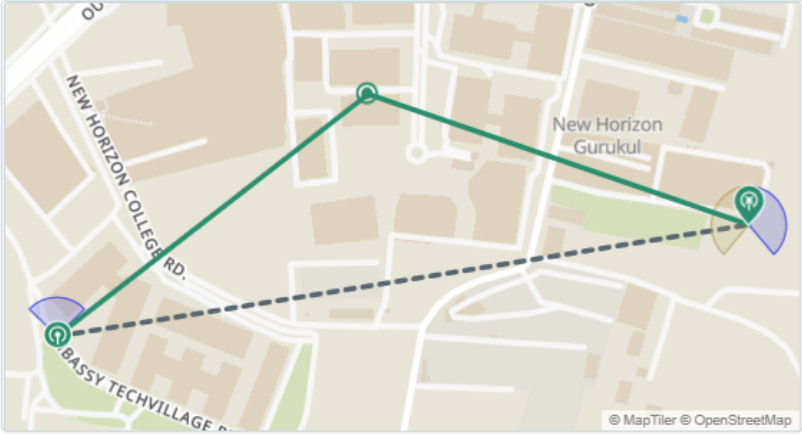
Link Type
 Wireless Wired

A-Node: A-Node Sector:

Z-Node: Z-Node Sector:

Backup CN Link ⓘ

Name:



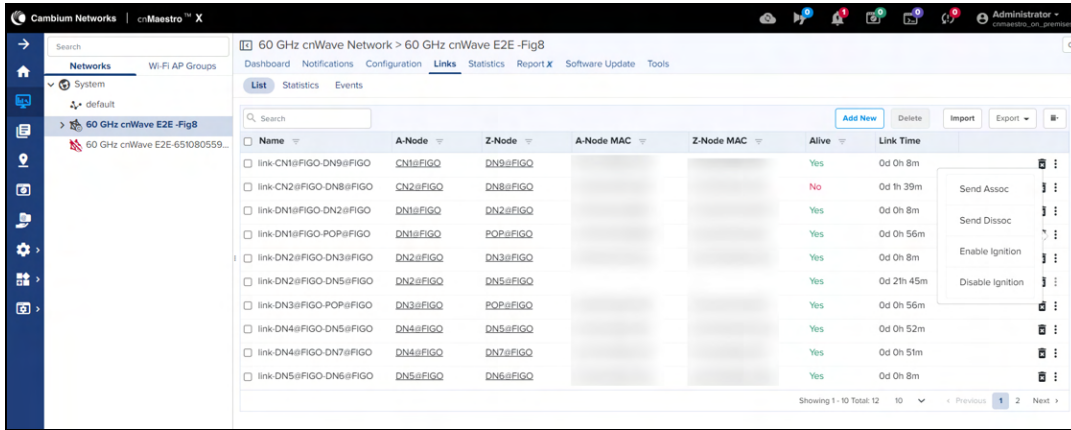
8. Click **Save**.
9. Once the link is successful it displays the **Alive** status as **Yes**.

60 GHz cnWave Network > 4Nodes-Onboard							
Dashboard Notifications Configuration Links Statistics Report X Software Update Tools							
List Statistics Events							
<input type="text" value="Search"/> <input type="button" value="Add New"/> <input type="button" value="Delete"/> <input type="button" value="Import"/> <input type="button" value="Export"/> 							
<input type="checkbox"/>	Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	Link Time
<input type="checkbox"/>	link-CN fa cloud D4	CN fa cloud	D4	12:04:56:88:00:FA	22:04:56:88:38:D4	Yes	0d 12h 42m
<input type="checkbox"/>	link-D4 PoP-Onboard-V5k-3083	D4	PoP-Onboard-V5k-3083	12:04:56:88:38:D4	22:04:56:88:30:83	Yes	42d 16h 53m
<input type="checkbox"/>	link-DN-D6-PoP-Onboard-V5k-3083	DN-D6	PoP-Onboard-V5k-3083	12:04:56:88:30:D6	12:04:56:88:30:83	Yes	42d 16h 53m


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

Available link options are:

- Send Assoc
- Send Dissoc
- Enable Ignition
- Disable Ignition

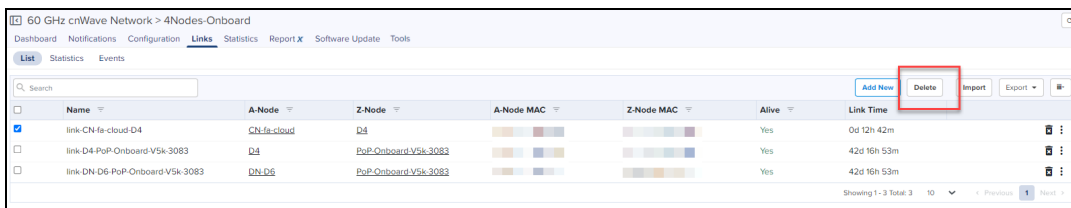


Delete Links

In **Links** tab you can delete the each individual links by clicking  delete icon or multiple links can be deleted by selecting the links and click delete.

To delete the links:

1. Navigate to **Links > List**.
2. Select the links to delete.



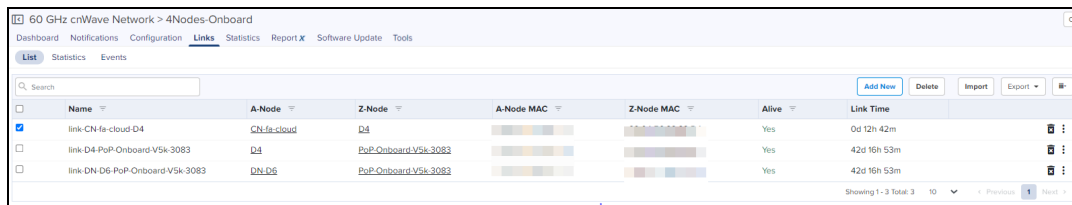
3. Click **Delete**.

Import Links

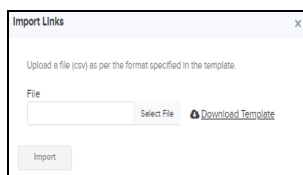
In **Links** tab you can import the E2E Controller Network Links.

To import the links:

1. Navigate to **Links > List**.
2. Select **Import**.



Import Links pops up.



3. Click **Download Template** to download the .CSV format file.

	A	B	C	D	E
1	A_NODE_NAME	A_NODE_MAC	Z_NODE_NAME	Z_NODE_MAC	LINK_TYPE
2	A node name of the device	Sector 1/2 MAC Address	Z node name of the device	Sector 1/2 MAC Address	Wireless or Wired
3	POP	12:04:56:44:55:66	DN1	22:04:56:33:44:55	wireless
4	DN1	12:04:56:33:44:55	CN1	12:04:56:11:22:33	wireless
5	DN1		CN2		wired
6					
7					

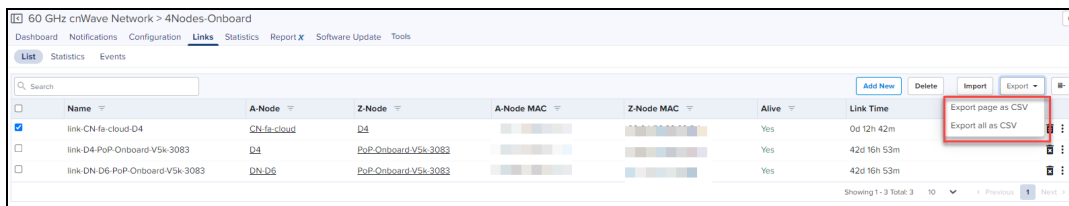
4. Select the file and click **Import**.

Export Links

In **Links** tab you can export the E2E Controller Network Links.

To export the links:

1. Navigate to **Links > List > select Export**.



2. It exports .csv file format as shown below.

1	A_NODE_NAME	A_NODE_MAC	Z_NODE_NAME	Z_NODE_MAC	LINK_TYPE
2	A node name of t	Sector 1/2 MAC	Z node name of t	Sector 1/2 MAC	Wireless or Wired
3	CN-2c	12:04:56:8B:00:0	pop	12:04:56:AA:BB	Wireless
4	CN	12:04:56:AA:BC	DN2	12:04:56:88:30	Wireless
5	DN	22:04:56:AA:BB	DN2	12:04:56:88:30	Wireless
6	DN	12:04:56:AA:BB	pop	22:04:56:AA:BB	Wireless
7	DN2	22:04:56:88:30	dn-44	12:04:56:88:31	Wireless
8	DN2	22:04:56:88:30	v3000	12:04:56:88:30	Wireless
9	dn-44	22:04:56:88:31	pop	12:04:56:AA:BB	Wireless

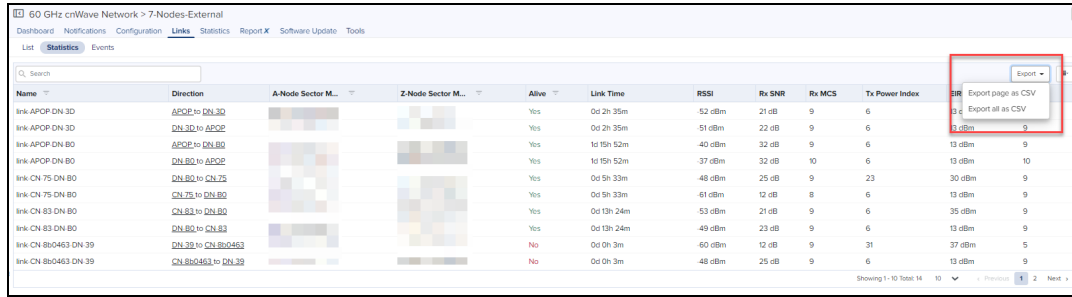
Statistics

Links Statistics pages provides details of Name, Direction, A-Node Sector MAC, Z-Node Sector MAC, Alive, Link Time, RSSI, Tx Power Index, A-node, Z-node, Type, Distance, Azimuth, Rx MCS, Tx MCS, Rx PER, Tx PER, Rx SNR, Tx SNR, Rx Beam Index, Tx Beam Index, EIRP, Rx Errors, Tx Errors, Rx Frames, Tx Frames on a single link of the node, generally in a page format.

Export Statistics

To export the Statistics :

1. Navigate to **Links > List > > select Export**.



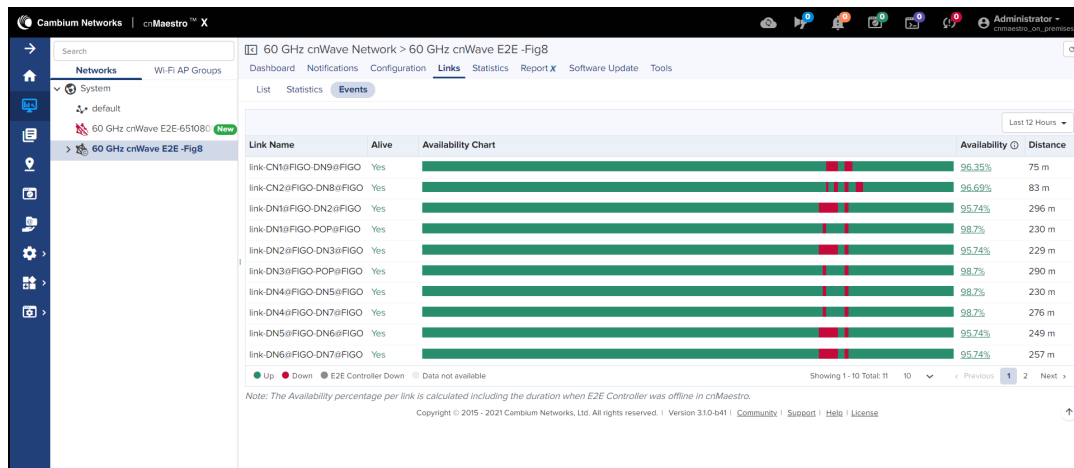
2. It exports .csv file format as shown below.

LINK_NAME	DIRECTION	A_NODE_ID	Z_NODE_ID	A_NODE_ID	Z_NODE_ID	ALIVE	TYPE	DISTANCE	AZIMUTH	RSSI	Rx_SNR	Rx_MCS	Rx_PER	Rx_BEAM	Tx_POWER	Rx_FRAME					
link-APOP-DN-3D	APOP to DN-3D	APOP	DN-3D	22:04:56:8	22:04:56:8	Yes	Wireless	147	83	-51	22	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	22:04:56:8	Yes	Wireless	147	83	-51	22	9	0.2	84	6	13	9	0.21	84	374	1488
link-APOP-DN-80	APOP to DN-80	APOP	DN-80	12:04:56:8	22:04:56:8	Yes	Wireless	94	-178.1	-40	32	9	0	32	6	13	9	0	35	92	30630
link-APOP-DN-80	DN-80 to APOP	APOP	DN-80	12:04:56:8	22:04:56:8	Yes	Wireless	94	-178.1	-37	32	10	0	6	13	10	0	0	1332	9183	443425
link-CN-75-DN-80	DN-80 to CN-75	DN-80	DN-80	12:04:56:8	22:04:56:8	Yes	Wireless	171	-151.2	-48	25	9	0.31	0	23	30	9	0.38	0	0	0
link-CN-75-DN-80	CN-75 to DN-80	DN-80	DN-80	12:04:56:8	22:04:56:8	Yes	Wireless	171	-151.2	-61	12	8	0.42	0	6	13	9	0.35	0	1944	443425
link-CN-83-DN-80	DN-80 to CN-83	DN-80	DN-80	12:04:56:8	22:04:56:8	Yes	Wireless	71	52.7	-53	21	9	0.81	58	6	35	9	0.06	58	385	2043
link-CN-83-DN-80	CN-83 to DN-80	DN-80	DN-80	12:04:56:8	22:04:56:8	Yes	Wireless	71	52.7	-49	23	9	0.04	112	6	13	9	0.08	112	0	339
link-CN-80463-D	DN-39 to CN-80463	DN-39	CN-80463	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	2896
link-CN-80463-D	CN-80463 to DN-39	DN-39	CN-80463	12:04:56:8	22:04:56:8	No	Wireless	199	-45.2	-48	25	9	0.04	45	6	13	9	0.56	45	54	62
link-DN-39-DN-3D	DN-39 to DN-3D	DN-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-39	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	164	232	
link-DN-39-DN-80	DN-80 to DN-39	DN-39	DN-80	22:04:56:8	12:04:56:8	Yes	Wireless	100	-70.5	-45	28	9	0.06	35	6	13	9	0.02	34	73	567
link-DN-39-DN-80	DN-39 to DN-80	DN-39	DN-80	22:04:56:8	12:04:56:8	Yes	Wireless	100	-70.5	-48	25	9	0.3	55	6	13	10	0.01	54	331	303

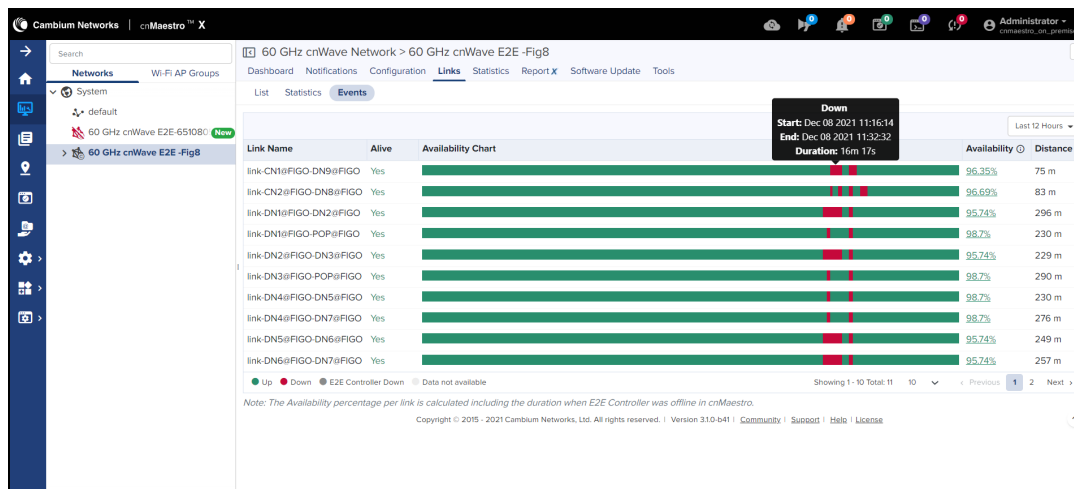
Events

Events provides the details of links availability and health from last 1 hour to 7 Days Period.

Figure 96 Links Events



It also calculates the Availability percentage per link, including the duration when E2E Controller was offline in cnMaestro.



Statistics

E2E Controller Statistics provides the following details:

- [Nodes Statistics](#)
- [BGP](#)

Nodes 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 information of **Device, IPv6 Address, Mode, Model, Status, Status Time, Site, Radio channel, Main Aux SFP, PoP Node, Software Version, Serial Number, Sync Mode, Zone, Fix Type, Satellites Tracked, Latitude, Longitude, and Height** on a single device, generally in a page format.

Figure 97 Nodes Statistics

Device	IPv6 Address	Mode	Model	Status	Status Time	Site	Sync Mode	Radio Channel	Main Aux SFP	PoP Node	Fix Type	Satellites Tracked	Latitude
CN1a	fd00::ceed:8830:8300::1	CN	V1000	Online	0d 6h 15m	S1	RF	4	⊙	⊙	No	-	-
DN-D4	fd00::ceed:8830:8303::1	DN	V5000	Online	0d 6h 18m	S3	RF	4.4	⊙	⊙	3D	9	12.934256
DN-d6	fd00::ceed:8830:8301::1	DN	V3000	Online	0d 6h 18m	S2	RF	2	⊙	⊙	No Fix	-	-
node-V5000-883083	fd00::ceed:8830:8302::1	DN	V5000	Online	0d 6h 18m	site-V5000-883083	RF	2.4	⊙	⊙	Yes	8	12.934008

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 Details of IPv6 Address.**

Figure 98 BGP

Peer	IPv6 Address	Status	ASN	Uptime
DN4@FIGO	8001::1	Online	65530	14m 27s
POP@FIGO	8001::1	Online	65530	12m 8s

Network	Next Hop
1 face:b00c::56	8001::3

Network	Next Hop
1 ::0	fe80::c6ad:34ff:fe45:a5b8
2 face:b00c:0:80::57	fe80::c6ad:34ff:fe45:a5b8

Network	Next Hop
1 face:b00c:0:80::57	8001::2
2 face:b00c::56	8001::2

Network	Next Hop
1 ::0	fe80::c6ad:34ff:fe45:a5b8
2 face:b00c::56	fe80::c6ad:34ff:fe45:a5b8

Reports


Reports page provides details on how to schedule and generate different types of data reports such as Devices, Active Alarms, Alarm History and Events. For further details, refer to [Reports](#).

Software Update

Allows the user to update with the latest device software.

To update the software, perform the below steps:

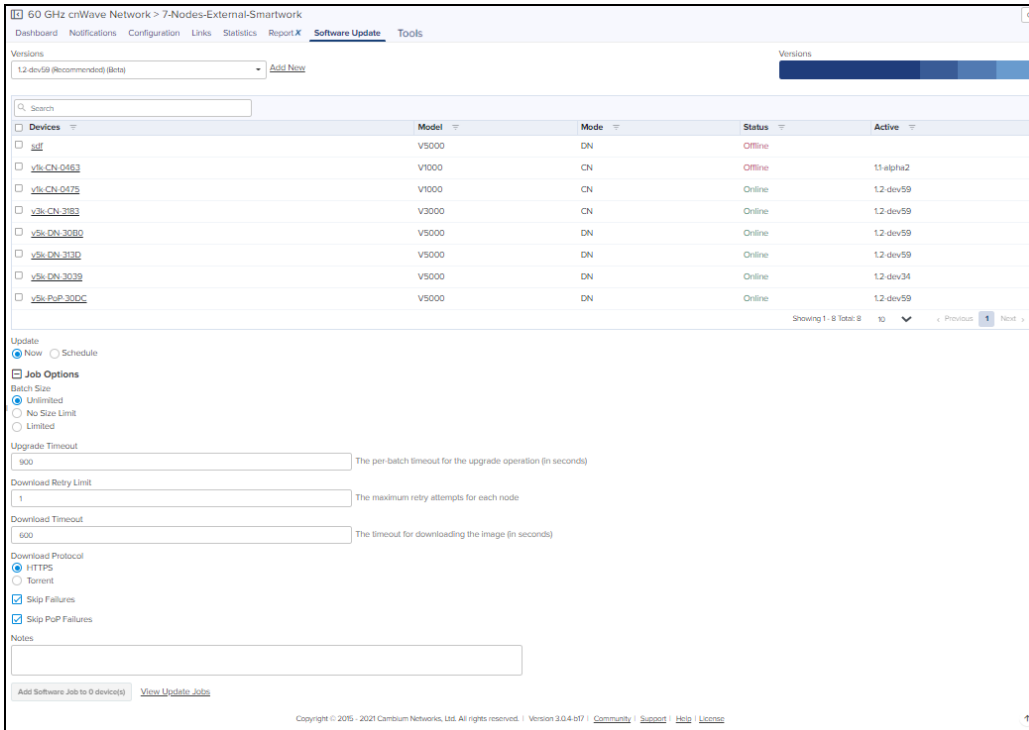
1. Select the **Network** and navigate to the **Software Update** tab.
2. In **Software Update** tab select the desired Versions from drop-down in **Versions** tab.
3. Select the **Device(s)** for the software update.
4. Click **Update Now** or **Schedule**.
5. In **Job options**:
 - Select type of **Batch Size** as Unlimited, No Size Limit, or Limited.
 - Enter **Upgrade Timeout**.
 - Enter **Download Retry Limit**.
 - Enter **Download Timeout**.
 - Select the Download Protocol as **HTTPS** or **Torrent**.




NOTE:
If E2E Controller version is 1.2 or above, HTTPS or Torrent options will be available.

- Enable the **Skip Failures** or **PoP Failures**.

6. Click **Add Software Job to device**.



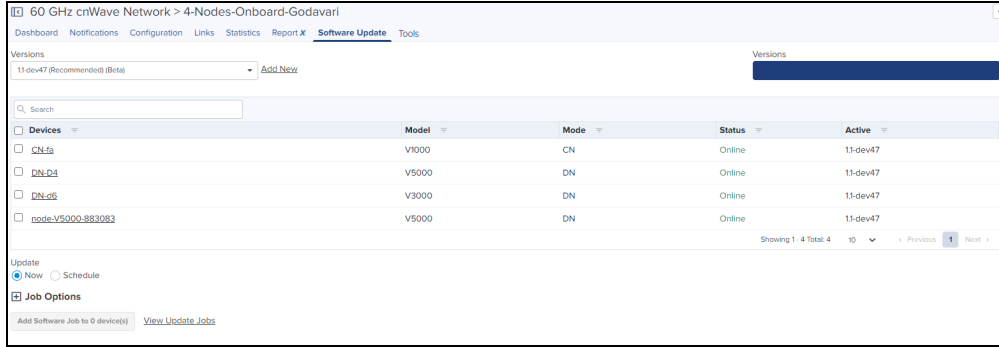
Devices	Model	Mode	Status	Active
all	V5000	DN	Offline	
v5k-CN-0463	V1000	CN	Offline	11-alpha2
v5k-CN-0475	V1000	CN	Online	1.2-dev59
v5k-CN-3163	V3000	CN	Online	1.2-dev59
v5k-DN-3080	V5000	DN	Online	1.2-dev59
v5k-DN-3130	V5000	DN	Online	1.2-dev59
v5k-DN-3009	V5000	DN	Online	1.2-dev34
v5k-PoP-3000C	V5000	DN	Online	1.2-dev59



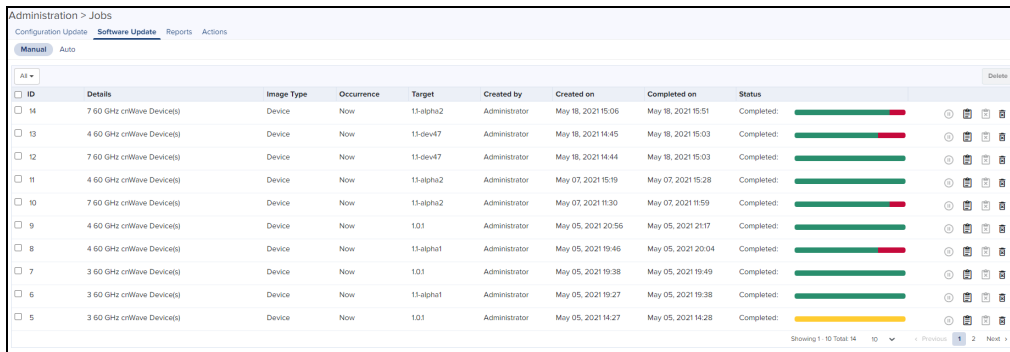
NOTE:
Onboard E2E controller will support only one synced software image. If user needs to sync another image, select the image from **Versions** drop down and click **Sync Selected Image**.

View Update Jobs

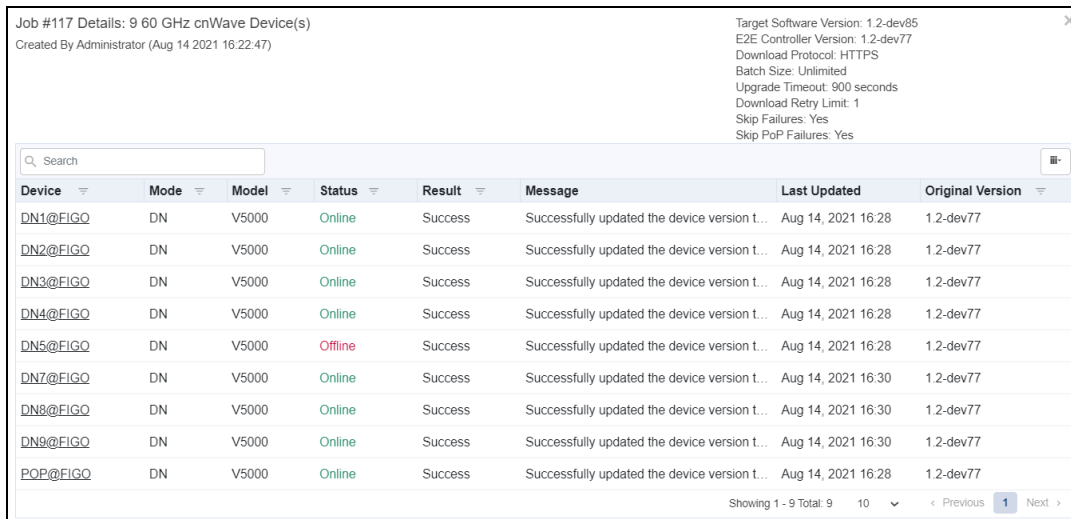
After adding the new Software Images, click **View Update Jobs**.



1. Navigate to the **Administration > Jobs > Software Update**.

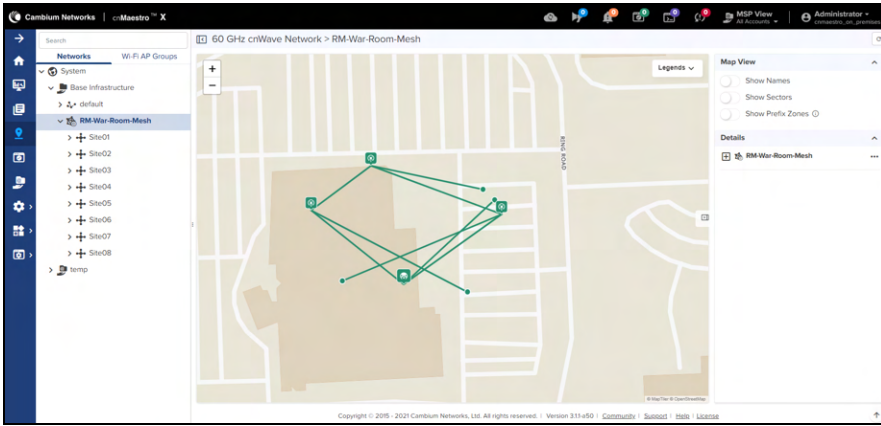


2. Click **Show More** to view the Job Details.

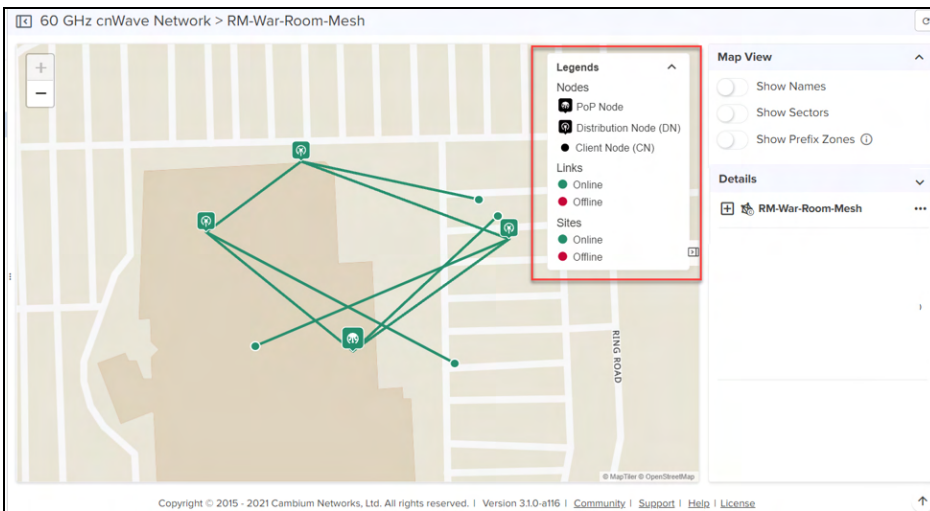


Map

User can view E2E Network and the 60 GHz cnWave devices in Map as shown below. Navigate to E2E Network and then select Map from left pane to view 60 GHz cnWave devices.



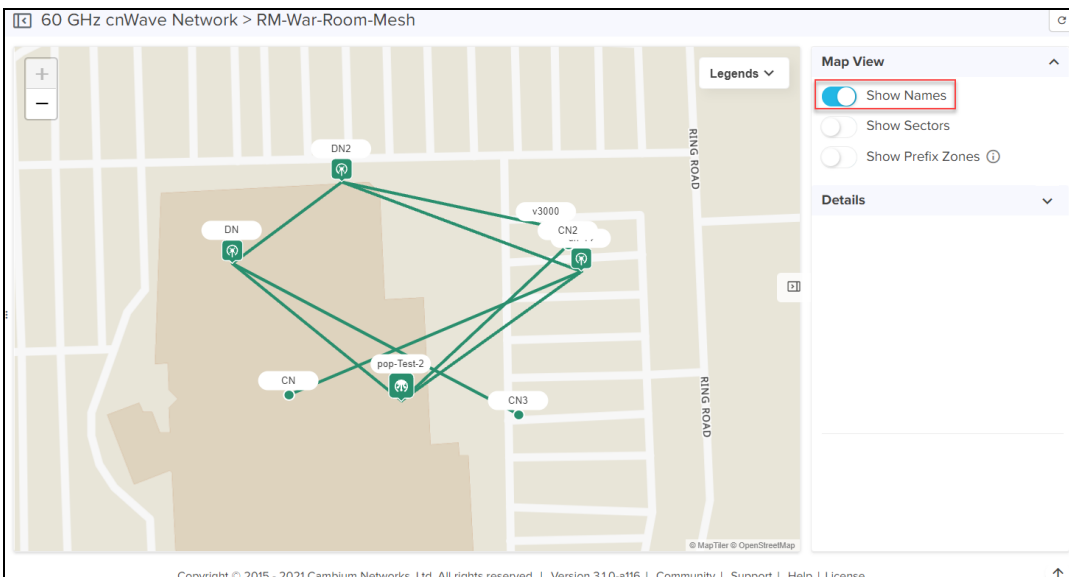
Click down arrow next to **Legends** to view the map legend.



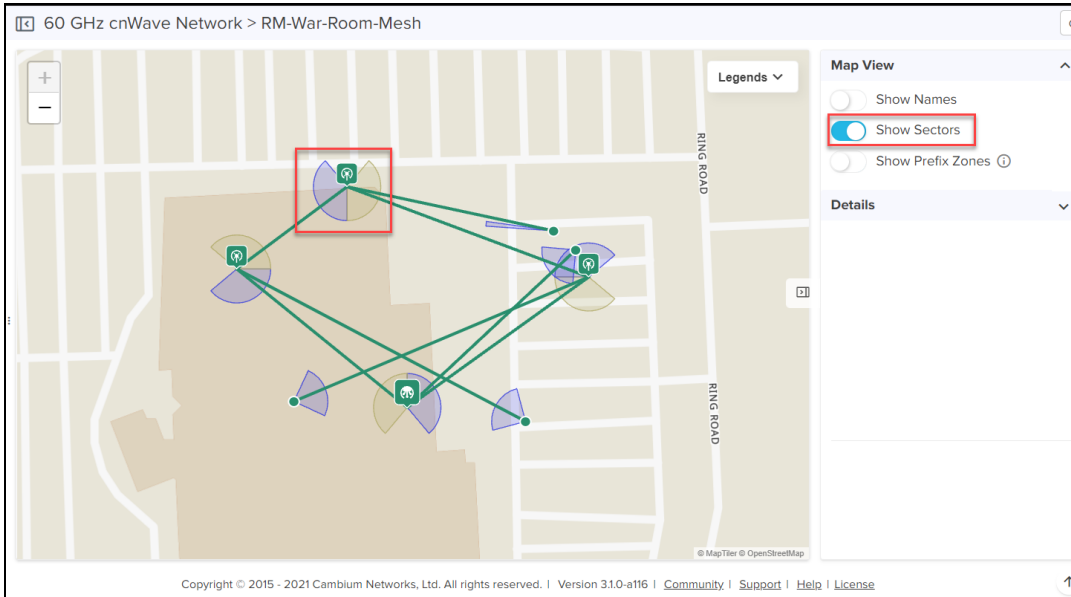
Map View

Map is viewed by **Names**, **Sectors**, and **Prefix Zones**. For **Map View** slide the button next to the field name as shown below.

- **Show Names** - shows the name of the nodes in the network.



- **Show Sectors** - shows the basic sector visualization of the nodes in the network.



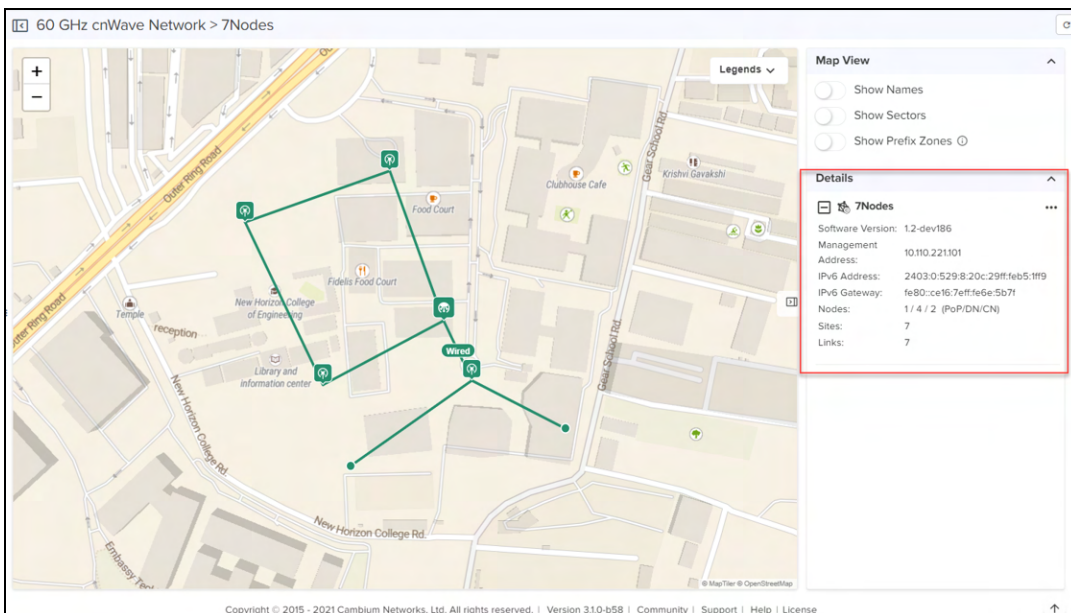
- **Show Prefix Zones** - shows the prefix zone of each PoP communicating with each other.

NOTE:

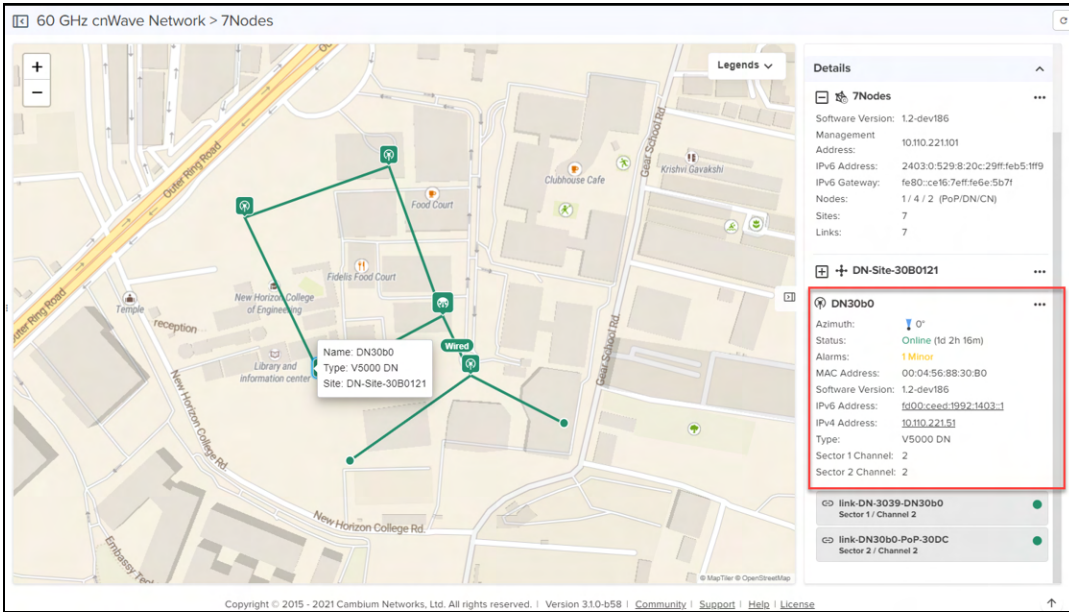
Show Prefix Zones is enabled only if **Prefix Allocation** is set to **Deterministic**.

E2E Network Details

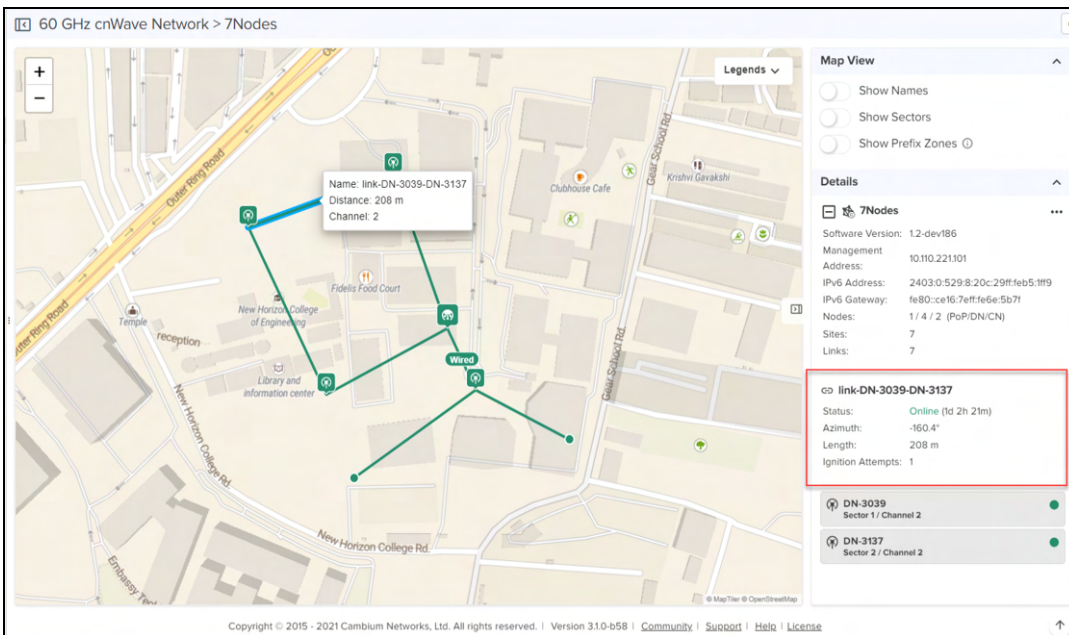
Click the down arrow next to **Details** to view E2E Network details in map. The following E2E Network details is as shown below.



Hover the cursor on the node, you can view the node **Name**, **Type**, and **Site**. Node details is shown when node is selected in the map. Node details is also shown in the right pane as shown below:



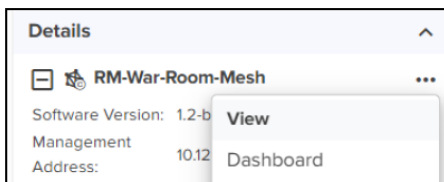
Hover the cursor on the links connected to the node, you can view the link **Name**, **Distance** and **Channel**. Link details is shown when link line in the map is selected. Link details is shown in the right pane as shown below:



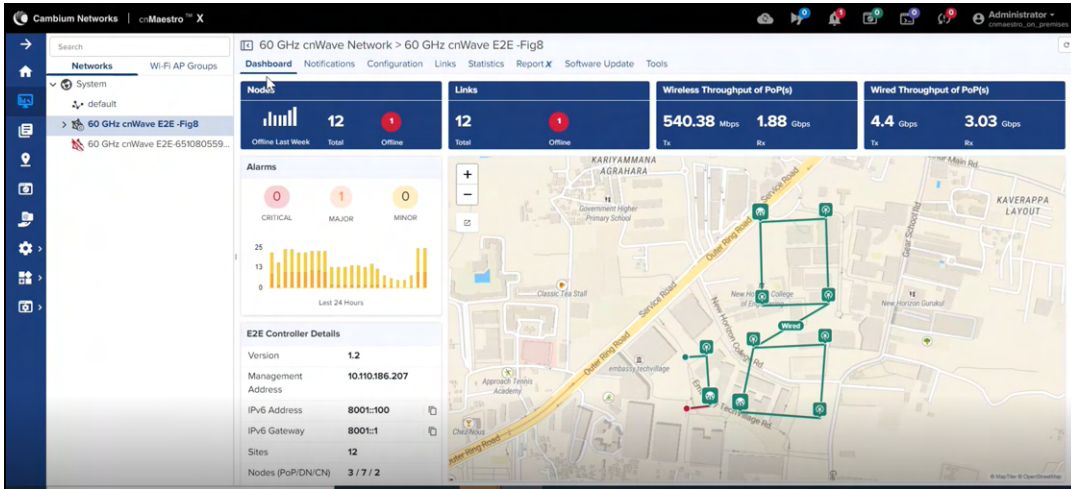
Links connected to nodes are represented in colors depending on the status of the link Green when Online or Red when Offline.

E2E Network Dashboard

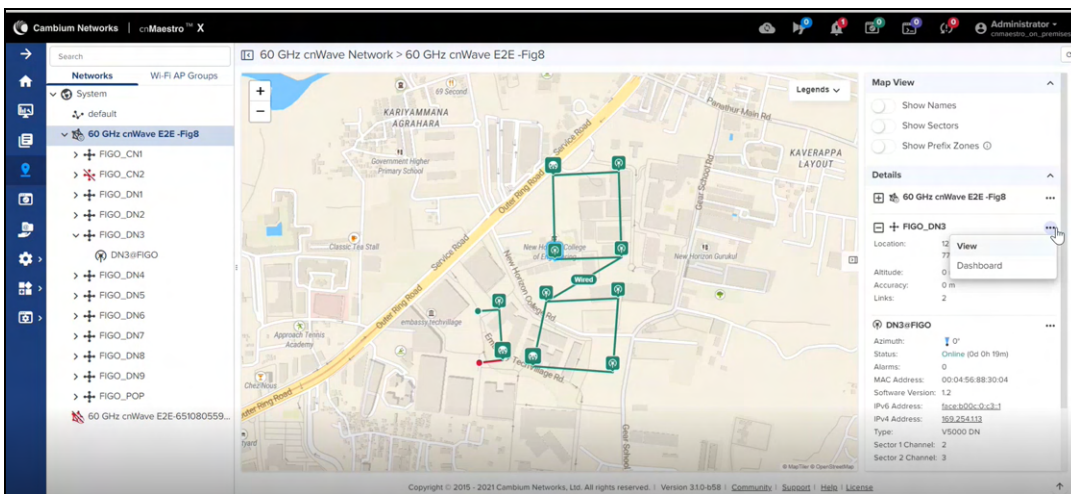
To view Dashboard of E2E Network click ... next to E2E Network in the right pane as shown below.



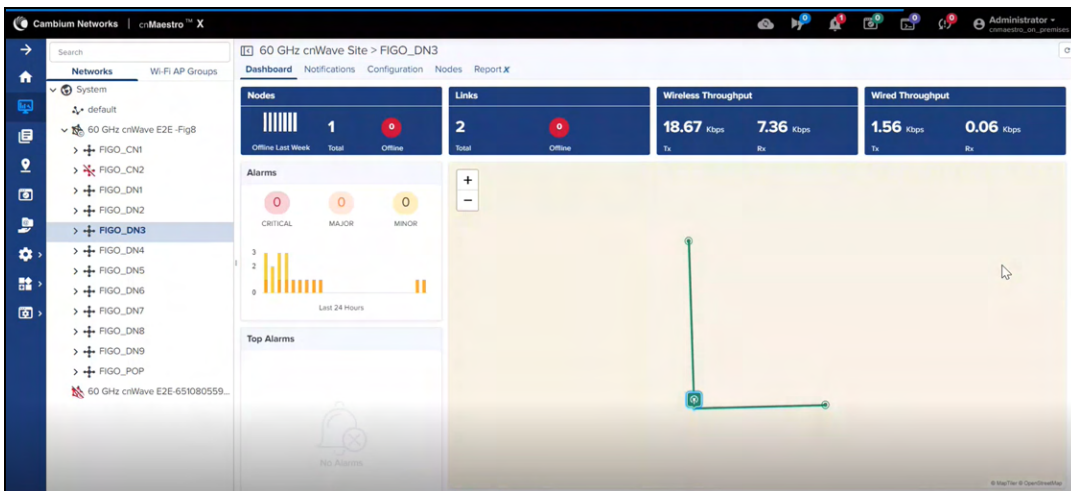
You will be directed to the 60 GHz cnWave Network Dashboard as shown below.



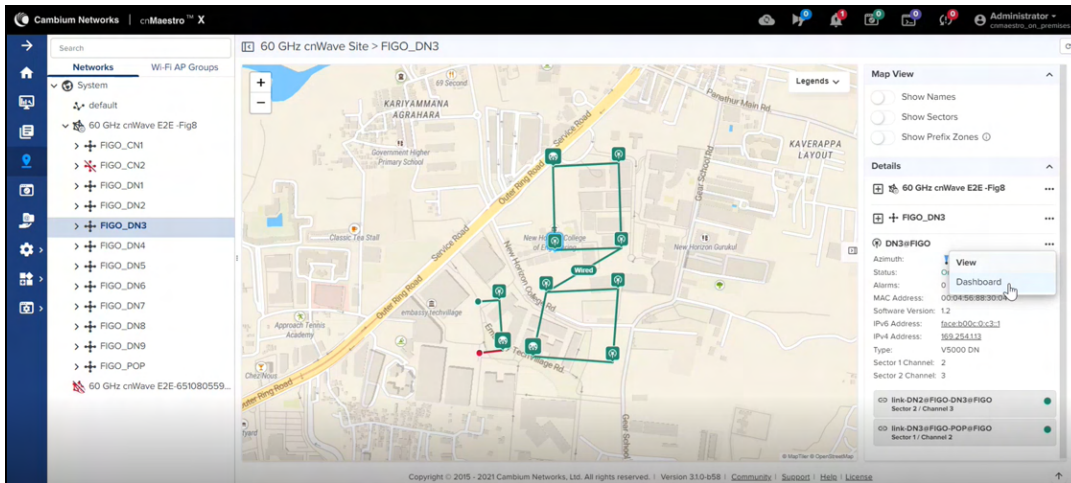
To view Dashboard of Site click **...** next to Site in the right panel as shown below.



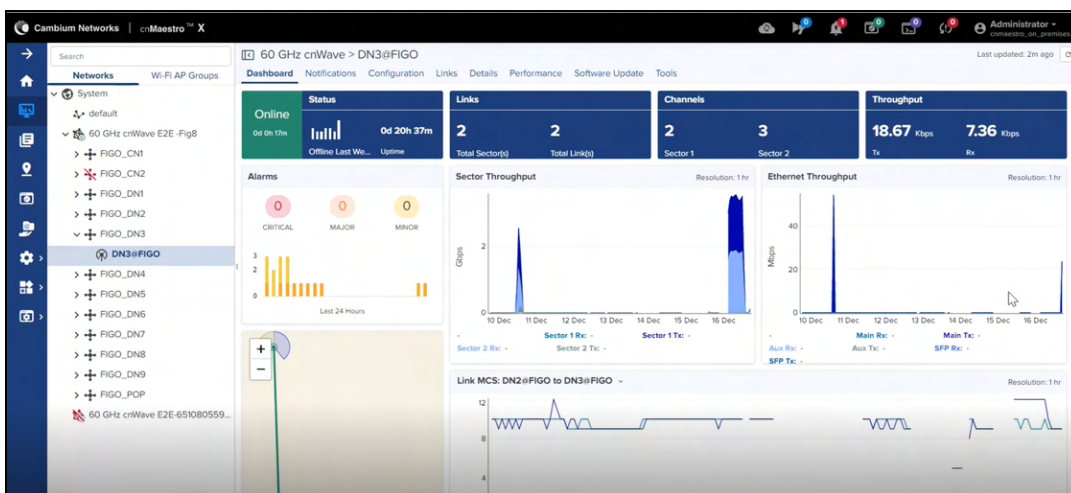
You will be directed to the 60 GHz cnWave Site Dashboard as shown below.



To view Dashboard of Device click **...** next to Device in the right pane as shown below.



You will be directed to the 60 GHz cnWave Device Dashboard as shown below.



Tools

In Tools page it allows the user to perform the following actions:

- [Operations](#)
- [Diagnostics](#)
- [Debug](#)
- [Remote Command](#)
- [Services](#)
- [Settings](#)

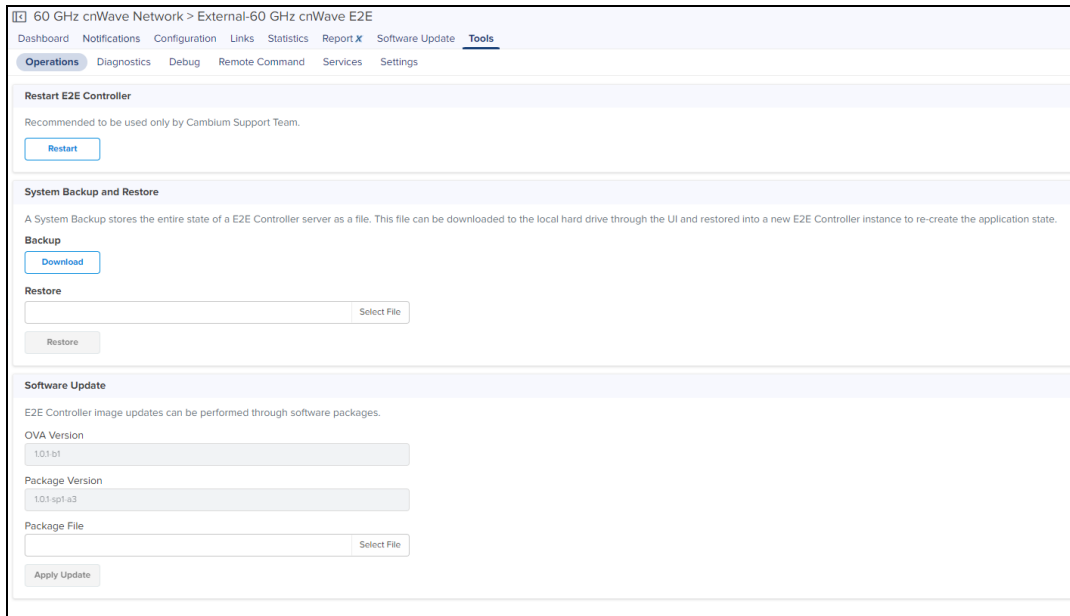
Operations

External E2E Controller deployment

If the nodes are 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.

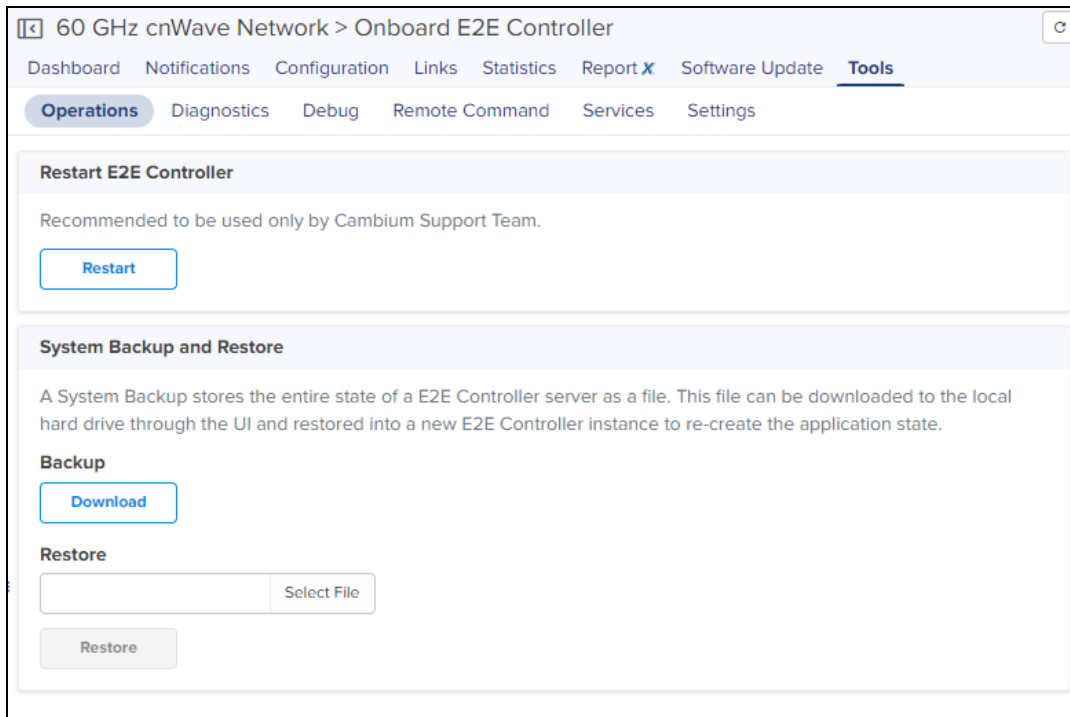
- The **Software Upgrade** is to upgrade E2E controller and can be done through E2E controller package.



Onboard E2E Controller deployment

If the nodes are running **Onboard E2E Controller** it displays the operations page as follows:

- **Restart E2E Controller** performs the **Restart**.
- A **System Backup and Restore** the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create.

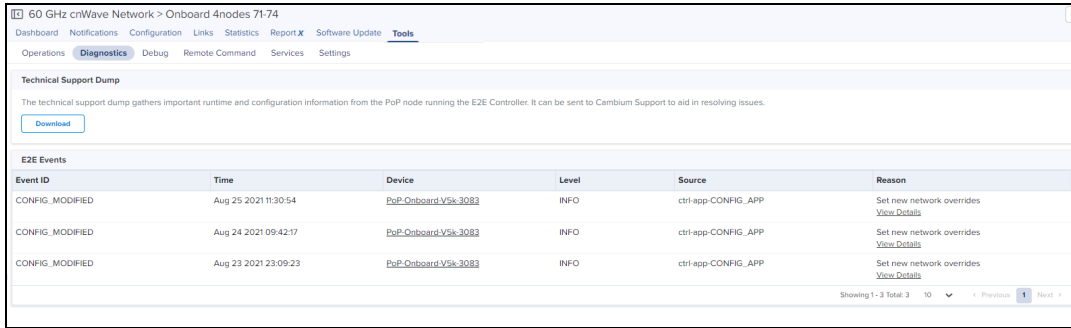


Diagnostics

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 99 Diagnostics



Debug

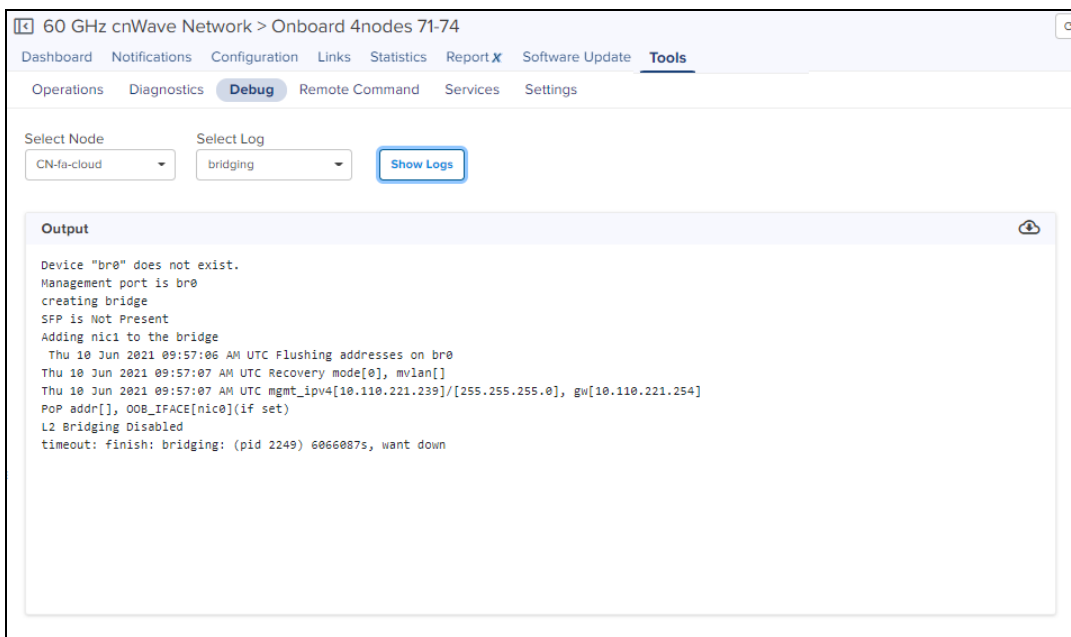
In **Debug** tab user can able to view or download the Node logs by executing the following log:


- bridging
- pop_config
- e2e_minion
- openr
- exabgp

To view the logs:

1. Navigate to **Tools > Debug**.
2. Select a node name from the **Select Node** drop-down list box.
3. Select the required log name from the **Select Log** drop-down list box.
4. Click **Show Logs**.

The output for the selected criteria appears as shown:



- Click the download  icon to download the generated output.

Remote Command

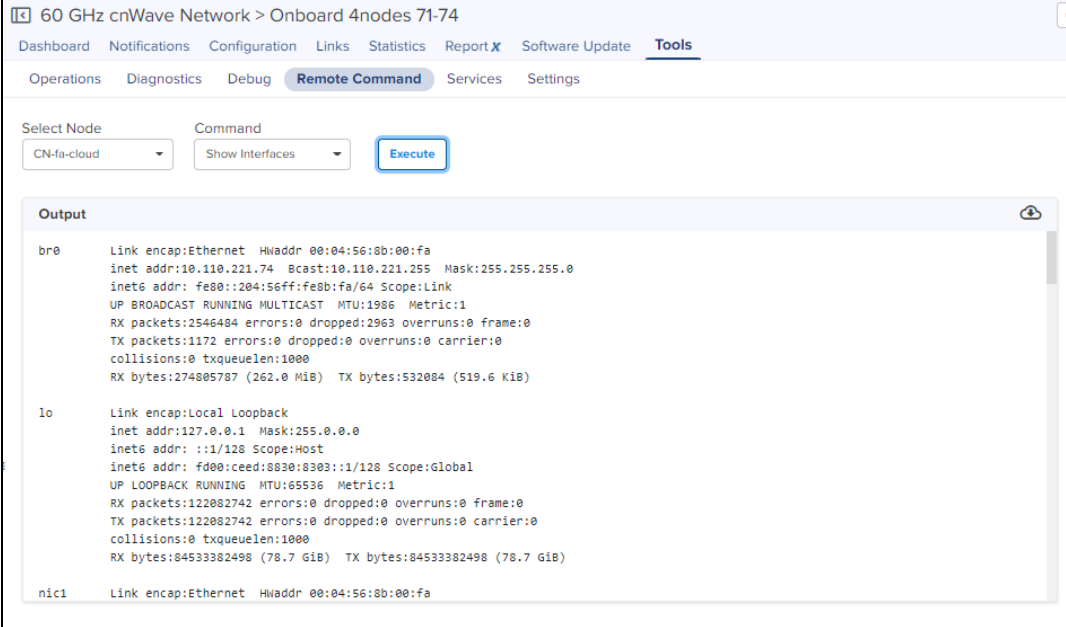
In **Remote command** tab user can able to view or download Command logs by executing the following command:

- Show Interfaces
- Show Routes
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show SFP Power Details (applicable for V5000 and V3000)

To Execute the command:

1. Navigate to **Tools > Remote Command**.
2. Select a node name from the **Select Node** drop-down list box.
3. Select the required command from the **Command** drop-down list box.
4. Click **Execute**.

The output for the selected criteria appears as shown:




The screenshot displays the 'Remote Command' interface for a '60 GHz cnWave Network > Onboard 4nodes 71-74'. The 'Tools' tab is active, and the 'Remote Command' sub-tab is selected. The 'Select Node' dropdown is set to 'CN-fa-cloud' and the 'Command' dropdown is set to 'Show Interfaces'. An 'Execute' button is visible. Below the command input, the 'Output' section shows the following network interface details:

```
br0    Link encap:Ethernet  Hwaddr 00:04:56:8b:00:fa
       inet addr:10.110.221.74  Bcast:10.110.221.255  Mask:255.255.255.0
       inet6 addr: fe80::204:56ff:fe8b:fa/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1986  Metric:1
       RX packets:2546484 errors:0 dropped:2963 overruns:0 frame:0
       TX packets:1172 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:274005787 (262.0 MiB)  TX bytes:532084 (519.6 KiB)

lo     Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       inet6 addr: fd00::ced:8830:8303::1/128 Scope:Global
       UP LOOPBACK RUNNING  MTU:65536  Metric:1
       RX packets:122082742 errors:0 dropped:0 overruns:0 frame:0
       TX packets:122082742 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:84533382498 (78.7 GiB)  TX bytes:84533382498 (78.7 GiB)

nic1   Link encap:Ethernet  Hwaddr 00:04:56:8b:00:fa
```

- Click the download  icon to download the generated output.

Services

In **Services** page user can view the services running in E2E Controller.

Figure 100 Services

Name	Version	Status	Uptime	CPU	Memory
cnAgent	1.1.0-r18	Running	5d 16h 1m	0.00%	0.74% [13.855MB]
e2e_controller	1.1	Running	5d 16h 1m	0.00%	10.16% [191.297MB]
e2e_minion	1.1	Running	5d 16h 1m	2.90%	1.89% [35.648MB]
nginx	1.17.0	Running	5d 16h 1m	0.00%	0.23% [4.414MB]
nms_aggregator	1.1	Running	5d 16h 1m	1.00%	0.92% [17.301MB]
stats_agent	1.1	Running	5d 16h 1m	4.70%	8.71% [164.043MB]

Settings

NOTE:

E2E Settings are not applicable for Onboard E2E Controller deployment.

External E2E Controller deployment

In **External E2E Controller Settings** page you can configure the **Network Configuration**, **IPv6 Routes**, **Remote SSH Management**, and **NTP Server**.

60 GHz cnWave Network > 7-Nodes-External-Smartwork
Tools

Operations
Diagnostics
Debug
Remote Command
Services
Settings

Network Configuration

E2E Controller IPv6 Address (eth0)
 Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

IPv6 Routes Automated IPv6 Routes to DNIs and CNIs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

Destination	Gateway	Type	Add New
default	fe80::ce16:7eff:fe6e:5b7f	dynamic	✖
fd00::ceed1681::56	2403:0:529:d:2403:0:27:fe01:202164	auto	✖

Remote SSH Management

Configure NTP Server

Enabled

NTP Server 1

NTP Server 2

NTP Server 3

NTP Server 4

Current System Time
 Thu, 12 Aug 2021 12:13:46 UTC

Status
 In Sync

Copyright © 2015 - 2021 Cambium Networks, Ltd. All rights reserved. | Version 3.0.4-022 | [Community](#) | [Support](#) | [Help](#) | [License](#)

In **Network Configuration** user can configure the **E2E Controller IPv6 Address** and **IPv6 Routes**.

NOTE:

Auto Manage Routes supports only for the cnMaestro X feature.

User can also enable the **Auto Manage Routes**. This automates IPv6 Routes to DNS and CNs based on the topology and PoP nodes status. It is applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

To Enable **Auto-Managed Routes**:

1. Navigate to **Tools > Settings > IPv6 Routes** tab.

Network Configuration

E2E Controller IPv6 Address (eth1)
fd20:ba5e:100/64 Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

IPv6 Routes

Auto Manage Routes **X** Automated IPv6 Routes to DNS and CNs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

Destination	Gateway	Type	
fd00:ceed:1eae:1100::/56	fd20:ba5e::5	static	<input type="button" value="X"/>

2. Enable **Auto-Managed Routes**.

Network Configuration

E2E Controller IPv6 Address (eth1)
fd20:ba5e:100/64 Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

IPv6 Routes

Auto Manage Routes **X** Automated IPv6 Routes to DNS and CNs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

Destination	Gateway	Type	
fd00:ceed:1eae:1100::/56	fd20:ba5e::5	static	<input type="button" value="X"/>

3. Click **Save**.
4. **Please Wait** window pops-up.

Please Wait ...

Activating Auto Manage Routes

If IPv6 routes is managed through auto manage routes in type it displays as **Auto**.

Network Configuration

E2E Controller IPv6 Address (eth0)
2403:0:529:d:a00:27ff:fe01:2121/64 Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

IPv6 Routes

Auto Manage Routes **X** Automated IPv6 Routes to DNS and CNs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

Destination	Gateway	Type	
default	fe80::ce16:7eff:fe6e:5b7f	dynamic	<input type="button" value="X"/>
fd00:ceed:1681:1a00::/56	2403:0:529:d:204:56ff:fe88:30dc	auto	<input type="button" value="X"/>

If cnMaestro X account is downgraded to Essential or if Auto Manage Routes is disabled. User can retain auto-managed routes of IPv6.

To Retain Auto-Managed Routes:

1. Navigate to **Tools > Settings > IPv6 Routes** tab.

Network Configuration

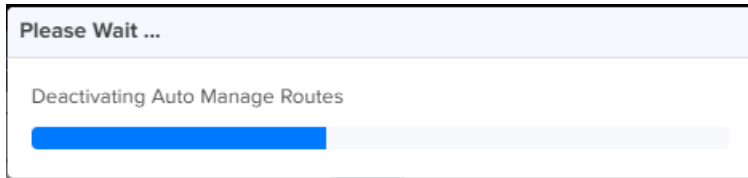
E2E Controller IPv6 Address (eth0)
 Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

IPv6 Routes

Auto Manage Routes **X** Automated IPv6 Routes to DNSs and CNs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

Destination	Gateway	Type
default	fe80::ce16:7eff:fe6e:5b7f	dynamic
fd00:ceed:1681:1a00::/56	2403:0:529:d:204:56ff:fe88:30dc	auto

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**.

Network Configuration

E2E Controller IPv6 Address (eth0)
 Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

IPv6 Routes

Auto Manage Routes **X** Automated IPv6 Routes to DNSs and CNs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

Destination	Gateway	Type
default	fe80::ce16:7eff:fe6e:5b7f	dynamic
fd00:ceed:1681:1a00::/56	2403:0:529:d:204:56ff:fe88:30dc	static

5. Enter the **IPv6 Interface**.
6. Click **Save**.

To add new **Static Routes**:

1. Click **Add New**.

Add Route

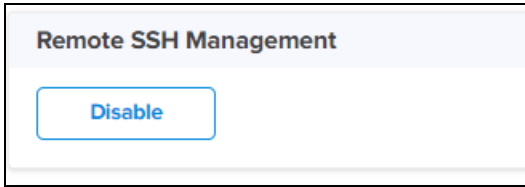
Destination

Gateway

2. Enter **Destination** and **Gateway**.
3. Click **Save**.

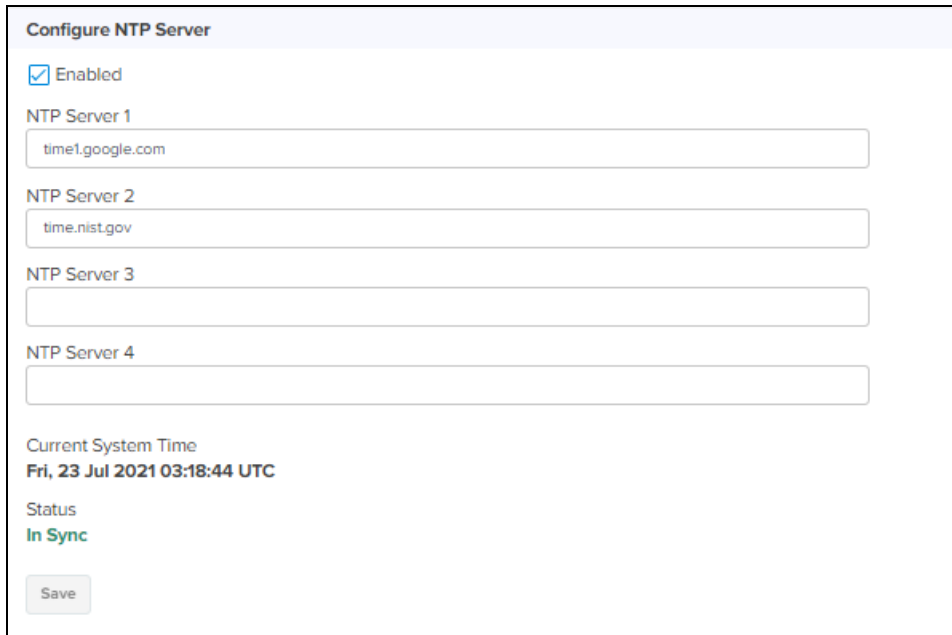
The user can configure the **NTP Settings** to configure the time configuration of the server with hostname or IP address.

Remote SSH Management allows the user to **Enable** and **Disable** Remote SSH Management.



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.

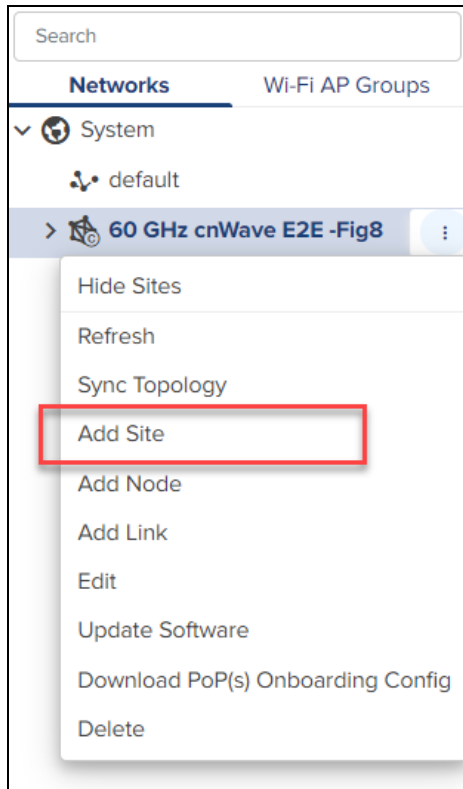


Site Configuration

Sites are located within the networks and wireless access points attached to it.

To Add a Site

1. Navigate to **Network** and click the icon  .
2. Select **Add Site** from the drop-down.



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.

Add Site
✕

Network

Name

Altitude

The altitude of the site (in meters above WGS84 ellipsoid).

Accuracy

The accuracy of the given position (in meters).

Latitude ⓘ Min = -90, Max = 90

Longitude ⓘ Min = -180, Max = 180

5. Click **Save**. Once the Site is configured it gets added under the E2E Network.

Search

Networks | Wi-Fi AP Groups

- System
 - default
 - 4Nodes-Onboard
 - External-E2E-232
 - PoP-Site**
 - S2
 - V3k-CN-301A
 - S3
 - S4

60 GHz cnWave Site > PoP-Site

Dashboard | Notifications | **Configuration** | Nodes | Report ✕

Network

Name

Altitude

The altitude of the site (in meters above WGS84 ellipsoid).

Accuracy

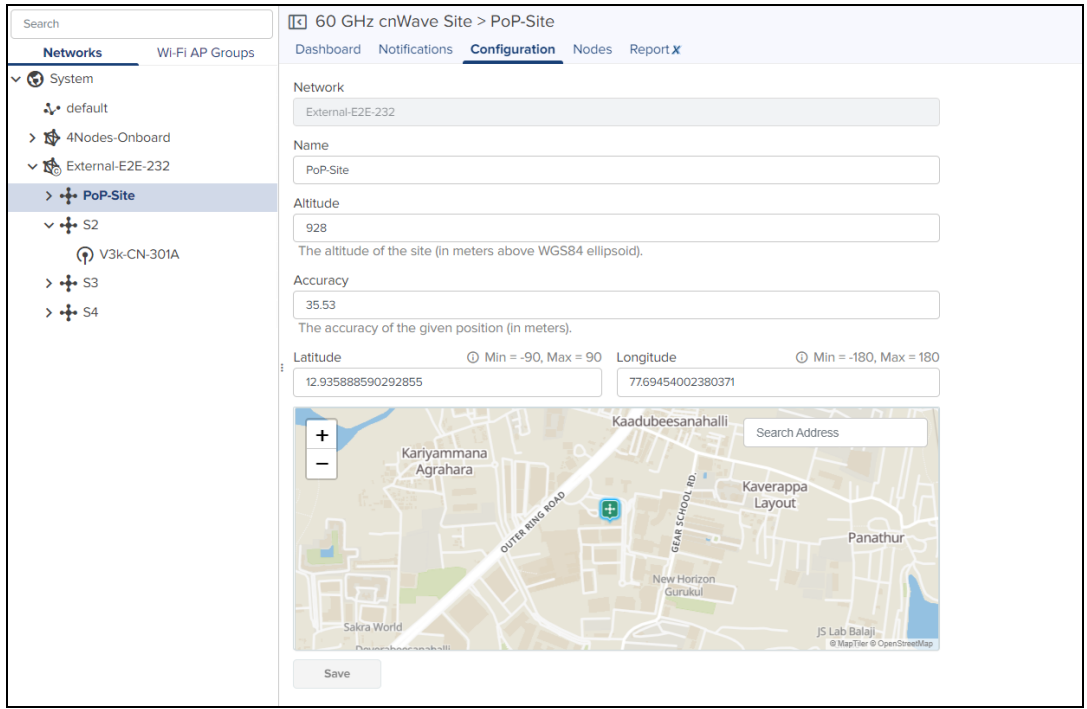
The accuracy of the given position (in meters).

Latitude ⓘ Min = -90, Max = 90

Longitude ⓘ Min = -180, Max = 180

To edit the **Site**, perform the following:

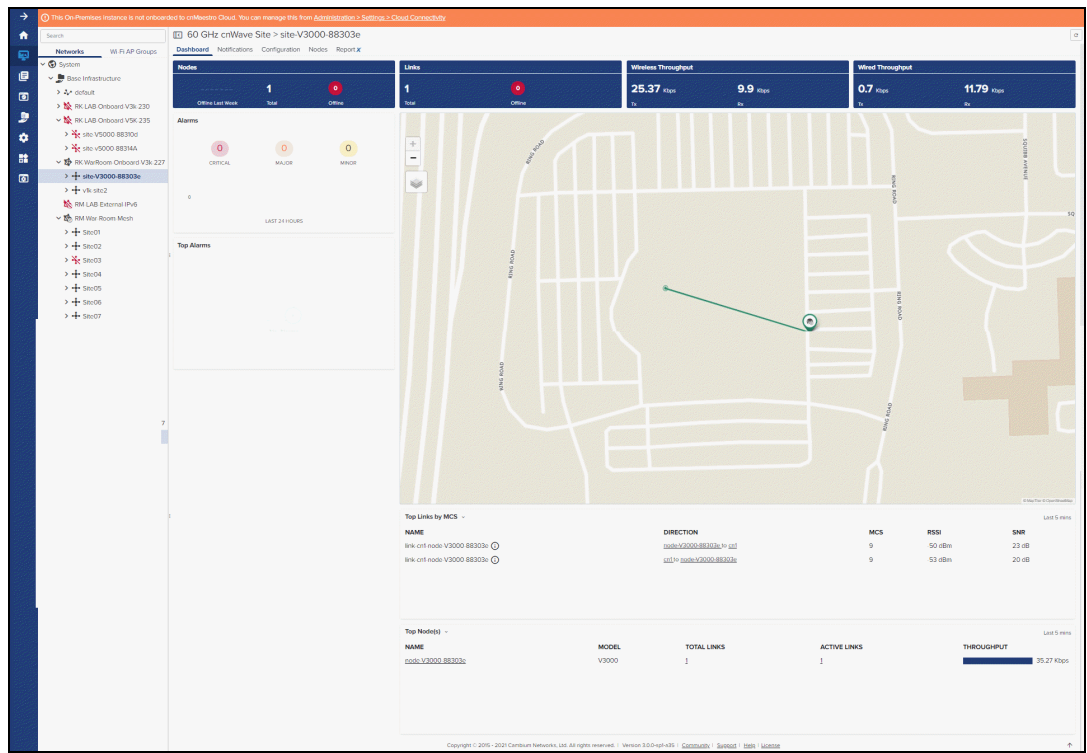
1. Navigate to **Network > Site > Configuration**.
2. Edit the details and click **Save**.



Site Dashboard

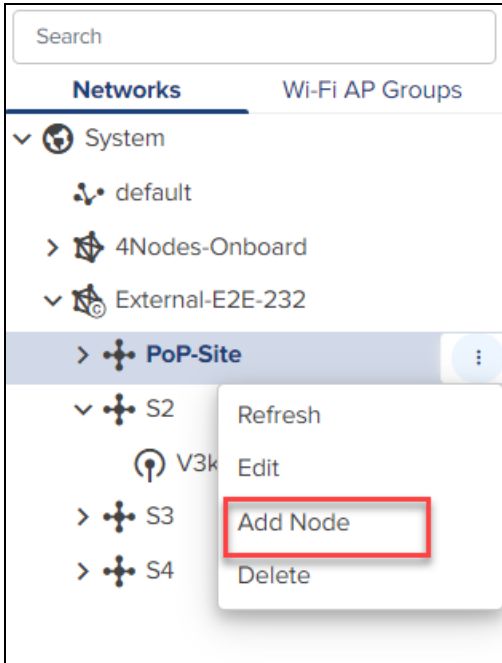
Dashboard pages are customized for each device type and aggregation level. The Site dashboard section displays the **Nodes**, **Links**, **Wireless Throughput**, **Wired Throughput**, **Alarms**, **Top Alarms**, **Top Links by MCS**, **Top Links by RSSI**, **Top Links by SNR**, **Top Node(s)**, **Top PoP(s)**, **Top DN(s)**, and **Top CN(s)**.

Figure 101 Site Dashboard

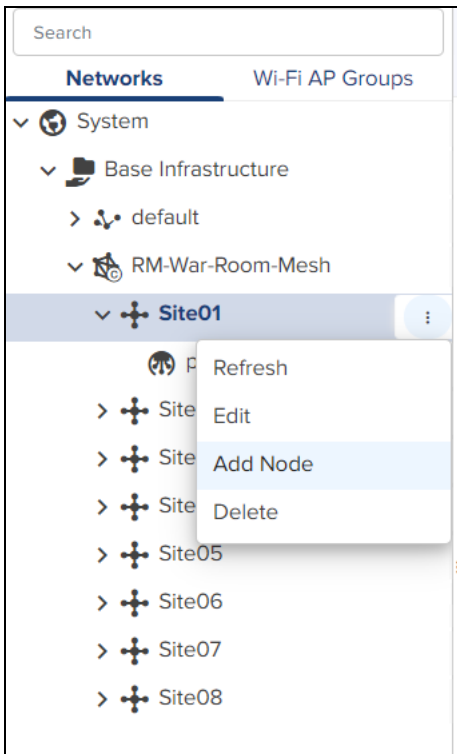


Node Configuration

Node can be configured through **Network** tree and **Site**. Select the **Network** click  select **Add Node**.



Select the **Site** click  select **Add Node**.



To Add a Node, perform the following steps:

1. Navigate to the **Network > Site > Nodes**.

Device	IPv6 Address	Mode	Model	Status	Status Time	Sync Mode	Radio Channel	Main Aux SFP	PoP Node	Fix Type	Satellites Tracked	Latitude	Longitude
CN-fs-cloud 00:04:56:88:00FA	fd00:cccc:8830:8303::1	CN	V1000	Online	5d 17h 7m	RF	4		No				

2. Add Node window pops-up once the user clicks Add new.

Add Node ×

Name

Network

Site

Mode

DN
 CN

PoP Node

MAC Address

Please enter a valid MAC address.

Supported formats: 00:00:00:00:00:00, 00-00-00-00-00-00, 000000000000

Model

Azimuth

Elevation

+ IPv4 Management

Adding the Node allows the user to create the different Nodes as shown below:

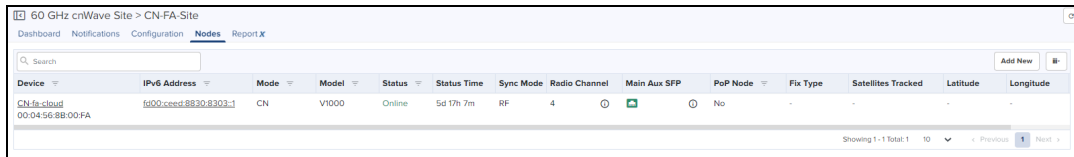
- PoP Node
- DN
- CN

PoP Node configuration

To add a PoP Node, perform the following steps:

1. Navigate to the **Network > Site > Nodes**.

2. Click **Add New**.




3. **Add Node** window pops-up.

A screenshot of the "Add Node" configuration window. The window has a title bar with "Add Node" and a close button. The form contains the following fields and options:

- Name:** An empty text input field.
- Network:** A dropdown menu showing "External-4Nodes-Godavari".
- Site:** A dropdown menu showing "CN#Site-v3k".
- Mode:** Radio buttons for "DN" (selected) and "CN". There is also an unchecked checkbox for "PoP Node".
- MAC Address:** A text input field containing "00:04:56:". Below it, supported formats are listed: "00:00:00:00:00:00, 00-00-00-00-00-00, 000000000000".
- Model:** A dropdown menu showing "V5000".
- Azimuth:** A text input field containing "0".
- Elevation:** A text input field containing "0".
- IPv4 Management:** A section with a collapsed icon and the following fields:
 - IPv4 Address:** An empty text input field.
 - Subnet Mask:** An empty text input field.
 - Gateway Address:** An empty text input field.
- Buttons:** "Save" and "Cancel" buttons at the bottom left.

4. Enter the **PoP Name**, select the Mode **DN**.

5. Enable **PoP Node**.



NOTE:
Once the PoP Node is enabled user needs to select the **Routing** and **Interface** details.

6. Enter the **MAC Address** and select the device **Model** from the drop-down.

7. Enter the **Azimuth** and **Elevation**.

8. In the **PoP Configuration**, select **BGP** or **Static Routing**.
9. In **Interface**, select **Aux** or **Main** or **SFP** or **Disabled**.

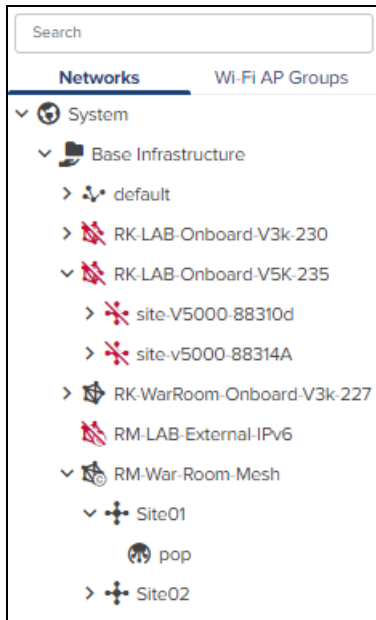
10. Enter the **IPv6** and **Gateway Addresses**.
11. In **IPv4 Management**, enter the **IPv4 Address**, **Subnet Mask** and **Gateway Address**.
12. Click **Save**.



NOTE:

Once the PoP Node is configured, **PoP(s) Onboarding Config.json** file gets downloaded automatically, that can be used to import and configure in the PoP Node UI.

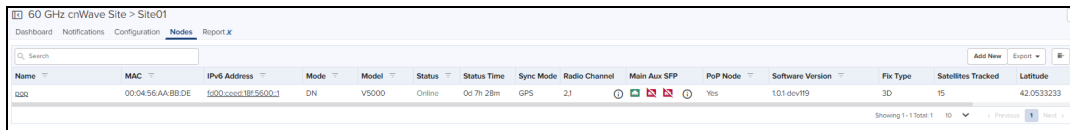
Once the **PoP** node is configured, it get listed under the **Site**.



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.

Add Node
×

Name

Network

External-4Nodes-Godavari

Site

CN#Site-v3k

Mode

DN
 CN

PoP Node

MAC Address

Supported formats: 00:00:00:00:00:00, 00-00-00-00-00-00, 000000000000

Model

V5000 ▾

Azimuth

Elevation

IPv4 Management

IPv4 Address

Subnet Mask

Gateway Address

Save

Cancel

4. Enter the **Node Name**, select the Mode **DN** or **CN**.
5. Enter the **MAC Address**, and select the device **Model** from the drop-down.
6. Enter the **Azimuth** and **Elevation**.

Add Node
×

Name

Network

Site

Mode
 DN CN
 PoP Node

MAC Address

Supported formats: 00:00:00:00:00:00, 00-00-00-00-00-00, 000000000000

Model

Azimuth Elevation

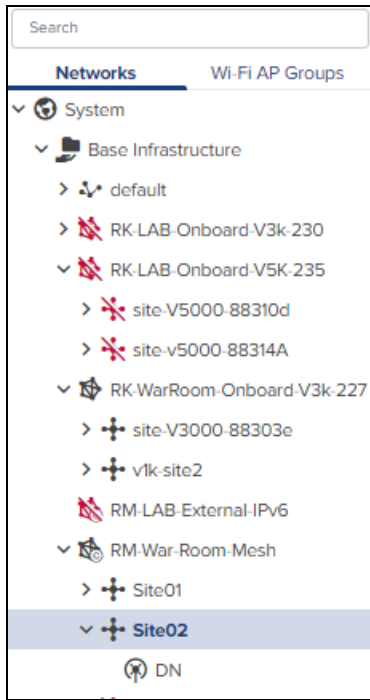
IPv4 Management

IPv4 Address

Subnet Mask

Gateway Address

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.

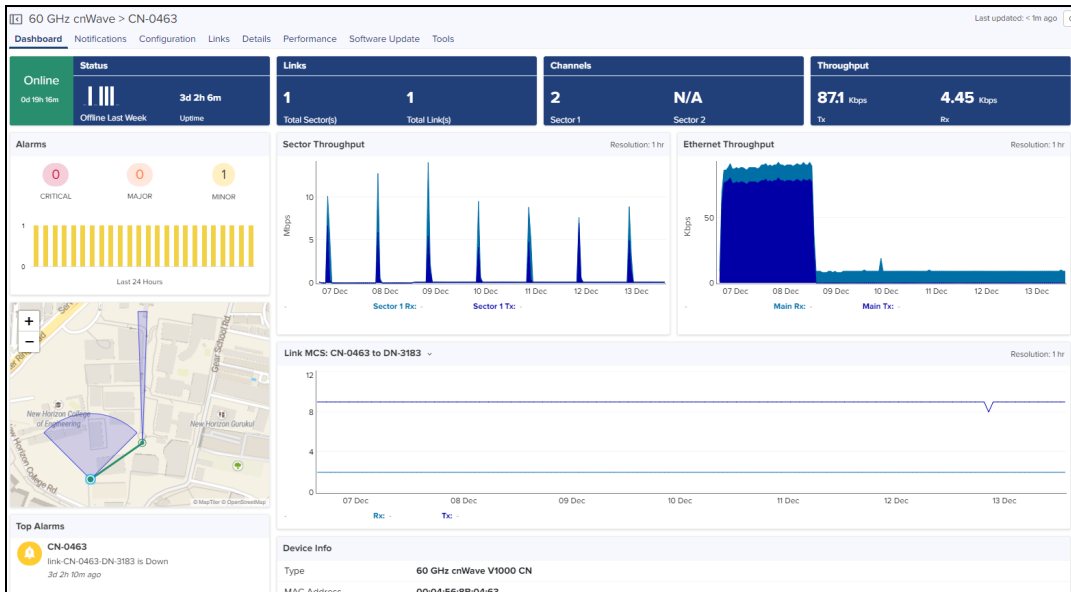


Replace Node

Replace Node allows to replace the existing faulty nodes with new nodes along with the configuration and links of existing faulty nodes.

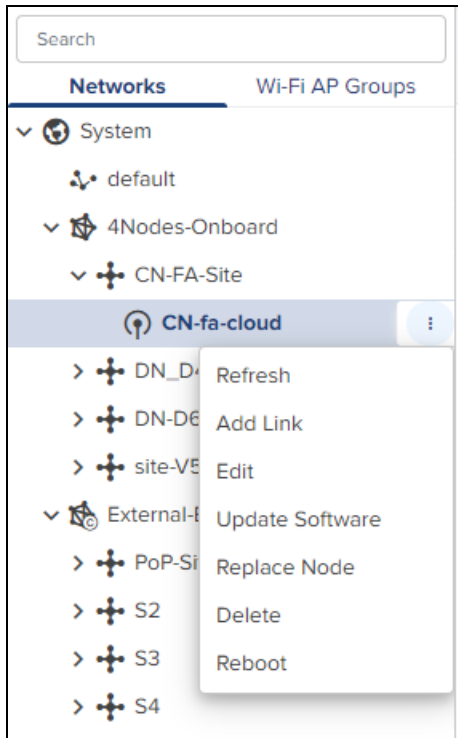
NOTE:

New node should be replaced with same model as existing node.

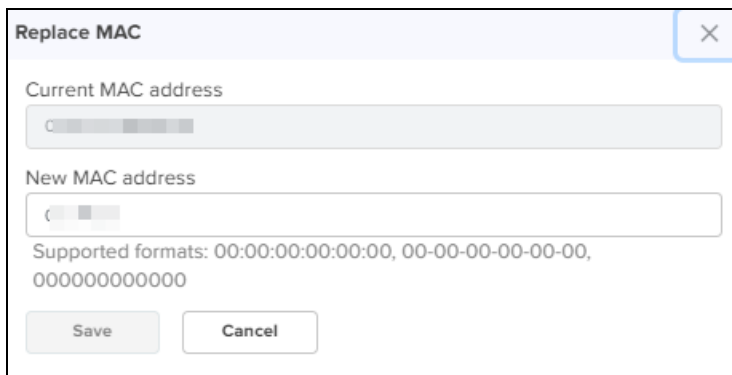


To replace Node, perform the following steps:

1. Navigate to **Node** tree menu and select the node.



2. Click  icon, Select **Replace Node** from the drop-down.
3. **Replace MAC** window pops-up.



4. Enter the **New MAC address**.
5. Click **Save**.

PoP Node

Once the PoP node is configured it displays the monitoring panel of the PoP node.

Dashboard

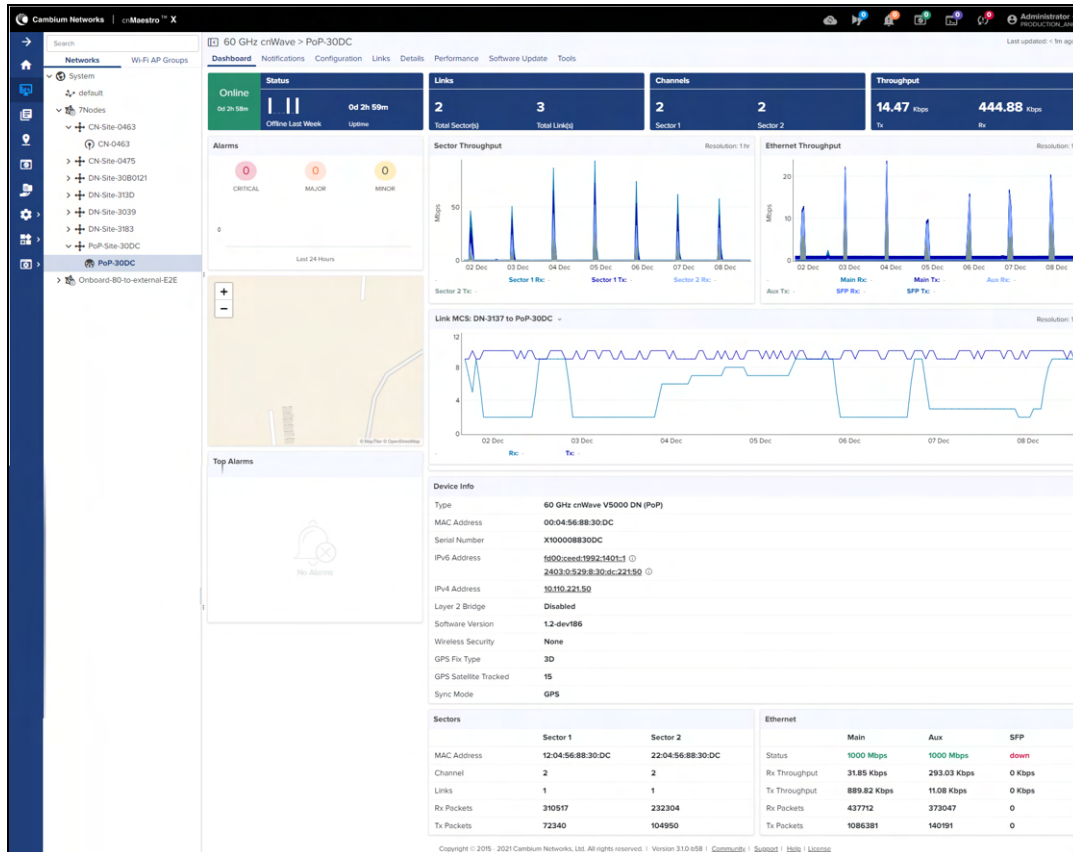
Dashboard pages can be customized for each device type and aggregation level. The PoP node dashboard section displays the **Status, Links, Channels, Throughput (sector1), Throughput (sector2), Throughput (Main), Throughput (AUX), Throughput (SFP), Alarms, Top Alarms, Links MCS, Device Info, Sectors, and Ethernet**.



NOTE:

- Throughput (sector1) for V3000 and V1000.
- Throughput (sector1 and sector2) for V5000.
- Throughput graph with Main for V1000.
- Other throughput graph with Main, Aux, SFP for V5000 and V3000.

Figure 102 PoP Node Dashboard



Configuration

Basic

In Basic page you can able to view and edit the details of PoP node such as **Name**, **Description**, **MAC Address**, **Azimuth**, and **Elevation**.

Figure 103 Basic

60 GHz cnWave > PoP-30DC

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network VLAN Security Advanced

Name
PoP-30DC

Description

MAC Address
00:04:56:88:30:DC

PoP node

Azimuth
0

Elevation
0

Save Reset

Radio

It allows the user to configure the EIRP, Adaptive Modulation, Sectors (channels, Polarity and Link(s) Golay), and GPS.

Figure 104 Radio

60 GHz cnWave > node-V5000-883083

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic **Radio** Network VLAN Security Advanced

EIRP

Maximum EIRP
28 Allowed range is 13 dBm to 38 dBm

RF Transmit Power
 Short range (<25m) optimized Long range optimized Initial Beam Forming transmit power setting

Adaptive Modulation

Minimum MCS
2 Range: [2, 12]

Maximum MCS
12 Range: [2, 12]

Sector 1

Channel/Polarity should originate from leaf nodes. Please make sure to change on the CNs first and then higher up on the DN.

Override	Name	Auto Configuration	Node Configuration
<input checked="" type="checkbox"/>	Channel	2	2
<input type="checkbox"/>	Polarity	Even	

Sector 1 Link (s) Golay

Override	Name	Auto Configuration (Rx/Tx)	Node Golay Rx	Node Golay Tx
<input type="checkbox"/>	link CN aS node-V5000-883083	2/2		

Sector 2

Channel/Polarity should originate from leaf nodes. Please make sure to change on the CNs first and then higher up on the DN.

Override	Name	Auto Configuration	Node Configuration
<input checked="" type="checkbox"/>	Channel	4	4
<input type="checkbox"/>	Polarity	Even	

Sector 2 Link (s) Golay

Override	Name	Auto Configuration (Rx/Tx)	Node Golay Rx	Node Golay Tx
<input type="checkbox"/>	link CN fa node-V5000-883083	2/2		
<input type="checkbox"/>	link DN D4 node-V5000-883083	2/2		

GPS

Force GPS Disable GPS sync at initiator/responder during assoc

Save Reset

Network

Network tab allows the user for the PoP configuration, E2E Controller Configuration, BGP Configuration, IPv6 Layer 3 CPE, IPv4 Management, OOB, Other Settings (Multi-PoP or Relay Port, Enable Aux port power) and Ethernet Ports.

Figure 105 Network

The screenshot shows the Network Configuration page for a 60 GHz cnWave node (node-V5000-883083). The page is divided into several sections:

- PoP Configuration:** Routing is set to Static Routing. The interface is set to Main. IPv6 Address is 1000ba5e-88-3083-88-3083. IPv6 Gateway Address is empty.
- BGP Configuration:** Local ASN is empty. KeepAlive is empty.
- IPv6 Layer 3 CPE:** IPv6 CPE Interface is set to Disabled.
- IPv4 Management:** IPv4 Address is 10.70.221.226. Subnet Mask is 255.255.255.0. Gateway IP Address is 10.70.221.254.
- Ethernet Ports:** Enable Main, Enable Aux, and Enable SFP are all checked.
- Other Settings:** Enable Aux port power is unchecked. Multi-PoP / Relay Port is set to Main. OOB Interface is set to Disabled.

Configure the Network as shown below:

1. Navigate to the **Configuration > Network**.
2. In **PoP Configuration**:
 - Select the appropriate option in **Routing** and **Interface**.
 - Enter **IPv6 Address**.
 - Enter **IPv6 Gateway Address** its optional.

This screenshot shows a close-up of the PoP Configuration section. The Routing is set to Static Routing and the Interface is set to Main. The IPv6 Address field contains the value 1000ba5e-88-3083-88-3083. The IPv6 Gateway Address field is empty.

3. In **E2E Controller Configuration**, enter the **IPv6 Address**.

The screenshot shows the E2E Controller Configuration page. The IPv6 Address field contains the value 8001::30. Below the field, there is a note: "If empty or Onboard mode enabled, PoP Address will be used".

4. In **BGP Configuration** add IPv6 Address.

BGP Configuration

Local ASN The autonomous system number (ASN) assigned to the PoP nodes

KeepAlive The BGP keepalive period in seconds

Summarized CPE Prefix Prefix summarizing network wide customized CPE Prefixes/Prefixes allocated by DHCPv6 Relay (that fall outside Seed Prefix range). Multiple prefixes require comma separation. Eg CN1 has 2001X:Y1110:64, CN2 has 2001X:Y1111:64. Summarized CPE Prefix would be 2001X:Y1110:63

IPv6 Address **ASN**

No Data

[Add New](#)

5. In **IPv6 Layer 3 CPE**

- Select **IPv6 CPE interface** as Aux, Main, or SFP.
- Enter **IPv6 CPE Prefix**.

IPv6 Layer 3 CPE

IPv6 CPE interface

Aux Main SFP Disabled

Choose the interface to run IPv6 SLAAC. Subnet allocated by the controller will be used as Prefix. This interface will not be part of Layer 2 bridge. Should be disabled for IPv4 CPE.

IPv6 CPE Prefix If empty, Subnet prefix allocated by the controller to the node will be used.

6. In **IPv4 Management:**

- Enter **IPv4 Address**.
- Enter **Subnet Mask**.
- Enter **Gateway IP Address**.

IPv4 Management

IPv4 Address IPv4 Management access is not allowed over IPv6 CPE INTERFACE


Subnet Mask

Gateway IP Address

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 Unknown Unicast Flood.
- Disable IPv6.
- Monitor PoP Interface Layer 2 tunnels will failover to next best PoP when the backhaul interface of this PoP is down.



NOTE:

The configuration is applicable only when static routing is used and IPv4 gateway is configured.

- Insert DHCP Option 82

Layer 2 Bridge

Disable Broadcast Broadcast packets (except DHCP Offer and DHCP Ack) in the downlink direction including client to client packets will be dropped.

Disable 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. The configuration is applicable when static routing is used and IPv4 gateway is configured.

Insert DHCP Option 82

Enabled Disabled DHCP option 82 will be inserted in the DHCP requests.

9. In Other Settings.

- Enable Aux port power
- Select **Multi-PoP / Relay Port** as Aux, Main, or SFP.

Other Settings

Enable Aux port power Enables the power out on the Aux port

Multi-PoP / Relay Port

Aux Main SFP Disabled Wired interface on which OpenR is run. Should be used when DNs are connected back to back and on PoPs in a multi PoP network.

10. In **OOB Interface** enable the appropriate option **Main** or **Aux** or **SFP**.

- Enter **IPv4 Address**.
- Enter **Subnet Mask**.

OOB


OOB Interface

Aux Main SFP Disabled Out of band management interface to access the device. Management VLAN will be bypassed and data traffic will not be routed or bridged on this interface.


IPv4 Address

Subnet Mask

11. Click **Save**.

	<p>NOTE:</p> <p>Once the configuration is updated successfully in cnMaestro, the same parameters needs to be entered in the UI of the PoP Node GUI.</p>
---	---

VLAN

	<p>NOTE:</p> <p>From Software Update Version 1.1 of all nodes, supports configuration of the VLAN Management and Ports.</p>
---	--

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 disable, Only PoP node Management VLAN ID can be configured.
- When Layer2 bridge is enable, all nodes Management VLAN ID can be configured.

Node running version 1.1:

- When Layer2 bridge is disable, Only PoP node Management VLAN ID, Priority with Outer Tag can be configured.
- When Layer2 bridge is enable, all node management VLAN and ports can be configured.

To add a Management VLAN:

1. Navigate to **Configuration > VLAN**.
2. Click **Enabled**.

60 GHz cnWave > node-V5000-883083

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network **VLAN** Security Advanced

Management

Enabled Disabled

VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

Add Outer Tag

Save Reset

3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.

60 GHz cnWave > node-V5000-883083

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network **VLAN** Security Advanced

Management

Enabled Disabled

VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

Add Outer Tag

S-VLAN ID Allowed range is 1 - 4094

S-VLAN Priority Allowed range is 0 - 7

QinQ EtherType EtherType indicates which protocol is encapsulated in the payload of an Ethernet Frame.

Save Reset

5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority**.
7. Enter **QinQ EtherType**.
8. Click **Save**.

If Layer 2 Bridge is enabled in **60 GHz cnWave Network > Configuration > Basic** page, then the user can configure Management VLAN and Ports of PoP node, DN and CN.



NOTE:

VLAN settings are not applicable if Relay Port, SFP Port, or Aux Port is enabled on Network page.

60 GHz cnWave > test-pop2

Dashboard
Notifications
Configuration
Links
Details
Performance
Software Update
Tools

Basic
Radio
Network
VLAN
Security
Advanced

☰

Management

Enabled Disabled

VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

Add Outer Tag

☰

Main Port

ⓘ VLAN settings are not applicable as PoP Interface is enabled on this port.

☰

SFP Port

Type
 Q QinQ Transparent

☰

Aux Port

Type
 Q QinQ Transparent

Save

Reset

To add a VLAN, perform the following steps:

1. Navigate to **Configuration > VLAN**.
2. Click **Enabled**.

60 GHz cnWave > test-pop2

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network **VLAN** Security Advanced

Management

Enabled Disabled

VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

Add Outer Tag

Main Port

i VLAN settings are not applicable as PoP Interface is enabled on this port.

SFP Port

Type

Q QinQ Transparent

Aux Port

Type

Q QinQ Transparent

3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.

60 GHz cnWave > test-pop2

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network **VLAN** Security Advanced

Management

Enabled Disabled

VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

Add Outer Tag

S-VLAN ID Allowed range is 1 - 4094

S-VLAN Priority Allowed range is 0 - 7

QinQ EtherType EtherType indicates which protocol is encapsulated in the payload of an Ethernet Frame.

Main Port

i VLAN settings are not applicable as PoP Interface is enabled on this port.

SFP Port

Type

Q QinQ Transparent

Aux Port

Type

Q QinQ Transparent

5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority**.
7. Enter **QinQ EtherType**.



NOTE:

VLAN settings configuration of Main Port, SFP Port, or Aux Port is similar.

8. Select Port **Q** or **QinQ** types.
 - a. If user selects **Q type** perform as follows:

Main Port

VLAN settings are not applicable as PoP Interface is enabled on this port.

SFP Port

Type
 Q QinQ Transparent

Untagged Packets
 Allow Drop

Native VLAN ID
 Allowed range is 1 - 4094

Native VLAN Priority
 Allowed range is 0 - 7

Allowed VLANs
 List of allowed VLANs. Comma separated, and/or range. e.g 100, 210-220

Ingress VLAN	Remark VLAN	
No Data		
Add New		

Ingress VLAN	Override Priority	
No Data		
Add New		

Aux Port

Type
 Q QinQ Transparent

- Select **Untagged Packets** Allow or Drop.
- Enter **Native VLAN ID**.
- Enter **Native VLAN Priority**.
- Enter **Allowed VLANs**.
- To add new **VLAN Remarking**.

Ingress VLAN	Remark VLAN	
No Data		
Add New		

- Click **Add New**.

Add

Ingress VLAN

Allowed range is 1 - 4094

Remark VLAN

Allowed range is 1 - 4094

Save Cancel

- Enter **Ingress VLAN** and **Remark VLAN**.
 - Click **Save**.
- To add new **VLAN Priority Override**.

Ingress VLAN	Override Priority
No Data	
Add New	

- Click **Add New**.

Add

Ingress VLAN

Allowed range is 1 - 4094

Override Priority

Allowed range is 0 - 7

Save Cancel

- Enter **Ingress VLAN** and **Remark VLAN**.
 - Click **Save**.
- Click **Save**.

b. If user selects **QinQ** type, then perform as follows:

SFP Port

Type
 Q QinQ Transparent

Untagged Packets
 Allow Drop

Single Tagged Packets
 Allow Drop

Native C-VLAN ID
 Allowed range is 1 - 4094

Native C-VLAN Priority
 Allowed range is 0 - 7

Native S-VLAN ID
 Allowed range is 1 - 4094

Native S-VLAN Priority
 Allowed range is 0 - 7

Allowed VLANs
 List of allowed VLANs. Comma separated, and/or range. e.g 100, 210-220

QinQ EtherType
 EtherType indicates which protocol is encapsulated in the payload of an Ethernet Frame.

Ingress VLAN	Remark VLAN
No Data	
Add New	

Ingress VLAN	Override Priority
No Data	
Add New	

Aux Port

Type
 Q QinQ Transparent

- In **Untagged Packets** select **Allow** or **Drop**.
- In **Single Tagged Packets** select **Allow** or **Drop**.
- Enter **Native C-VLAN ID**.
- Enter **Native C-VLAN Priority**.
- Enter **Native S-VLAN ID**.
- Enter **Native S-VLAN Priority**.
- Enter **Allowed VLANs**.
- Enter **QinQ EtherType**.
- To add new **VLAN Remarking**.

Ingress VLAN	Remark VLAN
No Data	
Add New	

- Click **Add New**

Add

Ingress VLAN

Allowed range is 1 - 4094

Remark VLAN

Allowed range is 1 - 4094

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- To add new **VLAN Priority Override**.

Ingress VLAN	Override Priority		
No Data			
Add New			

- Click **Add New**.

Add

Ingress VLAN

Allowed range is 1 - 4094

Override Priority

Allowed range is 0 - 7

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- Click **Save**.

Security

Security tab allows to reset the identity and password of the Radius user.

Figure 106 Security



Advanced

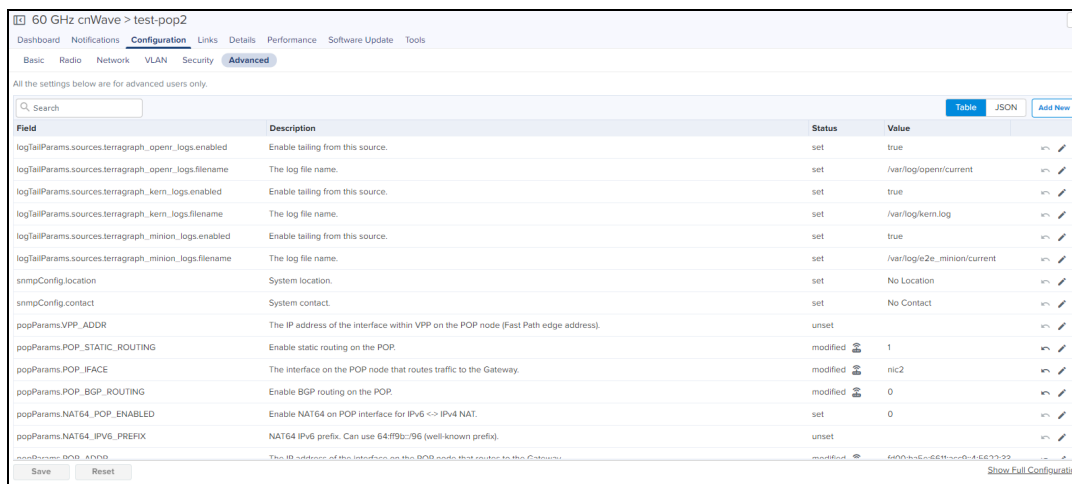
Advanced tab allows the advanced user to edit the settings of the **Table** and JSON format of the PoP Nodes.

Table

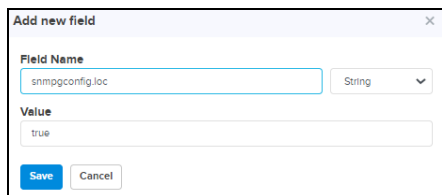
In the **Table** user can able to view and edit **Field Name** and **Value**.

To add a field, perform the following steps:

1. Navigate to **Configuration > Advanced**.
2. Click **Add New**.



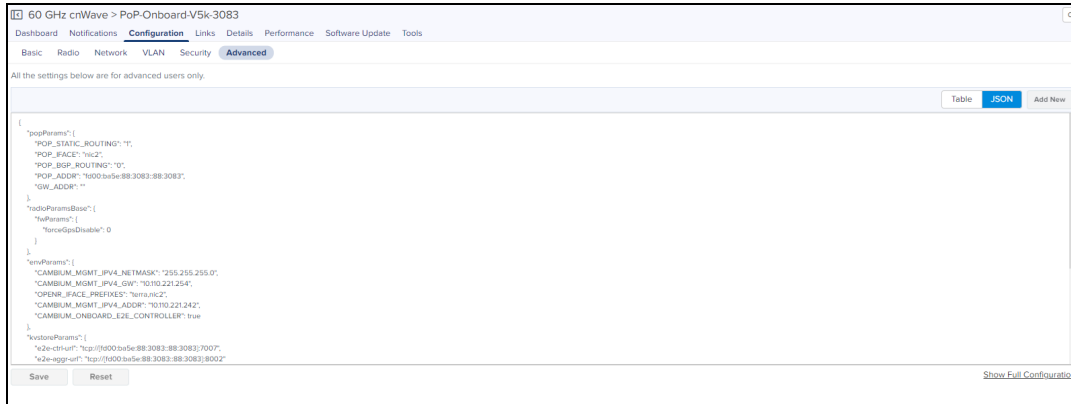
3. Enter the **Field Name** and **Value**.



4. Click **Save**.

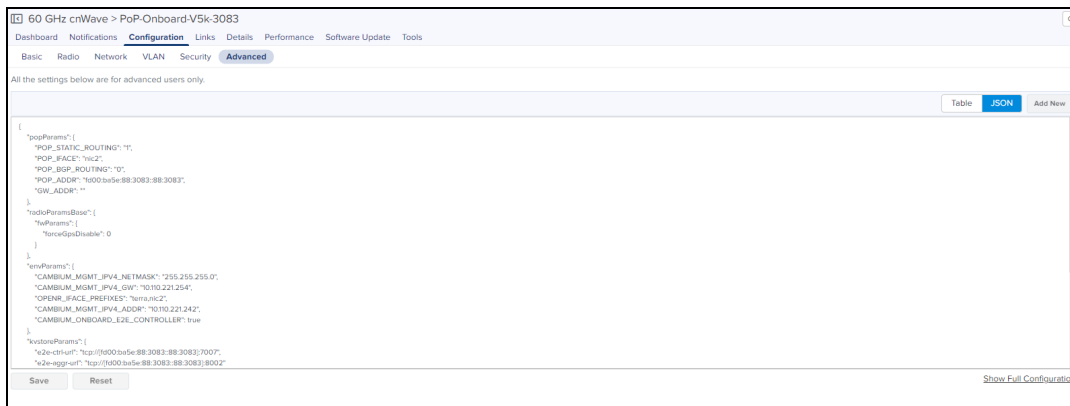
JSON

JSON allows Advanced user to download or view the JSON format.



To download the file, 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 the links between nodes, status 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 links.

Figure 107 List

Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	Link Time
link-DN-3080-PoP-30DC	DN-3080	PoP-30DC	22:04:56:88:30:80	12:04:56:88:30:DC	No	2d 2h 33m
link-DN-313D-PoP-30DC	DN-313D	PoP-30DC	12:04:56:88:31:3D	22:04:56:88:30:DC	No	2d 2h 33m
link-DN-3183-PoP-30DC	DN-3183	PoP-30DC	-	-	Yes	4d 20h 2m



NOTE:

Once the PoP node is configured successfully user needs to create a Site and DN to link the PoP as shown in the DN/CN Node link.

Export Link List

Export list allows the user to export the PoP links list.

To export the links, perform the following steps:

1. Navigate to **Links > List > select Export**.

2. It exports .csv file format as shown below.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
LINK_NAME	A_NODE	I_A_NODE	I_Z_NODE	I_Z_NODE	I_LINK_TYPE	ALIVE	IGNITION	DISTANCE	AZIMUTH	BACKUP_C	IGNITION	TIMESTAMP		
Link Name	A node	naI Sector	1/2 Z node	naI Sector	1/2 Z node	naI Sector	1/2 Z node	naI Sector	1/2 Z node	naI Sector	1/2 Z node	naI Sector	1/2 Z node	naI Sector
link-CN-fa-cloud-D4	CN-fa-clo	12:04:56:8 D4	22:04:56:8	Wireless	Yes	16	996	54.9	No	Enabled	2021-07-23T02:49:06.317Z			
link-D4-PoP-Onboard-V5k-3083	D4	12:04:56:8	PoP-Onbo	22:04:56:8	Wireless	Yes	0	988	158.8	No	Enabled	2021-07-23T02:49:06.317Z		
link-DN-D6-PoP-Onboard-V5k-3083	DN-D6	12:04:56:8	PoP-Onbo	12:04:56:8	Wireless	Yes	0	979	105.2	No	Enabled	2021-07-23T02:49:06.317Z		

Statistics

Links Statistics pages provides details of Name, Direction, A-Node Sector MAC, Z-Node Sector MAC, Alive, Link Time, RSSI, Tx Power Index, A-node, Z-node, Type, Distance, Azimuth, Rx MCS, Tx MCS, Rx PER, Tx PER, Rx SNR, Rx Beam Index, Tx Beam Index, EIRP, Rx Errors, Tx Errors, Rx Frames, Tx Frames on a single device, generally in a page format.

Name	Direction	A-Node Sector M...	Z-Node Sector M...	Alive	Link Time	RSSI	Rx SNR	Rx MCS	Tx Power Index	EIRP	Tx MCS
link-D4-PoP-Onboard-V5k-3083	D4 to PoP-Onboard-V5k-3083	12:04:56:88:38:D4	22:04:56:88:30:83	Yes	42d 19h 43m	-47 dBm	25 dB	10	6	13 dBm	9
link-D4-PoP-Onboard-V5k-3083	PoP-Onboard-V5k-3083 to D4	12:04:56:88:38:D4	22:04:56:88:30:83	Yes	42d 19h 43m	-50 dBm	23 dB	10	6	13 dBm	9
link-DN-D6-PoP-Onboard-V5k-3083	DN-D6 to PoP-Onboard-V5k-3083	12:04:56:88:30:D6	12:04:56:88:30:83	Yes	42d 19h 43m	-50 dBm	23 dB	9	6	35 dBm	9
link-DN-D6-PoP-Onboard-V5k-3083	PoP-Onboard-V5k-3083 to DN-D6	12:04:56:88:30:D6	12:04:56:88:30:83	Yes	42d 19h 43m	-54 dBm	20 dB	9	6	13 dBm	9

Export Statistics

Export list allow the user to export the PoP links Statistics.

To export the Statistics :

1. Navigate to **Links > List > select Export**.

Name	Direction	A-Node Sector M.	Z-Node Sector M.	Alive	Link Time	RSSI	Rx SNR	Rx MCS	Tx Power Index	EIRP
link-CN-fa-cloud-D4	CN-fa-cloud-to-D4	12-04-56-88-00-FA	22-04-56-88-38-D4	Yes	3d 19h 5m	-48 dBm	24 dB	9	6	13 dBm
link-CN-fa-cloud-D4	D4-to-CN-fa-cloud	12-04-56-88-00-FA	22-04-56-88-38-D4	Yes	3d 19h 5m	-49 dBm	24 dB	9	6	13 dBm

2. It exports .csv file format as shown below.

Name	Direction	A-Node Sector M.	Z-Node Sector M.	Alive	Link Time	RSSI	Rx SNR	Rx MCS	Tx Power Index	EIRP
link-APOP-DN-3D	APOP-to-DN-3D	22-04-56-88-30-DC	12-04-56-88-31-3D	Yes	0d 2h 35m	-52 dBm	21 dB	9	6	13 dBm
link-APOP-DN-3D	DN-3D-to-APOP	22-04-56-88-30-DC	12-04-56-88-31-3D	Yes	0d 2h 35m	-51 dBm	22 dB	9	6	13 dBm
link-APOP-DN-80	APOP-to-DN-80	12-04-56-88-30-DC	22-04-56-88-30-80	Yes	1d 15h 52m	-40 dBm	32 dB	9	6	13 dBm
link-APOP-DN-80	DN-80-to-APOP	12-04-56-88-30-DC	22-04-56-88-30-80	Yes	1d 15h 52m	-37 dBm	32 dB	10	6	13 dBm
link-CN-75-DN-80	DN-80-to-CN-75	12-04-56-88-04-75	12-04-56-88-30-80	Yes	0d 5h 33m	-48 dBm	25 dB	9	23	30 dBm
link-CN-75-DN-80	CN-75-to-DN-80	12-04-56-88-04-75	12-04-56-88-30-80	Yes	0d 5h 33m	-61 dBm	12 dB	8	6	13 dBm
link-CN-83-DN-80	CN-83-to-DN-80	12-04-56-88-31-83	22-04-56-88-30-80	Yes	0d 13h 24m	-53 dBm	21 dB	9	6	35 dBm
link-CN-83-DN-80	DN-80-to-CN-83	12-04-56-88-31-83	22-04-56-88-30-80	Yes	0d 13h 24m	-49 dBm	23 dB	9	6	37 dBm
link-CN-8B0463-DN-39	DN-39-to-CN-8B0463	12-04-56-88-04-63	22-04-56-88-30-39	No	0d 0h 3m	-60 dBm	12 dB	9	31	37 dBm
link-CN-8B0463-DN-39	CN-8B0463-to-DN-39	12-04-56-88-04-63	22-04-56-88-30-39	No	0d 0h 3m	-48 dBm	25 dB	9	6	13 dBm

Events

Events provides the details of the links from last 1 hour to 7 Days Period.

Figure 108 Events

Link Name	Alive	Availability Chart	Availability	Distance
link-DN-30B0-PoP-30DC	No	[Red bar]	0%	186 m
link-DN-313D-PoP-30DC	No	[Red bar]	0%	217 m

Note: The Availability percentage per link is calculated including the duration when E2E Controller was offline in cnMaestro.

It also calculates the Availability percentage per link, including the duration when E2E Controller was offline in cnMaestro.

Link Name	Alive	Availability Chart	Availability	Distance
link-DN-30B0-PoP-30DC	No	[Red bar]	0%	186 m
link-DN-313D-PoP-30DC	No	[Red bar]	0%	217 m

Note: The Availability percentage per link is calculated including the duration when E2E Controller was offline in cnMaestro.

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 109 Details Overview Page

The screenshot displays the 'Details Overview Page' for a 60 GHz cnWave APOP device. The interface includes a navigation bar with 'Overview' and 'Network' tabs. The main content is divided into several sections:

- System:** Lists device name (APOP), type (60 GHz cnWave V5000 DN (PoP)), MAC Address (00:04:56:88:30:DC), health (Online), uptime (0d 6h 42m), IP v6 Address (2001:3001:4001:201:1), software version (11-alpha2), firmware version (10.11.0.87), serial number (X100008830DC), onboarding date (May 06, 2021 20:34), available memory (79%), CPU utilization (5.49%), and sync mode (GPS).
- Sectors:** A table showing details for Sector 1 and Sector 2, including MAC Address, Channel, Links, Rx/Tx Packets, Security, Error Association, Channel Last State, Number Of Switches, and Baseband/RF Tile temperatures.
- Software Update:** Shows the current software version (11-alpha2) and a history of updates with dates, times, and success status.
- GPS:** Provides location data: Latitude (12.9339438), Longitude (77.6944361), Height (931 m), Fix Num Sat (13), and Fix Type (3D).
- Links:** A table showing the status of Wireless and Wired connections, with Total and Active counts.

Network

Network page provides the Ethernet details of Main, Aux, and SFP.

Figure 110 Details Network Page

The screenshot displays the 'Details Network Page' for a 60 GHz cnWave APOP device. The 'Network' tab is active, showing Ethernet statistics for three ports: Main, Aux, and SFP.

	Main	Aux	SFP
Status	1000 Mbps	down	down
Rx Throughput	7.23 Kbps	0 Kbps	0 Kbps
Tx Throughput	93.9 Kbps	0 Kbps	0 Kbps
Rx Packets	236958	0	0
Tx Packets	357475	0	0
Rx Errors	0	0	0
Tx Errors	0	0	0
Rx Drops	804	0	0
Tx Drops	0	0	0
Rx Frames	0	0	0

Tools

In Tools page user can able to view the Status, Debug, and Remote Command 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



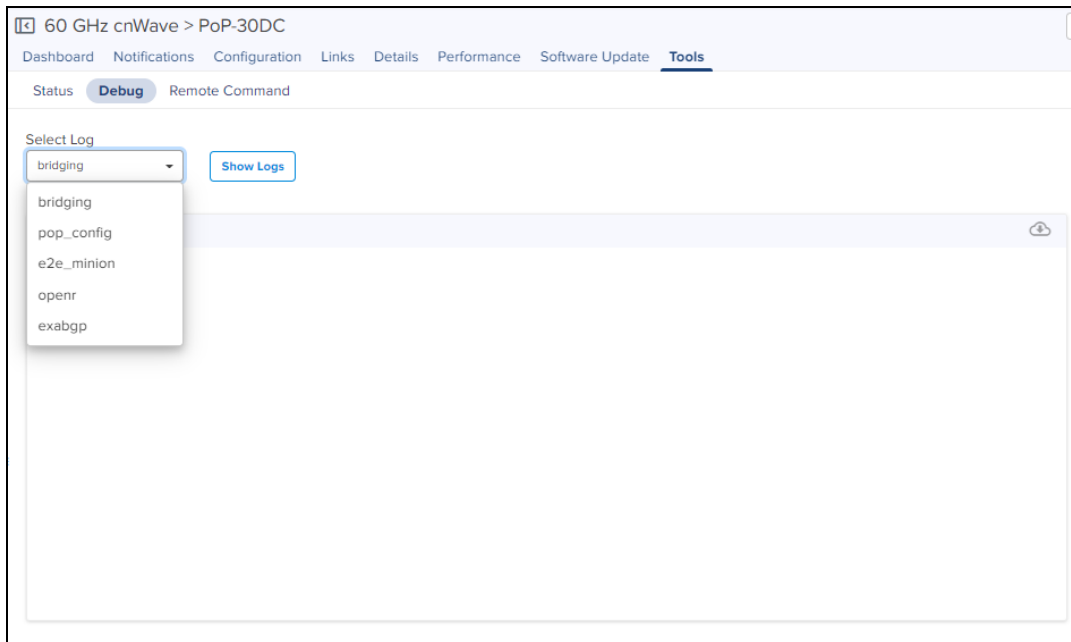
Debug

In **Debug** tab user view or download the PoP logs by executing the following log commands:

- Bridging
- pop-config
- e2e_minion
- openr
- exabgp



To view the logs, perform the following steps:

1. Navigate to **Tools > Debug**.
2. Select the required log name from the **Select Log** drop-down list box.



Once command is selected, it displays the output as shown below:



- Click  icon to download the generated output.
- Click  icon to refresh the generated output.

Remote Command

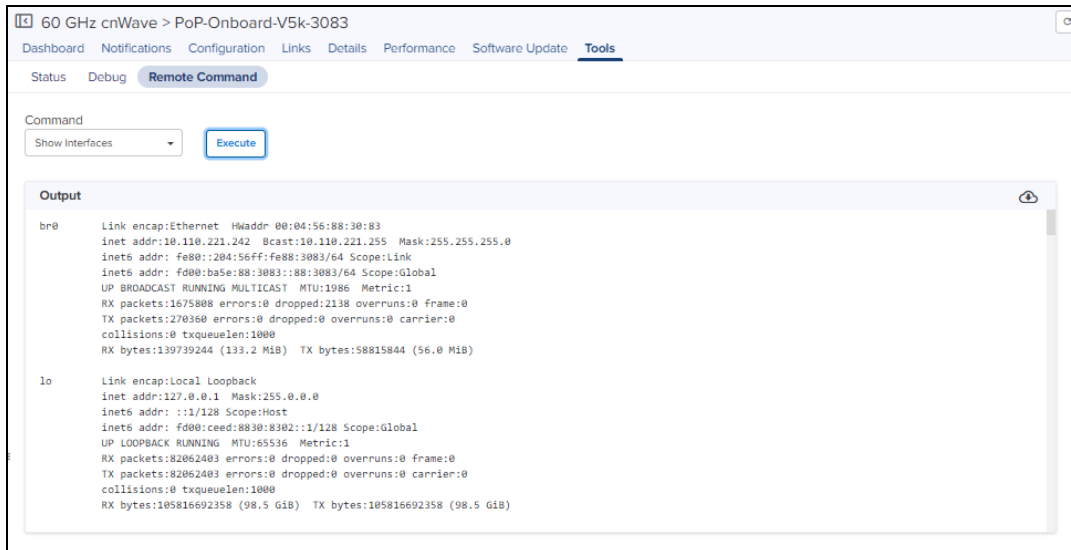
In **Remote command** tab user view or download Command logs by executing the following commands:


- Show Interfaces
- Show Routes
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show SFP Power Details (applicable for V5000 and V3000)

To Execute the command:

1. Navigate to **Tools > Debug**.
2. Select the required command from the **Command** drop-down list box.
3. Click **Execute**.

The output for the selected criteria appears as shown:



- Click the download  icon to download the generated output.

DN/CN Node

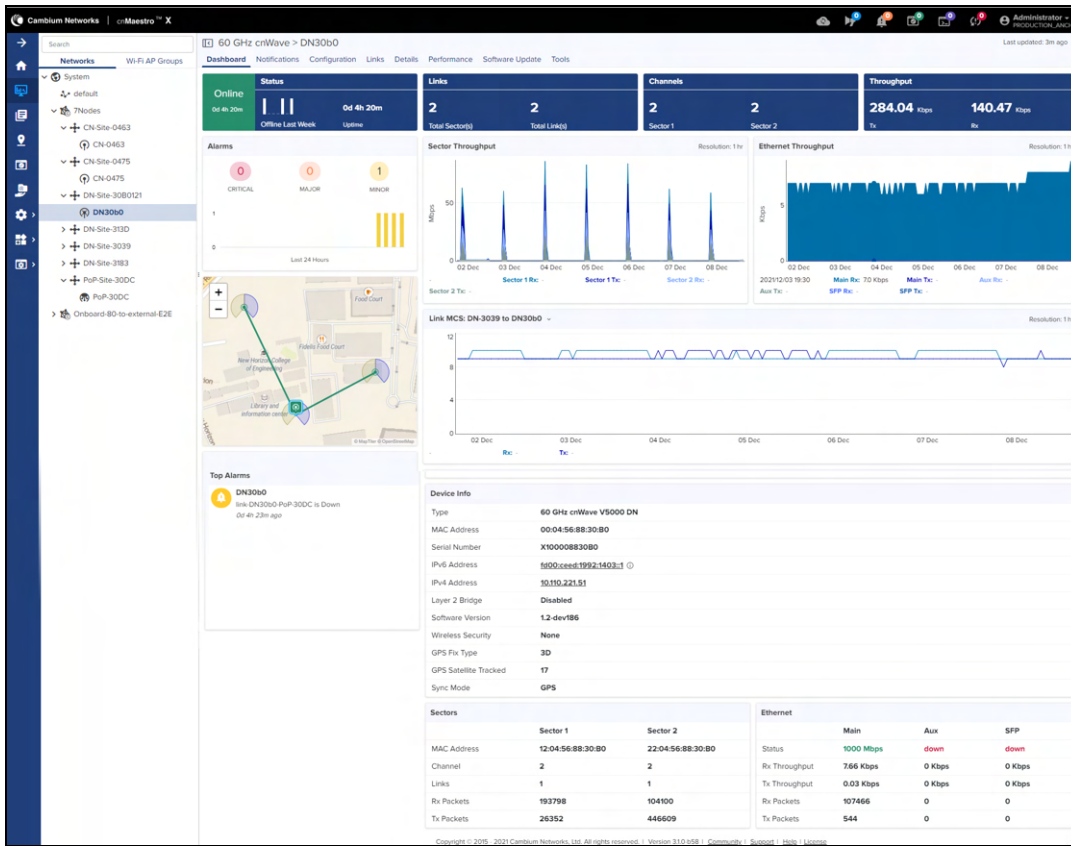
To create a new site, refer to [Site](#).

To create a sub 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 1)**, **Throughput (Sector 2)**, **Throughput (Main)**, **Throughput (Aux)**, **Throughput (SFP)**, **Alarms**, **Top Alarms**, **Links MCS**, **Device Info**, **Sectors**, and **Ethernet**.

Figure 111 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 **Description**, **Azimuth**, and **Elevation**.

Figure 112 Basic

60 GHz cnWave > CN-8b0463

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network VLAN Security Advanced

Name
CN-8b0463

Description


MAC Address
00:04:56:8B:04:63

Azimuth
0

Elevation
0

Save Reset

Radio

	NOTE: GPS option is not enable for v1000.
--	---

It allows the user to configure the **EIRP, Adaptive Modulation, Sectors (Channels and Golay), and GPS.**

Figure 113 Radio

60 GHz cnWave > CN-8b0463

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic **Radio** Network VLAN Security Advanced

EIRP

Maximum EIRP
38 Allowed range is 13 dBm to 38 dBm

IBF Transmit Power
 Short range (<25m) optimized Long range optimized Initial Beam Forming transmit power setting

Adaptive Modulation

Minimum MCS
2 Range - [2, 12]

Maximum MCS
12 Range - [2, 12]

Sector 1

Channel/Polarity should originate from leaf nodes. Please make sure to change on the CNs first and then higher up on the DNs.

Override	Name	Auto Configuration	Node Configuration
<input checked="" type="checkbox"/>	Channel	1	1
<input type="checkbox"/>	Polarity	Even	

Sector 1 Link (s) Golay

Override	Name	Auto Configuration (Rx/Tx)	Node Golay Rx	Node Golay Tx
<input type="checkbox"/>	link-CN-8b0463-DN-39	2/2		

[Override All](#)

Save Reset

Network

Network tab allows the user to edit the **Layer 3 CPE**, **IPv4 Management**, **Ethernet Ports**, and **Other Settings**.

Figure 114 Network

60 GHz cnWave > DN-3D

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic **Network** Radio VLAN Security Advanced

IPv6 Layer 3 CPE

IPv6 CPE interface
 Aux Main SFP Disabled Choose the interface to run IPv6 SLAAC. Subnet allocated by the controller will be used as Prefix. This interface will not be part of Layer 2 bridge. Should be disabled for IPv4 CPE.

IPv6 CPE Prefix
If empty, Subnet prefix allocated by the controller to the node will be used.

IPv4 Management

IPv4 Address
10.110.178.23 IPv4 Management access is not allowed over IPv6 CPE INTERFACE

Subnet Mask
255.255.255.0

Gateway IP Address
10.110.178.254

Ethernet Ports

Enable Main
 Enable Aux
 Enable SFP

Other Settings

Enable Aux port power Enables the power out on the Aux port

Relay Port Interface
 Aux Main SFP Disabled Wired interface on which OpenR is run. Should be used when DNs are connected back to back and on PoPs in a multi PoP network.

Save Reset

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 115 Security

The screenshot shows the configuration page for a Radius user in the 60 GHz cnWave interface. The breadcrumb path is "60 GHz cnWave > DN-3D". The "Configuration" menu is active, and the "Security" sub-tab is selected. The page contains three input fields: "Radius user identity" with the value "cambium", "Private key password" (empty), and "Radius user password" (empty). There are "Save" and "Reset" buttons at the bottom.

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 able to view, add, and edit **Field Name** and **Value**.

To add a field:

1. Navigate to **Configuration > Advanced**.
2. Click **Add New**.

60 GHz cnWave > CN-fa-cloud

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network VLAN Security **Advanced**

All the settings below are for advanced users only.

Search Table JSON Add New

Field	Description	Status	Value	
popParams.POP_STATIC_ROUTING	Enable static routing on ...	set	0	
popParams.VPP_ADDR	The IP address of the int...	unset		
popParams.POP_IFACE	The interface on the PO...	unset		
popParams.POP_BGP_ROUTING	Enable BGP routing on t...	set	0	
popParams.NAT64_IPV6_PREFIX	NAT64 IPv6 prefix. Can ...	unset		
popParams.NAT64_POP_ENABLED	Enable NAT64 on POP l...	set	0	
popParams.POP_ADDR	The IP address of the int...	unset		
popParams.GW_ADDR	The IP address of the G...	unset		
popParams.NAT64_IPV4_ADDR	IPv4 Address for NAT64 ...	unset		
snmpConfig.contact	System contact.	set	No Contact	
snmpConfig.location	System location.	set	No Location	
logTailParams.sources.terragraph_opentr_logs.enabled	Enable tailing from this s...	set	true	
logTailParams.sources.terragraph_opentr_logs.filename	The log file name.	set	/var/log/opentr/current	
logTailParams.sources.terragraph_minion_logs.filename	The log file name.	set	/var/log/e2e_minion/current	

Save Reset [Show Full Configuration](#)

3. Enter the **Field Name** and **Value**.

Add new field ✕

Field Name String ▼

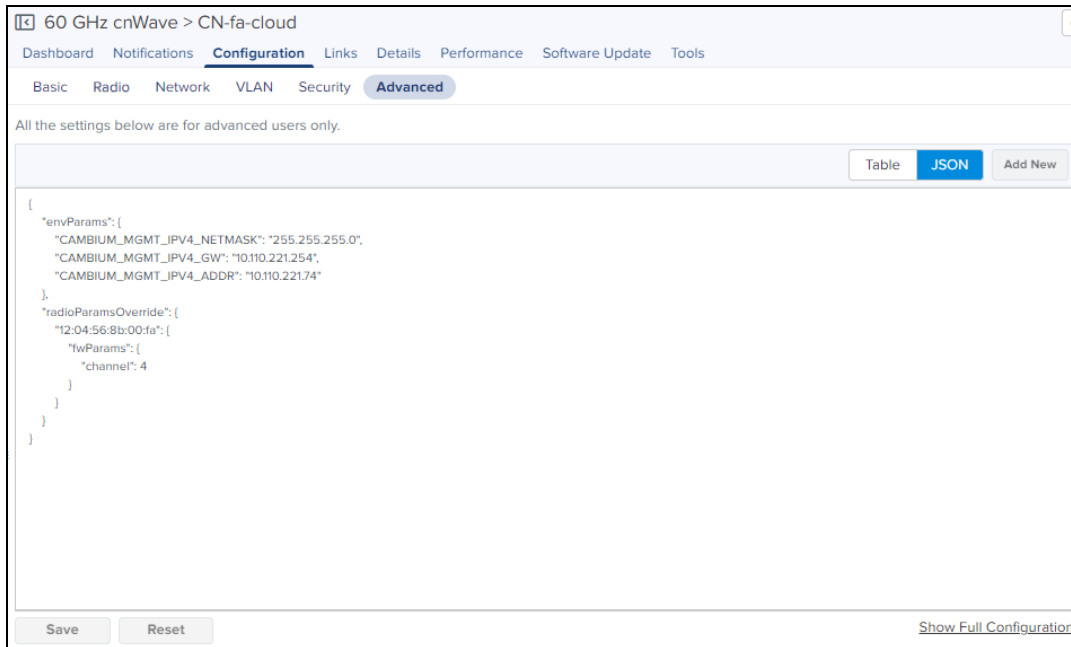
Value

Save Cancel

4. Click **Save**.

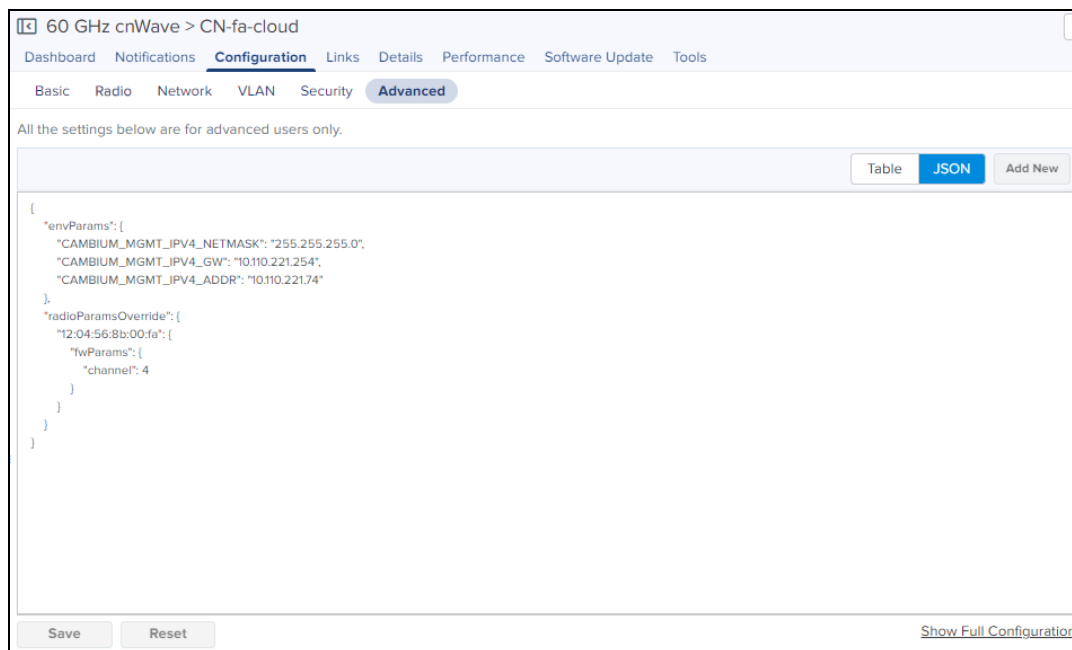
JSON

JSON allows Advanced user to view the JSON format.

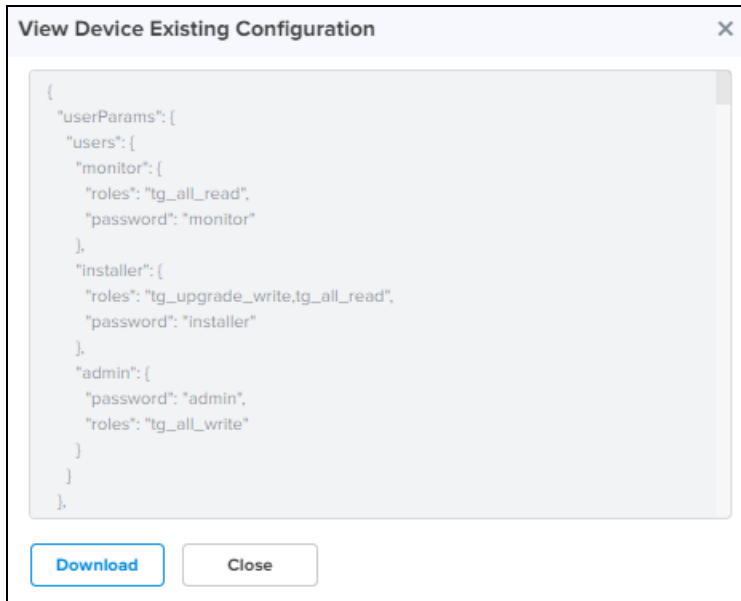


To download the file, perform the following steps:

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 116 List

Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	Link Time	Type	Ignition Attempts	Distance	Azimuth	Backup CN Link	Ignition Status
link-APDP DN 80	APDP	DN 80	12:04:56:88:30:DC	22:04:56:88:30:80	Yes	1d 15h 57m	Wireless	2	94	-178.1	No	Enabled
link-CN 75 DN 80	CN 75	DN 80	12:04:56:88:04:75	22:04:56:88:30:80	Yes	0d 5h 38m	Wireless	8031	171	-51.2	No	Enabled
link-CN 83 DN 80	CN 83	DN 80	12:04:56:88:31:83	22:04:56:88:30:80	Yes	0d 13h 30m	Wireless	21	71	52.7	No	Enabled
link-CN 39 DN 80	CN 39	DN 80	22:04:56:88:30:39	12:04:56:88:30:80	Yes	0d 9h 30m	Wireless	36	100	-70.5	No	Enabled

Statistics

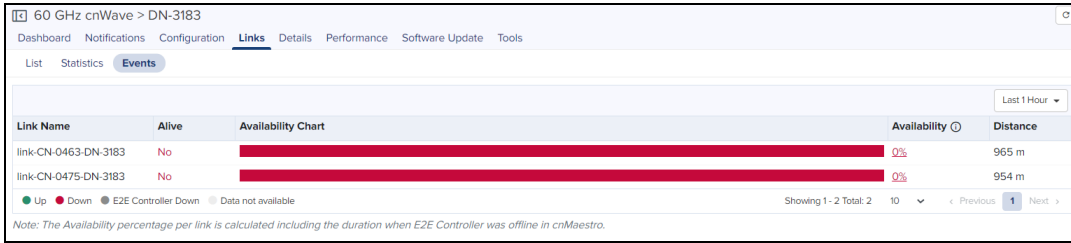
Links Statistics pages provides details of Name, Direction, A-Node Sector MAC, Z-Node Sector MAC, Alive, Link Time, RSSI, Tx Power Index, A-node, Z-node, Type, Distance, Azimuth, Rx MCS, Tx MCS, Rx PER, Tx PER, Rx SNR, Rx Beam Index, Tx Beam Index, EIRP, Rx Errors, Tx Errors, Rx Frames, Tx Frames on a single device, generally in a page format.

Name	Direction	A-Node Sector M.	Z-Node Sector M.	Alive	Link Time	RSSI	Rx SNR	Rx MCS	Tx Power Index	EIRP	Tx MCS
link-APDP DN 80	APDP to DN 80	12:04:56:88:30:DC	22:04:56:88:30:80	Yes	1d 15h 58m	40 dBm	32 dB	10	6	13 dBm	9
link-APDP DN 80	DN 80 to APDP	12:04:56:88:30:DC	22:04:56:88:30:80	Yes	1d 15h 58m	37 dBm	32 dB	10	6	13 dBm	10
link-CN 75 DN 80	CN 75 to DN 80	12:04:56:88:04:75	22:04:56:88:30:80	Yes	0d 5h 39m	62 dBm	12 dB	7	6	13 dBm	9
link-CN 75 DN 80	DN 80 to CN 75	12:04:56:88:04:75	22:04:56:88:30:80	Yes	0d 5h 39m	48 dBm	25 dB	9	23	30 dBm	9
link-CN 83 DN 80	CN 83 to DN 80	12:04:56:88:31:83	22:04:56:88:30:80	Yes	0d 13h 30m	53 dBm	21 dB	9	6	35 dBm	9
link-CN 83 DN 80	DN 80 to CN 83	12:04:56:88:31:83	22:04:56:88:30:80	Yes	0d 13h 30m	49 dBm	23 dB	9	6	13 dBm	9
link-CN 39 DN 80	CN 39 to DN 80	22:04:56:88:30:39	12:04:56:88:30:80	Yes	0d 9h 30m	48 dBm	25 dB	9	6	13 dBm	10
link-CN 39 DN 80	DN 80 to CN 39	22:04:56:88:30:39	12:04:56:88:30:80	Yes	0d 9h 30m	45 dBm	28 dB	9	6	13 dBm	9

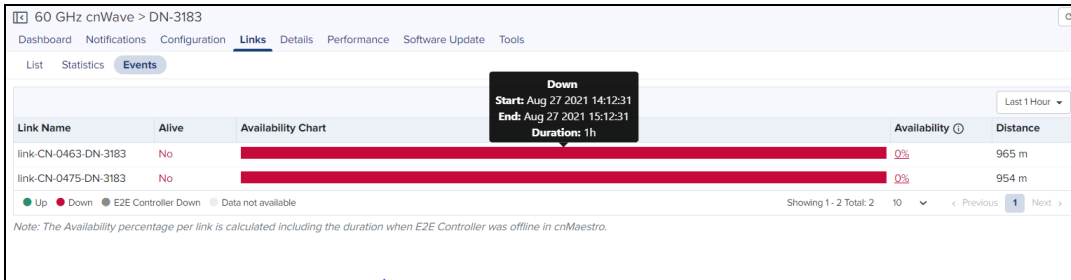
Events

Events provides the details of the links from last 1 hour to 7 Days, Ignition Attempts and Distance.

Figure 117 Events



It also calculates the Availability percentage per link, including the duration when E2E Controller was offline in cnMaestro.



Tools

In Tools page user can able to view the **Status**, **Debug** and **Remote Command** 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

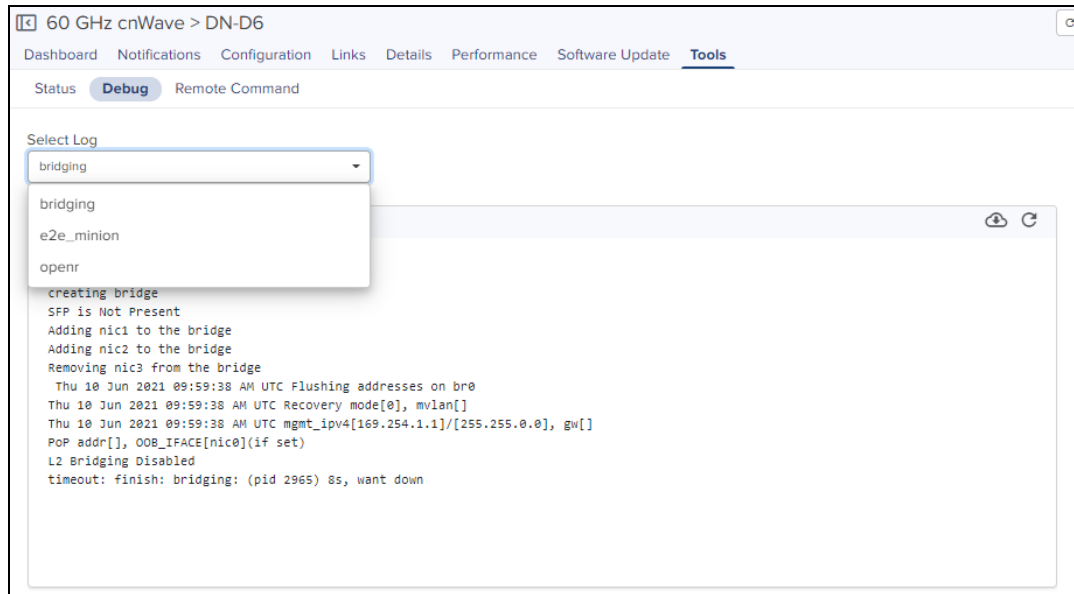
In **Debug** tab user can able to view or download the DN or CN logs by executing the following log commands:



- Bridging
- e2e_minion
- openr

To view the logs:

1. Navigate to **Tools > Debug**.
2. Select the required log name from the **Select Log** drop-down list box.

The output for the selected criteria appears as shown:



- Click the download  icon to download the generated output.
- Click the refresh  icon to refresh the generated output.

Remote Command

In **Remote command** tab user can able to view or download Command logs by executing the following commands:

- Show Interfaces
- Show Routes
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show SFP Power Details (applicable for V5000 an V3000)

To Execute the command:

1. Navigate to **Tools > Remote Command**.
2. Select the required command from the **Command** drop-down list box.
3. Click **Execute**.

The output for the selected criteria appears as shown:

60 GHz cnWave > CN-fa-cloud

Dashboard Notifications Configuration Links Details Performance Software Update **Tools**

Status Debug **Remote Command**

Command

Show Interfaces

Output


```

br0    Link encap:Ethernet  Hwaddr 00:04:56:8b:00:fa
       inet addr:10.110.221.239  Bcast:10.110.221.255  Mask:255.255.255.0
       inet6 addr: fe80::294:56ff:fe8b:fa/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1986  Metric:1
       RX packets:7897304 errors:0 dropped:9911 overruns:0 frame:0
       TX packets:109695 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:744361659 (709.8 MiB)  TX bytes:16924389 (16.1 MiB)

lo     Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       inet6 addr: fd00::cecd:8830:8303::1/128 Scope:Global
       UP LOOPBACK RUNNING  MTU:65536  Metric:1
       RX packets:385211774 errors:0 dropped:0 overruns:0 frame:0
       TX packets:385211774 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:262933754910 (244.8 GiB)  TX bytes:262933754910 (244.8 GiB)

nic1   Link encap:Ethernet  Hwaddr 00:04:56:8b:00:fa

```

- Click the download  icon to download the generated output.

Auto-Provisioning

cnMaestro On-Premises supports Auto-Provisioning for Wireless LAN devices (cnVision, Wi-Fi, and ePMP 1000 Hotspot) and fixed devices (PMP and ePMP). It is enabled at **Shared Settings > Auto-Provisioning**, and it allows one to automatically configure and approve devices based upon IP address.



NOTE:
Auto-Provisioning is supported only for cnMaestro On-Premises.

Creating Auto-Provisioning Rule

To create a rule for Auto-Provisioning, perform the following steps:

1. Navigate to **Shared Settings > Auto-Provisioning** page.

Shared Settings > Auto-Provisioning x

Automatically configure devices based upon its source subnet. Approved devices will automatically be configured and onboarded. Unapproved devices will be added to the Onboarding Queue and must be manually approved prior to onboarding. [Learn more](#)

Subnet (CIDR)	Device Type	Managed Account	Network	Site/Tower	Profile/Template	Description	Approve	Action
10.10.224.0/24	cnPilot Home (R-Series)	J\$M\$P	default				true	

Save

2. Click **Add** and following window appears.

Figure 118 Auto-Provisioning - Wireless Devices

Add Auto-Provisioning Rules [X]

Subnet (CIDR) ⓘ
xxx.xxx.xxx.xxx/xx

Device Type
cnPilot Home (R-Series) ▼

Managed Account
Base Infrastructure ▼

Network
default ▼

Site
None ▼

Configuration Method
 AP Group Template

AP Group
None ▼

Description
[Text Field]

Approve

Add **Cancel**

Figure 119 Auto-Provisioning - Fixed Devices

Add Auto-Provisioning Rules

Subnet (CIDR) ⓘ
xxx.xxx.xxx.xxx/xx

Device Type
ePMP

Managed Account
Base Infrastructure

Network
default

Tower
None

Template
None

Description

Approve

Add Cancel

3. Enter the following details:

- **Subnet:** 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, cnVision, Home (R-Series), ePMP, or 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:** Under which site the device should be onboarded, once device contacts the server, applicable for Enterprise (E) or Home (R).
- **Tower:** Under which site the device should be onboarded, once device contacts the server, applicable for ePMP AP or PMP AP.
- **Template:** To which template to be applied on the device when onboarding, once device contacts the server, applicable for ePMP AP or PMP AP.
- **AP Group:** To which AP Group to be applied on the device when onboarding, once device contacts the server, applicable for Enterprise (E) or Home (R).
- **Description:** Type the information to add additionally.
- **Approve:** The device should be auto-approve or needs manual approval for onboarding.

4. Click **ADD**.

Services

This section includes the following topics:

- [Managed Service Provider \(MSP\)](#)
- [API Client](#)
- [cnPilot Guest Access](#)
- [cnPilot Data Tunnels](#)
- [SNMP](#)
- [RADIUS Proxy](#)

Managed Service Provider (MSP)

This section includes the following topics:

- [Overview](#)
- [Configuring Managed Services](#)
- [Managed Services Administration](#)

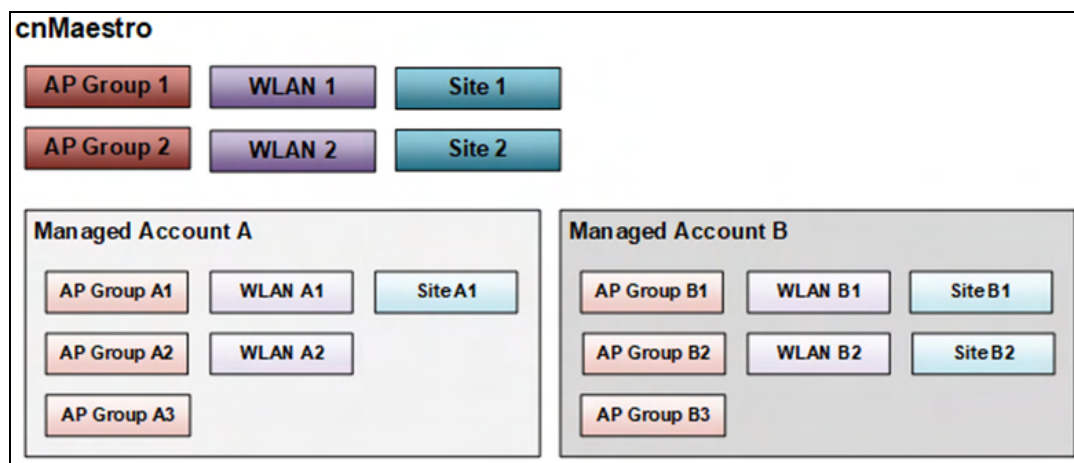
Overview

Managed Service Provider (MSP) allows a cnMaestro account owner to partition their installation into separate Managed Accounts – each with its own independent administration and configuration. This feature is for managed service providers who want to provision a full cnMaestro infrastructure for their customers but still maintain control over the individual deployments.

Managed Accounts

Managed Accounts group cnMaestro devices and configuration objects (such as AP Groups, WLANs, and Sites) into administration domains within a single cnMaestro instance. Managed Accounts are independent, and the devices added to them are configured using the objects in the Managed Account.

Figure 120 Managed Accounts



Scope

An account with MSP enabled has three scopes:

1. Global Scope for entities (Devices, Networks, Sites, etc.) that exist outside of Managed Accounts and are only available to Global cnMaestro Administrators.
2. Managed Account Scope for entities in Managed Accounts and accessible to Global Administrators and Managed Account Administrators.
3. Shared Scope applies to management objects such as AP Groups, WLANs, and Switch Groups. Shared Scope objects can be used across all Managed Accounts but not modified by them, though they can be copied into the Managed Account and then changed.

Access Points

Access Points exist in the global cnMaestro application, or they can be added to a single Managed Account.


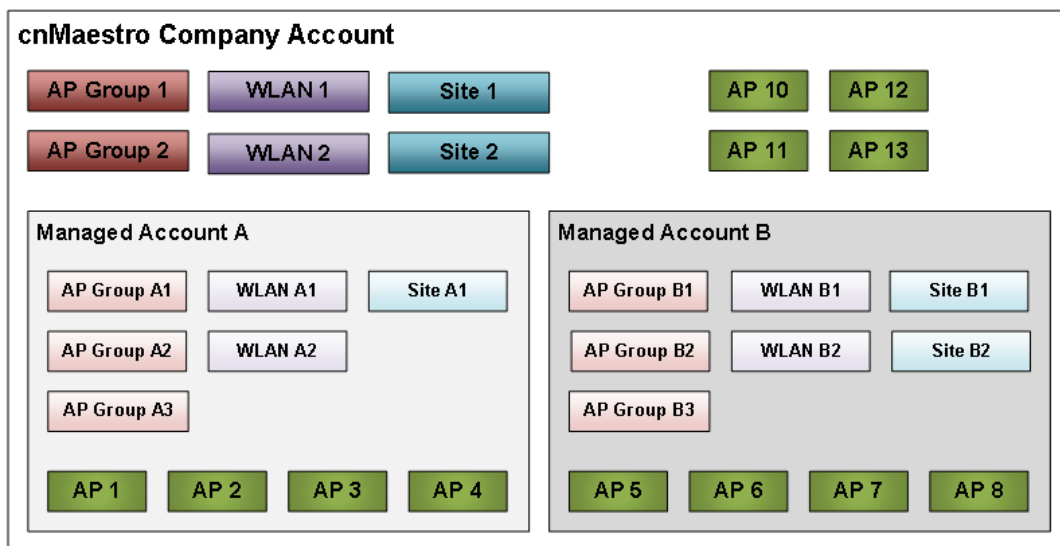
	NOTE: The Managed Service Provider feature supports all device types available within cnMaestro.
---	--

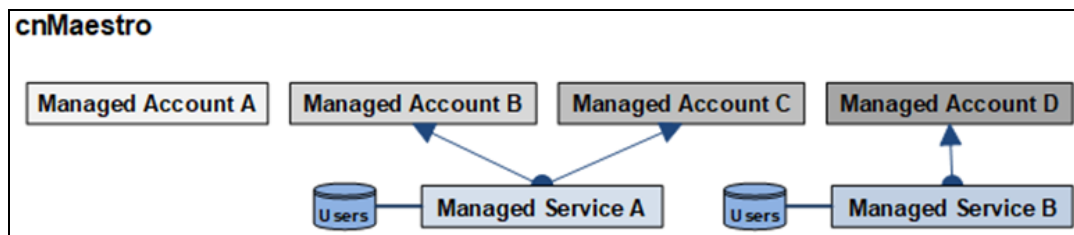
Figure 121 Access Points



Managed Service

A Managed Service creates customized version of the cnMaestro UI and assigns Managed Accounts. Each Managed Service can be mapped to many Managed Accounts.

Figure 122 Managed Service



Each Managed Service adds the following support to a Managed Account:

Support	Details
Administrator Database	Each Managed Service has its own independent database of users who can be assigned to multiple Managed Accounts.
Custom Login URL	The path of the Login URL used by Managed Service Administration can be tailored to represent the Managed Service. The path must be unique across all cnMaestro.
Managed Account UI	The Managed Account UI is customized for the Managed Service through graphics, colors, and text.

Managed Account UI

The Managed Account UI can be customized to represent the brand. A sample Managed Account UI is shown below:

Figure 123 Managed Account UI - Sample 1

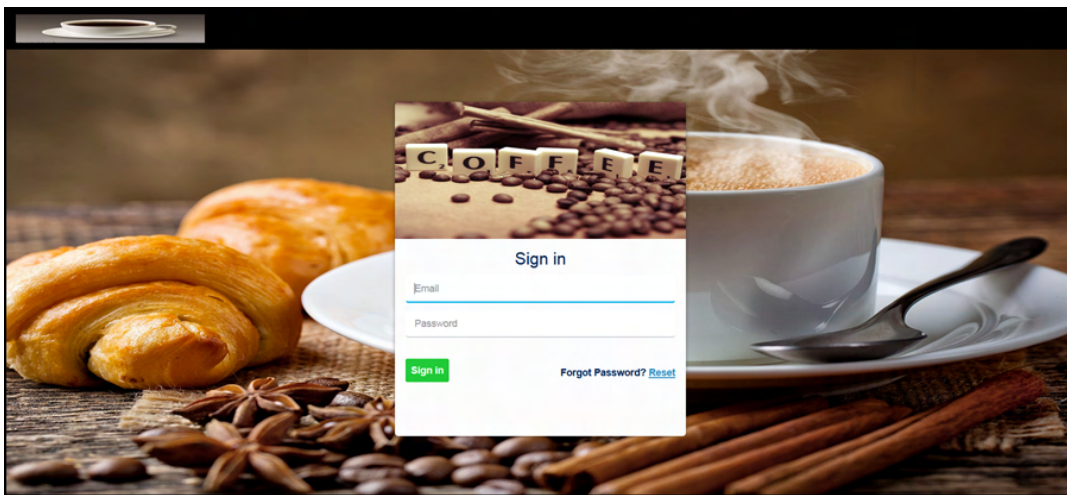
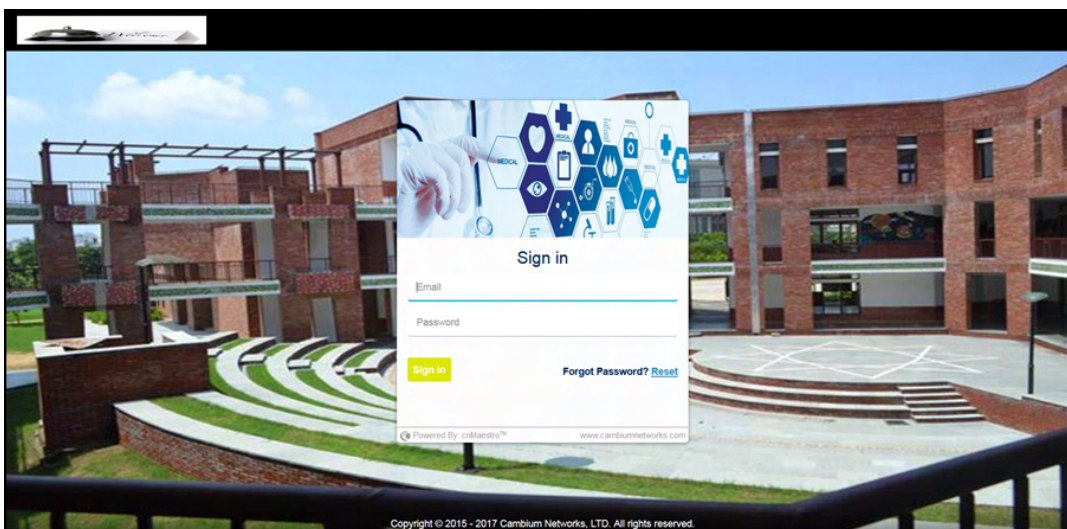


Figure 124 Managed Account UI - Sample 2



Managed Service Provider (MSP)

The MSP feature combines Managed Accounts with Managed Services.

Managed Service Provider**=****Managed Account****+****Managed Service**

Managed Service Users (Administrators)

Managed Service Users are assigned to Managed Accounts. They access nearly all the same features as the Global cnMaestro Administrators, except they are only allowed to manage the subset of devices and objects (AP Groups, WLAN, Sites, etc.) in their account.

Managed Service Users (Administrators) Roles

Managed Service Administrators 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 38: 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	Networks, Tower, and Site creation	All	All	View
Application Operations 2	Tech Dump, import/export server data, account type change (backhaul and Wi-Fi)	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	None	None	None

Table 38: Tenant Administrator Roles

Feature	Description	Administrator	Operator	Monitor
Administrator only)				
Audit logs	Log administration updates	All	All	All
Data Tunnel (Global cnMaestro Administrator only)	Data Tunnel configuration	None	None	None
Device Operations	Reboot device, Link Test, Connectivity Test	All	All	None
Device Override	Per-device configuration changes	All	All	View
Global Configuration	Templates and AP Groups; ability to apply configuration	All	View	View
Guest Portal	Guest Access	All	View	View (Sessions)
Monitoring	Statistics data from device	All	All	View
Notifications	Alarms and Events	All	All	View
Onboarding	Device approval	All	All	View
Reporting	Report generation view	All	All	All
Software Images (Global cnMaestro Administrator only)	Download device software images	All	None	None
System Operations	Reboot VM, change log level, system upgrade, system monitoring	None (Except System Monitoring)	None (Except System Monitoring)	None (Except System Monitoring)
Software Upgrade	Upgrade device	All	All	View
User Management	Manage users, roles, sessions	All	None	None

Configuring Managed Services

This section provides the following configuration details for Managed Services:

- Enable Managed Service Provider (MSP)
- Create Managed Services
- Create Managed Account
- Validate Managed Account Administrators

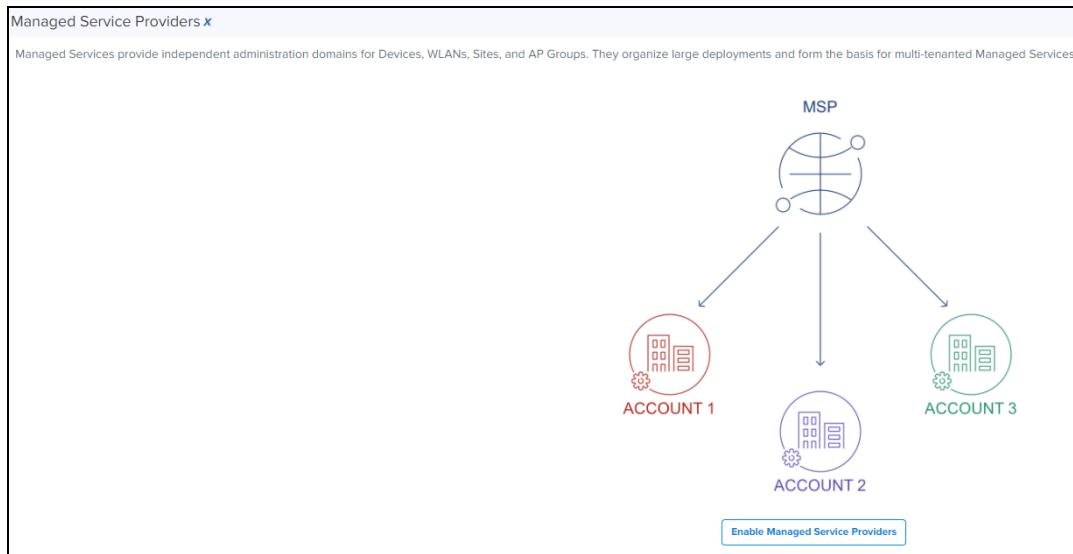
Enable Managed Service Provider (MSP)

By default, MSP is disabled in the cnMaestro UI.

To enable MSP:

1. Navigate to **Managed Service Providers** in the side-menu.
2. Click **Enable Managed Services**.

Figure 125 Enabling Managed Services



Additions in the cnMaestro UI when Managed Services is Enabled

- Once Managed Services is enabled, **Managed Account** and **Managed Services** tabs appears in the cnMaestro UI. The Managed Services page is replaced with Managed Accounts and Managed Services tables as shown below:

Figure 126 Managed Account and Managed Services Tabs

Name	Friendly Name	Managed Service	Status	Users	Networks	Devices	Alarms
JES:MIU			Enabled	0	2	25 of 25 offline	
Sys_MSP	Test	default	Enabled	0	1	2 of 2 offline	
TestACL:MSP	API mgmt Sys	Home_Mgmt	Enabled	1	1	0 of 0 offline	

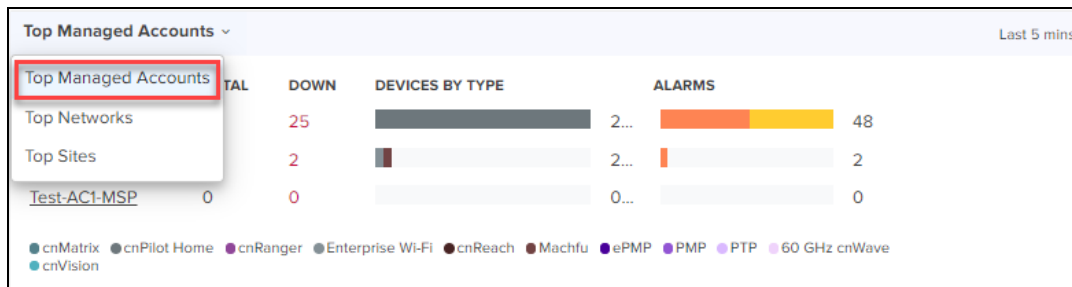
- The Header adds a select box that allows the global administrator to enter the context of Managed Accounts.

Figure 127 MSP Component in Header



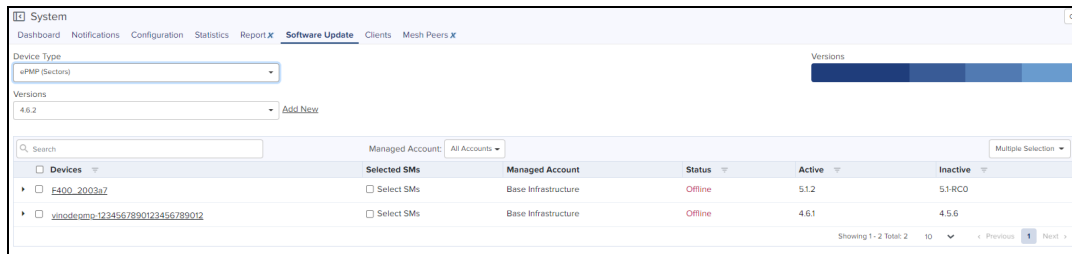
- The System Dashboard adds a Health component for Managed Accounts.

Figure 128 Dashboard > Managed Accounts



- Global tabs in the UI are updated with a Managed Account column.

Figure 129 Managed Account column



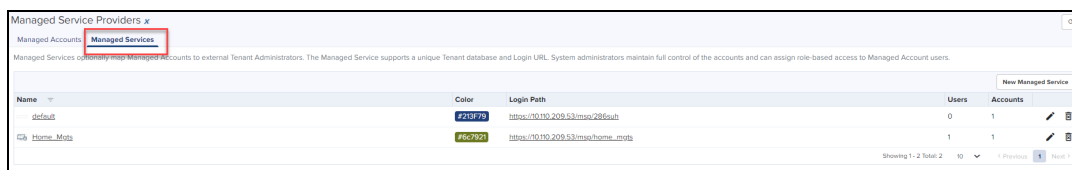
Create Managed Services

The user can create a Managed Service and map it to a Managed Account. The Managed Service supports an independent user database and a customized user interface. There is a default Managed Service, so creating a new service is optional.

Perform the following steps to create a Managed Service:

1. Select **Managed Service Providers** in the side-menu and select the **Managed Services** tab.

Figure 130 Managed Services tab



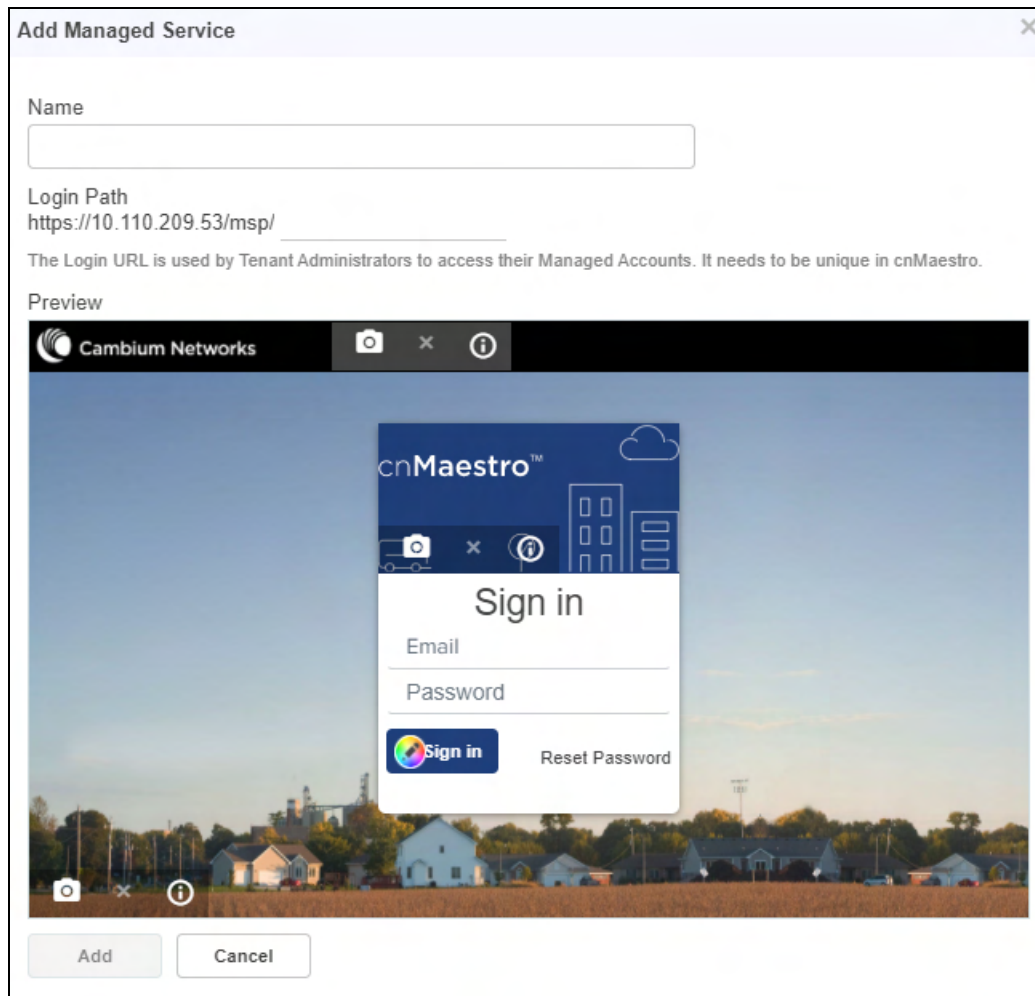
2. Click **Managed Service**.

Figure 131 Adding a New Managed Service



The following window appears.

Figure 132 Add New Managed Service window



3. Enter the following details:

Table 39: New Managed Service parameters

Parameter	Description
Name	Name of the service. This name is visible to Managed Account Administrators. A maximum of 64 characters are supported for the name.
Login Path	Managed Account Administrators log into cnMaestro using a standard URL with an additional Path that defines the Managed Service. For example: <a href="https://<cnmaestro on-premises ip>/msp/<Managed_service_path>">https://<cnmaestro on-premises ip>/msp/<Managed_service_path> Note: <ul style="list-style-type: none"> The Path name must be unique across all Managed Service accounts when cnMaestro is hosted in the Cambium Cloud. A maximum of 16 characters are supported for the path.

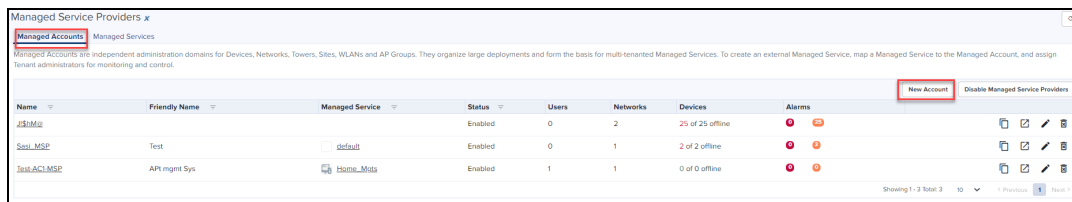
4. Click **Add**.

Create Managed Account

Perform the following steps to create a Managed Account:

1. Select **Managed Service Providers** in the side-menu and select the **Managed Account** tab.
2. Click **New Account**.

Figure 133 Managed Account tab



The following window appears:

Figure 134 Add Managed Account window

Add Managed Account

Name*

Friendly Name

Status

Enabled Disabled

Managed Service

default

ⓘ The Managed Service supports unique UI branding and Login URL.

Email

Role

Administrator

ⓘ Access all functionality, including adding/deleting local users.

3. Enter the following details:


Table 40: Managed Account parameters

Parameter	Description
Name	Name of the Managed Account. This is sent in the invitation email when Managed Account Administrators 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 Managed Account Administrators are logged out.

Table 40: Managed Account parameters

Parameter	Description
Managed Service	The Managed Service used for Managed Account Administrator.
Email	The email address of the first Managed Account Administrator. You can add more Users after the account has been created.
Role	The role of the Managed Account Administrator (Administrator, Operator, Monitor).

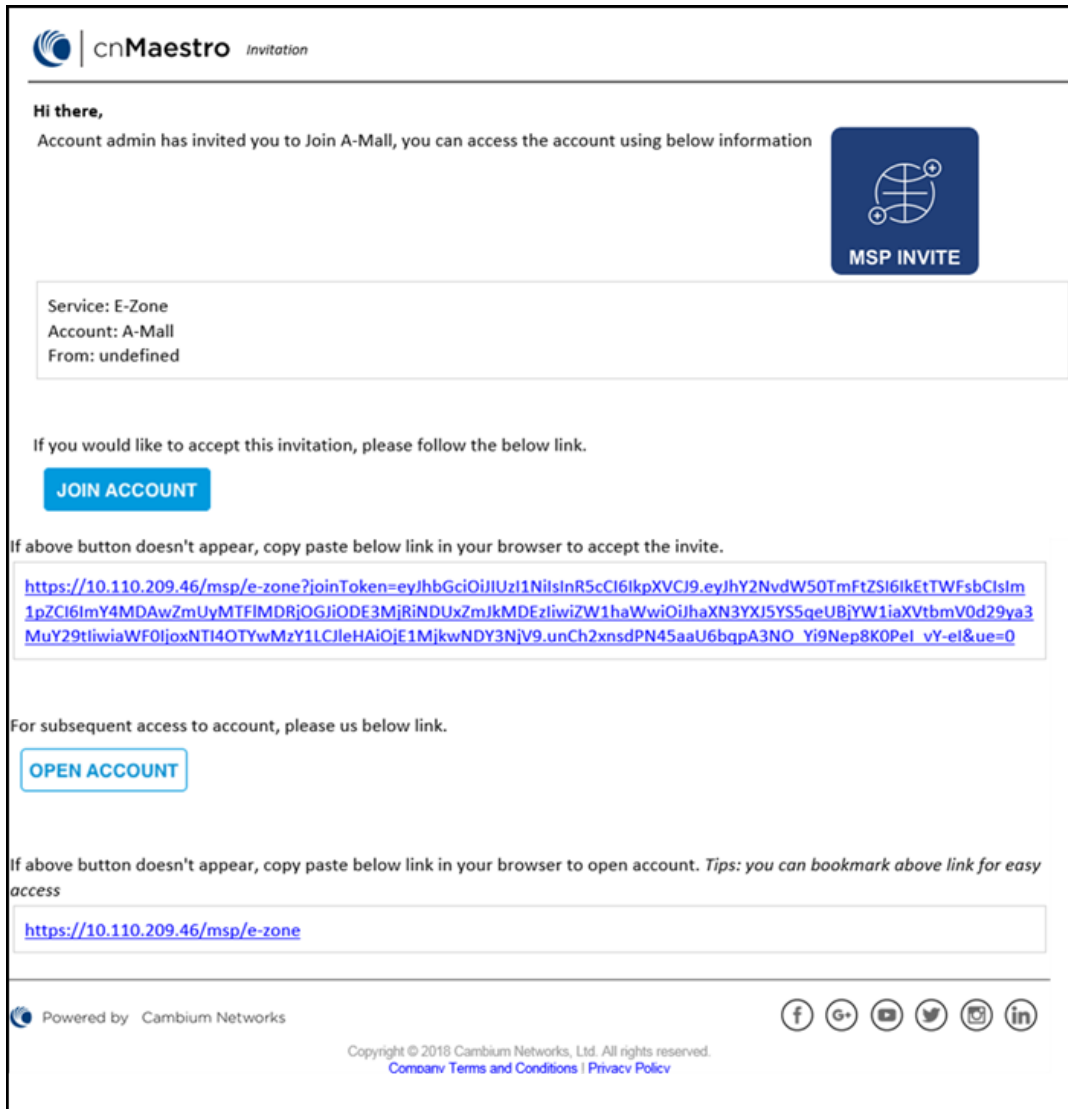
4. Click **Add**.

	NOTE: Users are allowed to edit the existing name of the Managed Account before validating the account.
---	---

Validate Managed Account Administrators

Once a Managed Account is created, the Managed Account Administrator is sent an email invitation. The email provides directions on how to access the Managed Account UI and set their password.

Figure 135 Sample Email invitation



Check Email for invite

An email is sent inviting the Managed Account Administrator to view their new Managed Service account. It has a link that must be clicked to enable access.

Figure 136 Checking Managed Account Administrator User Email



Create Account in Branded 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 Managed Service, they can use their existing email login to accept the invite for the new account. Switching between accounts is accomplished using the choice box in the UI header (upper-right).

Login to the Managed Account UI

Once the Managed Account Administrator (User) is created, use the Managed Service URL to login.

Figure 137 A Sample Login URL



Managed Services Administration

Overview

Once Managed Services is enabled, there are three ways for administrator to Managed Accounts.

- System View
- Managed Account View
- Managed Account Administrator (User) View

Important Points to Remember

Please note the following points for managed services administration:



NOTE:

- When a device is moved from one Managed 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 Service Provider feature can be disabled only if all devices in Managed Accounts are deleted or moved to Base Infrastructure account.
- Administrators of any Managed Accounts do not have access to the settings page of the On-Premises server to change the account type.
- When Global Super Administrators trigger Configure/Software/Reports Jobs, the Managed Account users cannot view them in any of the Managed Accounts.
- When Managed 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 Managed Accounts.
- The devices that have not started Software/Configure Jobs cannot be moved across Managed Accounts.
- The Global Super Administrator and the Managed 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 a Managed Account Administrator, the Auto Synchronization Job starts automatically with the configuration job ID as in Managed Account and reflects in both the Global Super Administrator and Managed Account Administrator accounts.

System View

At the System level, one can view APs, AP Groups, or Sites across all Managed Services 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 the Managed Accounts.

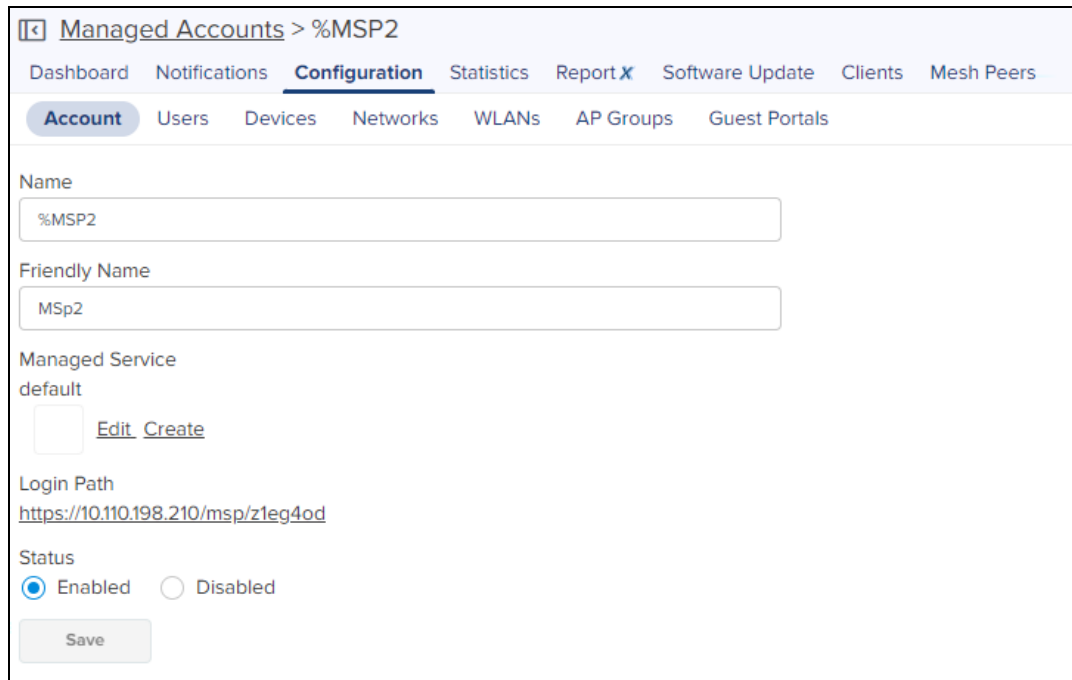
Figure 138 System View

Device	Managed Account	Health	Onboarding Status	Serial Number	IP Address	Type	AP Group	Tower/Site	Client Count
XV3-8-376F34	Base Infrastructure	Offline 12d 5h 12m	Onboarded 28d 7h 30m		10.110.208.12	XV3-8	Import_242qq	E-type	0

Managed Account View

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

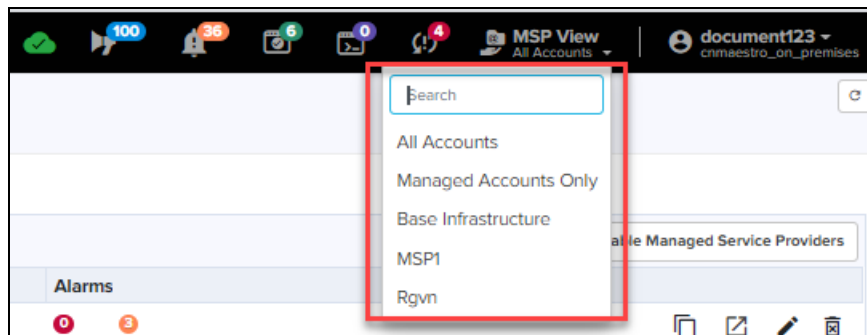
Figure 139 Managed Account View



Managed Account Administrator (User) View

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

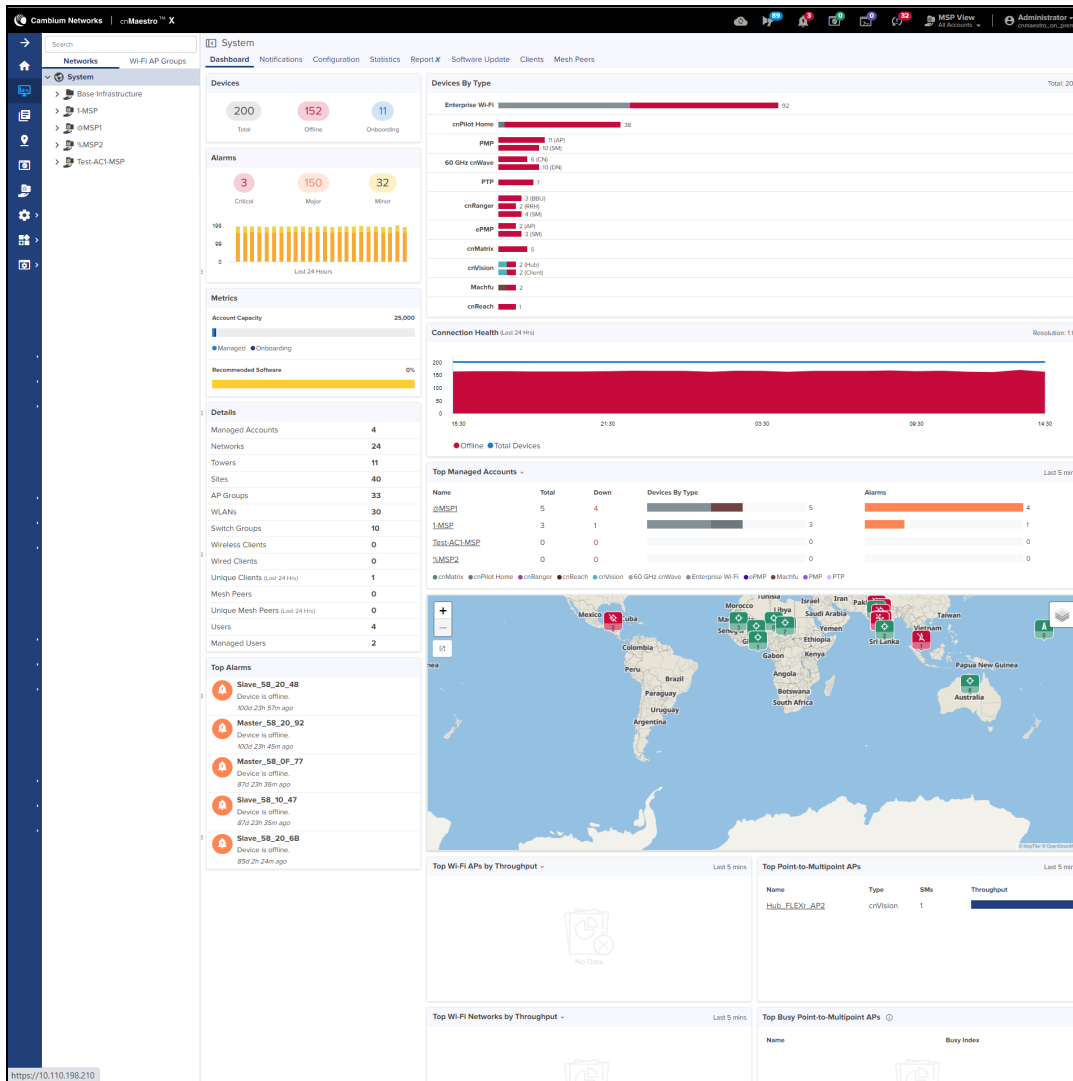
Figure 140 Managed Account View



System Dashboard

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

Figure 141 System Dashboard



Managed Account Administration

Object Scope

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

Table 41: Accessibility Scopes

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

**NOTE:**

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

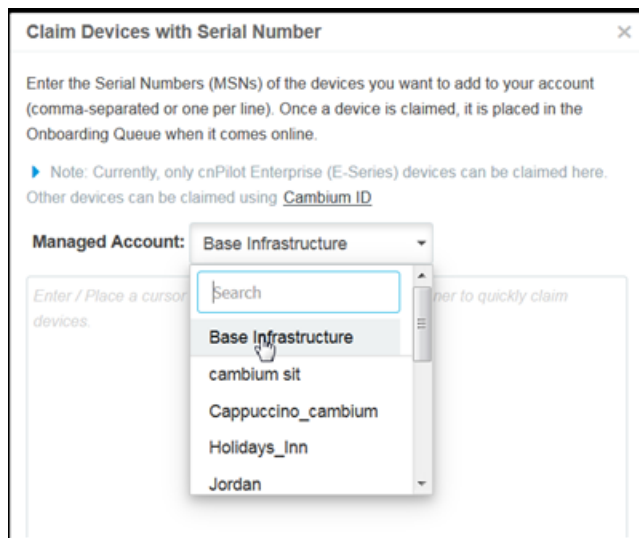
Device Management

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

System Onboarding

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

Figure 142 System Onboarding



Management Account Onboarding

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

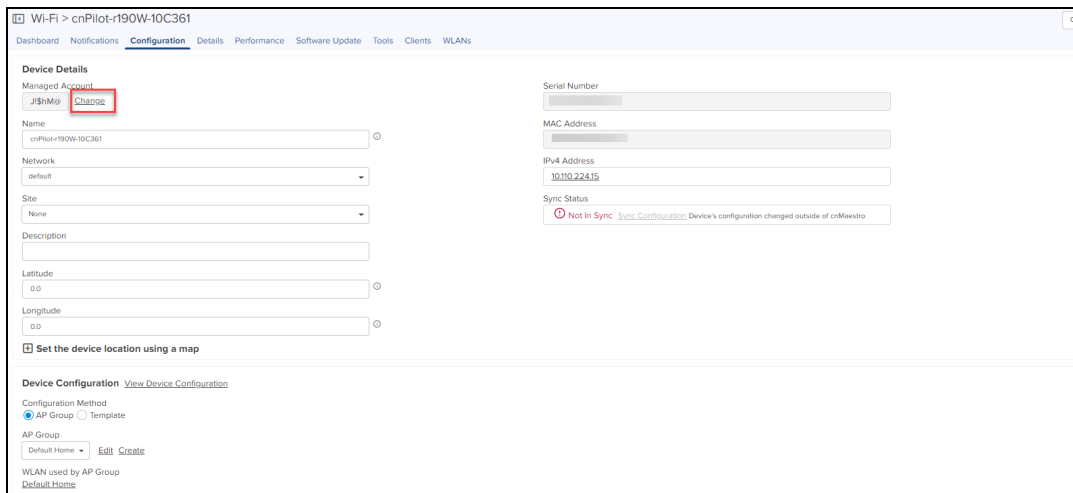
**NOTE:**

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

Moving a Device Between Managed Accounts

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

Figure 143 Moving a Device Between Managed Accounts



In Enterprise View, the device can be moved between Managed Accounts using a **Managed Account** icon in the Inventory tab.

Figure 144 Moving a device between Managed Accounts in Enterprise View

Managed Account	Status	Serial Number	IP Address	Type	AP Group	Site	Action
Regalia_Bengaluru	Offline (0d 23h 8m) Onboarded		10.110.208.164	cnPilot E500	fdghgf	EyeBis	[Managed Account Icon]
gayatri	Online (21d 23h 16m) Onboarded	N/A	10.110.208.123	ePMP 1000 Hotspot	N/A	eclients	[Action Icons]
gayatri	Online (21d 23h 15m) Onboarded		10.110.208.121	cnPilot E500	Default Enterprise		[Action Icons]
gayatri	Online (0d 22h 44m) Onboarded		10.110.208.122	cnPilot E410	fdghgf		[Action Icons]
Regalia_Bengaluru	Offline (1d 2h 31m) Onboarded		10.110.202.104	cnPilot E500	HT_Test_RGVN	EyeBis	[Action Icons]
Regalia_Bengaluru	Offline (1d 23h 49m) Waiting for Device	N/A	N/A	cnPilot	N/A		[Action Icons]
Ahmedabad	Online (0d 14h 37m) Onboarded		10.110.202.105	cnPilot E400	N/A	Ahmd-Building1	[Action Icons]
Base Infrastructure	Online (0d 23h 4m) Onboarded	N/A	10.110.32.137	cnPilot E400	Default Enterprise		[Action Icons]
Hyderabad_Tikona	Online (5d 2h 2m) Onboarded		10.110.202.103	cnPilot E400	For-E400-103	Hyd-Building1	[Action Icons]

Managed Account Deletion



NOTE:
All devices must be removed from the Managed Account before deleting it.

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

Figure 145 Managed Account Deletion

Name	Friendly Name	Managed Service	Status	Users	Networks	Devices	Alarms	Action
JShMa			Enabled	0	2	25 of 25 offline	[Alarms]	[Action Icons]
Sasi_MSP	Test	default	Enabled	0	1	2 of 2 offline	[Alarms]	[Action Icons]
TestACL:MSP	APs mgmt Sys	Home_Mgmt	Enabled	1	1	0 of 0 offline	[Alarms]	[Action Icons]

Disabling Managed Service Provider Feature

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



NOTE:

In the current release, only the global administrator of On-Premises account has control on the following features:

- Association ACL
- Auto-Provisioning
- Scheduled Backup
- Server Settings
- SMTP Server
- SNMP Configuration


API Client

Overview

cnMaestro supports a RESTful API as part of its On-Premises deployment. This API allows customers to read data and perform operations programmatically using their own client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. Modern programming languages have rich support for RESTful interfaces.

API Clients

API Clients are external applications that access the RESTful API over HTTPS using OAuth 2.0 Authentication. They require a Client ID and Client Secret for access, both of which are detailed later in this section. They are configured by navigating to **Services > API Clients**.

Application Name	Application Description	Client Id	Swagger	Actions
Test-App-20Jan	Test-NBAPI	rNc1BbrNcGsp2tg	JvUc2ud	  

RESTful API Specification

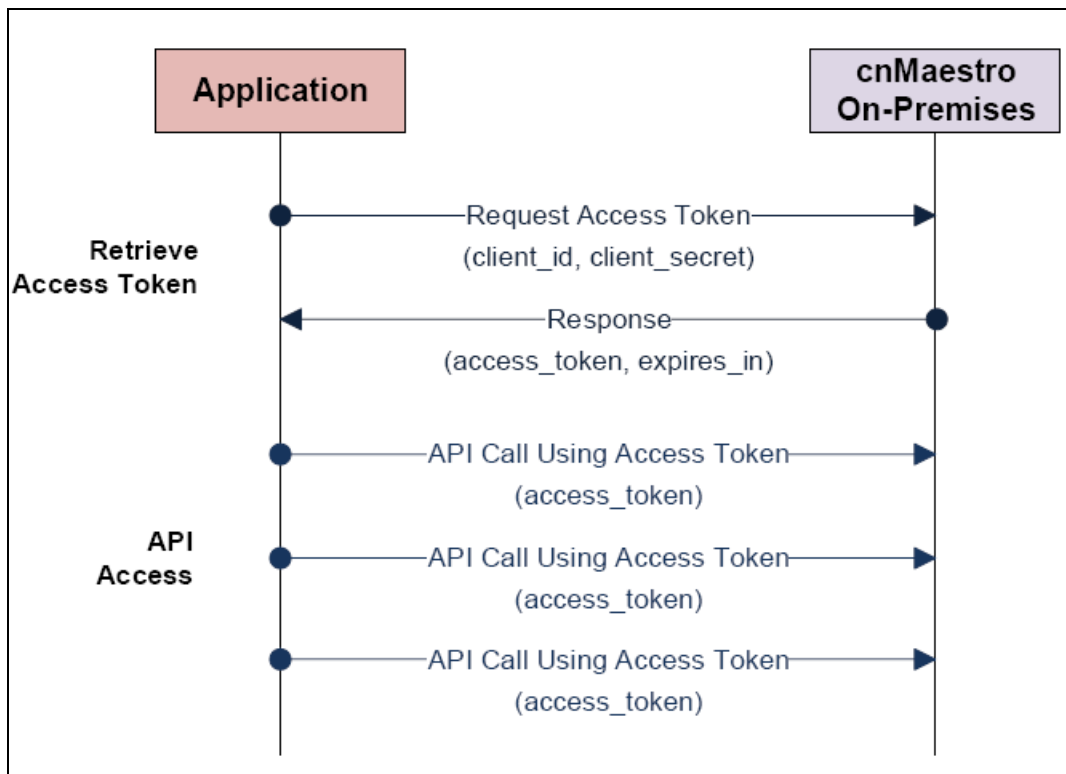


NOTE:

The cnMaestro API is changing to v2 in the 3.0 Release. v1 continues to be supported through 3.1.x. Cambium Networks recommends using v2 on any new API applications and updating from v1 as soon as possible. The changes to the v2 API are limited and described later in this chapter.

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.



Establishing 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 with 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

With the Access Token, the application can make cnMaestro API calls. The token is sent in an Authentication header on each API request. 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. Tokens will expire immediately if the Client API account that created them is deleted. The default expiration time for a token is 3600 seconds (1 hour). This is configurable in the UI.

Concurrent Access

Each client supports a single Access Token or multiple Access Tokens. Multiple Access Tokens allows concurrent access.

Single Access Token

If only one Access Token is enabled at a time, whenever a new Access Token is generated from the Client ID and Client Secret, the previous Token will immediately expire.

Multiple Access Tokens

If multiple access tokens are supported, then many clients can concurrently access the API. If another Access Token is created, the previous will remain valid until their original expiration.

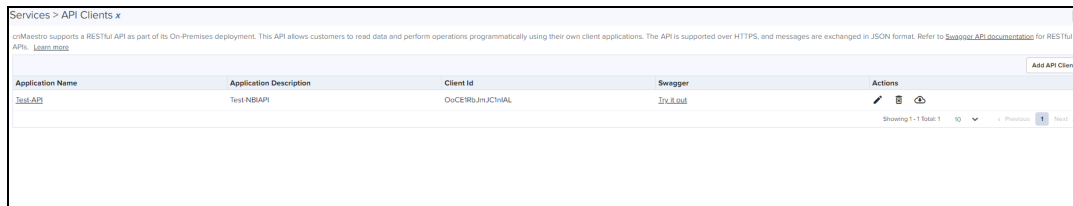
Rate Limiting

Request Rate Limiting is not enabled in the On-Premises version of cnMaestro. It is up to the application owner to make sure requests do not overtax the system.

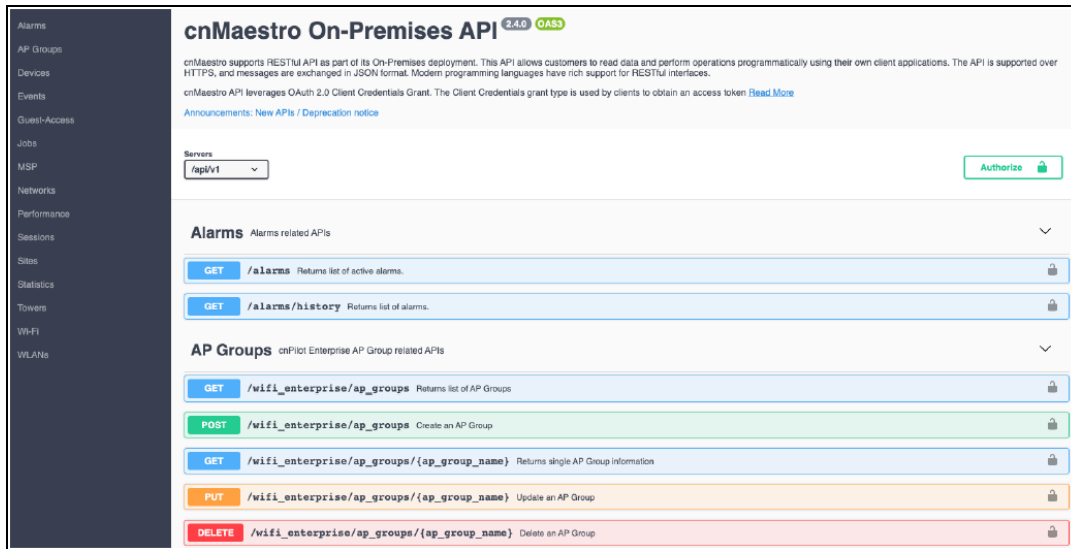
Swagger API

Introduction

The RESTful API documentation is now supported through Swagger. Swagger UI allows visualization and interaction with the API resources. You can access Swagger by navigating to **Services > API Clients** grid and clicking on **Swagger API documentation**.



Sample Swagger UI Screenshot

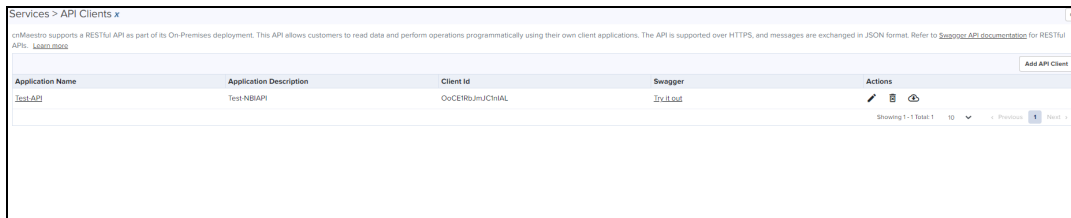


Client ID and Client Secret Generation

cnMaestro User Interface

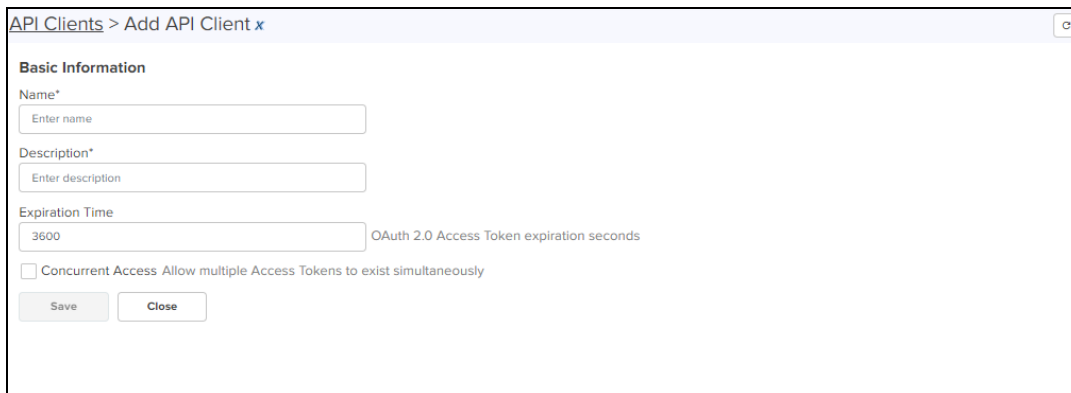
The Client Id and Client Secret are created in the cnMaestro UI by navigating to **Services > API Client**. Each client application should be added as an API Client.

Step 1: Navigate to Services > API Clients



Step 2: Create a New API Client

Select **Add API Client** to add a client, then fill in the requested details, and click **Save**.



Step 3: Download the Client ID and Client Secret

Download and store the Client ID and Client Secret by clicking **Download Credentials**. Both are required to create an API session.

API Clients > Edit API Client x

Name*
Test-API

Description*
Test-NBIAPI

Expiration Time
360000 OAuth 2.0 Access Token expiration seconds

Token Renewal Time
180000 OAuth 2.0 Access Token renewal seconds

OAuth 2.0 Access Credentials Download Credentials Expire All Tokens

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

Client Id
gP351LdPsogUGbPc

Client Secret
..... Show

Save Close

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



NOTE:

The steps below are for the On-Premises release of cnMaestro.

Access Token Request (RFC 6749, section 4.4.2)

In order 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 Web 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, instead of using the **Authorization** header, the credentials can be passed within the body of the **POST**:

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

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

Access Token Response (RFC 6749, section 4.4.3)

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

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

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:

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

Once 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

The following response codes are supported in cnMaestro and may be returned through the HTTP protocol.

Code	Description	Use in cnMaestro
400	Bad Request	Status field in request validation related errors.
502	Bad Gateway	Internal server error that may require a reboot.
403	Forbidden	An authenticated user tries to access a non-permitted resource.
500	Internal Server Error	A server-side error happened during processing the request.
405	Method Not Allowed	A method (GET, PUT, POST) is not supported for the resource.
404	Not Found	Server could not locate the requested resource.
501	Not Implemented	The request method is not recognized.
200	OK	Standard response for successful HTTP requests.
413	Payload Too Large	The request is larger than the server is willing to handle
431	Request Header Fields Too Large	The header fields are too large to be processed.
503	Service Unavailable	Internal server error that may require a reboot.
429	Too Many Requests	The client has sent too many requests in a given interval.
401	Unauthorized	User tried to access a resource without authentication.
422	Unprocessable Entity	The server understands the request but cannot process it.

HTTP Response Codes

Request Headers

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

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.

Context	Details
networks	Configured networks.
sites	Configured WiFi sites.
towers	Configured Fixed Wireless towers.

Sub-Resources

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

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 actual payload is presented in JSON format. The request URL is:

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

```
{
  "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. If the `start_time` and `stop_time` are mandatory query parameters and someone missed to provide them in the url gives the following error response with message and cause.

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

Parameters

Most APIs can be modified to 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 specific data to return from the server. If this parameter is missing, all available fields will be returned.

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.

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. Some of the standard filtering parameters are below:

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).

Field	Details
status	(Devices) Device status [online, offline, onboarding]
tower	(Devices) Configured Tower name.
type	(Devices) Device type [60ghz-cnwave, cnreach, cnmatrix, epmp, pmp, wifi-enterprise, wifi-home, wifi, ptp] (wifi includes wifi-home and wifi-enterprise).

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

Example: Retrieve all WiFi devices that are online.

Request:

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

Response:

```
{
  "paging": {
    "total": 1,
    "limit": 100,
    "offset": 0
  },
  "data": [
    {
      "ip": "233.187.212.38",
      "location": {
        "type": "Point",
        "coordinates": [
          77.55310127974755,
          12.952351523837196
        ]
      },
      "mac": "C1:00:0C:00:00:24",
      "msn": "SN-C1:00:0C:00:00:24",
      "name": "Hattie",
      "network": "Bangalore",
      "product": "cnPilot R201",
      "registration_date": "2017-05-23T21:28:37+05:30",
      "status": "online",
      "site": "Bangalore_Industrial",
      "type": "wifi-home",
      "hardware_version": "V1.1",
      "software_version": "2.4.4",
      "status_time": 1495560086
    }
  ]
}
```

Time Filtering

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

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

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

The parameters are below. If they are not specified, then the start or stop times will be open-ended.

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

Sorting

Sorting is supported on a selected 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.

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.

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 a metadata to convey total count and current offset and limit. Maximum number of results at any point is 100 even though limit 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:

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
<code>/api/v2/access/token</code>

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

Request

Headers

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

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

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

Body

The body needs to have the `grant_type`.

```
grant_type=client_credentials
```

Response

The response returns credentials for API access.

Body

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

Example

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

Token (alternate request)

POST
/api/v2/access/token

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

Request

Headers

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

Body

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

Response

The response to both forms is the same.

Body

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

Example

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

Validate Token

GET
<code>/api/v2/access/validate_token</code>

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

Request

HTTP Headers

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

Response

Body

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

Example

Request
<pre>curl https://10.110.134.12/api/v2/access/validate_token \ -X GET -k \ -H "Authorization: Bearer4e077cf457196eb4d27cf6f02686dc07763059"</pre>
Response
<pre>{"expires_in":85643}</pre>

Selected APIs

Overview

cnMaestro APIs are defined within the Swagger specification, accessed here

<https://docs.cloud.cambiumnetworks.com/api/3.0.0/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 difficult to present within Swagger.

cnMaestro v2 API

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

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

There are Unique API responses such as:

- [Device 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	cnReac h	cnVisio n	PTP	cnMatri x	60 GHz cnWave
ap_group	AP Group			X					
cbrs_state	CBRS state		X						
cbrs_status	CBRS status		X						
config.sync_reason	Configuration synchronization reason	X	X	X	X	X	X	X	
config.sync_status	Configuration synchronization status	X	X	X	X	X	X	X	
config.variables	Device is mapped to configuration variables	X	X	X	X	X	X	X	
config.version	Current configuration version	X	X	X	X	X	X	X	
country	Country	X	X	X		X			
country_code	Regulatory band						X		
description	Description	X	X	X	X	X	X	X	X
hardware_version	Hardware version	X	X	X	X	X	X	X	X
inactive_software_version	Inactive software version	X	X	X	X	X	X	X	
ip	IP address	X	X	X	X	X	X	X	X
ipv6	IPv6	X		X		X			X
last_reboot_reason	Reason for the last reboot (see 24.1)	X	X	X	X	X	X	X	

Name	Details	ePMP	PMP	Wi-Fi	cnReac h	cnVisio n	PTP	cnMatri x	60 GHz cnWave
link_symmetry	Link symmetry						X		
location	Location	X	X	X	X	X	X	X	X
mac	MAC address	X	X	X	X	X	X	X	X
managed_account	Managed account name	X	X	X	X	X	X	X	X
maximum_range	Maximum range (KM)	X	X			X	X		
msn	Manufacturer serial number	X	X	X	X	X	X	X	X
name	Device name	X	X	X	X	X	X	X	X
network	Network	X	X	X	X	X	X	X	X
product	Product name	X	X	X	X	X	X	X	X
registration_date	Registration date	X	X	X	X	X	X	X	X
role							X		
site	Site			X				X	X
site_id	Site unique identifier			X				X	X
software_version	Active Software version	X	X	X	X	X	X	X	
status	Status (online, offline, onboarding)	X	X	X	X	X	X	X	X

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	cnMatrix	60 GHz cnWave
status_time	Uptime/downtime time interval (sec)	X	X	X	X	X	X	X	X
tower	Tower	X	X		X	X	X	X	
type	Device type (epmp, pmp, wifi-home, wifi-enterprise, cnreach, ptp, cnmatrix, 60ghz-cnwave)	X	X	X	X	X	X	X	X

Statistics API Response (v2 format)

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

- 60 GHz cnWave
- cnMatrix
- cnReach
- Fixed Wireless
- PTP
- Wi-Fi

60 GHz cnWave

General

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

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

Networks

Name	Details	Mode
ipv6	IPv6 address	All

Radios (Array format)

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

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx_pkts	Received packets	All
ethports[].tx_pkts	Transmitted packets	All
ethports[].speed	Port speed and duplex	All

cnMatrix

General

Name	Details
cpu	CPU utilization
config_version	Configuration version
last_sync	Last synchronization (UTC Unix time milliseconds)
mac	MAC address
managed_account	Managed account name
memory	Available memory
mode	Device mode
name	Device name
network	Network
site	Site name
site_id	Site unique identifier
status	Status [online, offline, claimed, waiting, onboarding]
status_time	Uptime/downtime interval (seconds)
tower	Tower name
type	Device type

Networks

Name	Details
ip	IP address

cnReach

General

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

Networks

Name	Details	Mode
ip	IP address	All

Radios (Array format)

Name	Details	Mode
radios[].device_id	Device ID	Radios
radios[].id	Radio Id	Radios
radios[].linked_with	Linked with	Radios
radios[].mac	Radio MAC	Radios
radios[].margin	Margin	Radios
radios[].mode	Radio mode [ap, ep, rep]	Radios

Name	Details	Mode
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 (ePMP and PMP)

General

Name	Details	ePMP	PMP
ap_mac	AP MAC	SM	SM
config_version	Configuration version	AP/SM	AP/SM
connected_sms	Connected SM count	AP	AP
cpu	CPU utilization		AP/SM
distance	SM distance (KM)	SM	SM
gain	Antenna gain (dBi)	AP/SM	AP/SM
gps_sync_state	GPS synchronization state	AP/SM	
last_sync	Last synchronization (UTC Unix time milliseconds)	AP/SM	AP/SM
mac	MAC address	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM

Name	Details	ePMP	PMP
network	Network	AP/SM	AP/SM
reboots	Reboot count	AP/SM	
status	Status [online, offline, claimed, waiting, onboarding]	AP/SM	AP/SM
status_time	Uptime/downtime interval (seconds)	AP/SM	AP/SM
temperature	Temperature		AP/SM
tower	Tower name	AP	AP
vlan	VLAN		AP/SM

Networks

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

Radios

Name	Details	ePMP	PMP
radio.auth_mode	Authentication mode	SM	
radio.auth_type	Authentication type ePMP [open, wpa1, eap- ttls] PMP [disabled, enabled]	AP/SM	AP/SM
radio.channel_width	Channel width ePMP [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP [...]	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
radio.dl_err_drop_pkts	Downlink error drop packets	SM	
radio.dl_err_drop_pkts_ percentage	Downlink error drop packets percentage	SM	
radio.dl_frame_utilization	Downlink frame utilization		AP
radio.dl_lqi	Downlink Link Quality Indicator		SM
radio.dl_mcs	Downlink MCS	SM	
radio.dl_modulation	Downlink Modulation		SM
radio.dl_pkts	Downlink packet count	AP/SM	AP/SM
radio.dl_pkts_loss	Downlink packet loss		AP/SM
radio.dl_retransmits	Downlink Retransmission	AP/SM	
radio.dl_retransmits_pct	Downlink Retransmission percentage	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance		AP
radio.dl_snr	Downlink SNR (dB)	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal		SM

Name	Details	ePMP	PMP
radio.dl_snr_v	Downlink SNR (dB) vertical		SM
radio.dl_throughput	Downlink throughput	AP/SM	AP/SM
radio.frequency	RF frequency	AP/SM	AP/SM
radio.frame_period	Frame period		AP
radio.mac	Wireless MAC	AP/SM	
radio.mode	Radio mode [eptp-master, eptp- slave, tdd, tdd-ptp, ap/sm]	AP/SM	
radio.sessions_dropped	Session drops	AP	AP/SM
radio.software_key_throughput	Software key - max throughput		SM
radio.ssid	SSID	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
radio.tx_capacity	SM transmit capacity	SM	
radio.tx_power	Radio transmit power	AP/SM	AP/SM
radio.tx_quality	SM transmit quality	SM	
radio.ul_err_drop_pkts	Uplink error drop packets	SM	
radio.ul_err_drop_pkts_percentage	Uplink error drop packets percentage	SM	
radio.ul_frame_utilization	Uplink frame utilization		AP
radio.ul_mcs	Uplink MCS	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
radio.ul_pkts_loss	Uplink packet loss		AP/SM

Name	Details	ePMP	PMP
radio.ul_retransmits	Uplink Retransmission	SM	
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM
radio.ul_snr	Uplink SNR (dB)	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
radio.wlan_status	WLAN status [down, up]	AP/SM	

PTP

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 [AP, SM]	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

Wi-Fi

**NOTE:**

Mode is Enterprise, Home, or All.

General

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

Networks

Name	Details	Mode
ip	IP address	All
ipv6	IPv6 address	All
ip_dns	DNS	All
ip_dns_secondary	Secondary DNS	All
ip_wan	WAN IP	All

Name	Details	Mode
lan_mode_status	LAN mode status [no-data, half, full]	Enterprise
lan_speed_status	LAN speed status	All
lan_status	LAN status [down, up]	Home
netmask	Network mask	All

Radios (Array format)

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

Performance API Response (v2 format)

Performance API Response v2 Format are shown for following devices:

- 60 GHz cnWave
- cnMatrix
- cnReach
- Fixed Wireless
- PTP
- Wi-Fi

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/second	All
radios[].tx_bps	Transmit bits/second	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].max_rx	Ports maximum receive bytes	All
ethports[].max_tx	Ports maximum transmit bytes	All
ethports[].min_rx	Ports minimum receive bytes	All
ethports[].min_tx	Ports minimum transmit bytes	All

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx	Ports receive bytes	All
ethports[].tx	Ports transmit bytes	All

cnMatrix

General

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

Switch

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

Name	Details
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

Name	Details	Mode
radios[].rx_bytes	Receive bytes	Radios
radios[].throughput	Total throughput	Radios
radios[].tx_bytes	Transmit bytes	Radios

Fixed Wireless (ePMP and PMP)

General

Name	Details	ePMP	PMP
mac	MAC address	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM
network	Network	AP/SM	AP/SM
online_duration	Duration of device connection with server (seconds)	AP/SM	AP/SM
sm_count	Connected SM count	AP	AP
sm_drops	Session drops	AP/SM	AP
timestamp	Timestamp	AP/SM	AP/SM
tower	Tower	AP/SM	AP/SM
type	Device type	AP/SM	AP/SM
uptime	Device online time (seconds)	AP/SM	AP/SM

Radios

Name	Details	ePMP	PMP
radio.dl_frame_utilization	Downlink frame utilization		AP
radio.dl_kbits	Downlink usage (in Kbits on hour or minute basis)	AP/SM	
radio.dl_mcs	Downlink MCS	SM	

Name	Details	ePMP	PMP
radio.dl_modulation	Downlink modulation		SM
radio.dl_pkts	Downlink packet count	AP/SM	
radio.dl_pkts_loss	Downlink packet loss		AP/SM
radio.dl_retransmits_pct	Downlink retransmission percentage	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance		SM
radio.dl_snr	Downlink SNR	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
radio.ul_frame_utilization	Uplink frame utilization		AP
radio.ul.kbits	Uplink usage (in Kbits on hour or minute basis)	AP/SM	
radio.ul_mcs	Uplink MCS	SM	
radio.ul_modulation	Uplink modulation		SM
radio.ul_pkts	Uplink packet count	AP/SM	
radio.ul_pkts_loss	Uplink packet loss		AP/SM
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM
radio.ul_snr	Uplink SNR	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

PTP

General

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

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].max_rx	Ports maximum receive bytes	All
ethports[].max_tx	Ports maximum transmit bytes	All
ethports[].min_rx	Ports minimum receive bytes	All
ethports[].min_tx	Ports minimum transmit bytes	All
ethports[].pkt_error	Ports packet error	All
ethports[].port	Port name	All
ethports[].rx	Ports receive bytes	All
ethports[].tx	Ports transmit bytes	All

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

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

Name	Details	Mode
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].clients	Number of clients	All
radios[].id	Radio ID	All
radios[].rx_bps	Receive bits/second	All
radios[].throughput	Total throughput	All
radios[].tx_bps	Transmit bits/second	All



NOTE:

The specification for the equivalent v1 APIs is available in the Appendix.

- [Statistics API Response \(v1 Format\)](#)
- [Performance API Response \(v1 Format\)](#)

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": "eUROBR86HBgAGDEEVgQAGw4UWRUCACYVMgFPMV5ZWVfUVdGX1ZFJXxZR1dLBhMUMww", "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
prefixQs	True: Add query strings to landing URL on success. False: Remove query strings from landing URL on success. <code>prefixQs</code> and <code>action</code> values are driven based on WLAN configuration.
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.
msg	Message is based on RADIUS attribute reply message (18) in the RADIUS Access Accept or Reject message.
expiry	Displays the session time for the given guest session.
cmac	MAC address of the client.

60 GHz cnWave RESTful API

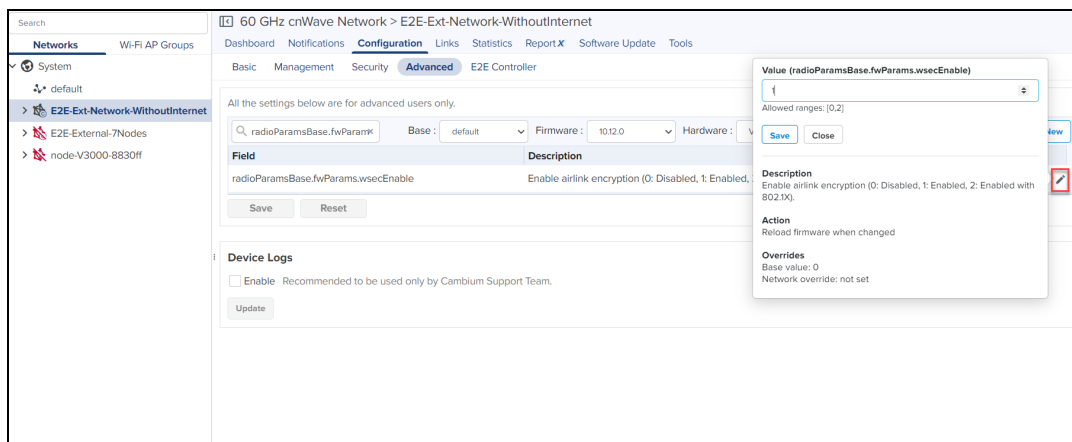
cnMaestro supports configuration overrides for 60 GHz cnWave E2E Network, E2E Controller, and Node(s) using the RESTful API.

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 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.

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 dots will be converted to objects and the last substring will be the key and value.

Example

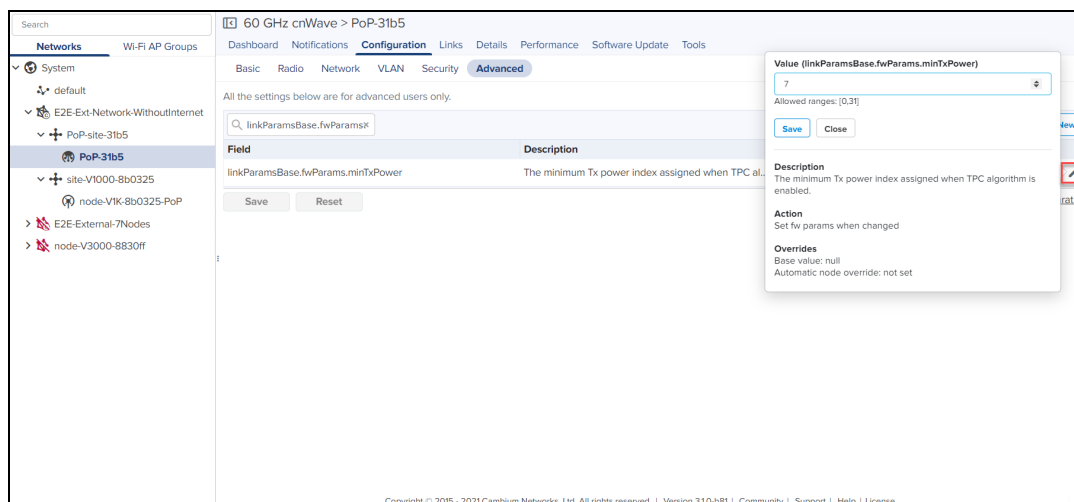
In case of field name `linkParamsBase.fwParams.minTxPower`, object to send in the API payload will be:

```
{
  "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 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"
  }
}
```

Field	Description	Status
prefixAllocParams.seedPrefix	Network seed prefix used for centralized and determ...	modified

Value (prefixAllocParams.seedPrefix)

fd00:ceed:8b03:2400::/56

Regular expression: [0-9a-fA-F:]{0-9}([0-9])

Description
Network seed prefix used for centralized and deterministic prefix allocation.

Action
Update prefix alloc params when changed

Overrides
Base value: undefined
Override: fd00:ceed:8b03:2500::/56

**WARNING:**

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

cnPilot Guest Access

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

The Guest Access feature creates a separate network for guests by providing Internet access to guest wireless devices (mobiles, laptops, etc).



NOTE:

The Guest Access feature is supported on cnPilot E-series Enterprise devices.

Configuration

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

Create the Guest Access Portal in cnMaestro

1. Basic details
2. Access Portal
3. Splash page
4. Sessions

Procedure for creating Guest Access

Prerequisites

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

Guest Portal Name	Description	Managed Account	Event Logging	Free Access	Paid Access	Voucher Access
SASL_GAP	SDR testing	Base Infrastructure	Yes	Yes	No	Yes



NOTE:

The Floating Management IP should be used to access the Guest Access Portal. This means DNS should be mapped to the Floating Management IP, and not to one of the unique IP addresses of the cnMaestro instances.

2. Click **Add Portal**. A maximum of four portals can be created per account.
3. Enter **Name** and **Description**.

Add Guest Portal
✕

Managed Account

Base Infrastructure
▼

Name*

Description

Client Login Event Logging

Save

Cancel

4. Click **Save**.

Basic Details

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

Guest Access Portal > test

Basic

Access

Splash

Sessions

Managed Account

Base Infrastructure

Name*

test

Description

Client Login Event Logging

Save



NOTE:

A name once created for the Portal cannot be changed.

Access Portal

The Access Portal tab has three different access types:

- Free
- Paid
- Vouchers

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

Free Access Type Configuration

Free access type contains **session validity, renewable frequency, client rate limits, and social login configurable parameters.**


You can select authentication using Google, Facebook, Twitter, and Office 365, or all. 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 42: Free Access Type Parameters

Parameter	Description
Add Whitelist	It contains options for configuring the IP address or the domain name.
Client Rate Limit	It contains options for configuring downlink and uplink parameters in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limits are applied.
Client Quota Limit	<p>The data quota limit feature has been added for RADIUS-based as well as for 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 accent point to which the client is connected. The access point keeps track of the data limits Access Point also sends client statistics to the controller every thirty minutes. In case of multiple devices allowed for a given policy then the data quota limits enforcement has some limitations and works with the latency of thirty minutes during which the cumulative data quota limits of the devices can be exceeded beyond the configured data quota limits.</p> <p>The similar behavior is supported through RADIUS attributes for RADIUS-based onboard guest access clients.</p> <p>RADIUS_VENDOR_ID_CAMBIUM 9 (17713) 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)</p>

Table 42: Free Access Type Parameters

Parameter	Description
	RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL_GIGWORDS (156) The gigwords attributes are used for supporting data quota limits above 4GB 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.
Social Login	Consists of the following options: <ul style="list-style-type: none"> Domain URL: The redirected URL in client when trying to access the Internet. Google: Consists of ID and Secret options to configure, which admin can create from https://console.developers.google.com/iam-admin/projects 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 reply back URL.
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.



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.

Paid Access Type Configuration

Paypal has been added as a payment gateway support where end users can purchase Internet connection using either the credit card or their existing paypal accounts. For purchasing the Internet plans, the 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 he plans to use it on multiple devices.

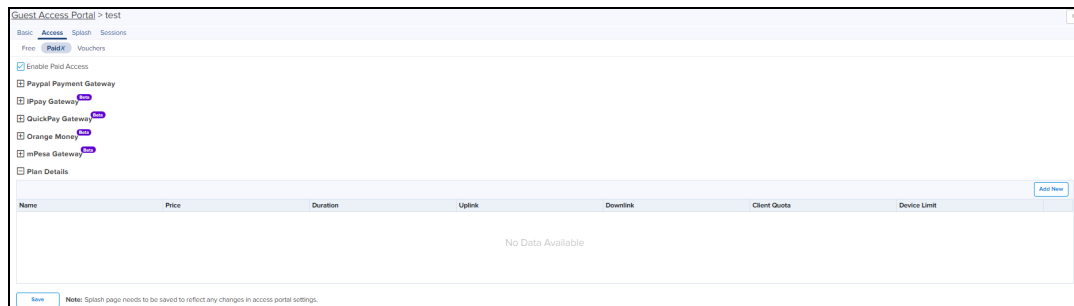


Table 43: Paid Access Type Parameters

Parameter	Description
General	<ul style="list-style-type: none"> • Plan Name: The name of the plan. • Session Duration: The duration for which the client is allowed network access. • Client Rate Limit: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limits are applied. • Device Limit: The device limit allow that number of devices to be connected or select the unlimited to connect any number of devices.

Add New Field
✕

Plan Name

Plan Cost

USD ▼

Session Duration

Min(s) ▼

Downlink Rate Limit

Kbps

Uplink Rate Limit

Kbps

Quota Type

None ▼

Device Limit

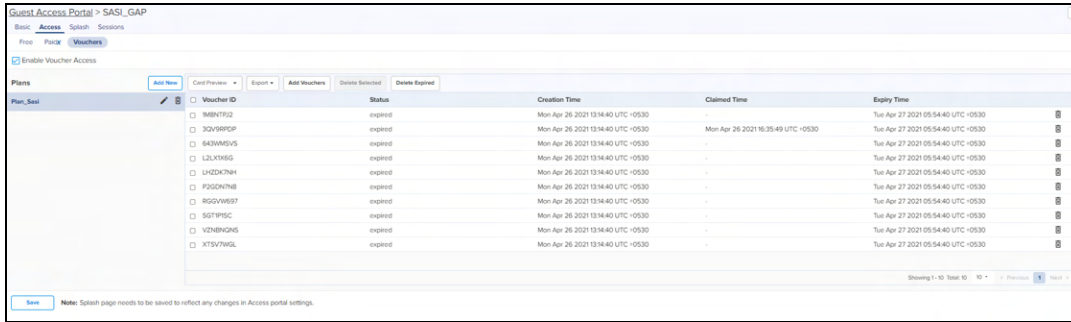
Unlimited

Save

Voucher Access Type Configuration

Important Points to Remember

- Vouchers can only be generated after enabling **Vouchers** and creating at least one **Voucher plan**.
- A maximum of 50,000 Vouchers per portal can be created on cnMaestro On-Premises.
- A maximum of 1,000 Vouchers per portal can be created on the Cloud-hosted version. (cloud.cambiumnetworks.com).
- Total number of generated Vouchers = Vouchers Unclaimed + Vouchers Claimed + Vouchers Expired.
- The admin can export all/valid/current page Voucher codes as PDF/CSV document.



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

1. Create a plan

- a. Navigate to **Services > Access Control Portal** page and select **Access Control** tab.
- b. Enable **Vouchers**
- c. Click **Add New Plan**.

The window with general and design parameters for the plan is displayed.

Table 44: Voucher Access Type Parameters

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

Add New plan
✕

Plan Details

Name

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

Voucher Expiry Min(s) ▾ Valid range is 1-2628000 min(s)

Downlink Rate Limit Kbps

Uplink Rate Limit Kbps

Quota Type None ▾

Voucher Device Limit Unlimited

Bind Voucher to Device

Vouchers Design

Background Image Browse ▾

Title ▾

Message ▾

Access Code Message ▾

Internet Access Voucher

Enjoy complimentary Internet services for 1 hr

Here is your access code

XXXXXXXX

Save
Cancel

Table 45: Adding Vouchers

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

- a. Select a plan.

Enable Voucher Access

Plans Add New

Plan-A > ✎ ✕

- b. Add Vouchers.

Add more cards ✕

Quantity

Generate
Generate & Export

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

Guest Access Portal > test

Basic: Access Splash Sessions

Free **Voucher**

Enable Voucher Access

Plans

Add New
Card Preview
Export
Add Vouchers
Delete Selected
Delete Expired

Voucher ID	Status	Creation Time	Claimed Time	Expiry Time
No Generated Vouchers				

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

c. Sample Voucher Code.



NOTE:

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

Splash Page

The Splash page refers to the page to which a wireless client is redirected when it connects to the guest portal. Administrators can create their own splash page by modifying the default logo, background, and text to be displayed in the splash 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 enabled, then the client sees both Free and Voucher related parameters.

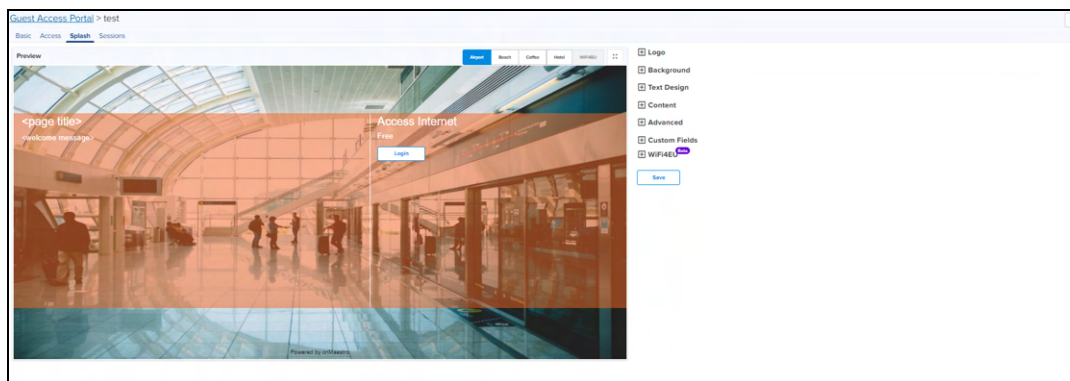


Table 46: Splash Page Parameters

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 appear as the background.
Background Placement	Choose the option from the drop-down list for placing the background image in the splash page.
Custom Fields	Expand Custom Field option. The user can customize the fields in the Splash 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.
Footer	Enter the text to appear as the footer of the page. You can choose the font style and size for the footer.
Logo	Browse and select the logo the needs to be appear on the splash page.
Login Title	Text to appear for login.
Login Success Message	Message to appear after successful login.
Login Failure Message	Message to appear any error while login.
Login Button	Enter the text that should appear on the window to submit.
Message	Text to appear as the welcome text. You can choose the font style and size for the welcome text.
Opacity	The transparency of background image.
On Success Redirect to URL	Enter the URL to be redirected to the page like Google, Twitter, and Facebook, etc.
Page Title	Text to appear as the title of the page. You can choose the font style and size for the title.
Please wait Message	Text to appear in the waiting screen.
Repeat Background	Enable the check box if you want the background image to be repeated.
Server Error Message	Text to appear if there is an error while contacting server.
Select Plans Label	Enter the text to appear in the label to select plan.
Text Design	Choose the appropriate colors for the background, logo in the background, content area, and for the text.

Table 46: Splash Page Parameters

Parameter	Description
Terms Agree Button	Text to appear in the terms agree button.
Terms Cancel Button	Text to appear in the terms cancel button.
Voucher Code	Enter the text to appear in Voucher Code, Voucher Label, Enter Voucher Code Message, and Voucher Code Error Message.
Voucher Label	Enter the text to appear in Voucher Label.
Voucher Code Error Message	Enter the text to appear in Voucher Code Error Message.
WiFi4EU	WiFi4EU provides free, high-quality Internet access only across the European Union.

WiFi4EU

WiFi4EU provides the free, high-quality Internet access across the European Union. Administrator can enable the **WiFi4EU** check box to provide access to the free Internet.

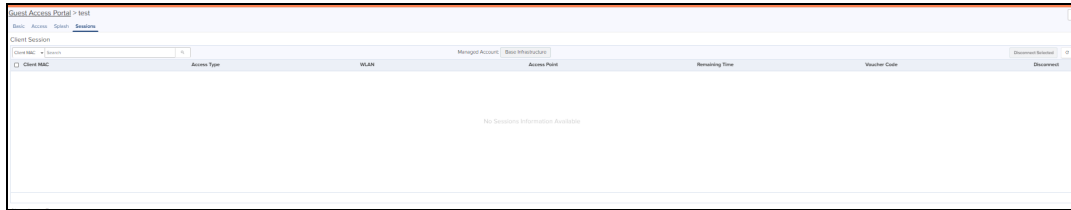
Table 47: WiFi4EU Type Parameters

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

Sessions

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

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



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

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

Table 48: 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.

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.

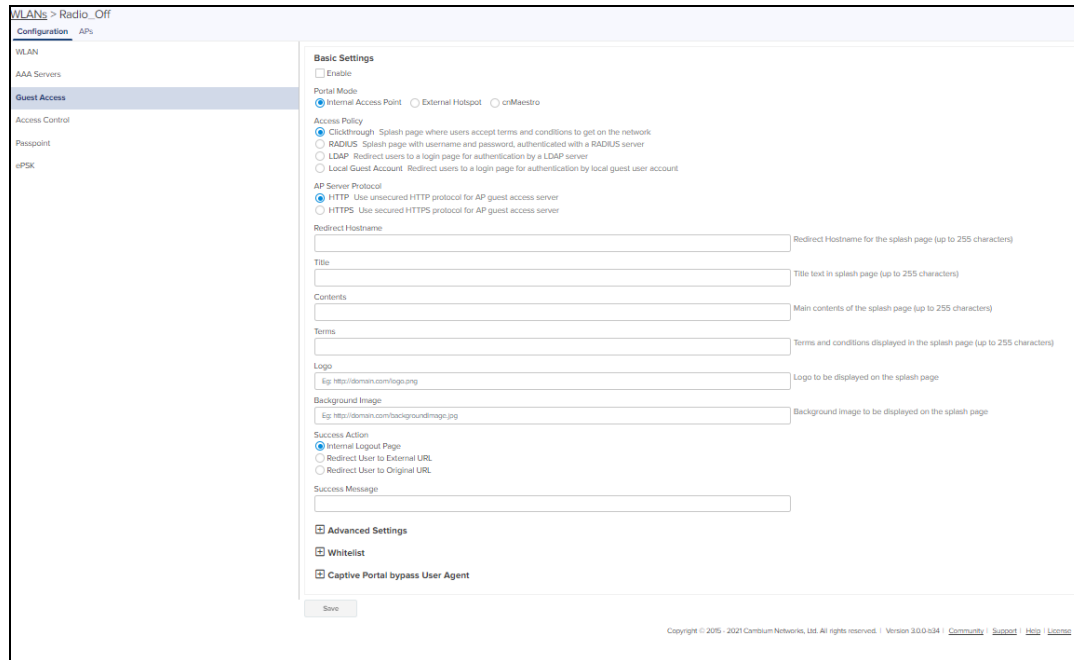


NOTE:

The client gets the fully configured splash page for login only if the Access Point is onboarded into the server.

Configuration at Device Side

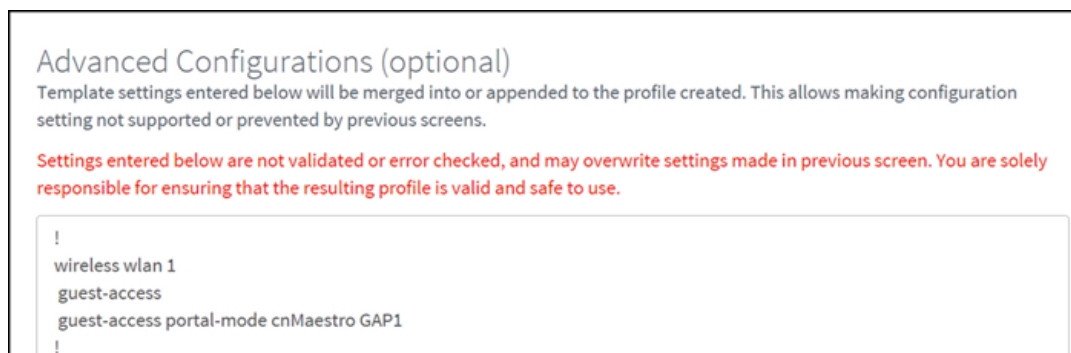
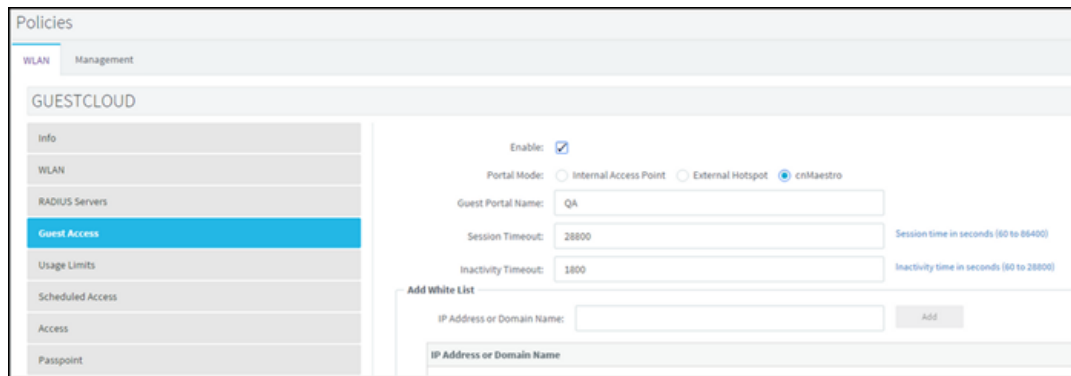
1. Login to the device.
2. Navigate to **Configuration > WLAN > Guest Access**.



3. Select the check box to enable Guest Access.
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 in configuring SMS authentication:

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

SMS Authentication

Enable

SMS Gateway Provider
Twilio

Auth Token

Account SID

From
US (+1)

OTP Template
Your OTP is %code%

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

To configure SMS Authentication on cnMaestro:

1. Enable SMS Authentication feature.
2. In SMS Gateway provider, select your required gateway from the drop-down list.
3. Enter the **User Name**.
4. Enter the **Sender ID**. This field is optional. This allows user to send SMS through the ID which he chooses.
5. Enter **API Key**.
6. Select your **Account Type** from the drop-down list.
7. Enter the OTP Template. The OTP template should include “%code%. %code% replaces the OTP code in the SMS.

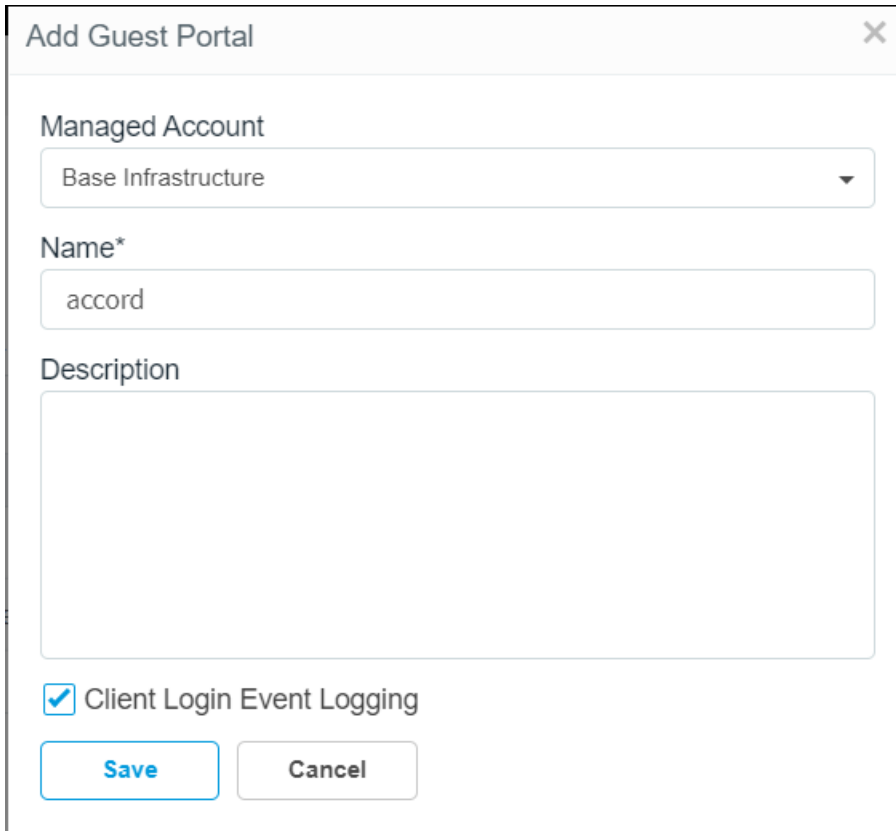
Guest Access using Social Login

Configuration

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

Create Guest Access profile on cnMaestro:

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



Add Guest Portal

Managed Account
Base Infrastructure

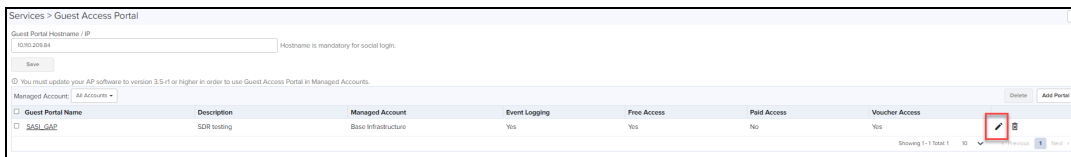
Name*
accord

Description

Client Login Event Logging

Save **Cancel**

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



Services > Guest Access Portal

Guest Portal Hostname / IP
10.10.208.84

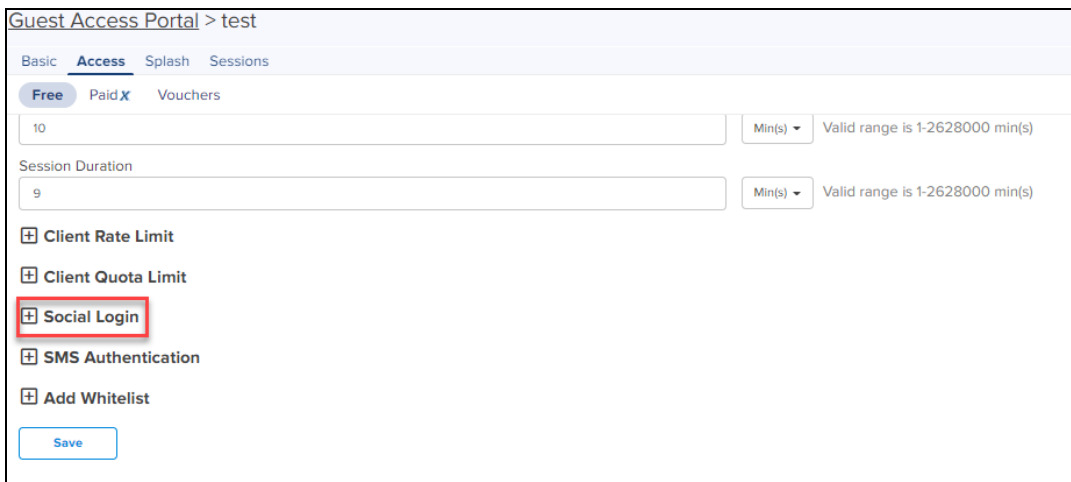
Save

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

Guest Portal Name	Description	Managed Account	Event Logging	Free Access	Paid Access	Voucher Access
SAGL_GAB	SDR testing	Base Infrastructure	Yes	Yes	No	Yes

Showing 1-1 Total 1

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



Guest Access Portal > test

Basic **Access** Splash Sessions

Free Paid X Vouchers

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

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

Client Rate Limit

Client Quota Limit

Social Login

SMS Authentication

Add Whitelist

Save

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

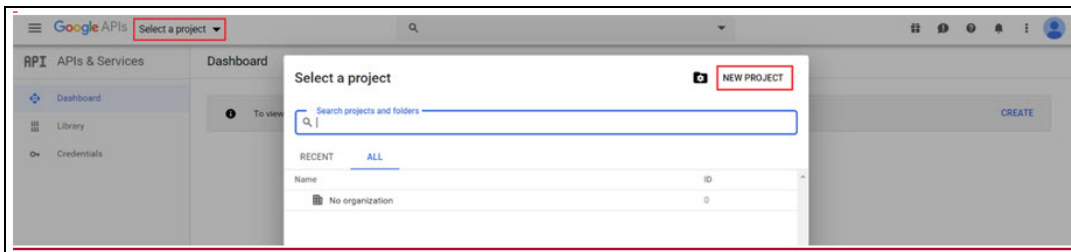
The screenshot shows the 'Social Login' configuration page for a Guest Portal. The 'Guest Portal Hostname / IP' is set to 'cnsonprem4.camwvk.com'. There are checkboxes for 'Google', 'Twitter', 'Facebook', and 'Office 365', all of which are checked. Each checked service has associated input fields for 'Id', 'Consumer API Key', and 'Consumer API Secret Key'. The 'Callback URL' is pre-filled with 'https://cnsonprem4.camwvk.com/cn-ctrl/guest/cnmaestro/Z2tjnAD/Guest-ManagedAccount/twitterCallback'. The 'Reply URL' is pre-filled with 'https://cnsonprem4.camwvk.com/cn-ctrl/guest/cnmaestro/Z2tjnAD/Guest-ManagedAcc'. There is a 'Show' button next to the 'Secret' field and a 'Configure this URL in the Social login application settings.' note.

API Key Generation

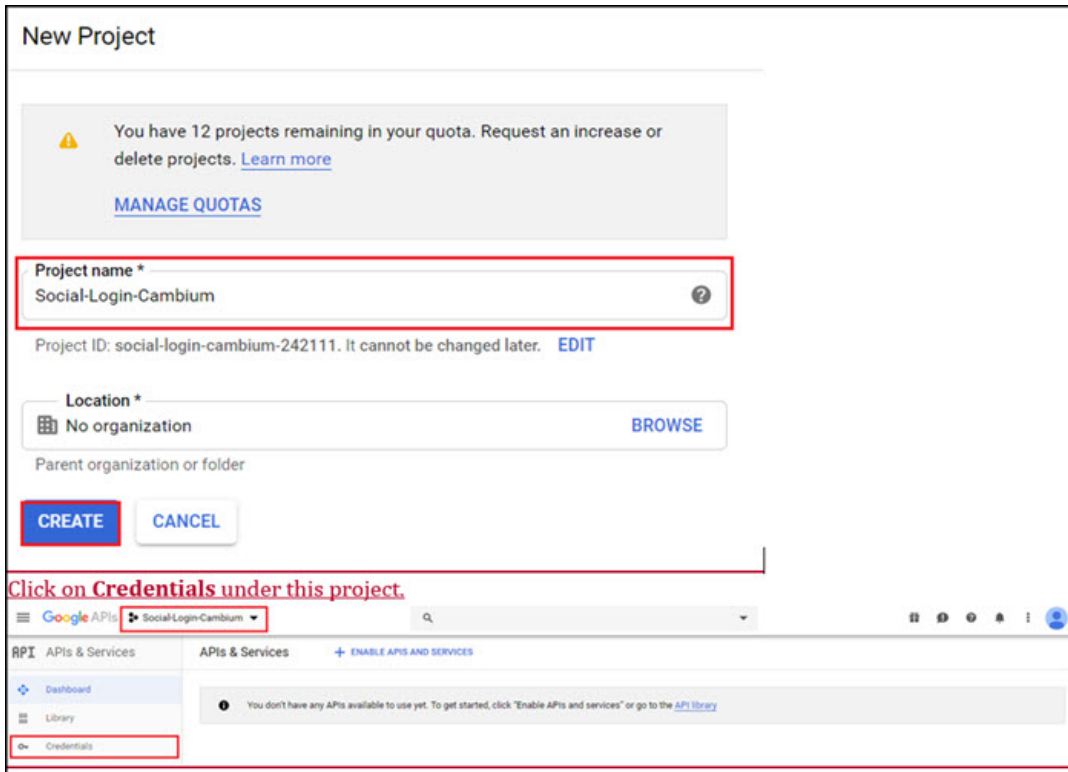
Creating APIs to integrate cnMaestro with Google, Twitter, Facebook, and Office 365.

Google

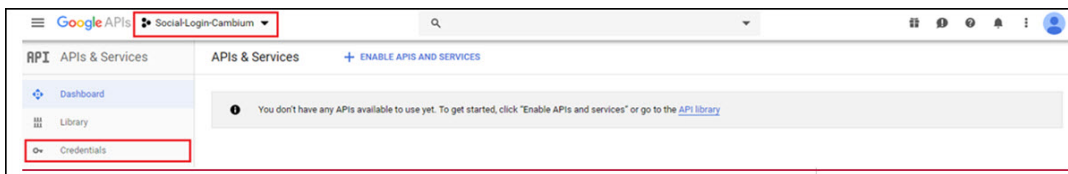
1. Login to Google Account and navigate to <https://console.developers.google.com>.
2. Click **Select a Project** and then click **New Project**.



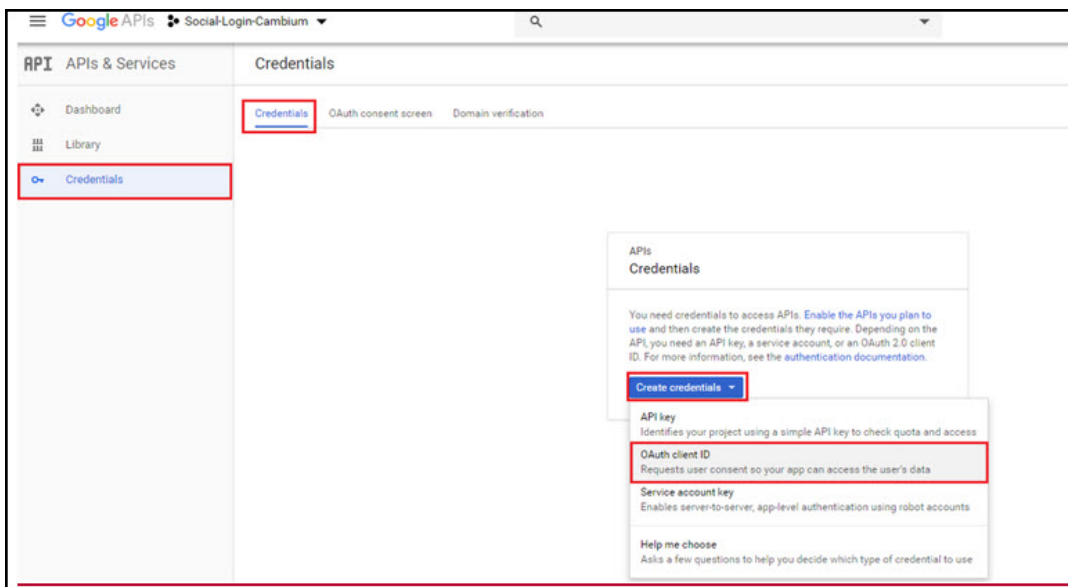
3. Enter a **Name** and click **CREATE**.



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



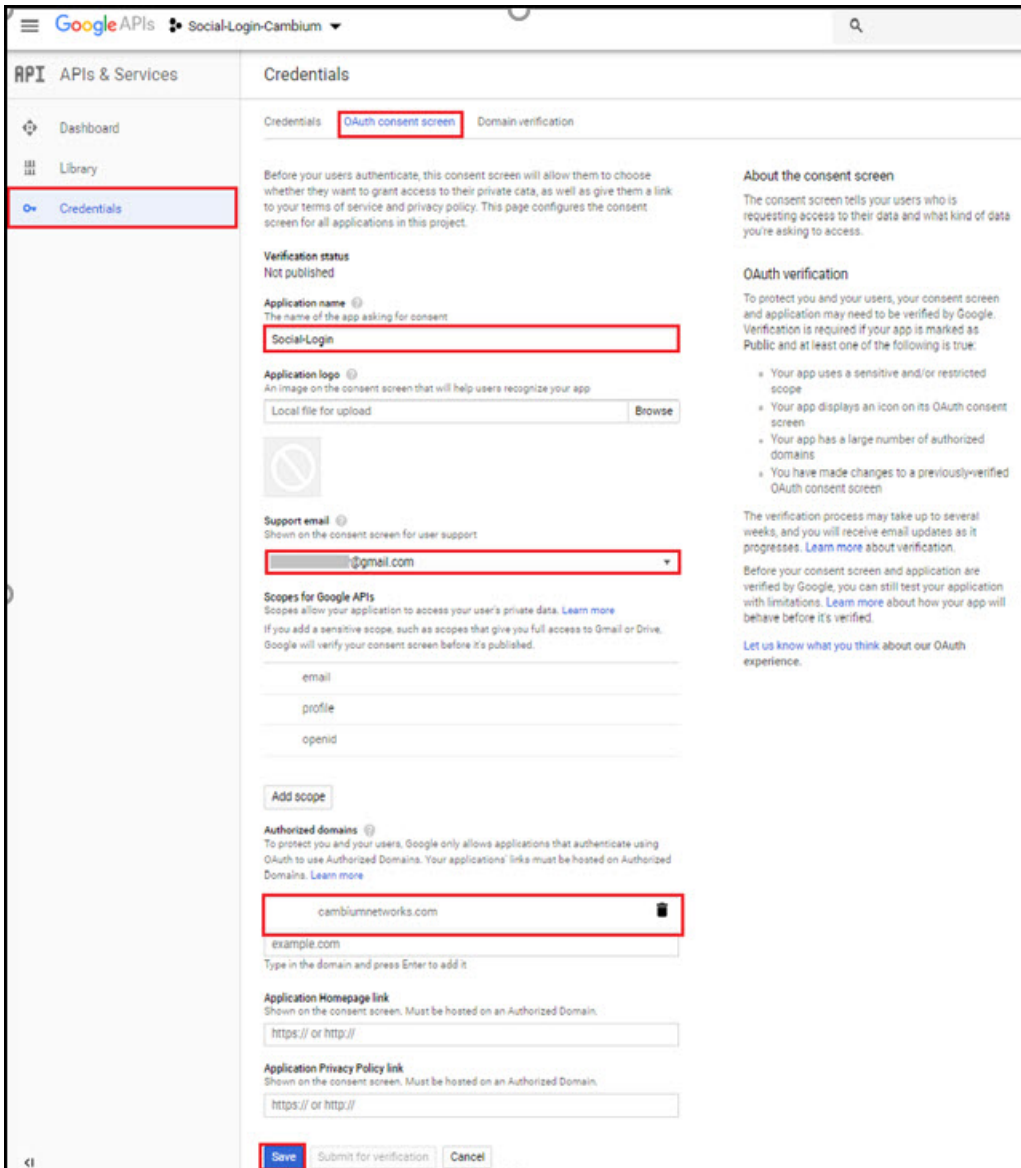
5. Under **Credentials** tab create OAuth Client ID.



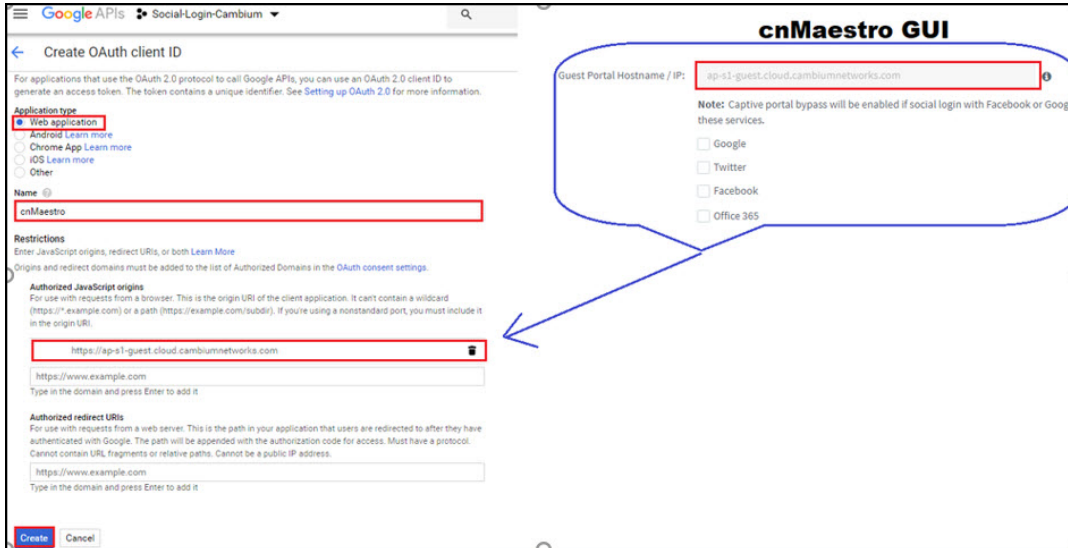
6. Click **Configure Consent Screen**.



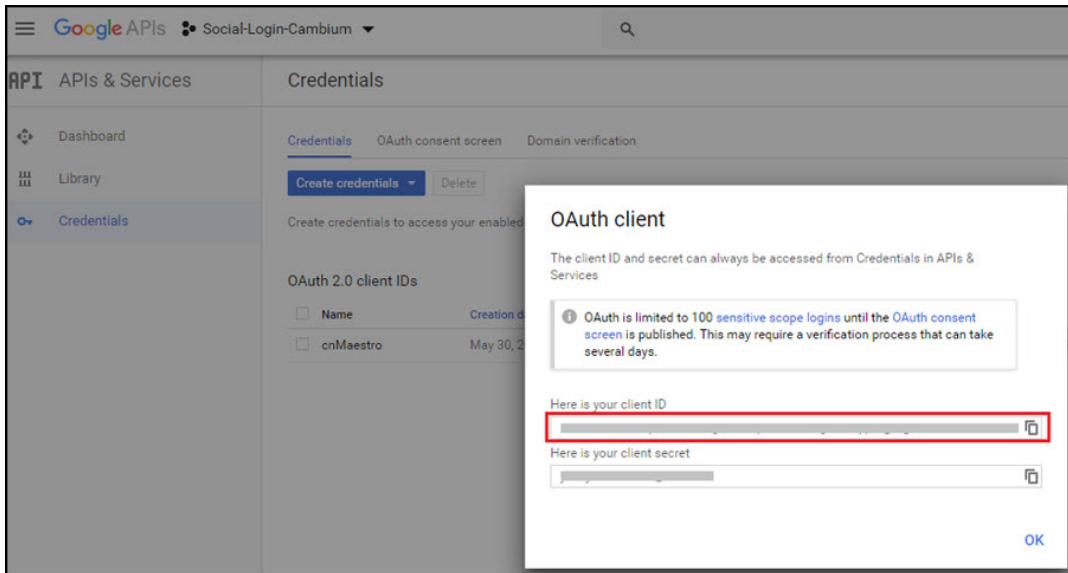
7. Assign a name to the application, map to the email ID, add cambiumnetworks.com to the authorized domain and click **Save**.



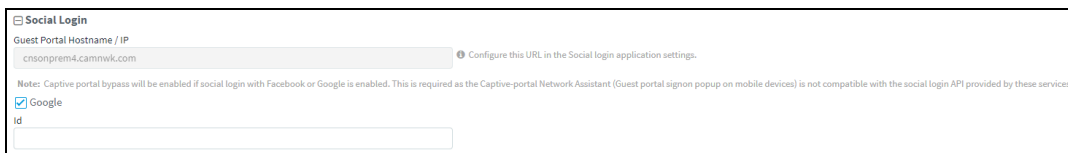
8. It redirects to creation of OAuth Client ID.
9. Select **Application type** as **Web Application**, give a Name, add Guest Portal Hostname url/IP which cnMaestro UI provides and click **Create**.



10. It redirects to the screen showing Client ID and Client Secret.

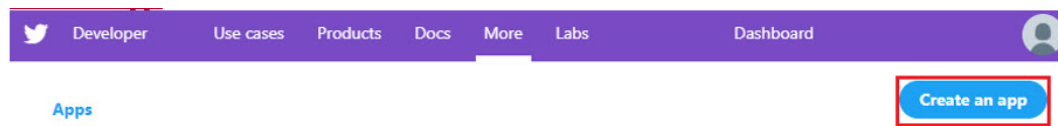


11. Copy the Client ID and paste it to the cnMaestro enabling Google under Social Logins and click **Save**.



Twitter

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



App details Keys and tokens Permissions

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

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

App name (required)
TestTwitter
Maximum characters: 32

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

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

Allow this application to be used to sign in with Twitter Learn more
 Enable Sign in with Twitter

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

Terms of Service URL
https://ap-s1-s1-5pkodub@un.cloud.cambiumnetworks.com

Privacy policy URL
https://ap-s1-s1-5pkodub@un.cloud.cambiumnetworks.com

Organization name
Cambium

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

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

Cancel Save

cnMaestro GUI

Twitter
Consumer API Key:
Consumer API Secret Key:
Callback URL: https://ap-s1-guest.cloud.cambiumnetworks.com/cn-ctrl/guest/75692

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

App details **Keys and tokens** Permissions

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

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

3. Paste them to cnMaestro UI for Twitter social login.

The screenshot shows a configuration form for Twitter social login. It includes a checked checkbox for 'Twitter', a text input field for 'Consumer API Key', another text input field for 'Consumer API Secret Key', and a text input field for 'Callback URL' containing the URL: `https://cnsonprem4.camnwk.com/cn-ctrl/guest/cnmaestro/Z2tjnAD/Guest-ManagedAccount/twitte`.

Facebook

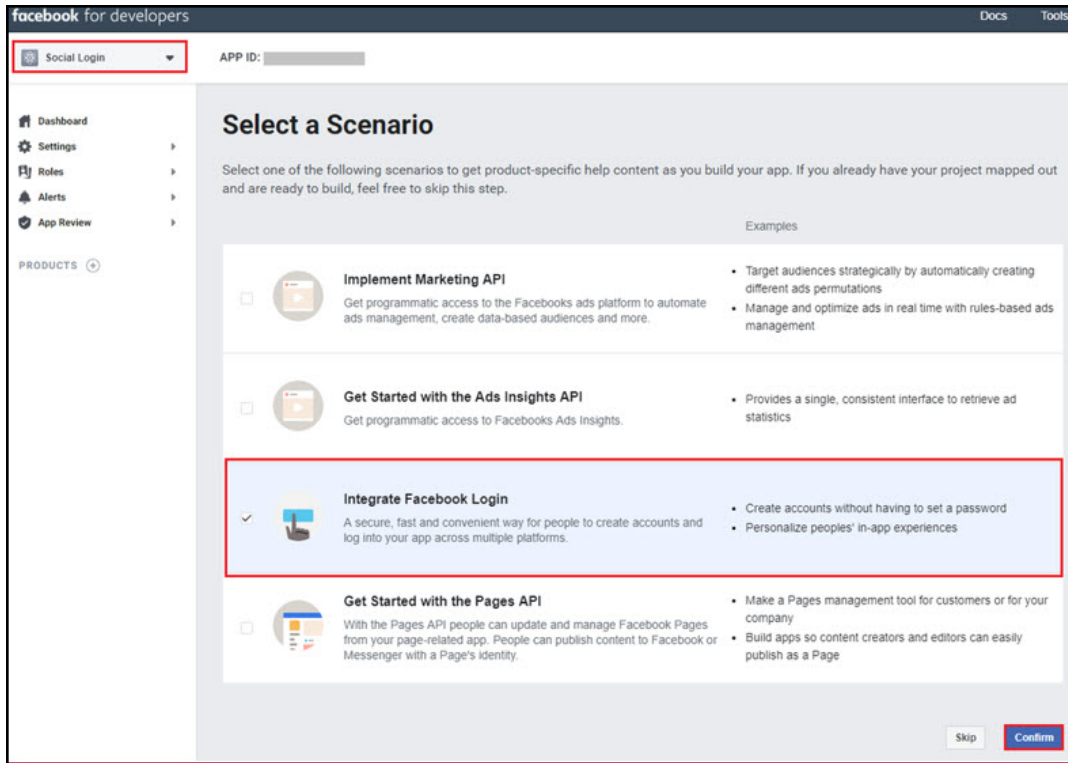
1. Login to Facebook Account and access <https://developers.facebook.com/apps/>, and click **Add a New App**.

The screenshot shows the 'facebook for developers' interface. A search bar labeled 'Search apps' is visible. A red box highlights the 'Add a New App' button, which features a plus sign icon and the text 'Add a New App'.

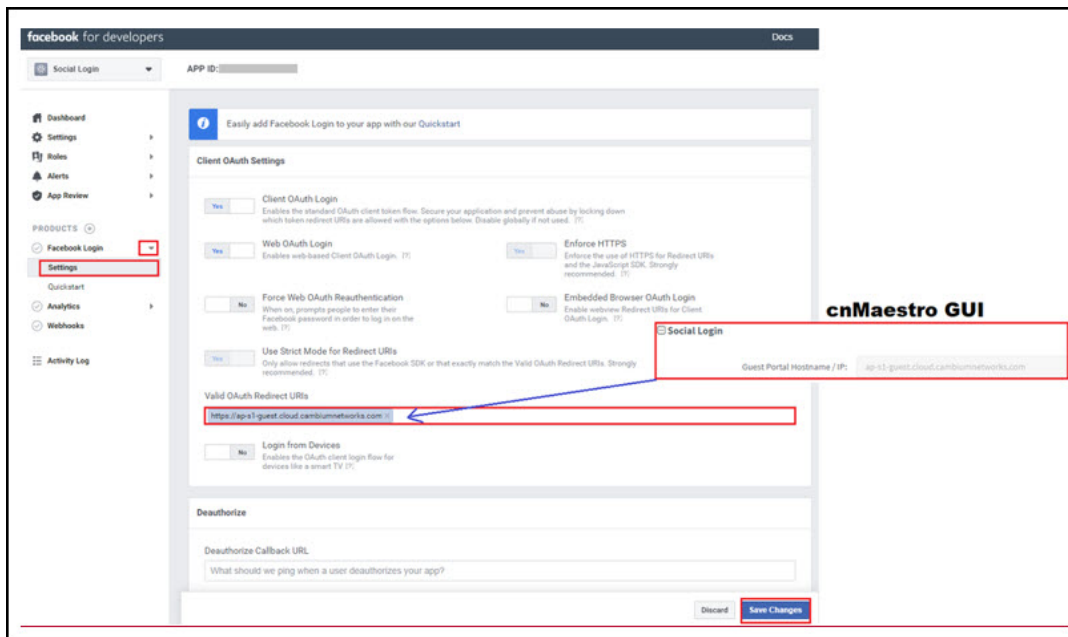
2. Enter App Display Name, Contact Email and click **Create App ID**.

The screenshot shows the 'Create a New App ID' form. It includes the heading 'Create a New App ID' and the sub-heading 'Get started integrating Facebook into your app or website'. There are two text input fields: 'Display Name' with the value 'Social Login' and 'Contact Email'. At the bottom, there is a checkbox for 'By proceeding, you agree to the Facebook Platform Policies' and two buttons: 'Cancel' and 'Create App ID'.

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



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



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

Social Login APP ID: [redacted]

Dashboard
 Settings
Basic
 Advanced
 Roles
 Alerts
 App Review

PRODUCTS
 Facebook Login
 Analytics
 Webhooks
 Activity Log

App ID: [redacted] App Secret: [redacted] Show

Display Name: Social Login Namespace: [redacted]

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

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

App Icon (1024 x 1024): [redacted] Category: Choose a Category
 Find out more information about app categories here

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

Facebook

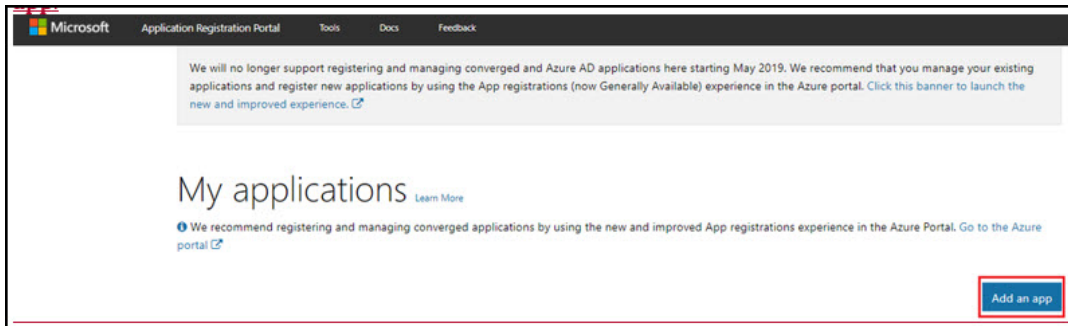
Id: [redacted]

Secret: [redacted] Show

Reply URL: <https://cnsonprem4.camnw.com/cn-ctrl/guest/cnmaestro/Z2tjnAD>

Office 365

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



New Application Registration

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

Name

Social Login

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

Create application

Cancel

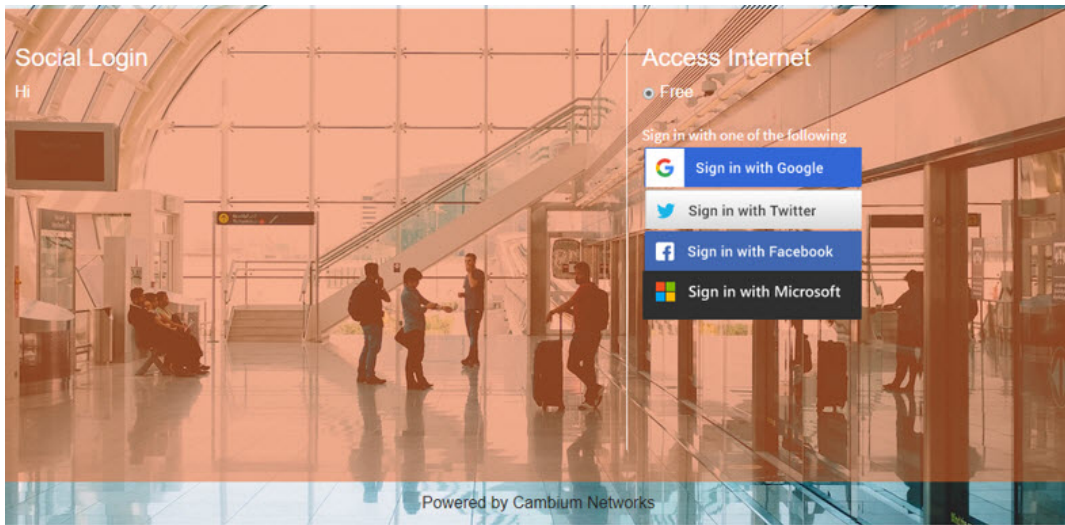
After adding your App name and clicking Create application, it redirects to App page.

1. Copy Application ID and paste it to cnMaestro Guest Access page under Office 365.
2. Click **Generate New Password**.
3. Copy reply URL from cnMaestro and paste it under Redirect URLs.
4. Add my.centrify.com to the Whitelist on the cnMaestro.

The screenshot displays the 'New Application Registration' page in the Azure portal. The application name is 'Social Login'. The Application ID is 'XXXXXXXX-12345-4565-aabbcc', which is highlighted with a red box and a circled '1'. A blue arrow points from this ID to the text 'Copy and paste it to cnMaestro', which in turn points to the 'Guest Portal Hostname / IP' field. The 'Guest Portal Hostname / IP' is 'ap-s1-guest.cloud.cambiumnetworks.com'. Under 'Application Secrets', the 'Type' is 'Password/Public Key', and the 'Password' is 'y0q*****', both highlighted with red boxes and circled '2'. The 'Created' date is 'Feb 15, 2019 11:44:35 AM'. In the 'Platforms' section, the 'Redirect URLs' field contains 'https://ap-s1-guest.cloud.cambiumnetworks.com/assets/views/office.html', highlighted with a red box and circled '3'. The 'Whitelist' section shows 'aaq0175.my.centrify.com' added, highlighted with a red box and circled '4'. A red text note at the bottom right says 'Add aaq0175.my.centrify.com to the whitelist'.

Sample Template

Sample client login page is displayed as shown below:



SMS Authentication

The gateway provider sends a text SMS containing the OTP to end users phone number. Once OTP is received the client can enter the OTP and get the 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 by cnMaestro user to go through 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 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 what all components does it need to be provided in the HTTP request and try to build the corresponding cnMaestro configuration.

In general, all SMS API documents show some example curl commands which can be used to create an SMS request with the server. Curl examples clearly show the required components in the request and helps 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 part of the SMS API request. It also provides a way to handle the SMS API response and validate the API success or failure case. How to handle the reply can be found under 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 just provide some meaningful name to identify this SMS Gateway service provider.

HTTP Request Type

Based on the SMS gateway provider and the API document information, identifies 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 some components as follows:

- Static components which are part of the request.
- Two dynamic components which are the 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 our 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”.

So what we have done here is removed the message and mobile number query strings from that URL and configured rest all. 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 here in this given format of “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. Then 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 config settings expose some authorization token or auth token and the provided HTTP header key value will be configured as “Bearer nZYIoU7QoUxfD03ct1CC2YvInql7DmUAH6RYz01K1” 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.

In our 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 config:

Example 1

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

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

Example 2

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

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

Example 3

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

```
}
```

Success Key Name to be configured based on the above example is status.

JSON Reply Success Key Value

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

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

- Sent
- Queued
- Success
- Message Accepted

So in this configuration one can add multiple such values that should be matched for the success case for the value as received for the “JSON Reply Success Key Name” field.

JSON Reply Failure Key Name

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

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

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 Failure 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 config:

Example 1

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

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

Example 2

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

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

XML Reply Success Element Value

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

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

- Sent
- Queued
- Success
- Message Accepted

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

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

Example 1

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

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

Example 2

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

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

Example 3

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

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

XMI 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 146 : Guest Access Portal

The screenshot shows the configuration page for the Guest Access Portal in cnMaestro. The page is titled "Guest Access Portal > SASI_GAP" and has tabs for "Basic", "Access", "Splash", and "Sessions". The "Access" tab is selected, and there are sub-tabs for "Free", "Paid", and "Vouchers".

Under the "Free" sub-tab, the following options are visible:

- Enable Free Access
- Enable Logout functionality for the guest client
- Bypass Captive Portal Detection

Under the "Client Session" section:

- Renewal Frequency: 1000 (Min(s) dropdown, Valid range is 1-2628000 min(s))
- Session Duration: 1000 (Min(s) dropdown, Valid range is 1-2628000 min(s))

Under the "Client Rate Limit" section:

- Client Rate Limit

Under the "Client Quota Limit" section:

- Client Quota Limit

Under the "Social Login" section:

- Social Login

Under the "SMS Authentication" section:

- Enable
- SMS Gateway Provider: Twilio (dropdown)
- Auth Token: [text input]
- Account SID: [text input]
- From: US (+1) (dropdown)
- OTP Template: Your OTP is %code% (text input)


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

At the bottom of the page, there is an "Add Whitelist" section with a plus icon and a "Save" button.

cnPilot GRE Tunnels

This chapter provides the following information:

- [Overview](#)
- [Typical Deployment Model \(Two Port Solution\)](#)
- [Access Control List \(ACL\) Configuration](#)

	NOTE: GRE Tunnels feature is deprecated in release 3.0.0 and will be removed in a future release 3.1.0.
---	---

Overview

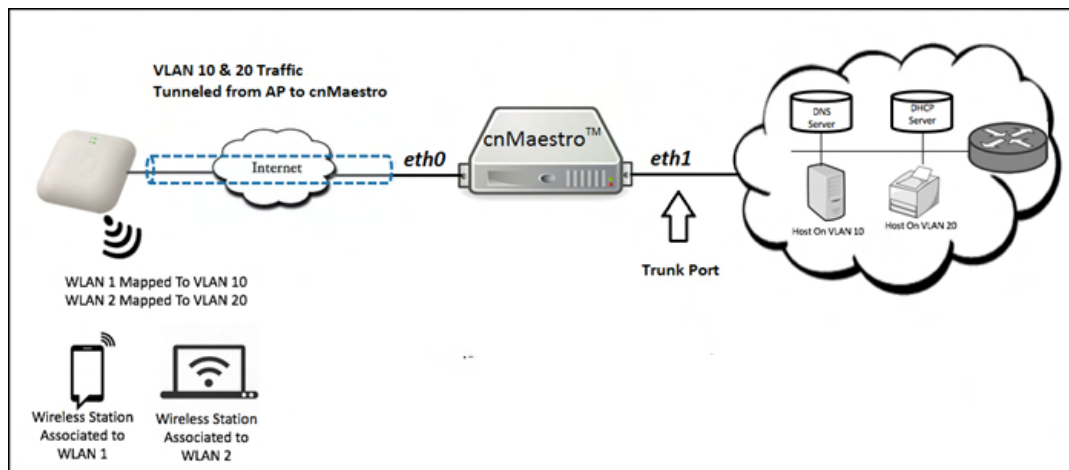
While deploying access points, the ability to tunnel wireless traffic from the APs to a tunnel concentrator (L2GRE/EoGRE) often plays a key role. By using the tunnel feature, the following can be avoided:

- Reconfiguration of switches and routers (for VLANs)
- Networking issues that arise when the clients IP range is not routable

The APs support L2GRE tunnel feature starting with release 3.1.1-r16. The cnMaestro On-Premises accepts tunneled traffic from the APs. With end to end tunnel solution from Cambium Networks, it is easy to get up the network fast and in reliable way.

Typical Deployment Model (Two Port Solution)

Figure 147 Typical Deployment Model (Two Port Solution)



In this deployment model, cnMaestro is equipped with two ports:

- **Primary Ethernet port (eth0)** is configured with cnMaestro IP address and all the communication between the APs and the cnMaestro On-Premises takes place at this port.
- In **Aux/bridge port (eth1)**, all the wireless clients traffic received from the APs will be transferred after removing the tunnel headers. This port comes up as a trunk port with allowed VLANs and other relevant configurable parameters from the cnMaestro UI.

Multicast/Broadcast Handling with Multiple APs on Tunnel Concentrator

In any type of deployment, multiple APs creates tunnel with the concentrator. In such scenario, the multicast/broadcast traffic (such as DHCP discovers, ARP Requests) generated by the wireless clients needs to be forwarded to aux/bridged port of the concentrator as well as to all the APs connected to the concentrator. Similarly, when any multicast/broadcast traffic is received on the aux/bridged port of the concentrator it needs to be sent to all the connected APs. In many situations, this broadcast can impact the performance and is better to restrict such traffic to flow out to all the APs.

Tunnel Concentrator is equipped with ACL feature which allows to restrict such traffic. There are many different ways by which ACL can drop the traffic. Each restriction is defined by an ACL rule. Refer ACL Configuration section for detailed information.



NOTE:

Default rules in the ACL prevents the unnecessary broadcast and multicast to go out towards the APs.

Inter AP Wireless Client Communication (through Concentrator)

Different wireless clients on different APs can be configured to use same or different VLANs. When clients on different APs but on same VLAN try to communicate with each other, then the concentrator bridges the traffic received from one AP to other(s) access point(s) (if not restricted by ACL rules). However, when clients on different APs are using different VLANs (different subnets) then concentrator does not forward traffic from one AP to another AP.

Access Control List (ACL) Configuration

ACL provides mechanism to filter out the unwanted traffic passing through the tunnel as well as traffic going between the APs. ACL provides many options to deny or permit the traffic. Traffic can be denied / permitted based on MAC layer, IP layer, and Protocol layer along with direction of flow. ACL is configured with the help of rules, each of them comes with a precedence. In these rules, **IN** direction refers to traffic coming from APs to the concentrator and **OUT** direction refers the reverse.

ACL comes up with default rules that prevent unnecessary broadcast and multicast to go out towards APs. With these rules, the inter AP communication is blocked.

Figure 148 ACL Configuration

Precedence	Policy	Direction	Type	Rule	
1	permit	in	proto	udp any 68 any 67	✎
2	permit	out	proto	udp any 67 any 68	✎
3	deny	out	proto	udp any 68 any 67	✎
4	deny	out	mac	any any any any	✎
9	deny	out	mac	any multicast	✎
10	permit	any	mac	any any	✎

Save Note: Configuration needs to be saved to reflect any changes.

The following are the screenshots for the different ACL rule categories:

MAC Layer ACL

Figure 149 MAC Layer ACL

Add ACL ✕

Precedence
5

Policy
Permit

Direction
In

Type
MAC

Source MAC

Destination Mac

Add ACL

IP Layer ACL

Figure 150 IP Layer ACL

Add ACL ✕

Precedence
5

Policy
Permit

Direction
In

Type
IP

Source IP / Mask

Destination IP / Mask

Add ACL

Transport Layer ACL

Figure 151 Transport Layer ACL

Add ACL ✕

Precedence
5 ▼

Policy
Permit ▼

Direction
In ▼

Type
Proto ▼

Protocol
UDP ▼

Source IP / Mask

Source Port

Destination IP / Mask

Destination Port

[Add ACL](#)


SNMP

This chapter provides the following information:

- [Overview](#)
- [Enable SNMP](#)
- [Configure SNMP Parameters](#)
- [cnMaestro MIB \(Management Information Base\)](#)

Overview

Currently, cnMaestro On-Premises supports SNMPv2c for basic monitoring data and online/offline traps and is a cnMaestro X feature.

	NOTE: SNMP uses UDP port 161 for GET requests and UDP port 162 for TRAPs.
---	---

Enable SNMP

To enable SNMPv2c, navigate to **Administration > Settings > Optional Features** and enable **SNMP management**.

This turns on SNMP functionality within the UI; however, the server itself does not start until the SNMP Configuration is completed.


	NOTE: SNMP Services does not start until a valid configuration exists.
---	--

Figure 152 Enable SNMP

Optional Features
SNMP
<input checked="" type="checkbox"/> Enable SNMP X This feature requires configuration

Configure SNMP Parameters

To configure SNMP Parameters, perform the following:

1. Navigate to **Services > SNMP Configuration** (this tab is only visible if SNMP is enabled).

Figure 153 Configure SNMP

Services > SNMP Configuration x

SNMPv2c RO Community
cambium1
SNMPv2c read-only community string (max 64 characters)

Trap Receiver
172.26.110.3
SNMP trap server ip address

Trap Community
cambium
SNMPv2c trap community string (max 64 characters)

Save Discard

2. Enter the **SNMPv2c RO Community String** name (maximum limit is 64 characters).
3. Enable the **Trap Receiver** check box and enter the IP Address.



NOTE:

The user can configure the desired Trap Community string value in the cnMaestro SNMP configuration page.

4. Enter the **SNMPv2c Trap Community** string name (maximum limit is 64 characters).
5. Click **Save**.



NOTE:

If there are thousands of devices in your cnMaestro account, you should set your MIB browser or snmpget command to use a minimum timeout of 20 minutes.

cnMaestro MIB (Management Information Base)

The cnMaestro MIB can be downloaded from [Cambium Support Center](#).

By default, the following OIDs are supported when SNMPv2 is enabled in cnMaestro On-Premises:

- .1.3.6.1.2.1 (mib-2)
- .1.3.6.1.4.1.2021 (UCD)
- .1.3.6.1.6.3.1.1 (snmpV2 - snmpMIB)
- .1.3.6.1.6.3.1.2 (snmpV2 - snmpMIBConformance)
- .1.3.6.1.4.1.17713.23 (CAMBIUM - cnMaestro)

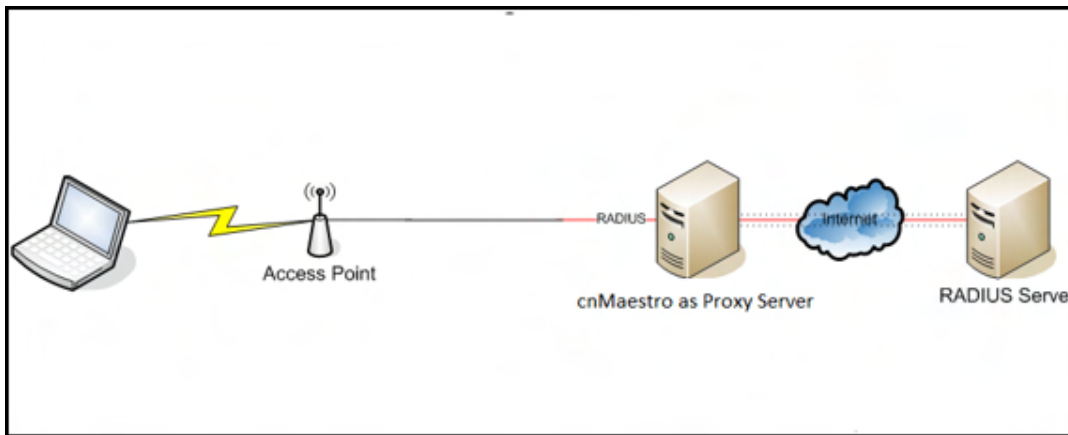
RADIUS Proxy

Overview

cnMaestro On-Premises can act as a proxy server to authenticate RADIUS requests for cnPilot Wi-Fi devices. In this scenario, cnMaestro acts as Network Access Server (NAS) for the RADIUS server.

In the below scenario, the Access Point sends RADIUS packets to cnMaestro On-Premises, and cnMaestro sends them to the RADIUS server. cnMaestro can act as a proxy for either authentication or accounting messages.

Figure 154 RADIUS Proxy on cnMaestro On-Premises



NOTE:
RADIUS Proxy is cnMaestro X feature.

Minimum cnMaestro On-Premises Version Requirements

- Minimum cnMaestro On-Premises release version required: 1.4.1-b1.
- Minimum cnPilot AP release required: 3.3.



NOTE:
This feature is not available on the cnMaestro Cloud version.

RADIUS Proxy Configuration

Follow the below procedure to configure RADIUS proxy on cnMaestro On-Premises:

1. Navigate to **Shared Settings > AP Groups and WLANs** page.
2. Select **Enterprise WLAN** to edit, and then select **AAA Servers**
3. Under AAA servers, select **Proxy RADIUS through cnMaestro** check box .
4. Configure Authentication Server details.
5. Configure Accounting Server details.
6. Configure NAS-Identifier. For this, include NAS-Identifier attribute to use in RADIUS Request packets and Default to system name.
7. Push the configuration from cnMaestro to AP.

Figure 155 RADIUS Proxy Configuration

WLANs > Default Enterprise

Configuration APs

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Warning: AAA Servers are configured separately for each WLAN.

Proxy RADIUS through cnMaestro X

Proxy RADIUS packets through cnMaestro (on-premises) instead of directly to the RADIUS server from the AP

Authentication Server

1. Host Secret Port* Realm

2. Host Secret Port* Realm

3. Host Secret Port* Realm

Timeout 3 Timeout in seconds for each request attempt (1-30)

Attempts 1 Number of attempts before giving up (1-3)

Accounting Server

Advanced Settings

Save

Copyright © 2015 - 2021 Cambium Networks, Ltd. All rights reserved. | Version 3.10-677 | [Contact Us](#) | [Support](#) | [Help](#) | [License](#)

Citizen Broadband Radio Service (CBRS)

Citizen Broadband Radio Service subscription for CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz).

	<p>NOTE: User must have an account in cnMaestro Cloud prior to enabling CBRS services in On-Premises.</p>
--	--

Enabling CBRS in Cloud

1. Login to cnMaestro Cloud account <https://cloud.cambiumnetworks.com/>.
2. Navigate to **Services > CBRS** page.
3. Select preferred **Spectrum Access System (SAS)** vendor.

4. Click **I accept the CAMBIUM NETWORKS, LTD. "CBRS" TERMS OF SERVICES/I accept the CBRS Service payment terms** to activate **Enable**.
5. Click **Enable**.
6. In **Billing Information** window pops up; enter the following:

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.

- Click **Save**.

CBRS Account

We require a Business Contact and a Technical Contact for your account. [Learn More](#)

Business Contact

First Name

Last Name

Email

Phone

Street Address

City

Zip Code/Postal Code

State

Country

United States

Technical Contact

Same as Business Contact

First Name

Last Name

Email

SAS Portal Contact

Cambium will set up a SAS portal account on your behalf. Please indicate whether you want us to use your Business Contact or Technical Contact for this purpose. Note that Google requires a Gmail address for registration.

Business Contact Technical Contact Other

Email (if not Business Contact or Technical Contact)

7. The **Account** page displays:

- Token
- Status
- Total Devices
- SAS
- Contact Details
- Payment Details

Services > CBRS

Account | Management Tool | Domain Proxy View

Please contact [Cambium Support](#) to disable CBRS operations or to change SAS Vendor. [Learn more](#)

Token

Status

- ✓ Account Created
- ✓ Payment Method Verified
- ✓ SAS ID Allocated
- ✓ Account Enabled
- Effective Mar 06 2020 17:13:24 (12h4 14h 54m)

Total Devices

1 APs, 1 SIMs

Spectrum Access System (SAS)

Federated Wireless (Developer/CD)

Contact Details

To make changes to the contact details, overwrite the existing entry and click "Update". [Learn more](#)

Business Contact

First Name

Last Name

Email

Phone

9876543

Street Address

city, state

City

BANGALORE

Zip Code/Postal Code

987654

State

.jharband

Country

India

Technical Contact

First Name

Last Name

Kar

Email

SAS Portal Contact

Cambium will set up a SAS portal account on your behalf. Please indicate whether you want us to use your Business Contact or Technical Contact for this purpose. Note that Google requires a Gmail address for registration.

Business Contact Technical Contact Other

Email (if not Business Contact or Technical Contact)

Payment Details

To update your payment method, make a selection under "Add Payment Method" and enter the new payment method details, then click "Submit".

Credit Card

*****1111 (expiration 1/2023)

Add Payment Method

Add Credit Card Details Add ACH Payment Details

a. **Token:**


Token used for authenticated communication with the SAS through Cambium Domain Proxy. It is generated automatically once CBRS is enabled for the Cloud account.

b. **Status:**

- Displays the account status.

Pending Status	Success Status
<p>Status</p> <ul style="list-style-type: none"> ✓ Account Created ✗ Payment Method Verification Pending ✗ SAS-ID Allocation Pending <p>● Effective Jul 07 2020 16:54:10 (< 1m)</p> <p>Total Devices ⓘ Usage History</p> <p>0 APs, 0 SMs</p>	<p>Status</p> <ul style="list-style-type: none"> ✓ Account Created ✓ Payment Method Verified ✓ SAS-ID Allocated ✓ Account Enabled <p>● Effective Mar 19 2020 15:02:02 (110d 2h 0m)</p> <p>Total Devices ⓘ Usage History</p> <p>3 APs, 68 SMs</p>

1. **Account Creation:** Displays as Created once the account is enabled. Refer to **Step f** for entering contact information and enabling account.
2. **Payment Method:** Displays as Verified once the Payment Details are approved. Refer to **Step g** Payment Details.
3. **SAS ID:** Once the payment details are verified, the SAS ID is allocated automatically.


	<p>NOTE</p> <p>It may take 1 day to get the SAS ID.</p>
---	--

4. **Effective:**

- **Grey** : indicates the **Pending Status**.
- **Green** : indicates **Success**.
- **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**.

<p>Total Devices ⓘ Usage History</p> <p>0 APs, 0 SMs</p>
--

	<p>NOTE</p> <p>Initially the device counts will be 0 APs and 0 SMs.</p>
---	--

- d. **SAS:** Displays the SAS vendor preferred by the operator.

	<p>NOTE</p> <p>Contact Cambium support to disable CBRS operation or to change SAS Vendor.</p>
---	--

- 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 **Step 6**. Review and update if necessary, else press ahead to **Step g**.

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 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, etc. This page requires:

- **First Name**
- **Last Name**
- **Email**
- **Phone**
- **Street Address.**
- **City**
- **Zip code/Postal Code**
- **State**
- **Country**


Technical Contact

Cambium Networks communicates with the **Technical Contact** such as software updates, publication of 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 you want us to use the **Business Contact**, **Technical Contact**, or **Other**.

	<p>NOTE Google requires a Gmail address for registration.</p>
---	--

- Click **Update**.

Contact Details
 To make changes to the contact details, overwrite the existing entry and click "Update". [Learn more](#)

Business Contact

First Name

Last Name

Email

Phone

Street Address

City

Zip Code/Postal Code

State

Country

Technical Contact

First Name


Last Name

Email

SAS Portal Contact
 Cambium will set up a SAS portal account on your behalf. Please indicate whether you want us to use your Business Contact or Technical Contact for this purpose. Note that Google requires a Gmail address for registration.

Business Contact Technical Contact Other

Email (if not Business Contact or Technical Contact)

	<p>NOTE</p> <p>Clicking update the Account Page will overwrite the current entries.</p>
---	--

g. Payment Details

Select one of the payment methods below:

- Add Credit Card Details
- Add ACH Payment Method

Payment Details

Credit Card

*****0004 (expiration 1/2021)

Add Payment Method

Add 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**.

CBRS

Account Management Tool Domain Proxy View

Add Payment Method

Add Card Details Add ACH Payment Method

Please Fill in Your Credit Card Details

Card Type Amex JCB VISA MasterCard DISCOVER

Card Number

Expiration Date - Select One / - Select One

CVV

Cardholder Name

= Required Field

Add ACH Payment Method

Enter the following and click **Submit**:

- **ABA/Routing Number.**
- **Bank Account Number.**
- Select one of the following **Account Type**:
 - Checking
 - Saving
 - Business Checking
- **Bank Name and Account Holder Name.**

CBRS

Account Management Tool Domain Proxy View

Add Payment Method

Add Card Details Add ACH Payment Method

Please Enter Your Payment Details

ABA/Routing Number

Bank Account Number

Account Type - Select One

Bank Name

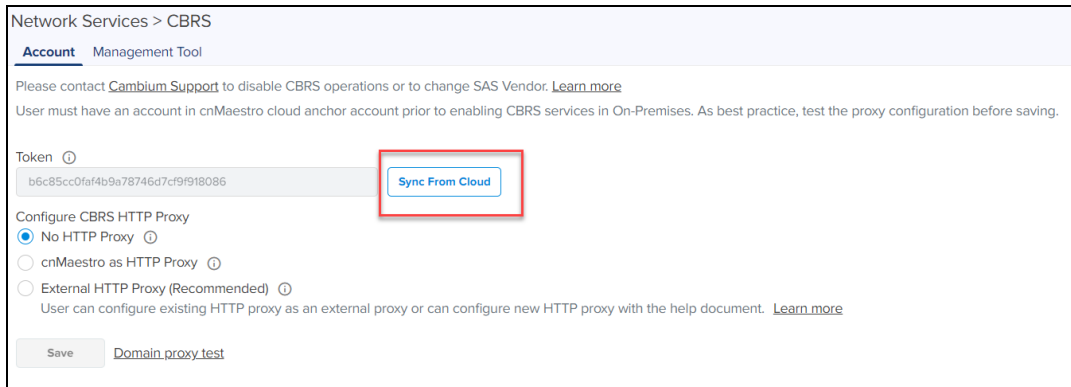
Account Holder Name

= Required Field

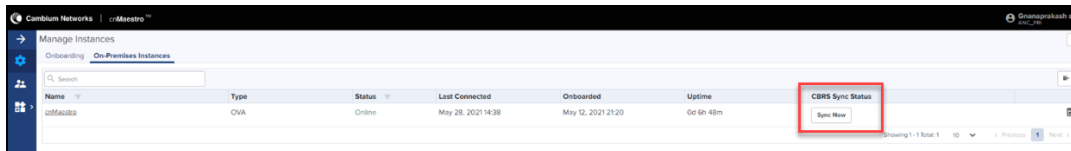
Enabling CBRS in On-Premises

Perform the following to enable CBRS:

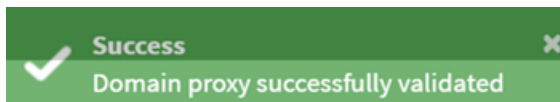
1. On successful activation of the CBRS service in the Cloud Anchor account, cnMaestro generates a Token.
2. Onboard the On-Premises to Anchor account.
3. User can Sync the CBRS token from On-premises or Anchor account
 - a. In On-Premises CBRS accounts page click **Sync From Cloud** to synchronize the CBRS token.



- b. Navigate to the **Anchor account > Manage Instances > On-Premises Instances** and click **Sync Now** on CBRS sync status.



4. Select HTTP Proxy mode for SAS communication (refer to [CBRS HTTP Proxy Configuration Options](#)).
5. Click **Save token**. CBRS service will be enabled.
6. Click **Domain Proxy Test** to test Domain Proxy connectivity. If the test is successful, it will display the following message:

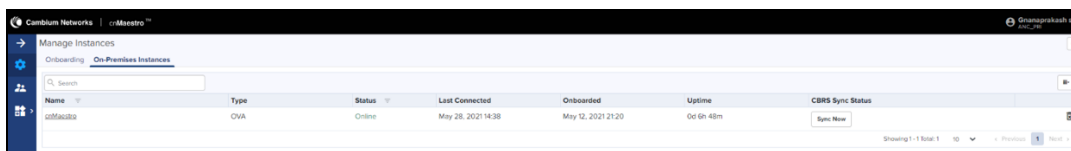


Share CBRS Configuration to the On-Premises Instance

NOTE:

From version 3.0.3 cnMaestro supports Synchronize CBRS Configuration to On-Premises instance.

Once On-Premises is connected to the Anchor Account, the user can synchronize CBRS details (SAS ID, Token) to the cnMaestro On-Premises instance to register CBRS devices.



Network Services > CBRS

[Account](#) Management Tool

Please contact [Cambium Support](#) to disable CBRS operations or to change SAS Vendor. [Learn more](#)

User must have an account in cnMaestro cloud anchor account prior to enabling CBRS services in On-Premises. As best practice, test the proxy configuration before saving.

Token ⓘ

b6c85cc0faf4b9a78746d7cf9f918086 [Sync From Cloud](#)

Configure CBRS HTTP Proxy

No HTTP Proxy ⓘ

cnMaestro as HTTP Proxy ⓘ

External HTTP Proxy (Recommended) ⓘ

User can configure existing HTTP proxy as an external proxy or can configure new HTTP proxy with the help document. [Learn more](#)

[Save](#) [Domain proxy test](#)

If the user shares (sync) CBRS details configured on Anchor account to connected On-Premises and if any devices are registered in On-Premises with different CBRS token or SAS ID it displays the deregister error as shown below.

Name	Type	Status	Last Connected	Onboarded	Uptime
cnMaestro18464	OVA	Online	Jun 11, 2021 16:58	Jun 11, 2021 16:58	0d 2h 33m

Showing 1 of Total 1 | 10 | Previous | Next

CBRS HTTP Proxy Configuration Options

Cambium recommends using External HTTP Proxy for a highly available deployment, because cnMaestro software updates may take a few minutes to complete, during which time communication with SAS through the Domain Proxy will be affected.

No HTTP Proxy

Network Services > CBRS

[Account](#) Management Tool

Please contact [Cambium Support](#) to disable CBRS operations or to change SAS Vendor. [Learn more](#)

User must have an account in cnMaestro cloud anchor account prior to enabling CBRS services in On-Premises. As best practice, test the proxy configuration before saving.

Token ⓘ

b6c85cc0faf4b9a78746d7cf9f918086 [Sync From Cloud](#)

Configure CBRS HTTP Proxy

No HTTP Proxy ⓘ

cnMaestro as HTTP Proxy ⓘ

External HTTP Proxy (Recommended) ⓘ

User can configure existing HTTP proxy as an external proxy or can configure new HTTP proxy with the help document. [Learn more](#)

[Save](#) [Domain proxy test](#)

- In On-Premises **No HTTP Proxy** is selected by default.
- CBRS-compliant devices communicate with the Domain Proxy directly through the Cambium Domain Proxy.



NOTE:

The On-Premises server and CBRS devices must have Internet access to communicate directly to the Cambium Domain Proxy.

cnMaestro as HTTP Proxy

Network Services > CBRS

Account Management Tool

Please contact [Cambium Support](#) to disable CBRS operations or to change SAS Vendor. [Learn more](#)

User must have an account in cnMaestro cloud anchor account prior to enabling CBRS services in On-Premises. As best practice, test the proxy configuration before saving.

Token ⓘ
b6c85cc0fa4b9a78746d7c9f918086 [Sync From Cloud](#)

Configure CBRS HTTP Proxy

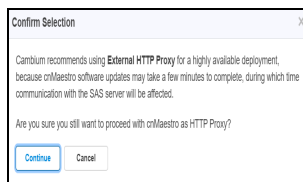
No HTTP Proxy ⓘ

cnMaestro as HTTP Proxy ⓘ

External HTTP Proxy (Recommended) ⓘ
User can configure existing HTTP proxy as an external proxy or can configure new HTTP proxy with the help document. [Learn more](#)

[Save](#) Domain.proxy.test

- Select **cnMaestro as HTTP Proxy** and a window pops-up. Click **Yes**.



Warning:

Cambium recommends using External HTTP Proxy for a highly available deployment, because cnMaestro software updates may take a few minutes to complete, during which time communication with SAS through the Domain Proxy will be affected.

- CBRS-compliant devices communicate with the Cambium Domain Proxy through the local cnMaestro On-Premises HTTP Proxy.



NOTE:

cnMaestro On-Premises must have Internet access.

External HTTP Proxy

Network Services > CBRS

Account Management Tool

Please contact [Cambium Support](#) to disable CBRS operations or to change SAS Vendor. [Learn more](#)

User must have an account in cnMaestro cloud anchor account prior to enabling CBRS services in On-Premises. As best practice, test the proxy configuration before saving.

Token ⓘ
b6c85cc0fa4b9a78746d7c9f918086 [Sync From Cloud](#)

Configure CBRS HTTP Proxy

No HTTP Proxy ⓘ

cnMaestro as HTTP Proxy ⓘ

External HTTP Proxy (Recommended) ⓘ
User can configure existing HTTP proxy as an external proxy or can configure new HTTP proxy with the help document. [Learn more](#)

External Proxy Url ⓘ

[Save](#) Domain.proxy.test

CBRS-compliant devices can communicate with the Cambium Domain Proxy through an External HTTP Proxy such as HA Proxy. Cambium recommends configuring High Availability on the HTTP Proxy.



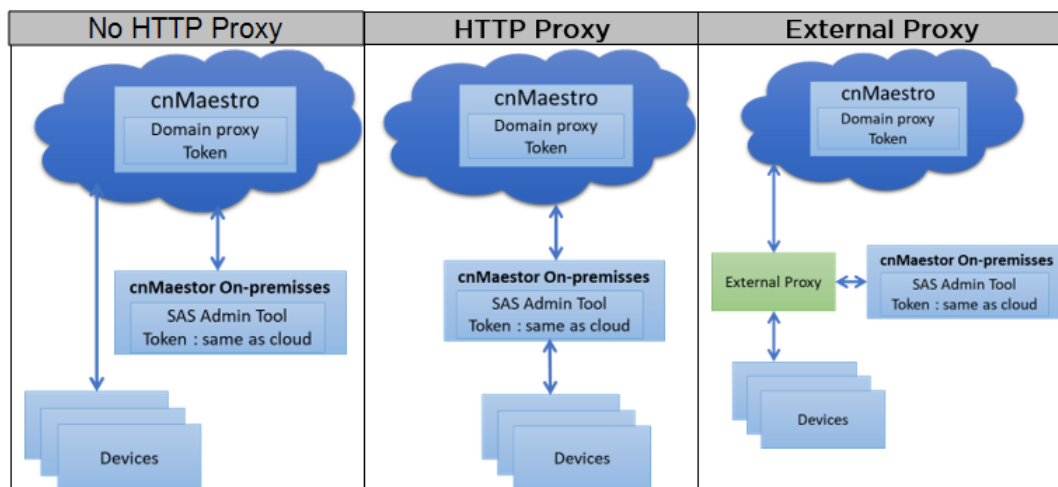
NOTE

The External HTTP Proxy method is preferred, because upgrades to cnMaestro could result in proxy downtime and lost CBRS connectivity.

- Configure the external HTTP Proxy to access the SAS Server through the Domain Proxy.
- Set the External HTTP Proxy as <http://proxy-ip:port number>.

Example: <http://11.110.0.101:9090>

For more details, refer [Using a Domain Proxy for CBRS connectivity](#).



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 is 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 started and managed by an authorized CPI (Certified Professional Installer). CPIs are required to enter necessary credentials to run and modify the CBRS parameters.

A CBRS sector view is shown below:

Services > CBRS

Account **Management Tool**

SAS Admin Tool helps CPI (Certified Professional Installer) to manage CBRS-compliant devices prior to installation.
CPI info is never stored either in the client side or server side.
After adding a new sector or AP, click on that newly added AP to allow you to start the tool.

Mac Search [View Jobs](#) [Add AP/BHM/RRH](#) [Import Sector](#) [Relinquish Grant](#) [Download Report](#)

<input type="checkbox"/> Device Name	Device Type	User ID	Tool Frequency (MHz)	Operating Frequency ...	Grant Type	Sector ID	Spectrum Reuse ID	Status
<input type="checkbox"/> AP_208-129	PMP 450i Connectorized	cambiumuser	N/A	3655 - 3685	Single	0a-00-3e-45-4...		
<input type="checkbox"/> AP_208-181	PMP 450i Connectorized	cambiumuser	3655 - 3675	3655 - 3675	Multiple	0a-00-3e-45-5...		
<input type="checkbox"/> AP_208-44	PMP 450i Connectorized	cambiumuser	3645 - 3675	3660 - 3670	Multiple	0a-00-3e-45-2...		
<input type="checkbox"/> AP_208-46	PMP 450i Connectorized	cambiumuser	3650 - 3670	3660 - 3670	Single	0a-00-3e-45-4...		
<input type="checkbox"/> RRH-202-111	Beta 3GHz cnRanger 210 RRH	cambiumuser	N/A	3610 - 3630	Single	58-c1-7a-36-ft...		

Showing 1 - 5 Total: 5 10 < Previous 1 Next >

Download Report

The Download Report allows the user to download multiple device reports in a .CSV format.

Services > CBRS

Account **Management Tool**

SAS Admin Tool helps CPI (Certified Professional Installer) to manage CBRS-compliant devices prior to installation.
CPI info is never stored either in the client side or server side.
After adding a new sector or AP, click on that newly added AP to allow you to start the tool.

Mac Search [View Jobs](#) [Add AP/BHM/RRH](#) [Import Sector](#) [Relinquish Grant](#) **[Download Report](#)**

<input type="checkbox"/> Device Name	Device Type	User ID	Tool Frequency (MHz)	Operating Frequency ...	Grant Type	Sector ID	Spectrum Reuse ID	Status
<input checked="" type="checkbox"/> AP_208-129	PMP 450i Connectorized	cambiumuser	N/A	3655 - 3685	Single	0a-00-3e-45-4...		
<input checked="" type="checkbox"/> AP_208-181	PMP 450i Connectorized	cambiumuser	3655 - 3675	3655 - 3675	Multiple	0a-00-3e-45-5...		
<input type="checkbox"/> AP_208-44	PMP 450i Connectorized	cambiumuser	3645 - 3675	3660 - 3670	Multiple	0a-00-3e-45-2...		
<input type="checkbox"/> AP_208-46	PMP 450i Connectorized	cambiumuser	3650 - 3670	3660 - 3670	Single	0a-00-3e-45-4...		
<input type="checkbox"/> RRH-202-111	Beta 3GHz cnRanger 210 RRH	cambiumuser	N/A	3610 - 3630	Single	58-c1-7a-36-ft...		

Showing 1 - 5 Total: 5 10 < Previous 1 Next >

Relinquish Grant

The Relinquish Grant relinquishes all grants of selected sector and places devices in the Registered state. The device will start Multi-Grant procedure if Multi-Grant feature is enabled on device.

Services > CBRS

Account **Management Tool**

SAS Admin Tool helps CPI (Certified Professional Installer) to manage CBRS-compliant devices prior to installation.
CPI info is never stored either in the client side or server side.
After adding a new sector or AP, click on that newly added AP to allow you to start the tool.

Mac Search [View Jobs](#) [Add AP/BHM/RRH](#) [Import Sector](#) **[Relinquish Grant](#)** [Download Report](#)

<input type="checkbox"/> Device Name	Device Type	User ID	Tool Frequency (MHz)	Operating Frequency ...	Grant Type	Sector ID	Spectrum Reuse ID	Status
<input checked="" type="checkbox"/> AP_208-129	PMP 450i Connectorized	cambiumuser	N/A	3655 - 3685	Single	0a-00-3e-45-4...		
<input checked="" type="checkbox"/> AP_208-181	PMP 450i Connectorized	cambiumuser	3655 - 3675	3655 - 3675	Multiple	0a-00-3e-45-5...		
<input type="checkbox"/> AP_208-44	PMP 450i Connectorized	cambiumuser	3645 - 3675	3660 - 3670	Multiple	0a-00-3e-45-2...		
<input type="checkbox"/> AP_208-46	PMP 450i Connectorized	cambiumuser	3650 - 3670	3660 - 3670	Single	0a-00-3e-45-4...		
<input type="checkbox"/> RRH-202-111	Beta 3GHz cnRanger 210 RRH	cambiumuser	N/A	3610 - 3630	Single	58-c1-7a-36-ft...		

Showing 1 - 5 Total: 5 10 < Previous 1 Next >



NOTE

- Relinquish Grant can be performed only for the Config_Synced devices which are running in Single Grant.
- PMP devices should be upgraded to release 20.2, that supports the Multi-Grant feature.

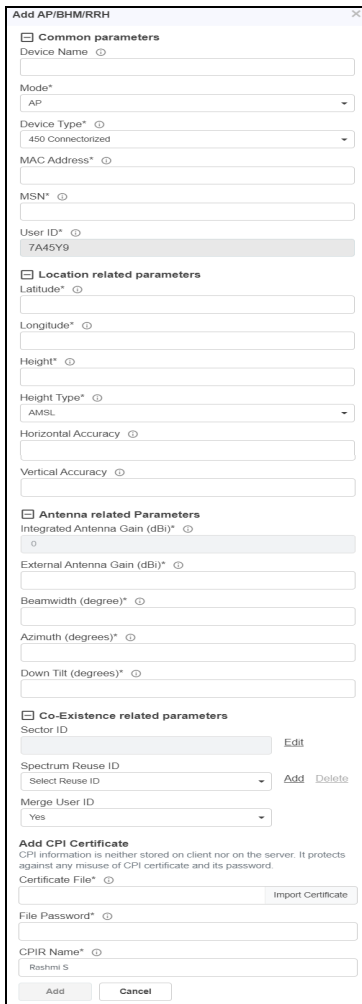
Creating a Management Tool Sector

A sector can be created in two ways:

- Add AP/BHM/RRH : Adding all parameters manually of an AP/BHM/RRH.
- Import Sector: Upload a file with all sector device details.

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 Merge User ID.
 - **Add CPI Certificate:** Certificate File, File Password, CPIR Name.



- Click **Add** to add a sector.



NOTE:

Merge User ID is applicable only for PMP devices, when SAS is Federated Wireless or CommScope.

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, Beam-width, 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.




NOTE:
Refer to [CBRS Device Parameters](#) for additional details.

Import Management Tool Sector

To import a sector, perform the following steps:

1. Navigate to **Services > CBRS > Management Tool** and click **Import Sector**.

2. 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
3. Click **Import Excel** to select Import Sector template file. File must be Microsoft Excel format (.xlsx) or OpenDocument Spreadsheet (ods) formats.
4. Enter CPI credentials:
 - a. Upload CPI Certificate File by clicking **Import Certificate**.
 - b. Enter **CPI File Password**.
 - c. Enter **CPI Registered Name**.
5. Enter the **Sector ID**.
6. Select **Spectrum Reuse ID** from the drop-down.
7. Select **Merge User ID**.
 - Selecting **Yes** to **Merge User ID** prefixes the User ID to the Sector ID and Spectrum Reuse ID in the registration message of the SAS.

	<p>NOTE</p> <ul style="list-style-type: none"> • Merge User ID is applicable only for PMP devices, when SAS is selected as Federated Wireless or CommScope. • 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.
---	---

8. Click **Import**.
- Import status is displayed as **Success**, **Info**, and **Invalid**.

✔ **Success:** 2Device(s) have been claimed. ▼
✘ **Invalid:** 1 Device(s) are not valid. ▼

9. Details of Success, Info and Invalid can be seen by clicking arrow (▼).

✘ **Invalid:** 1 Device(s) are not valid. ▲

MAC	Error
0a-00-3e-45-11-e4	Serial Number is invalid

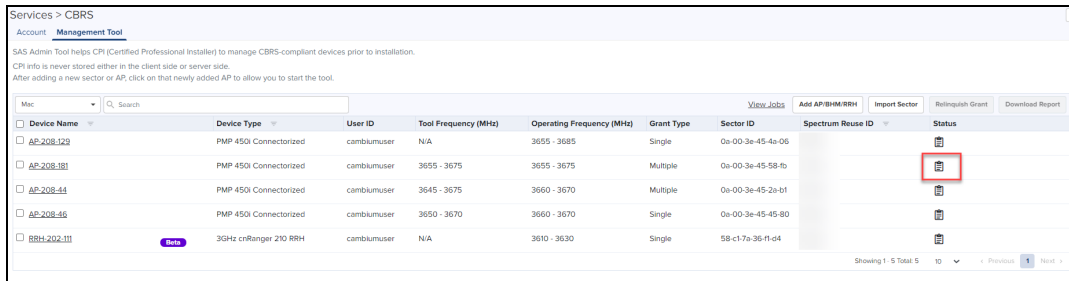
10. If the device is already claimed, it can be onboarded by clicking the **onboard** link.






i **Info:** 2 MAC(s) already claimed. Please onboard these devices, if not onboarded yet. ▼

Management Tool Sector Statistics

To view Sector Statistics, perform the following steps:

1. Navigate to **Services > CBRS > Management Tool**.
2. Click **View Sector Statistics**  under **Status**.



Device Name	Device Type	User ID	Tool Frequency (MHz)	Operating Frequency (MHz)	Grant Type	Sector ID	Status
AP-208-129	PMP 450i Connected	cambiumuser	N/A	3655 - 3685	Single	0a-00-3e-45-4a-06	
AP-208-181	PMP 450i Connected	cambiumuser	3655 - 3675	3655 - 3675	Multiple	0a-00-3e-45-58-7b	
AP-208-44	PMP 450i Connected	cambiumuser	3645 - 3675	3660 - 3670	Multiple	0a-00-3e-45-2a-b1	
AP-208-46	PMP 450i Connected	cambiumuser	3650 - 3670	3660 - 3670	Single	0a-00-3e-45-45-80	
RRH-202-111	3GHz cRanger 210 RRH	cambiumuser	N/A	3610 - 3630	Single	58-c1-7a-36-f1-d4	

3. **Sector Statistics** window pops up.


AP-208-46 Sector Statistics ✕

Device Information

Registered 2

Grant Information

Authorized 2



NOTE:

Refer to the [Live Status Update](#) for additional details.

Search Management Tool Sector

To search for a sector:

1. Navigate to **Services > CBRS > Management Tool**.
2. Select search option **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 in the search option, it displays the both AP devices and the related SM device.
- If an SM devices is entered in the search option, it displays only the SM devices.

4. Filtered 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.

2. All devices of sector is displayed.

Management Tool > AP-208-129

Tool Frequency (MHz): N/A
Operating Frequency (MHz): 3655 - 3685

Device Name	Device Type	Mode	Health	MSN	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Action
<input type="checkbox"/> AP-208-129	PMP 450I Co...	AP	Online	M9VH0V7S...	44.426736	-110.473536	N/A	22	● Unregistered	Not Synced	
<input type="checkbox"/> SM-208-130	PMP 450 Int...	SM	Online	M9VH0030...	44.426736	-110.473536	N/A	22	● Unregistered	Not Synced	

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

Sector Details View

- The Sector Details view displays the following fields by default:
 - Device Name, Device Type, Mode, Health, MSN, Latitude, Longitude, Sync Expiry Time, Height, Grant Status, Sync State, and Actions.


Management Tool > AP-208-129

Tool Frequency (MHz): N/A
Operating Frequency (MHz): 3655 - 3685

Device Name	Device Type	Mode	Health	MSN	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Action
<input type="checkbox"/> AP-208-129	PMP 450I Co...	AP	Online	M9VH0V7S...	44.426736	-110.473536	N/A	22	● Unregistered	Not Synced	
<input type="checkbox"/> SM-208-130	PMP 450 Int...	SM	Online	M9VH0030...	44.426736	-110.473536	N/A	22	● Unregistered	Not Synced	

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

- SM can be added in the sector by manually entering all parameters using the **Add SM** button or uploading a file containing SM details using the **Import SMs** button.

- Action column can edit or delete any device in the sector. Edit and Delete buttons will available depending of device state. Refer to [Edit Device](#) and [Delete Device](#) for more details.
- Click  on top bar to include additional fields in Sector Details view.

General

Device

Mode

Health

MSN

CBSD ID

Sync Expiry Time

Horizontal Accuracy

Vertical Accuracy

ECGI (E-UTRAN Cell Global Identifier)

Grant Status

Sync State

Location

Latitude

Longitude

Height

Height Type

Antenna

Integrated Antenna Gain (dBi)

External Antenna Gain (dBi)

Beamwidth (degree)

Azimuth (degrees)

Down Tilt (degrees)

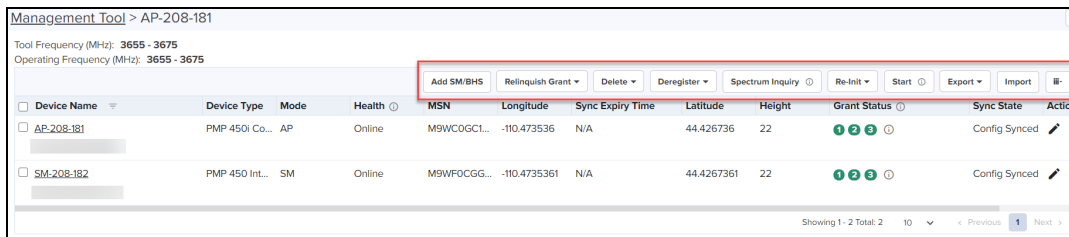
Max EIRP (dBm)

Requested EIRP (dBm)

Granted EIRP (dBm)

SAS Recommended EIRP (dBm)

- Use the following buttons to control CBRS procedure:




Management Tool > AP-208-181

Tool Frequency (MHz): 3655 - 3675
Operating Frequency (MHz): 3655 - 3675

Device Name	Device Type	Mode	Health	MSN	Longitude	Sync Expiry Time	Latitude	Height	Grant Status	Sync State	Action
AP-208-181	PMP 450I Co...	AP	Online	M9WC0GCL...	-110.473536	N/A	44.426736	22	1 2 3 ⊙	Config Synced	
SM-208-182	PMP 450 Int...	SM	Online	M9WF0CGG...	-110.4735361	N/A	44.4267361	22	1 2 3 ⊙	Config Synced	

Showing 1 - 2 Total: 2 | 10 | Previous | Next

- **Start** and **Stop** manage the 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 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 which generated in Wide-Grant mode.
- Once the sector is authorized (enters the AUTHORIZED state),  button transfers grant details from Management Tool to real devices.

Add SM or BHS

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Add SM/BHS** button to add SM in a sector.

Add SM/BHS

Common parameters

Device Name

Device Type*

450 Connector/hood

MAC Address*

MSN*

Location related parameters

Latitude*

Longitude*

Height*

Height Type*

Horizontal Accuracy

Vertical Accuracy

Antenna related Parameters

Integrated Antenna Gain (dBi)*

External Antenna Gain (dBi)*

Beamwidth(degrees)*

Azimuth (degrees)*

Down Tilt (degrees)*

Add CPI Certificate
CPI information is neither stored on client nor on the server. It protects against any misuse of CPI certificate and its password.

Certificate File*

File Password

CPIR Name*

Administrator

3. Enter all parameters under following categories:
 - a. **Common:** Device Name, Device Type, MAC Address, and MSN.
 - b. **Location:** Latitude, Longitude, Height and Height Type, Horizontal Accuracy and Vertical Accuracy.
 - c. **Antenna Parameters:** Integrated Antenna Gain, External Antenna Gain, Beam width, Azimuth and Down Tilt.
 - d. **Add 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 SMs** button to import SMs in 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 OpenDocument Spreadsheet (ods) formats.
6. Enter CPI Credentials:
 - Upload CPI Certificate File by clicking **Import Certificate** button.
 - Enter CPI File Password.
 - Enter CPI Registered Name.
7. Click **Import**.

Import status is displayed under **Success**, **Info** and **Invalid** sections.

8. Details of Success, Info and Invalid can be seen by clicking **▼**.

MAC	Error
	Serial Number is invalid

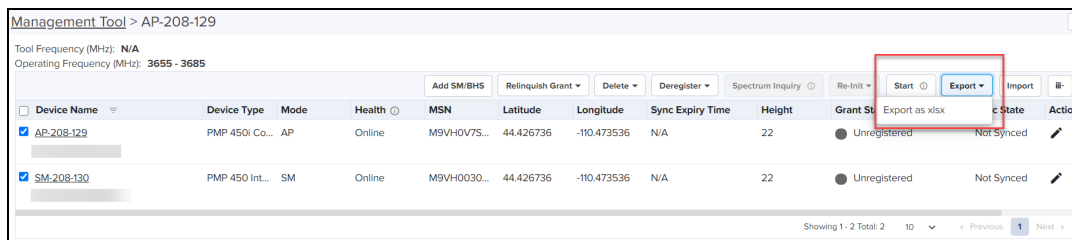
9. If the device is already claimed, it can be onboarded by clicking **onboard** link.

10. Once the user clicks **Import**, a job will be scheduled.

Job Status (import): **Scheduled** [Stop Job](#)

Export Sector

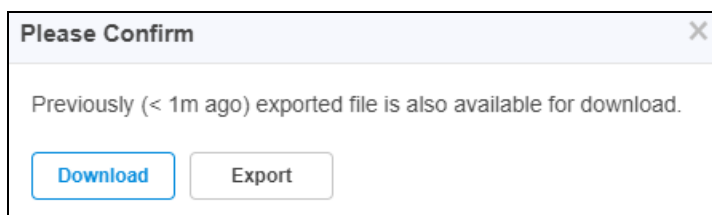
1. Navigate to **Services > CBRS > Management Tool** and then select a **sector**.
2. Click **Export** button to export the sector(export as xlsx).




3. Once the user clicks as **xlsx**, a job will be scheduled.

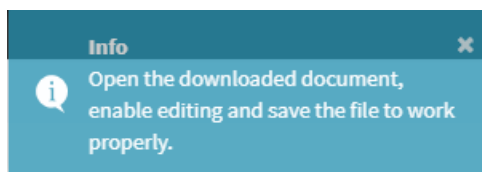
Job Status (Export): **Completed** [Download](#)

4. Once the Job status is Completed, click **Download** to download the Sector xlsx.



 **NOTE:**
Download button is enabled only for two hours after the export job completes.

5. User can use the downloaded .xlsx file for importing 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.

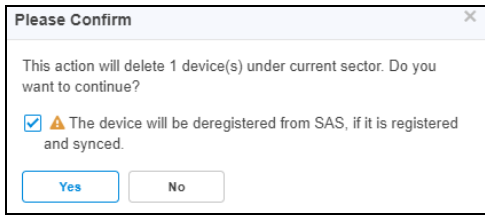
5. Click **Save**.

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 considered 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 [CBRS State Diagram](#)).
4. Once the SM is selected, click **Delete** to display **All** or **Selected**. Click **Selected**.
 - **All** : delete the complete registered SM devices.
 - **Selected** : delete the selected device.

Device Name	Device Type	Mode	Health	MSN	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Action
AP-208-129	PMP 450I Co...	AP	Online	M9VH0V75...	44.42		N/A	22	Unregistered	Not Synced	
SM-208-130	PMP 450 Int...	SM	Online	M9VH0030...	44.426736	-110.473536	N/A	22	Unregistered	Not Synced	

5. Click **Yes** to confirm.



6. Once the user clicks **Yes**, a job will be scheduled.

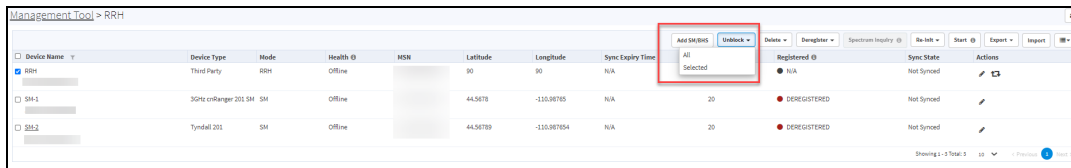


7. Deleting an AP:

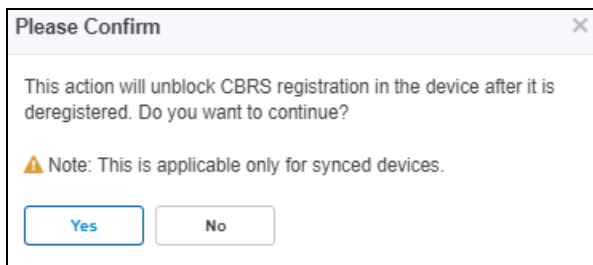
- All SMs of the sector must be deregistered before deleting an AP. Refer to [Deregistration](#) procedure to deregister all SM devices.
- Select AP of the sector to delete. Start CBRS procedure.
- Click **Delete**.

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 deregistration flag on the device.
3. Once the device is selected, click **Unblock** and choose **All** or **Selected** from the drop-down.
 - **All** : unblock the complete registered devices.
 - **Selected** : unblocks the selected single device.



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 Wider-Grant sector.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Start** to start CBRS procedure of a sector.
3. Once the user clicks start, the **Spectrum Inquiry** window pops up.

Spectrum Inquiry (Wed Mar 31 2021 22:42:13 UTC +0530)

Editing the co-existence parameter will reset the SAS timer. Edit only if really needed

SAS provided spectrum availability view

This feature will enable multi grant on the tool.

Sorted By Ranking

Sorted By Frequency

● Unavailable ● PAL ● Selected frequency range ● GAA

Co-Existence Configuration

Sector ID: Spectrum Reuse ID:

Spectrum Reuse ID Statistics

Spectrum Reuse IDs already defined in your Network

Spectrum Reuse ID	Center Frequency (MHz)/Channel Bandwidth (MHz) [Sector Count]
Balaji	3655/20 [3]

EIRP computation

Devices are listed with calculated maxEIRP and requested EIRP based on the selected center frequency and channel bandwidth. Click Save to update the EIRP of devices and continue the procedure

I understand, SAS may take up to 5h 40m to fully process the co-ex parameters and the Spectrum Inquiry response may not be updated yet

Center Frequency (MHz)*: Channel BW (MHz)*: SAS Allowed Total MaxEIRP (dBm):



NOTE:

- Multi-Grant is enabled by default.
- Sorted By Ranking is applicable for users selecting Google or Federated Wireless SAS.

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 to **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**.

Once the Sector is created it displays as shown below:

Management Tool > AP-208-129

Tool Frequency (MHz): N/A
Operating Frequency (MHz): 3655 - 3685

Device Name	Device Type	Mode	Health	MSN	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Actions
AP-208-129	PMP 450 Conn...	AP	Online	M9VH0V7SVT3P	44.426736	-10.473536	2d 2h 25m	22	Registered	Not Synced	<input type="button" value="Edit"/> <input type="button" value="Refresh"/>
SM-208-100	PMP 450 Intri...	SM	Online	M9VH0030N2TH	44.426736	-10.473536	N/A	22	Unregistered	Not Synced	<input type="button" value="Edit"/>

Showing 1 - 2 Total: 2



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 in multiple of 10 MHz channel. 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 and status will be updated accordingly..

To enable Multiple Grant for 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:

Spectrum Inquiry (Wed Mar 31 2021 20:22:41 UTC +0530)

Editing the co-existence parameter will reset the SAS timer. Edit only if really needed

SAS provided spectrum availability view
 This feature will enable multi grant on the tool.

Sorted By Ranking

Rank	Max EIRP (dBm per MHz)	Frequency Range (MHz)
1	36	3570-3580
2	36	3580-3590
3	36	3590-3600
4	36	3600-3610
5	36	3610-3620
6	36	3620-3630
7	36	3630-3640
8	36	3640-3650
9	36	3650-3660
10	36	3550-3560
11	36	3560-3570
12	36	3640-3650
13	36	3650-3660
14	36	3660-3670
15	36	3670-3680

Sorted By Frequency

Rank	Max EIRP (dBm per MHz)	Frequency Range (MHz)
10	36	3550-3560
11	36	3560-3570
1	36	3570-3580
2	36	3580-3590
3	36	3590-3600
4	36	3600-3610
5	36	3610-3620
6	36	3620-3630
7	36	3630-3640
12	36	3640-3650
13	36	3650-3660
14	36	3660-3670
15	36	3670-3680
8	36	3680-3690
9	36	3690-3700

Legend: Unavailable (grey), PAL (orange), Selected frequency range (blue), GAA (green)

Co-Existence Configuration

Sector ID: 03-00-3e-45-4a-06 | Spectrum Reuse ID: Balaji | [Edit](#)

Spectrum Reuse ID Statistics

Spectrum Reuse IDs already defined in your Network

Spectrum Reuse ID	Center Frequency (MHz)/Channel Bandwidth (MHz) [Sector Count]
Balaji	3685/20 [3685/20] [3685/20]

EIRP computation

Devices are listed with calculated maxEIRP and requested EIRP based on the selected center frequency and channel bandwidth. Click Save to update the EIRP of devices and continue the procedure

I understand, SAS may take up to 7h 59m to fully process the co-ex parameters and the Spectrum Inquiry response may not be updated yet

Center Frequency (MHz)*: Please Select | Channel BW (MHz)*: Please Select | SAS Allowed Total MaxEIRP (dBm): [] | [Calculate Max EIRP](#)

**NOTE:**

- Multi-Grant is enabled by default.
- Merge User ID is applicable only for PMP devices, if user selects SAS is either Federated Wireless or CommScope.

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**.

Once the Sector is created with Multiple Grants will be displayed as shown below:

Device Name	Device Type	Mode	Health	MSN	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Actions
AP-208-381	PMP 450I Comm...	AP	Online	M9WC0GCH40F	44.426736	-110.473536	N/A	22	1 2 3 4	Config Synced	✎
SM-208-382	PMP 450I Integr...	SM	Online	M9WFOCGG7L3F	44.4267361	-110.4735361	N/A	22	1 2 3 4	Config Synced	✎

To view the Grant Status click the info icon

Grant Status

1 Authorized
Last Heartbeat: Mar 31 2021 22:51:27
Frequency (MHz): 3655 - 3660
Channel BW (MHz): 5

2 Authorized
Last Heartbeat: Mar 31 2021 22:51:27
Frequency (MHz): 3660 - 3670
Channel BW (MHz): 10

3 Authorized
Last Heartbeat: Mar 31 2021 22:51:27
Frequency (MHz): 3670 - 3675
Channel BW (MHz): 5

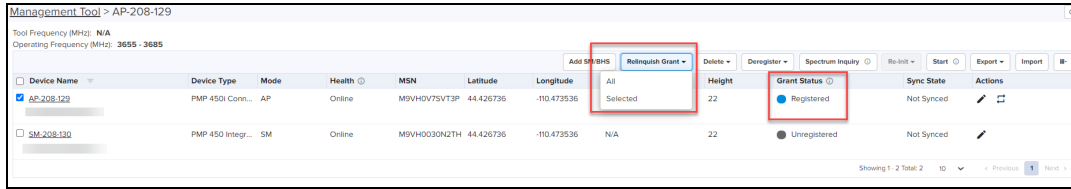
Relinquish Grant

The Relinquish Grant relinquishes all grants of selected sector. This will make devices to go to Registered state. The device will start Multi-Grant procedure if Multi-Grant feature is enabled on device.

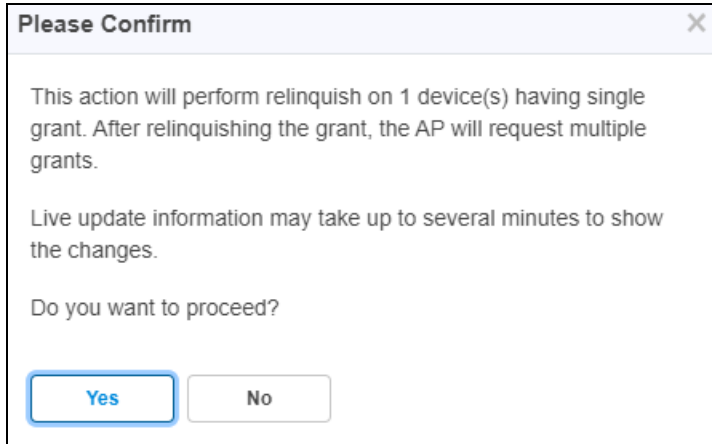
To Relinquish Grant Perform as follows:

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 SM devices.

- **Selected** : Relinquish the selected device.



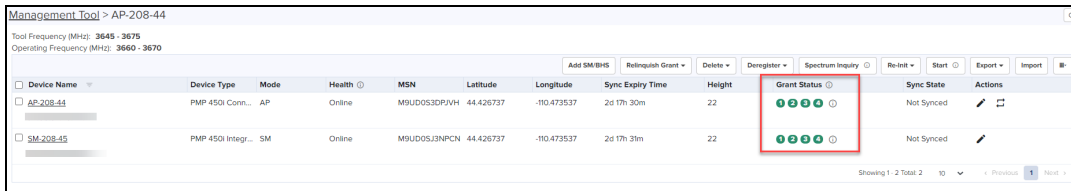
3. Click **Yes** to confirm the action.



NOTE:

Live update information may take upto several minutes to display the changes of reflected relinquish status.

Once the user clicks **Yes**, **Wider Grant** gets converted to the **Multiple Grants** as shown below:



Stop CBRS Procedure

The **Stop** button allows the user to stop 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 of a sector.



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 **Re-init** button. Clicking **Re-init** reinitializes selected devices are reinitialized 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** button. 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 the user to deregister devices from the Domain Proxy.

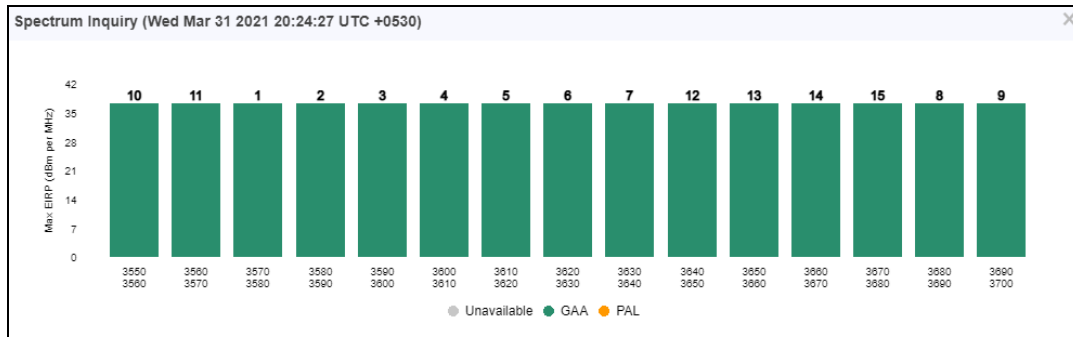
1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** if the CBRS procedure is already running.
3. Select one or more devices which need to be deregistered.
4. Click **Deregister** to deregister selected devices.
5. Once the user clicks **Deregister**, once a job will be scheduled.

Job Status (Deregistration): **Completed**

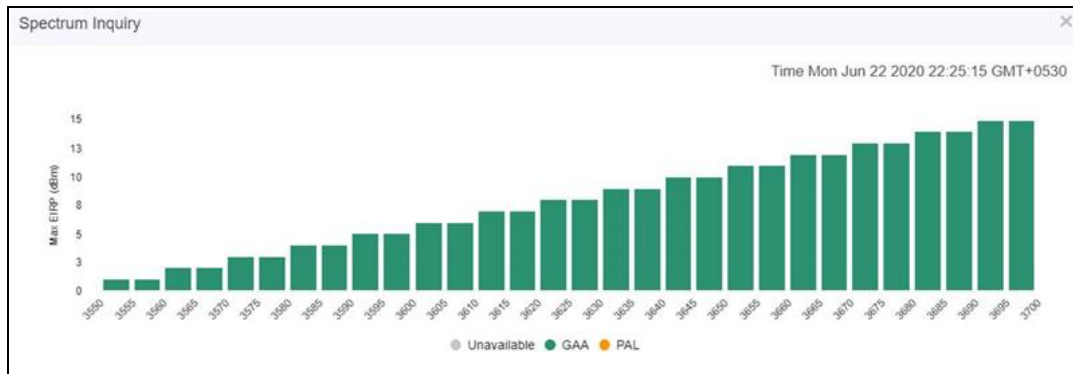
6. If deregistration fails, the reasons will be indicated under .

Spectrum Inquiry

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Spectrum Inquiry** button.
3. **Spectrum Inquiry** status button is enabled once the device is registered (REGISTERED state) to the SAS.
 - If the selected SAS is not Google, EIRP is unsupported, and Spectrum Inquiry is displayed as shown below:



- If the user is selected SAS is **Google**, it supports EIRP. Spectrum Inquiry displays as below:



- **GAA**: General Authorized Access
- **PAL**: Priority Access License

Spectrum availability can be checked by hovering over frequencies.

Device Sync

The Sync procedure allows user to transfer grant information from Management Tool to respective device.

For a PMP sector, the Sync action can only be performed on an AP or BHM. The SM and BHS gets synced automatically when it comes online.

For an LTE sector, which supports a Cambium SM with a 3rd party BBU and RRH, the sync action will sync the Cambium SMs in this sector.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Sync** button to perform sync procedure.
3. Click **Yes** on the pop-up or click **NO** to cancel the sync procedure.

Once **Yes** is clicked, the Management Tool will check the accessibility of AP/BHM before proceeding with sync.

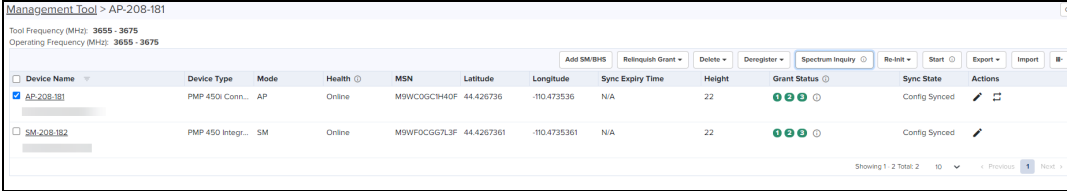


NOTE:

- PMP SM cannot be manually synced. It is only synced automatically.
- Once the device is synced, for both PMP and LTE devices, primary management is transferred from the tool to the device itself. However, some actions and procedures are still supported on the tool. See the [CBRS Consolidated Procedures Guide](#) for more details.
- Sync procedure copies complete CBRS parameters to device and enables CBRS to transmit with configured parameters.

Live Status Update

Once the device is Config synced, displays the CBRS details like CBSD ID, Grant ID, CBSD Grant State and Last Heartbeat Time from the devices every 5 minutes.



Device Name	Device Type	Mode	Health	MSN	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Actions
AP-208:381	PMP 450i Conn...	AP	Online	M9WC0GC1H40F	44.426736	-110.473536	N/A	22	●●●○	Config Synced	✎
SM-208:382	PMP 450 Integr...	SM	Online	M9WFOCGG7L3F	44.4267361	-110.4735361	N/A	22	●●●○	Config Synced	✎

It displays the possible single Grant state such as:

- Authorized
- Deregistering
- Grant
- Grant Suspended
- Grant Terminate
- Registered
- Registering
- Relinquished Spectrum
- Relinquishing Spectrum
- Unregistered
- Unknown

Management Tool Sync

The Sync procedure allows the user to transfer grant information from the Management Tool to a real device. The Sync action can only be performed on an AP or BHM. The SM and BHS are synced automatically when they come online. Once the AP/BHM/SM/BHS are synced, no further action is taken from Management Tool.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Sync** to perform the synchronization procedure.
3. Click **Yes** to enable CBRS on AP/BHM after successful sync or click **No** to cancel synchronization procedure.

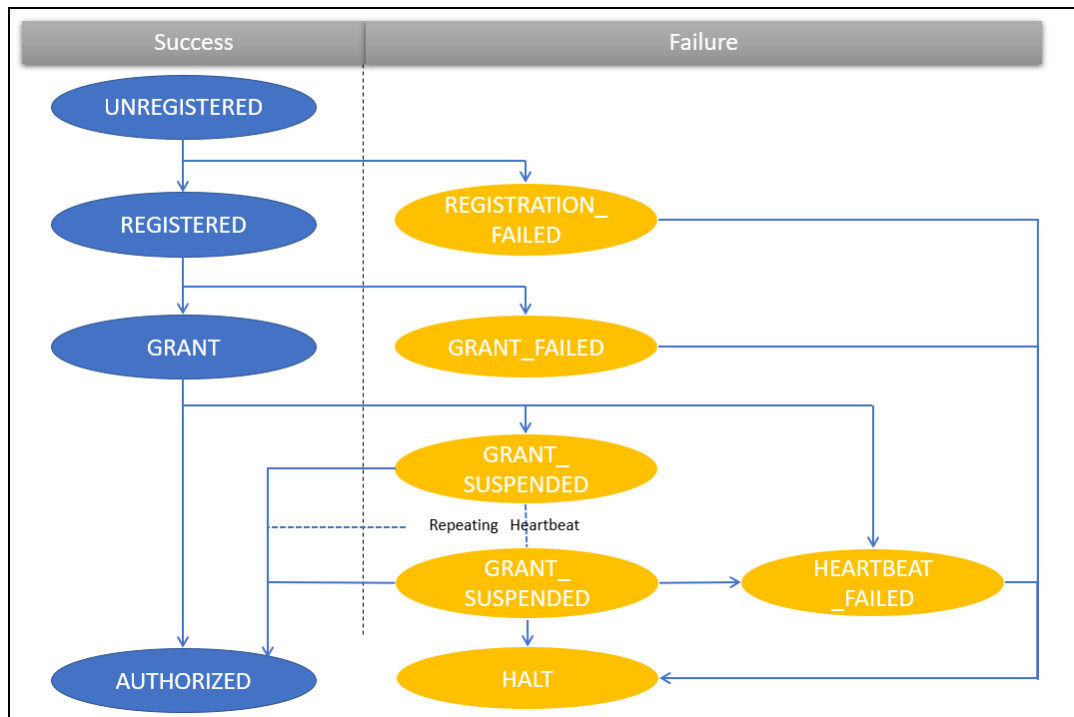
Once **Yes** is clicked, the Management Tool checks the accessibility of AP/BHM and proceeds with sync.



NOTE:

- AP or BHM requires manual Sync whereas SM or BHS does not require manual Sync. The latter two are synced automatically.
- Once the device is synced, it cannot be administered by the Management Tool.
- The Sync procedure copies CBRS parameters to the device and enables CBRS to transmit with configured parameters.

CBRS State Diagram



NOTE:

GRANT_SUSPENDED is a temporary suspend state where HEARTBEAT messages are sent for an extended period prior to getting AUTHORIZED.

The CBRS procedure has the following states:

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 (max 120 characters. This is to identify device on SAS Admin: it does not get copied to the device via sync.
	Device Type	Drop-down selection of supported devices.
	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_

Category	Parameter	Details
		FAILED.
Location	Height	Device antenna height in meters.
	Height Type	Should be AGL or AMSL as follows: <ul style="list-style-type: none"> AGL height is measured relative to the ground level. AMSL height is measured relative to the mean sea level.
	Horizontal Accuracy	A positive number in meters to indicate the accuracy of the device antenna horizontal location.
	Latitude	Latitude of the device antenna location in degrees.
	Longitude	Longitude of the CBSD antenna location in degrees.
	Vertical Accuracy	A positive number in meters to indicate the accuracy of the device antenna vertical location.
Co-Existence Related Parameters	Sector ID	The default AP MAC address and allows editing the default MAC address.
	Spectrum Reuse ID	The Spectrum Reuse ID defined in the network.
	Merge 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 calculates 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.
	Certificate File	CPI's (Certified Professional Installer) certificate.

Category	Parameter	Details
Add Certificate	CPIR Name	CPI's registered name.
	File Password	CPI's private password.

Using a HTTP Proxy Server for CBRS Connectivity

Proxy Suggestions for CBRS Connectivity

We do not recommend against using cnMaestro On-Premises, as a HTTP Proxy for CBRS connectivity. Normally, upgrades to cnMaestro that result in a small amount of downtime do not impact network devices under management. In the case of CBRS even a brief outage of the proxy during upgrade will result in a network outage.

External Proxy Requirements

If you already use a forward proxy in your network, continue to use it rather than set up a new one. Connections will be made using HTTP CONNECT to sas.cbrs.cambiumnetworks.com and your proxy needs to allow this. A TLS intercepting proxy (such as a security gateway) will break connectivity.

Squid as External Proxy

The following configuration will work for an external proxy configuration, but it does not offer high-availability, and it may not be in line with your network standards. We have tested this configuration using on fresh installs of:

- Ubuntu 20.04 / Squid Cache: Version 4.10
- Centos 7 / Squid Cache: Version 3.5.20

```
## WARNING:
## While this config may work for your use case,
we encourage you to follow your own best practices and modify this file for your network.
## Tested on squid version 4.10
## This localnet ACL is not useful unless you want to use this proxy for anything other than
a cbrs proxy.
#acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
#acl localnet src fc00::/7 # RFC 4193 local private network range
#acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
## This cbrs ACL limits connections to sas.cbrs.cambiumnetworks.com only.
acl cbrs dstdomain sas.cbrs.cambiumnetworks.com
## Updates require access to destinations under cloud.cambiumnetworks.com
## This is a separate ACL for readability, but can be combined with the cbrs ACL if
preferred.
acl cloud dstdomain .cloud.cambiumnetworks.com
## This group blocks http CONNECT to non-standard https ports
acl SSL_Ports port 443
acl CONNECT method CONNECT
http_access deny CONNECT !SSL_Ports
## Allow access only to the sas and cloud acls. Add your own ACLs here if needed
http_access allow CONNECT cbrs
http_access allow CONNECT cloud
http_access deny all
## We dont need any cache for proxying cbrs traffic cache deny all Port config, change this
to suit your requirements
http_port 3128
```


HA for Squid external proxy

Since a standalone proxy is a single point of failure, we recommend using an HA setup for Squid. This can be done using Pacemaker or DRDB.

LTE

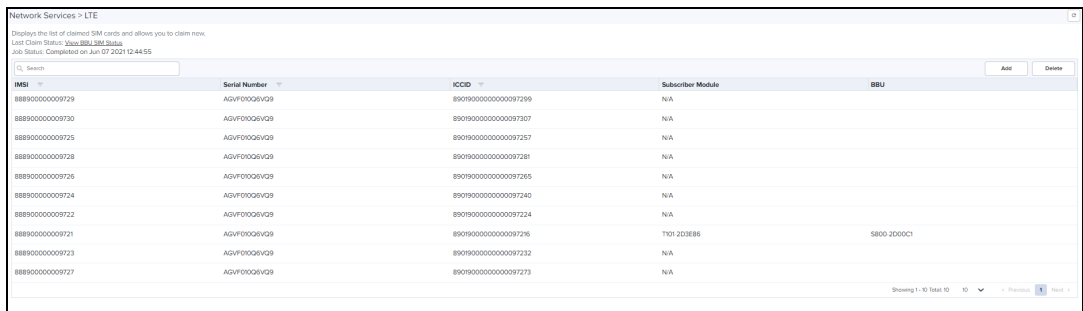
cnMaestro supports LTE as part of its On-Premises deployment. LTE allows customers to onboard the SM with IMSI into cnMaestro.

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

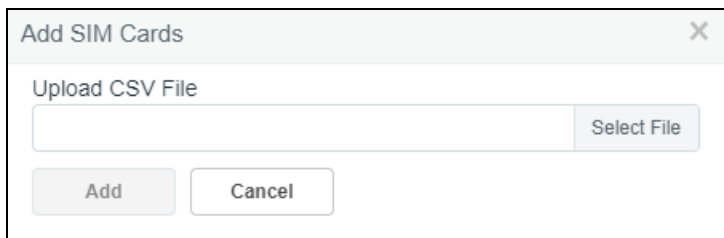
To add a SIM card:

1. Navigate to **Services > LTE**.



IMSI	Serial Number	ICCID	Subscriber Module	BBU
88890000009729	AGVF00G6VQ9	890190000000000097299	N/A	
88890000009730	AGVF00G6VQ9	890190000000000097307	N/A	
88890000009725	AGVF00G6VQ9	890190000000000097257	N/A	
88890000009728	AGVF00G6VQ9	890190000000000097281	N/A	
88890000009726	AGVF00G6VQ9	890190000000000097265	N/A	
88890000009724	AGVF00G6VQ9	890190000000000097240	N/A	
88890000009722	AGVF00G6VQ9	890190000000000097224	N/A	
88890000009721	AGVF00G6VQ9	890190000000000097216	T101-2D3E86	S800-20D0C1
88890000009723	AGVF00G6VQ9	890190000000000097232	N/A	
88890000009727	AGVF00G6VQ9	890190000000000097273	N/A	

2. Click **Add**. The following window appears:



Add SIM Cards

Upload CSV File

Select File

Add Cancel

3. Select the CSV file and click **Add**.

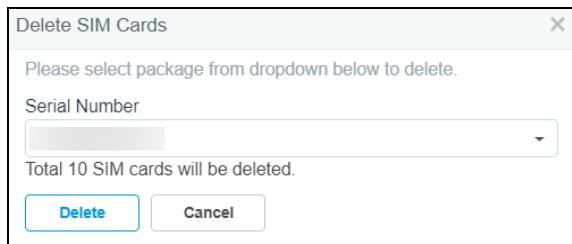


Note:

User can download the .CSV file from the Cloud account once the Serial Number is validated from the cnMaestro Cloud data base.

Delete SIM Cards

To delete a SIM card from the list, click **Delete**. The following window pops-up.



Delete SIM Cards

Please select package from dropdown below to delete.

Serial Number

Total 10 SIM cards will be deleted.

Delete Cancel



Note:

IMSI numbers are deleted with the mapped Serial Number.

Viewing BBU SIM Status

Allows the users to view the status of the SIM connected to the BBU:

1. Navigate to **Services > LTE**.

Network Services > LTE

Display the list of claimed SIM cards and allows you to claim new.
Last Claim Status: [View BBU SIM Status](#)
Job Status: Completed on Jun 07 2021 12:44:55

IMSI	Serial Number	ICCID	Subscriber Module	BBU
88890000009729	AGVF0009VG9	89019000000000097299	N/A	
88890000009730	AGVF0009VG9	89019000000000097307	N/A	
88890000009725	AGVF0009VG9	89019000000000097257	N/A	
88890000009728	AGVF0009VG9	89019000000000097281	N/A	
88890000009726	AGVF0009VG9	89019000000000097265	N/A	
88890000009724	AGVF0009VG9	89019000000000097240	N/A	
88890000009722	AGVF0009VG9	89019000000000097224	N/A	
88890000009721	AGVF0009VG9	89019000000000097216	T301 2D0E86	5800 2000C1
88890000009723	AGVF0009VG9	89019000000000097232	N/A	
88890000009727	AGVF0009VG9	89019000000000097273	N/A	

Showing 1 - 10 Total: 10

2. Click **View BBU SIM Status**.

BBU Sim Status


Search

Name	IP	MAC	State	Last Updated Time
S800-2D0172	192.168.158.60		SKIPPED	Feb 19 2020 15:12:00
S800-2D009D	10.120.253.60		SKIPPED	Feb 19 2020 15:12:00
S800-2D006D	10.120.242.20		SKIPPED	Feb 19 2020 15:12:00
S800-2D01B1	10.120.152.5		SKIPPED	Feb 19 2020 15:12:00
RV-S800-2D0067	10.120.110.1		COMPLETE	Feb 19 2020 15:12:00
Zurich Tower BBU	10.120.108.60		COMPLETE	Feb 19 2020 15:12:00
S800-2D00E2	10.110.243.20		COMPLETE	Feb 19 2020 15:12:00
S800-	10.110.243.16		FAILURE	Feb 19 2020 15:12:00
S800-	10.110.243.12		COMPLETE	Feb 19 2020 15:12:00
S800-2D00C7	10.110.243.12		SKIPPED	Feb 19 2020 15:12:00

Showing 1 - 10 Total: 14

cnArcher Installation Summary

cnArcher is a mobile application used to install PMP Subscriber Modules (SMs), ePMP (SMs), and cnRanger SM. The installation summary provides an overview of the data collected by cnArcher during the installation process.

	<p>NOTE</p> <ul style="list-style-type: none"> • cnArcher Installation Summary is a cnMaestro X feature. • cnArcher Installation summary of PMP SM is available for users in cnMaestro Cloud and OnPremises from 3.1.0 release.
---	--

To view the installation summary:

1. Navigate to **Network Services > cnArcher Installation Summary**.
The **cnArcher Installation Summary** page appears.
2. You can **Search** cnArcher Summary details by using **MAC Address, Name at Installation, Date and Time, Added By, and Comments**.

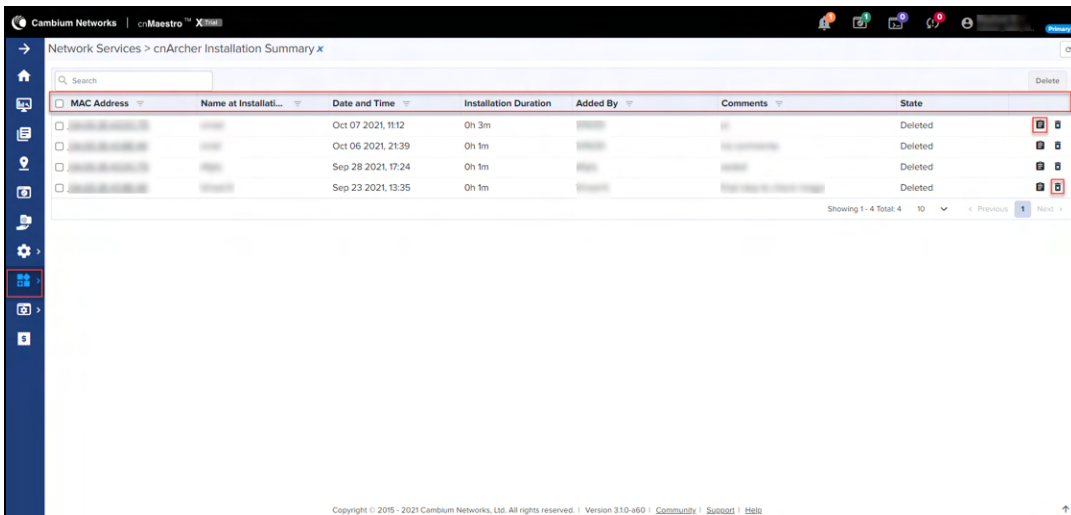


Table 49: Fields in cnArcher Installation Summary

Field	Description
MAC Address	MAC address of the device.
Name at Installation	Name given to the device when installed.
Date and Time	Date and time of installation.
Installation Duration	Duration of installation.
Added By	Name of the user adding the device.
Comments	Comments about the installation.
State	Current state of the device such as Managed or Deleted.

3. Click **View Details**  icon to view detailed Installation Summary.

Installation Summary : deo-sm-450b on Nov 09 2021, 11:34

Summary	Configuration
SM Name: deo-sm-450b	IP Address/Setting: 10.110.246.167/Static
MAC Address: [REDACTED]	Subnet: 255.255.255.0
MSN: [REDACTED]	Gateway: 10.110.246.254
Product: PMP 450b High Gain SM 3.6 ...	DNS: 10.110.12.110
Software Version: CANOPY 20.3.1 (Build DEV-2...	Management VLAN: Not Configured
RSSI: -52.2 dBm	Data VLAN: Not Configured
SSR: 3	Security: none
External Antenna: No External Antenna	PSK: -
Start Timestamp: Nov 09 2021, 11:28	Status: Onboarded
End Timestamp: Nov 09 2021, 11:31	Software Update: No change
Added By: VINOD	Template: Not Configured
Comment: deviceinstallation 450b	Onboarding Details: -

Photos & Location: 4b

Link Test Result			
Time	Mode	Throughput Uplink/Downlink	Modulation Uplink/Downlink
Nov 09 2021, 11:30	Extrapolated	1.7 Mbps / 47.1 Mbps	4 X / -

AP Scan Result			
AP MAC	AP Bandwidth	AP Frequency	Registered
[REDACTED]	40 MHz	3625.0 MHz	Yes

Table 50: Summary fields in cnArcher Installation

Field	Description
SM Name	Name of the device.
MAC Address	MAC address of SM.
MSN	Serial number of device.
Product	Device model and type .
Software Version	Software version of device.
RSSI	Receiver Signal Strength Indicator (RSSI) of SM.
SSR	Signal Strength Ratio (SSR).

Table 50: Summary fields in cnArcher Installation

Field	Description
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.
Comment	Comments about the installation process.

Configuration

Table 51: Configuration fields in cnArcher Installation

Field	Description
IP Address/Setting	IP settings such as for DHCP or Static IP allocation.
Subnet	Subnet mask of the device.
Gateway	IP address of the gateway.
DNS	Name of the DNS server.
Management VLAN	Configured Management VLAN.
Data VLAN	Configured Data VLAN.
Security	Security settings.
PSK	Type of PSK (Pre-Shared Key): WPA or WPA2.
Status	Current SM state such as Onboarded or Already Onboarded.
Software Update	Software version provided to upgrade.
Template	Name of the configuration template to apply.
Onboarding Details	Onboarding details related to SM.

Photos and Location

Photos and Location displays the photos taken during installation. You can view a maximum of four photos at a time.

Link Test Result

Link Test Result displays the link related test results with respect to throughput.

Table 52: Link Test Results fields


Field	Description
Mode	Modes such as Extrapolated Link Test or Link Test with Bridging.
Modulation Uplink/Downlink	Uplink and Downlink Modulation.
Time	Time at which the link test was performed.
Throughput Uplink/Downlink	Uplink and Downlink Throughput.

AP Scan Result

AP Scan Result displays a list of scanned APs.

Table 53: Fields in AP Scan Result

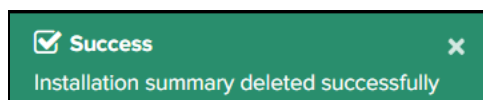
Field	Description
AP MAC	MAC address of the AP.
AP Bandwidth	Bandwidth of the AP.
AP Frequency	Frequency of the AP.
Registered	Details of the registered SM.


4. Click **Delete**  icon to delete single or multiple entries from the **cnArcher Installation Summary** page.
5. Click **Yes** to proceed to delete.

Please confirm

Are you sure you want to delete?

6. A confirmation message is displayed on a successful delete.



	<p>NOTE</p> <p>cnArcher uploads Installation Summary with cnMaestro when Internet connection is available to users mobile device. This feature is support only in Android.</p>
---	---

Administration

This section includes the following topics:

- User Management
- Server Management
- Syslog
- Webhooks
- Audit Logs

User Management

This chapter provides the following details:

- Authentication
- Local Users
- Authentication Servers
- Session Management

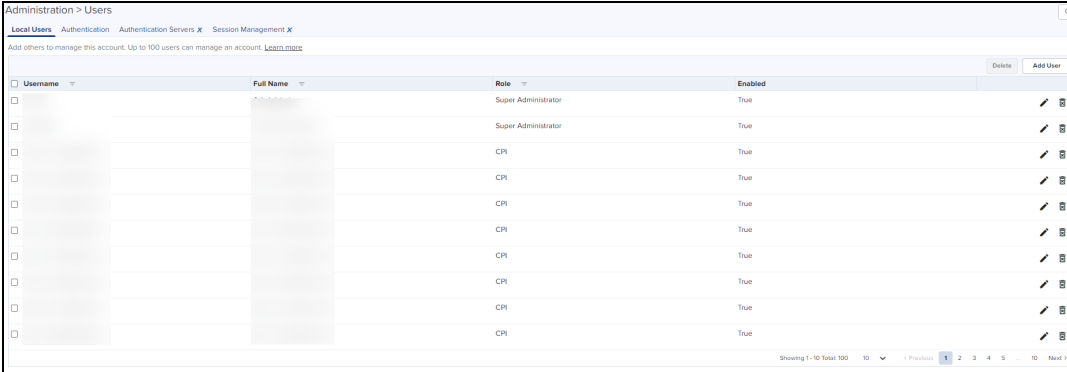
Authentication

cnMaestro On-Premises supports a Primary mode of authentication and an optional Secondary mode. If the Primary mode is Local Users (users specified in cnMaestro in the Users tab), no Secondary mode is available. If the Primary mode is an Authentication Server, then the Secondary mode will be set to Users and cannot be changed.

Local Users

To add Local Users, navigate to **Administration > Users**.

Figure 156 Adding Users



Username	Full Name	Role	Enabled	
		Super Administrator	True	[edit] [delete]
		Super Administrator	True	[edit] [delete]
		CPI	True	[edit] [delete]
		CPI	True	[edit] [delete]
		CPI	True	[edit] [delete]
		CPI	True	[edit] [delete]
		CPI	True	[edit] [delete]
		CPI	True	[edit] [delete]
		CPI	True	[edit] [delete]
		CPI	True	[edit] [delete]

Role-Based Access

Each user is assigned a Role that defines their authorization. On successful authentication, every request from this user is processed in light of their Role.

cnMaestro supports the following user Roles:

- **Super Administrator** – Super Administrators can perform all operations.

- **Administrator** – Administrators can modify cnMaestro application functionality, but they are not able to edit User, API, or Server configuration.
- **Operator** – Operators are able to configure device-specific parameters and view all configuration.
- **Monitor** – Monitors have only view access.
- **CPI** – CPI can perform onboarding the devices using the CBRS tool and has the view access only.



NOTE:

- cnMaestro On-Premises allows the user to limit the number of concurrent sessions for each Role and display current active user sessions.
- CPI role is authorized only when the **CBRS** is enabled.

Role-Mappings

The table below defines how Roles are authorized to access specific features.

Table 54: Role-Mappings

Feature	Description
Authentication Services	Create and configure Authentication servers. <ul style="list-style-type: none"> • Super Administrator - All • Administrator - None • Operator - None • Monitor - None • CPI - None
API Management	API Client. administration. <ul style="list-style-type: none"> • Super Administrator - All • Administrator - None • Operator - None • Monitor - None • CPI - None
Application Operations	Application level operations such as to create, update and delete operations for Networks, Towers/Sites. Bulk device configuration. <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Application Settings	Change global application configuration and onboarding key. <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None

Table 54: Role-Mappings

Feature	Description
Configuration/Software Update and Scheduled Report Jobs	Manage configuration/software update and scheduled report related jobs <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator - All ● Monitor - None ● CPI - None
Data Tunnel	Data tunnel configuration. <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator - View ● Monitor - View (Statistics tab only) ● CPI - View (Statistics tab only)
Device Operations	Device operations such as reboot device, link test, connectivity test, technical support file download, and Wi-Fi performance test. <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator - All ● Monitor - None (except Wi-Fi Performance test which is supported in On-Premises only) ● CPI - None (except Wi-Fi Performance test which is supported in On-Premises only)
Device Overrides	Per-device configuration, including updating AP Group and applying configuration. <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator - All ● Monitor - None ● CPI - None
Global Configuration	The ability to create and apply configuration for global features such as Templates, WLANs, AP Groups, auto-provisioning, and bulk sync configuration. <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator -View ● Monitor - None ● CPI - None
Guest Portal	Guest Portal configuration.

Table 54: Role-Mappings

Feature	Description
	<ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator -View ● Monitor - View (sessions only) ● CPI - View (sessions only)
Monitoring	<p>Display of monitoring data at all levels, VM Monitoring</p> <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator - All ● Monitor - View ● CPI - View
Managed Service Provider (MSP)	<p>MSP operations such as modification of branded service, managed account and user invitations.</p> <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - View ● Operator - None ● Monitor - None ● CPI - None <p>Note: Operator/Monitor users are not permitted to move devices across managed accounts.</p>
Notifications	<p>Alarms and Events management.</p> <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator - All ● Monitor - View ● CPI - None
Onboarding	<p>Device approval, modifying individual device configuration, and performing software update.</p> <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator - All ● Monitor - None ● CPI - All
Reporting	<p>Report generation.</p> <ul style="list-style-type: none"> ● Super Administrator - All ● Administrator - All ● Operator - All

Table 54: Role-Mappings

Feature	Description
	<ul style="list-style-type: none">● Monitor - All● CPI - All
Session Management	Capability to view and logout other users sessions. <ul style="list-style-type: none">● Super Administrator - All● Administrator - All● Operator - None● Monitor - None● CPI - None
Software Images	Upload and delete device software images. <ul style="list-style-type: none">● Super Administrator - All● Administrator - All● Operator - None● Monitor - None● CPI - None
Software Upgrade	Upgrade the device with the latest software. <ul style="list-style-type: none">● Super Administrator - All● Administrator - All● Operator - All● Monitor - None● CPI - None

Table 54: Role-Mappings

Feature	Description
SNMP Configuration	SNMPv2c configuration parameters. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All• Operator -View• Monitor - None• CPI - None
System Operations	System operations such as Reboot VM, change log level, system upgrade, system monitoring, uploading SSL certificate, import/export server data and server tech dump, and upload/delete device software images. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All• Operator - None• Monitor - None• CPI - None
User Management	User management operations such as manage users and roles. <ul style="list-style-type: none">• Super Administrator - All• Administrator - View• Operator - None• Monitor - None• CPI - None

Creating Users and Configuring User Roles

To add a user:

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

3. Enter the **Username**.
4. Enter the **Full Name**.
5. Enter the **Password**.
6. Confirm the Password by entering the same password.

To configure User Roles:

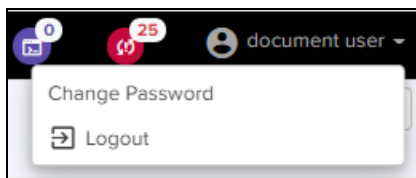
7. Select any one of the role for the user from the Role drop-down:
 - Super Administrator
 - Administrator
 - Operator
 - Monitor
 - CPI
8. Choose the **State** as Enabled or Disabled.
9. Click **Save**.

To edit or delete a user, click the Edit icon or the Delete icon against the user in the **Administration > Users** page.

Changing Password

Change Password option is available only for local users.

Figure 157 Changing Password



Ensure the primary Authentication must be local users to **Change Password** option. After changing the password, the current session will get logged out.

Also, ensure that there are no parallel sessions with the same users before going for **Change Password** option.

To change password:

1. Click the drop-down icon next to the username in the top right corner of the UI.
2. Enter the following details:
 - a. The Current Password.
 - b. A new password for this user.
 - c. Confirm the Password by entering the same password.
3. Click **Save**.

Figure 158 Changing Password Parameters

Authentication Servers

cnMaestro supports authentication and authorization with TACACS+, RADIUS, LDAP, and Active Directory servers, and is a cnMaestro X feature.

Authentication Server

Authentication Servers can be configured by cnMaestro Super Administrators. The following operations are available:

- [List All Authentication Servers](#)
- [Create New Authentication Server Configuration](#)
- [Secondary Server Authentication](#)
- [Edit an Existing Authentication Server Configuration](#)
- [Delete an Existing Authentication Server Configuration](#)
- [Verify the Role of the User](#)
- [Show User Groups for Active Directory](#)

List All Authentication Servers

To view all the Authentication servers which are configured in cnMaestro, navigate to **Administration > Users > Authentication Servers**.

Figure 159 List of Authentication Servers

Name	Type	Host	Port
test_TACACS+	TACACS+	10.10.209.61	49
test_RADIUS_ip	RADIUS	10.10.209.61	1812

Create New Authentication Server Configuration

1. Navigate to **Administration > Users > Authentication Servers**.
2. Click **Add New Authentication Server**.

Figure 160 Authentication Server

TACACS+


The fields that are present when TACACS+ server is selected are listed below:

Table 55: TACACS+ Parameters

Parameter	Description
Server Settings	
Authentication Server Name	Global name of the server
IP Address/Host name	Enter the FQDN (Fully Qualified Domain Name) of the server or the IP address of the server.
Port	TCP port of the server. (Default value is 49)

Table 55: TACACS+ Parameters

Parameter	Description
Shared Secret	Shared secret key for communicating with the server.
Service Name	Name defined in the service configuration table configured by TACACS+ server administrator. This is used to configure service and corresponding user groups.
Role Mappings	TACACS+ user groups should be mapped to one or more cnMaestro Roles. Refer Role-Based Access section to view the supported Roles on cnMaestro. Enter the role strings that are configured in the TACACS+ server. Atleast one mapping must be completed for this feature to work correctly.



NOTE:
TACACS+ server administrator should setup the service name and corresponding user group as per the configuration.

RADIUS

The fields present when RADIUS is selected are listed below:

[Administration](#) > Add Authentication Server x

Server Settings

Authentication Server Name

Authentication Server Type

IP Address/Hostname*

Port

Shared Secret

Role Mappings

Map Radius Groups to cnMaestro Roles. Atleast one mapping must be completed in order for this feature to work correctly.

Super Administrator

Administrator

Operator

Monitor

CPI

Table 56: RADIUS Parameters

Parameter	Description
Server Settings	
Authentication Server Name	Global name of the server.
IP Address/Hostname	Enter the FQDN (Fully Qualified Domain Name) of the server or the IP address of the server.
Port	UDP port of the server (Default is 1812).
Shared Secret	Shared secret key for communicating with the server.
Role Mappings	Radius user groups should be mapped to one or more cnMaestro Roles. Refer the Role-Based Access section to view cnMaestro supported Roles. Enter the role strings that are configured in the Active Directory server. At least one mapping must be completed for this feature to work correctly.

**NOTE:**

The RADIUS administrator should setup user group as per configuration. The RADIUS administrator can choose a user group and the same should be configured on cnMaestro Authentication server configuration.

Active Directory

The fields present when Active Directory is selected are listed below:

Administration > Add Authentication Server x

Server Settings

Authentication Server Name

Authentication Server Type

IP Address/Hostname*

Port

Base DN*

SSL/TLS Security

Certificate

Role Mappings

Map Active Directory Groups to cnMaestro Roles. Atleast one mapping must be completed in order for this feature to work correctly.

Super Administrator

Administrator

Operator

Monitor

CPI

Table 57: Active Directory Parameters

Parameter	Description
Server Settings	
Authentication Server Name	Global name of the server.
BASE DN	Distinguished Name for Active Directory.
IP Address	IP address of the server.
Port	TCP port of the server. (default 389). When SSL/TLS option is enabled, the port will automatically change to 636.
SSL/TLS	Select this check box if Active Directory connection should be secured over SSL/TLS as LDAPS. Browse and select the Root certificate of the Active Directory server in .PEM format.
Role Mappings	Active Directory user groups should be mapped to one or more cnMaestro Roles. Refer the Role-Based Access section to view cnMaestro supported Roles. Enter the role strings that are configured in the Active Directory server. Atleast one mapping must be completed in order for this feature to work correctly.



NOTE:

The Active Directory administrator should setup user group as per configuration. The Active Directory administrator can choose a user group and the same should be configured on cnMaestro Authentication server configuration.

Examples:

CN=super-admin

CN=admin

CN=network

CN=operator



NOTE:

If Role is not configured in TACACS+/RADIUS server or group is not configured in Active Directory, you cannot login to cnMaestro.



NOTE:

A user with valid credentials will not be able to login if:

1. cnMaestro role to Authentication server's user group mapping is missing in Authentication server configuration
2. User group of the user is not configured in Authentication server and is a required field for cnMaestro login.

LDAP

The fields present when LDAP is selected are listed below:

Administration > Add Authentication Server x

Server Settings

Authentication Server Name

Authentication Server Type

IP Address/Hostname*

Port

Suffix*

Base DN*

LDAP Password*

SSL/TLS Security

Certificate

Role Mappings

Map LDAP Groups to cnMaestro Roles. Atleast one mapping must be completed in order for this feature to work correctly.

Super Administrator

Administrator

Operator

Monitor

CPI

Table 58: LDAP Parameters

Parameter	Description
Server Settings	
Authentication Server Name	Global name of the server.
Base DN	Base DN is generally the Admin DN used to log in to LDAP server. For example: cn=admin,dc=xyz,dc=com.
Certificate	Browse and update with root certificate in .PEM format.
IP Address/Hostname	Provide IP address for LDAP and hostname of server if SSL/TLS is enabled.
LDAP Password	LDAP Password is the admin password used by Admin DN to log in.
Port	TCP port of the server. (Default for LDAP is 389 and for LDAPs is 636)

Table 58: LDAP Parameters

Parameter	Description
Suffix	Suffix is the DNS name. For example: dc= xyz, dc=com.
SSL/TSL Security	<p>Select this check box LDAP connection should be secured over SSL/ TLS as LDAPS. Browse and select the Root certificate of the Active Directory server in .PEM format.</p> <p>Note:</p> <ul style="list-style-type: none"> ■ If you enable SSL/TSL Security check box, the default port will appear as 636 in the Port text box. ■ If you disable SSL/TSL Security check box, the default port will appear as 389 in the Port text box.
Role Mappings	<p>RADIUS user groups should be mapped to one or more cnMaestro Roles. Refer the Role-Based Access section to view cnMaestro supported Roles.</p> <p>Enter the role strings that are configured in the Active Directory server. At least one mapping must be completed for this feature to work correctly.</p>

Secondary Server Authentication

In addition to the primary server authentication, cnMaestro On-Premises now supports configuration for secondary external server for authentication. Secondary authentication and primary authentication servers should be different.



NOTE:

Same authentication will not be shown on the server. For example, If we select primary as Test-TAC-IP, then we cannot select the same in secondary authentication.

Tertiary authentication is always default to the local users. Local users logs in only when primary and secondary are not reachable or when the services are not being run on authentication server. If the primary server is not reachable then fallback happens to the secondary authentication server. If the secondary authentication server is not reachable then fallback happens to tertiary authentication. If primary authentication server is running properly then users belonging to primary authentication server can only be logged in. If secondary authentication server is running properly then users belonging to secondary authentication server can only be logged in.

Figure 161 Secondary Server Authentication

Administration > Users

Local Users **Authentication** Authentication Servers X Session Management X

Please select how users should authenticate to cnMaestro. [Learn more](#)

Primary Authentication*

Test-TAC-IP Add Authentication Server


Secondary Authentication

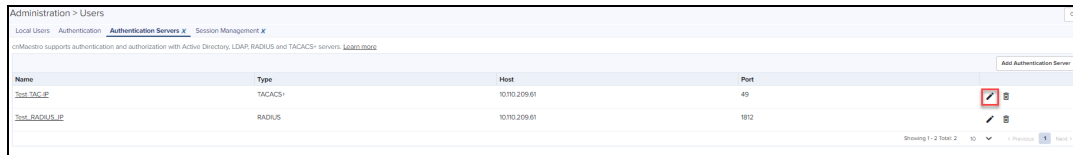
Local Users

Submit

Edit an Existing Authentication Server Configuration

To edit an existing Authentication Server configuration:

1. Navigate to **List all Authentication Servers** page.
2. Click the name of the server or **Edit** icon().



Refer [Create New Authentication Server Configuration](#) section for explanation of fields on **Edit** page.

Delete an Existing Authentication Server Configuration


To delete an existing Authentication Server configuration:

1. Navigate to **List all Authentication Servers**.
2. Click **delete**.

Primary authentication order will change as Local Authentication if this server is setup as Primary Authentication under **Manage Authentication Server Authentication** section.

Verify the Role of the User

- To know and verify the role of the **Active Directory** user:

1. Navigate to **List all Authentication Servers** page.
2. Click the **test** icon () next to any of the Active Directory type. The following window appears:

Test Accounts (Test-AD-SSL)

Active Directory User ID*

Active Directory password*

Account to Verify*


Test Cancel

3. Provide the following details:

- Active Directory User ID
- Active Directory Password
- Account to Verify

4. Click **Test**.

- To know and verify the role of the **LDAP** user:

1. Navigate to **List all Authentication Servers** page.
2. Click the **test** icon () next to any of the LDAP type. The following window appears:

5. Enter the name of the **Account to Verify**.
6. Click **Test**.

Show User Groups for Active Directory

cnMaestro administrator can view user groups for Active Directory server type configuration by providing valid user credentials to login to Active Directory. The user details can then be viewed as shown below:

1. Enter **Active Directory User ID**. The User ID should be a valid string (Eg: user@example.com).
2. Enter **Active Directory password**.
3. Enter **Account to Verify**.

For searching the group of the user, the Users ID should follow the user@example.com format.

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 log out Operator and Monitor accounts.

Sessions

Displays the detailed information on the user sessions.

Figure 162 Session Management > Sessions

Username	Managed Account	Role	Client IP	Start Time	Duration	Idle Time	Logout
Administrator	Base Infrastructure	Super Administrator	172.25.10.129	Thu Jan 21 2021 11:23:20 UTC -0530	18d 1h 28m	0d 0h 0m	[Logout]
Super user	Base Infrastructure	Super Administrator	172.25.10.959	Thu Jan 21 2021 13:33:49 UTC -0530	18d 0h 17m	0d 0h 0m	[Logout]
Administrator	Base Infrastructure	Super Administrator	172.25.10.33	Tue Feb 02 2021 16:54:41 UTC -0530	6d 5h 56m	0d 0h 0m	[Logout]
Administrator	Base Infrastructure	Super Administrator	172.25.10.221	Mon Jan 25 2021 12:03:10 UTC -0530	14d 10h 48m	0d 0h 0m	[Logout]
Administrator	Base Infrastructure	Super Administrator	10.10.32.74	Wed Jan 27 2021 13:38:29 UTC -0530	12d 12h 43m	0d 0h 0m	[Logout]
Administrator	Base Infrastructure	Super Administrator	172.25.10.87	Wed Jan 27 2021 13:38:29 UTC -0530	12d 0h 13m	0d 0h 0m	[Logout]
Administrator	Base Infrastructure	Super Administrator	172.25.10.107	Wed Jan 27 2021 17:36:25 UTC -0530	12d 5h 15m	0d 0h 0m	[Logout]
Administrator	Base Infrastructure	Super Administrator	172.25.10.87	Wed Jan 27 2021 18:14:08 UTC -0530	12d 4h 37m	0d 0h 0m	[Logout]
Administrator	Base Infrastructure	Super Administrator	10.10.92.176	Wed Jan 27 2021 21:18:30 UTC -0530	12d 1h 33m	0d 0h 0m	[Logout]
Administrator	Base Infrastructure	Super Administrator	172.25.10.77	Thu Jan 28 2021 17:19:29 UTC -0530	11d 5h 32m	0d 0h 0m	[Logout]

Server Management

This chapter provides the following details:

- Monitoring
- Settings
- Operations
- SSL Certificate
- Syslog

Monitoring

The Server tab provides monitoring and operations for the virtual machine instance.

Navigate to **Administration > Server**.

Figure 163 Monitoring cnMaestro Server Instance



Settings

This section provides the following details:

- Basic
- Configure NTP Server
- Configure Email Server
- Login Security Banner

Basic

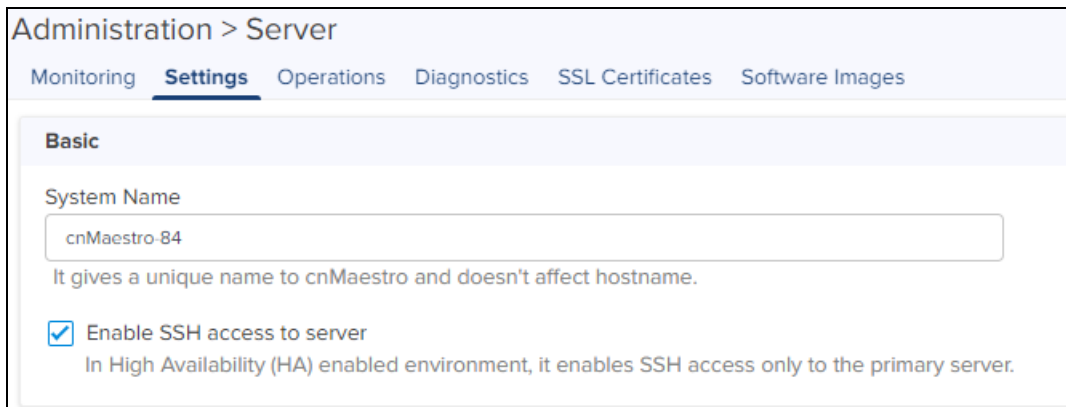
The user can enter the **System Name** and enable the **SSH access to cnMaestro server**.



NOTE:

In High Availability (HA) enabled environment, it enables SSH access only to the primary server.

Figure 164 System Name

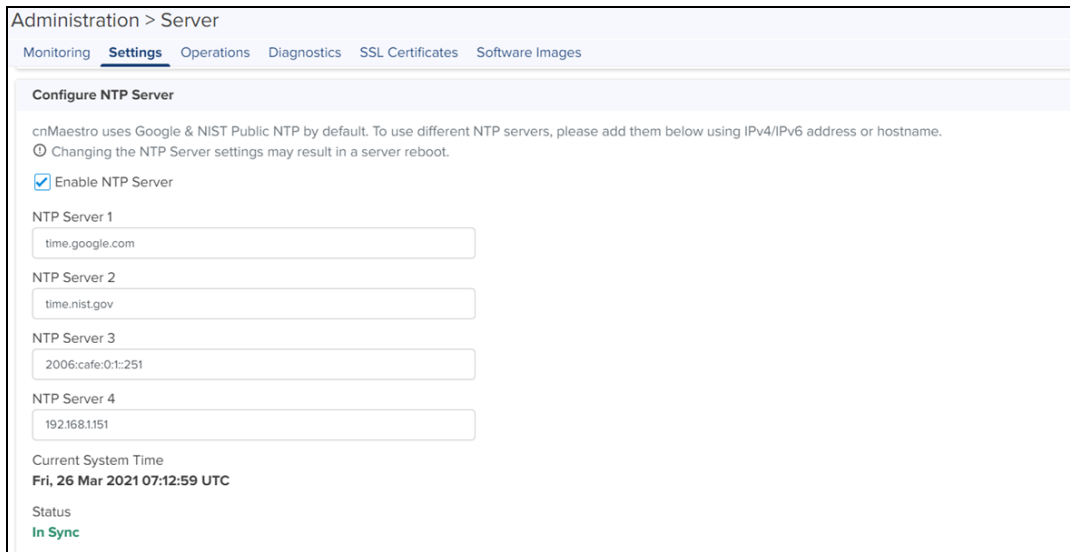


Configure NTP Server

The user can configure the NTP Server to configure the time configuration of the server with hostname or IP address.

To configure the NTP server:

1. Navigate to **Administration > Server > Settings > Configure NTP Server** tab.
2. Enable the **NTP Server**.
3. Enter **Host Name** or **IP Address**. It displays **Current System Time** and **Status** of the server.



Configure Email Server

The user can configure the email server to send and receive email messages.

To configure the email server:

1. Navigate to **Administration > Server > Settings > Configure Email Server** tab.

Figure 165 Email Server

Configure Email Server
Configure SMTP server to manage cnMaestro users pertaining to MSP and to send email notifications.

Enable SMTP Server

Port*
587

Host*
smtp.gmail.com

Username
conrad@conrad.com

Password

Sender Email*
conrad@conrad.com

Encryption
 None TLS STARTTLS

Ignore server certificate validation

Send Test Mail

Login Security Banner
Configure security banner to be displayed on login screens.

Enable Security Banner during Login

Enable User must accept security banner before login

Security Banner Notice
This is a PRIVATE CONFIDENTIAL device. In the absence of use only for authorized use only. Unauthorized or improper use of this system may result in administrative disciplinary action against user and company penalties.

Banner content (max 1024 characters)

Save Discard

Copyright © 2015- 2021 Cambium Networks, Inc. All rights reserved. | [Version 200-04871](#) | [Contact Us](#) | [Support](#) | [998](#) | [License](#)

2. Select the **Enable SMTP Server** check box.
3. Enter the **Port** number.
4. Enter name of the **Host**.
5. Enter the **Username**.
6. Enter the **Password**.
7. Enter the **Sender Email**.
8. To send the email in an encrypted format, select any one of the following:
 - **None:** Uses port number 587 for communication which is not secured.
 - **TLS:** Uses port number 465 for encrypted communication. When this option is selected, upload CA certificate.
 - **STARTTLS:** For encrypted communication on port number 587, choose STARTTLS option. When this option is selected, upload CA certificate.
9. Select the **Ignore Server Certificate Validation** checkbox.
10. Click **Send Test Email**.

Figure 166 Specifying email address

Send Test Mail

Recipient Email*

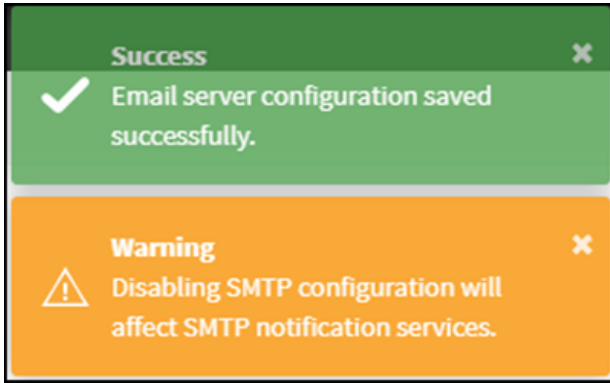
Send Now Cancel

11. Enter the **Recipient Email**.
12. Click **Send Now**.




NOTE:

When user tries to disable SMTP configuration a warning message pops-up.



Email Notifications

The Email Notifications feature allows the Super Administrator and the Administrator users to add subscribers (Email IDs) for receiving different types of alerts by means of Emails.

	<p>NOTE: Email Subscribers are limited to two per account.</p>
---	---

The severity of alerts are classified as follows:

- Critical
- Major
- Minor

The content of the email alert is in JSON or HTML format. The subscriber gets an email alert only when the global setting is enabled.

To receive email notifications, the user need to enable **Notification** checkbox. If SMTP settings are disabled, then below notification message does not pop-up.

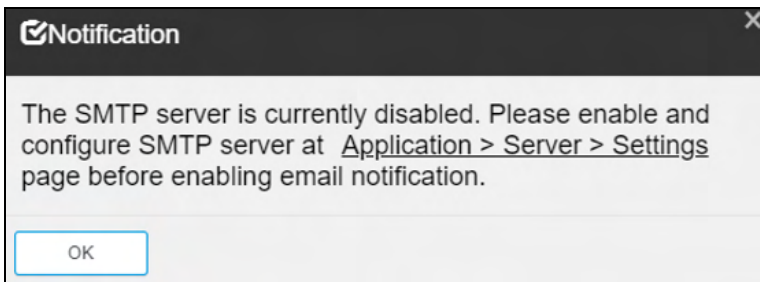
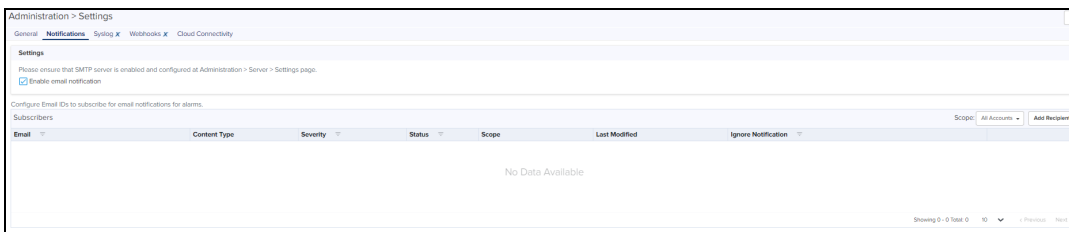


Figure 167 Email notifications



You can use the filter option for the following fields:

- Email
- Severity

- Status
- Ignore Notification

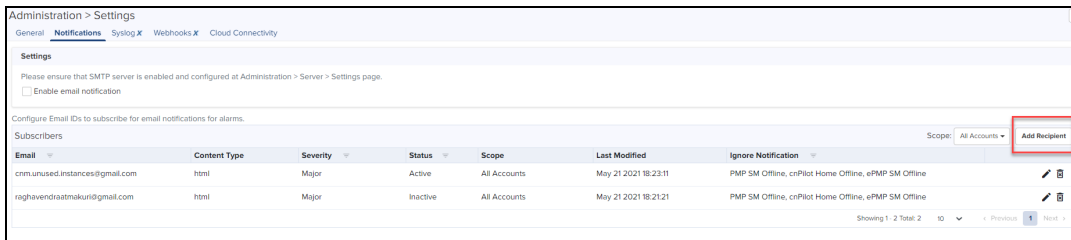
You can use the sorting option for the following fields:

- Content Type
- Last Modified Date

Adding Recipient to Subscriber Table

1. Navigate to **Administration > Settings > Notifications** and click **Add Recipient**.

Figure 168 Adding Subscribers



The following window is displayed:

The 'Add Email Subscriber' dialog box contains the following fields and options:

- Active
- Severity: Major (dropdown menu)
- Email: Enter Email ID (text input)
- Content Type: HTML, JSON
- Managed Account: All Accounts (dropdown menu)
- Ignore Notification: cnPilot Home Offline, ePMP SM Offline, PMP SM Offline
- Buttons: Add, Cancel



NOTE:


Managed Account option will appear only if MSP feature is enabled.

2. Select the **Severity** level.
3. Enter **Email**.
4. Select the **Content Type** as **HTML** or **JSON**.
5. Select the **Managed Account** list.
6. Select the appropriate option (s) for **Ignore Notification**.
7. Click **Add**.

All alarms of chosen severity and above are sent through email as explained below:

- If severity **Critical** is selected, then we receive only critical alarms.
- If severity **Major** is selected, then we receive critical and major alarms.
- If severity **Minor** is selected, then we receive critical, major, and minor alarms.


HTML Email Example


CLEAR

1

Notification Details

Type Time	Account Tower/Site	Name Type IP Address	Message
CLEAR <small>14:10 (UTC +05:30)</small>	Base Infrastructure	cnPilot R201P12345678 <small>cnPilot r201P 10.110.224.74</small>	Device is offline.



MAJOR

1

Notification Details

Type Time	Account Tower/Site	Name Type IP Address	Message
MAJOR <small>14:02 (UTC +05:30)</small>	Base Infrastructure	cnPilot R201P12345678 <small>cnPilot r201P 10.110.224.74</small>	Device is offline.

JSON Email Example


cnMaestro Notifications <[redacted]@gmail.com> | [External] cnMaestro Notification

```

{
  "acknowledged_by": "",
  "code": "STATUS",
  "duration": 360122,
  "id": "5bec030f3f8f840c1a079ffe",
  "mac": "[redacted]",
  "message": "Device is offline",
  "managed_account": "Base Infrastructure",
  "name": "Status",
  "ip": "10.110.208.30",
  "network": "default",
  "severity": "major",
  "site": "sid",
  "source": "PMP 450m AP",
  "source_type": "pmp",
  "status": "active",
  "time_raised": 1542193635297,
  "tower": "",
  "isSite": null,
  "mode": "ap"
}

```

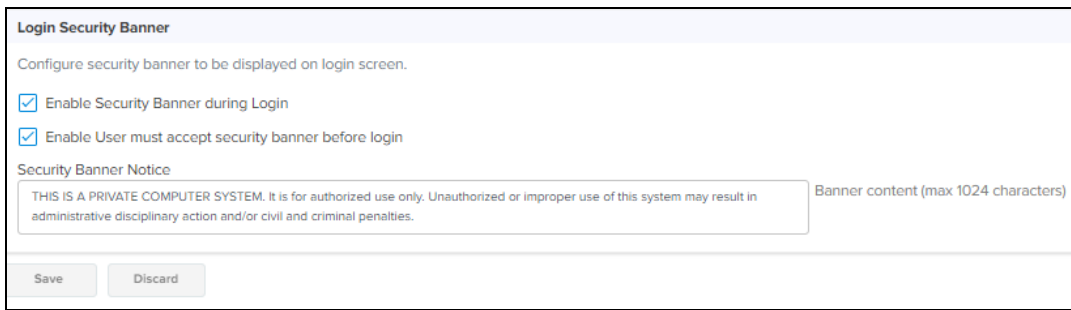
Login Security Banner

For security purpose, a banner will be displayed before the login window appears in cnMaestro On-Premises. If the user needs to be aware of any critical information, it is displayed within the security banner.

To enable :

1. Navigate to **Administration > Server > Settings > Security Banner**.

Figure 169 Enabling Security Banner

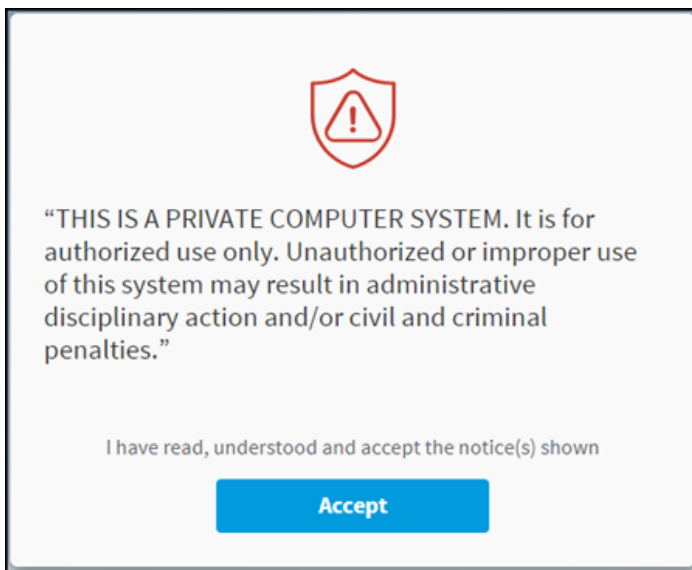


The screenshot shows a configuration window titled "Login Security Banner". Below the title, it says "Configure security banner to be displayed on login screen." There are two checked checkboxes: "Enable Security Banner during Login" and "Enable User must accept security banner before login". Below these is a text area labeled "Security Banner Notice" containing the text: "THIS IS A PRIVATE COMPUTER SYSTEM. It is for authorized use only. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties." To the right of the text area is a label "Banner content (max 1024 characters)". At the bottom of the window are two buttons: "Save" and "Discard".

2. Enable the following options:
 - Enable Security Banner during Login
 - User must accept security banner before Login (If enabled, the user should accept the banner before login else the user can directly login, with the banner that is displayed.)
3. Enter the **Security Banner Notice**.
4. Click **Save**.

A sample security banner window is shown below:

Figure 170 Security Banner



Click **Accept**. The login window is displayed.

Operations

This section provides the following details:

- [Reboot Virtual Machine](#)
- [Update cnMaestro Software](#)
- [System Backup](#)
- [In-System Upgrade](#)

Reboot Virtual Machine



Warning:

All devices goes offline when the virtual devices is rebooted.

Update cnMaestro Software

Package Types

cnMaestro On-Premises software is released in two forms:

OVA Image

The OVA image contains all software needed to run the cnMaestro application. It is installed on a virtual machine and releases intermittently to update system software. Moving to a new OVA image requires an in-system upgrade of the current OVA (no import and export of data is required after the 2.0 release). The OVA is approximately 3.0 GB in size.

Package Upgrade

The package file is installed on top of an OVA image; and updates the cnMaestro application. Packages releases more frequently and provide a faster upgrade path for enhancements. Packages can be installed by downloading them from Cambium and uploading them through the UI (at **Administration > Server > Operations**).



NOTE:

1. The general update flow will be an OVA file followed by package releases. For significant system-level updates, a new OVA file will be generated.
2. Refer to [Cloud connectivity](#) page for download of software from cnMaestro Cloud.

System Backup

Cambium recommends customers periodically backup their system as a precautionary measure. To Backup navigate to **Server > Operations > System Backup and Restore**. Backups can be done manually, in real-time, or scheduled to execute daily or weekly. cnMaestro can also automatically transfer backup files off-box using FTP or SFTP (this support is configured under **Settings > Optional Features > Scheduled Jobs**).

A System Backup stores the entire state of cnMaestro On-Premises as a file. This file can be downloaded to the local hard drive through the UI and imported into a new cnMaestro instance to recreate the application state. Only one System Backup is available at any time, and a later entry overwrites an earlier one.

Generate Backup



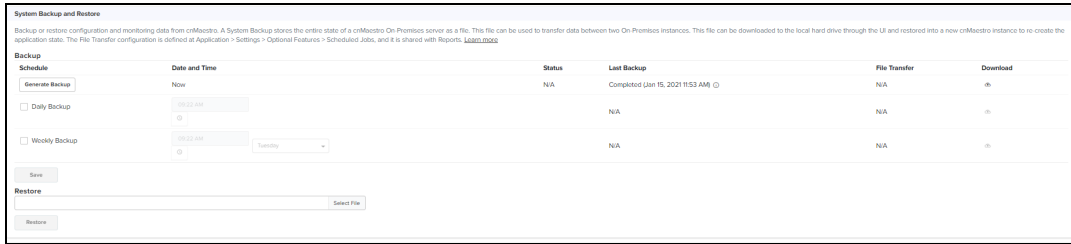
NOTE:

From 3.0.0 release, backup generated by On-Premises instance will have configuration data and historical monitoring data only for current month excluding client's data. It is suggested to take backup at the last day of the month if needed. Please refer to [Data Backup](#) for more information.

The user can create a system backup through a system backup job at **Administration > Server > System Backup and Restore**. The created backup file can be downloaded to the user's local machine for archiving.

To generate the system backup job:

1. Navigate to **Administration > Server > Operations > System Backup and Restore**.




2. Select any one of the following:

- **Daily Backup:** You can set time exceeding the current system time. The backup files will be generated every data at the scheduled time.
- **Weekly Backup:** The backup files will be generated for a specified day and time on a weekly basis .

You can download the last backup file using the download icon in the table. The file transfer configuration is defined at **Administration > Settings > Optional Features > Scheduled Jobs** and it is shared with Reports. If FTP is enabled, then a copy of each backup file will be stored in the configured FTP/SFTP server. The FTP column table displays the status of the upload to the FTP/SFTP server.

3. Click **Generate Backup** button.



NOTE:

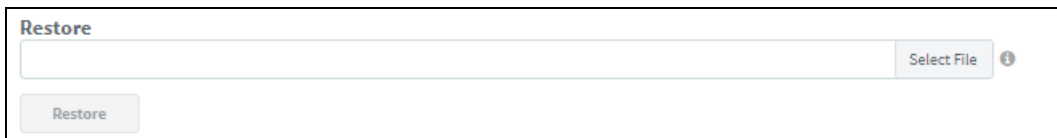
Only the latest backup is retained in the disk and available to download. The old backup is deleted once the new backup is generated.

To view the system backup job:

Click **View System Backup Jobs** link in **Operations > System Backup and Restore** or navigate to **Administration > Jobs > System Backups**.

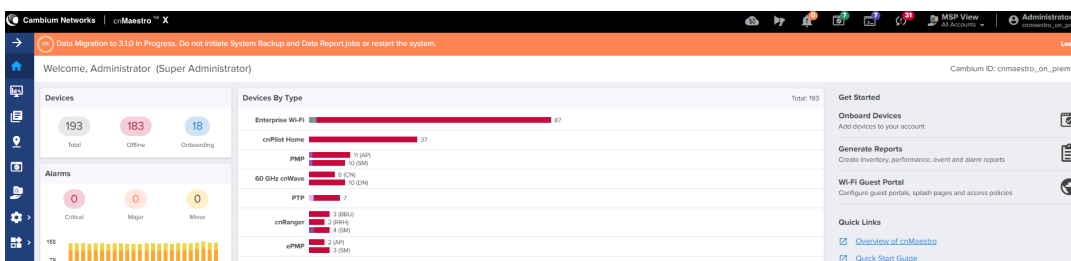
Restore Backup

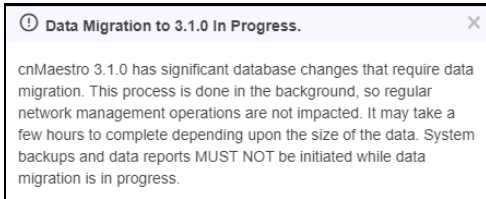
The user can now restore the downloaded system backup file to the new cnMaestro instance to recreate the application state under **Manage > Server > Operations > System Backup and Restore**.



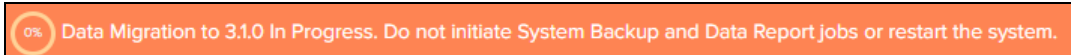
To restore backup files, select the file from **Restore From Backup** option and click **Restore**.

Data migration to 3.1.0 from lower version takes some amount of time depending upon the size of backup file. During migration, the below banner is displayed:





In 3.1.0 release, when we import the backup data, the following banner displays in the top of cnMaestro On-Premises UI and it will be there until the indexing is completed.



	<p>NOTE:</p> <ul style="list-style-type: none">• The indexing will happen whenever the user navigates to different UI pages. For example, when the user navigates to WLAN-AP group page, the respective indexing will be created and the banner will be displayed in the top of the UI.• Database indexing pauses during the database migration and emails once indexing the webhooks.• Do not Import data or Export data when the Migration banner is running.
--	--

OVA Update Process

Updating an OVA image can be managed through the following process (which assumes the hardware has enough hard disk space for two instances of cnMaestro).

1. Export the cnMaestro Server data from the old instance.
2. Stop the old instance.
3. Start the new instance (using the directions presented above).
4. Import the data into the new instance.
5. Set the IP address of the new instance to that of the old instance.

Clone Virtual Machine

Cambium also recommends backing up (or cloning) the virtual machine prior to updating cnMaestro software.

In-System Upgrade

In-System Upgrade is the ability to update the cnMaestro software without performing a system export followed by an import. Essentially all updates are performed within a single VM image. In-System Upgrade works in both Standalone and High Availability environments. The mechanism of the upgrade should be transparent to the user: they specify to upgrade the system on one instance, and the upgrade is propagated to both instances. The coordination happens automatically.

Software Update

The basic UI allows the user to upload a new OVA, and install it. This process is used for both standalone and HA installations. The Software Upgrade can be done through OVA or package.


Package Upgrade

1. Navigate to **Administration > Server > Operations > Software Update**.
2. Click **Package**.

- Browse and select the "cnmaestro-package_2.5.0.tar.gz file". You can upload the file from **Local** or **Download from cnMaestro Cloud**.
- Click **Apply Update** or **Download and Apply**.

Figure 171 Package Upgrade

OVA Upgrade

	<p>NOTE:</p> <p>Ensure to have minimum of 1 GB free RAM in the cnMaestro On-Premises server for the OVA to upgrade successfully.</p>
---	---

- Navigate to **Administration > Server > Operations > Software Update**.
- Click **OVA**.
- Browse and select the "cnmaestro-on-premises_3.0.0-b30_amd64.ova" file. You can upload the file from **Local** or **Download from cnMaestro Cloud**.

- Click **Upload OVA**, or **Download OVA**. After upload it will progress with Staging.

OVA Upgrade Using CLI

- Copy the OVA file into the location "/srv/storage/tmp"
- Execute the command `sudo /srv/bin/sudo cnmaestro-image stage /srv/storage/tmp/<OVA file name>`
- Staging Status can be verified in UI under **Server > Operation > OVA**.

In the CLI, it can be verified by executing the command `sudo /srv/bin/cnmaestro-image status`

If you are unable to apply the upgrade OVA using the UI, there is a command line mechanism that can be used as a failsafe. See **Appendix > Maintenance > Command Line Alternatives > Apply OVA Upgrade** for more details.

Diagnostics

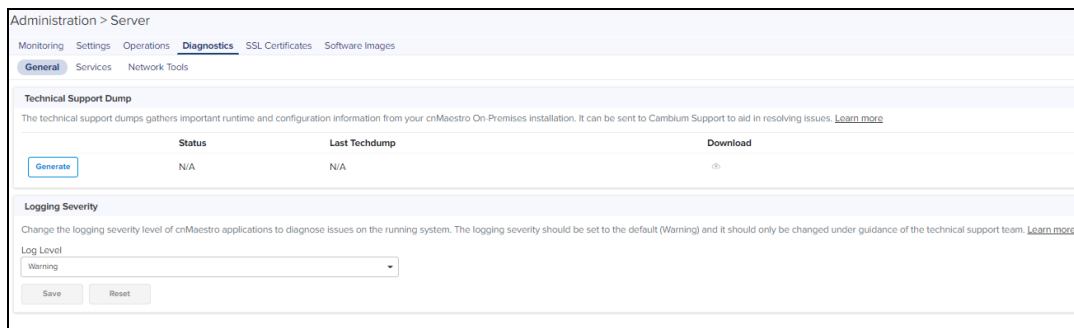
This section provides the following details:

- [Server Technical Support Dump](#)
- [Logging Severity](#)
- [Services](#)

Server Technical Support Dump

The technical support dump gathers important runtime information on the cnMaestro instance. It is accessed at **Administration > Server > Diagnostics** and can be used by Cambium Networks Support to aid in resolving issues.

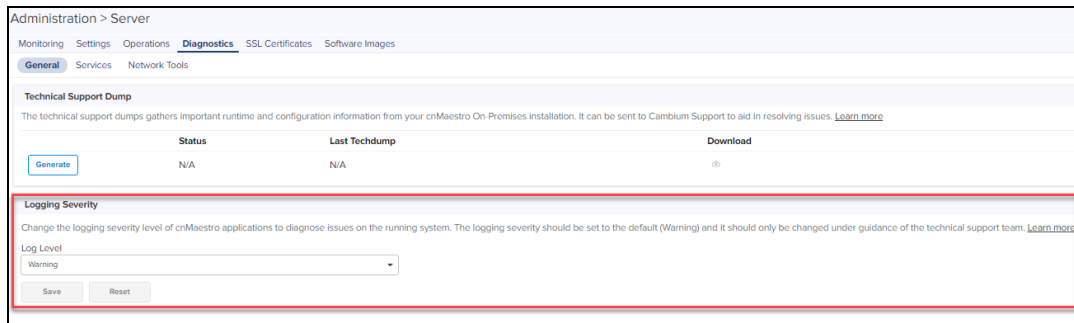
Figure 172 Technical Support Dump



Logging Severity

Change the severity level of the messages logged by the cnMaestro system. These messages are not accessible directly, but can be downloaded as part of the Technical Support Dump. The Log Level Severity can be changed at runtime and it does not require reboot of server to take effect.

Figure 173 Logging Level



Services

Real time display of the status of critical cnMaestro services.

Figure 174 Services

Name	Status	Uptime	CPU	Memory
cnmaestro-health	Running	6d 14h 32m	0.2%	1.2% (48.47MB)
cnmaestro-smp	Running	6d 14h 31m	0.0%	1.1% (43.20MB)
mongod	Running	6d 14h 33m	0.2%	4.4% (175.96MB)
nginx	Running	6d 14h 31m	0.0%	0.0% (1.46MB)
postgresql	Running	6d 14h 33m	0.0%	0.7% (26.29MB)
rabbitmq-server	Running	6d 14h 33m	0.1%	2.6% (103.26MB)
redis-server	Running	6d 14h 33m	0.0%	0.2% (6.99MB)
snmpd	Running	6d 14h 31m	0.0%	0.2% (9.87MB)
vsftpd	Running	6d 14h 32m	0.0%	0.0% (0.72MB)

Network Tools

The Network Tools page consolidates a number of operations that can be performed on cnMaestro On-Premises. The operations are listed below:

Table 59: Network Tools

Tools	Description
DNS Lookup	Lists the DNS records for a domain in priority order.
Ping	Network ping to a hostname or IP address.
Traceroute	Lists the hosts or IP addresses showing the route of the test packets starting from the selected monitoring location to the destination Domain or IP.

Figure 175 Network Tools

Administration > Server

Monitoring Settings Operations **Diagnostics** SSL Certificates Software Images

General Services **Network Tools**

Test Type: Ping

IP Address or Hostname:

Number of Packets (c): Min = 1, Max = 10

Buffer Size (s): Min = 1, Max = 65507

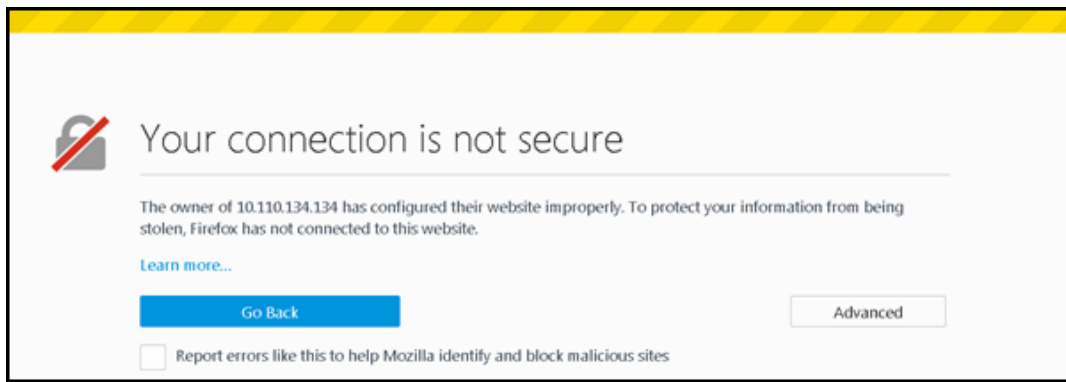
Start Ping

Result

SSL Certificate

cnMaestro On-Premises generates a self-signed certificate when it boots the first time. Because the root CA is not present in standard browsers, cnMaestro users (administrators or Captive Portal customers) receive an SSL error message as shown below:

Figure 176 SSL Error Message



Certificate Management

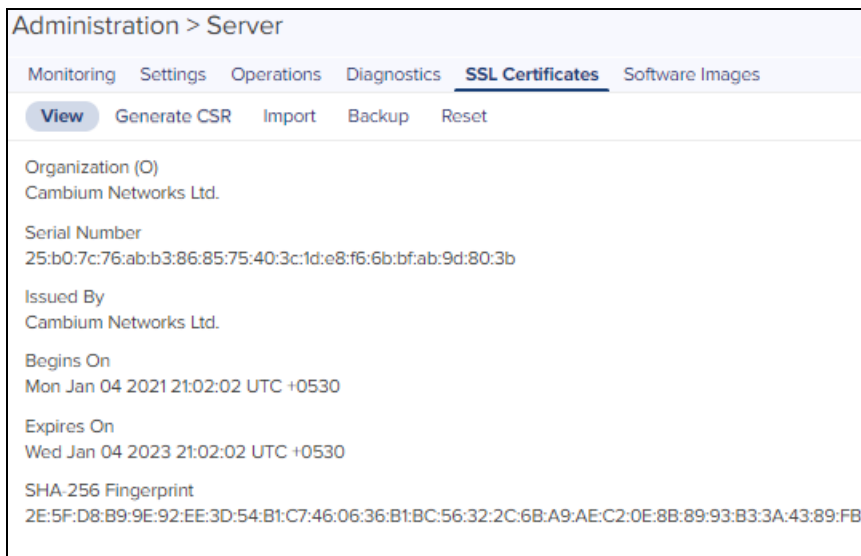
To fix the browser error, cnMaestro needs to host a certificate from a trusted certificate authority, and map the FQDN (fully qualified domain name) used to access cnMaestro. This requires the administrator to export a CSR (Certificate Signing Request) and import the signed Certificate back into cnMaestro.

The following options are available to manage the certificates:

- [View Certificate](#)
- [Generate a Certificate Signing Request \(CSR\)](#)
- [Import a Certificate](#)
- [Backup Management](#)
- [Reset](#)

View Certificate

To view the certificate details, click **View** tab.



Generate a Certificate Signing Request (CSR)

A certificate-signing request leverages the current Private Key and exports a CSR that can be forwarded to any Certificate Authority.

To generate a CSR:

1. Navigate to **Administration > Server > SSL Certificates**.

2. Select **Generate CSR** tab.

Administration > Server

Monitoring Settings Operations Diagnostics **SSL Certificates** Software Images

View **Generate CSR** Import Backup Reset

Generate a Certificate Signing Request (CSR) from the Private Key installed in cnMaestro. The CSR is used by a Certificate Authority to create a Signed Certificate mapped to a FQDN (fully qualified domain name). This allows browsers to trust the Guest Access Portal without a warning.

Country (C)

Common Name (CN)
 FQDN (fully qualified domain name) here.

Organization (O)

Organization Unit (OU)

City/Locality (L)

State/Province (ST)

Subject Alternative Name (SAN)

3. Specify the parameters as in the below table:

Table 60: Configuring CSR Parameters

Parameter	Description
Common Name	Enter FQDN name of the cnMaestro server. This is either the Domain Name or the IP Address.
Organization (O)	Enter the name of the organization.
Organization Unit (OU)	Enter the name of the organization unit.
City/Locality (L)	Enter the name of the city.
State/Province (ST)	Enter the name of the state.
Subject Alternative Name (SAN)	Enter DNS or IP Address.
Country (C)	Select the name of the country from the drop-down list.

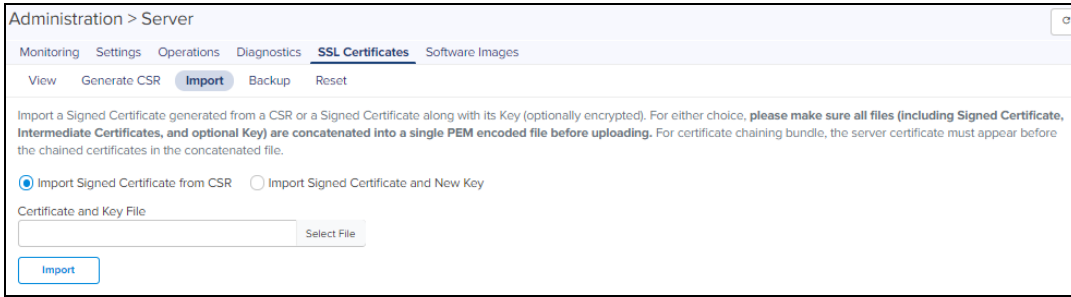
4. Click **Generate CSR**., the user is prompted to save a cnMaestro .csr file to their hard drive. The CSR can then be sent to a Certificate Authority and signed.

Import a Certificate



Once the CSR has been transferred to the Certificate Authority to create a certificate, it can be imported back into cnMaestro. cnMaestro will validate the certificate maps correctly to the stored Private Key, and disallow the import if incorrect. Alternatively, the user can append the Private Key to the Certificate file in PEM format and upload both if certificate and key is generated outside cnMaestro. User can also provide password optionally if key is generated with the password. This will replace both the Certificate and Key on cnMaestro.

To import a certificate:

1. Click **Import** tab.



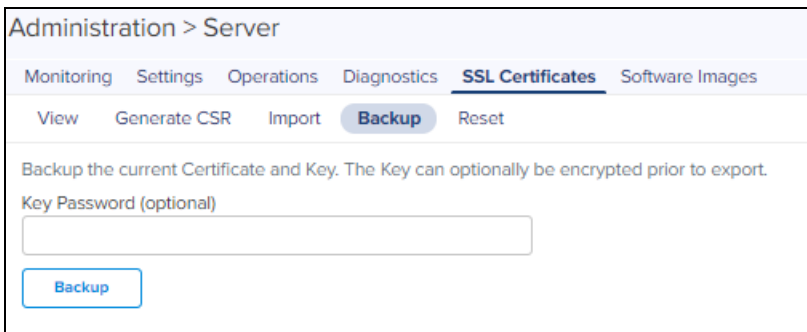
2. Select any one of the below options:
 - a. Import signed Certificate from CSR
 - b. Import signed Certificate and new Key
3. Browse and upload the Certificate and Key file.
4. Click **Import**.

	The Certificate, and any optional intermediate certificates should be appended and stored in a single PEM-encoded file prior to submission. The signed Certificate should be positioned at the top of the file, followed by any intermediate certificates.
	When importing a Certificate and Key, a single PEM-encoded file should be submitted with entries in the following order: Certificate, intermediate certificates, and Key. If the Key is encrypted, a password should be provided in the textbox on the UI at the time of import.

Backup Management

cnMaestro generates a 4096-bit Private Key when it boots up. This section allows the customer export this Key and current Certificate for backup. These will be exported as a single file, and the Key can optionally be encrypted with a password. To backup the certificate and the key:

1. Click **Backup** tab.



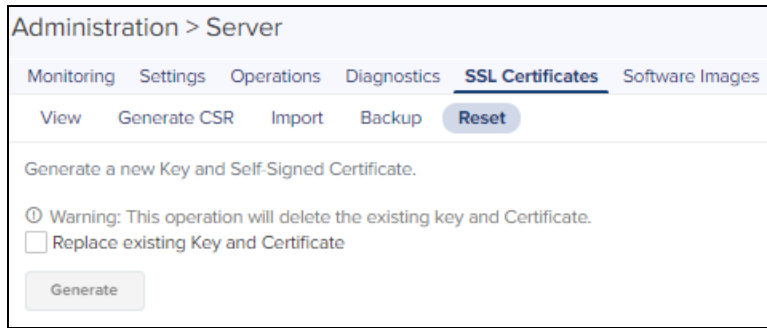
2. Enter the password for the key in the Key **Password** textbox.
3. Click **Backup**.

Reset

It replaces the current Private Key and Certificate and recreates them from scratch. The Certificate is self-signed, and it can be replaced using the Certificate import mechanism detailed above.

To generate a new private key:

1. Click **Reset** tab.



2. Select the **Replace the existing Key and Certificate** checkbox.
3. Click **Generate**.

Manage Software Images

This section provides the following details:

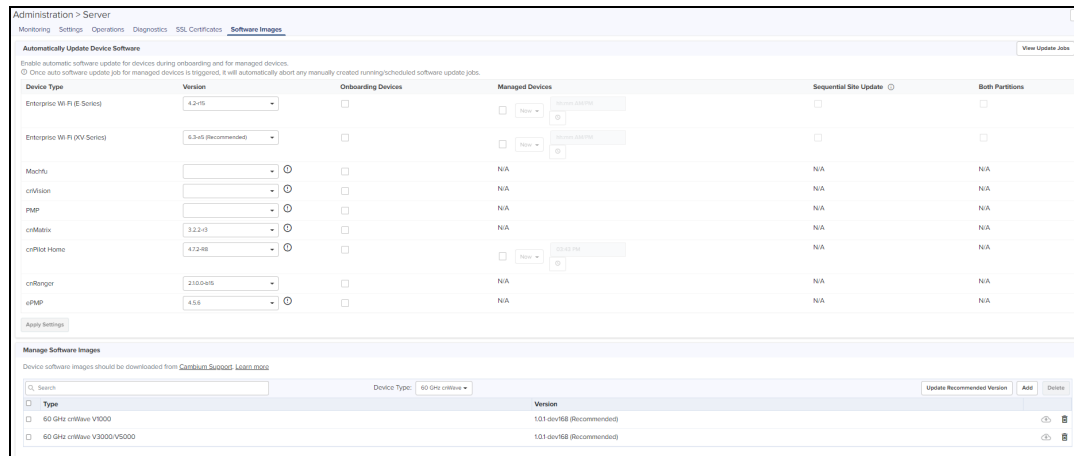
- [Overview](#)
- [Automatically Update Device Software](#)

Overview

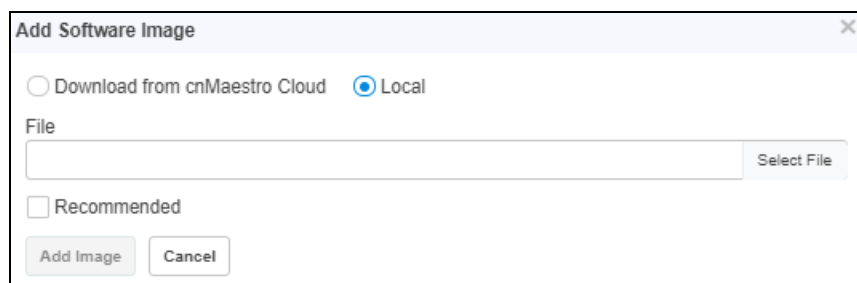
cnMaestro On-Premises allows one to add new device software images as they are released by the device teams. Adding new device software is a manual process: one needs to first download the images from the Cambium Support Center and then upload them into cnMaestro.

The steps are shown below for local upload:

1. Navigate to <https://support.cambiumnetworks.com/files> and download the device image to your laptop.
2. In the cnMaestro On-Premises UI, navigate to **Administration > Server > Software Images** tab.



3. Select the image file and then click **Add** button.
4. Add Software Image window pops-up



5. Once file is successfully uploaded to the server, it will appear in the grid.



NOTE

cnMaestro uses the name of the uploaded file to determine the version and device type. Please do not change the file name during the upload or download process.

All the check box will be disabled by default.

Add Images

Once the On-Premises server is synced with the cloud, the user can upload the software images from cloud directly to the On-Premises.

To upload Software Image perform as follows:

1. Navigate to **Administration > Server > Software Images**.

Device Type	Version	Onboarding Devices	Managed Devices	Sequential Site Update	Both Partitions
Enterprise Wi-Fi (E-Series)	4.2-16	<input type="checkbox"/>	<input type="checkbox"/> Download from Cloud	<input type="checkbox"/>	<input type="checkbox"/>
Enterprise Wi-Fi (CV-Series)	6.3-65 (Recommended)	<input type="checkbox"/>	<input type="checkbox"/> Download from Cloud	<input type="checkbox"/>	<input type="checkbox"/>
Micrifi	<input type="text"/>	<input type="checkbox"/>	N/A	N/A	N/A
cnWave	<input type="text"/>	<input type="checkbox"/>	N/A	N/A	N/A
PMP	<input type="text"/>	<input type="checkbox"/>	N/A	N/A	N/A
cnMatrix	3.2-43	<input type="checkbox"/>	N/A	N/A	N/A
crPilot Home	472-88	<input type="checkbox"/>	<input type="checkbox"/> Download from Cloud	N/A	N/A
crRanger	210-0-95	<input type="checkbox"/>	N/A	N/A	N/A
ePMP	4.5-8	<input type="checkbox"/>	N/A	N/A	N/A

Type	Version
<input type="checkbox"/> 60 GHz cnWave V1000	1.01 dev188 (Recommended)
<input type="checkbox"/> 60 GHz cnWave V3000/V5000	1.01 dev188 (Recommended)

2. Click **Add Image**.

3. **Add Software image** window appears.

- If the On-Premises account has onboarded to any anchor account in cloud.
 - a. Click **Download from cnMaestro Cloud**,
 - b. Select **Device Type**.

Add Software Image [X]

Download from cnMaestro Cloud
 Local

Device Type

60 GHz cnWave New

Available Images

Name	Version	Release Date
<input checked="" type="radio"/> 60 GHz cnWave V1000	1.0	N/A
<input type="radio"/> 60 GHz cnWave V3000/V5000	1.0	N/A
<input type="radio"/> 60 GHz cnWave V1000	1.0.1-dev122	N/A
<input type="radio"/> 60 GHz cnWave V3000/V5000	1.0.1-dev122	N/A
<input type="radio"/> 60 GHz cnWave V3000/V5000	1.0.1-dev124	N/A
<input type="radio"/> 60 GHz cnWave V1000	1.0.1-beta4	N/A
<input type="radio"/> 60 GHz cnWave V3000/V5000	1.0.1-beta4	N/A
<input type="radio"/> 60 GHz cnWave V1000	1.0.1-dev118	N/A

Recommended

- c. Select the Version and
- d. Click **Add Image**.
- If the On-Premises account is not onboarded to any anchor account in cloud.
 - a. Click **Local**.

Add Software Image [X]

Download from cnMaestro Cloud
 Local

File

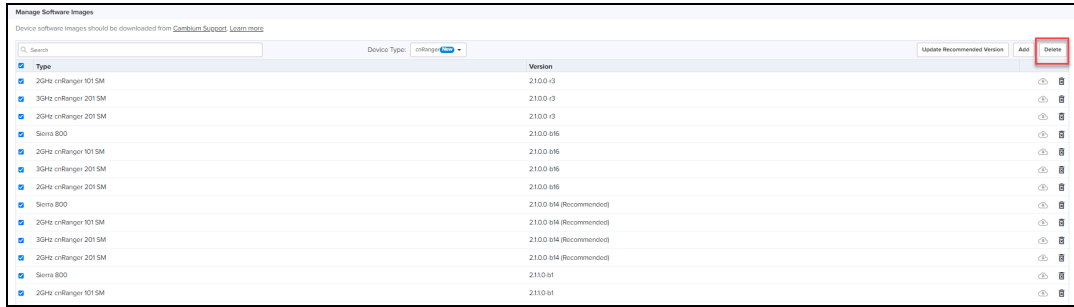
Recommended

- b. **Select File** from the local desktop.
- c. Click **Add Images**.

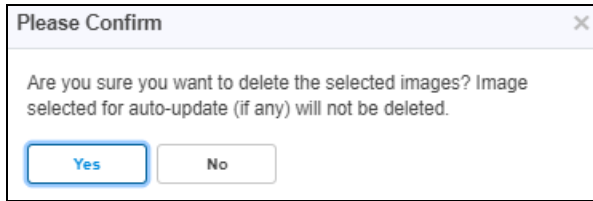
Delete Images

To delete Software Image perform as follows:

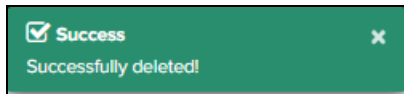
1. Navigate to **Administration > Server > Software Images**.



2. Select the images to be deleted and Click **Delete**.
3. Click **Yes** in Please confirm window to delete the images.



4. It will display the Success message as shown below:

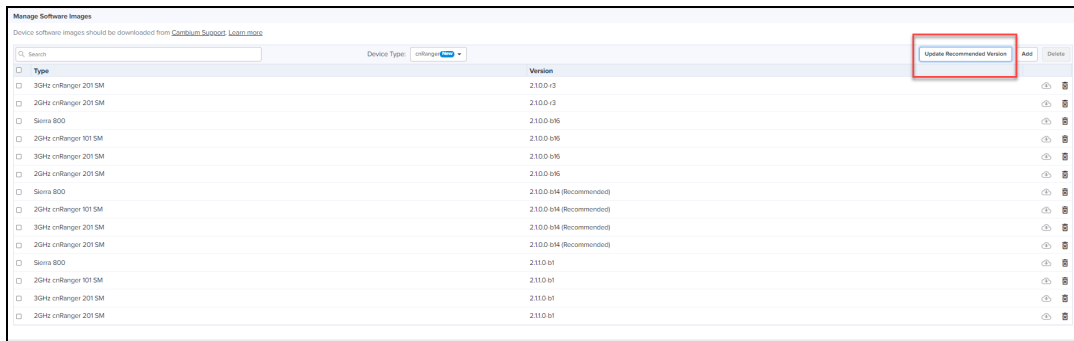


Update Recommended Version

Update recommended version allows the user to update the Version with the recommended version available from the drop-down.

To update recommended version perform as follows:

1. Navigate to **Administration > Server > Software Images**.



2. Click **Update Recommended Version** and window pops-up.



3. Select the **Version** from the drop-down and click **Save**.

Automatically Update Device Software

cnMaestro Cloud allows one to update the device software during onboarding and for managed devices.

Adding update device software is a manual process as follows:

1. Navigate to **Administration > Server > Software Images > Automatically Update Device Software** tab.
2. Select the version file and then click **onboarding/Managed Devices**.



NOTE:

Enable the onboarding check box, to avoid the failure of onboarding devices with minimum supported version rather than the recommended version.

3. Enable the checkbox as follows:

- Enable **Managed Devices** flag only for Wi-Fi devices (E series and R series).
- Enable **Sequential Site Update** and **Both Partitions** flag only for only E-Series and XV-Series devices.

4. Click **Apply Settings**.



NOTE:

- Once auto software update job for managed devices is triggered, it will automatically abort any manually created running/scheduled software update jobs.
- To avoid failures in onboarding devices having minimum supported version other than recommended version enable the onboarding checkbox.

Figure 177 Automatically Update Device Software

The screenshot displays the 'Automatically Update Device Software' configuration page. At the top, there are navigation tabs: Monitoring, Settings, Operations, Diagnostics, SSL, Certificates, and Software Images. The main heading is 'Automatically Update Device Software' with a 'View Update Jobs' button. Below the heading, there is a note: 'Enable automatic software updates for devices during onboarding and for managed devices. Once auto software update job for managed devices is triggered, it will automatically abort any manually created running/scheduled software update jobs.'

Device Type	Version	Onboarding Devices	Managed Devices	Sequential Site Update	Both Partitions
Enterprise Wi-Fi (E-Series)	4.2v11	<input type="checkbox"/>	<input type="checkbox"/> None	<input type="checkbox"/>	<input type="checkbox"/>
Enterprise Wi-Fi (XV-Series)	6.3v12	<input type="checkbox"/>	<input type="checkbox"/> None	<input type="checkbox"/>	<input type="checkbox"/>
MeshFi		<input type="checkbox"/>	NA	NA	NA
crVision	4.6-18C26	<input type="checkbox"/>	NA	NA	NA
PMP	16.2.3	<input type="checkbox"/>	NA	NA	NA
crMatrix	4.0v4	<input type="checkbox"/>	NA	NA	NA
crPlot Home	4.4.2-R2	<input type="checkbox"/>	<input type="checkbox"/> None	NA	NA
crRanger	21.0.0-R5	<input type="checkbox"/>	NA	NA	NA
eRMP	4.6-18C26	<input type="checkbox"/>	NA	NA	NA

Apply Settings

Manage Software Images
Device software images should be downloaded from [Cambium Support](#). [Learn more](#)

Search: Device Type: Version: Update Recommended Version: Add Delete

Type	Version
<input type="checkbox"/> crMatrix	4.01-12 (Recommended)

Webhooks

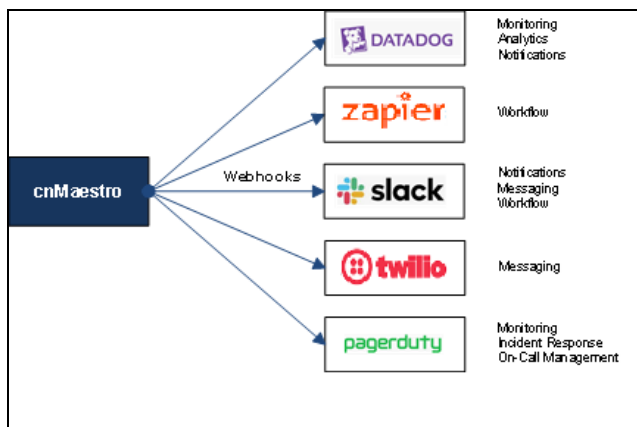
cnMaestro Webhooks provides real-time streaming for alarms using a push notification model. Webhooks data is HTTPS posted to an external Web service. They enable the following benefits:

Benefit	Details
Cloud Friendly	Webhooks are a standard mechanism for Cloud alerts and inter-service asynchronous communication.
Firewall Friendly	HTTPS is generally amenable for outgoing and incoming firewall connections.
Real-Time	Alarms to be sent to third-party services in real-time.
Security	All communication is over HTTPS, and the target domain is validated. Optional security parameters are available for client authentication.
TCP	Webhooks use TCP instead of UDP, so they can alert when the external system is down, or the event was not received.
Third-Party Support	Many Cloud and On-Premises services support Webhooks.

Integrations

Webhooks enable integration with external Cloud services, such as Slack, Twilio, Zapier, Datadog, PagerDuty, etc. They can also be supported using a local HTTPS server and custom applications. Once configured, cnMaestro streams alarms to these services over HTTPS to the configured URL. Some example services are provided below:

Figure 178 Webhook Integration with External Cloud Services



The Webhooks payload is sent in a JSON or a URL-encoded format, and the parameters are comparable to the alarm details present in the RESTful API and email notifications. In addition, cnMaestro also provides default and custom Webhooks templates, so the data format can be tailored to specific services.

Limits

Webhooks are limited to 2 entries per account. In a managed services environment, each managed account can have two Webhooks.

cnMaestro Webhooks Configuration

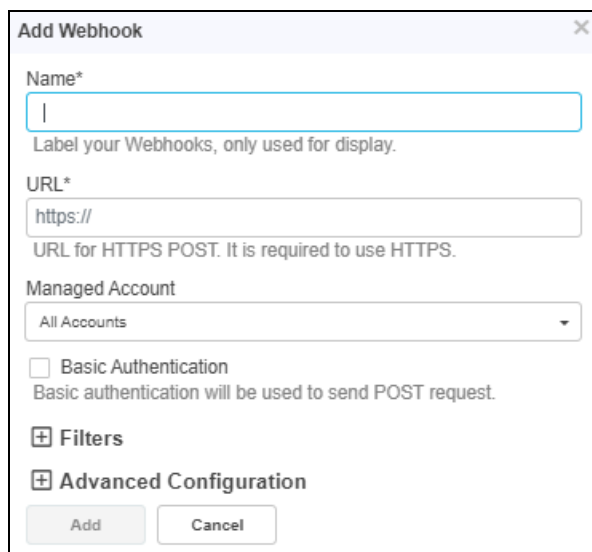
1. Navigate to **Administration > Settings > Webhook**.



Enable	Name	Type	URL	Managed Account	Severity	Device Types	Last Status	Last Status Time	
<input checked="" type="checkbox"/>	webhooks_1	Alarms	webhook.18c7856102c209024279162c29c...	All Accounts	Minor, Major, Critical	All	NA	NA	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input checked="" type="checkbox"/>	webhooks	Alarms	webhook.18c7856102c209024279162c29c...	All Accounts	Minor, Major, Critical	All	Success	2d 6h 41m ago	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

2. Click **Add Webhook**. The following window appears:

Figure 179 Configure: Add Webhook parameters Page



Add Webhook

Name*

Label your Webhooks, only used for display.

URL*

URL for HTTPS POST. It is required to use HTTPS.

Managed Account







Basic Authentication
Basic authentication will be used to send POST request.

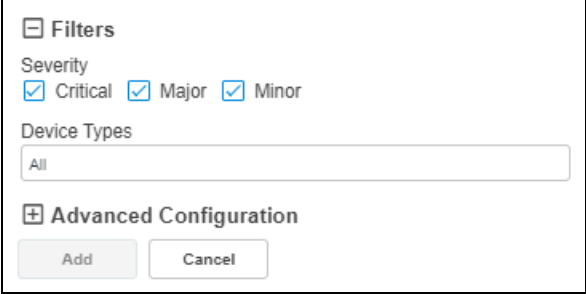


Filters

Advanced Configuration

3. Enter the parameters as shown in the below table.

Table 61: Add Webhook parameters

Parameter	Description				
<p>Advanced Configuration - Content type and Template</p>	<p>You can choose content-type as JSON or URL-Encoded Form.</p> <p>cnMaestro supports default and custom templates for the payload. Custom templates allow specialized payload formats. Enable the Custom checkbox and upload your own custom payload JSON. Details on templates are presented later.</p> <p>The Webhooks JSON payload follows the same format as the cnMaestro RESTful API, with a few additional Webhook-specific variables/keys.</p> <div data-bbox="428 516 930 804" style="border: 1px solid black; padding: 5px;"> <p><input checked="" type="checkbox"/> Advanced Configuration</p> <p>Content Type</p> <p><input type="radio"/> application/x-www-form-urlencoded</p> <p><input checked="" type="radio"/> application/json</p> <p>Template</p> <p><input checked="" type="radio"/> Default</p> <p><input type="radio"/> Custom Add your own custom payload. Learn more</p> <p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p> </div>				
<p>Basic Authentication</p>	<p>Optionally add HTTPS Basic Authentication to the Webhook 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 HTTP request.</p> <table border="1" data-bbox="428 1024 1511 1472"> <tr> <td data-bbox="428 1024 574 1247" style="text-align: center;">  </td> <td data-bbox="574 1024 1511 1247"> <p>Note 1:</p> <p>The username and password for Basic Authentication are different from cnMaestro user credentials. These credentials are used at your endpoint, few external integrations like Slack only require Webhooks URL, for integrations where Basic Authentication is not required.</p> </td> </tr> <tr> <td data-bbox="428 1247 574 1472" style="text-align: center;">  </td> <td data-bbox="574 1247 1511 1472"> <p>Note 2:</p> <p>Basic Authentication is an HTTP standard which that adds an “Authorization: Basic <credentials>” header to the HTTPS POST request. Credentials are Base64 encoded username and password, encoded the following way: Base64(username:password)</p> </td> </tr> </table>		<p>Note 1:</p> <p>The username and password for Basic Authentication are different from cnMaestro user credentials. These credentials are used at your endpoint, few external integrations like Slack only require Webhooks URL, for integrations where Basic Authentication is not required.</p>		<p>Note 2:</p> <p>Basic Authentication is an HTTP standard which that adds an “Authorization: Basic <credentials>” header to the HTTPS POST request. Credentials are Base64 encoded username and password, encoded the following way: Base64(username:password)</p>
	<p>Note 1:</p> <p>The username and password for Basic Authentication are different from cnMaestro user credentials. These credentials are used at your endpoint, few external integrations like Slack only require Webhooks URL, for integrations where Basic Authentication is not required.</p>				
	<p>Note 2:</p> <p>Basic Authentication is an HTTP standard which that adds an “Authorization: Basic <credentials>” header to the HTTPS POST request. Credentials are Base64 encoded username and password, encoded the following way: Base64(username:password)</p>				
<p>Filters</p>	<p>You can filter the alarms based on severity such as Minor, Major, or Critical. You can also select multiple severities.</p> <p>Device type allows to select the particular device from the drop-down.</p>				

Parameter	Description
	
Managed Account	<p>If cnMaestro is configured for MSP (Managed Service Provider), you can map the Webhooks to a Managed Account.</p> <div data-bbox="423 638 1510 770">  <p>Note A maximum of two Webhooks can be configured per Managed Account.</p> </div>
Name and URL	<p>Webhooks label for display and filtering purposes. This will also be included in the default payload as Webhook_name. The URL defines the endpoint for the HTTPS POST request. Only HTTPS is supported.</p>
Type	<p>Type of cnMaestro notification to configure Webhook.</p> <div data-bbox="423 1012 1510 1165">  <p>Note cnMaestro release 2.4.0 supports only alarms as the type for Webhooks configuration.</p> </div>

For example, Configuration Sync Alarm from e500 Device default payload is as shown below:

```
{
  "ip": "10.110.212.130",
  "network": "FR",
  "message": "Failed to push configuration to device",
  "name": "Configuration Sync",
  "severity": "minor",
  "source_type": "wifi-enterprise",
  "Device Model": "cnPilot e500",
  "status": "active",
  "time_raised": "2019-07-29T11:36:35+00:00",
  "site": "lehavre",
  "tower": "",
  "duration": "0",
  "id": "5d3eda434e222e0a28d14372",
  "code": "CONFIG_SYNC",
  "mac": "00:04:56:BB:14:4E",
  "acknowledged_by": "",
  "source": "E500-BB144E-Test-LAB-A",
  "managed_account": "",
  "webhook_retry_count": "0",
  "webhook_timestamp": "2019-07-29T11:36:35+00:00",
  "webhook_name": "cnmaestro_webhook"
}
```

Types of 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 62: Types of Variables

Variable	Description
\$ACKNOWLEDGED_BY	Alert acknowledged by
\$ALARM_DURATION	Alarm duration (seconds)
\$ALARM_ID	Alarm ID (e.g. 9bd4Gc313a4d1e8fie2482df7b77628)
\$ALARM_MSG	Alarm message (e.g.: "GPS Sync state changed to Synchronized")
\$ALARM_NAME	Alarm name (e.g.: Configuration Sync)
\$ALARM_SEVERITY	Alarm severity (e.g. critical, major, minor)
\$ALARM_STATUS	Alarm status (e.g. active)
\$ALARM_TIME_RAISED	Alarm raised time (ISO 8601 Date format: 'YYYY-MM-DDTHH:mm:ssZ')
\$ALERT_CODE	Alert code (e.g. STATUS)
\$DEVICE_MAC	Device MAC address (e.g: AA:BB:CC:DD:EE:FF)
\$DEVICE_MODEL	Device Model (e.g: ePMP 1000, cnPilot r201)
\$DEVICE_NAME	Device name
\$DEVICE_IP	Device IP Address (e.g. 192.168.0.1)
\$DEVICE_TYPE	Device type (e.g.Wi-Fi-enterprise)
\$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)
\$TOWER_NAME	Tower name (note: 'value will be blank if the device is not under a Tower')
\$WEBHOOK_NAME	Webhook name
\$WEBHOOK_RETRY_COUNT	Retry count (note: only present if Webhook is retried; default is 0)
\$WEBHOOK_TIMESTAMP	Webhook sent time (ISO 8601 Date format: 'YYYY-MM-DDTHH:mm:ssZ')

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.



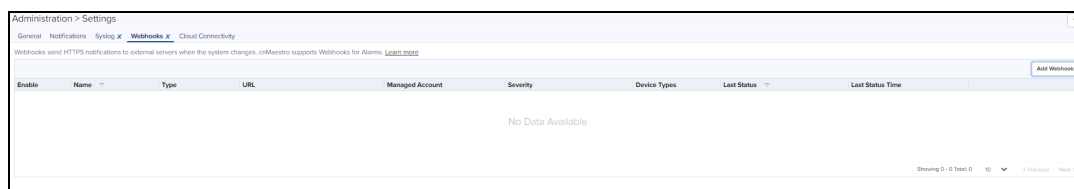
Note

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.

Viewing Configured Webhooks

To view the status of configured Webhooks, navigate to **Administration > Settings** page.




Figure 180 Viewing Configured Webhooks



cnMaestro [Webhooks Configuration](#) provide details on the parameters displayed:

Table 63: Webhook parameters

Parameter	Description
Device Type	The Device Type filter on Webhook.
Enable	Select Enable checkbox to enable the Webhook.
Last Status	Last status of Webhook
Last Status Time	Last Webhook send time.
Managed Account	If the MSP Service is enabled, this is the type of account (E.g. All Accounts, Base Infrastructure, or Managed Account Name).
Name	Label to identify the Webhook.
Severity	Alarm Severity filter on Webhook.
Type	Type of notification. (e.g. Alarm).
URL	The URL where HTTPS POST requests will be sent.

Parameter	Description
	Edit the Webhook.
	Send a test message. It can be used to test Webhook's reachability.
	Delete a Webhook.

Status Check

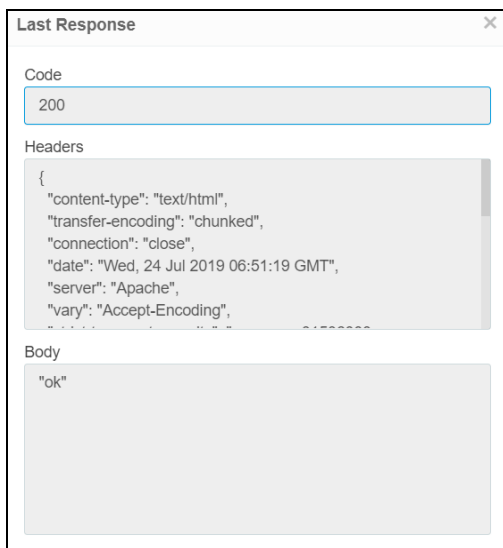
Click **View Details** to check the status of message sent last.

Figure 181 Status check view



View Details displays the response Code, Headers and Body of Webhooks endpoint.

Figure 182 Last response code

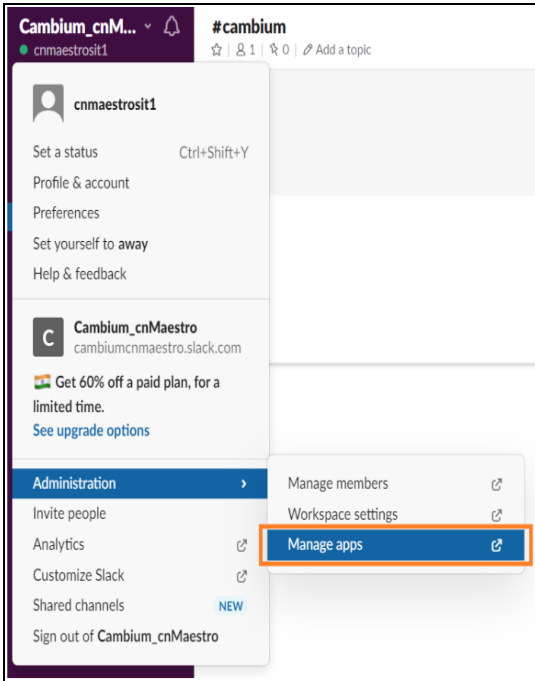


Custom Template Examples

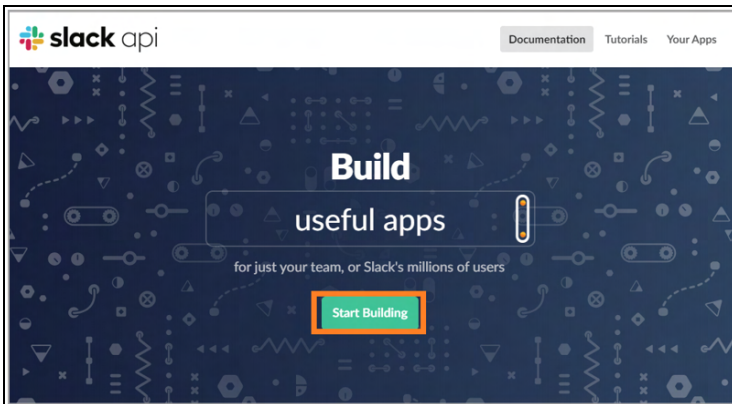
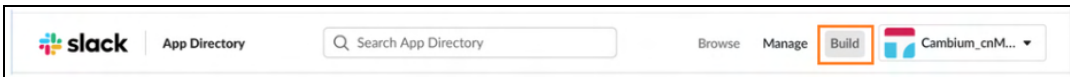
Slack Configuration

Slack is a platform for team communication, offering instant messaging, document sharing, and knowledge search. Following is a simple example of configuring Slack integration with cnMaestro Webhooks using a custom Template.

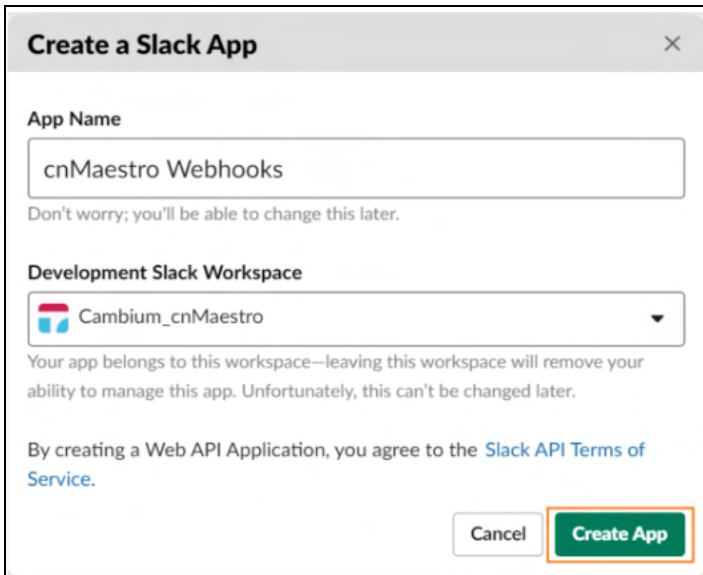
1. On your Slack Screen, click on your workspace name at the top of the left-hand menu and open **Administration** > **Manage** apps.



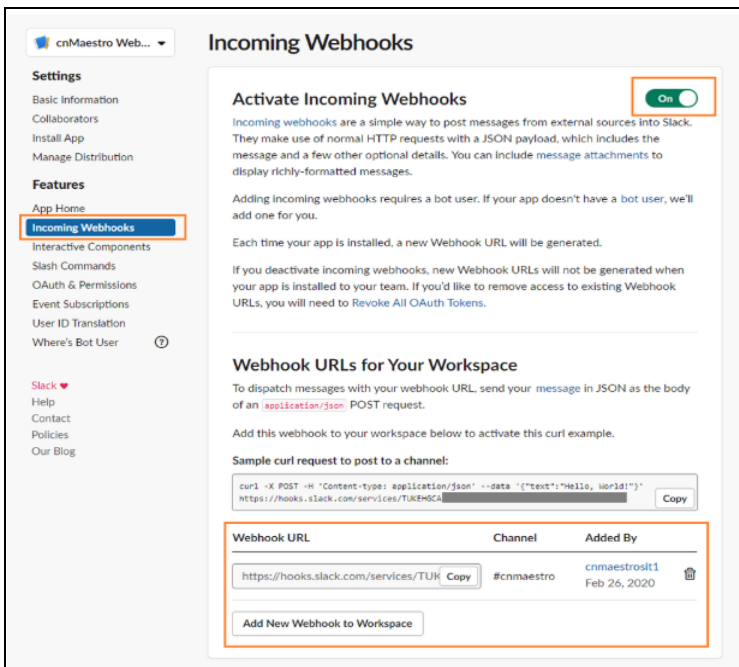
2. In the apps screen, click the Build and then the **Start Building**.



3. In the **Create Slack App** screen, enter an app name of your choice and select your Slack Workspace in the drop-down. Click **Create App**.



4. In the **Basic Information** tab, select **Incoming Webhooks** from the left menu and create a webhook, providing all the permission and targeted Slack Channel details.



5. From the above screen copy the **Webhook URLs**, which needs to be used as URL in cnMaestro Webhooks in the next steps.

NOTE

Learn more about Slack Webhook and expected JSON format at <https://api.slack.com/incoming-webhooks>

6. Login to cnMaestro and navigate to **Administration > Settings > Webhook**.
7. Click **Add Webhook**. Paste the URL from Slack and Expand **Advanced Configuration**.

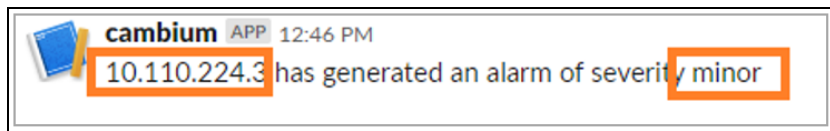
Slack expects a custom JSON payload (<https://api.slack.com/incoming-webhooks>), The simple one is as follows:

```
{
  "text" : "<message>"
}
```

For this example, we are using the following custom template with variables \$DEVICE_IP and \$ALARM_SEVERITY in the formatted message.

```
{
  "text" : "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY"
}
```

- Once an alarm occurs, the following message appears in the configured Slack channel. Notice the variables have been replaced with actual values.

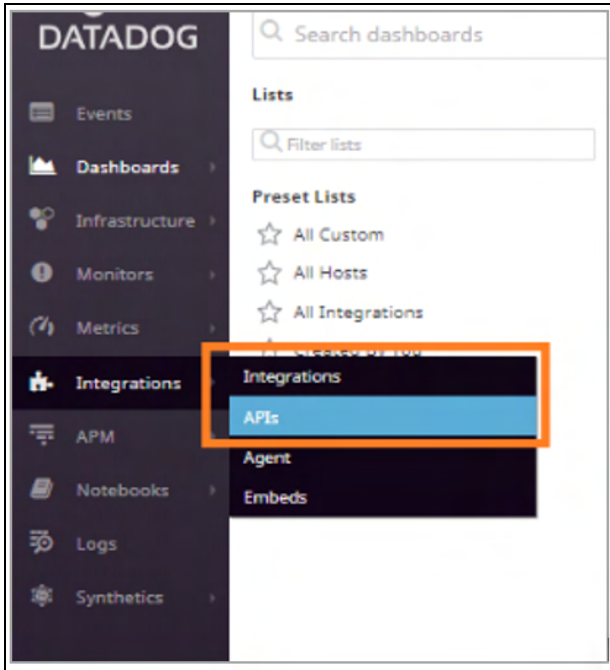


Datadog Configuration

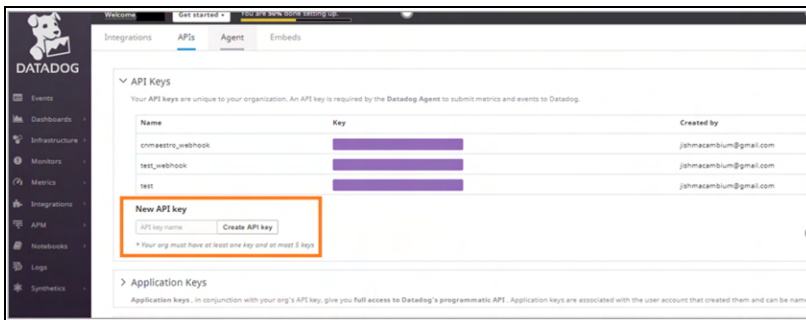
Datadog is a service for IT, Operations and Development teams who write and run applications at scale.

Following is an example of how to create Datadog events using cnMaestro Webhooks and custom templates. Sign up to <https://app.datadoghq.com/signup> and set up your Datadog agent. The agent can also be set up outside the cnMaestro UI device.

1. On your Datadog dashboard, navigates to **Integrations** and open **APIs > API keys**.



2. In the API keys, create a new API key and enter a name for the API key created.



Add the API key to https://api.datadoghq.com/api/v1/events?api_key=<YOUR_API_KEY>, this URL is used as cnMaestro Webhook URL.

3. Datadog expects a custom JSON payload, following is a simple Datadog specific payload format using cnMaestro Webhook variables.

```
{
  "title": "$DEVICE IP",
  "text": "Alarm of severity $ALARM_SEVERITY $ALARM_STATUS",
  "priority": "normal",
  "tags": ["$WEBHOOK_NAME"],
  "alert_type": "warning"
}
```

Note

Learn more about Datadog Events and expected JSON format at <https://docs.datadoghq.com/api/?lang=bash#events>.

4. Login to cnMaestro and navigate to **Administration > Settings > Webhook**.
5. Click **Add Webhook**. Paste the URL from Datadog and expand **Advanced Configuration**.

Edit Webhook ✕

Name*

Label your Webhooks, only used for display.

URL*

URL for HTTPS POST. It is required to use HTTPS.

Managed Account

Basic Authentication
Basic authentication will be used to send POST request.

Filters

Advanced Configuration

Content Type
 application/x-www-form-urlencoded
 application/json

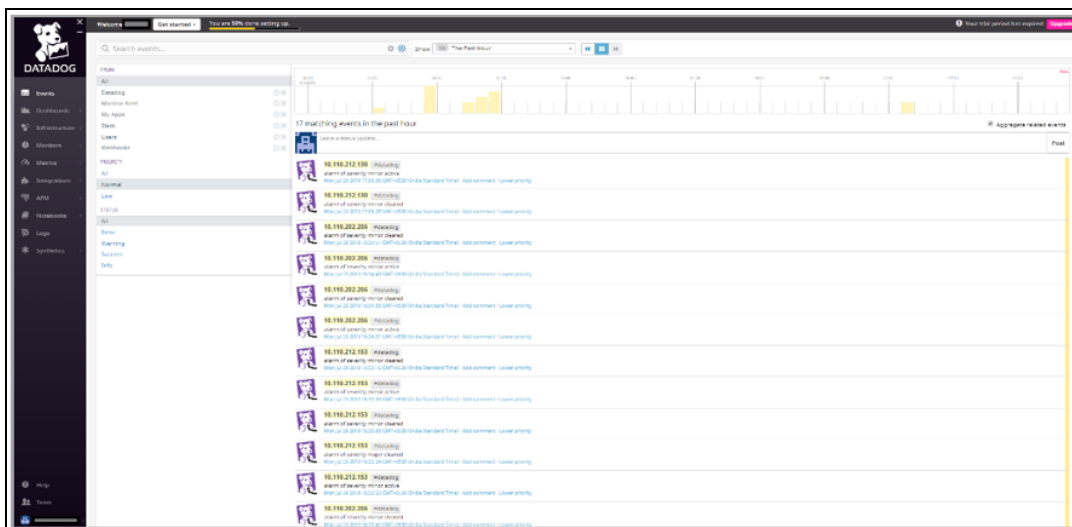
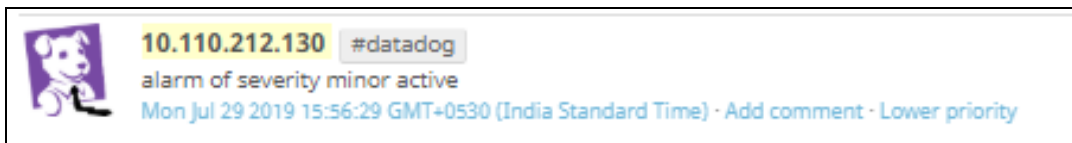
Template
 Default
 Custom Add your own custom payload. [Learn more](#)

```

{
  "title": "$DEVICE_IP ",
  "text": "alarm of severity $ALARM_SEVERITY
$ALARM_STATUS ",
  "priority": "normal",
  "tags": [
    "$WEBHOOK_NAME"
  ],
  "alert_type": "warning"
}

```

6. Once an Alarm occurs, the following message appears to configure Datadog events. This can be checked in Datadog dashboard at **Events > My Apps**.



PagerDuty configuration

PagerDuty is an incident management platform that provides reliable notifications, automatic escalations, on-call scheduling, and other functionality to help teams detect and fix infrastructure problems quickly.

Following is a simple example of configuring PagerDuty integration with cnMaestro Webhooks. We can use both default or custom templates in JSON and x-www-form-urlencoded content types.

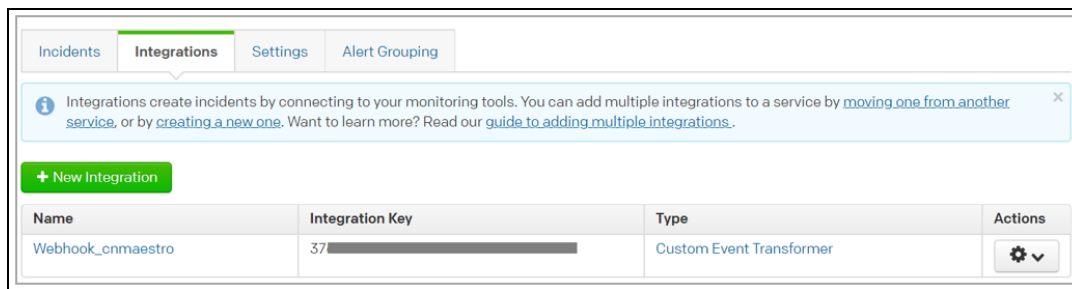
To begin, login to PagerDuty or create a new account.

<https://app.pagerduty.com/>

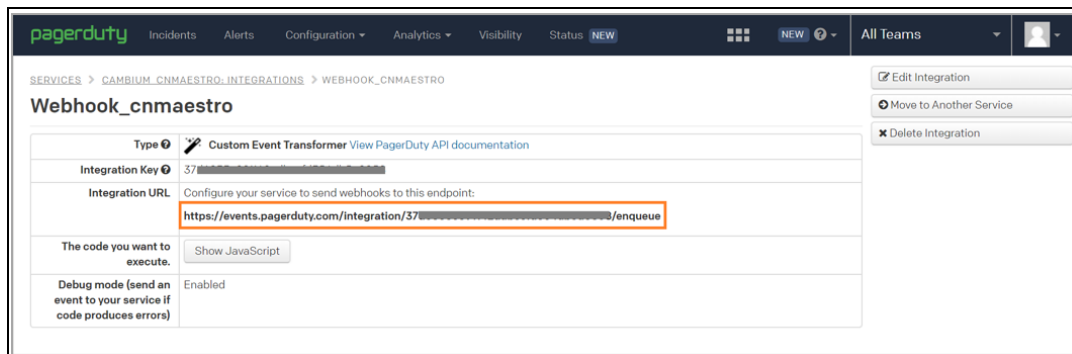
To capture the cnMaestro alarms you need to add a new integration into PagerDuty using a Transformer tool.

After login to your PagerDuty account, to add an integration:

1. Navigate to **Configuration > Services**.
2. If you are creating a new service for your integration, click **Add New Service**. If you are adding your integration to an existing service, click the Name of the service you want to add the integration, navigate to the **Integrations** tab, then click **New Integration**.
3. Select the Integration **Type** as **Custom Event Transformer**. Complete the remaining incident settings as desired and save by clicking the **Add Service/Integration** at the bottom.



4. Click on the Name of your new integration to view the details.




Integration URL is used in configuration of cnMaestro Webhooks.

https://events.pagerduty.com/integration/<integration_key>/enqueue

5. Login to cnMaestro and navigate to **Administration > Settings > Webhook**.
6. Click **Add Webhook**. copy and paste the integration URL from PagerDuty and expand **Advanced Configuration**.

You can use the custom payload or default option in cnMaestro. For this example, we are using the following custom template with variables \$DEVICE_IP and \$ALARM_SEVERITY in the formatted message.

```
{
  "text" : "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY"
}
```

	<p>Note</p> <p>Learn more about PagerDuty and different integrations at https://support.pagerduty.com/docs/webhooks.</p>
---	---

7. Once an Alarm occurs, the following message appears in configured service’s incidents. Notice the variables have been replaced with actual values.



Twilio Configuration

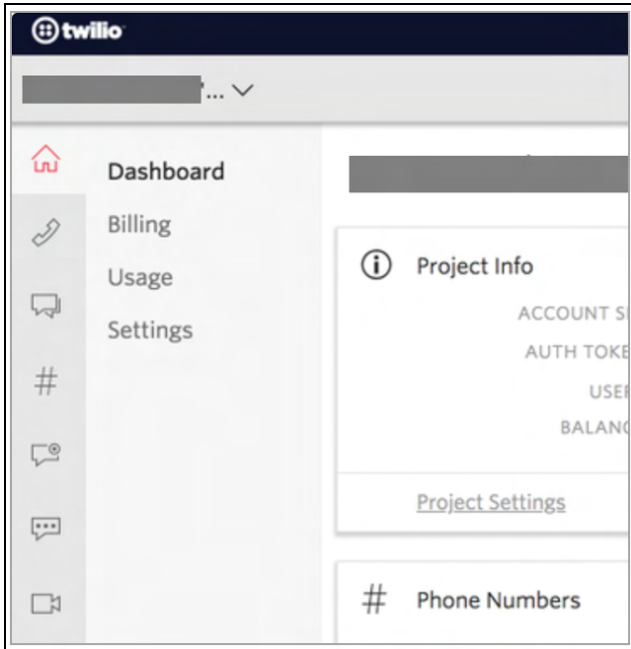
Twilio is a developer platform for communications. Software teams use the Twilio API to add capabilities like voice, video, and messaging to their applications. Twilio is mainly used as an SMS service provider for websites and apps.

Twilio supports HTTP Basic Authentication. This allows you to protect the URLs on your web server so only you and Twilio can access them.

Following is an example of integrating Twilio with cnMaestro Webhooks using an application/x-www-form-urlencoded custom template.

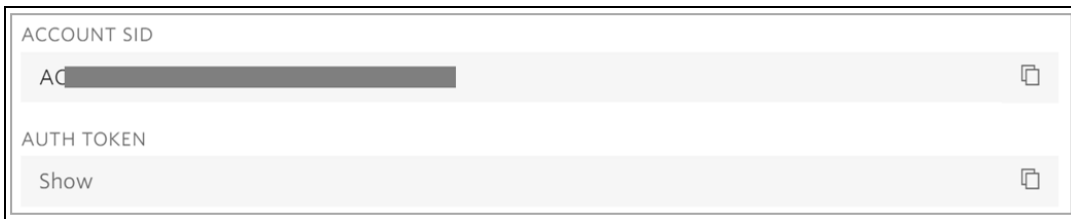
To send a cnMaestro alarm as an SMS directly to a phone, we are going to use the Twilio's API to programmatically send text messages.

1. Login to Twilio or create a new account. <https://www.twilio.com/>
2. After login to your Twilio account, navigate to your console **Dashboard**.

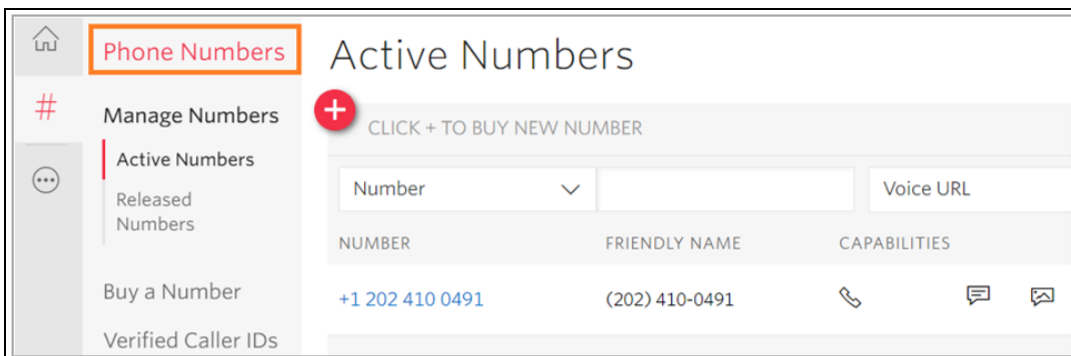


Make a note of the Account SID, Auth Token values on the main twilio.com/user/accountpage - you need it when you configure the cnMaestro Webhooks with Basic Authentication username and password.

3. Add the **Account SID** to [Add the Account SID to https://api.twilio.com/2010-04-01/Accounts/ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/Messages.json](https://api.twilio.com/2010-04-01/Accounts/ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/Messages.json), this URL will be used as cnMaestro Webhook URL.



4. Go to **Phone Numbers** under All Products and Services in the console to get the phone number or click on the red plus (+) icon to add a new number and note down the assigned number.




5. Login to cnMaestro and navigate to **Administration > Settings > Webhook**.
6. Click **Add Webhook**. Fill the Account SID and Auth Token from Twilio for URL and Basic Authentication and expand **Advanced Configuration**.

Using the custom payload option in cnMaestro, specify a custom payload adapted to Twilio’s format.

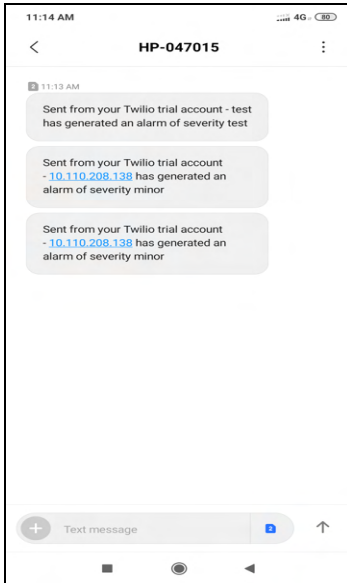
```
{
  "Body": "<message>",
  "From": "+<country_code><Twilio_number>",
  "To": "+<country_code><destination_number>"
}
```

For this example, we are using the following custom template with variables \$DEVICE_IP and \$ALARM_SEVERITY in the formatted message.

```
{
  "Body": "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY",
  "From": "+12024100491",
  "To": "+91*****"
}
```

	<p>NOTE</p> <p>To configure Twilio to cnMaestro Webhooks you should use application/x-www-form-urlencoded as content type.</p> <p>Learn more about Twilio and expected JSON format at https://www.twilio.com/docs/usage/api</p>
---	--

7. Once an Alarm occurs in cnMaestro, the following message will be sent to the destination number from the Twilio number. Notice the variables have been replaced with actual values.



Zapier Configuration

Zapier is an online platform that aims to connect various apps together to automate workflows.

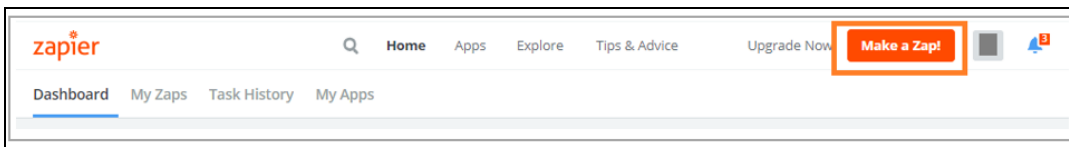
With Zapier you can build Zaps that perform your automation for you. These automations are achieved by mixing a Trigger with actions available on your favourite apps. Zapier supports hundreds of apps. You can mix and match triggers and actions to automate.

Following is an example of configuring Zapier integration with cnMaestro Webhooks. For example, you could make a Zap that would automatically save alarms from cnMaestro Webhooks to a new row on a Microsoft Excel. Zapier can catch a Webhook POST from cnMaestro, automatically adding the information to a new row in Excel.

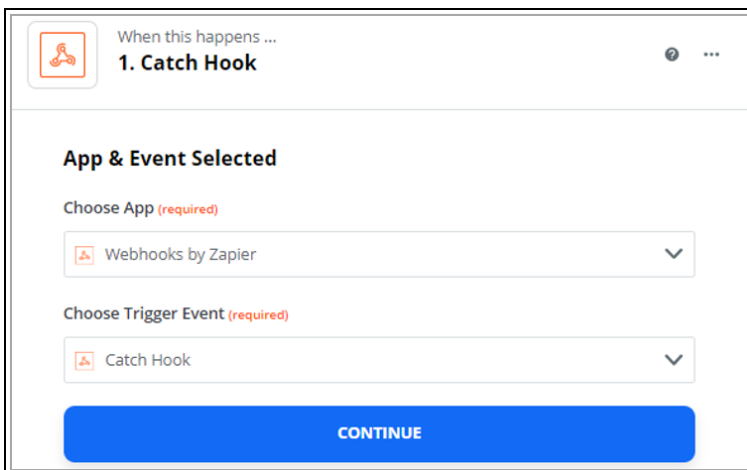
First, Login to Zapier or create a new account.

[/https://zapier.com/](https://zapier.com/)

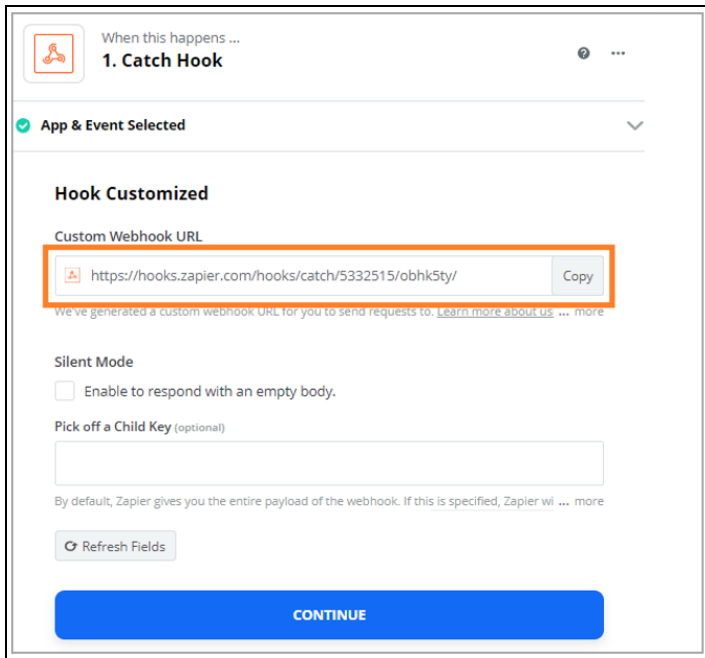
1. After login to your Zapier account, navigate to dashboard.
2. On your Zapier dashboard, click on **Make a Zap** at the top right-hand side.



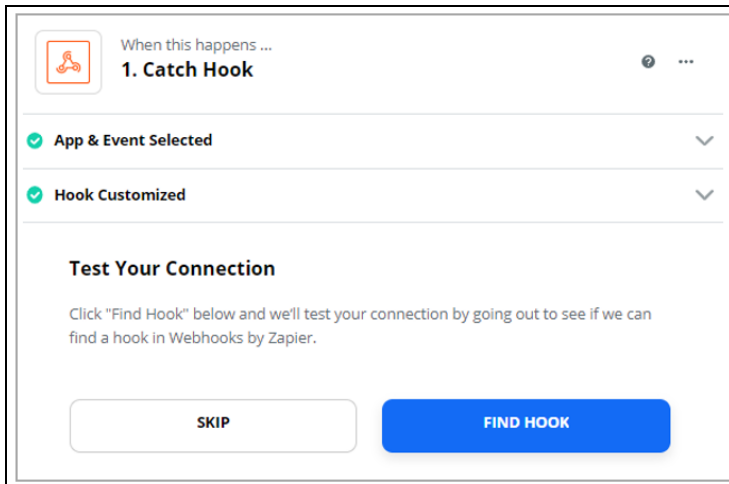
3. Choose **Webhooks by Zapier** and **Catch Hook** as the trigger app and trigger event.



4. To customize your webhook trigger, copy the given URL and configure it in your cnMaestro Webhook.



5. Click continue redirects to **Test your connection** page.

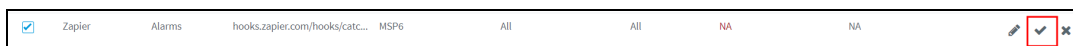


6. To test the connection, open cnMaestro Webhooks and configure the given custom URL from Zapier then can customize and fill the **Advanced Configuration**.

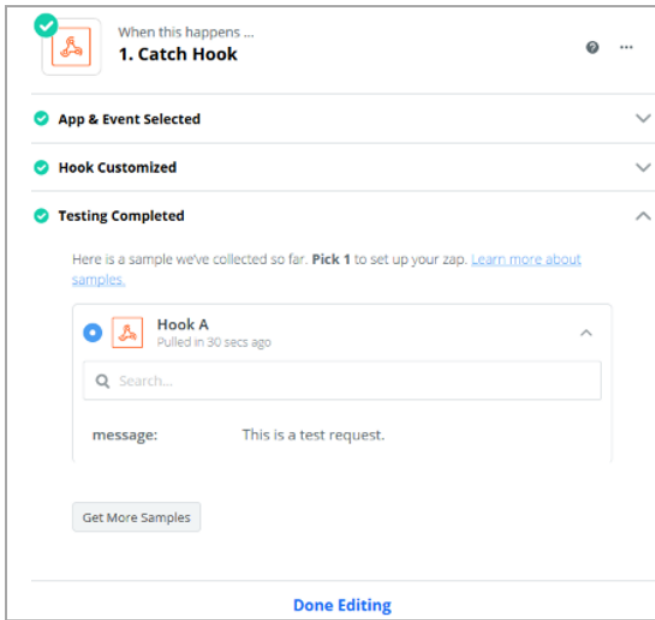
You can use the custom payload or default option in cnMaestro. For this example, we are using the following custom template with variables \$DEVICE_IP and \$ALARM_SEVERITY in the formatted message.

```
{
  "text" : "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY"
}
```

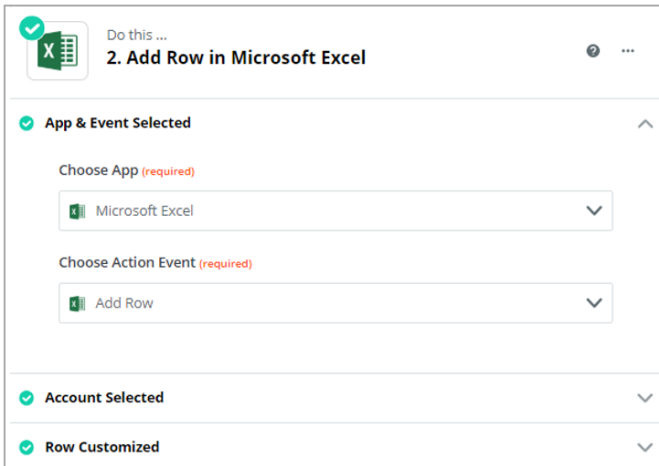
7. Send a test webhook by clicking on the test icon on the right-hand side of the webhook table.



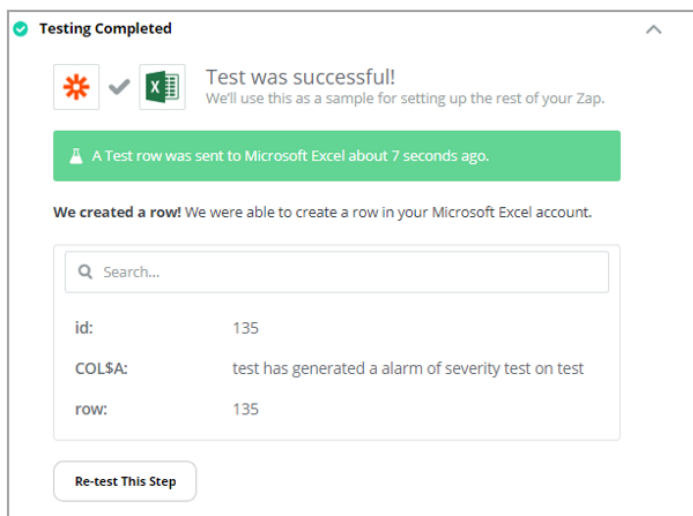
8. Now go back to Zapier and click **Find Hook** to complete the testing.



9. Set up Microsoft Excel as the action for your Zap, action event, connect your excel account and customize.



10. To check if your action works as expected. Click **Send Test** to run the action step. The next screen shows whether Zapier has been able to successfully perform the action step or not.





Note

Learn more about how Zapier supports different apps at <https://zapier.com/help/>.

11. Once an Alarm occurs, the following message appears in the configured excel sheet. Notice the variables replaces with actual values.

1	10.110.208.138 has generated an alarm of severity minor
2	

Audit Logs

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 183 Audit Logs

Result	Time	Type	Module	Action	Source	IP Address	Description
Success	Tue Feb 09 2021 09:12:25 UTC -0530	Operations	Email Notifications	Edit	document user	172.26.10.78	Email notification settings updated
Success	Tue Feb 09 2021 09:04:17 UTC -0530	Security	Administrator	Login	document user	172.26.10.78	document user logged in successfully
Success	Mon Feb 08 2021 22:17:12 UTC -0530	Provisioning	ACL	Edit	document user	172.26.10.18	ACL info update performed
Success	Mon Feb 08 2021 17:09:44 UTC -0530	Operations	TEMPLATE	Create	document user	172.26.10.254	Template backup initiated for device '0A:00:3E:8B:83:95'
Success	Mon Feb 08 2021 09:39:07 UTC -0530	Security	Administrator	Login	document user	172.26.10.254	document user logged in successfully
Success	Fri Feb 05 2021 23:31:26 UTC -0530	Security	Administrator	Login	Administrator	172.26.10.133	Administrator logged in successfully
Success	Fri Feb 05 2021 18:53:53 UTC -0530	Security	Administrator	Login	Administrator	10.10.208.19	Administrator logged in successfully
Success	Fri Feb 05 2021 10:09:47 UTC -0530	Security	Administrator	Login	document user	172.26.10.216	document user logged in successfully
Success	Fri Feb 05 2021 10:08:58 UTC -0530	Security	Administrator	Logout	document user	172.26.10.216	User document user logged out
Success	Fri Feb 05 2021 07:57:08 UTC -0530	Security	Administrator	Login	document user	172.26.10.181	document user logged in successfully

The following table describes the Audit Logs parameters and their descriptions.

Table 64: Audit Log Parameters

Parameter	Description
Action	Displays the action performed by the user (create, delete, download, etc.).
Description	Textual description of the task.
Export	Enable export as CSV or PDF.
IP Address	IP address of the Web browser or API application.
Module	Module generating entry (AAA, administrator, alarm).
Result	The result of the audit log as Success or Failed .
Source	Administrator or API client name.
Source Type	Entity making the update: administrator or API client.
Type	Type of the log entry (configuration, operation, onboarding, security).
Time	The time when the action was performed.

Log Action

An action log contains a set of transactions. Each transaction contains one or more Actions. Each Action has a name and input parameters. Some Actions have output parameters.

The following Actions will be supported for individual Audit Log entries. Each activity performed in the server is detailed in this table.

Table 65: Log Action Parameters

Parameter	Description
Claim	Claim a device in the network operator.
Cloud-Connect	Provides the status of the On-Premises to Cloud account connection.
Create	Create an object in the network device.
Delete	Delete an object in the network device.
Download	Download a file.
Edit	Edit an existing device detail.
Link Test	Perform a Link Test.
Login	Login to a device.
Logout	Logout from a device.
Mail	Mail ID of a device.
Move	Move a device from the server.
Reboot	Reboot a device.
Reset	To reset a device
Upload	Upload a file on the server.

Audit Modules

Auditing activity is mapped to individual modules within cnMaestro. A breakdown of the available modules is listed below.

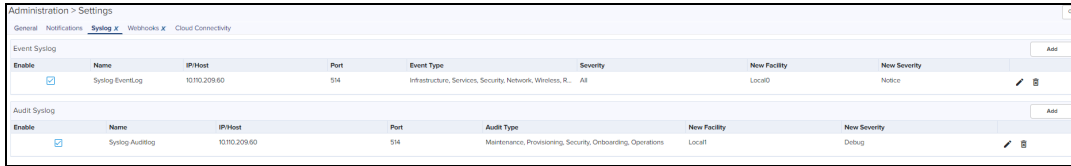
Module	Type (s)	Description
ACL	provisioning	Adding Editing Removing the ACL Entries
Administrator	provisioning operations security	User Management: Login, Users, Roles, Email, etc.
Alarm	provisioning	Alarms and Alarm History.
API	provisioning	API Management: API Clients and Webhooks
Auditing	provisioning	Auditing Infrastructure
Auto-Provision	provisioning	Auto-Provisioning

Module	Type (s)	Description
CBRS	Services	CBRS
Data-tunnel	provisioning	Data Tunneling
Device	provisioning operations	Device management
Guest-Portal	provisioning	Guest Portal
Infrastructure	provisioning	Site, Network, Tower Management
Jobs	provisioning operations	Jobs Infrastructure
License	licensing	Update license details
MSP	operations	Operations covering Managed Services and Managed Account
Onboard	provisioning operations	Onboarding Queue
Report	provisioning operations	Data Reports
Software-Upgrade	provisioning operations	Software Upgrade: device image import/export, upgrade device
SIM	provisioning	SIM claim and delete
System	provisioning operations security	System Services: VM management, change log level, system upgrade, system monitoring, software images, system settings
Template	provisioning	Template-Based Configuration
Tools	provisioning operations	Technical support dump, networking operations, etc.
Webhooks	provisioning	Webhooks configuration and management
Wi-Fi	provisioning operations security	AP Groups, WLANs: edit W-Fi configuration objects

Syslog

cnMaestro supports Notification Syslog (Event Log) and Audit Syslog. The generated Event Logs and Audit Logs are sent to the syslog server configured under **Administration > Settings** page. Every syslog has a Facility and a Severity level. Maximum of five entries can be added in Notification syslog and Audit syslog.

Figure 184 Syslog



The following table describes the parameters in Syslog server:

Table 66: Syslog Server Parameters

Field	Description
<input checked="" type="checkbox"/>	Enable the notification syslog or audit syslog.
Event Type	The type of event (Infrastructure, Network, Operation, Security and Wireless). You can select one or multiple events.
IP/Host	The IP address provided to the server.
Name	The username provided to the server.
New Facility	The type of program logging the message. The allowed facilities are local 0 to local 7.
New Severity	The severity of the system log message.
Port	IP address or hostname provided to the server.
Severity	The initial severity of the generated syslog messages (i.e. Critical, Major, Minor or Notify).

Event Syslog

Notification messages are filtered based upon Type (which may be slightly different between Events and Alarms) and Severity.

Click **Add** to add a new Event Syslog window pop-up.

Event Syslog
✕

Name

IP/Host

Port

Event Type

Infrastructure
 Network
 Registration
 Operations
 Services
 Security
 Wireless

Severity

Critical
 Major
 Minor
 Notify

New Facility

Local0
▾

Locally used facilities

New Severity

Emergency
▾

System is unusable



NOTE:

At least one Event Type or Severity must be selected.


1. Enter **Name**.
2. Enter the **IP/Host** address.
3. Enter the **Port** number. Port 514 is the default for syslog
4. Select **Event Type**.
5. Select **Severity Type**.
6. Select the **New Facility** from the drop-down list.

Facility	Description
Local 0-Local 7	It is the locally used facilities.

7. In the **New Severity** drop-down, select the type of Severity. Please refer to the below Severity table:

Value	Severity	Description
0	Emergency	System is unusable.
1	Alert	Action must be taken immediately.
2	Critical	Critical conditions of hard device errors.
3	Error	Error conditions

Value	Severity	Description
4	Warning	Warning conditions.
5	Notice	Normal but significant conditions. Conditions that are not error conditions but may require special handling.
6	Informational	Informational messages.
7	Debug	Debug-level-messages.

8. Click  to edit the Event Syslog. The dialog box appears:

Event Syslog
✕

Name

IP/Host

Port

Event Type
 Infrastructure
 Network
 Registration
 Operations
 Services
 Security
 Wireless

Severity
 Critical
 Major
 Minor
 Notify

New Facility
 ▼
manage.account.syslog.facility.19

New Severity
 ▼
Normal but significant conditions

9. Repeat the above steps to update an existing Notification Syslog.

Audit Syslog

The Audit Syslog separates messages based upon Audit Type.

Click **Add** a new Audit Syslog window pops-up.

Audit Syslog
✕

Name

IP/Host

Port

Audit Type


Maintenance
 Onboarding
 Operations
 Provisioning
 Security

New Facility

Locally used facilities

New Severity

Normal but significant conditions



NOTE:

At least one Audit Type must be selected.

1. Enter **Name**.
2. Enter the **IP/Host** address.
3. Enter the **Port** number. The port number 514 is the standard syslog port.
4. Filter by **Audit Type**.
5. Select **New Facility** from the drop-down list.

Facility	Description
Local 0-Local 7	Available facilities.

6. Select the type of **Severity**.
7. Click **Add**.

Cloud Connectivity

Overview

Cloud Anchor accounts exist alongside Cloud NMS accounts, which enable device management through cloud.cambiumnetworks.com. Anchor accounts are attached to cnMaestro On-Premises installations and have their own Cambium ID. All new cnMaestro On-Premises 3.1.0 deployments must connect to an Anchor account at installation, and all existing cnMaestro instances will need to connect to an Anchor account before updating to cnMaestro 3.2.0.

The Anchor account collects statistics and automatically pushes announcements of new device firmware and cnMaestro software images. cnMaestro On-Premises reports the following details to the Anchor account:

Type	Details
System	Uptime, Processor, RAM, Disk, Virtualization Vendor
Devices	Count, Type
Application	Software Version, User Types and Count, Account View, Country
Features	MSP, CBRS, Wi-Fi Performance, Auto-Provisioning, SNMP, etc.

Anchor accounts also simplify CBRS provisioning and billing by aggregating multiple On-Premises instances. In future, Anchor accounts will be used to manage On-Premises cnMaestro X subscriptions.

You must create an Anchor account before connecting the On-Premises instance, as shown below:

1. Navigate to <https://cloud.cambiumnetworks.com>.
2. Click **Create Account**.



3. In account type, select **Anchor**.

Create a Cloud Account
A Cloud Account is required to manage devices in cnMaestro.

Cambium ID: The Cambium ID is a string that uniquely identifies this account. It consists of letters, numbers, and underscores, and it is used to onboard devices. It is also written to devices managed by cnMaestro (and can be accessed in their UI). Once set, the Cambium ID can only be changed by contacting Cambium Support.

Create a Cambium ID. For example: ACME_Broadband_Inc

Cloud Account Name: A friendly name for this account. This could be the name of the company.

cambiumnetworks

Country: The country where devices in this account are located.

India

Time Zone: The time zone used to calculate daily statistics.

ET/GMT-12 (UTC -12:00)

Account Type: Select the type of account. If you plan to host private copies of cnMaestro in your data center, then select the Anchor choice. This account will allow your local cnMaestro servers to connect to the cnMaestro Cloud to simplify firmware upgrades, license management etc.

MMS (via cnMaestro cloud for device management)

Anchor (host a copy of cnMaestro in your own data center, connected to this account)

60 GHz cnWave Beta Program:

I agree to the Terms of Service for 60 GHz cnWave Beta Program.

I agree to the cnMaestro Terms of Service.

[Create Account](#)

4. Click **Create Account**.

Onboarding Key

Once the Anchor Account is created, an Onboarding Key needs to be set, to allow On-Premises instances to connect.

1. Navigate to the **Manage Instances** page and edit the **Onboarding Key**. This key will be entered into the cnMaestro On-Premises UI to connect to the Anchor Account.

The screenshot shows the 'Manage Instances' page in the cnMaestro interface. The 'Onboarding' tab is selected, showing 'On-Premises Instances'. The 'Cambium ID' is 'ANC_PRI'. The 'Enable Onboarding' checkbox is checked. Below, there is a text input field for the 'Onboarding Key' with a masked password (seven dots). 'Save' and 'Cancel' buttons are at the bottom.

2. Once the On-Premises server onboards, the On-Premises Instances page lists all servers in the account.

The screenshot shows the 'On-Premises Instances' table. It has columns for Name, Type, Status, Last Connected, Onboarded, Uptime, and CBS Sync Status. One instance named 'cnMaestro' is listed with Type 'OVA', Status 'Online', Last Connected 'May 31, 2021 02:31', Onboarded 'May 28, 2021 21:28', Uptime '2d 20h 27m', and a 'Sync Now' button.

Name	Type	Status	Last Connected	Onboarded	Uptime	CBS Sync Status
cnMaestro	OVA	Online	May 31, 2021 02:31	May 28, 2021 21:28	2d 20h 27m	Sync Now

Click the instance host name, to view the collected information specific to the On-Premises server.

Connecting cnMaestro On-Premises to Anchor Account

Perform the following steps to connect the cnMaestro On-Premises server with the Cloud Anchor Account:

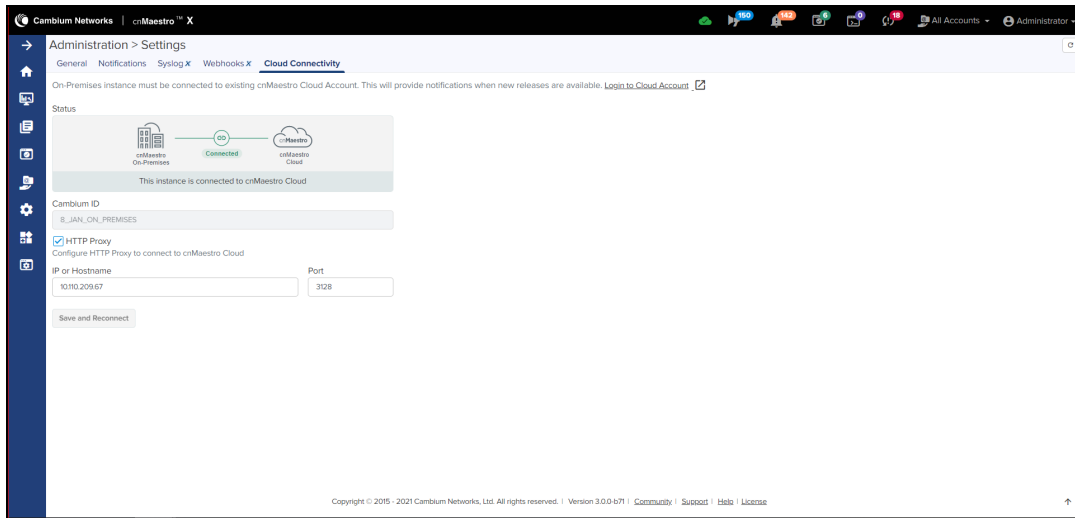
1. Navigate to the **Administration > Settings > Cloud Connectivity** in the cnMaestro On-Premises UI.
2. Enter the **Cambium ID** for the Cloud Anchor Account.
3. Enter the **On-boarding Key** created in the section above.
4. Enable **HTTP Proxy** if required by setting the IP address or Host Name.



NOTE:

Enable **HTTP Proxy** only when On-Premises server needs to connect with public network through proxy.

5. Click **Save and Connect**.



NOTE:

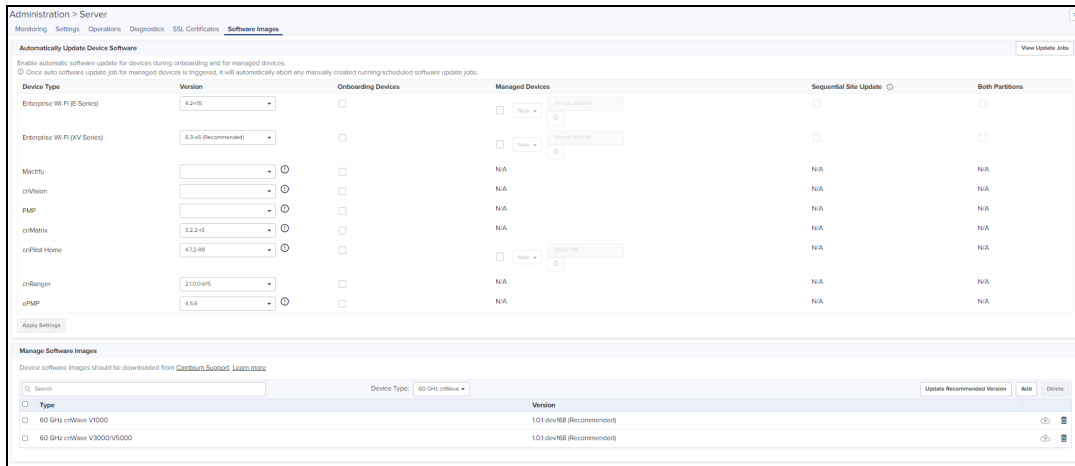
- During the retry time it will take 15 minutes to connect the On-Premises with Anchor Cloud account.
- For every 1 hour it updates the periodic inventory status of On-Premises to Cloud.

Software Images

Once the On-Premises server is synced with the cloud, the user can upload the software images from cloud directly to the On-Premises.

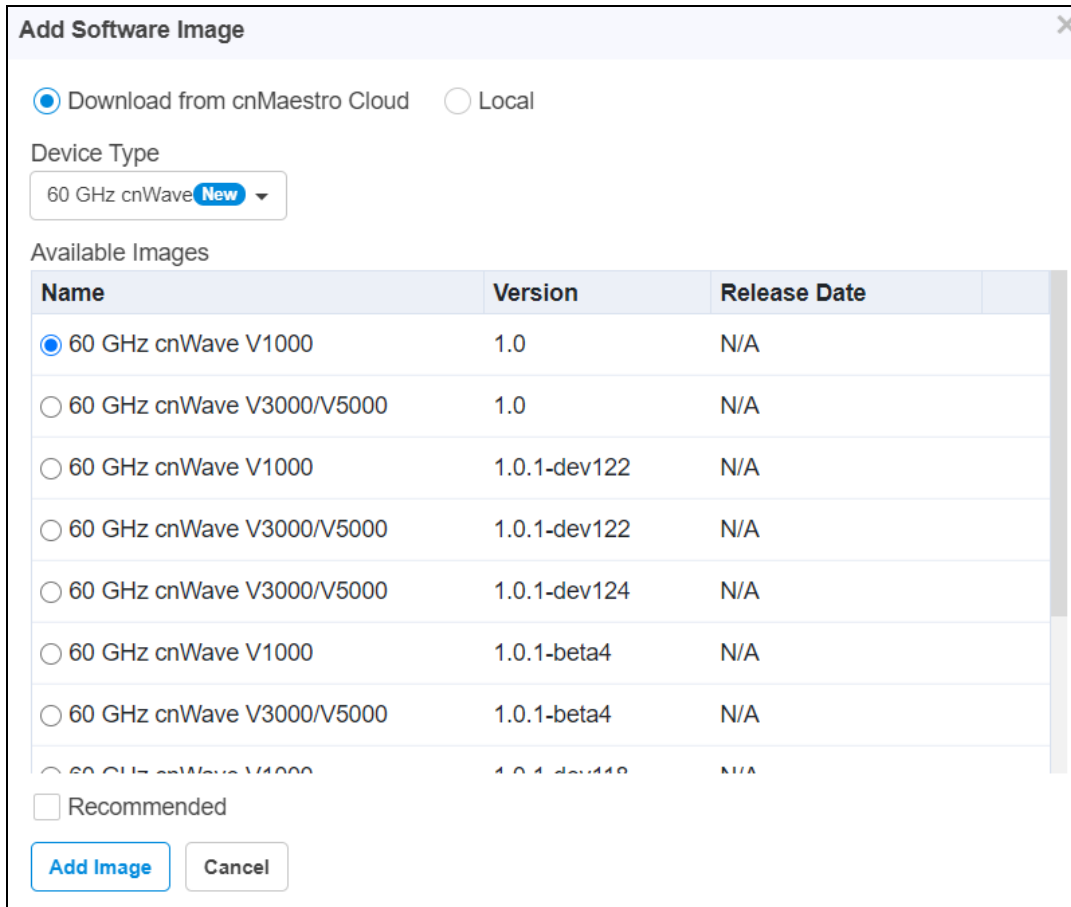
To upload Software Image perform as follows:

1. Navigate to **Administration > Server > Software Images**.



2. Click **Add Image**.

3. Click **Download from cnMaestro Cloud** and select **Device Type**.



4. Select the Version and click **Add Image**.

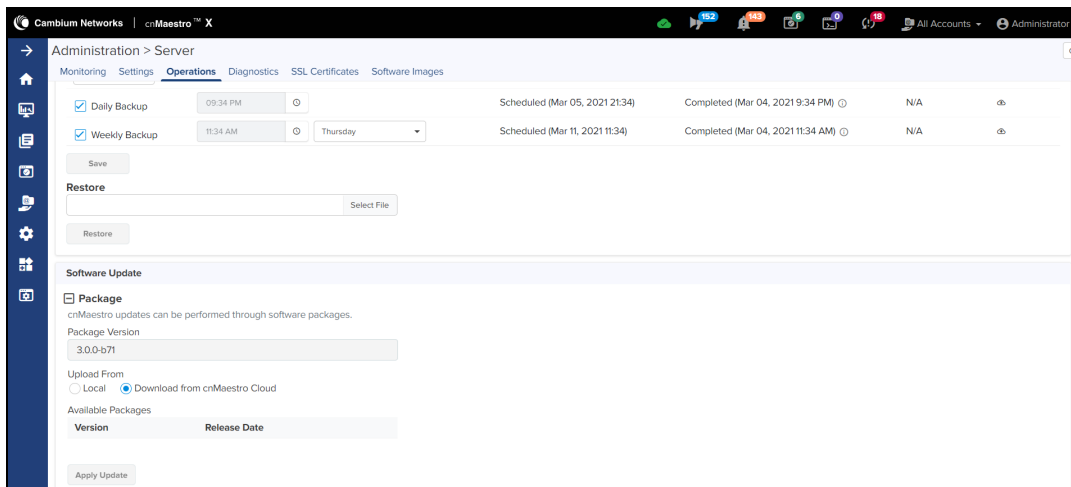
cnMaestro System Update

Package

Once the Cloud is synced with the On-Premises, user can upload the package from Cloud to On-Premises.

To upload a Package, perform the following:

1. Navigate to **Administration > Operations > Package**.
2. Select option **Download from cnMaestro Cloud** under **Upload From**.
3. Click **Apply Update**.



OVA

Once the Cloud is synced with the On-Premises user can upload the software package from Cloud to On-Premises.

To upload an OVA Image, perform the following:

1. Navigate to **Administration > Server > Operations > OVA**.
2. Select option **Download from cnMaestro Cloud**.
3. Select OVA listed in the table.
4. Click **Upload OVA**.

OVA
Software Updates are performed using OVA files. To revert to an older cnMaestro image, make sure a backup file already exists for the image version.

OVA Version
3.0.0-r19

Partition 1
3.0.0-r19 (active)

Partition 2

Upload From
 Local Download from cnMaestro Cloud (Version: 3.1.0-a28)

OVA File

Appendix

This section includes the following topics:

- [Maintenance](#)
- [Deployments](#)
- [Windows DHCP](#)
- [Network Port Requirements](#)
- [Contacting Cambium Networks](#)

Maintenance

This section provides the following details:

- [Command Line Alternatives](#)
- [SSH Access](#)
- [Data Backup](#)
- [Extending the Data Disk](#)
- [Account Recovery](#)
- [Application Account Recovery](#)
- [Configure Network Time Protocol \(NTP\)](#)

Command Line Alternatives

Cambium Networks highly recommends using the cnMaestro UI for all application operations; however, in case the cnMaestro system is not executing correctly, a number of command-line alternatives exist. You can access these by logging into the cnMaestro CLI (through the VM Console) and selecting the “Shell” option to launch a Unix shell.

Export cnMaestro Data

Navigate to **Manage > Server > Operations > System Backup** to the UI version of this command. From the command line the data can be exported using the following:

```
sudo cnmaestro-export
```

The location of the exported data file is printed when the command completes. It can then be copied to an external directory using SCP or FTP. From there it can be imported into a different cnMaestro instance.

Import cnMaestro Data

Navigate to **Manage > Server > Operations > System Backup** to the UI version of this command. From the command line the data can be imported using the following:

```
sudo cnmaestro-import <data file>
```

The data file needs to be copied to the cnMaestro instance prior to executing this command. This can be done using either SCP or FTP.

Technical Support Dump

The UI version of this command is located at: **Manage > Server > Diagnostics > Technical Support Dump**. From the command line the technical support dump can be exported using the following:

```
sudo cnmaestro-techdump
```

The location of the file will be printed when the command completes. It can then be copied to an external directory using SCP or FTP and then sent to Cambium support personnel.

Apply OVA Upgrade

This section describes a failsafe mechanism to apply an OVA Upgrade using the Command Line. First make the image accessible to the operating system either by downloading it through SCP (and storing in /srv/storage/tmp/) or mounting a shared folder. Then execute the following commands:

- Extract and stage the image into the unused partition

```
sudo /srv/bin/cnmaestro-image stage <OVA Filename>
```

- View status of the extraction (wait until it completes/hits 100% -- about 10 minutes)

```
watch -n2 sudo /srv/bin/cnmaestro-image status
```

- Boot into the new image. Use the inactive partition from the status command

```
sudo /srv/bin/cnmaestro-image upgrade <os2 or os1>
```



NOTE:

Above mentioned steps are only a failsafe if the UI upgrade is unavailable. They should not be used for downgrades, which are unsupported.

Apply Package Update

Navigate to **Manage > Server > Operations > Apply cnMaestro Package** to the UI version of this command. From the command line an update package can be applied using the following:

```
sudo /srv/bin/cnmaestro-image patch <package-file>
```

The upgrade file needs to be copied to the cnMaestro instance prior to executing this command. This can be done using either SCP or FTP. The update file itself is downloaded from Cambium Networks and only updates the cnMaestro application.

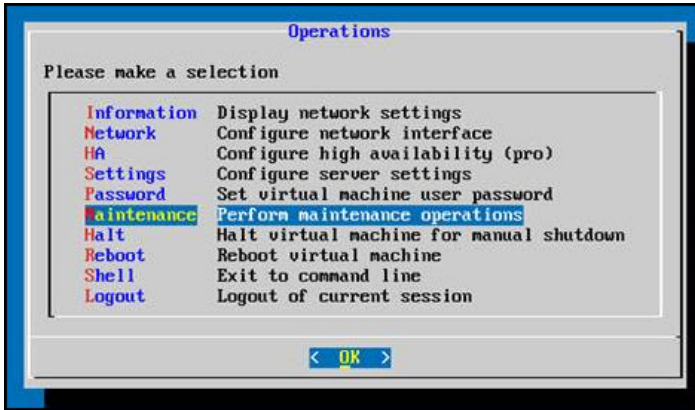
SSH Access

cnMaestro supports SSH access using the 'cambium' user account and password. Enabling this feature is not recommended, due to the password security, but it is available if needed.

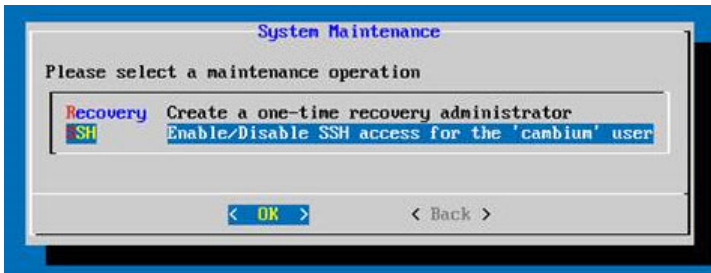
Enabling SSH Access

Follow the below steps to enable SSH access:

1. From the **Operations** page, select **Maintenance**.



2. Select **SSH** for the SSH Server page.



3. Select **Enable SSH** option.



A screen pops-up if SSH is enabled successfully.



You can then log into the cnMaestro system using the same 'cambium' account used to log in through the Console.

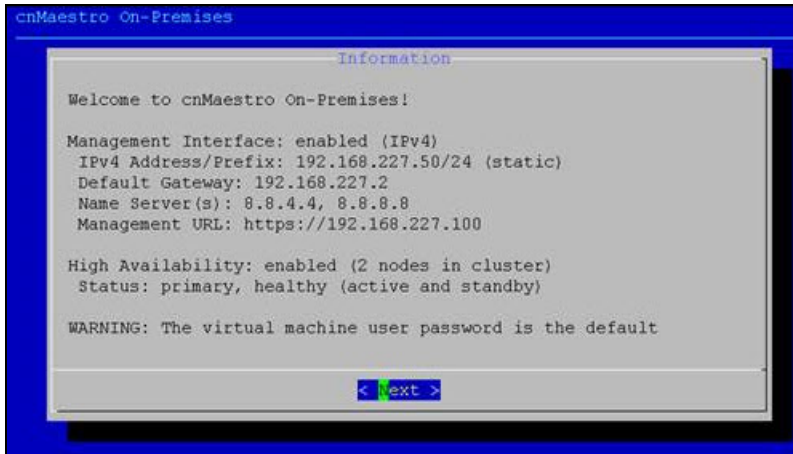
```
# ssh cambium@192.168.127.51
```



NOTE:

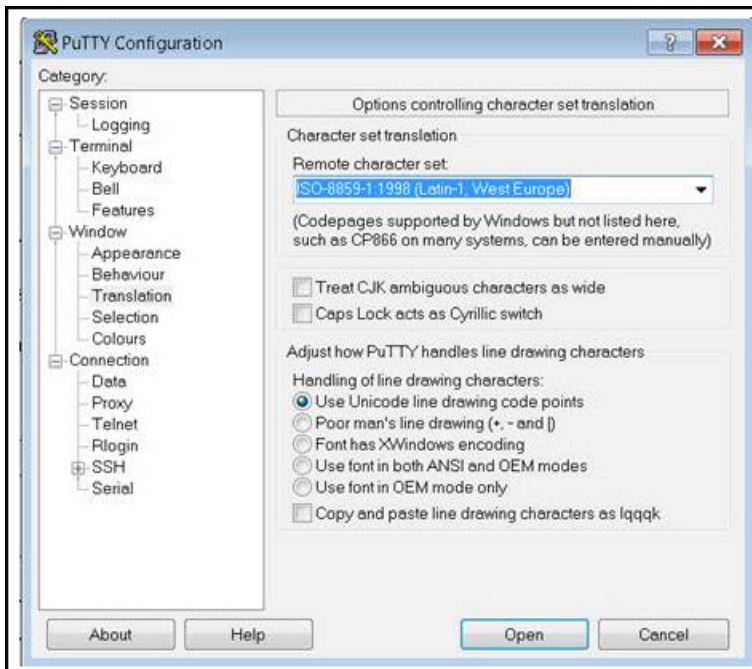
The 'cambium' user has sudo access, so if using SSH, be sure to change the default password of this user before enabling the feature.

The Windows application putty, by default, will not print the dialog correctly, and the customer needs to set the Translation accordingly.

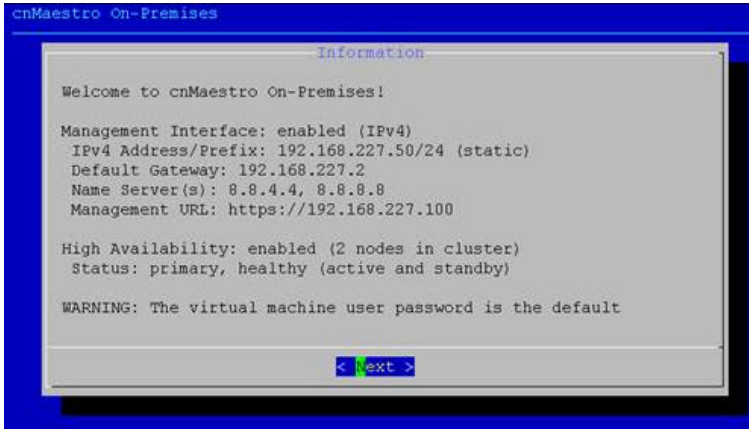


NOTE:

When accessing the CLI from putty on Windows, you may need to change the Remote Character Set (Window > Translation in the putty Configuration dialog) to "ISO-8859-1 1998 (Latin-1, West Europe)" to correctly display the menu.



After setting the configuration properly, the window appears as below:



Data Backup

Overview



NOTE:

cnMaestro backups taken from version 3.0.0 and later will only include statistics for the last month (in addition to configuration). To backup all statistics in a cnMaestro X account (up to 2 years), one needs to periodically copy the data disk outside of cnMaestro.

cnMaestro On-Premises stores its configuration and statistics on a virtual "data" disk. This disk could be tens of gigabytes in size. Backing up the disk requires snapshotting and copying it using the virtualization infrastructure.

cnMaestro configuration backups should normally be made using the standard cnMaestro backup mechanism available through the UI. When full historical data is required, a snapshot-based disk backup mechanism should be used.

cnMaestro backups

Standard cnMaestro backups are done through the cnMaestro UI. They are fast: ideal for pre-change checkpointing or upgrades. They can be executed on-demand or on a schedule, and they are a quick way to restore cnMaestro configuration. Standard backups also restore the last week of device statistics, but they do not save any Wi-Fi Client statistics.



NOTE:

Standard cnMaestro backups are performed using the cnMaestro UI.

Full Backups

Full backups copy all cnMaestro data, including configuration and long-term statistics. They can be taken from a running system, but they can only be restored when the system is shut down, because they require the data disk to be swapped.

The method of creating snapshot backups varies per virtualization technology, but the basics are the same: a point in time snapshot of the data disk is created, and the snapshot is used as the source for the backup.

If snapshot backups are taken of a running instance, the backup will be "crash consistent". This means the instance will be restored to a state similar to the instant before a power loss or reset. While small amounts of uncommitted

data may be lost, this is generally safe, because the cnMaestro data is stored transactionally. If you prefer to have a fully consistent backup, power down the instance before taking the snapshot backup. In the case of the HA cluster, always take data backup of the Primary Server only.



NOTE:

It is recommended to only use snapshot backup methods, as data is constantly being written, and backups otherwise are likely to be inconsistent or unusable.



NOTE:

Recommended HA data restore procedure is as follows:

1. Power OFF the existing Secondary Server, so that the Primary Server will be in Peer-Down state.
2. Replicate or attach the disk of the backed-up Primary Server to the newly created server.
3. After backup replication is done, Power OFF the existing Primary (cnMaestro Active) Server and Power ON the newly created server. The new server will become Primary (cnMaestro Active) in Peer-Down state.
4. Power ON the Secondary Server. HA replication will occur.

Virtualization System specific Backup Methods

VMware

Dedicated backup software for either VMware or your datastore device is recommended. A basic disk clone backup without additional backup software can be performed through the following:

- Delete all existing snapshots
- Create a new snapshot of the disk
- Clone the disk using [vmkfstools](#)
- Delete the snapshot

Disk clone backup using additional backup software can be performed using this alternatives [Veeam Backup & Replication](#) or [Vinchin Backup](#).

Standard snapshot-based backups work with existing VMware-supported backup tools, and are likely to work with your existing backup solution. It is not recommended attempting to backup snapshot or disk files directly from storage.



NOTE:

The backup process will consume resources and may impact performance of all VMs, henceforth plan backup accordingly. Initial full backups are likely to take a long time depending on disk size and type.

Hyper-V

It is recommended to use dedicated backup software for Hyper-V, a basic crash-consistent disk backup can be made using either Hyper-V manager or ([Export-VM](#)). There are a number of backup solutions available, if snapshot backup is supported it will successfully backup cnMaestro data disks. Test your backup solution before starting backup process. If you do not have an existing backup solution for your VMs, disk backup using additional software using the alternatives such as [Veeam Backup & Replication](#) or [Vinchin Backup](#).

Citrix Hypervisor (XenServer)

To backup Citrix Hypervisor refer [Back up and restore hosts and VMs](#). There are a number of backup solutions available, if snapshot backup is supported it will successfully backup cnMaestro data disks. Test your backup solution before starting backup process. If you do not have an existing backup solution for your VMs, disk backup using additional software using the alternative such as [Vinchin Backup](#).

Extending the Data Disk

cnMaestro has two virtual disks, one for the operating system, and the second for data. If the data disk becomes overloaded, it can be extended. This is done by increasing the disk size through the virtual machine, and then following the command line instructions in this guide.

The process will have two phases:

- Phase 1: Expand the virtual disk (using the virtual machine infrastructure).
- Phase 2: Extend the cnMaestro partition and file system (using the command line instructions listed below).

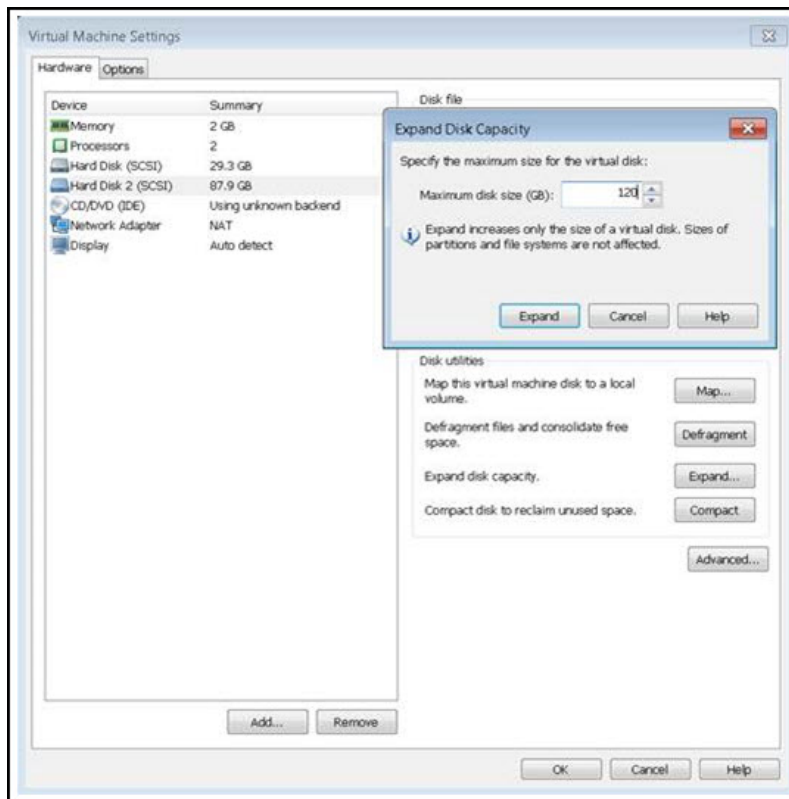


NOTE:

Please take a backup copy of your virtual machine before performing any operations below.

VMware Workstation Disk Expansion

To expand the virtual disk in VMware Workstation, make sure the virtual machine has no VMware snapshots and is currently turned off. You can then select Hard Disk 2 and click **Expand** to select a new disk size. Only expansion is allowed (the data disk can grow but not shrink). An Expand Disk Capacity window launches to update the size. Once a new disk size is chosen, restart cnMaestro. A similar mechanism is used for ESXi.



VirtualBox Disk Expansion

VirtualBox requires command line expansion of the virtual disk. One also needs to convert the disk format from VMDK to VDI before the transformation, and then back again when finished. The commands below are for the Windows installation of VirtualBox. The steps are to convert to VDI; then resize the VDI disk; then convert back to VMDK.

Once the resized.vmdk is created, replace the current Disk 2 in the VirtualBox UI with the resized vmdk and restart the virtual machine.

```
> "C:\Program Files\Oracle\VirtualBox\VBoxManage" clonehd source.vmdk clone.vdi --format vdi
> "C:\Program Files\Oracle\VirtualBox\VBoxManage" modifyhd clone.vdi --resize 120000
> "C:\Program Files\Oracle\VirtualBox\VBoxManage" clonehd clone.vdi resized.vmdk --format vmdk
```

Once the resized.vmdk is created, replace the current Disk 2 in the VirtualBox UI with the resized vmdk and restart the virtual machine.

Partition and File System Updates

cnMaestro will not recognize the additional disk space until the partition is extended. So after the reboot, launch the cnMaestro CLI and select **Shell** to exit to the command line. There type the following commands to grow the partition and file system disk; then convert back to VMDK.

```
$ sudo growpart /dev/sdb 1
$ sudo resize2fs /dev/sdb1
```

You can validate the command completed successfully by typing `df -k` and reviewing the size of `/dev/sdb1 (/mnt/data)`.

```
cambium@cnmaestro:~$ df -k
Filesystem            1K-blocks    Used Available Use% Mounted on
udev                  1003608         0   1003608   0% /dev
tmpfs                  204800    10272   194528   6% /run
/dev/mapper/cnmaestro--vg-root 28377236 3622112 23290600  14% /
tmpfs                  1023992         4   1023988   1% /dev/shm
tmpfs                   5120         0     5120   0% /run/lock
tmpfs                  1023992         0   1023992   0% /sys/fs/cgroup
/dev/sda1              736752    106512   592816  16% /boot
/dev/sdb1             125783080  429028 125354052   1% /mnt/data
tmpfs                   204800         0     204800   0% /run/user/1000
```

Account Recovery

cnMaestro has two types of accounts: the Virtual Machine (Console) account and the cnMaestro Application account. Both of these can be recovered if the administrator password is lost.

Virtual Machine (Console) Account Recovery

cnMaestro is installed on Ubuntu Server and can leverage the Ubuntu Recovery Mode process to reset the "Cambium Networks" Console login password. The steps are the following:

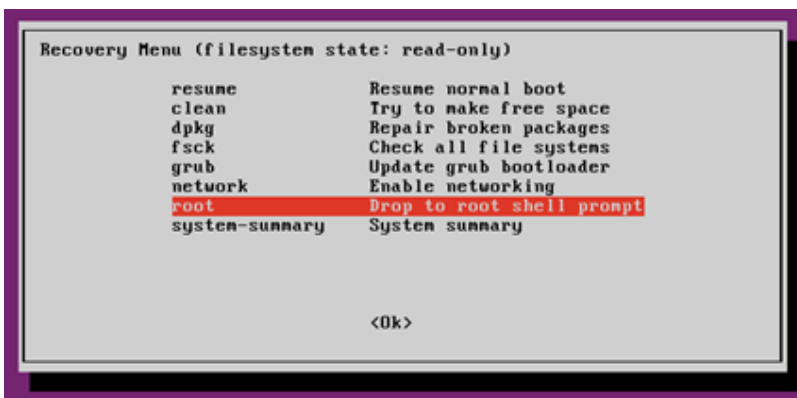
1. When booting up cnMaestro in the VM Console after a full shutdown, quickly press and hold the Shift key after the BIOS has finished loading. This will launch the GNU GRUB menu.



2. Select Advanced Options and then Ubuntu Recovery Mode



3. Once in the Recovery Menu, select the **root** option to enter a root shell

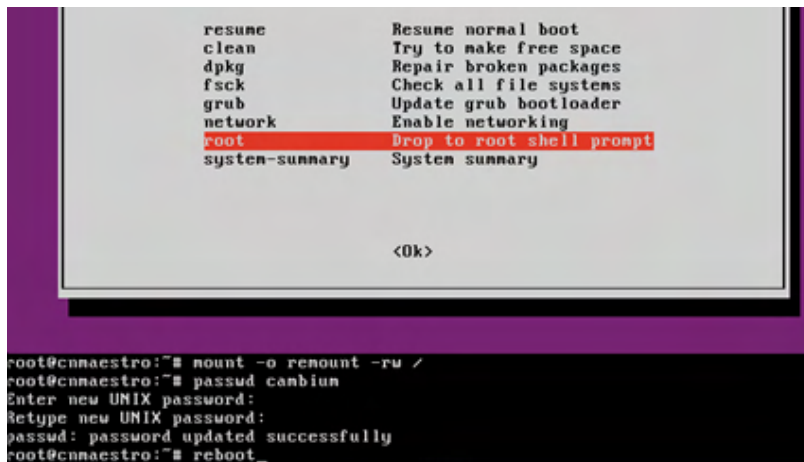


4. The shell will display a command parser along the bottom of the screen. Type the following (without the '#') to reset the password of the **cambium** user.

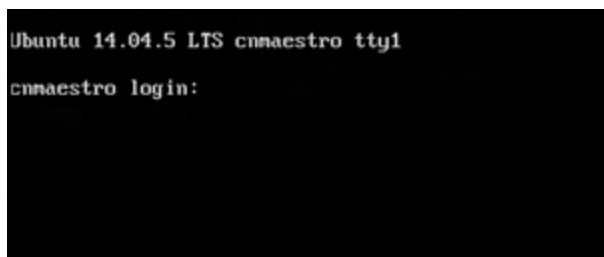
```

# mount -o remount -rw /
# passwd cambium
# reboot

```

5. You should now be able to login to the console using the new password.



cnMaestro Application Account Recovery

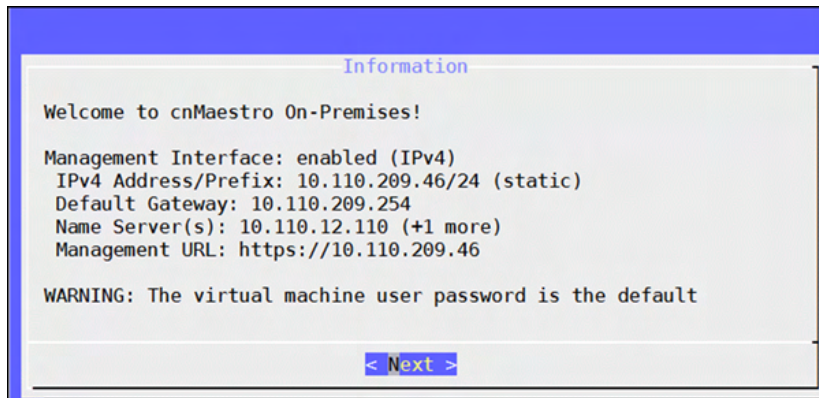
Application Account recovery is useful if you are unable to log in to the cnMaestro UI. It allows you to create a one-time password through the command line, so you can access the UI as a Super Administrator and update current authentication settings.

Application Account Recovery

Console administrators can create a one-time password providing Super Administrator access to the cnMaestro UI for a single session (the password will expire in one hour or after a single use). This is a fail safe mechanism that allows cnMaestro access to update current authentication settings.

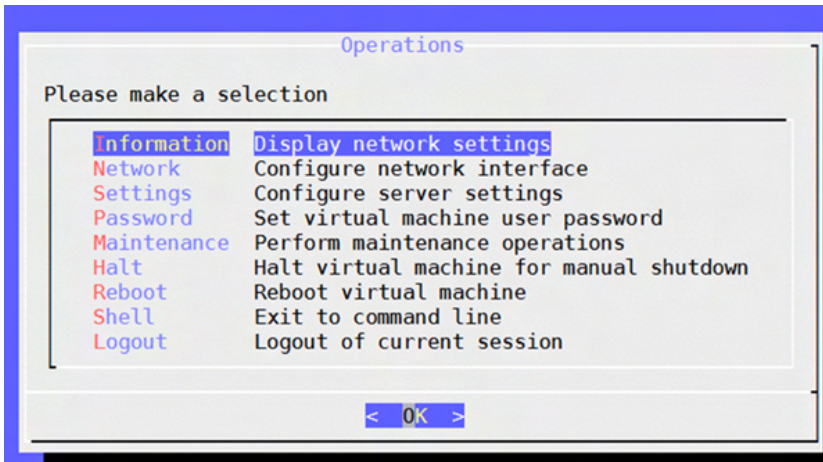
To create a one-time password:

1. Log into the cnMaestro Console and following window pops-up:

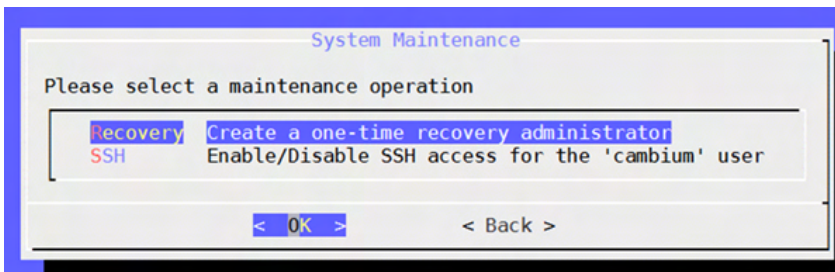


2. Click **Next**.

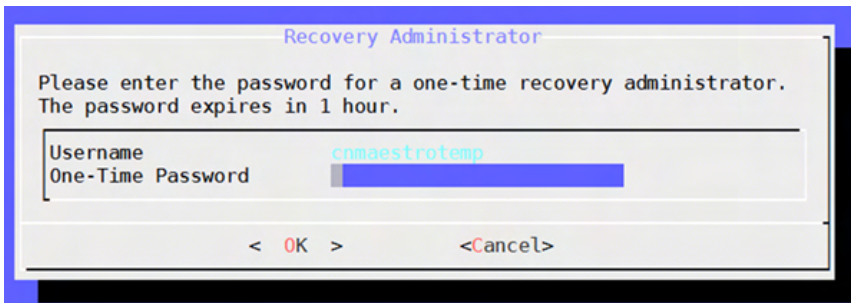
3. Select **Information** and click **Ok**.



4. Select **Recovery** tab and click **Ok**.



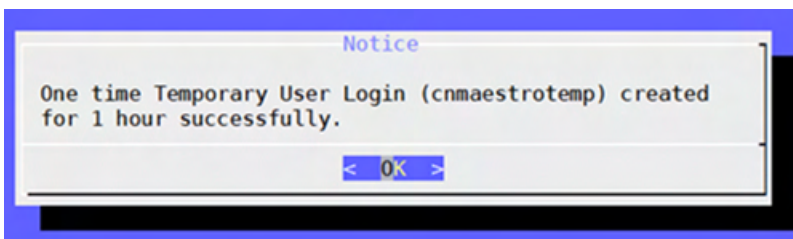
5. Enter the password in the **OneTime Password** text box.



NOTE:

The username for temporary user login is **cnmaestrotemp**. It cannot be changed.

6. Click **OK**. The following window is displayed:



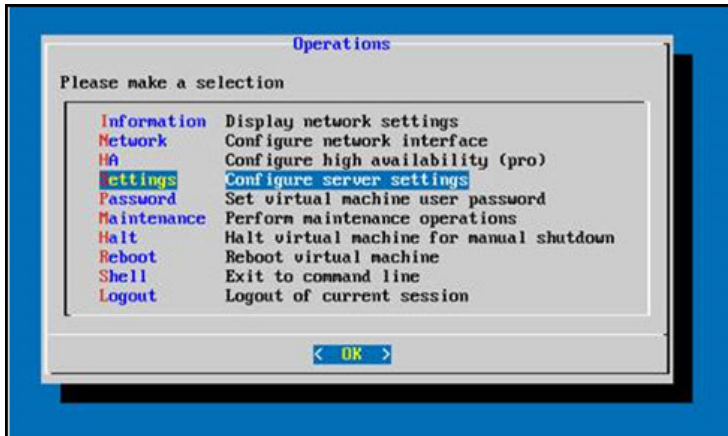
Configure Network Time Protocol (NTP)

cnMaestro uses NTP for time synchronization. This is particularly important for HA environments. By default, NTP is configured to use Google NTP services. NTP can be disabled, if one wants to leverage the NTP feature of VMware, or changed to enable a customized group of NTP servers.

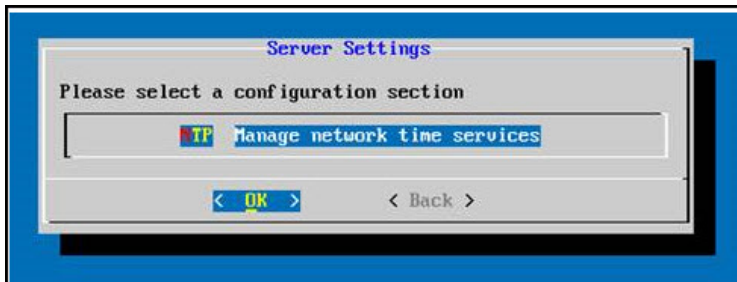
Disabling NTP Support

Follow the below steps to disable NTP Support:

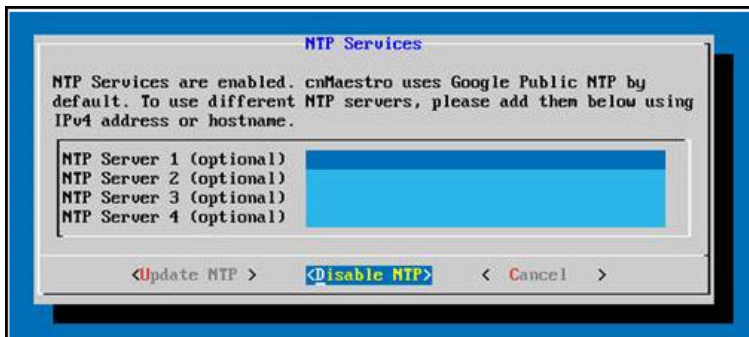
1. From the **Operations** page, select **Settings**.



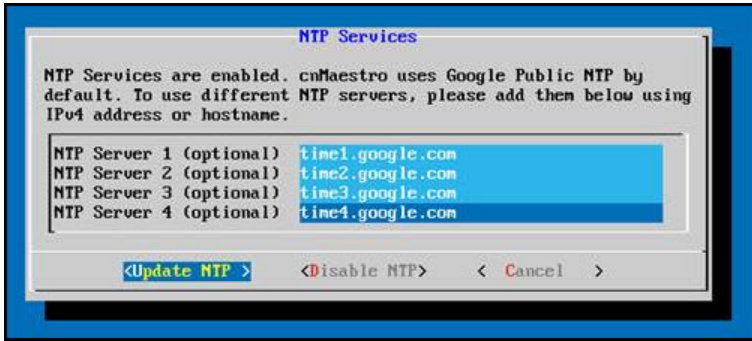
2. Select NTP to **Manage Network Time Services**.



3. To disable NTP, select the **Disable NTP** Option.



4. Set custom NTP servers and Update NTP.



Statistics API Response (v1 Format)

API v1 is replaced by v2 in cnMaestro 3.0.0 release. It will be supported from cnMaestro 3.2.0 release and no longer be supported.

This section provides the Statistics API response v1 Format for the following devices:

- [cnMatrix](#)
- [cnReach](#)
- [Fixed Wireless](#)
- [PTP](#)
- [Wi-Fi](#)

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
mode	Device mode
name	Device name
network	Network
site	Site name
site_id	Site unique identifier
status	Status [online, offline, claimed, waiting, onboarding]

Name	Details
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
ip_wan	WAN IP	All

Radios

Name	Details	Mode
radio.radio1.device_id	Device ID	Radios
radio.radio1.linked_with	Linked with	Radios
radio.radio1.mac	Radio MAC	Radios
radio.radio1.margin	Margin	Radios
radio.radio1.mode	Radio mode [ap, ep, rep]	Radios
radio.radio1.neighbors	Radio neighbors	Radios
radio.radio1.network_address	Network address	Radios
radio.radio1.noise	Average noise (dB)	Radios
radio.radio1.power	Transmit power	Radios
radio.radio1.rssi	RSSI value (dB)	Radios
radio.radio1.rx_bytes	Receive bytes	Radios
radio.radio1.software_version	Current software version.	Radios
radio.radio1.temperature	Radio temperature	Radios
radio.radio1.tx_bytes	Transmit bytes	Radios
radio.radio1.type	Radio type [ptp, ptmp]	Radios
radio.radio2.device_id	Device ID	Radios
radio.radio2.linked_with	Linked with	Radios
radio.radio2.mac	Radio MAC	Radios
radio.radio2.margin	Margin	Radios
radio.radio2.mode	Radio mode [ap, ep, rep]	Radios
radio.radio2.neighbors	Radio neighbors	Radios
radio.radio2.network_address	Network address	Radios
radio.radio2.noise	Average noise	Radios
radio.radio2.power	Transmit power	Radios

Name	Details	Mode
radio.radio2.rssi	RSSI value (dB)	Radios
radio.radio2.rx_bytes	Receive bytes	Radios
radio.radio2.software_version	Radio current software version.	Radios
radio.radio2.temperature	Radio temperature	Radios
radio.radio2.tx_bytes	Transmit bytes	Radios
radio.radio2.type	Radio type [ptp, ptmp]	Radios

Fixed Wireless

General

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

Name	Details	ePMP	PMP
temperature	Temperature		AP/SM
tower	Tower name	AP	AP
vlan	VLAN		AP/SM

Networks

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

Radios

Name	Details	ePMP	PMP
radio.auth_mode	Authentication mode	SM	
radio.auth_type	Authentication type ePMP [open, wpa1, eap- ttls] PMP [disabled, enabled]	AP/SM	AP/SM
radio.channel_width	Channel width ePMP [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP [...]	AP/SM	AP/SM
radio.color_code	Color code		AP/SM
radio.dfs_status	DFS status ePMP:	AP/SM	AP/SM

Name	Details	ePMP	PMP
	[not-applicable, channel-availability-check, in-service, radar-signal-detected, alternate-channel-monitoring, not-in-service] PMP: [Status String]		
radio.dl_err_drop_pkts	Downlink error drop packets	SM	
radio.dl_err_drop_pkts_percentage	Downlink error drop packets percentage	SM	
radio.frequency	RF frequency	AP/SM	AP/SM
radio.frame_period	Frame period		AP
radio.dl_frame_utilization	Downlink frame utilization		AP
radio.dl_lqi	Downlink Link Quality Indicator		SM
radio.dl_mcs	Downlink MCS	SM	
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	Downlink Retransmission	AP/SM	
radio.dl_retransmits_pct	Downlink Retransmission percentage	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance		AP
radio.dl_snr	Downlink SNR (dB)	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
radio.mac	Wireless MAC	AP/SM	
radio.mode	Radio mode [eptp-master, eptp-slave, tdd, tdd-ptp, ap/sm]	AP/SM	
radio.sessions_dropped	Session drops	AP	AP/SM

Name	Details	ePMP	PMP
radio.software_key_throughput	Software key - max throughput		SM
radio.ssid	SSID	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
radio.tx_capacity	SM transmit capacity	SM	
radio.tx_power	Radio transmit power	AP/SM	AP/SM
radio.tx_quality	SM transmit quality	SM	
radio.ul_err_drop_pkts	Uplink error drop packets	SM	
radio.ul_err_drop_pkts_percentage	Uplink error drop packets percentage	SM	
radio.ul_frame_utilization	Uplink frame utilization		AP
radio.ul_mcs	Uplink MCS	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
radio.ul_pkts_loss	Uplink packet loss		AP/SM
radio.ul_retransmits	Uplink Retransmission	SM	
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM
radio.ul_snr	Uplink SNR (dB)	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
radio.wlan_status	WLAN status [down, up]	AP/SM	

PTP

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

Radios

Name	Details	Mode
ethernet.aux_ interface.rx_frames	Aux Rx Frames Oversize	All
ethernet.aux_ interface.tx_util	Aux Tx Bandwidth Utiliization	All
ethernet.aux_ interface.rx_util	Aux Rx Bandwidth Utiliization	All
ethernet.aux_ interface.speed	Aux speed and duplex	All
ethernet.main_psu_ interface.rx_frames	Main PSU Rx Frames Oversize	All
ethernet.main_psu_ interface.rx_util	Main PSU Rx Bandwidth Utiliization	All
ethernet.main_psu_ interface.speed	Main PSU speed and duplex	All
ethernet.main_psu_ interface.tx_util	Main PSU Tx Bandwidth Utiliization	All
ethernet.sfp_interface.rx_ frames	SFP Rx Frames Oversize	All
ethernet.sfp_interface.rx_ util	SFP Rx Bandwidth Utiliization	All
ethernet.sfp_ interface.speed	SFP speed and duplex	All
ethernet.sfp_interface.tx_ util	SFP Tx Bandwidth Utiliization	All
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

Name	Details	Mode
radio.rx_frequency	Receive frequency	All
radio.tx_frequency	Transmit frequency	All
radio.tx_power	Radio transmit power	All

Wi-Fi

	<p>NOTE: Mode is Enterprise, Home, or All.</p>
---	---

General

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

Network

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

Name	Details	Mode
radio.24ghz.airtime	Airtime	All
radio.24ghz.bssid	Radio mac	Enterprise
radio.24ghz.channel	Channel	All
radio.24ghz.multicast_rate	Multicast rate	All
radio.24ghz.noise_floor	Noise floor	All
radio.24ghz.num_clients	Number of clients	All
radio.24ghz.num_wlans	Number of WLANs	Enterprise
radio.24ghz.power	Transmit power	All
radio.24ghz.quality	RF Quality description	Enterprise
radio.24ghz.radio_state	Radio state	Enterprise
radio.24ghz.rx_bps	Receive bits/second	Enterprise
radio.24ghz.rx_bytes	Receive bytes	All

Name	Details	Mode
radio.24ghz.tx_bps	Transmit bits/second	Enterprise
radio.24ghz.tx_bytes	Transmit bytes	All
radio.24ghz.unicast_rates	Unicast rates	All
radio.24ghz.utilization	Radio utilization	Enterprise
radio.5ghz.airtime	Airtime	All
radio.5ghz.bssid	Radio mac	Enterprise
radio.5ghz.channel	Channel	Enterprise
radio.5ghz.multicast_rate	Multicast rate	All
radio.5ghz.noise_floor	Noise floor	All
radio.5ghz.num_clients	Number of clients	Enterprise
radio.5ghz.num_wlans	Number of WLANs	Enterprise
radio.5ghz.power	Transmit power	All
radio.5ghz.quality	RF quality description	Enterprise
radio.5ghz.radio_state	Radio state	Enterprise
radio.5ghz.rx_bps	Receive bits/second	Enterprise
radio.5ghz.rx_bytes	Receive bytes	All
radio.5ghz.tx_bps	Transmit bits/second	Enterprise
radio.5ghz.tx_bytes	Transmit bytes	All
radio.5ghz.unicast_rates	Unicast rates	All
radio.5ghz.utilization	Radio utilization	Enterprise

Performance API Response (v1 Format)

This section provides the performance API response v1 Format for the following devices:

- [cnMatrix](#)
- [cnReach](#)
- [Fixed Wireless](#)
- [PTP](#)
- [Wi-Fi](#)

General

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

Switch

Name	Details
switch.rx.broadcast_pkts	Receive broadcast packets
switch.dl_kbits	Downlink usage (in kbits on hour or minute basis)
switch.dl_throughput	Downlink throughput (Kbps)
switch.ul_kbits	Uplink (in Kbits on hour or minute basis)
switch.rx.multicast_pkts	Receive multicast packets
switch.ul_throughput	Uplink throughput (Kbps)
switch.rx.pkts_err	Receive Packet error
switch.rx.unicast_pkts	Receive unicast packets
switch.tx.broadcast_pkts	Transmit broadcast packets
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
site	Site	All
sm_count	Connected SM count	All
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios

Name	Details	Mode
radio.radio1.neighbors	Radio neighbors	Radios
radio.radio1.noise	Average noise	Radios
radio.radio1.power	Transmit power	Radios
radio.radio1.rssi	RSSI value	Radios
radio.radio1.rx_bytes	Receive bytes	Radios
radio.radio1.throughput	Total throughput	Radios
radio.radio1.tx_bytes	Transmit bytes	Radios
radio.radio2.neighbors	Radio neighbors	Radios
radio.radio2.noise	Average noise	Radios

Name	Details	Mode
radio.radio2.power	Transmit power	Radios
radio.radio2.rssi	RSSI value	Radios
radio.radio2.rx_bytes	Receive bytes	Radios
radio.radio2.throughput	Total throughput	Radios
radio.radio2.tx_bytes	Transmit bytes	Radios

Fixed Wireless

General

Name	Details	ePMP	PMP
mac	MAC address	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM
network	Network	AP/SM	AP/SM
online_duration	Duration of device connection with server (seconds)	AP/SM	AP/SM
sm_count	Connected SM count	AP	AP
sm_drops	Session drops	AP/SM	AP
timestamp	Timestamp	AP/SM	AP/SM
tower	Tower	AP/SM	AP/SM
type	Device type	AP/SM	AP/SM
uptime	Device online time (seconds)	AP/SM	AP/SM

Radios

Name	Details	ePMP	PMP
radio.dl_frame_utilization	Downlink frame utilization		AP
radio.dl_kbits	Downlink usage (in Kbits on hour or minute basis)	AP/SM	
radio.dl_mcs	Downlink MCS	SM	

Name	Details	ePMP	PMP
radio.dl_modulation	Downlink modulation		SM
radio.dl_pkts	Downlink packet count	AP/SM	
radio.dl_pkts_loss	Downlink packet loss		AP/SM
radio.dl_retransmits_pct	Downlink retransmission percentage	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance		SM
radio.dl_snr	Downlink SNR	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
radio.ul_frame_utilization	Uplink frame utilization		AP
radio.ul.kbits	Uplink usage (in Kbits on hour or minute basis)	AP/SM	
radio.ul_mcs	Uplink MCS	SM	
radio.ul_modulation	Uplink modulation		SM
radio.ul_pkts	Uplink packet count	AP/SM	
radio.ul_pkts_loss	Uplink packet loss		AP/SM
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM
radio.ul_snr	Uplink SNR	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

PTP

General

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

Ethernet

Name	Details	Mode
ethernet.aux_ interface.max_rx	AUX maximum receive bytes	All
ethernet.aux_ interface.max_tx	AUX maximum transmit bytes	All
ethernet.aux_ interface.min_rx	AUX minimum receive bytes	All
ethernet.aux_ interface.min_tx	AUX minimum transmit bytes	All
ethernet.aux_ interface.pkt_error	AUX packet error	All
ethernet.aux_interface.rx	AUX receive bytes	All
ethernet.aux_interface.tx	AUX transmit bytes	All
ethernet.link_loss	Link loss	All
ethernet.main_psu_ interface.max_rx	Main PSU maximum receive bytes	All

Name	Details	Mode
ethernet.main_psu_interface.max_tx	Main PSU maximum transmit bytes	All
ethernet.main_psu_interface.min_rx	Main PSU minimum receive bytes	All
ethernet.main_psu_interface.min_tx	Main PSU minimum transmit bytes	All
ethernet.main_psu_interface.pkt_error	Main PSU packet error	All
ethernet.main_psu_interface.rx	Main PSU receive bytes	All
ethernet.main_psu_interface.tx	Main PSU transmit bytes	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.rx_throughput	Receive throughput	All
ethernet.sfp_interface.max_rx	SFP maximum receive bytes	All
ethernet.sfp_interface.max_tx	SFP maximum transmit bytes	All
ethernet.sfp_interface.min_rx	SFP minimum receive bytes	All
ethernet.sfp_interface.min_tx	SFP minimum transmit bytes	All
ethernet.sfp_interface.pkt_error	SFP packet error	All
ethernet.sfp_interface.rx	SFP receive bytes	All

Name	Details	Mode
ethernet.sfp_interface.tx	SFP transmit bytes	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

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

Name	Details	Mode
radio.24ghz.clients	Number of clients	All
radio.24ghz.rx_bps	Receive bits/second	Enterprise
radio.24ghz.throughput	Total throughput	All
radio.24ghz.tx_bps	Transmit bits/second	Enterprise

Name	Details	Mode
radio.5ghz.clients	Number of clients	All
radio.5ghz.rx_bps	Receive bits/second	Enterprise
radio.5ghz.throughput	Total throughput	All
radio.5ghz.tx_bps	Transmit bits/second	Enterprise

Deployments

VMware ESXi Installation

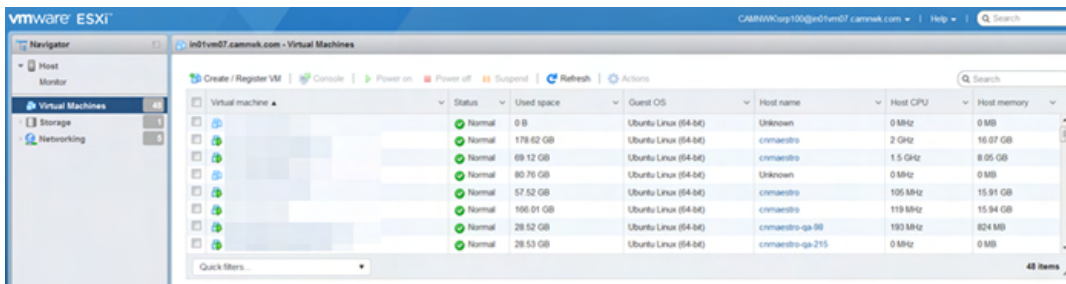


NOTE:

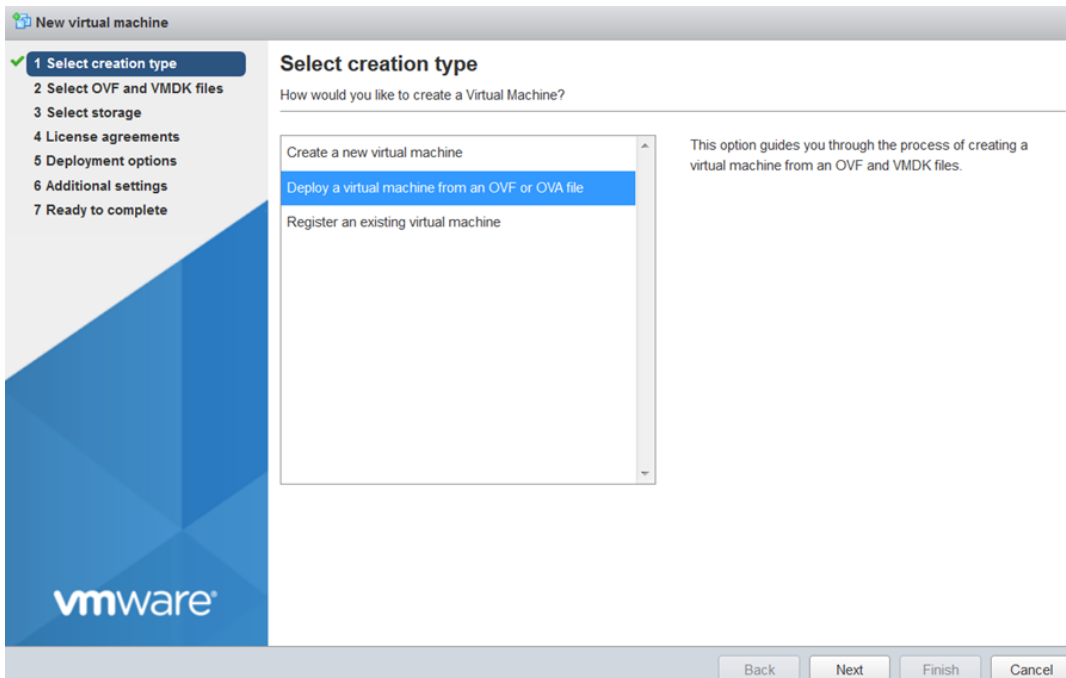
Deploying ESXi is an involved process. The steps below assume you have VMware ESXi version 6.0.0 Update 3 (Build 7967664) or higher already installed on hardware. If you don't have an ESXi hypervisor available, you can download it from VMware website. VMware provides directions for installing the ESXi ISO on a server.

cnMaestro VM Deployment

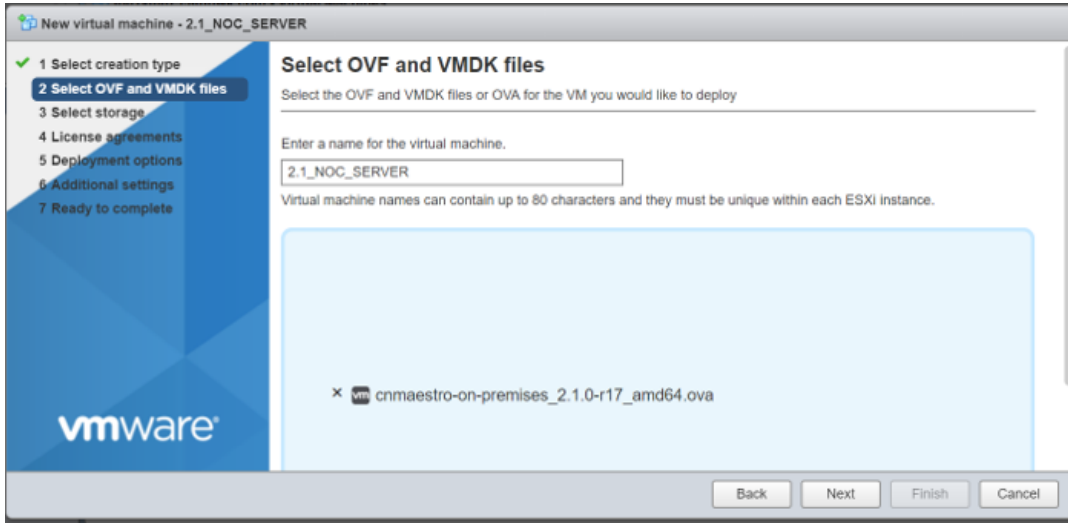
1. Login into ESXi host.
2. Click **Virtual Machines**.



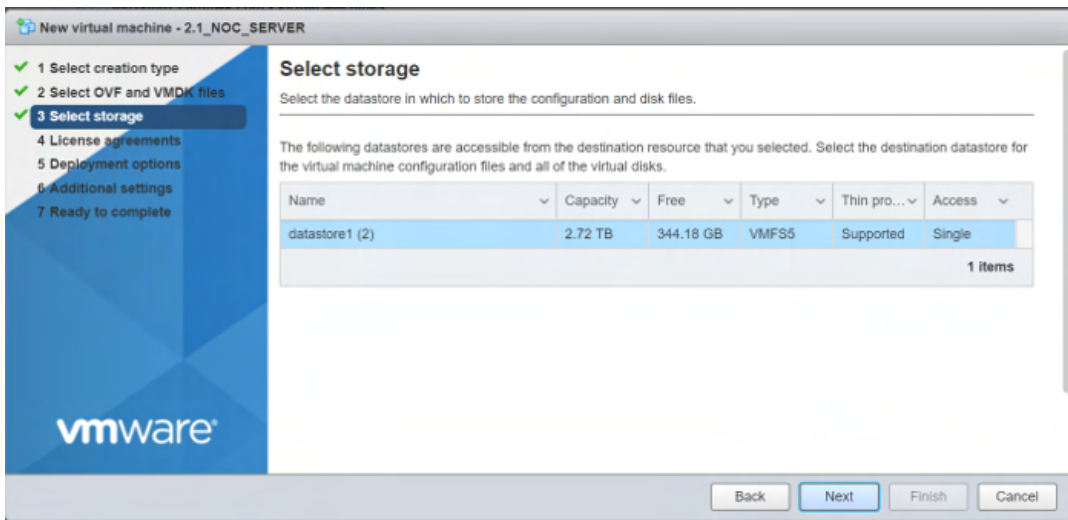
3. Click **Create/Register VM**.



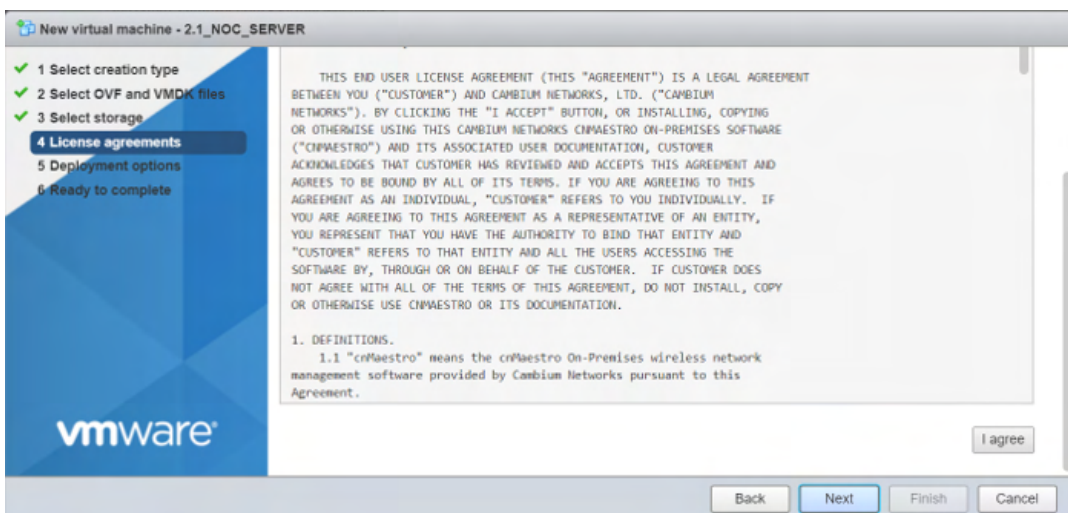
4. Click **Next**.



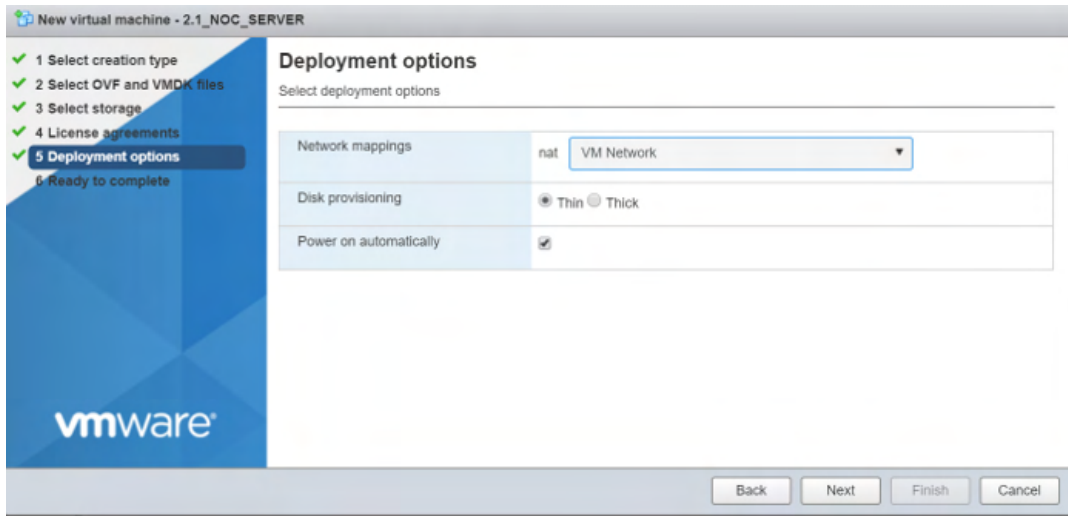
4. Select datastore which has more space



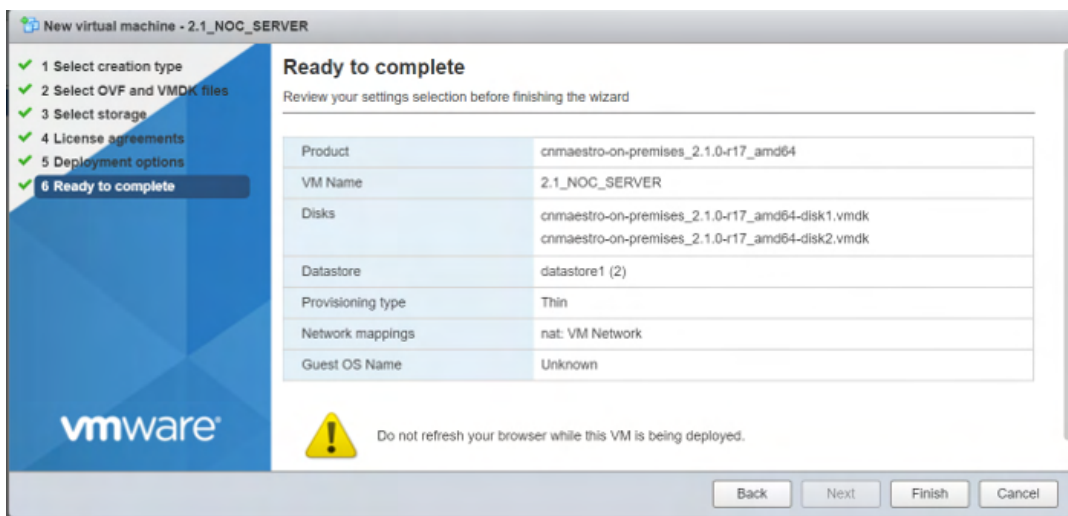
5. Click **Next**.



6. Click **I Agree** the license agreements and click **Next**.

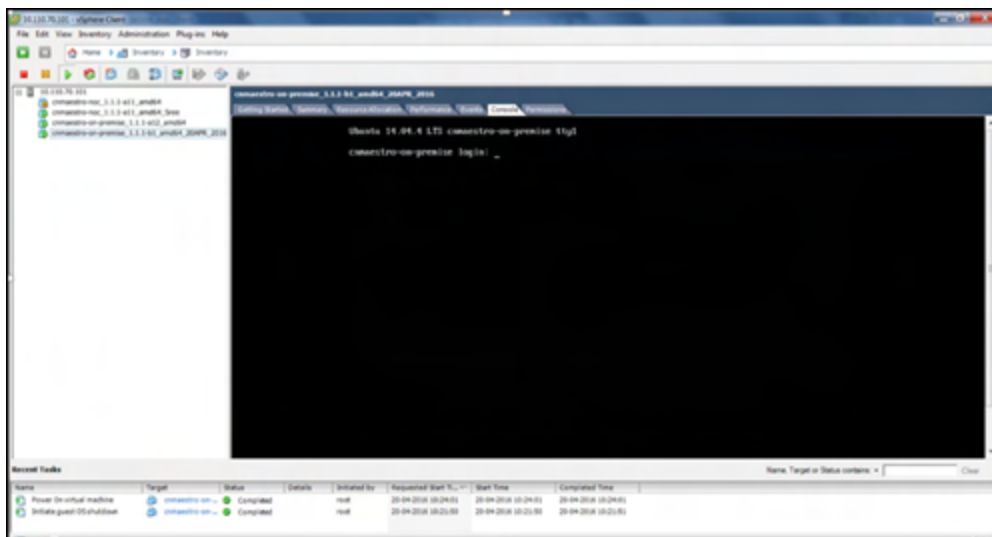


7. Select the network and click **Next**.



8. Verify the details and click **Finish** to complete deployment.

9. When the loading is complete, a virtual machine with the name chosen will appear. Choose the VM and click **power on** button.



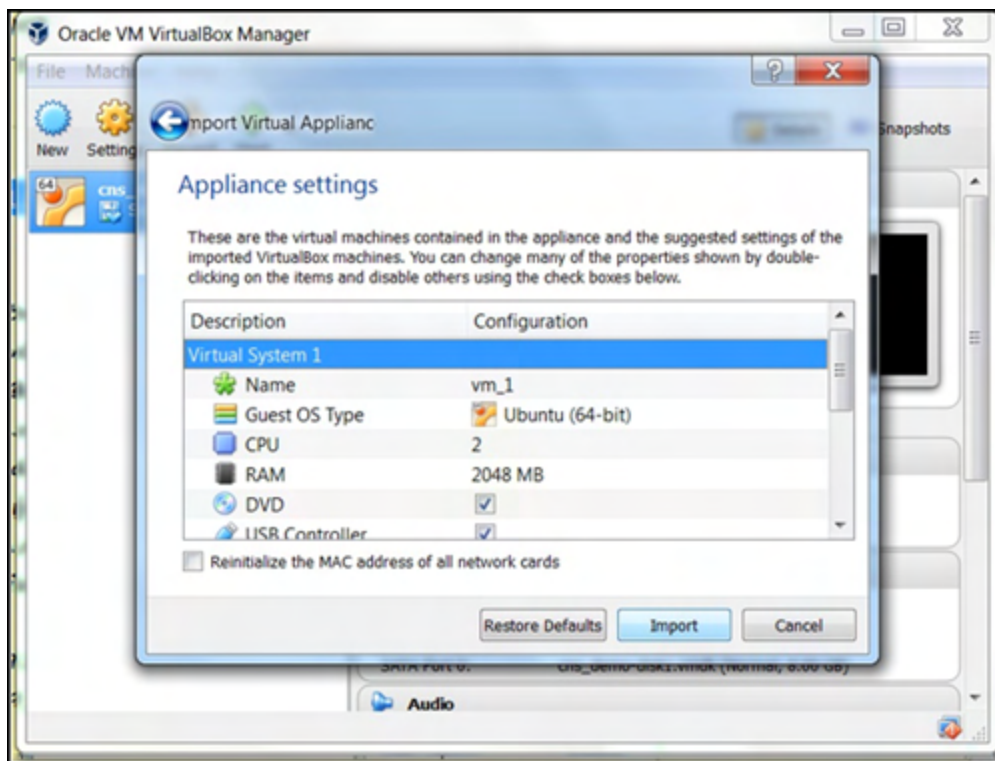
10. Enter the default credentials (cambium/cnmaestro) in the console tab.

Oracle VirtualBox 5 Installation

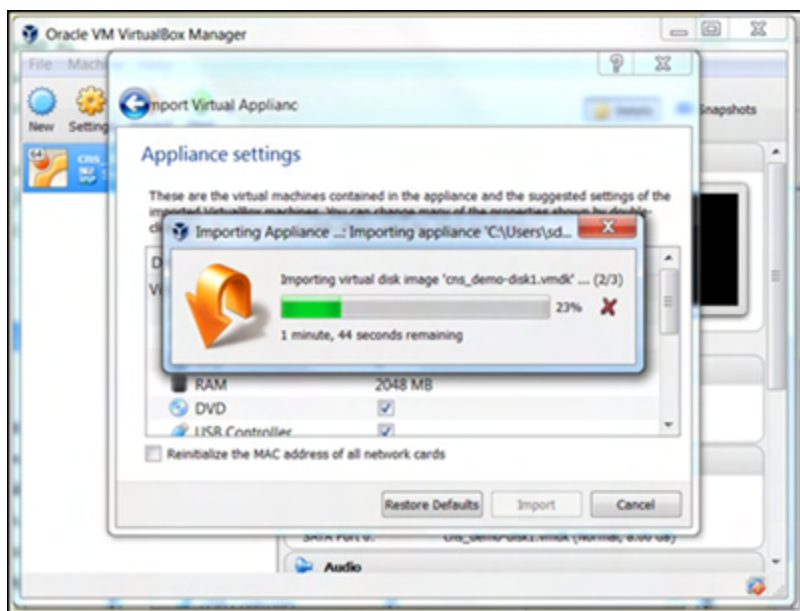
Deployment

The steps to import cnMaestro On-Premises into Oracle VirtualBox are below. VirtualBox is not recommended for a production environment.

1. Open Oracle VirtualBox Manager, and select **File > Import Appliance**.
2. Browse and select CnMaestro On-Premises release OVA file and click **Next** to continue.
3. Configure the resources required for the VM.

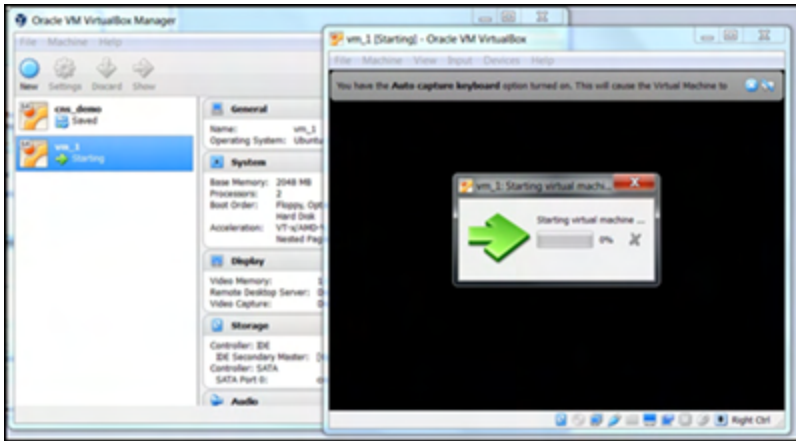


4. Click **Import**.



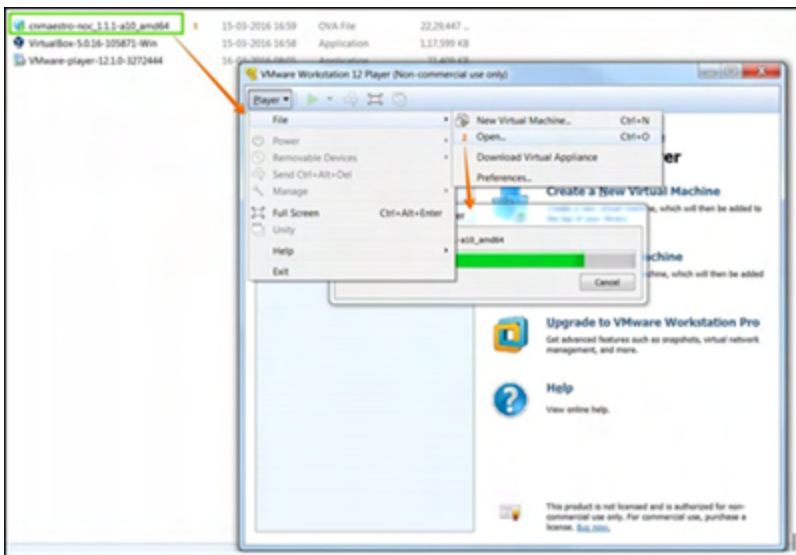
5. The new VM will appear on the left panel. Select the VM and click **start VM** and navigates to the configuration screen.

The new virtual machine appears in the left panel. After the VM is started, customer gets the login screen, and continue to configure cnMaestro and access the UI.

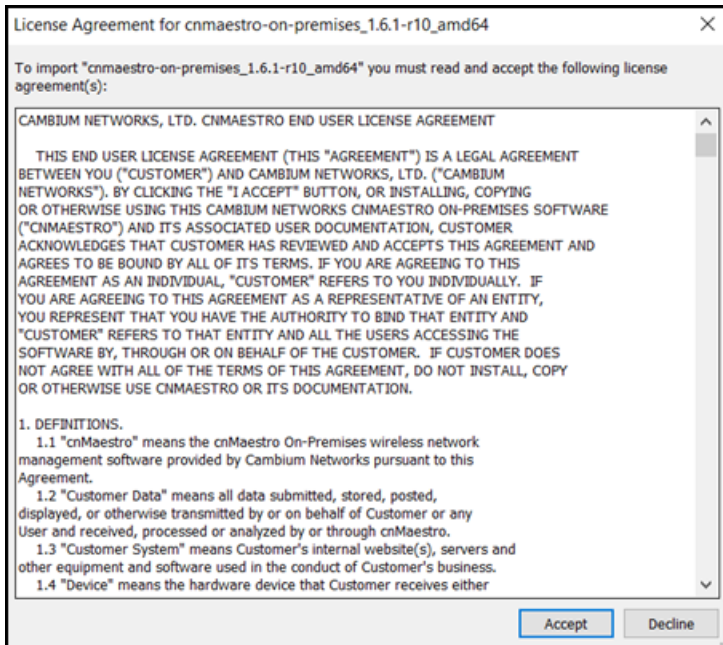


VMWare Workstation

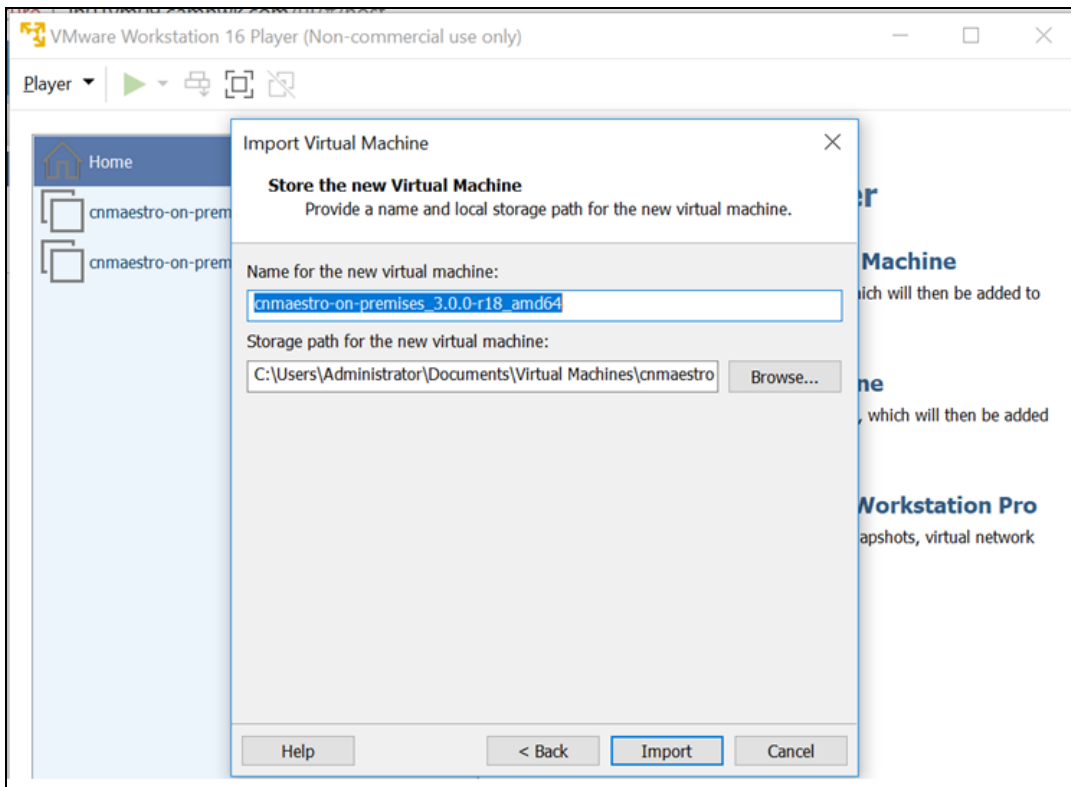
1. Open VMware workstation player. Navigate to **Player > File > Open Menu** and select CnMaestro On-Premises release OVA file.



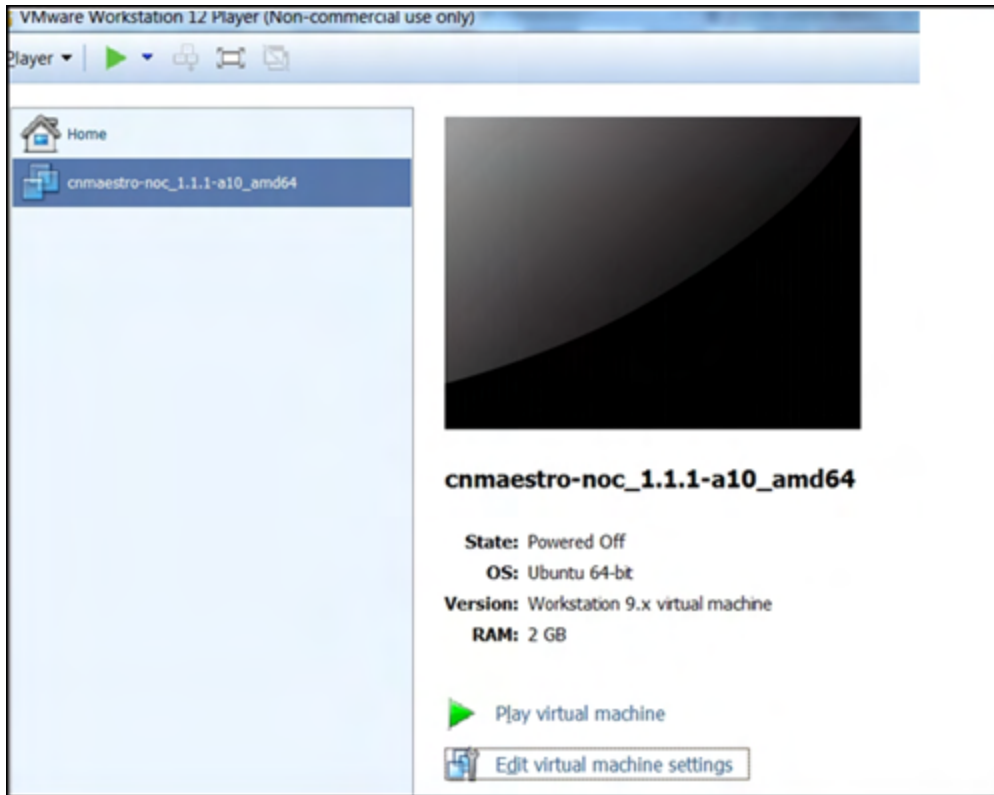
2. Accept the cnMaestro EULA, once the EULA is accepted, cnMaestro will be imported into the VM environment and it could take a couple minutes.



3. Click **Import** to start the deployment.



4. Once the file is loaded, click **Play** and wait for the configuration screen.



KVM Installation



NOTE:

KVM is not officially recommended for cnMaestro deployment. The directions below are for customers who want to evaluate the system in a KVM 0.9.5 or later environment.

Deployment

After installing KVM on the hardware, follow the below steps to import cnMaestro On-Premises into KVM:

1. Extract cnMaestro On-Premise OVA

```
$ tar xvf cnmaestro-on-premises_1.2.1-b19_amd64.ova
```

```
cnmaestro-on-premises_1.2.1-b19_amd64.ovf
```

```
cnmaestro-on-premises_1.2.1-b19_amd64.mf
```

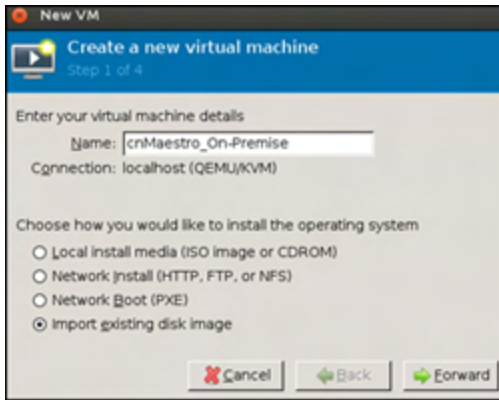
```
cnmaestro-on-premises_1.2.1-b19_amd64-disk1.vmdk
```

2. Convert vmdk image to qcow2

```
$ qemu-img convert -O qcow2 cnmaestro-on-premises_1.2.1-b19_amd64-disk1.vmdk cnmaestro-on-premises_1.2.1-b19_amd64.qcow
```

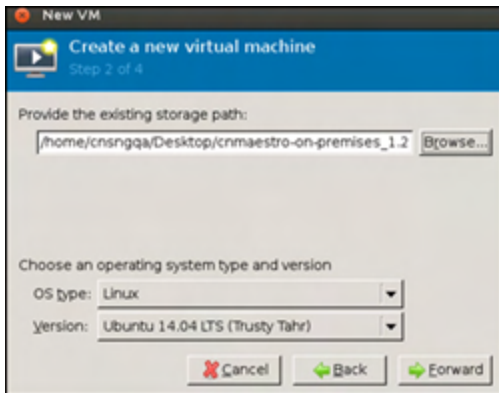
3. Create New VM

- a. Launch Virtual Machine manager.
- b. Create new VM.
- c. Choose **import existing disk image**.
- d. Click **Forward**.



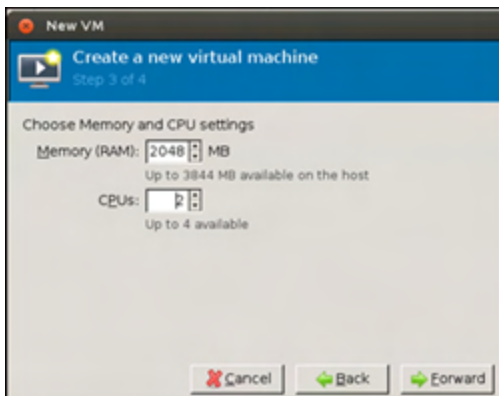
4. Select disk image file

- a. Choose **qcow2** image that is created in earlier steps.
- b. Select OS type as **Linux**
- c. Click **Forward**.



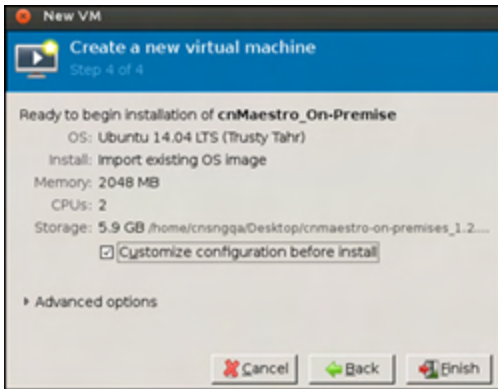
5. Configure Memory and CPU

Configure Memory and CPU settings as per the requirements.



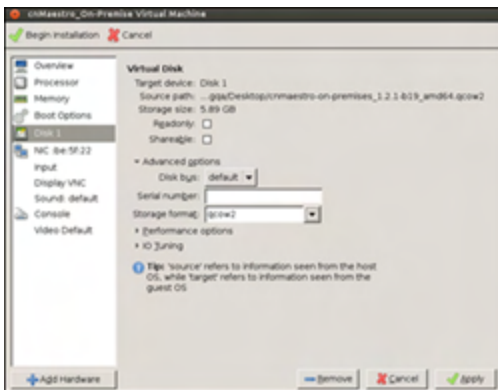
6. Customize other VM Configuration

- a. Select **Customize Configuration before install** check box
- b. Click **Finish**.



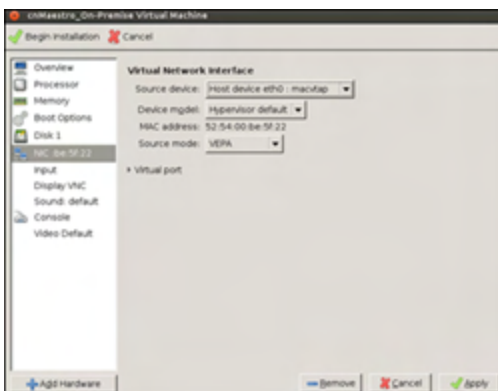
7. Set Disk format to qcow2

- a. Select **Disk** from the options on the left side.
- b. Expand **Advance options** section.
- c. Choose Storage format: as “qcow2”.
- d. Click **Apply**.



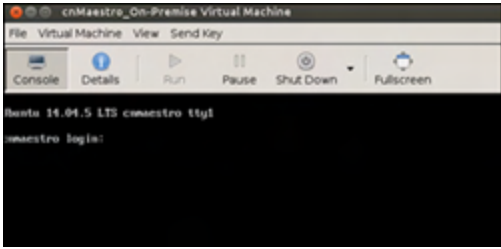
8. Configure Network Adapter

- a. Select NIC from the left pane.
- b. Select the appropriate source device. Default: NAT.
- c. Click **Apply**.



9. Begin Installation

- a. Click **Begin installation** on the top left. It would take few minutes to complete.
- b. After installation console may show blank for some time. Wait for 10-15 minutes. Restart VM if **cnmaestro login:** prompt is not shown.



Windows DHCP

This section details how to configure a Microsoft Windows-based DHCP server to send DHCP Options to Cambium Networks devices such as ePMP, ePMP 1000 Hotspot, and cnPilot Enterprises and Home devices.

Following settings has to be configured:

- Configuring Option 60
- Configuring Option 43
- Configuring Option 15
- Configuring Vendor Class Identifiers
- Defining DHCP Policies

DHCP servers are a popular way to configure clients with basic networking information such as an IP address, default gateway, network mask, and DNS server. Most DHCP servers have the ability to also send a variety of optional information, including the Vendor-Specific Option Code Option 43. When a Cambium device requests Option 43 Vendor Specific Information, the DHCP server responds with values configured by the DHCP administrator.

Configuring Option 60

This section describes how to configure the Vendor Class Identifier Code (option 60) on a Microsoft Windows-based DHCP server. As mentioned in the overview section, option 60 identifies and associates a DHCP client with a particular vendor. Since option 60 is not a predefined option on a Windows DHCP server, you must add it to the option list.

Windows DHCP Server Configuration

1. On the DHCP server, open the DHCP server administration tool by clicking **Start > Administrative Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Select **Set Predefined Options**.
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information and click **OK** to save.

Field	Information
Name	CambiumOption60
Code	60
Data Type	String (select the Array check box also)
Description	Cambium AP vendor class identifier

5. In the Predefined Options and Values dialog box, make sure **060 CambiumOption60** is selected from the Option Name drop-down list.
6. In the Value field, enter the following information: String: Cambium, Cambium-WiFi-AP, Cambium-cnPilot r200P, Cambium-cnPilot R201P
7. Click **OK** to save this information.

8. Under the server, select the scope you want to configure and expand it. Select **Scope Options**, then select **Configure Options**.
9. In the Scope Options dialog box, scroll down and select **060 CambiumOption60**. Confirm the value is set as mentioned in point 7 above and click **OK**.



NOTE:

The Data type should be string. If only one device type is to be onboarded to the cnMaestro server, then there is no need to select the Array option. If multiple device types need to be onboarded, then please select the Array option, so the value can contain multiple option 60 entries.

Configuring Option 43

Option 43 returns the cnMaestro URL to the Cambium Devices.

Windows DHCP Server Configuration

1. On the DHCP server, open the server administration tool by clicking **Start > Administration Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Select **Set Predefined options**
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information:

Field	Information
Name	CambiumOption43
Code	43
Data Type	String
Description	Cambium AP Option 43

5. Click **OK** to save this information.
6. In the Predefined Options and Values dialog box, make sure **043 CambiumOption43** is selected from the Option Name drop-down list.
7. In the Value field, enter the following information: String: `https://<NOC Server Hostname/IP>`
8. Click **OK** to save this information.



NOTE:

If Option 43 is already in predefined options with the data type as Binary, then it cannot be changed to string. If this is the case, while defining the policies, specify the values in the ASCII column in the Actions tab of the policy after selecting Option 43. This will be detailed in the Policies section later in the document.

Configuring Option 15

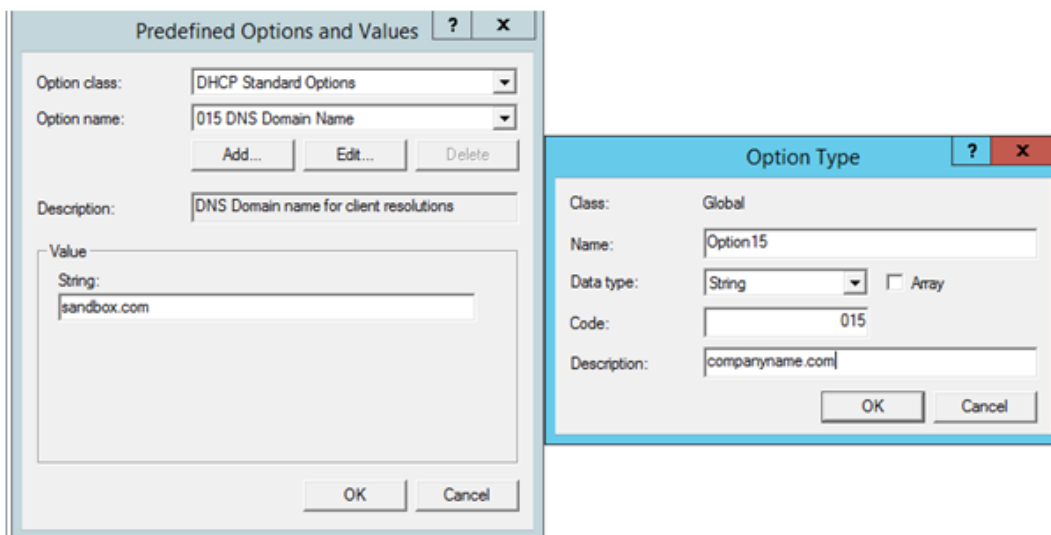
Option 15 returns the domain name to the Cambium Devices.

Windows DHCP Server Configuration

1. On the DHCP server, open the server administration tool by clicking **Start > Administration Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Click on Set Predefined Options
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information:

Field	Information
Name	CambiumOption15
Code	15
Data Type	String
Description	Cambium AP Option 15

5. Click **OK** to save this information.
6. In the Predefined Options and Values dialog box, make sure **015 CambiumOption15** is selected from the Option Name drop-down list.
7. In the Value field, enter the following information: String: <companyname.com>
8. Click **OK** to save this information.



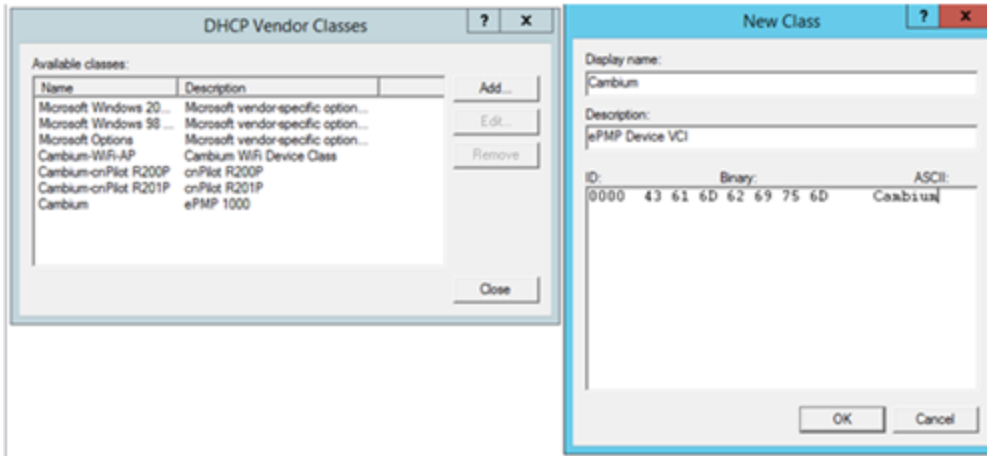
NOTE:

In the DNS Server, the user needs to map the cnMaestro hostname to the IP address of the cnMaestro On-Premises server.

Configuring Vendor Class Identifiers

1. On the DHCP server, open the server administration tool by clicking **Start > Administration Tools > DHCP**.

- Find your server and right-click on the scope to be configured under the server name. Click on the **Define Vendor Classes** and click the **Add** button in the dialog box that appears.
- Provide the Display name, Description and then click in the ASCII column and enter the value as Cambium as shown in the below figure, and then click **OK**.



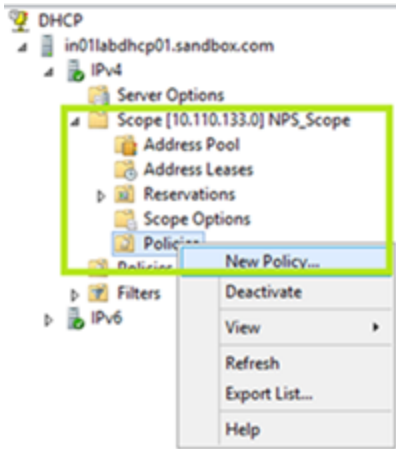
The above example is for an ePMP device. In order to create the VCI for other device types, please follow the same steps, and in the ASCII column provide the following values:

Product	VCI (DHCP Option 60)
cnPilot R200P	Cambium-cnPilot r200P
cnPilot R201P	Cambium-cnPilot R201P
cnPilot R190	Cambium-cnPilot R190
cnPilot Enterprise	Cambium-WiFi-AP
ePMP	Cambium
ePMP 1000 hotspot	Cambium-WiFi-AP

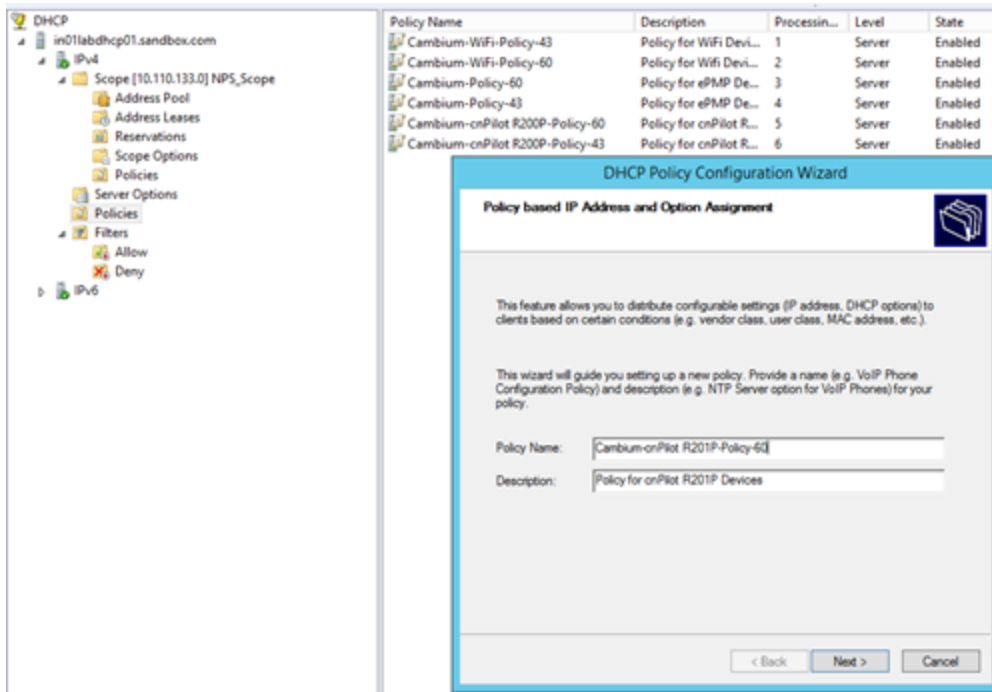
Configuring the Policies at the SCOPE Level

Once Options 43, 60, 15, and Vendor Classes are created, one needs to create policies at scope level. This allows the DHCP server to send the Option 43 and 60 to the Cambium Devices -- based on their VCI for that device. The policy will make sure these options are only sent if the VCI matches that provided by the device.

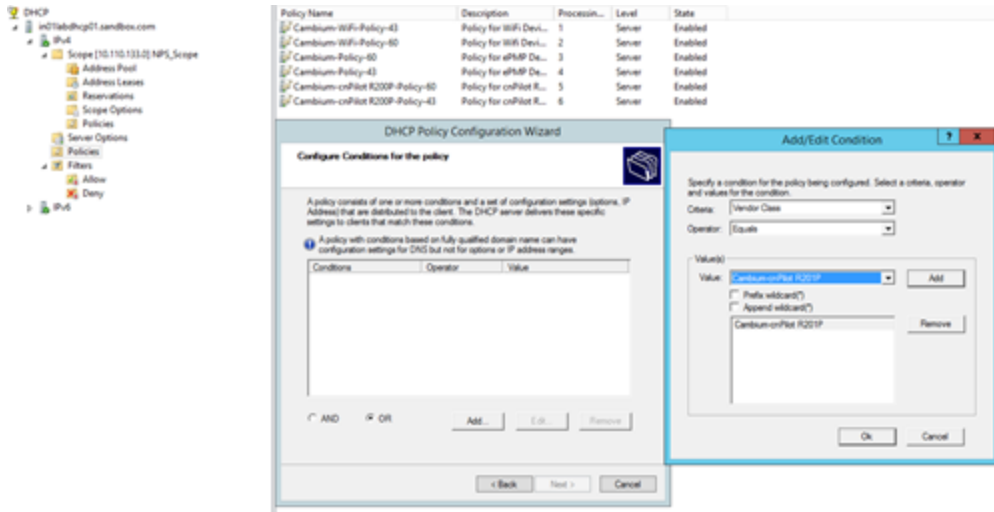
- Select the scope in which you want to create the policy, and then right click on the Policies option. Select New Policy.



2. In the pop-up, enter the Policy Name and Description and click **Next** button.



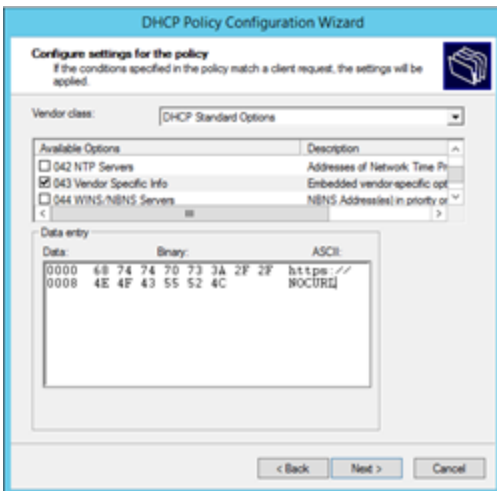
3. The Policy consists of Matching conditions based on Vendor Class, user class, MAC Address, Client Identifiers, FQDN and Relay Agent Information. For Cambium Devices we need Vendor Class based match conditions only.
 - a. In the dialog, click on the **Add** button and in the pops-up select the Criteria as **Vendor Class**, the Operator as **Equals**, and the Value as the VCI created for the Cambium Device type.
 - b. For example, for cnPilot R201P device the Vendor Class selection is “Cambium-cnPilot R201P”.
 - c. Click **Add** and then **OK** in the pop-up. Click **Next** in the Policy Configuration Wizard.

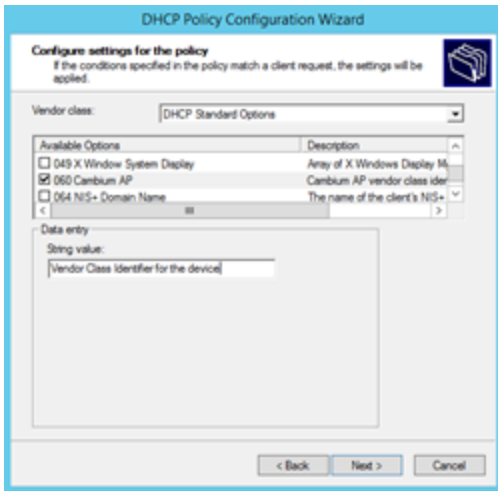


4. In the policy configuration settings wizard, select the option **No** and click **Next**.

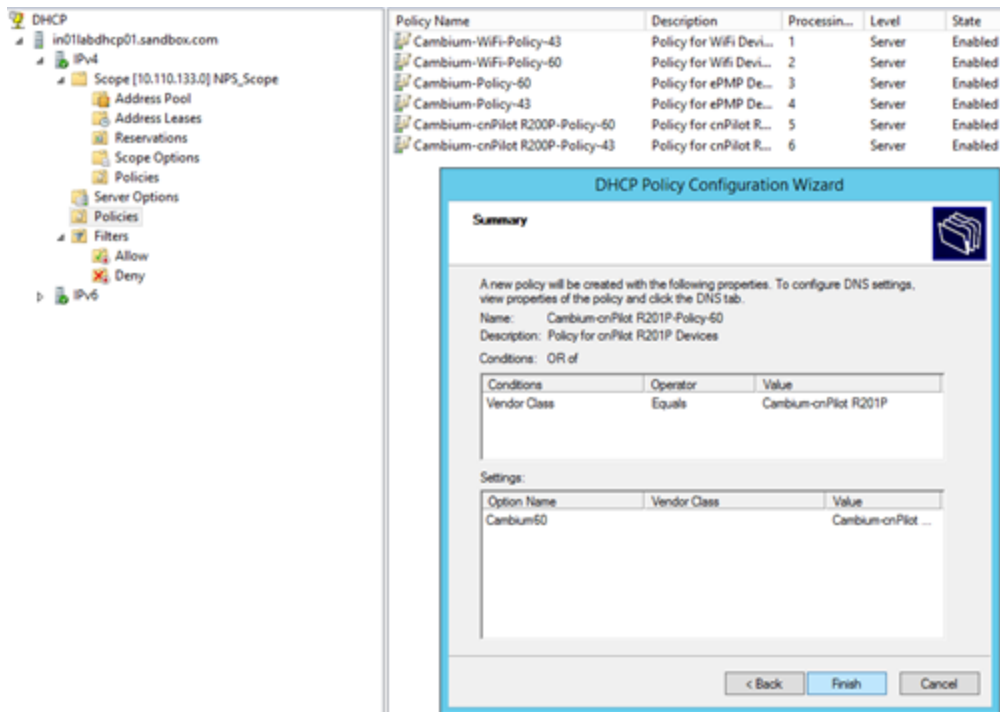


Then select the vendor class as DHCP standard options and Select the options 43 and 60 from the available options and specify the values that need to be sent to the device. Click **Next** once the options are selected and values are specified.





5. Click Finish in the final settings page. The policy is displayed in the RHS pane.



The above Policy is a generic one. For all the device types, the policies should be created in a similar way --, with the match conditions and action as follows:

Also the Policies can be created at the Scope level or Server level. If separate scope is defined for Cambium devices, it is better to define scope level policies; otherwise the policies can be defined at the Server level in the similar way.

Device Type	Match Condition	Actions
cnPilot E-Series	Vendor Class for E400/E410/E425H/E500/E501S/E502S/E505/E600	Cambium option 43 and 60 selected and values specified
cnPilot Home	Vendor Class for cnPilot R190/R195/R200/R201	Cambium option 43 and 60 selected and values specified
ePMP	Vendor Class for ePMP	Cambium option 43 and 60 selected and values specified
ePMP 1000 Hotspot	Vendor Class for Hotspot	Cambium option 43 and 60 selected and values specified

Citrix Hypervisor Installation

Overview

cnMaestro can be installed on Citrix Hypervisor (formerly known as XenServer). The OVA image can be downloaded from the Cambium Support Center <https://support.cambiumnetworks.com/>.

Resources

The following resources are required for deployment.


	<p>Note:</p> <ol style="list-style-type: none"> If NBI APIs or Performance Data Reports are extensively used, vCPUs and RAM should be increased by 50%. SSD disks are recommended to improve performance.
---	--

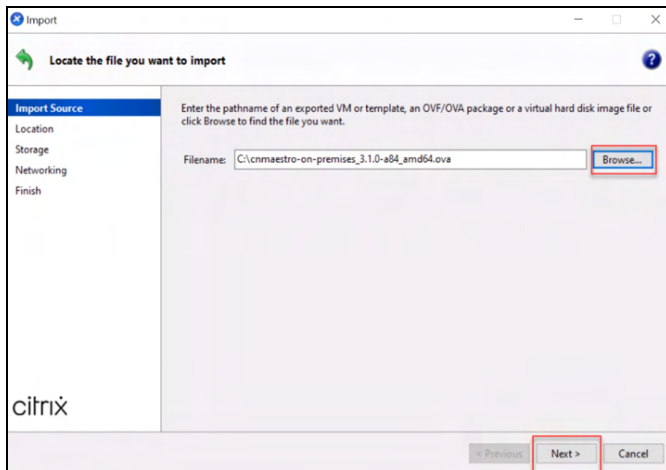
Table 67: Supported devices

Number of Devices	Wireless Clients	Number of vCPUs	RAM Size (GB)	Hard Disk (GB)
1 - 100	Up to 1500	2	4	120
101 - 1,000	Up to 15,000	4	4	120
1,001 - 4,000	Up to 60,000	4	8	150
4,001 - 10,000	Up to 150,000	8	16	250

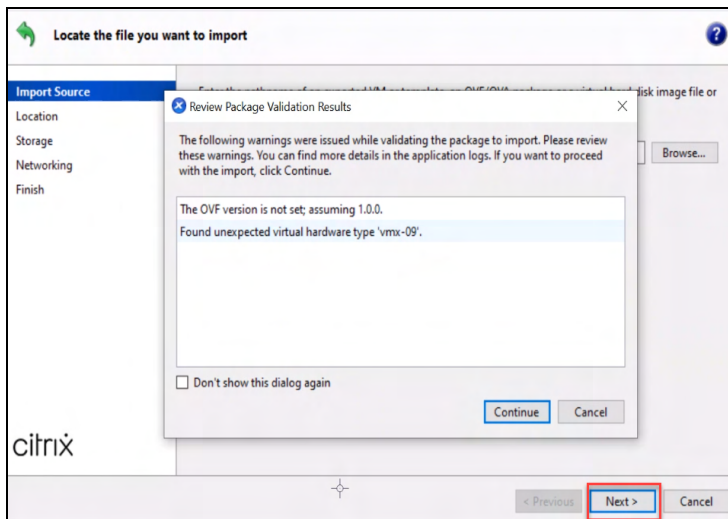
Import using Citrix Hypervisor

Perform the following steps to install the Citrix Hypervisor:

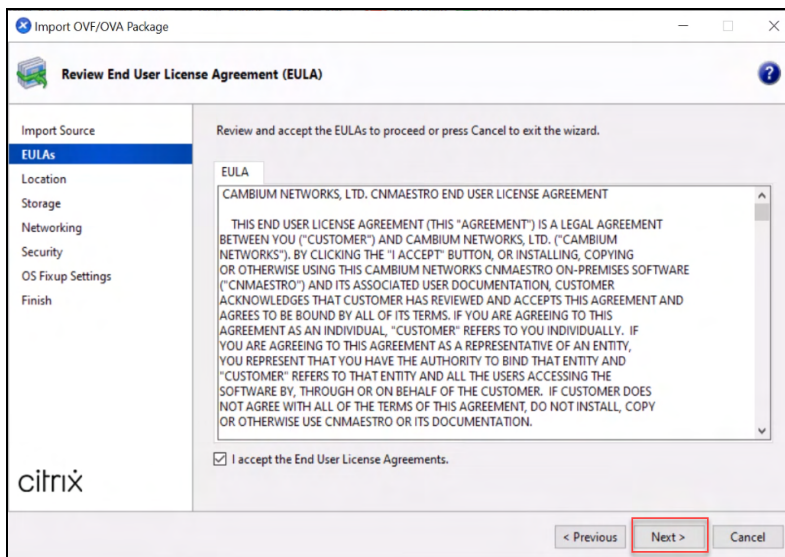
1. Navigate to **XenCenter** and right-click **citrix hypervisor**.
2. Click **Import**.
3. Click **Next** on the import wizard, browse to the downloaded OVA and click **Next**.



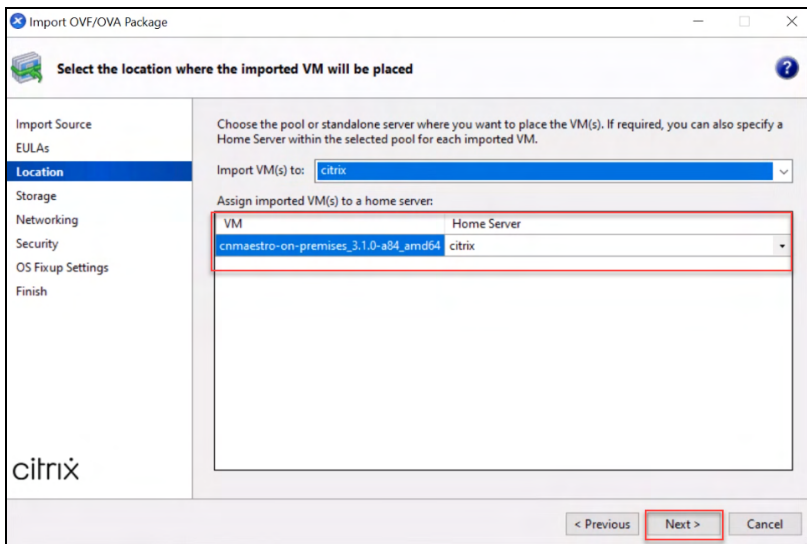
4. Review the Package Validation results and click **Next**.



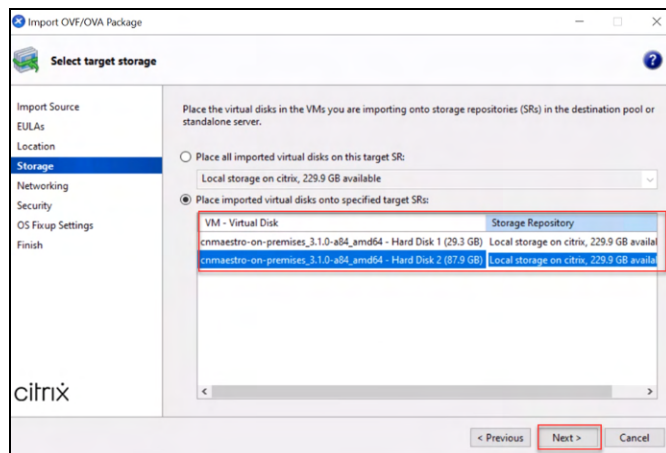
5. Accept the EULA.



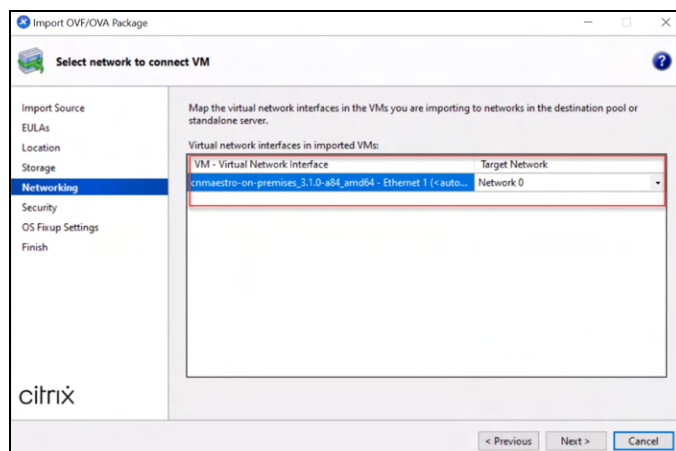
6. Select the location where the imported VM will be placed.



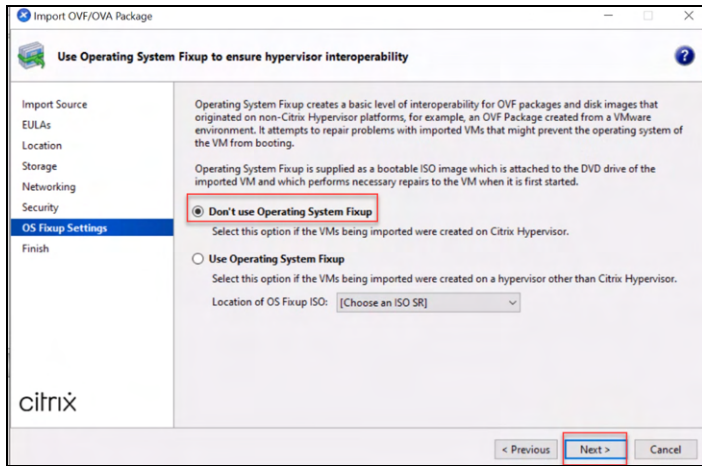
7. Select a storage repository for the second/data disk.



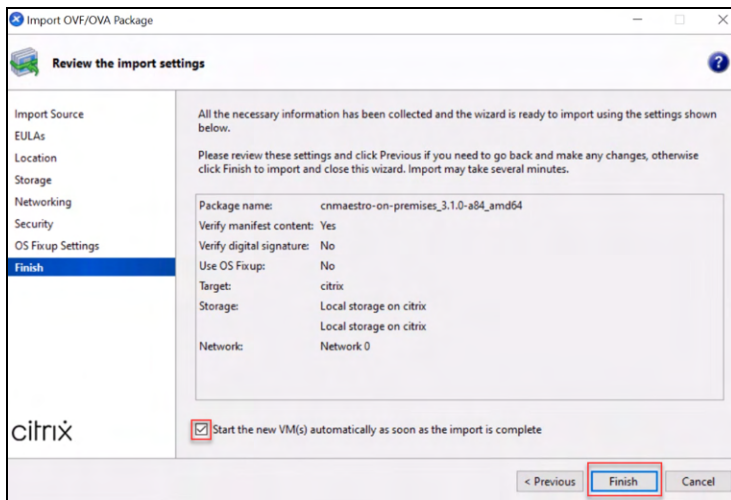
8. Select a network.



9. Verify the included manifest to ensure the OVA is not damaged. Select **Don't use Operating System Fixup**.

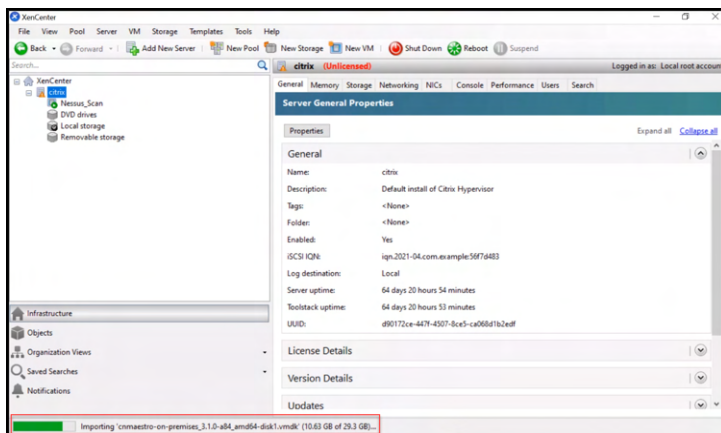


10. Enable the check box to start a new VM when the import completes.

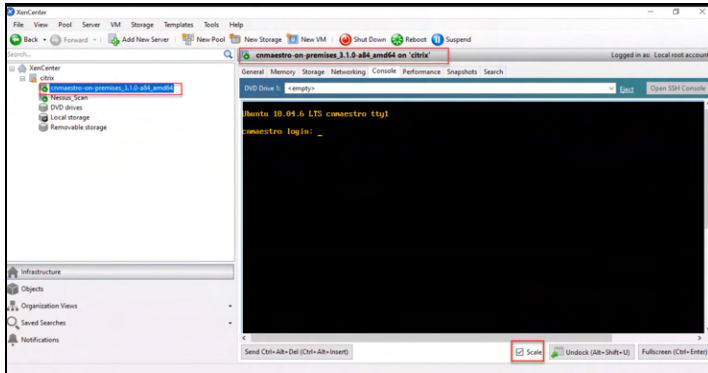


11. Click **Finish**.

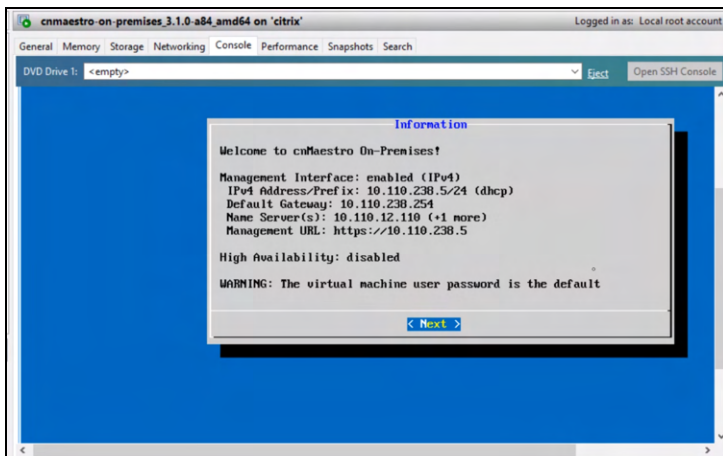
The Import might take few minutes depending on the network, number of hard disks, and the Storage Repository speed. Once the Import completes, start the VM. The Import status can be viewed in the status bar as shown in the figure below.



12. The new VM will appear on the left panel. Select the VM and click **Start VM** and navigate to the configuration screen.



13. Open the **Console** tab and login with user name **cnmaestro** and default password **cnmaestro**.
14. If needed, the **Scale** option may make the console easier to view.
15. The console provides status as well as a basic settings interface for the appliance.



Access cnMaestro

SSH Access



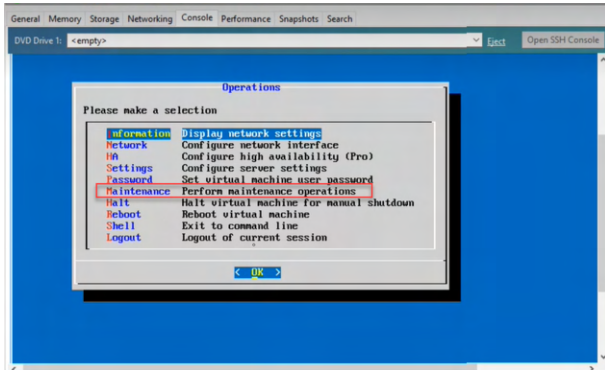
Note:

- The TUI warns if you have not changed the default password.
- Uncheck **Scale** option to view console.

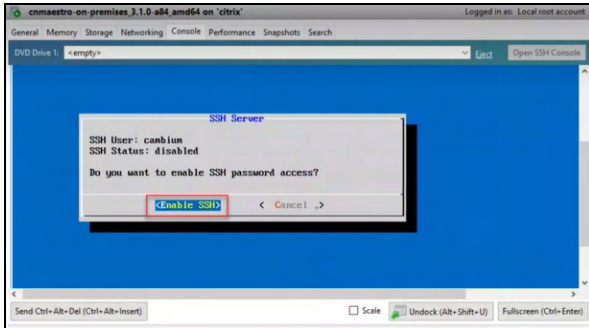
SSH access is disabled by default.

To enable SSH

1. Navigate to **Maintenance > SSH** in the menu.



2. Select **Enable SSH**.



Once enabled, you can access cnMaestro over SSH. You must change the default password before enabling SSH.

HTTPS Access

You can launch the web UI over HTTPS by entering the cnMaestro IP address in the browser. The default SSL certificate is self-signed and will generate a self-signed certificate error. After logging in, you can upload a custom certificate by navigating to **Administration > Server > SSL Certificates** in the web UI.

Advanced Options

Expand the Data Disk



Warning:

Always take a snapshot of the data volume before expanding it.

The data volume can be expanded at any time as the number of devices in the account increases. The process consists of two parts:

- Expand the volume through Citrix Hypervisor
- Expand the file system within cnMaestro

Expand the volume through Citrix Hypervisor

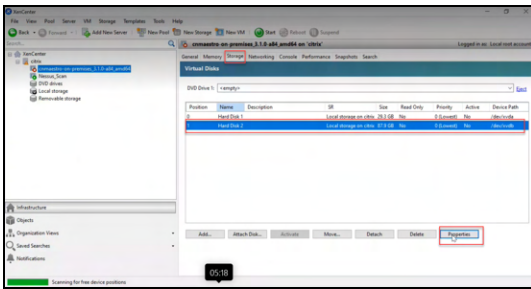
Expand the volume using the Citrix Hypervisor:



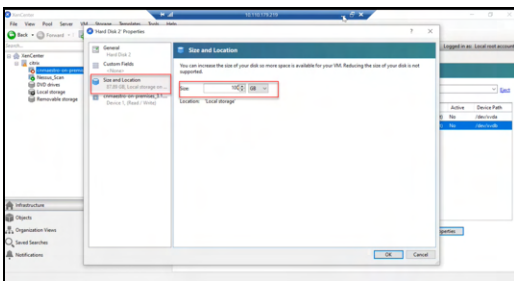
Note:

Shutdown the VM before increasing the hard disk size.

1. Open the VM Storage tab.



2. Right-click on the data disk (by default **Hard Disk 2** is selected).
3. Click **Properties**.
4. In the **Size and Location** tab, increase size of hard disk selected and click **OK**.



5. Restart the VM.

Expand the file system within cnMaestro

If the file system is not automatically expanded, you may need to do this manually. You can do this by using the cnMaestro Console or SSH.

1. Login to cnMaestro through SSH and exit to the command line.
2. Run `lsblk` command to determine the disk that maps to the data store.
 - The name might be different, depending on the type of image originally selected for the instance.
3. Grow the partition to use the full disk.

For example, expand partition 1 of the `/dev/xvdb` device:

```
sudo growpart /dev/xvdb 1
```

4. Grow the file system mapping to `/mnt/data`. For the above example, execute the below command:

```
sudo resize2fs /dev/xvdb1
```

```
tmpfs 391M 4.5M 386M 2% /run
/dev/mapper/system-osl 7.3G 4.8G 2.5G 69% /
tmpfs 2.0G 48K 2.0G 1% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup
/dev/mapper/system-tmp 1.8G 5.7M 1.7G 1% /tmp
/dev/mapper/system-osl 7.3G 34M 6.9G 1% /mnt/osl
/dev/mapper/system-log 5.5G 77M 5.1G 2% /var/log
/dev/xvdb1 464M 83M 354M 19% /boot
/dev/xvdb1 51G 723M 51G 1% /mnt/data
tmpfs 391M 0 391M 0% /run/user/1000
Cambiumcnmaestro-5 sudo growpart /dev/xvdb 1
CHANGED: partition1 start=2048 old: size=18431792 end=18432000 new: size=209713119,end=20971517
resize2fs 1.44.1 (24-Mar-2018)
Filesystem at /dev/xvdb1 is mounted on /mnt/data; on-line resizing required
old_desc_blocks = 11, new_desc_blocks = 13
The filesystem on /dev/xvdb1 is now 2624139 (4k) blocks long.
Cambiumcnmaestro-5 df -kh
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0 1.9G   0% /dev
tmpfs           391M   4.5M 386M   2% /run
/dev/mapper/system-osl 7.3G  4.8G 2.5G  69% /
tmpfs           2.0G   48K 2.0G   1% /dev/shm
tmpfs           5.0M    0 5.0M   0% /run/lock
tmpfs           2.0G    0 2.0G   0% /sys/fs/cgroup
/dev/mapper/system-tmp 1.8G  5.7M 1.7G   1% /tmp
/dev/mapper/system-osl 7.3G  34M 6.9G   1% /mnt/osl
/dev/mapper/system-log 5.5G  77M 5.1G   2% /var/log
/dev/xvdb1      464M  83M 354M  19% /boot
/dev/xvdb1      51G  724M 51G   1% /mnt/data
tmpfs           391M    0 391M   0% /run/user/1000
Cambiumcnmaestro-5
```

Network Requirements

Inbound Ports

The following table provides information about network port requirements for inbound:

Table 68: Inbound Port Details

Serial Number	Port Number	Port Type	Purpose
1	443	TCP	HTTPs Web Access and device communication
2	18301	TCP/UDP	Wi-Fi Performance Test
3	161	UDP	SNMP Communication
4	22	TCP	Data Replication (High Availability)
5	8300	TCP	Distribution Synchronization (High Availability)
6	8301	TCP/UDP	Distribution Synchronization (High Availability)
7	3799	UDP	RADIUS CoA for RADIUS Proxy feature

Outbound Ports

The following table provides information about network port requirements for outbound:

Table 69: Outbound Port Details

Serial Number	Port Number	Port Type	Purpose
1	18301	TCP/UDP	Wi-Fi Performance Test
2	162	UDP	SNMP Trap Receiver
3	465 and 587	TCP	SMTP Server communication
4	20 and 21	TCP	FTP and SFTP communication
5	49	TCP/UDP	TACAC Server communication
6	1812	UDP	Free Radius Server Authentication communication
7	1813	UDP	RADIUS Server Accounting communication
8	389 and 636	TCP/UDP	LDAP or Active Directory (AD) server communication
9	514	UDP	Syslog server

Custom Network Scripts

If your network requirements are more complex than cnMaestro configuration, you can script custom networking commands, so they are executed after cnMaestro initializes networking. The commands are added to the file `/srv/files/etc/cnmaestro-network.override`, which also contains directions and a sample static route.

Contact Cambium Networks

Support Website	http://www.cambiumnetworks.com/support
Main Website	http://www.cambiumnetworks.com
cambium Community	http://community.cambiumnetworks.com
Sales Enquiries	solutions@cambiumnetworks.com
Support Enquiries	https://www.cambiumnetworks.com/support/contact-support/
Telephone Number List	http://www.cambiumnetworks.com/support/contact-support
Address	Cambium Networks Limited, 3800 Golf Road, Suite 360, Rolling Meadows, IL 60008 USA.