Cambium Networks™

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.

© 2021 Cambium Networks Limited. All Rights Reserved

Contents

Contents 3
Introduction 13
Overview 13
Supported Browsers 15
Supported Virtualization Infrastructures 16
Device Software 17
Software Download 20
Differences with cnMaestro Cloud 20
Quick Start 22
Installation 22
Virtualization 22
Desktop Virtualization 22
Bare Metal Hypervisor 22
cnMaestro Deployment 22
Device Software 32
PMP Configuration Prerequisites 39
DHCP Options (Linux) 40
UI Navigation 44
Basic 44
Account View 44
Access and Backhaul Account 45
Enterprise Account 45
Industrial Internet Account 46
Home Page 46
Page Structure 46
Page Navigation 47
Menu 47
Header 47
Access and Backhaul Account 47
Overview 47
Device Tree Navigation 47
Enterprise Account 53
Overview 53
System 53
Devices 53
AP Groups and WLANs 54

Sites 54
Side Menu 55
Section Tabs 55
System Status 56
Logout 56
Architecture 58
Overview 58
Networking 58
Device Onboarding 60
Overview 60
60 GHz cnWave Onboarding 60
Pre-Configuration and Approval of Devices (Optional) 64
Device/Agent Authentication (Optional) 64
Claiming the Wi-Fi Devices from AP Group 65
Claiming the Wi-Fi Devices from Site Dashboard 66
High Availability (HA) 68
Overview 68
Primary vs Secondary 68
Shared (Floating) IP Address 68
Network Ports 68
Recommendations 69
Dual Interfaces 69
Add eth1 Network Adapter 69
HA Cluster Setup 71
Bootstrap (Primary) 71
Accept (Primary) 71
Join (Secondary) 71
Basic HA Cluster Creation Flow 72
Secondary Server 74
HA Menus 75
High Availability Cluster Menu (pre-Bootstrap) 75
High Availability Menu (post-Bootstrap) 75
New Cluster 76
Accept Join Requests 76
Join Existing Cluster 77
Validate SSH Fingerprints 77
HA Cluster Status 77
Delete Node 79
Leave Cluster 80

Information 80
Behaviour of cnMaestro features When HA is Enabled 80
Monitoring 82
Network Monitoring 82
Dashboard 82
KPI (Key Performance Indicators) 82
Device Health 83
Connection Health 83
Charts and Graphs 84
Notifications 84
Overview 84
Events 85
Alarms 87
Statistics and Details 88
Performance 96
Maps 108
Map Navigation 109
Mode 110
Tools 112
60 GHz cnWave Tools 112
cnMatrix Tools 112
cnPilot Home Tools 114
cnRanger Tools 115
cnReach Tools 116
cnVision Tools 117
Enterprise Wi-Fi Tools 119
ePMP Tools 122
Machfu 125
PMP Tools 126
Tower-to-Edge View 128
WIDS 129
Detecting Rogue APs 129
cnPilot Dashboards 133
Device Dashboard 133
Overview 133
Clients 133
Network Info 136
Mesh Peers 138
Neighbors 138

Site Dashboard 139
Wi-Fi Devices Availability (Total and Offline) 139
Wireless 140
Throughput 140
RF Quality 140
AP Types 140
Top Wi-Fi APs 140
Channel Distribution by Band 141
Radio/WLAN Distribution by Band 141
Clients by SNR 141
Clients by Performance 142
Clients Graph 142
Throughput Graph 142
Statistics 143
Wireless Clients 143
Floor Plan 144
Inventory 145
Inventory Export 145
Bulk Delete 145
Bulk Reboot 146
Schedule Reboot 147
CSV Configuration Import 147
Sample Configuration File 148
Sample Configuration File (60 GHz cnWave) 148
Uploading a Configuration File 149
Reports 152
Generating Reports 152
Device Report 152
Performance Report 157
Active Alarms Report 162
Alarms History Report 162
Events Report 163
Clients Report 163
Mesh Peers Report 164
Remote Upload 165
Report Jobs 166
Provisioning 167
Software Update 167
Software Update Overview 167

Create Software Update Job 168
Software Update 170
Viewing Running Jobs in Header 174
cnReach Bulk Software Upgrade 174
Fixed Wireless Configuration 177
Overview 177
Configuration Templates 177
Configuration Variables 178
Macros 178
Variable Caching 179
Device Type-Specific Configurations 179
Variable Validation 179
Sample Templates 179
Template File Creation 179
Template 179
Configuration Update 181
Device Selection 181
Device Type 181
Device Table 181
Configuration Update Steps 183
Configuration Backup 183
Jobs 187
Configuration Update 187
Wireless LAN Configuration 188
cnPilot Home and Enterprise Wi-Fi 188
Configure cnPilot using cnMaestro 188
Create an AP Group 194
Pre-Defined Overrides 199
User-Defined Overrides (Advanced) 199
User-Defined Variables (Advanced) 199
Synchronize (Sync) Configuration 200
Configuration Job Status 201
Factory Reset 201
Association ACL 203
Overview 203
Configuring Association ACL 203
cnMatrix Switches 204
Switch Groups Configuration 204
Synchronize (Sync) Configuration 210

Policy Based Automation(PBA) 211
Switches 214
Switch Ports 219
Device Details 226
60 GHz cnWave Network Configuration 230
Managing E2E Network 230
Site Configuration 260
Node Configuration 263
PoP Node 271
DN/CN Node 287
Auto-Provisioning 295
Creating Auto-Provisioning Rule 295
Services 297
Managed Service Provider (MSP) 297
Overview 297
Managed Accounts 297
Managed Service 298
Managed Service Provider (MSP) 299
Managed Service Users (Administrators) 300
Configuring Managed Services 301
Enable Managed Service Provider (MSP) 302
Create Managed Services 303
Create Managed Account 305
Validate Managed Account Administrators 306
Managed Services Administration 308
Overview 308
System Dashboard 309
Managed Account Administration 310
Device Management 311
Disabling Managed Service Provider Feature 313
API Client 314
Overview 314
API Clients 314
RESTful API Specification 315
Authentication 315
Swagger API 316
Introduction 316
Sample Swagger UI Screenshot 317
Client ID and Client Secret Generation 317

cnMaestro User Interface 317
API Session 318
Introduction 318
Retrieve Access Token 318
Access Resources 320
API Details 320
HTTP Protocol 320
REST Protocol 321
Parameters 323
Access API 328
Token (basic request) 328
Token (alternate request) 329
Validate Token 330
Selected APIs 331
Overview 331
cnMaestro v2 API 331
Devices API Response (v2 Format) 332
Statistics API Response (v2 Format) 334
Performance API Response (v2 Format) 346
cnPilot Guest Access 354
Configuration 354
Create the Guest Access Portal in cnMaestro 354
Mapping the Device to Guest Access Portal in cnMaestro 364
Access Types 366
Guest Access using Social Login 366
SMS Authentication 377
Generic SMS Gateway Configuration 377
cnPilot GRE Tunnels 384
Overview 384
Typical Deployment Model (Two Port Solution) 384
Multicast/Broadcast Handling with Multiple APs on Tunnel Concentrator 385
Inter AP Wireless Client Communication (through Concentrator) 385
Configuring L2GRE/EoGRE Tunnel Concentrator 385
Logs and Statistics 386
Access Control List (ACL) Configuration 386
MAC Layer ACL 387
IP Layer ACL 387
Transport Layer ACL 388
SNMP 389

Overview 389
Enable SNMP 389
Configure SNMP Parameters 389
cnMaestro MIB (Management Information Base) 390
RADIUS Proxy 391
Overview 391
Minimum cnMaestro On-Premises Version Requirements 391
RADIUS Proxy Configuration 391
Citizen Broadband Radio Service (CBRS) 393
Enabling CBRS in Cloud 393
Enabling CBRS in On-Premises 399
Synchronize CBRS Configuration to the On-Premises Instance 400
CBRS HTTP Proxy Configuration Options 400
Management Tool 403
Using a HTTP Proxy Server for CBRS Connectivity 425
Proxy Suggestions for CBRS Connectivity 425
External Proxy Requirements 425
Squid as External Proxy 425
HA for Squid external proxy 425
LTE 426
Adding SIM Cards 426
Administration 428
User Management 428
Authentication 428
Local Users 428
Creating Users and Configuring User Roles 433
Changing Password 434
Authentication Servers 435
Session Management 443
Server Management 444
Monitoring 444
Settings 444
Operations 450
Update cnMaestro Software 451
System Backup 451
In-System Upgrade 453
Diagnostics 455
SSL Certificate 456
Certificate Management 457

Manage Software Images 460
Webhooks 464
Integrations 464
Limits 465
cnMaestro Webhooks Configuration 465
Types of Variables 468
Error and Retransmission 469
Viewing Configured Webhooks 469
Status Check 470
Custom Template Examples 470
Audit Logs 485
Syslog 488
Cloud Connectivity 492
Overview 492
Creation of Cloud Anchor Account 492
Connecting cnMaestro On-Premises to Anchor Account 493
Software Images 494
cnMaestro System Update 495
Appendix 497
Maintenance 497
Command Line Alternatives 497
Export cnMaestro Data 497
Import cnMaestro Data 497
Technical Support Dump 498
Apply OVA Upgrade 498
Apply Package Update 498
SSH Access 498
Enabling SSH Access 498
Data Backup 501
Overview 501
Virtualization System Specific 501
Account Recovery 502
Virtual Machine (Console) Account Recovery 502
cnMaestro Application Account Recovery 504
Configure Network Time Protocol (NTP) 504
Disabling NTP Support 504
Extending the Data Disk 505
VMware Workstation Disk Expansion 505
VirtualBox Disk Expansion 506

Partition and File System Updates 506
Application Account Recovery 507
Statistics API Response (v1 Format) 508
Performance API Response (v1 Format) 520
Deployments 528
VMware ESXi Installation 528
cnMaestro VM Deployment 528
Oracle VirtualBox 5 Installation 531
VMWare Workstation 532
KVM Installation 535
Deployment 535
Windows DHCP 538
Configuring Option 60 538
Windows DHCP Server Configuration 538
Configuring Option 43 539
Windows DHCP Server Configuration 539
Configuring Option 15 539
Windows DHCP Server Configuration 540
Configuring Vendor Class Identifiers 540
Configuring the Policies at the SCOPE Level 541
Network Requirements 546
Inbound Ports 546
Outbound Ports 546
Custom Network Scripts 547
Contact cambium Networks 548

Introduction

This section includes the following topics:

- Overview
- Quick Start
- UI Navigation
- Architecture
- Device Onboarding
- High Avaliability

Overview

cnMaestro On-Premises is a standalone version of cnMaestro Cloud that can be installed in a customer's data center. Its functionality is nearly identical to Cloud – though compacted into a single package executed on a virtual machine. The primary features of both products include:

Table 1: cnMaestro Features

Feature	Description
60 GHz cnWave Network Onboarding and Configuration	Manages 60 GHz cnWave Networks added to your account.
Advanced Troubleshooting	Displays tower-to-edge status in a single graphic, view Wi-Fi client details and health, and troubleshoot client connectivity directly on the AP.
AP Group Dashboard	Aggregate Wireless LAN AP statistics by configuration group.
AP Groups Configuration (Wireless LAN)	AP Groups supports configuration of all Enterprise Wi-Fiand cnPilot Home devices. Specify a time for configuration of AP Groups.
Audit Logs	Record administrator activity.
Automatically Update Device Software	Automatically update device software version during onboarding.
Bulk Image Upgrade	Upgrade the software images in a sector or across sectors in a single job. Queue upgrade jobs during the day, so they can be run in the evening, when the network is less utilized.
CBRS	Manage Citizen Broadband Radio Service subscription for the CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz).
Configuration Backup	Store configuration from all Fixed Wireless devices (cnVision, PMP and ePMP) and cnReach devices which are currently online.
Cloud Connectivity	This will allow us to do many synchronization things in On-Premises instances, similar to Cloud will have the inventory stats from instances.

Table 1: cnMaestro Features

Feature	Description
Data Reports	Export devices, performance, active alarm, alarm history, clients, mesh peers and event statistics in a CSV format.
Device Inventory	Access your devices at the system level, or by network, site, Ap group levels, tower, or sector. Device data can be exported in PDF or CSV formats.
Email Notifications	Send email alerts for alarm status changes.
Enterprise View	Select a simplified UI tailored for Enterprise Wi-Fi and cnMatrix devices.
Guest Access Portal	Allow clients to connect to wireless service through a free model or paid access or by buying Vouchers.
Hierarchical Dashboards	Visualize your devices from tower to edge with customized dashboards for each device type.
High Availability (HA)	Enable Layer 2 High Availability through an Active-Standby (1+1) architecture.
IPv6 Support	For device and management traffic.
Long Term Historical Data	Support for: • All the performance graphs for Wi-Fi APs and cnMatrix support historical data up to last 1 year. • All the performance graphs for Fixed Wireless Broadband devices support historical data up to last 2 years. • All the performance graphs for IIoT devices support historical data up to last 1 year.
LTE	Manage the cnRanger device.
Managed Server Provider (MSP)	Allow cnMaestro account owners to partition their installation into separate Managed Accounts – each with its own independent administration and configuration.
Maps and Map Modes	Leverage maps to position your devices and visualize their health and connectivity. Change the map mode to graphically display various wireless key performance indicators.
Mesh Peers	Displays the details of available Mesh clients.
Multiple Account View	Support for: • Enterprise (which includes Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) and cnMatrix) • Industrial Internet Account (which manage Fixed Wireless, Wi-Fi and IIoT deployments including: 60 GHz cnWave, cnRanger, cnPilot Home (cnPilot R-Series), Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot), cnReach, cnMatrix, cnVision, Machfu, ePMP, PMP, and PTP. • Access and Backhaul View (which includes manage Fixed Wireless and Wi-Fi deployments including: 60 GHz cnWave, cnRanger, ePMP , cnPilot Home (cnPilot R-Series), Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot), cnMatrix, cnVision, and PMP, PTP,

Table 1: cnMaestro Features

Feature	Description
Notifications	View immediate status with stateful alarms, and troubleshoot customer issues by filtering on alarm history and reviewing events.
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.
Scheduled Configuration Update	Specify a time to configure device configuration.
Scheduled Software Update	Specify a time to install device software.
Site Dashboard	Aggregate Wireless LAN AP statistics by location.
Statistics and Trending	View historical radio and network statistics.
Switch Groups	Supports the configuration of all cnMatrix Switches.
Syslog	Forward audit logs and event logs to a configured external Syslog server.
Template-Based Configuration	Push configuration to single devices or to groups of devices across your network using templates. (cnPilot Home Series, cnReach, cnMatrix, cnVision, ePMP and PMP devices only). Specify a time for configuration of Template.
User Session Management	Track current cnMaestro users and force logoff.
Webhooks	Send alarm notification to the external servers.
Zero Touch Onboarding	Allows PMP SMs and ePMP SMs to automatically appear in onboarding queue, provided parent AP is already onboarded.

Supported Browsers

cnMaestro On-Premises supports the following browsers:

Table 2: Supported Browsers

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

Supported Virtualization Infrastructures

cnMaestro On-Premises is released as an Open Virtualization Archive (OVA) file. The following platforms are supported:

Table 3: Supported Virtualization Infrastructures

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

NOTE:

cnMaestro On-Premises is also available as an Amazon Machine Image (AMI) that can be accessed through the AWS Marketplace. The details can be accessed here: https://aws.amazon.com/marketplace/pp/Cambium-Networks-Ltd-cnMaestro-Wireless-Network-Ma/B07RJCL6MF.

Hardware Requirements

cnMaestro On-Premises is pre-configured with 2 virtual drives of approximately 120 GB total size. The image supports up to 10,000 devices (including cnMatrix, cnReach, cnPilot, ePMP, PMP, and PTP).

The virtual Hardware Requirements are listed below:

NOTE:
The virtual hardware is different than the physical hardware. Virtual hardware executes the cnMaestro application; physical hardware executes the VMware virtualization infrastructure in addition to the cnMaestro application (and possibly other independent applications).

NOTE:

- For best performance, servers with recent generation Intel Core i7 or Xeon CPUs are recommended. Older quad-core CPUs may not scale sufficiently. A Geek bench Multi-Core score of 4,500 should be sufficient for 100 devices, 8,000 for 4,000 devices, and 13,400 for 10,000 devices.
- If RADIUS Proxy through cnMaestro feature is enabled, then system resources especially vCPUs and RAM should be increased to 2 times of Hardware Requirements as specified in the below mentioned table.
- If NBI APIs and multiple Performance reports are enabled, then the System resources especially vCPUs and RAM should be increased to 1.5 times of Hardware Requirements as specified in the below mentioned table.
- Cambium Networks recommends using an SSD drive to improve performance.

Table 4: Hardware Requirements

Number of Devices	Wireless Clients	Number of vCPUs	RAM Size (GB)	Hard Disk (GB)
1 to 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

NOTE:
To onboard devices into cnMaestro On-Premises, the devices must at least be running the software version displayed in Table 5.

For a particular on-premise release, the minimum Device Software version is already embedded within cnMaestro. It can be downloaded to your local computer using the steps described in Software Download.

Newer device software may also be available from the Cambium website at https://support.cambiumnetworks.com/files.

Table 5: Minimum Device Versions

Device	Version
60 GHz cnWave V1000	1.0.1
60 GHz cnWave V3000	1.0.1
60 GHz cnWave V5000	1.0.1
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 5: Minimum Device Versions

Device	Version
cnPilot r195W	4.5.2
cnPilot r200/r201	4.4.2-R2
cnPilot r195P	4.7
cnPilot XV2-2	6.1
cnPilot XV3-8	6.0
cnRanger Tyndall 101	1.0.1.0-r1
cnRanger Tyndall 201	2.0-r1
cnRanger Sierra 800	1.0.1.0-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 2000	3.0.1
ePMP 3000	4.4.1
ePMP MP 3000	4.5
ePMP 1000 Hotspot	3.2.1-r6
ePMP Elevate	3.2
ePMP Elevate SXGLIT5/LHG5	4.3.2.1
ePMP Elevate XM/XW	3.2
ePMP Force 130 5 GHz	4.3.2
ePMP Force 130 2.4 GHz	4.4
ePMP Force 180/200	2.6.2
ePMP Force 190	3.5

Table 5: Minimum Device Versions

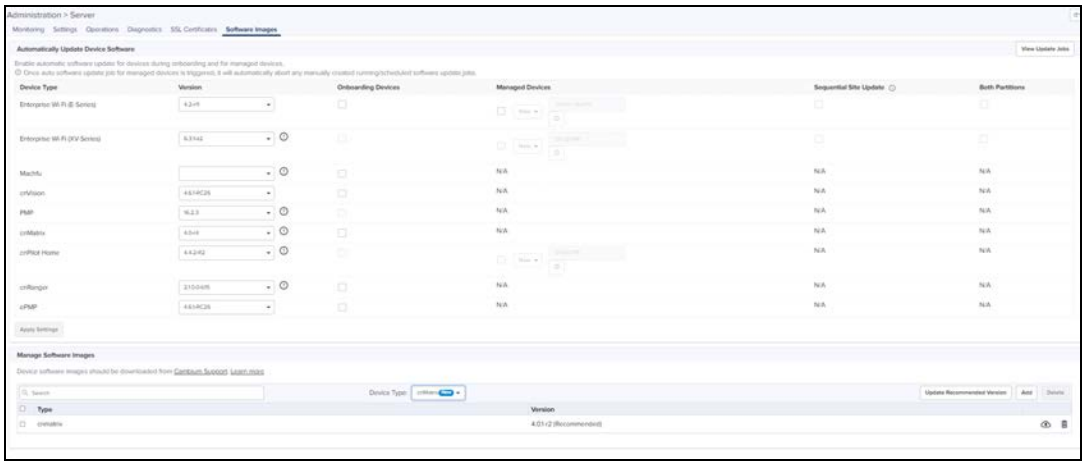
Device	Version
ePMP Force 200L	4.7.0
ePMP Force 300	4.1
ePMP Force 300 CSM	4.3.2
ePMP Force 300-13	4.4
ePMP Force 300-13L	4.5.2
ePMP Force 300-13LC	4.6
ePMP Force 300-19	4.4
ePMP Force 300-19R	4.4
ePMP Force 300-22L	4.6
ePMP Force 300-25L	4.6
ePMP Force 400	5.1.0.18
ePMP Force 425	5.1.0.18
ePMP PTP 550	4.1
ePMP PTP 550E	4.4.2
Machfu	7.1.2-1.1.0.5
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

Software Download

> **NOTE:**
> By default, Cambium do not provide any builds during OVA upgrade, user can upload device build by clicking add image button. Once uploaded user can use download icon to download the available images or by two options on add image by clicking local and download from cloud. For further info refer to Manage Software Images.

Device software can be accessed from the cnMaestro UI. The software is located at: **Administration > Server > Software Images**. Select your device type to display the available images, and then click the download icon ( ). Device software can also be accessed from the download page of Cambium Networks Support site. (https://support.cambiumnetworks.com/files).

Figure 1 Software Download



> **NOTE:**
> Current device software is included with the virtual machine software; however, it is not updated automatically. New device software releases need to be manually added. Additional details are provided later in the document.

Differences with cnMaestro Cloud

While the majority of features in cnMaestro On-Premises are identical to cnMaestro Cloud, there are some notable differences. A brief overview is listed below, and each will be discussed in-depth later in the document.

Table 6: Differences with Cloud

Difference with Cloud	Details
Account Recovery	Locally resolve password issues with cnMaestro On-Premises system account and Web UI.
Auto-Provisioning	Allow new cnPilot, cnVision, ePMP, and PMP devices to be provisioned and approved automatically using the subnet of the device.
Certificate Management	SSL certificate management for administration of UI and Guest Access Portal.
cnMaestro Software Upgrade	On-Premises has two types of software upgrade: • Virtual machine upgrade requires the customer to replace the entire virtual

Table 6: Differences with Cloud

Difference with Cloud	Details
	machine with a new instance. Configuration and data are exported from the old instance and imported to the new. • Package upgrade only updates the cnMaestro software; it does not require a virtual machine reinstallation. • OVA upgrade availability support is added in 2.1.0 release onwards. Please refer OVA Image.
Configuration Backup	Configuration Backup pulls and stores configuration from all Fixed Wireless devices (cnVision, PMP and ePMP) and cnReach devices which are currently online.
Deployment	The Cloud version is fully hosted and maintained by Cambium Networks at 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	In the Cloud version, all devices access cloud.cambiumnetworks.com. In the On-Premises version, devices contact the local cnMaestro server instead. This means they need to be configured to access the server before they can be managed. This can be accomplished on the device using the device UI or SNMP. Alternatively, DHCP options can be configured to provide the cnMaestro URL when the device boots up.
Device Image Management	In the Cloud, device images are automatically available. In the On-Premises version, new images need to be downloaded from support center and added to the cnMaestro server.
Local and Authentication Server Administrators	Support for local administrators (with a user name and password maintained by cnMaestro) or authentication services (including TACACS+ or Active Directory) for administration access
Onboarding	In the Cloud, devices are onboarded using either the device Manufacturer Serial Number (MSN) or through the Cambium ID (entered on the device). In On-Premises, all devices contacting cnMaestro are added to the onboarding queue, where they can be approved and managed.
On-Premises Console	Simple CLI, available through the virtual machine console, which allows one to configure networking parameters and update the system password.
RESTful API	HTTPS RESTful API for inventory, monitoring, performance, notification, and basic provisioning.
Server Management	Virtual machine performance parameters such as disk, memory, and CPU utilization.
SNMP (basic)	Basic SNMP support for inventory and alarms.
System Events	System generated Events in On-Premises server instance.
System Log	Forward events to a remote system log server.
Webhooks	Send alarm notification to the external servers.
Wireless LAN Speed Test	Speed test between wireless LAN APs and cnMaestro.

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 the first time.

Virtualization

There are two types of Virtualization architecture cnMaestro On-Premises supports: Desktop Virtualization and Bare-Metal Hypervisor.

Desktop Virtualization

Desktop Virtualization executes a virtual machine within an existing operating system environment (Windows, Mac, or Linux). The administrator installs virtualization software, such as VMware workstation or an Oracle virtualbox, and it executes in tandem with other desktop applications. cnMaestro can then be installed within 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.

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, and it takes time to set it 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.

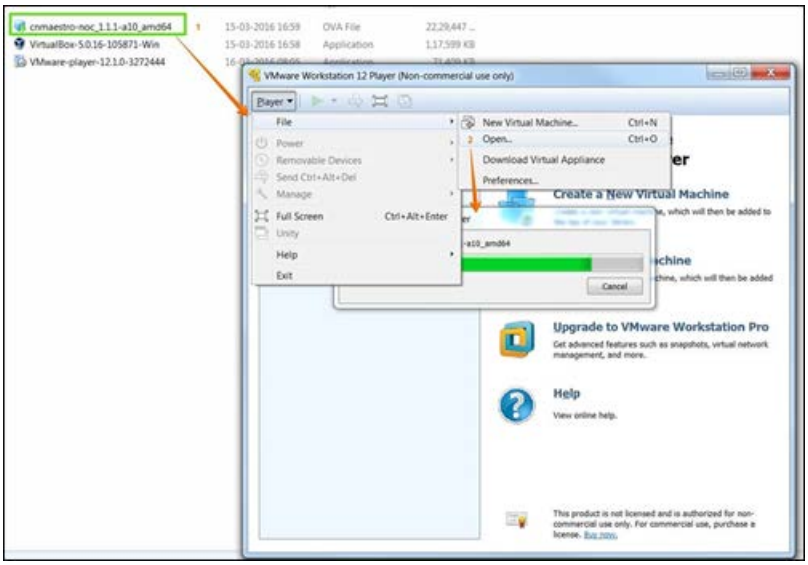
cnMaestro Deployment

This document presents cnMaestro deployment using VMware workstation player. Directions for VMware vSphere ESXi and VirtualBox are found in the appendix. VMware workstation player (and Oracle virtualbox) tend to be the easiest to install and evaluate, though ESXi is preferred for production.

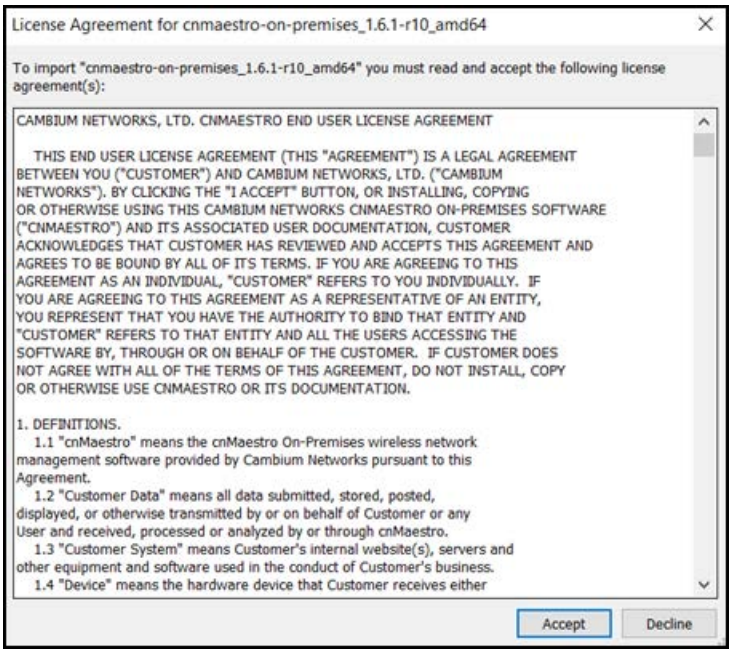
VMware Workstation Player

Follow the steps to import cnMaestro On-Premises into VMware Workstation Player as shown below.

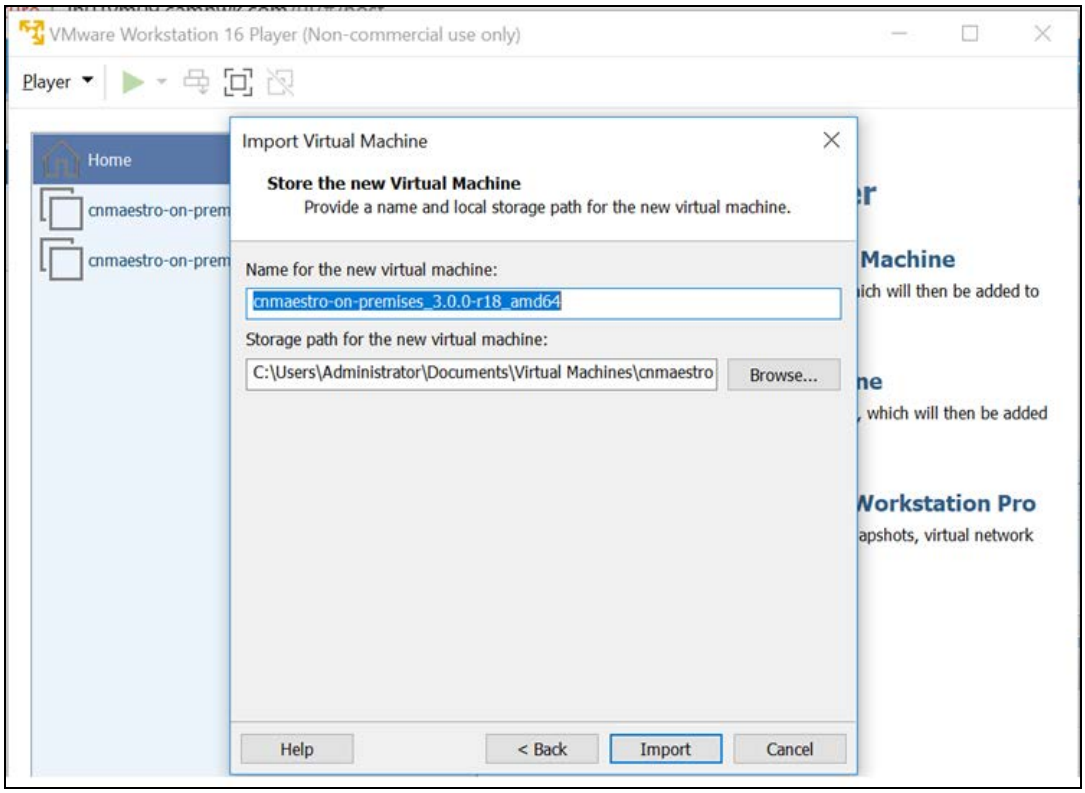
1. Install OVA File.
2. Open VMware workstation player chose **Player > File > Open** Menu. Select cnMaestro OVA file to import.



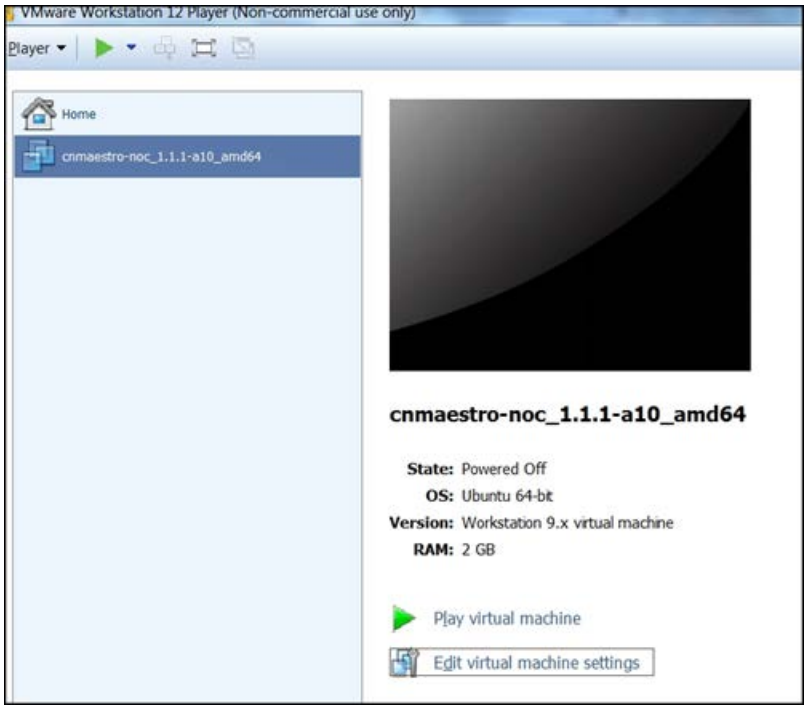
3. Accept the cnMaestro EULA, once the EULA is accepted, cnMaestro will be imported into the VM environment and it could take a couple minutes.



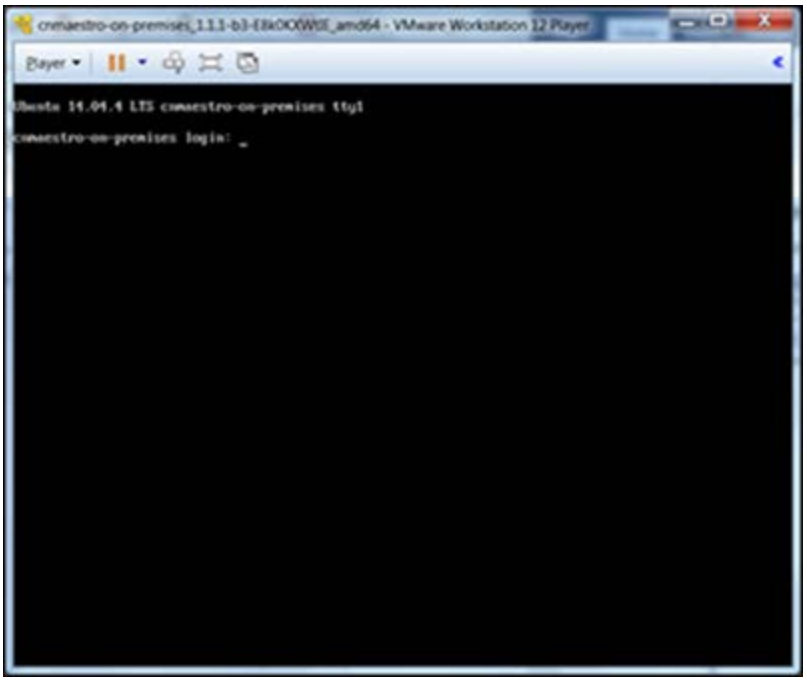
4. Click **Import** to start the deployment.



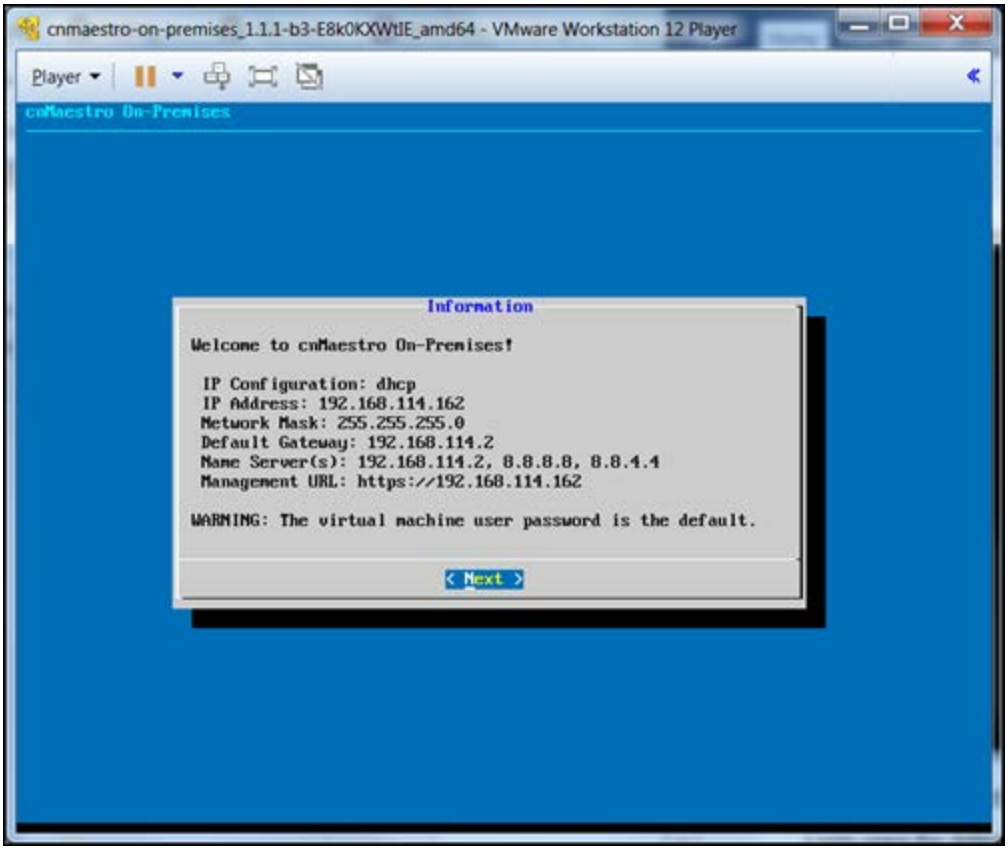
5. Click **Play** to start the Virtual Machine.



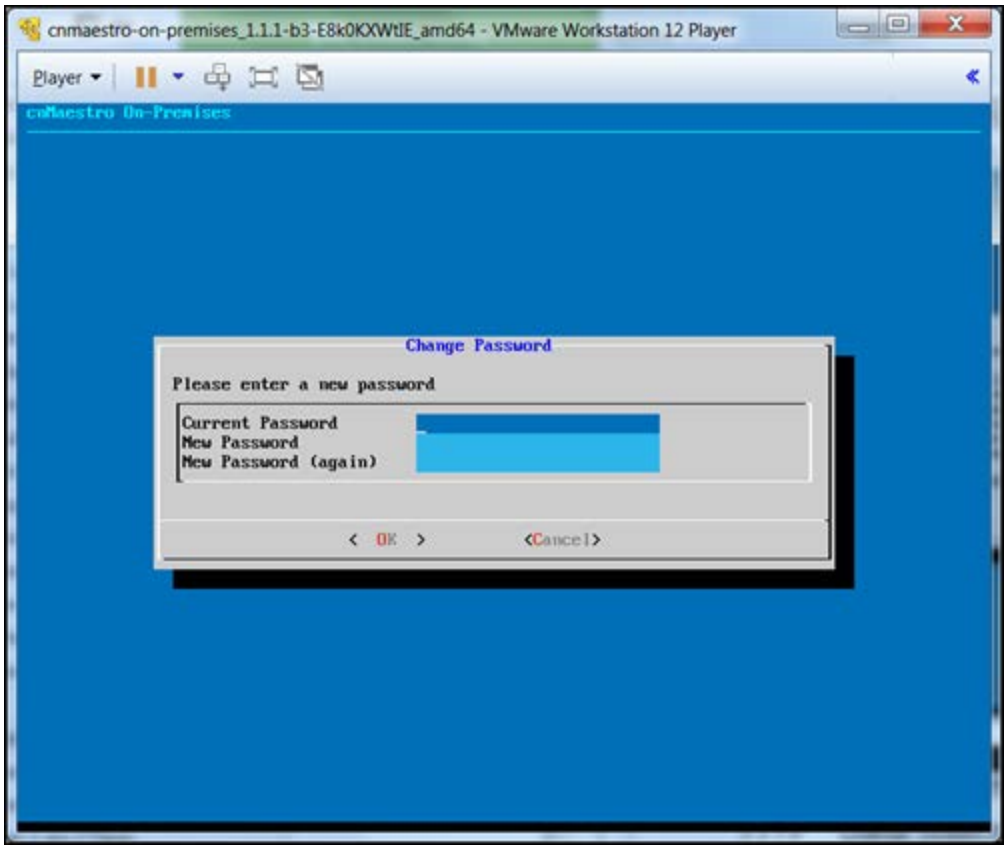
6. Login to the cnMaestro Console.
7. The virtual machine console is the only way to access the cnMaestro CLI (Command Line Interface).
8. Login using the default username/password (cambium/cnmaestro).



9. View Information Page.
10. The CLI displays the current network settings and allows you to change IP configuration and select a new system password.



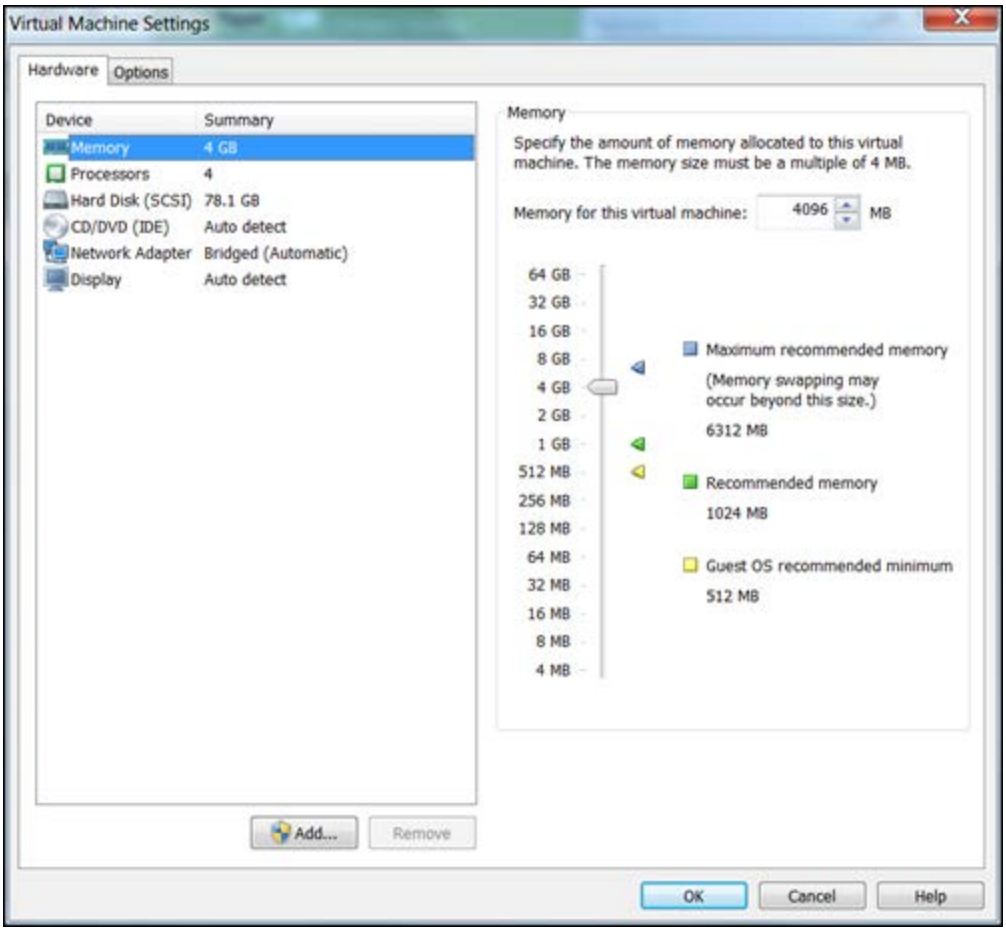
11. Change System Password and click **Next.**
12. Navigates to the **Change Password** page and update the password.



13. Change virtual machine configuration.

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.

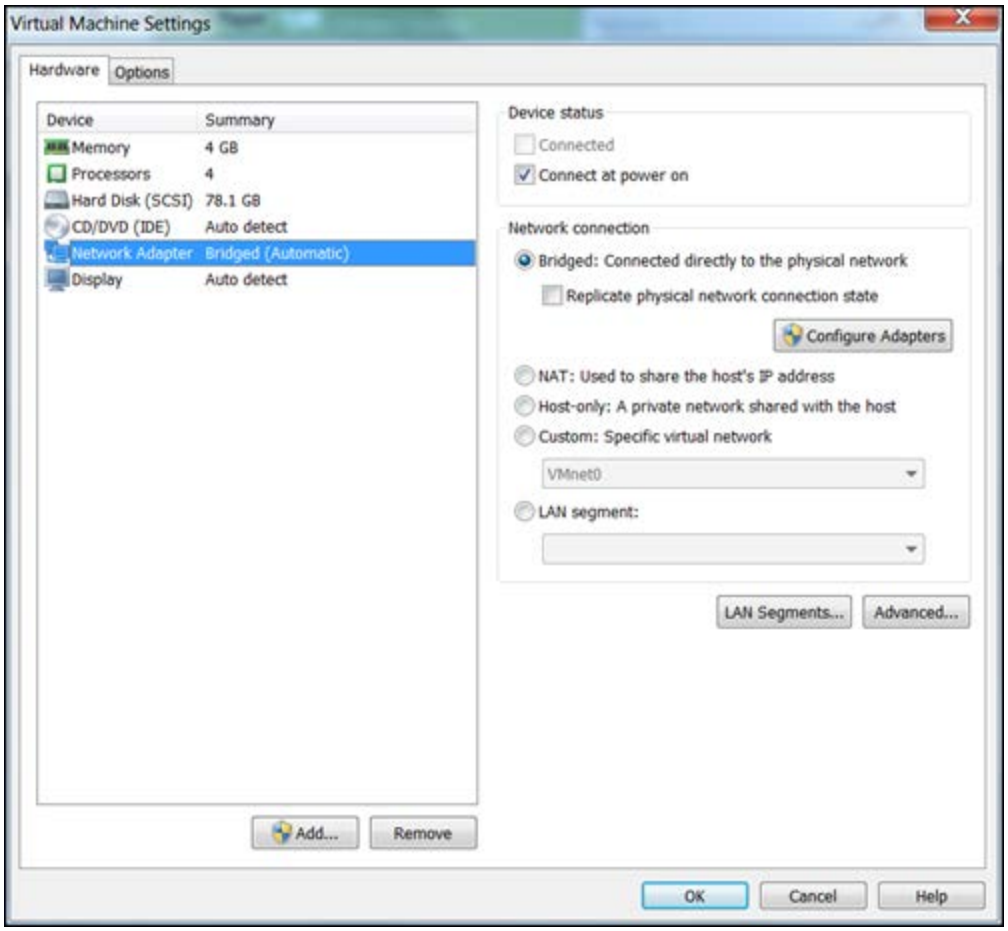
	NOTE: If you are evaluating more than 100 devices, we recommend to use 4 GB of memory and 4 processors.



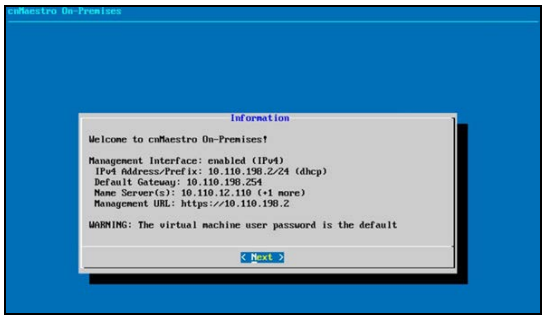
Configure Networking

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 LAN. Instead VMware should be configured so the virtual machine network interface is shared with the device.

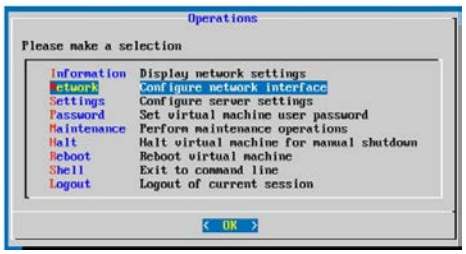
1. Set network adapter to be bridged.
2. In the VMware settings, select **Bridged** for the Network Adapter state and select the **Network Adapter** > **Configure Adapter.**



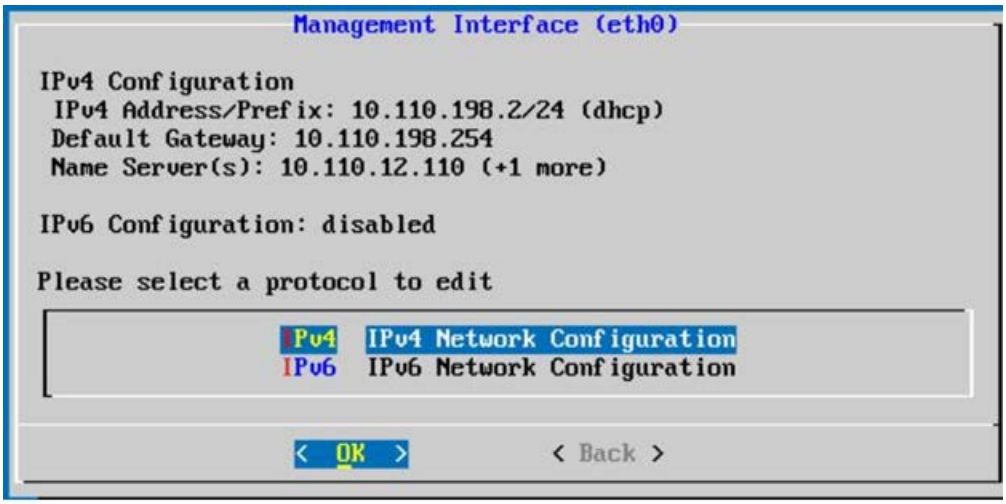
3. Restart cnMaestro.
4. Then restart the virtual machine and login. It displays the IP address from the LAN instead of local to the device.



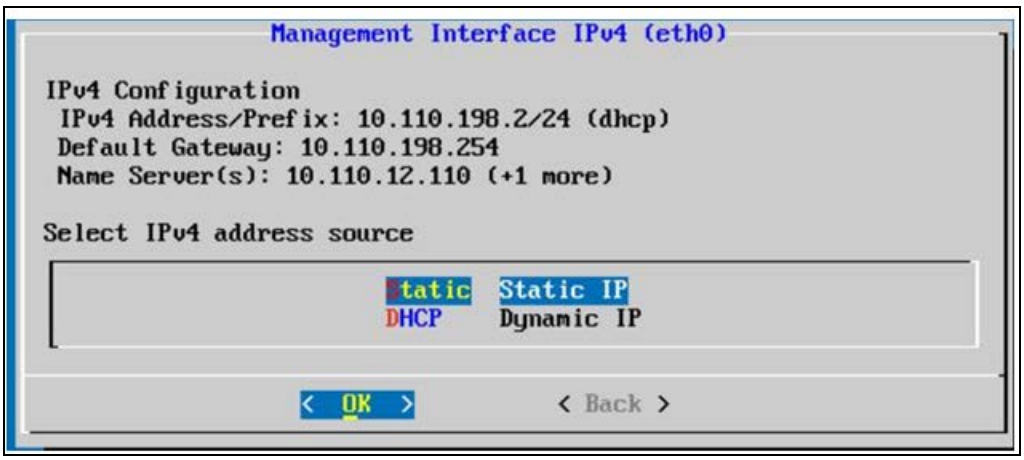
5. Click **Next** to view the **Operations** Menu and select **Network**.



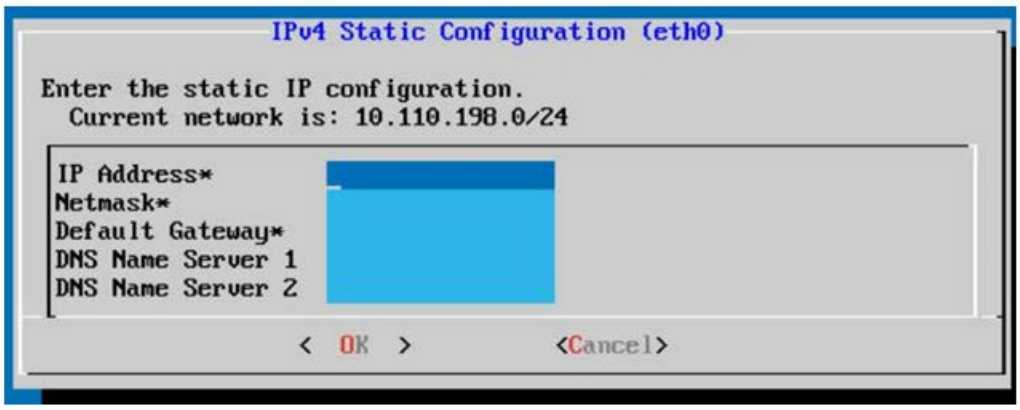
6. **Management Interface** window appears.



7. Select **Static IP Address.**



8. Configure **IPv4 Static Configuration** parameters.



cnMaestro supports a single eth0 interface.

Single Interface (eth0)

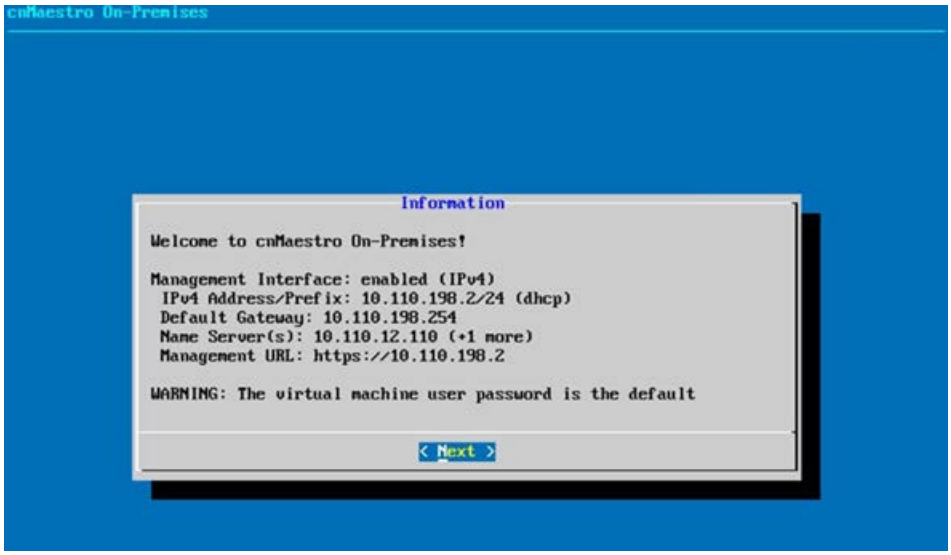
Name	Interface	Details
Management/Cluster/Device	eth0	User interface, cluster, API, device control traffic.

Protocols (IPv4, IPv6)

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

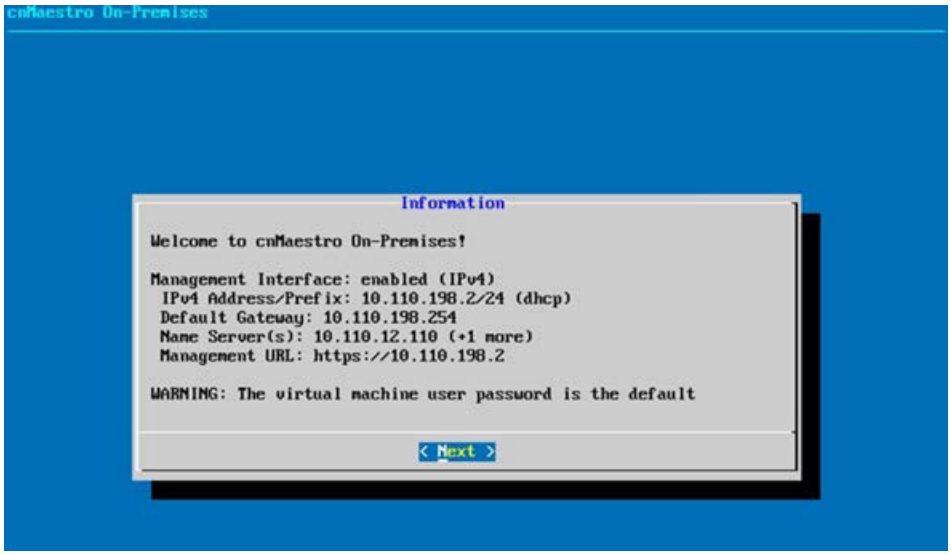
Information Page

The On-Premises **Information** page presents the high-level runtime network status for eth0 interface.



9. Validate the Changes.

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

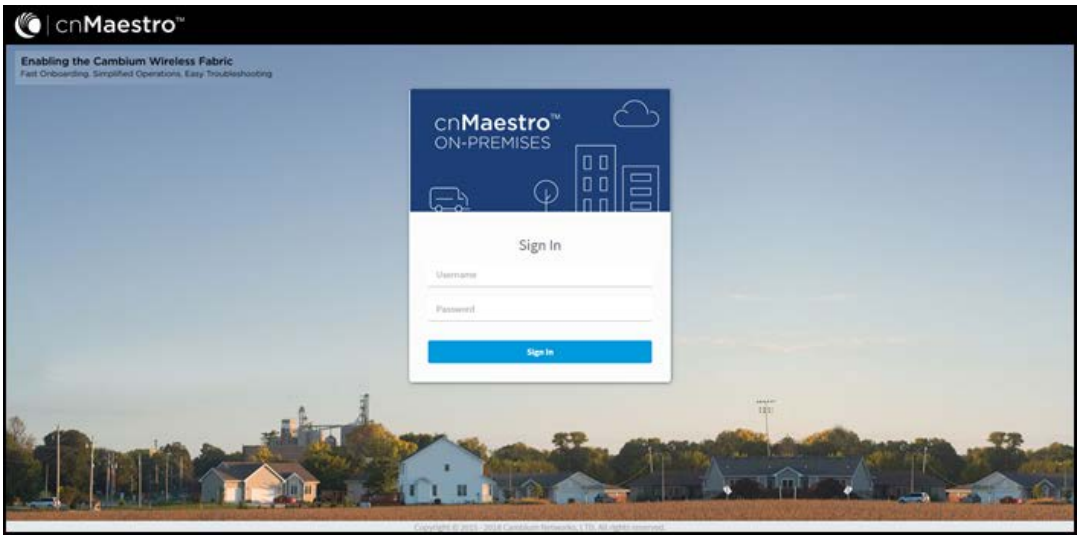


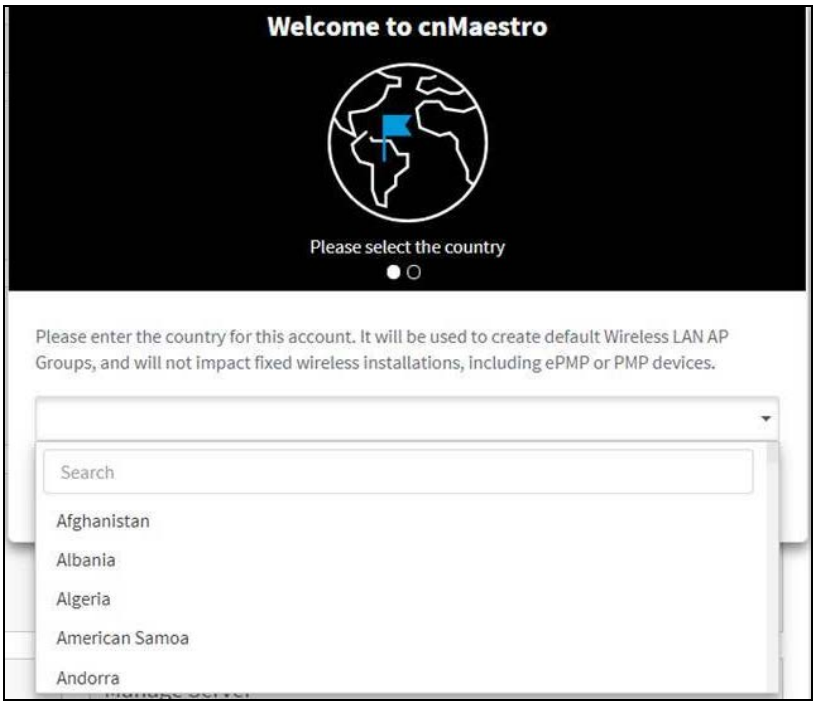
cnMaestro UI Access

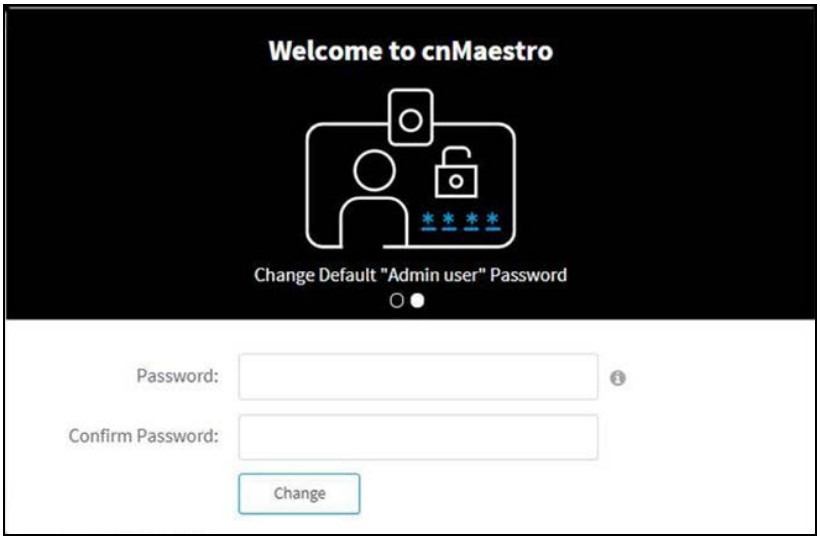
1. Access the UI through virtual machine by providing the IP Address.

The cnMaestro UI requires HTTPS. The default username/password are admin/admin.

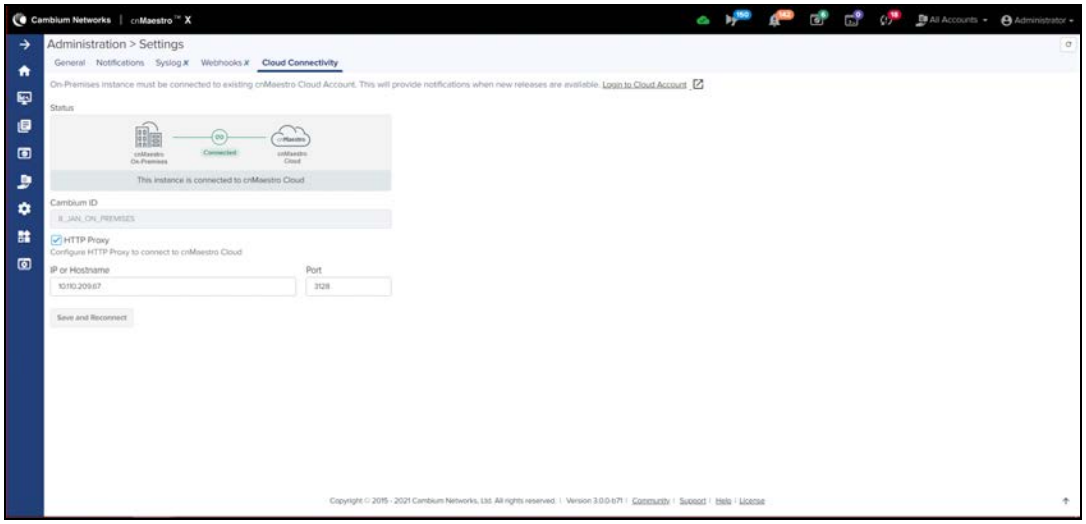
> **NOTE:**
> The browser will display an untrusted certificate error when you access cnMaestro On-Premises. This is because it uses a self-signed certificate.


cnMaestro
Enabling the Cambium Wireless Fabric
cnMaestro
ON-PREMISES
Sign In
Username
Password
Sign In


Welcome to cnMaestro
Please select the country
Please enter the country for this account. It will be used to create default Wireless LAN AP Groups, and will not impact fixed wireless installations, including ePMP or PMP devices.
Search
Afghanistan
Albania
Algeria
American Samoa
Andorra


Welcome to cnMaestro
Change Default "Admin user" Password
Password:
Confirm Password:
Change

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



> **NOTE:**
>
> In future cnMaestro releases, customers will be required to connect their On-Premises installation to the Cloud using an Anchor account, which is a special cnMaestro Cloud Account that communicates with On-Premises instances. This step is optional in this release, but Cambium Networks recommends customers do it now in preparation. To know more about the Anchor Account refer to Cloud Connectivity.

3. Navigate to **Administration > Server** to monitor and operate the virtual machine instance.

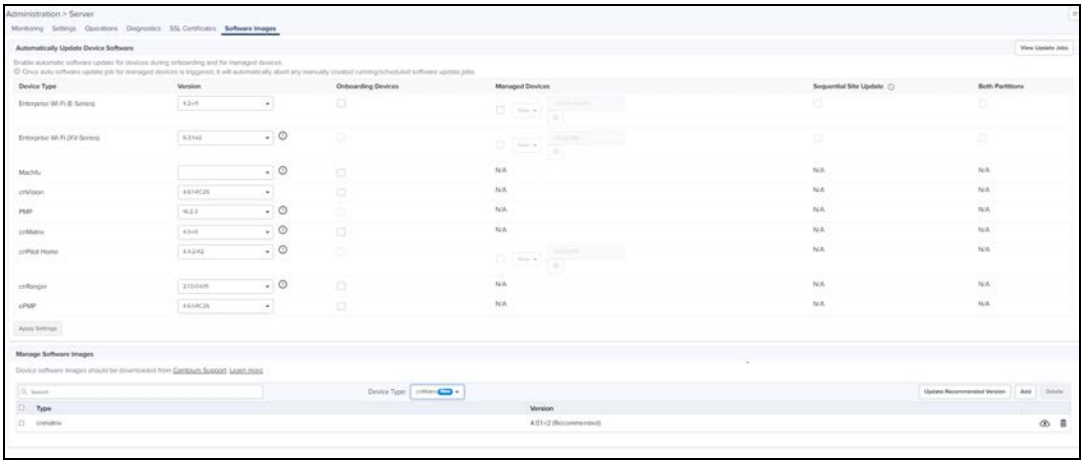
Device Software

> **NOTE:**
>
> By default, Cambium do not provide any builds during OVA upgrade, user can upload device build by clicking add image button. Once uploaded user can use download icon to download the available images or by two options on add image by clicking local and download from cloud. For further info refer to Manage Software Images.

Devices must have the correct beta 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.

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

Figure 2 Device Software



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

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

1. Static URL configured on the device

2. Using DHCP Option 43

3. Using DHCP Option 15

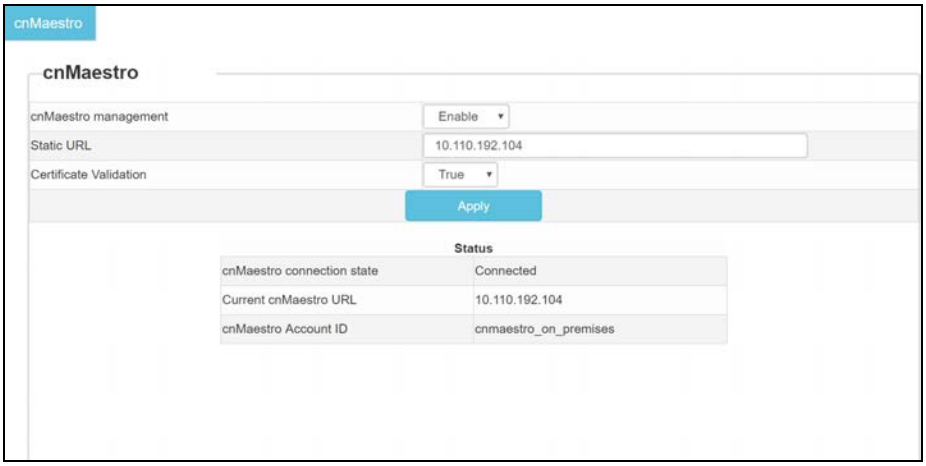
If none of these are present, the default action is to access the cnMaestro Cloud URL: https://cloud.cambiumnetworks.com

Static URL

If a static URL is configured in the device UI, the device will always try to connect using it.

cnMatrix

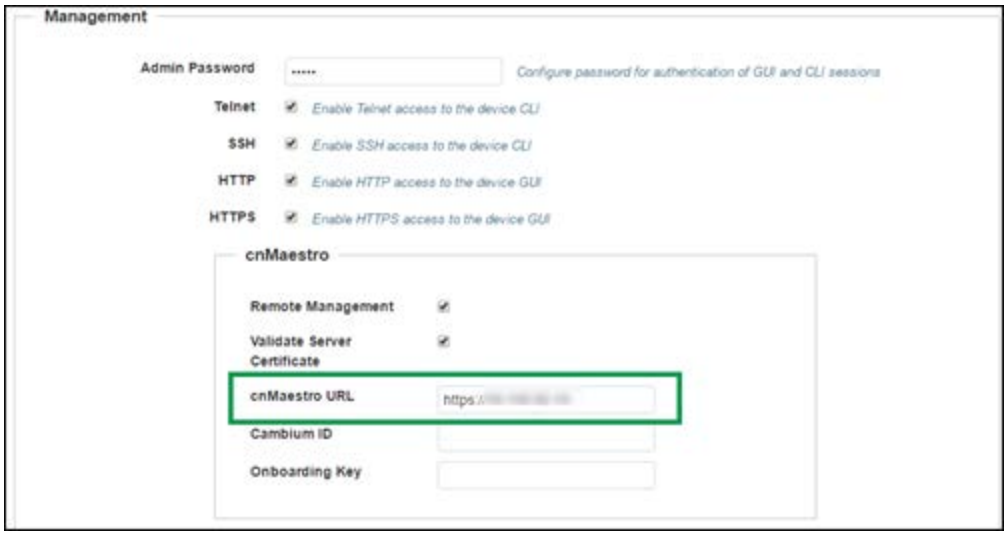
1. Navigate to **System > cnMaestro** tab.
2. Enter **static URL**.



cnPilot Enterprise

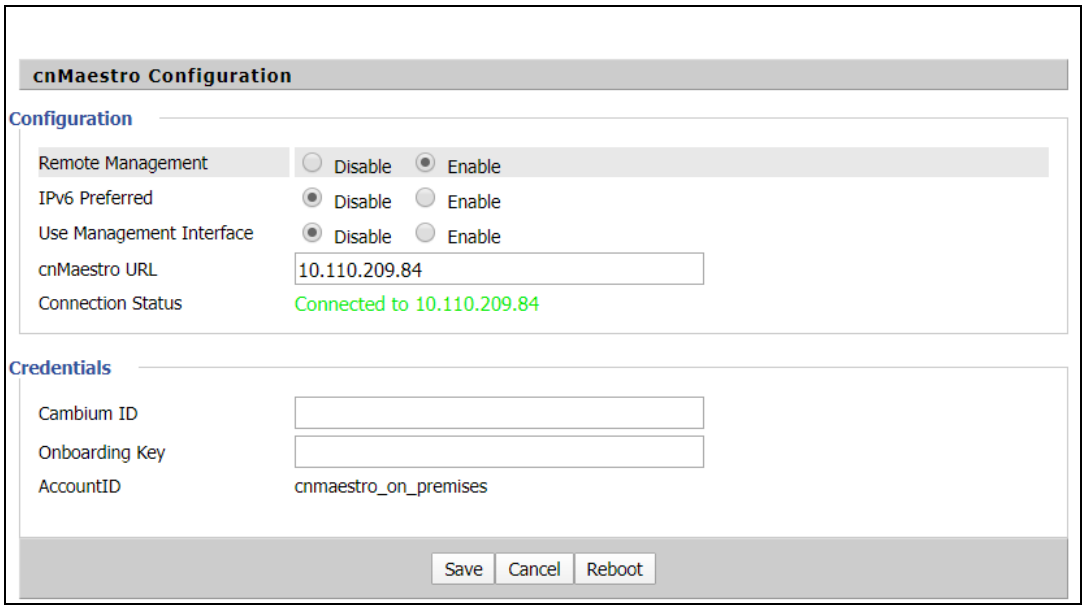
1. Navigate to **Configure > System > Management.**

2. Enter **cnMaestro URL**.



cnPilot Home

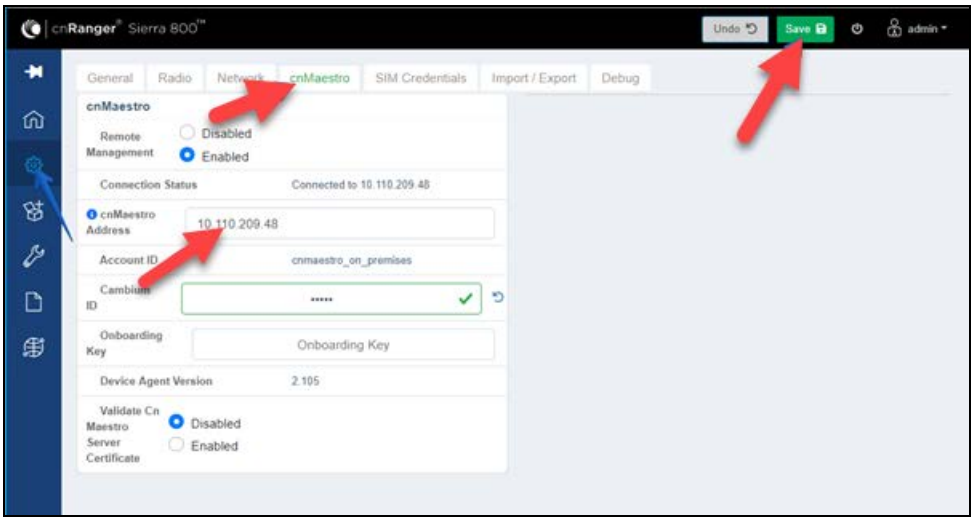
1. Navigate to **Administrator > cnMaestro** tab.
2. Enter **cnMaestro URL**.



cnRanger

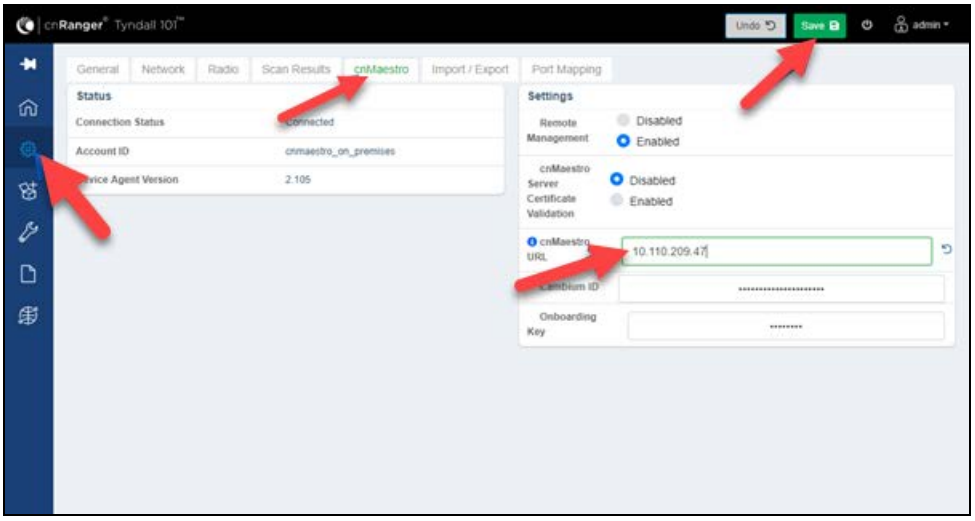
Setting static URL for cnMaestro on Sierra 800

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



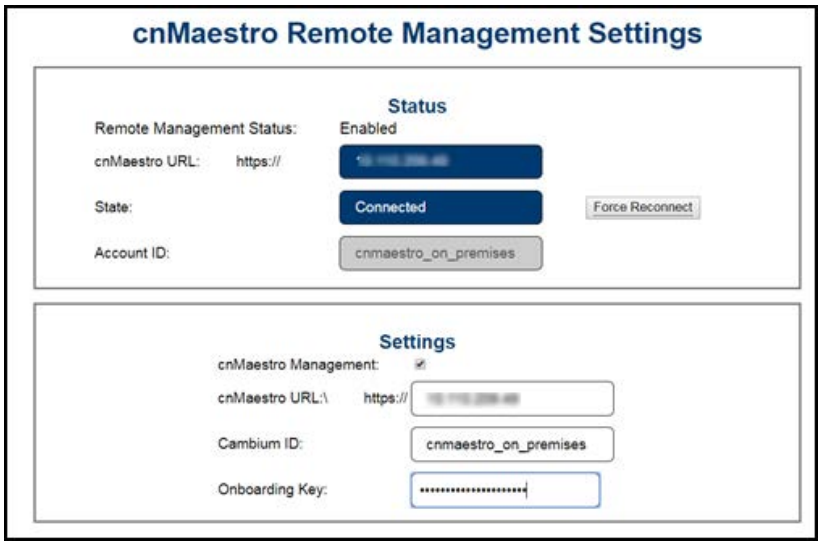
Setting static URL for cnMaestro on Tyndall 101

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



cnReach

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

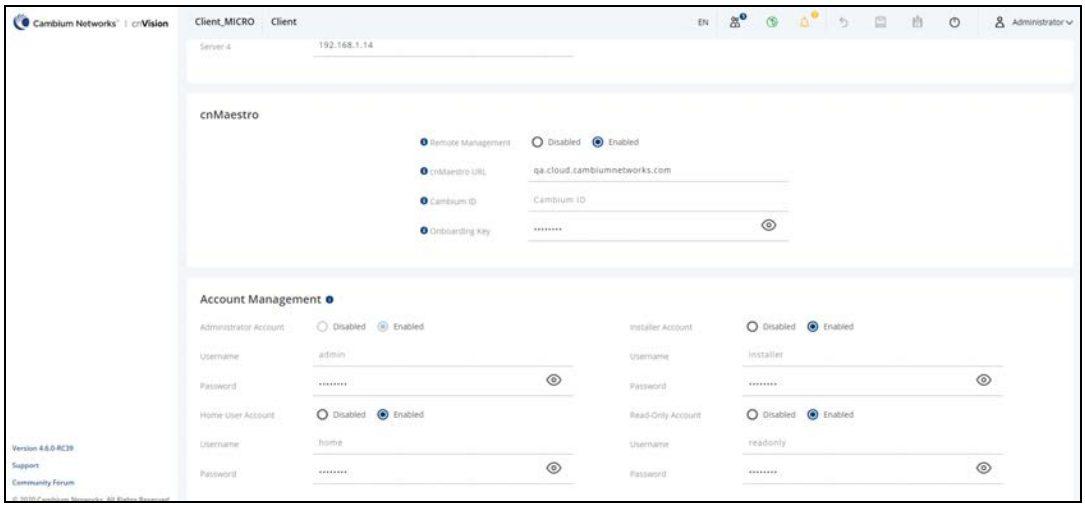


2. Click cnMaestro **Management** checkbox
3. Enter **cnMaestro URL**, **Cambium ID** and **Onboarding** key.

cnVision Client

In the cnVision Client device UI,

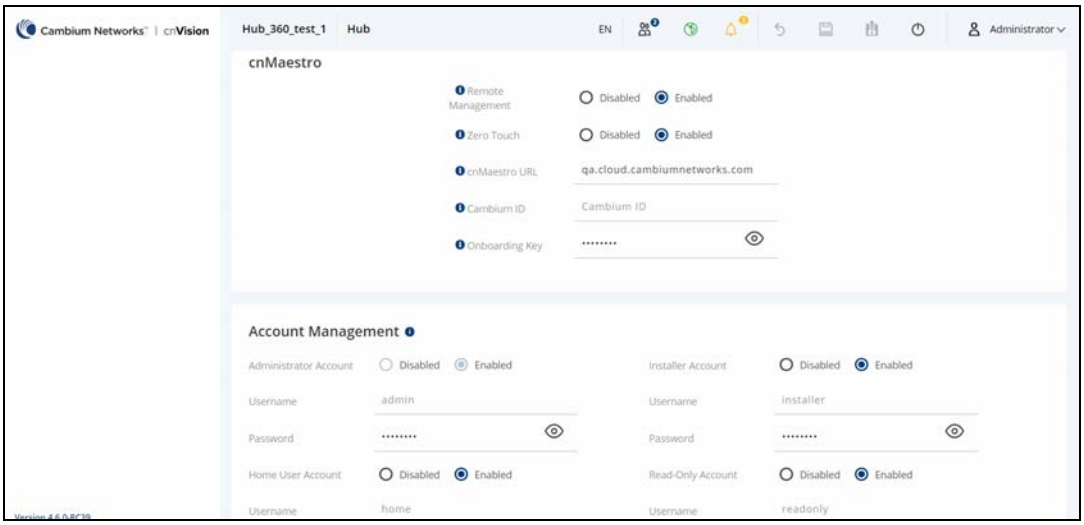
1. Navigate to **Configuration > System > Device Management**.
2. Under cnMaestro section, enter cnMaestro URL.
3. Click **Save**.



cnVision Hub

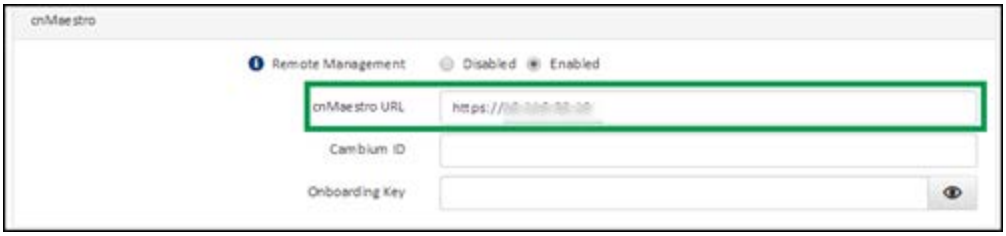
In the cnVision Hub device UI,

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



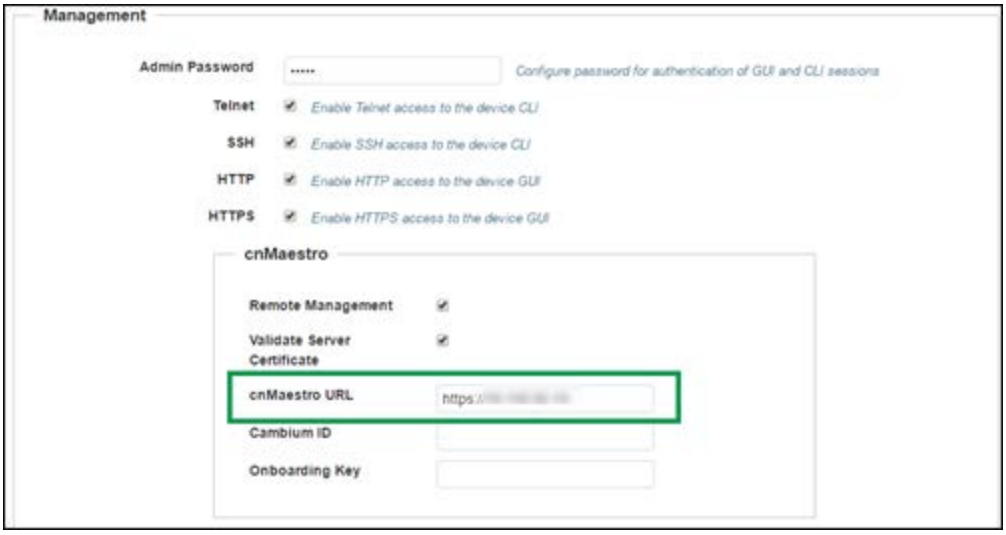
ePMP 1000 AP/SM

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



ePMP 1000 Hotspot

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

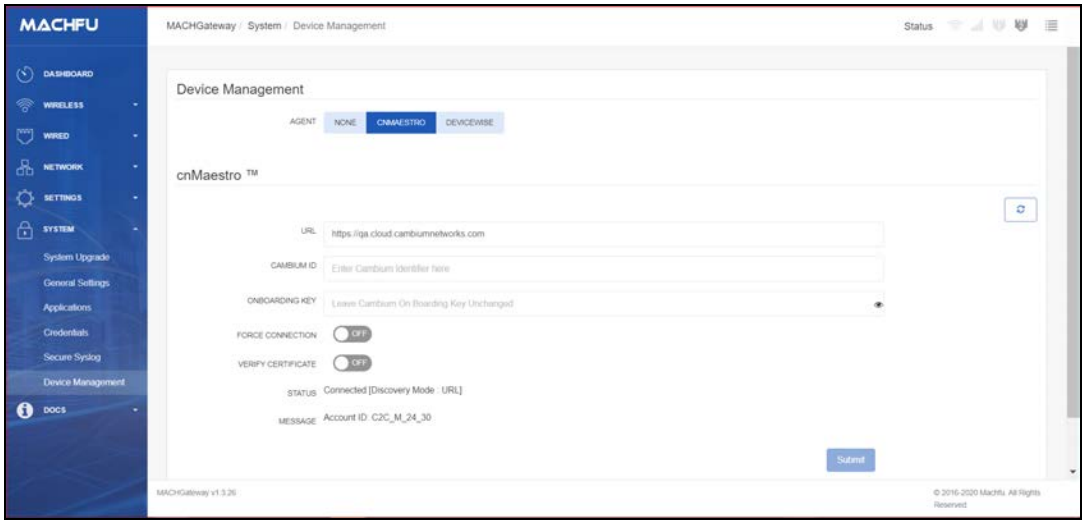


Machfu

In the Machfu device UI,

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

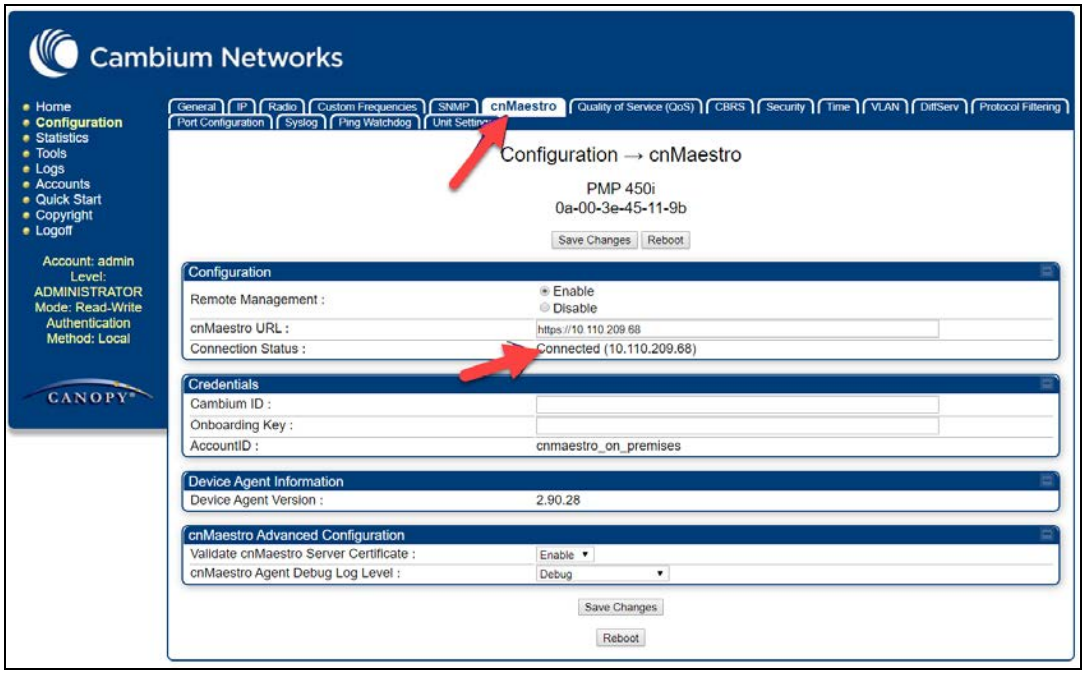
3. Click **Save**.



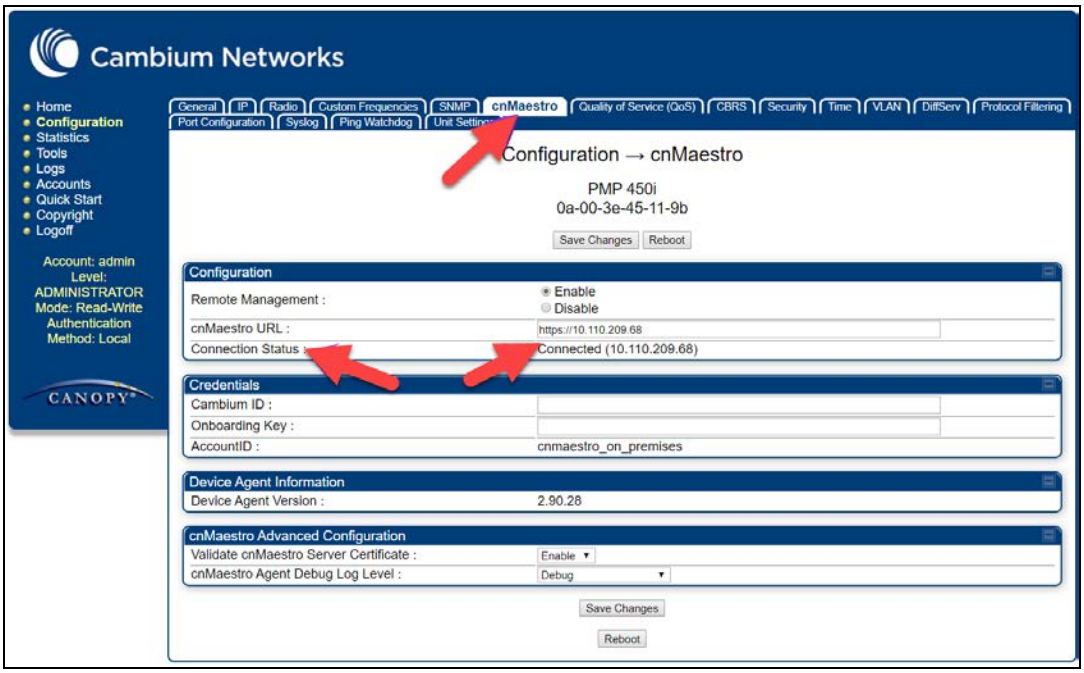
PMP

1. Navigate to **Configuration > cnMaestro tab**.

2.Enter **cnMaestro URL**.



4. To check the cnMaestro connection status, navigate to **Configuration > cnMaestro** tab > check **Connection Status.**



PMP Configuration Prerequisites

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

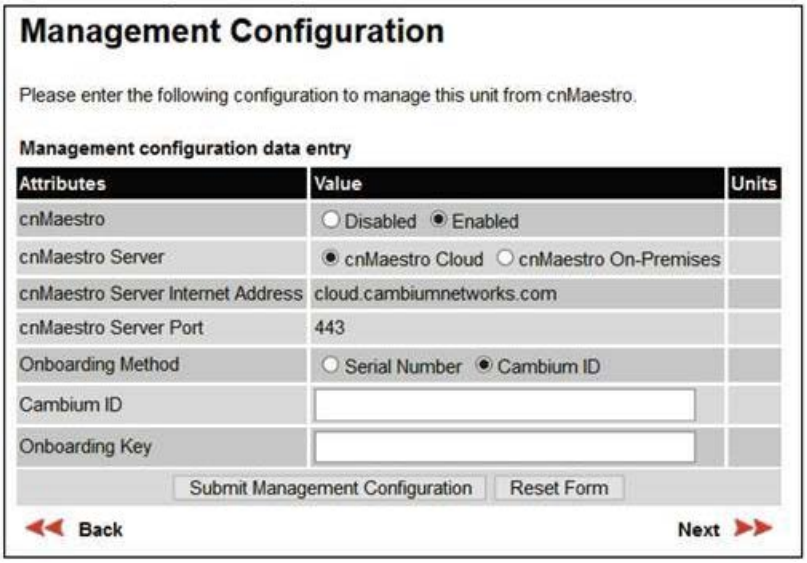
- Remote Management Interface with standalone config should be enabled.
- Remote Management IP address should be public IP address.
- DNS server configuration should be filled.

AP

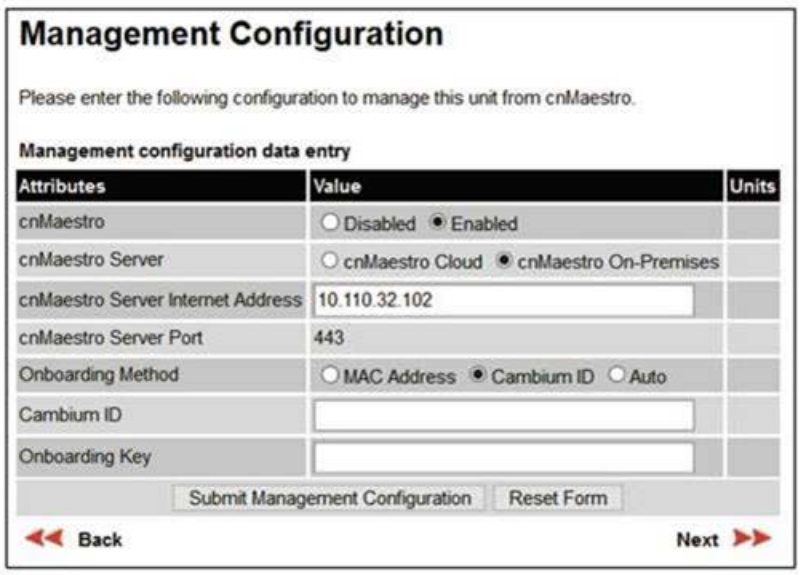
- IP address should be public IP address.
- DNS server configuration should be filled.

PTP

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



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



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 that will tell the devices how to access the cnMaestro (so the URL doesn't 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 Appendix: Windows DHCP Options Configuration for configuring DHCP options for windows.

NOTE:
DHCP Options, as described in this section, 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 (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:

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 450b SM	Cambium PMP 450b SM
PMP 450 SM	Cambium PMP 450 SM
PMP 450i AP	Cambium PMP 450i AP
PMP 450i SM	Cambium PMP 450i SM
PMP 450i BHM	Cambium PTP 450i BHM
PTP 450i BHS	Cambium PTP 450i BHS
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”, then 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

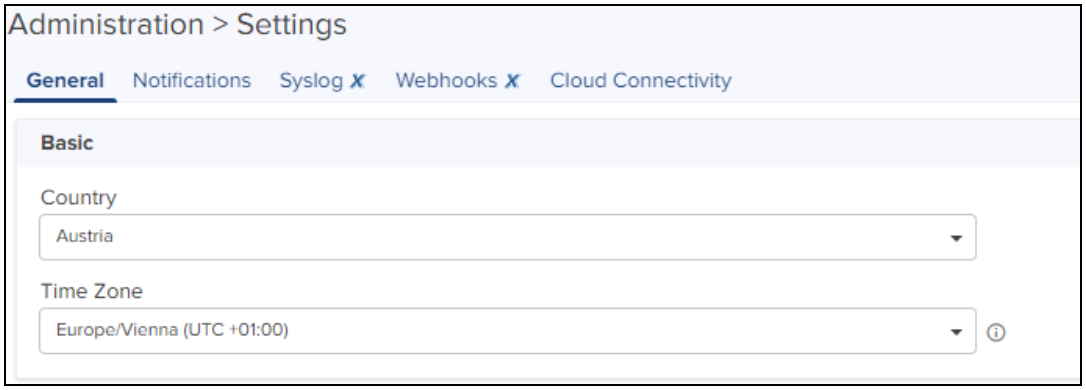
cnMaestro On-Premises provides a number of ways to navigate its content.

This section includes the following topics:

- Basic
- Account View
- Home Page
- Page Structure
- UI Navigation
- Access and Backhaul Account
- Enterprise Account
- Side Menu
- Section Tabs
- System Status
- Logout

Basic

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

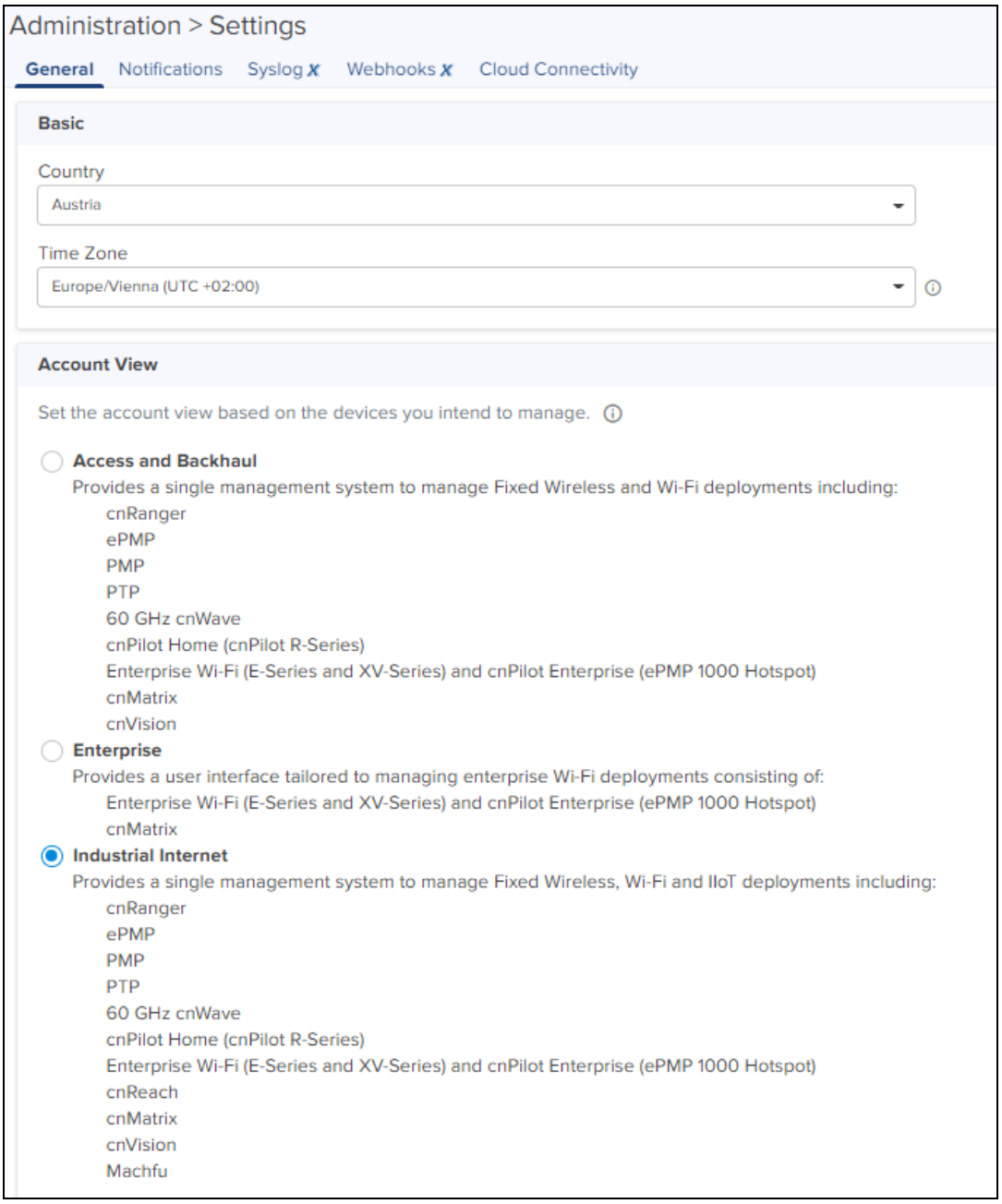


NOTE:

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

Account View

cnMaestro supports three separate account view, based upon the composition of devices installed. The type is set when the UI is first accessed, but it can be changed later through the **Administration > Settings** page.



Access and Backhaul Account

The Access and Backhaul Account supports all fixed wireless and Wi-Fi deployment devices as well as wireless LAN. The device types include 60 GHz cnWave, cnMatrix, cnPilot Home (cnPilot R-Series), cnRanger, cnVision, ePMP, Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot), PMP, and PTP.

Enterprise Account

The Enterprise account supports the Enterprise Wi-Fi deployments, which includes the cnMatrix, Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot). It provides a simplified UI that only displays Wi-Fi components (hiding fixed wireless features such as Towers).

The account type can be changed at any time, with the following restriction: to select the Enterprise view, all devices other than cnMatrix, Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot)need to be removed from the account.

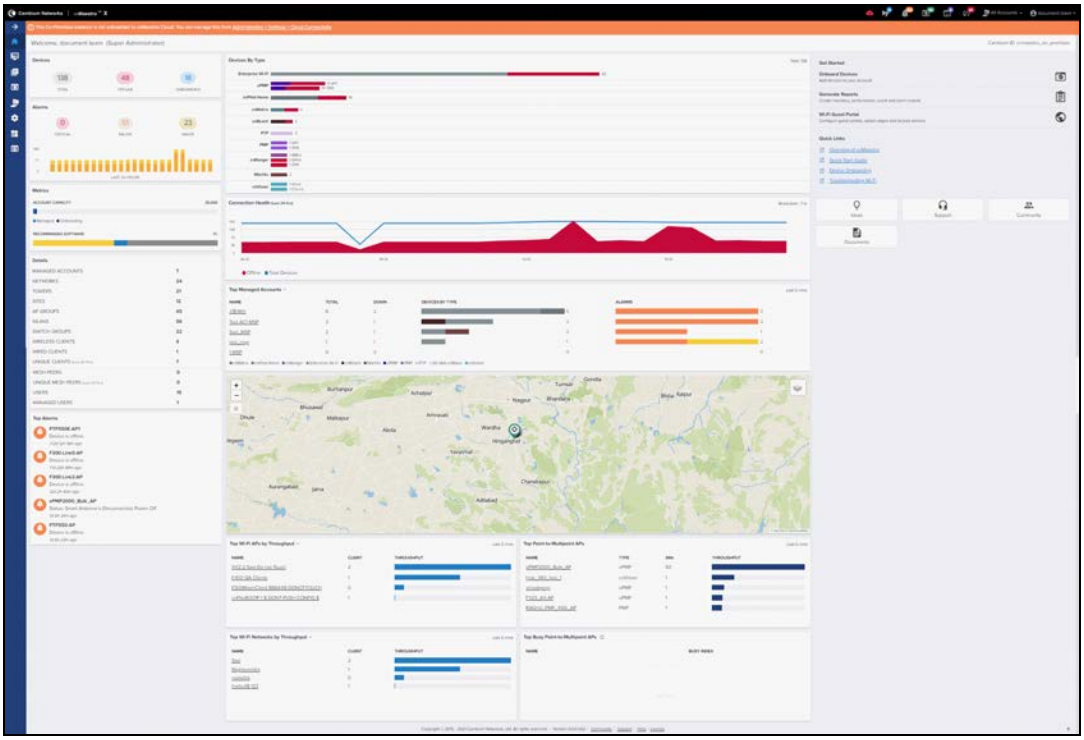
Industrial Internet Account

Industrial Internet Account provides a single management system to manage fixed wireless, Wi-Fi, and cnReach deployments. The device types include 60 GHz cnWave, cnMatrix, cnRanger, cnReach, cnPilot Home (cnPilot R-Series), cnVision, ePMP, Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot), Machfu, PMP, and PTP.

Home Page

The Home Page is the first page displayed when the user logs into cnMaestro On-Premises. It provides links to the core functional areas in the UI, as well as Cambium Networks support center, community, and documentation. It can be accessed from any page in the UI by clicking the **Home** tab.

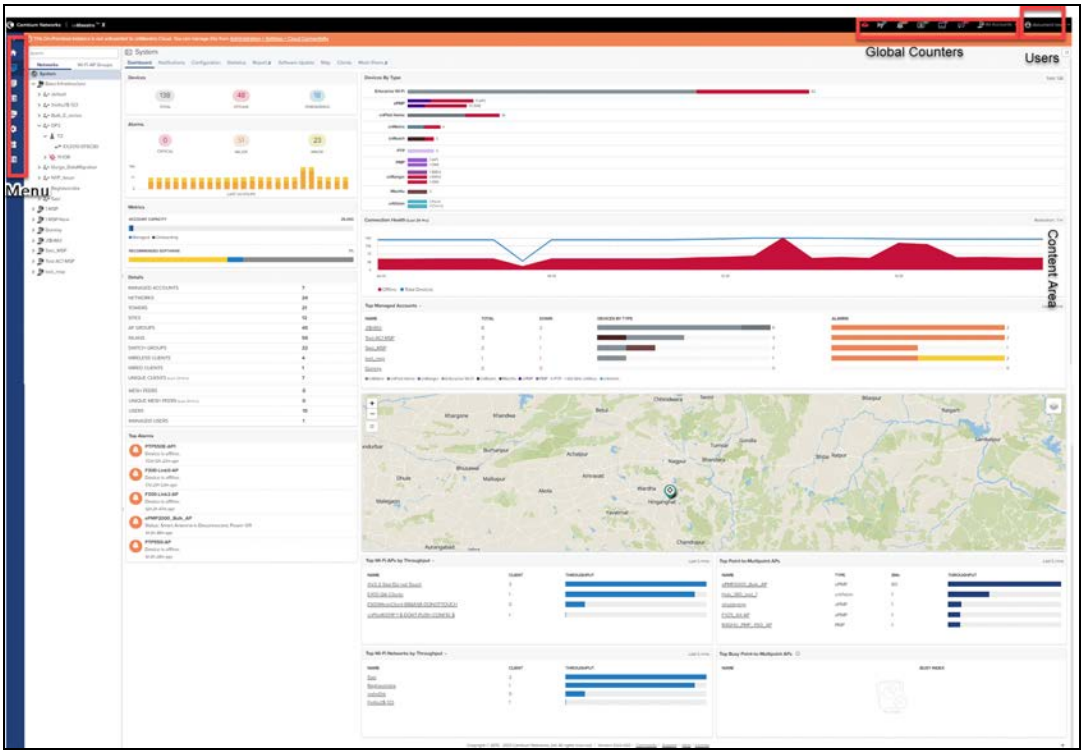
Figure 3 cnMaestro On-Premises - Home Page



Page Structure

Most of the cnMaestro On-Premises pages follow a standard structure, which consists of a left-side menu and a content area. In many pages, tabs provide navigation through the content for a particular section.

Figure 4 cnMaestro On-Premises - Page Structure



Page Navigation

The cnMaestro On-Premises pages include tabs such as **Configuration, Statistics, Report, Software Update, Map, Clients, Mesh Peers, Tools, Dashboard**, **Notifications**, **Software Update**, and **Tools**. 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 level. The context, or level in the hierarchy, is selected in the device tree, which is defined below.

Menu

The Menu provides basic navigation to all the pages in the UI. The menu is different between the Access and Backhaul view and the fixed wireless view.

Header

The page header supports basic counters for alarms, onboarded devices, pending jobs, MSP global filter if MSP is enabled, and out-of-sync devices.

Access and Backhaul Account

Overview

The Access and Backhaul view is similar to the Enterprise view, with the exception it leverages a hierarchical tree to display device installations. In this view, customers are able to group their fixed wireless devices into networks, and display their point-to-multipoint devices in tower-based sectors. All navigations are performed using the tree.

Device Tree Navigation

The device tree is segmented into two tabs: Network and Wi-Fi AP Groups.

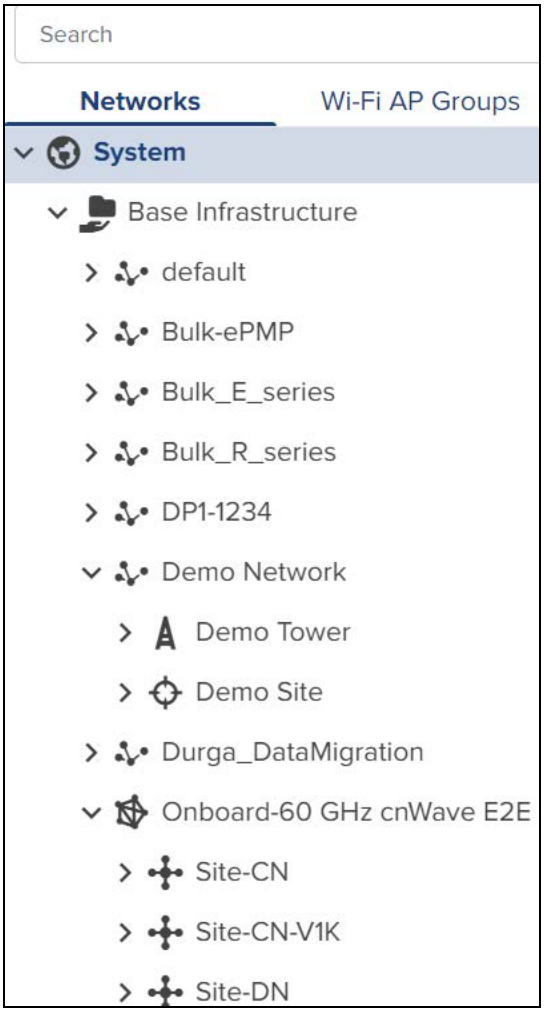
Networks Tab

The **Networks** tab displays a hierarchical view of the devices. It consists of **System, Networks, Towers, Sites, PoPs, DNs, CNs and Devices** (**Towers** are only visible in the fixed wireless view) and (PoP is only visible in the 60 GHz cnWave E2E Network). There is a strict ordering for how nodes can fit in the hierarchy, and as one navigates through and selects nodes, the pages update to display data from the node chosen.

The user can navigate the nodes by single-clicking a row to select it, thereby updating the content area to display the data from the node. Selecting an arrow icon opens the node and displays the next level of hierarchy. Note

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

Figure 5 Device Tree Navigation



The structured hierarchy has the following devices:

Table 8: Structured Hierarchy Nodes

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

Table 8: Structured Hierarchy Nodes

Icon	Name	Description
	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	PTP Master device located in a network and optionally mapped to a Tower.
	PTP Slave	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 a Network or launch the Software Update 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) and the devices like 60 GHz cnWave. The actions supported across the tree include the following:

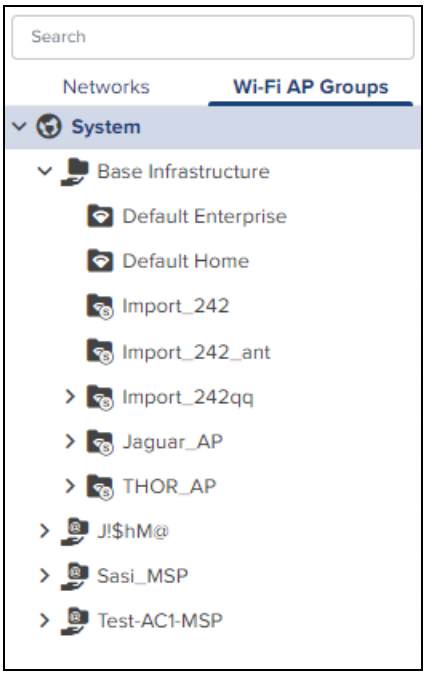
Table 9: Tree Menu

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 cannot be edited.
Flash LEDs	Enterprise Wi-Fi	The LEDs of the device enables to identify and locate the device.
Reboot	Devices	Reboot the device.
Refresh	All	Refresh the node in the tree. This refreshes the node and its children only, not the entire tree.
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.
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 **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 aggregate statistics for the devices managed and present them within the AP Groups dashboard.

Figure 6 Wi-Fi AP Groups



Map Navigation

Maps are presented in dashboard screens as well as a dedicated map display. Maps often show Tower, Site, and Devices located in proximity. Map nodes can also be double-clicked to navigate to the selected Device, Site, or Tower. By selecting a node in the map, the Device Tree gets updated to reflect that node.

Figure 7 Map Navigation

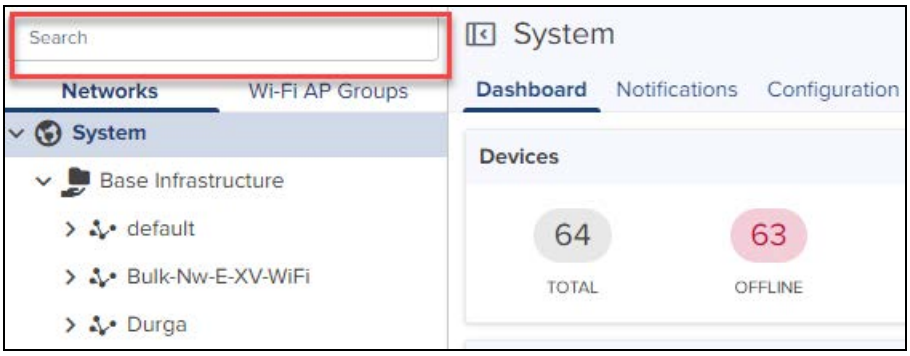
Table Navigation

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 IP Address, Serial Number, Device Name and MAC Address. Once the node is found and selected, one can jump to it in the hierarchical tree.

Figure 8 Node Search



Enterprise Account

Overview

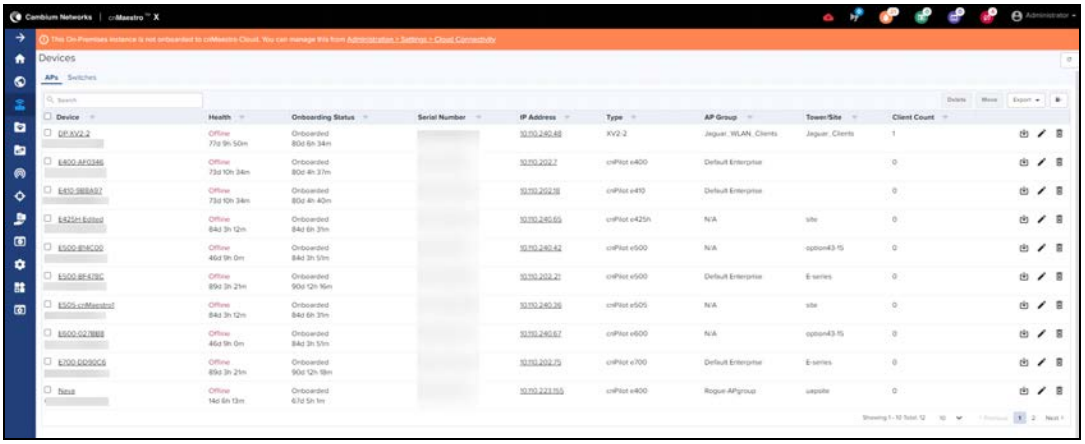
The Enterprise account differs from Access and Backhaul in that it is largely table-driven. It does not have the quick buttons or the Device Tree, instead it has direct navigation for APs, AP Groups, WLANs, and Sites. Each of these are presented in tabular form, and clicking on the row entry will launch the management page.

System

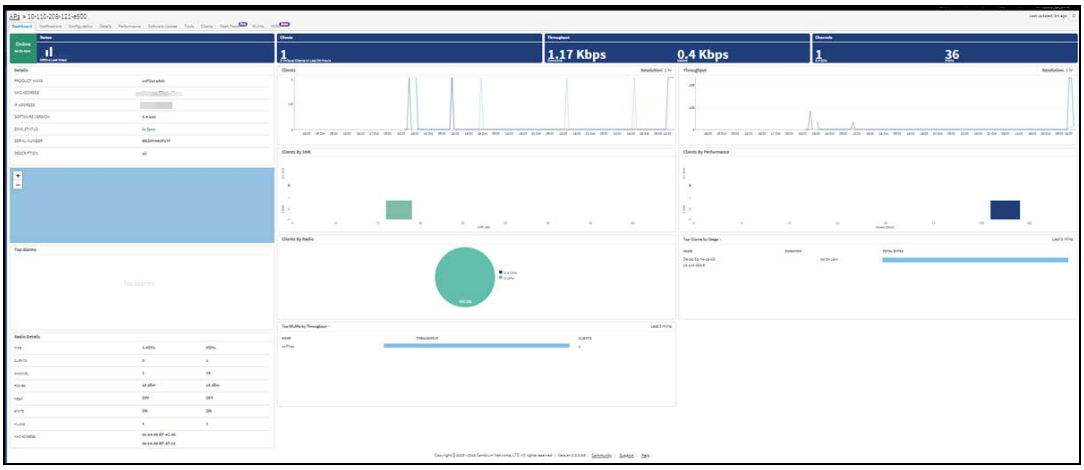
The System Dashboard and global functionality is presented in the **System** menu. It aggregates data across the entire installation.

Devices

The **Devices** section provides a searchable table listing all the APs and the Switches in the system.



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, Reports, etc.

Figure 9 AP Groups

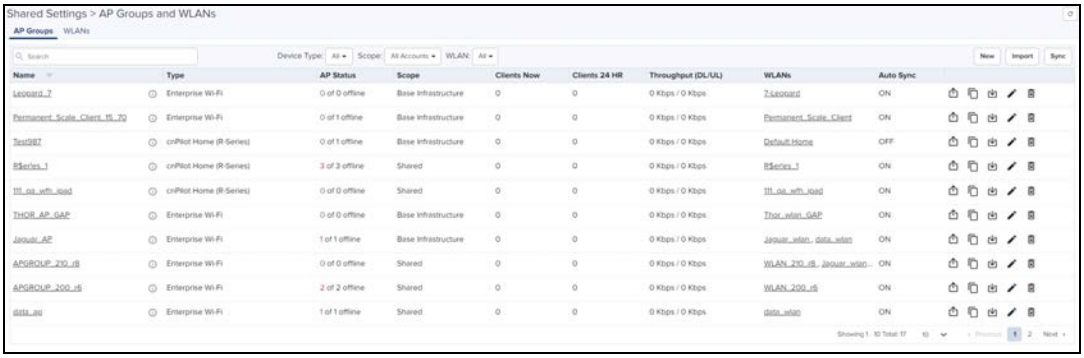
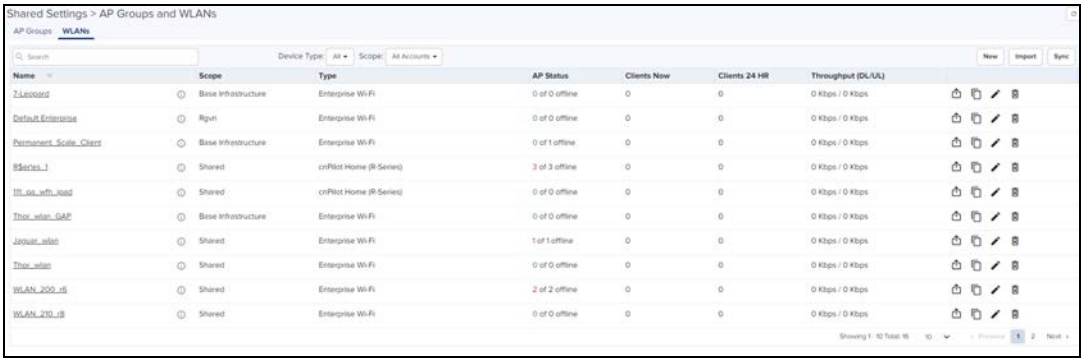


Figure 10 WLANs



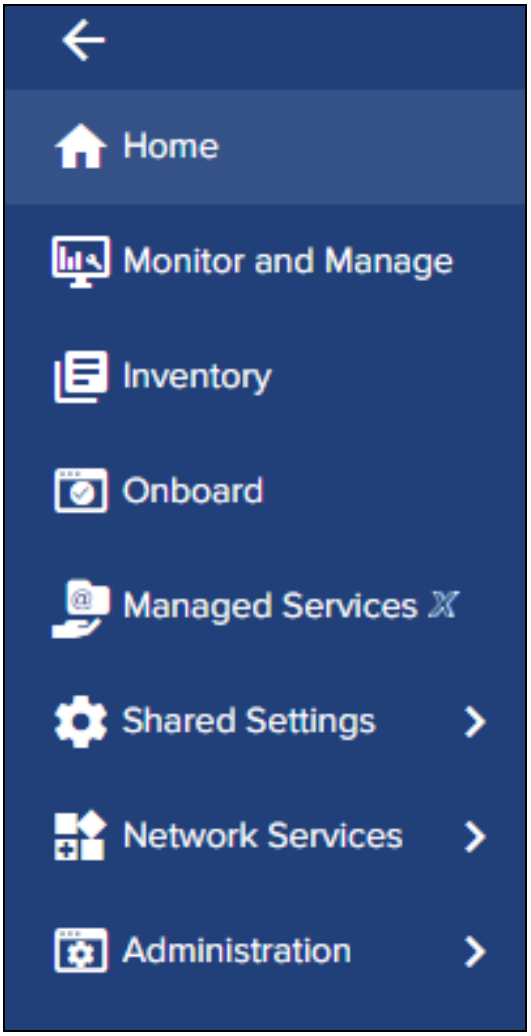
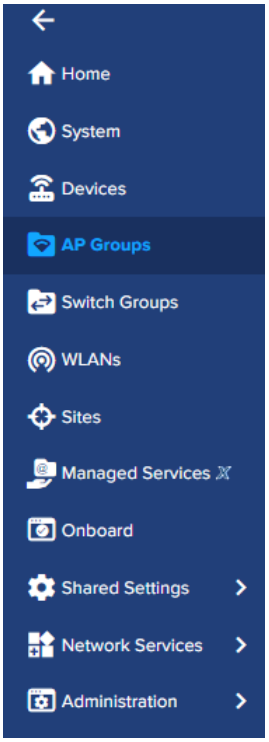
Sites

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

Side Menu

The side menu provides high-level navigation through the cnMaestro UI. Click **pin** icon at the top to expand/collapse.

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

Side Menu for Access and Backhaul View and Industrial Internet	Side Menu for Enterprise View
	

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 10: Section Tabs

Page	Tabs
Site	Dashboard | Notifications | Configuration | Statistics | Report | Floor Plan | APs | Clients | WIDS | Mesh Peers
System	Dashboard | Notifications | Configuration | Statistics | Report | Software Update | Clients| Map | Mesh Peers
Wi-Fi AP	Dashboard | Notifications | Configuration | Details | Performance | Software Update | Tools | Clients | Mesh Peers | WLANs | WIDS
Wi-Fi AP Group	Dashboard | Notifications | Configuration | Statistics | Report | APs | Clients | Mesh Peers

System Status

The UI header has a number of system status icons that provide a single point to view selected global statistics and operations parameters. Their meanings are highlighted below:

Table 11: System Status Icons

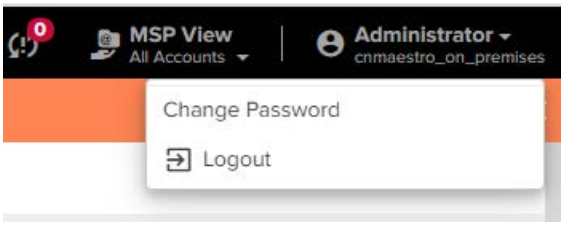
Icon	Name	Description
	Active Software Upgrade Jobs	The number of devices in the onboarding queue that are registered to the account but which need to be manually accepted prior to completing their onboarding.
	Announcements	If cnMaestro Cloud is synced with the On-Premises announcement notifies the latest 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 appropriate UI page for management.

Logout

The user icon in the upper right corner allows the user to logout of cnMaestro On-Premises.

Figure 11 Logout



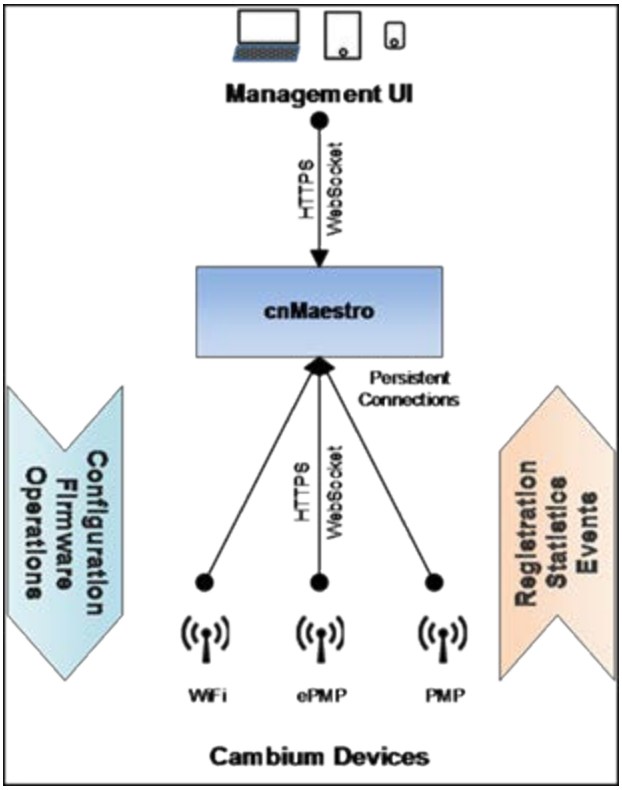
Architecture

Overview

The cnMaestro On-Premises architecture is similar to cnMaestro Cloud: devices connect to cnMaestro over HTTP, with Cloud, the devices access cloud.cambiumnetworks.com. With On-Premises, the devices must be configured with the IP Address/URL of the cnMaestro instance.

A simplified architecture diagram is below:

Figure 12 On-Premises Architecture



The management connection to cnMaestro is initiated by the devices and remains persistent. Traffic flows in both directions: devices forward events and statistics to the cnMaestro server, and cnMaestro applies configuration, updates software, and executes operations on the devices.

Networking

Devices to contact cnMaestro, they must be configured with its IP address or hostname. This is accomplished using the device UI or SNMP. Alternatively, the URL can be configured on the DHCP server and propagated to the device through DHCP options (when the device retrieves its IP address). Customers who own their DHCP infrastructure generally prefer this method.

NOTE:
1. Devices must have a route to the cnMaestro On-Premises server in order to be managed.
2. You should configure a static IP address or hostname for cnMaestro server, so it will persist over time.
3. An outbound connection from the Cambium Device must be allowed for port 443.
4. An outbound connection will also be required for port 80 with 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 443.

- 60 GHz cnWave (E2E Controller) 1.0.1-r2
- 60 GHz cnWave (Node) 1.0.1
- cnPilot E-Series / ePMP 1000 Hotspot: 3.2.1-r6
- cnPilot R-Series: 4.4.2-R2
- cnReach: All versions
- cnRanger 1.0.1.0-r1
- ePMP: 3.2
- PMP: 15.0.1
- PTP: All versions

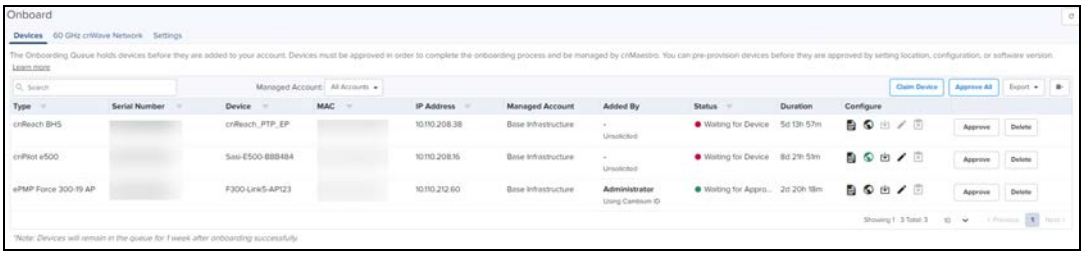
Device Onboarding

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.

> **NOTE:**
> Onboarding devices is different between Cloud and On-Premises. With On-Premises, when a device is configured with the cnMaestro URL, it is placed in the onboarding queue by default, from which it can be approved into the account. In contrast, with Cloud one needs to enter the serial number 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.

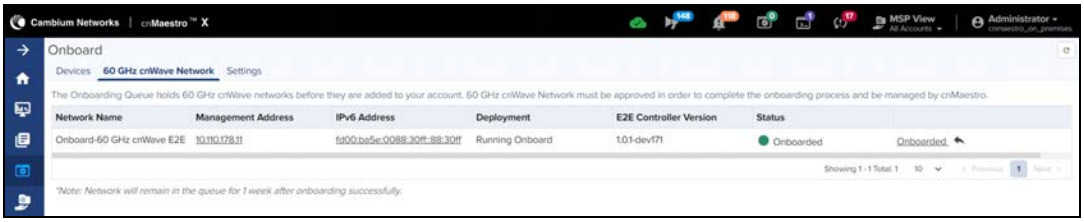
Figure 13 Onboarding Devices



60 GHz cnWave Onboarding

The Onboarding queue holds 60 GHz cnWave E2E Networks before they are added to the account until the user approves the E2E Controller Network to complete the onboard process by accessing through the **Onboard** page or Tree menu.

Once the onboarding process is approved and it can be managed by cnMaestro.

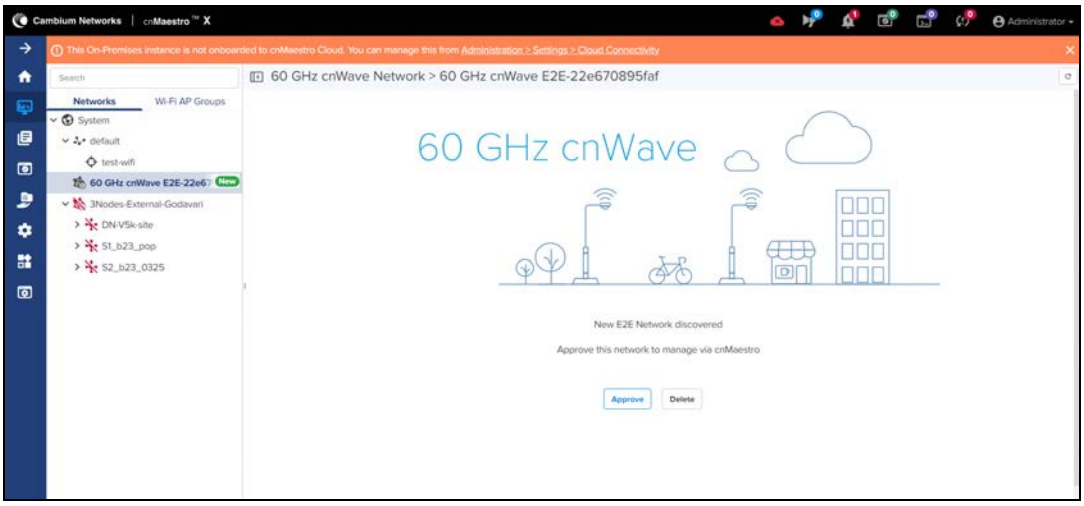


> **NOTE:**
> If **Auto Generate IPv6 Addresses** is enabled, E2E Controller fetches the IPv6 addresses automatically.

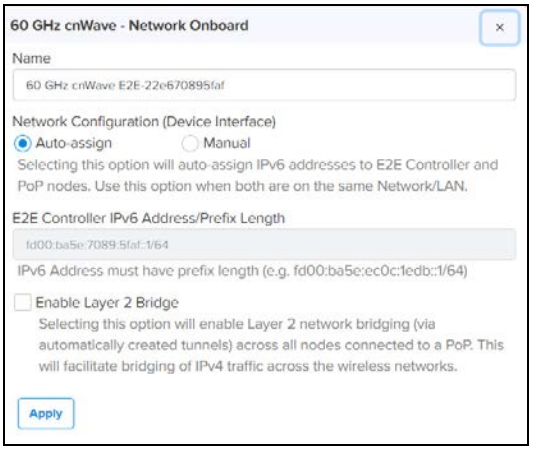
External E2E Controller Onboarding

To Onboard the E2E controller Network through **Manage** page:

1. Navigate to **Manage > Network >** select **60 GHz cnWave E2E Controller**
2. Click **Approve** and **60 GHz cnWave – Network Onboard** window pops-up.

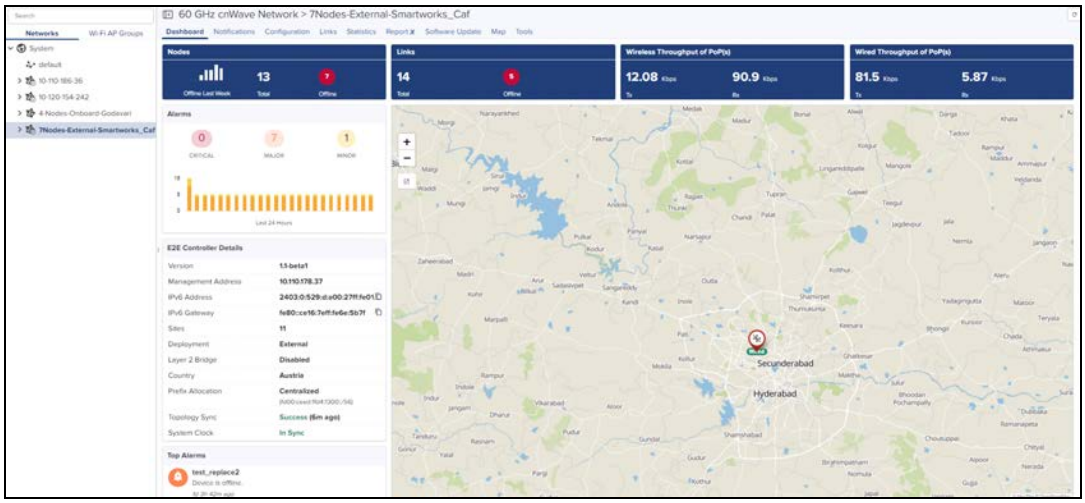


3. By default **Auto-assign** is selected User can select either **Auto-assign** or **Manual** to update IPv6 address in E2E Network and wait for a while utill IPv6 address gets updated.
4. After the updation, user can **Enable Layer 2 Bridge** which is optional.

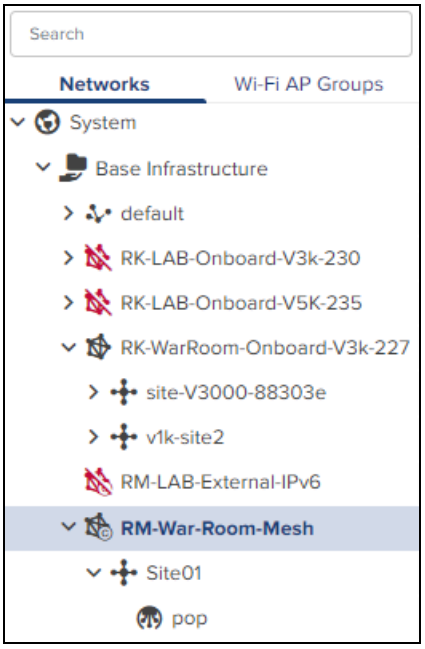


5. Click **Apply.**
6. Wait for a while till network onboard is successful.

7. Once it is successfully onboarded, the E2E Network UI shows the Dashboard of the network as shown below:



External E2E Controller network icon will be indicated with icon as shown below:

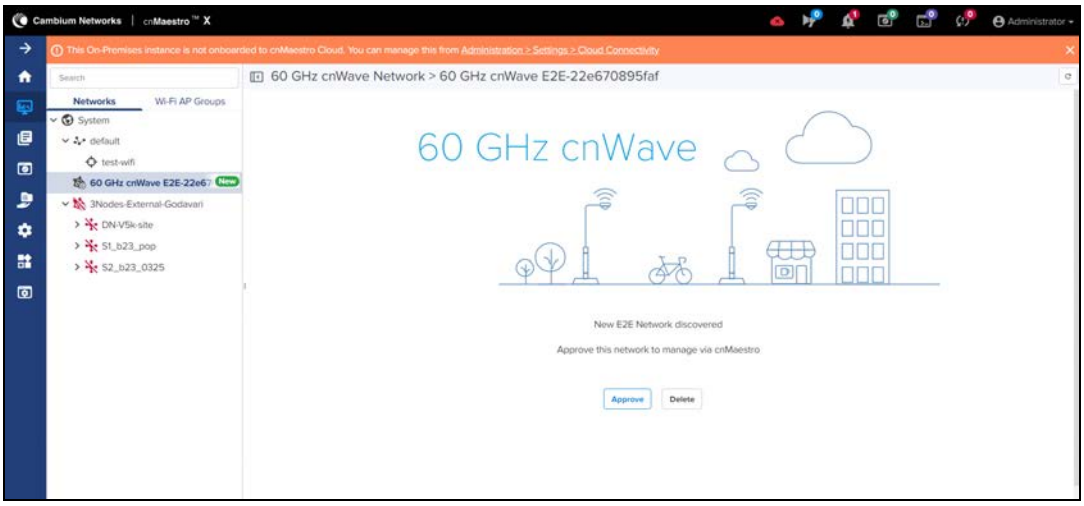


Device E2E Controller (Running Onboard) Onboarding

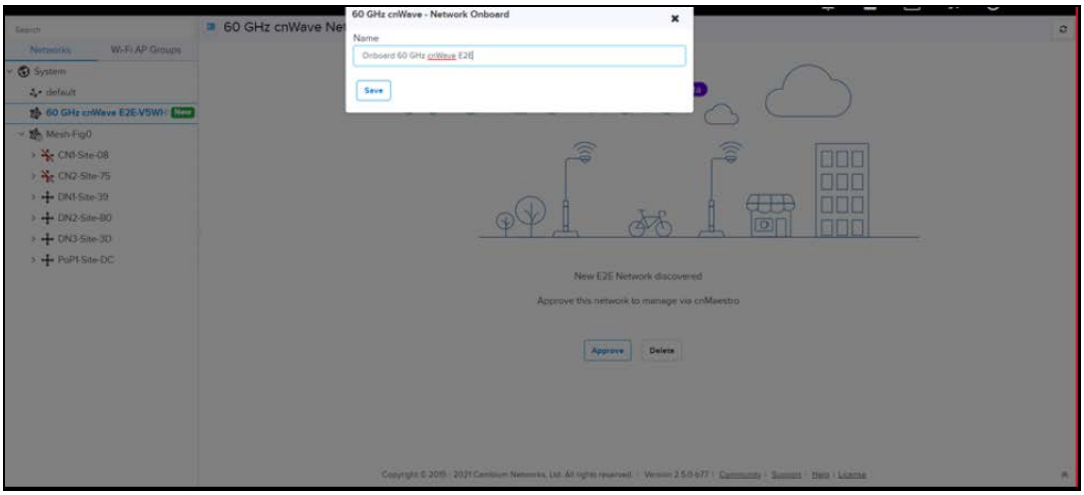
Once cnMaestro remote management details are configured through onboard E2E controller. The E2E controller network will be discovered in the cnMaestro.

To approve proceed as follows:

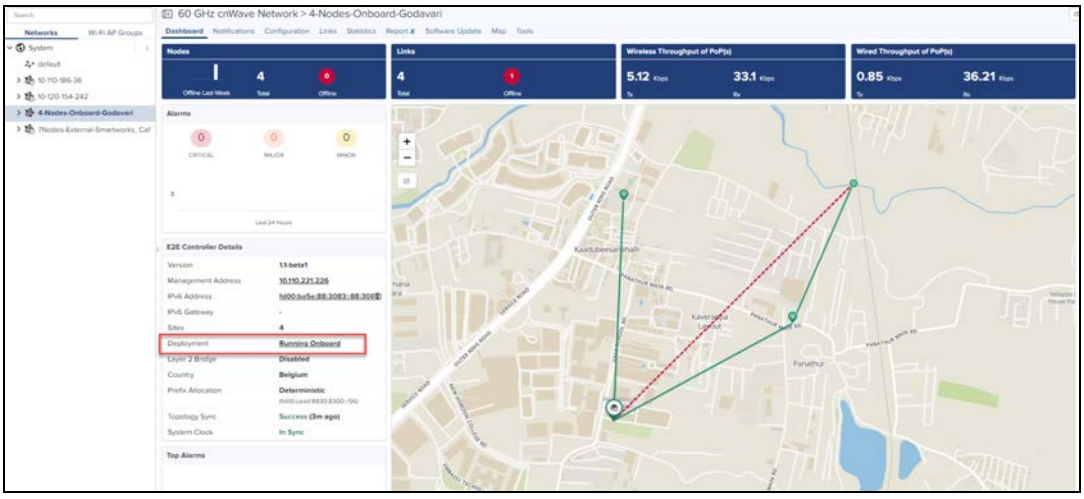
1. Navigate to **Manage > Network >** select **60 GHz cnWave E2E Network.**
2. Click **Approve** and **60 GHz cnWave-Network Onboard** window appears and provides option to Edit Network name.



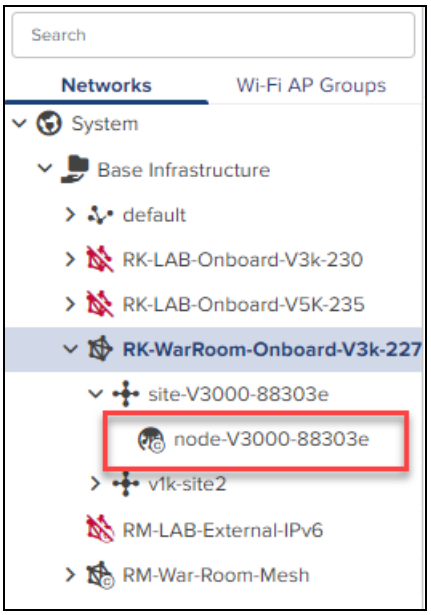
3. click **Save**.



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



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

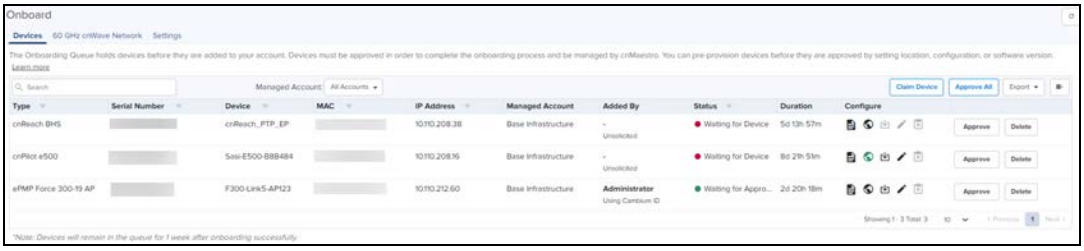


Pre-Configuration and Approval of Devices (Optional)

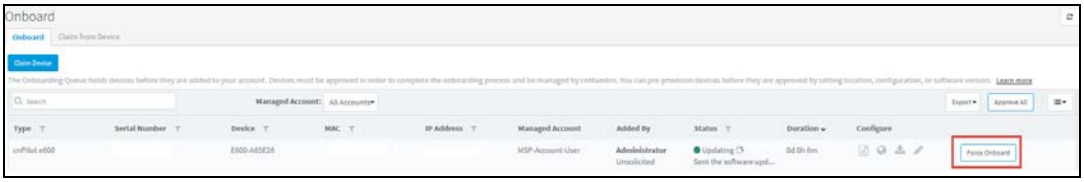
To automatically configure and approved devices when they access cnMaestro, add the device MAC address to the **Onboard >** click **Settings**. Adding devices here places them in the onboarding queue, where they can be pre-configured and/or pre-approved.

If this step is not configured, the devices would automatically show up in the onboarding queue, where they can be approved.

Figure 14 Pre-Configuration and Approval of Devices



NOTE:
If the device gets struck in the onboarding page, the **Force Onboard** button automatically enable. Click the **Force Onboard** for the device to be onboarded.

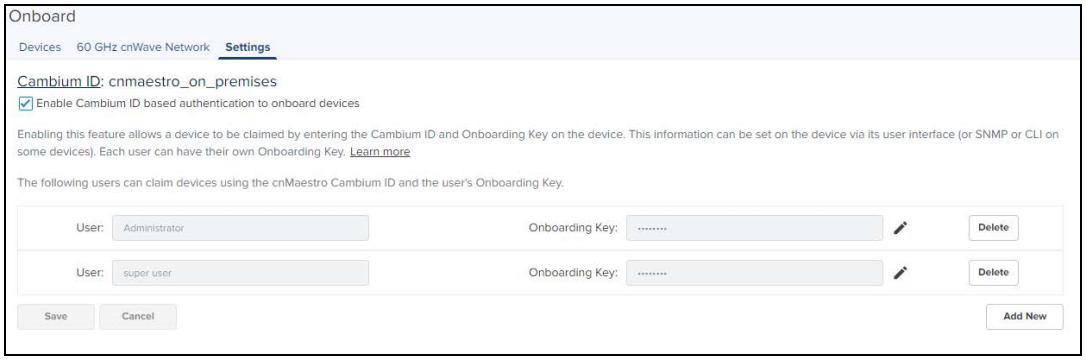


Device/Agent Authentication (Optional)

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 will allow 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 would only be used to require device authentication before addition to the onboarding queue.

Figure 15 Device/Agent Authentication



Claiming the Wi-Fi Devices from AP Group

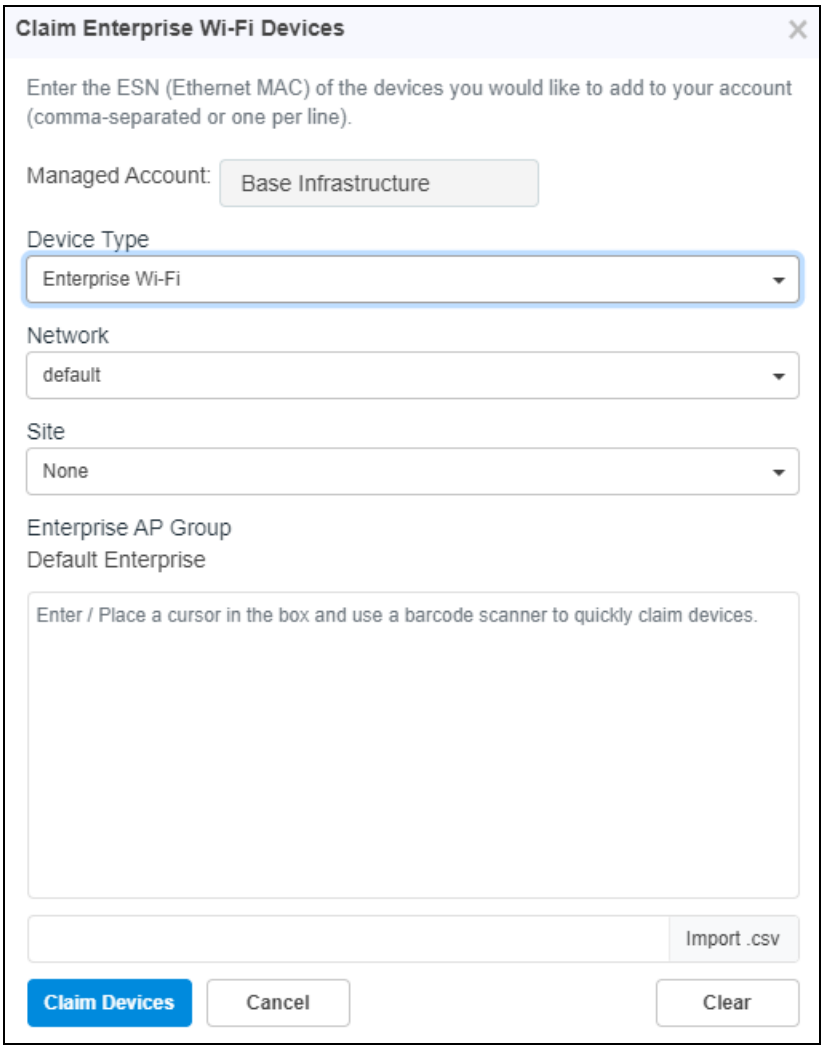
To claim multiple devices from the AP Group in Cloud, navigate to the **Wi-Fi AP Groups** tree view and click the drop-down menu for the selected **AP Group** .

1. Click the **Claim Devices** option.
2. In the pop-up dialog that appears select the Device type, Network and Site under which these devices needs to be placed and by default the devices claimed under this group will have the configuration settings from this AP Group.

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

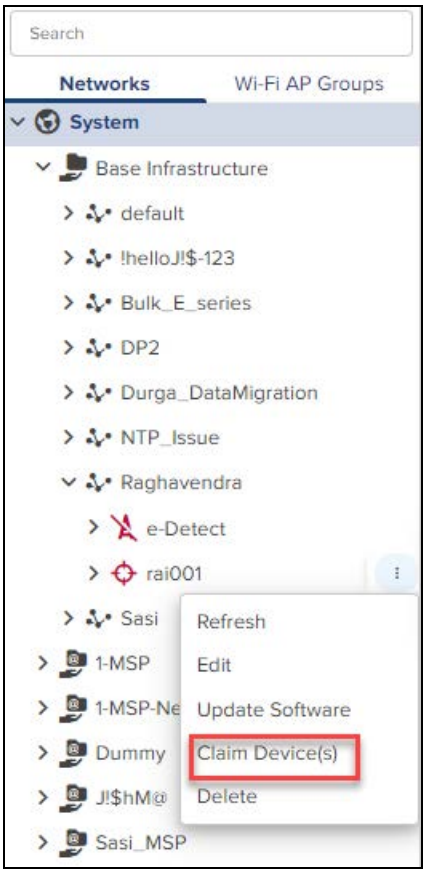
3. Specify the MAC Address of the devices line-by-line or comma-separated, or click **Import .csv** option to import the device MAC addresses from a file.
4. Click **Claim Devices** to add to the selected AP Group with the configuration applied.

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

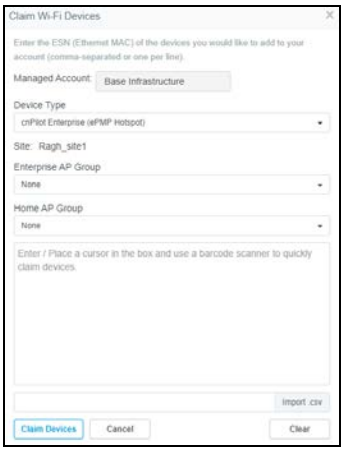


Claiming the Wi-Fi Devices from Site Dashboard

1. To claim multiple devices from the site dashboard, navigate to **Manage > Networks** tree view and select the drop-down menu for the Site.
2. Click **Claim Devices** from the drop-down.



3. In the pop-up dialog select the AP Group that should be applied for cnPilot E (Enterprise) and R (Home) series devices. The devices claimed under this Site will have the configuration settings from the selected AP Group.



4. Specify the MAC number 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 click **Apply Configuration**.

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

High Availability (HA)

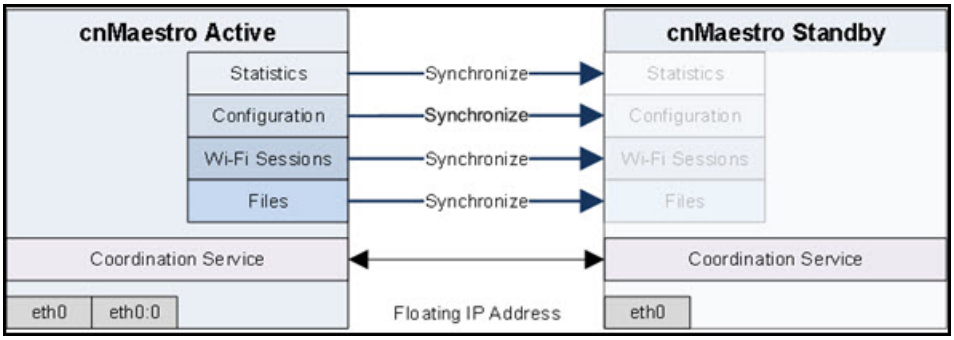
This section includes the following topics:

- Overview
- HA Cluster Setup
- HA Menus

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 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

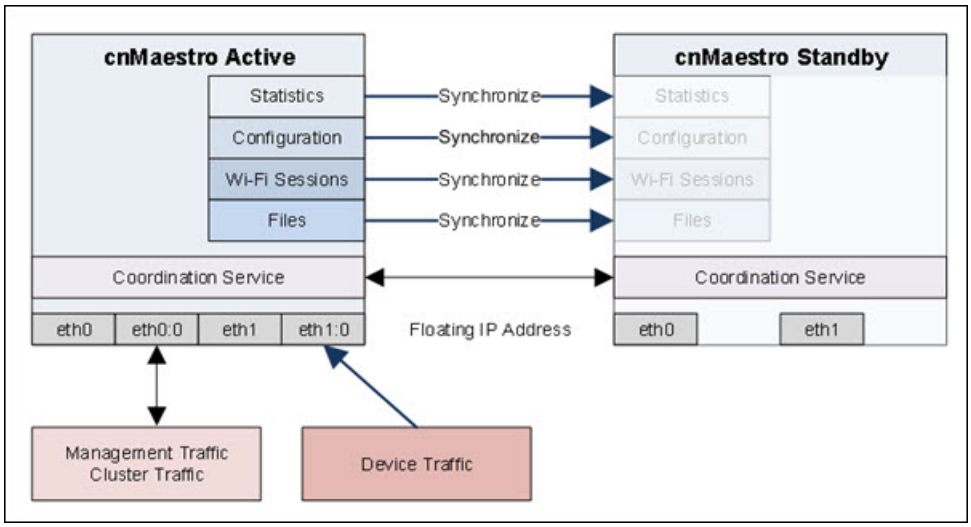
Cambium Networks recommends backing up virtual machines prior to starting HA. To take daily automated backups of cnMaestro data, navigate to **Administration > Server > System Backup and Restore**.

Dual Interfaces

cnMaestro can be configured with two interfaces, eth0 and eth1, on VMware workstation and ESXi. These allows traffic to be segmented into Management/Cluster and device, though strict separation is not currently enforced (so the UI can still be launched from the Device IP). The implementation allows deployments with separate management and control subnets to integrate more easily with cnMaestro.

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

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 determine how eth0 and eth1 are mapped to the running VM: the PCI ordering does not necessarily follow the order of 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 from that presented in the UI. This may result in a second interface mapped to eth0 instead of eth1. In order to resolve this, you may need to update VMware configuration.

VMware Workstation

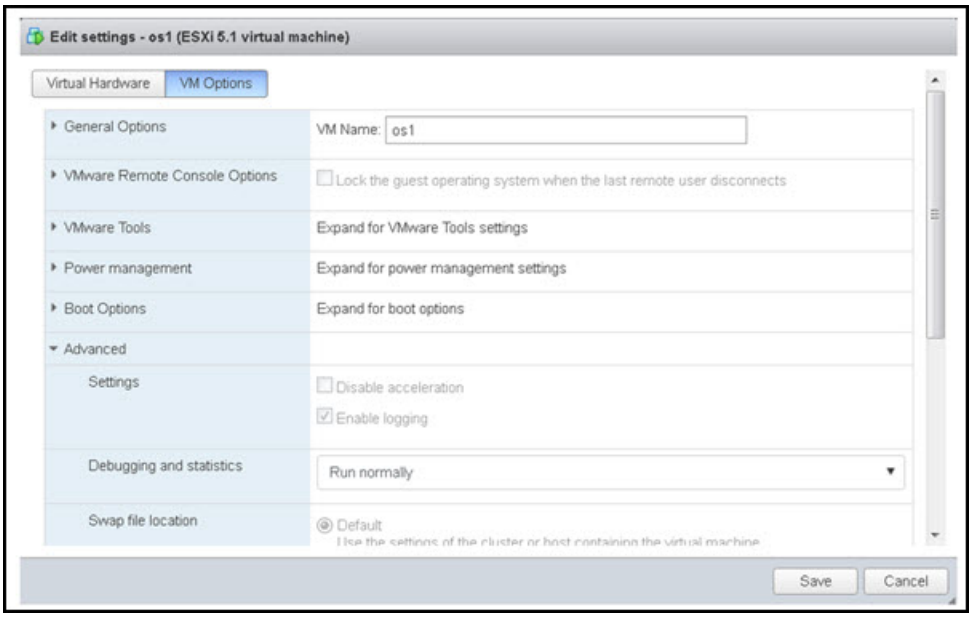
In VMware Workstation, edit the configuration file (ending in .vmx) in the virtual machine home directory. After shutting down the VM, change the following two entries, so the eth0 PCI number is lower than eth1.

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

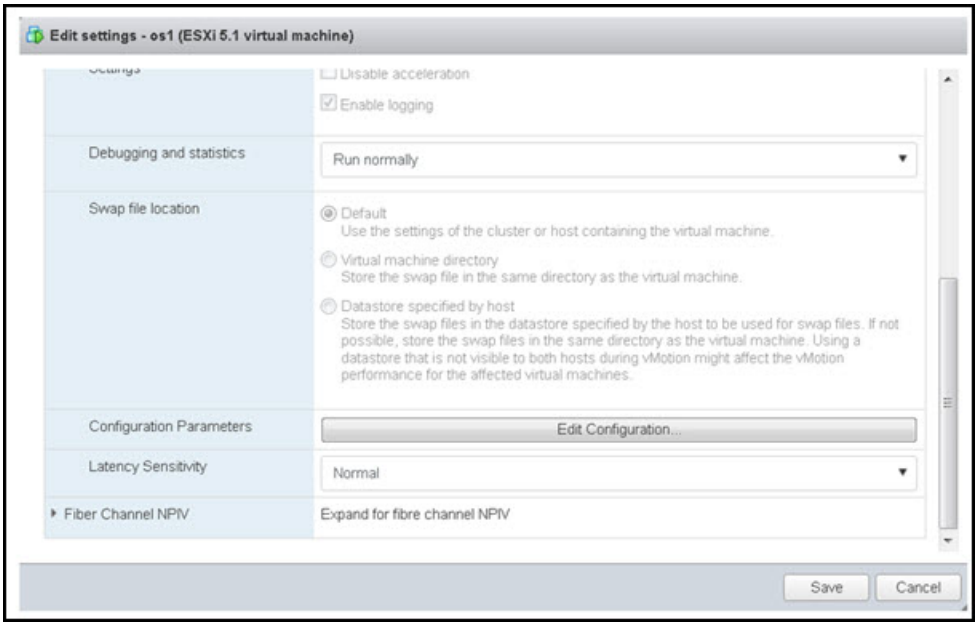
VMware ESXi

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

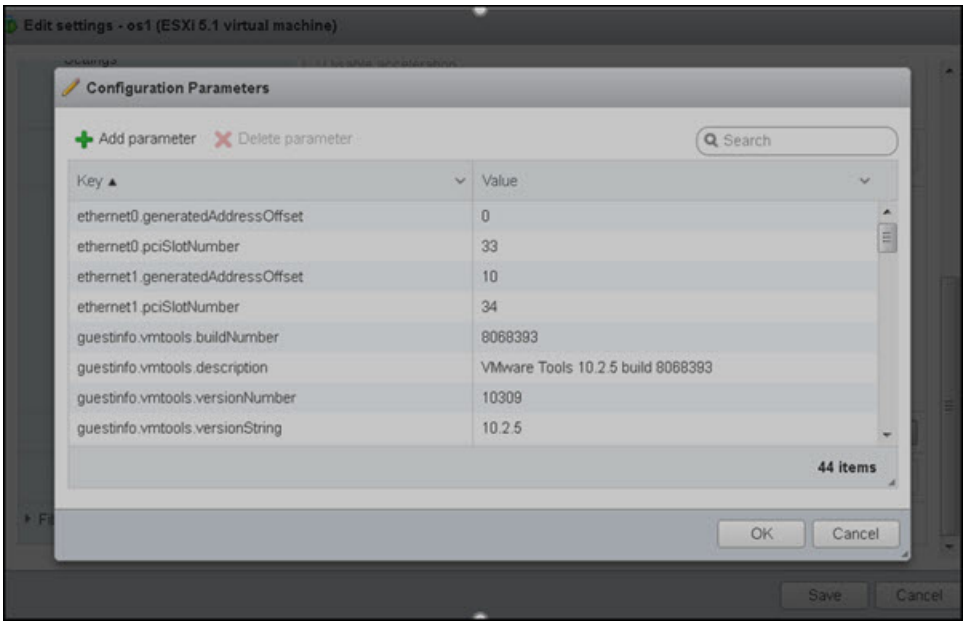
1. Select **Edit Settings** of the VM and choose **VM Options > Advanced**.



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



This launches a screen that allows updating the PCI numbers.



HA Cluster Setup

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

Bootstrap (Primary)

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

Accept (Primary)

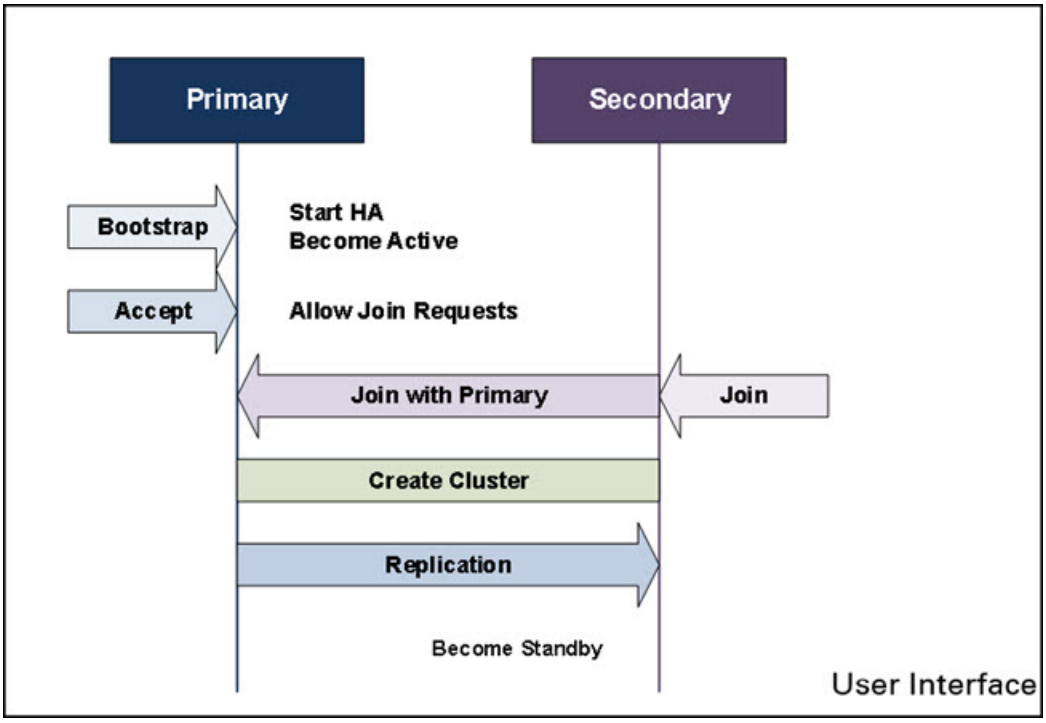
The Primary server then configures a shared secret to allow a Secondary system to join the cluster. The secret is used for authentication, and it is valid for 30 minutes.

Join (Secondary)

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

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

Figure 17 Accept/Join

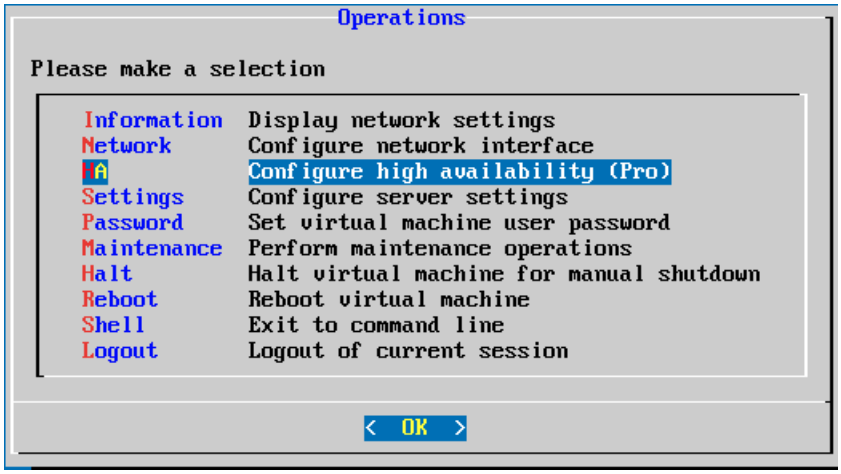


Basic HA Cluster Creation Flow

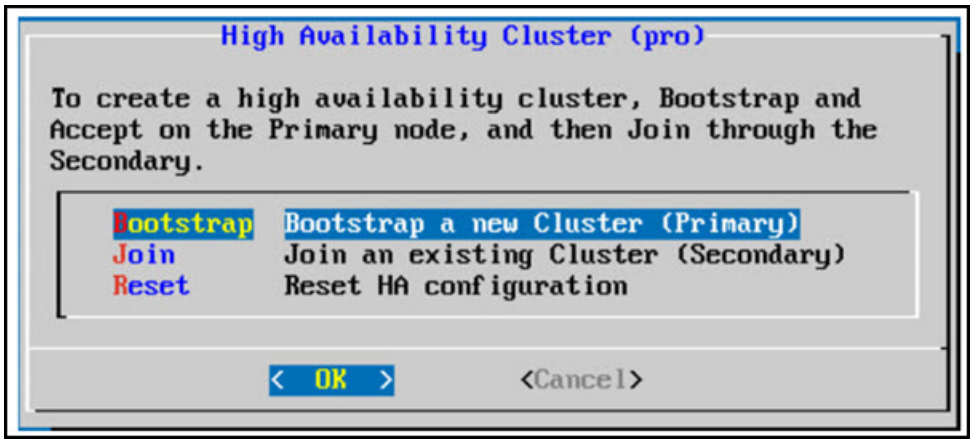
A general HA configuration flow is presented below. Each page will be discussed independently in later sections.

Primary Server

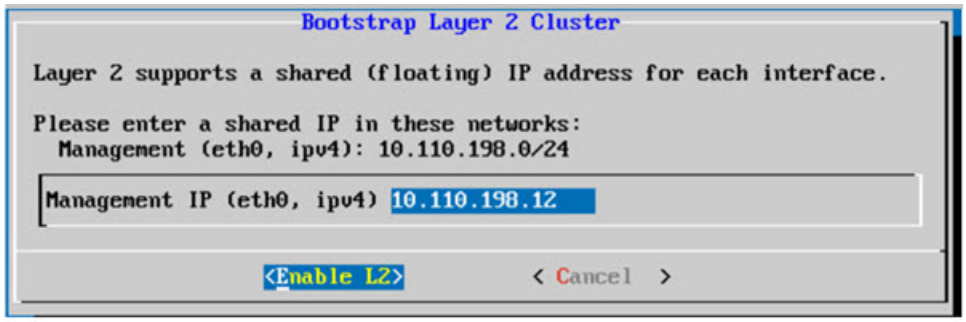
1. After logging into cnMestro console, from **Operations** tab, select **HA** and click **OK**.



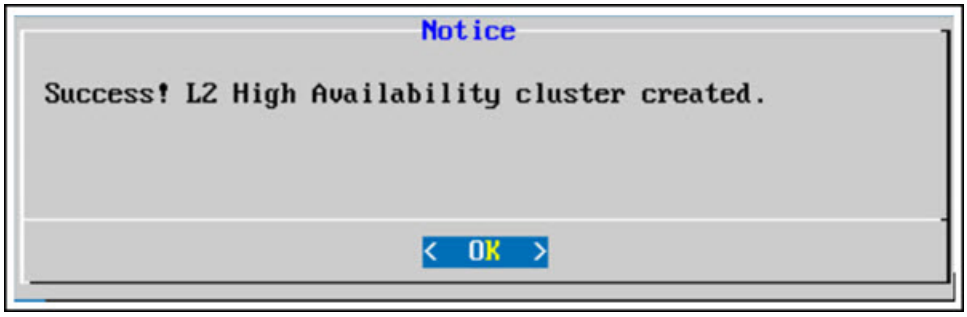
2. From **High Availability Cluster** tab, select **Bootstrap** and click **OK**.



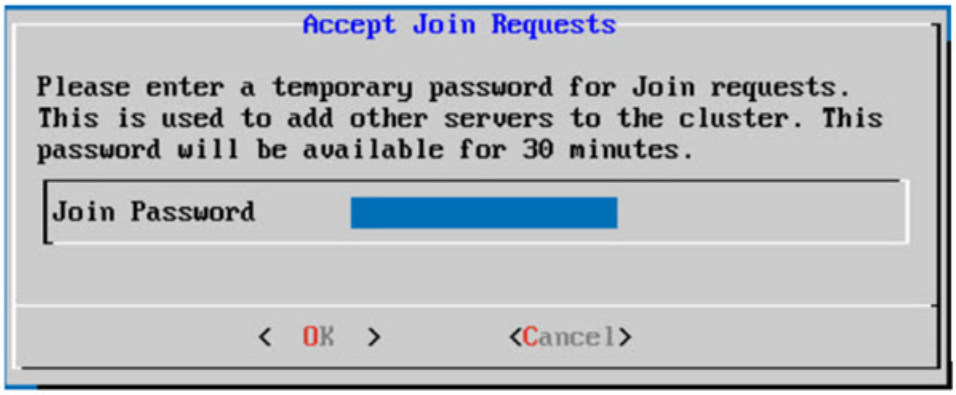
3. From the **Bootstrap Layer 2 Cluster** tab, enter **Management IP** and click **Enable L2**.The Management IP must be on the same subnet as the eth0 interface.



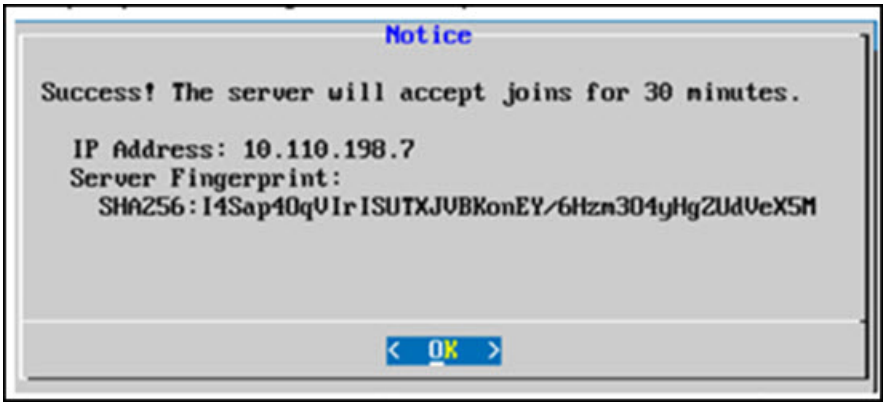
4. When the L2 High Availability Cluster is created, success window pops-up as shown below:



5. Primary Bootstrap is successfully completed now. Click **OK**, which redirects to Accept/Join requests page to create the Password (shared secret) used to Join a second system.
6. The password is used by the Secondary to authenticate and join the Cluster. It is valid for 30 minutes.

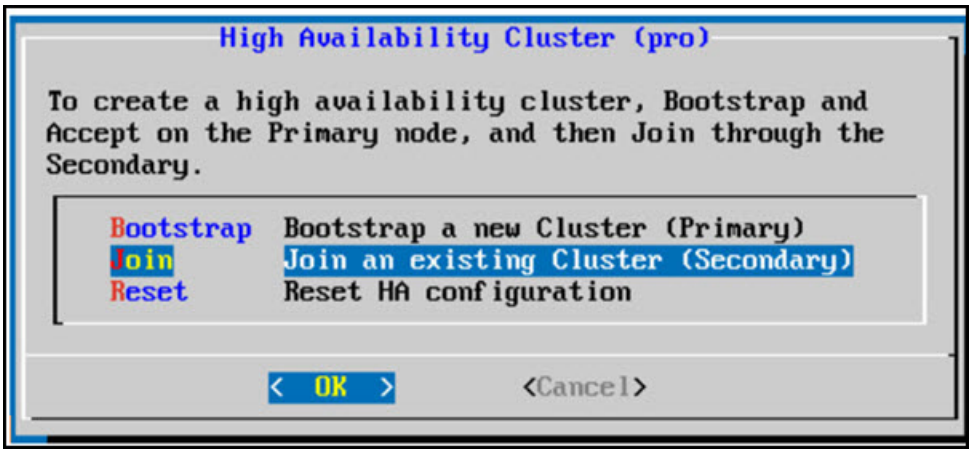


7. When the **Join Password** is set, click **OK** to initialize the system for 30 minutes. A SSH Fingerprint is also generated during this step. Match the fingerprint to the one displayed during the Join process.

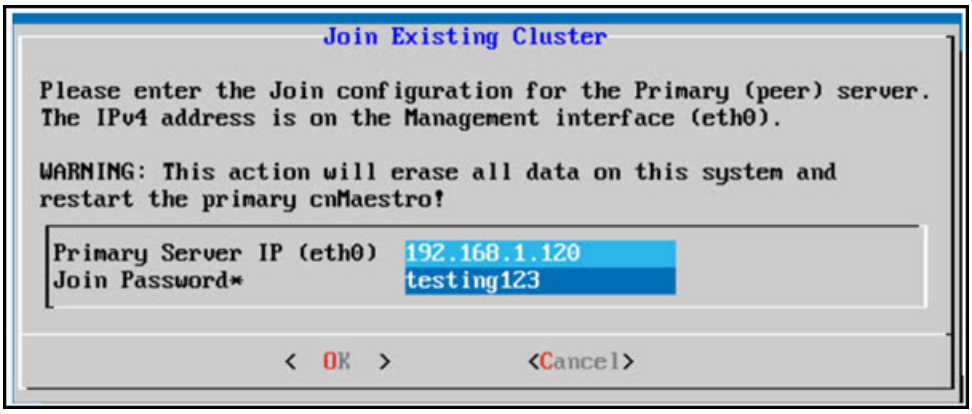


Secondary Server

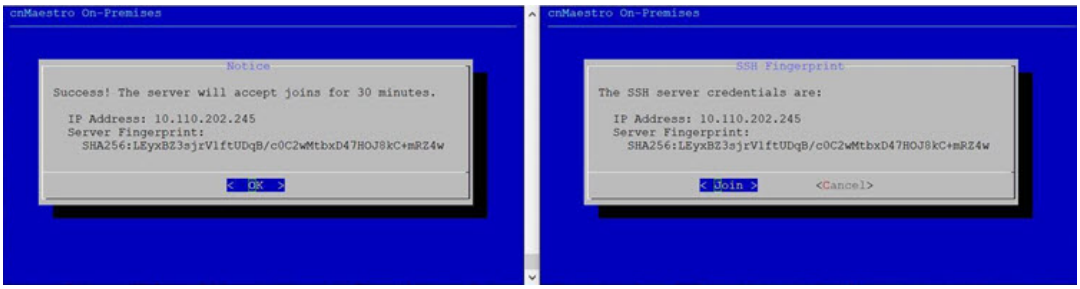
1. On the Secondary cnMaestro server, from the **High Availability Cluster** menu, select **Join** and click **OK**.



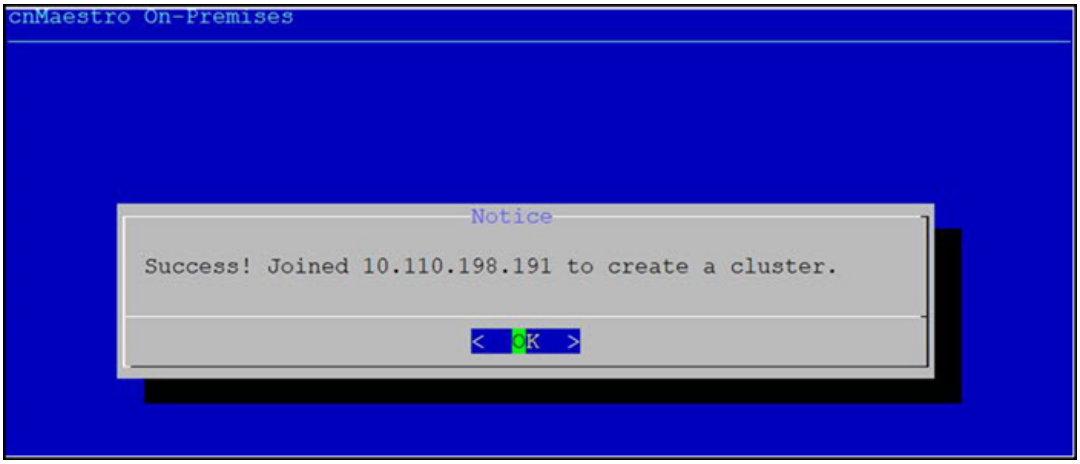
2. The Join existing Cluster window appears. Enter the Primary server **eth0** IP and the **Join Password**, click **OK**.



3. A pop-up 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 they are different, the Primary server is incorrect, and the Join should be cancelled.



4. After verifying and continuing, the successfully joined cluster window will appear.

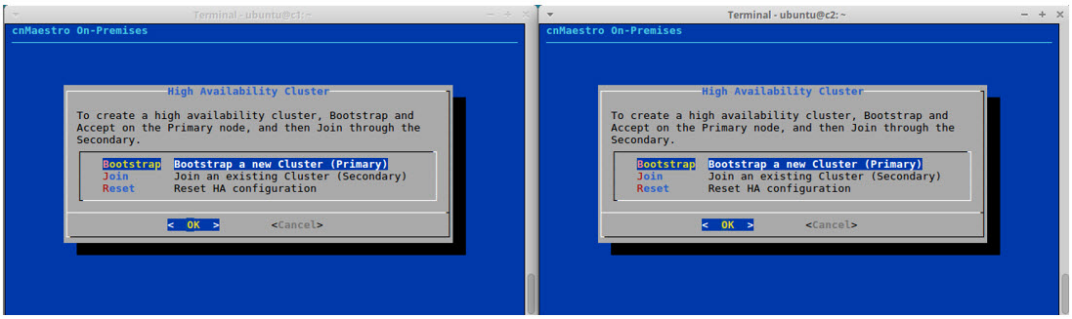


HA Menus

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

High Availability Cluster Menu (pre-Bootstrap)

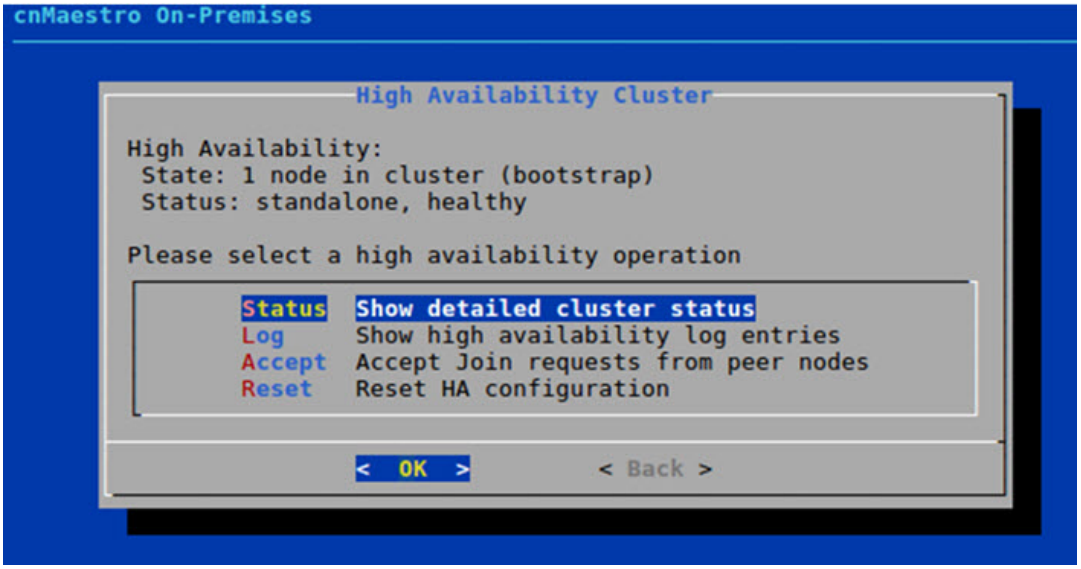
This menu is available before HA is enabled, and the cluster has been created.



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)

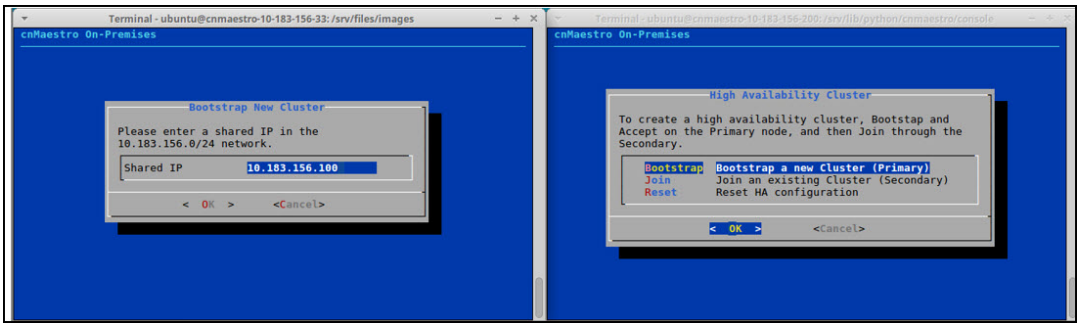
This menu is available after a successful Bootstrap.



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

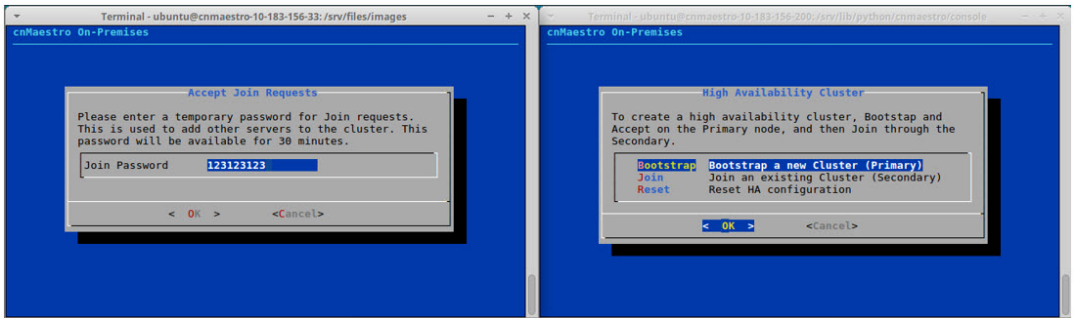
New Cluster

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 should be used for cnMaestro access.



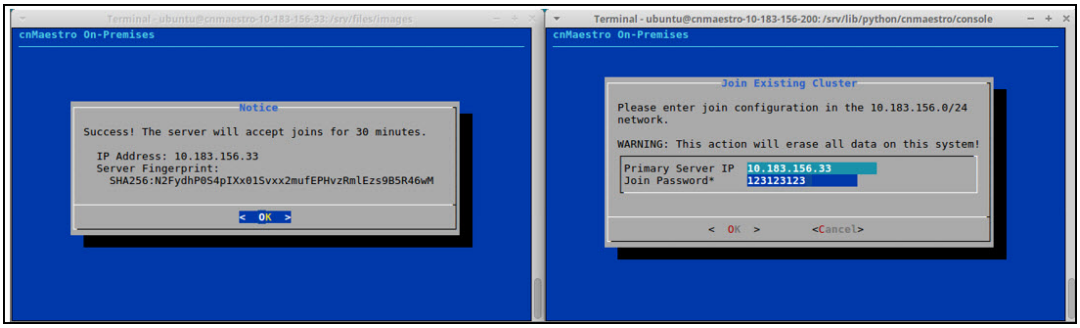
Accept Join Requests

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



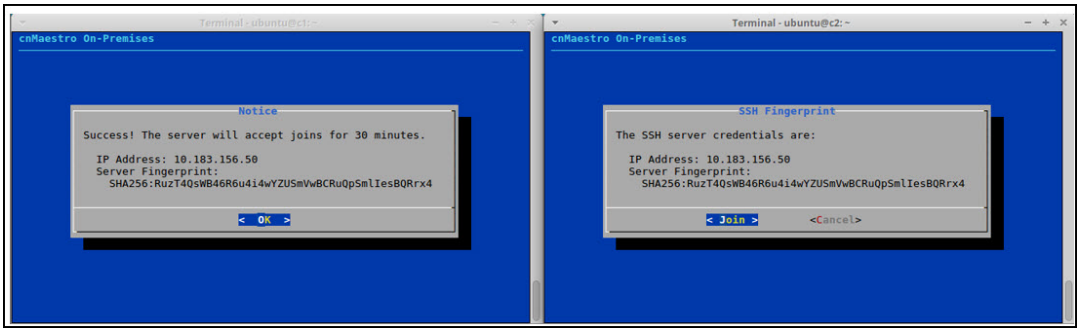
Join Existing Cluster

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.



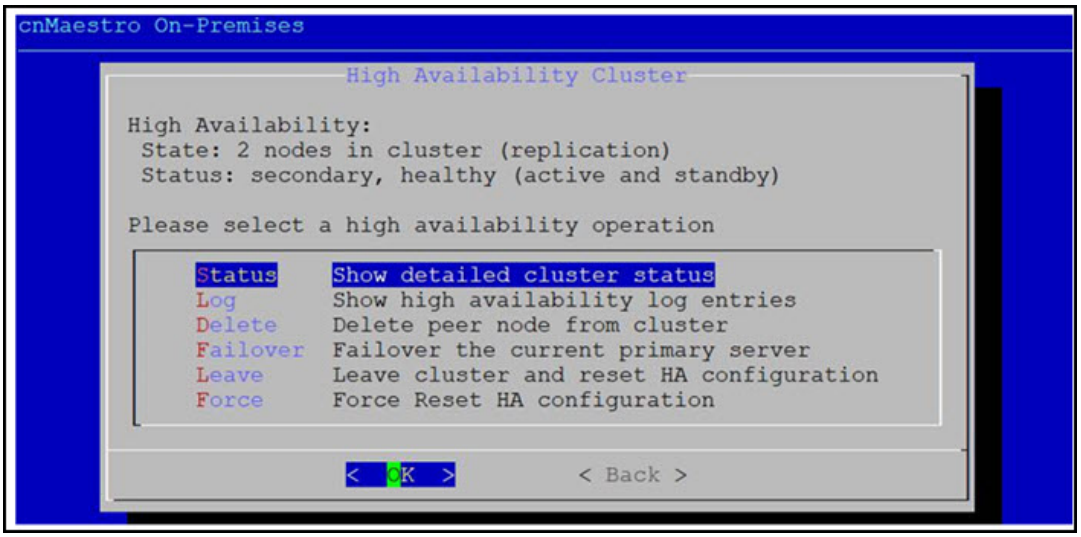
Validate SSH Fingerprints

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.



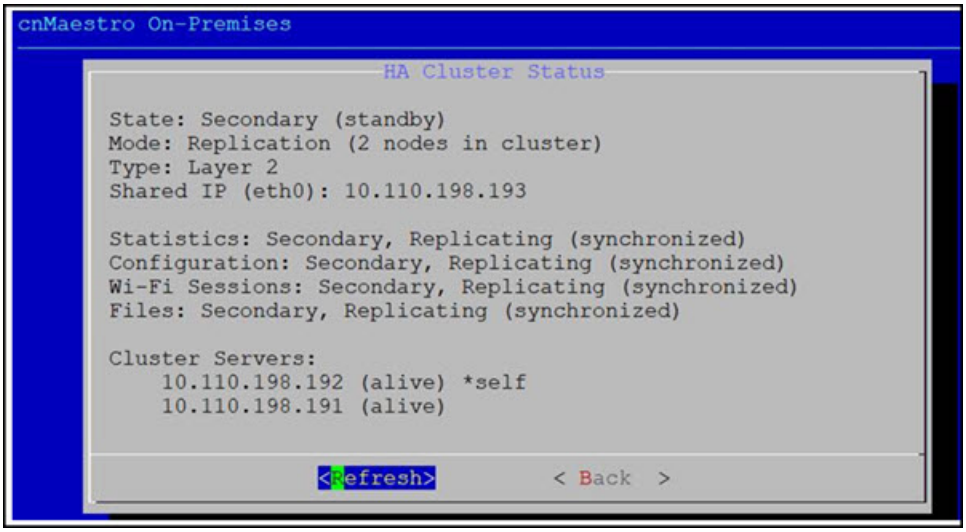
HA Cluster Status

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.

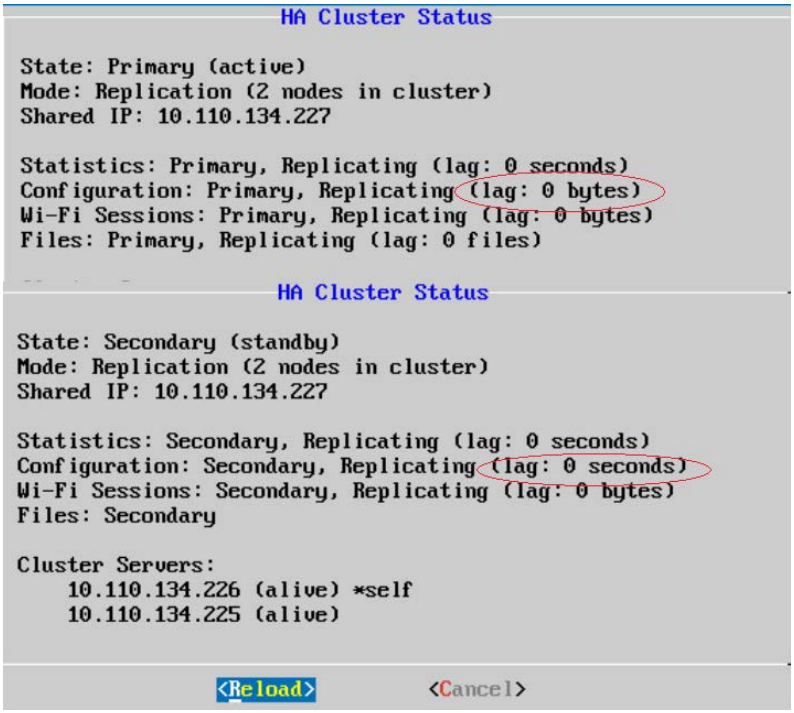


Accept	Set a password used by another system to join the Cluster.
Delete	Delete a node from the Cluster.
Failover	Failover to the current Standby node. This is not visible while standalone.
Force	Forcibly Reset HA configuration. This causes a non-graceful reset of the current node, and it does not delete 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:



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.



NOTE:
There may be discrepancy in the Primary and Secondary lag value it may display the results in bytes or seconds.

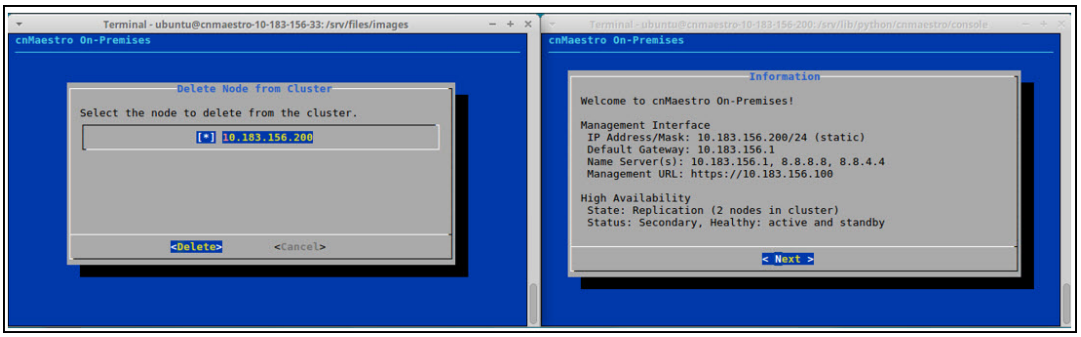
Delete Node

Delete from Cluster

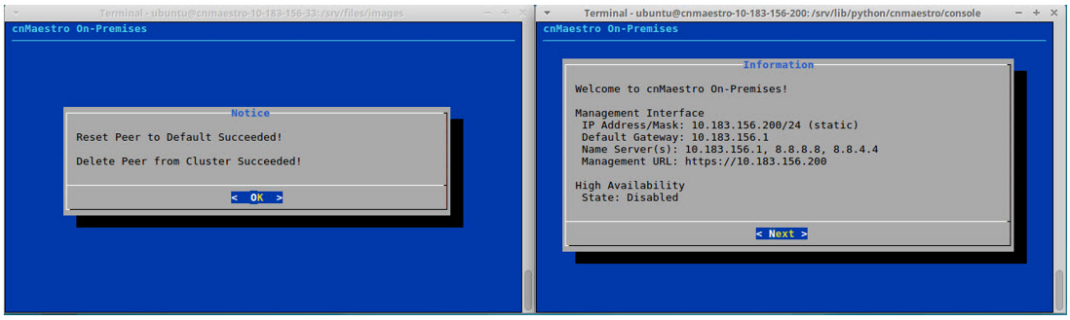
Deleting removes the peer node from the cluster. Navigate to **Operations > HA**, select **Delete** and click **Ok**.

Use the spacebar 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.

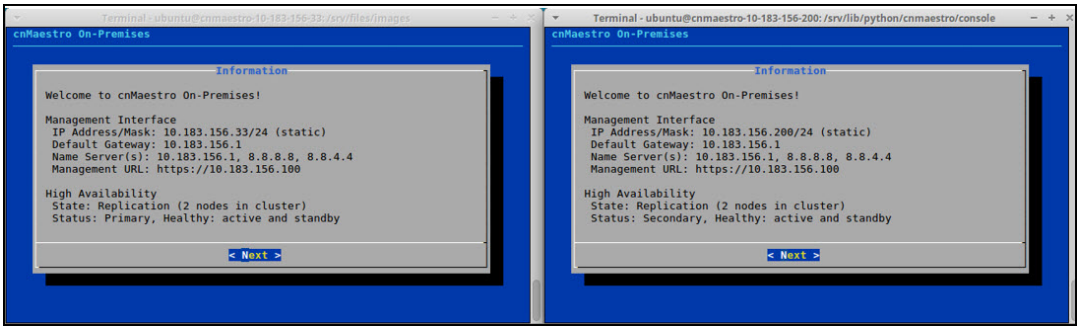


Leave Cluster

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

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 failover happens when the Device approval is in-progress, then the "Device Approval" will get stuck. We have to re-initiate the "Approve All"	
Software update jobs	If the failover happens when the Software Update job is in-progress, then the devices software update will get Timeout after failover.	
	Software update breakup	Impact after failover
	Software update to 50 devices with "Devices to update in parallel" set as 10	10 devices which were in parallel update will get impacted. After failover Job will get Timed out after 5 minutes. We 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. We have to retrigger Software update for these 50 devices
Configuration push jobs in running state	If the failover happens when the Configuration Update is in-progress, then the Configuration update will get Timeout.	
	Configuration update breakup	Impact after failover
	Configuration Update to 50 devices with "Devices to update in parallel" set as 10	10 devices which were in parallel update will get impacted. After failover Job will get Timed out after 5 minutes. We have to retrigger Config update for these 10 devices
	Configuration 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. We have to retrigger Config update for these 50 devices
OVA upgrade	If the failover happens when the OVA upgrade is in progress, then we have to re-initiate OVA upgrade	
	OVA upgrade	Impact after failover
	Failover happens during OVA file upload	File upload will get cancelled. We have to re-trigger it
	Failover happens during 10 % to 100% of OVA upgrade	OVA upgrade will get cancelled. We have to re-trigger it
	Failover happens after 100% of OVA upgrade and before "Apply"	File upload will get cancelled. We have to re-trigger it
	Failover happens during 10 % to 100% of OVA upgrade	OVA upgrade will get cancelled. We have to re-trigger it
	Failover happens Just before we proceed with "Apply"	No impact here, "Apply" can be done after failover.

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 section includes the following:

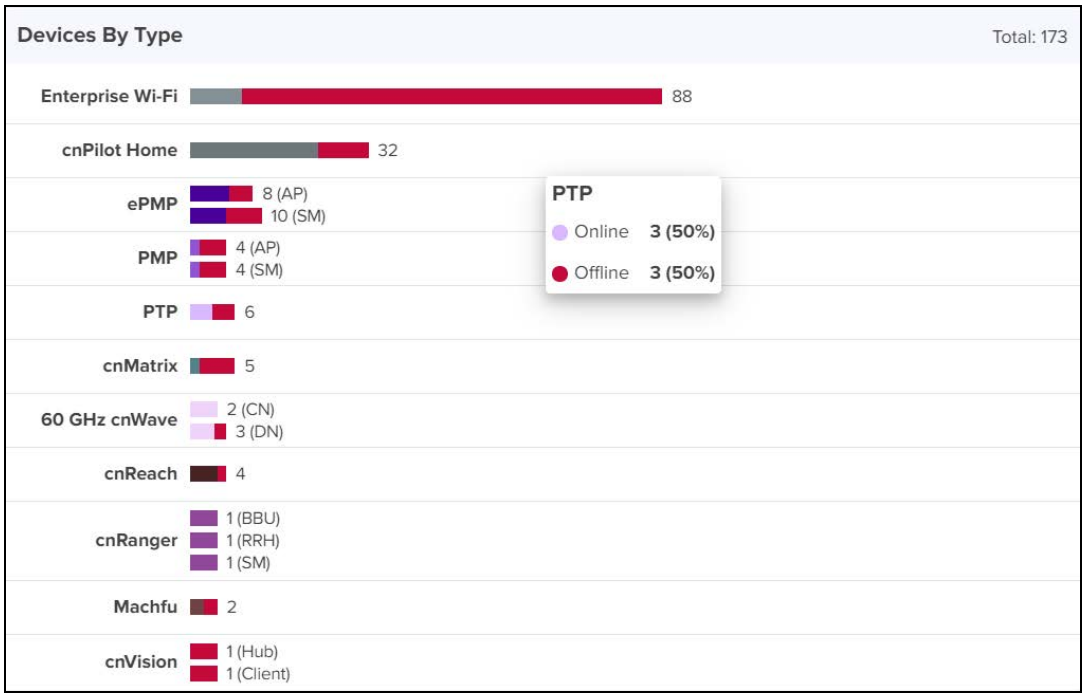
- Dashboard
- Notifications
- Statistics and Details
- Performance
- Maps
- Tools
- WIDS

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 aggregate dashboard data for the devices they contain.

KPI (Key Performance Indicators)

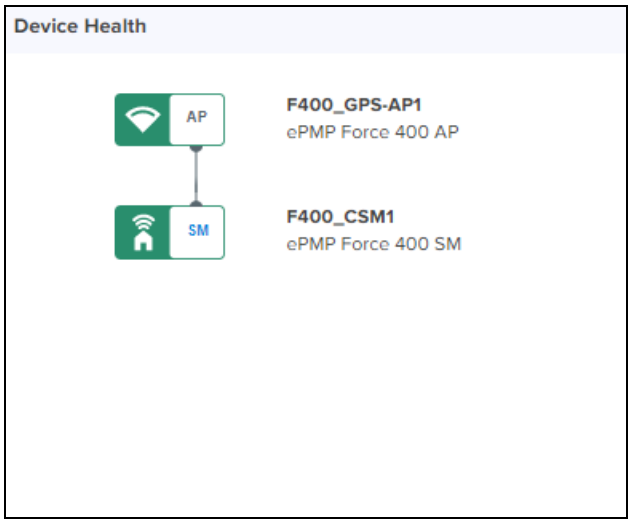
Each page has a set of KPIs tailored to the node type. These present a current value and often historical trend data.



Device Health

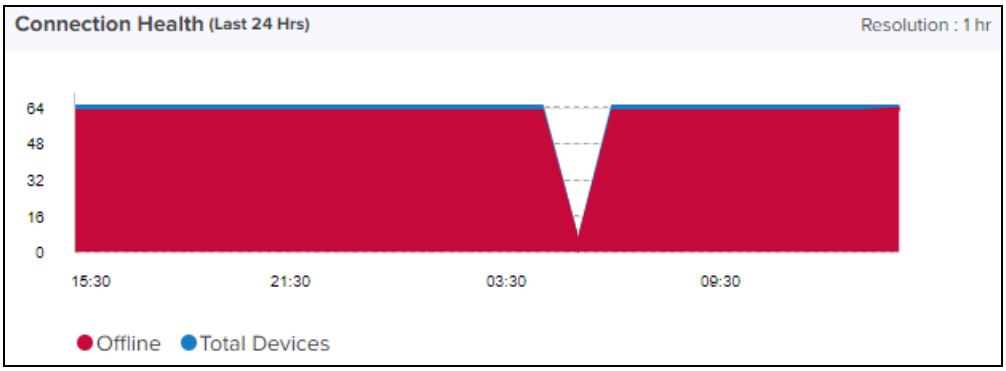
Device Health displays the health of the network from the tower to the edge.

Figure 18 Device Health



Connection Health

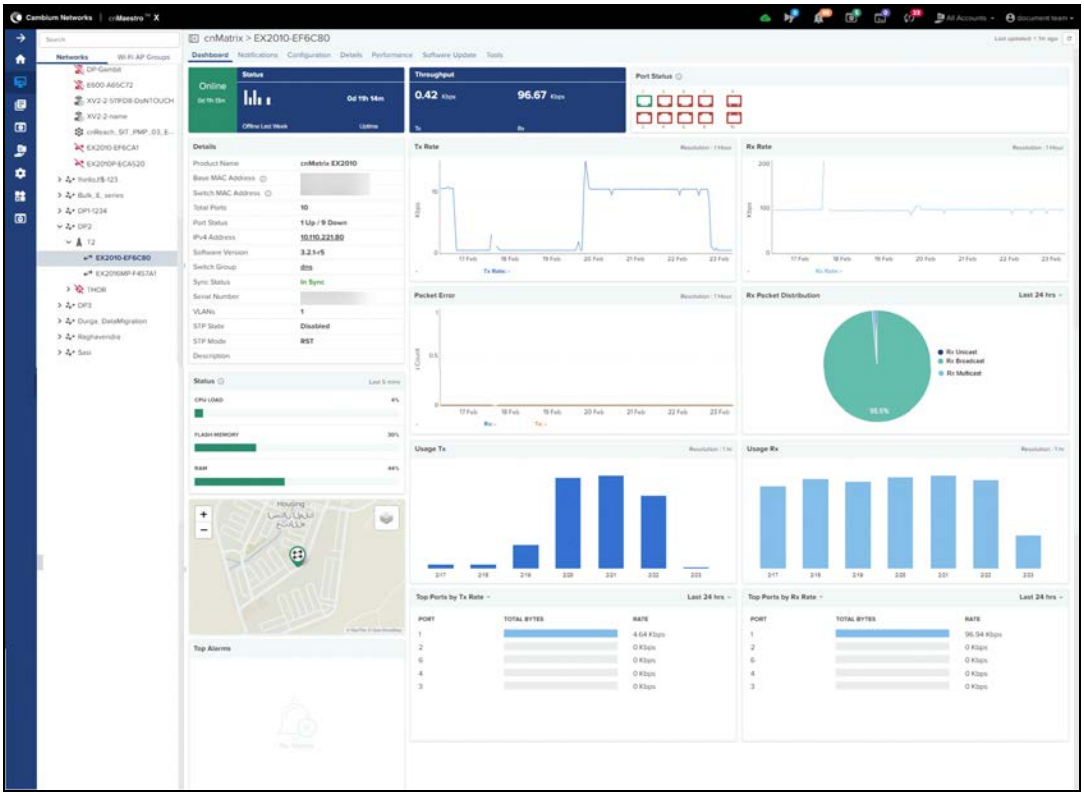
Connection Health displays the health of the devices connected to the network.



Charts and Graphs

Contextual charts and graphs provide details on important dashboard metrics.

Figure 19 Charts and Graphs



Notifications

Overview

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

Table 12: Notification Overview

Type	Description
Alarms	Alarms have state and persist as long as the problematic activity continues; they reflect the current health of the devices in the network. **NOTE:** After every server reboot or restart alarm displays as shown below: • cnMaestro takes upto 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.
Alarm History	Expired Alarms are added to the Alarm History. The Alarm History displays historical active alarm counts.
Events	Events are stateless, transient messages that occur in response to an input or action, such as if the CPU exceeds a threshold or a device association fails. Events are fire-and-forget; they are stored in an Event Table and provide a history of device activity.

Event/Alarm Source

Identity of the source device affected by 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 Networks, Towers, and Sites. When a device is selected, such as an AP, the notifications will only be presented 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 of each 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 13: 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

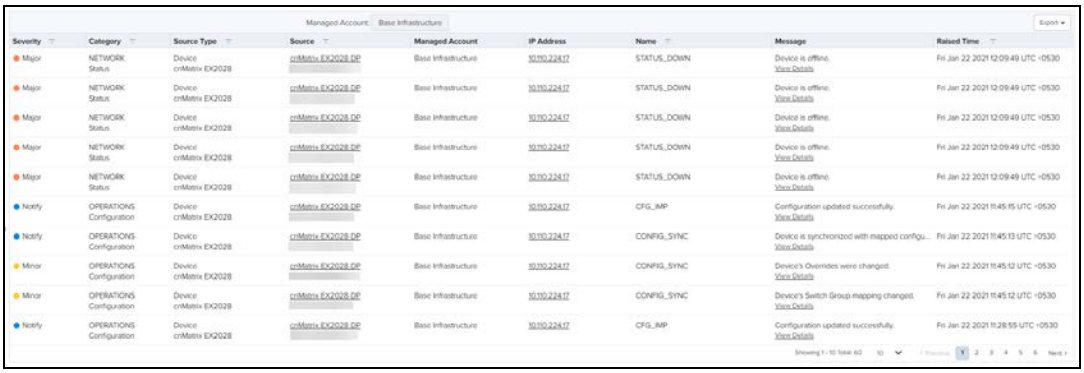
The event data in a table can be exported in a CSV or PDF file format.

Support for System Events

The source type can be either **Device** or **System**. Events generated by the system will be filtered using the source type **System** and the events generated by the device will be filtered using source type **Device**.

Each and every system event can be categorized under one type.

Figure 20 System Events



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

Table 14: System Event Types and Definitions

System 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: Devices
Operations	Event related to system-level processes, such as pushing configuration, installing images, etc. Source: Devices
Other	Events which are not related to above categories listed under the others. Source: Devices

Table 14: System Event Types and Definitions

System Event Category	Description
Registration	Events related to managing/unmanaging devices. Source: Devices
Security	Events related to logging into the devices, establishing secure links, and potentially recognizing scans and security breaches in the future. Source: cnMaestro, Devices, Clients
Services	Events related to additional services that may be added to the product in the future. There may not be any services events in the first release. Source: cnMaestro and Devices
Wireless	Events related to issues/notifications with the PTP/PMP radio connectivity, Wi-Fi Clients, etc. Source: Devices

Alarms

Alarm Life Cycle

The basic alarm life cycle has the following states:

Table 15: Alarm Life Cycle

State	Description
Acknowledged	Active alarms can be acknowledged, which signifies they are known and being handled. Acknowledgment does not affect the total alarm count – it is a convenience to the administrator.
Active	The alarm remains active until the combination of inputs that generated it are cleared.
Inactive	Inactive alarms remain visible in the active alarm table for 10 minutes, before they are moved to alarm history. An alarm becomes inactive when the inputs that generated it are no longer present. An Inactive alarm can be pulled back to the Active/Acknowledged states if a new event reactivates the alarm.
Raised	The creation of the alarm.

Alarm Severity

Alarms have a severity that determines how they are handled.

Table 16: 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 is clear and is used for inactive alarms.

Alarm Types

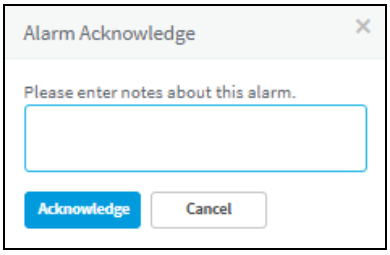
Table 17: Alarm Types

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. This is for convenience – 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 not change any of the alarm counts – either at the page or the system level. The only way the alarm count is decreased is when alarms become inactive.

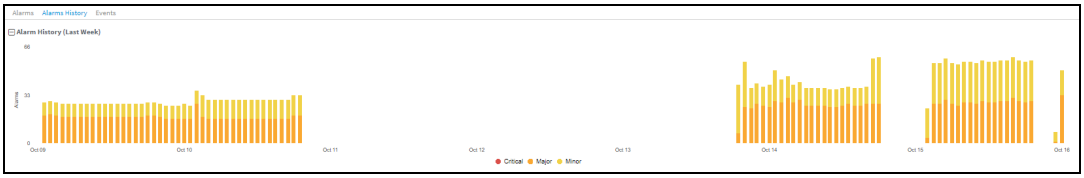
Figure 21 Alarm Acknowledge



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 22 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 that is generally found in cnMaestro Statistics and Details sections (separated by Device Type).

Table 18: Device Statistics

60 GHz cnWave Nodes	**General** • Device • IPv6 Address • Main Aux SFP • Mode • Model • Network • PoP Node • Radio Channel • Serial Number • Site • Status • Status Time • Software Version • Sync Mode • Zone **GPS** • Fix Type • Height • Latitude • Longitude • Satellites Tracked
cnMatrix	**General** • Device • IP Address • Product Name • Serial Number • Status **Traffic** • Throughput (Rx) • Throughput (DL)
cnPilot Home	**General** • Device • IP Address • Product Name • Serial Number • Status **Wireless** • Radios (Channel)
cnRanger BBU	**General**

Table 18: Device Statistics

	• Device • IP Address • Registered SM Count • Serial Number • Status **Traffic** • Throughput (DL) • Throughput (UL)
cnRanger SM	**General** • Device • IP Address • IMSI • Serial Number • Status **Traffic** • Throughput (DL) • Throughput (UL) **Wireless** • Bandwidth • Frequency • MCS (DL) • MCS (UL) • RSSI • RSRP • RSRQ
cnReach	**General** • Device • IP Address • Neighbors • Radio • Role • Status **Radio** • Average Noise • Radio Temperature • RSSI • SNR • Tx Power **Traffic** • Throughput (DL) • Throughput (UL)
cnReach XIO	**General** • Active S/W Version • Device • IP Address • Product Name • Serial Number

Table 18: Device Statistics

	• Status
cnVision Client	**General** • Device • DFS Status • Distance • IP Address • Status • Serial Number • Session Time **Network** • LAN Interface • LAN Interface 2 • WAN IP Address **Traffic** • Retransmission Rate (DL) • Retransmission Rate (UL) • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Connected AP • MCS (UL) • MCS (DL) • QualityCapacity • RSSI (DL) • RSSI (UL) • SSID • Tx Power • Wireless MAC
cnVision Hub	**General** • Device • DFS Status • IP Address • Registered SM Count • Reregistration Count • Status • Serial Number

Table 18: Device Statistics

	Network • LAN Interface • LAN Interface 2 **Traffic** • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Bandwidth • DL/UL Ratio • Max Range • Frequency • SSID • Tx Power
Enterprise WiFi	**General** • Device • IP Address • Product Name • Serial Number • Status **Wireless** • Radios (Channel)
ePMP AP	**General** • Device • DFS Status • IP Address • Reregistration Count • Registered SM Count • Serial Number • Status **Network** • LAN Interface • LAN Interface 2 **Traffic** • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Bandwidth • DL/UL Ratio • Frequency • Maximum Range • SSID

Table 18: Device Statistics

	• Tx Power
ePMP SM	**General** • Device • Distance • DFS Status • IP Address • Status • Session Time • Serial Number **Network** • LAN Interface • LAN Interface 2 • WAN IP Address **Traffic** • Retransmission Rate (DL) • Retransmission Rate (UL) • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Capacity • Connected AP • MCS (DL) • MCS (UL) • Quality • RSSI (DL) • RSSI (UL) • SSID • Tx Power • Wireless MAC
Machfu	**Cell** • 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 **Ethernet**

Table 18: Device Statistics

	• Ethernet • Ethernet Enabled • Ethernet MAC • Ethernet Link • Ethernet Link Speed • Ethernet IP Address • Ethernet Gateway • Ethernet Mask • Ethernet Tx Rate • Ethernet Rx Rate • Ethernet Mode **General** • Device • Status • IP Address **GPS** • GPS Altitude • GPS Time • GPS Satellites in use • GPS Status • GPS Accuracy • GPS Fix Time **VPN** • VPN Type • VPN Link • VPN Server • VPN IP **Wireless Client** • WC Enabled • WC SSID • WC Link • WC RSSI • WC MAC • WC IP • WC Gateway • WC Mask • WC Tx Rate • WC Rx Rate

Table 18: Device Statistics

	Wireless Access Point • WAP Enabled • WAP SSID • WAP Link • WAP MAC • WAP IP • WAP Mask • WAP Mode • WAP Tx Rate • WAP Rx Rate
PMP AP	**General** • Device • DFS Status • IP Address • Registered SM Count • Reregistration Count • Serial Number • Status **Network** • LAN Interface **Traffic** • Busy Index (DL) • Busy Index (UL) • Frame Utilization (DL) • Frame Utilization (UL) • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Bandwidth • Color code • DL/UL Ratio • Frequency • Maximum Range • Tx Power
PMP SM	**General** • Device • DFS Status • Distance • IP Address • Session Time • Serial Number • Status **Network** • LAN Interface

Table 18: Device Statistics

	• WAN IP Address **Traffic** • Packet Loss (DL) • Packet Loss (UL) • Packet Loss (Overcapacity) (DL) • Packet Loss (Overcapacity) (UL) • Packet Loss (Error Drop) (DL) • Packet Loss (Error Drop) (UL) • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Color Code • Connected AP • Horizontal SNR (UL) • Horizontal SNR (DL) • LQI (DL) • LQI (UL) • Modulation (DL) • Modulation (UL) • RSSI Imbalance • RSSI (DL) • Tx Power • Vertical SNR (UL) • Vertical SNR (DL)
PTP	**General :** • Device • IP Address • Product Name • Status **Network :** • Aux Interface • Main PSU Interface • SFP Interface **Wireless :** • 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), 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, cnRanger, cnPilot Enterprise, cnPilot Home, cnReach, ePMP AP, ePMP SM, PMP AP, PMP SM, and PTP.

Table 19: Performance Graph

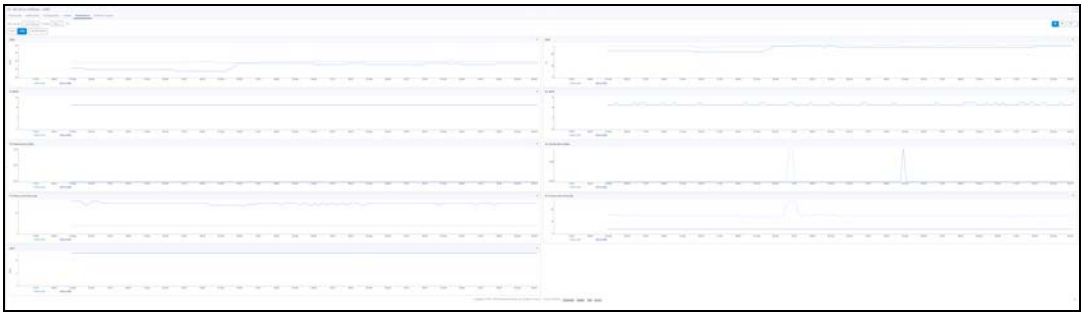
Device	Fields
60 GHz cnWave (Node)	Displays the following graphs: • Available Memory • CPU Utilization
60 GHz cnWave (Links)	Displays the following graphs: • EIRP • RSSI • Rx MCS • Rx Frames (Per Second) • Rx Packet Error Ratio • SNR • Tx MCS • Tx Packet Error Ratio • Tx Frames (Per Second) 
cnMatrix	Displays the following graphs: • CPU • Packet Error • Rx Packets • Throughput • Tx Packets

Table 19: Performance Graph

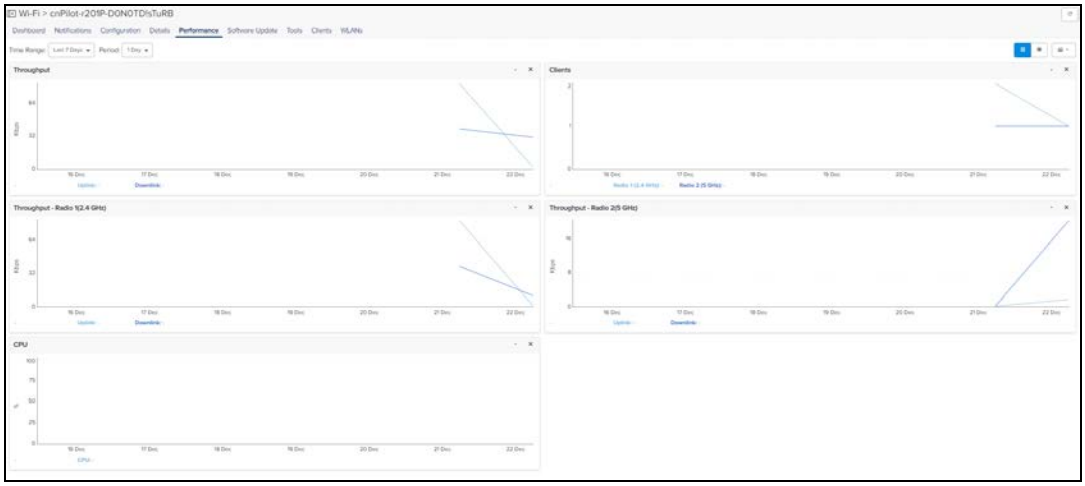
Device	Fields
cnPilot Home	Displays the following graphs: • CPU • Clients • Throughput • Throughput - Radio 1(2.4 GHz) • Throughput - Radio 2(5 GHz) 
cnReach	Displays the following graphs: • Noise • Neighbors • RSSI • Throughput • Transmit Power

Table 19: Performance Graph

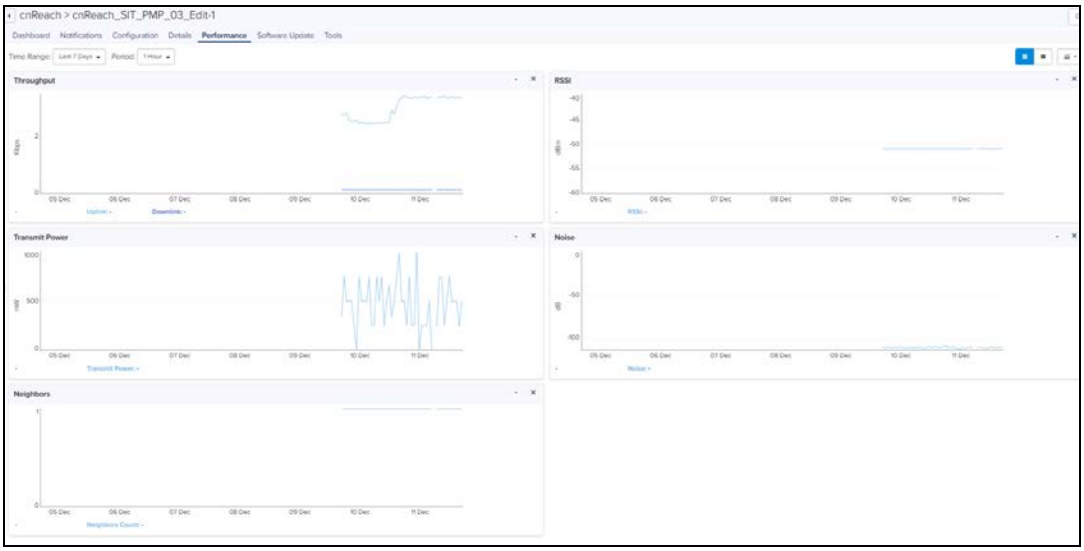
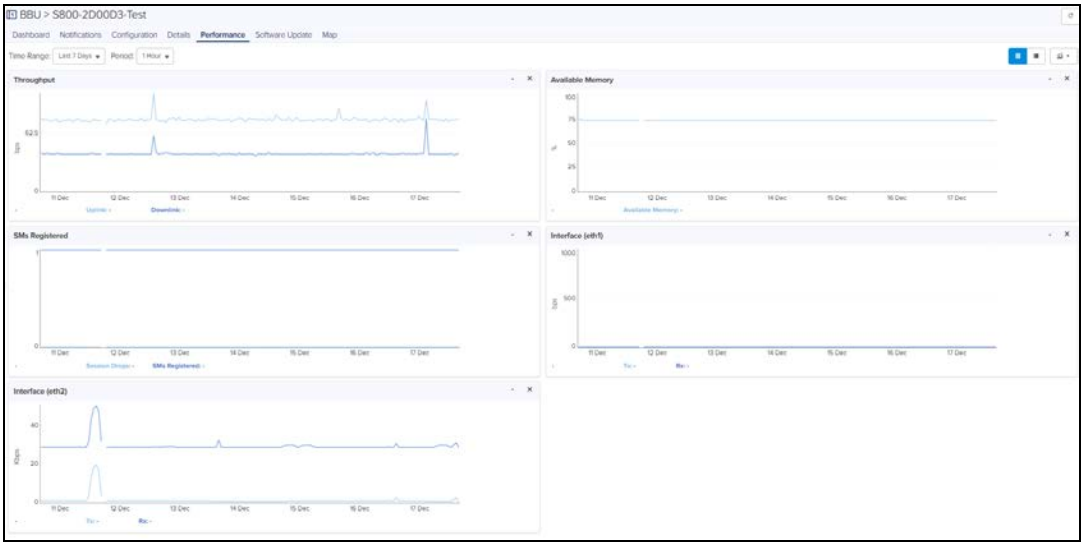
Device	Fields
	
cnRanger BBU	Displays the following graphs: • Available Memory • Interface (eth1) • Interface (eth2) • SMs Registered • Temperature • Troughput 
cnRanger RRH	Displays the following graphs: • Ambient Temperature • CPU • Die Temperature

Table 19: Performance Graph

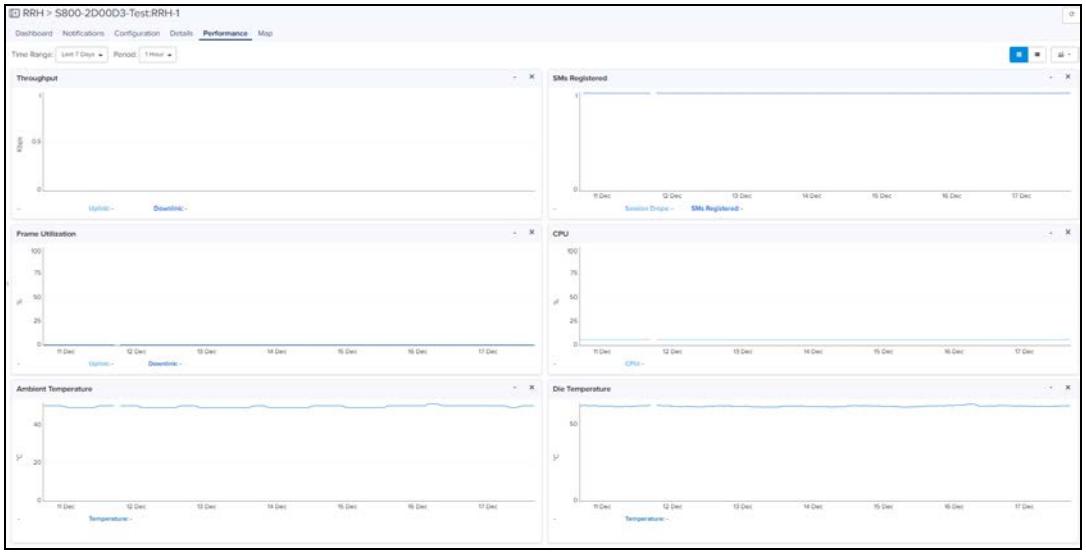
Device	Fields
	• Frame Utilization • SMs Registered • Throughput 
cnRanger SM	Displays the following graphs: • Available Memory • CPU • MCS • RSRP • RSSI • RSRQ • SINR • Throughput

Table 19: Performance Graph

Device	Fields
cnVision Client	Displays the following graphs: • CPU • MCS • Retransmission • RSSI • SNR • Session Drops • Throughput

Table 19: Performance Graph

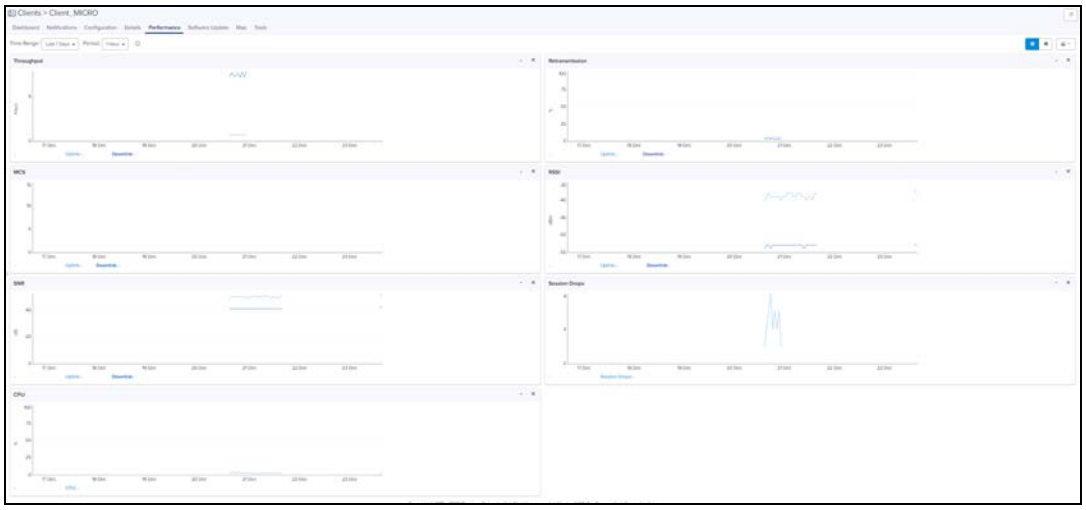
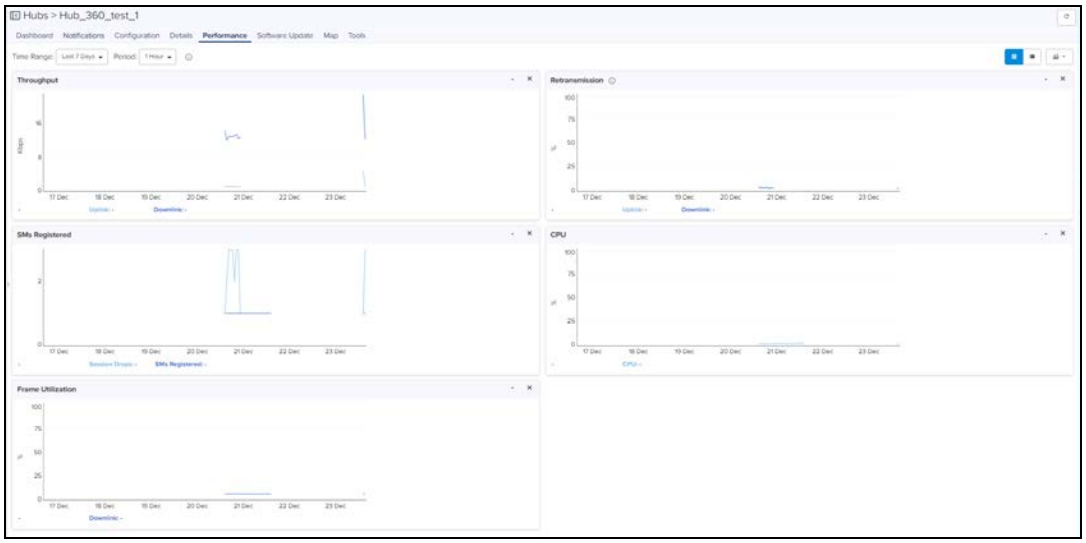
Device	Fields
	
cnVision Hub	Displays the following graphs: • CPU • Frame Utilization • Retransmission • SMs Registered • Throughput 
Enterprise Wi-Fi	Displays the following graphs: • Airtime (2.4 GHz) • Airtime (5 GHz) • Available Memory • Clients • CPU

Table 19: Performance Graph

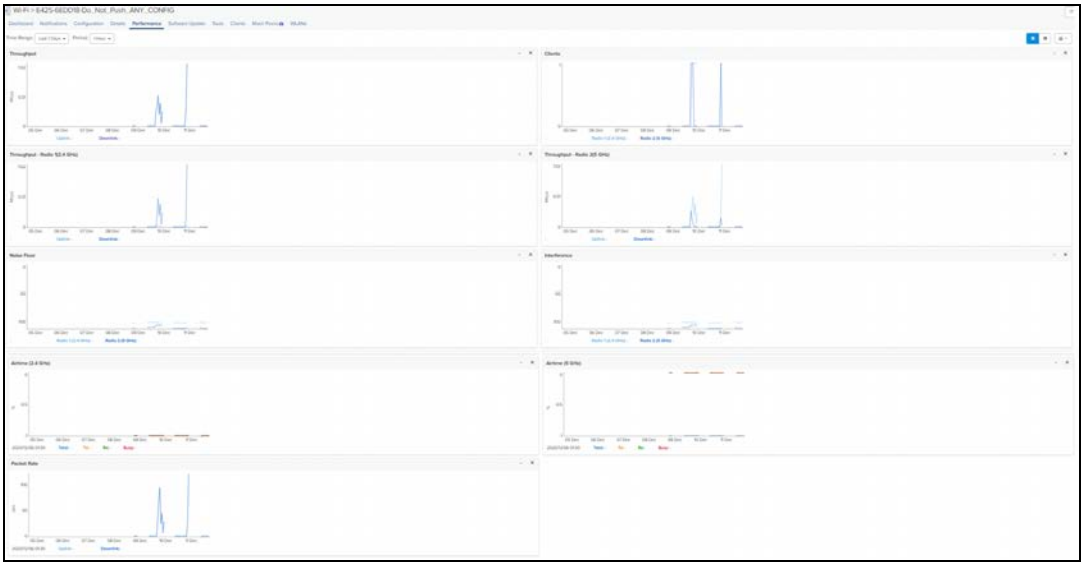
Device	Fields
	• Interference • Noise Floor • Packet Rate • Throughput • Throughput - Radio 1 (2.4 GHz) • Throughput - Radio 2 (5 GHz) 
ePMP AP	Displays the following graphs: • CPU • Frame Utilization • Retransmission • SMs Registered • Throughput

Table 19: Performance Graph

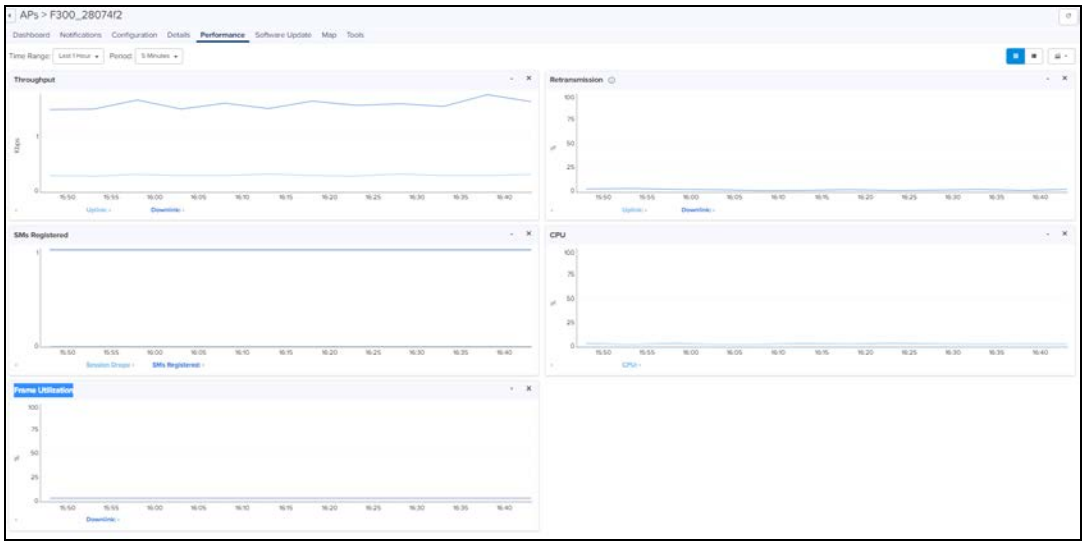
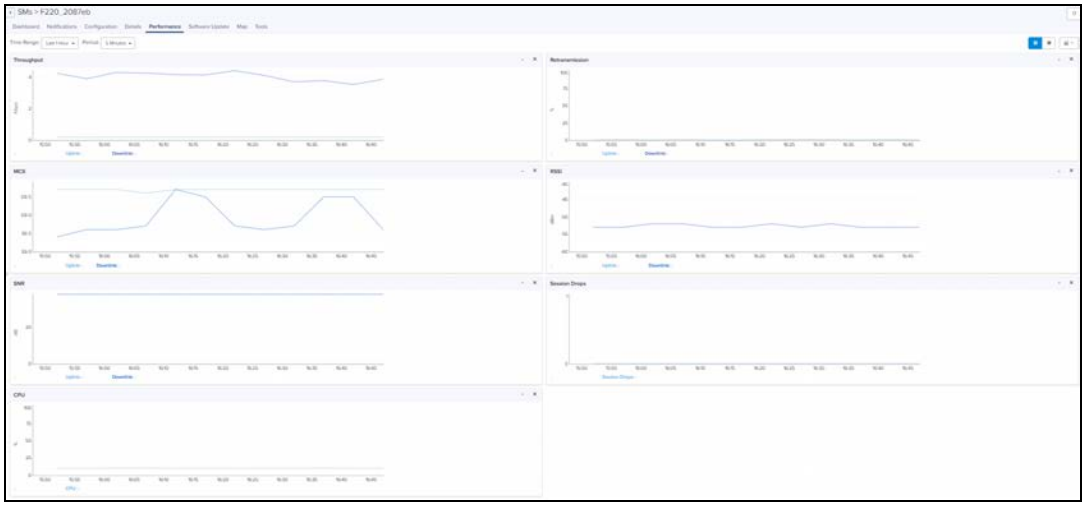
Device	Fields
	
ePMP SM	Displays the following graphs: • CPU • MCS • Retransmission • RSSI • Session Drops • SNR • Throughput 
Machfu	Displays the following graphs: • Cellular Throughput • Cellular RSSI • CPU Load

Table 19: Performance Graph

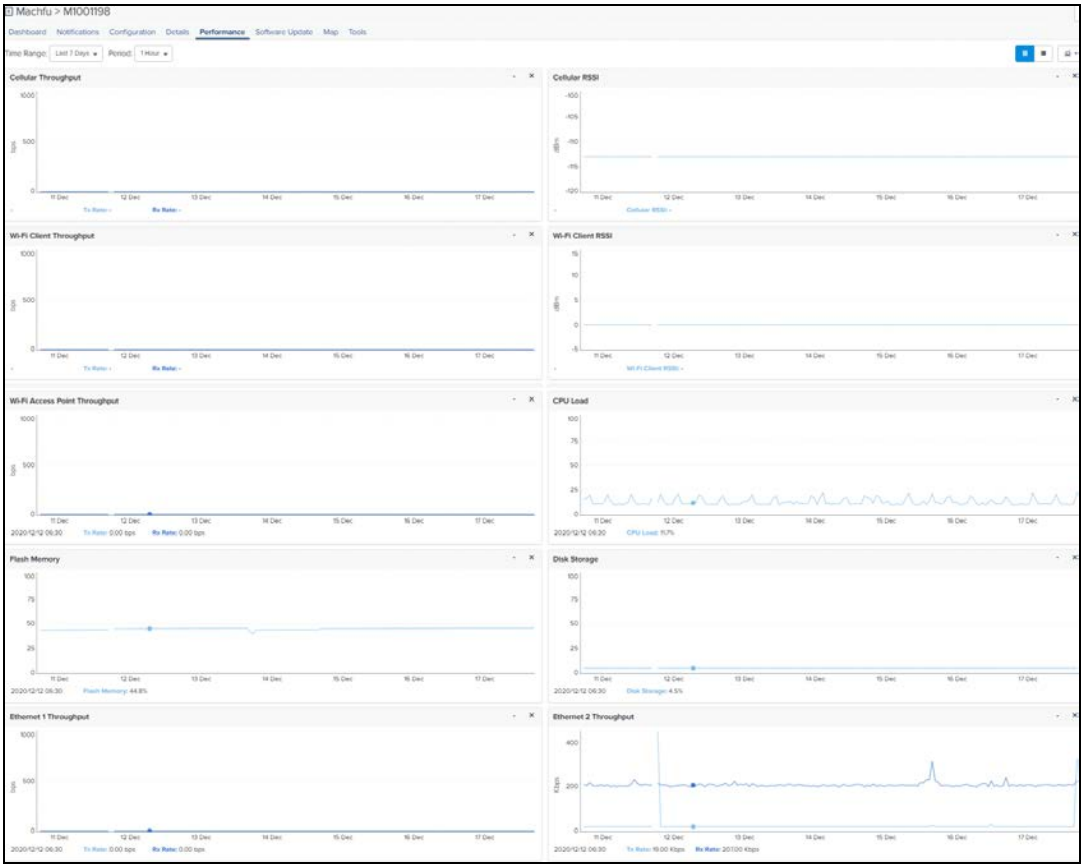
Device	Fields
	• Disk Storage • Ethernet 1 Throughput • Ethernet 2 Throughput • Flash Memory • Wi-Fi Client Throughput • Wi-Fi Client RSSI • Wi-Fi Access Point Throughput 
PMP AP	Displays the following graphs: • CPU • Frame Utilization • SMs Registered • Throughput

Table 19: Performance Graph

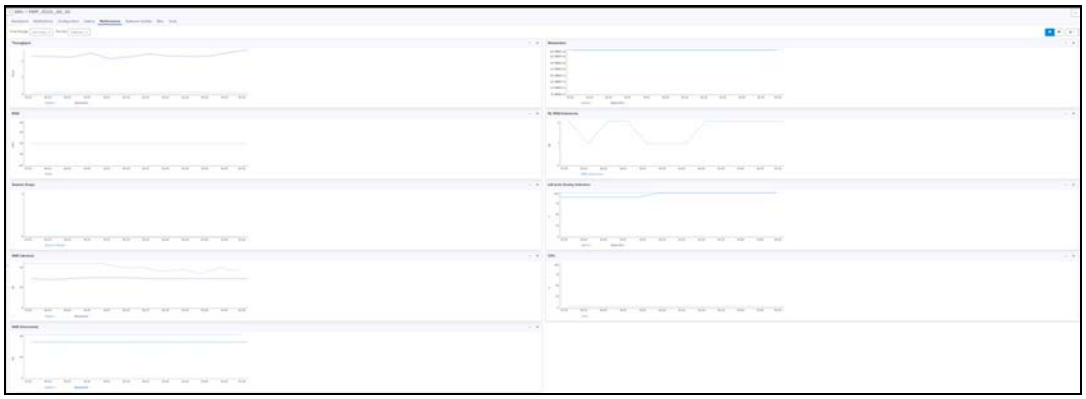
Device	Fields
PMP SM	Displays the following graphs: • CPU • DL RSSI Imbalance • LQI (Link Quality Indicator) • Modulation • RSSI • Session Drops • SNR (Horizontal) • SNR (Vertical) • Throughput 
PTP and HCMP Masters	Displays the following graphs: • Aux Throughput • Channel Utilization • Capacity • Link Loss • Main PSU Throughput

Table 19: Performance Graph

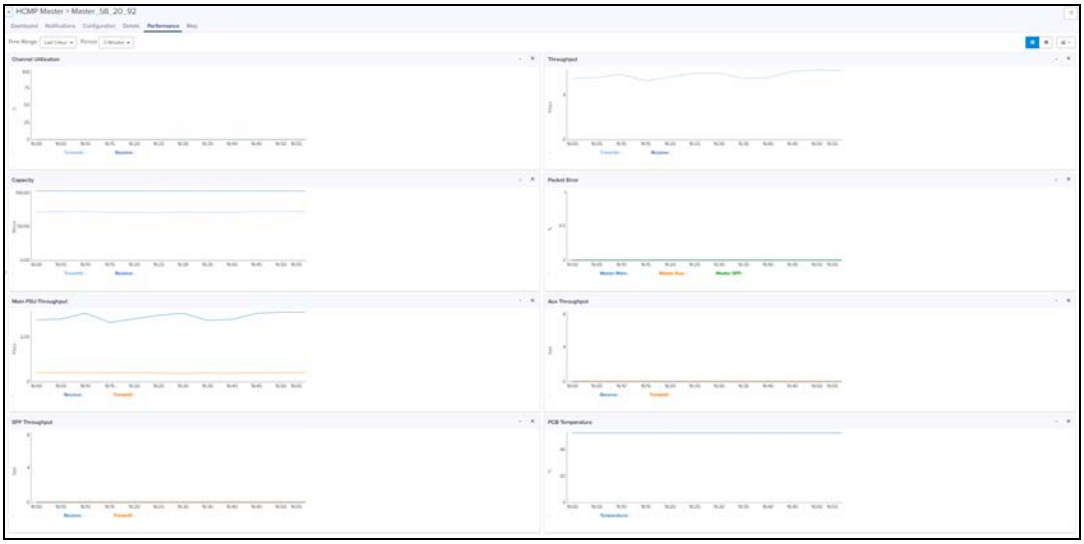
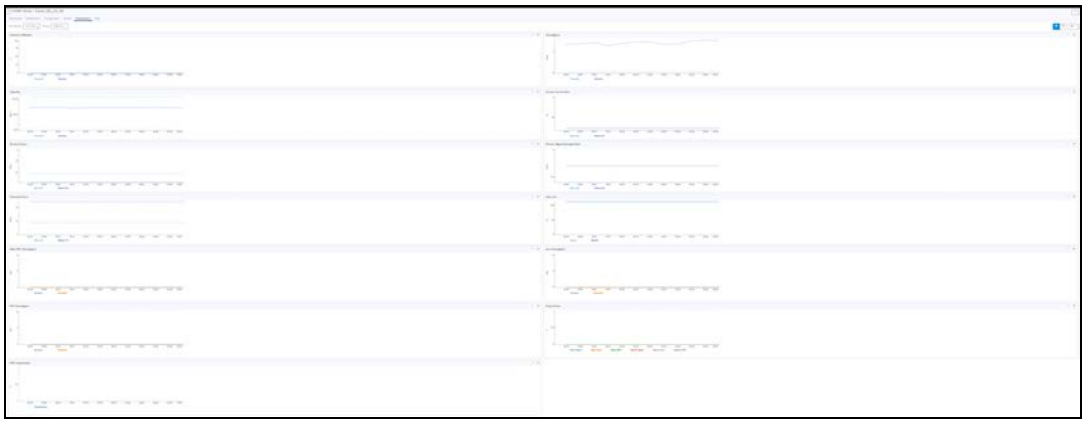
Device	Fields
	• Packet Error • PCB Temperature • Receive Vector Error • Receive Power • Receive Signal Strength Ratio • SFP Throughput • Throughput • Transmit Power 
PTP and HCMP Slaves	Displays the following graphs: • Aux Throughput • Channel Utilization • Capacity • Main PSU Throughput • Link Loss • Packet Error • PCB Temperature • Receive Vector Error • Receive Power • Receive Signal Strength Ratio • SFP Troughput • Throughput • Transmit Power

Table 19: Performance Graph

Device	Fields
	

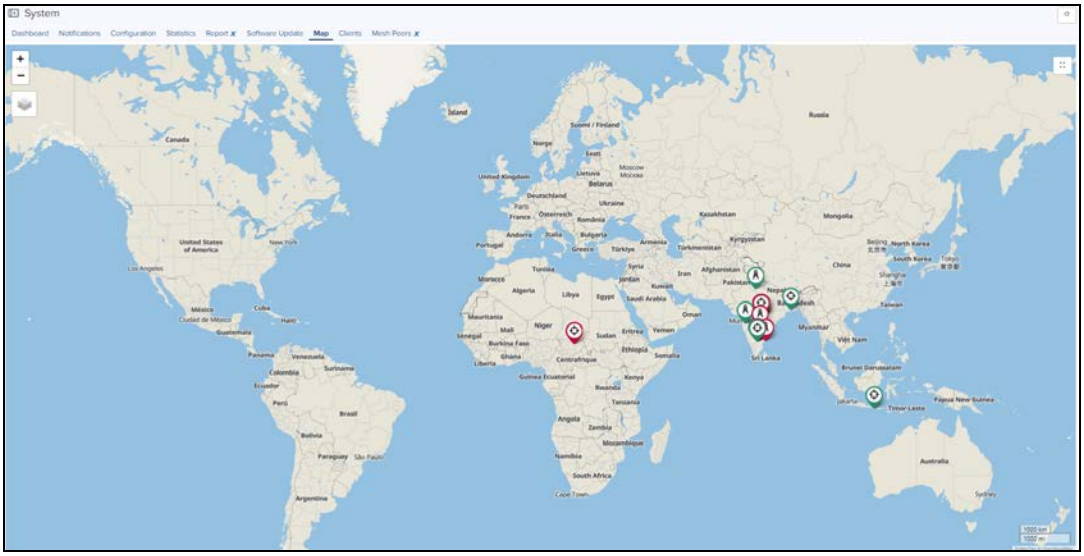
Maps

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 maps:

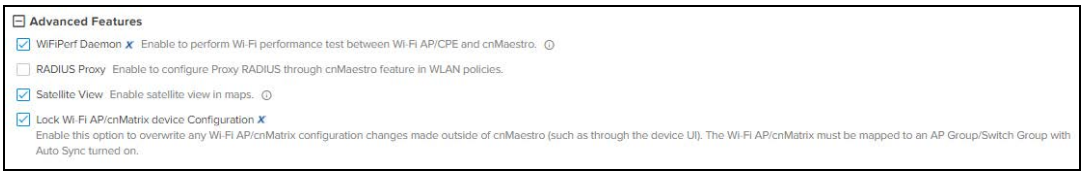
- Street view
- Satellite view

Figure 23 Map Street View



To enable satellite view:

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



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

Figure 24 Map Satellite View

Map Navigation

There are a number of ways to navigate through the map display.

Double Click	If the user double-clicks on the following items on the Map, the UI should auto-navigate to the Dashboard of that item: • 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.
Single Click	If the user single-clicks on the following items on the Map, auto-select the same item in the tree: • ePMP SM • Tower
Standard Components	In the upper-left corner are generic map navigation components that allow one to zoom in and out. One 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 20: Mode

Mode	Details
Alarm Status	Highlights devices based upon alarm count (critical, major, minor).
Average MCS (ePMP only)	Displays the uplink or downlink average MCS per device.
Device Status	Displays whether a device is up (green) or down (red).
Frequency	Displays the sector frequency.
Link Quality Indicator (PMP only)	Displays the uplink or downlink average indicator per device.
Reregistration Count	Displays the nodes based upon the number of re-registrations in the last 24 hours. The more reregistration, the larger the node will display.
Retransmission Percentage (ePMP only)	Displays the percentage of packets retransmitted between ePMP SM and AP on the wireless link.

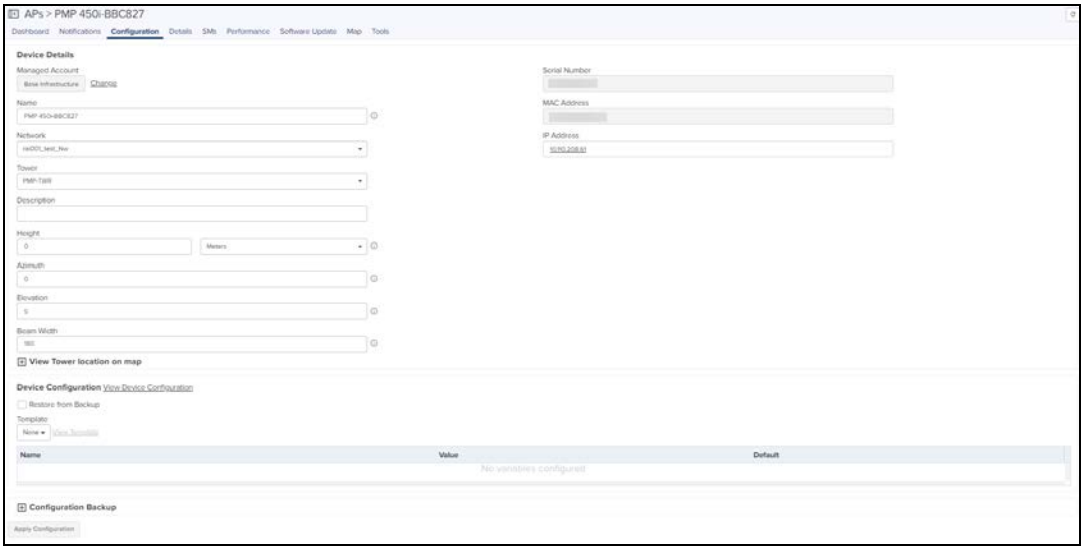
Embedded Maps

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

Sector Visualization

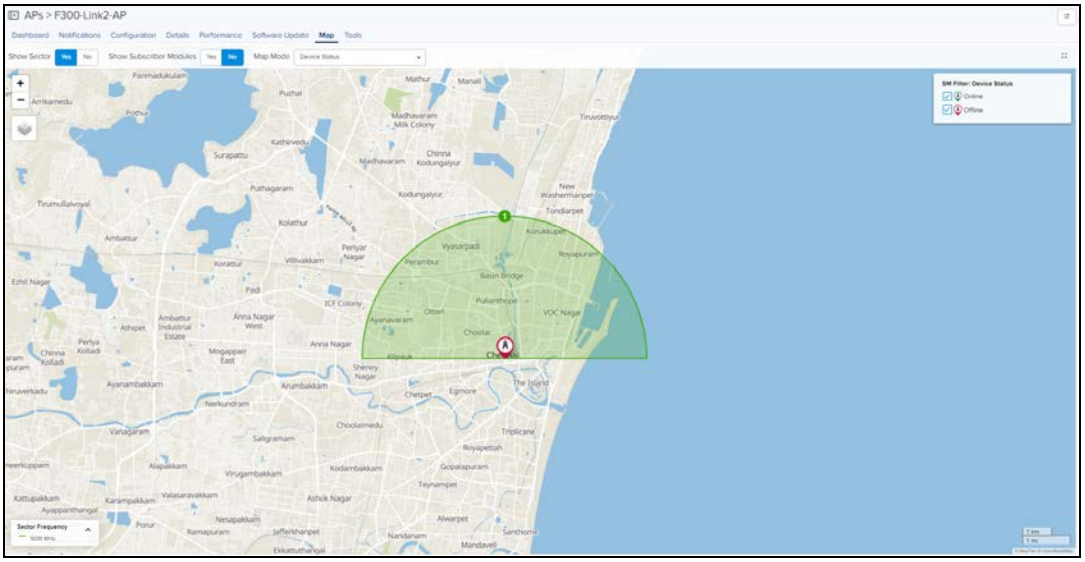
cnMaestro is able to present a basic sector View for ePMP and PMP fixed wireless devices. This requires configuration of Height, Azimuth, Elevation and Beam Width under ePMP/PMP AP configuration. This configured data is used to generate the sector view: the presentation is not based upon link planning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

Figure 25 AP Configuration Page



A new option for **Sector Visualization** is available in map view. By selecting the **Show Sector** option, the following map is displayed:

Figure 26 Sector Visualization



In addition to Sector Visualization, a new option is available to show/hide Subscriber Modules. This is present at System, Network, Tower, and AP levels. You can also choose to set the color of SMs based upon frequency or online/offline state.

> **NOTE:**
> The default settings to **show subscriber** modules is **No.**

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, Services, and Settings. Refer to E2E Network Tools.

In Nodes **Tools** tab you can view the status and Debug 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.

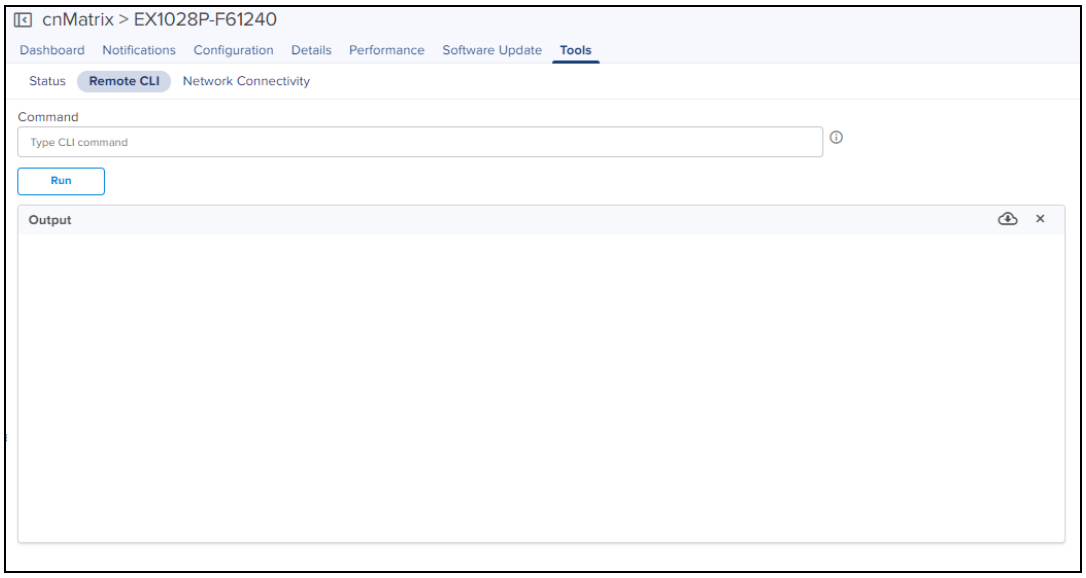
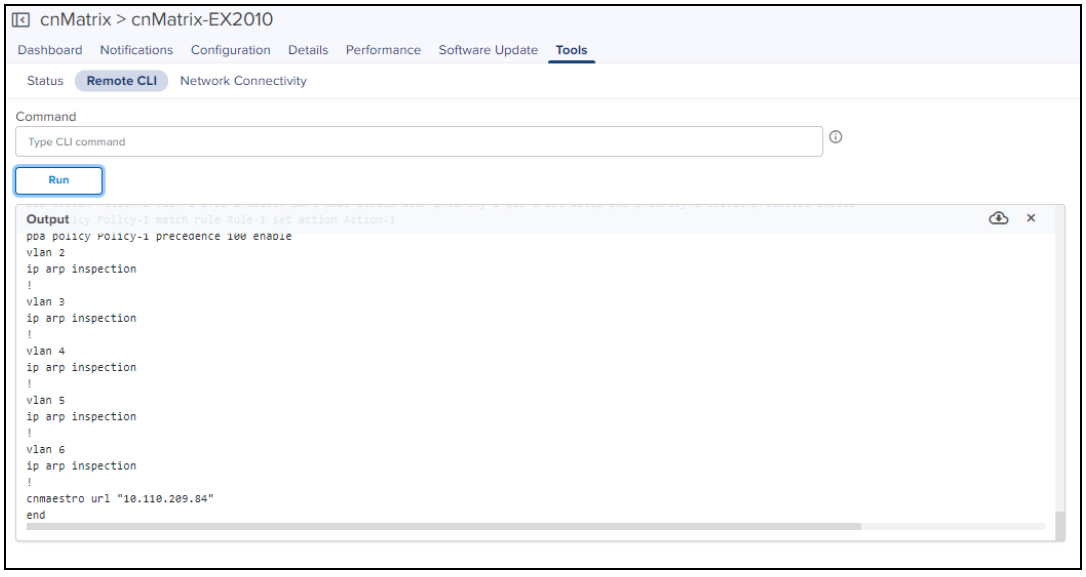


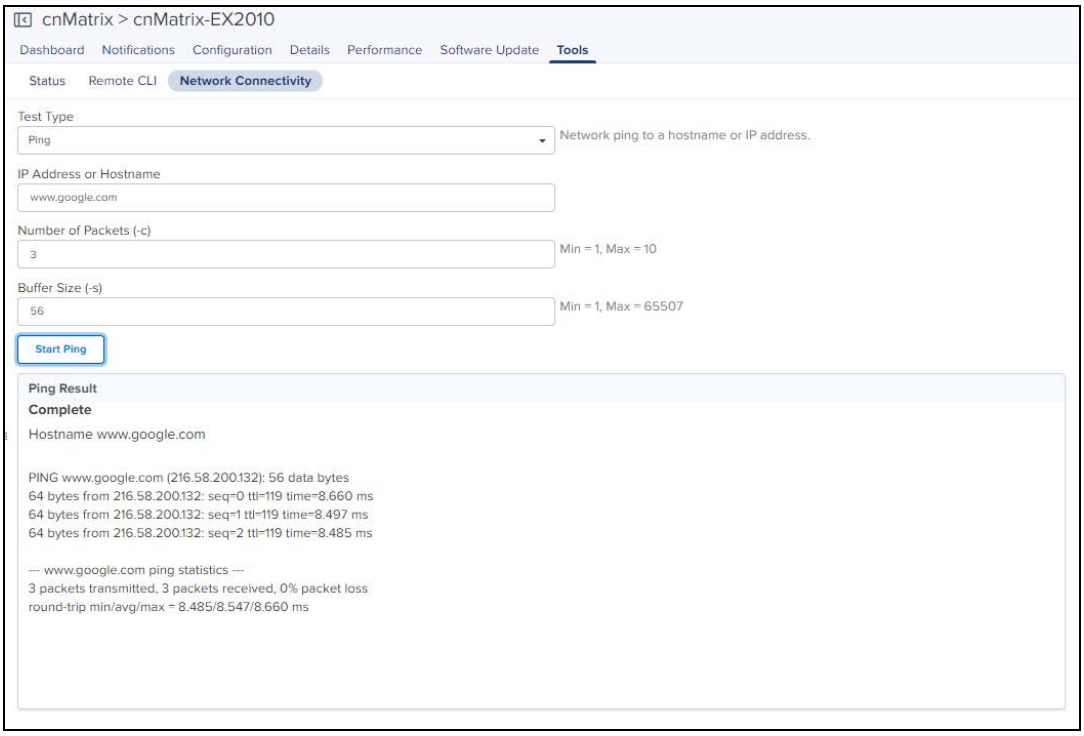
Table 21: CnMatrix Tools

Tools	Description
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.

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



- Click icon to download the generated output.
- Click icon to clear the generated output.



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 22: 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 27 cnPilot Tools Enterprise WiFi

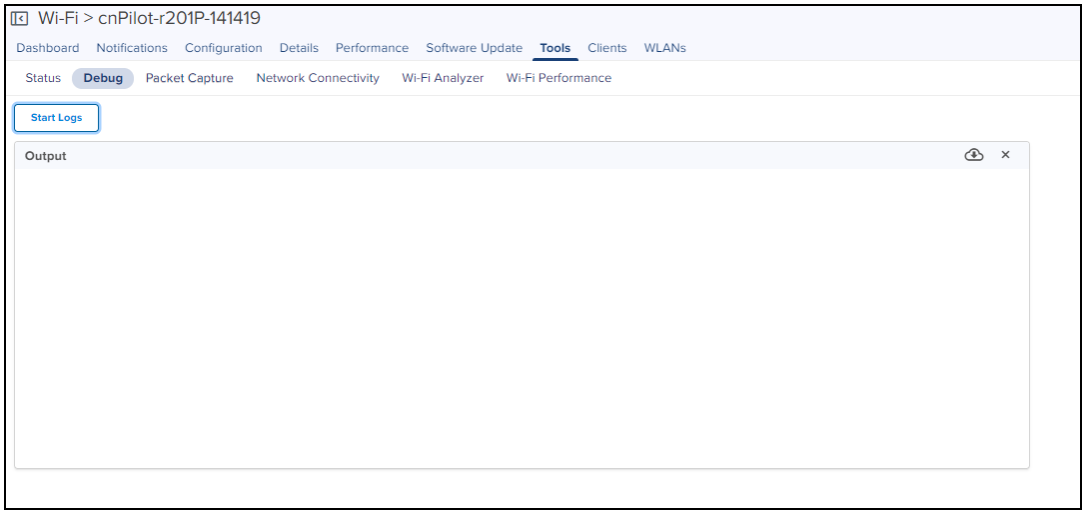


Figure 28 cnPilot Tools Status

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

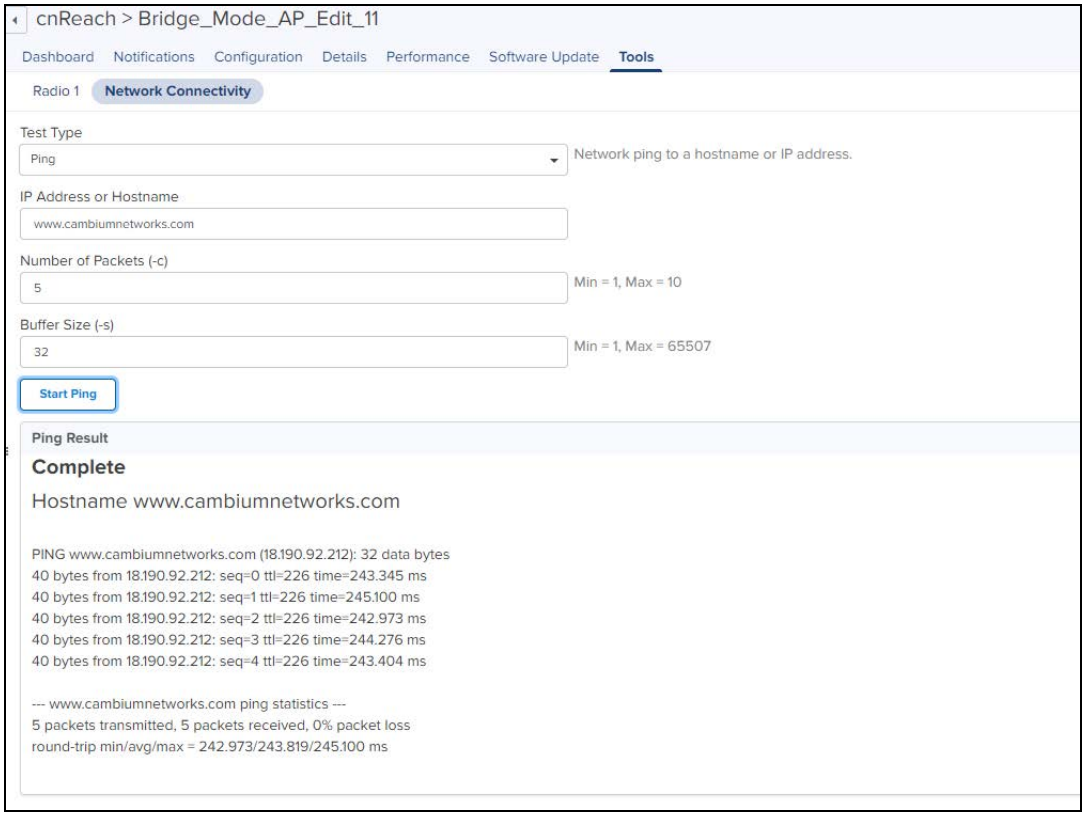
The Tools page for cnReach devices consolidates a number of operations into a single troubleshooting interface.

The operations are listed below:

Table 23: 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 29 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 24: cnVision Tools

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

Table 24: cnVision Tools

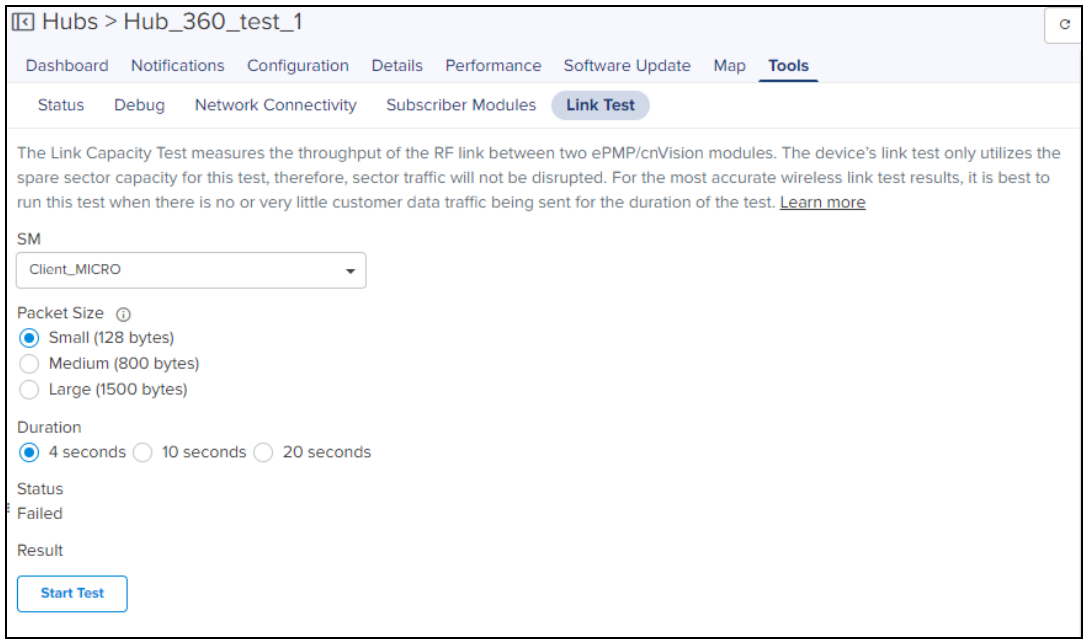
Field	Description
Subscriber Modules	Displays the SM linked to the Hub and allows to reboot and download the tech support file.
Link Test	The Link Capacity Test measures the throughput of the RF link between two cnVision modules. cnVision link test only utilizes the spare sector capacity for this test, 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.. 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.. • If an cnVisiosn Hub is selected you can choose the SM from the list and start the test.  Displays the following fields: • **Packet Size**: Choose the Packet Size to use for the throughput test. • **Duration**: Choose the time duration in seconds to use for the throughput test. • If an cnVision Client is selected, click Start Test to run the link test.

Table 24: cnVision Tools

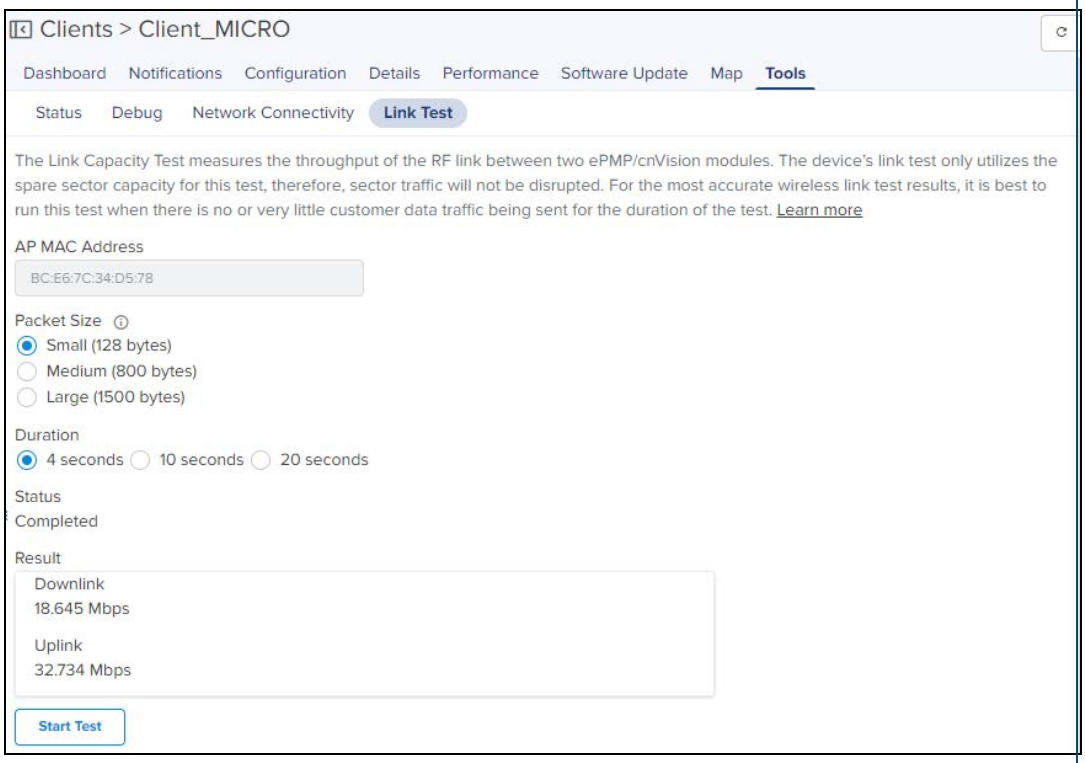
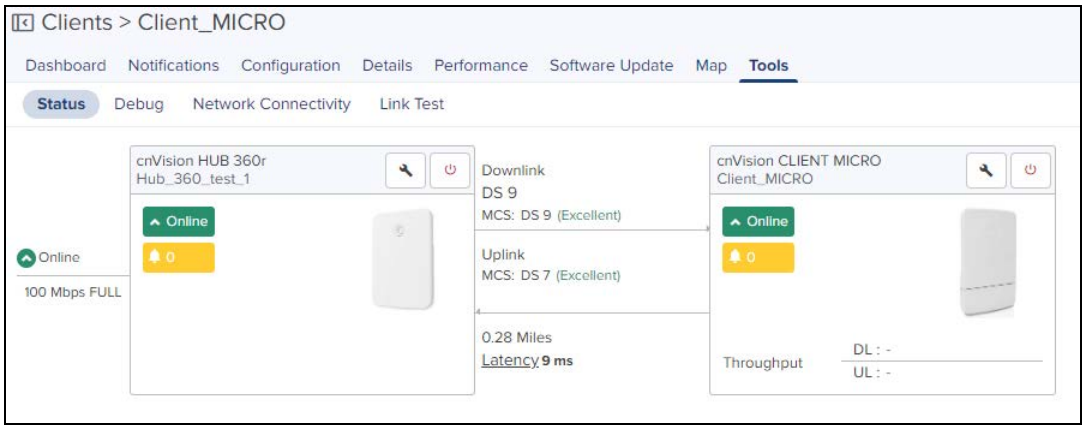
Field	Description
	 Displays the following fields: • **Packet Size**: Choose the Packet Size to use for the throughput test. • **Duration**: Choose the time duration in seconds to use for the throughput test.

Figure 30 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 25: 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 31 Enterprise Wi-Fi Tools

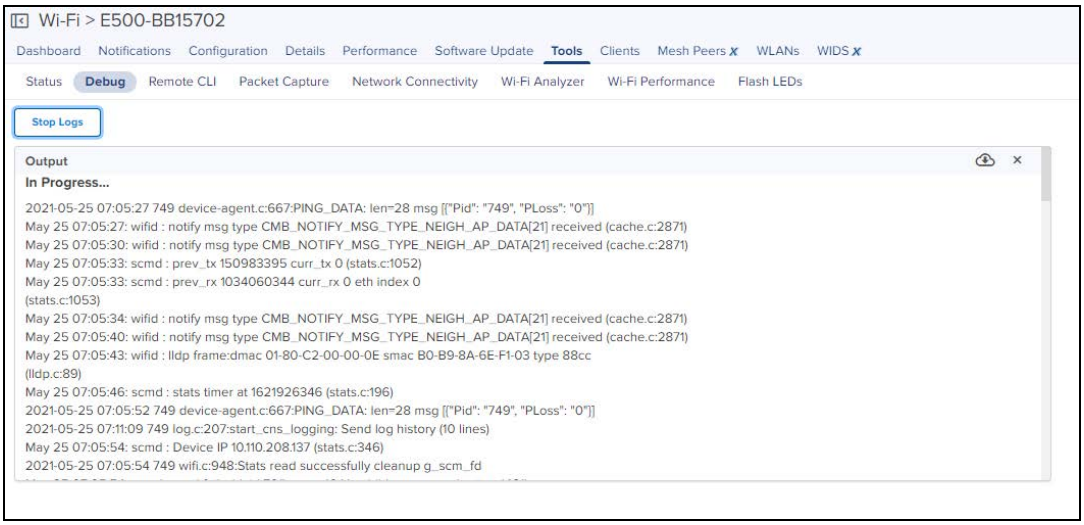


Figure 32 Enterprise Wi-Fi Remote CLI Tools

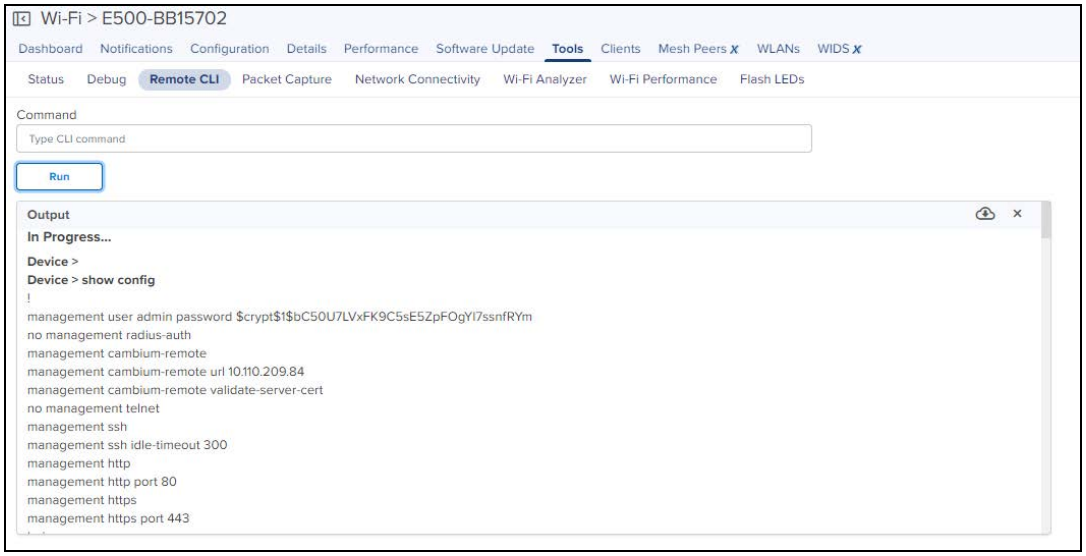
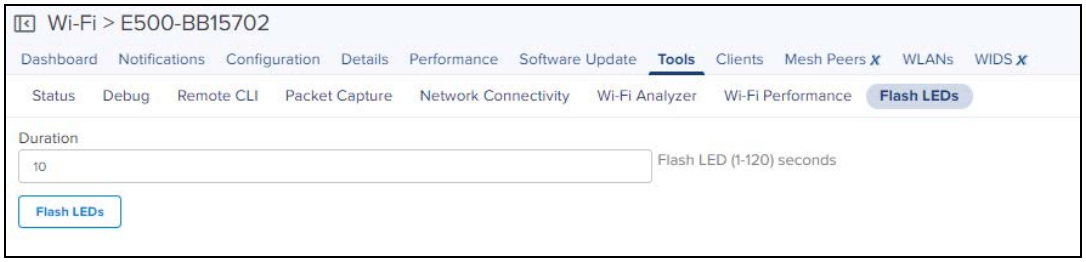


Figure 33 Flash LEDs

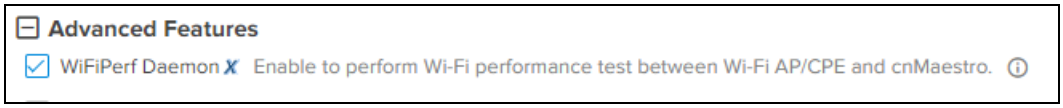


Wi-Fi Performance Test

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.

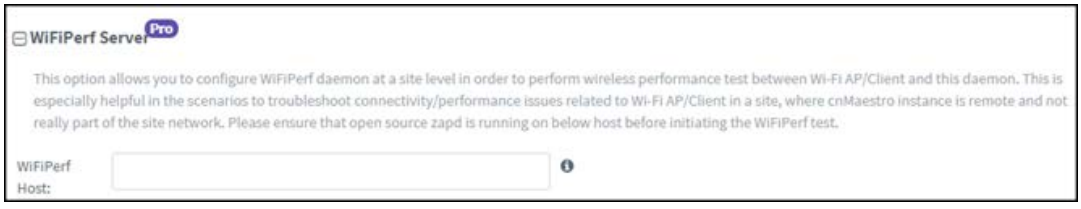
- **cnMaestro Instance :** To enable Wi-Fi performance test, navigate to **Administration > Settings > Advanced Features** page and enable **WiFiPerf Daemon** option.



- **Locally installed Wi-Fi Performance Server** : Wifiperf performance interoperates 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** > **WiFiPerf Server** page.



	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.
	NOTE: For more details on Wi-Fi performance (wifiperf) feature, refer here.

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 26: ePMP Tools

Tools	Description
Debug	Displays the log details.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the status.
Link Test	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.. Displays the link related test result with respect to Throughput. Link Test can be performed on the ePMP AP and its SM link. In order to run this operation, select the device and then the **Tools** tab. • If an ePMP AP is selected you can choose the SM from the list and start the test.

Table 26: ePMP Tools

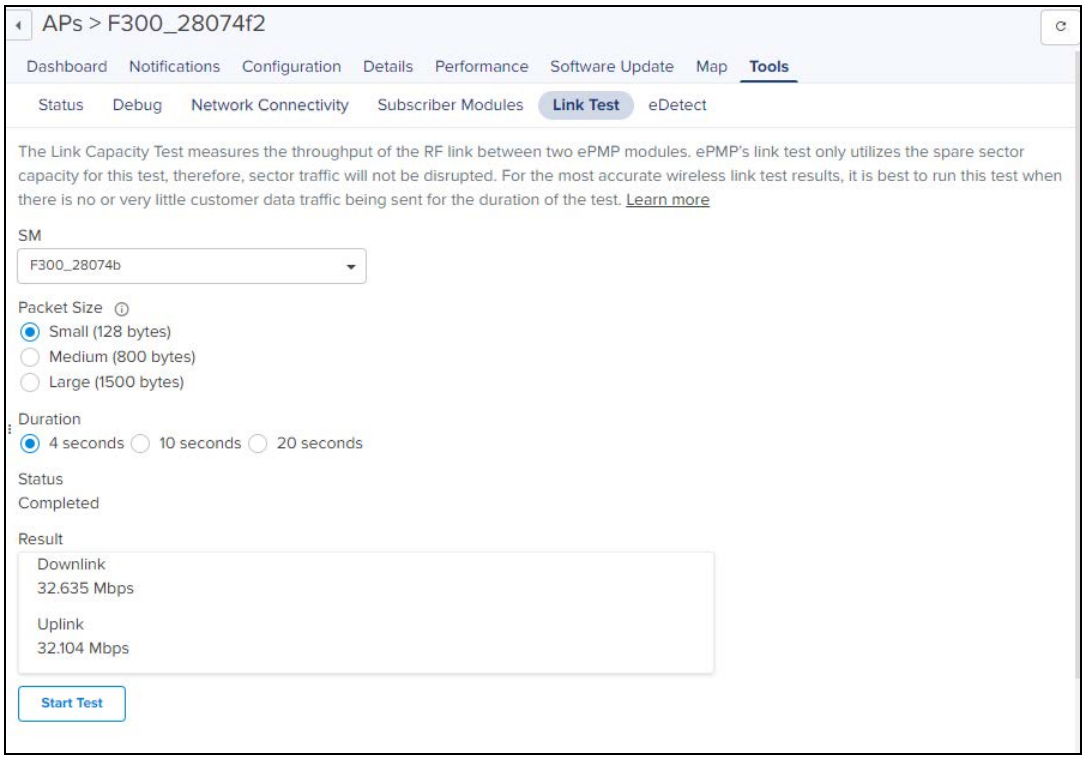
Tools	Description
	 Displays the following fields: • **Packet Size**: Choose the packet size to use for the throughput test. • **Duration**: Choose the time duration in seconds to use for the throughput test: • If an ePMP SM is selected, click Start Test to run the link test.

Table 26: ePMP Tools

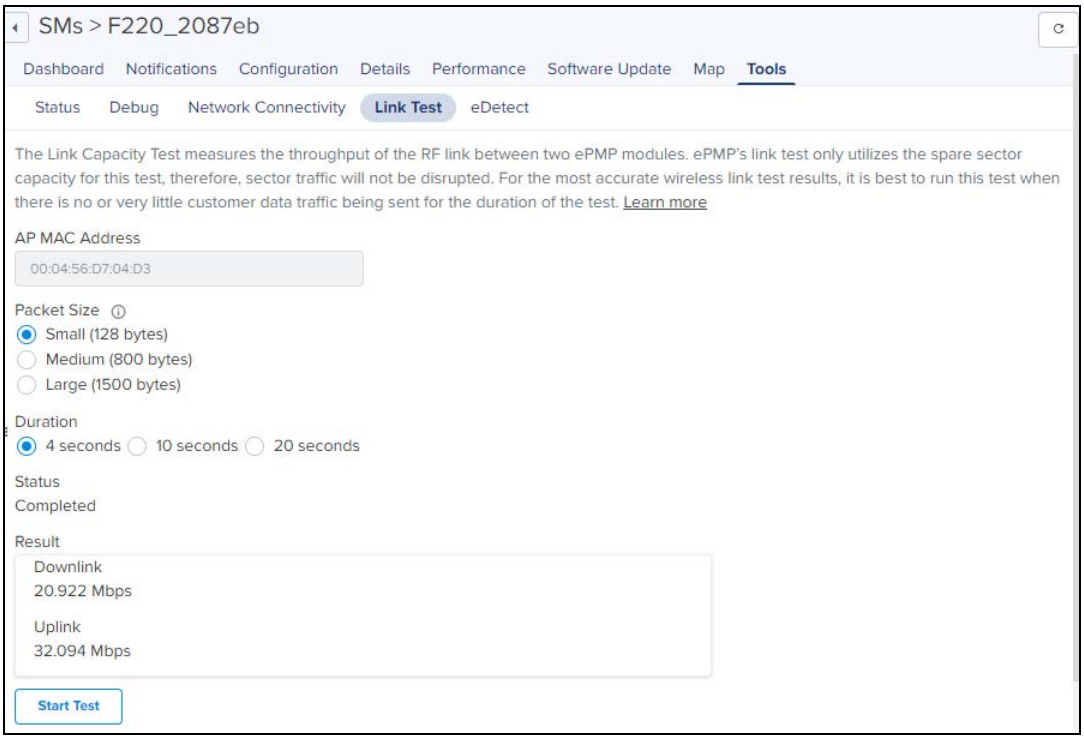
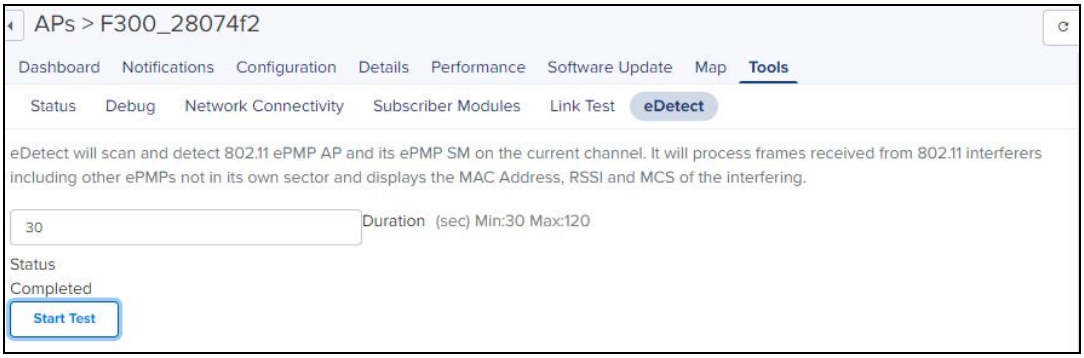
Tools	Description
	 Displays the following fields: • **Packet Size**: Choose the Packet Size to use for the throughput test. • **Duration**: Choose the time duration in seconds to use for the throughput test.
eDetect	eDetect is supported on the ePMP AP or SM. It is also launched from the **Tools** tab. The eDetect tool (not available in ePMP Master/Slave mode) is used to measure the 802.11 interference at the ePMP radio or system when run from the AP or the SM, on the current operating channel. When the tool is run, the ePMP device processes all frames received from devices not connected to the ePMP system and collects the interfering frame's information such as MAC Address, RSSI, and MCS. Configure the duration for which the AP scans for interference.  Configure the duration for which the SM scans for interference.

Table 26: ePMP Tools

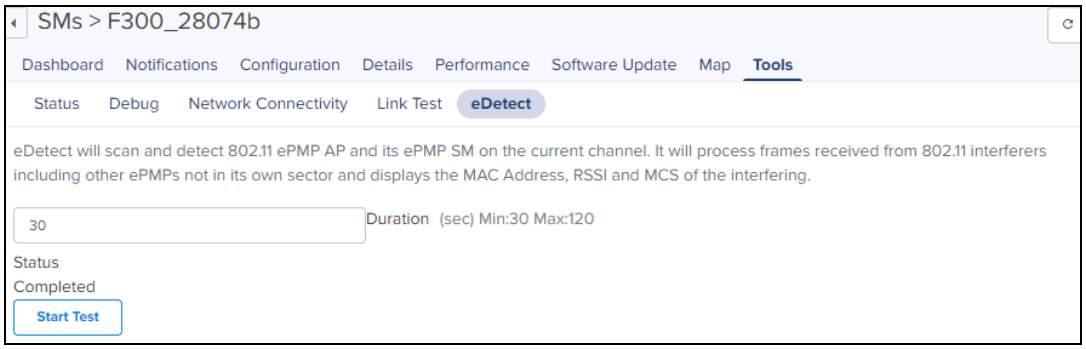
Tools	Description
	

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 27: PMP Tools

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

Table 27: PMP Tools

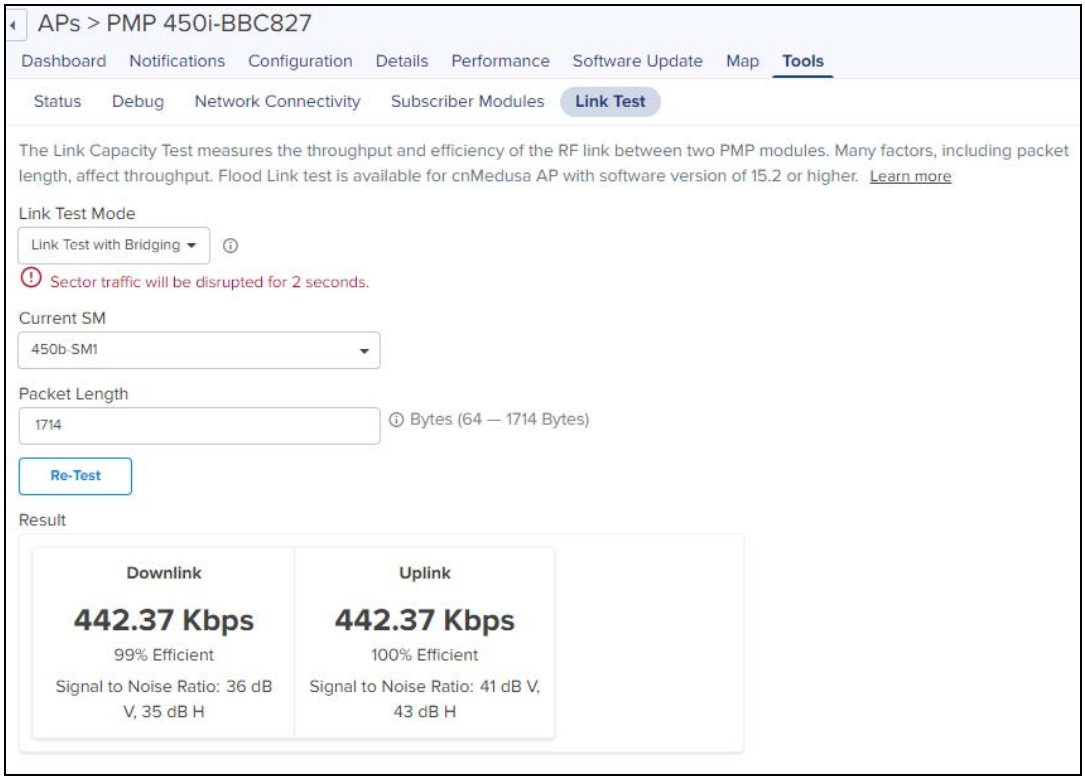
Tools	Description
Subscriber Modules	Lists all the SMs connected to the selected AP. This is available for PMP APs only.
Link Test	The Link Capacity Test measures the throughput and efficiency of the RF link between two PMP modules. Many factors, including packet length, affect throughput. Packets are added to one or more queues in the AP in order to fill the frame. Throughput and efficiency are then calculated during the test The Link Capacity Test tool has following modes: • **Link Test without Bridging** - Tests radio-to-radio communication, but does not bridge traffic. • **Link Test with Bridging** - Bridges traffic to "simulated" Ethernet ports, providing a status of the bridged link. • **Link Test with Bridging and MIR -** Bridges the traffic during test and also adheres to any MIR (Maximum Information Rate) settings for the link. • **Extrapolated Link Test**: Estimates the link capacity by sending few packets and measuring link quality. Displays the link related test result with respect to Throughput and Interference. Link Test can be performed on the PMP AP and its SM link. In order to run this operation, select the device and then the **Tools** tab. • If a PMP AP is selected you can choose the SM from the list and start the test.  • If a PMP SM is selected, click **Start Test** to run the Link Test.

Table 27: PMP Tools

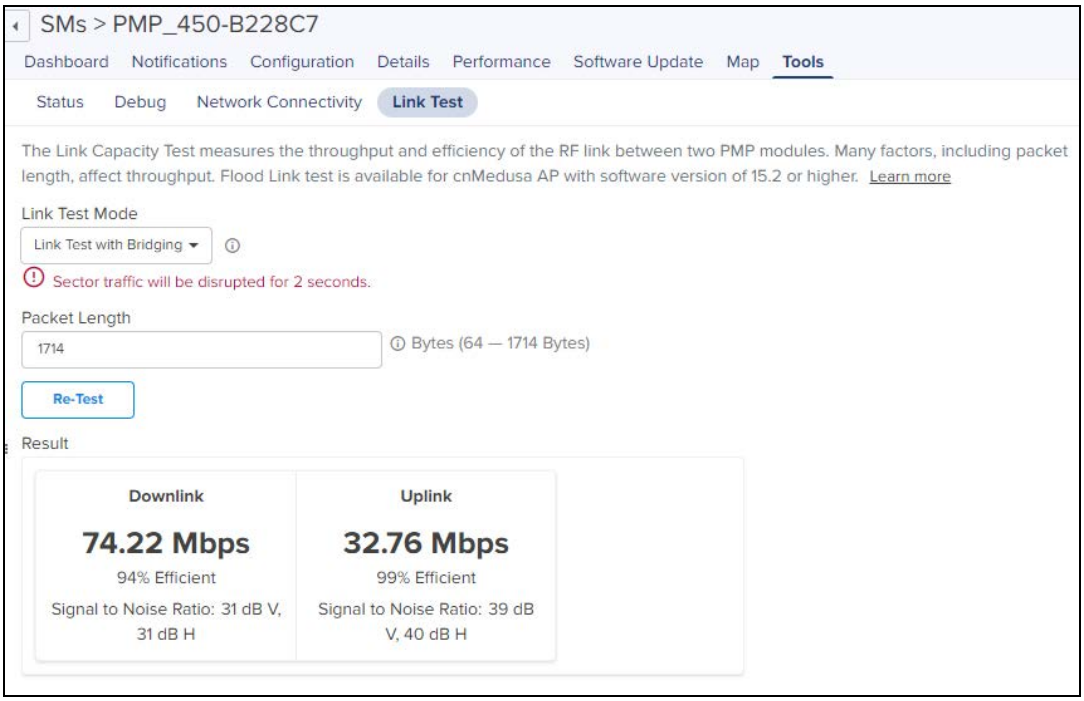
Tools	Description
	

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.

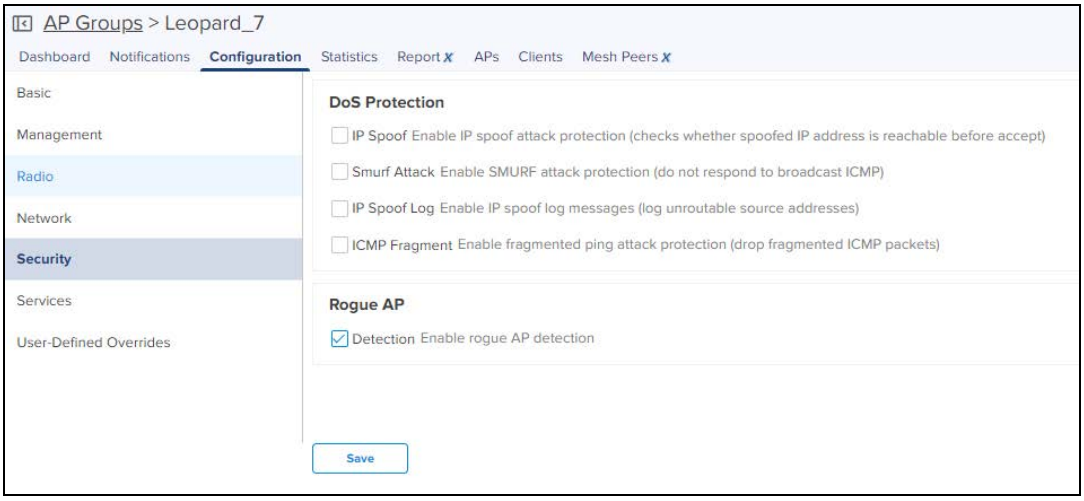
Detecting Rogue APs

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):

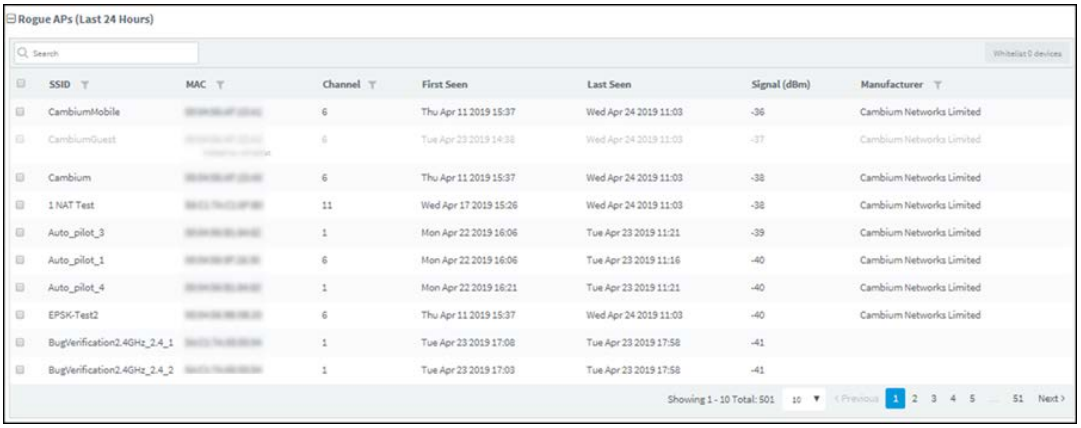
1. Navigate to **AP Groups > Configuration > Radio** (Available on both radio 2.4 GHz and 5 GHz) page.
2. Select the **Enable OCS** check box under **OCS** tab.

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:

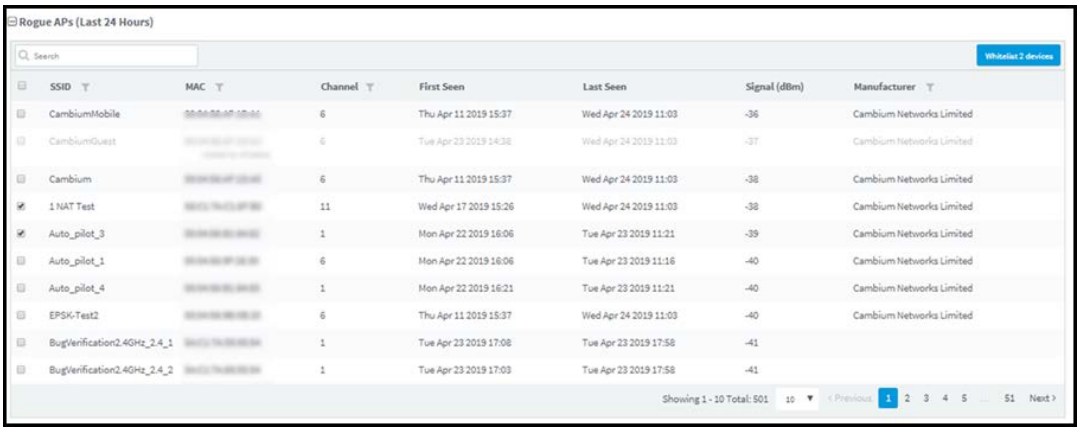
1. Navigate to **APs > WIDS** page.
2. Click **Add Whitelist** under **Site Whitelist** tab.
3. Enter **MAC** and **SSID** of the device to be whitelisted.
4. Click **Save**.

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

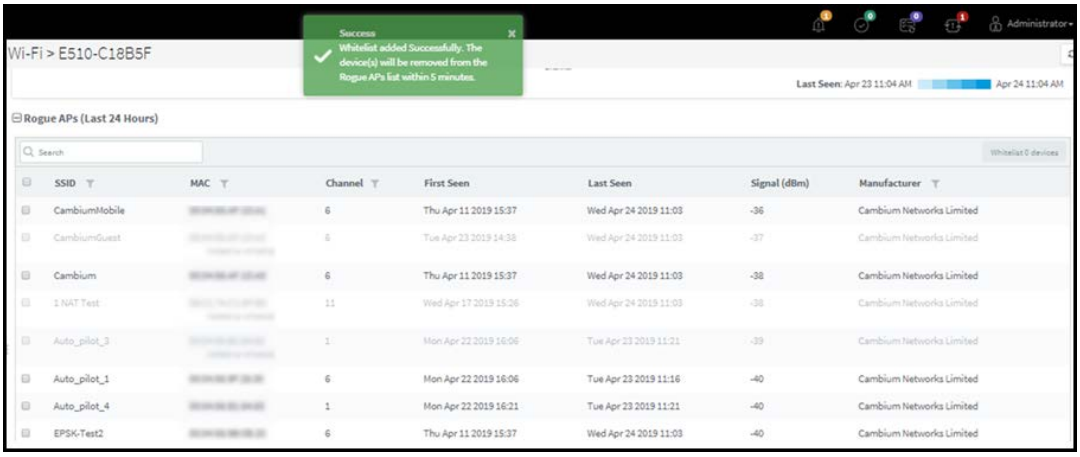


To whitelist multiple Rogue APs:

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

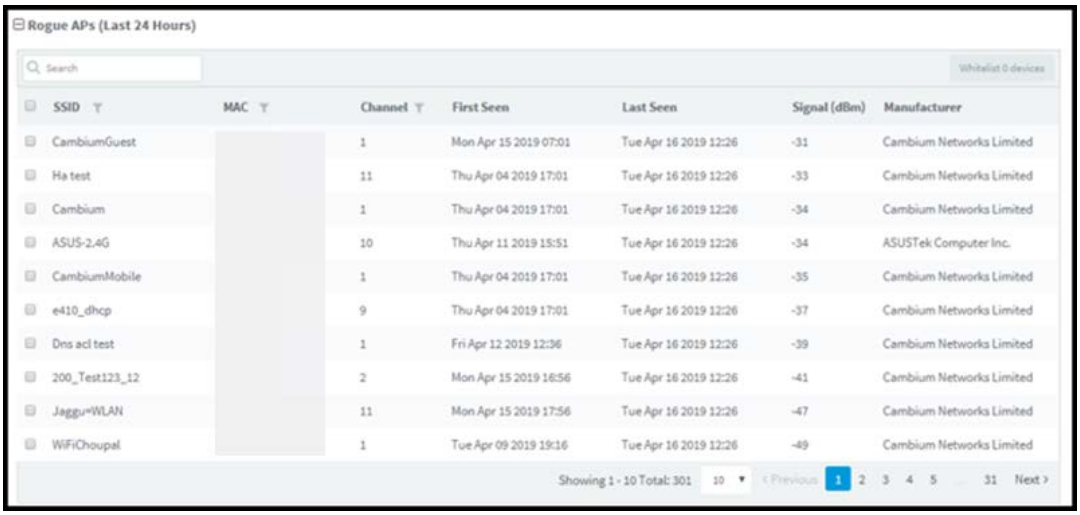


The following pop-up is displayed after successfully adding the Rogue APs to the whitelist.



View List of Rogue APs

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

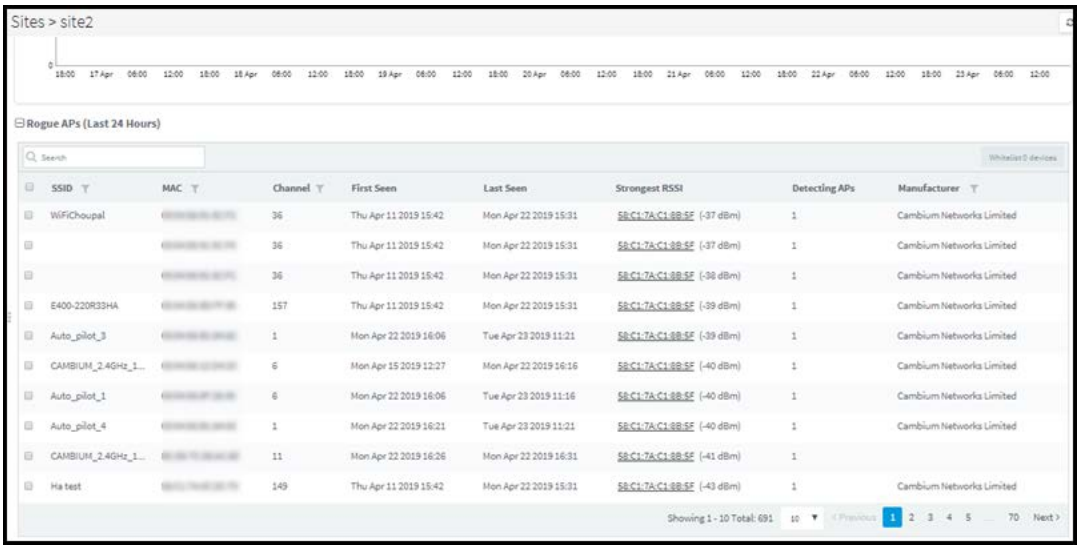


The following parameters are displayed:

- **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)

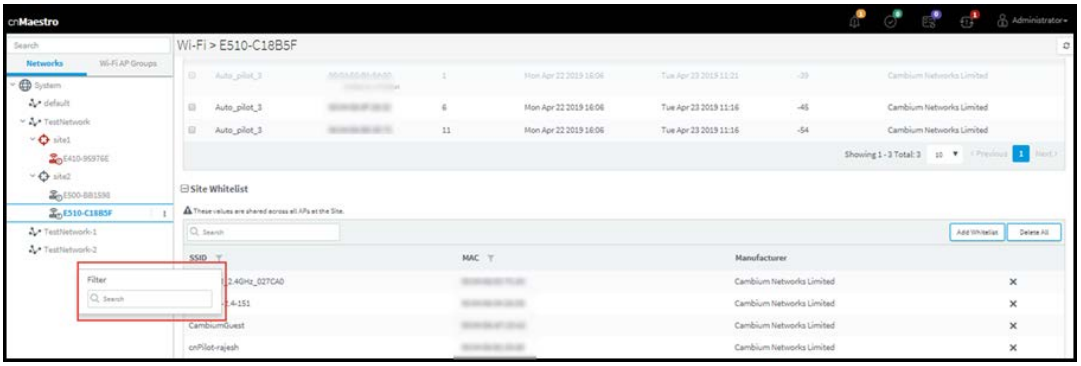
You can view list of Rogue APs at the Site level in the Monitor page:



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.



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

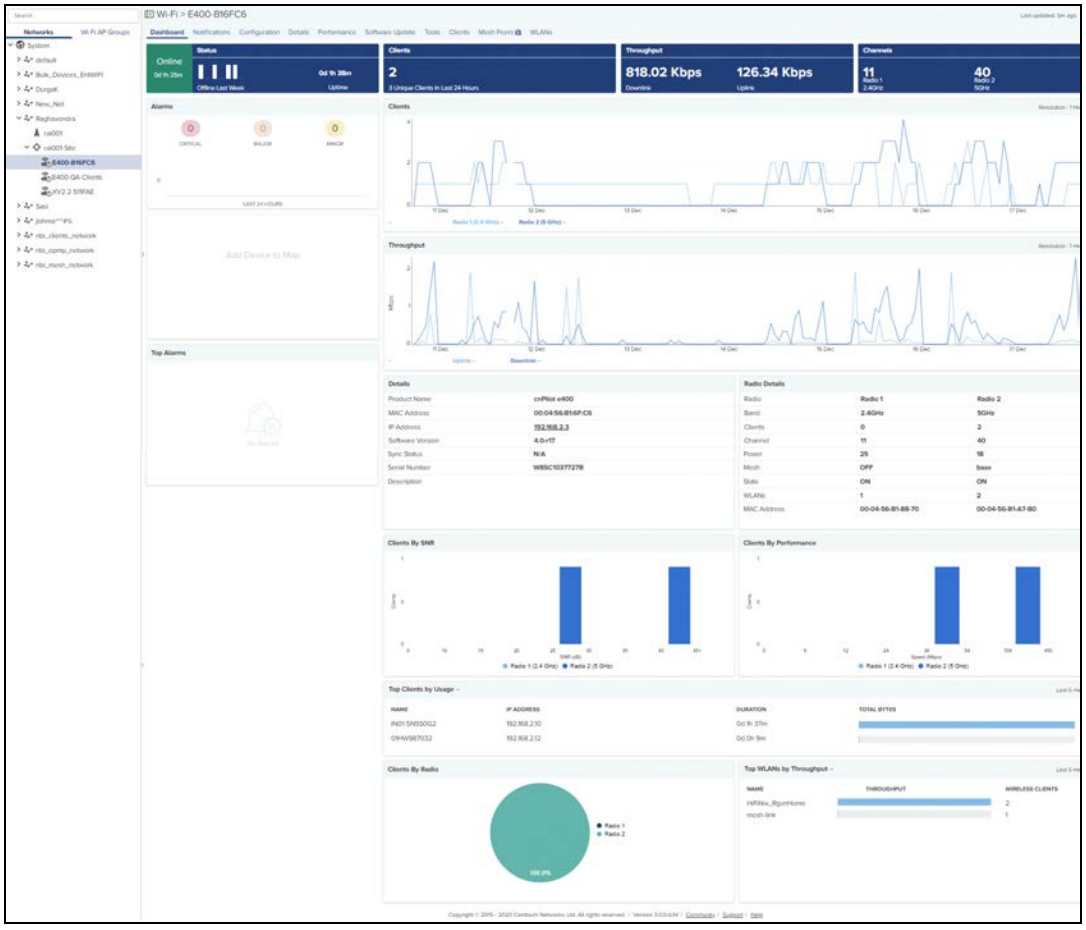
The Device Dashboard page displays details of all the Wi-Fi devices in cnMaestro. It mainly focuses on the following parameters:

- 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 R-Series:

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

Figure 38 cnPilot Home: Device Dashboard > Wired Clients Page

Following parameters displays for Wireless Clients of R-Series:

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

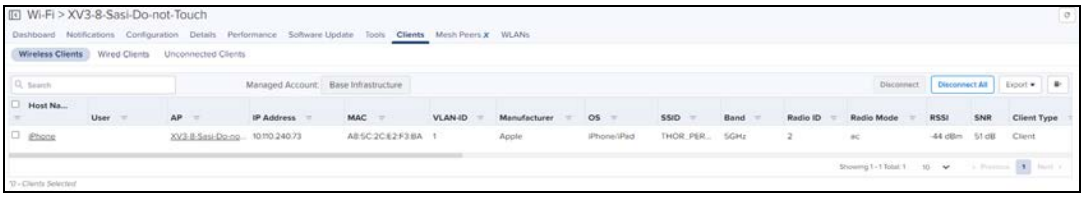
Figure 39 cnPilot Home: Device Dashboard > Wireless Clients Page

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



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

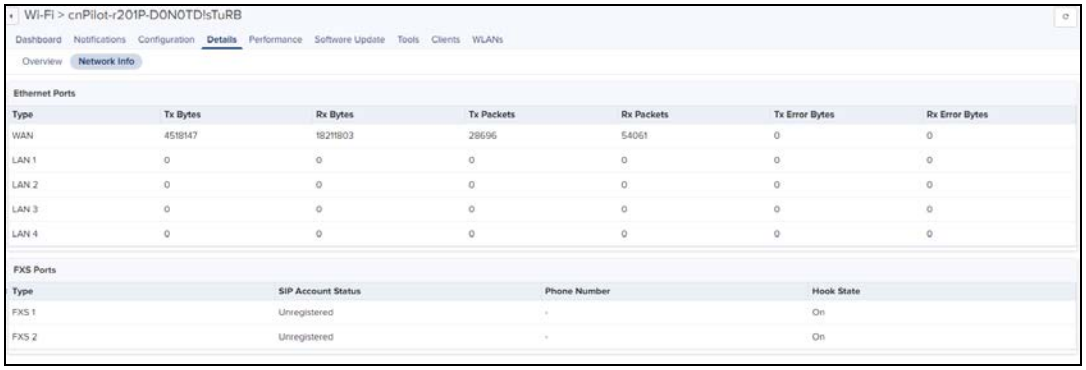
Network Info

The Network Info section displays the details of the Network.

Following parameters are displayed for R-Series:

- 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 42 cnPilot Home: Device Dashboard > Network Info Page



Following parameter details are displayed in E-Series:

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

- PPPoE

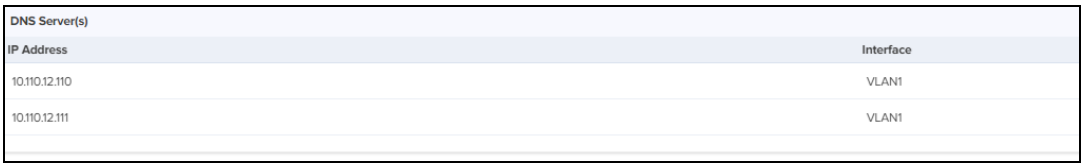
Figure 43 Enterprise Wi-Fi: Device Dashboard > Network Info Page

IPv6 Routes

IPv6 Routes

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

DNS Servers



DNS Server(s)

IP Address	Interface
10.110.12.110	VLAN1
10.110.12.111	VLAN1

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 44 PTP: Device Dashboard > Network Info Page

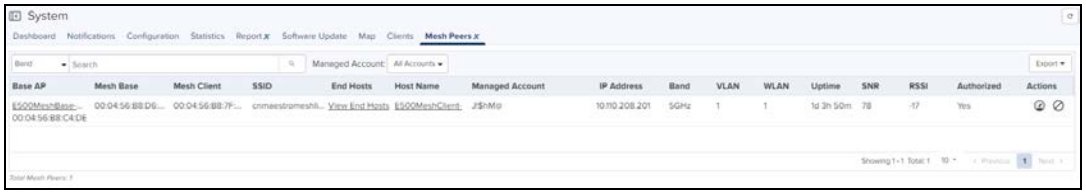
Ethernet Ports

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

Mesh Peers

The **Mesh Peers** tab displays information related to mesh 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 45 Device Dashboard > Mesh Peers Page

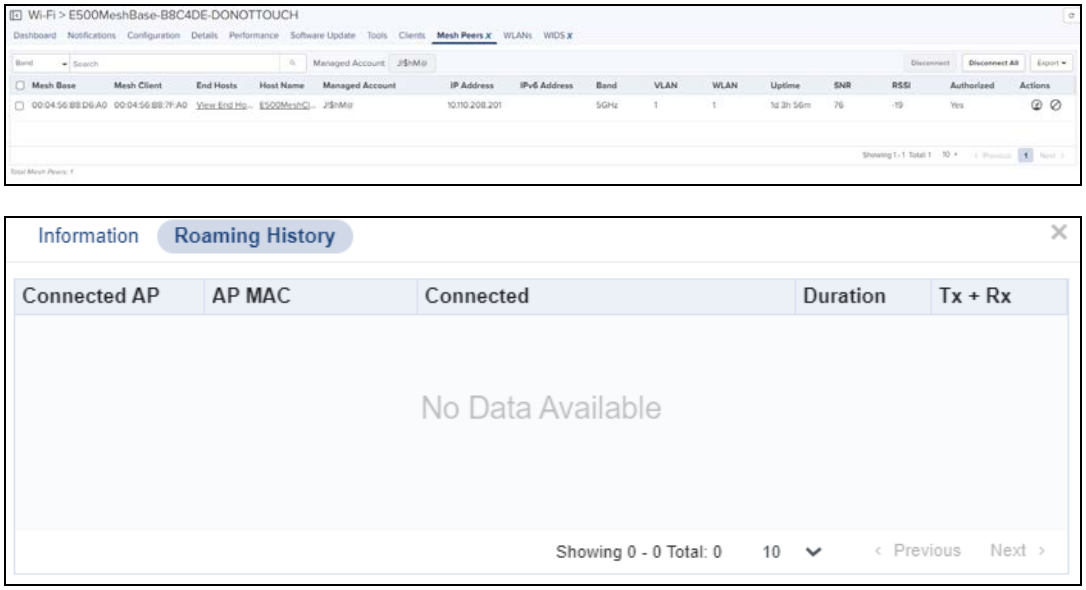


You can also perform the Wi-Fi performance test by clicking the icon in the **Action** field.

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.

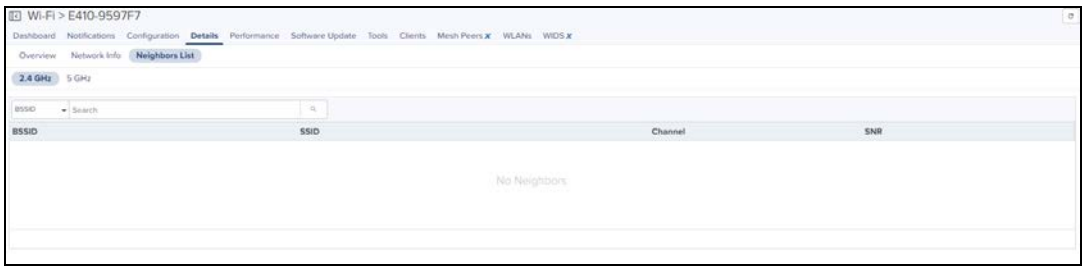
Figure 46 Roaming History for Mesh Peers



Neighbors

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

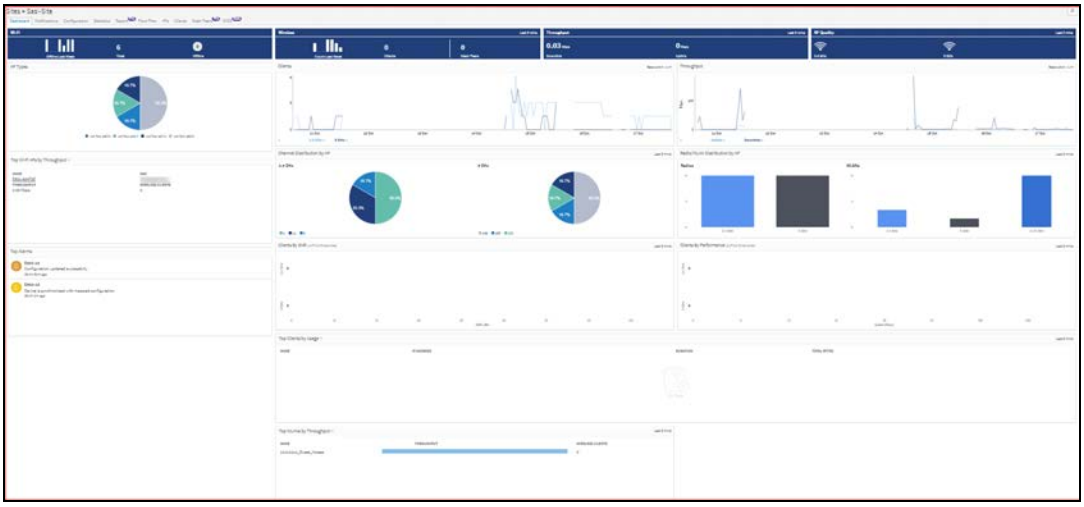
Figure 47 Device Dashboard > Neighbors Page



Site Dashboard

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

Figure 48 Site Dashboard



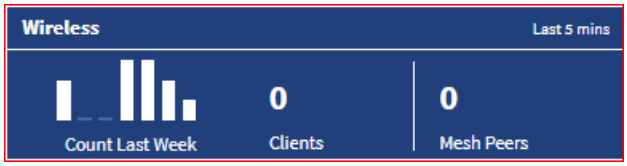
The Site Dashboard displays the following parameters:

- AP Types
- Channel Distribution by Band
- Clients by SNR
- Clients by Performance
- Floor Plan
- RF Quality
- Radio/WLAN Distribution by Band
- 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.

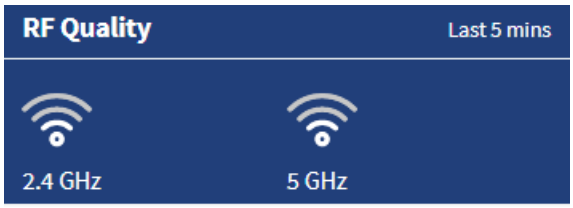
Wireless



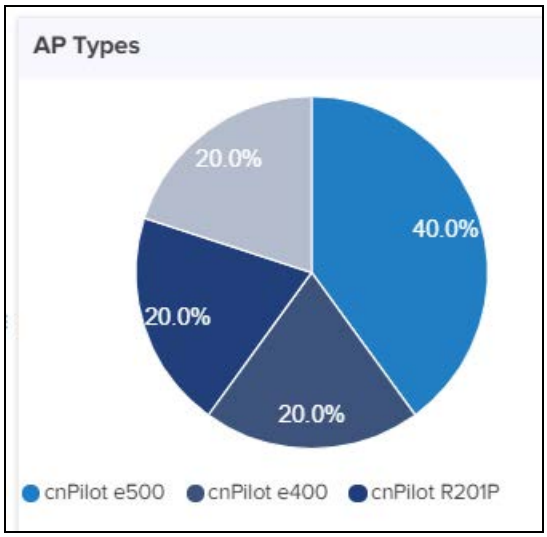
Throughput

Displays aggregated throughput for all the clients.

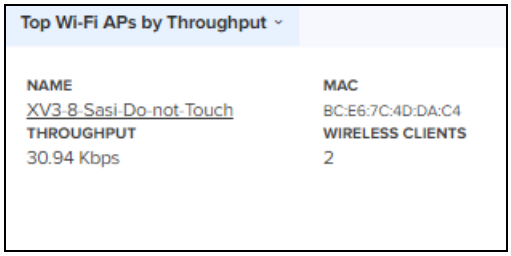
RF Quality



AP Types

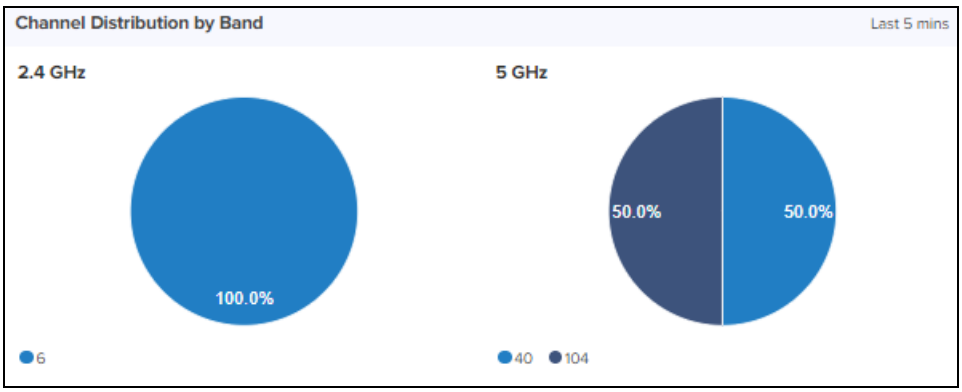


Top Wi-Fi APs

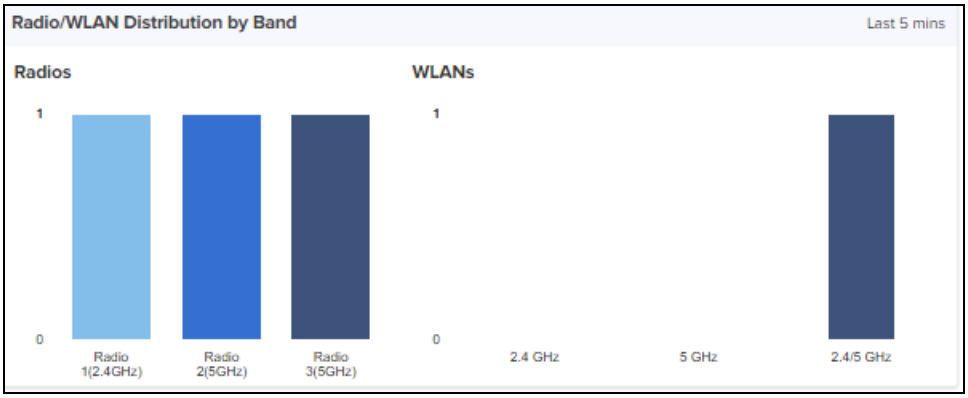


Channel Distribution by Band

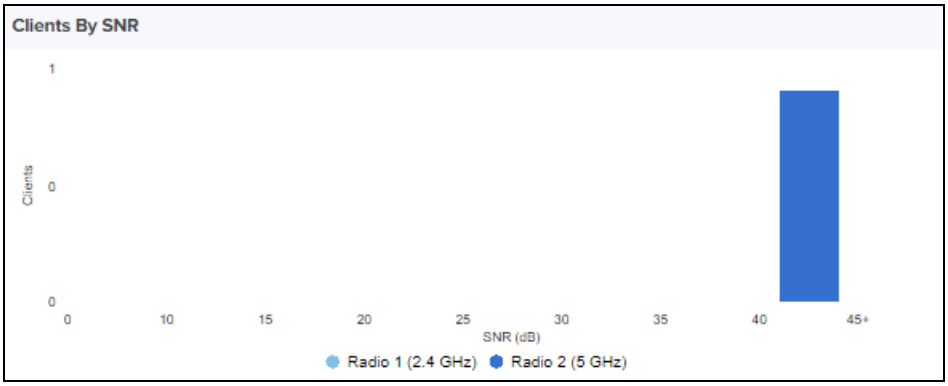
Channel Distribution by AP displays usage of channels in 2.4 GHz and 5 GHz. This helps users in planning and implementing WLANs within a high-density environment.



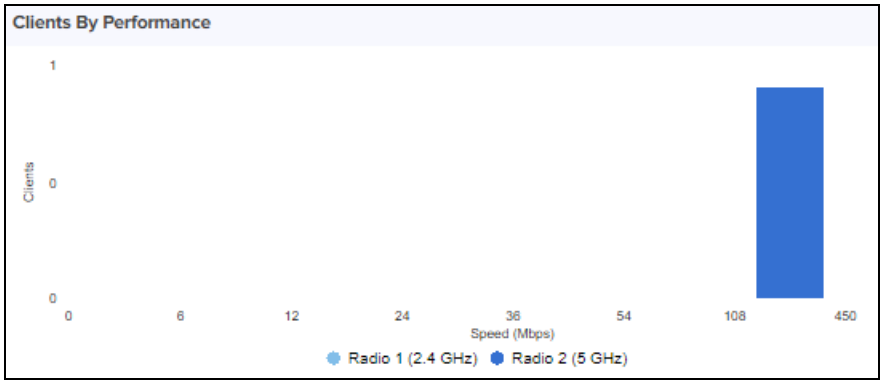
Radio/WLAN Distribution by Band



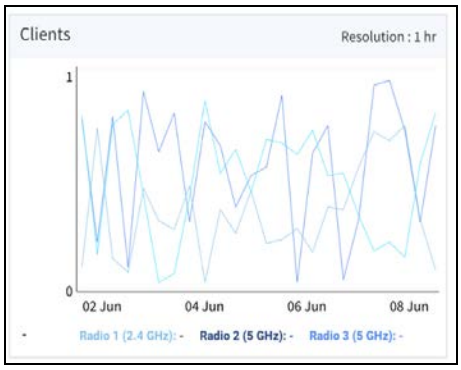
Clients by SNR



Clients by Performance

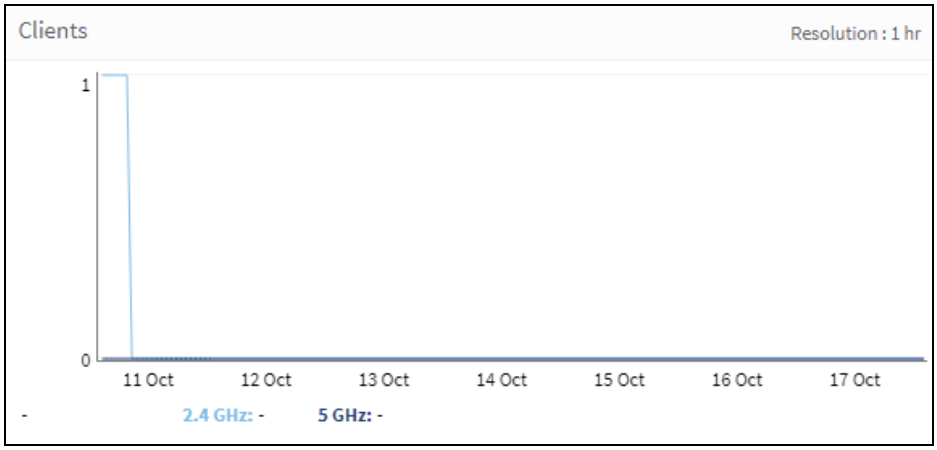


Clients By Performance (For XV3-8)



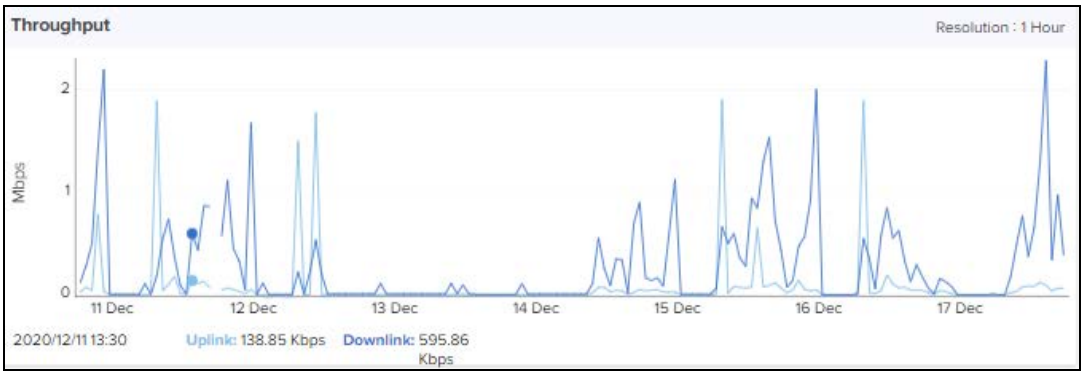
Clients Graph

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.

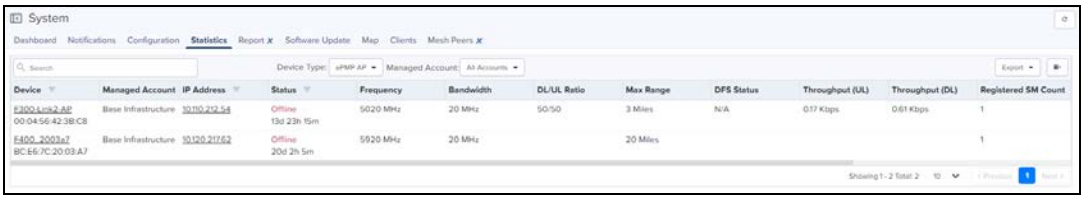


Statistics

Statistics displays following parameters:

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

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



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.

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 & gif
- File size: not more than 5 mb.

Inventory

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 49 Inventory - Access and Backhaul and Industrial Internet View

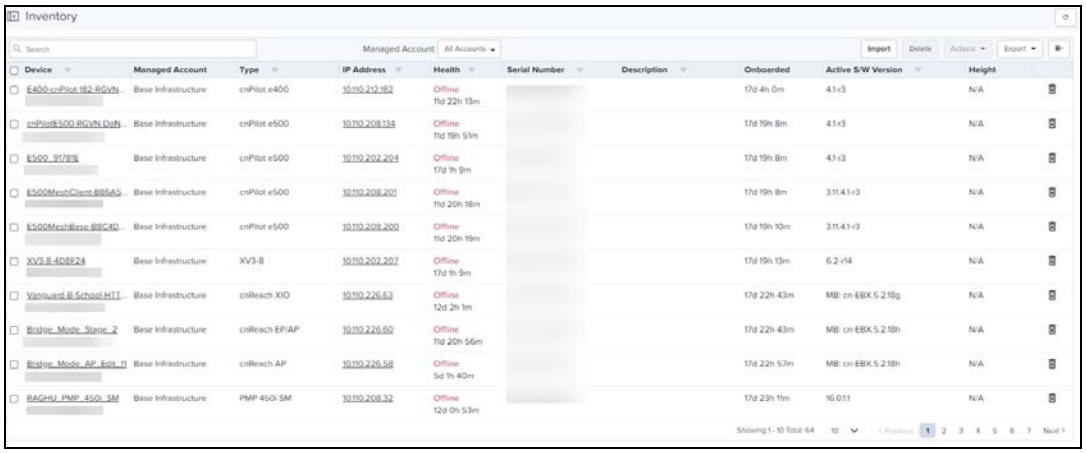
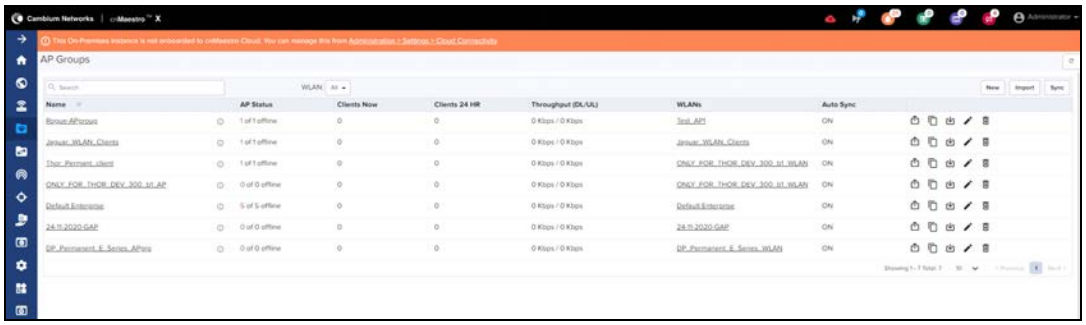


Figure 50 Inventory - Enterprise View



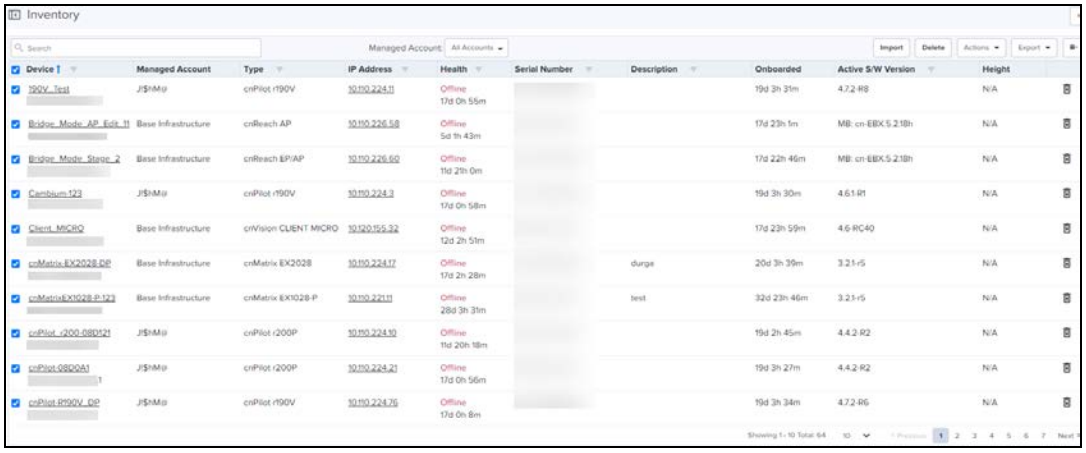
Inventory Export

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 51 Bulk Delete



To delete devices using Bulk Delete:

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.

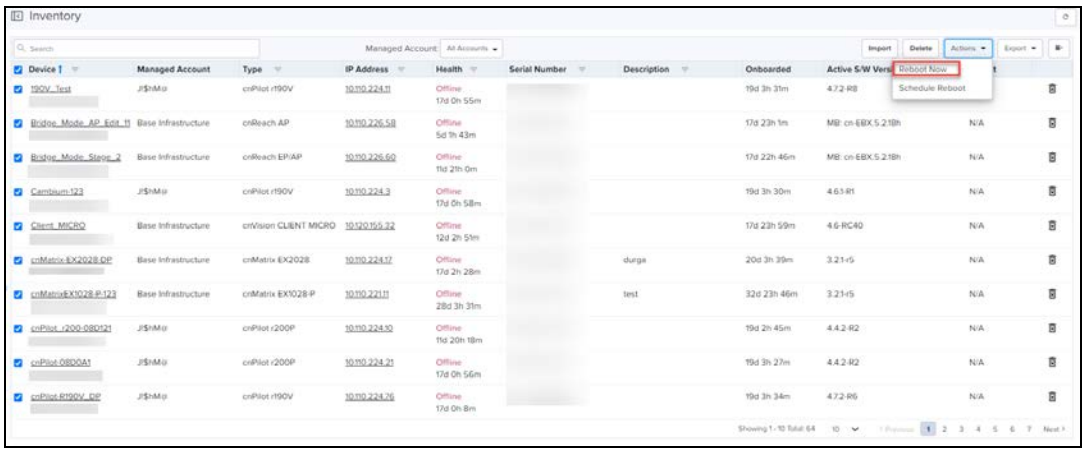
Bulk Reboot

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 52 Bulk Reboot

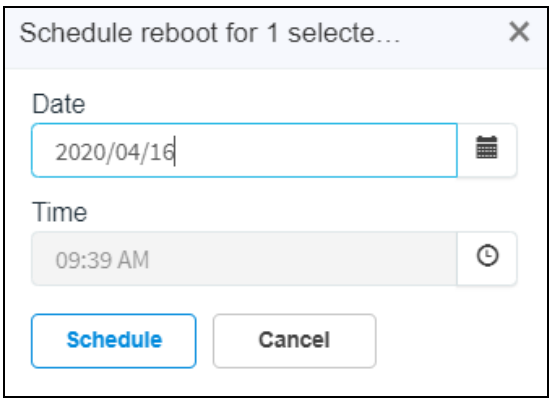


To reboot devices using Bulk Reboot:

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/devices by selecting **Schedule reboot** from **Actions** drop-down list, and by providing the **Date** and **Time**.



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

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.

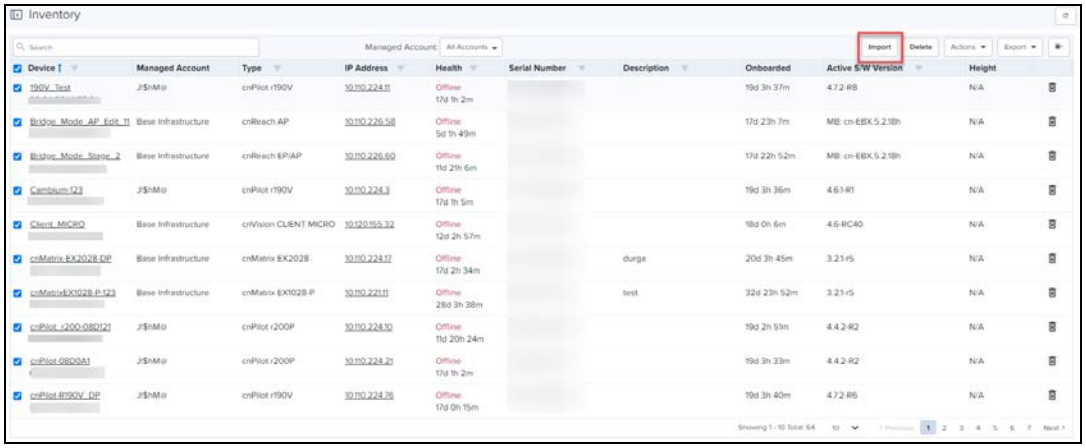
The following parameters are supported for ePMP/PMP AP in the CSV file:

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

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

- Latitude
- Longitude

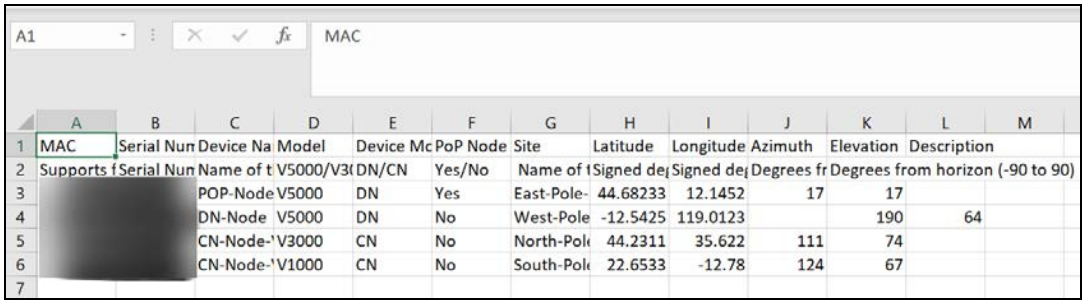
Figure 53 Import Device Configuration



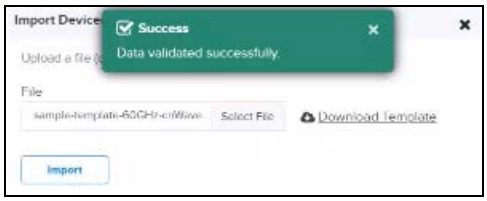
Sample Configuration File

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

Sample Configuration File (60 GHz cnWave)



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

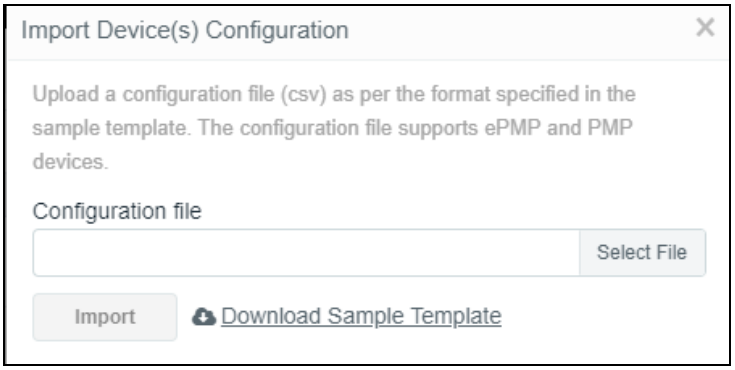
To upload a configuration file (CSV) as per the format specified in the sample template:

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.

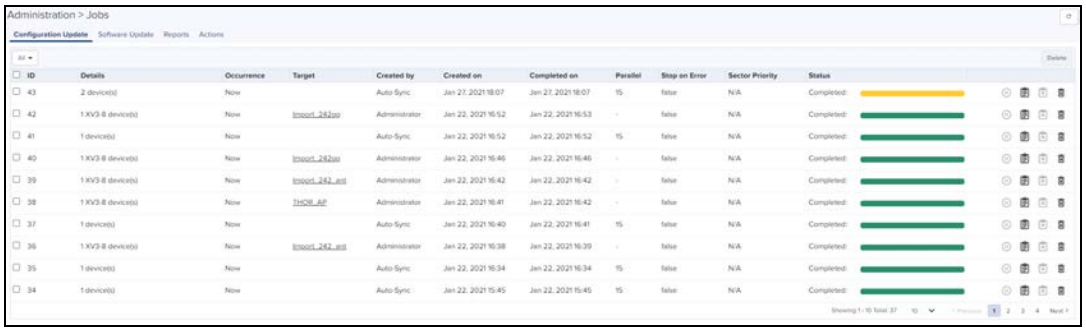
3. Click **Import**.

Figure 54 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.



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

Table 28: CSV Importing Error

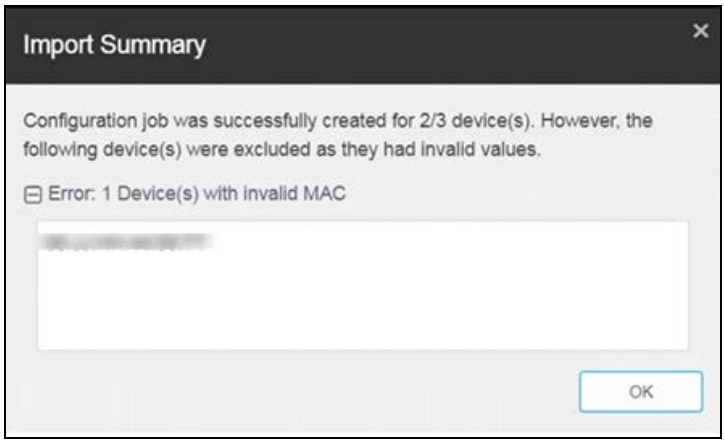
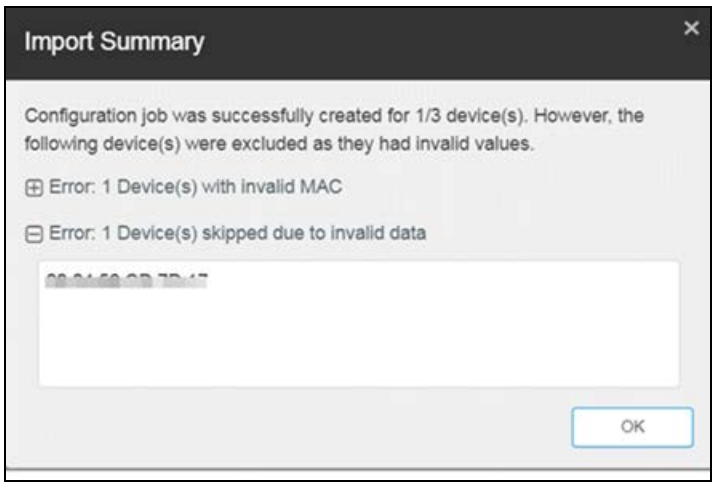
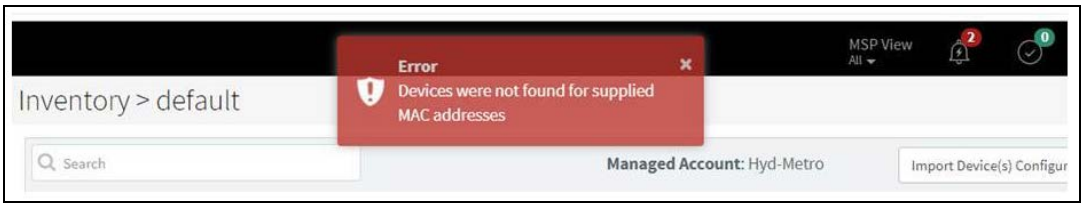
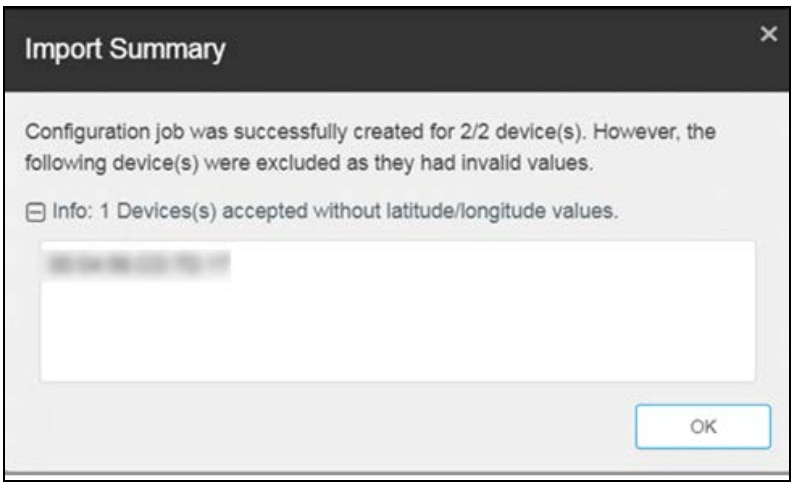
Error	Description
Error1: Error: {Count of Devices} Device (s) with invalid MAC	This error is displayed if the uploaded CSV file contains invalid MAC Address. 
Error2: {Count of Devices} Device (s) skipped due to invalid data	This error is displayed if the uploaded CSV file contains invalid Data or data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

Table 28: CSV Importing Error

Error	Description
	
Error4: Info: 1 Devices(s) accepted without latitude/longitude values	This error is displayed when the latitude and longitude values are tried to push on to ePMP AP or PMP AP which are under a Tower. 

Reports

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

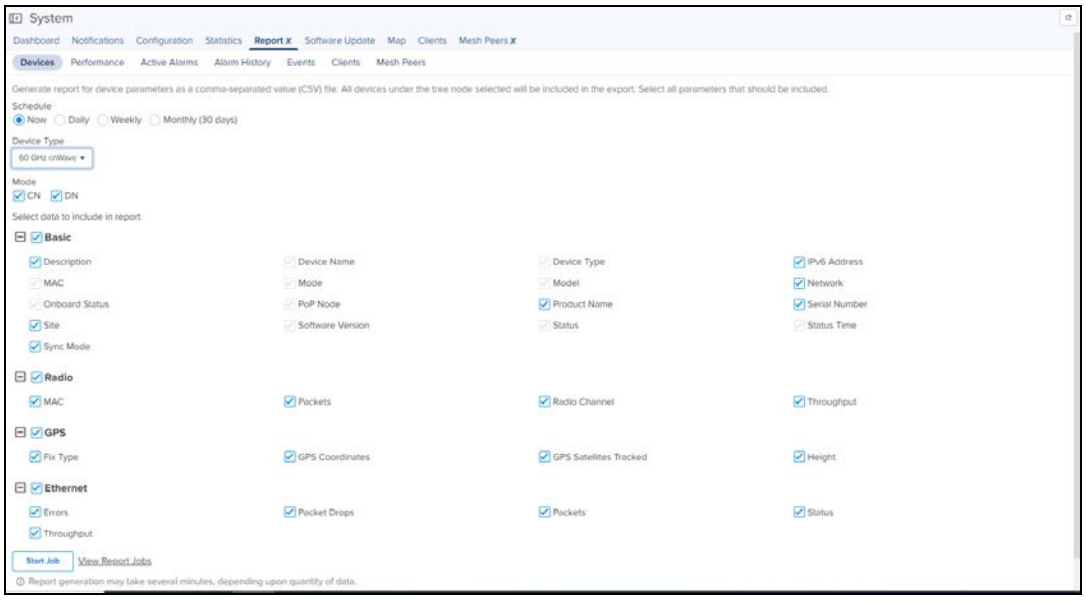
Device Report

To generate device reports:

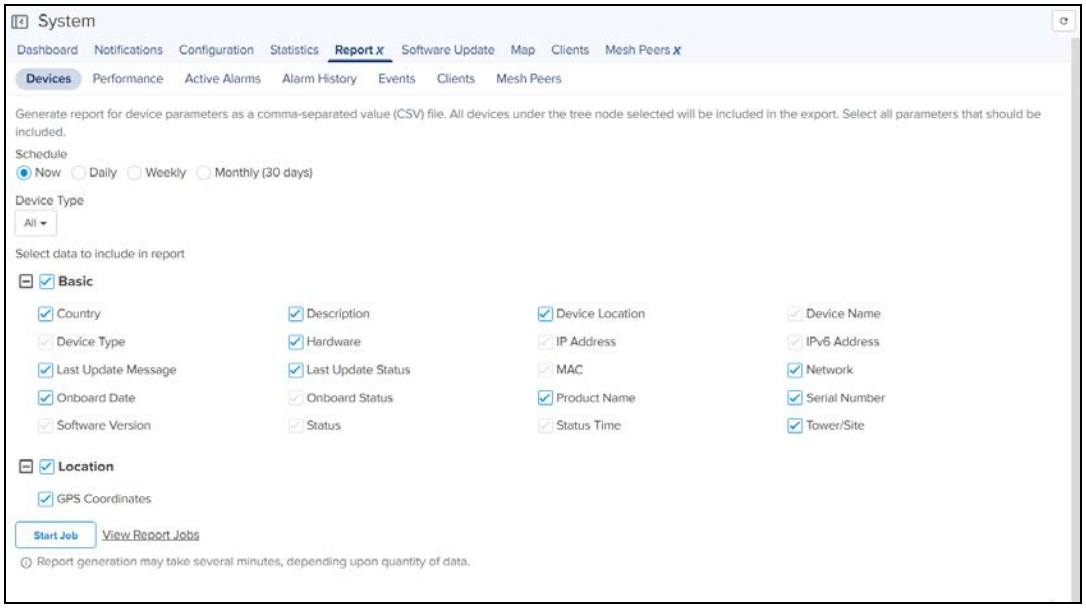
1. Navigate to **Report > Devices** tab.
2. Select the device type for which the user wants to generate the report or select **ALL** for generating the report for All device types.
3. Click **Start Job** or **Schedule** based the Selected **Export (Now, Daily, Weekly, or Monthly).**

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

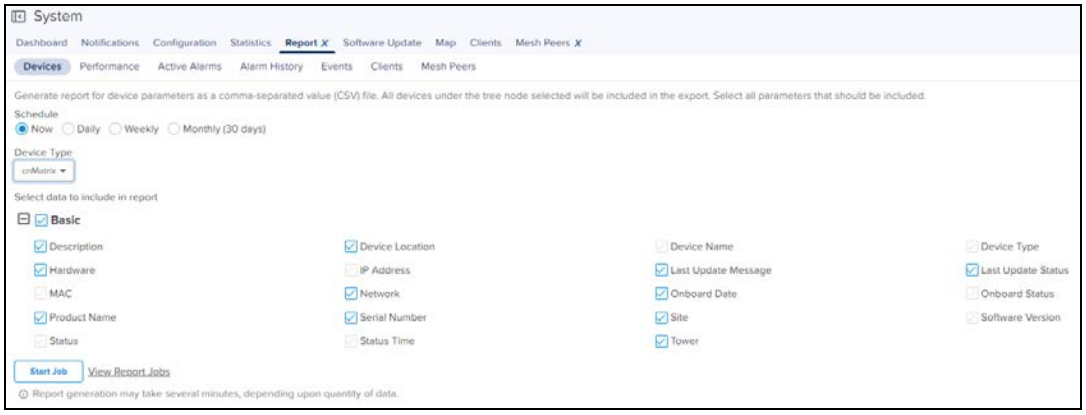
- If 60 GHz cnWave with enabling CN or DN or both is selected as the **Device Type**, then Basic, Radio, GPS, and Ethernet Data of CN or DN will be exported.



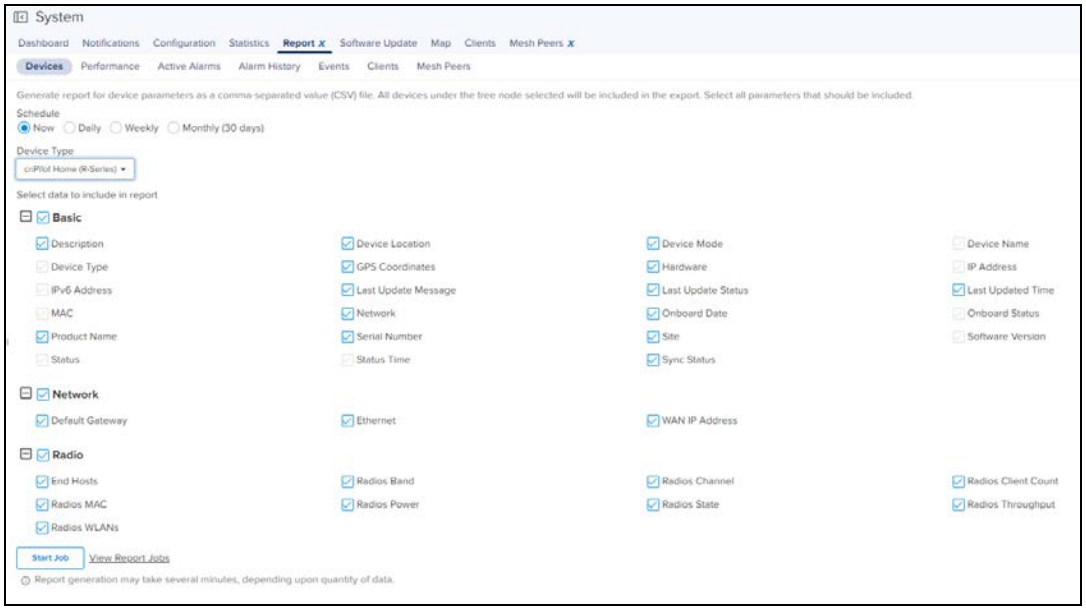
- If **ALL** is selected as the **Device Type**, the Basic Data Export parameters will be exported.



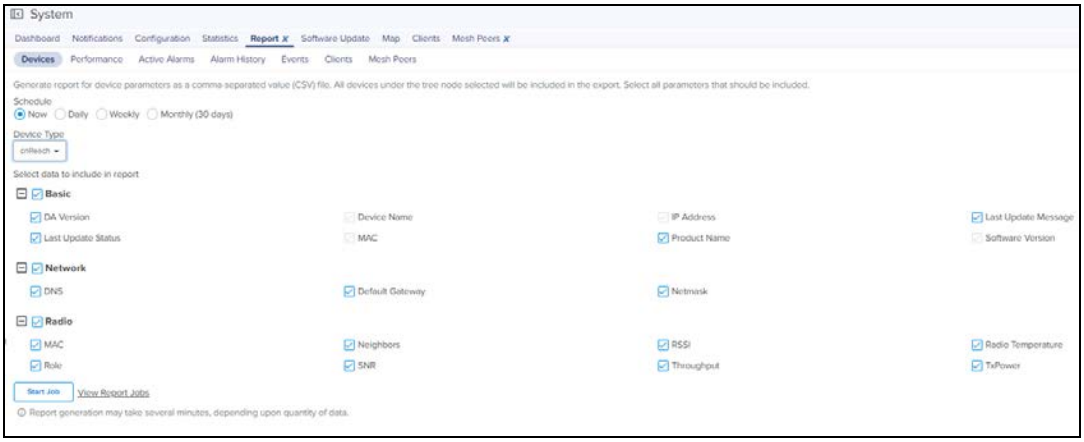
- If cnMatrix is selected as the **Device Type**, then Basic data will be exported.



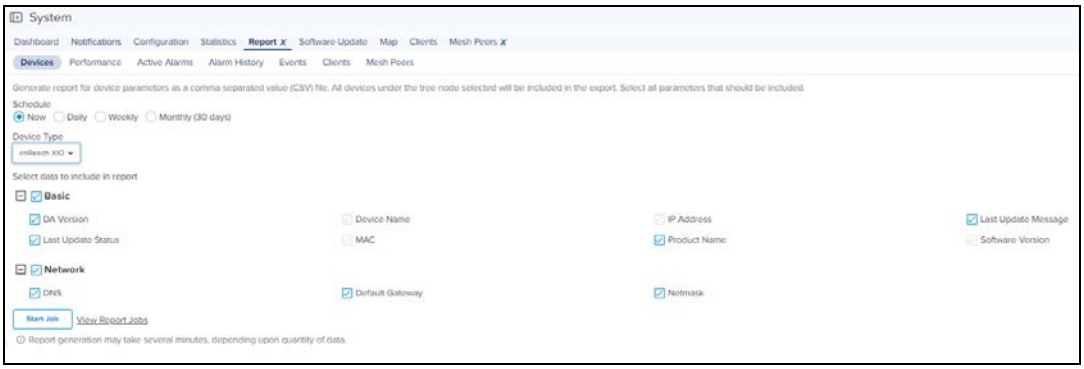
- If cnPilot Home (R-Series) is selected as the **Device Type**, then Basic, Network and Radio Data will be exported.



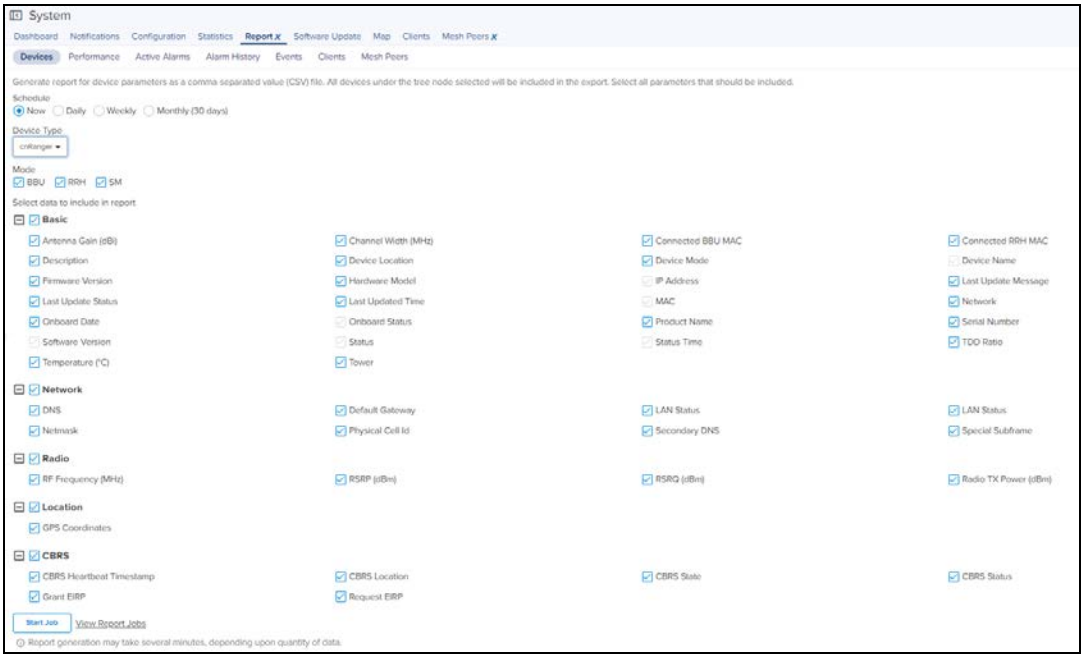
- If cnReach is selected as the **Device Type**, then Basic, Radio and Network Data will be exported.



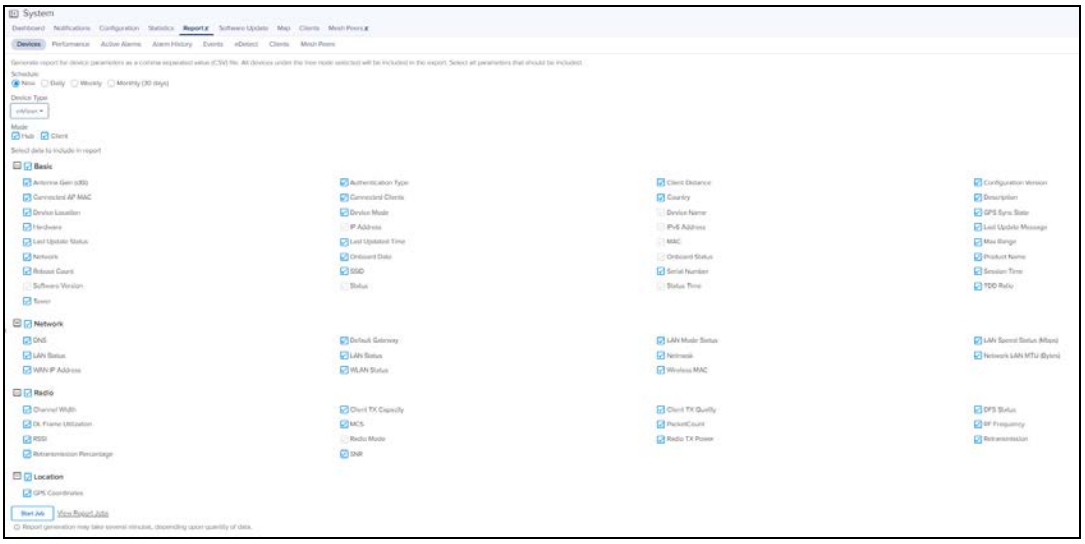
- If cnReach XIO is selected as the **Device Type**, then Basic, Radio and Network Data will be exported.



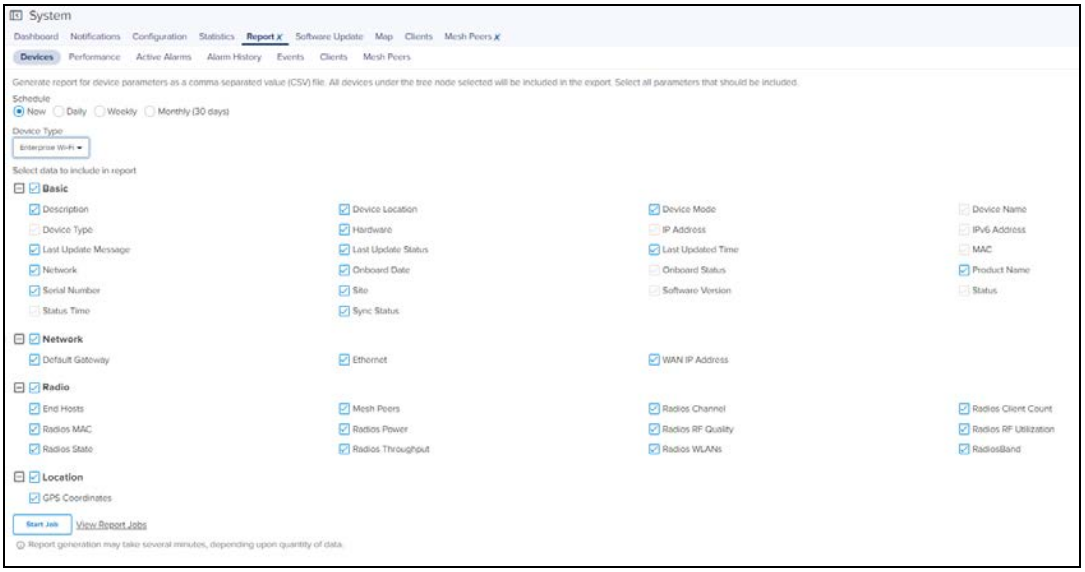
- If cnRanger is selected as the **Device Type**, then Basic, Radio, Location, CBRS, and Network Data will be exported.



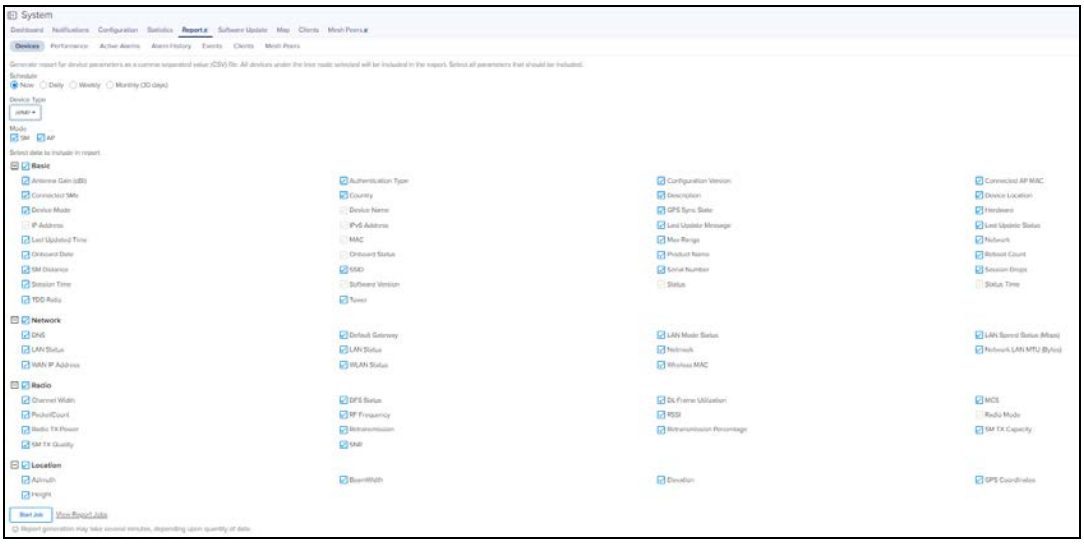
- If cnVision is selected as the **Device Type**, then Basic, Network, Location and Radio Data will be exported.



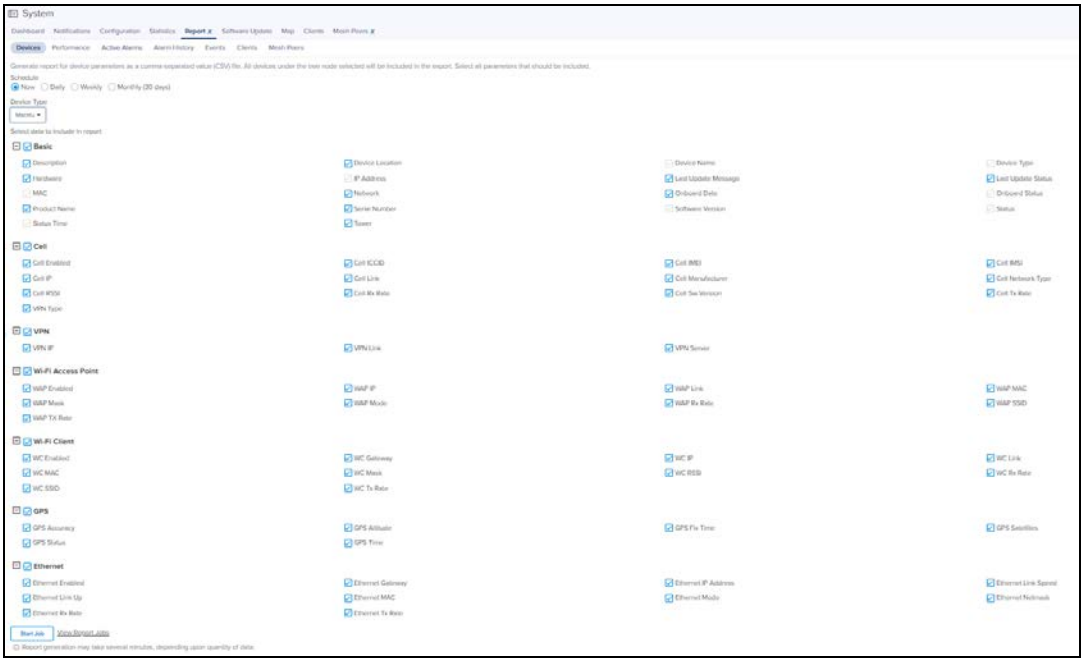
- If Enterprise Wi-Fi is selected as the **Device Type**, then Basic, Network, Location, and Radio Data will be exported.



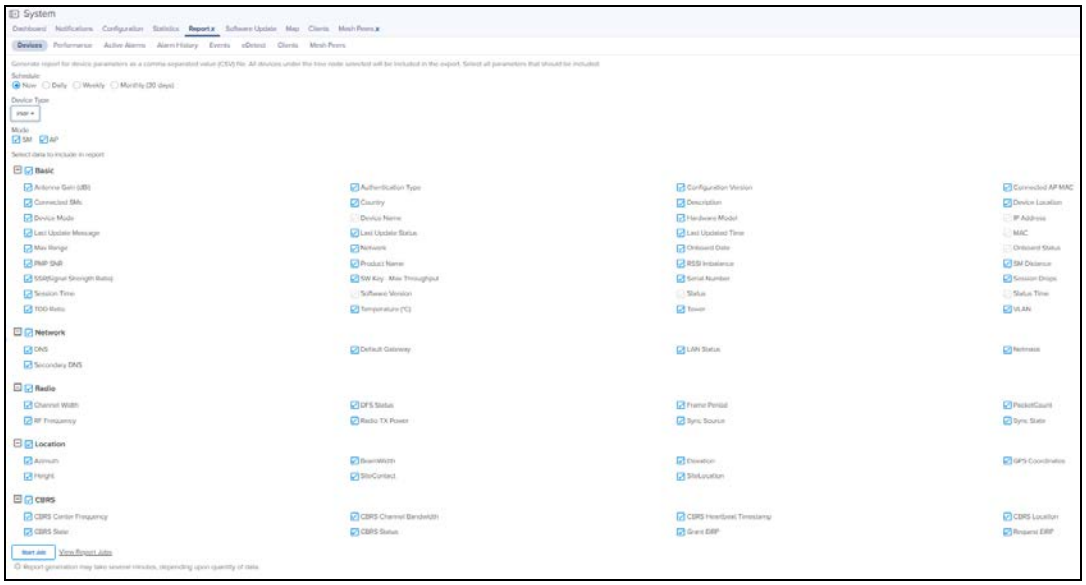
- If ePMP is selected as the **Device Type**, then Basic, Network, Location and Radio data will be exported. User can select to generate the report for either AP or SM or both. Based on the AP or SM selection, the data related to AP or SM will be exported.



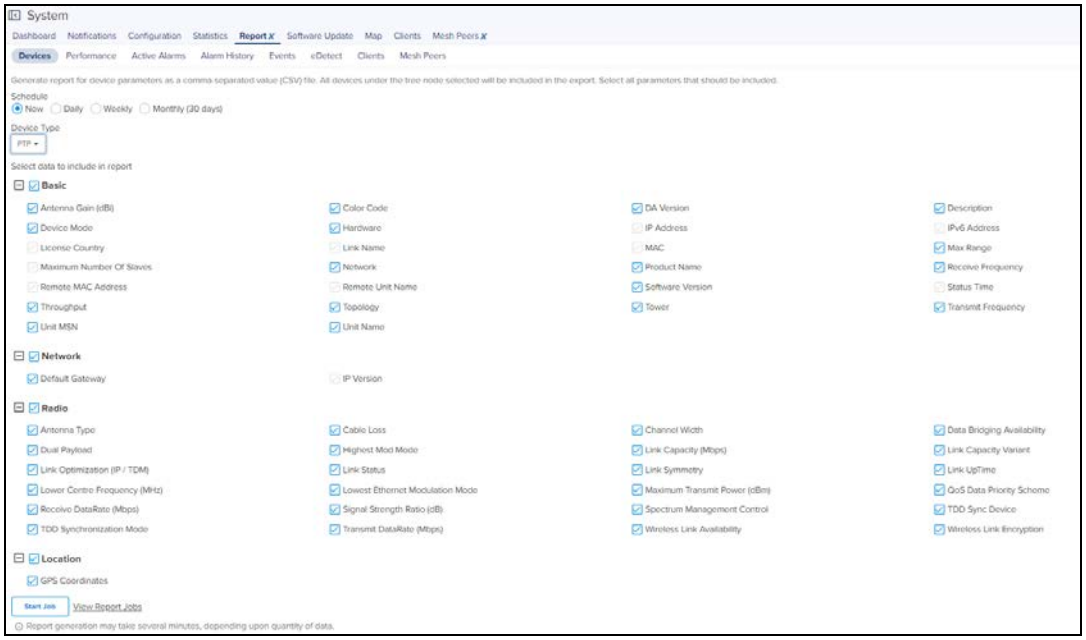
- If Machfu is selected as the Device Type, then Basic, Cell, VPN, Wi-fi Access Point, Wi-Fi Client, GPS and Ethernet data will be exported.



- 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.



	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 Interval** based on which the report can be generated for Last Day or Last Week or custom Interval.
3. Select **Interval** to report at either 5 Minutes or 1 Hour or 1 Day.
4. Select **Device Type.**
5. Click **Start Job** or **Schedule** based the selected **Export (Now, 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 55 60 GHz cnWave Performance Report (Node Type)

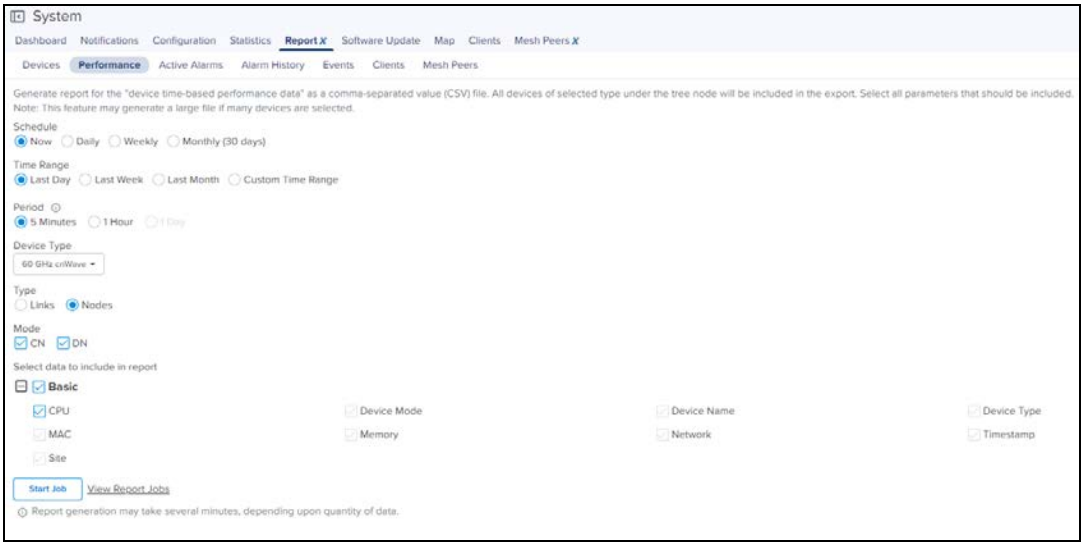
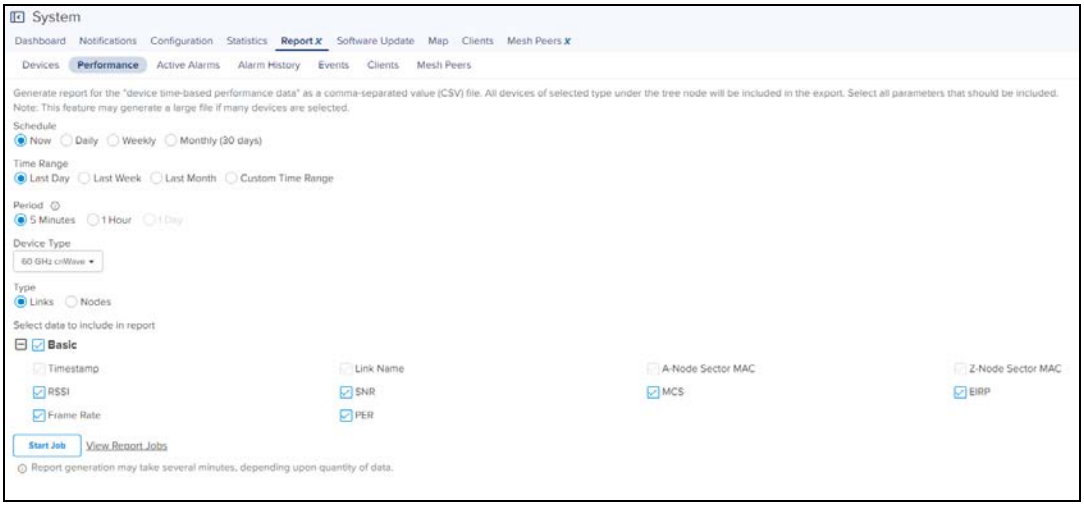
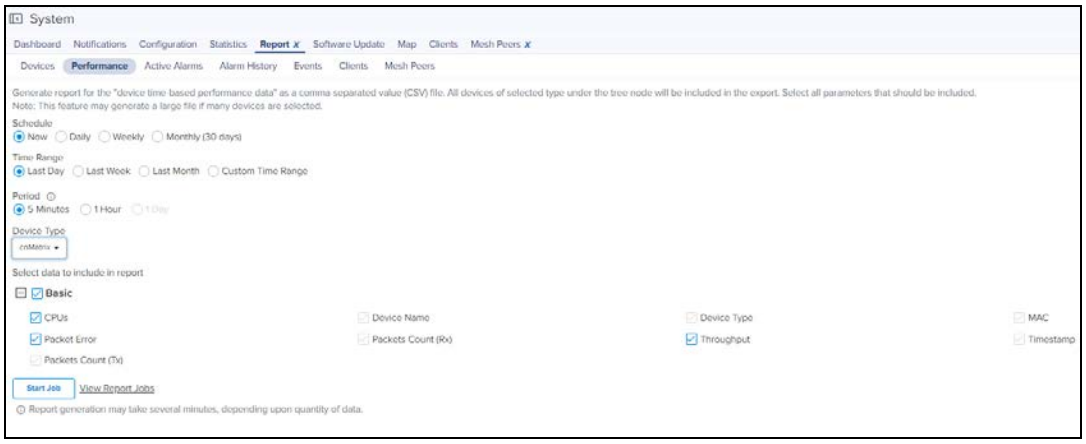


Figure 56 60 GHz cnWave Performance Report (Links Type)



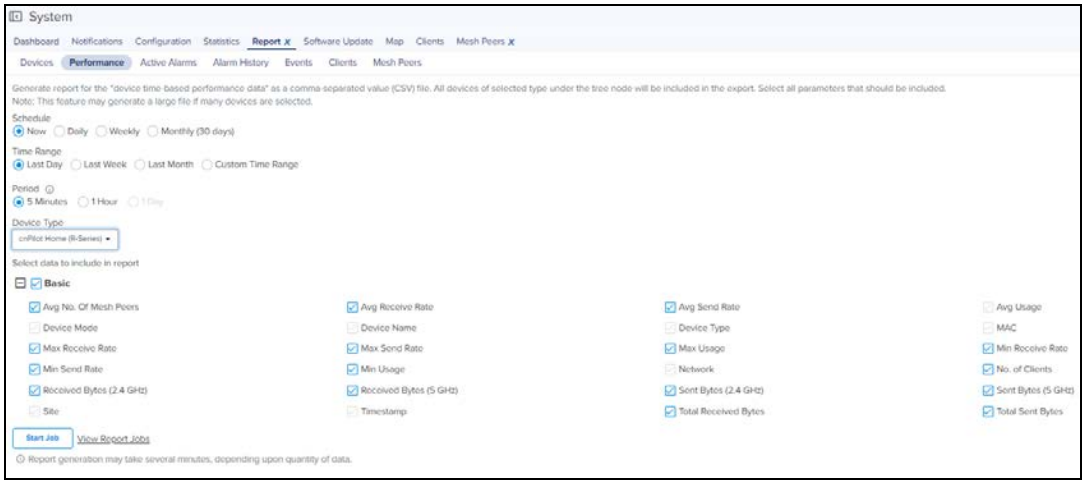
cnMatrix Performance Report

Figure 57 cnMatrix Performance Report



cnPilot Home (R-Series) Performance Report

Figure 58 cnPilot Home (R-Series) Performance Report

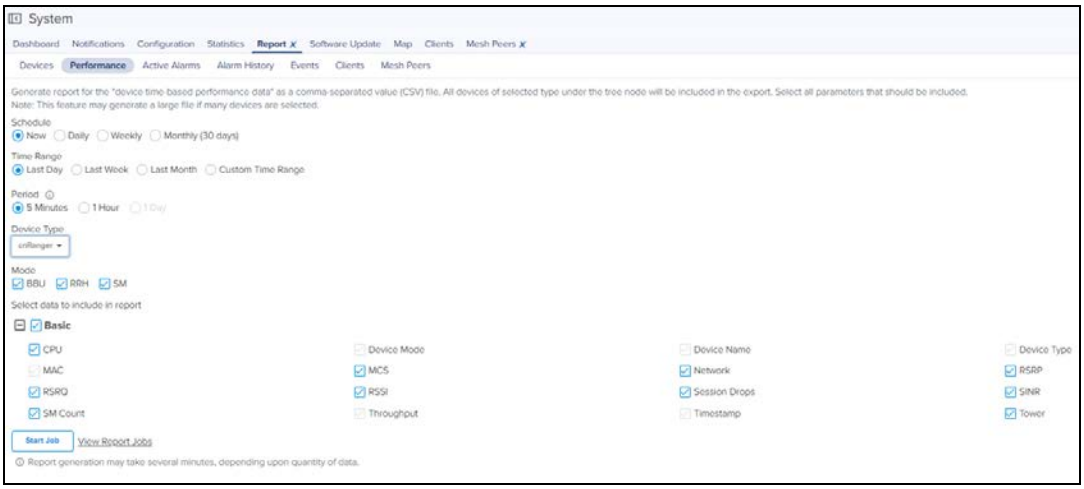


cnReach Performance Report

Figure 59 cnReach Performance Report

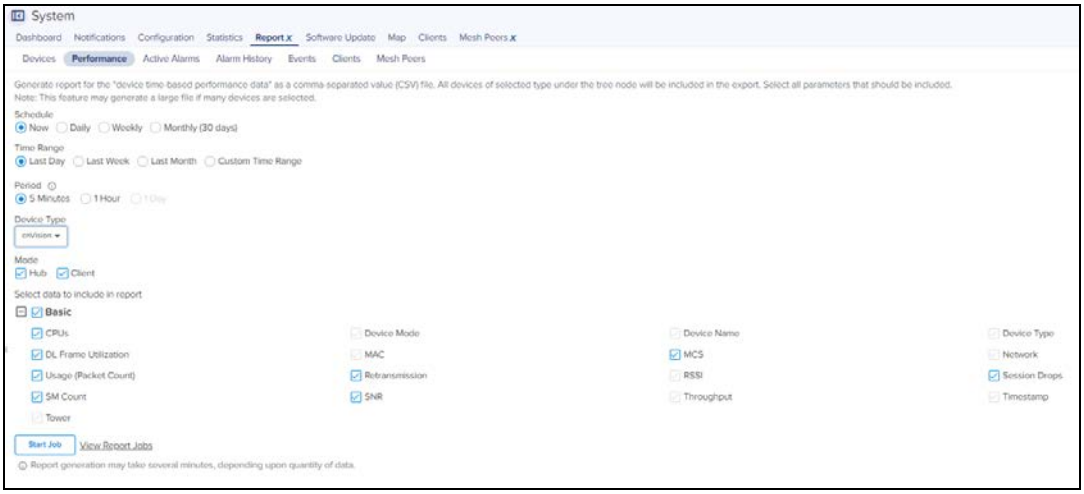
cnRanger Performance Report

Figure 60 cnRanger Performance Report



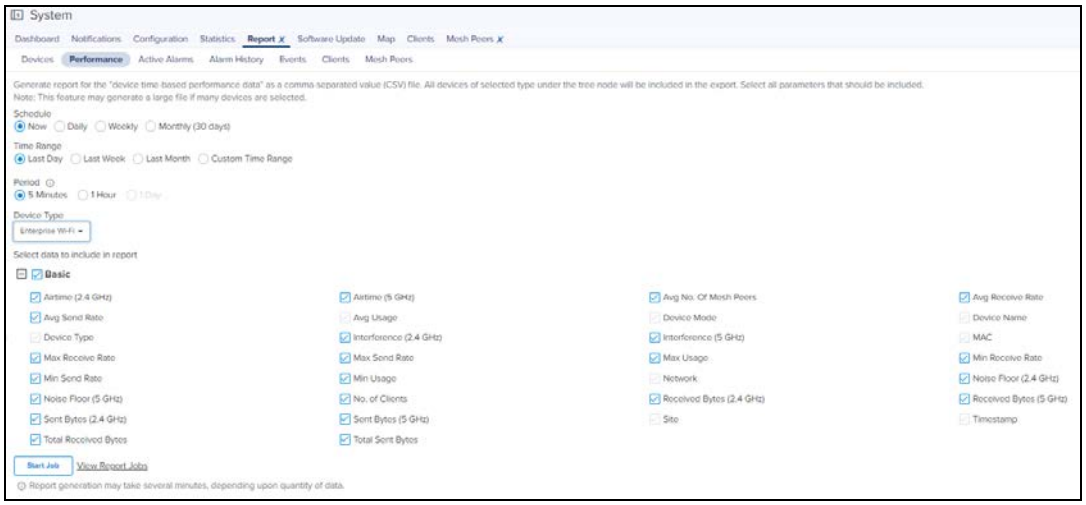
cnVision Performance Report

Figure 61 cnVision Performance Report



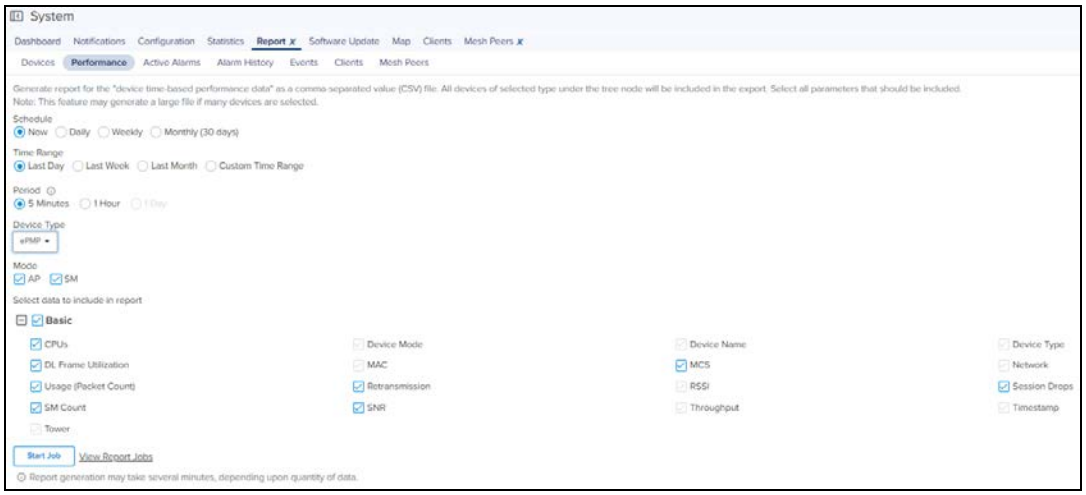
Enterprise Wi-Fi Performance Report

Figure 62 Enterprise Performance Report



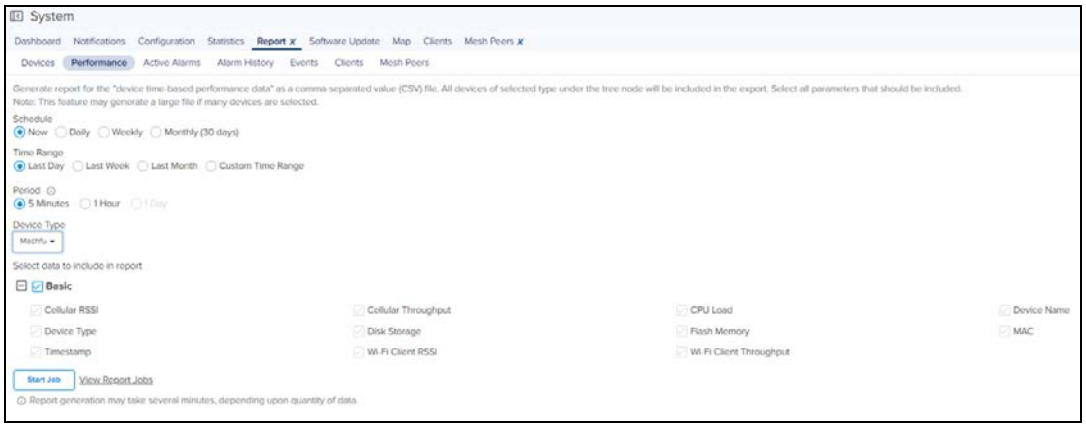
ePMP Performance Report

Figure 63 ePMP Performance Report



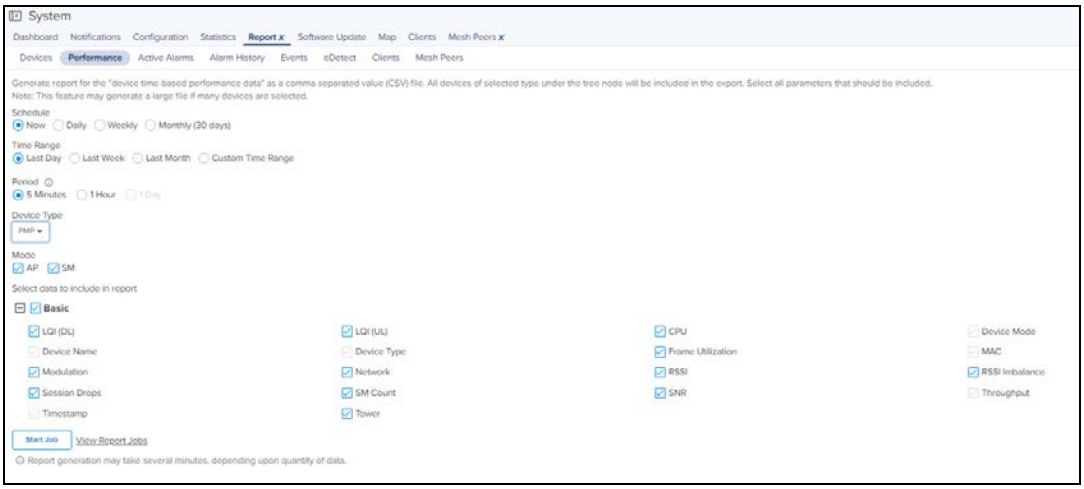
Machfu Performance Report

Figure 64 Machfu Performance Report



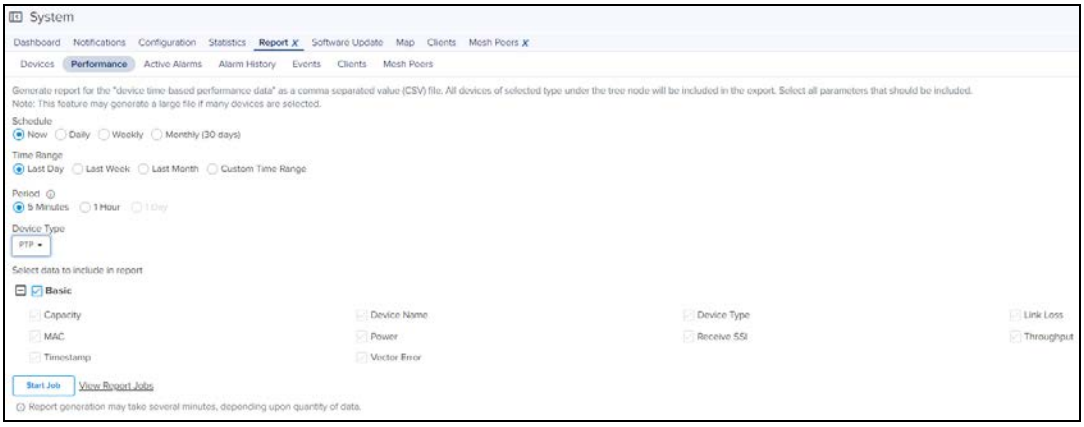
PMP Performance Report

Figure 65 PMP Performance Report



PTP Performance Report

Figure 66 PTP Performance Report

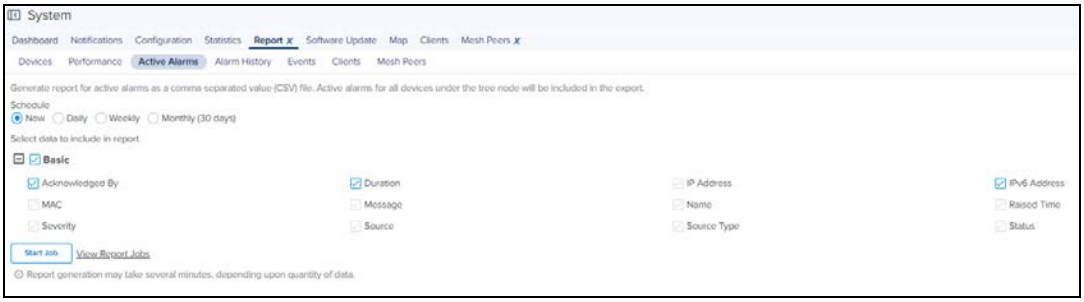


Active Alarms Report

To generate the Active Alarms reports, navigate to **Report > Active Alarms** and select the **Data Export** tab.

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

Figure 67 Active Alarms Report

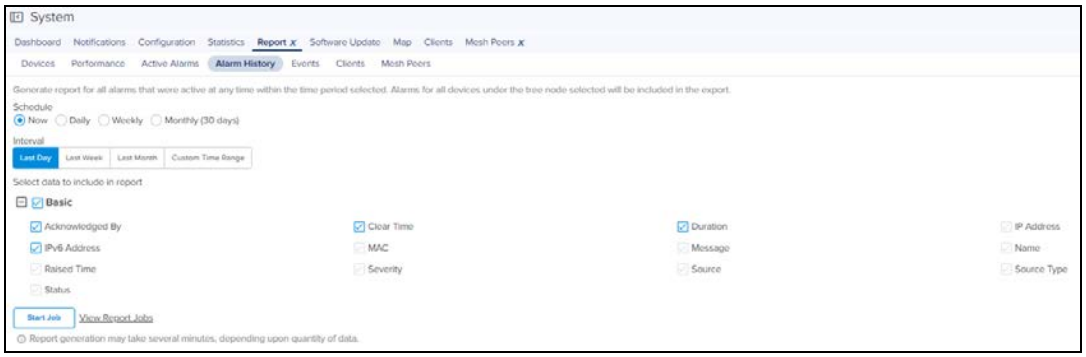


Alarms History Report

To generate the Active Alarms reports, navigate to **Report > Alarm History** and select the **Data Export** 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 68 Alarms History Report

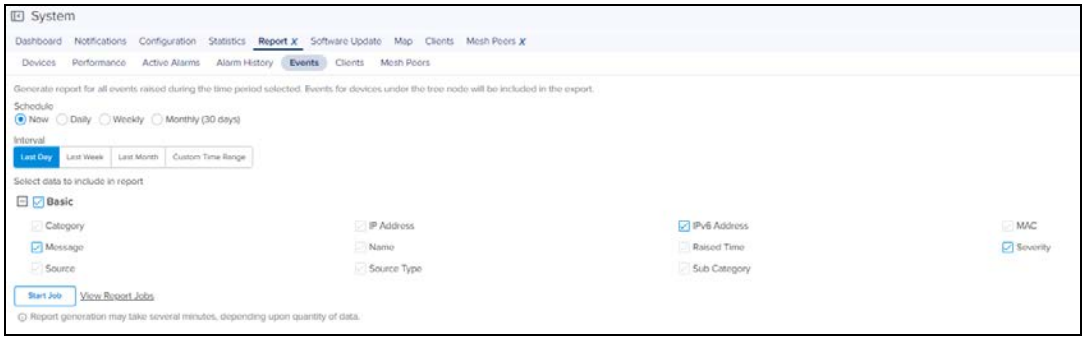


Events Report

To generate the Events reports:

1. Navigate to **Report > Events** tab and select the **Data Export** tab.
2. Select the **Time Interval** based on which the report can be generated **Last Day** or **Last Week** or **Custom Interval** and Reporting Interval of either 5 Minutes or 60 Minutes.
3. Click **Start Job** or **Schedule** based the Selected **Export (Now, Daily** or **Weekly).**

Figure 69 Events Report



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

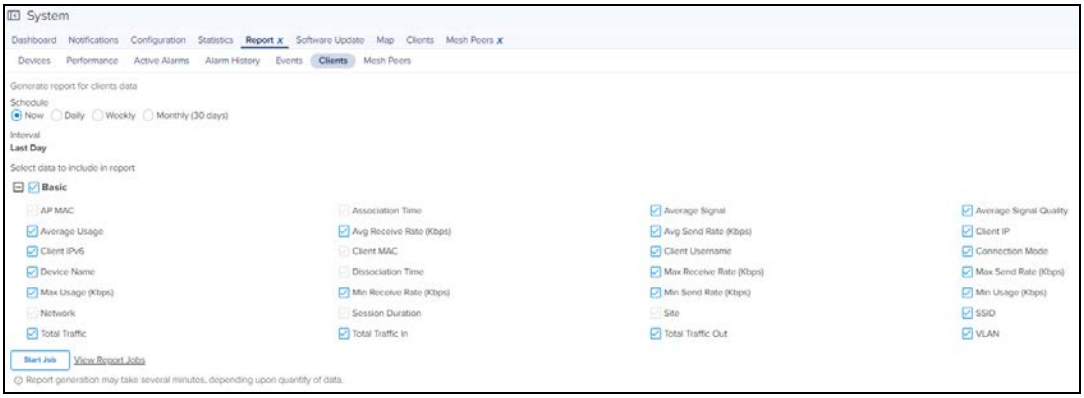
Clients Report

> **NOTE:**
>
> Clients Data is available for Last day or last 24 Hrs only.

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

1. Navigate to **Report > Clients** tab and select the **Data Export** tab.
2. Select the **Time Interval** based on which the report can be generated **Now, Daily** or **Weekly**.
3. Click **Start Job** or **Schedule** based the selected **Export (Now, Daily, Weekly,** or **Monthly).**

Figure 70 Clients Report



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

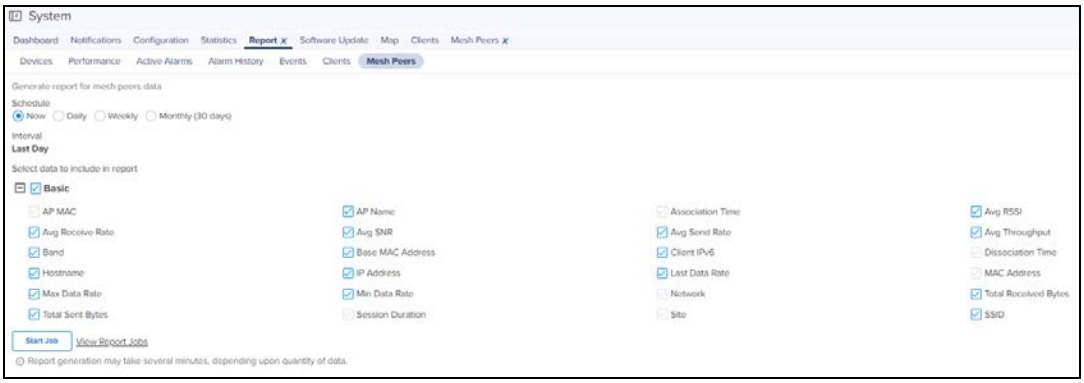
Mesh Peers Report

> **NOTE:**
>
> Mesh Peers is available for Last day or last 24 Hrs only.

To generate the Mesh Peers report:

1. Navigate to **Administration > Settings page** and enable **Detailed Mesh Statistics** check box under **Advanced Features**. The **Mesh Peers** tab appears in **Reports** page.
2. Select the **Data Export** tab under **Mesh Peers** tab.
3. Click **Start Job** or **Schedule** based the Selected **Export (Now, Daily, Weekly,** or **Monthly).** The Mesh Report for the last 24 hours will be generated.

Figure 71 Mesh Peers Report



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.

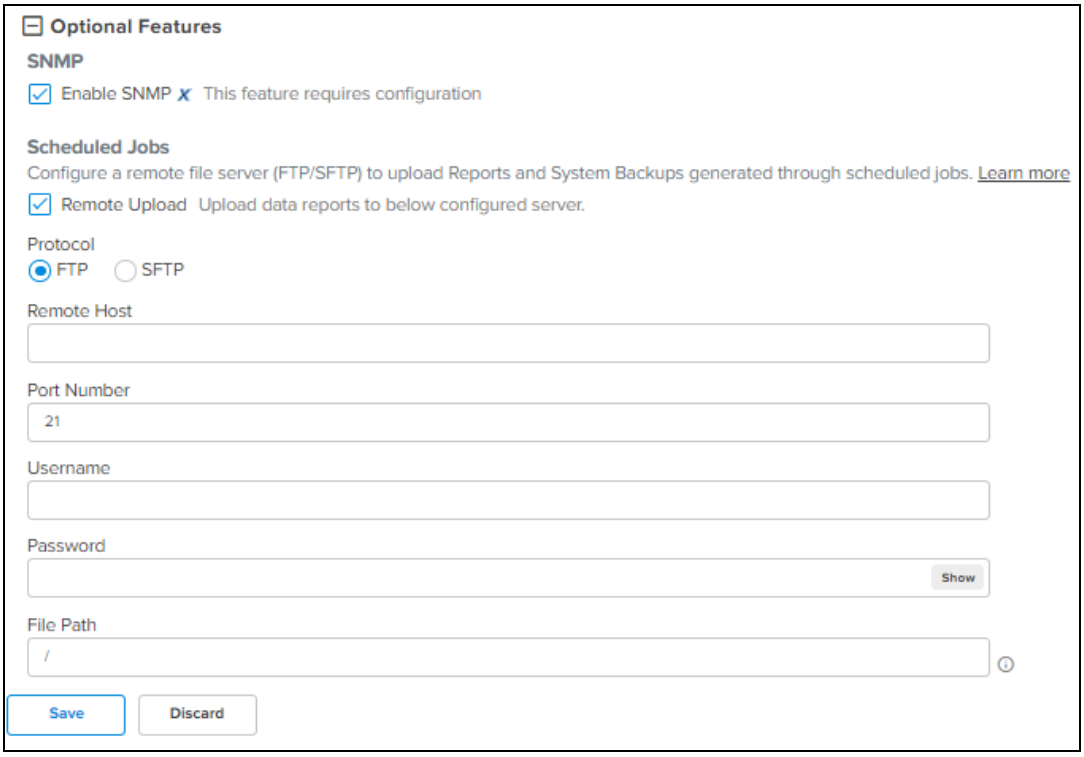
Remote Upload

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**.

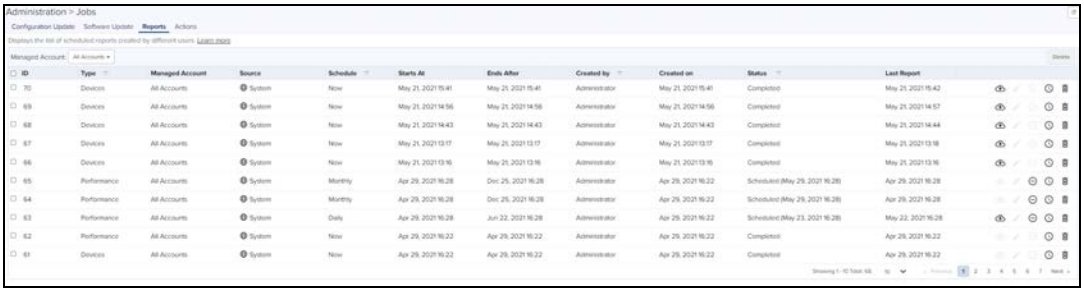
Figure 72 Scheduling Reports



Report Jobs

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

Figure 73 Report Jobs



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

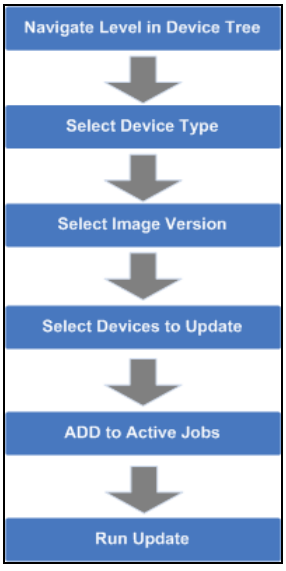
The **Software Update** tab displays the device update details for cnMaestro On-Premises. This section includes the following:

- 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 74 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.

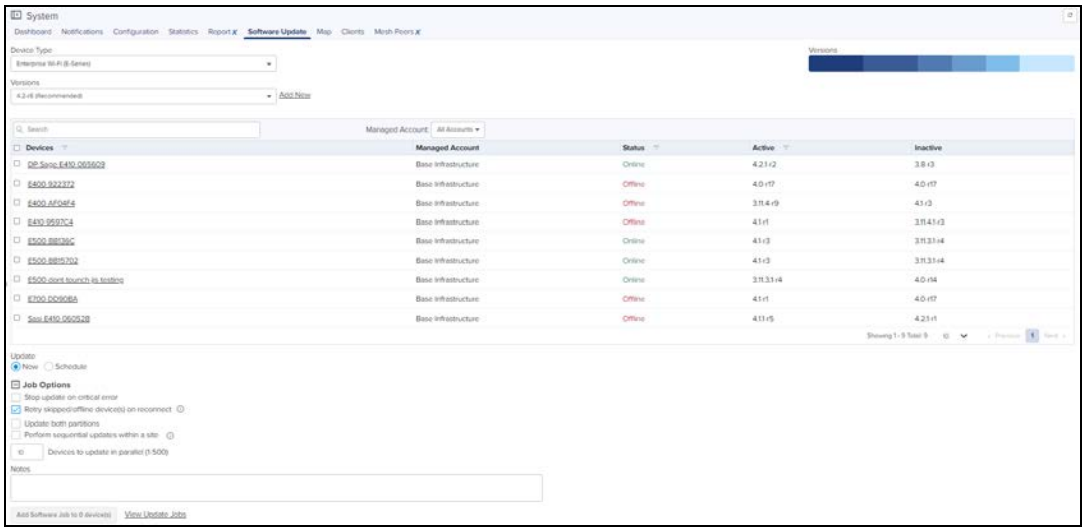
Device Type

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 75 Software Update Dashboard Enterprise Wi-Fi (E-Series)



NOTE:

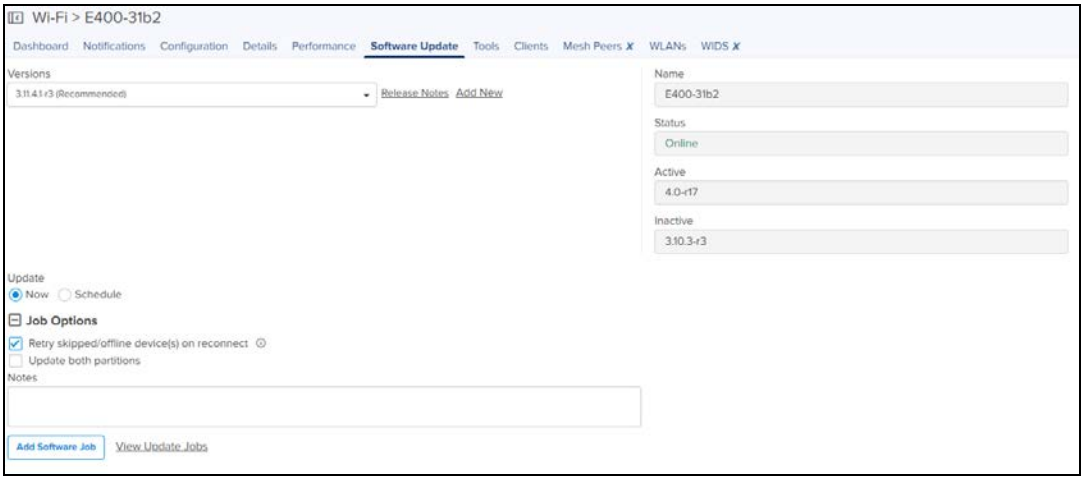
Update both partition option is available at System/Managed Account/Network/Site/Device levels.

Perform sequential updates with in 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:

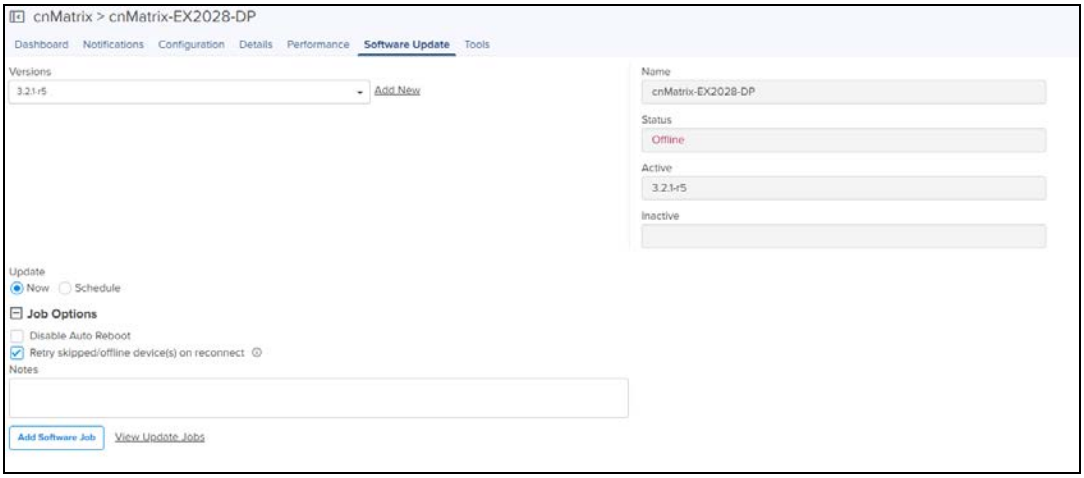
- **Enable:** The selected target image will be upgraded in both active and inactive portions of device.
- **Disable:** The selected target image will be upgraded in only active portion of device.

Figure 76 Software Update Dashboard Device level



If **perform sequential updates with in 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 device.

Figure 77 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 78 Software Update Dashboard (cnRanger)

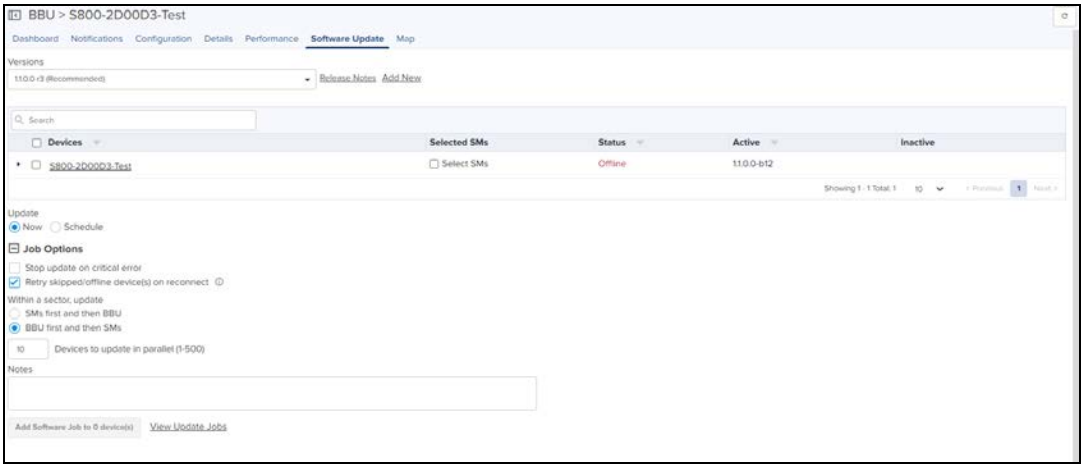
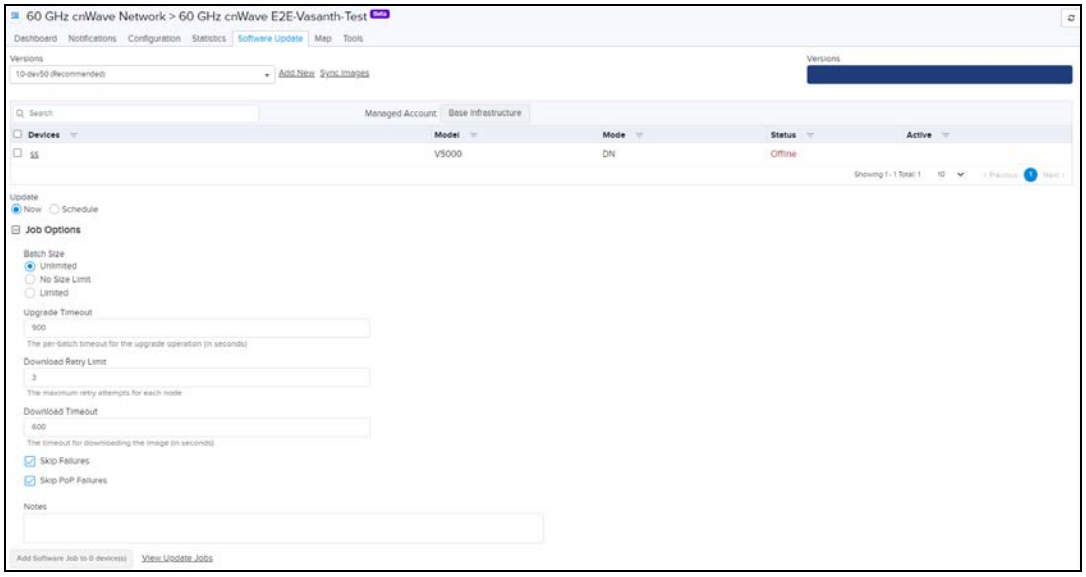


Figure 79 Software Update Dashboard (60 GHz cnWave)



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 80 Scheduling Software Update Job

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

Software Update

The software version on the devices can be auto/manually 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 > Jobs > Software Update >Manual/Auto** page.
2. Select the **Manual/ Auto** page for updating the device software feature.
3. Choose the software version depending on the device type.
4. Click **Start**.

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

Figure 81 Manual Update Page

> **NOTE**
>
> Manual update can be aborted at any point of time by clicking **Abort**.

Figure 82 Auto Update Page

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

You need to download the newly released image from the Support Site. Refer Syslog for more details.

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, we cannot do the manual software update.

The following parameters are visible (though some are only available for certain device types).

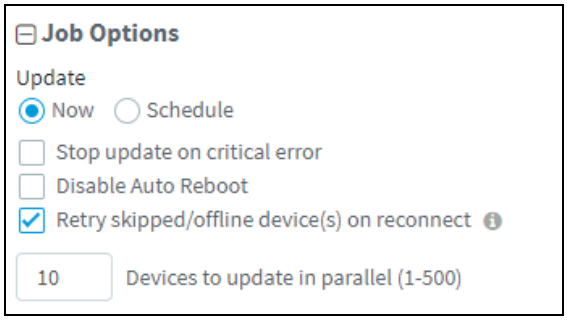
Table 29: Parameters Displayed in Device Table

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



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.

NOTE:
The device which undergoes **Retry Software Update**, does not create a new Job.

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 30: 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

NOTE:

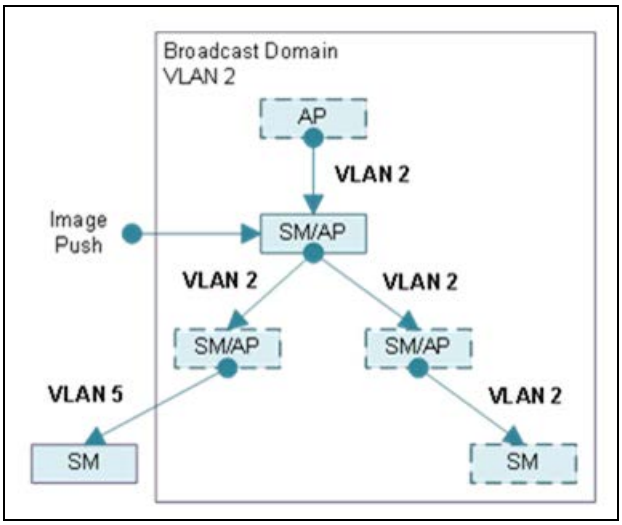
1. Devices which are already completed display as **Completed** with a message update complete along with the status as **Completed**.
2. Devices which are ongoing display as **Aborted** with a message **Manually Aborted** with the status as **Aborted**.
3. Devices which have not yet started display 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.



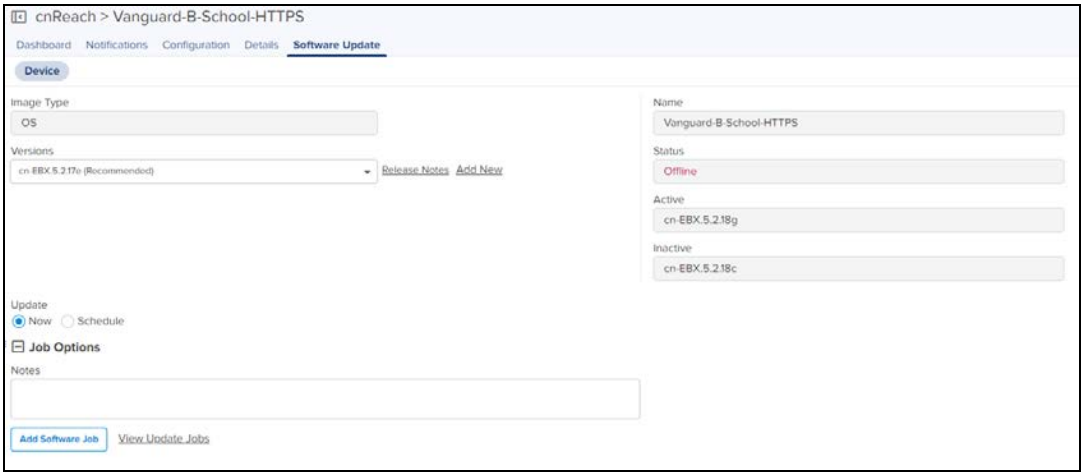
The **Bulk Software Upgrade** is optional, and meant to be used for efficiency. One can still use the standard Software Update mechanism to transfer images to cnReach devices one-at-a-time, though the distribution could be many hours or days.

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 started, the distribution continues until stopped, so be sure to manually stop the process when complete.

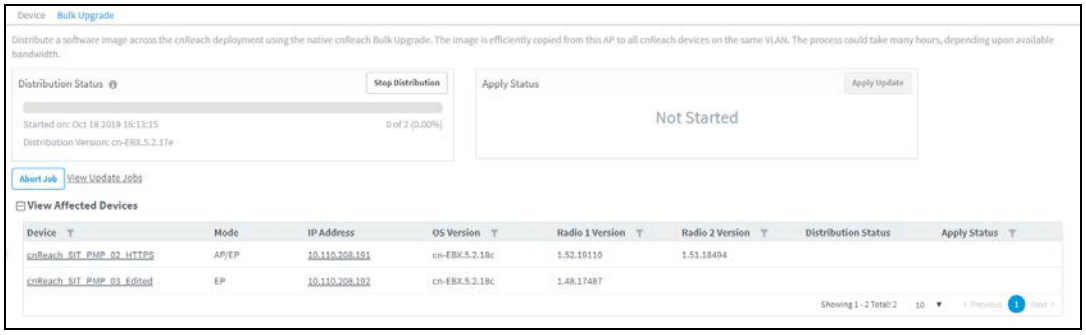


NOTE:

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

Upgrade Tracking

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



Fixed Wireless Configuration

This chapter provides the following information:

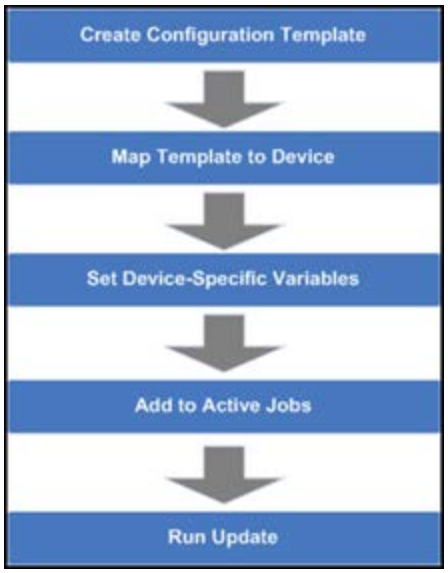
- Overview
- Configuration Templates
- Configuration Variables
- Configuration Update

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 85 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 86 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:

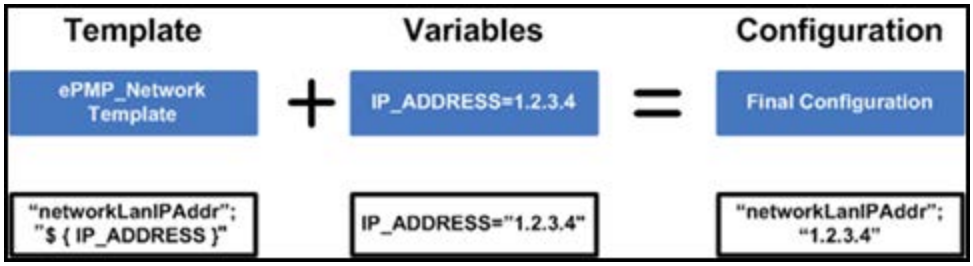
"networkLanIPAddr": $ {IP ADDRESS="10.1.1.254"},

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 87 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 88 Template configuration (ePMP/PMP)

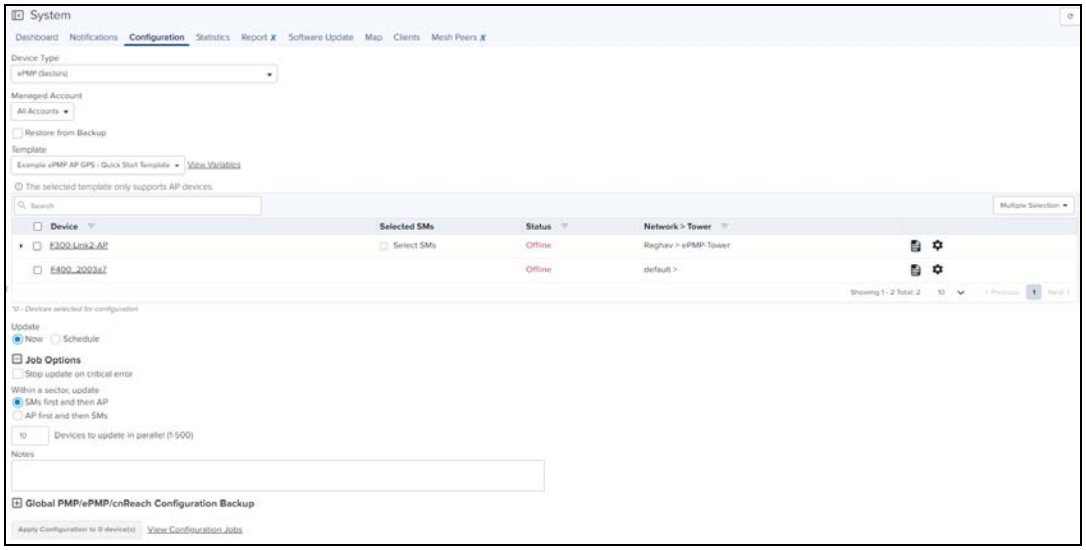


Figure 89 Template configuration (cnPilot Home R-Series)

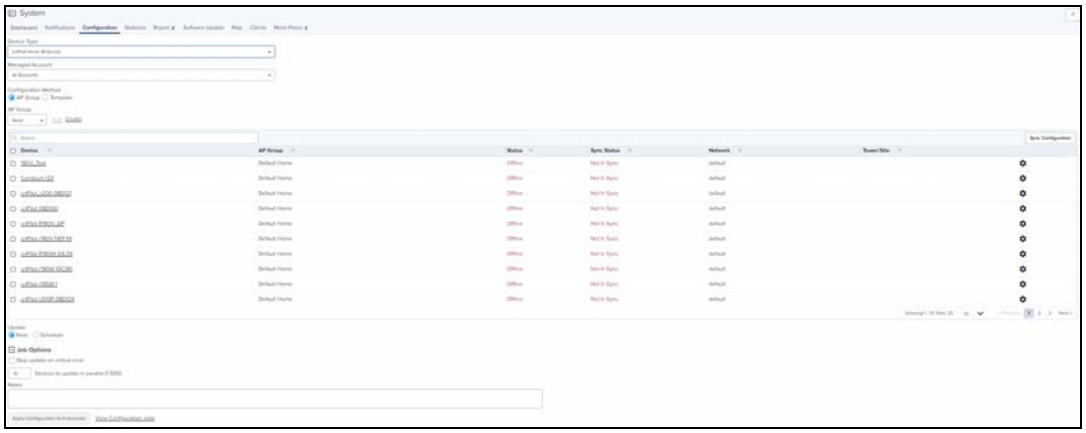


Figure 90 Template configuration (cnVision)

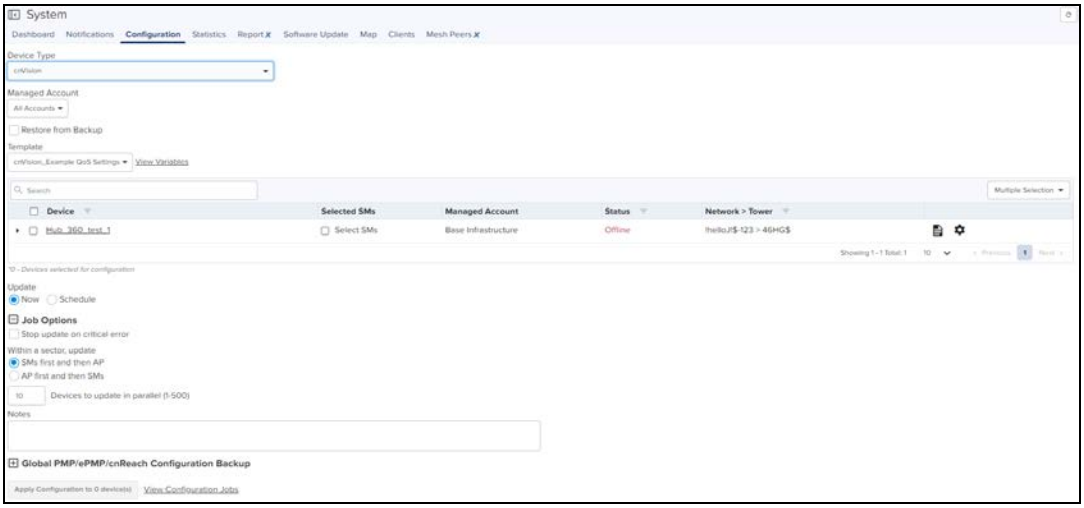
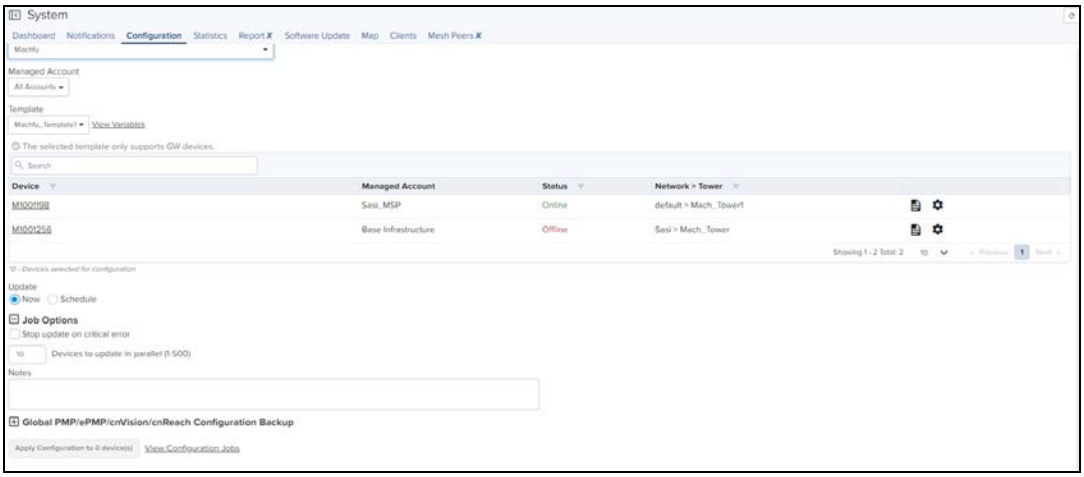


Figure 91 Template configuration (Machfu)



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 31: 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.

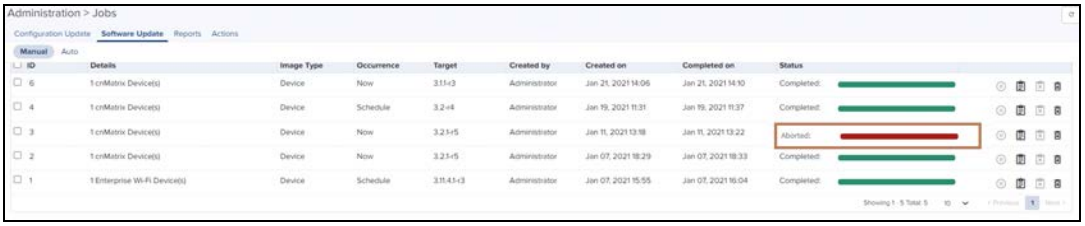
Update Ordering

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 92 Abort Configuration



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

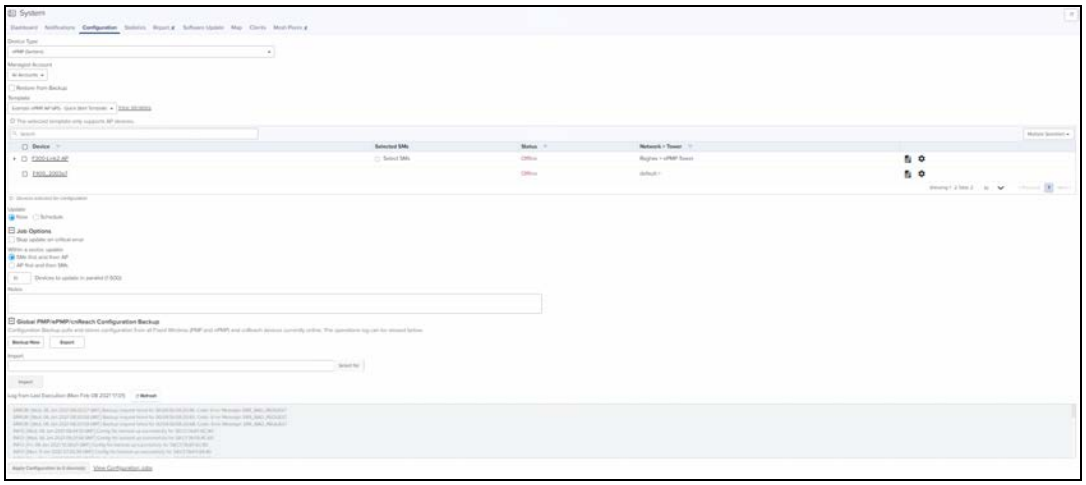
Configuration Backup pulls and stores configuration from Fixed Wireless devices (PMP and ePMP) and cnReach devices which are currently online.

The backup operations log can be done through:

- System level
- Device level

System Level

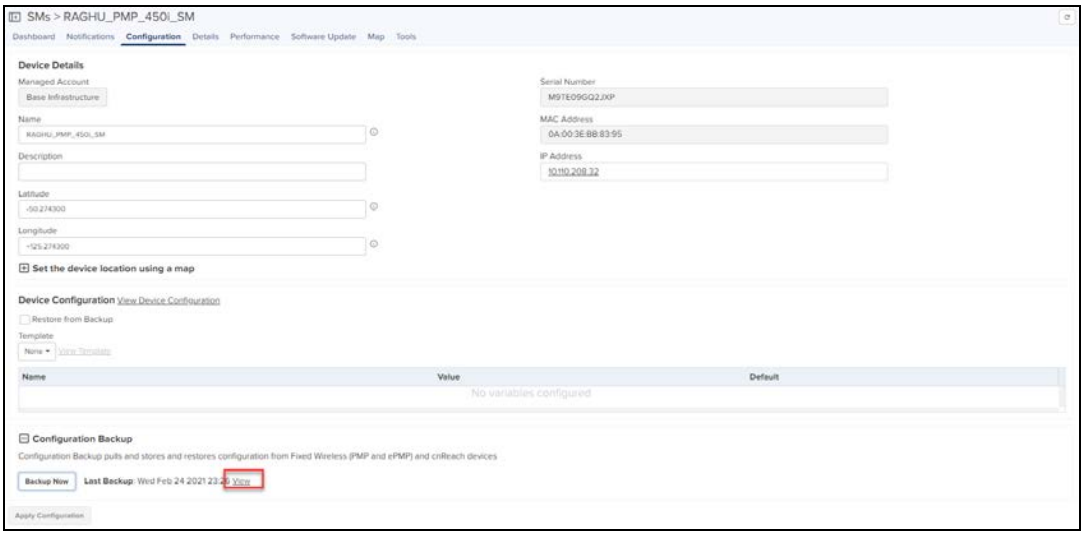
1. Navigate to **Manage > Configuration**.
2. Select cnReach/cnVision/PMP/ePMP (Sectors) from the following **Device Type** drop-down list:
3. In **Global cnReach/PMP/ePMP Configuration Backup** click **Backup Now.**



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.**

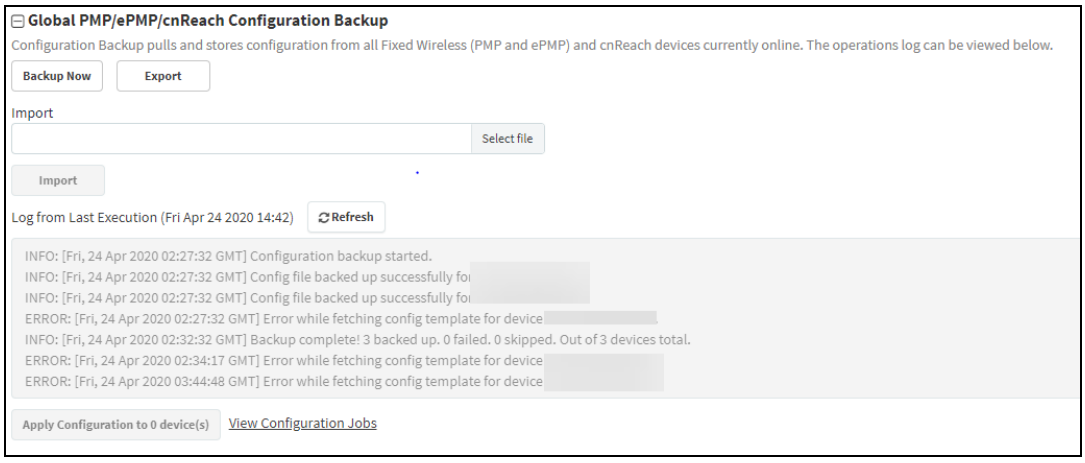


3. Click **View** to view the backup data.

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:

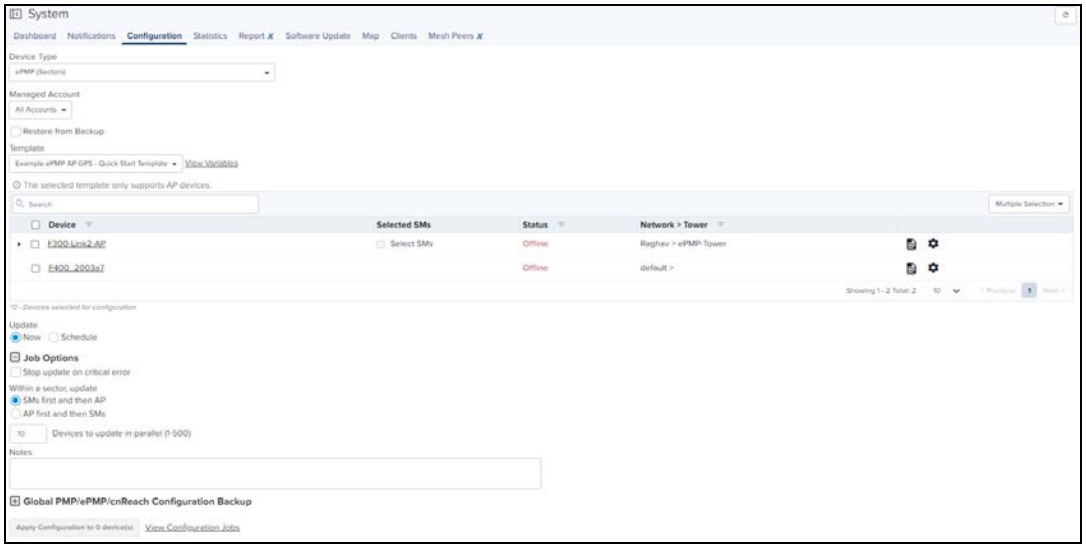
- System level

- Device level

System Level

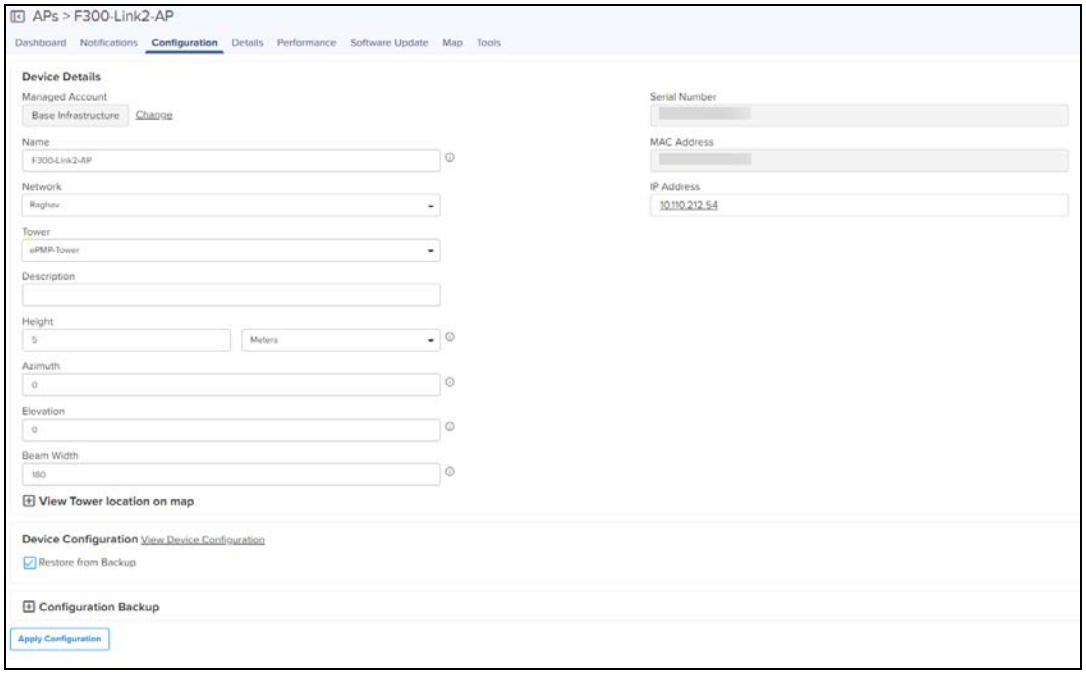
Perform as follows to restore the configuration backup of the device.

1. Navigate to **Manage >** select **System/Managed Account/ Networ/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 32: 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 (Advanced)
- User-Defined Variables (Advanced)
- 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

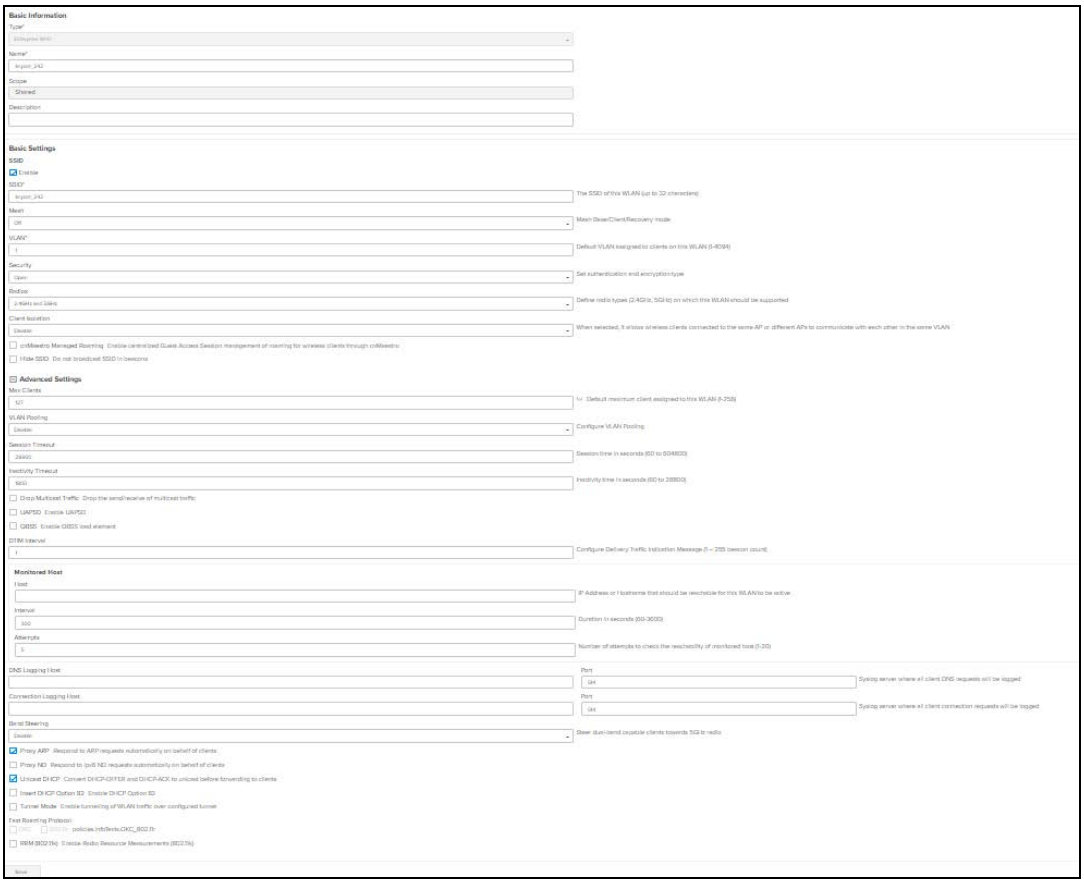
To create a WLAN, navigate to **Shared Settings > AP Groups and WLANs** (or the WLAN page in the Wireless LAN View) and select **New WLAN**. As with AP Groups, WLANs are separated into cnPilot Home and cnPilot Enterprise types. cnPilot Enterprise WLANs are able to configure WLAN, RADIUS, Guest Access, 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.



3. Click **Save**.

Creating a ePSK WLAN

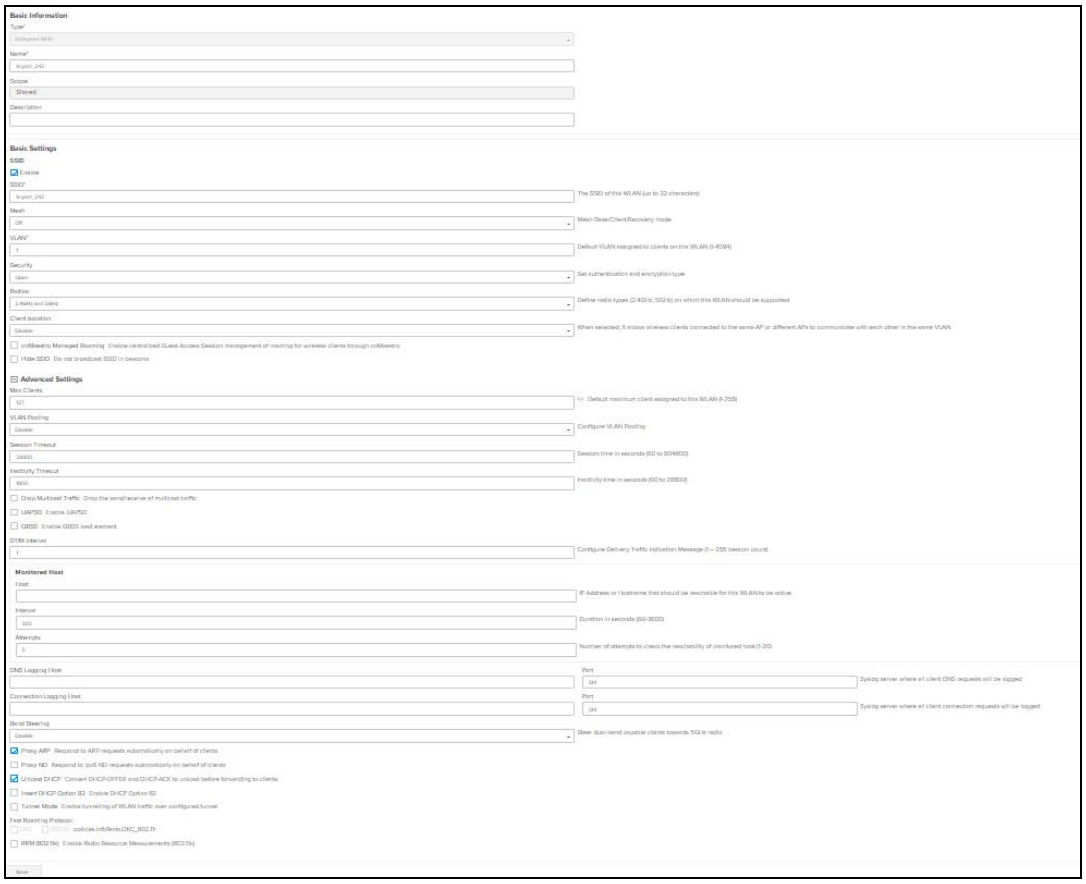
To create a WLAN, navigate to **Shared Settings > AP Groups and WLANs** (or the WLAN page in the Wireless LAN View) and select **New WLAN**. As with AP Groups, WLANs are separated into cnPilot Home and cnPilot Enterprise types. cnPilot Enterprise WLANs are able to configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters. cnPilot Home WLANs can configure SSID, Scheduled Access, and Access parameters.

NOTE:

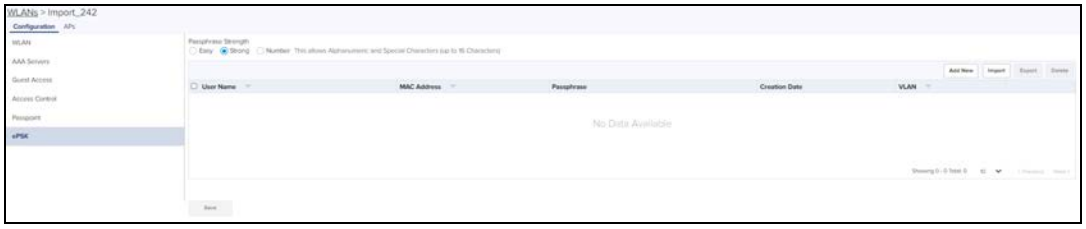
- The special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z0-9_-*&%#@!<>.()[]^~`$). The user can also rename them if required.
- In cnMaestro X pro user allowed to create 1024 espk per Wlan.
- By default password will not be configured. User has to configure the password for WLAN.

Steps to create WLAN policy:

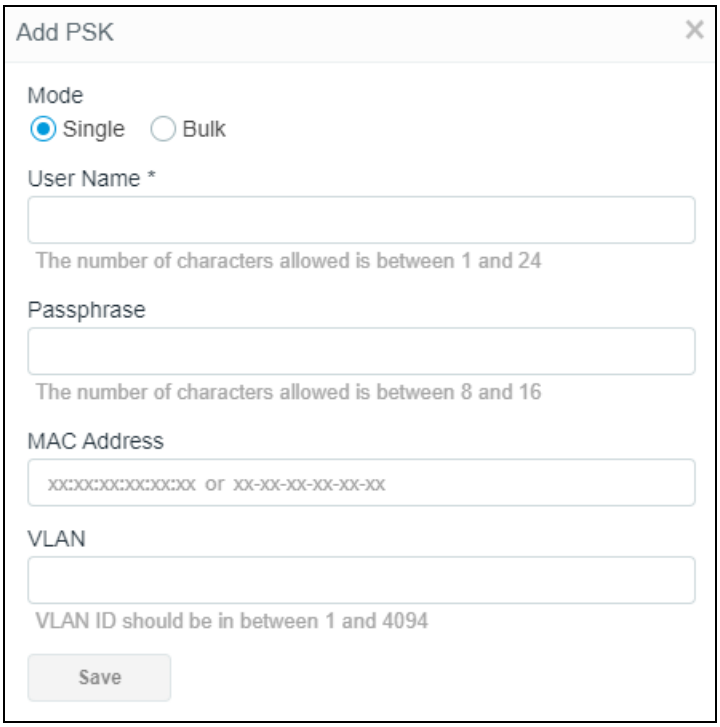
1. From homepage navigate to **WLANs.**
2. Click **New WLAN**, provide basic parameters to WLAN, and ensure **WPA2 Pre-Shared keys** is enabled in Security drop-down.



3. Click **Save**.
4. Navigate to **ePSK** tab. Select the **Passphrase Strength** as **Easy** or **Strong** or **Number**.



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.

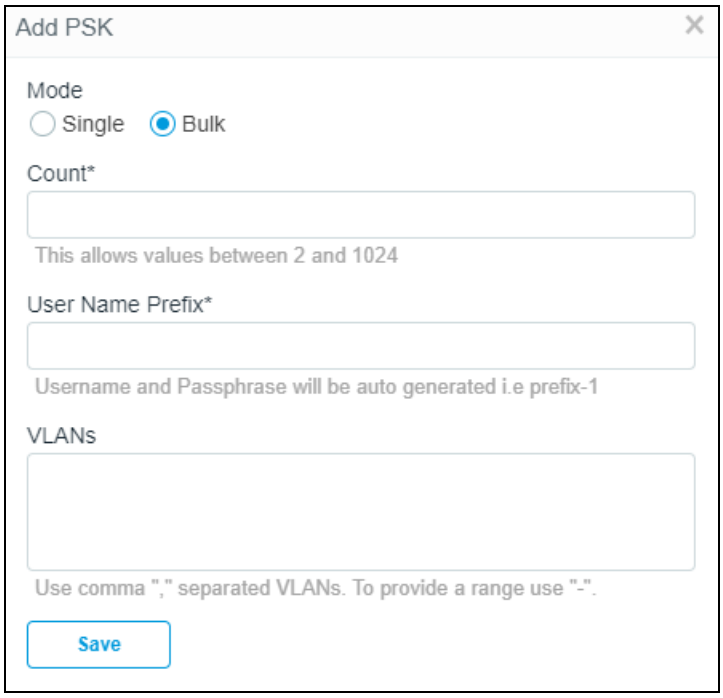


NOTE:

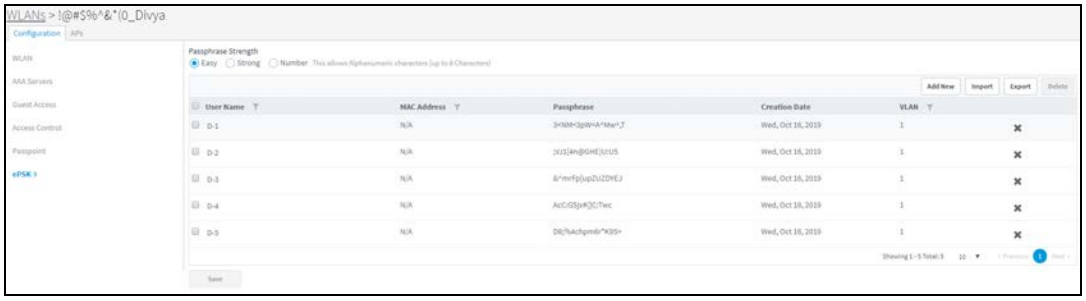
Passphrase is optional and it will be automatically generated based on the selected passphrase strength.

6. In **Single** Mode we can see single entry only.

7. In **Bulk** Mode, **Count** and **User Name Prefix** are mandatory fields. Enter the **Count** and **User Name Prefix**.

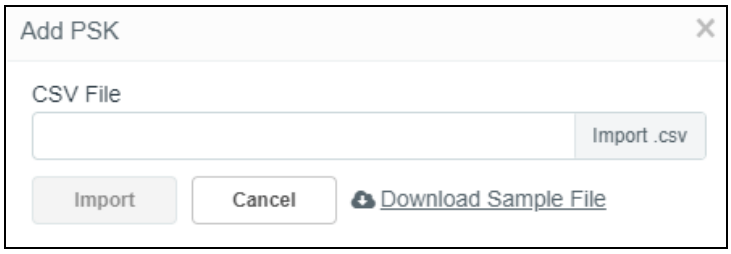


8. In **Bulk** Mode we can see many entries.

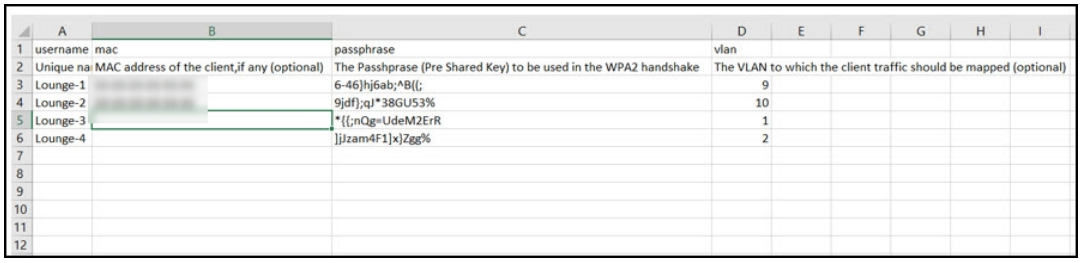


Import ePSK

1. Click **Import**. A dialogue box appears.
2. Select **import.csv** and import the file.



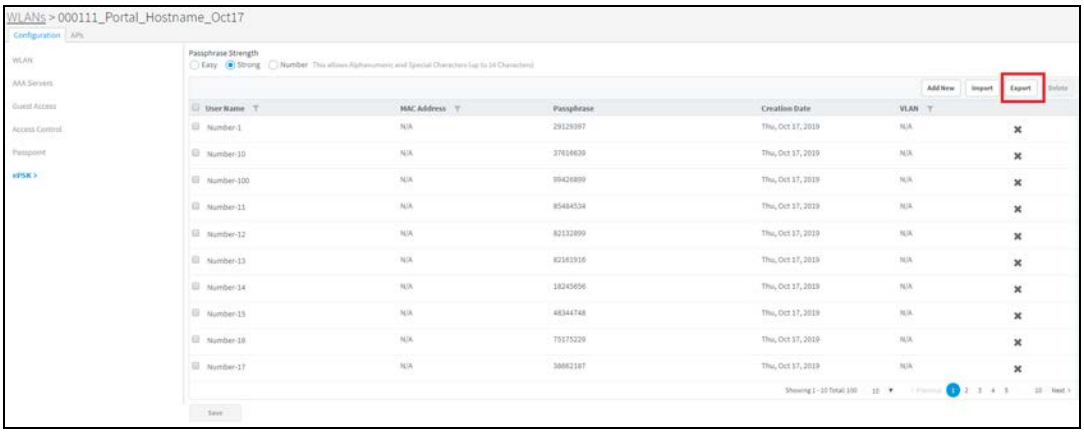
3. When you click **Download Sample File**, you can see Sample ePSK excel sheet.



	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;^B({;	9					
4	Lounge-2		9jdf};qJ*38GU53%	10					
5	Lounge-3		*{{;nQg=UdeM2ErR	1					
6	Lounge-4		]jJzam4F1]x]Zgg%	2					
7									
8									
9									
10									
11									
12									

Export ePSK

1. Click **Export**. A dialogue box appears.
2. Select **export.csv** and export the file.

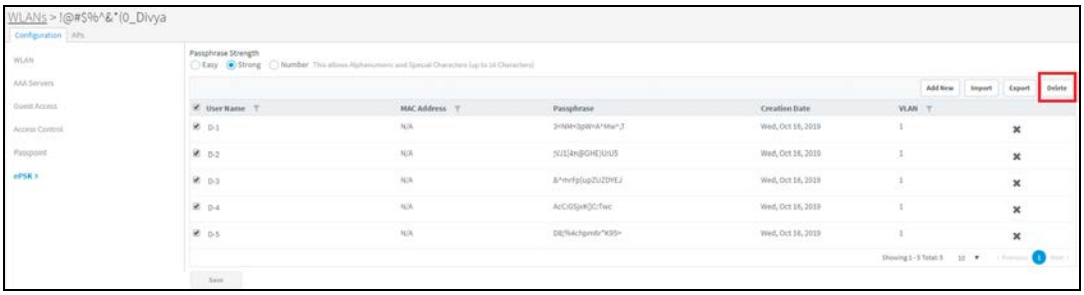


3. When you click **Download Sample File**, you can see Sample ePSK excel sheet.

	A	B	C	D	E	F	G	H	I
1	username	mac	passphrase	vlan					
2	Unique na	MAC addr	The Passh	The VLAN to which the client traffic should be mapped (optional)					
3	Room-1		WVghr8SmY_a;;Q(e						
4	Room-2		a{n5&HepkJ~=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**.



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,

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.

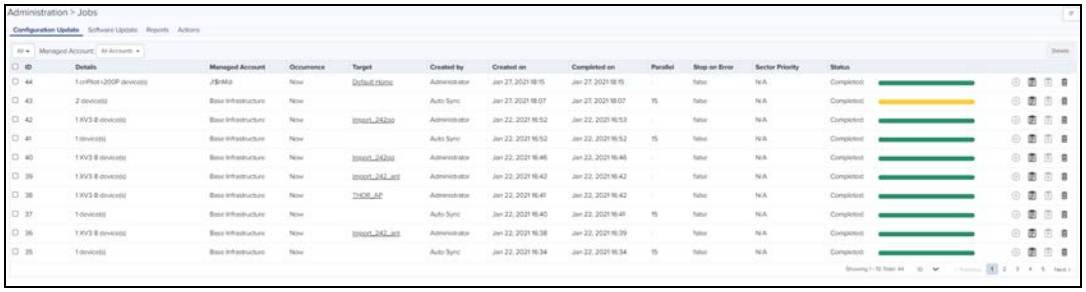
To enable this feature:

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.

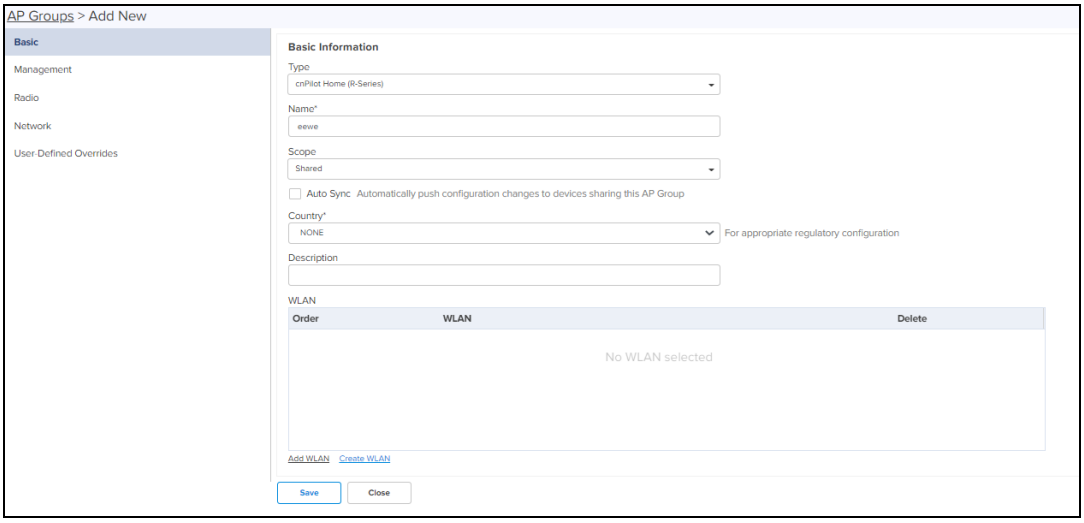


Retry Configure

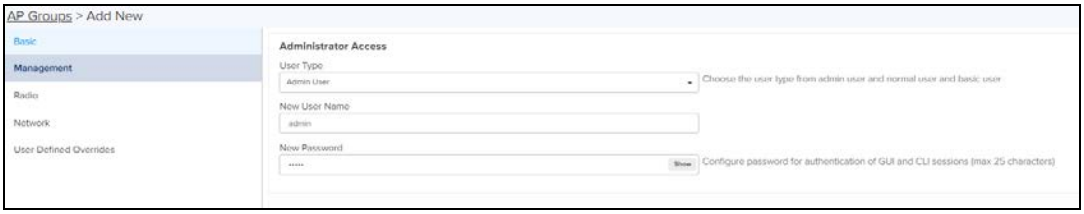
When the user tries to apply any AP Group on the device and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as "Device was offline", in the **Jobs** page. In this case, when device comes up and connects to cnMaestro, then cnMaestro will create an Auto-sync 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.



Default password: **admin** of cnPilot R-series should be changed before upgrading to the build 4.6-RX.



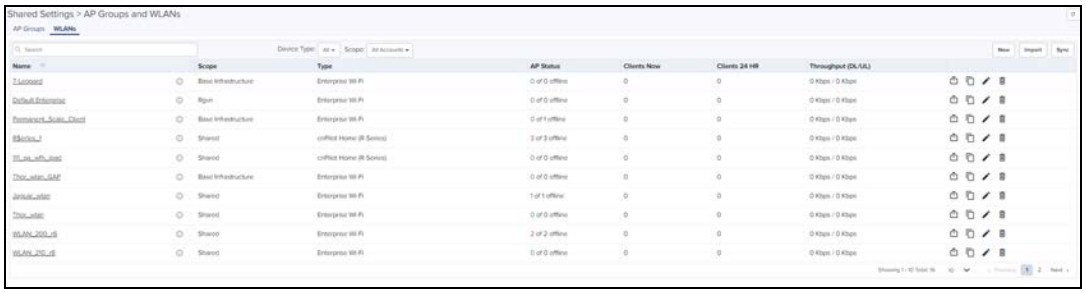
Once after the upgradation of build 4.6-RX, default password; **admin** becomes invalid and password needs to be reset through the WAN.

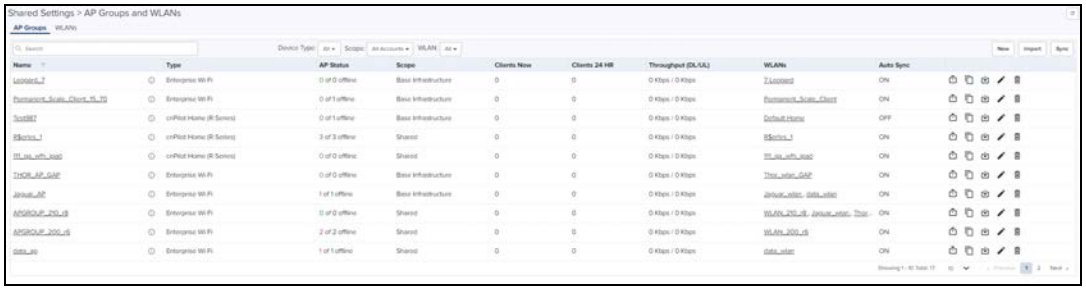
NOTE:

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.





To export WLAN and AP Group,

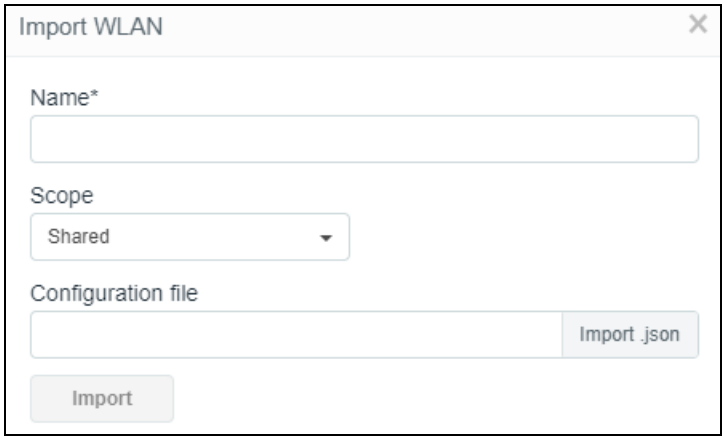
1. Navigate to **Shared Settings > AP Groups and WLANs page > WLAN** or **AP Group** tab (according to the choice).
2. Click **Export**.

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**.



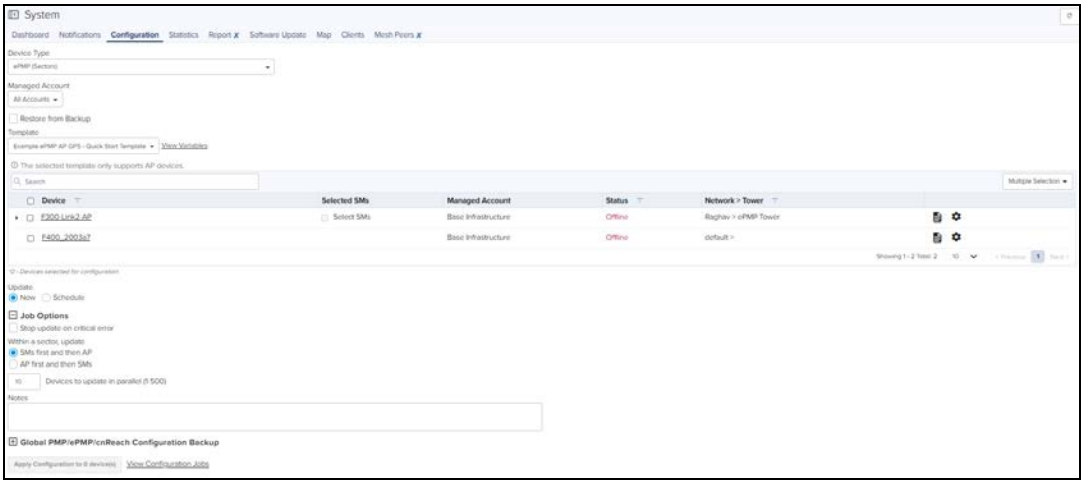
3. Enter the **Name.**
4. Select the **Configuration file** in Json format.
5. Click **Import**.

NOTE:

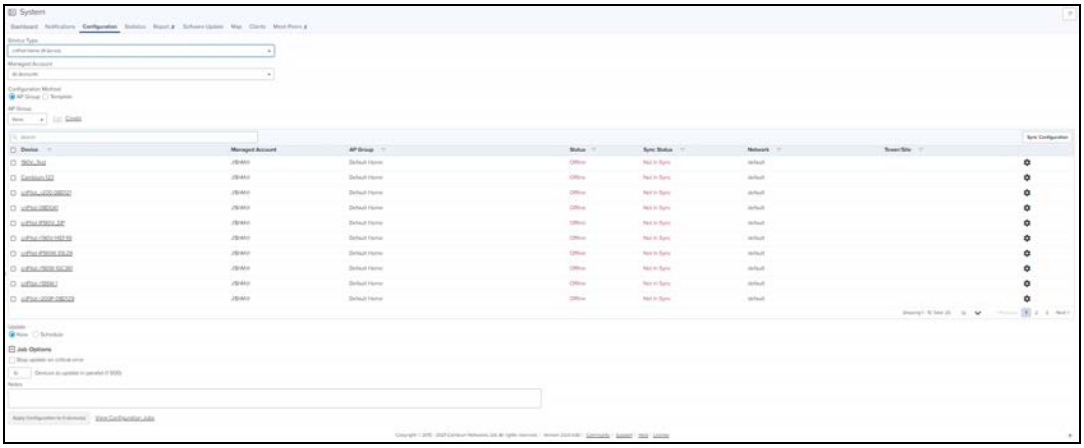
- To import an AP Group, ensure that all the associated WLANs in that AP Group are already imported. If the WLAN associated with the AP Group is unavailable, an error message will be displayed during AP Group import.
- If the name is not provided for WLAN or AP Group while importing, it will take the 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:



1. Select the **AP Group**.
2. Select the list of Wi-Fi Devices.
3. Click **Apply Configuration.**

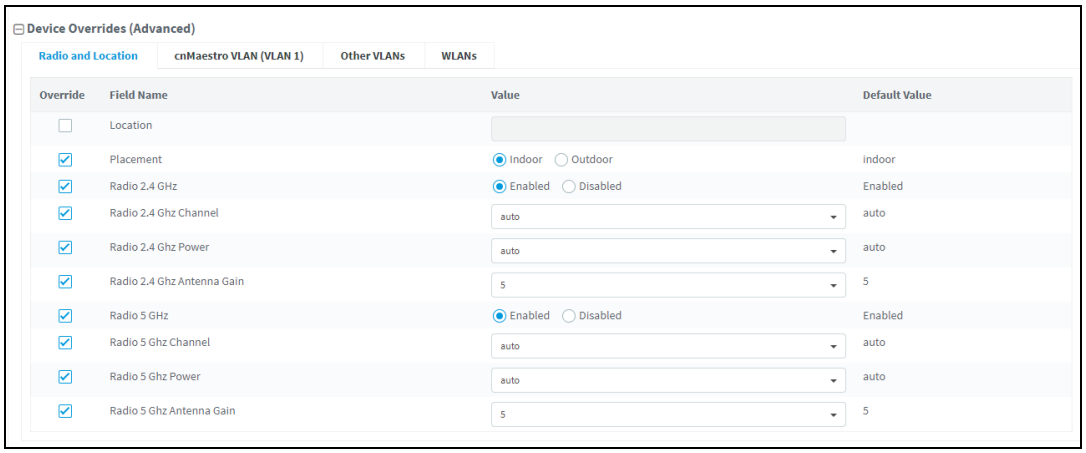


Pre-Defined Overrides

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.



User-Defined Overrides (Advanced)

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 can be pushed to the device using CLI commands through the User-Defined Override mechanism

This can be explained with the following example, in which country-code and hostname are appended to the end of the configuration, and will override any settings in the UI

```
country-code IN

hostname Wi-Fi_Device
```

User-Defined Variables (Advanced)

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 ${varaibleName=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.

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.

1. **Enterprise Wi-Fi AP Groups** by default synchronize automatically (so any change of AP Group or WLAN, followed by a Save, will immediately push configuration to the devices without manual intervention).
2. **cnPilot Home AP Groups** by default synchronize manually. Updates to them (or the WLANs to which they map) need manual synchronization to push configuration to the devices.

Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately. Navigate to **Administration > Sync Configuration**.

Sync Configuration only displays devices currently out-of-sync with a mapped AP Group .

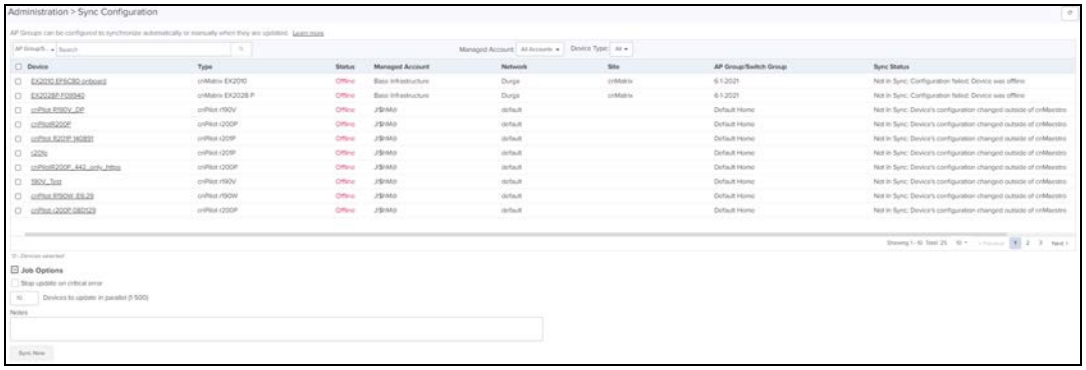
Sync Configuration has the following fields:

- AP Group (AP Group to which device is mapped)
- Device (Hostname)
- Device Type
- Network (Network in which device is present)
- Status (Up/Down)
- Site (Site under which device is present)
- Sync Status (Sync status will tell whether job is completed or failed)

Steps to do Sync Configuration:

1. Click the **Sync Configuration** in the top right of the **Configuration > WLAN and AP Groups or Manage > Configuration > Device Details or Jobs** tab.

2. Select devices you wish to synchronize.

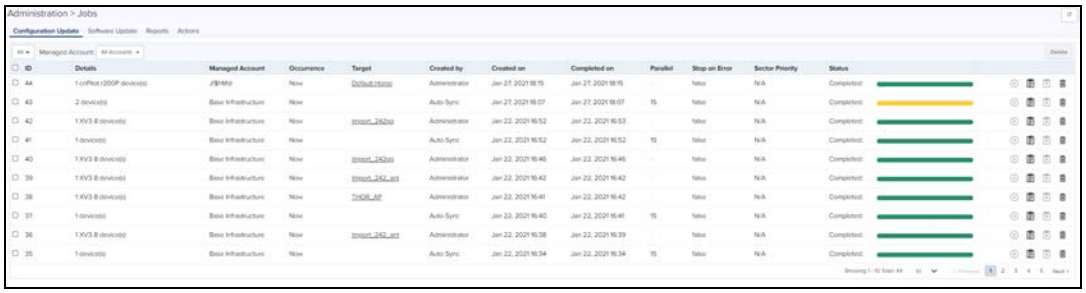


3. Click the **Sync Now**.

> **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.



> **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.

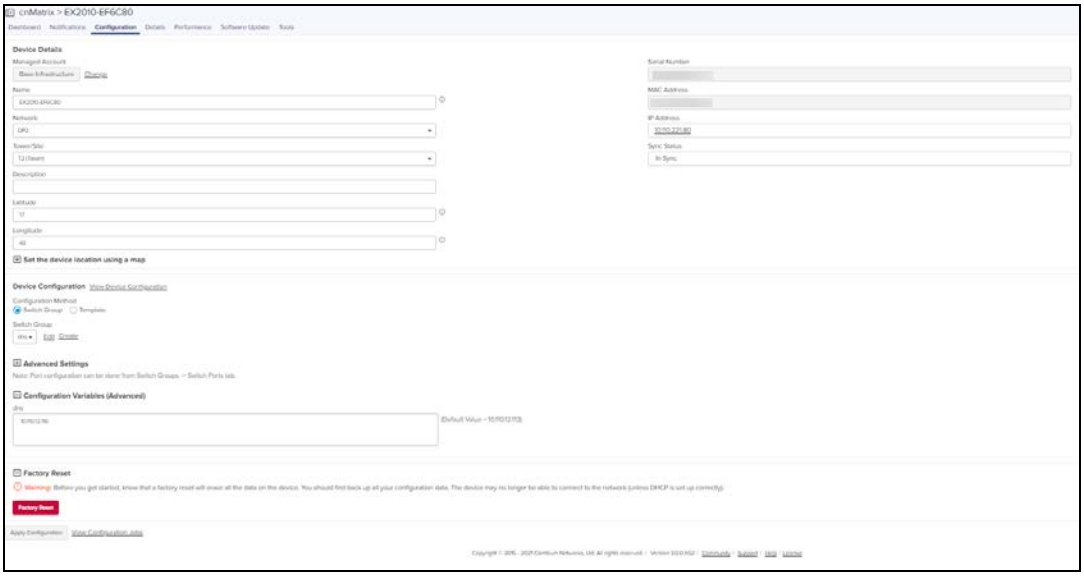
Factory Reset

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.

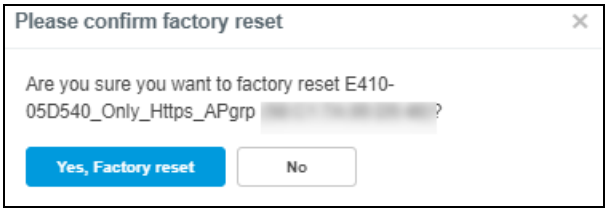
To factory reset the device from cnMaestro:

1. Navigate to the **Configuration** tab of the device.

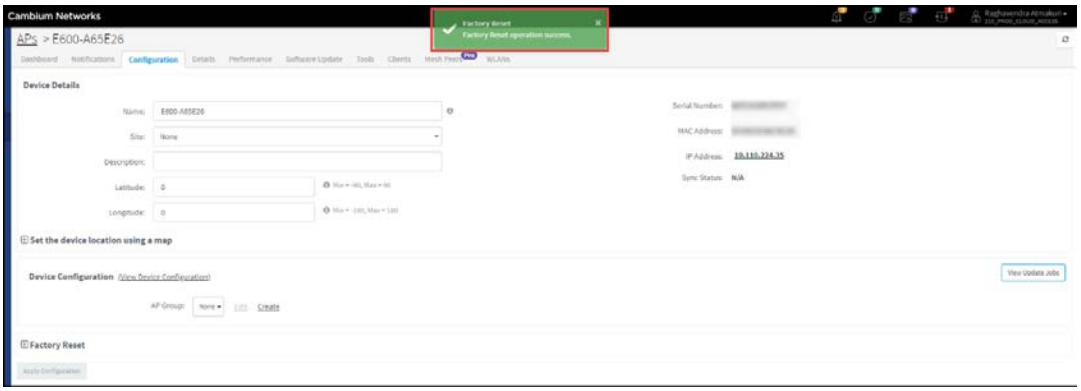
2. Select **Factory Reset.**



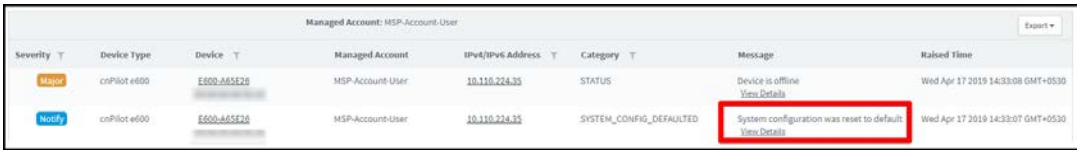
3. Click **Factory Reset**.



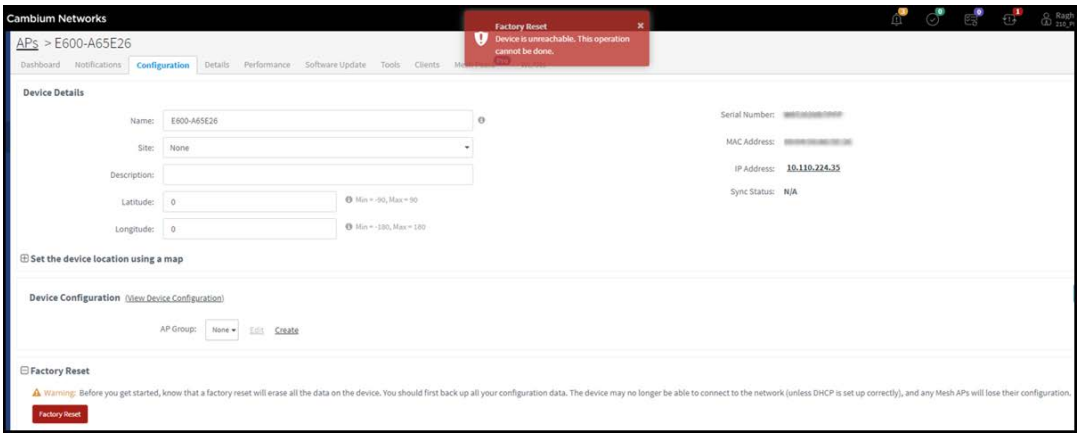
The following window pops-up if you click **Yes, Factory reset** option.



Once the Factory Reset is successful, the following message is displayed in the **Notifications** tab.



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.

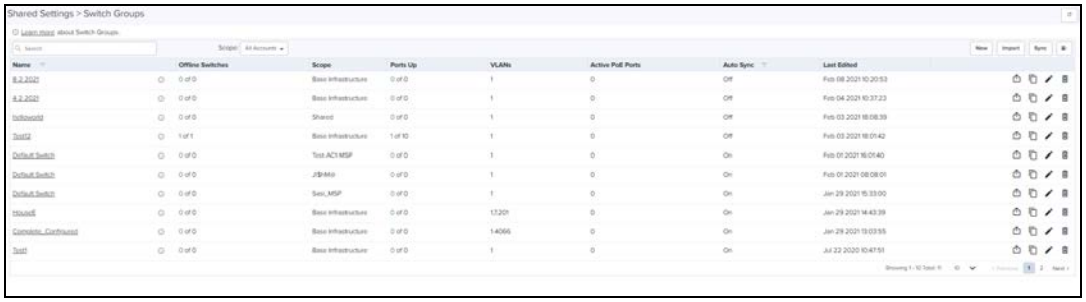
Configuration is common to all switches belonging to a Switch Group:

- 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.

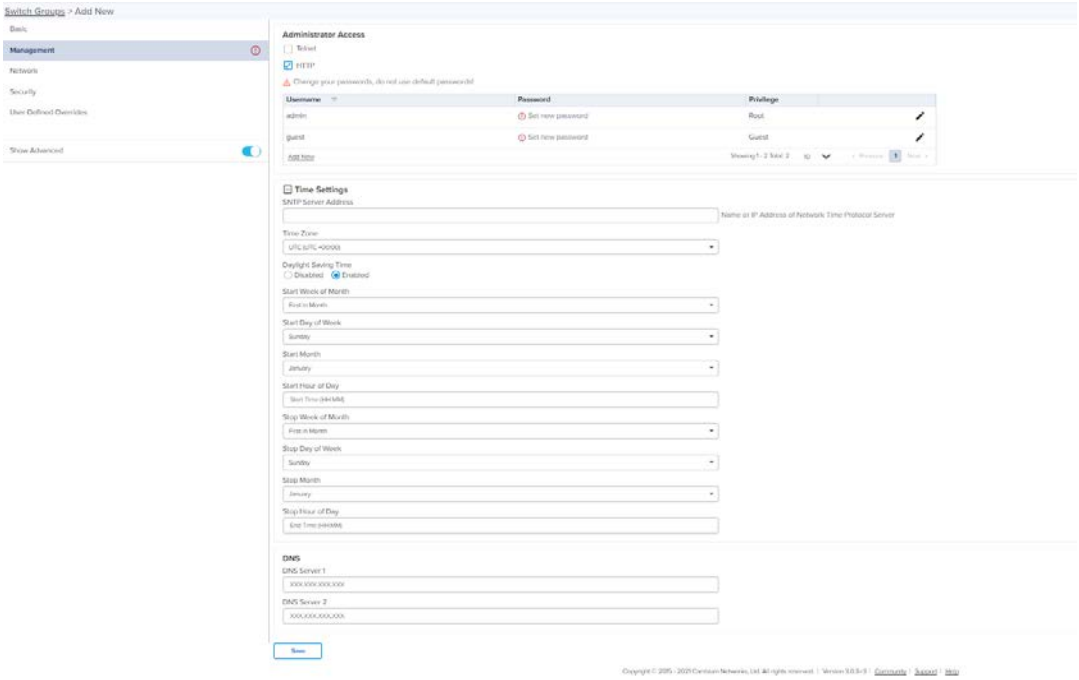
1. Navigate to **Configuration > Switch Groups > Basic.**
2. On the **Basic** page enter device identification data such as:
   - Name
   - Scope
   - Contact
   - Description
   - WISP Configuration

> **Note:**
>
> The special characters can be used to create names of Switch Groups (Eg: a-zA-Z_-*&%#@!<>.() []^~`$1234567890).

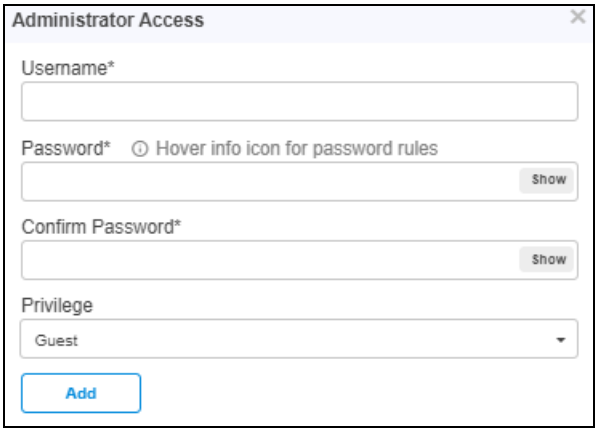
3. Click **Save**.

Management

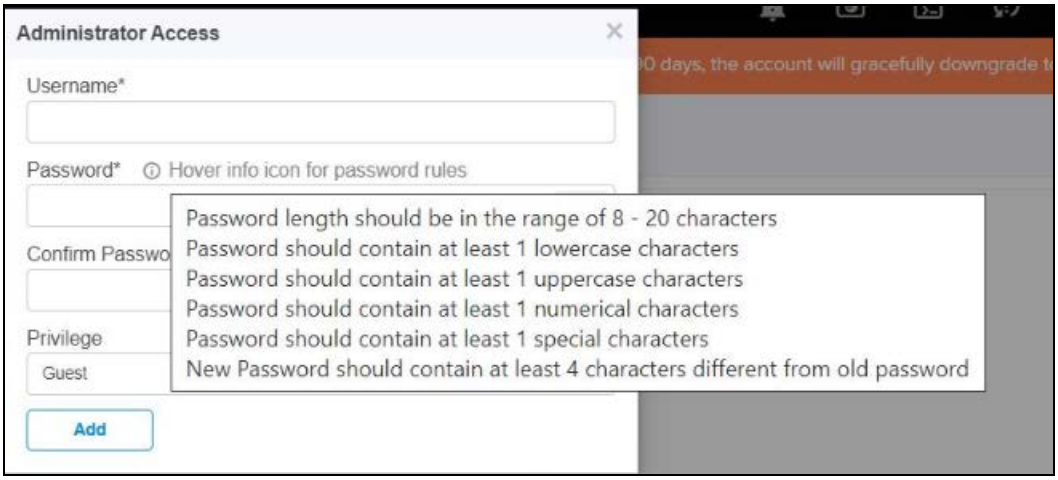
1. Navigate to **Management** page**.**
2. Enable the **Daylight Saving Time** and enter the details.



3. Click **Add New** to add **Administrator Access**, enter the details and click **Add.**



4. Password should match the special characters as shown below:

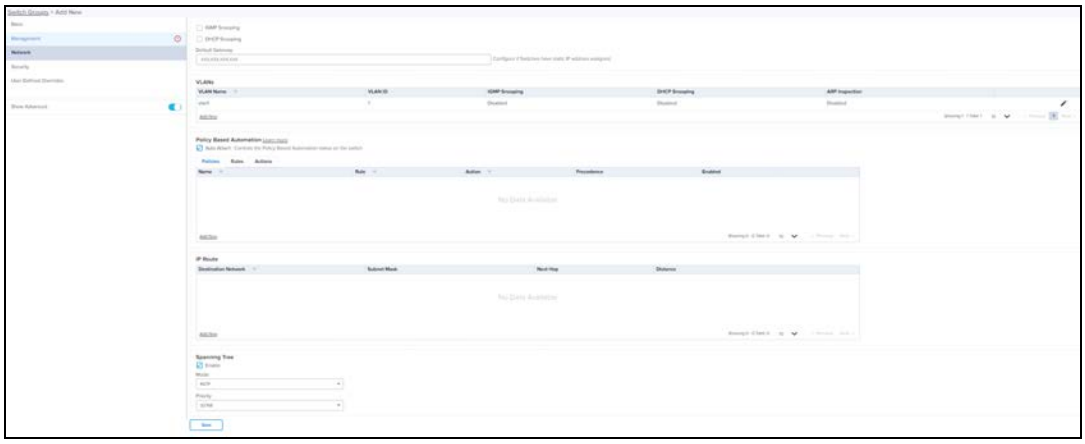


5. Click **Save.**

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**.

2. Click **Save**.

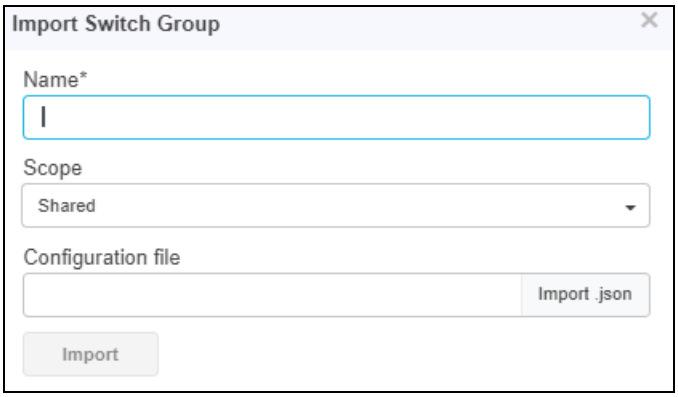
User-Defined Overrides

> **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

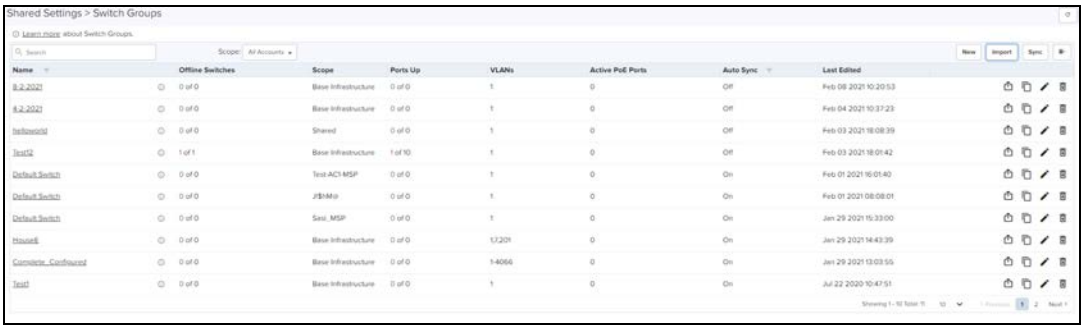
1. Click **Import Switch Group**. A dialogue box appears.
2. Select **import.json** and import the file.



3. When you click **Download Sample File**, you can see Sample excel sheet.
4. Click **Import**

Delete Switch Group

To delete Switch Group from the list click **Delete** icon of the specific device row.



Retry Configure

When the user tries to apply any Switch Group on the device and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as " Device was offline", in the Jobs page. In this case, when 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).

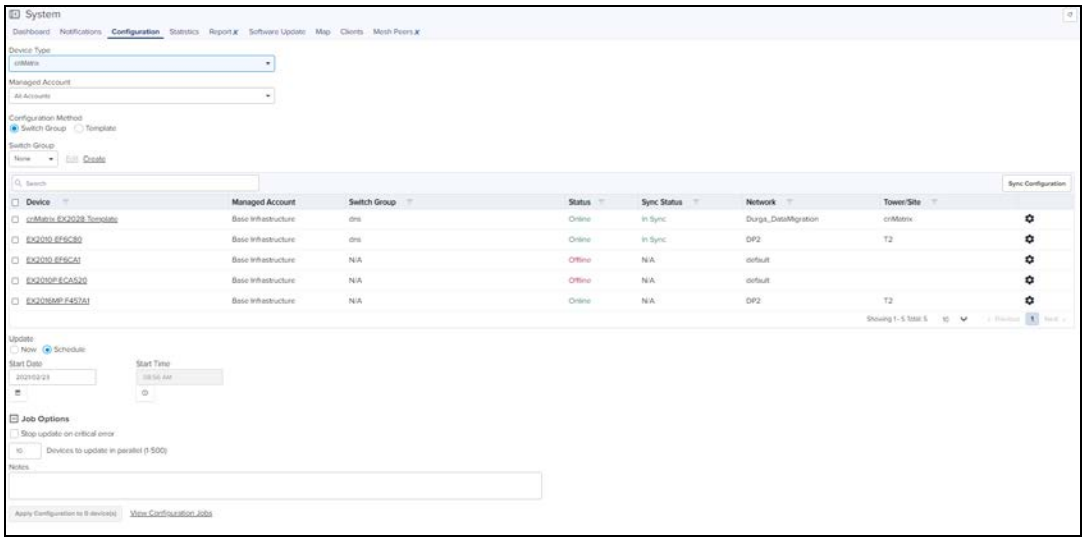
NOTE:

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.**



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**.

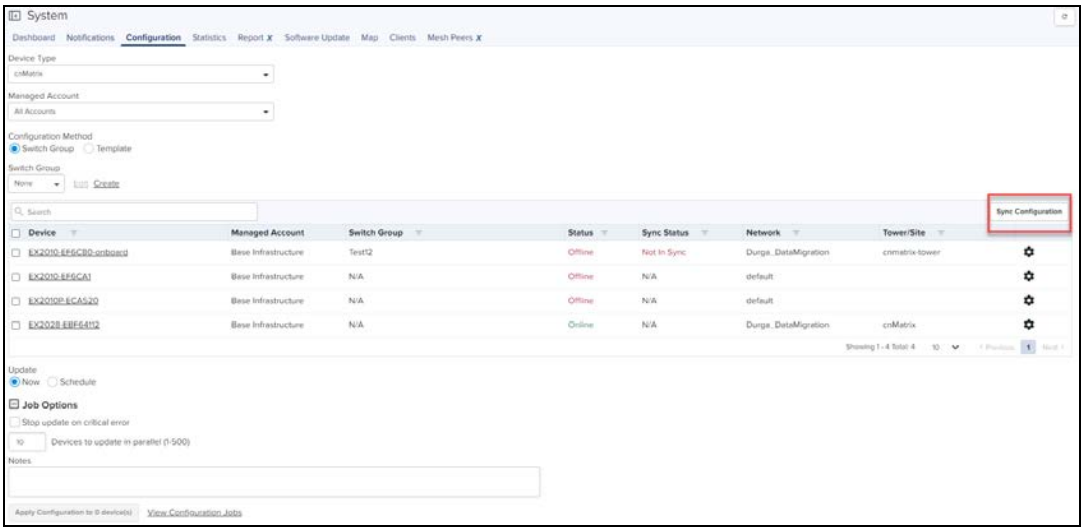
Sync Configuration has the following fields:

- 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)

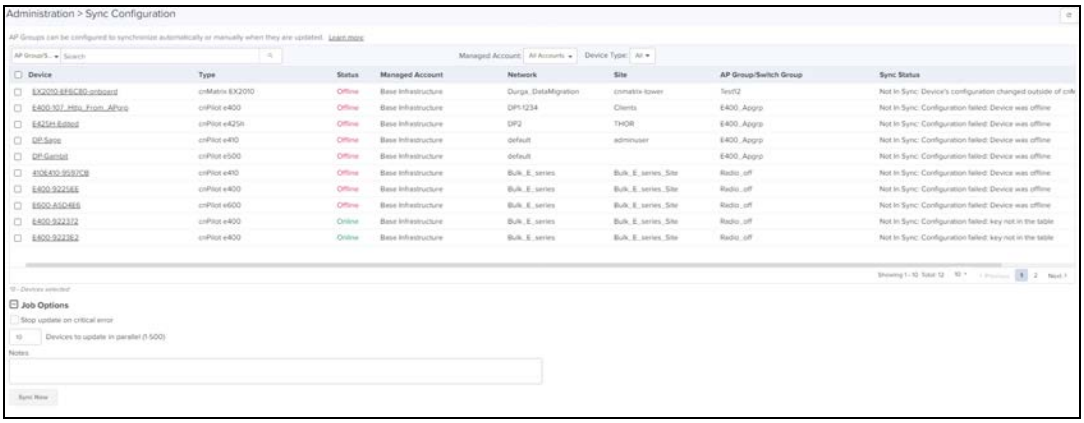
Steps to do Sync Configuration:

Navigate to **Manage > Network > Configuration > Device Details or Jobs** tab.

1. Select devices to synchronize and click the **Sync Configuration**.



2. Automatically it navigates to **Administration > Sync Configuration** and select devices to synchronize.



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.

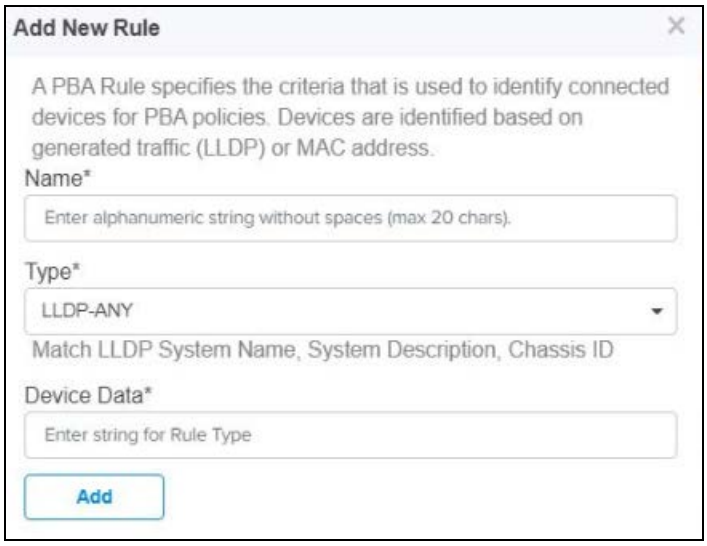
PBA configuration is common to all switches within a switch group.

> **NOTE:**
>
> Dynamic PBA updates are indicated by asterisk * on the Switch Dashboard and on the Switch Ports pages.

Configure the PBA as follows:

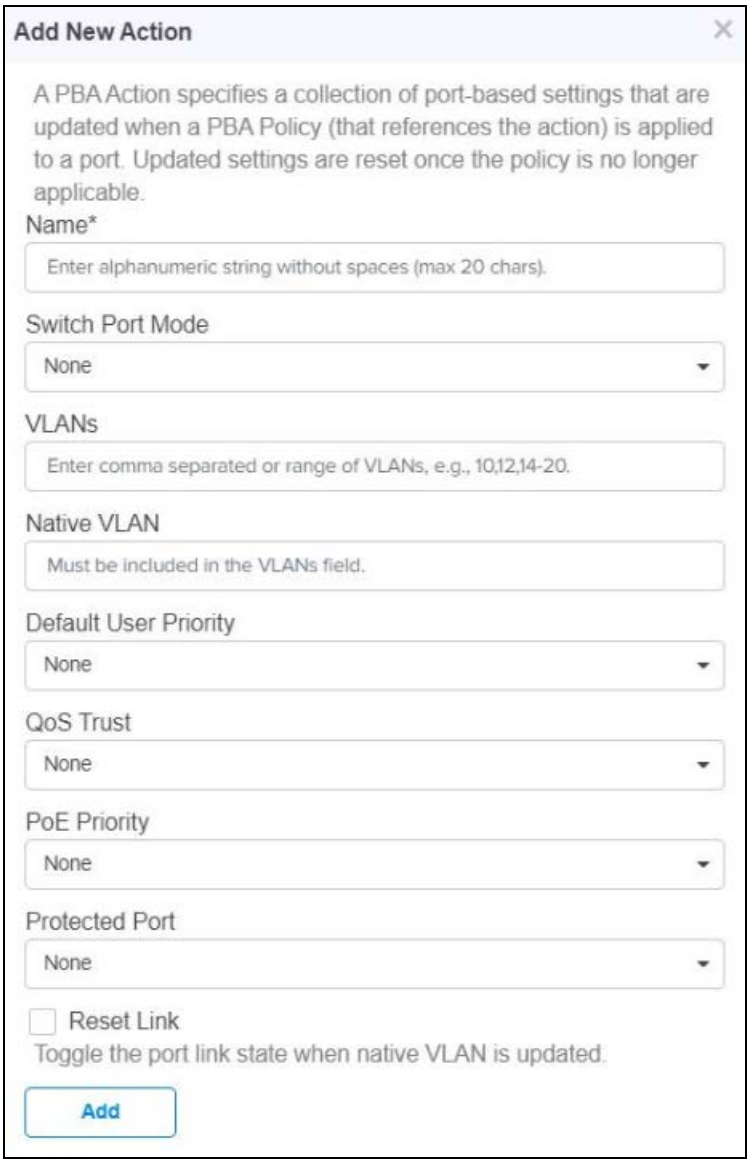
1. Navigate to **Switch Groups > Configuration > Network > Policy Based Automation.**
2. Navigate to **Rules tab.**

3. Click **Add New** to set the rules.



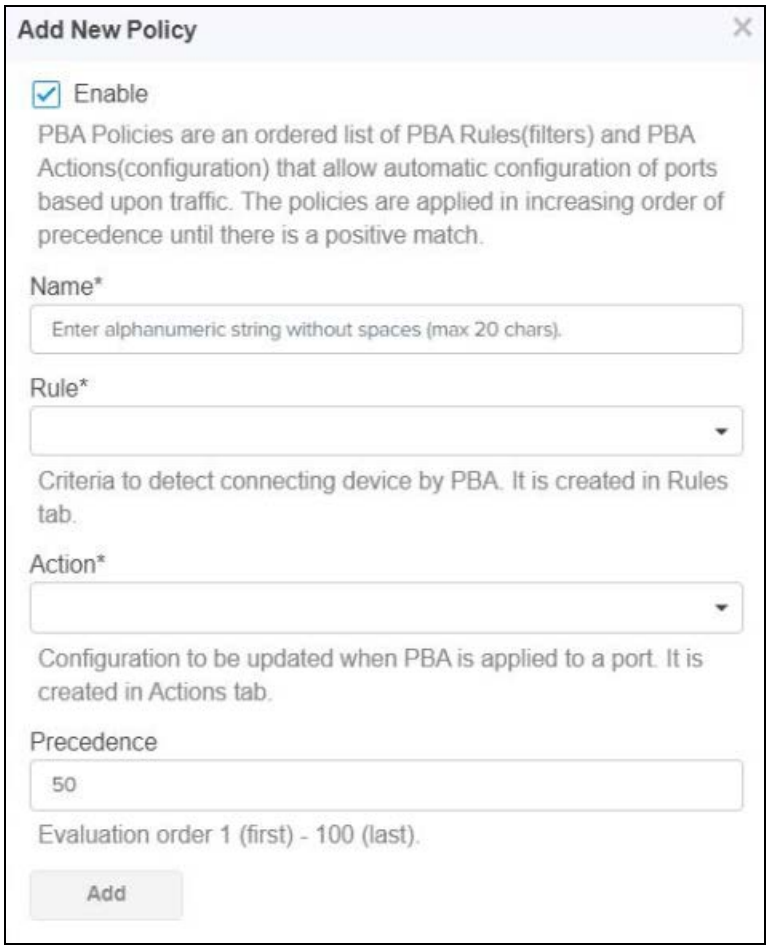
4. Click **Add.**
5. Navigate to **Actions** tab.

6. Click **Add New** to set the actions.

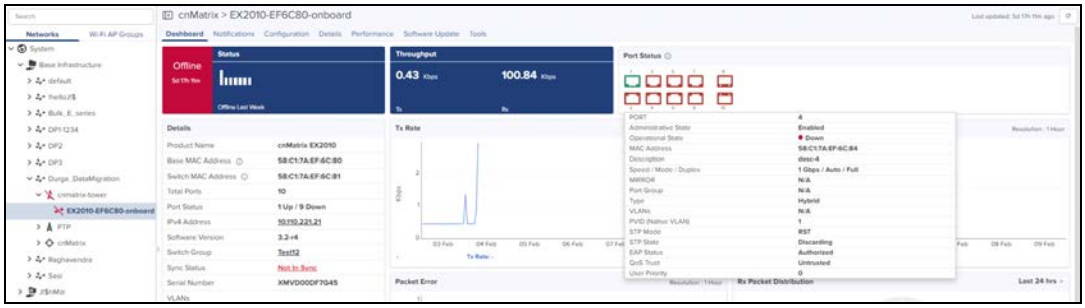


7. Click **Add**.
8. Navigate to **Policies.**

9. Click **Add New** to set the policies.



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.



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:

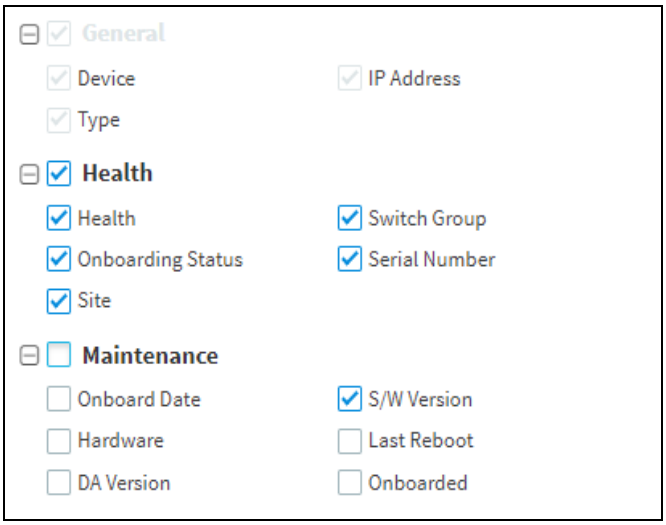
- Navigate to **Switch Groups >** select the switch from the list and click **Switches** page to view and edit the onboarded switches.

The Switches details view displays following fields by default:

- Device, Health, Onboarding Status, Serial Number, IP Address, Switch Group, Type, Site and Action tab.

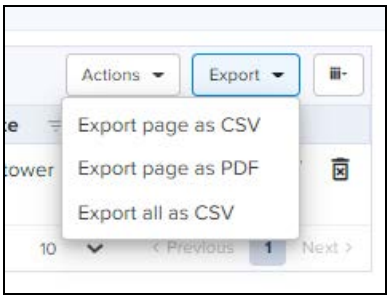
Action column can be used to edit or delete any device of the Switches.

User can click on top bar to include additional fields in Switches Detail view.



Export Switches

1. Click **Export**. A dialogue box appears.

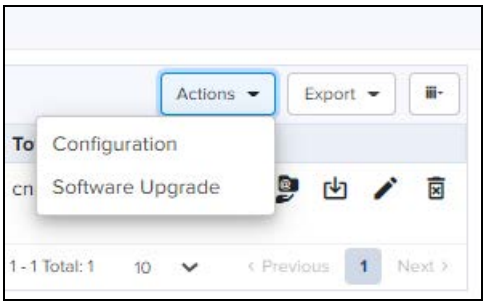


2. Select **Export page as CSV/PDF/all as CSV** and export the file.

Action

Action column can be used to edit or delete any device of the Switches.

1. Click **Action**. A dialogue box appears.



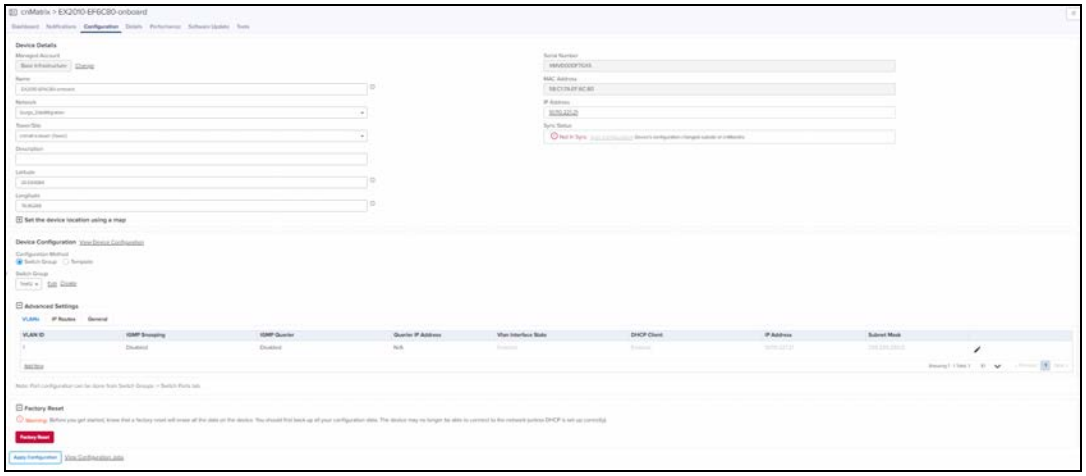
2. Select **Configuration** to edit the device details or click Edit icon
3. Select **Software Upgrade** to update the device software or click
4. Click to delete the selected device from the list.

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.

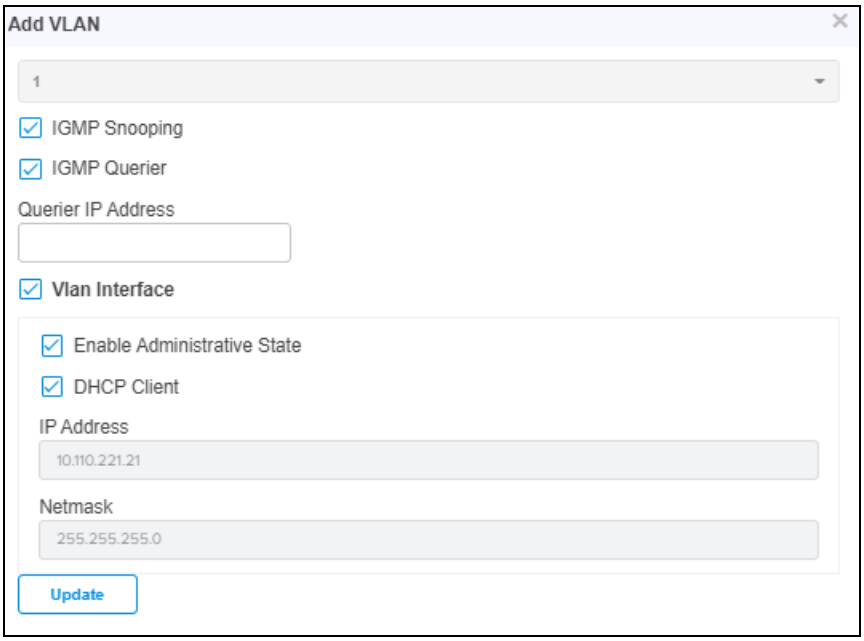
Navigate to the **Advanced Settings** and configure the following parameters:

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.

2. Click Edit Icon or Add New.
3. Enter the required details and click **Add**

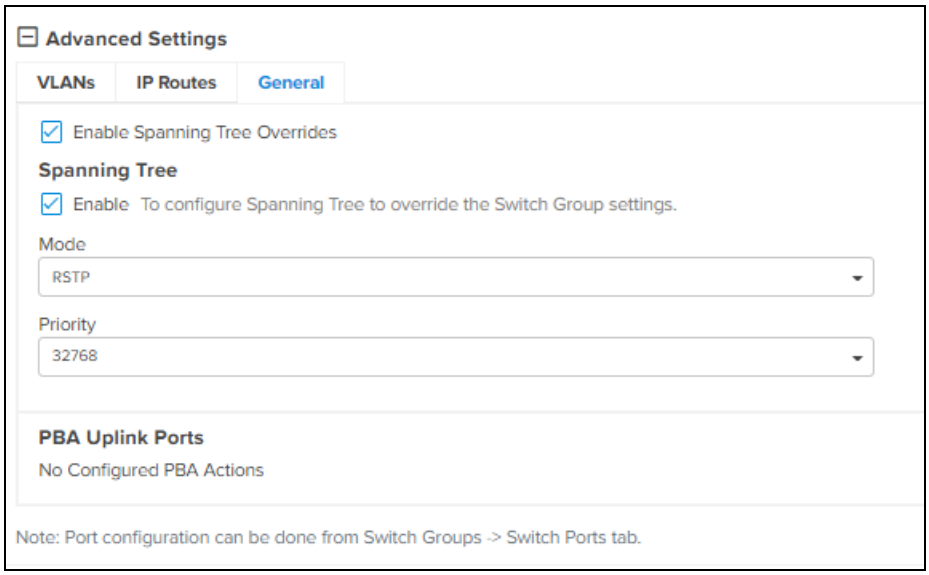


General

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.



NOTE:

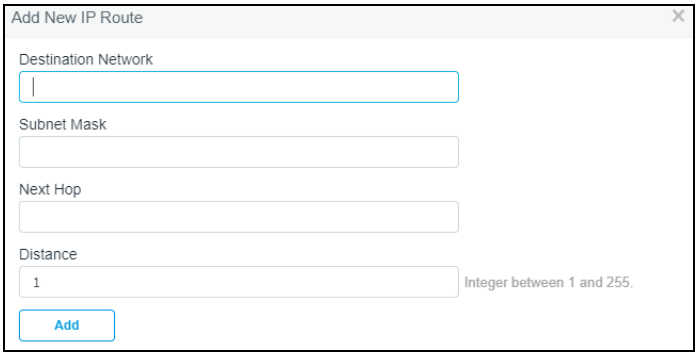
If Spanning Tree is disabled the overrides feature will be disabled on the Switch configuration.

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.**

1. Click **Add New**.
2. Enter the parameters such as Destination Network, Subnet Mask, Next Hop, and Distance.
3. Click **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.

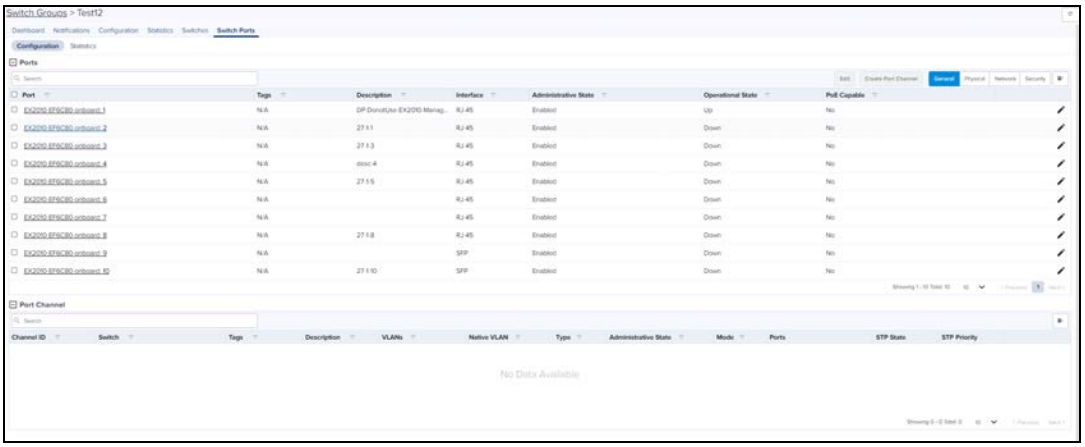
To view the Switch Ports, navigate to **Shared Settings > Switch Groups > Switch Ports**.

Ports

cnMaestro **Switch Ports Configuration** tab allows the user to configure the following parameters:

- General
- Physical
- Network
- Security

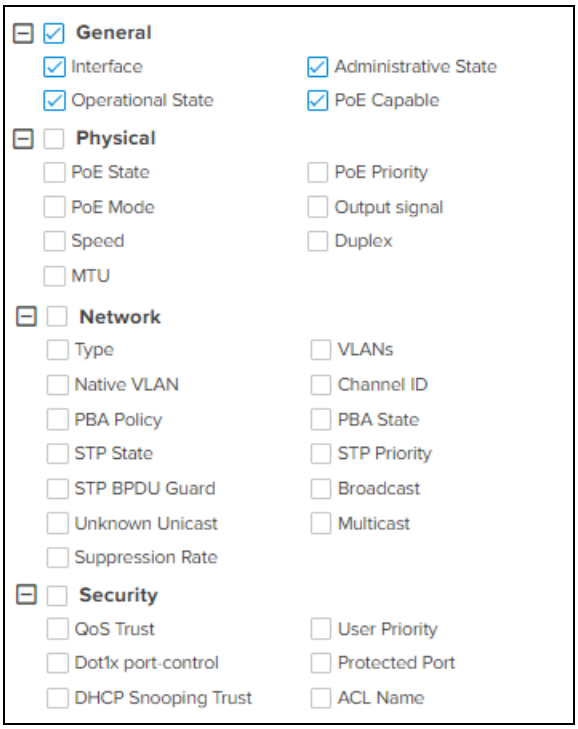
General Tab



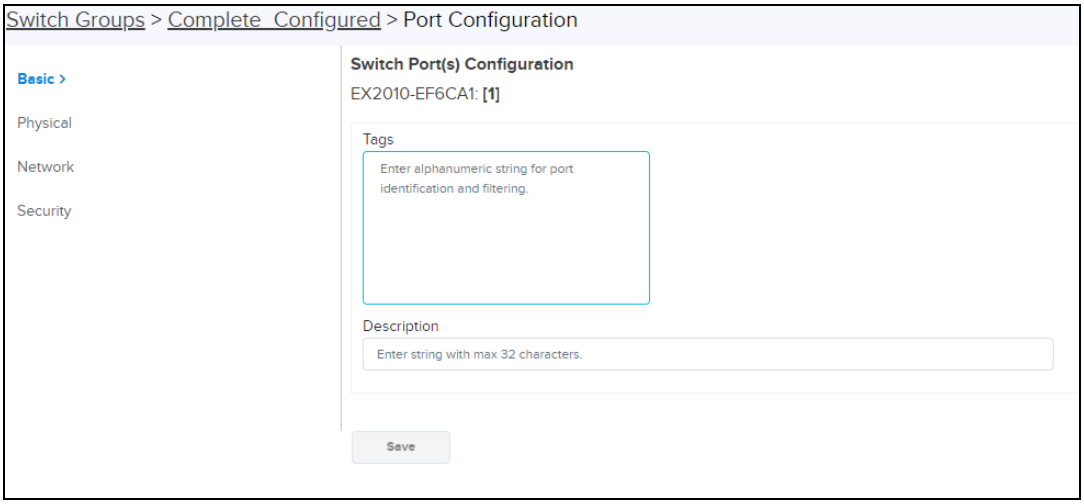
The **Ports General** details view displays following fields by default:

- 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.



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.**

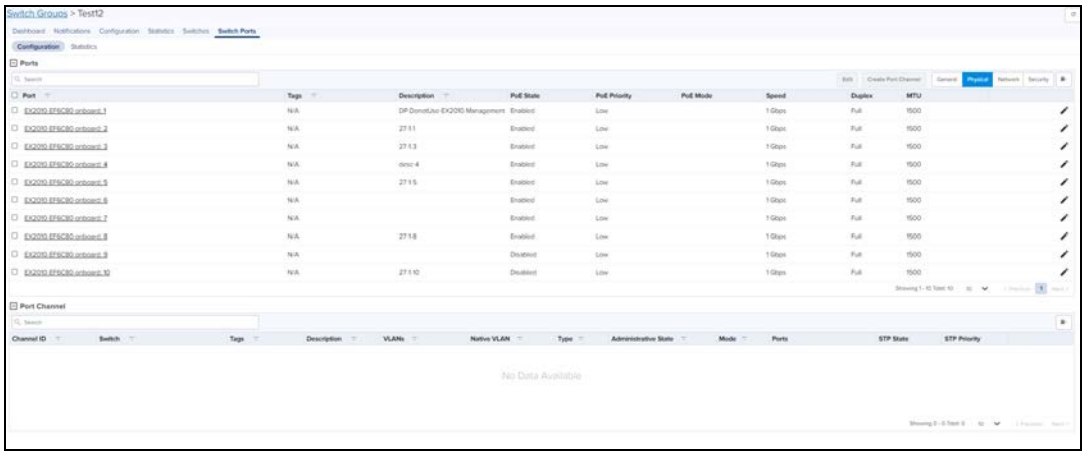


3. Enter the **Tags** and **Description** details.
4. Click **Save**.

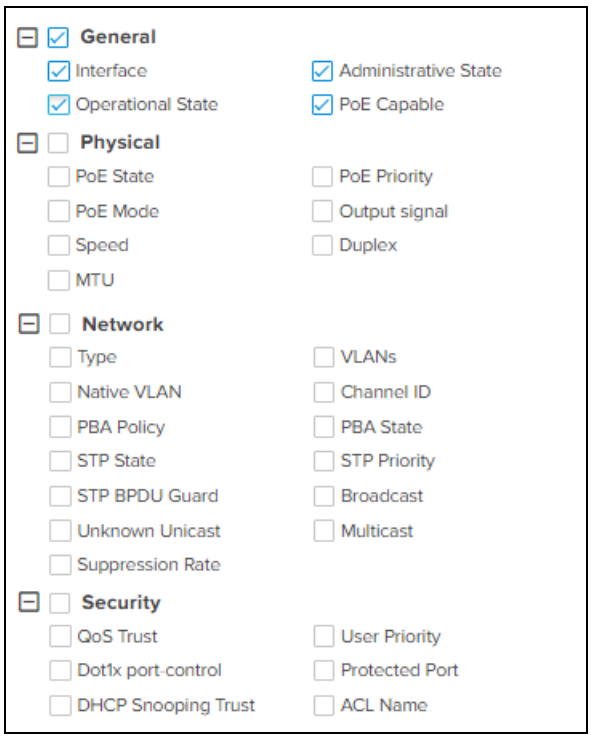
Physical Tab

The **Ports Physical** details view displays following fields by default:

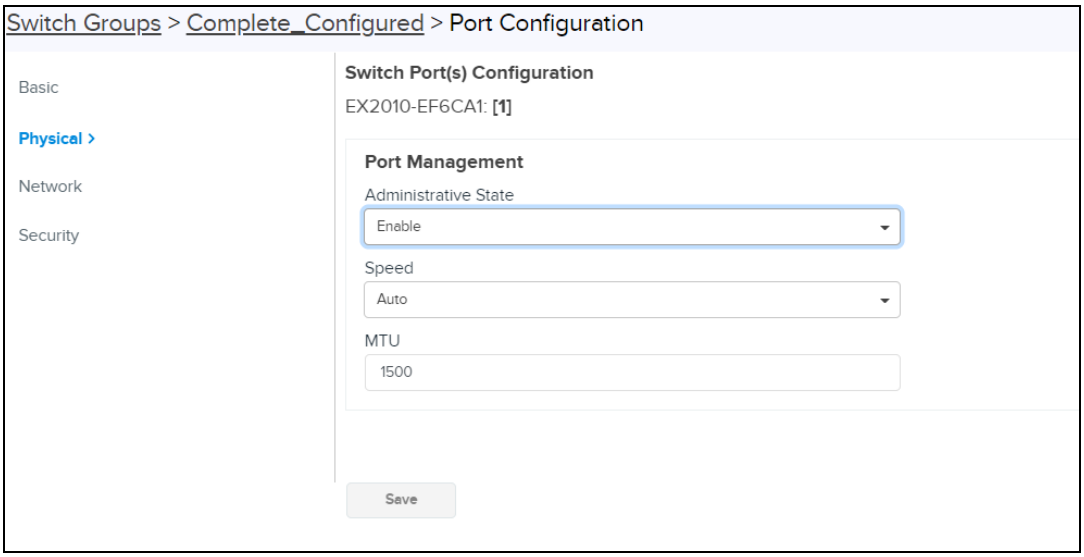
- Port, Tags, Operational State, PoE State, PoE Priority, Speed, Duplex, MTU, and Edit.



User can click on top bar to include additional fields in **Ports Physical** Detail view.



1. Click Edit icon or Port device in the list to edit the **Ports Configuration** Physical tab details.

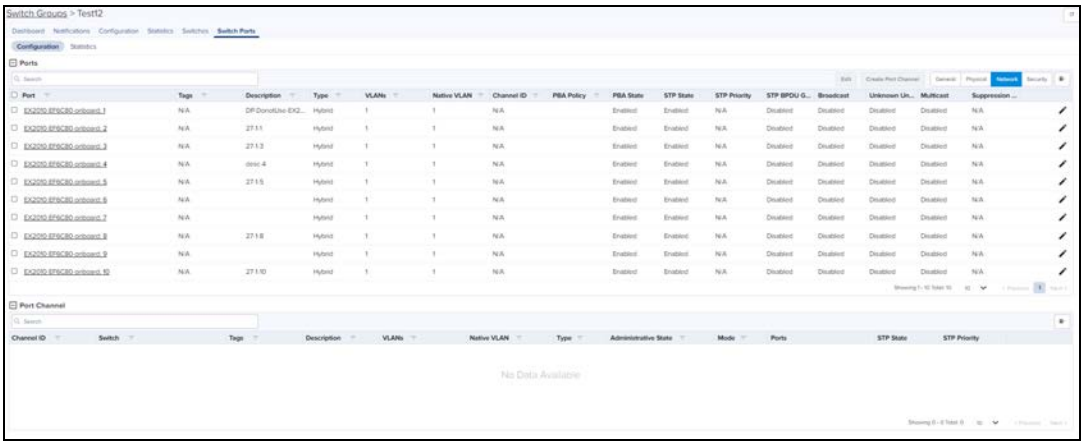


2. Enter the **Port Management** and **PoE** details.
3. Click **Save.**

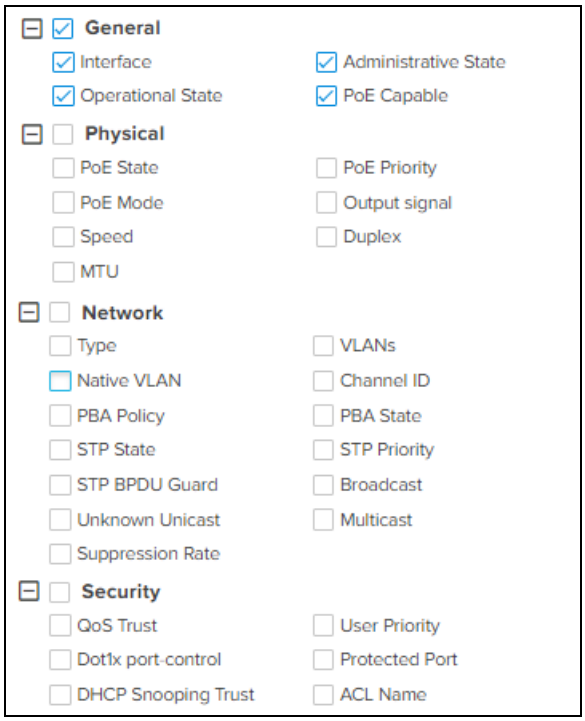
Network Tab

The **Ports Network** details view displays following fields by default:

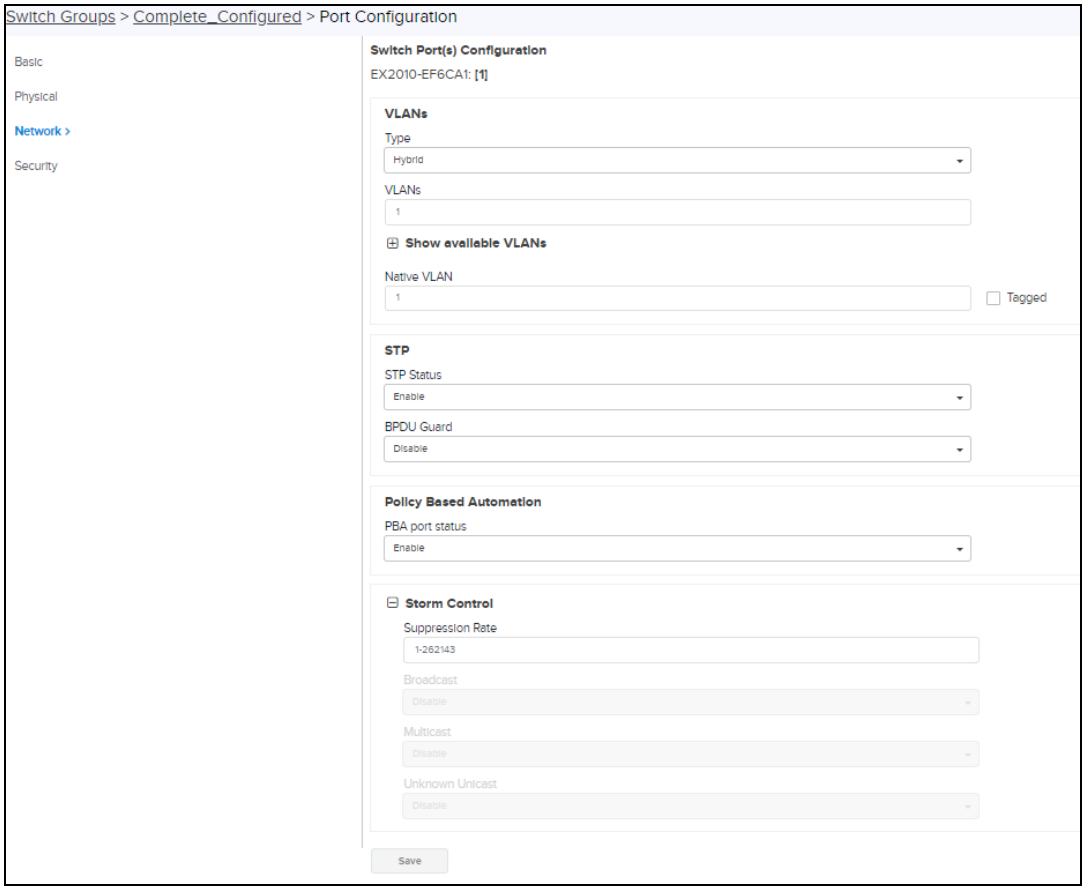
- Port, Tags, Type, VLANs, Native VLAN, Channel ID, PBA Policy, PBA State, STP State, STP Priority, and Edit.



User can click on top bar to include additional fields in **Ports Network** Detail view.



1. Click Edit icon or Port device in the list to edit the **Ports Configuration** Network tab details.

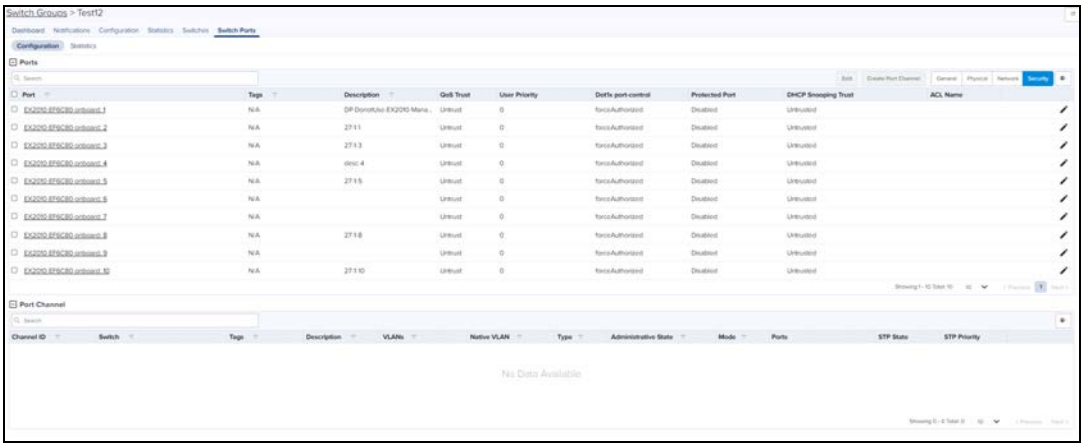


2. Enter **VLANs, STP, Policy Based Automation,** and **Strom Control** details.
3. Click **Save.**

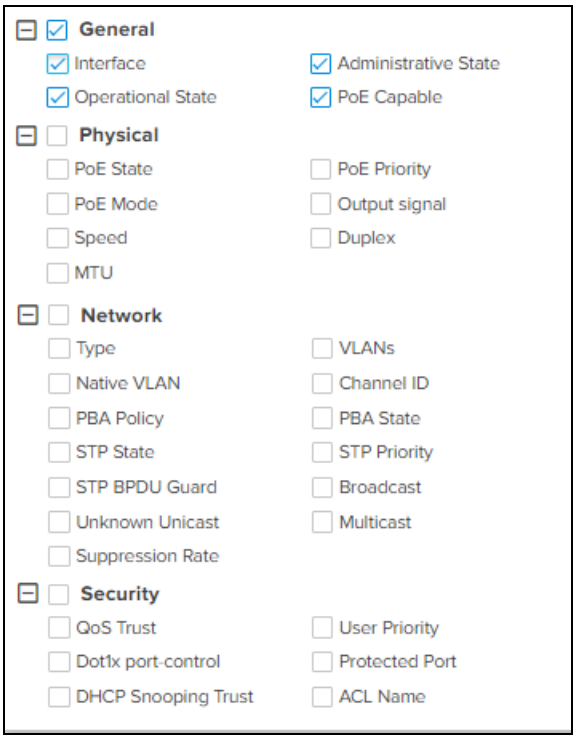
Security Tab

The **Ports Security** details view displays following fields by default:

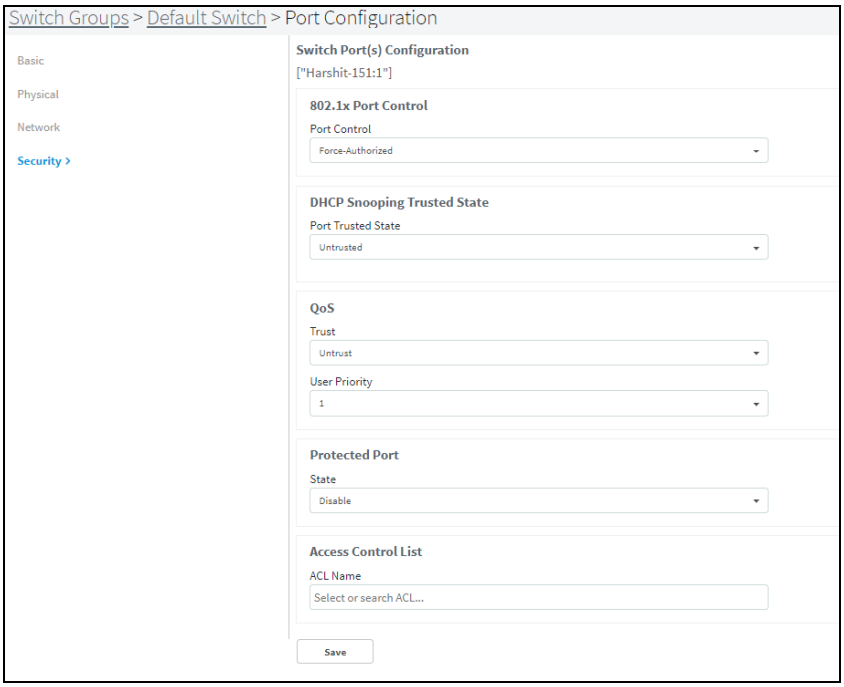
- Port, Tags, QoS Trust, User Priority, Dot1x port-control, Protected Port, DHCP Snooping Trust, ACL Name, and Edit.



User can click on top bar to include additional fields in **Ports** Network Detail view.



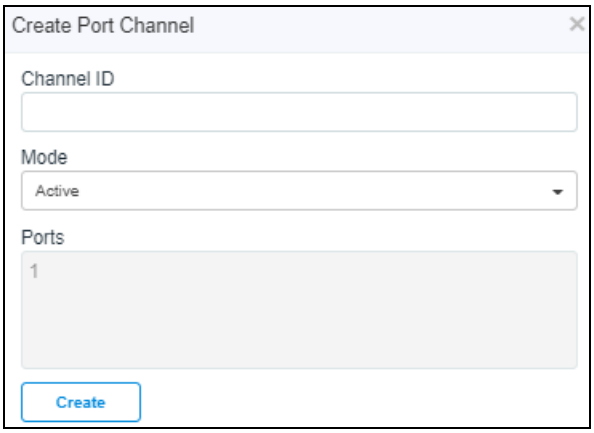
1. Click Edit icon or Port device in the list to edit the Ports Configuration Security tab details.



2. Enter **802.1xPort Control, DHCP Snooping Trusted State, QoS, Protected Port, Access Control List** details.
3. Click **Save.**

Port Channel

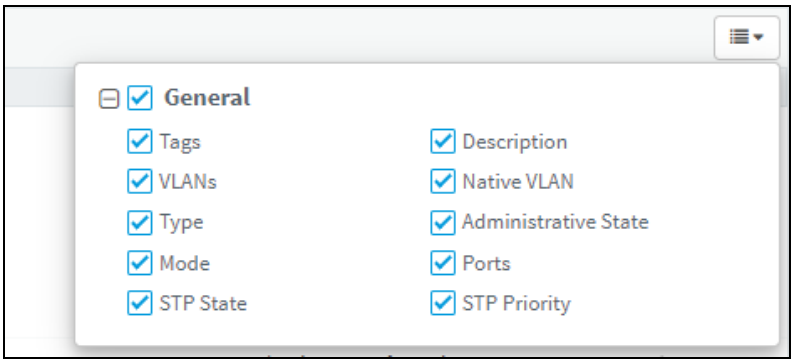
1. To create a Port Channel, select a **Port** from the list under the specific parameters and click **Create Port Channel**.
2. **Create Port Channel** window pops-up, enter details.
3. Click **Create**.



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.

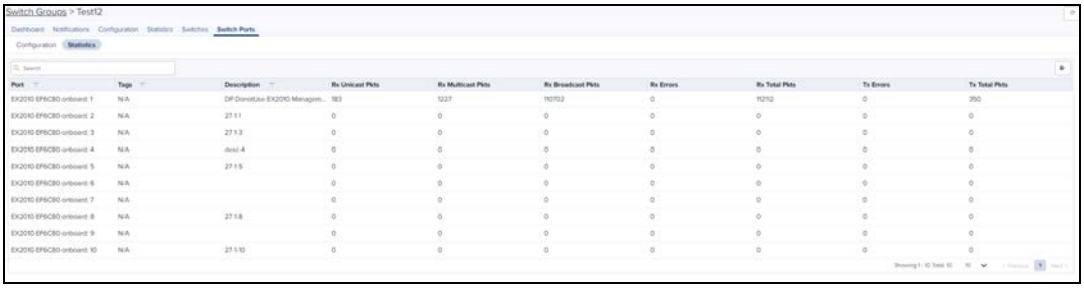
User can click on top bar to include additional fields in **Port Channel** Detail view.



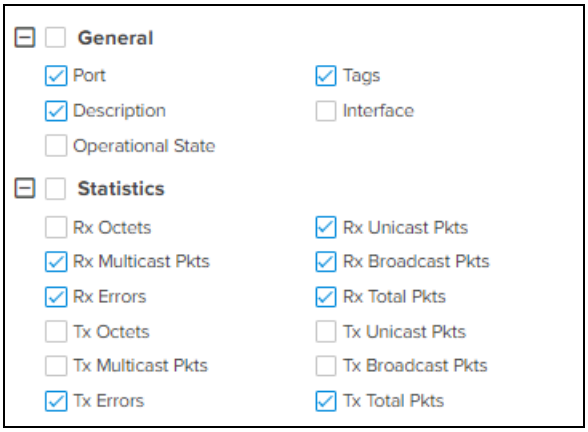
Statistics

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**.

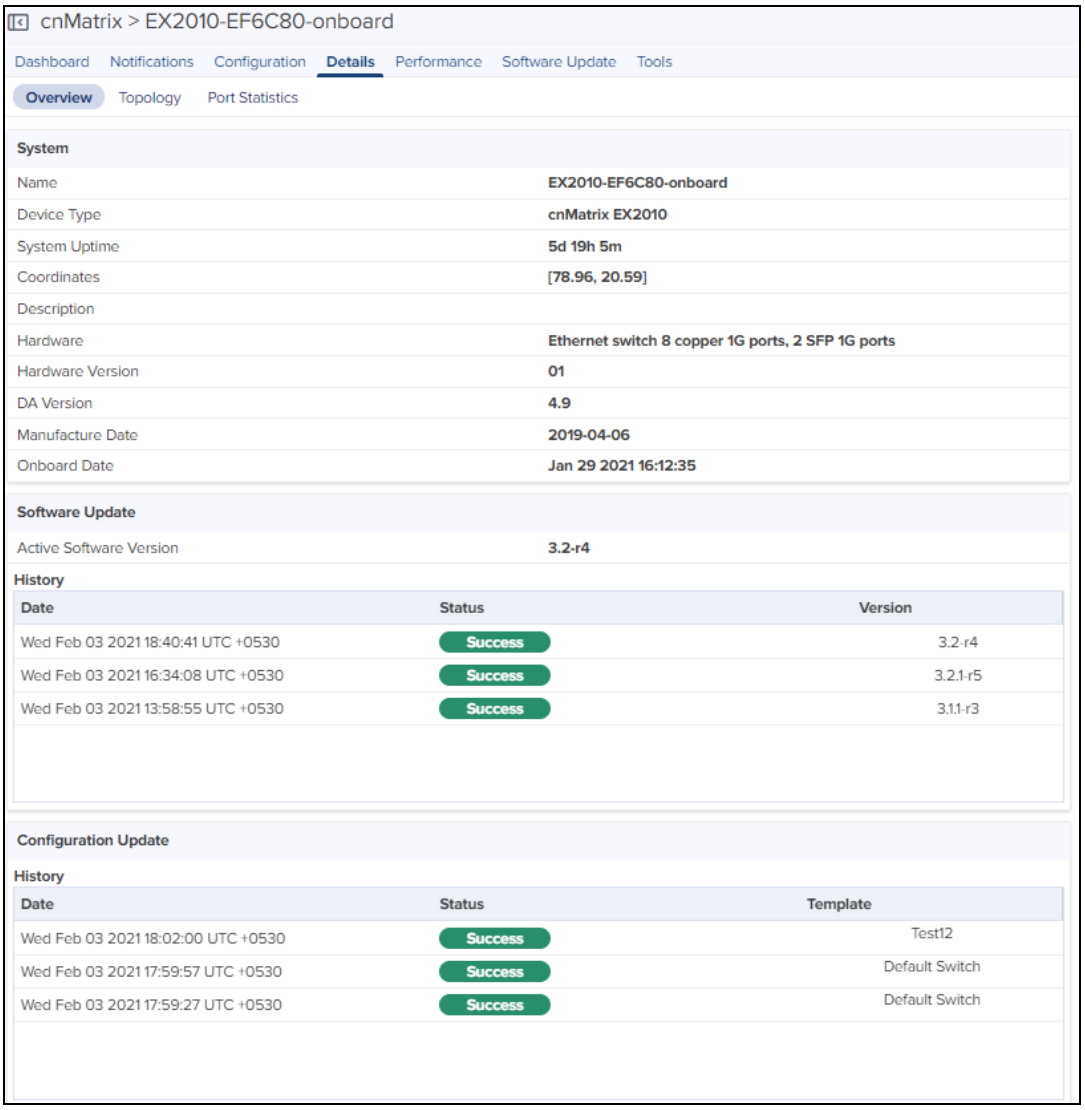


User can click on top bar to include additional fields in **Statistics** Detail view.



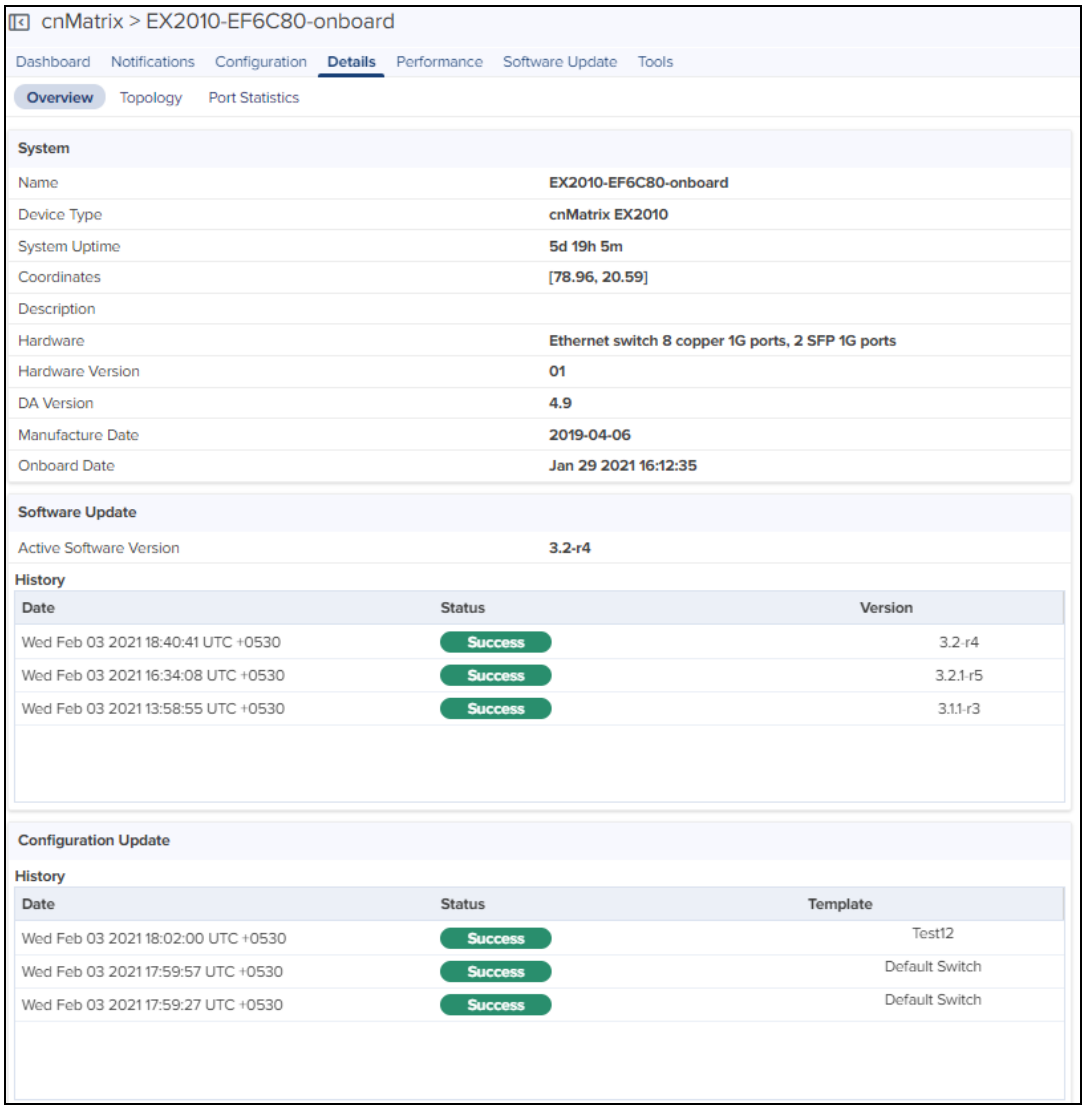
Device Details

Details page provide the information about the switches **Overview**, **Topology**, and **Port Statistics**.



Details Overview

To view the details of the overview page, navigate to the **Details > Overview** tab.

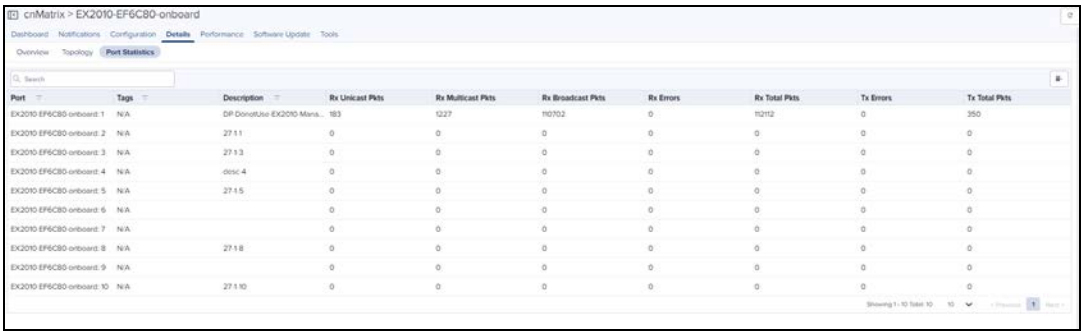


Topology

To view the details of the Topology page, navigate to the **Details > Topology** tab.

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 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
1
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.

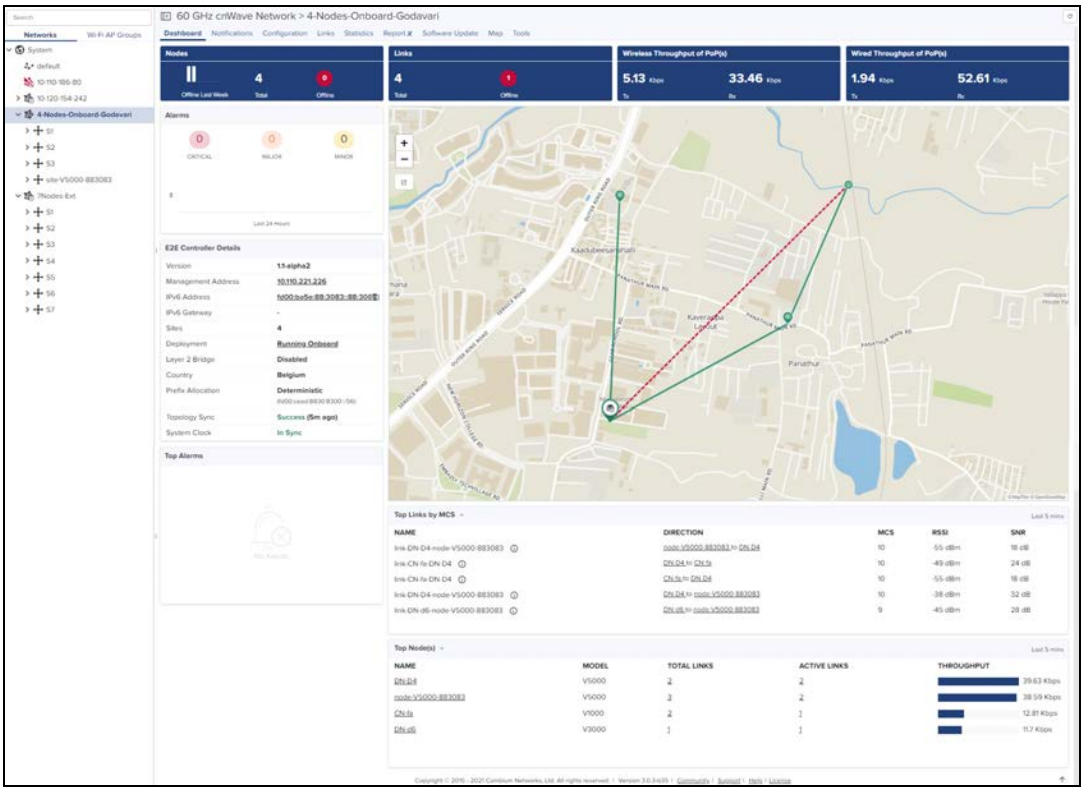
Managing E2E Network

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, 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).**



E2E Controller Details

E2E Controller Details displays the details such as **Version**, **Management Address, IPv6 Address, IPv6 Gateway, Sites, 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.**

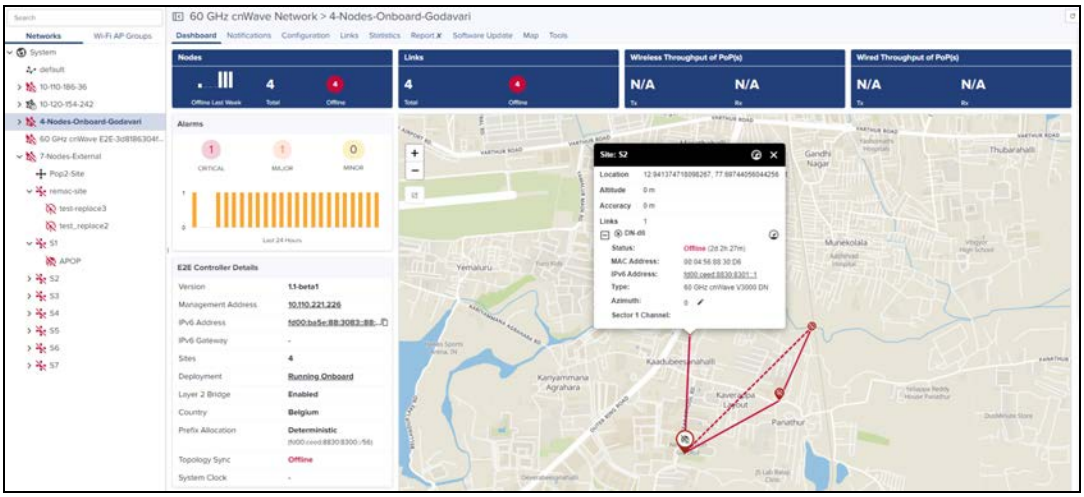
E2E Controller Details	
Version	**1.1-beta1**
Management Address	**10.110.221.226**
IPv6 Address	**fd00:ba5e:88:3083::88:..**
IPv6 Gateway	-
Sites	**4**
Deployment	**Running Onboard**
Layer 2 Bridge	**Enabled**
Country	**Belgium**
Prefix Allocation	**Deterministic** (fd00:ceed:8830:8300::/56)
Topology Sync	**Offline**
System Clock	-

- If External E2E controller is managed by cnMaestro, it displays deployment as **External.**

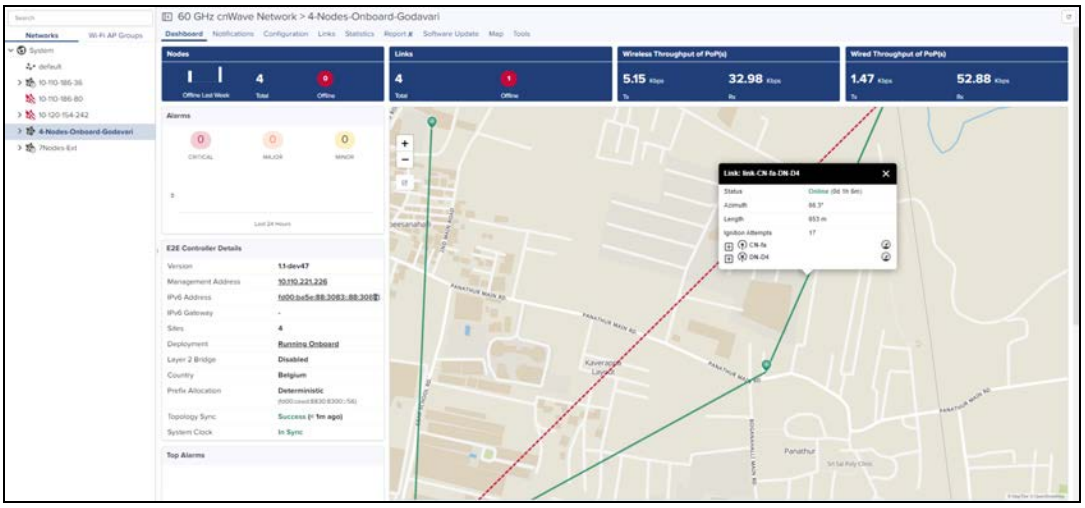
E2E Controller Details	
Version	**1.0.1**
Management Address	**10.110.178.37**
IPv6 Address	**2403:0:529:d:a00:27ff:f..**
IPv6 Gateway	**fe80::ce16:7eff:fe6e:5b7f**
Sites	**9**
Deployment	**External**
Layer 2 Bridge	**Disabled**
Country	**Austria**
Prefix Allocation	**Centralized** (fd00:ceed:1fd4:1300::/56)
Topology Sync	**Offline**
System Clock	-

Dashboard Maps

In the dashboard map, when user selects the particular **PoP, DN** or **CN** it pops-up the Node details. It also allows the user to navigates to the particular **Site** and **Node dashboard** by clicking the **Dashboard** icon in the pop-up.

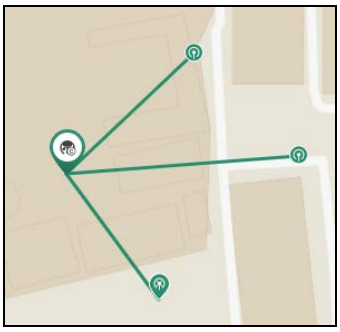


When user selects the particular link, the link details pops-up as shown below and it also allows the user to navigates to the particular **Site** and **Node dashboard** by clicking the **Dashboard** icon in the pop-up.

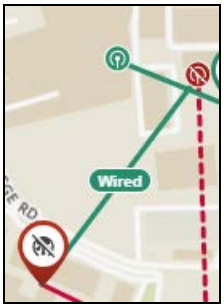


- Dotted line displays the Backup CN link between the DN and CN.

- Continuous line displays the link between the wireless network.



- Continuous line with **Wired** tag displays the link between the wired network.



To navigate to the Maps page click the Map view .

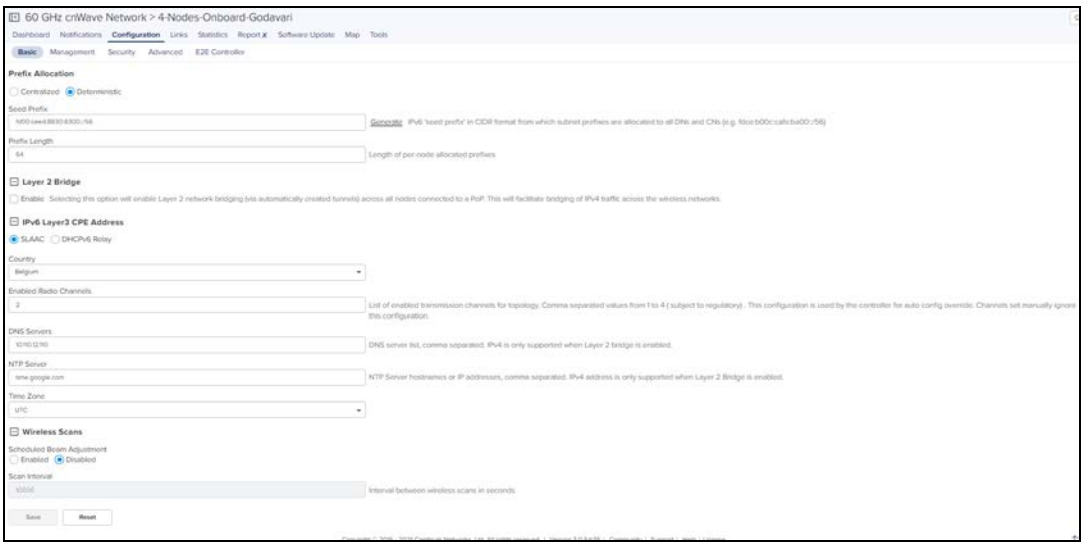
Notifications

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:

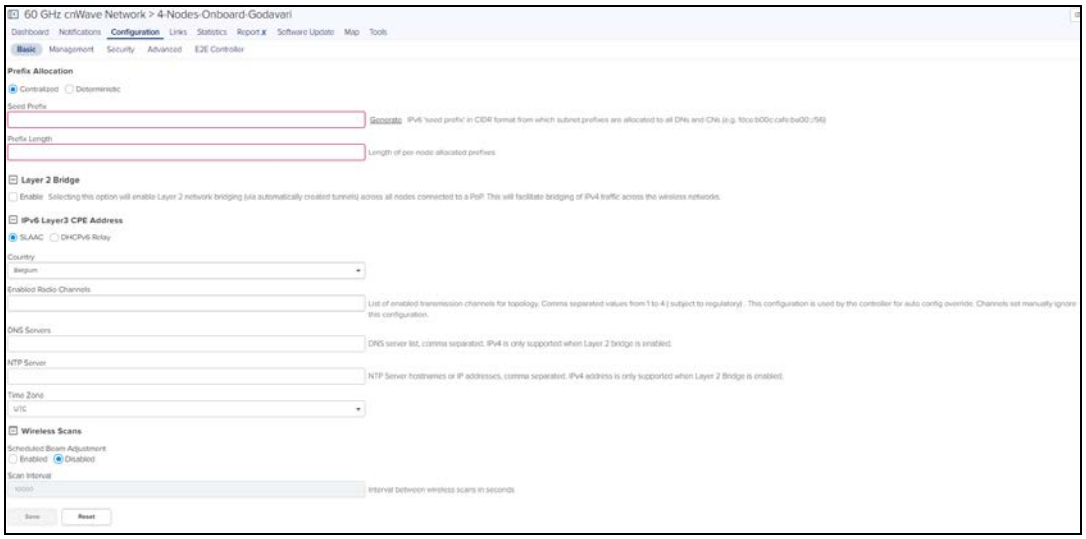
- Basic
- Management
- Security
- Advanced
- E2E Controller



NOTE:
Once user selects the **Auto-assign** IPv6 Addresses while configuring E2E Controller and PoP node. Uses the same IPv6 during the prefix allocation.

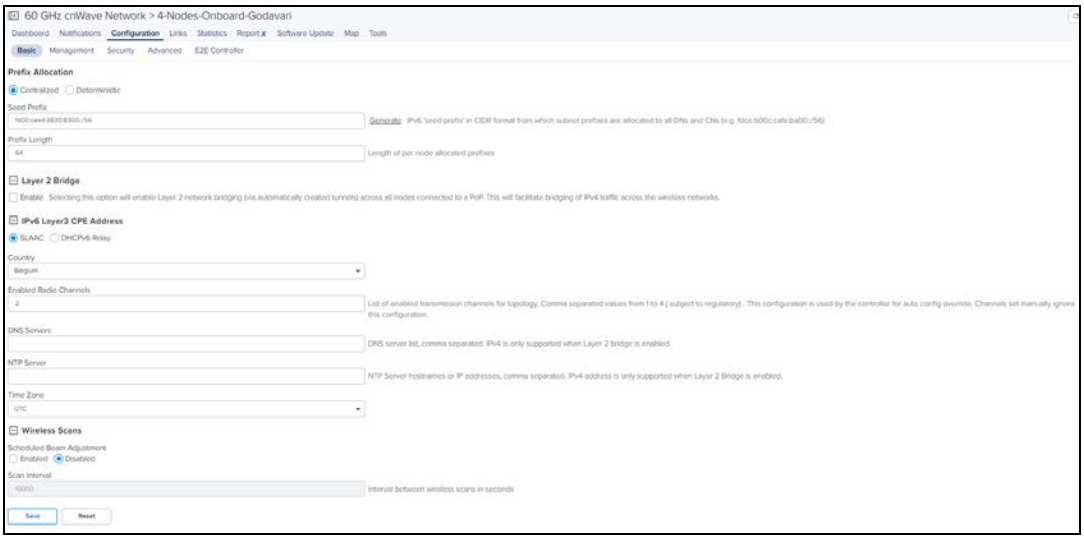
Basic Configuration

1. Navigate to **Configuration** > **Basic** to configure the **Prefix Allocation.**

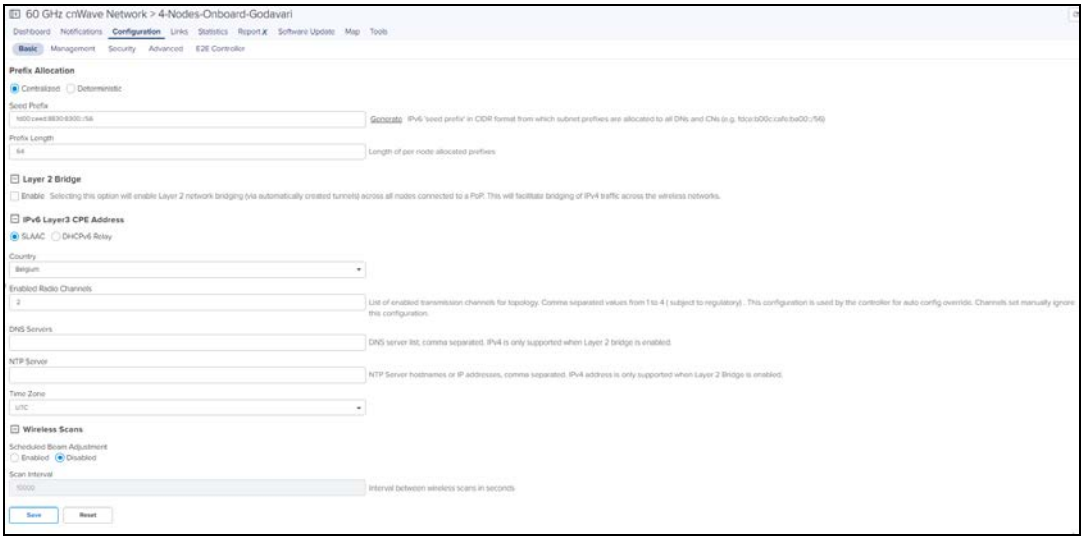


NOTE:
Prefix allocation automatically gets updated, when E2E Controller is managed by cnMaestro.

2. Select **Centralized** or **Deterministic** to allocate the IP for the nodes.



3. Enter the **Seed Prefix** and **Prefix Length**.

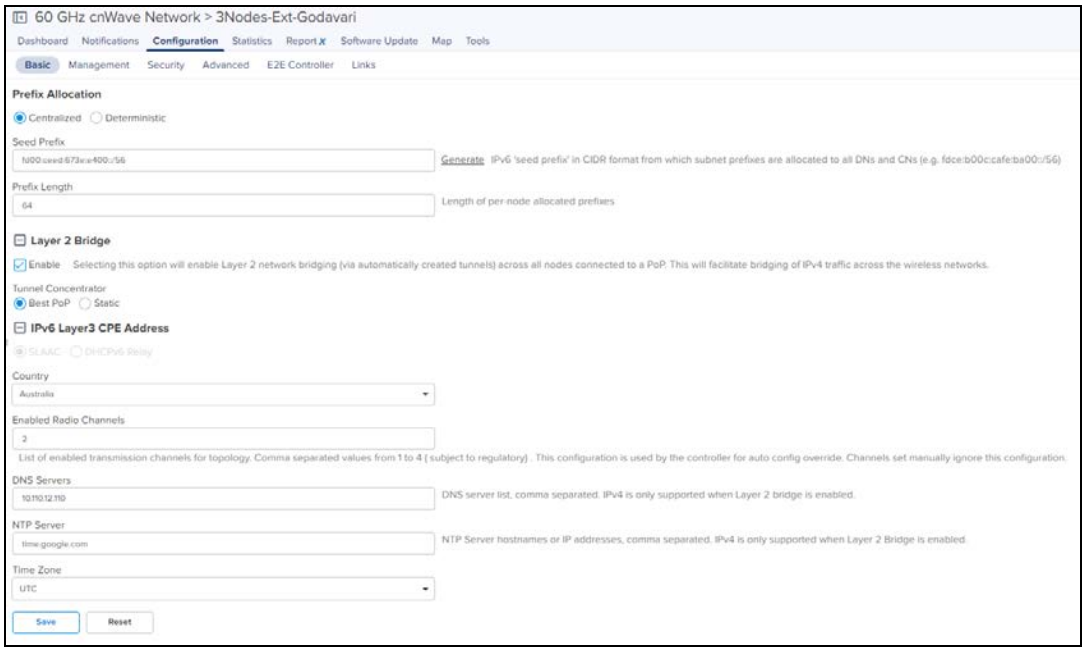


4. Enabling **Layer 2 Bridge** is optional.

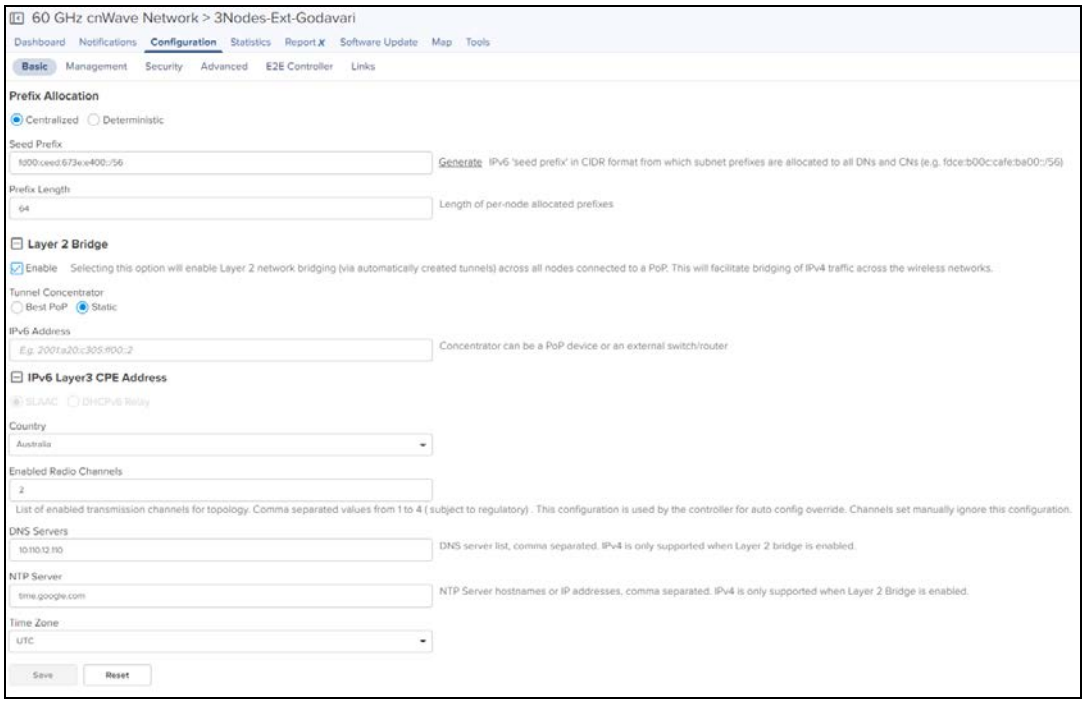
   Enabling this option will enable Layer 2 network bridging (via automatically created tunnels) connected across all nodes and facilitates bridging of IPv4 traffic across the wireless networks. It also enables the configuration of VLAN Management and Ports on all PoP, DN, and CN Nodes.

   If Layer 2 Bridge is enabled configure as shown below:

   - Select the **Tunnel Concentrator** as **Best PoP** or **Static.**



- If user selects **Tunnel Concentrator** as **Static.**
- Enter the Concentrator can be an external switch/router when static is selected.

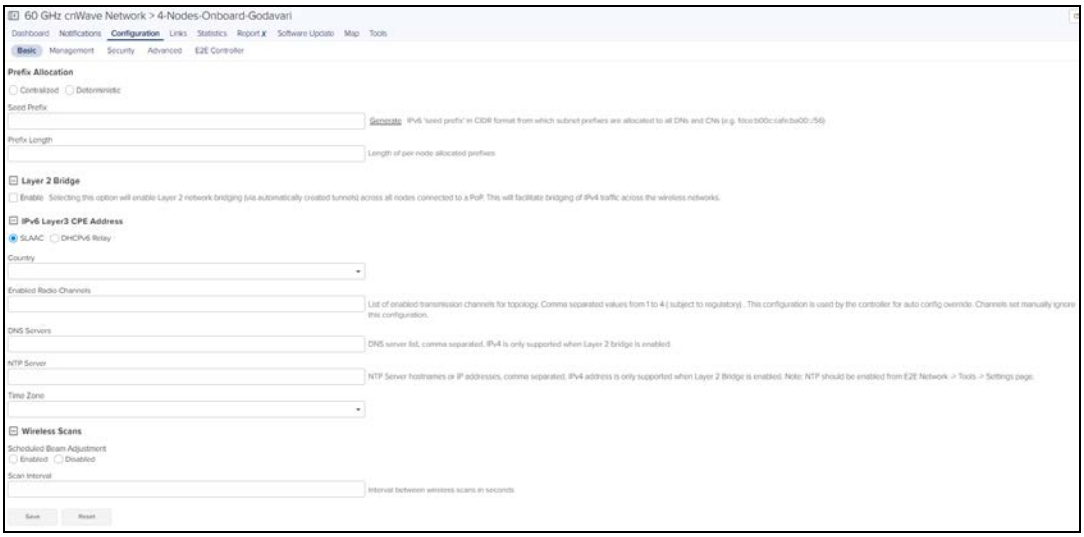


NOTE:

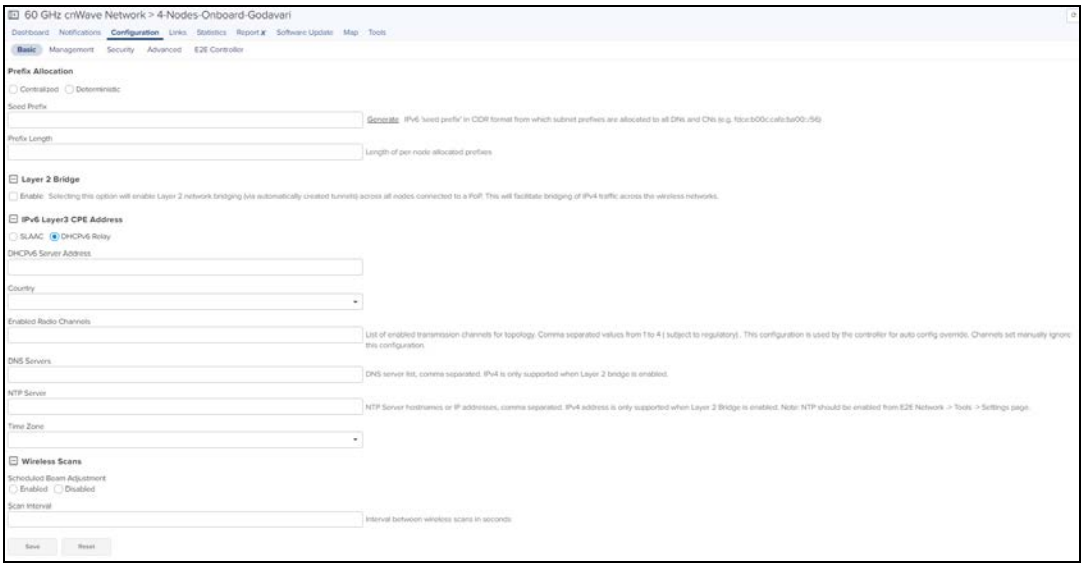
IPv6 Layer3 CPE Address can be enabled when E2E Controller is running 1.1 verison and Layer 2 Bridge is disabled.

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.



- If user selects **IPv6 Layer3 CPE Address** as **DHCPv6 Relay.**
  User can configure the DHCPv6 server address.



NOTE:

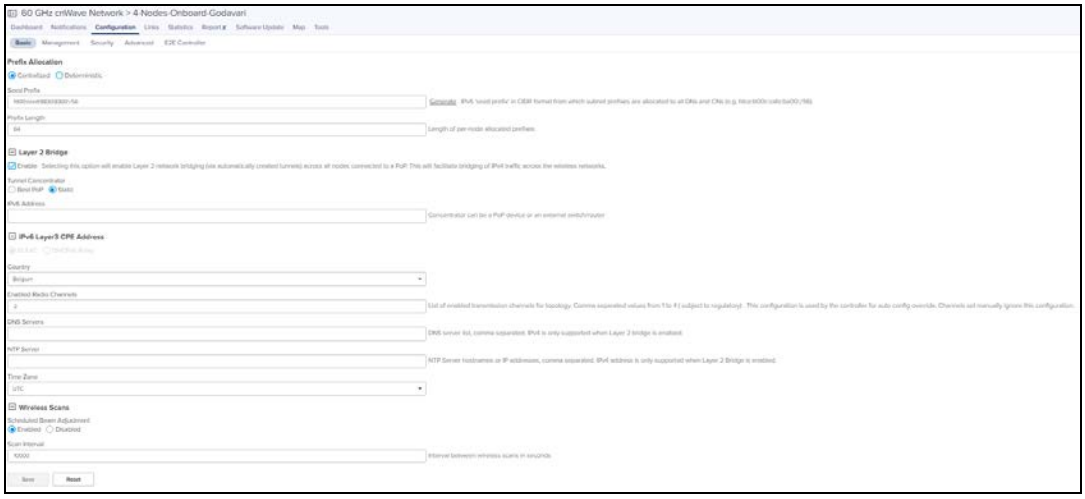
- By default **Country** is **Other**, user can configure it.
- By default **Enabled Radio Channels** is 2, user can configure channel if required.
- Enter the **Hostnames** or **IP address** of NTP server

6. Select the Country from the drop-down.
7. Enter the channel number in **Enable Radio Channels** and **DNS Servers.**
8. Enter **NTP Server.**
9. Select the **Time Zone** from the drop-down.

NOTE:

By default **Wireless Scans** will be disabled.

10. In **Wireless Scans** enable the **Scheduled Beam Adjustment**.

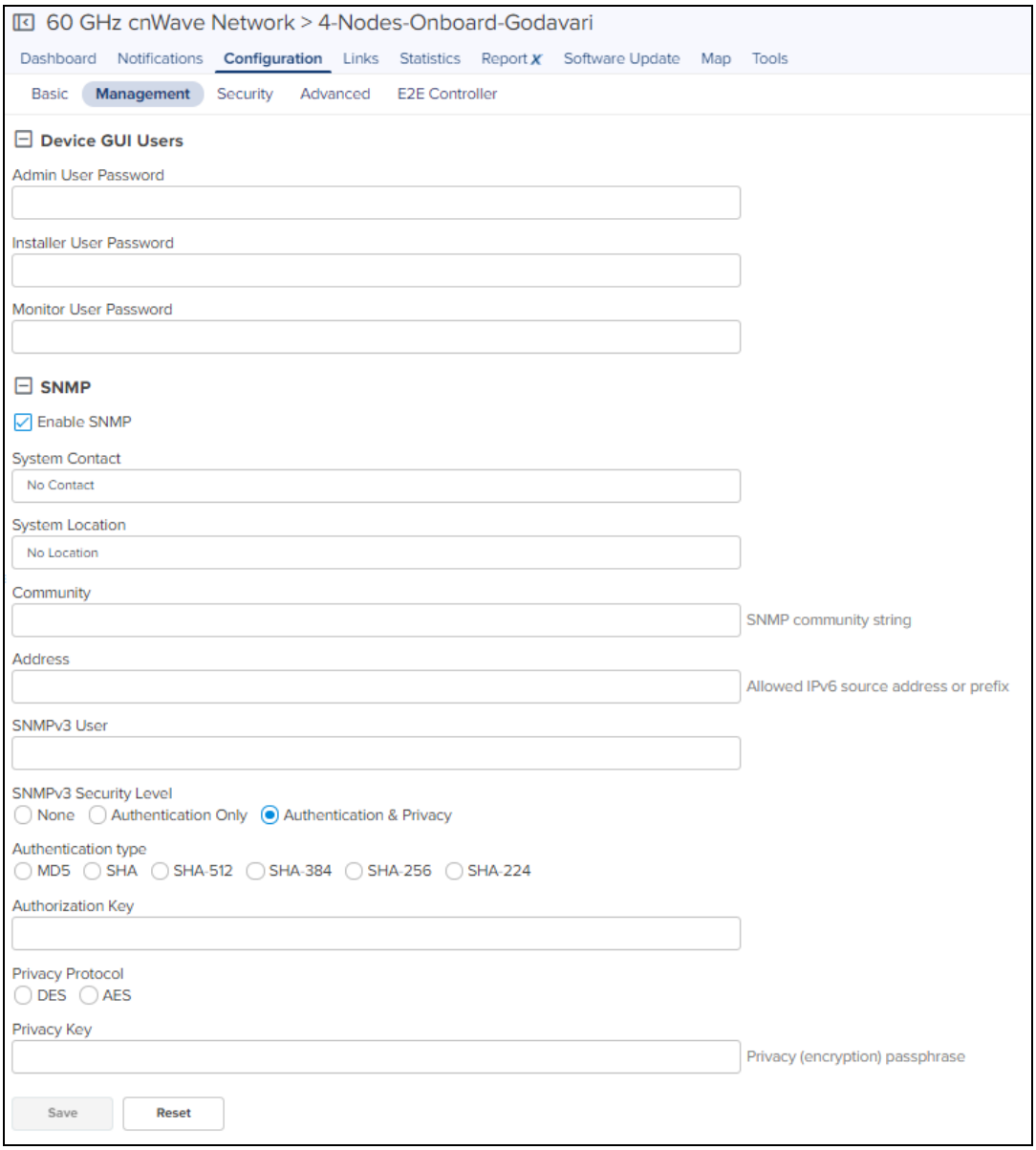


11. Click **Save.**

Management

Management configuration allows user to configure and manage the credentials of the administrator and it allows enable **SNMP**.

1. Navigate to **Configuration** > **Management** to set the **Device GUI Passwords** and to enable the **SNMP**.



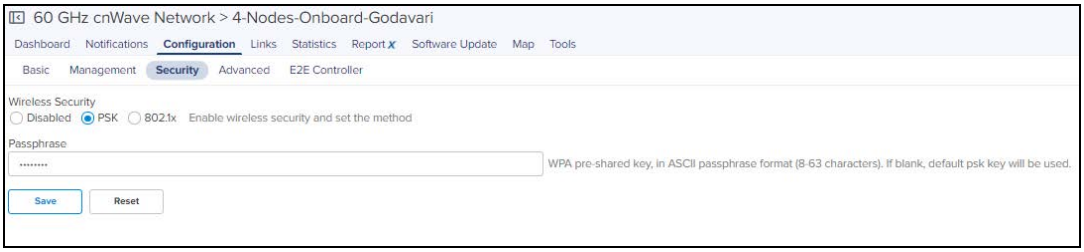
2. Click **Save.**

Security

Security page allows the user to enable the wireless security **PSK** or **802.1x.** Disabling option unscure the devices.

To Enable PSK :

1. Navigate to **Configuration** > **Security** tab.
2. Select **PSK** in **Wireless Security**.



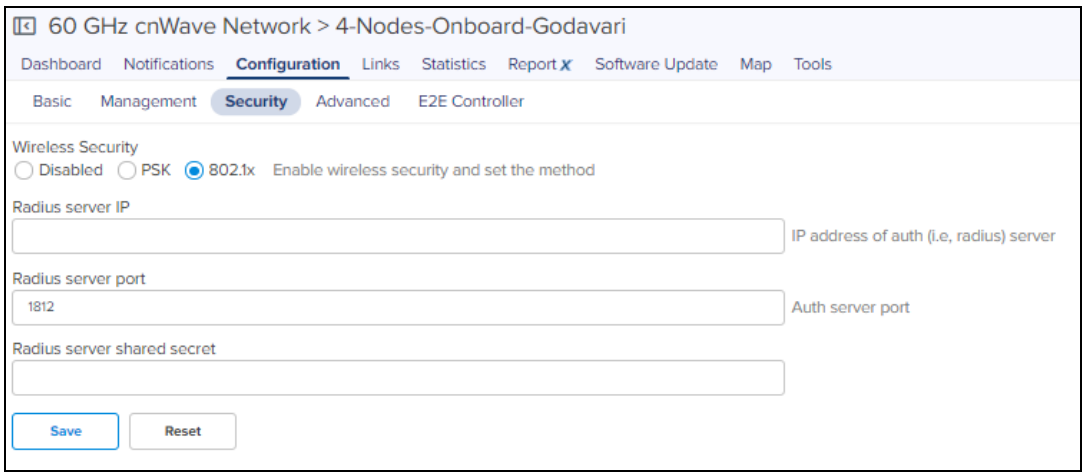
3. Enter the **Passphrase**.

> **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**.

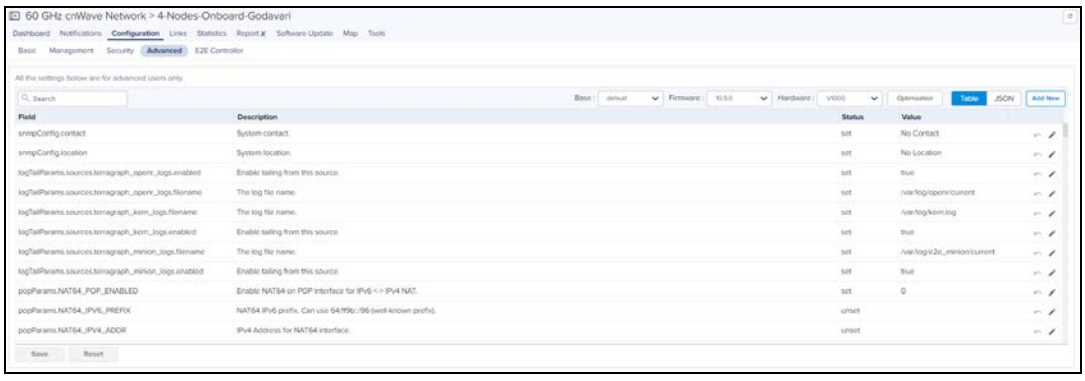


3. Enter the **Radius server IP.**
4. Enter the **Radius Server port.**
5. Enter the **Radius Server Shared Secret.**
6. Click **Save**.

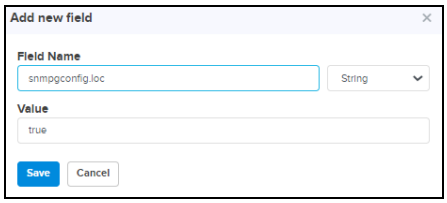
Advanced

Advanced tab allows the advanced user to set **Field Name** and **Value**.

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**

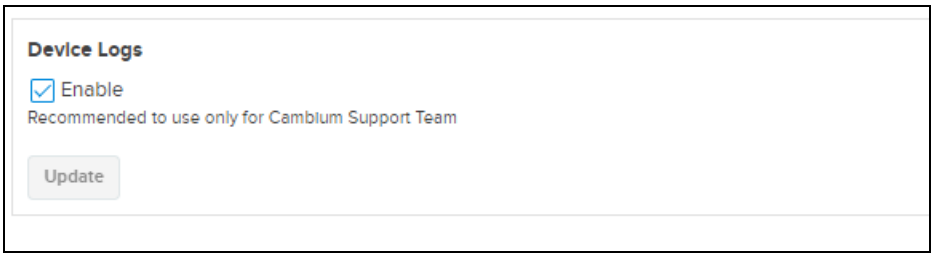


3. Enter the **Field Name** and **Value.**



4. Click **Save.**

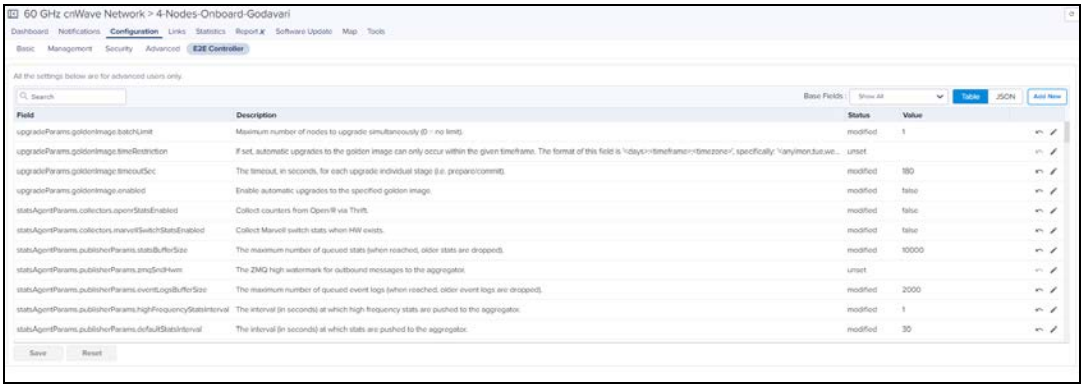
To Enable the Device logs, navigate to **Configuration** > **Advanced** > select **Enable** Device logs.



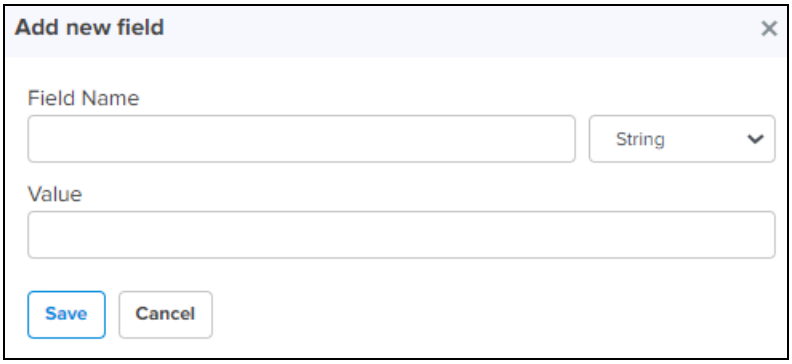
E2E Controller

E2E Controller allows the advanced user to add **Field Name** and **Value.**

1. Navigate to **Configuration** > **E2E Controller.**
2. Click **Add New.**



3. Enter the **Field Name** and **Value.**



4. Click **Save.**

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 and wired link.

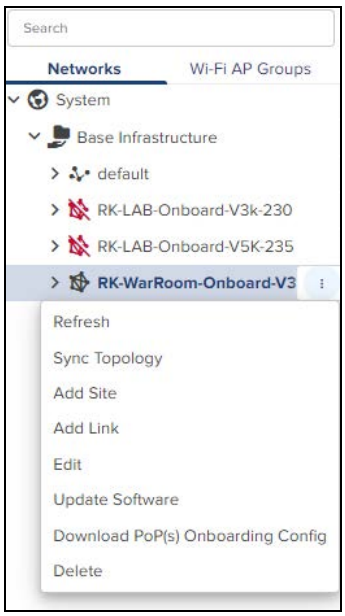
- List
- Statistics

- Events

List

To add a link:

1. Navigate to the E2E Network tree menu click ⋮ icon and click **Add Link** from the drop-down or navigate to **Network > Links > List > Add New**.



2. **Add Link** window pops-up.
3. Select **Link Type** Wireless or Wired.

Figure 93 Wireless

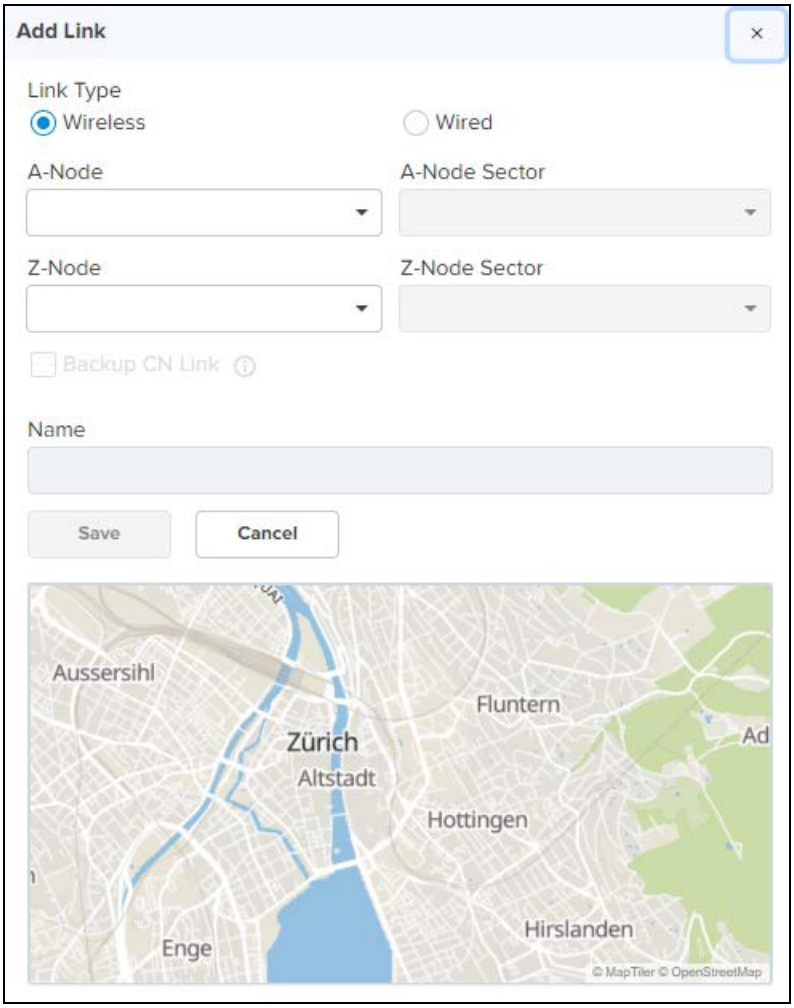
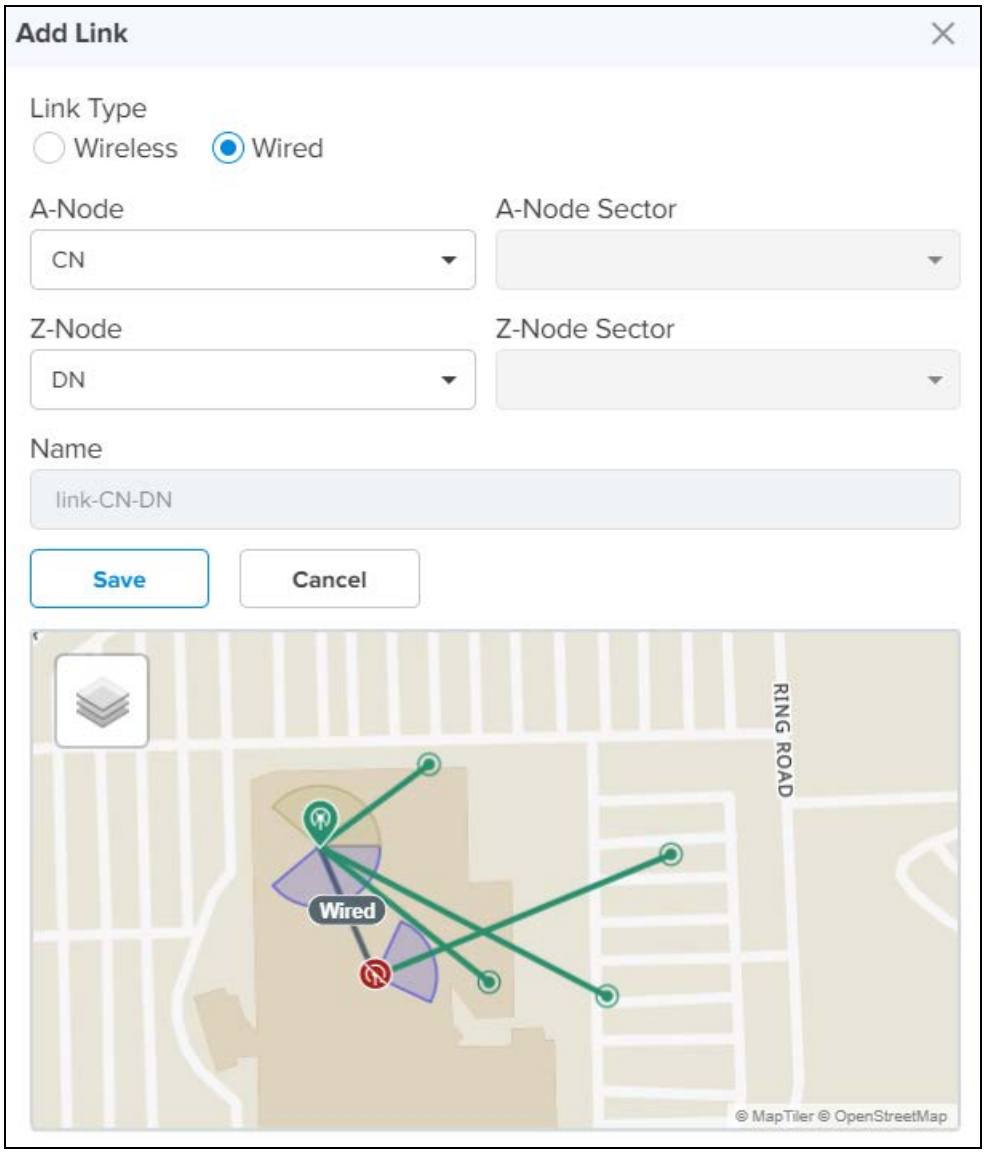
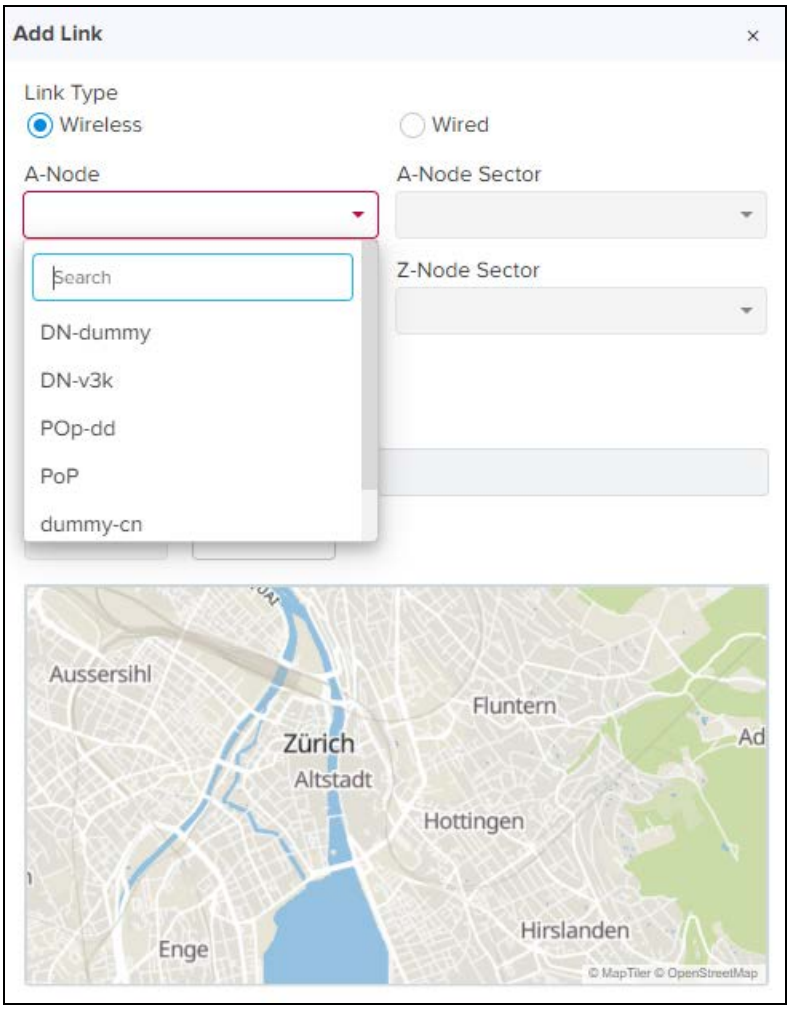


Figure 94 Wired

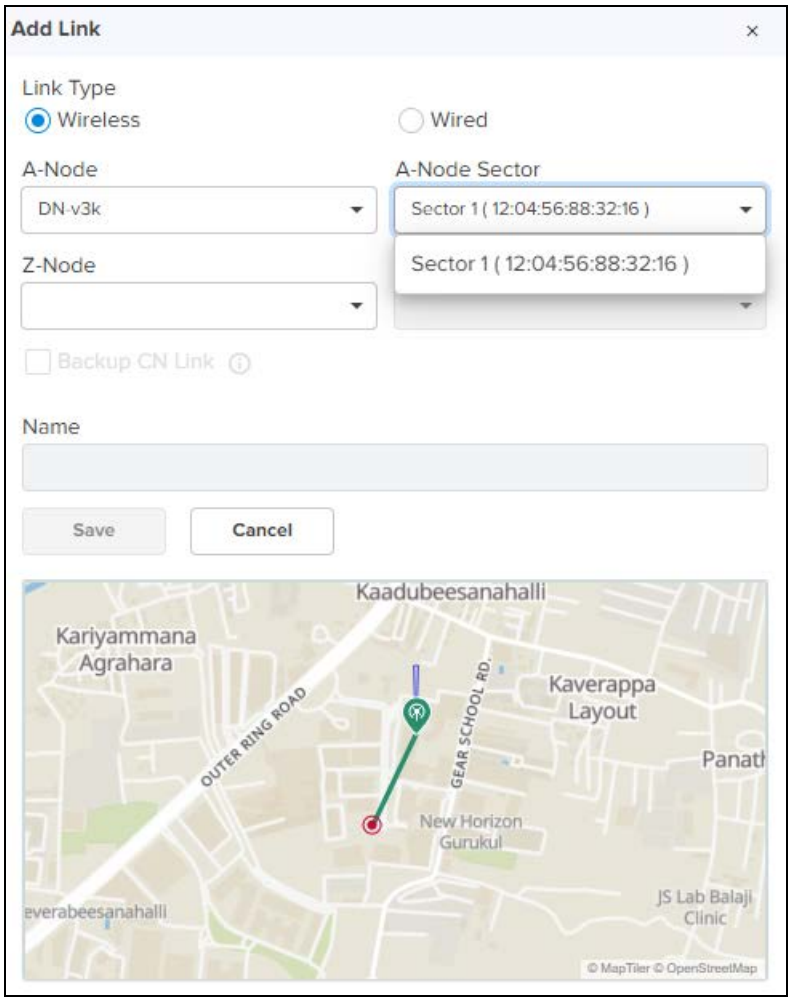
	NOTE: In Wired Link Type Sector will be disabled



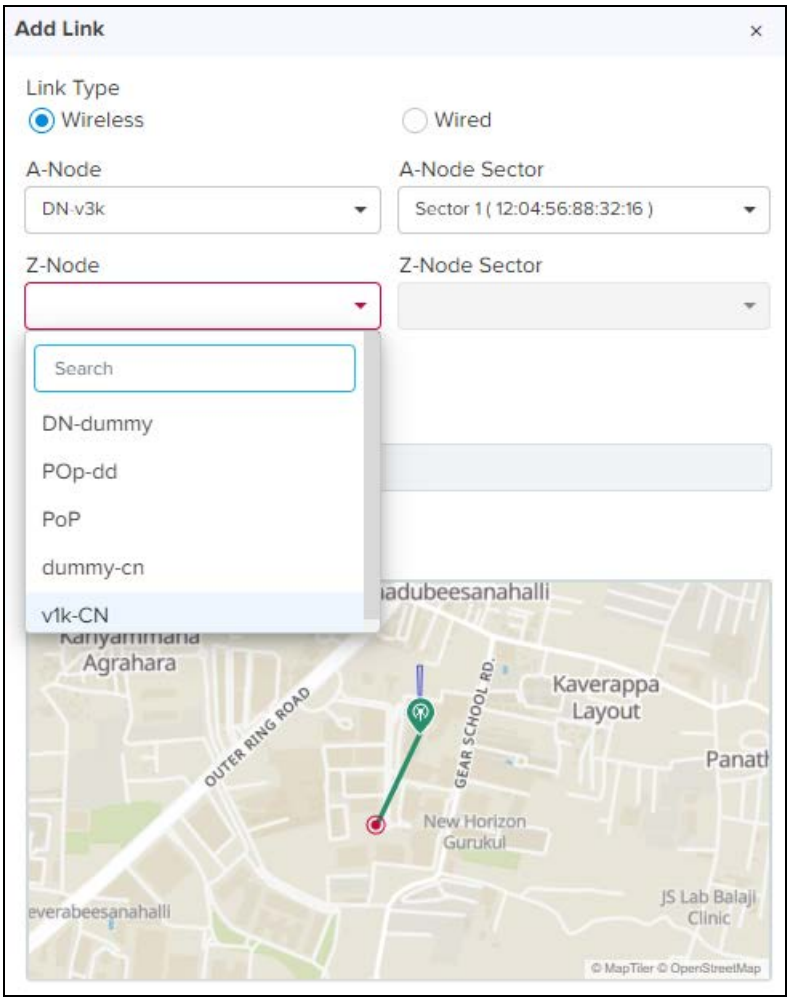
4. Select the **Node** from the drop-down in **A-Node.**



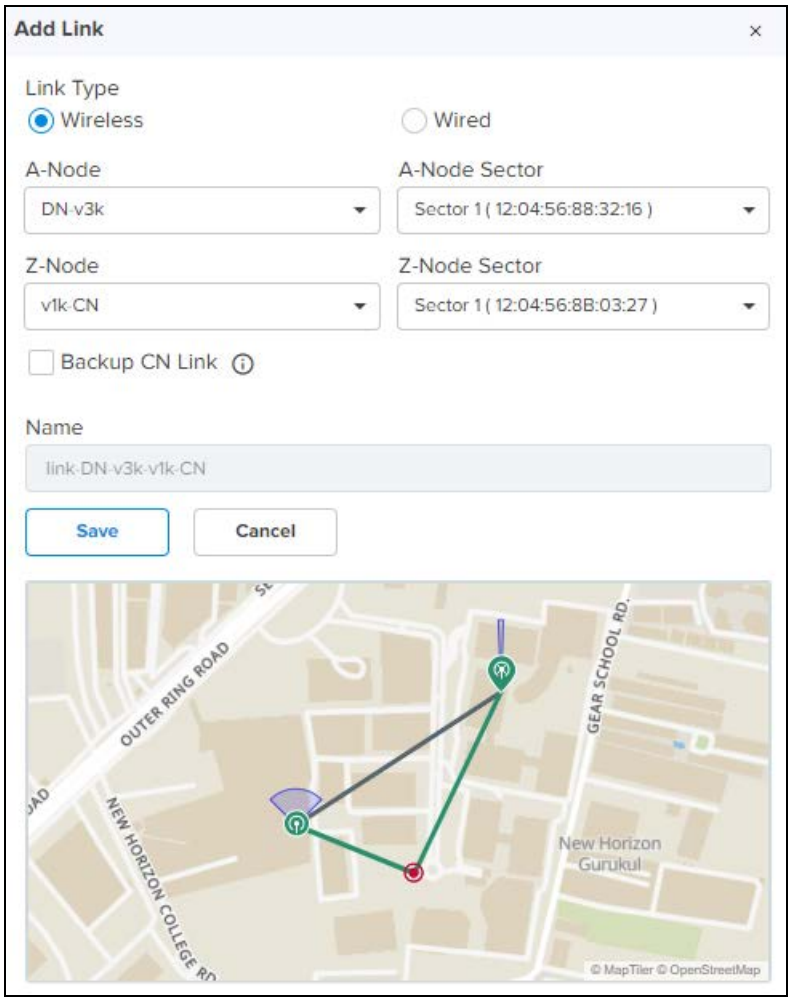
5. Select the **Sector** of the node from the drop-down in **A-Node Sector.**



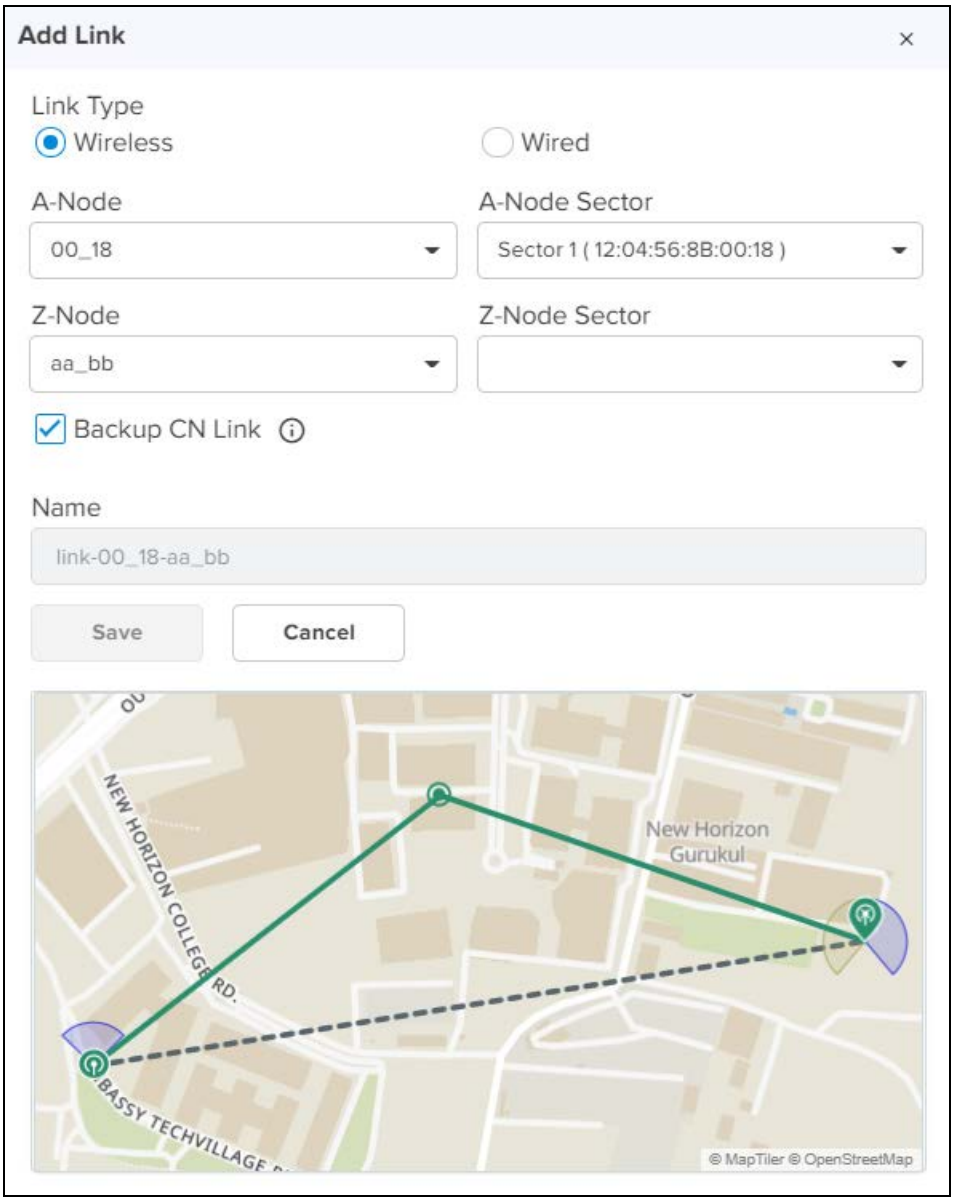
6. Select the **Node** from the drop-down in **Z-Node.**



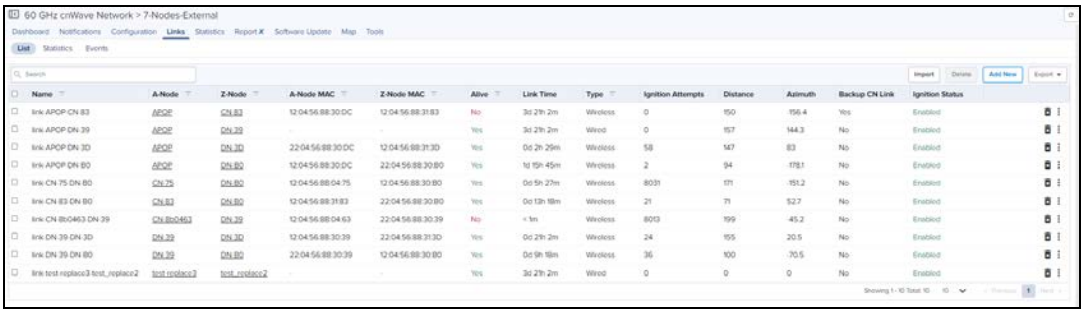
7. Select the **Sector** of the node from the drop-down in **Z-Node Sector.**



8. Enable the **Backup CN Link**.
   - If the link between PoP or DN and CN gets disconnected. This Backup CN link provides the backup connectivity from DN or PoP to particular CN.



9. Click **Save**.
10. Once the link is successful it displays the **Alive** status as **yes**.



Available link options are:

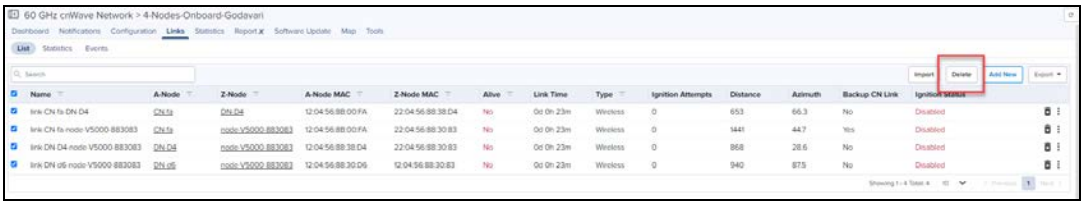
- Send Assoc to A-Node
- Send Assoc to Z-Node
- Send Dissoc to A-Node
- Send Dissoc to Z-Node

- Enable Ignition
- Disable Ignition

Delete Links

To delete the links :

1. Navigate to **Links** > **List** > select the links.

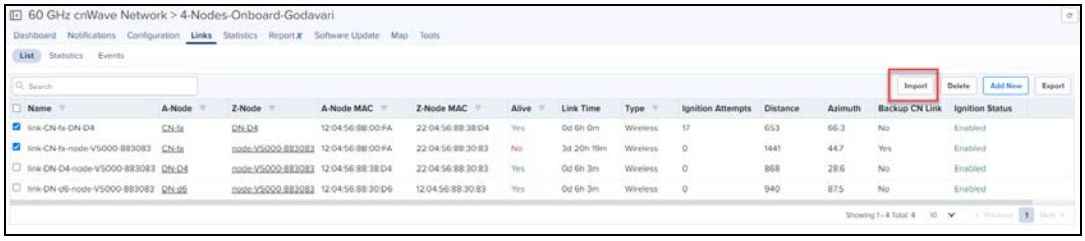


2. Click **Delete**.

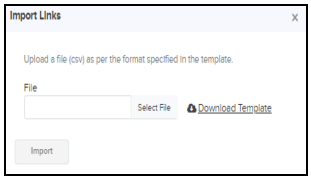
Import List

To import the links :

1. Navigate to **Links > List >** select **Import.**



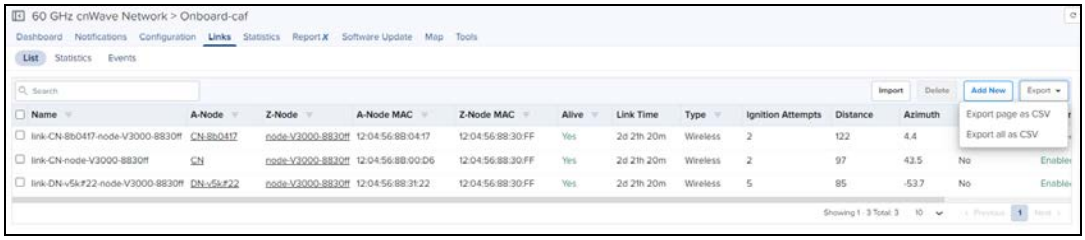
2. Import Links window pops-up select the file and click **Import**.



Export List

To export the links :

1. Navigate to **Links** > **List** > select **Export.**

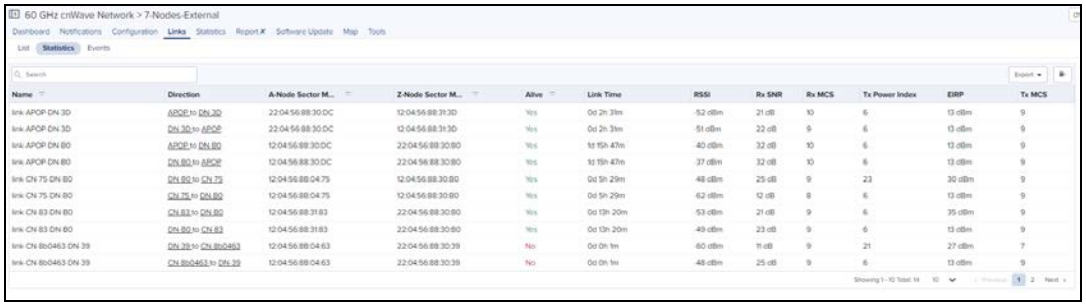


2. It exports .csv file format as shown below.

	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 tl	Sector 1/2 MAC	Wireless or Wired
3	CN-2c	12:04:56:8B:00:2	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	22:04:56:88:30:6	dn-44	12:04:56:88:31:	Wireless
8	DN2	22:04:56:88:30:6	v3000	12:04:56:88:30:	Wireless
9	dn-44	22:04:56:88:31:4	pop	12:04:56:AA:BB	Wireless

Statistics

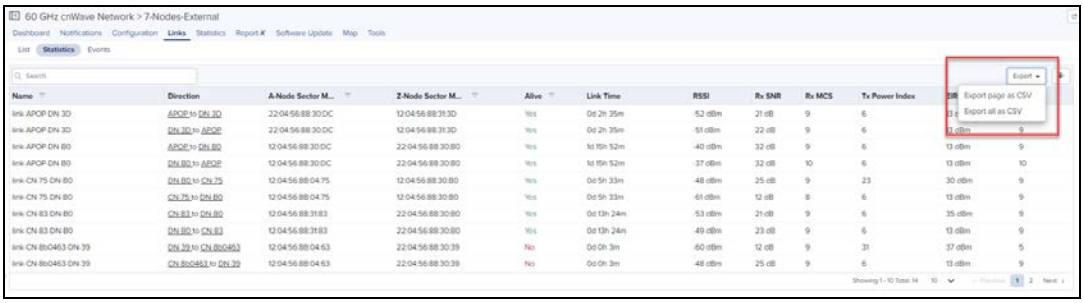
Links Statistics pages provides details of **Name, Direction, A-Node Sector MAC, Z-Node Sector MAC, Alive, Link Time, RSSI, Tx Power Index, A-node, Z-node, Type, Distance, Azimuth, Rx MCS, Tx MCS, Rx PER, Tx PER, Rx SNR, Rx Beam Index, Tx Beam Index, EIRP, Rx Errors, Tx Errors, Rx Frames, Tx Frames** on a single device, generally in a page format.



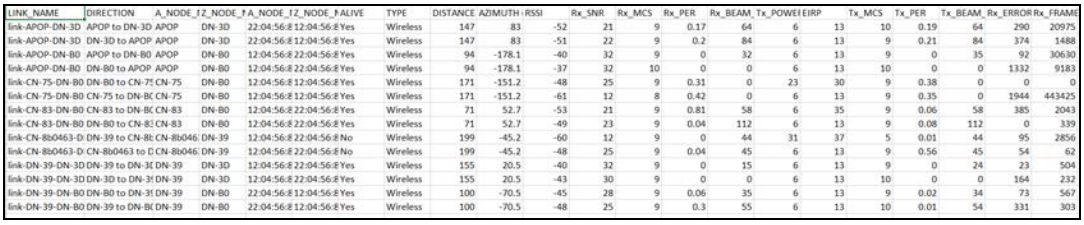
Export Statistics

To export the Statistics :

1. Navigate to **Links > List >** > select **Export.**



2. It exports .csv file format as shown below.



Events

Events provides the details of the links from last 1 hour to 7 Days, Ignition Attempts and Distance.

Figure 95 Links Availability

It also calculates the Availability percentage per link, including the duration when E2E Controller was offline in cnMaestro.

Statistics

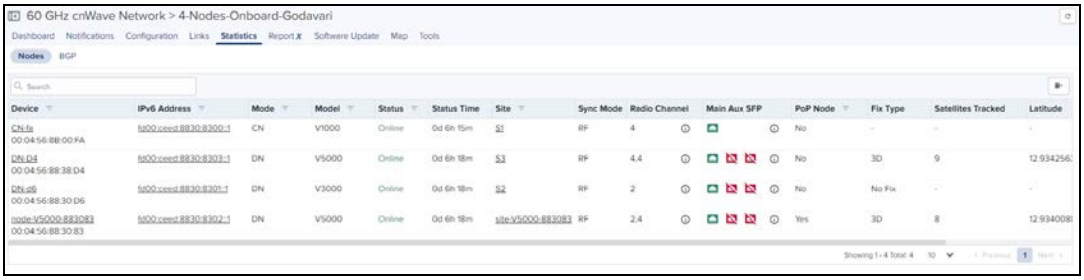
E2E Controller Statistics provides the following details:

- Nodes
- BGP

Nodes Statistics

Nodes provide a tabular aggregation of data, including General information on the devices 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 and allows to export **Nodes Statistics.**

Figure 96 Nodes Statistics

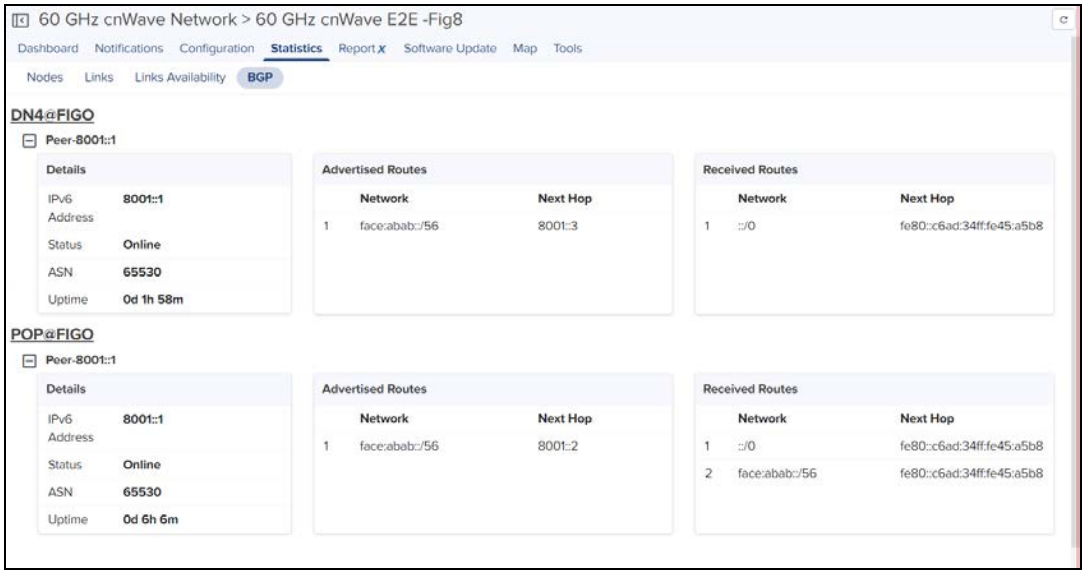


BGP

> **NOTE:**
>
> BGP statistics displays only if BGP option is enabled in Routing in PoP configuration.

BGP provides the details of **Advertised Routes, Received Routes,** and **Details of IPv6 Address.**

Figure 97 BGP



Reports

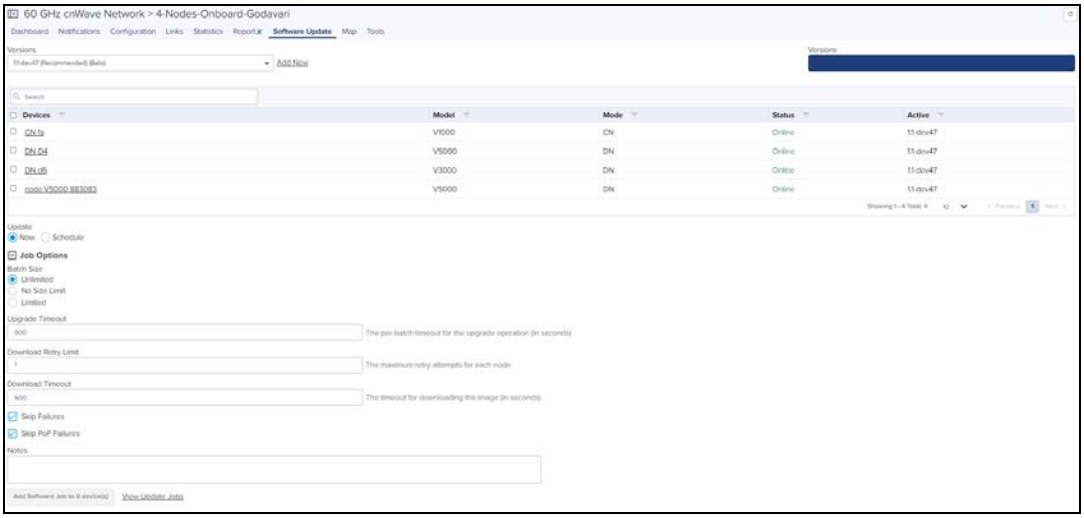
Reports page provides details on how to schedule and generate different types of data reports such as Devices, Active Alarms, Alarm History and Events. For further details refer to Reports.

Software Update

Allows the user to update with the latest device software.

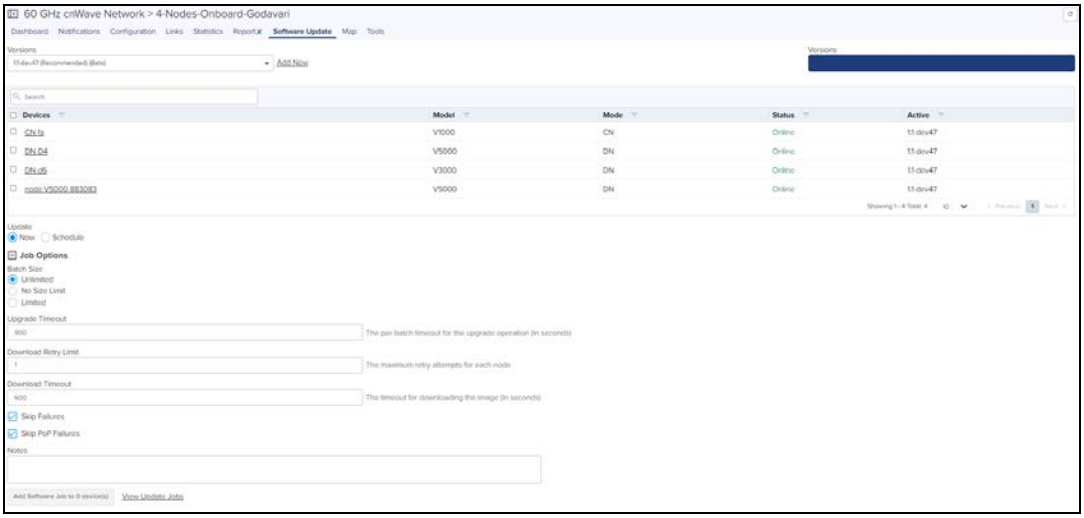
To update the software:

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**.
4. Click **Add Software Job to device.**



NOTE:
Onboard E2E controller will support only one synced image. If user needs to sync another image, select the image from Versions drop down and click **Sync Image.**

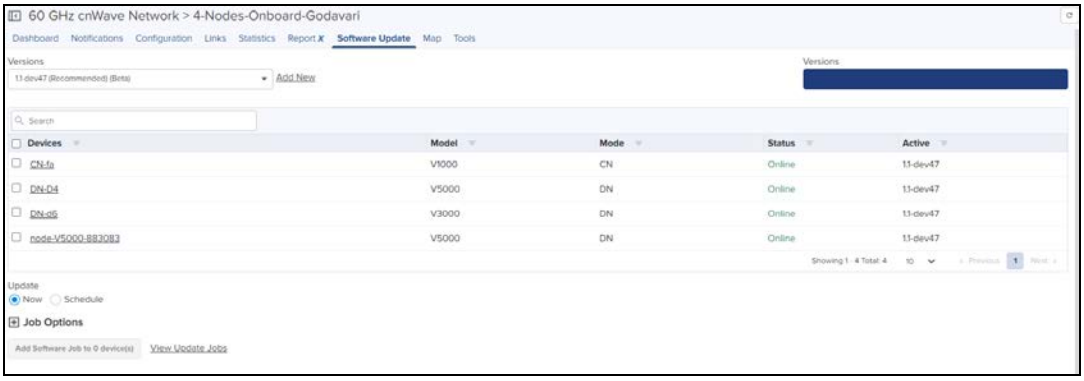
To Add a new version of the software click **Add New**. It navigates to the Software Images tab to add new version.



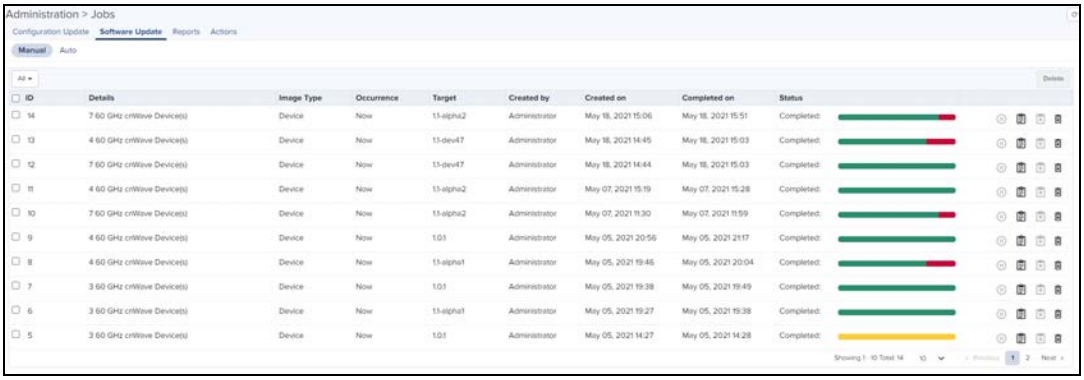
> **NOTE:**
> After Adding New image, user may needs to wait for 30 seconds to 1 minute and needs to click the refresh button.

View Update Jobs

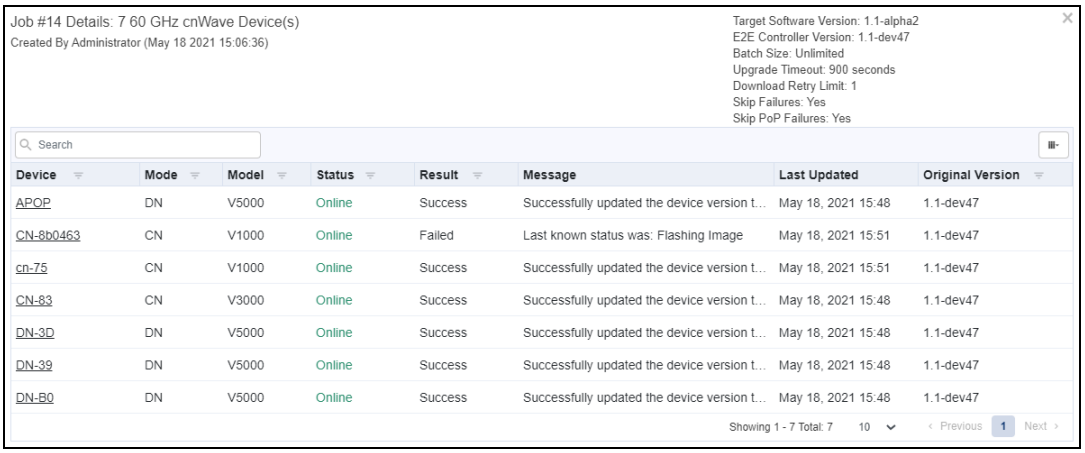
After adding the new Software Images, click **View Update Jobs.**



1. Navigate to the **Administration > Jobs > Software Update**.

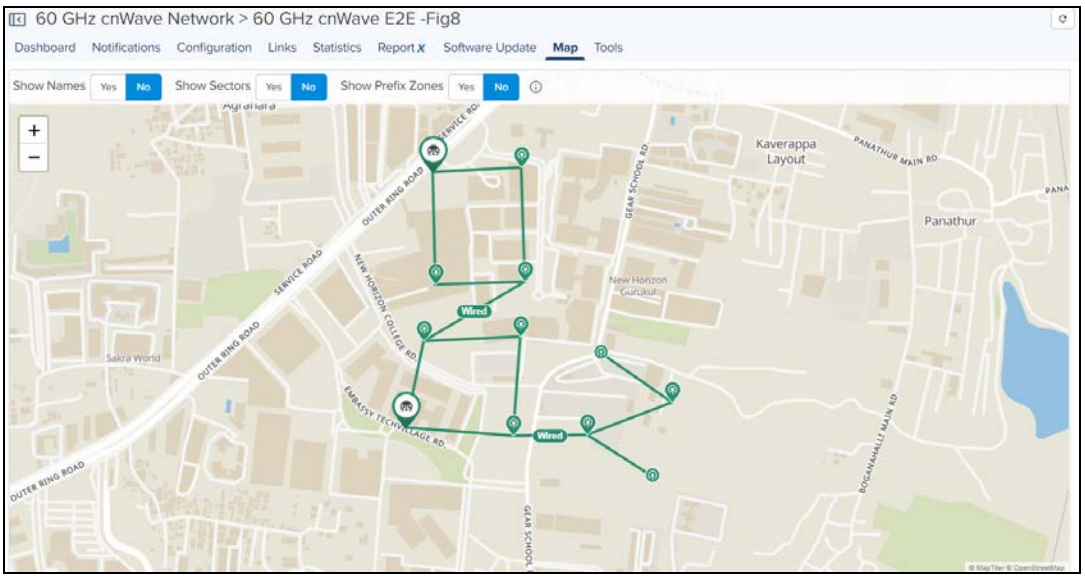


2. Click **Show More** to view the Job Details.



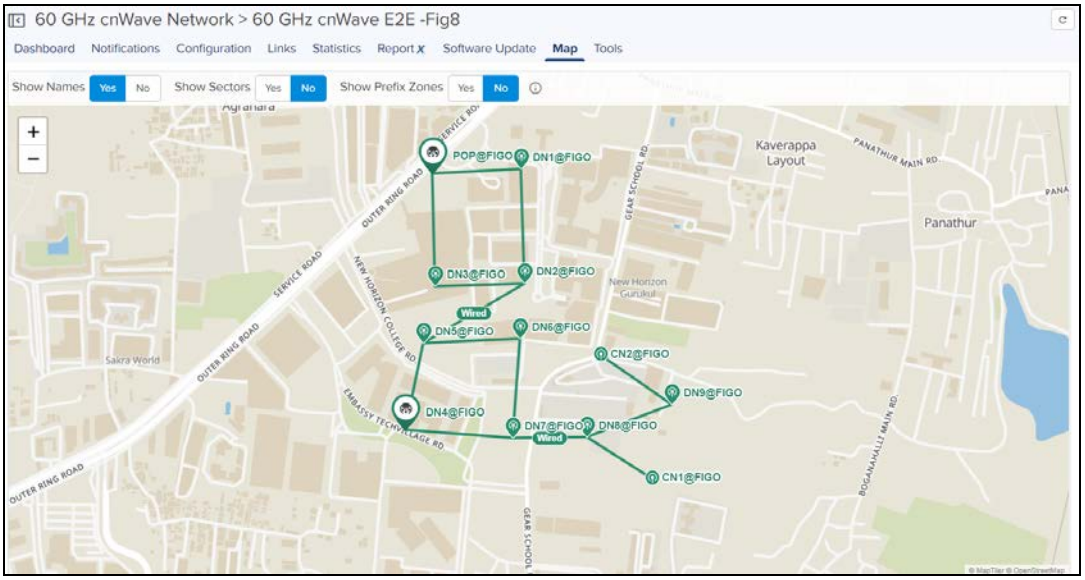
Maps

Maps provide a visualization for **Site, PoP, DN** and **CN**. They display links connectivity between devices. An example map is presented below:



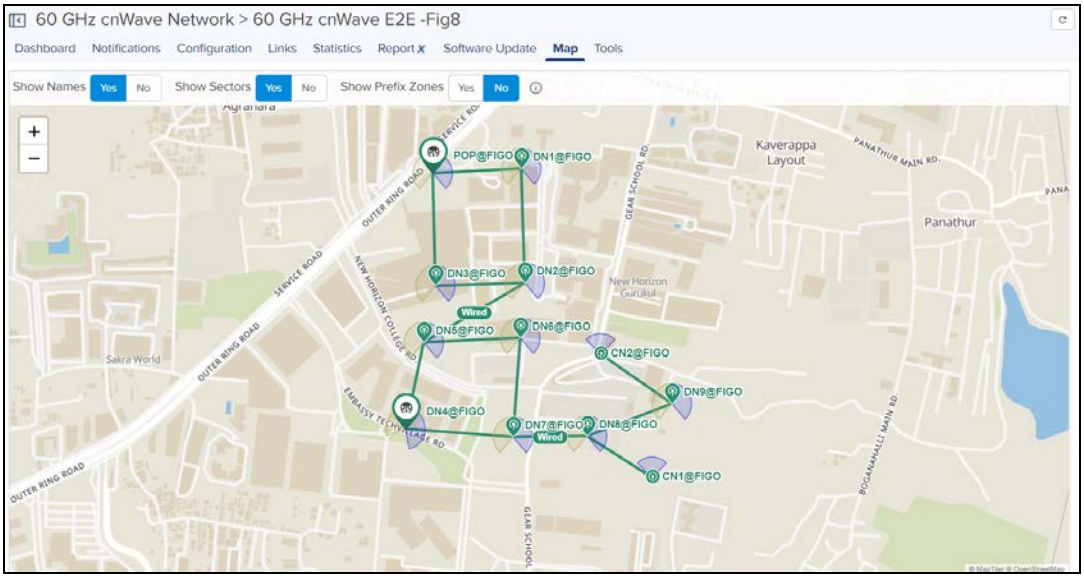
When the user selects the **Show Name** as Yes

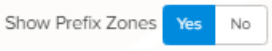
. It displays the names of the Nodes as shown below:



When the user selects the **Show Sectors** as Yes

. It displays the Sectors area of the Nodes as shown below:

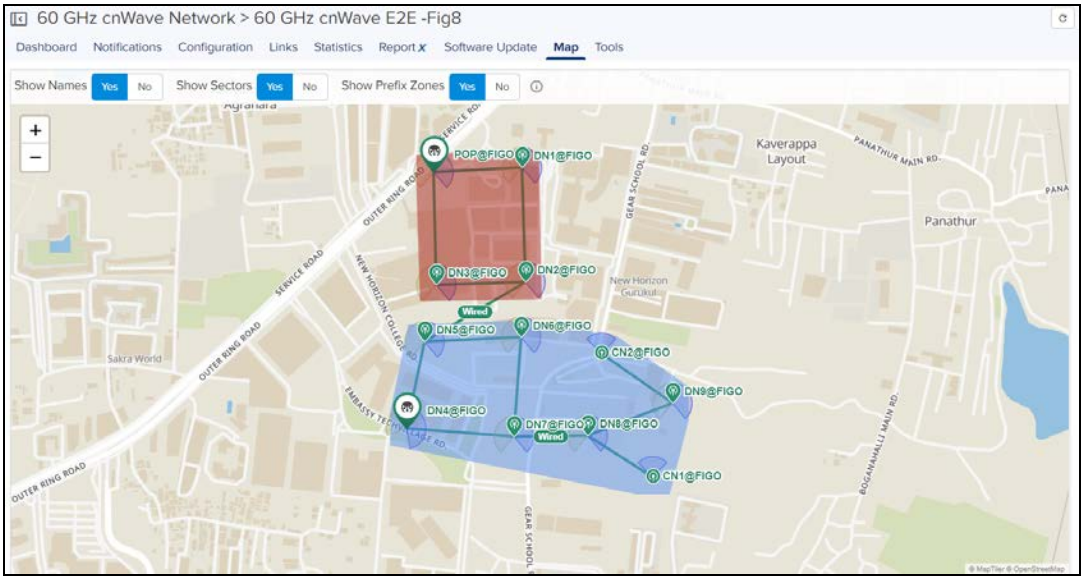


When the user selects the **Show Prefix Zones** as Yes 

. It displays the zones of the Nodes as shown below:

NOTE:

Show Prefix Zones gets enabled only if Prefix Allocation is set to **Deterministic**.



Tools

In Tools page it allows the user to perform the following actions:

- Operations
- Diagnostics
- Services

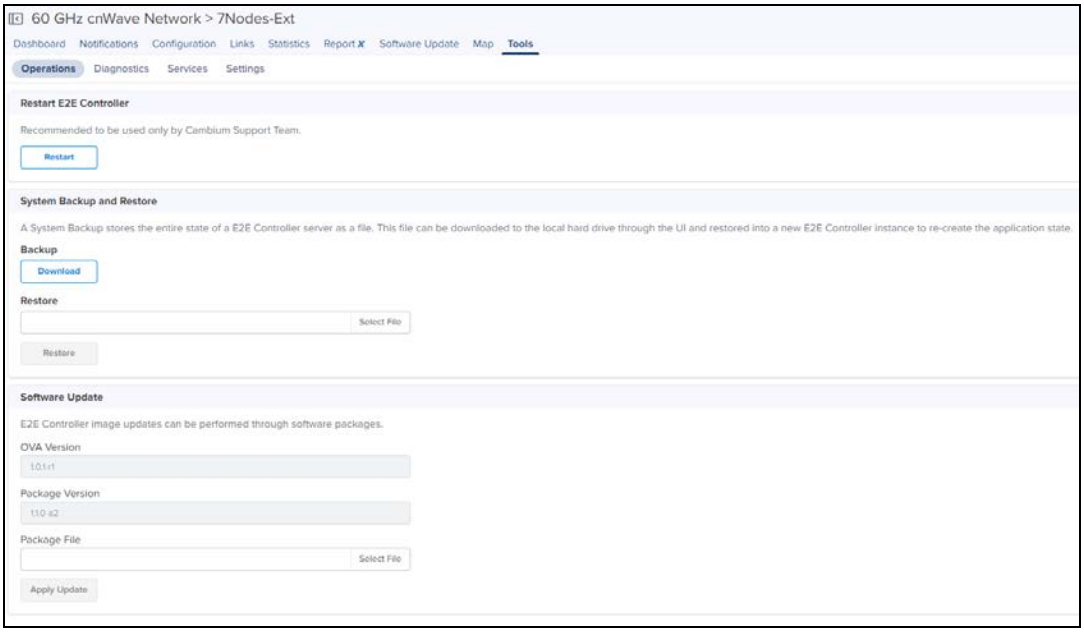
- Settings

Operations

External E2E Controller deployment

If the device is deployed through **External E2E Controller** it displays the operations page as follows:

- **Restart E2E Controller** performs the **Restart.**
- A **System Backup and Restore** the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create.
- The **Software Upgrade** is to upgrade E2E controller and can be done through E2E controller package.



Onboard E2E Controller deployment

If the device is running **Onboard E2E Controller** it displays the operations page as follows:

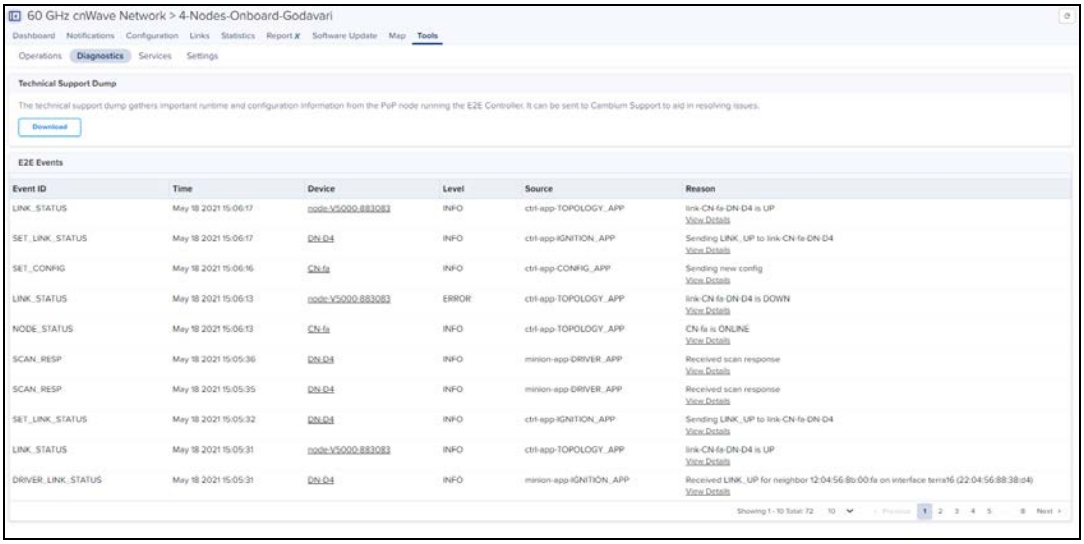
- **Operations** page allows the user to **Restart E2E Controller** and perform the **System Backup**. It also stores the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create the application state.

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.

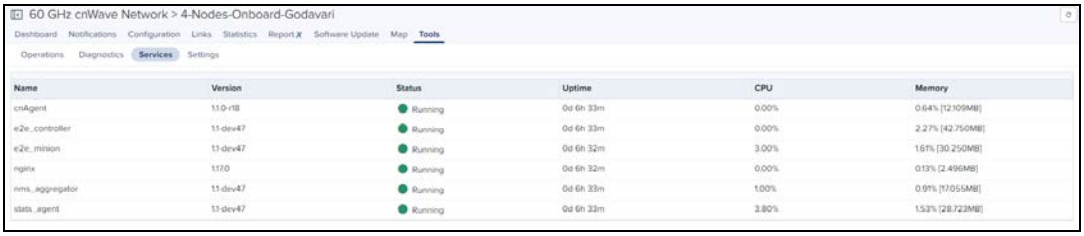
Figure 98 Diagnostics



Services

In **Services** page user can view the services running in E2E Controller.

Figure 99 Services



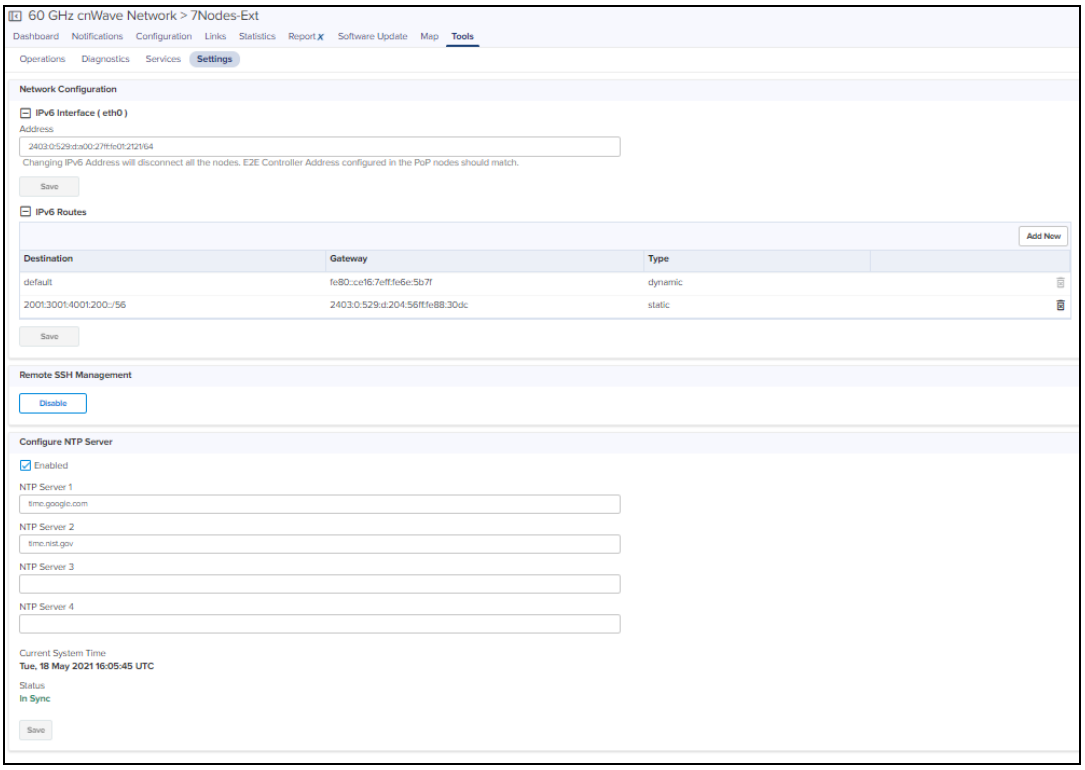
Settings

> **NOTE:**
>
> E2E Settings are not applicable for Onboard E2E Controller deployment.

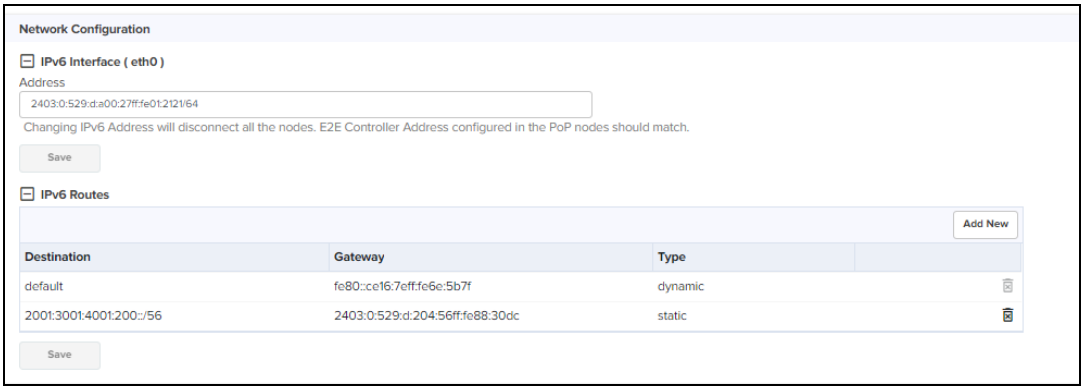
External E2E Controller deployment

If the device is deployed through **External E2E Controller** it displays the Settings page as follows:

Remote SSH Management allows the user to Enable and Disable Remote SSH Management.



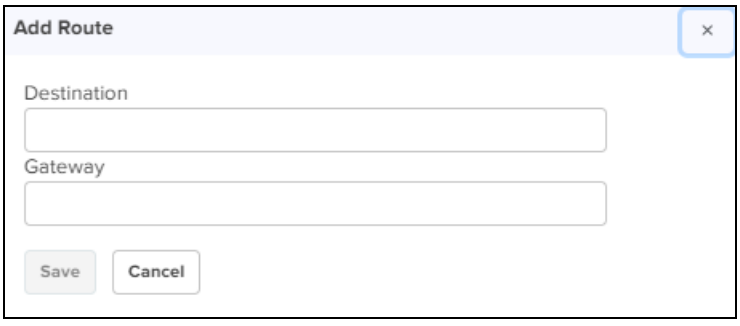
In **Network Configuration** user can configure the **IPv6 Interface E2E Controller** and **IPv6 Routes**.



- Enter the **IPv6 Interface** and click **Save**.

To add new **IPv6 Routes**:

1. Click **Add New**.

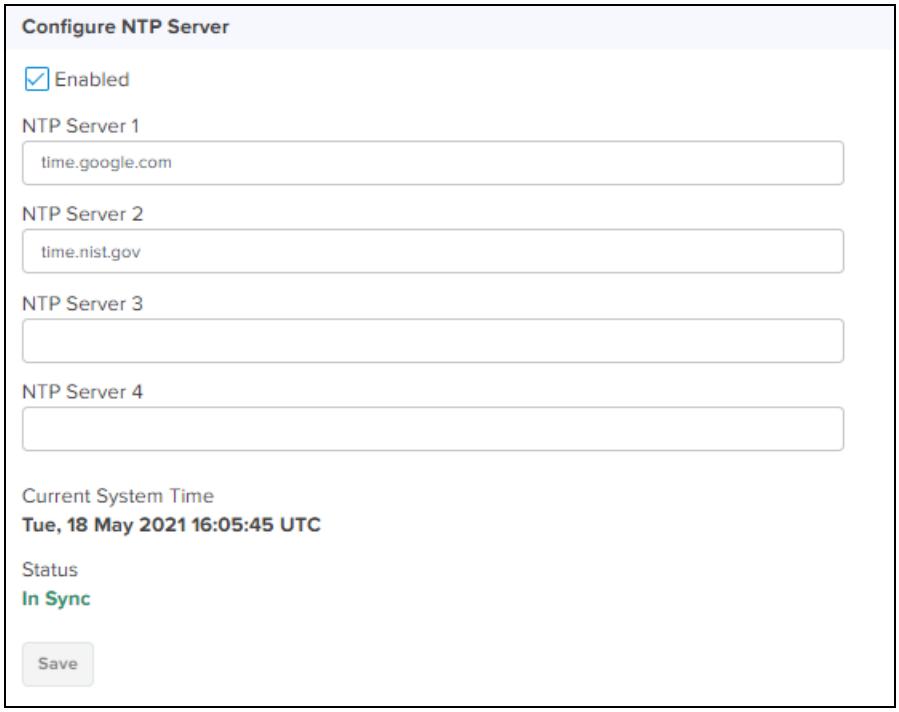


2. Enter **Destination** and **Gateway**.
3. Click **Save.**

The user can configure the **NTP Settings** to configure the time configuration of the server with hostname or IP address.

To configure the NTP server:

1. Navigate to **Tools > Settings> NTP Settings** tab.
2. Enable the **NTP Settings**.
3. Enter **Host Name** or **IP Address**. It displays **Current System Time** and **Status** of the server.

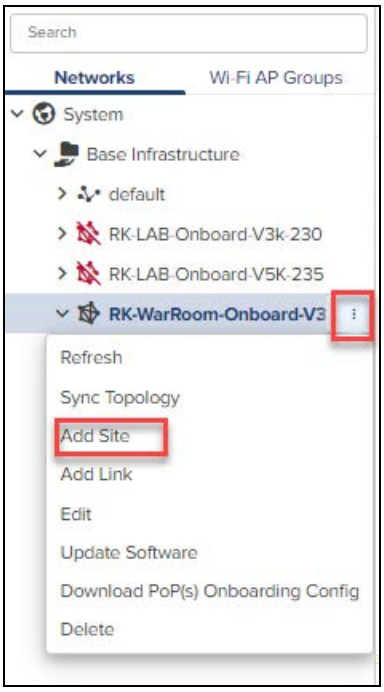


Site Configuration

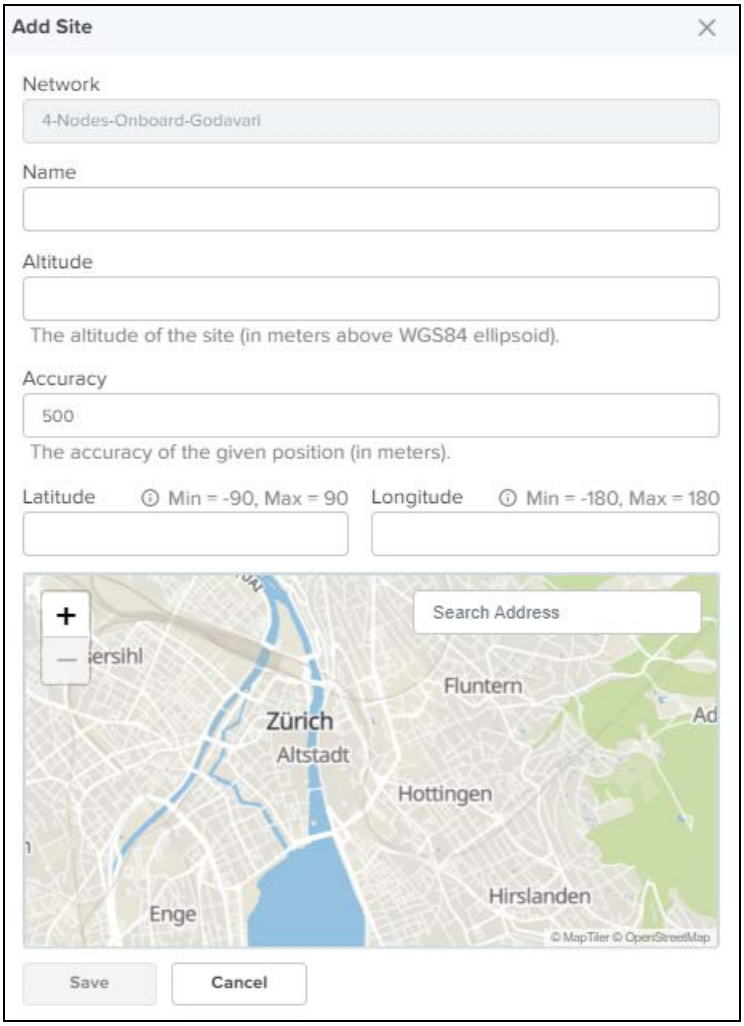
Sites are located within the networks and wireless access points attached to it.

To Add a Site

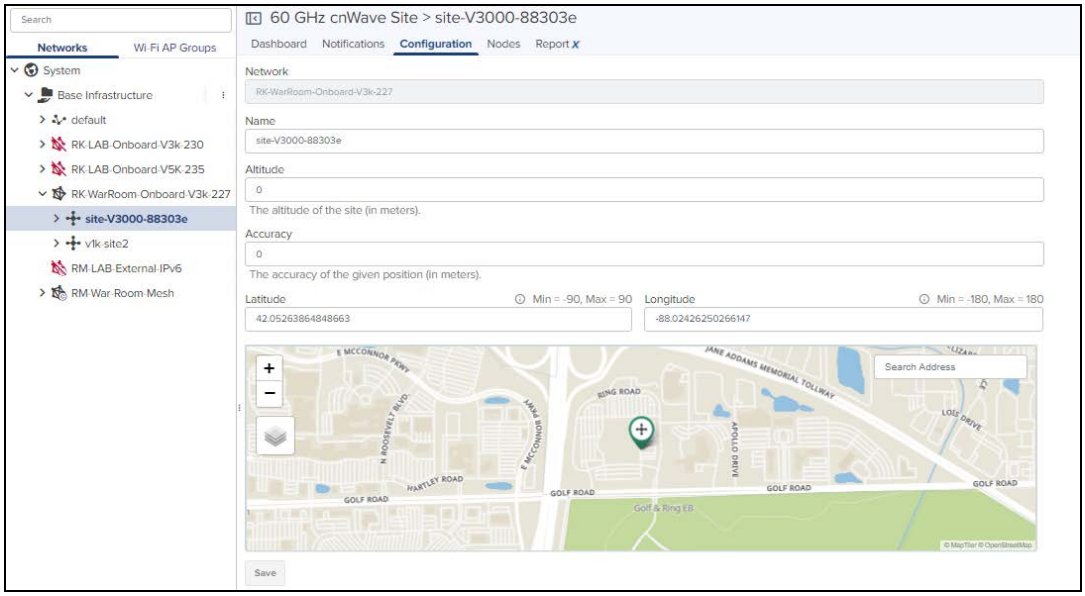
1. Navigate to **Network** and click the icon ⋮.
2. Select **Add Site** from the drop-down.



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.

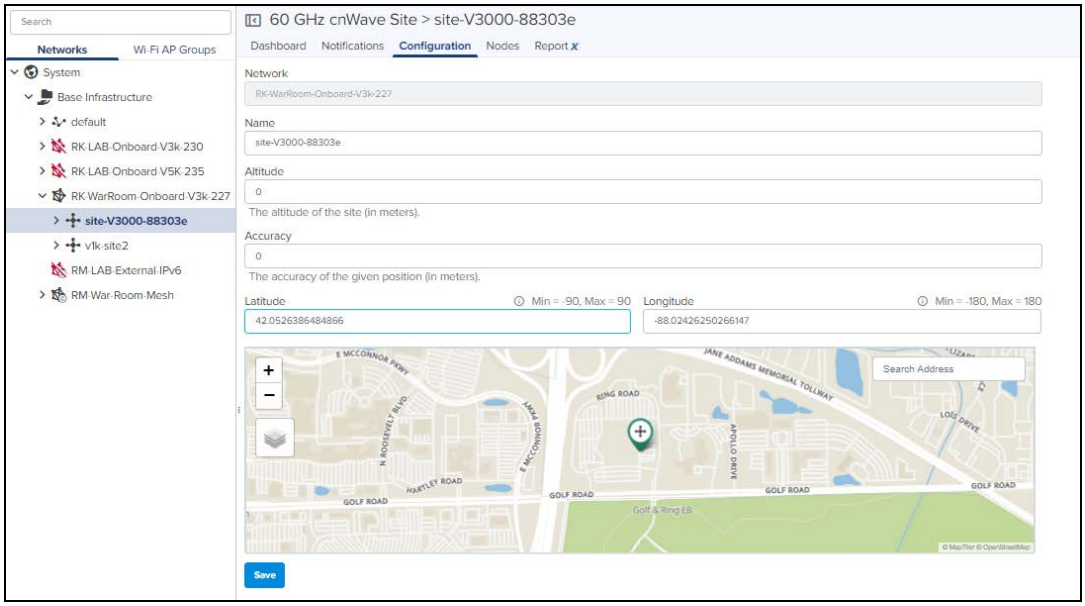


5. Click **Save**. Once the Site is configured it gets added under the E2E Network.



To edit the **Site** perform the following:

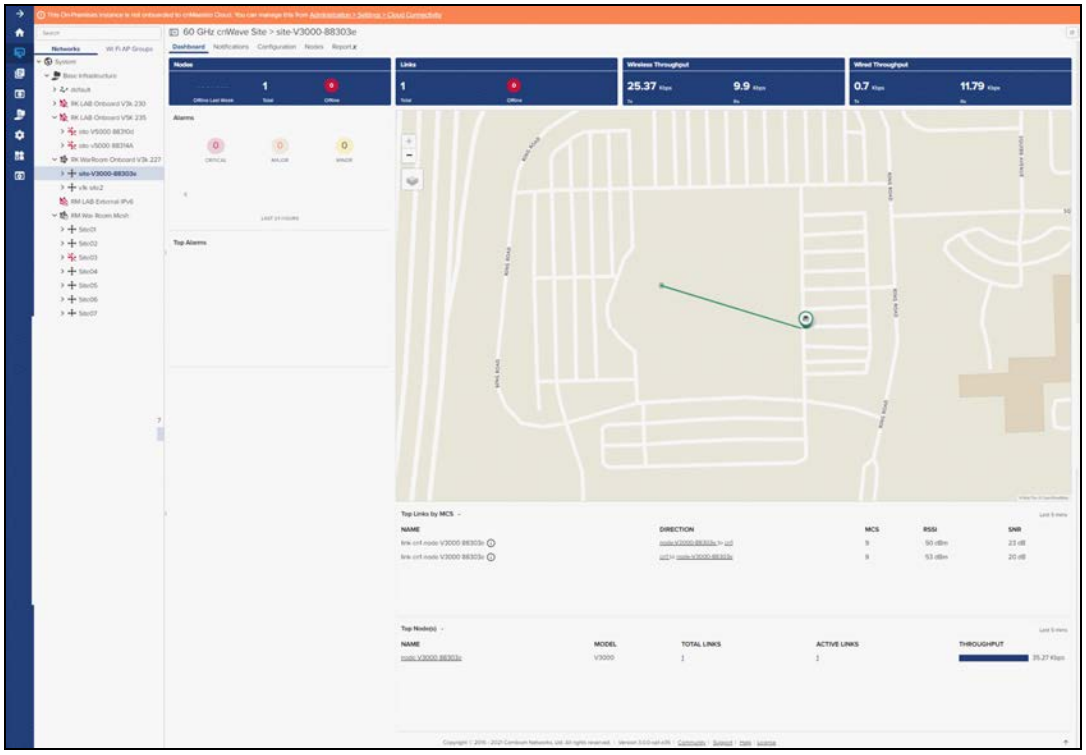
1. Navigate to **Network** > **Site** > **Configuration**.
2. Edit the details and click **Save.**



Site Dashboard

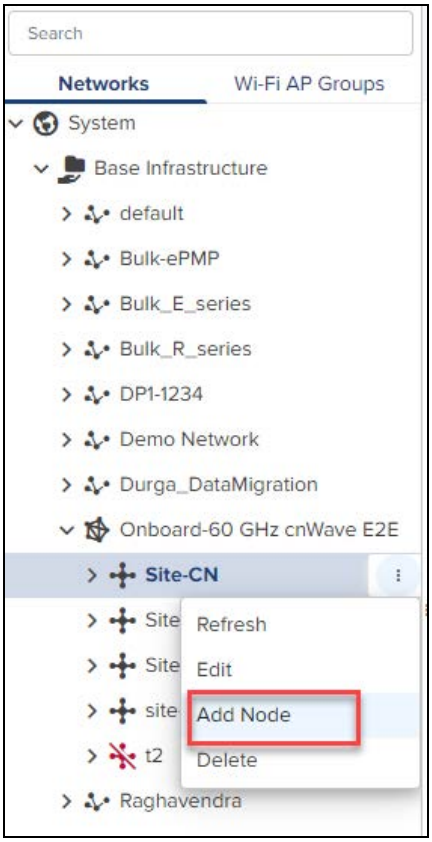
Dashboard pages are customized for each device type and aggregation level. The Site dashboard section displays the **Nodes, Links, Wireless Throughput, Wired Throughput, Alarms, Top Alarms, Top Links by MCS, Top Links by RSSI, Top Links by SNR, Top Node(s), Top PoP(s), Top DN(s), and Top CN(s).**

Figure 100 Site Dashboard



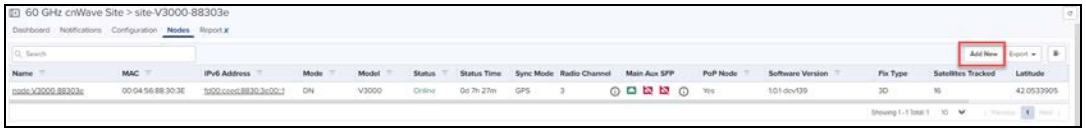
Node Configuration

Node can be configured through the **Site Menu** option by clicking the ⋮ icon in **Site Network tree** menu or through **Network** > **Site** > **Nodes** and click **Add.**

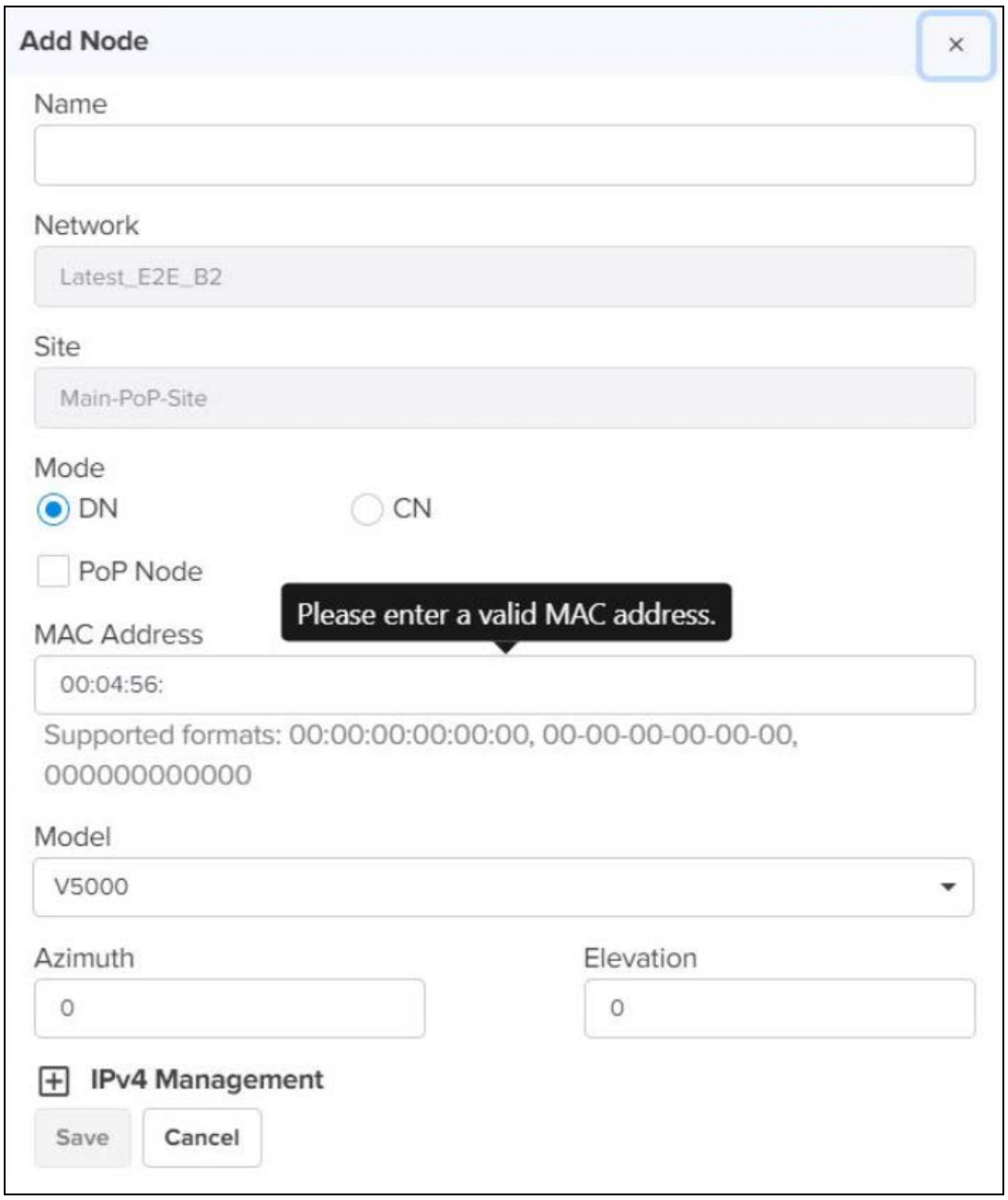


To Add a Node:

1. Navigate to the **Network** > **Site** > **Nodes.**



2. **Add Node** window pops-up once the user clicks **Add new.**



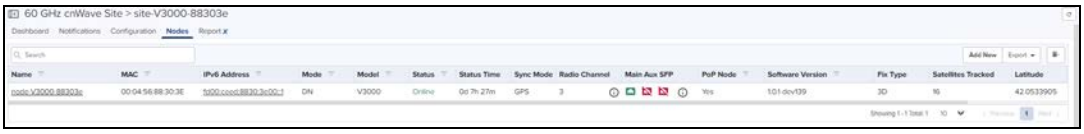
Adding the Node allows the user to create the different Nodes as shown below:

- PoP Node
- DN
- CN

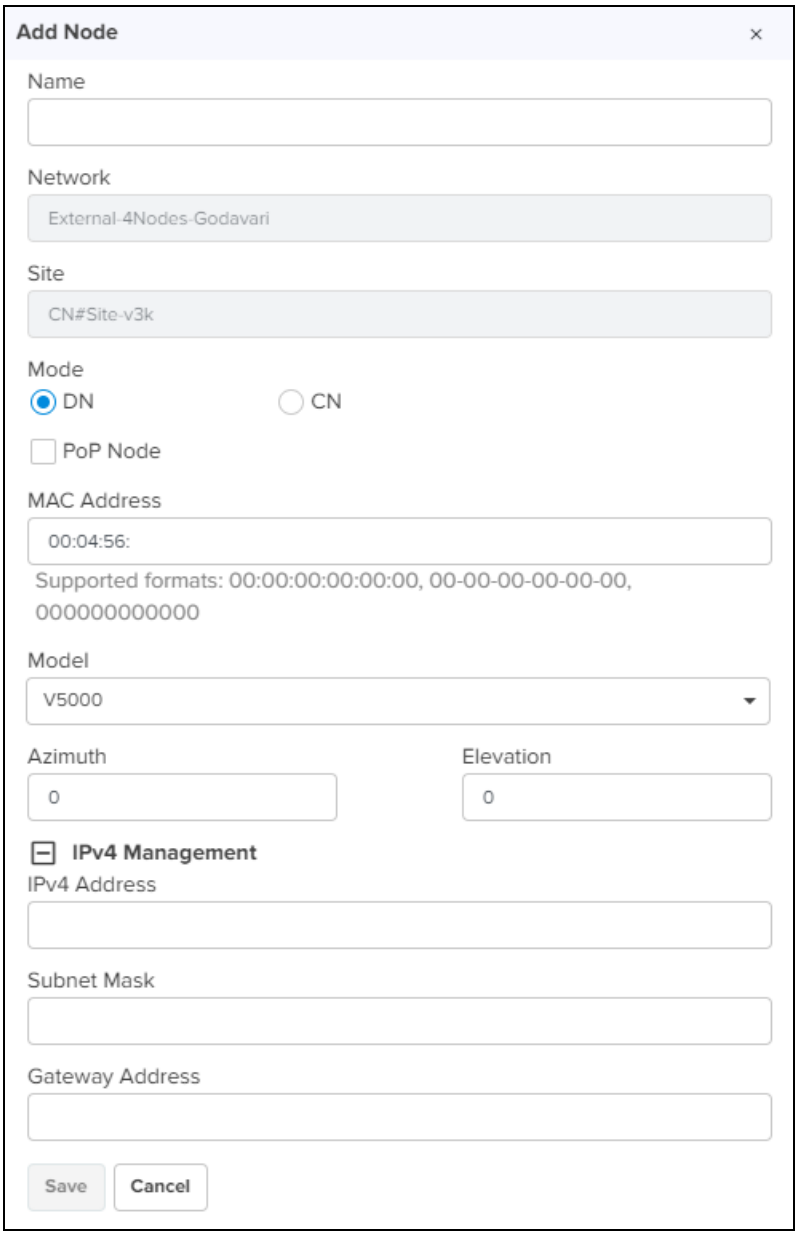
PoP Node configuration

To add a PoP Node:

1. Navigate to the **Network** > **Site** > **Nodes.**
2. Click **Add New.**



3. **Add Node** window pops-up.



4. Enter the **PoP Name**, select the Mode **DN.**
5. Enable **PoP Node**.

NOTE:
Once the PoP Node is enabled user needs to select the **Routing** and **Interface** details.

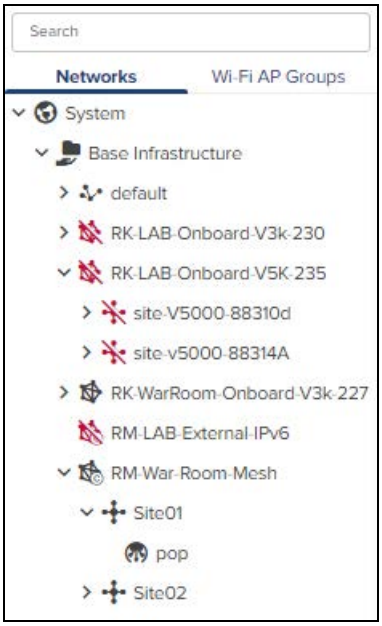
6. Enter the **MAC Address** and select the device **Model** from the drop-down.
7. Enter the **Azimuth** and **Elevation**.
8. In the **PoP Configuration** select **BGP** or **Static Routing**.
9. In **Interface** select **Aux** or **Main** or **SFP** or **Disabled**.

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, which can be used to import and configure in the PoP Node UI.

Once the **PoP** node is configured it get listed under the **Site.**

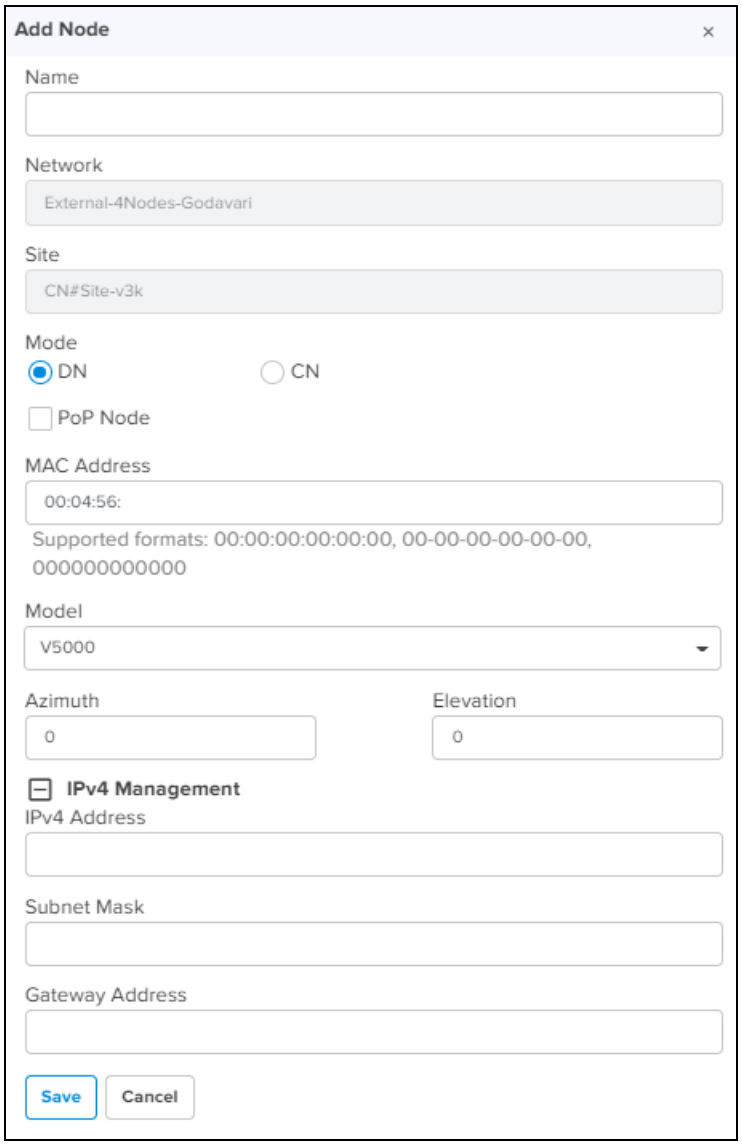


DN/CN Node configuration

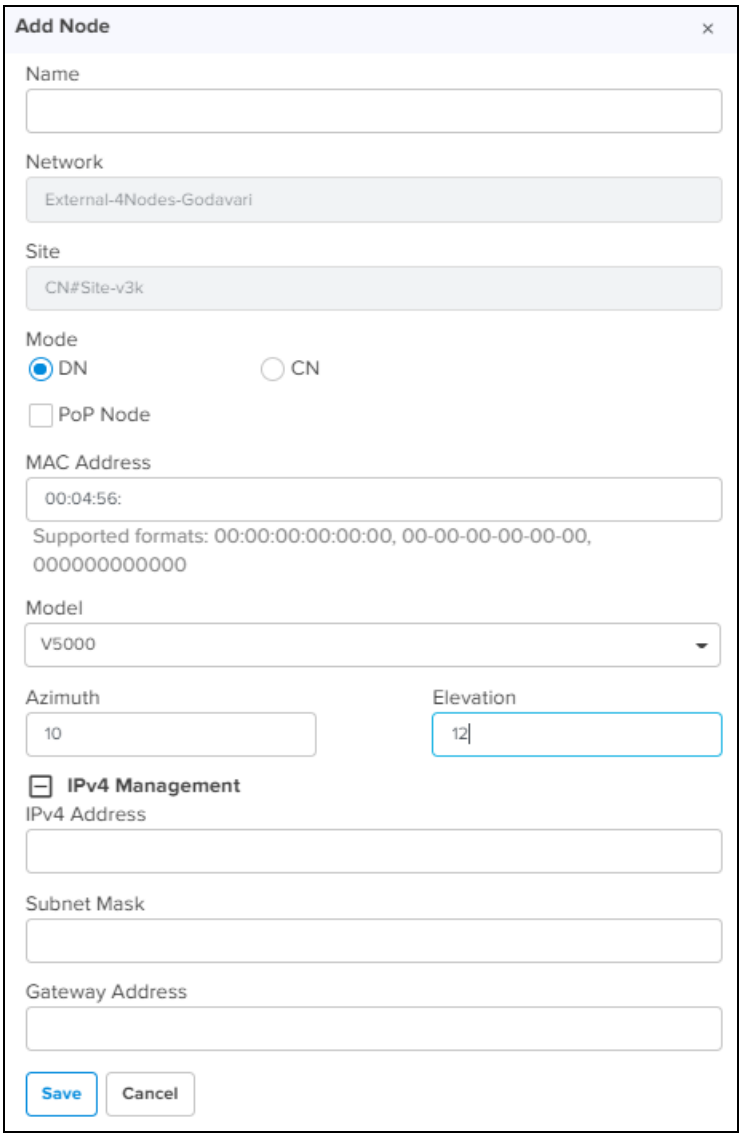
To add DN/CN node:

1. Navigate to the **Network** > **Site** > **Nodes.**
2. Click **Add New.**

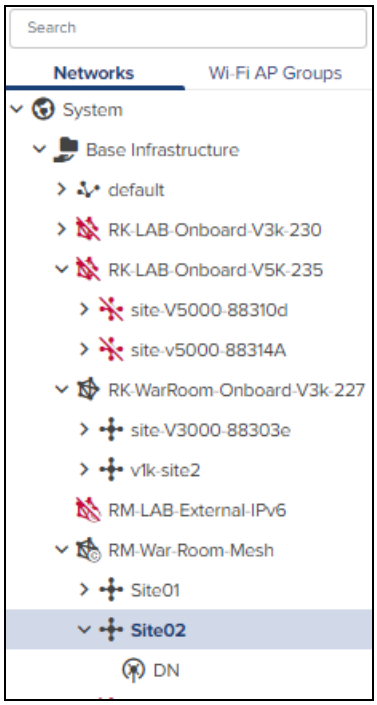
3. **Add Node** window pops-up.



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**.



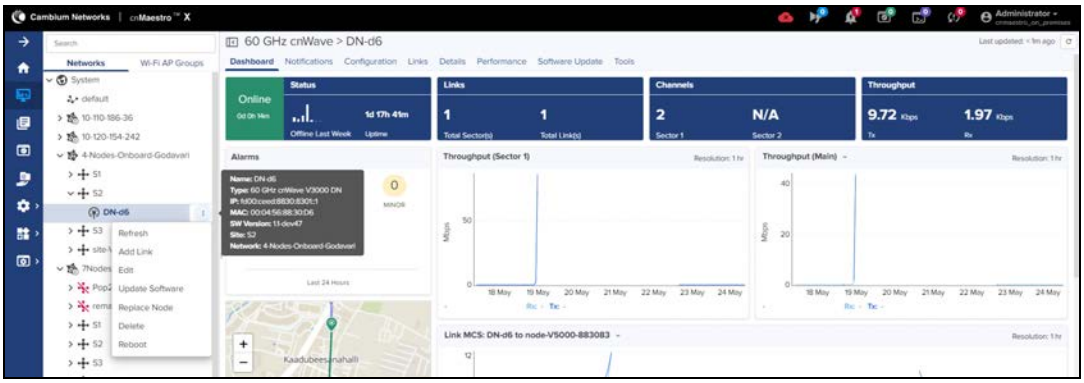
7. In IPv4 Management enter the **IPv4 Address, Subnet Mask** and **Gateway Address**.
8. Click **Save.**
9. Once the **DN/CN** node is configured, it gets listed under the Site**.**



Replace Node

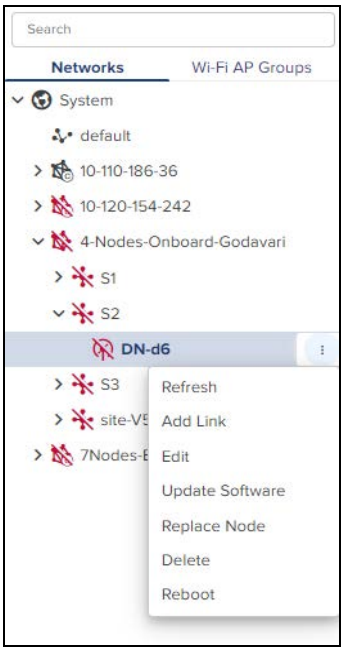
Replace Node allows to replace the existing faulty nodes with new nodes along with the configuration and links of existing faulty nodes.

	NOTE: New node should be replaced with same model as existing node.



To replace Node:

1. Navigate to **Node** tree menu and select the node.



2. Click icon and Select **Replace Node** from the 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.

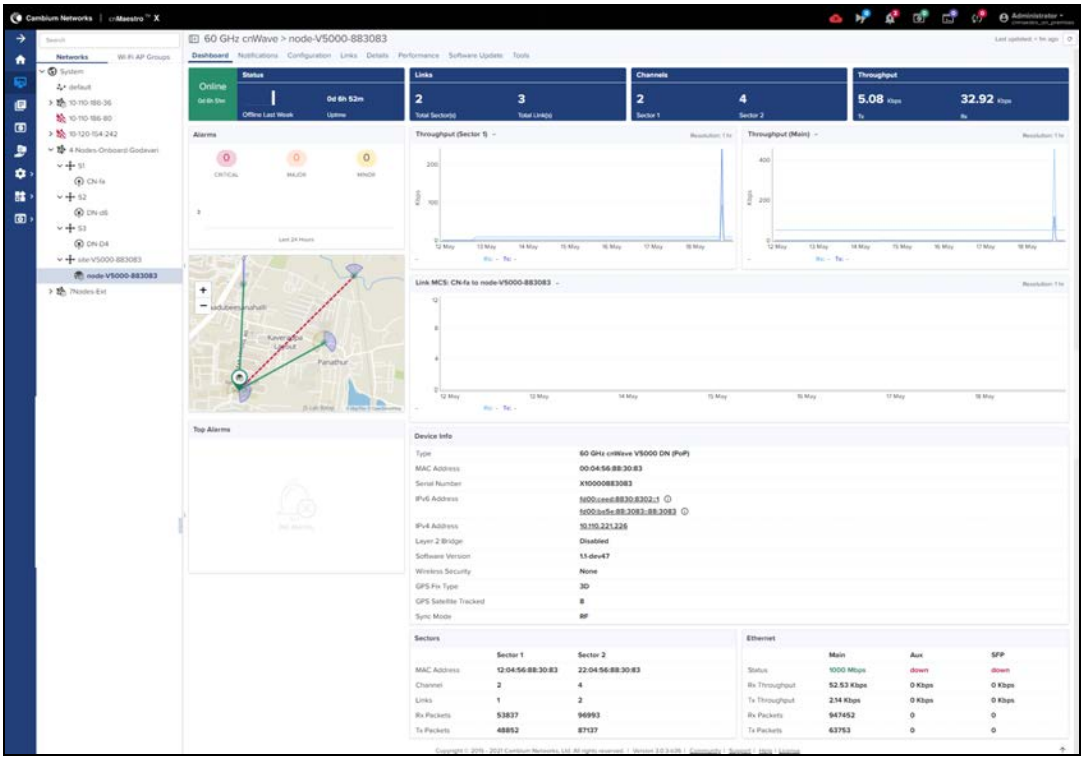
Dashboard

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, Links DN, Links PoP, 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 101 PoP Node Dashboard

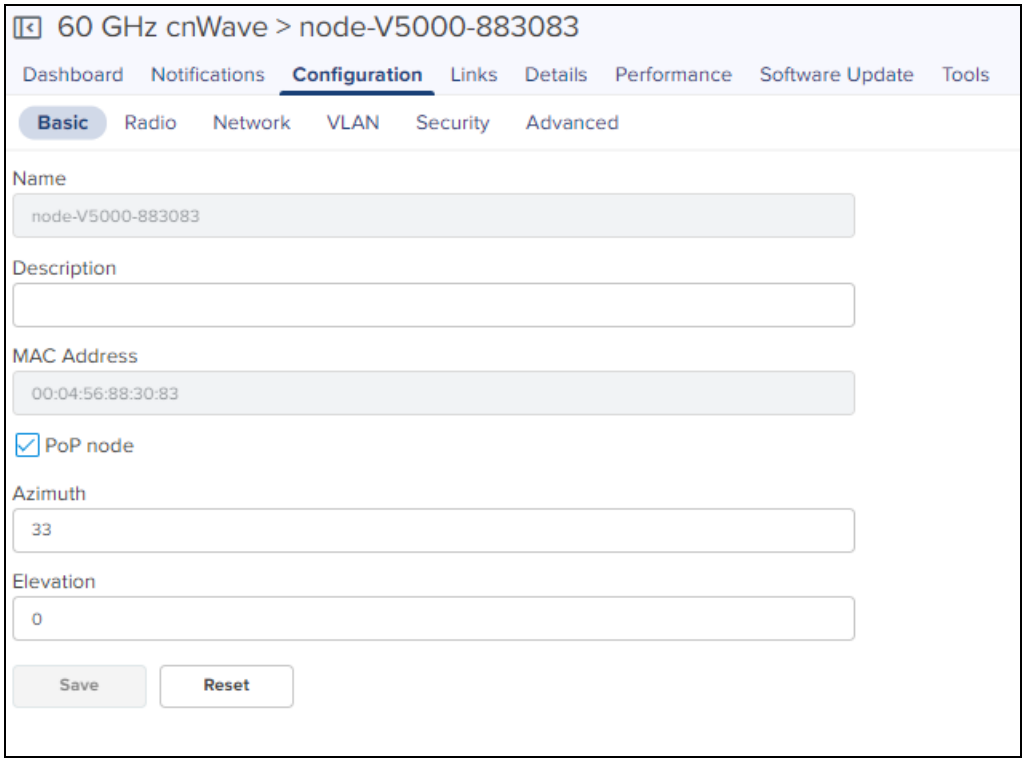


Configuration

Basic

It displays the basic details of PoP node such as **Name, Description, MAC Address, Azimuth,** and **Elevation**.

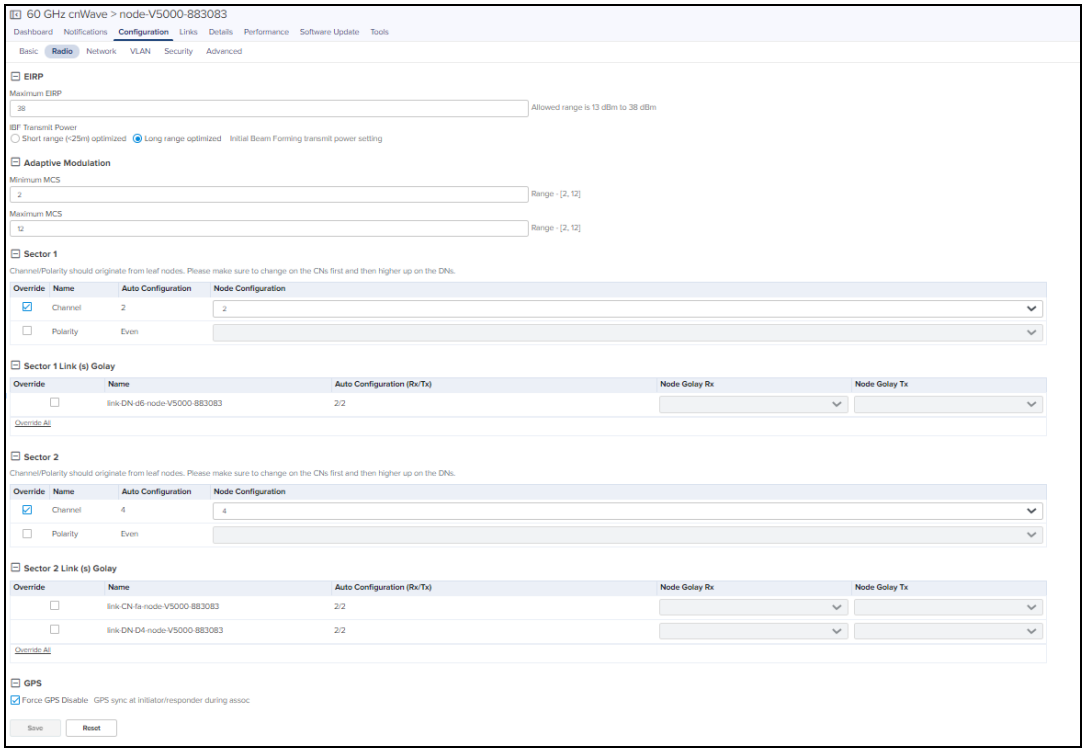
Figure 102 Basic



Radio

It allows the user to configure the **EIRP**, **Adaptive Modulation**, **Sectors (channels, Polarity and Link(s) Golay)**, and **GPS**.

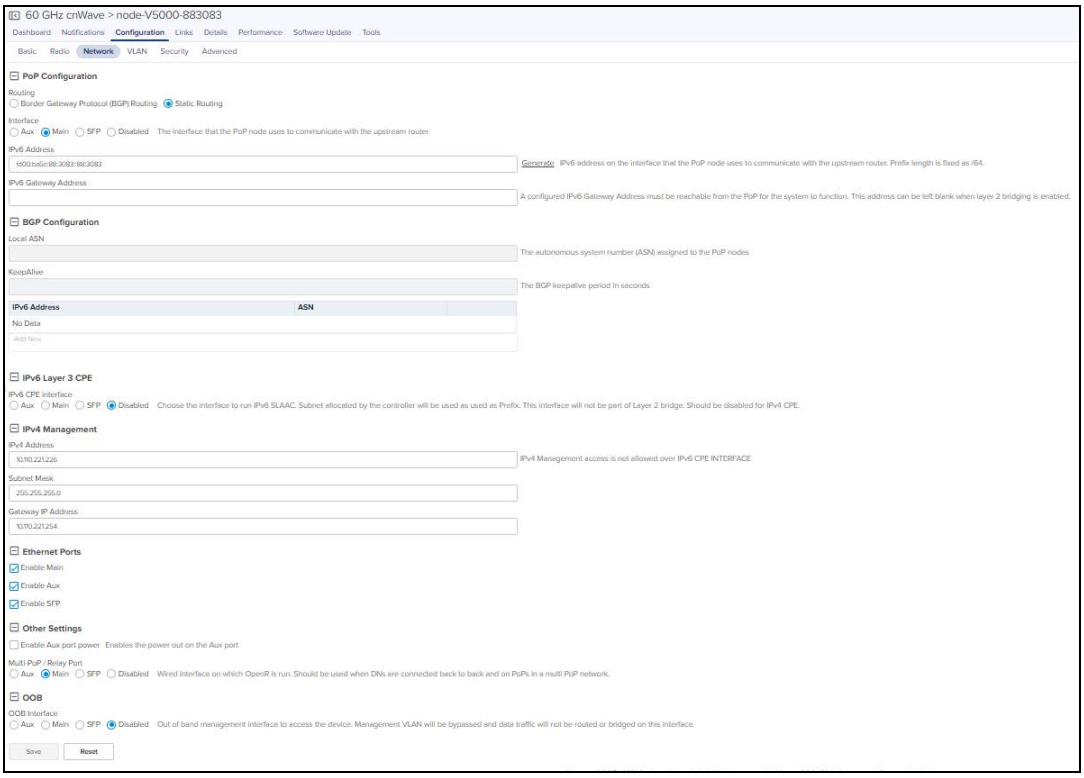
Figure 103 Radio



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.**

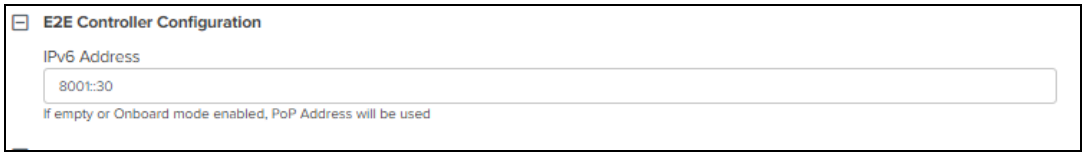
Figure 104 Networks



In the Network tab user needs to configure the **PoP Configuration** and **E2E Controller** as shown below:

1. Navigate to the **Configuration** > **Network** > **PoP Configuration**.
2. Select the appropriate option in **Routing** and **Interface**.
3. Enter the **IPv6 Adddress.**

4. In **E2E Controller Configuration**, enter the **IPv6 Address.**



5. Click **Save.**

NOTE:

Once the configuration is updated successfully in cnMaestro, the same parameters needs to be entered in the UI of the **PoP Node GUI**.

VLAN

NOTE:

From Software Update Version 1.1 of all nodes, supports configuration of the VLAN Management and Ports.

Virtual Local Area Networks (VLANs) is a broadcast domain in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set and traffic will be tagged when transporting over wireless.

NOTE:

Only PoP node Management VLAN can be configured, if Layer 2 Bridge is not enabled in **E2E Network > Configuration > Basic** page.

Node running version 1.0.1:

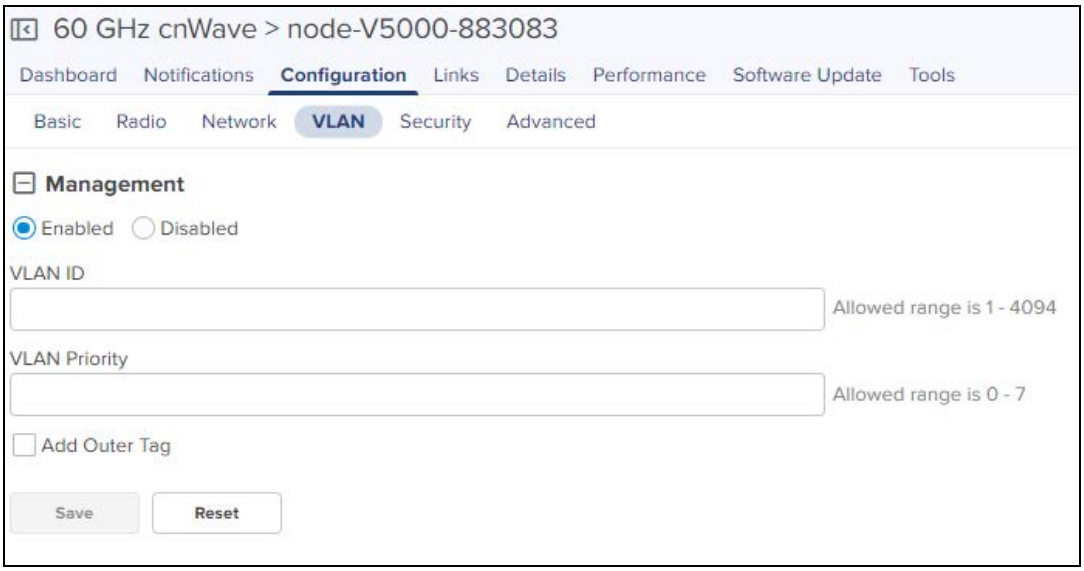
- When Layer2 bridge is disable, Only PoP node Management VLAN ID can be configured.
- When Layer2 bridge is enable, all nodes Management VLAN ID can be configured.

Node running version 1.1:

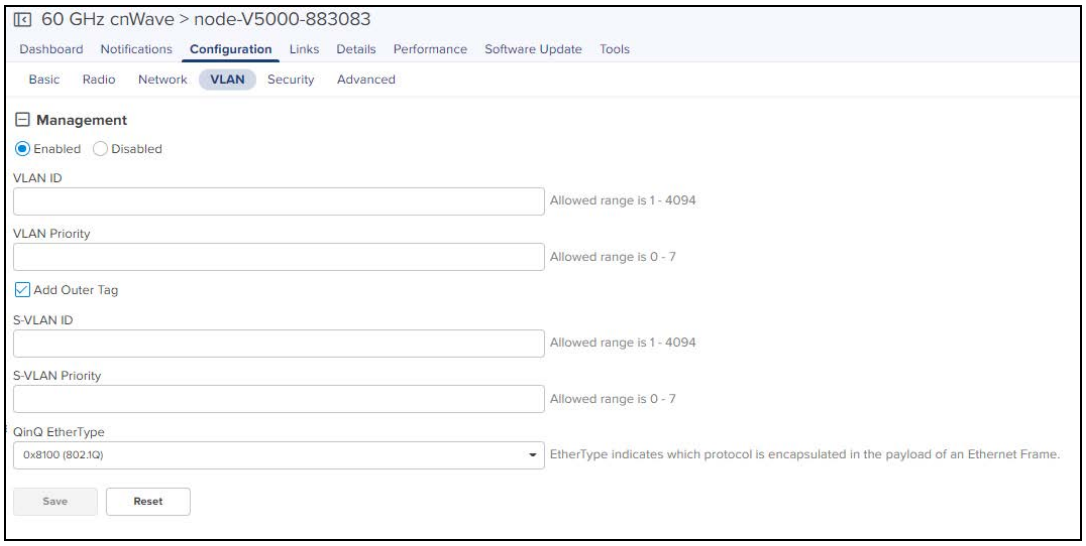
- When Layer2 bridge is disable, Only PoP node Management VLAN ID, Priority with Outer Tag can be configured.
- When Layer2 bridge is enable, all node management VLAN and ports can be configured.

To add a Management VLAN:

1. Navigate to **Configuration > VLAN.**
2. Click Enabled.



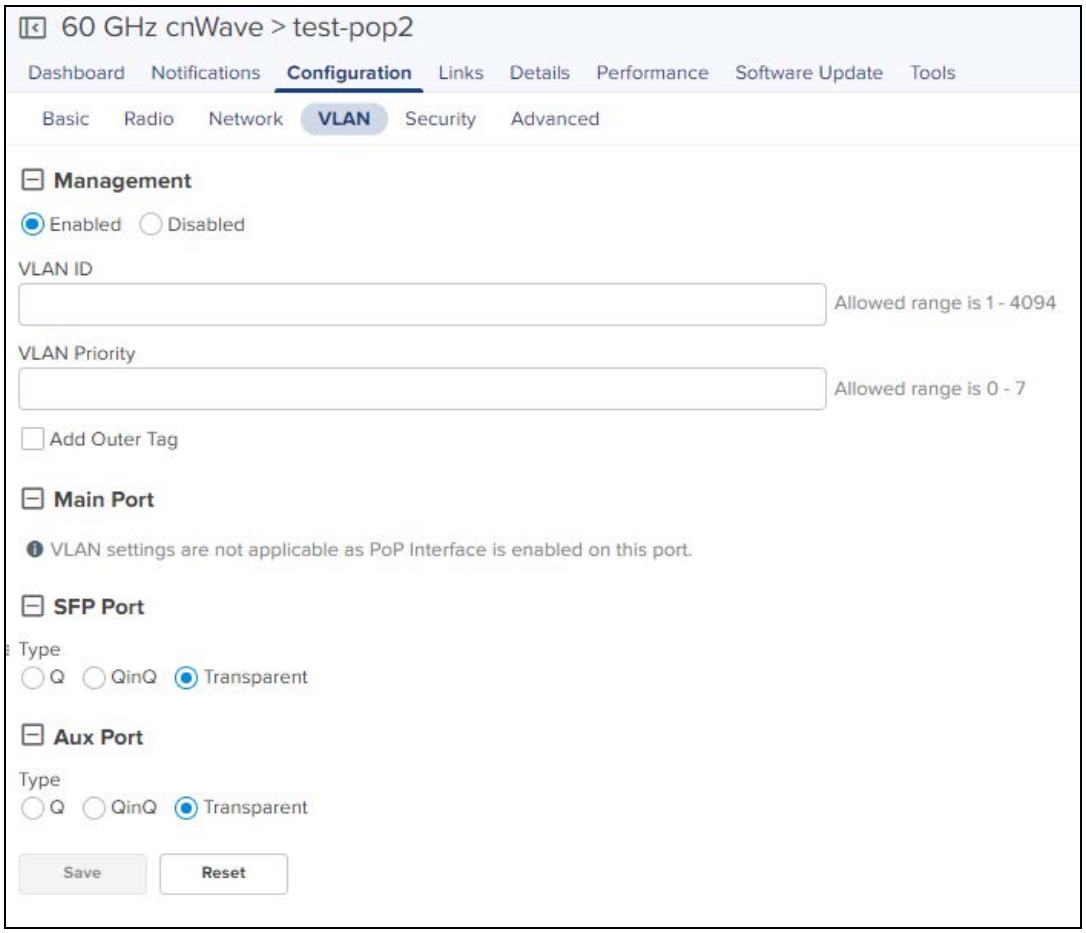
3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.



5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority.**
7. Enter **QinQ EtherType.**
8. Click **Save.**

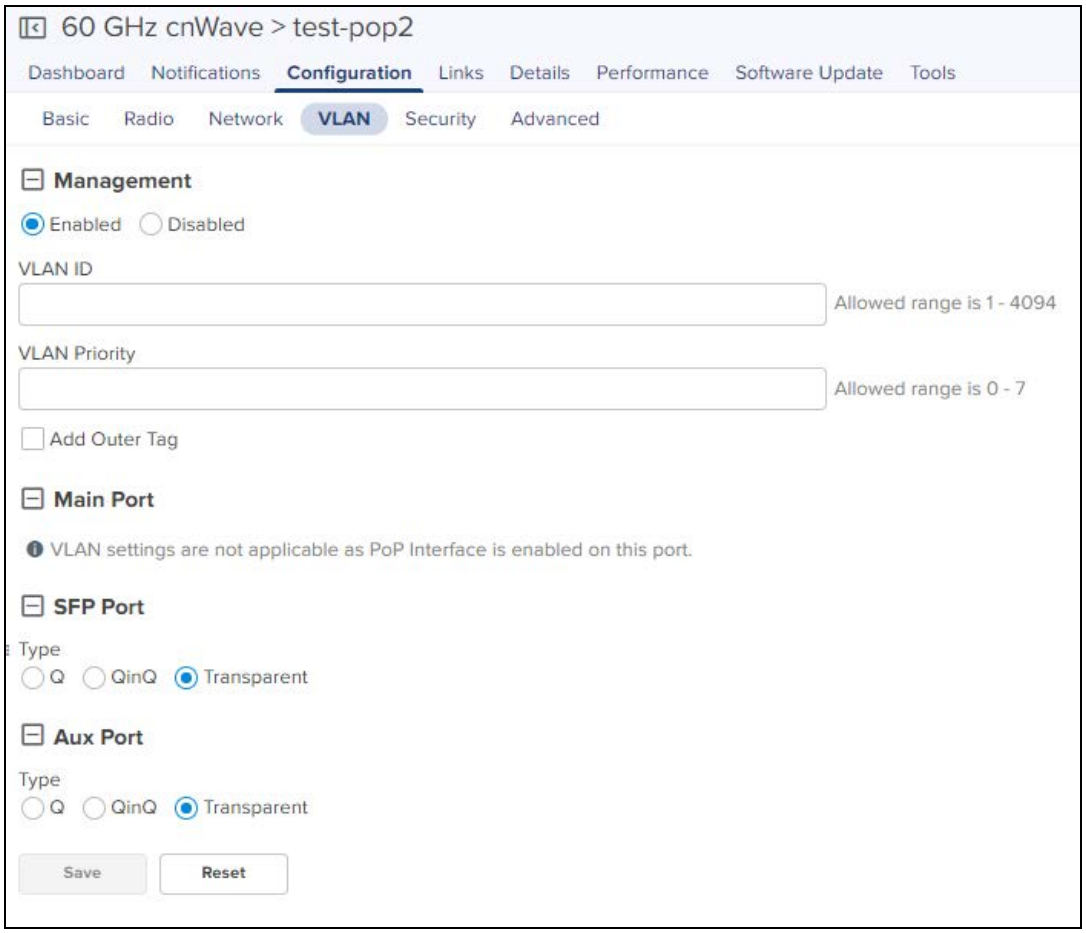
If Layer 2 Bridge is enabled in **60 GHz cnWave Network > Configuration > Basic** page. User can configure Management VLAN and Ports of PoP node, DN and CN.

	NOTE: VLAN settings are not applicable if Relay Port, SFP Port, or Aux Port is enabled on Network page.

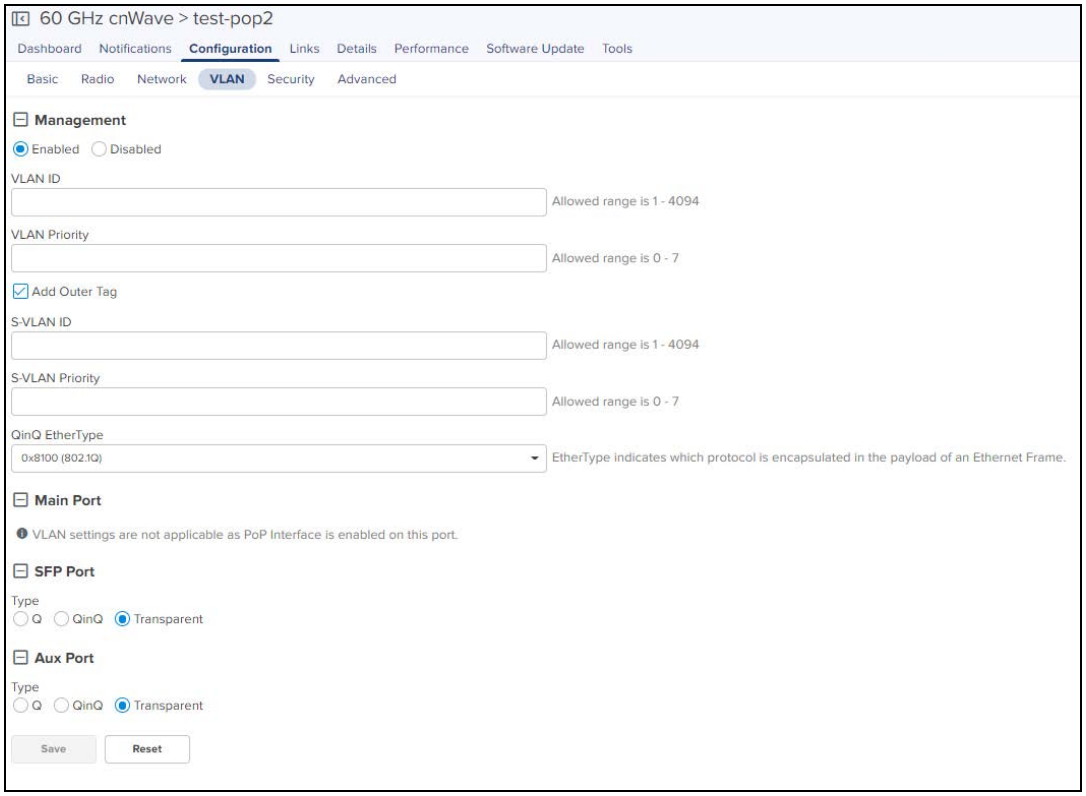


To add a VLAN:

1. Navigate to **Configuration > VLAN.**
2. Click Enabled.



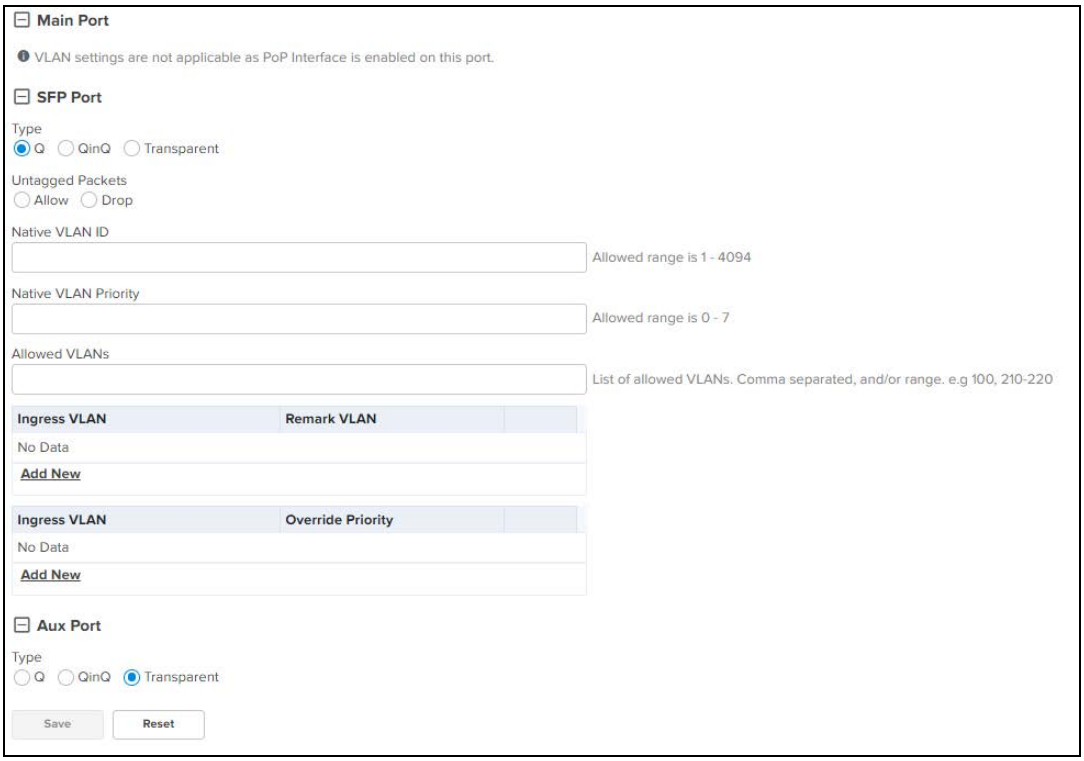
3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.



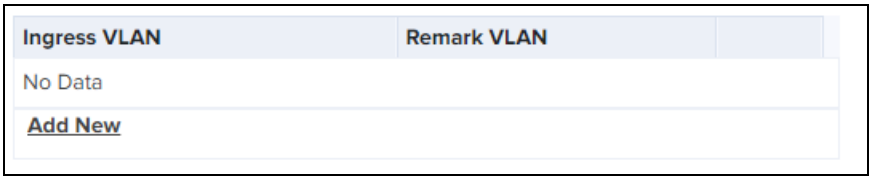
5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority.**
7. Enter **QinQ EtherType.**

> **NOTE:**
> VLAN settings configuration of Main Port, SFP Port, or Aux Port is similar.

8. Select Port **Q** or **QinQ** types.
   a. If user selects **Q type** perform as follows:



   - Select **Untagged Packets** Allow or Drop.
   - Enter **Native VLAN ID.**
   - Enter **Native VLAN Priority**.
   - Enter **Allowed VLANs**.
   - To add new **VLAN Remarking.**



   - Click Add New

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

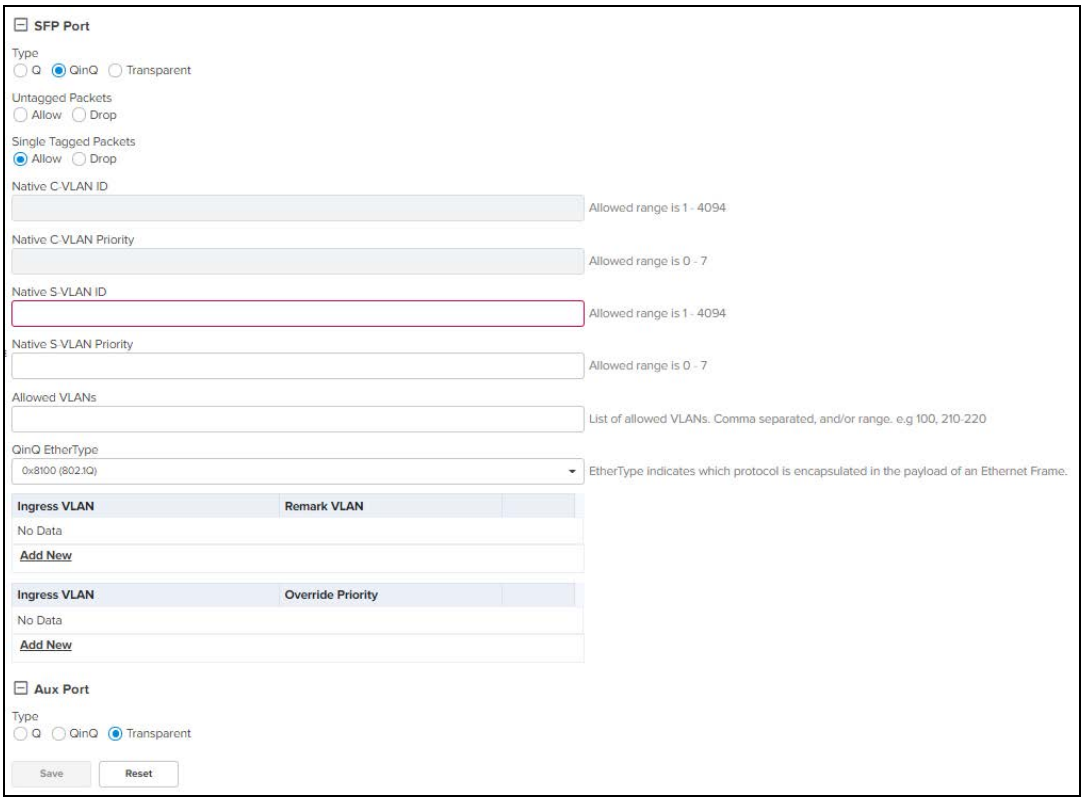
- To add new **VLAN Priority Override**.

- Click **Add New**.

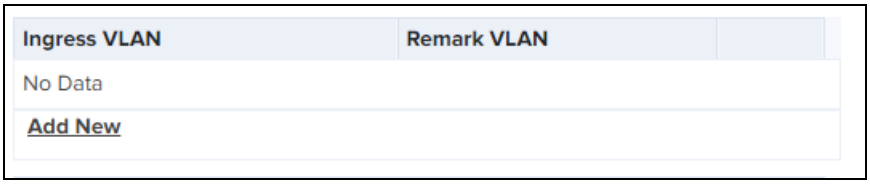
- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- Click **Save**.

b. If user selects **QinQ** type perform as follows:



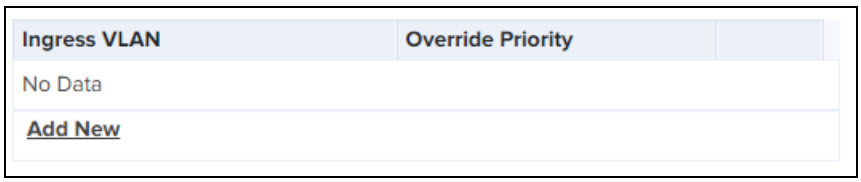
- In **Untagged Packets** select **Allow** or **Drop.**
- In **Single Tagged Packets** select **Allow** or **Drop.**
- Enter **Native C-VLAN ID.**
- Enter **Native C-VLAN Priority**.
- Enter **Native S-VLAN ID**.
- Enter **Native S-VLAN Priority**.
- Enter **Allowed VLANs**.
- Enter **QinQ EtherType**.
- To add new **VLAN Remarking.**



- Click Add New

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- To add new **VLAN Priority Override**.



- Click **Add New**.

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- Click **Save**.

Security

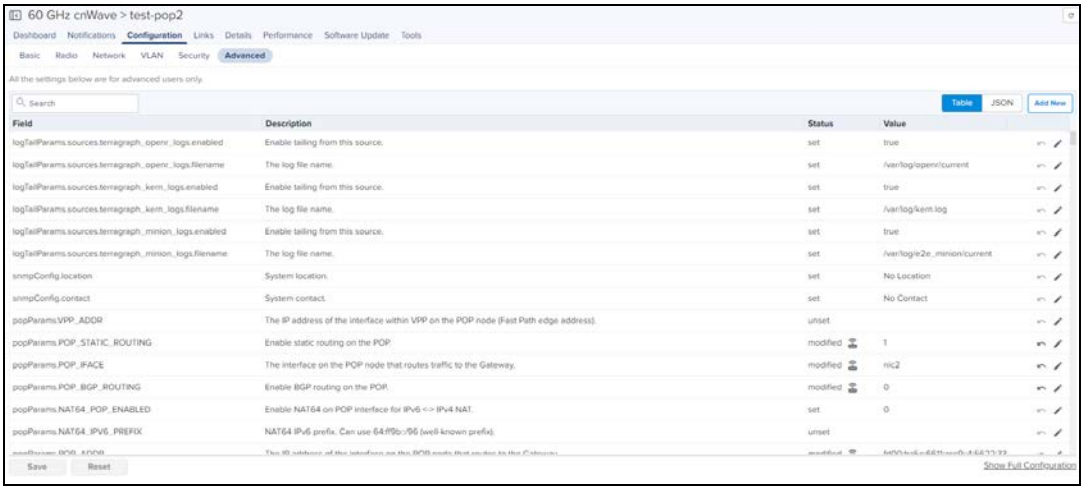
Security tab allows to reset the identity and password of the Radius user.

Figure 105 Security

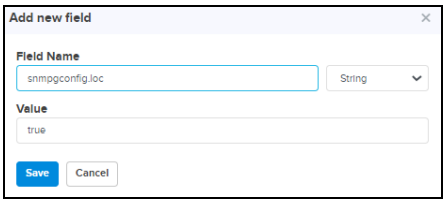
Advanced

Advanced tab allows the advanced user to set **Field Name** and **Value**.

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



3. Enter the **Field Name** and **Value.**



4. Click **Save.**

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.

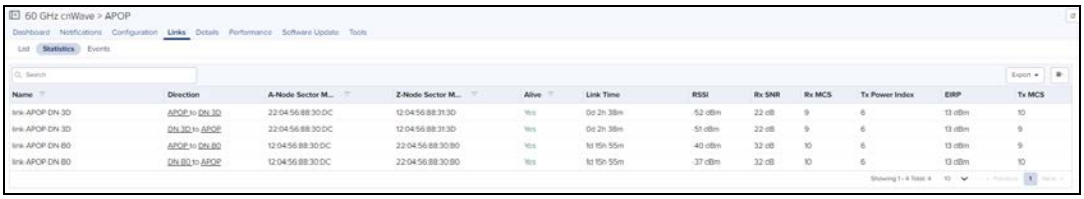
Figure 106 List

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.

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.



Events

Events provides the details of the links from last 1 hour to 7 Days, Ignition Attempts and Distance.

Figure 107 Events

It also calculates the Availability percentage per link, including the duration when E2E Controller was offline in cnMaestro.

Details

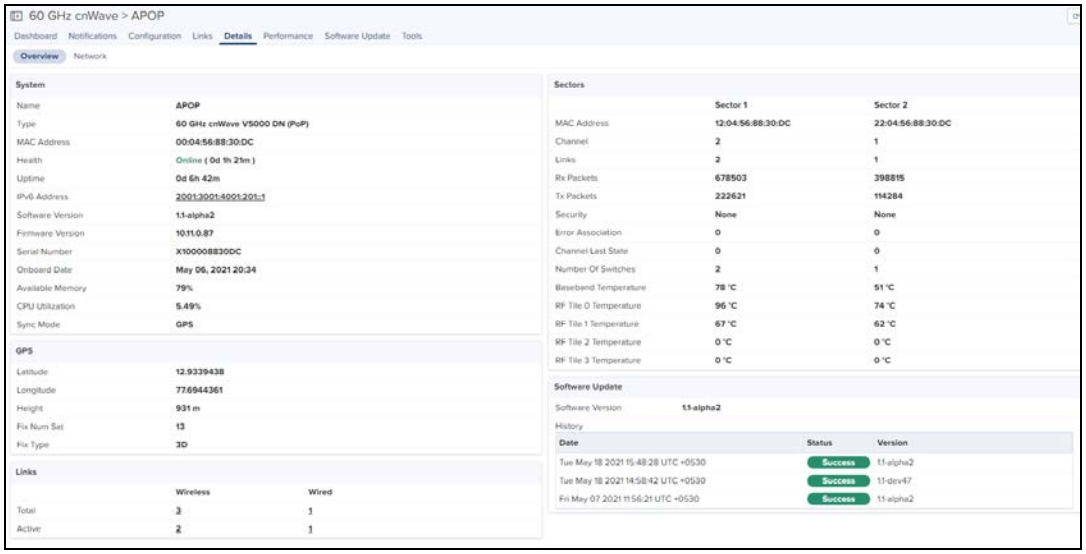
Details page provides the following device information:

- Overview
- Network

Overview

Overview page provides the device details and it also details of the last 3 software update history.

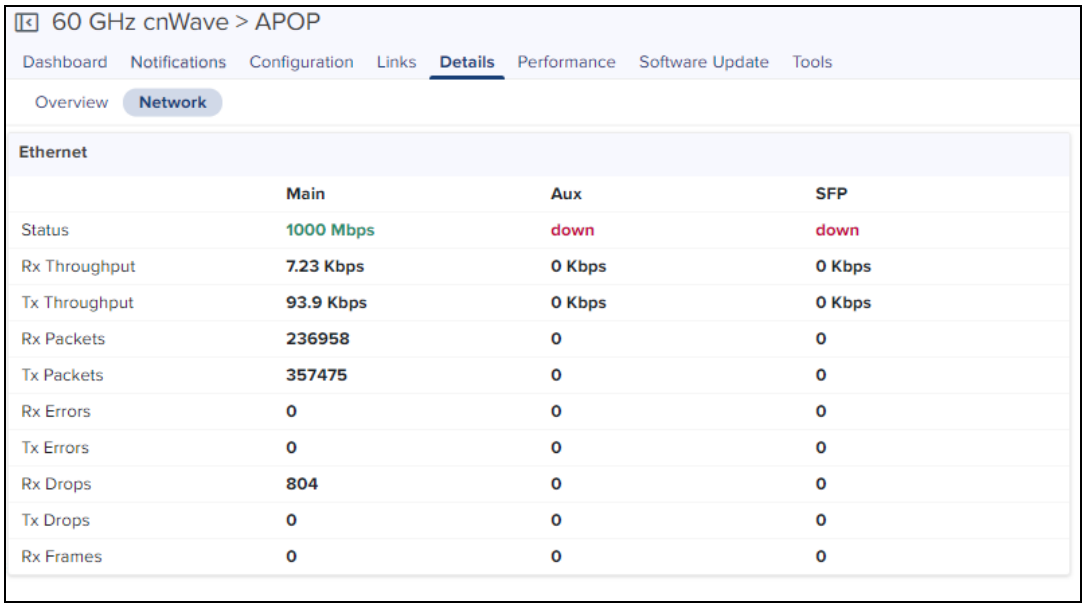
Figure 108 Details Overview Page



Network

Network page provides the **Ethernet** details of **Main, Aux**, and **SFP**.

Figure 109 Details Network Page



Tools

In Tools page user can able to view the **Status** and **Debug** of the device.

Status

In **Status** tab you can view the status of the device:

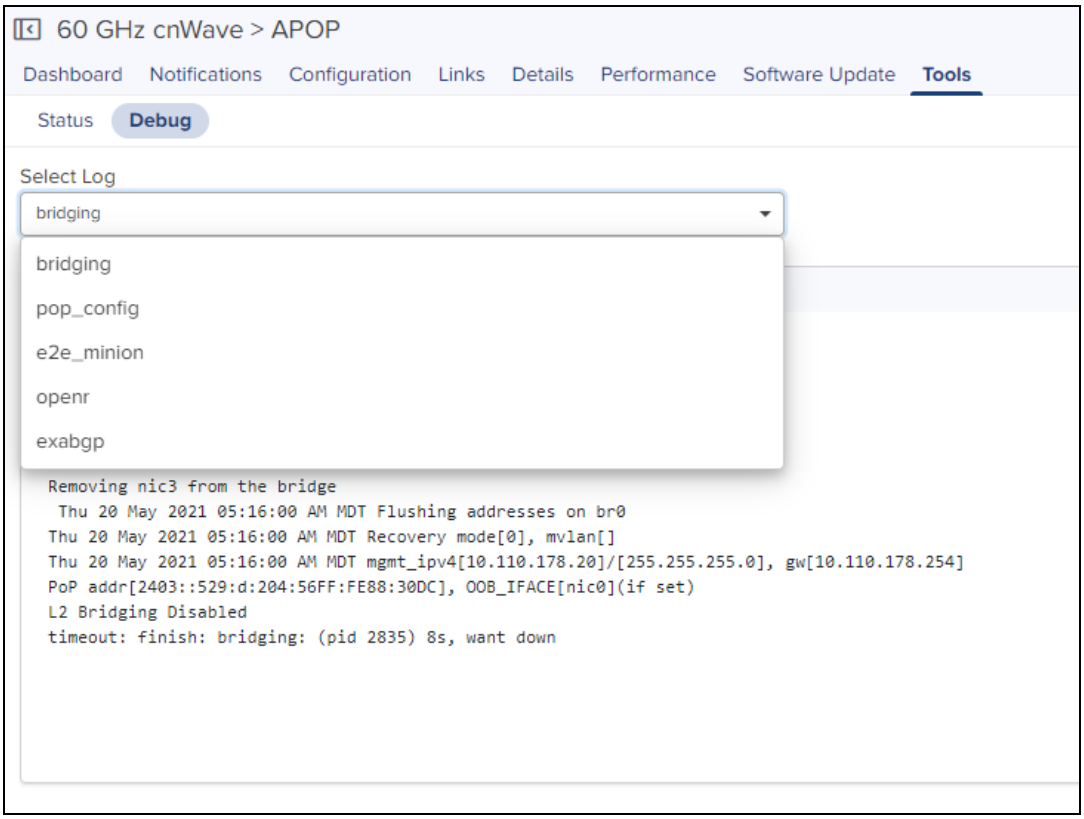
- Critical alarms
- Download Tech Support File
- Online or Offline

- Reboot the device.
- Restart Minion

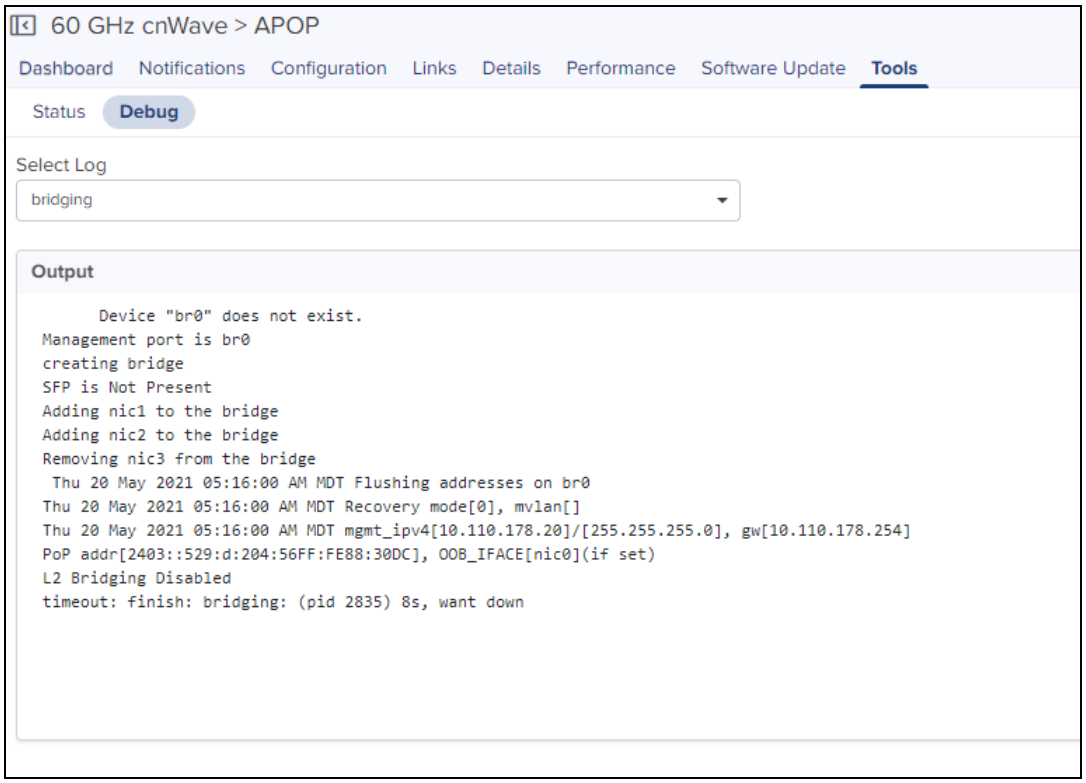
Debug

In **Tools > Debug**, select the below mentioned command type from the drop-down:

- Bridging
- pop-config
- e2e_minion
- openr
- exabgp



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.

DN/CN Node

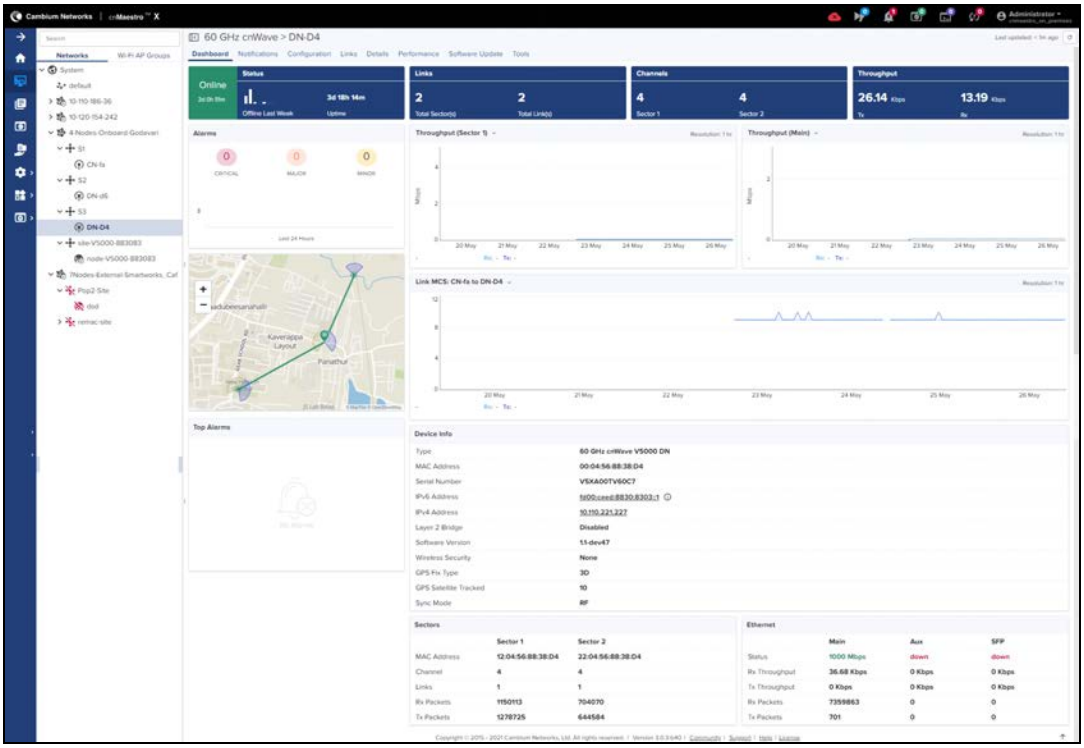
To create a new site, refer to Site.

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 110 DN/CN Node Dashboard



Configuration

Configuration page allows the user to configure the following details of CN/DN:

- Basic
- Radio
- Network
- VLAN
- Security
- Adavanced

Basic

It allows to configure and reset the basic details of DN/CN node such as **Description, Azimuth**, and **Elevation**.

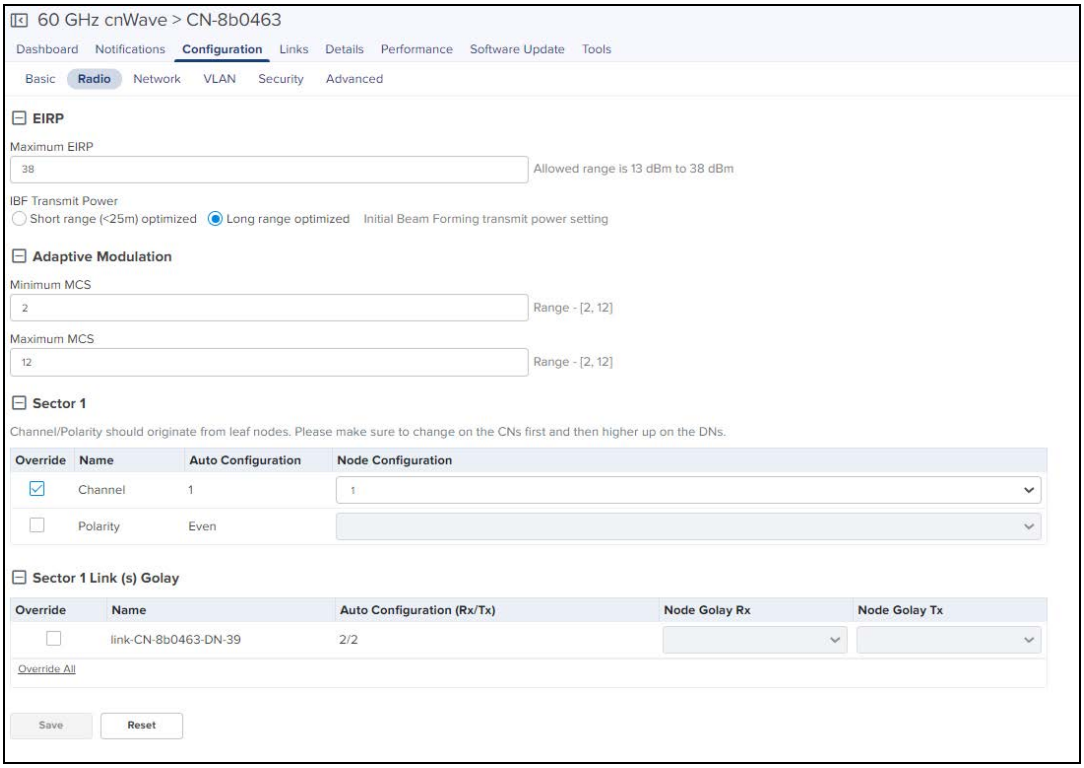
Figure 111 Basic

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**.

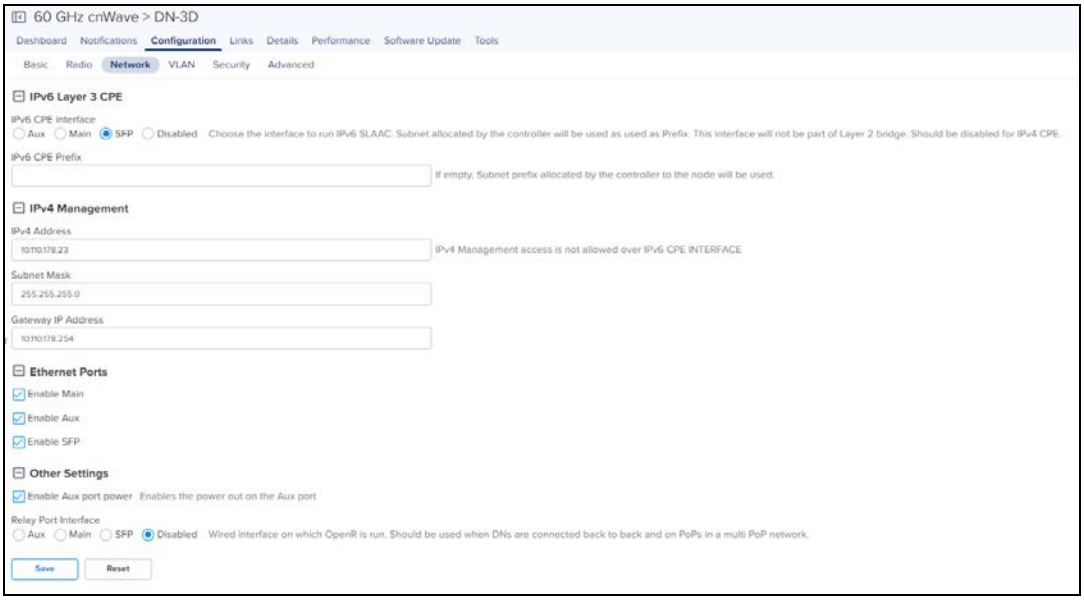
Figure 112 Radio



Network

Network tab allows the user to edit the **Layer 3 CPE, IPv4 Management**, **Ethernet Ports,** and **Other Settings.**

Figure 113 Network



VLAN

VLAN configuration of CN/DN is same as PoP Node VLAN as shown above.

NOTE:

Enable Layer 2 Bridge in **60 GHz cnWave > Configuration > Basic** page to configure the CN/DN VLAN.

Security

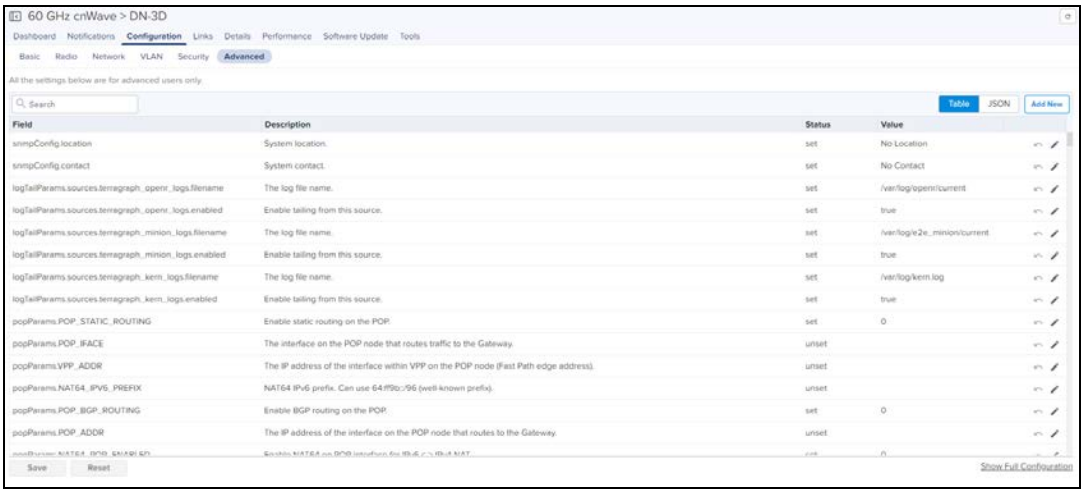
Security tab allows to reset the identity and password of the Radius user.

Figure 114 Security

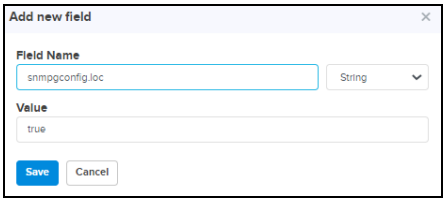
Advanced

Advanced tab allows the advanced user to set Field Name and Value.

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



3. Enter the **Field Name** and **Value.**



4. Click **Save.**

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.

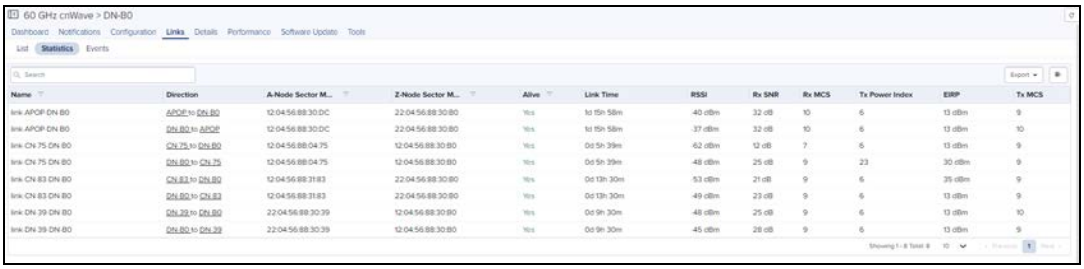
List

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 115 List

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.



Events

Events provides the details of the links from last 1 hour to 7 Days, Ignition Attempts and Distance.

Figure 116 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** and **Debug** of the device.

Status

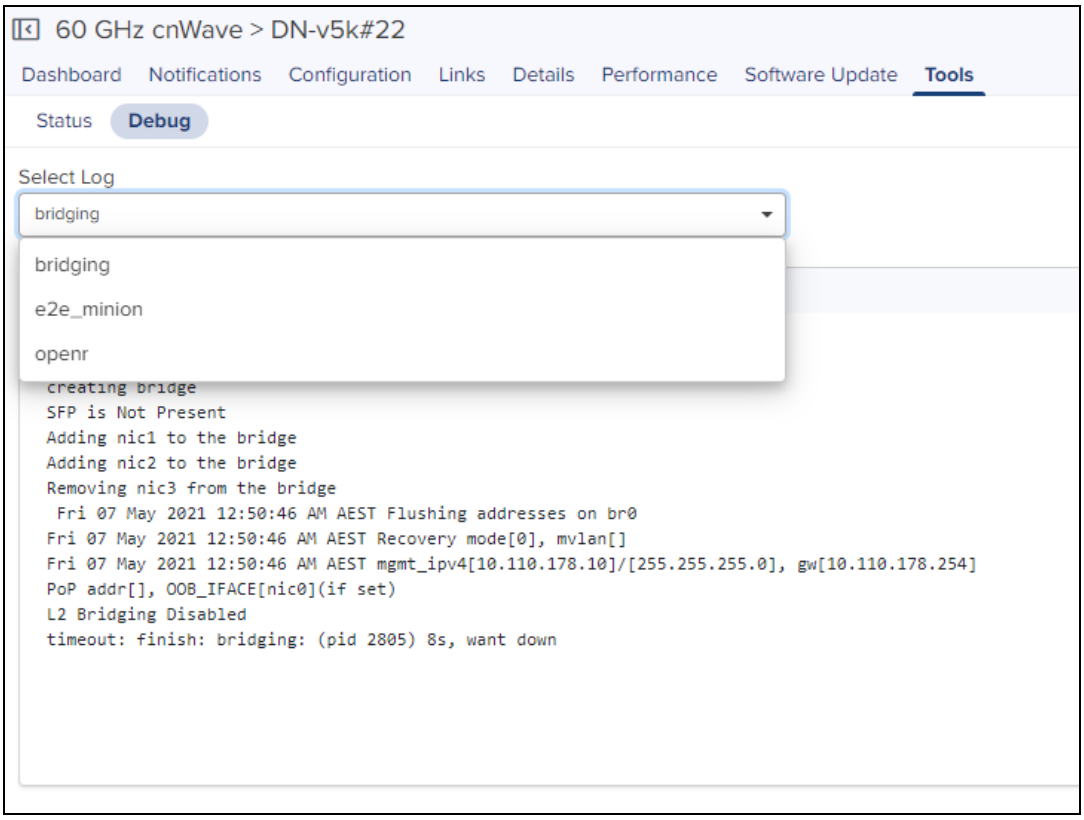
In **Status** tab you can view the status of the device:

- Critical alarms
- Download Tech Support File
- Online or Offline
- Reboot the device.
- Restart Minion
- Factory reset

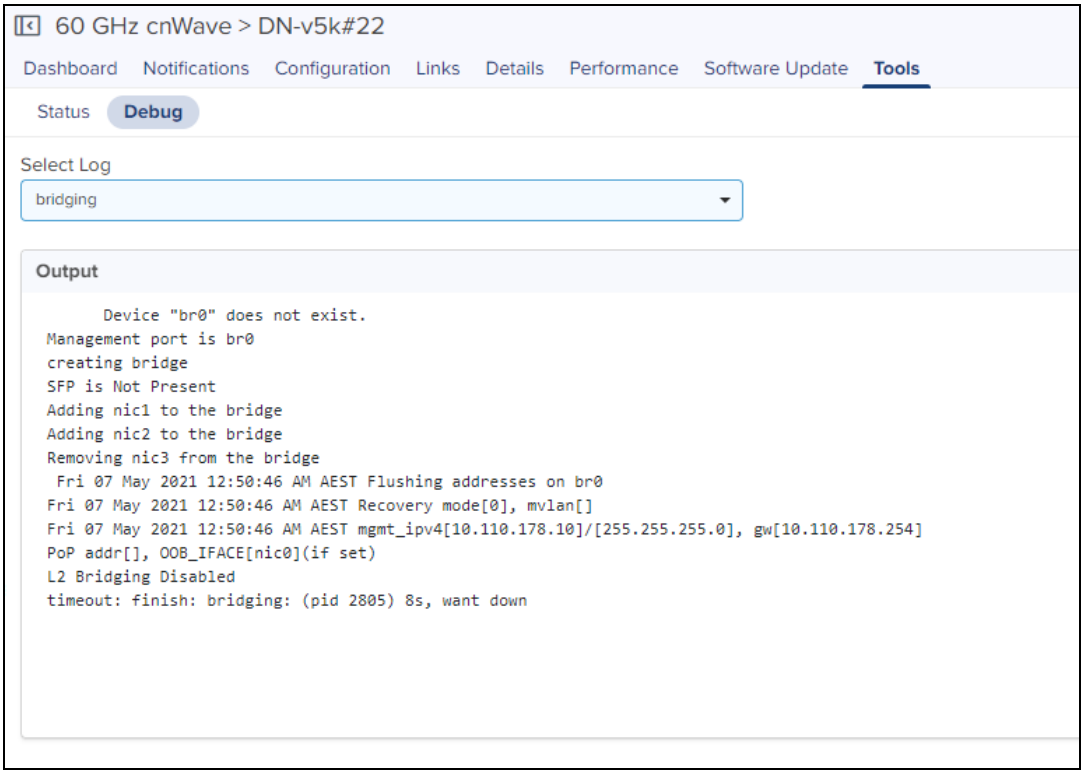
Debug

In **Tools > Debug**, select the below mentioned command type from the drop-down:

- Bridging
- e2e_minion
- openr



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.

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:

1. Navigate to **Shared Settings > Auto-Provisioning** page.

2. Click **Add** and following window appears.

Figure 117 Auto-Provisioning - Wireless Devices

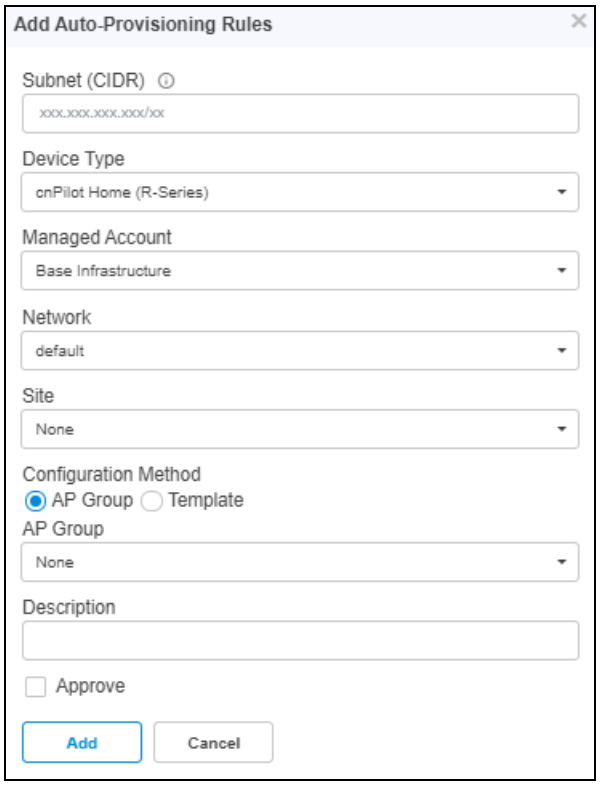
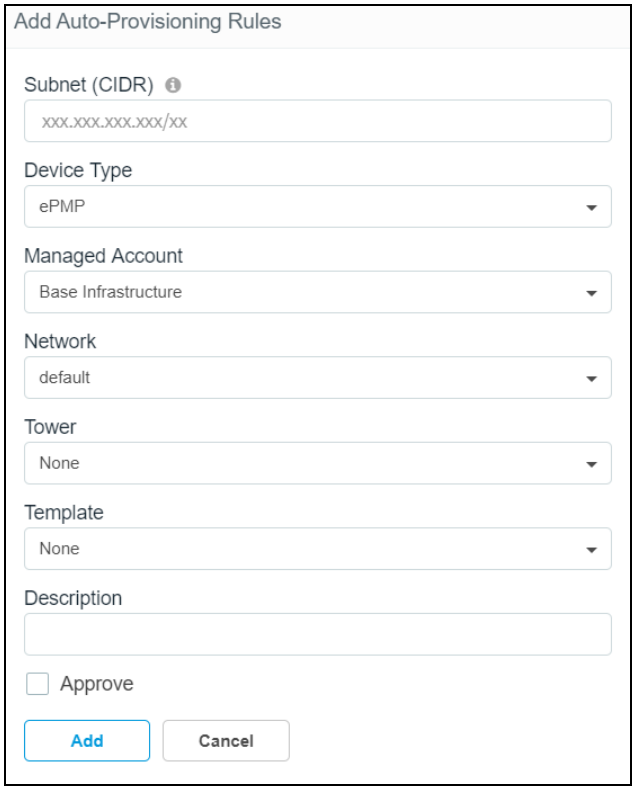


Figure 118 Auto-Provisioning - Fixed Devices



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**.

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

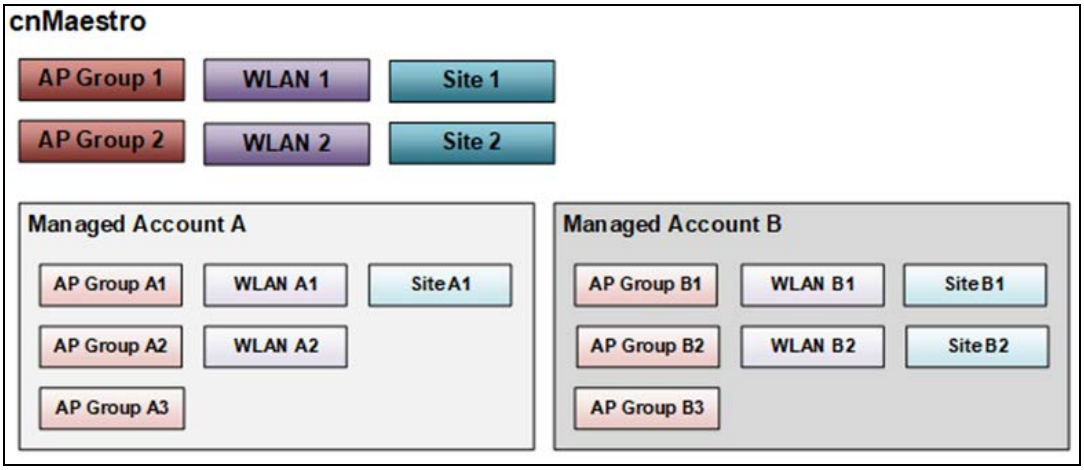
Overview

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 119 Managed Accounts



Scope

An account with MSP enabled has three scopes:

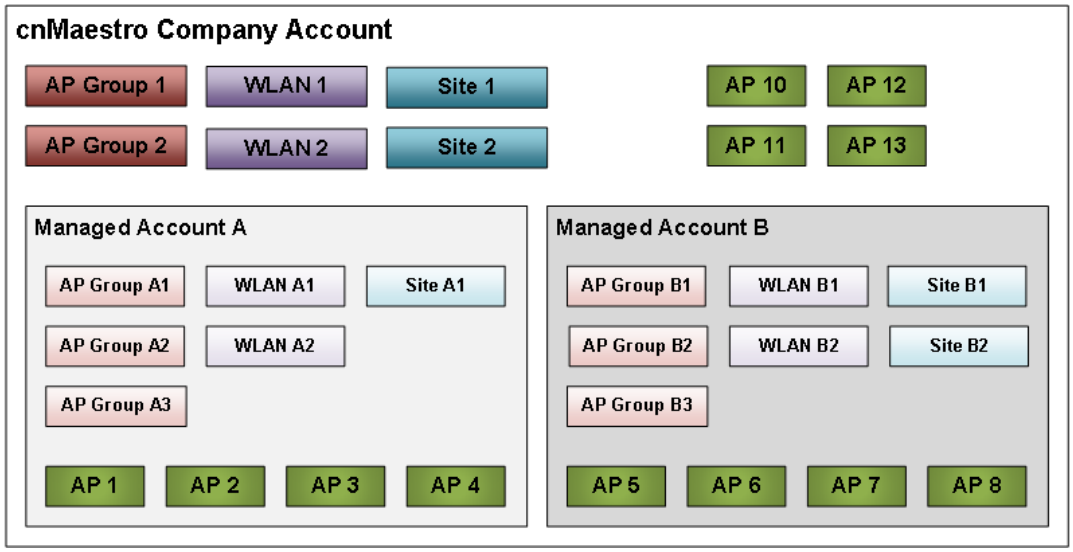
1. Global Scope for entities (Devices, Networks, Sites, etc.) that exist outside of Managed Accounts and are only available to Global cnMaestro Administrators.
2. Managed Account Scope for entities in Managed Accounts and accessible to Global Administrators and Managed Account Administrators.
3. Shared 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.

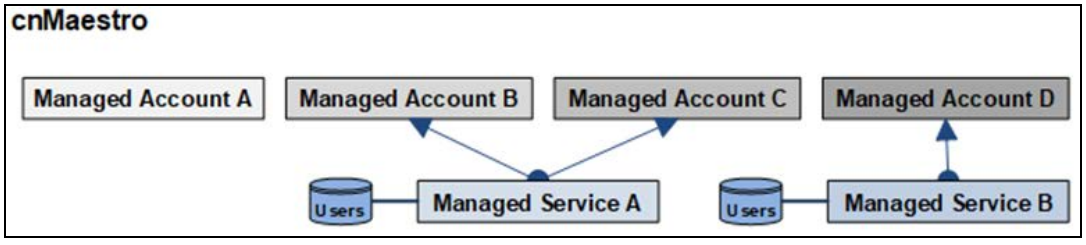
Figure 120 Access Points



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 121 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 122 Managed Account UI - Sample1

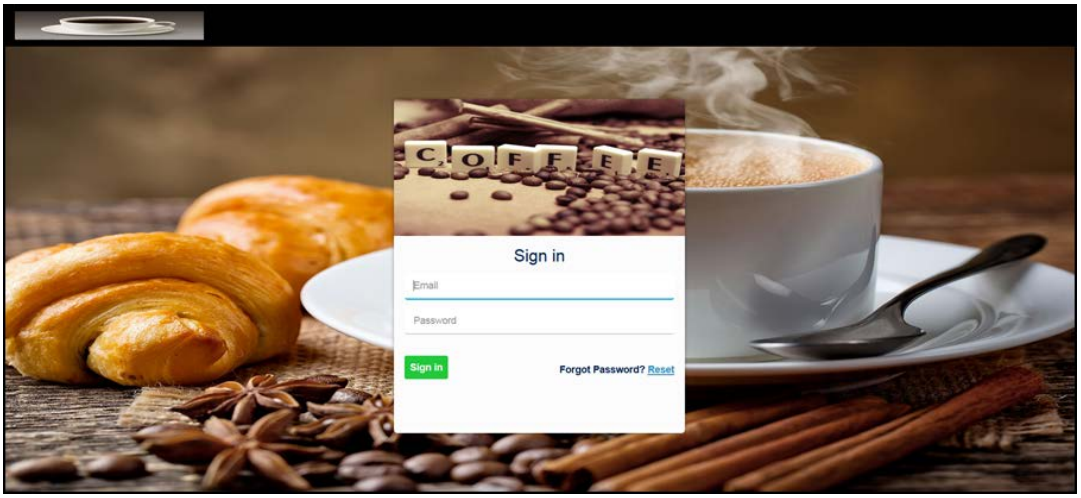
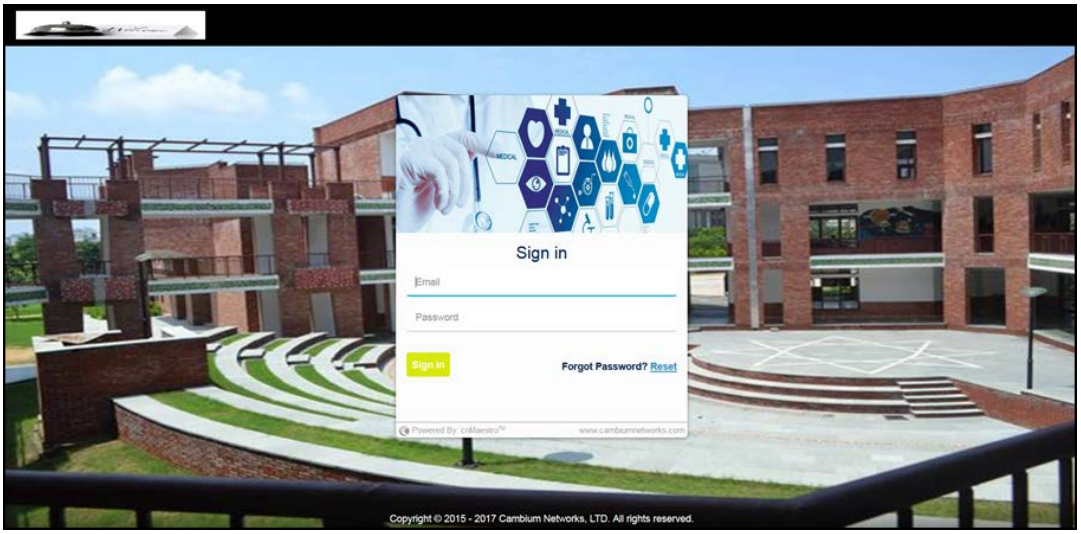
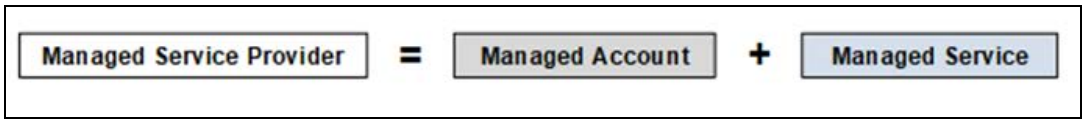


Figure 123 Managed Account UI - Sample2



Managed Service Provider (MSP)

The MSP feature combines Managed Accounts with Managed Services.



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 33: 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 33: Tenant Administrator Roles

Feature	Description	Administrator	Operator	Monitor
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

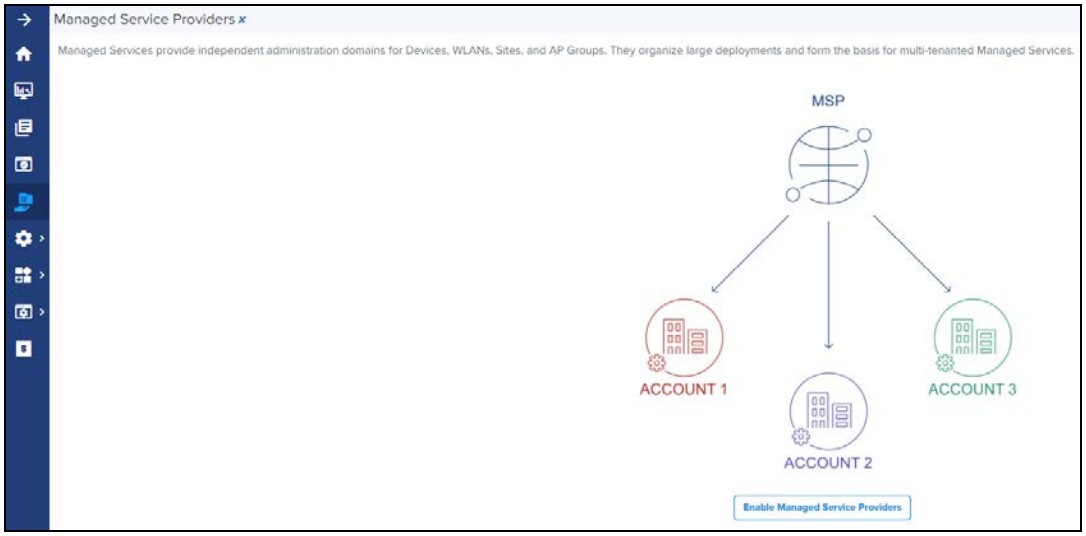
Enable Managed Service Provider (MSP)

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**.

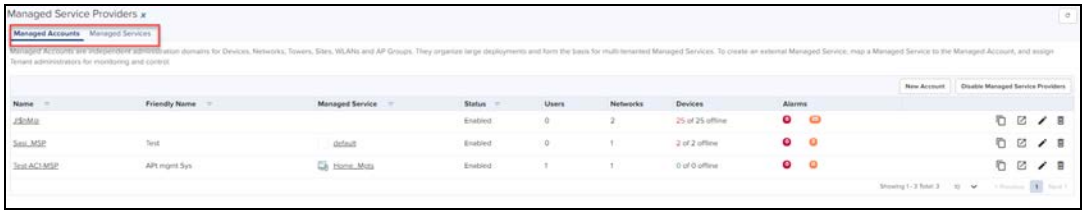
Figure 124 Enabling Managed Services



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 125 Managed Account and Managed Services Tabs

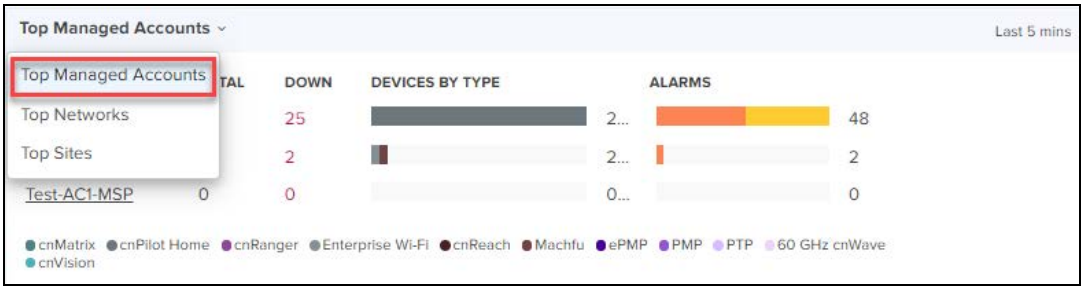


- The Header adds a select box that allows the global administrator to enter the context of Managed Accounts

Figure 126 MSP Component in Header

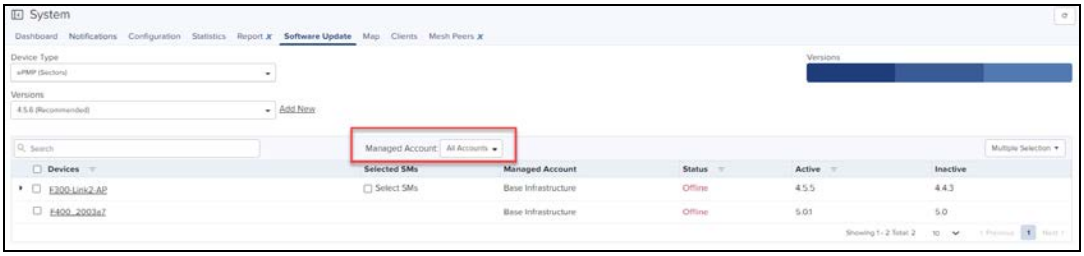
- The System Dashboard adds a Health component for Managed Accounts

Figure 127 Dashboard > Managed Accounts



- Global tabs in the UI are updated with a Managed Account column.

Figure 128 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 one 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.

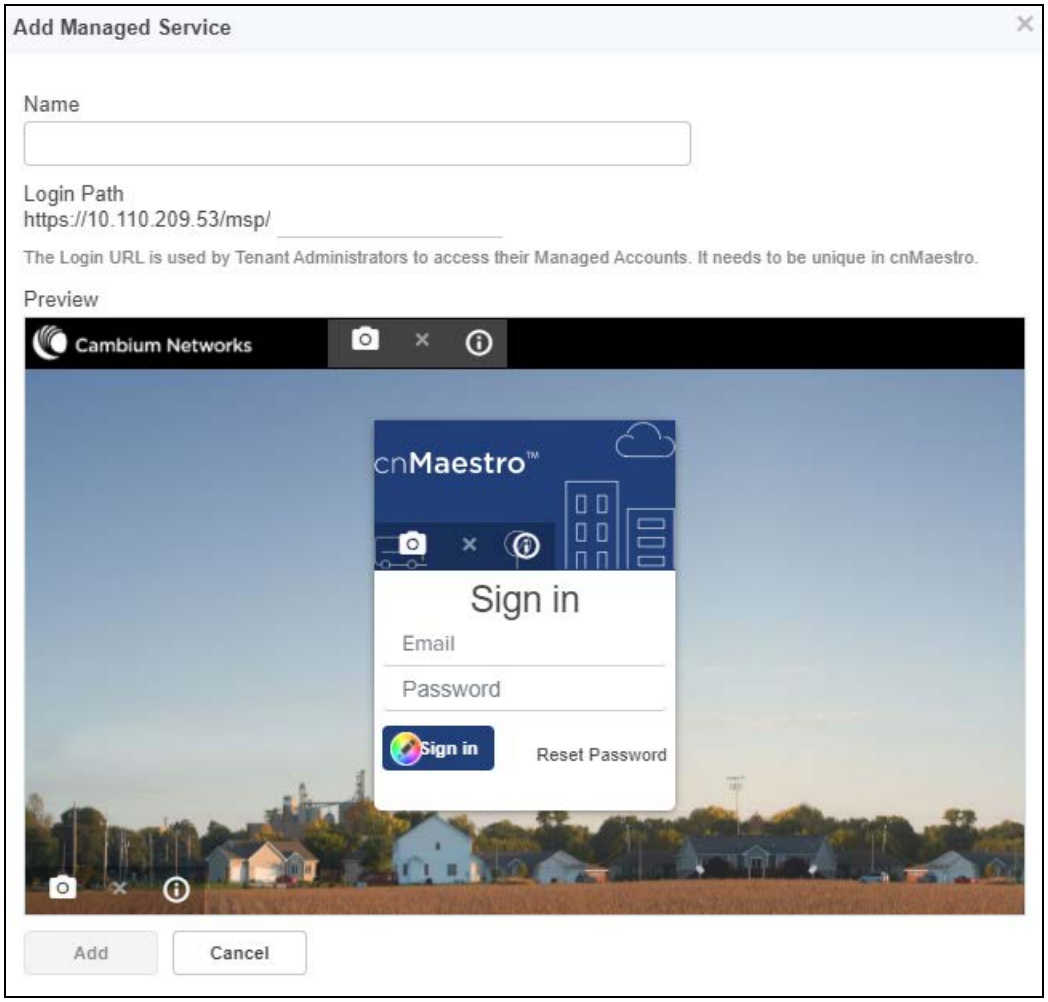
Figure 129 Managed Services Tab

2. Click **Managed Service**.

Figure 130 Adding a New Managed Service

The following window appears.

Figure 131 Add New Managed Service Window



3. Enter the following details:

Table 34: 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: https://<cnmaestro on-premises ip>/msp/<Managed_service_path> **Note:** • 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.

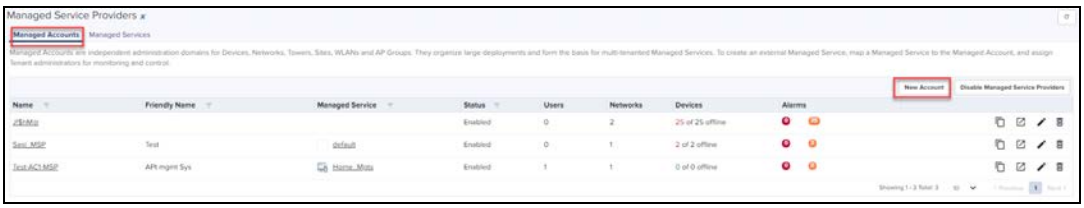
4. Click **Add**.

Create Managed Account

Perform the following steps to create a Managed Account:

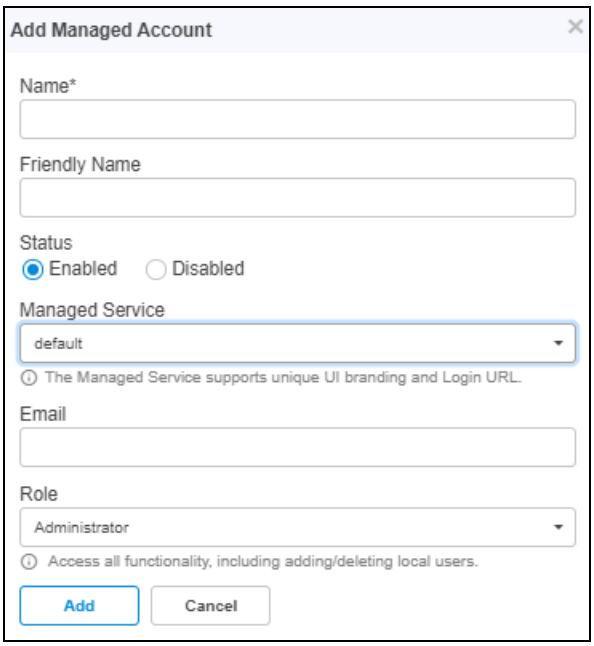
1. Select **Managed Service Providers** in the side-menu and select the **Managed Account** tab.
2. Click **New Account**.

Figure 132 Managed Account Tab



The following window appears.

Figure 133 Add Managed Account window



3. Enter the following details:

Table 35: 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.
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).

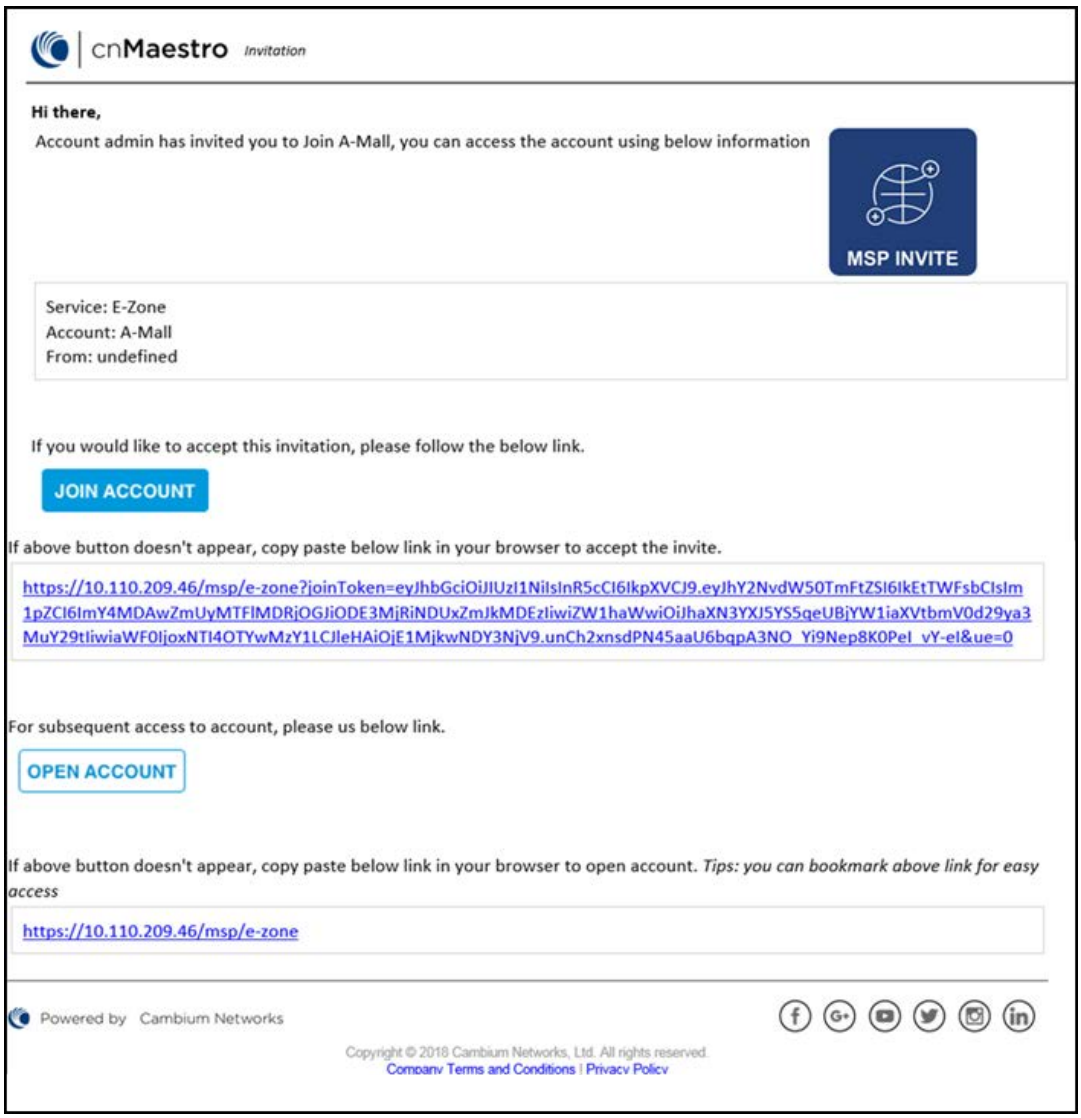
4. Click **Add**.

	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.

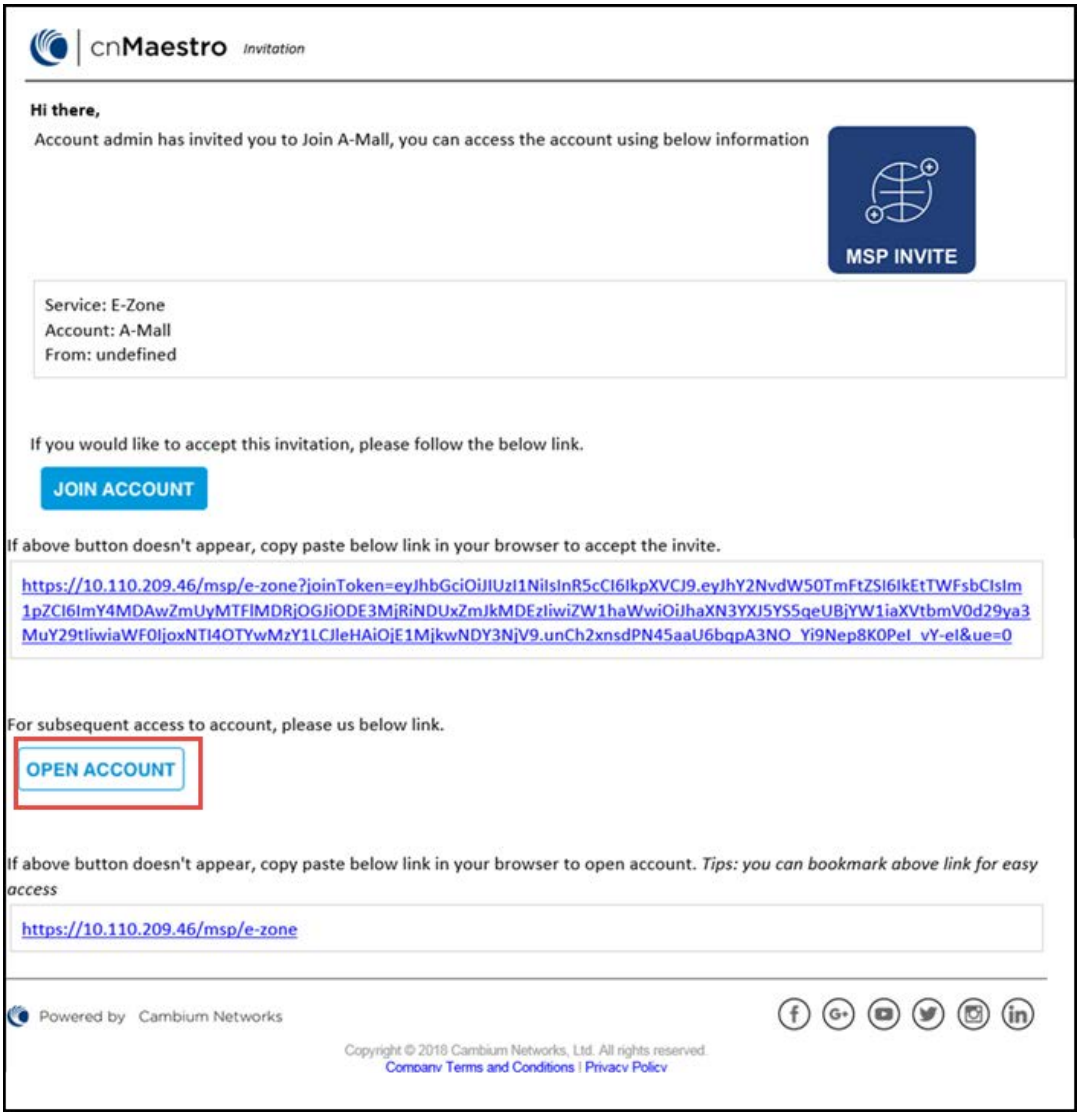
Figure 134 Sample Email Invitation



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 135 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 136 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

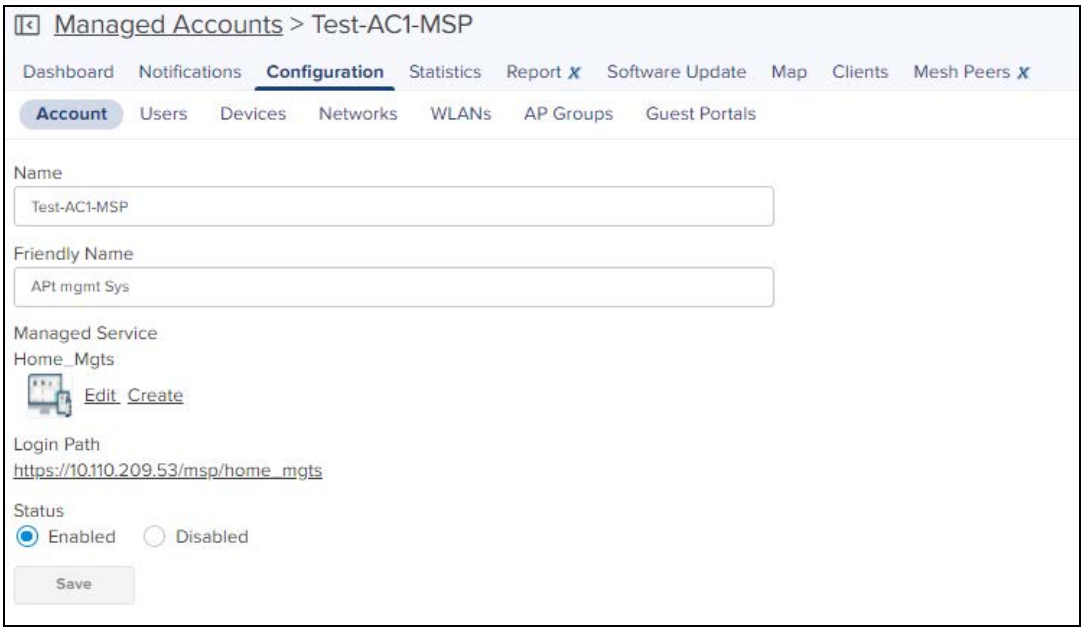
At the System level, one can view APs, AP Groups, or Sites across all Managed Services in a single, unified table. This allows one to review the status of all accounts in context to each another. The following figure displays the AP table, and specifies which APs are mapped to the Managed Accounts.

Figure 137 System View

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, Software Update, Reports, Clients, etc.

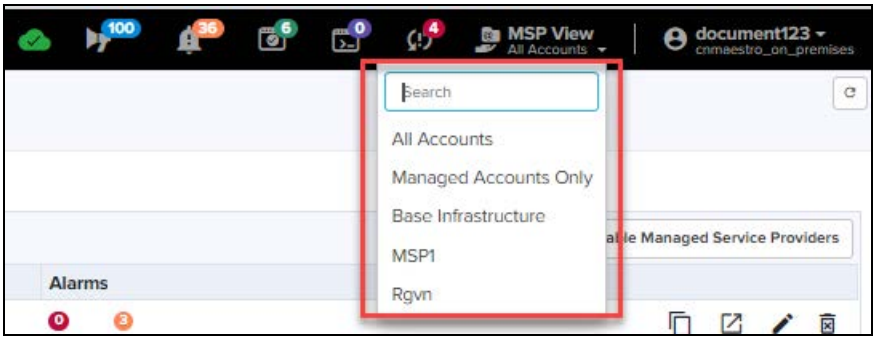
Figure 138 Managed Account View



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.

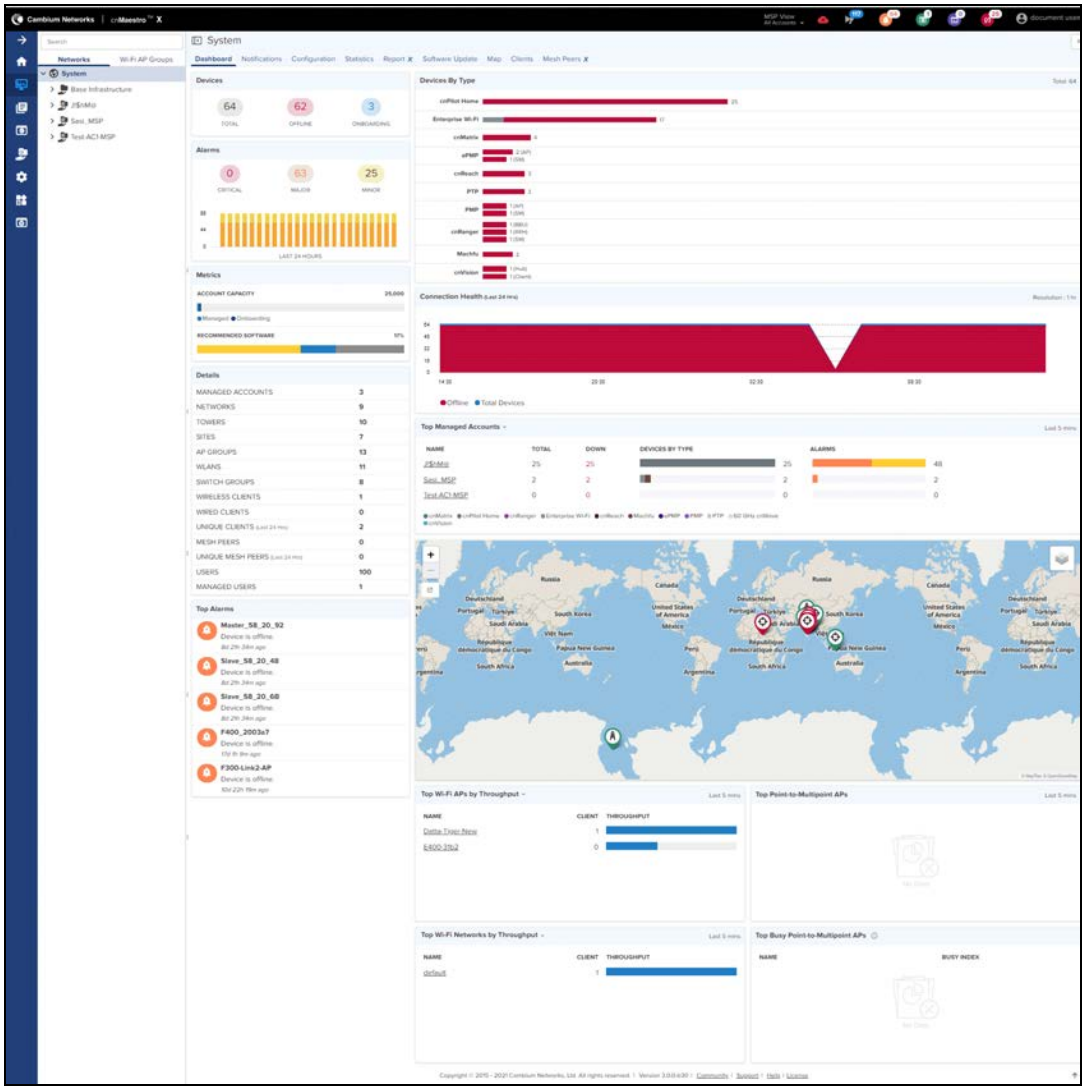
Figure 139 Managed Account View



System Dashboard

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

Figure 140 System Dashboard



Managed Account Administration

Object Scope

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

Table 36: 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.

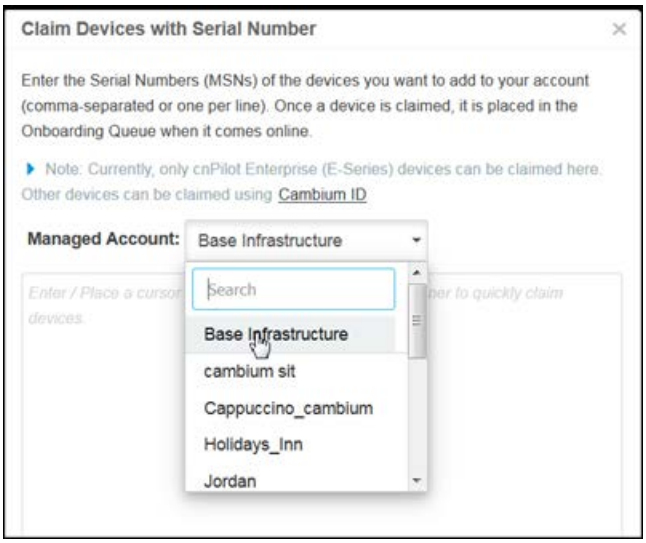
Device Management

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 141 System Onboarding



Management Account Onboarding

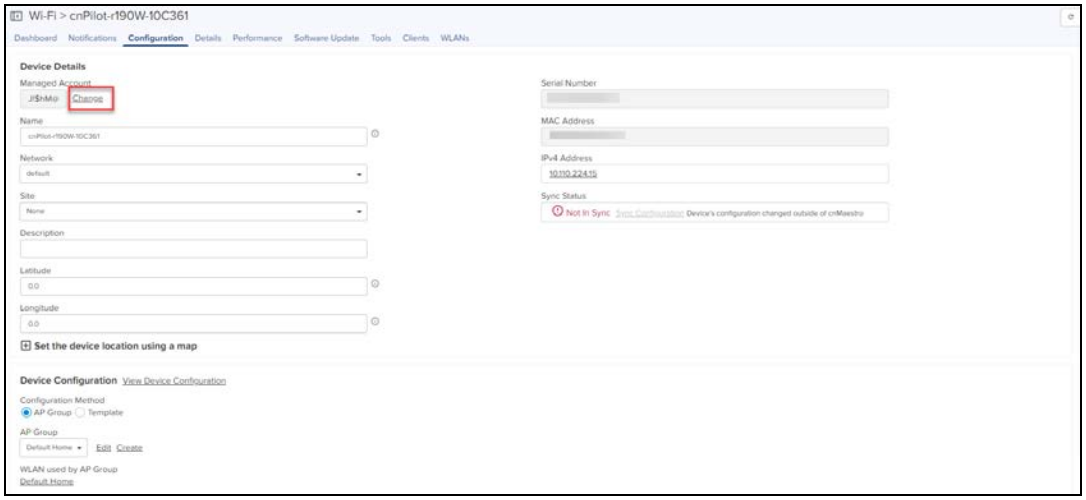
Onboarding through the Managed Account UI automatically places the devices in the Managed Account.

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

Moving a Device Between Managed Accounts

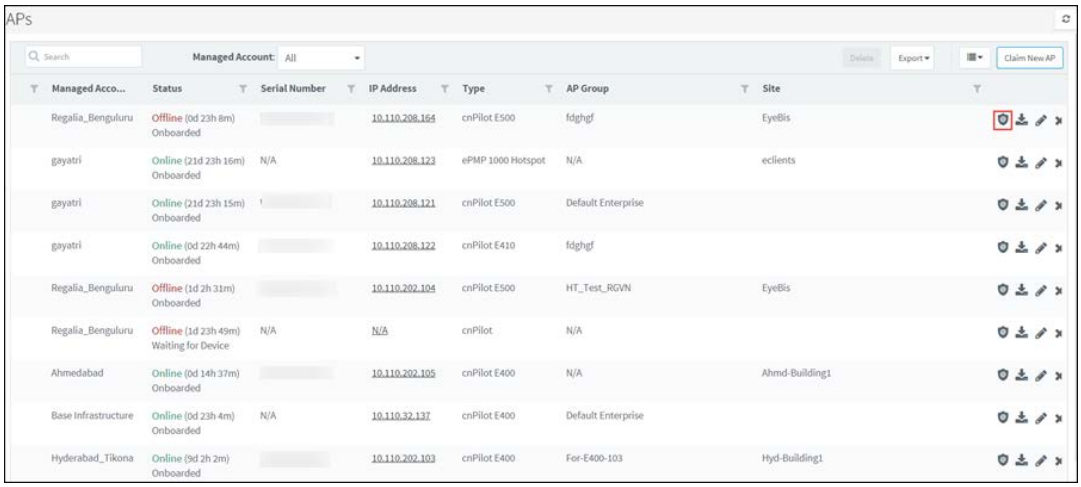
You can move a device from one Managed Account to another by using the **Change** option in account device managed page.

Figure 142 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 143 Moving a device between Managed Accounts in Enterprise View



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 144 Managed Account Deletion

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

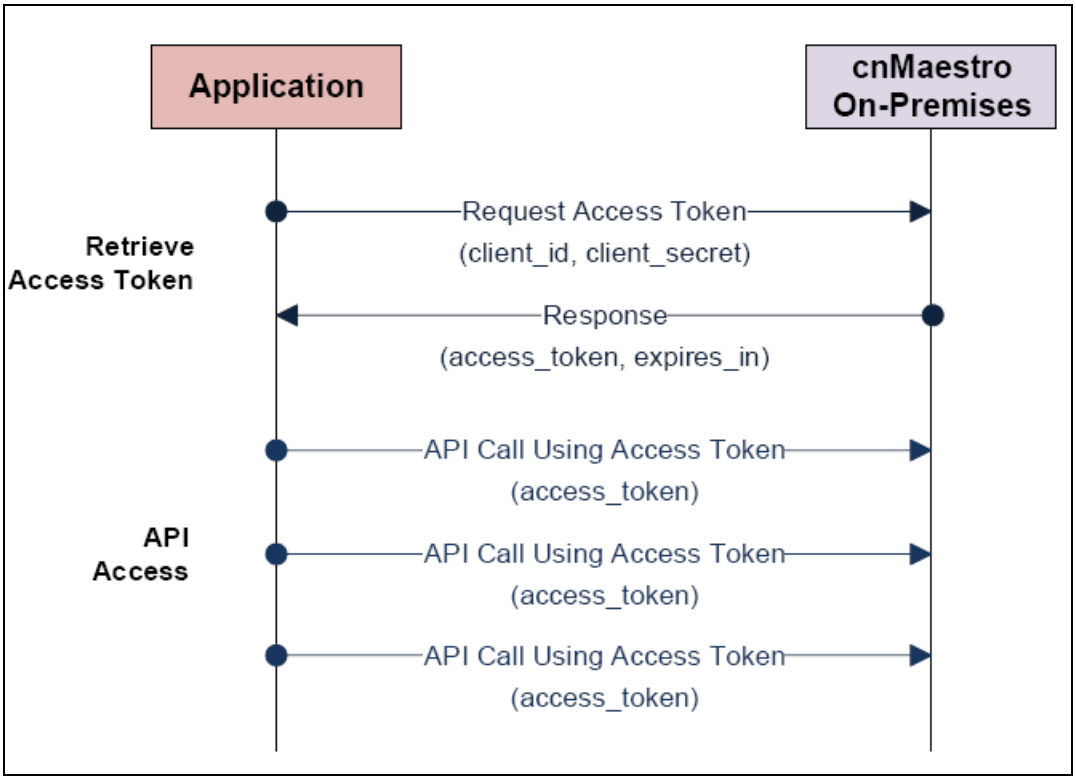
API Clients are external applications that access the RESTful API over HTTPS using OAuth 2.0 Authentication. They require a Client ID and Client Secret for access, both of which are detailed later in this section. They are configured by navigating to **Services > API Clients**.

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.



Establish 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

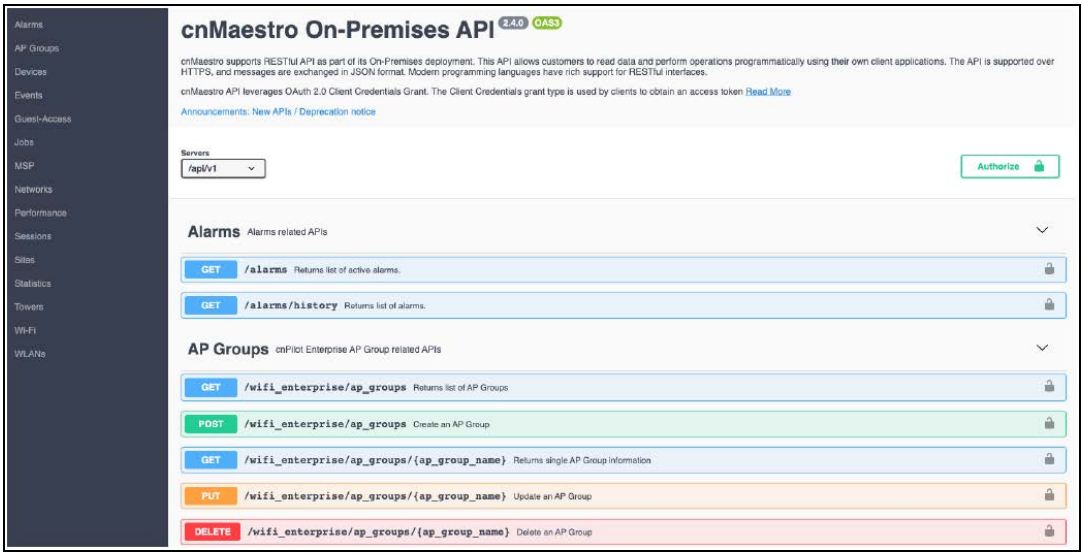
Request Rate Limiting is not enabled in the On-Premises version of cnMaestro. It is up to the application owner to make sure requests do not overtax the system.

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

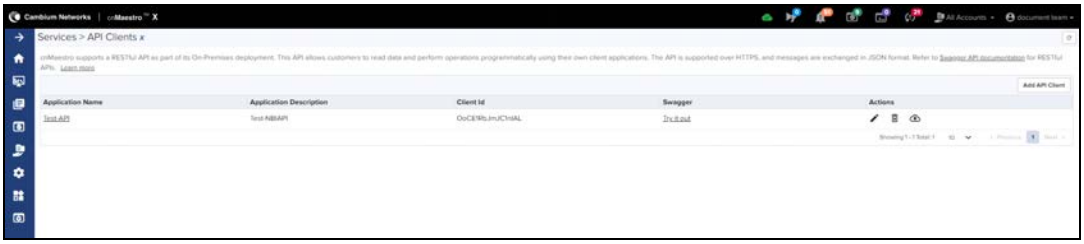


Client ID and Client Secret Generation

cnMaestro User Interface

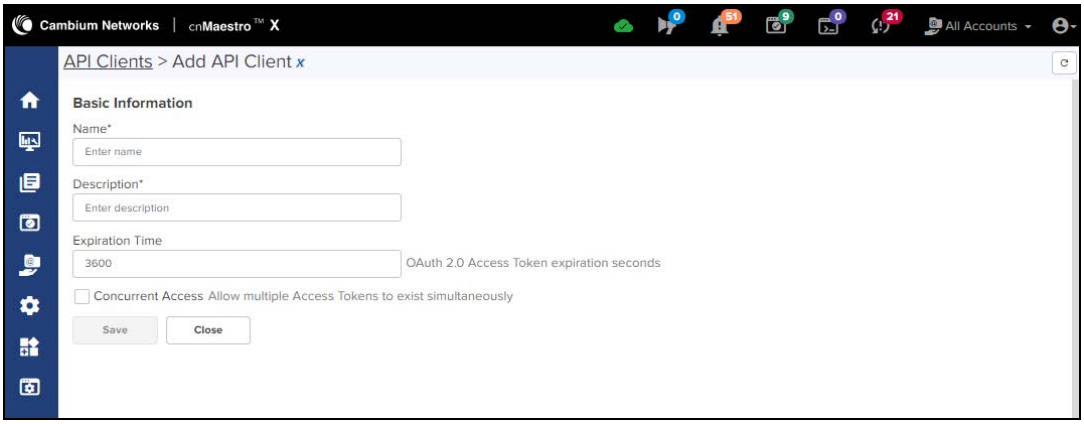
The Client Id and Client Secret are created in the cnMaestro UI by navigating to **Services > API Client**. Each client application should be added as an API Client.

Step 1: Navigate to Services > API Clients



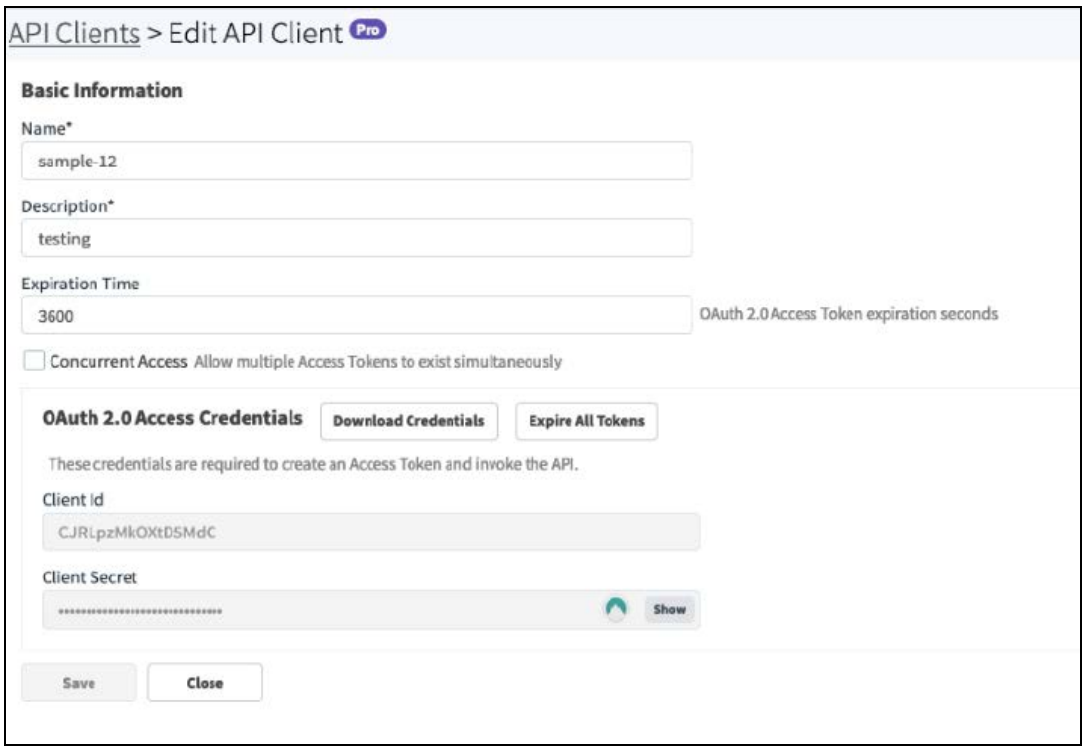
Step 2: Create a New API Client

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 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

cnMaestro On-Premises

> **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":"2YotnFZFEjr1zCsicMWpAA",
"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
invalid_request	Required parameter is missing from the request.
invalid_client	Client authentication failed.
unauthorized_client	The client is not authorized to use the grant type sent.
unsupported_grant_type	The grant type is not supported.

An example error response is below:

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

Access Resources

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 will give 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).
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": "W8SF0759MBDH",
"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
`/api/v2/access/token`

Generate an Access 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.

```
{
"access_token":"2YotnFZFEjr1zCsicMWpAA", "token_type":"bearer",
"expires_in":3600
}
```

Example

Request

curl https://10.110.134.12/api/v2/access/token \

```
-X POST -k \
-u 8YKCxq72qpjnYmXQ:pcX5BmdJ2f4QLM5RfgsS4jOtxAdTRF \
-d grant_type=client_credentials
```

Response

```
{"access_token":"d587538f445d30eb2d48e1b7f7a6c9657d32068e","token_type":" bearer","expires_
in":86400}
```

Token (alternate request)

POST

`/api/v2/access/token`

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

Request

Headers

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

Body

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

Response

The response to both forms is the same.

Body

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

```
{
"access_token":"2YotnFZFEjr1zCsicMWpAA", "token_type":"bearer",
"expires_in":3600
}
```

Example

Request

curl https://10.110.134.12/api/v2/access/token \

```
-X POST -k \
-d grant_type=client_credentials \
-d client_id=8YKCxq72qpjnYmXQ \
-d client_secret=pcX5BmdJ2f4QLM5RfgsS4jOtxAdTRF
```

Response

```
{"access_token":"ee4e077cf457196eb4d27cf6f02686dc07763059","token_type":" bearer","expires_
in":86400}
```

Validate Token

GET

`/api/v2/access/validate_token`

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

Request

HTTP Headers

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

Response

Body

Name	Details
expires_in	Time in seconds that the API session will remain active.

```
{
'expires_in': 86399
}
```

Example

Request

curl https://10.110.134.12/api/v2/access/validate_token \

```
-X GET -k \
-H "Authorization: Beareree4e077cf457196eb4d27cf6f02686dc07763059"
```

Response

```
{"expires_in":85643}
```

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	cnReach	cnVision	PTP	cnMatrix	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	
link_symmetry	Link symmetry						X		

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	cnMatrix	60 GHz cnWave
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

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.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	

Name	Details	ePMP	PMP
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
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	

Name	Details	ePMP	PMP
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 utiliization	All
ethports[].speed	Ports speed and duplex	All
ethports[].tx_util	Ports transmit bandwidth utiliization	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

Name	Details	Mode
ip_wan	WAN IP	All
lan_mode_status	LAN mode status [no-data, half, full]	Enterprise
lan_speed_status	LAN speed status	All
lan_status	LAN status [down, up]	Home
netmask	Network mask	All

Radios (Array format)

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

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
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)

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

cnReach

General

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

Radios (Array format)

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

Fixed Wireless (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	
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	

Name	Details	ePMP	PMP
radio.ul_snr_h	Uplink SNR (dB) horizontal		SM
radio.ul_snr_v	Uplink SNR (dB) vertical		SM
radio.ul_throughput	Uplink Throughput (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)

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

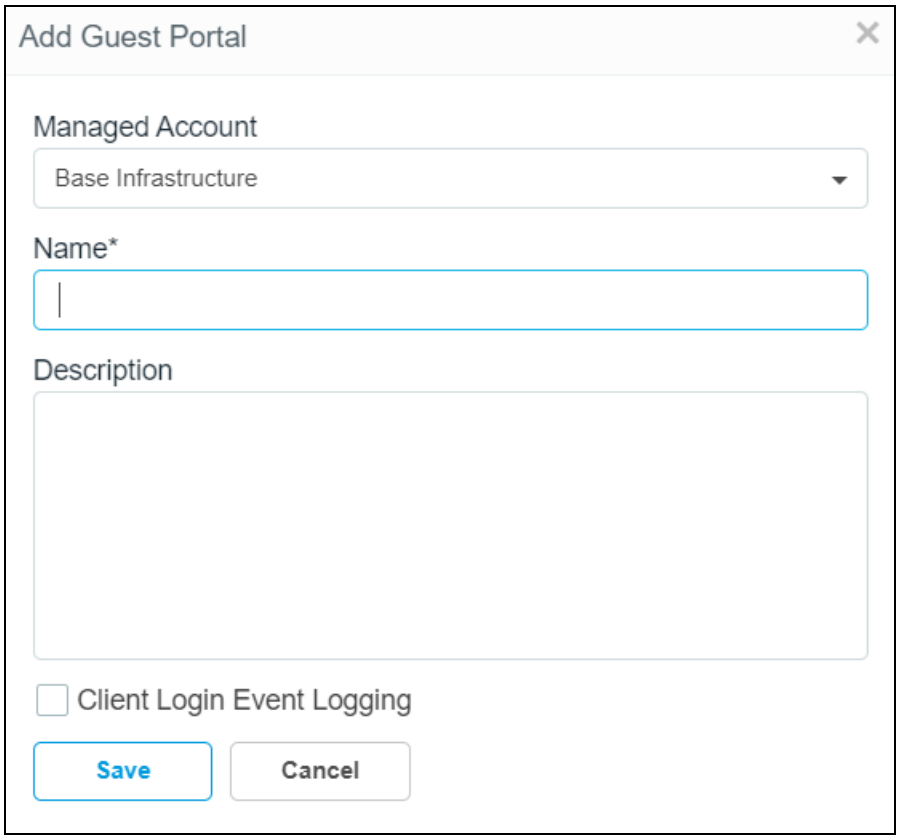
Procedure for creating Guest Access

Prerequisites

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

> **NOTE:**
>
> The Floating Managemnt 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.

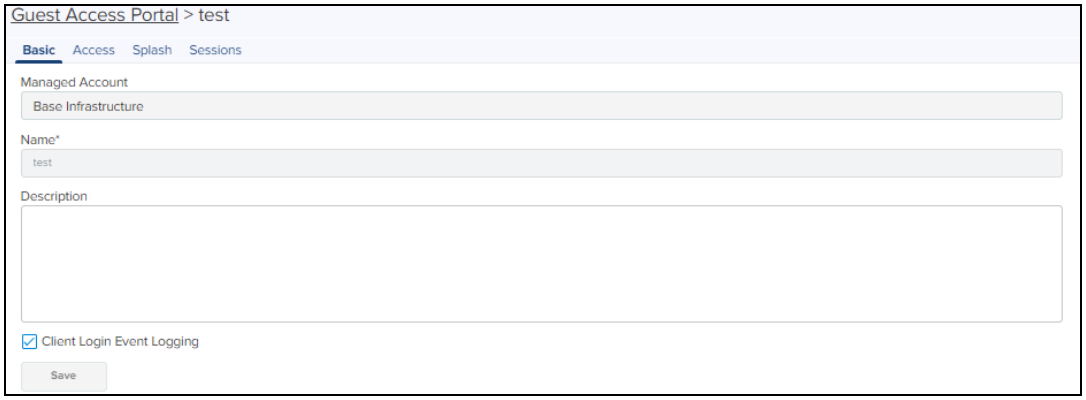
2. Click **Add Portal**. A maximum of four portals can be created per account.
3. Enter **Name** and **Description**.



4. Click **Save.**

Basic Details

The Basic Details page contains the Managed Account Type Name and Description.



NOTE:

A name once created for the Portal cannot be changed.

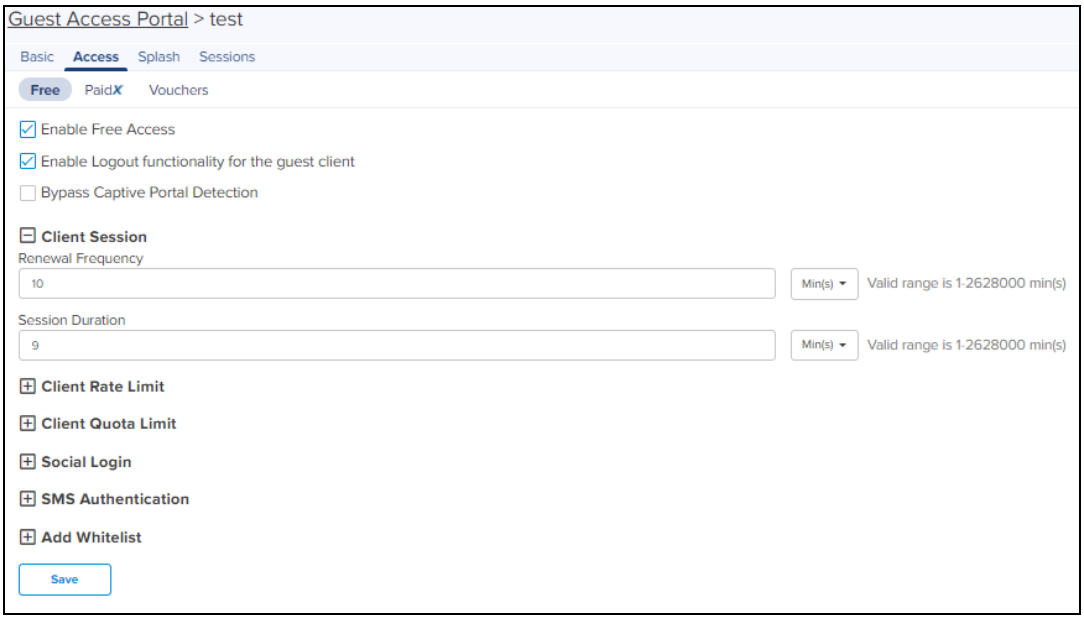
Access Portal

The Access Portal tab has 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 37: 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	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 logins 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. The similar behavior is supported through RADIUS attributes for RADIUS-based onboard guest access clients. RADIUS_VENDOR_ID_CAMBIUM 9 (17713) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP (151) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN (152) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP_GIGWORDS (153) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN_GIGWORDS (154) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL (155)

Table 37: 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: • 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:

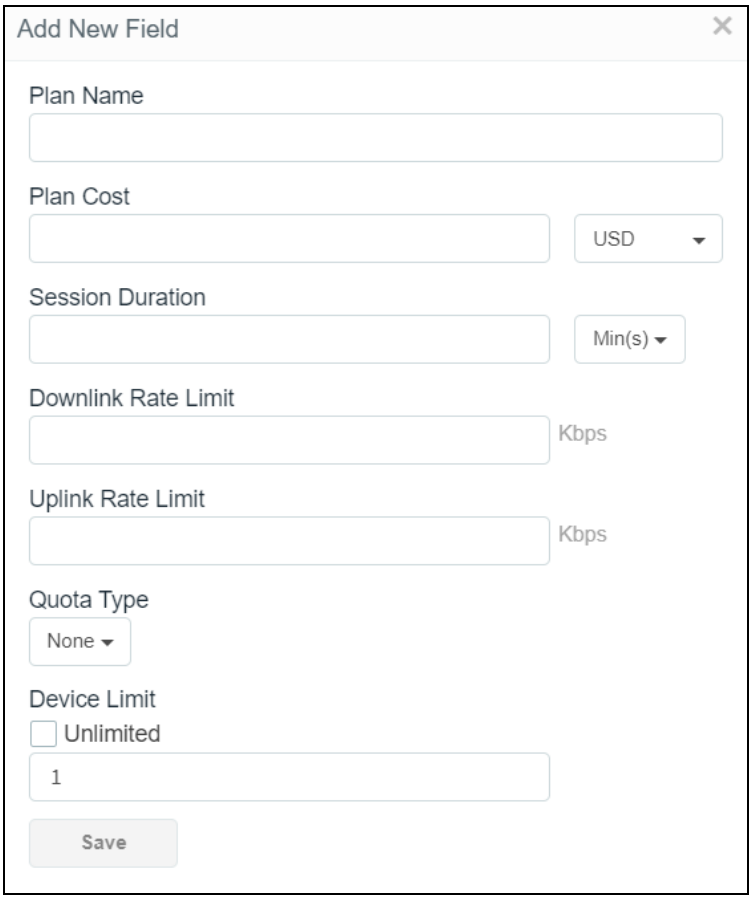
- Renewal frequency should be greater than session expiration.
- Client will get Social login options only when enabled in Access Control page in portal.
- If Social login is enabled, it is mandatory in free access method for client to login through Google/Facebook/Twitter/Office 365.

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 38: Paid Access Type Parameters

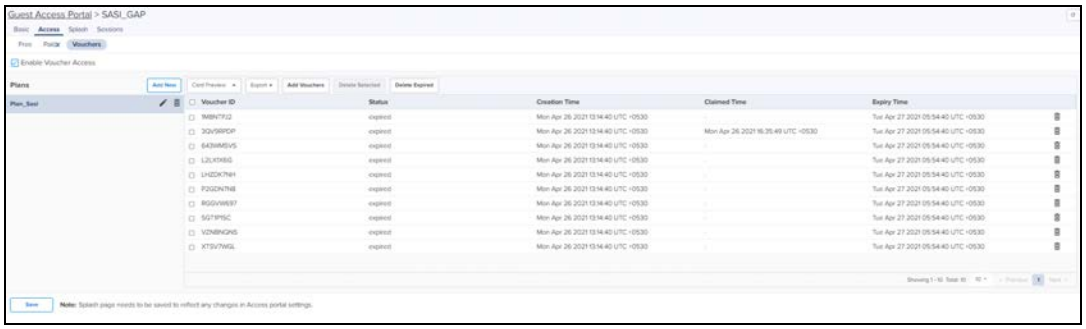
Parameter	Description
General	• **Plan Name**: The name of the plan. • **Session Duration:** The duration for which the client is allowed network access. • **Client Rate Limit**: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter 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.



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 39: Voucher Access Type Parameters

Parameter	Description
Design	• **Color:** There are options to modify colors for the title, message, code, and background. • **Background Image:** You can browse and select a background image for this page. • **Title**: The tiltle of the voucher plan. • **Message:** Detailed information about the plan. • **Access Code Message:** 8 digit access code will be provided to use the voucher. With all the above parameters, administrators can create their own design for the card with text, color and message to be displayed on card.
General	• **Name**: The name of the plan. • **Session Duration:** The duration for which the client is allowed network access. • **Voucher Expiry**: The expiry time for the generated vouchers. Once this time lapses, the Vouchers cannot be used. • **Client Rate Limit**: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a **Client Rate Limit** parameter is blank, no limits are applied.

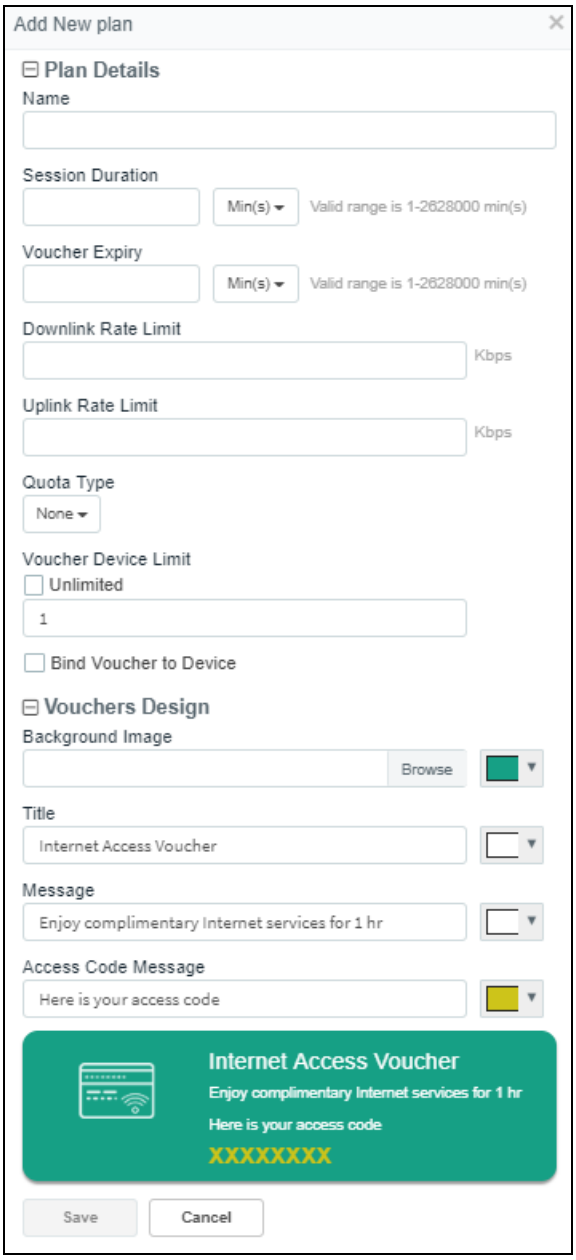
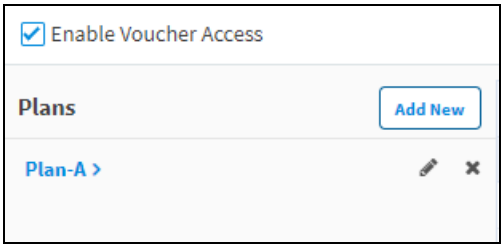


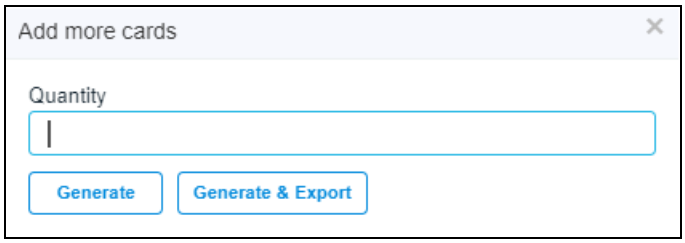
Table 40: Adding Vouchers

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

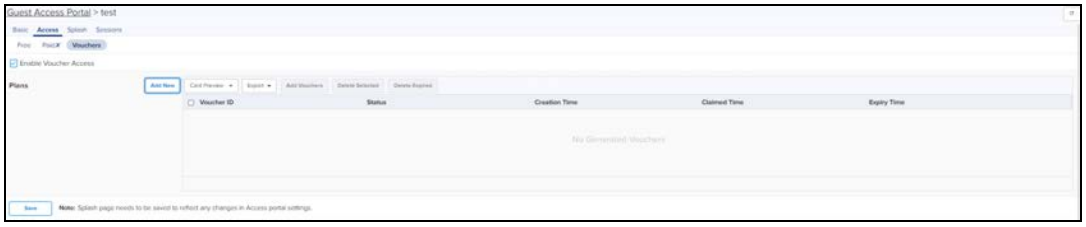
a. **Select a plan**



b. **Add Vouchers**



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



c. **Sample Voucher Code**

NOTE:
The modified values in the Access Portal page reflectes 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.

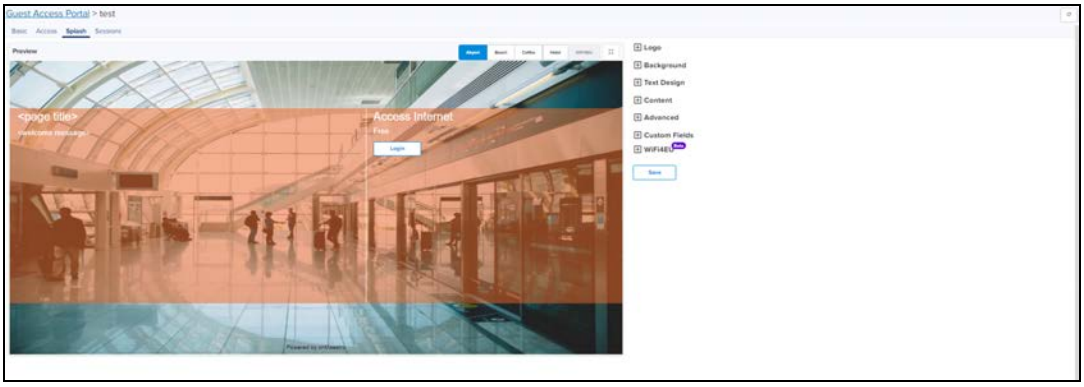


Table 41: Splash Page Parameters

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.
Terms Agree Button	Text to appear in the terms agree button.

Table 41: Splash Page Parameters

Parameter	Description
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** checkbox to provide access to the free Internet.

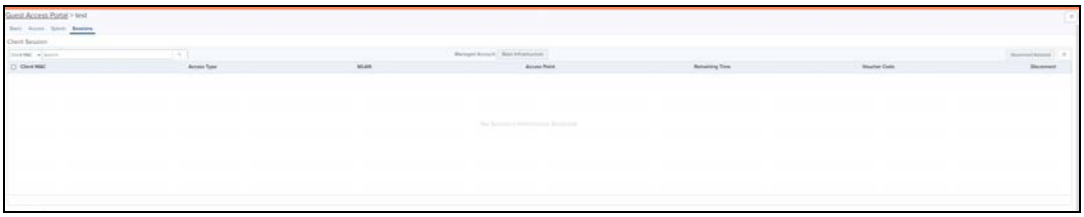
Table 42: WiFi4EU Type Parameters

Parameter	Description
General	• **Network UUID**: Universally Unique Identifier (UUID) that the EC attribute is generated when the network installation is created in the Installation. • **Language:** Allows to select the preferred language. • **Enable Self Test Mode**: Allows the browsers background script verification. • **Show Logo:** Displays the WiFi4EU logo provided by the European union.

Sessions

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

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



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

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

Table 43: 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

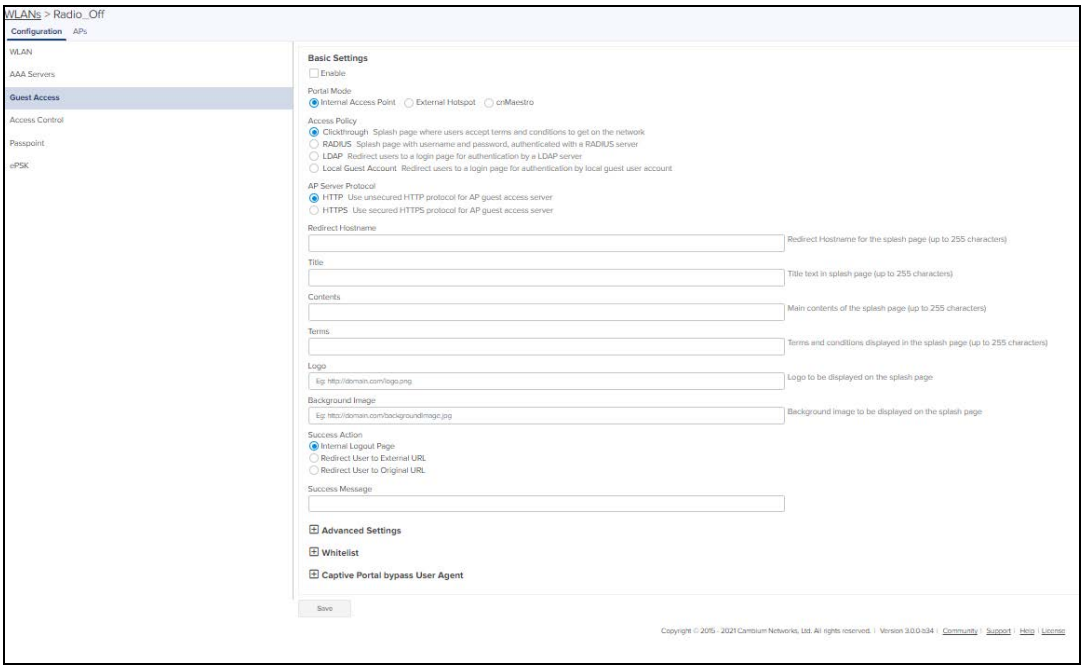
The administrator needs to configure the name of the Guest Access Portal in the device which redirects the device to cnMaestro for client connectivity.

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

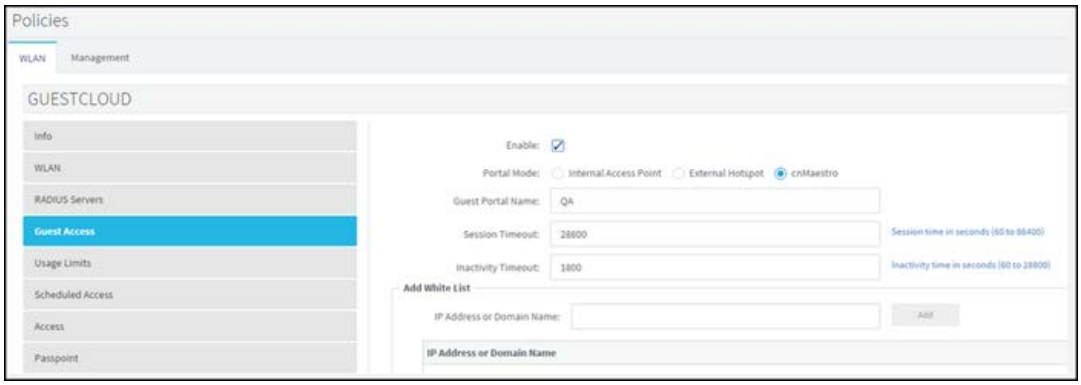
1. Login to the device.
2. Navigate to **Configuration > WLAN > Guest Access**.

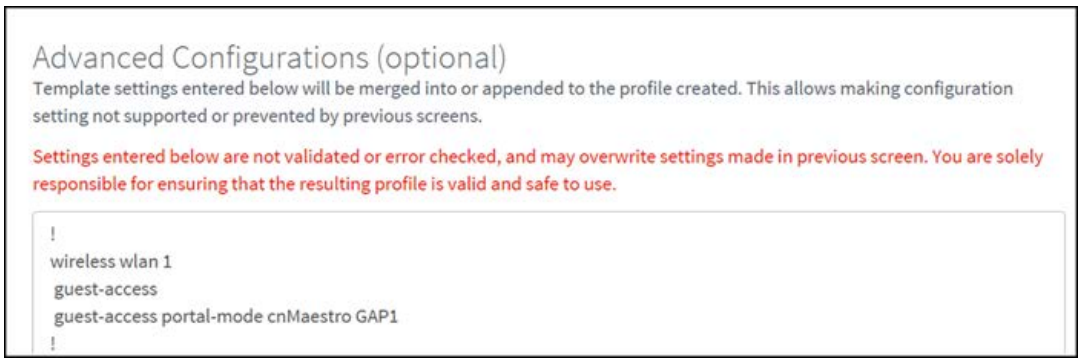


3. Select the check box to enable Guest Access.
4. Choose the **Portal Mode** radio as **cnMaestro**.
5. In the **Guest Portal Name** text box, select the name of the portal that was created in cnMaestro and enter the respective parameters.

Configuration at cnMaestro Side

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

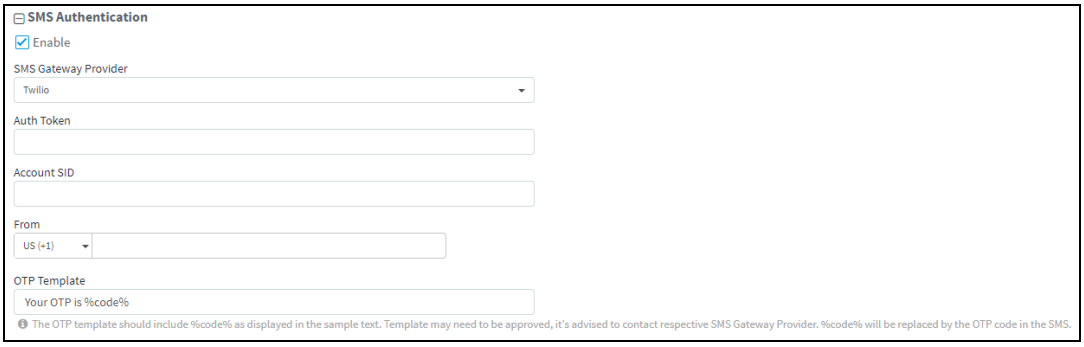




Access Types

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	✓



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 will allow 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.

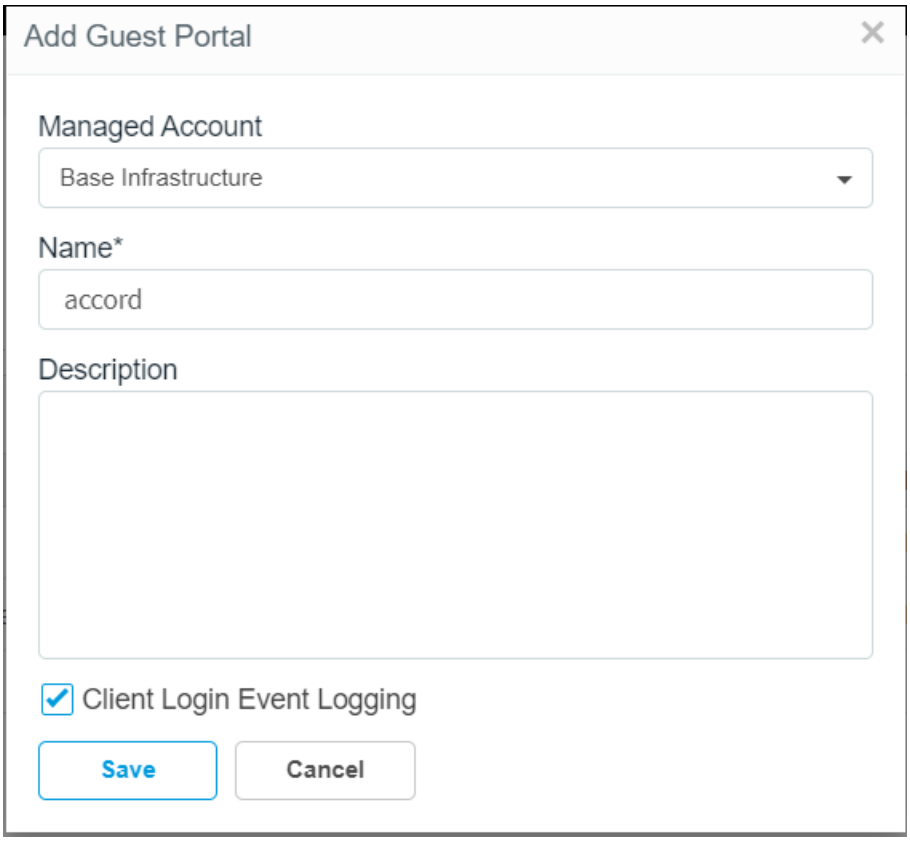
Guest Access using Social Login

Configuration

To achieve cnMaestro Guest Access using Social Logins like Google, Twitter, Facebook, Office 365:

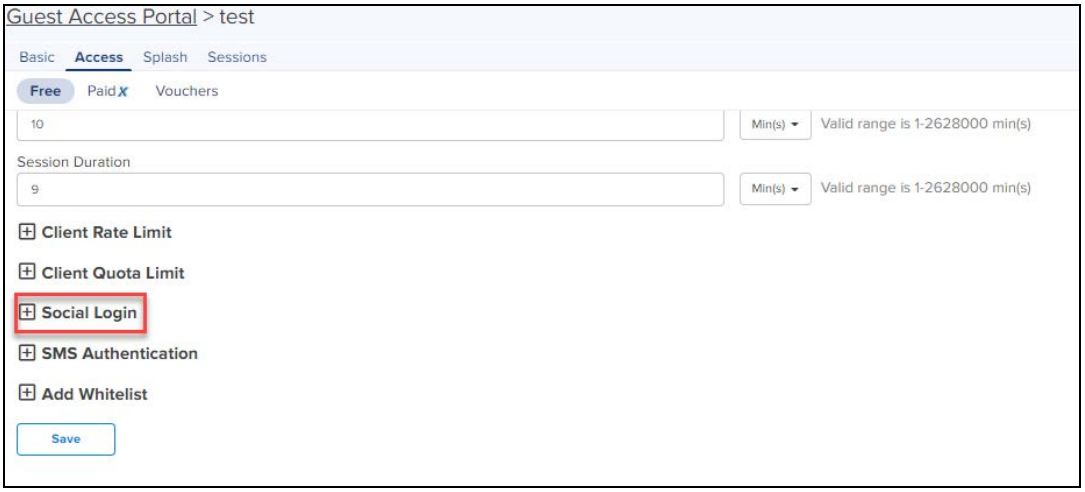
Create Guest Access profile on cnMaestro:

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**.

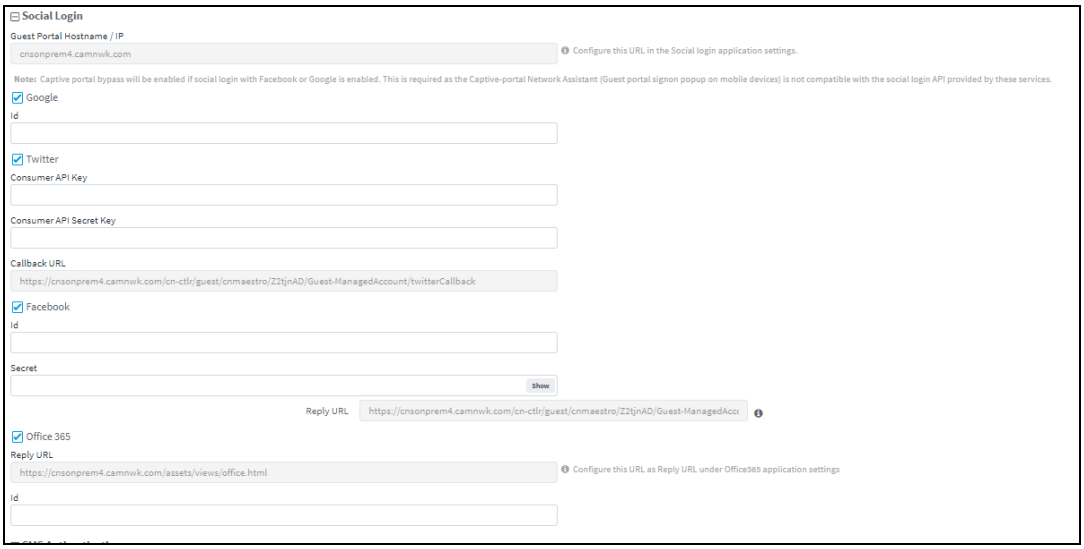


4. Click **Edit Guest Portal Details.**

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



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



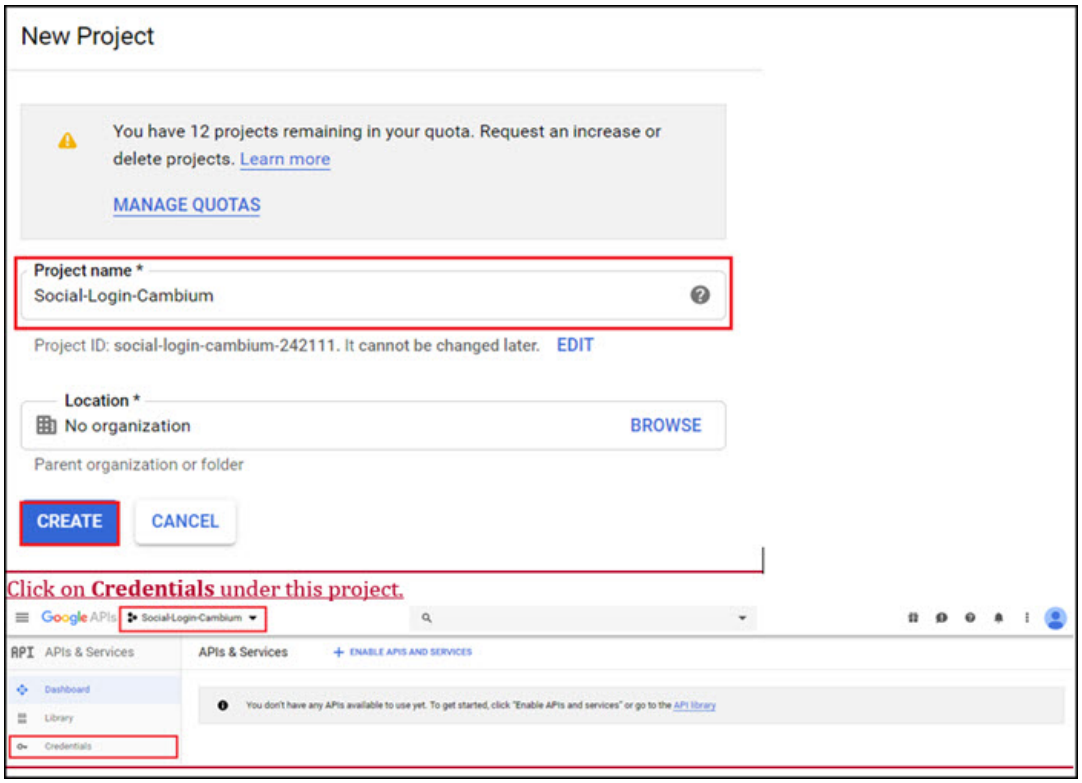
API Key Generation

Creating APIs to integrate cnMaestro with Google, Twitter, Facebook and Office 365.

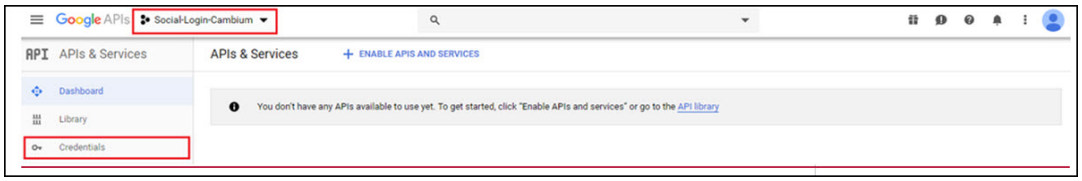
Google

1. Login to Google Account and navigate to https://console.developers.google.com.
2. Click **Select a Project** and then click **New Project.**

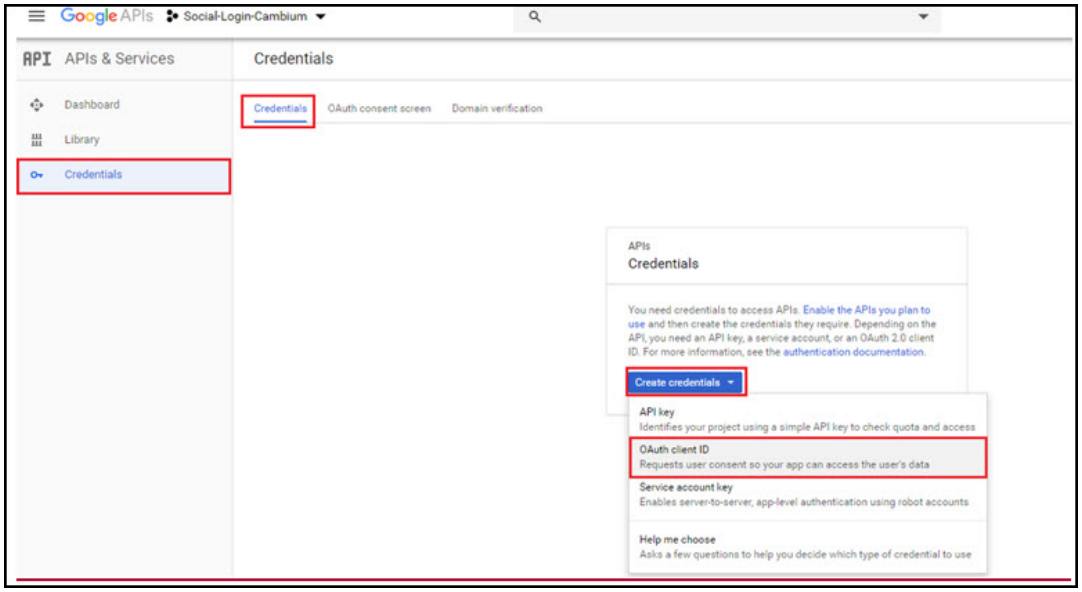
3. Enter a **Name** and click **CREATE**.



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

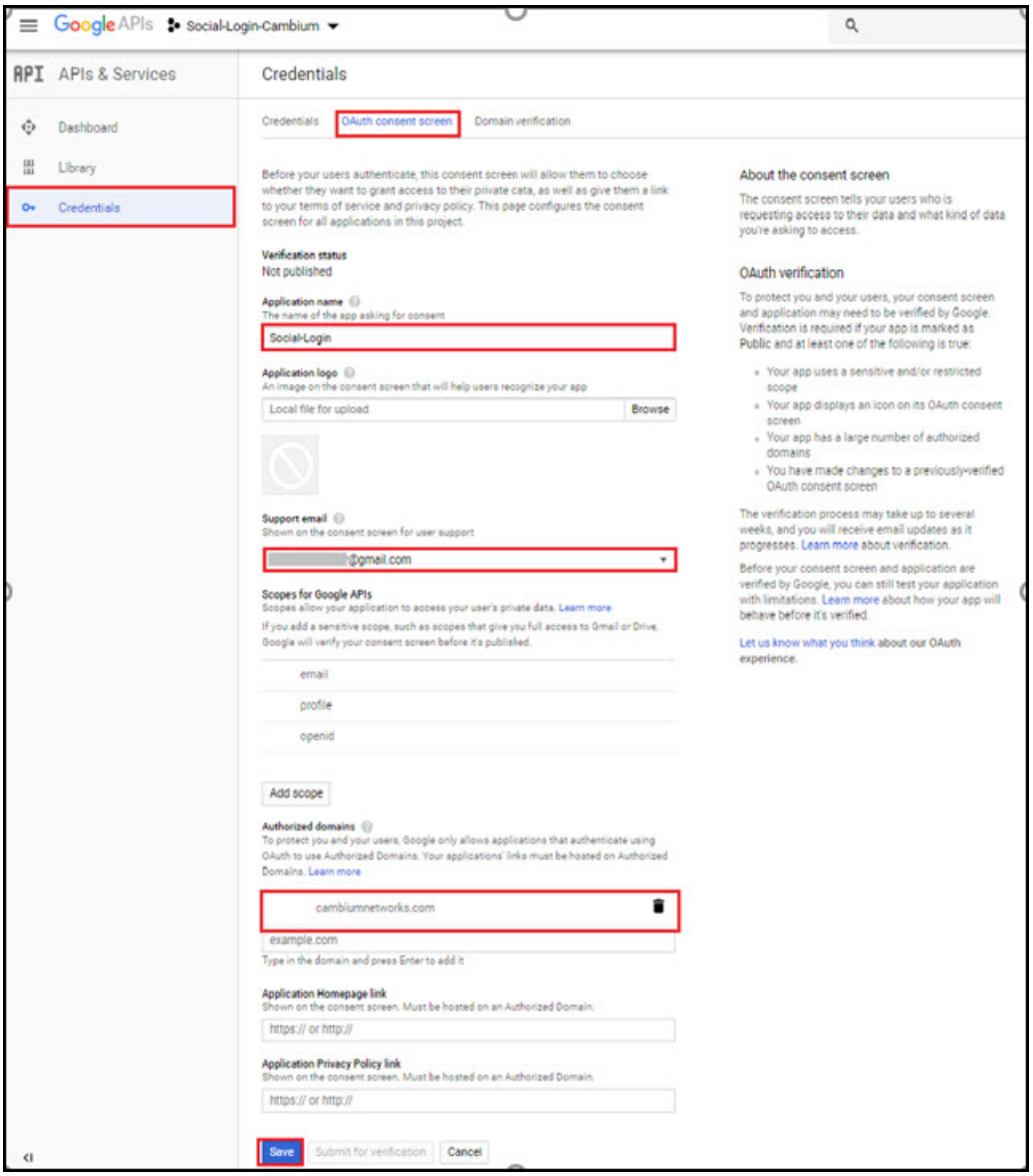


5. Under **Credentials** tab create OAuth Client ID.

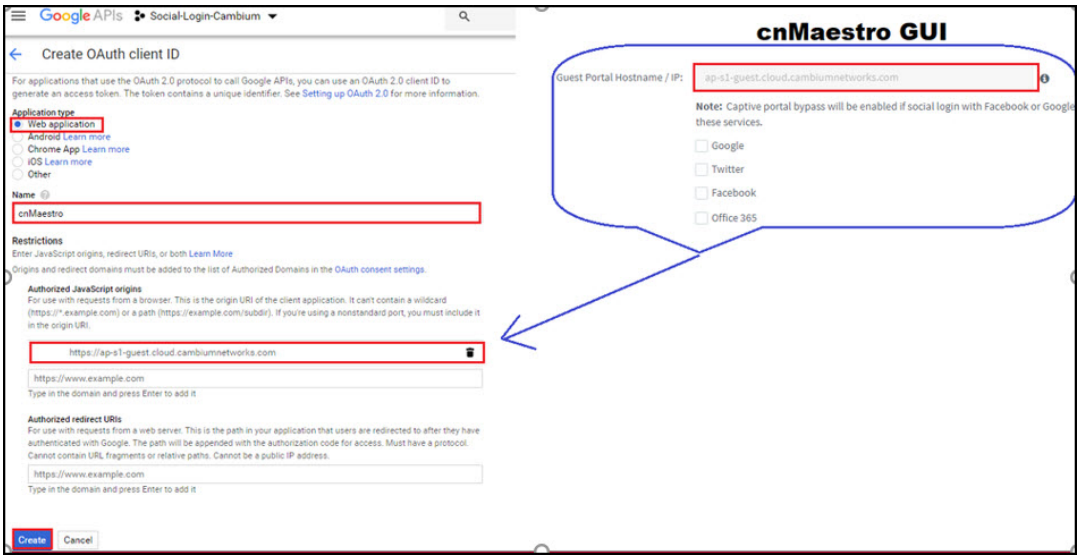


6. Click **Configure Consent Screen**.

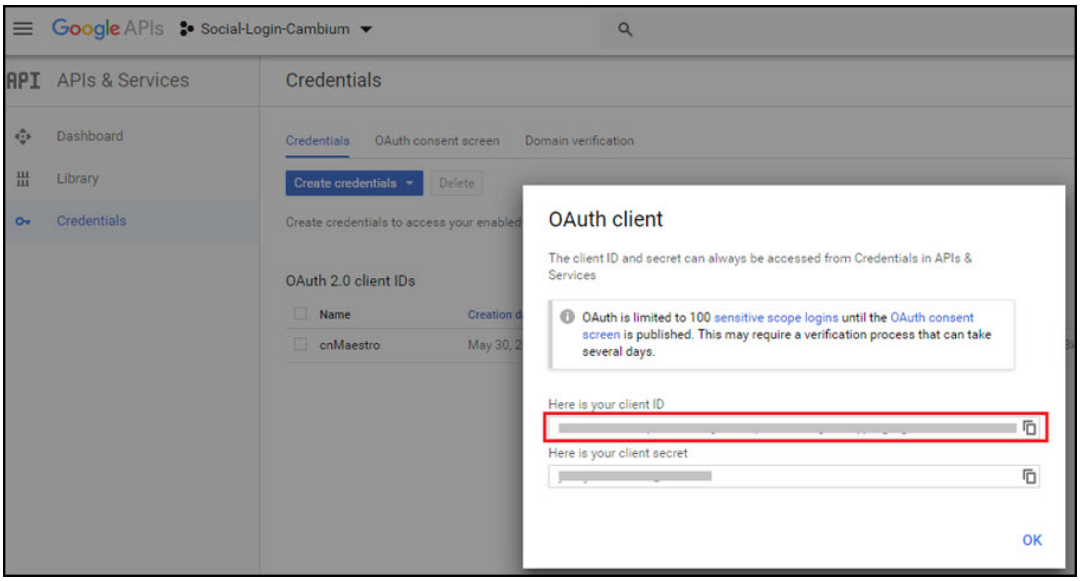
7. Assign a name to the application, map to the email ID, add cambiumbnetworks.com to the authorized domain and click **Save**.



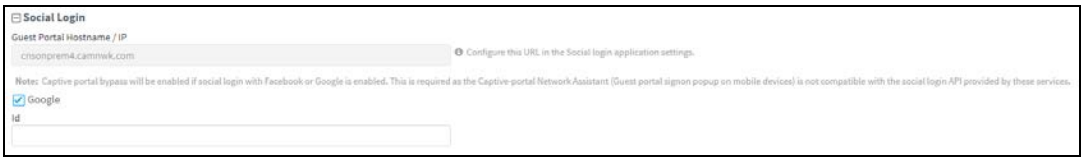
8. It redirects to creation of OAuth Client ID.
9. Select **Application type** as **Web Application**, give a Name, add Guest Portal Hostname url/IP which cnMaestro UI provides and click **Create**.



10. It redirects to the screen showing Client ID and Client Secret.

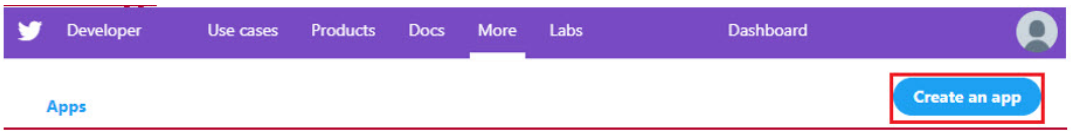


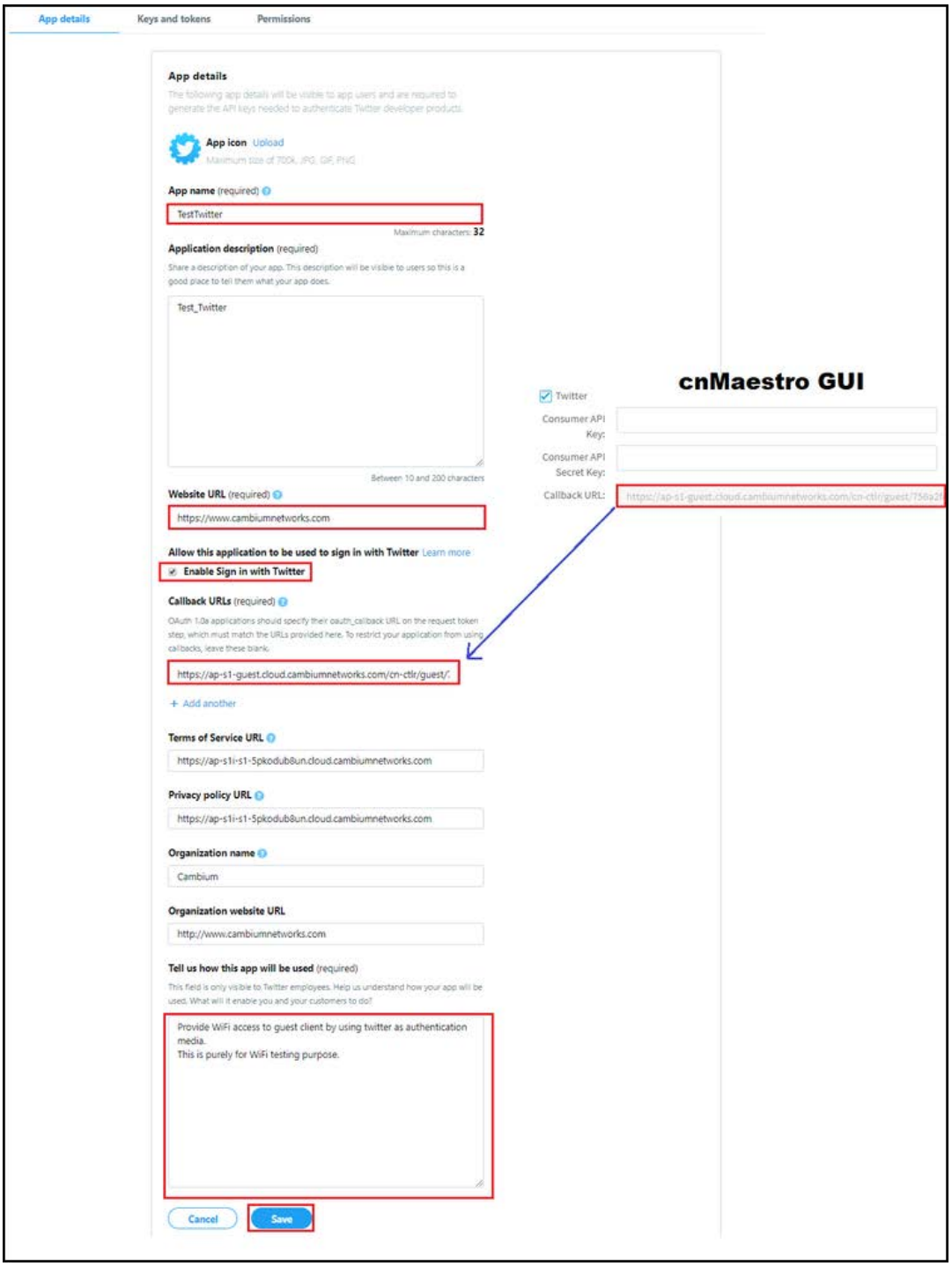
11. Copy the Client ID and paste it to the cnMaestro enabling Google under Social Logins and click **Save**.



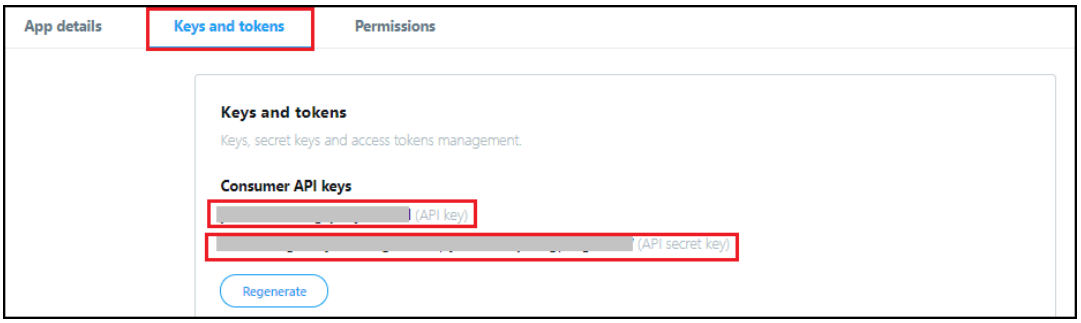
Twitter

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





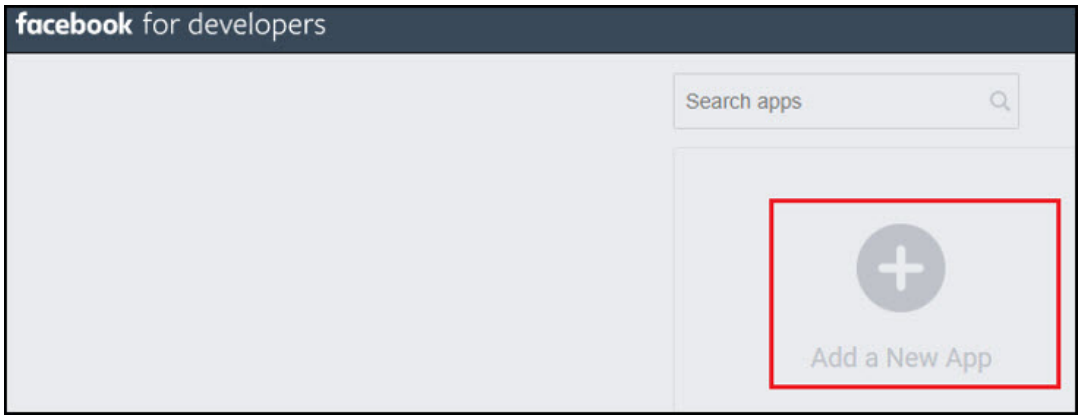
2. Click **Keys** and **Tokens** and copy Consumer API Key and Consumer API Secret Key.



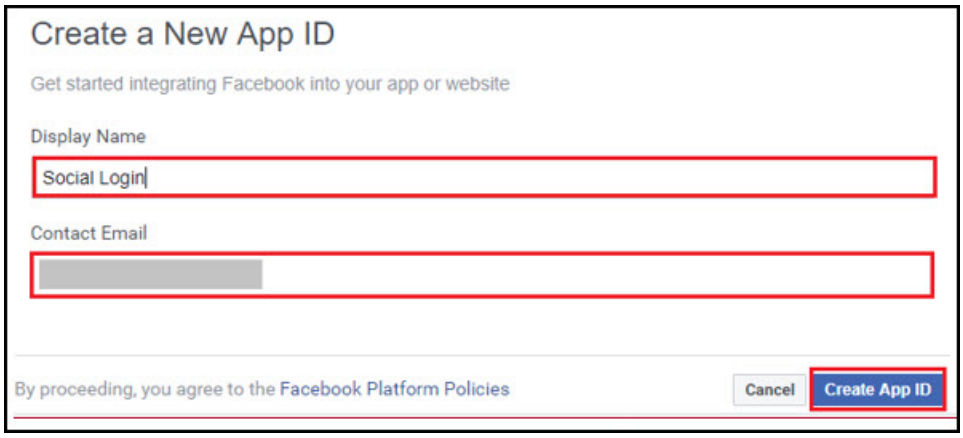
3. Paste them to cnMaestro UI for Twitter social login.

Facebook

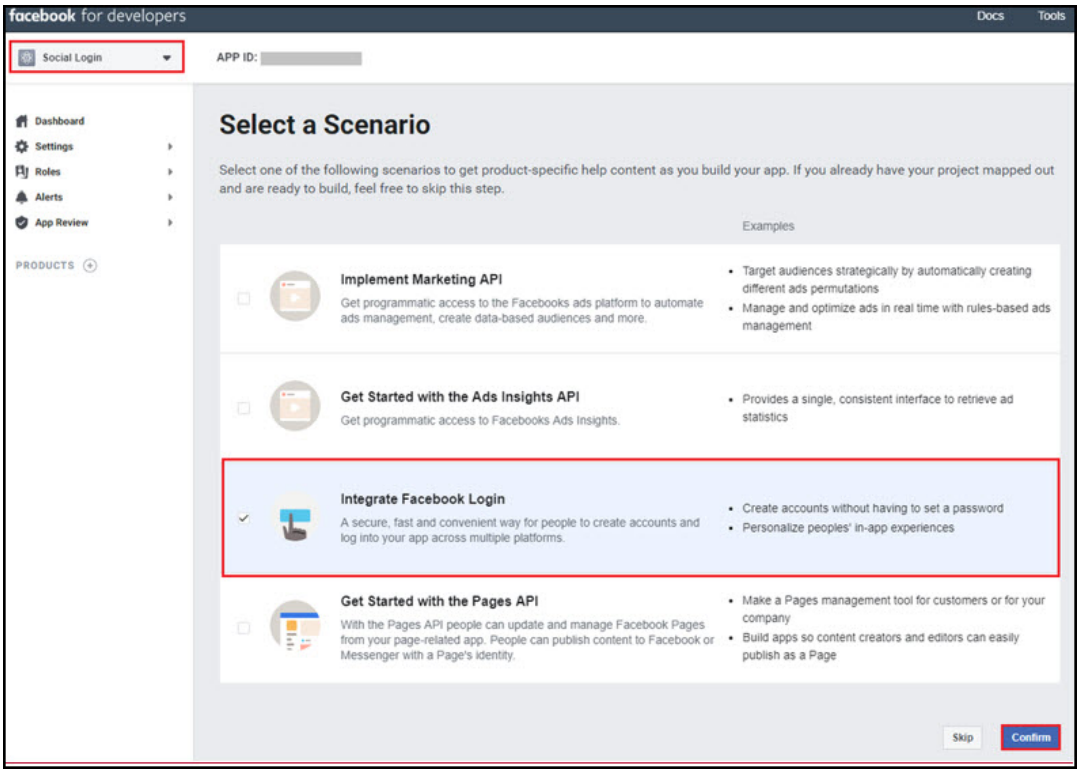
1. Login to Facebook Account and access **https://developers.facebook.com/apps/**, and click **Add a New App**.



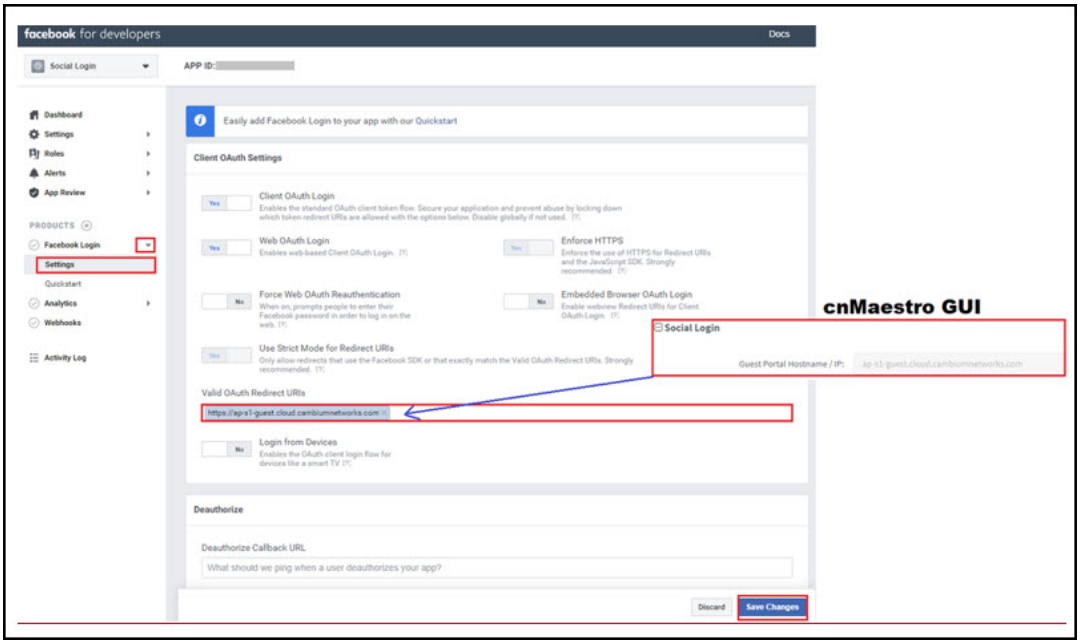
2. Enter App Display Name, Contact Email and click **Create App ID**.



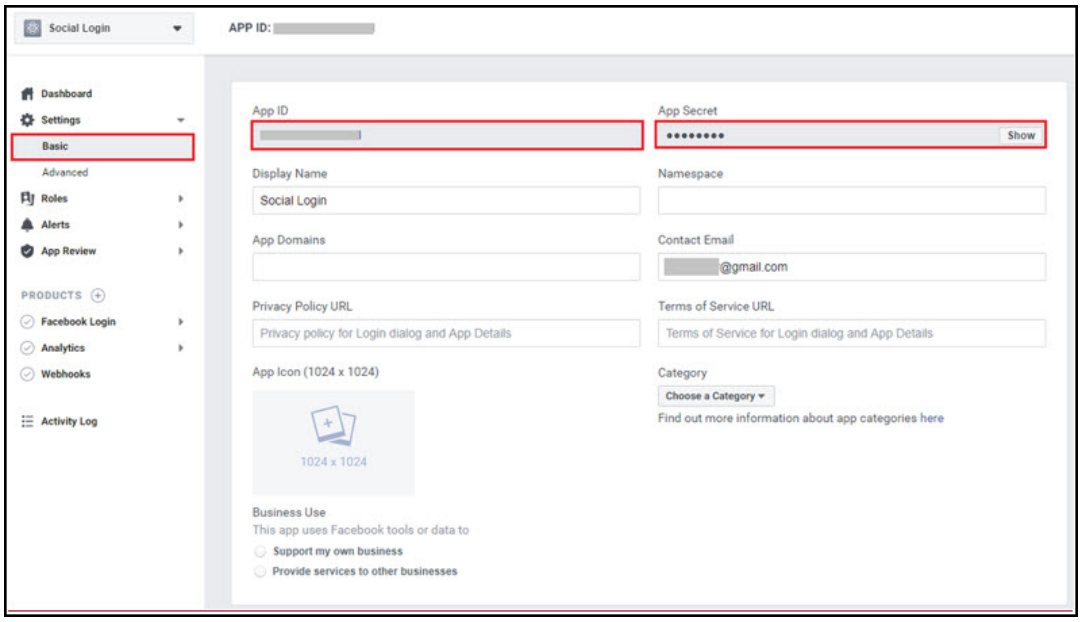
3. Select a Scenario as Integrate Facebook Login and click **Confirm.**



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

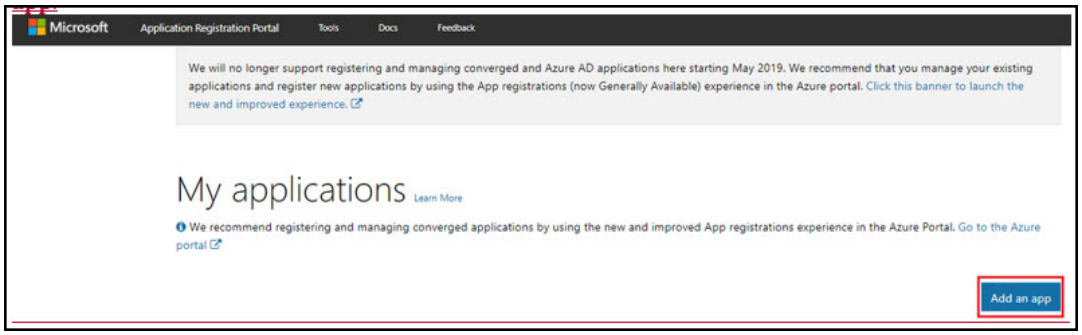


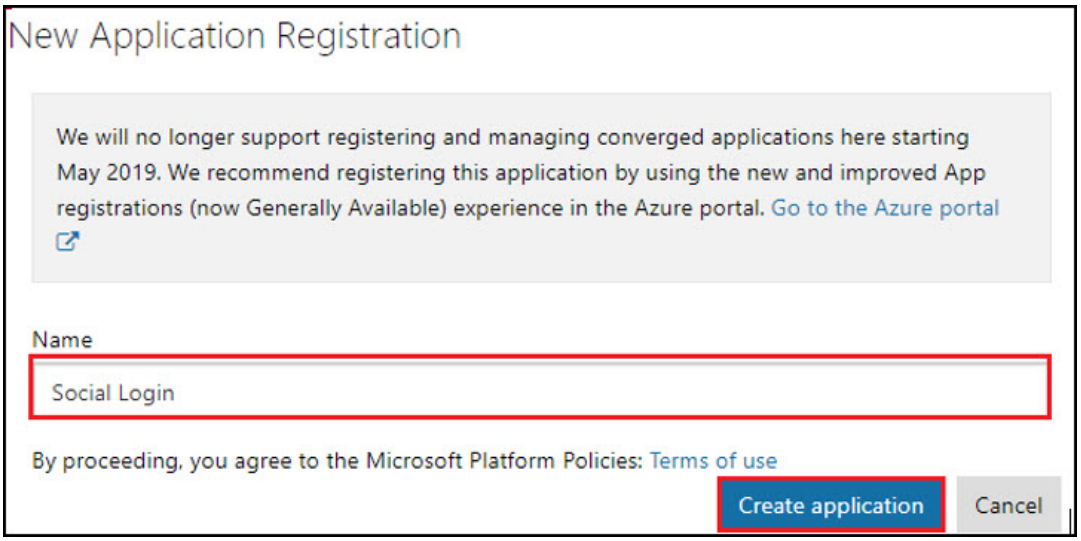
5. Navigate to **Settings** > **Basic** and copy **App ID** and **App Secret**.



Office 365

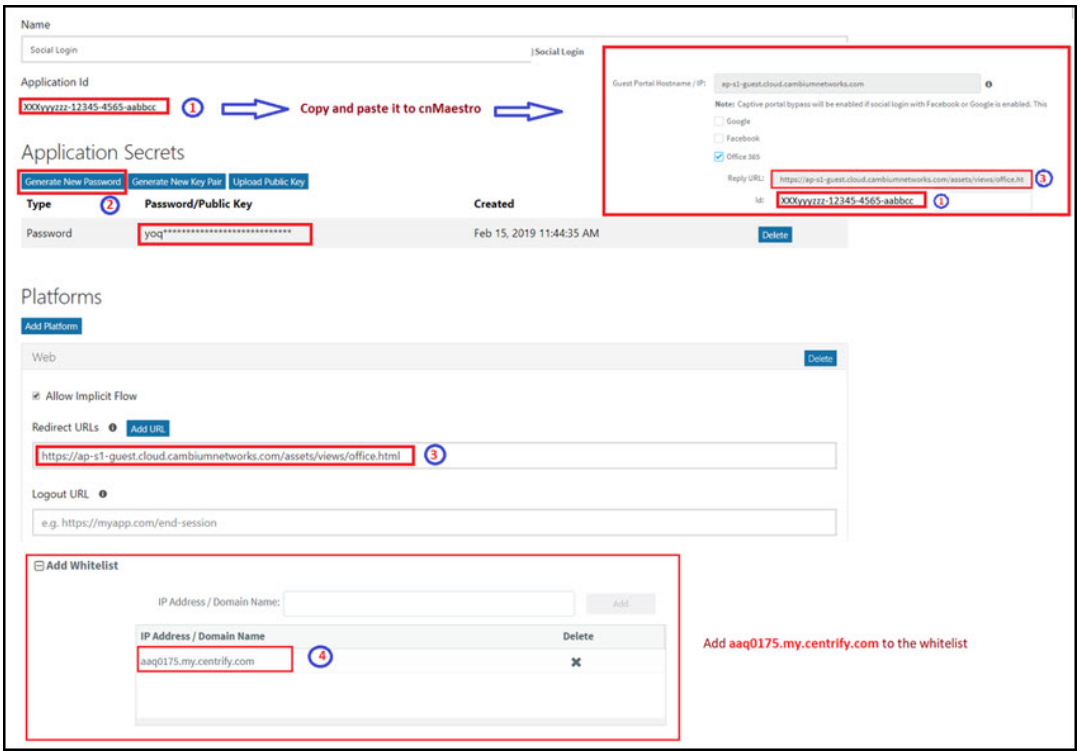
1. Login to Office 365 Account and access https://apps.dev.microsoft.com/ and click **Add an App**.





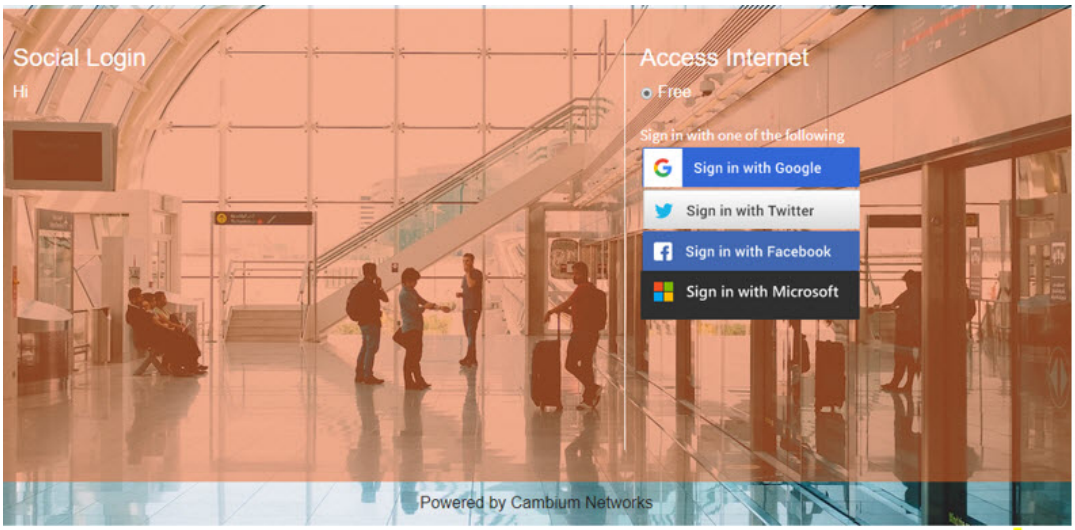
After adding your App name and clicking Create application, it redirectes to App page.

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.



Sample Template

Sample client login page is displayed 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 nZYIoU7QoUxfD03ct1CC2YvInqI7DmUAH6RYz01K1” in this configuration.

Dynamic Components

Message Parameter Name

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

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 please 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 sents out shortly.

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

- Sent
- Queued
- Success
- Message Accepted

So in this configuration one can add multiple such values that should be matched for the success case for the value as received for the “JSON Reply Success Key Name” field.

JSON Reply Failure Key Name

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

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

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

- Sent
- Queued
- Success
- Message Accepted

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

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

Example 1

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

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

Example 2

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

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

Example 3

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

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

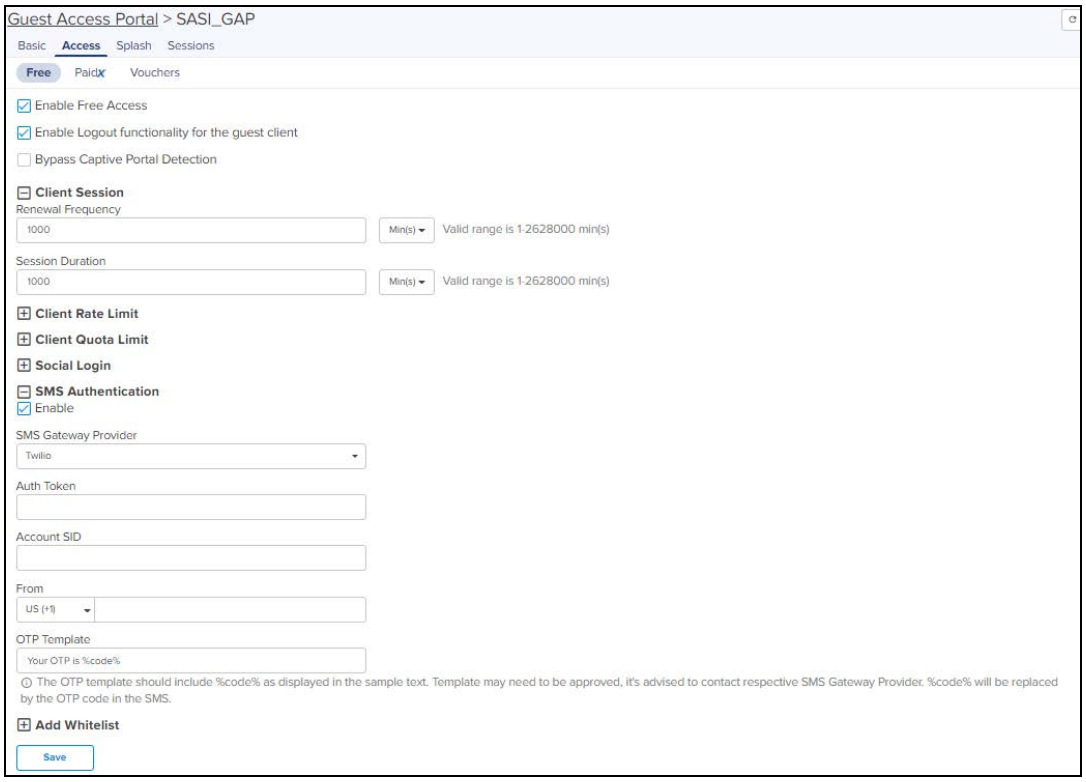
XMl Reply Failure Element Value

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

Based on our examples the error can be mapped to multiple values like 13|12|-1 etc so in this configuration, one can add multiple such values which should be matched for the failure case for the value as received for the “XML Reply Failure Element” field.

Sample Configuration in the cnMaestro

Figure 145 : Guest Access Portal



cnPilot GRE Tunnels

This chapter provides the following information:

- Overview
- Typical Deployment Model (Two Port Solution)
- Configuring L2GRE/EoGRE Tunnel Concentrator
- 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

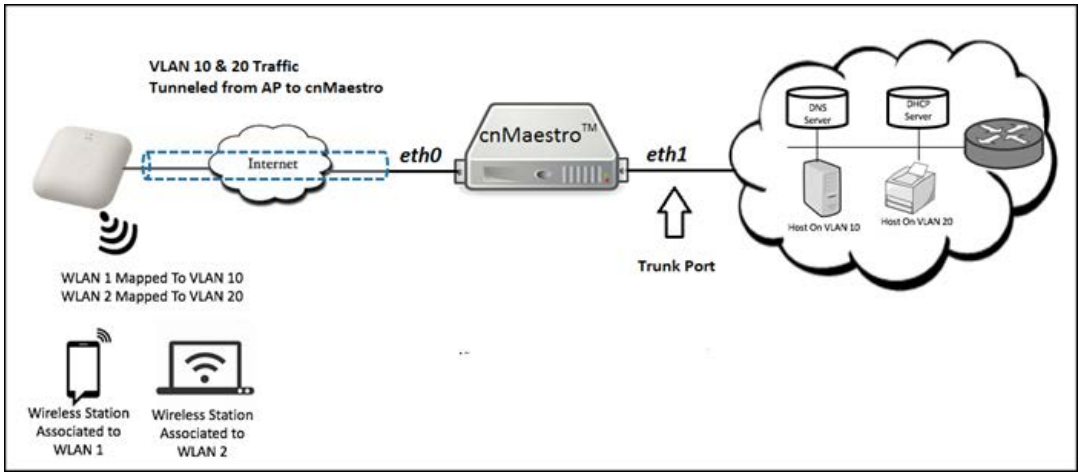
While deploying access points, the ability to tunnel wireless traffic from the APs to a tunnel concentrator (L2GRE/EoGRE) often plays a key role. By using the tunnel feature, the following can be avoided:

- 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 146 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.

Configuring L2GRE/EoGRE Tunnel Concentrator

To configure L2GRE/EoGRE tunnel concentrator, navigate to **Services > Data Tunnel**.

Figure 147 Configuring L2GRE/EoGRE Tunnel Concentrator

NOTE:

Ensure that Promiscuous mode is enabled on the virtual interface that is mapped to Auxiliary/bridge port of GRE.

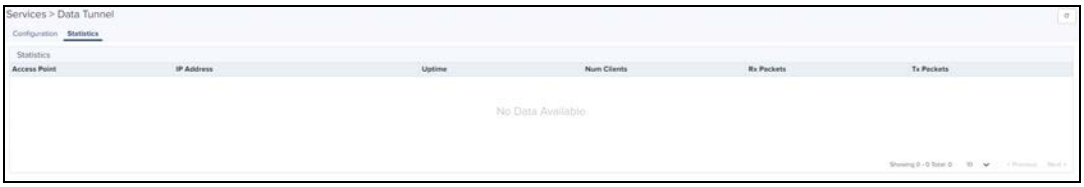
Table 44: Parameters displayed in configuring data tunnel page

Parameter	Description
Allowed VLANs	Represents list of VLANs allowed through the tunnel. This list is used for allowed VLANs on aux/bridge port and also serve as a filtering list for inter AP packet forwarding.
Bridged Port	Configures Aux/Bridged port. Using this configuration, tunnel concentrator is configured either for two port solution or single port solution.
Tunnel Status	Represents whether the tunnel is enabled or not.

Logs and Statistics

- **Collecting Logs**: Logs are useful for debugging purpose. All related tunnel specific logs can be found in /var/log/aurora/tunnel.log
- **Statistics**: Tunnel statistics are available under **Services > Data Tunnel >Statistics**.

Figure 148 Logs and Statistics

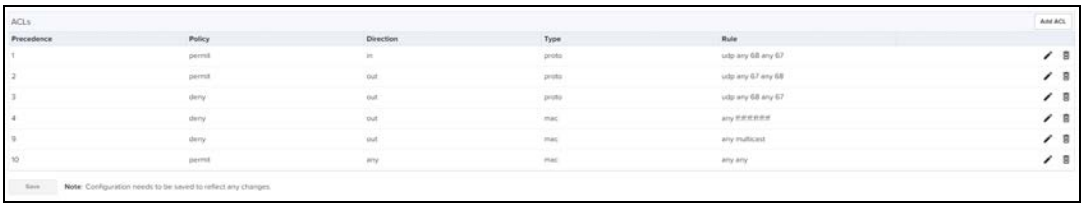


Access Control List (ACL) Configuration

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.

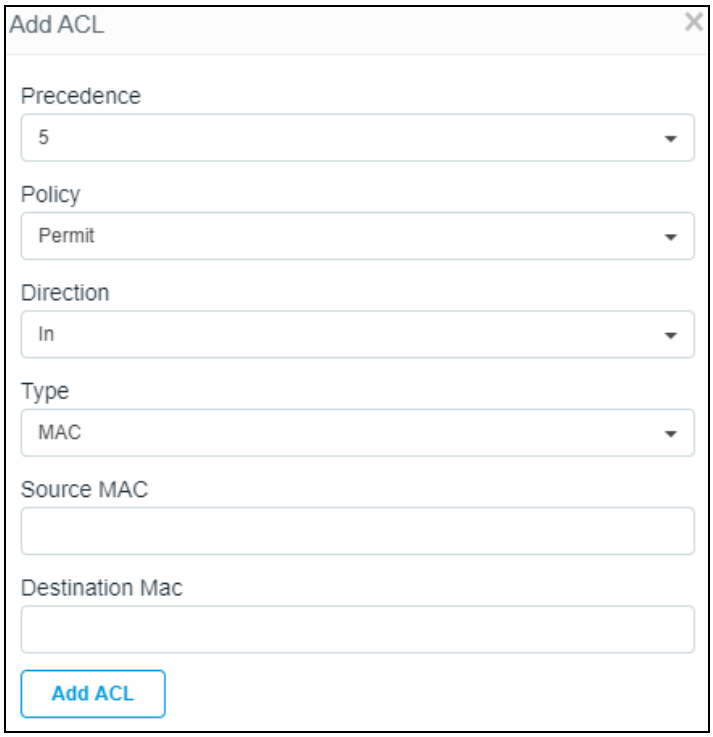
Figure 149 ACL Configuration



Following are the screenshots for the different ACL rule categories:

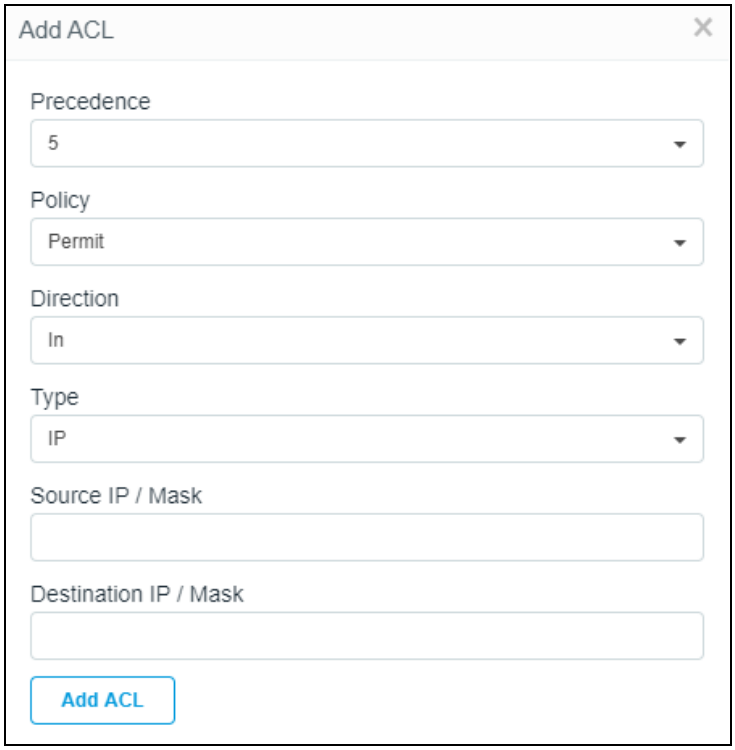
MAC Layer ACL

Figure 150 MAC Layer ACL



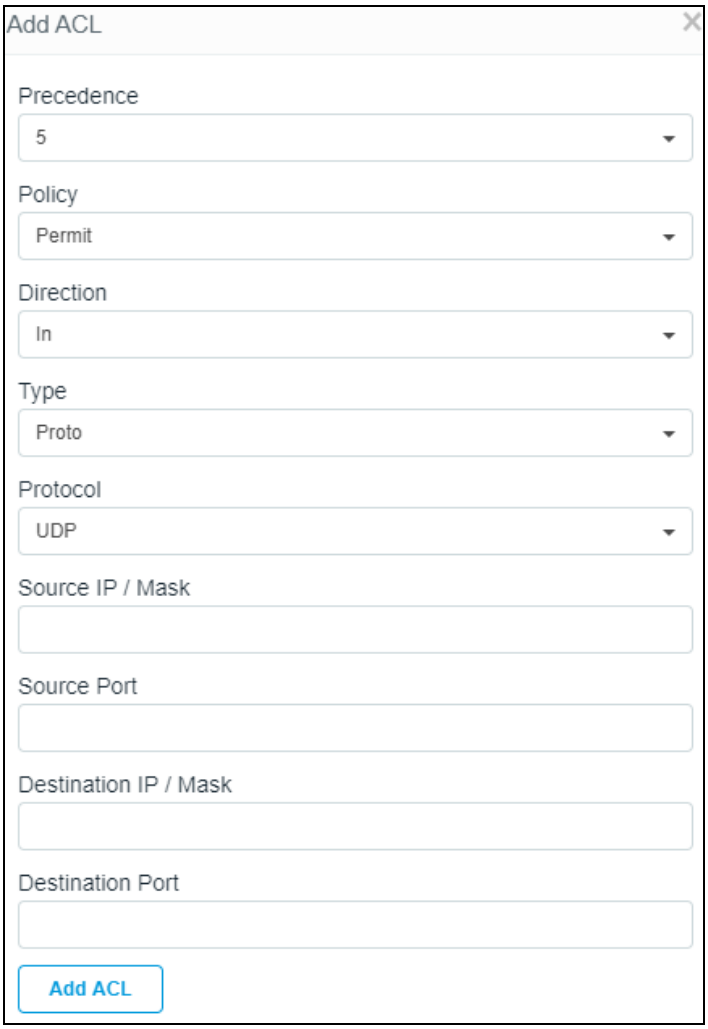
IP Layer ACL

Figure 151 IP Layer ACL



Transport Layer ACL

Figure 152 Transport Layer 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.

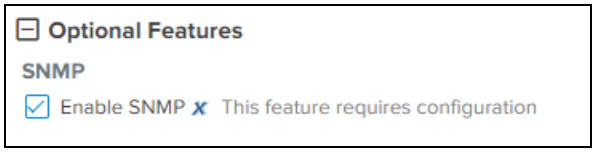
Enable SNMP

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 will not start until the SNMP Configuration is completed.

> **NOTE:**
> SNMP Services will not start until a valid configuration exists.

Figure 153 Enable SNMP



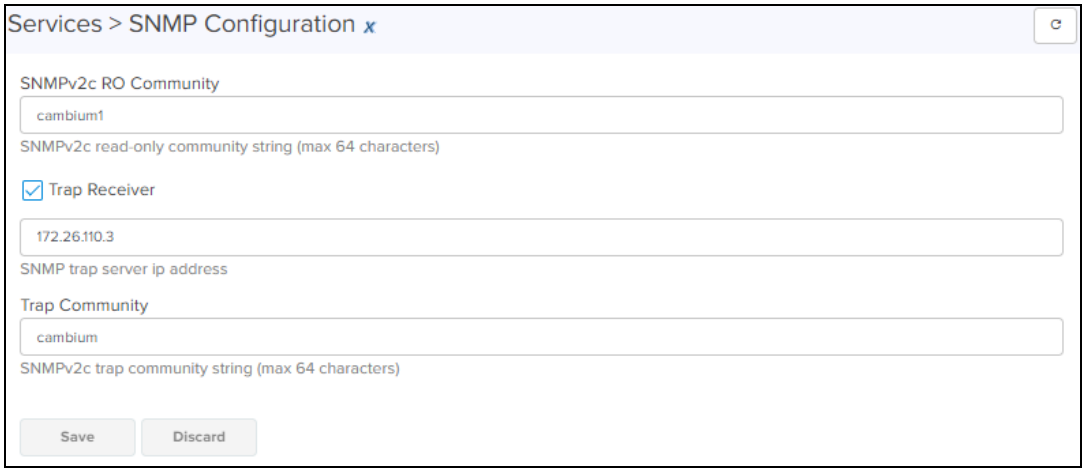
1. Click **Save**.

Configure SNMP Parameters

To configure SNMP Parameters:

1. Navigate to **Services > SNMP Configuration** (this tab is only visible if SNMP is enabled)

Figure 154 Configure SNMP



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)

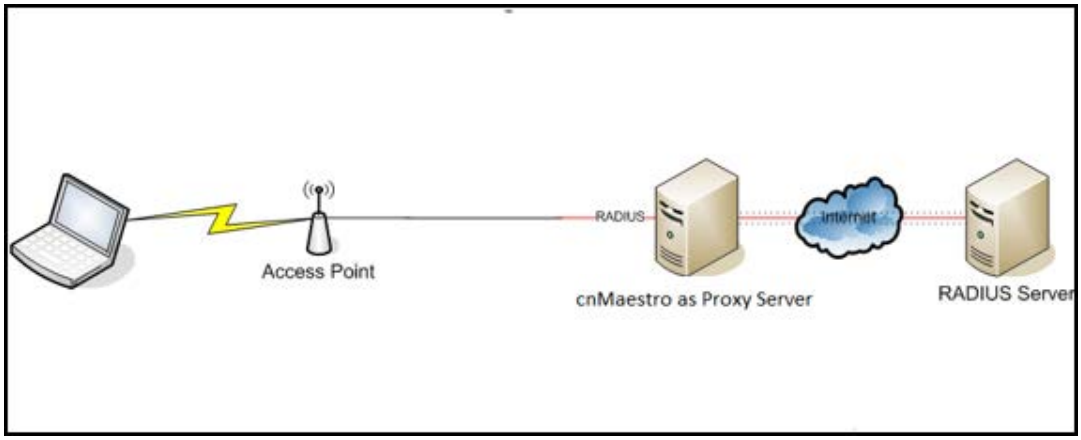
RADIUS Proxy

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 155 RADIUS Proxy on cnMaestro On-Premises



Minimum cnMaestro On-Premises Version Requirements

- Minimum cnMaestro On-Premises release version required: 1.4.1-b1.
- Minimum cnPilot AP release required: 3.3.

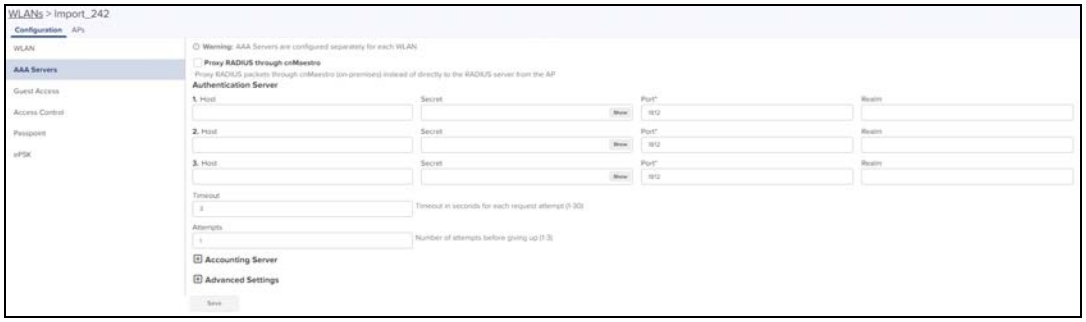
> **NOTE:**
> This feature is not available on the Cloud version of cnMaestro.

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 156 RADIUS Proxy Configuration



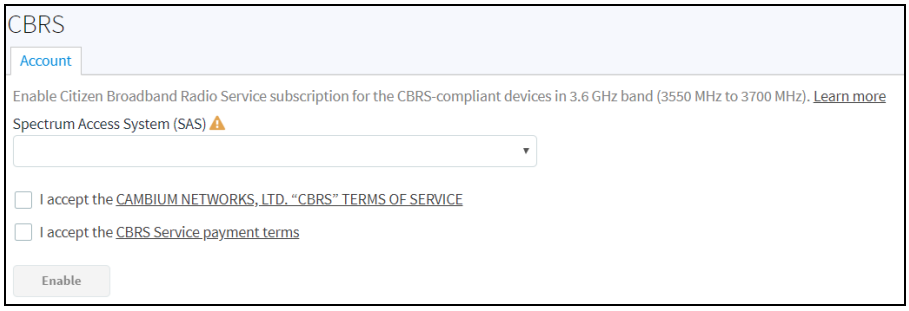
Citizen Broadband Radio Service (CBRS)

Citizen Broadband Radio Service subscription for CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz).

> **NOTE:**
> User must have an account in cnMaestro Cloud prior to enabling CBRS services in On-Premises.

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. **Billing Information** window pop-ups; enter the below input/sections:

   Business Contact

   - First Name
   - Last Name
   - Email
   - Phone
   - Street Address
   - Zip Code
   - Country
   - State

   Technical Contact

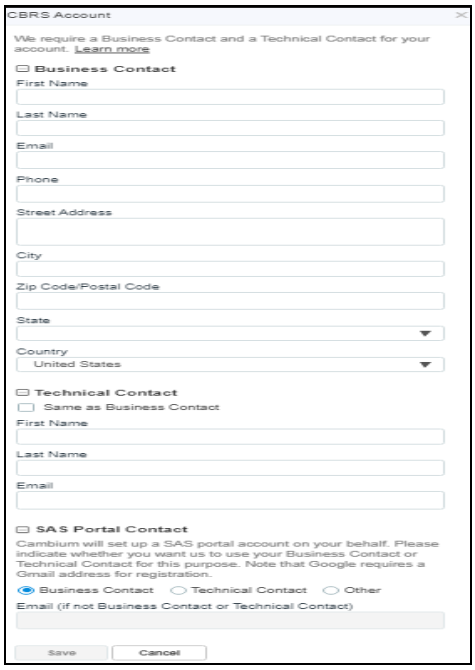
   Enable **Same as Business Contact** if the Technical Contact is the same.

   - First Name
   - Last Name
   - Email

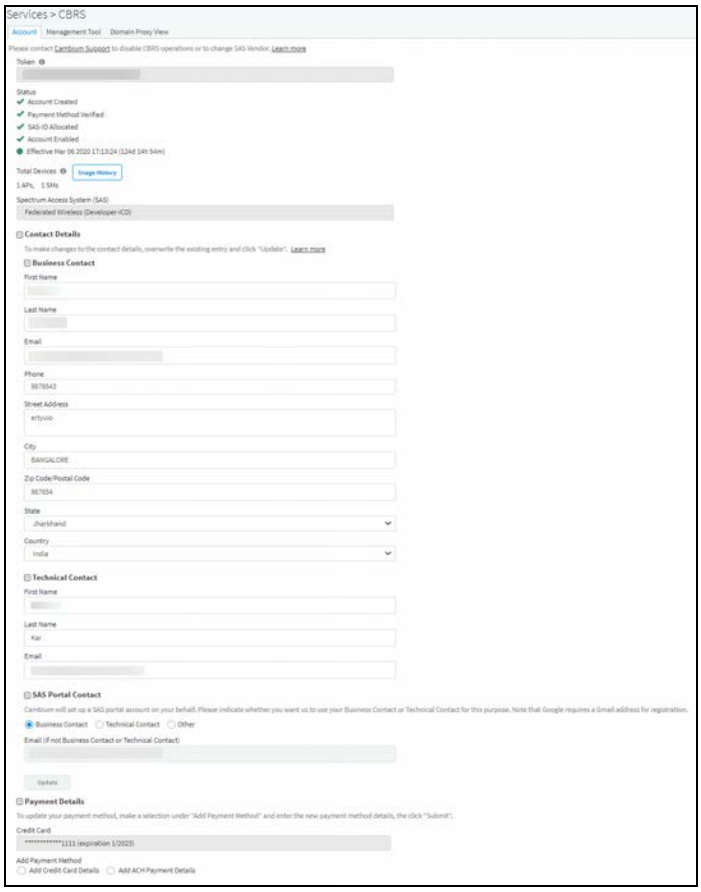
   SAS Portal Contact

Cambium Networks sets up the SAS portal account on behalf of the operator. Please select whether you want to use a Business Contact, Technical Contact, or Other.

- Click **Save.**



7. The **Account** page displays:
   - Token
   - Status
   - Total Devices
   - SAS
   - Contact Details
   - Payment Details



a. **Token:**

The Token is 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	Sucess Status
Status ✔ Account Created ✖ Payment Method Verification Pending ✖ SAS-ID Allocation Pending ● Effective Jul 07 2020 16:54:10 (< 1m) Total Devices ⓘ Usage History 0 APs, 0 SMs	Status ✔ Account Created ✔ Payment Method Verified ✔ SAS-ID Allocated ✔ Account Enabled ● Effective Mar 19 2020 15:02:02 (110d 2h 0m) Total Devices ⓘ Usage History 3 APs, 68 SMs

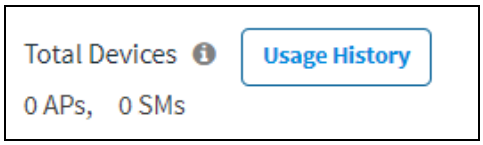
1. **Account Creation**: Once the CBRS account is enabled, it displays the status as **Created**. Refer to **Step f** for entering contact information and enabling account.
2. **Payment Method**: After adding the Payment Details with verification, displays the status as Verified. Refer to **Step g** to add payment method after enabling account.
3. **SAS-ID**: Once the payment details are verified, the SAS ID is allocated automatically and displays the status as **Allocated**.

NOTE

When the SAS ID allocation is pending or unavailable in the server, even after the payment details are configured and verified, it may take 1 day to get the SAS ID.

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, and **Usage History** provides the list of devices registered with **Month** and **Year.**



NOTE

Initially the device counts will be 0 APs and 0 SMs.

d. **SAS:** Displays the SAS vendor preferred by the operator.

NOTE

Contact Cambium support to disable CBRS operation or to change SAS Vendor.

e. **SAS:** An operator needs to select which SAS vendor they prefer.

f. **Contact Details:**

For new CBRS account migrations to the CBRS server, this information would have already been entered prior to **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, changes in the CBRS initiative 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.

- **First Name**- Enter the operator's First Name.
- **Last Name** - Enter the operator's Last Name.
- **Email** - Enter the valid email ID.
- **Phone** - Contact phone number.
- **Street Address** - Operator's company address.
- **City** - Enter the city in the selected state.
- **Zip code/Postal Code -** Enter the valid zip/postal code.
- **State** - Select the state from the drop-down.
- **Country -** Select the country from the drop-down.

Technical Contact

Cambium Networks communicates with the **Technical Contact** for all technical aspects of the CBRS Service, such as software updates, publication of release notes, learning guides, technical issues, etc.

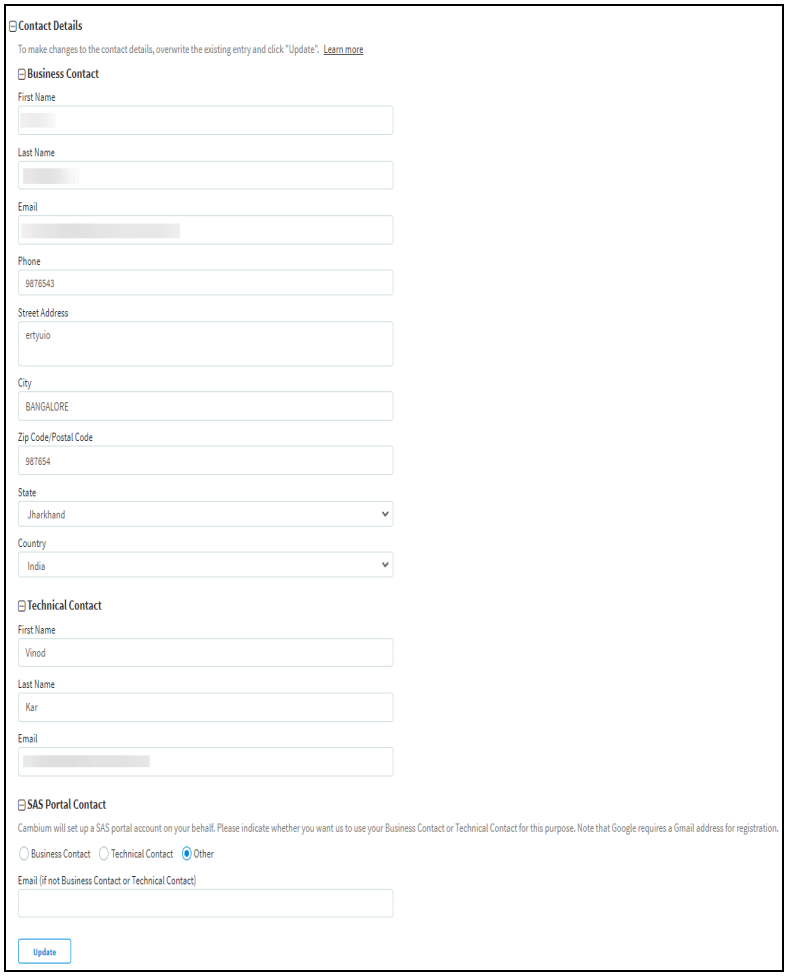
- **First Name** - Enter the authorized prime technical contact's first name.
- **Last Name** - Enter the authorized prime technical contact's last name.
- **Email -** Enter the authorized prime technical contact's email address.

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.**

> **NOTE**
>
> Google requires a Gmail address for registration.

- Click **Update.**

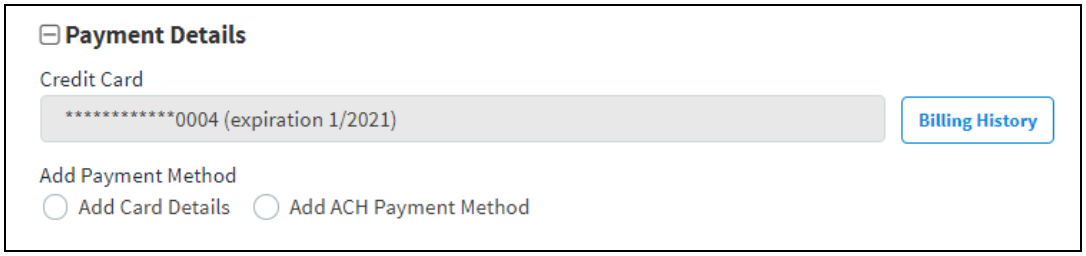


> **NOTE**
>
> Once you click update, the **Account Page** will be overwritten by the current entries.

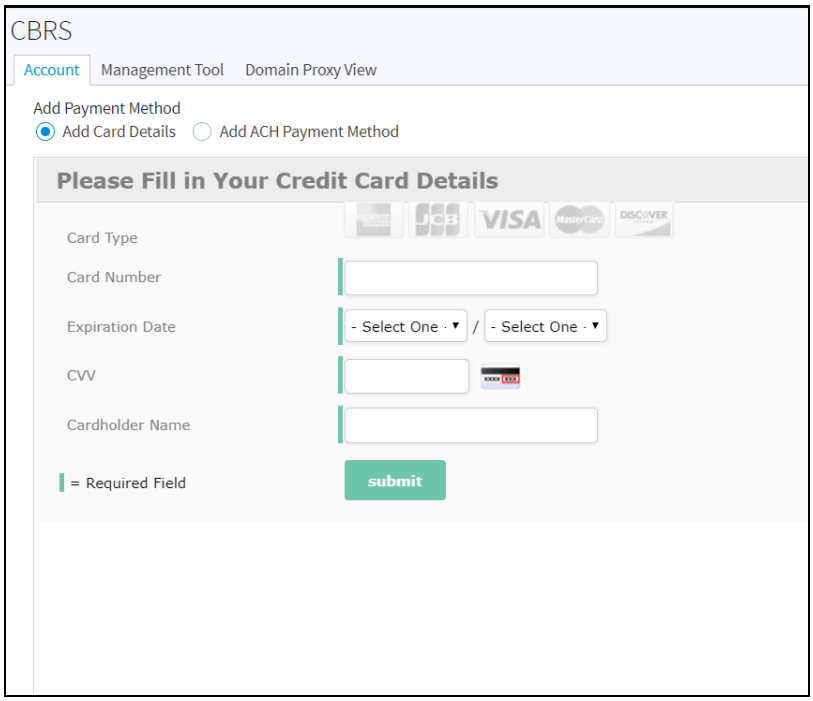
g. **Payment Details**

Select one of the payment methods below:

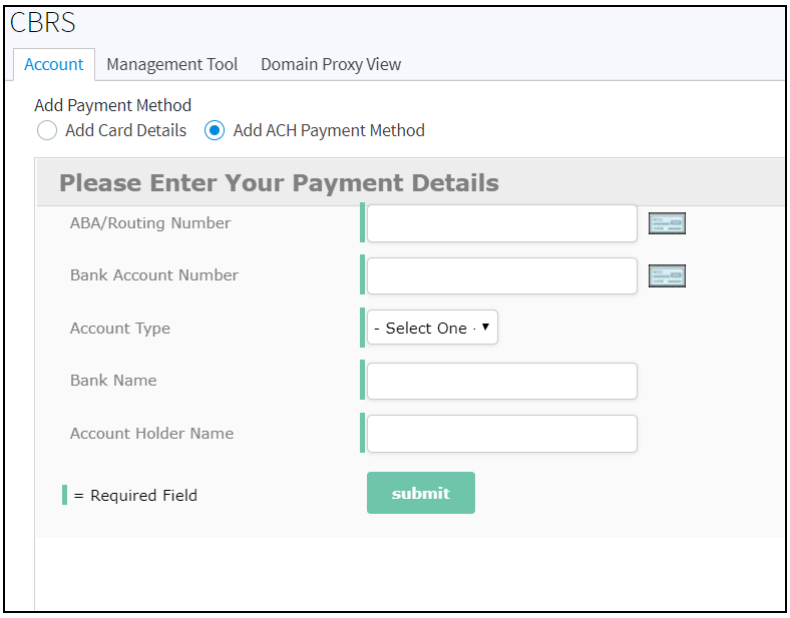
- Add Card Details
- Add ACH Payment Method



- **Add Card Details**
  - Enter the 16 digit Credit **Card Number**.
  - Select the **Expiration Date** and **Year** on the card.
  - Enter the **CVV** and **Cardholder Name**.
  - Click **submit**.



  - **Add ACH Payment Method**
    - Enter the **ABA/Routing Number**.
    - Enter the **Bank Account Number**.
    - Select one of the following **Account Type:**
      - Checking
      - Saving
      - Business Checking
    - Enter the **Bank Name** and **Account Holder Name**.

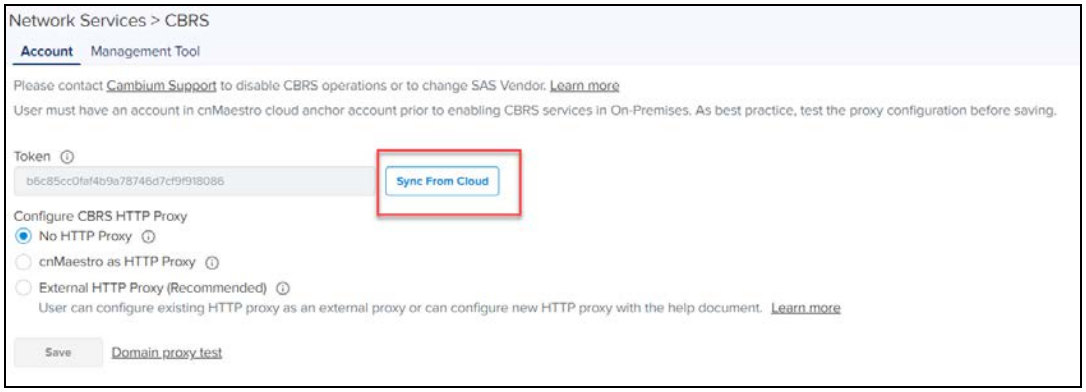


- Click **submit.**

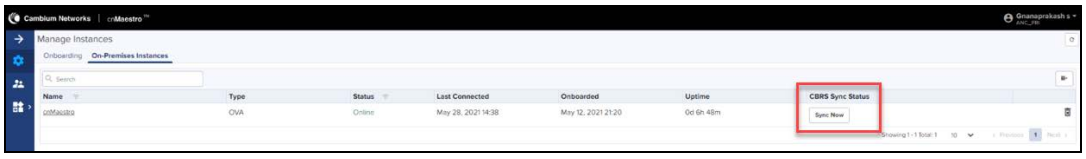
Enabling CBRS in On-Premises

Perform the following to enable CBRS:

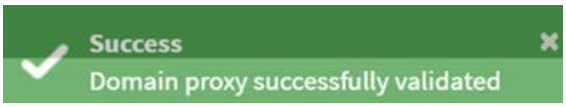
1. On successful activation of the CBRS service in the Cloud Anchor account, cnMaestro generates a Token.
2. Onboard the On-Premises to Anchor account.
3. User can Sync the CBRS token from On-premises or Anchor account
   a. In On-Premises CBRS accounts page click **Sync From Cloud** to synchronize the 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:

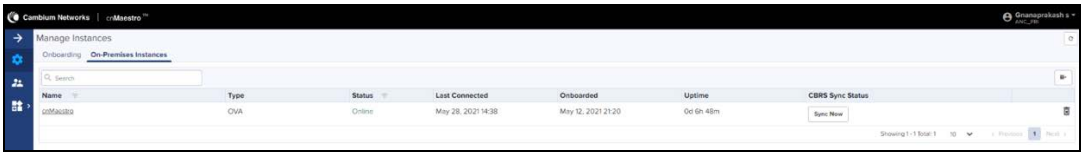


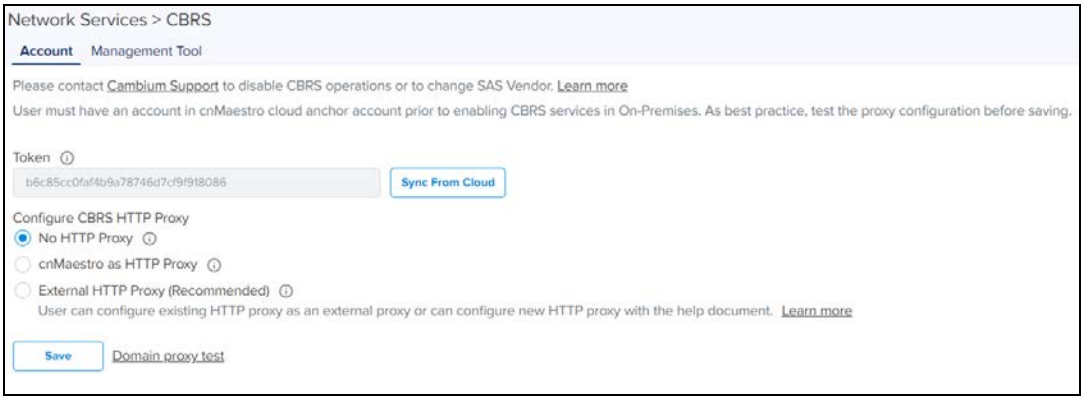
Synchronize CBRS Configuration to the On-Premises Instance

NOTE:

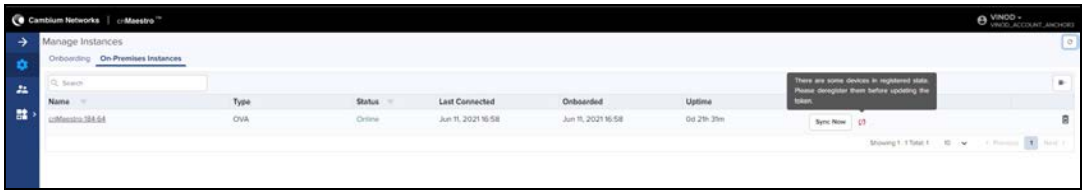
From version 3.0.3 cnMaestro supports Synchronize CBRS Configuration to On-Premises instance.

Once On-Premises is connected to the Anchor account and the link is established between the Anchor account and cnMaestro On-Premises, the user can synchronize the CBRS details (Token, SAS ID) to the cnMaestro On-Premises instance to register CBRS devices.





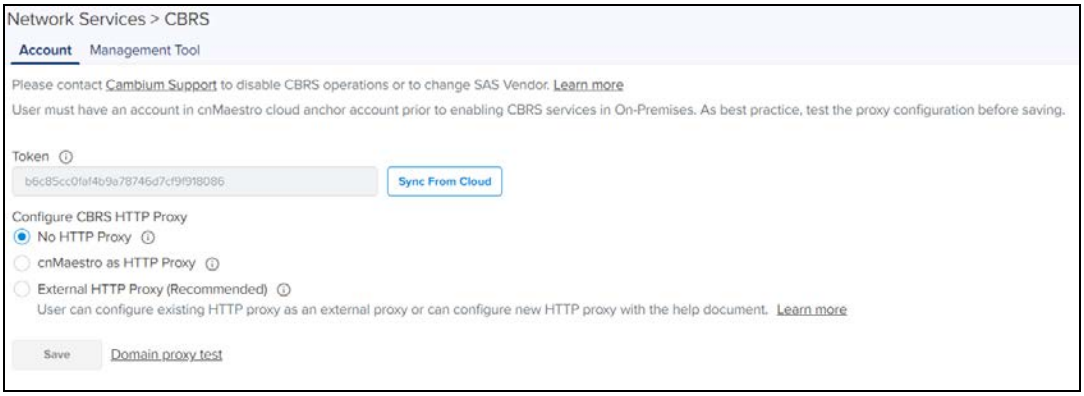
- If user tries to Sync with the same SAS ID and with different CBRS token, during synchronization it pushes the new token to the existing CBRS devices without any heartbeat loss or deregistration of devices.
- If the user tries to synchronize through Cloud with different SAS ID and CBRS token, it displays an error that the devices should be derigistered from On-Premises and needs to push the token.



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.

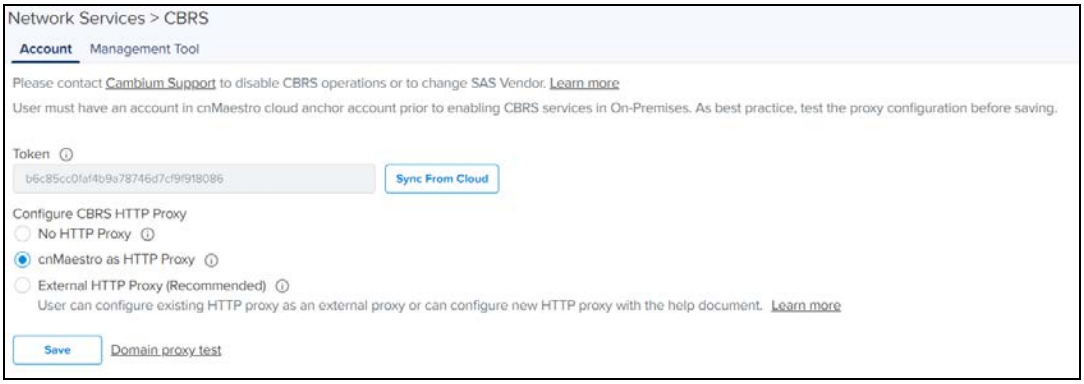
No HTTP Proxy



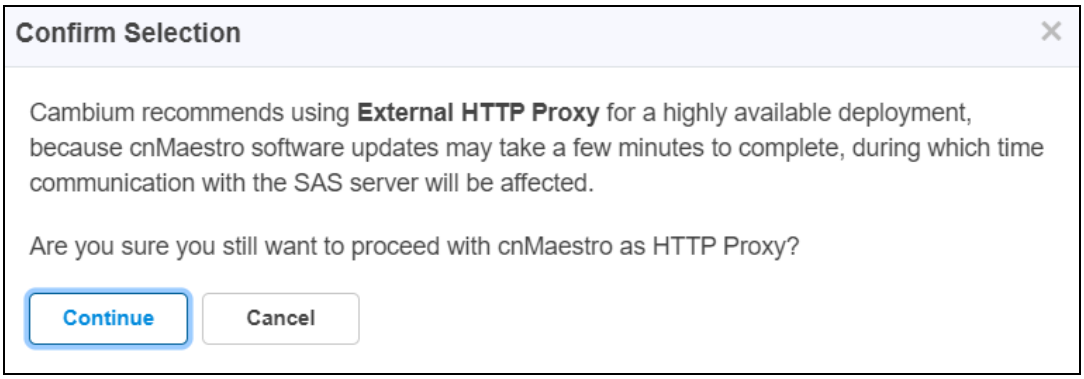
- In On-Premises **No HTTP Proxy** is selected by default.
- CBRS-compliant devices communicate with the Domain Proxy directly through the Cambium Domain Proxy.

> **NOTE:**
>
> The On-Premises server and CBRS devices must have Internet access to communicate directly to the Cambium Domain Proxy.

cnMaestro as HTTP Proxy



- Select **cnMaestro as HTTP Proxy** and a window pops-up. click **Yes.**



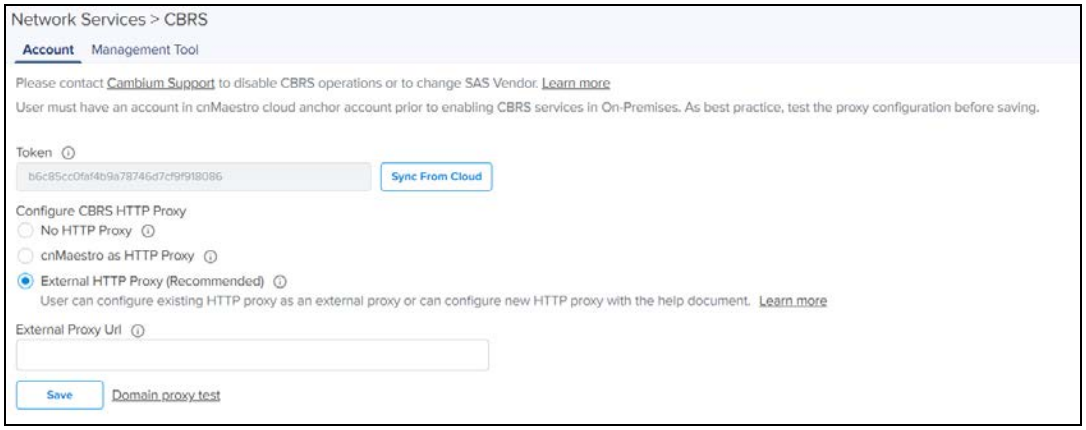
Warning:

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



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.

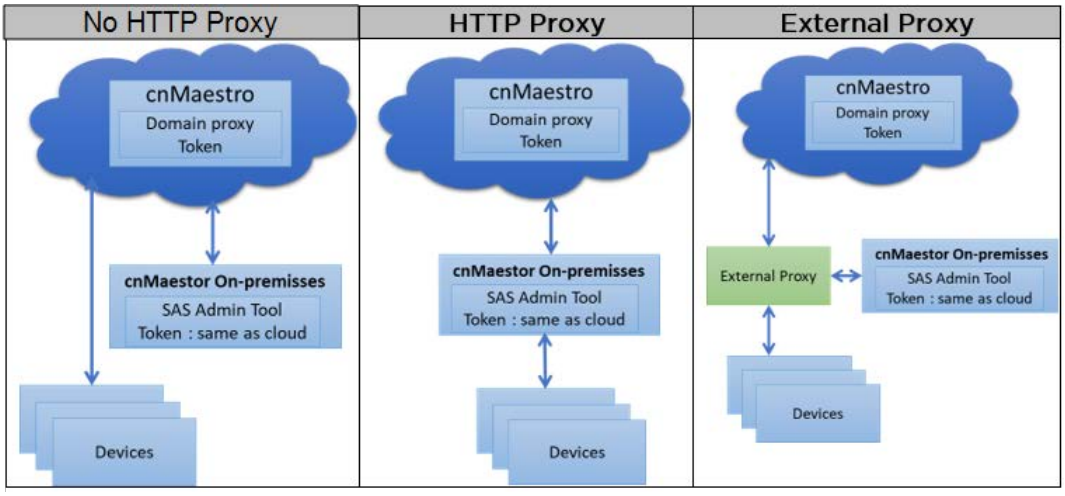
NOTE

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

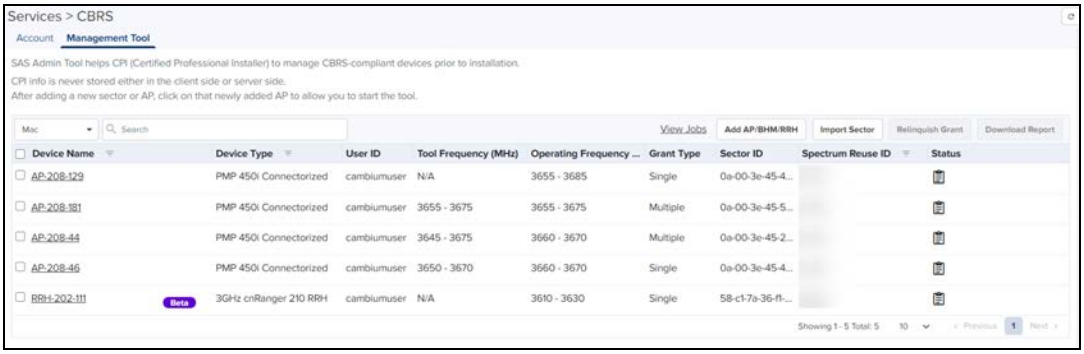
The Management Tool helps run the CBRS procedure before physically connecting CBRS-complaint devices to the network. The following Cambium CBRS-compliant devices operate in 3.6 GHz band frequency, ranging from 3550 to 3700 MHz:

> **NOTE**
>
> cnMaestro release 3.0.2 supports CBRS Multi-Grant feature. PMP devices require release 20.2 software to support Multi-Grant feature.

- PMP 450m AP 3 GHz
- PMP 450i AP and SM 3 GHz
- PMP 450 AP and SM 3.6 GHz
- PMP 450b 3 GHz (to be supported in future)
- 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

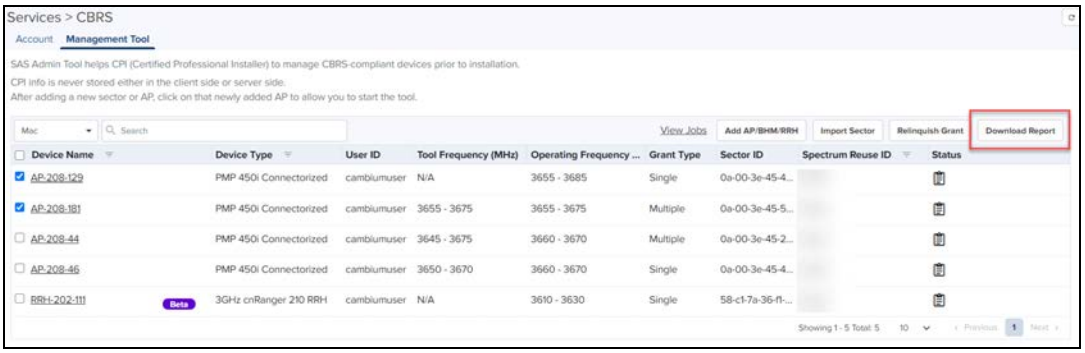
The CBRS procedure can be started and managed by an authorized CPI (Certified Professional Installer). CPIs are required to enter necessary credentials to run and modify the CBRS parameters.

A sector view of CBRS page is shown below:



Download Report

The Download Report allows the user to download multiple device reports in a **.CSV** format.



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.

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, which supports the Multi-Grant feature.

Creating a Management Tool Sector

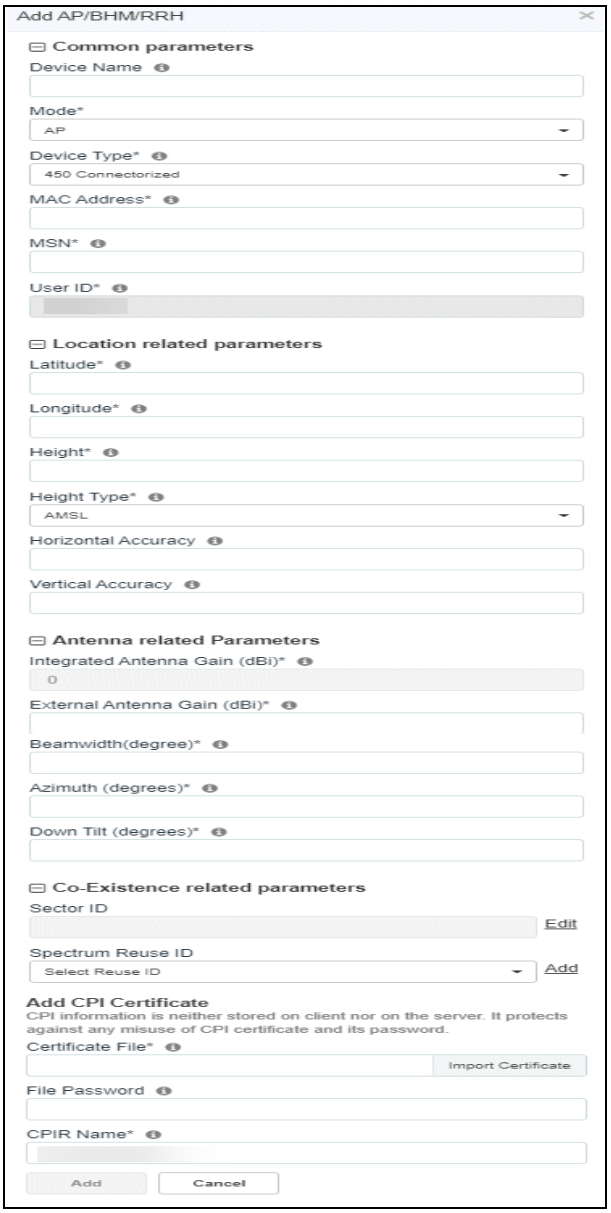
A sector can be created in two ways:

- Add AP/BHM/RRH : Adding all parameters manually of an AP/BHM/RRH.
- Import Sector: Uploading 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 and Spectrum Reuse ID.
- **Add CPI Certificate**: Certificate File, File Password, CPIR Name.



- Click **Add** to add a sector.

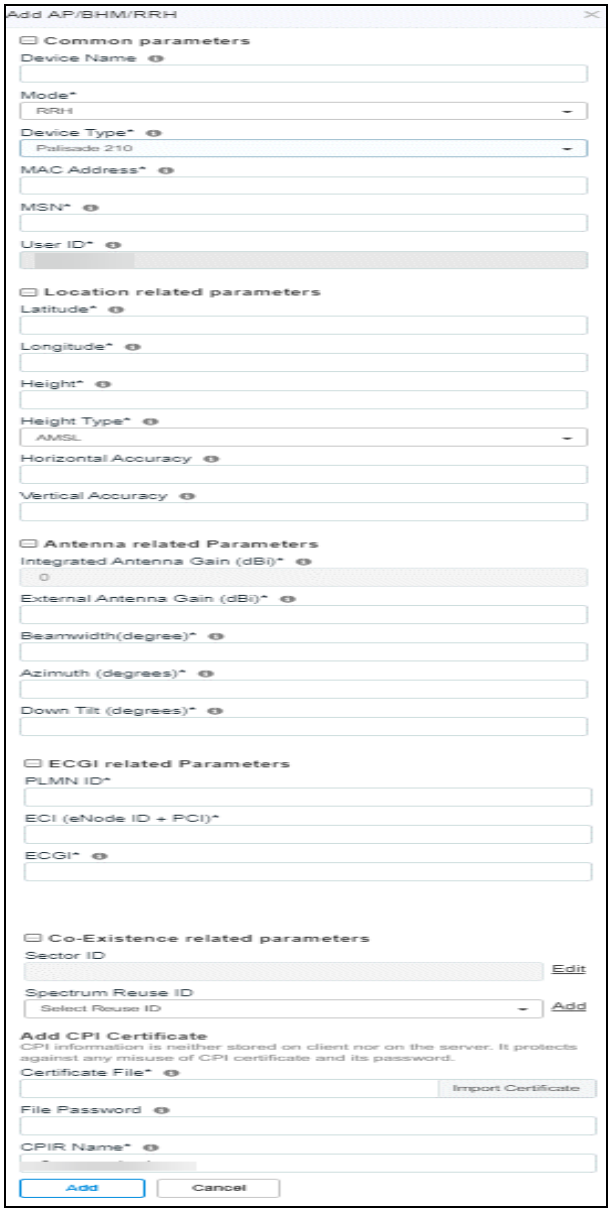
> **NOTE:**
> Refer to CBRS Device Parameters for additional details.

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.

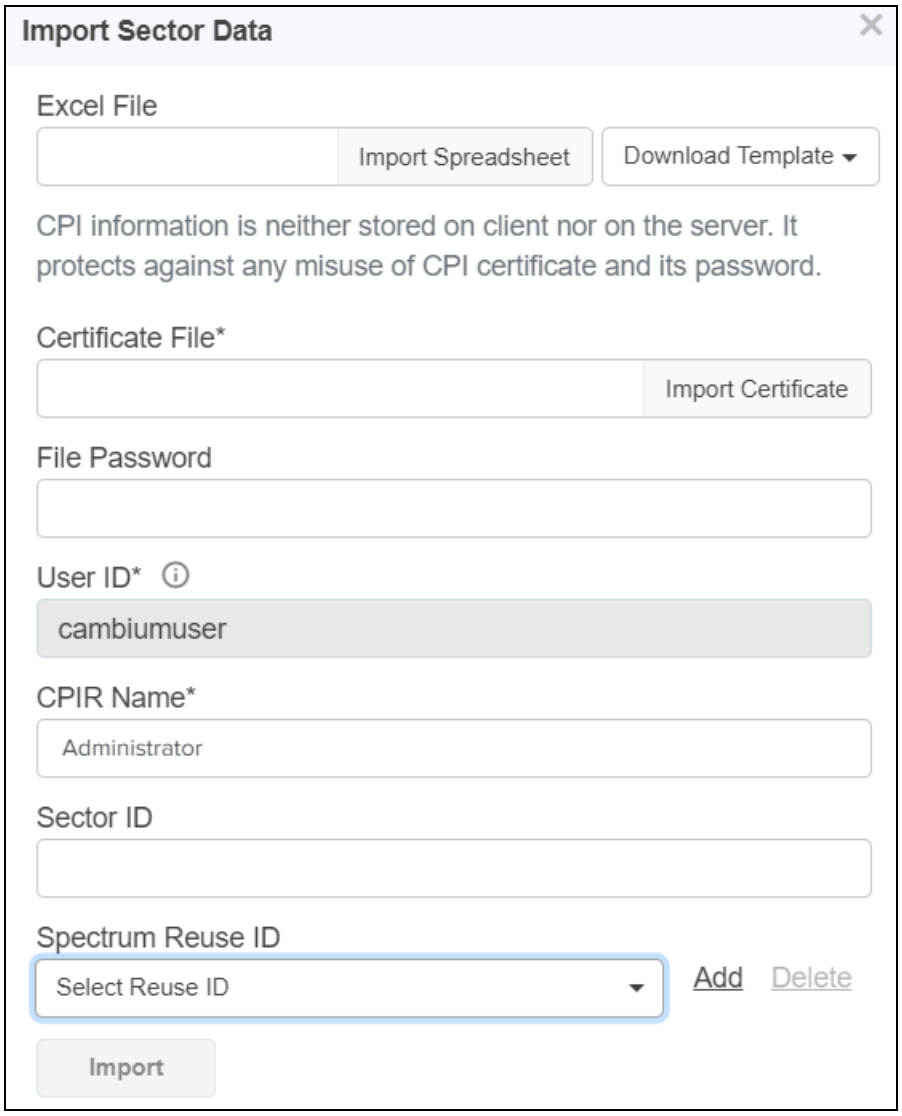
- **Add CPI Certificate**: Certificate File, File Password, CPIR Name.



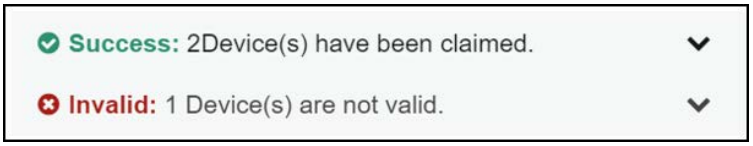
Import Sector

To import a sector:

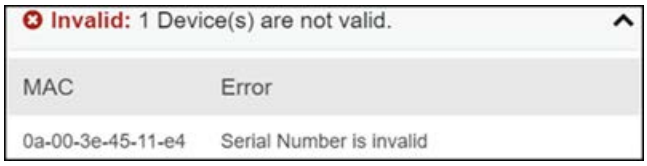
1. Navigate to **Services > CBRS > Management Tool** and click **Import Sector**.



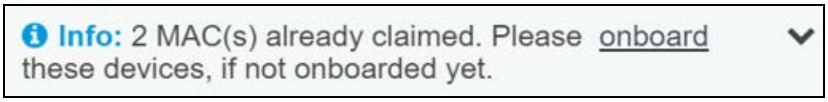
2. Click **Download Template** if user does not have Import Sector template. Users can download two different template formats: **PMP Excel** or **PMP ODS**.
3. Click **Import Excel** to select Import Sector template file. File must be Microsoft Excel format (.xlsx) or OpenDocument Spreadsheet (ods) 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. Click **Import** once the file is selected.
6. Import status is displayed as **Success, Info,** and **Invalid.**



7. Details of Success, Info and Invalid can be seen by clicking arrow ( ).



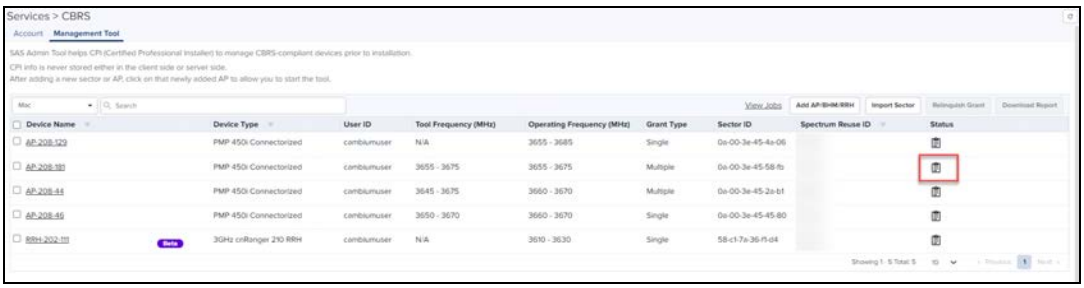
8. If the device is already claimed, it can be onboarded by clicking the **onboard** link.



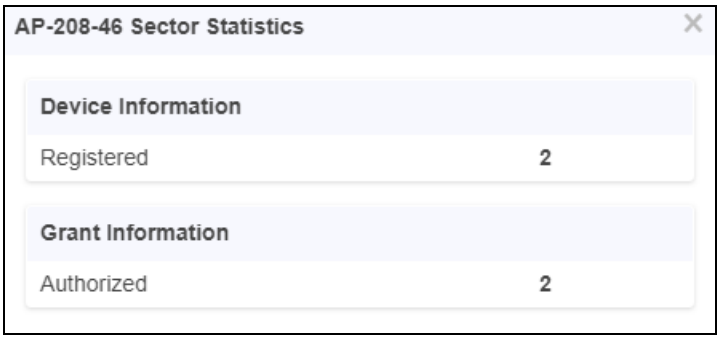
Management Tool Sector Statistics

To view Sector Statistics:

1. Navigate to **Services > CBRS > Management Tool.**
2. Click **View Sector Statistics** under **Status**.



3. **Sector Statistics** window pops-up and displays as shown below:



NOTE:

Refer to the CBRS State Diagram for additional details.

Search Management Tool Sector

To search for a sector:

1. Navigate to **Services > CBRS > Management Tool.**
2. Select search option **CBSD** or **MAC:**

- **CBSD**: Search by CBSD ID
- **MAC**: Search by MAC ID

3. Enter text in search box to display filtered records.

NOTE:

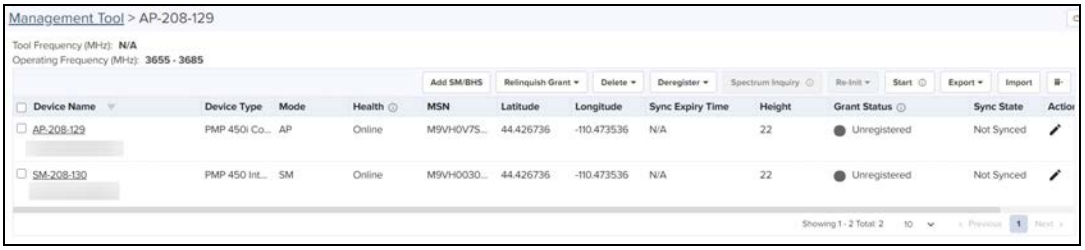
- If an AP device is entered in the search option, it displays the both AP devices and the related SM device.
- If an SM devices is entered in the search option, it displays only the SM devices.

4. Filtered AP or sectors can be cleared by clicking or **Clear** button.

Sector View

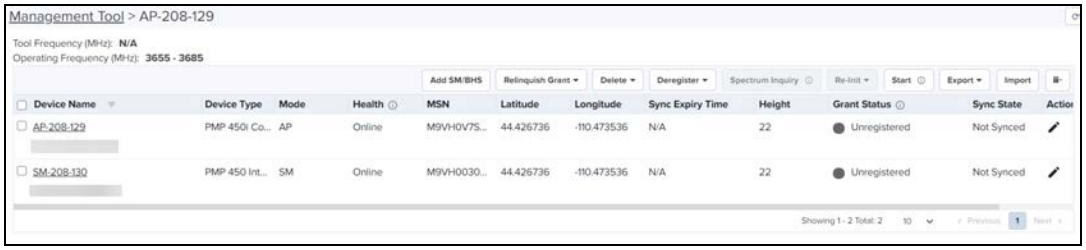
1. Click a sector from the Sector AP column to get the list of devices.

2. All devices of sector is displayed.

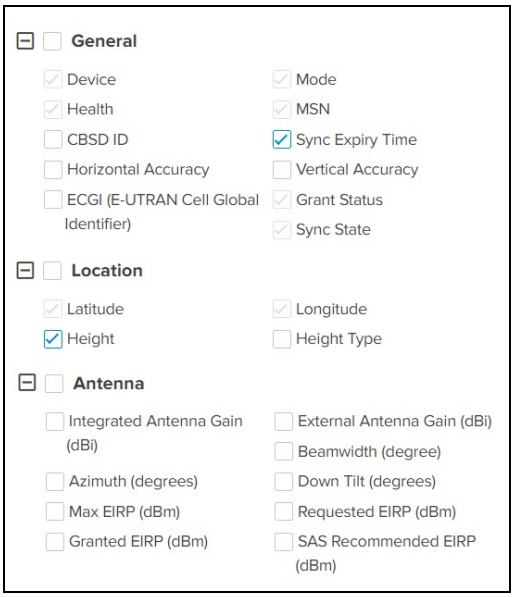


Sector Details View

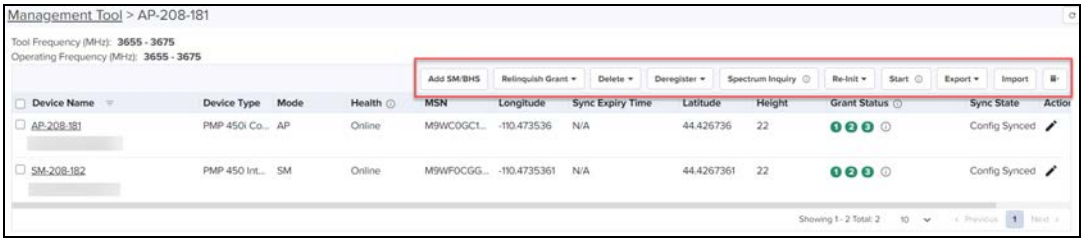
- The Sector Details view displays the following fields by default:
  - Device Name, Device Type, Mode, Health, MSN, Latitude, Longitude, Sync Expiry Time, Height, Grant Status, Sync State, and Actions.



- 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.

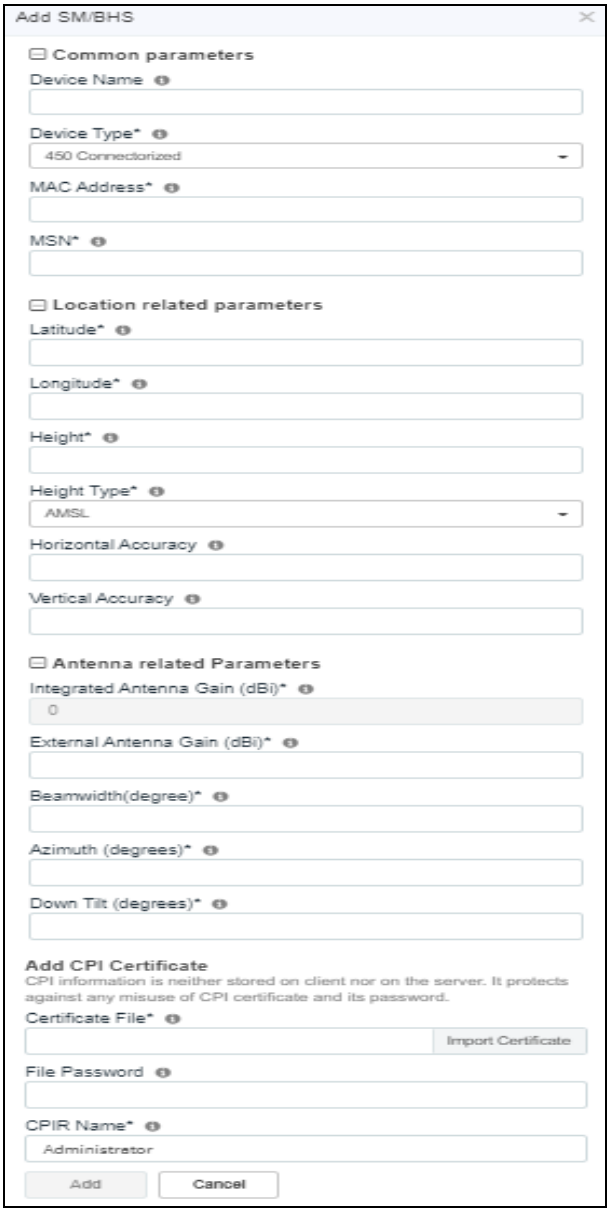


- Use the following buttons to control CBRS procedure:



  - **Start** and **Stop** manage the CBRS procedure of a sector.
  - **Reinitialize**: re-starts the CBRS procedure from UNREGISTERED state.
  - **Deregister:** deregisters the device (single or multiple).
  - **Spectrum Inquiry**: checks the availability of frequencies.
  - **Delete**: deletes device (single or multiple).
  - **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.

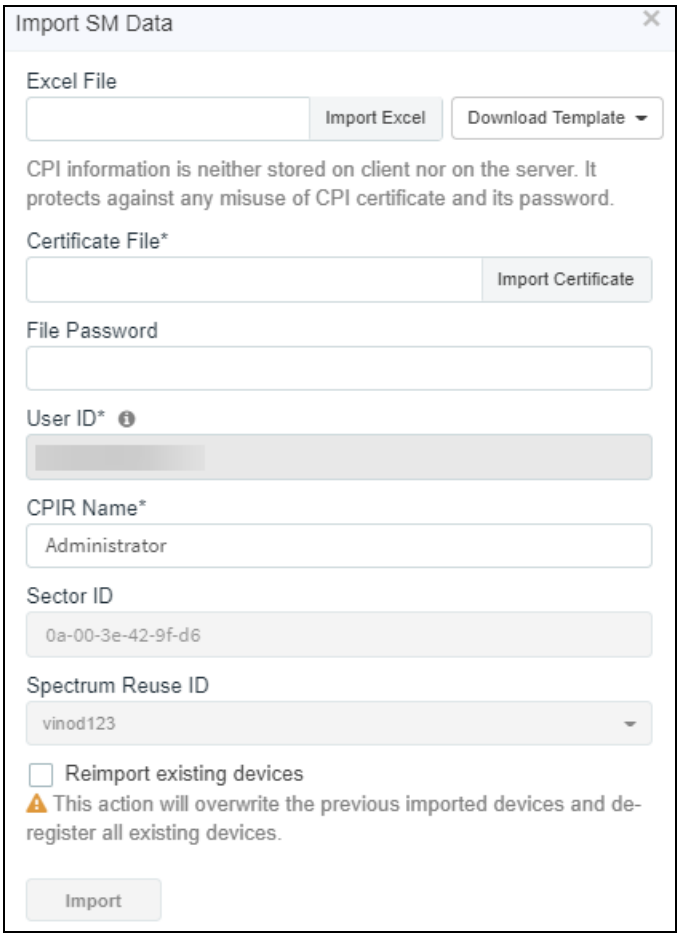
Add SM/BHS



1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Add SM/BHS** button to add SM in a sector.
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 **Re-Import Devices** to overwrite the previous imported data and deregister all existing devices.

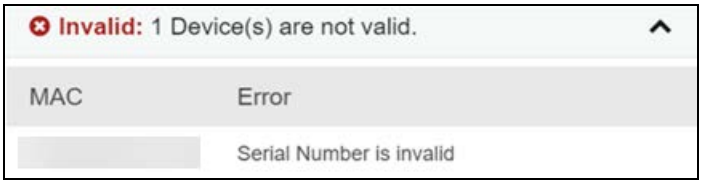


4. Click **Download Template** if user does not have Import Sector template. Users can download two different template formats: **PMP Excel** or **PMP ODS**.
5. Click **Import Excel** to select Import Sector template file. File must be Microsoft Excel format (.xlsx) or OpenDocument Spreadsheet (ods) formats.
6. Enter CPI Credentials:

- Upload CPI Certificate File by clicking **Import Certificate** button.
- Enter CPI File Password.
- Enter CPI Registered Name.

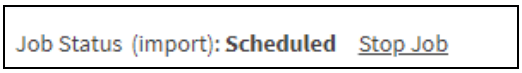
7. Click **Import** button once the file is selected.
8. Import status is displayed under Success, Info and Invalid sections.

9. Details of Success, Info and Invalid can be seen by clicking .



10. If the device is already claimed, it can be onboarded by clicking **onboard** link.

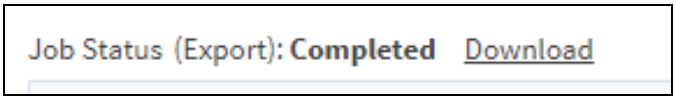
11. Once the user clicks **Import**, a job will be scheduled and updated once complete.



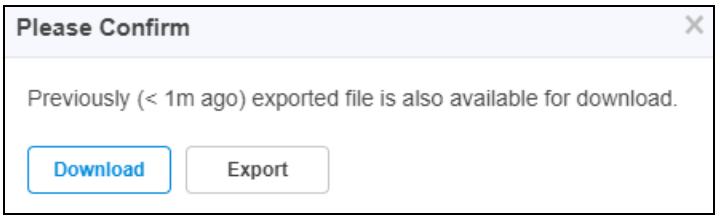
Export Sector

1. Navigate to **Services > CBRS > Management Tool** and then select a **sector**.
2. Click **Export** button to export the sector and pop-up a window **as xlsx**.

3. Once the user clicks as **xlsx**, a job will be scheduled and will update once complete.



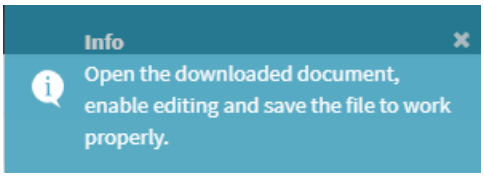
4. The Requested EIRP column of the exported spreadsheet is the most recent configuration value known to the tool, not the most recent value updated from the device via the LIVE status feature, even though the tool displays the updated value from the device on the GUI. Take, for example, an operator who originally loaded a spreadsheet into the tool with an AP requested EIRP of 35 dBm. The operator pushes that configuration/grant to the device, but weeks later they decide to relinquish that grant and request for a new grant for 37 EIRP. Let's assume the relinquish and new grant request was done directly on the AP.
5. The AP would live update cnMaestro with the new EIRP value of 37, which would be displayed on the CBRS Management Tool UI. However, an export from the tool would populate the newly created spreadsheet with the tool database value of 35 EIRP.
6. Once the Job status is Completed, click **Download** to download the Sector xlxs.



NOTE:

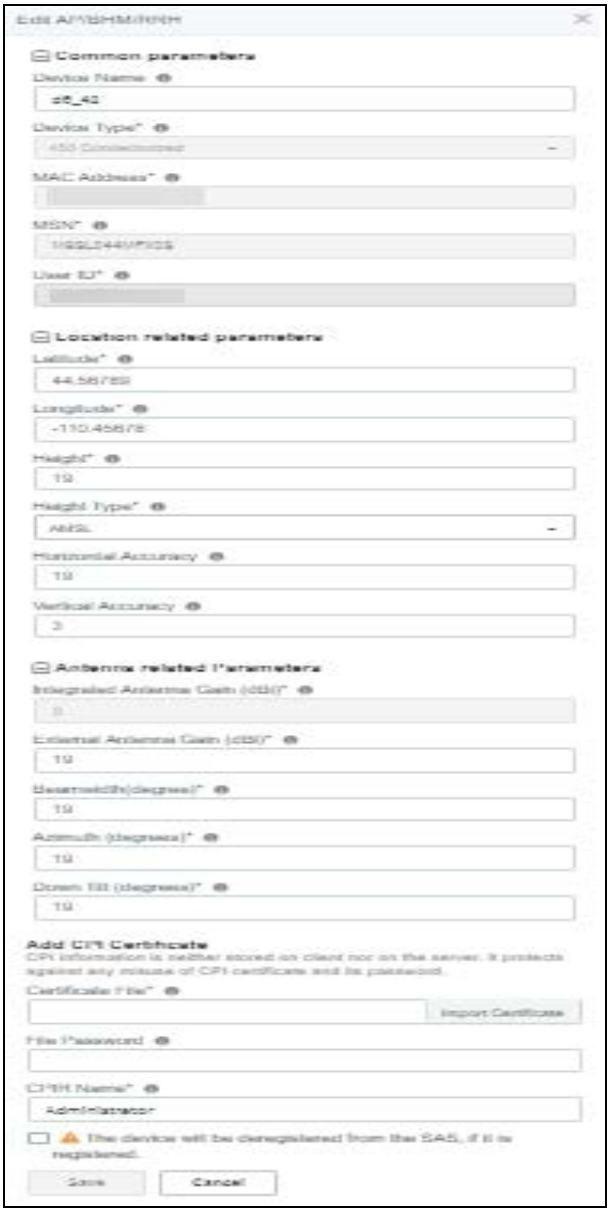
Download button is enabled only for two hours from the time of export job status is completed. After two hours, the user needs to schedule the export job to download the latest xlxs file.

7. User can use the downloaded .xlxs 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 I**mport Certificate** button.
   - Enter CPI File Password.
   - Enter CPI Registered Name.

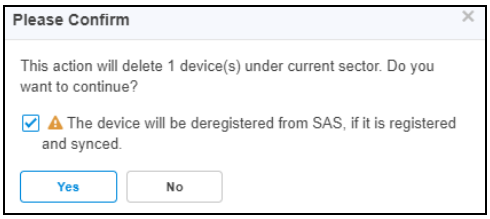


5. Click **Save.**

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 de-register 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.

5. Display pops-up to confirm the action and click **Yes.**



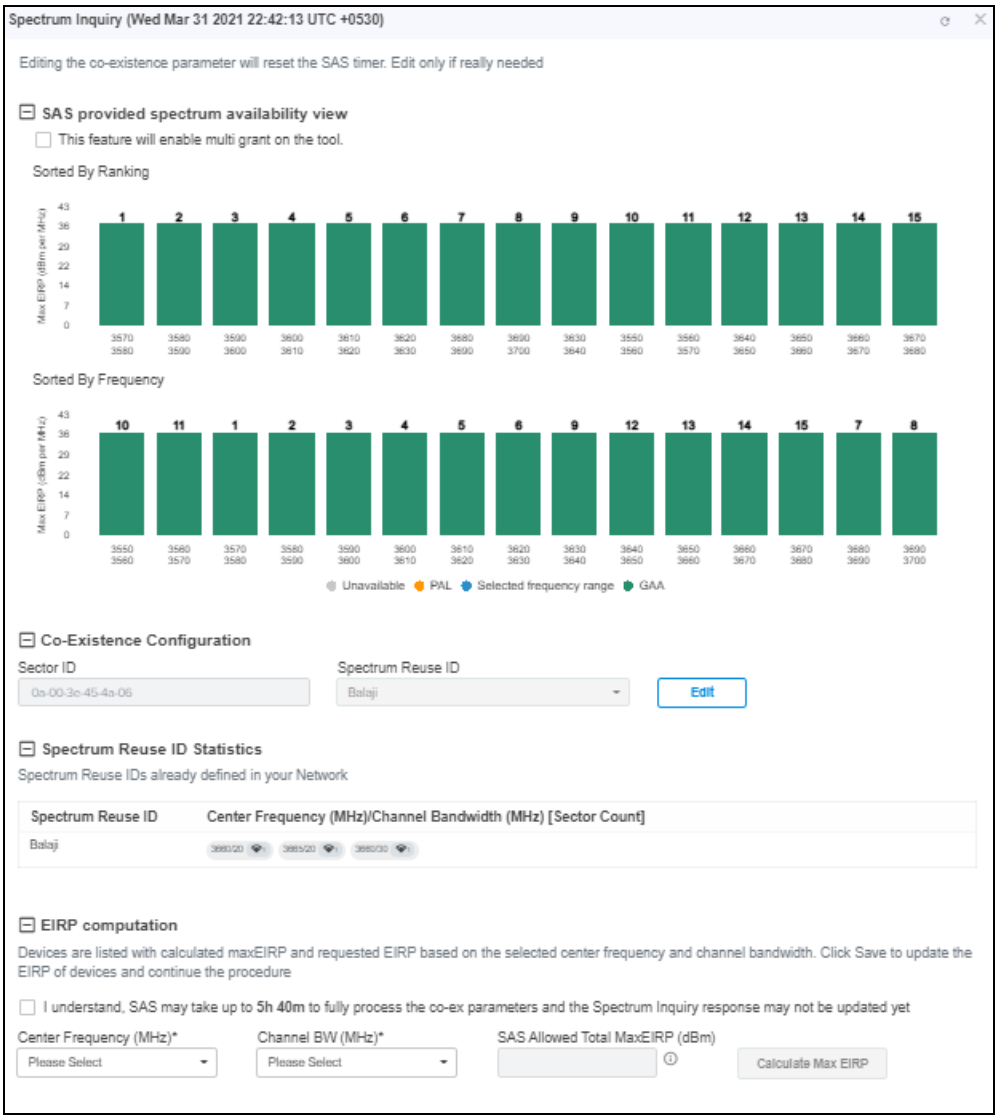
6. Once the user clicks **Yes**, a job will be scheduled and update once complete.

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**.

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.



NOTE:

Multi-Grant is enabled by default.

4. User can disable the Multi-Grant feature by disabling the checkbox **This feature will enable multi grant on the tool** to create Wide-Grant. To create Multiple Grant, refer Multiple Grant.
5. Click Edit to edit **Co-Existence Configuration** and **EIRP Computation.**
   - **Spectrum Reuse ID Statistics** displays the devices running on different sector, channels, and bandwidth based on the **Spectrum Reuse ID**.
6. Once the Spectrum Inquiry is verified, click **Save**.

Once the Sector is created it displays as shown below:

NOTE:

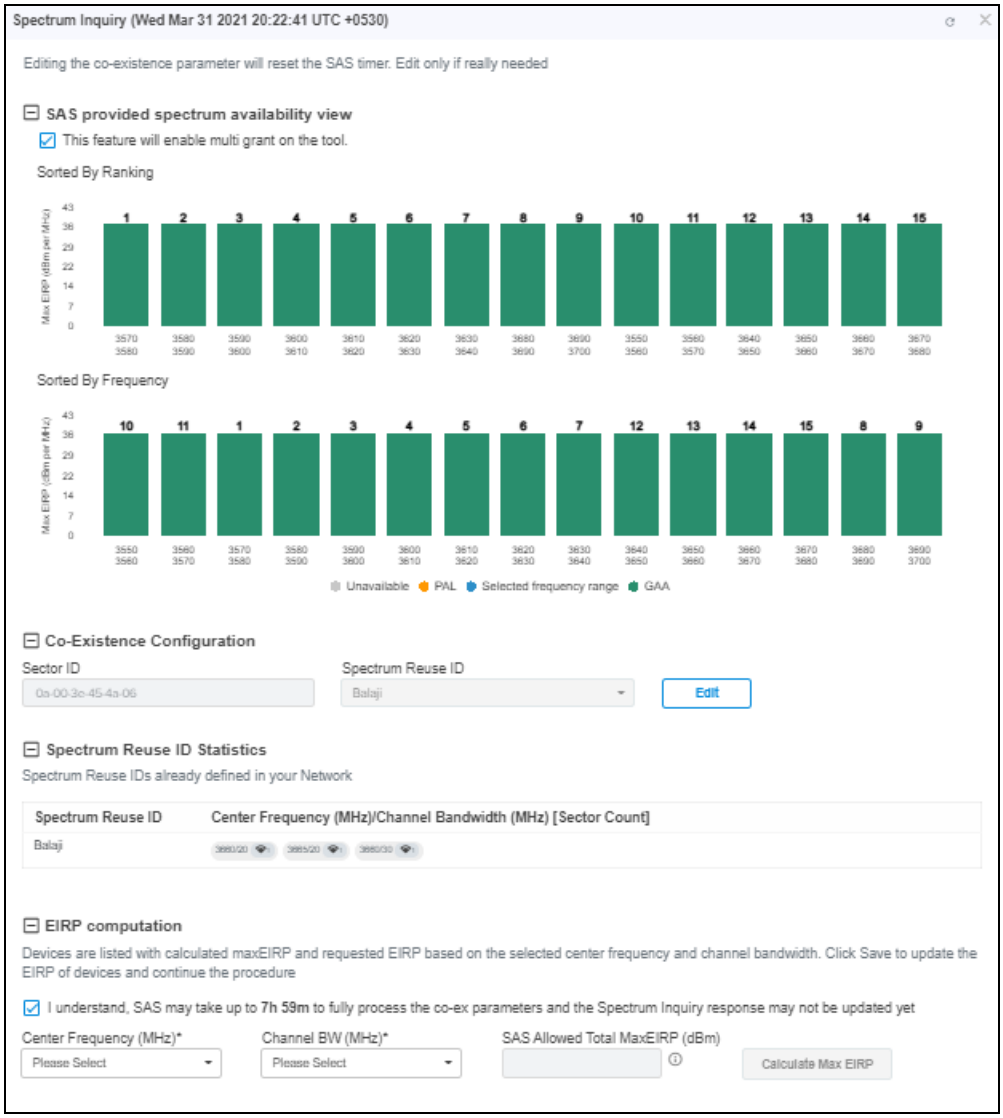
- If the device is already synced with the Management Tool, the CBRS Start and Stop procedures are not applicable for all the synced devices.
- If user does not see the **Start** button, it means the CBRS procedure is already running.
- If all devices of the sector are in AUTHORIZED or HALT status and the user tries to start the CBRS procedure, the **Start** button will go to Stop state (as CBRS procedure is completed for all devices).

Multi-Grant

Multi-Grant feature divides selected channel bandwidth 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.



NOTE:

Multi-Grant is enabled by default.

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.

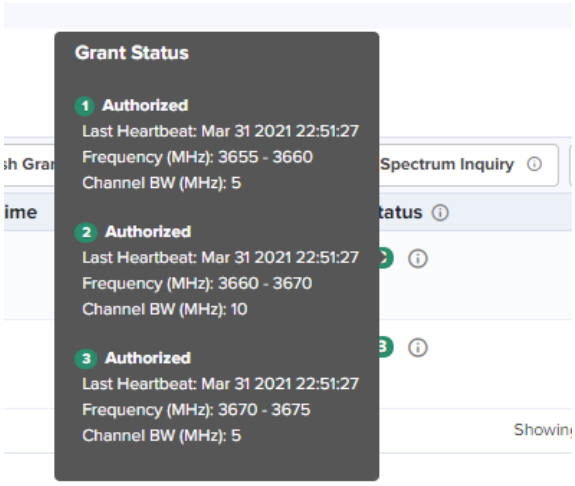
NOTE:

SAS may take upto 7 to 8 hours to fully process the Co-Existence parameters.

6. Once the Spectrum Inquiry is verified, click **Save**.

Once the Sector is created with Multiple Grants will be displayed as shown below:

To view the Grant Status click the info icon displays as shown below:



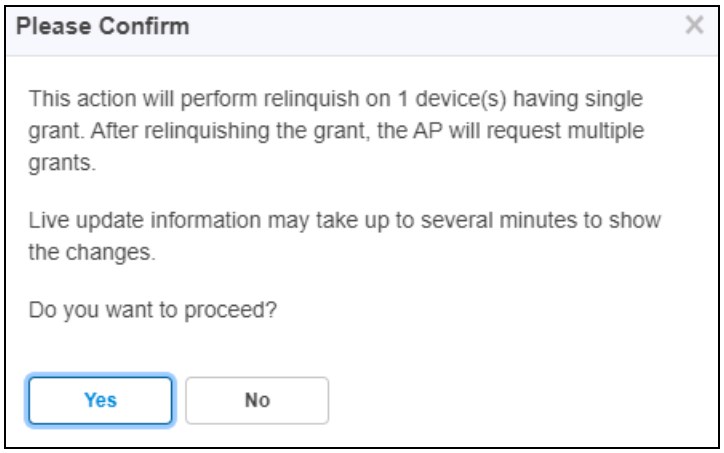
Relinquish Grant

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 **Reinitialize** 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 **Reinitialize** button. On click of **Reinitialize** the 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 **Reinitialize** button after pressing **Stop** button. It is due to a delay in properly stopping the CBRS procedure.

4. Click **Reinitialize** to start the reinitialization 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 and update once complete.

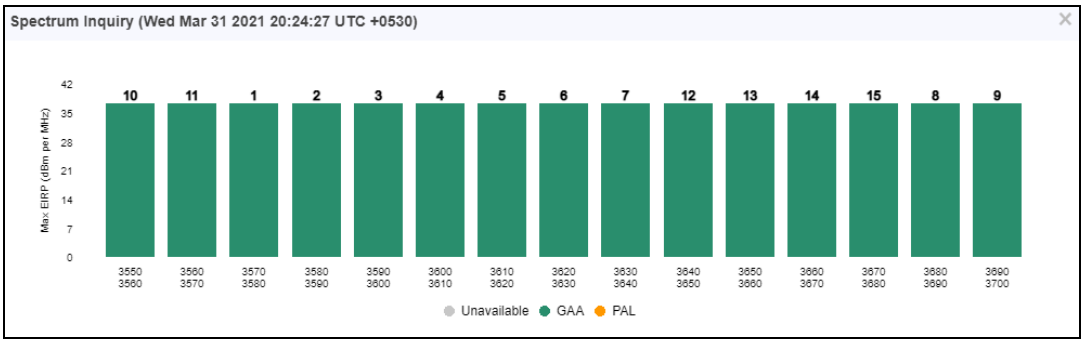
Job Status (Deregistration): **Completed**

6. In case, the deregistration fails, the reasons will be indicated under .

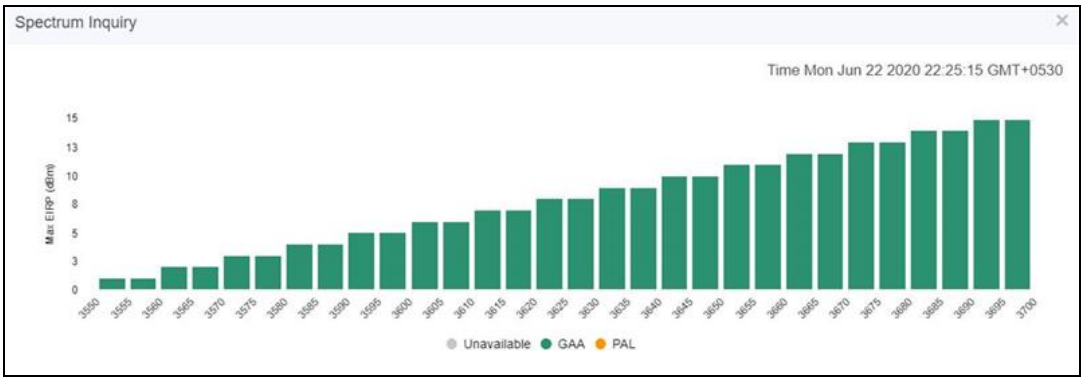
Spectrum Inquiry

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Spectrum Inquiry** button.
3. **Spectrum Inquiry** status button is enabled once the device is registered (REGISTERED state) to the SAS.

- If the selected SAS is not Google, EIRP is unsupported, and Spectrum Inquiry is displayed as shown below:



- If the users is selected SAS is **Google,** it supports **EIRP.** Spectrum Inquiry displays as below:



- **GAA**: General Authorized Access
- **PAL**: Priority Access License

Spectrum availability can be checked by hovering over frequencies.

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.

It displays the possible single Grant state such as:

- *Unregistered*
- *Registered*
- *Registering*
- *Grant*
- *Grant Suspended*
- *Grant Terminate*
- Relinquished Spectrum
- *Relinquishing Spectrum*
- *Authorized*
- Deregistering
- *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.

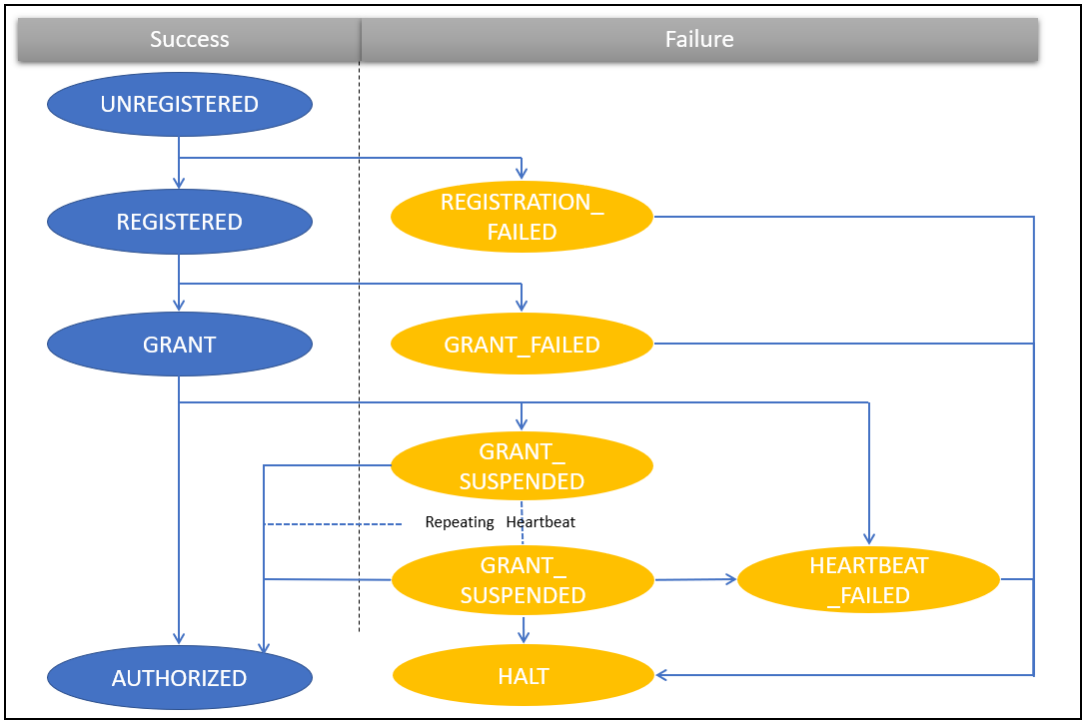
1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Sync** to perform the synchronization procedure.
3. Click **Yes** to enable CBRS on AP/BHM after successful sync or click **No** to cancel synchronization procedure.

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:

- *Authorized*
- *Deregistered*
- *Deregistering*

- *Deregistration Failed*
- *Granted*
- *Grant Failed*
- *Grant Suspended*
- *Grant Wait*
- *Halt*
- *Heartbeat*
- *Heartbeat Failed*
- *Others*
- *Registration Failed*
- *Registered*
- *Registering*
- Relinquished Spectrum
- *Relinquishing Spectrum*
- *Relinquishing*
- *Unknown*
- *Unregistered*

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_ FAILED.

Category	Parameter	Details
Location	Height	Device antenna height in meters.
	Height Type	Should be AGL or AMSL as follows: • AGL height is measured relative to the ground level. • AMSL height is measured relative to the mean sea level.
	Horizontal Accuracy	A positive number in meters to indicate the accuracy of the device antenna horizontal location.
	Latitude	Latitude of the device antenna location in degrees.
	Longitude	Longitude of the CBSD antenna location in degrees.
	Vertical Accuracy	A positive number in meters to indicate the accuracy of the device antenna vertical location.
Co-Existence Related Parameters	Sector ID	The default AP MAC address and allows editing the default MAC address.
	Spectrum Reuse ID	The Spectrum Reuse ID defined in the network.
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.
Add Certificate	Certificate File	CPI's (Certified Professional Installer) 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

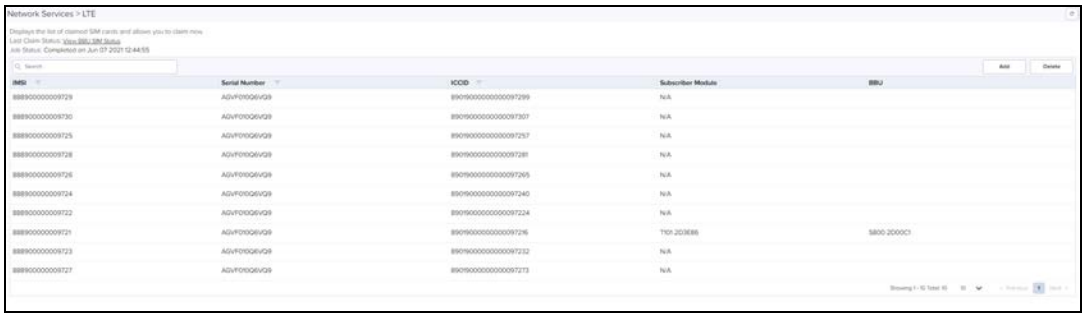
cnMaestro supports LTE as part of its On-Premises deployment. LTE allows customers to onboard the SM with IMSI into cnMaestro.

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).

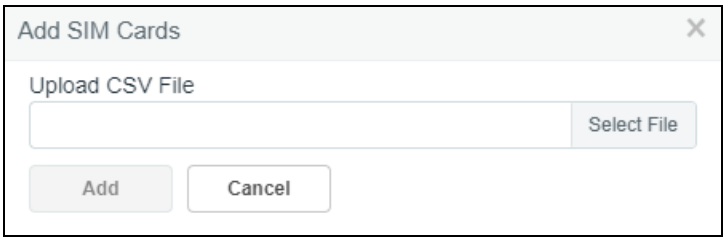
Adding SIM Cards

To add a SIM card:

1. Navigate to **Services > LTE.**



2. Click **Add.** The following window appears.

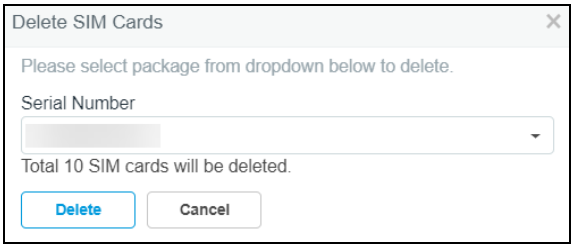


3. Select the CSV file and click **Add**.

> **NOTE:**
>
> For further information on claiming the SIM through a cnMaestro account, refer to https://support.cambiumnetworks.com/files/cnranger/beta

Delete SIM Cards

To delete a SIM card from the list click **Delete.** The following window pops-up.



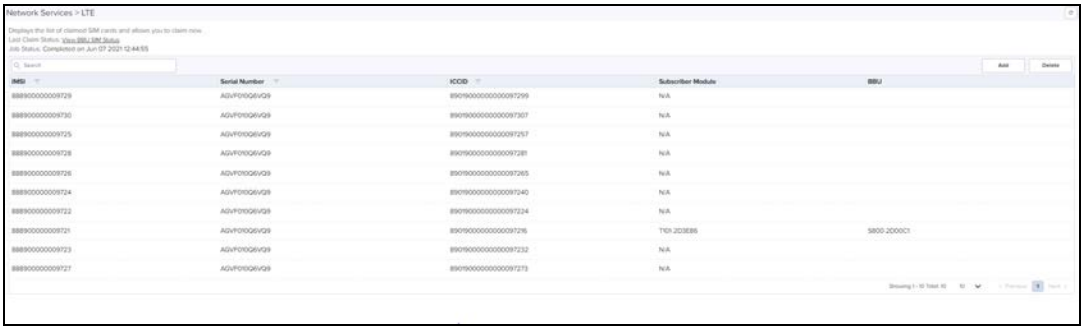
Note:

IMSI numbers are deleted with the mapped Serial Number.

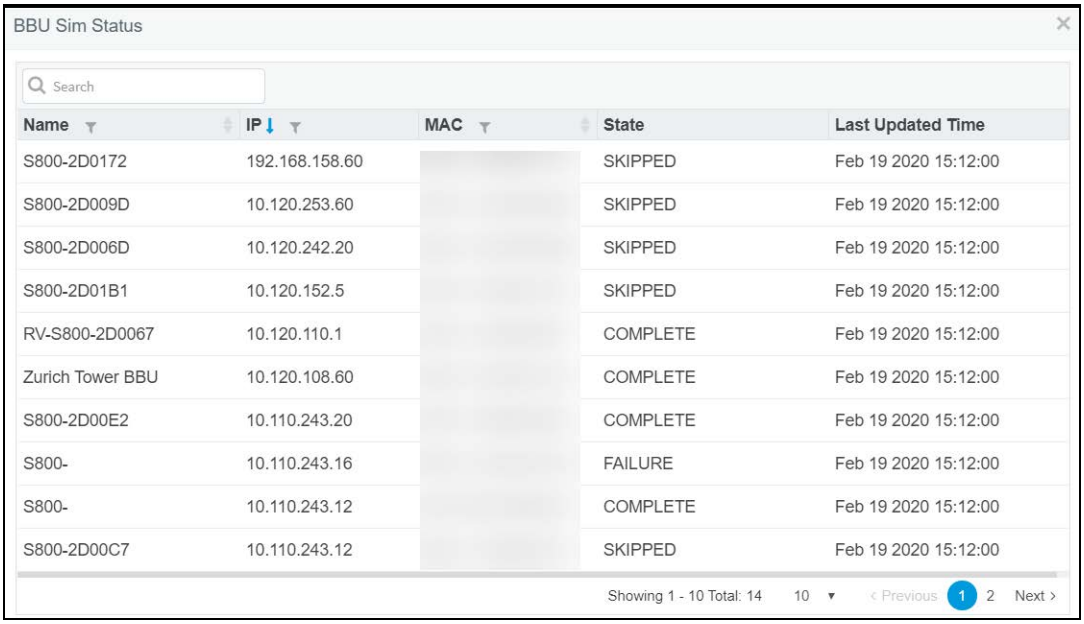
Viewing BBU SIM Status

Allows the users to view the status of the SIM connected to the BBU:

1. Navigate to **Services > LTE.**



2. Click **View BBU SIM Status.**



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

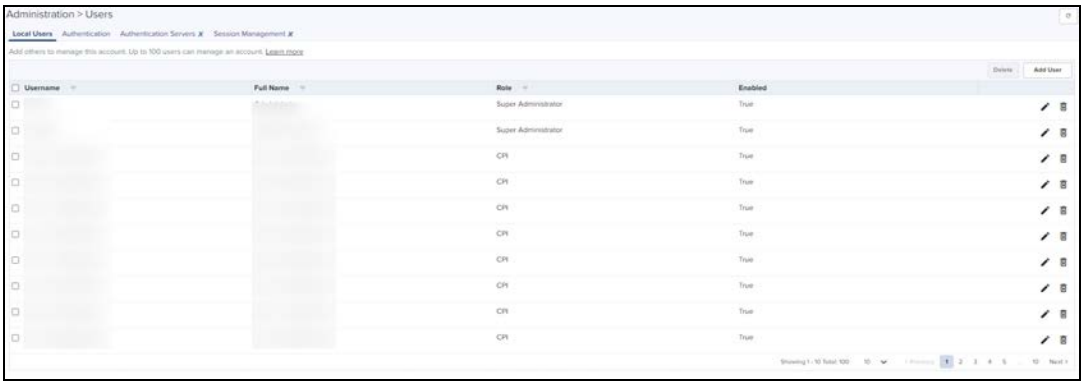
Authentication

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 157 Adding Users



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 45: Role-Mappings

Feature	Description
Authentication Services	Create and configure Authentication servers. • Super Administrator - All • Administrator - None • Operator - None • Monitor - None • CPI - None
API Management	API Client. administration. • 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. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Application Settings	Change global application configuration and onboarding key. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None

Table 45: Role-Mappings

Feature	Description
	• CPI - None
Configuration/Software Update and Scheduled Report Jobs	Manage configuration/software update and scheduled report related jobs • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Data Tunnel	Data tunnel configuration. • 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. • 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. • 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. • Super Administrator - All • Administrator - All • Operator -View • Monitor - None • CPI - None

Table 45: Role-Mappings

Feature	Description
Guest Portal	Guest Portal configuration. • Super Administrator - All • Administrator - All • Operator -View • Monitor - View (sessions only) • CPI - View (sessions only)
Monitoring	Display of monitoring data at all levels, VM Monitoring • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - View
Managed Service Provider (MSP)	MSP operations such as modification of branded service, managed account and user invitations. • Super Administrator - All • Administrator - View • Operator - None • Monitor – None • CPI - None **Note:** Operator/Monitor users are not permitted to move devices across managed accounts.
Notifications	Alarms and Events management. • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - None
Onboarding	Device approval, modifying individual device configuration, and performing software update. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - All
Reporting	Report generation. • Super Administrator - All • Administrator - All

Table 45: Role-Mappings

Feature	Description
	• Operator - All • Monitor - All • CPI - All
Session Management	Capability to view and logout other users sessions. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Software Images	Upload and delete device software images. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Software Upgrade	Upgrade the device with the latest software. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None

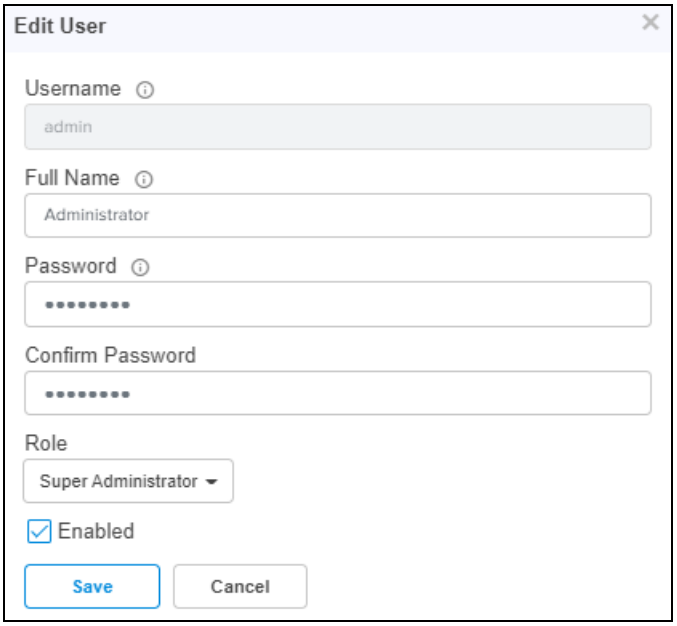
Table 45: Role-Mappings

Feature	Description
SNMP Configuration	SNMPv2c configuration parameters. • 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. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
User Management	User management operations such as manage users and roles. • Super Administrator - All • Administrator - View • Operator - None • Monitor - None • CPI - None

Creating Users and Configuring User Roles

To add 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

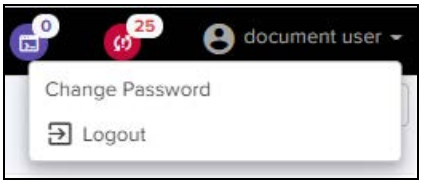
8. Choose the **State** as Enabled or Disabled.
9. Click **Save**.

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 158 Changing Password



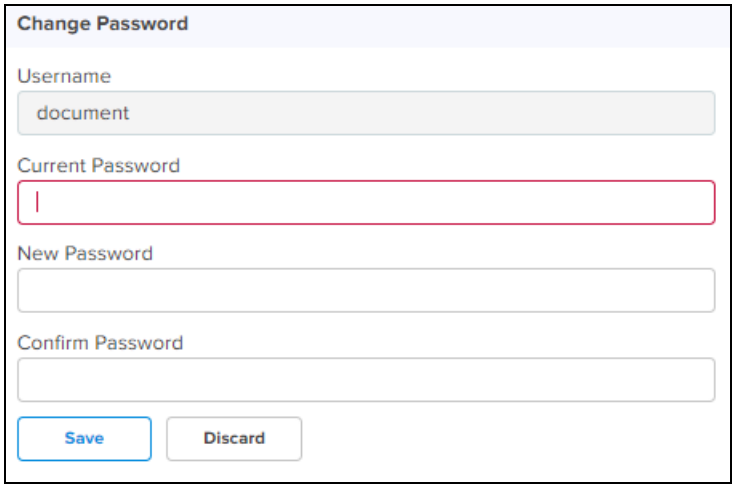
Ensure the primary Authentication must be local users to **Change Password** option. After changing the password, the current session will get logged out.

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 159 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

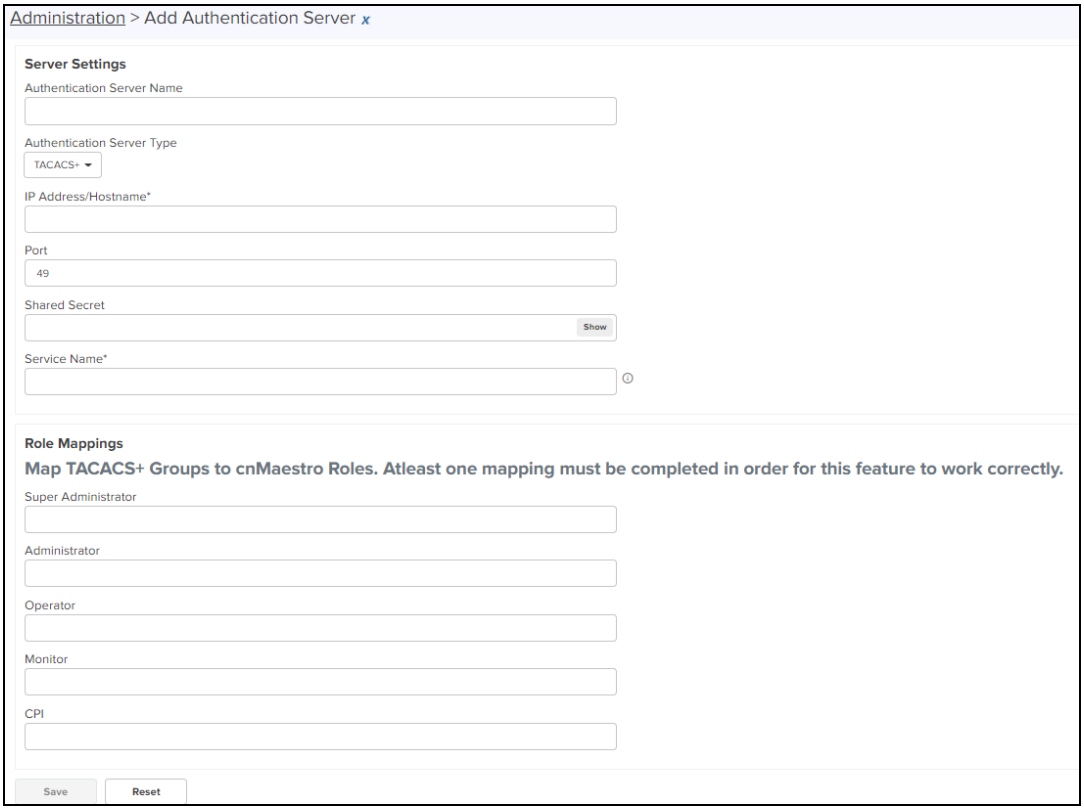
To view all the Authentication servers which are configured in cnMaestro, navigate to **Administration > Users > Authentication Servers**.

Figure 160 List of Authentication Servers

Create New Authentication Server Configuration

1. Navigate to **Administration > Users > Authentication Servers**.
2. Click **Add New Authentication Server**.

Figure 161 Authentication Server



TACACS+

The fields that are present when TACACS+ server is selected are listed below:

Table 46: 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)
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:

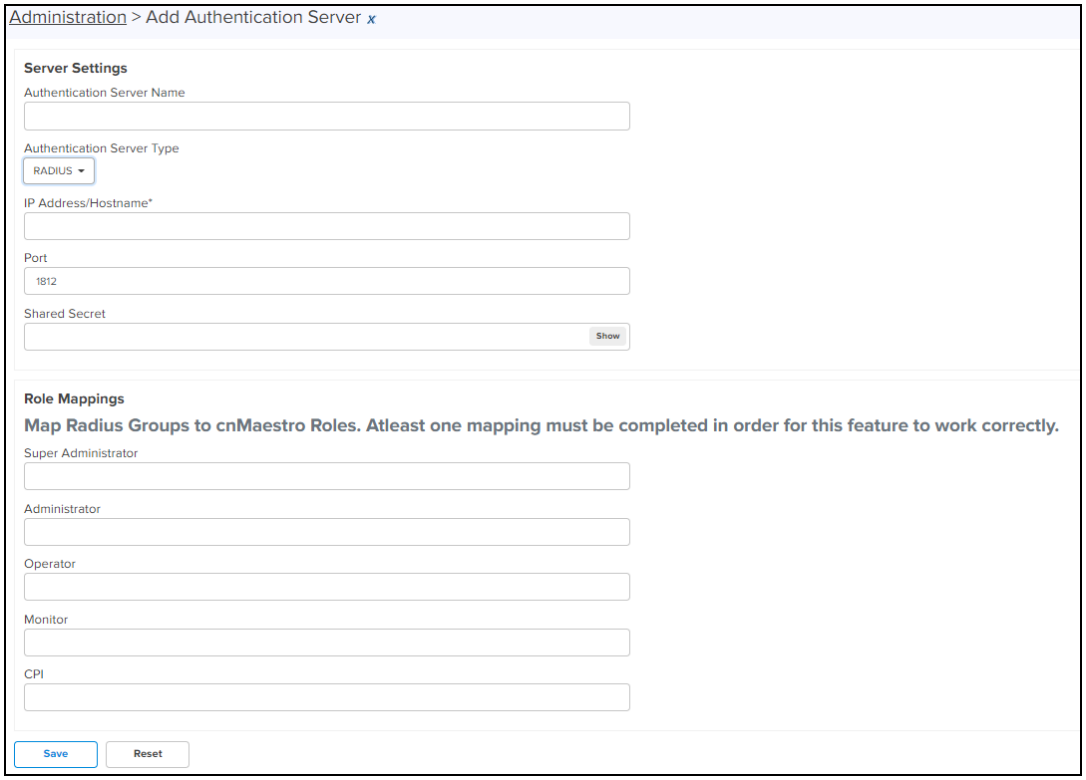


Table 47: RADIUS Parameters

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:

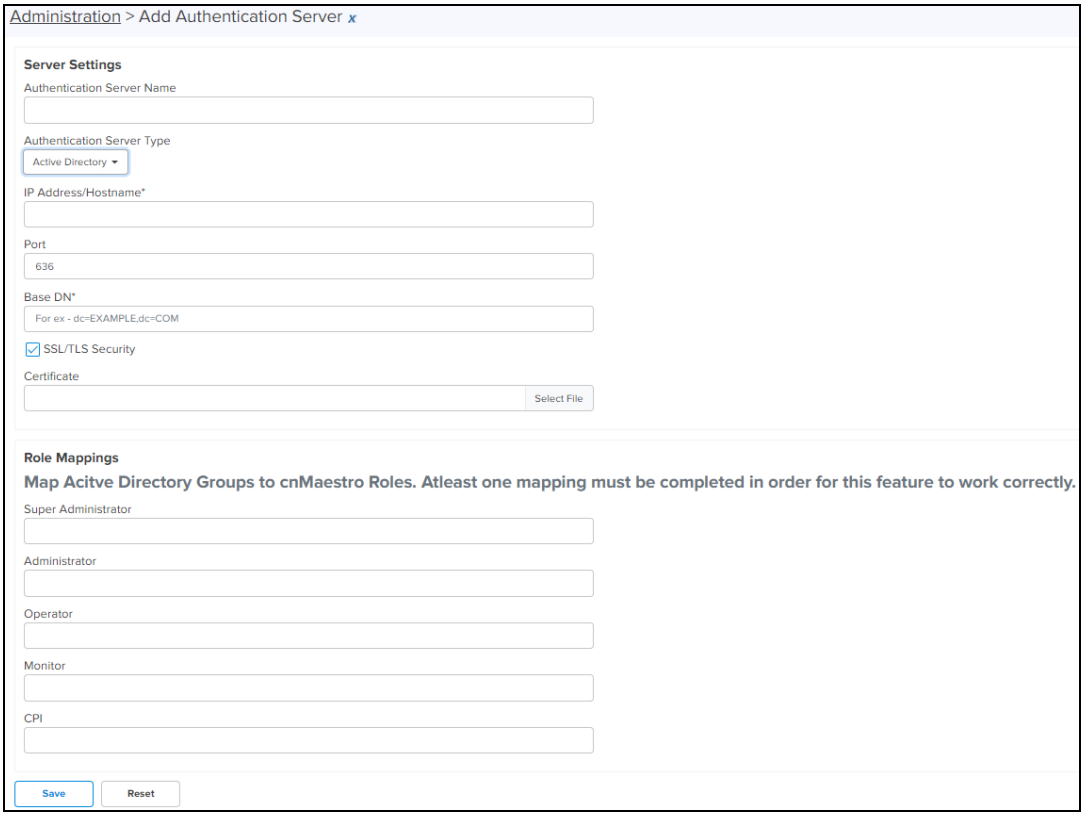


Table 48: Active Directory Parameters

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.

Table 48: Active Directory Parameters

Parameter	Description
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 to 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:

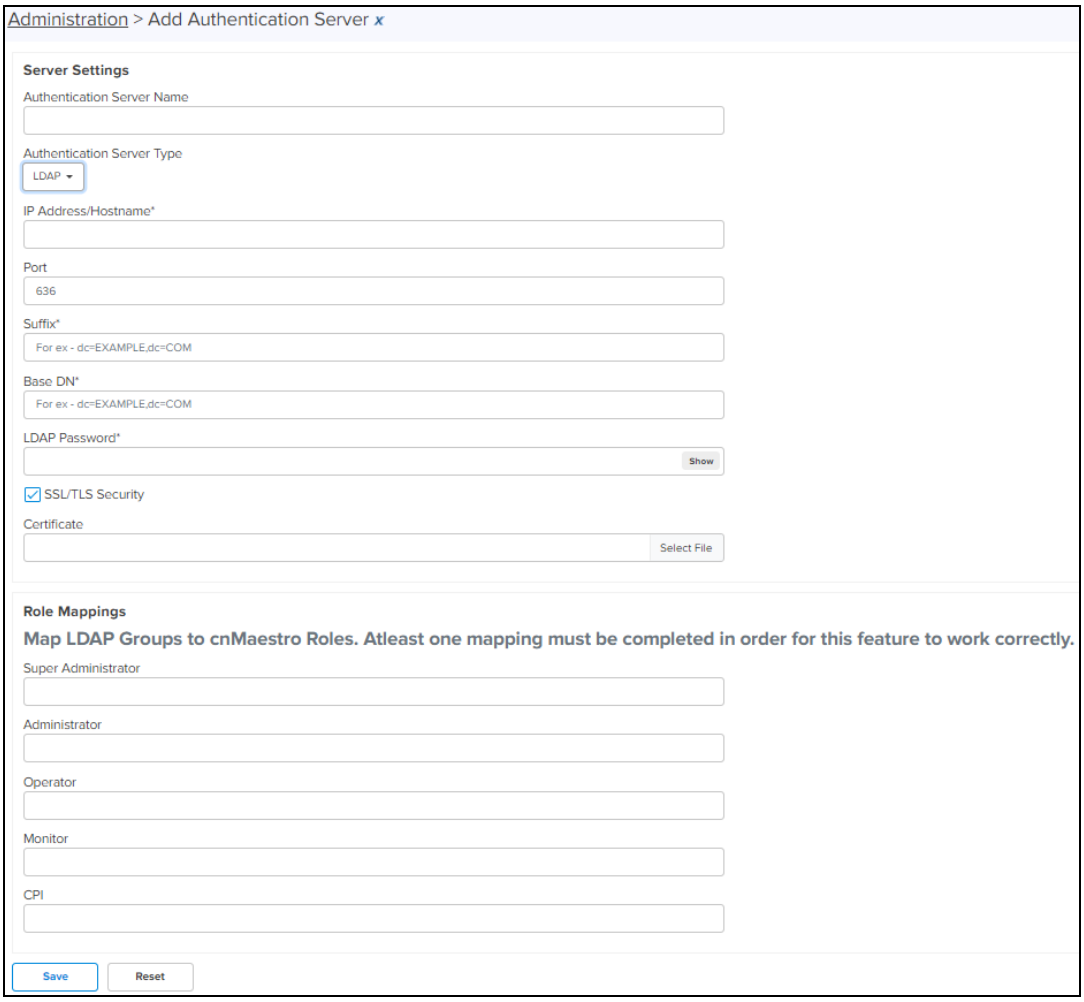


Table 49: LDAP Parameters

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 49: LDAP Parameters

Parameter	Description
Suffix	Suffix is the DNS name. For example: dc= xyz, dc=com.
SSL/TSL Security	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. **Note:** ■ 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	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.

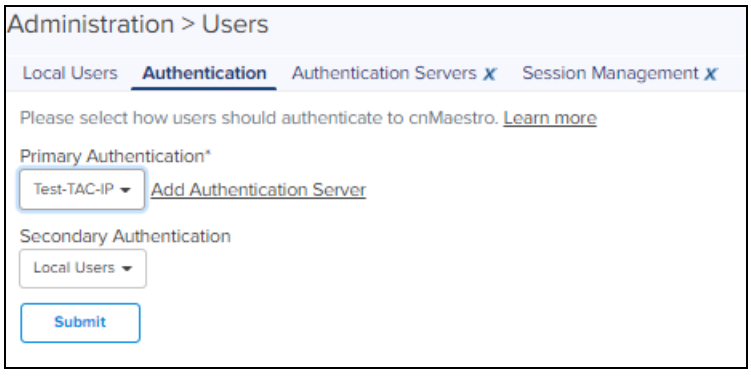
Secondary Server Authentication

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 162 Secondary Server Authentication



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**.

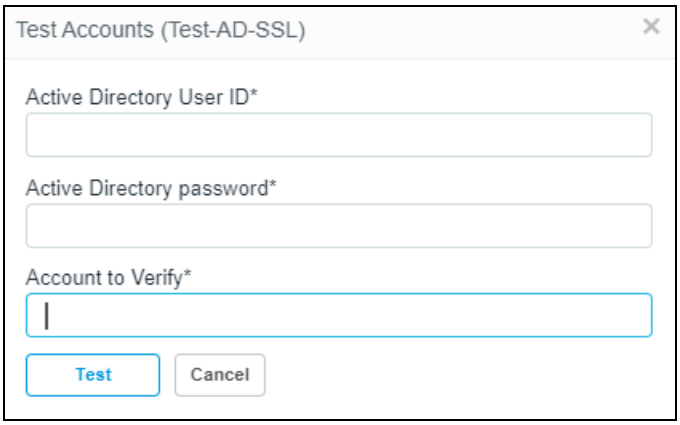
Primary authentication order will change as Local Authentication if this server is setup as Primary Authentication under **Manage Authentication Server Authentication** section.

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:



3. Provide the following details:

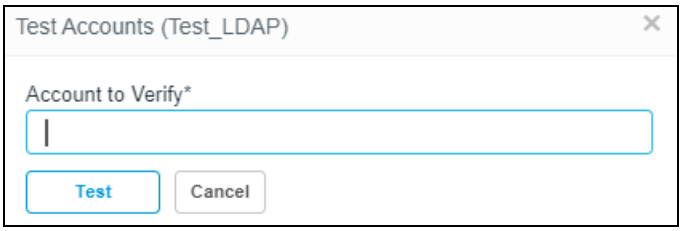
- Active Directory User ID
- Active Directory Password
- Account to Verify

4. Click **Test**.

- To know and verify the role of the **LDAP** user:

1. Navigate to **List all Authentication Servers** page.

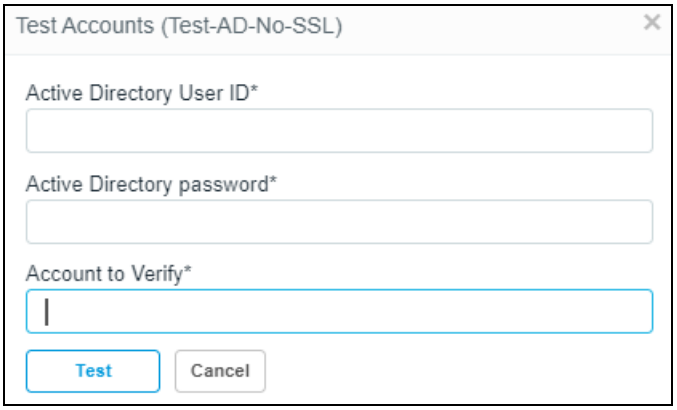
2. Click the **test** icon ( ) next to any of the LDAP type. The following window appears:



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.

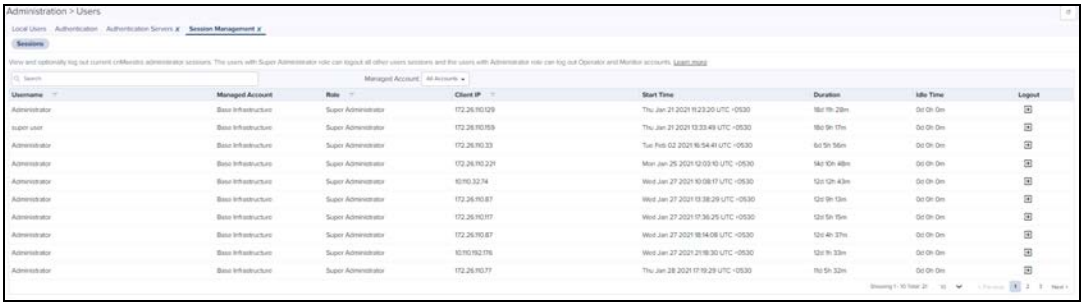
Session Management

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 163 Session Management > Sessions



Server Management

This chapter provides the following details:

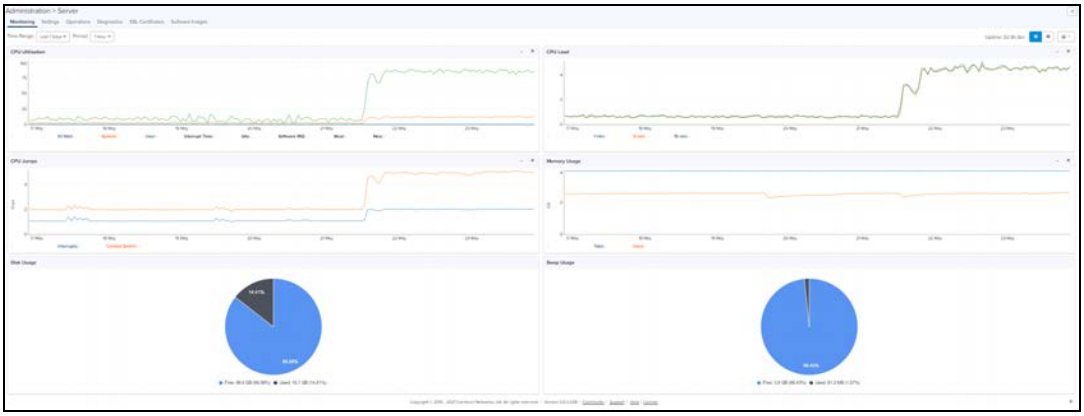
- Monitoring
- Settings
- Operations
- SSL Certificate
- Syslog

Monitoring

The Server tab provides monitoring and operations for the virtual machine instance.

Navigate to **Administration > Server.**

Figure 164 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.

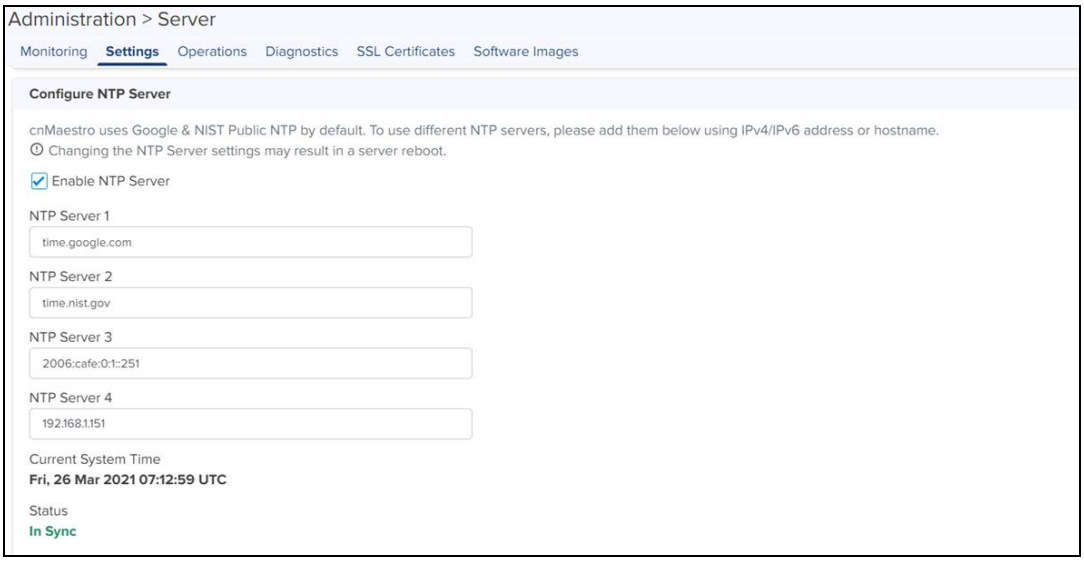
Figure 165 System Name

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.



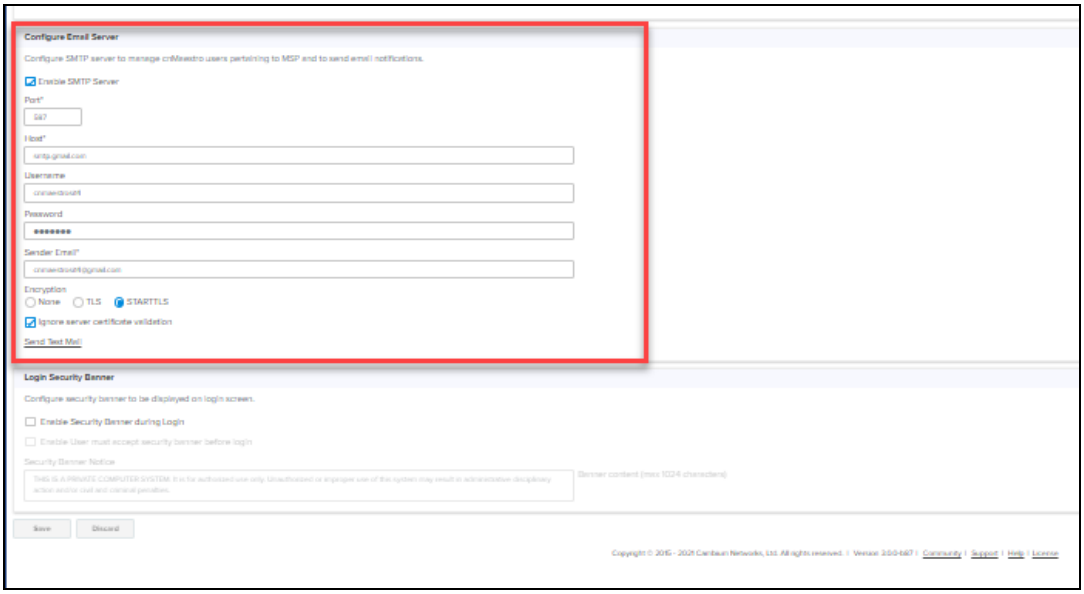
Configure Email Server

The user can configure the email server to send and receive email messages.

To configure the email server:

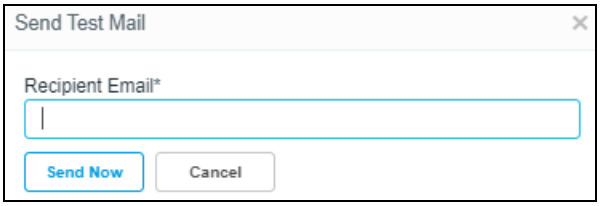
1. Navigate to **Administration > Server > Settings > Configure Email Server** tab.

Figure 166 Email Server



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**.

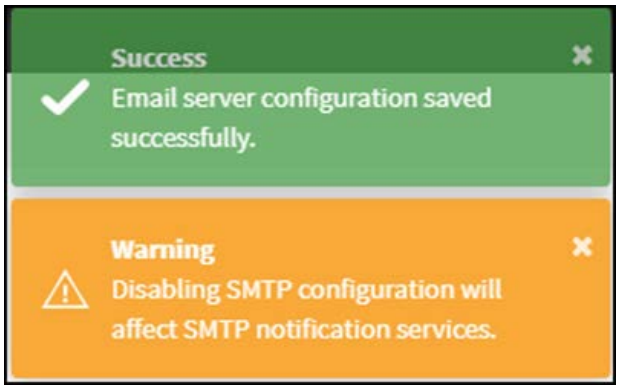
Figure 167 Specifying email address



11. Enter the **Recipient Email**.
12. Click **Send Now**.

NOTE:

When user tries to disable SMTP configuration a warning message pops-up.



Email Notifications

The Email Notifications feature allows the Super Administrator and the Administrator users to add subscribers (Email IDs) for receiving different types of alerts by means of Emails.

> **NOTE:**
> Email Subscribers are limited to two per account.

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.

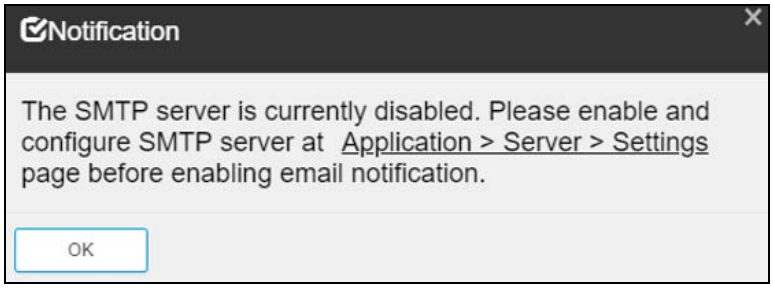


Figure 168 Email notifications

You can use the filter option for the following fields:

- Email
- Severity

- Status
- Ignore Notification

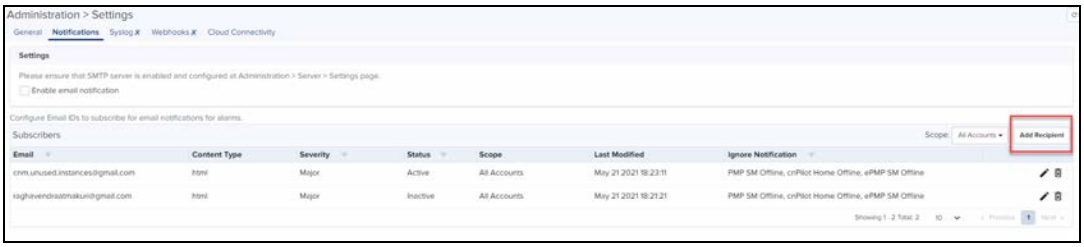
You can use the sorting option for the following fields:

- Content Type
- Last Modified Date

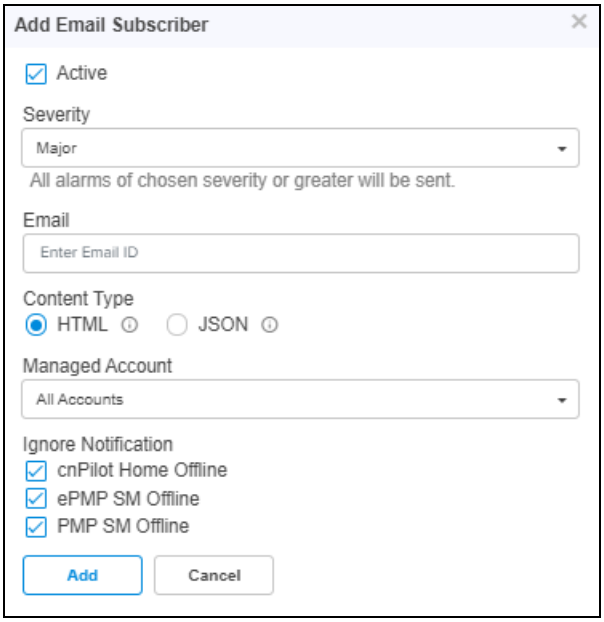
Adding Recipient to Subscriber Table

1. Navigate to **Administration > Settings > Notifications** and click **Add Recipient**.

Figure 169 Adding Subscribers



The following window is displayed:



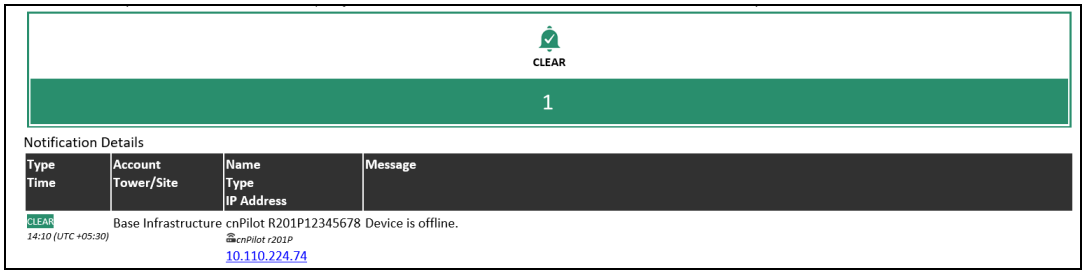
> **NOTE:**
> Managed Account option will appear only if MSP feature is enabled.

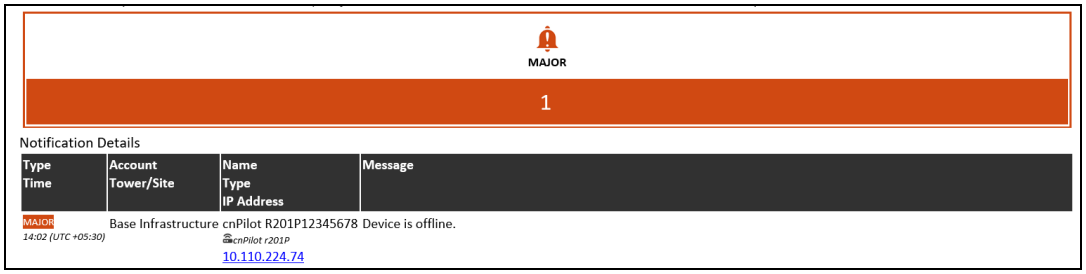
2. Select the **Severity** level.
3. Enter **Email**.
4. Select the **Content Type** as **HTML** or **JSON** .
5. Select the **Managed Account** list.
6. Select the appropriate option (s) for **Ignore Notification.**
7. Click **Add**.

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





JSON Email Example

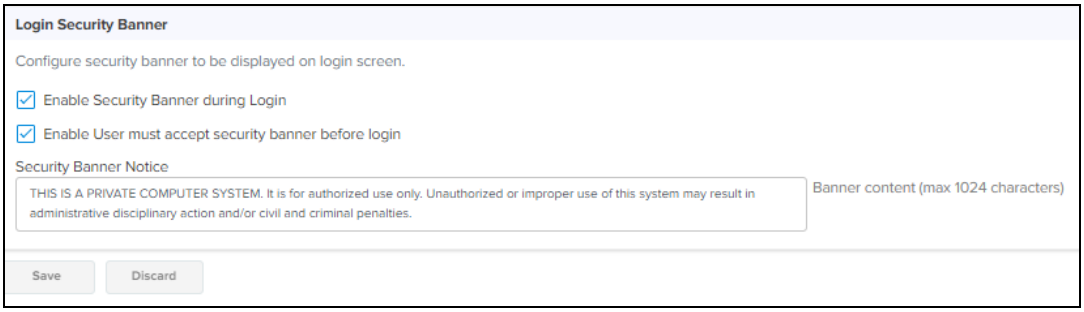
Login Security Banner

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**.

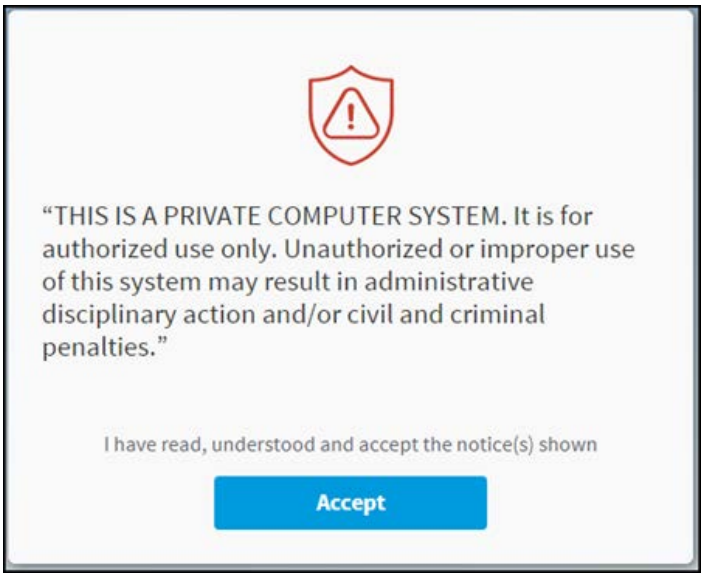
Figure 170 Enabling Security Banner



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 171 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-premise instance will have only current month data. It is suggested to take backup at the last day of the month if needed. Please refer to Data Backup for more info.

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.

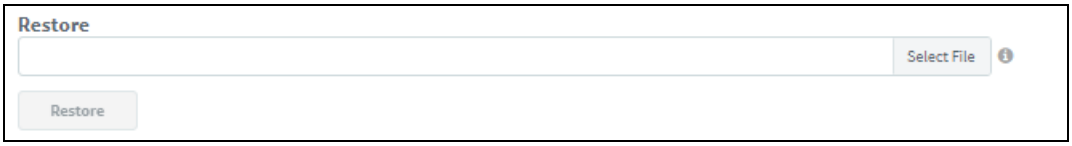
> **NOTE:**
>
> Only the latest backup is retained in the disk and available to download. The old backup is deleted once the new backup is generated.

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**.

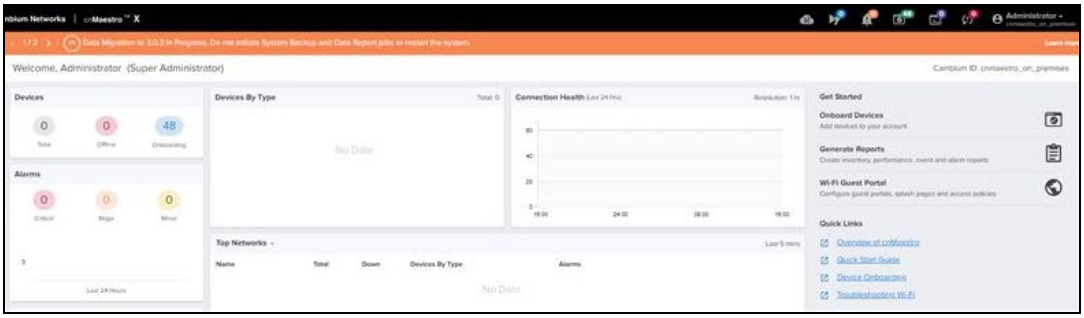
Restore Backup

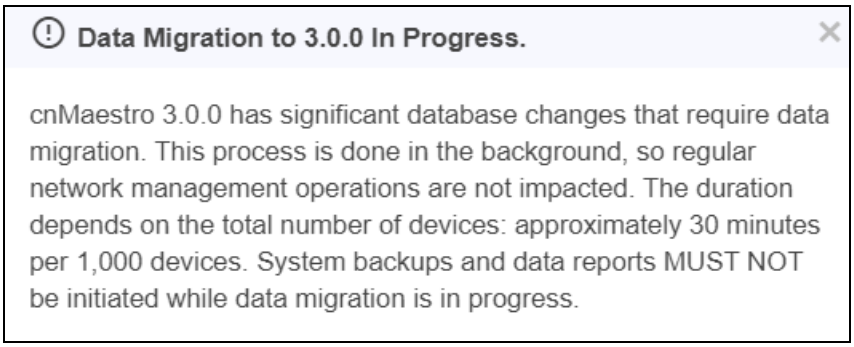
The user can now restore the downloaded system backup file to the new cnMaestro instance to recreate the application state under **Manage** > **Server** > **Operations** > **System Backup and Restore**.



To restore backup files, select the file from **Restore From Backup** option and click **Restore**.

Data migration to 3.0.3 from lower version takes some amount of time depending upon the size of backup file. During migration, the below banner is displayed:





In 3.0.3 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.

NOTE:

- 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

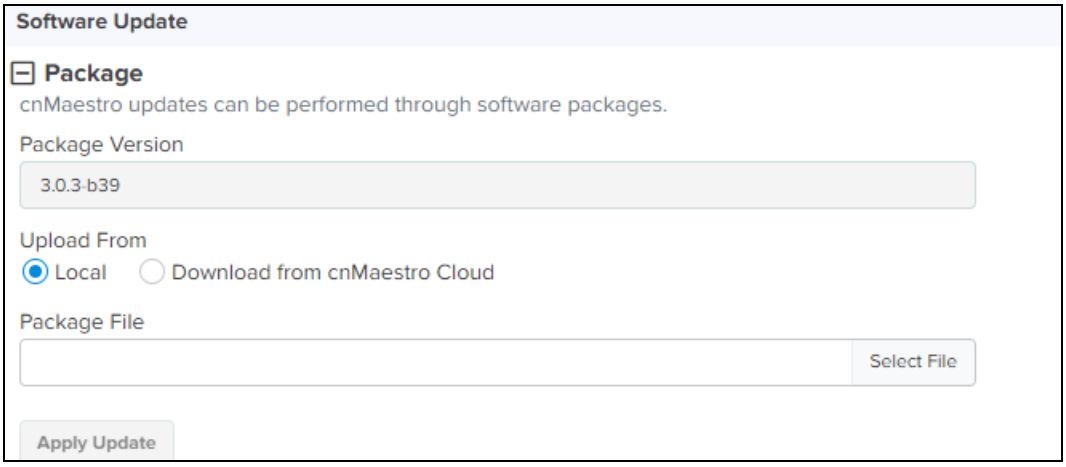
The basic UI allows the user to upload a new OVA, and install it. This process is used for both standalone and HA installations. The Software Upgrade can be done through OVA or package.

Package Upgrade

1. Navigate to **Administration > Server > Operations > Software Update**.

2. Click **Package**.
3. Browse and select the **cnmaestro-package_2.5.0.tar.gz** file.
4. Click **Apply Update.**

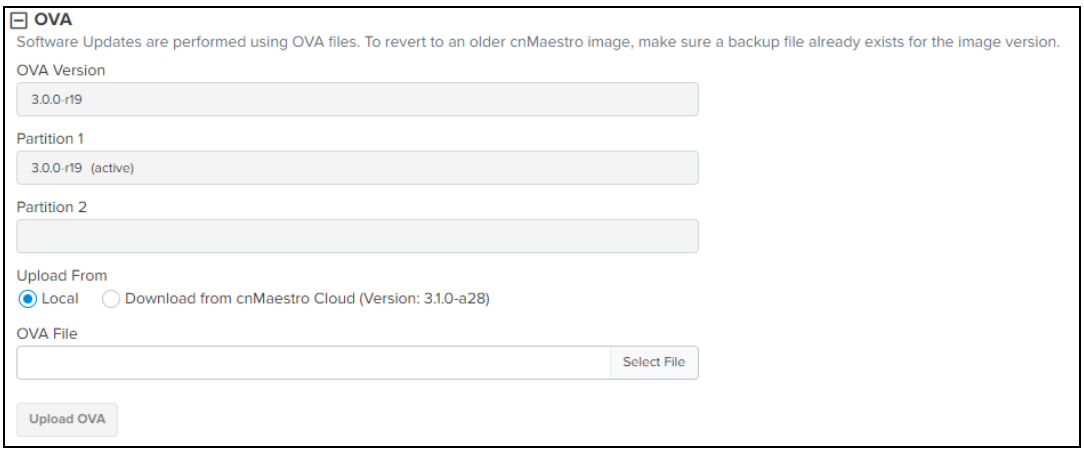
Figure 172 Package Upgrade



OVA Upgrade

> **NOTE:**
> Ensure to have minimum of 1 GB free RAM in the cnMaestro On-Premises server for the OVA to upgrade successfully.

1. Click **OVA**.
2. Select the “cnmaestro-on-premises_3.0.0-b30_amd64.ova” file.
3. Click **Upload OVA**. After upload it will progress with Staging.



4. Click **Apply** to upgrade to higher version.

OVA Upgrade Using CLI

1. Copy the OVA file into the location “/srv/storage/tmp”
2. Execute the command **sudo /srv/bin/sudo cnmaestro-image stage /srv/storage/tmp/<OVA file name>**
3. Staging Status can be verified in UI under **Server** > **Operation** > **OVA**.

In the CLI, it can be verified by executing the command sudo /srv/bin/cnmaestro-image status

If you are unable to apply the upgrade OVA using the UI, there is a command line mechanism that can be used as a failsafe. See **Appendix > Maintenance > Command Line Alternatives > Apply OVA Upgrade** for more details.

Diagnostics

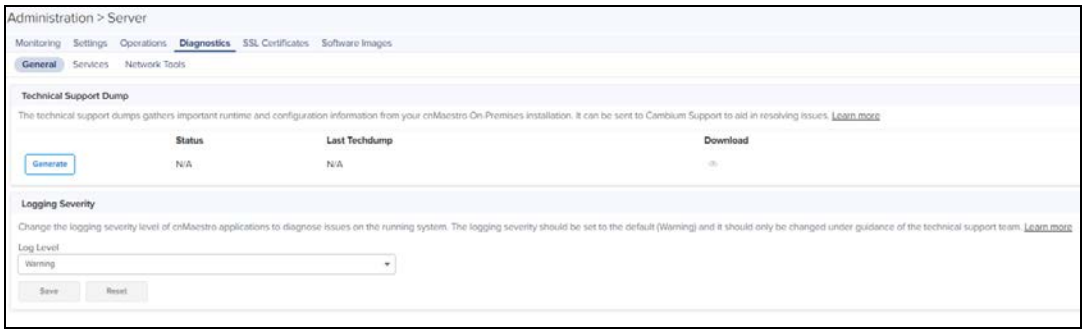
This section provides the following details:

- Server Technical Support Dump
- Logging Severity
- Services

Server Technical Support Dump

The technical support dump gathers important runtime information on the cnMaestro instance. It is accessed at **Administration > Server > Diagnostics** and can be used by Cambium Networks Support to aid in resolving issues.

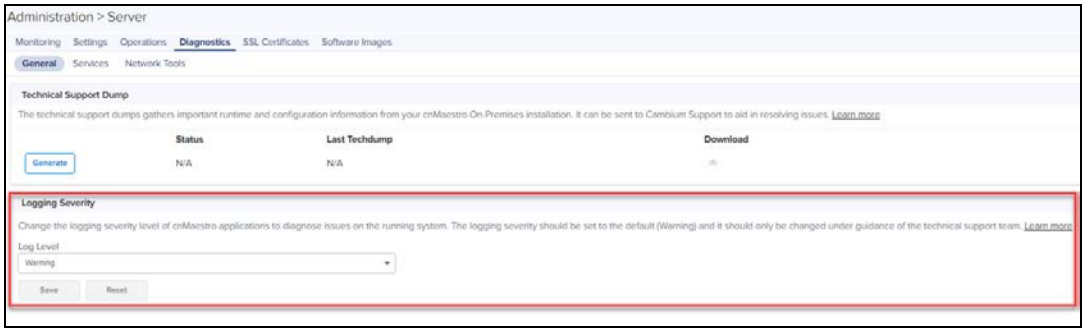
Figure 173 Technical Support Dump



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 174 Logging Level



Services

Real time display of the status of critical cnMaestro services.

Figure 175 Services

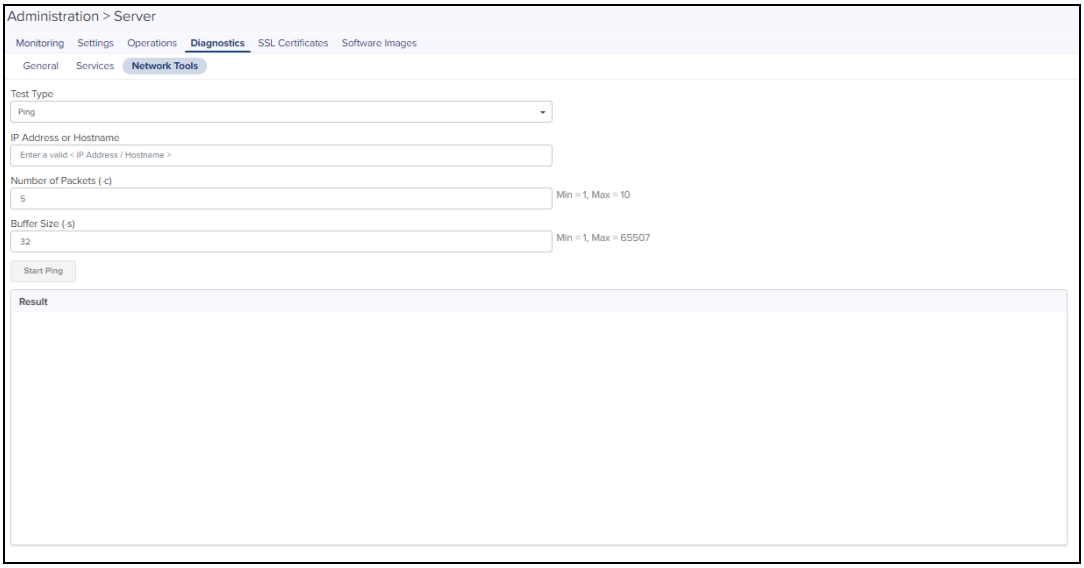
Network Tools

The Network Tools page consolidates a number of operations that can be performed on cnMaestro On-Premises. The operations are listed below:

Table 50: 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.

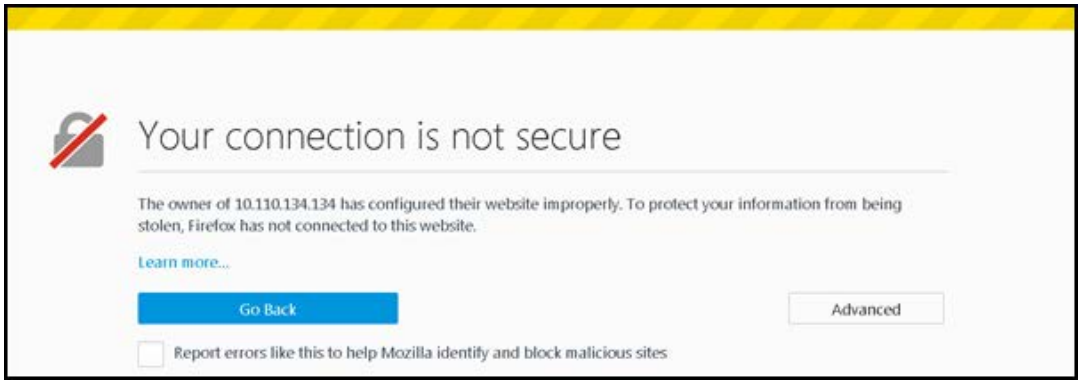
Figure 176 Network Tools



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 177 SSL Error Message



Certificate Management

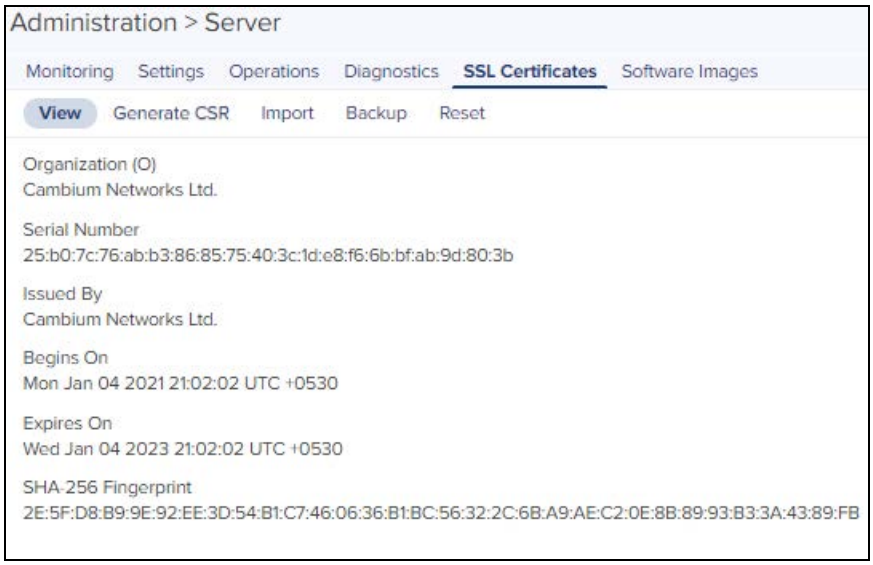
To fix the browser error, cnMaestro needs to host a certificate from a trusted certificate authority, and map the FQDN (fully qualified domain name) used to access cnMaestro. This requires the administrator to export a CSR (Certificate Signing Request) and import the signed Certificate back into cnMaestro.

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.



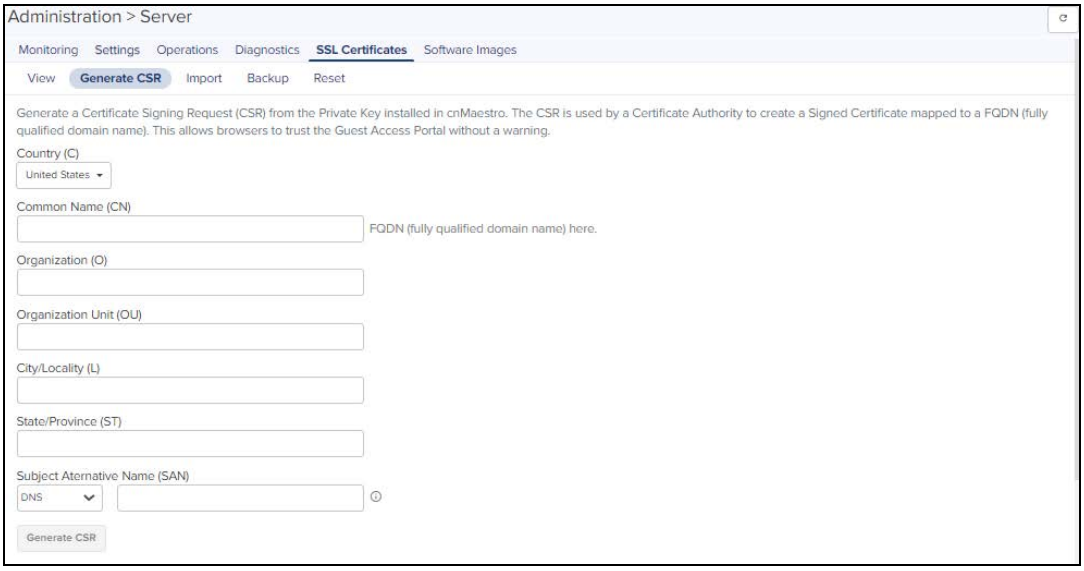
Generate a Certificate Signing Request (CSR)

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.



3. Specify the parameters as in the below table:

Table 51: 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.

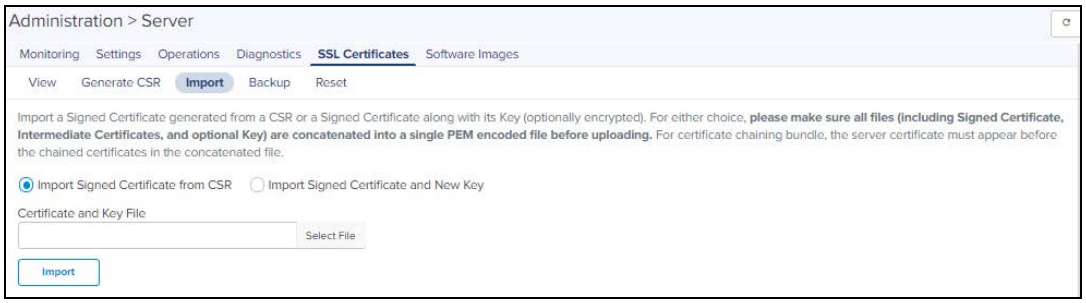
4. Click **Generate CSR**., the user is prompted to save a cnMaestro .csr file to their hard drive. The CSR can then be sent to a Certificate Authority and signed.

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.



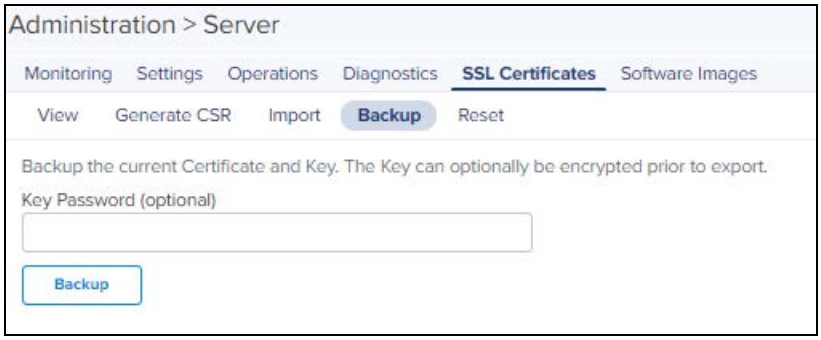
2. Select any one of the below options:
   a. Import signed Certificate from CSR
   b. Import signed Certificate and new Key
3. Browse and upload the Certificate and Key file.
4. Click **Import**.

	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.



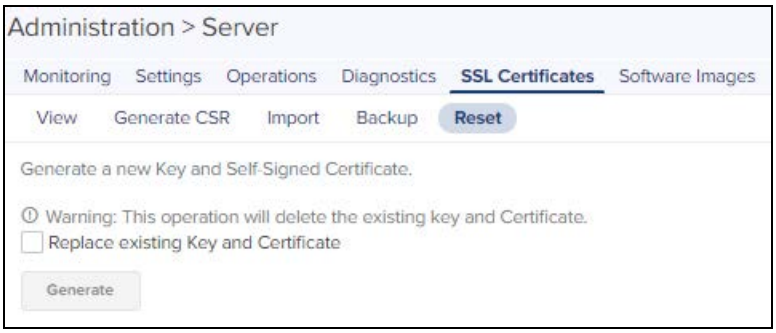
2. Enter the password for the key in the Key **Password** texbox.
3. Click **Backup**.

Reset

It replaces the current Private Key and Certificate and recreates them from scratch. The Certificate is self-signed, and it can be replaced using the Certificate import mechanism detailed above.

To generate a new private key:

1. Click **Reset** tab.



2. Select the **Replace the existing Key and Certificate** checkbox.
3. Click **Generate**.

Manage Software Images

This section provides the following details:

- Overview
- Automatically Update Device Software

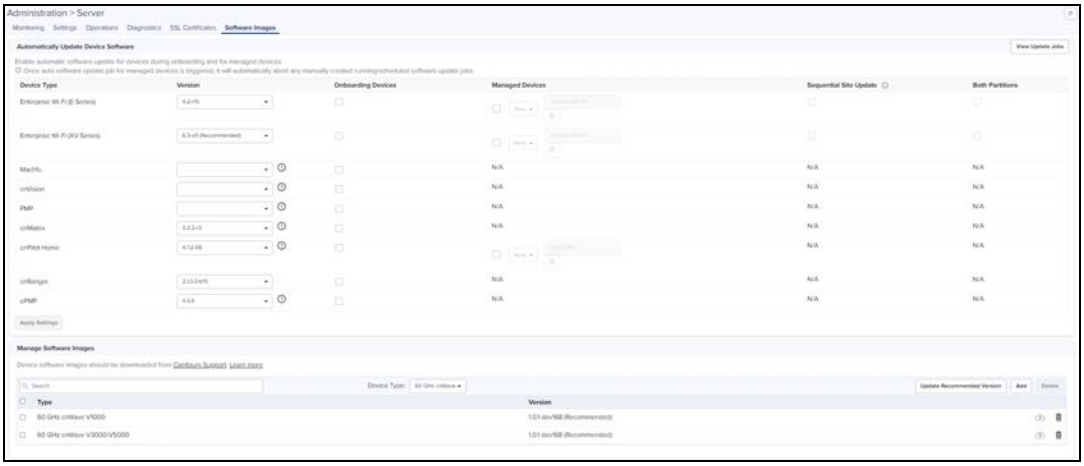
Overview

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:

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 **Import Software** button.
4. Once file is successfully uploaded to the server, it will appear in the grid.

Figure 178 Managing Device Software Images



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.

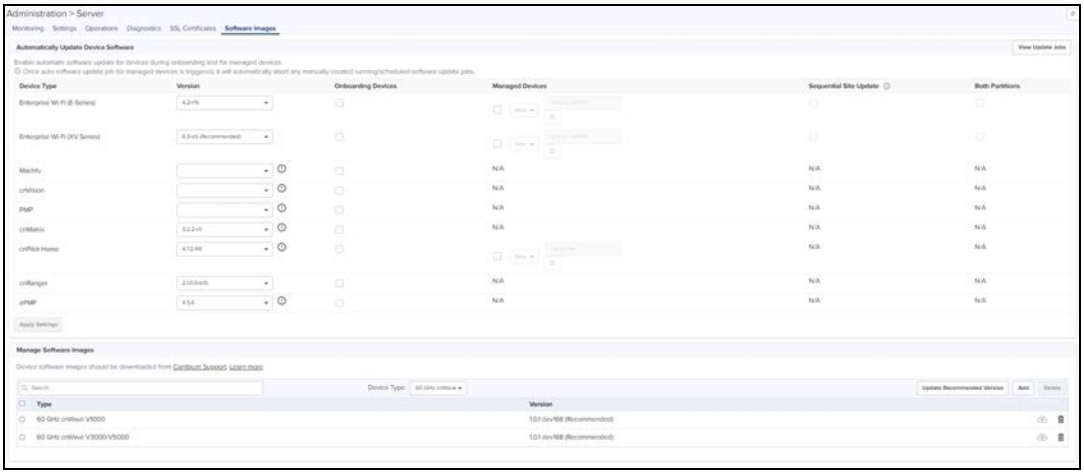
All the check box will be disabled by default.

Add Images

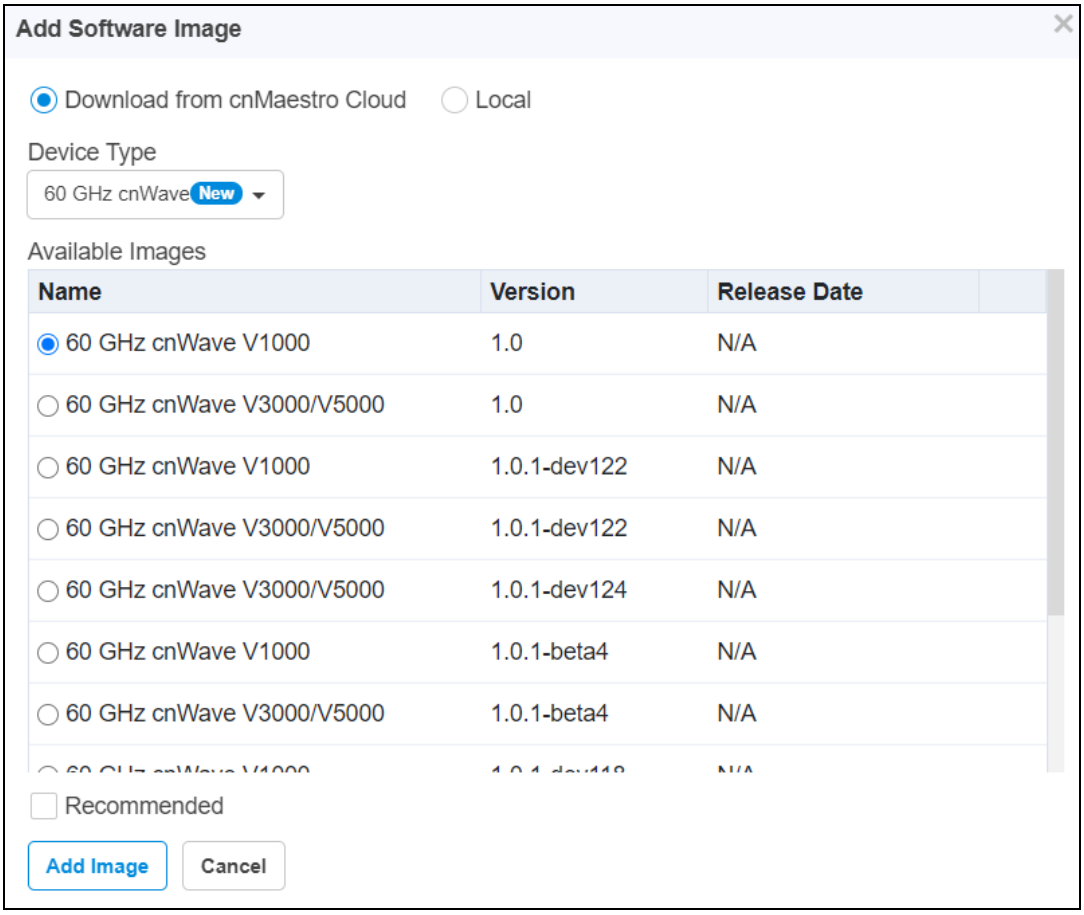
Once the On-Premises server is synced with the cloud, the user can upload the software images from cloud directly to the On-Premises.

To upload Software Image perform as follows:

1. Navigate to **Administration > Server > Software Images.**



2. Click **Add Image.**
3. Click **Download from cnMaestro Cloud** and select **Device Type**.

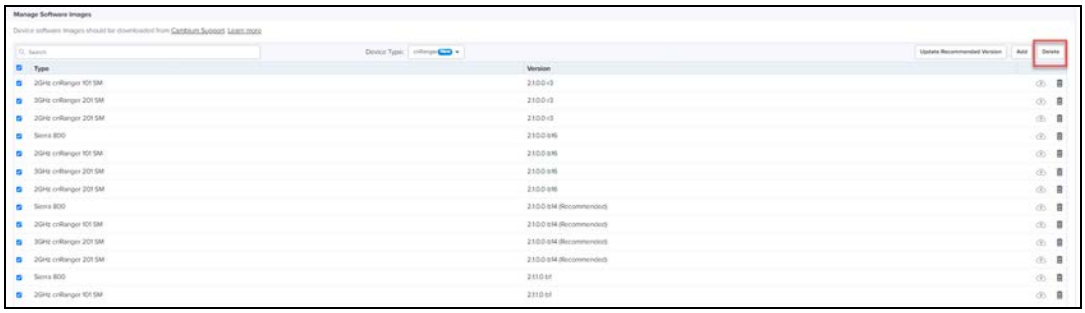


4. Select the Version and click **Add Image.**

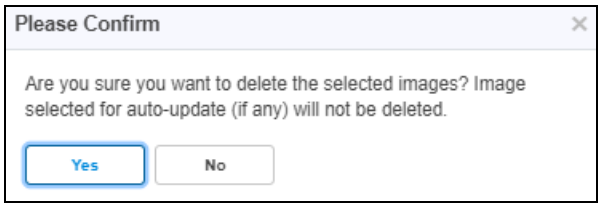
Delete Images

To delete Software Image perform as follows:

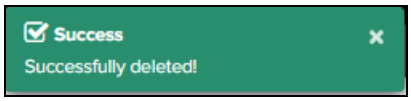
1. Navigate to **Administration > Server > Software Images.**



2. Select the images to be deleted and Click **Delete.**
3. Click **Yes** in Please confirm window to delete the images.



4. It will display the Success message as shown below:

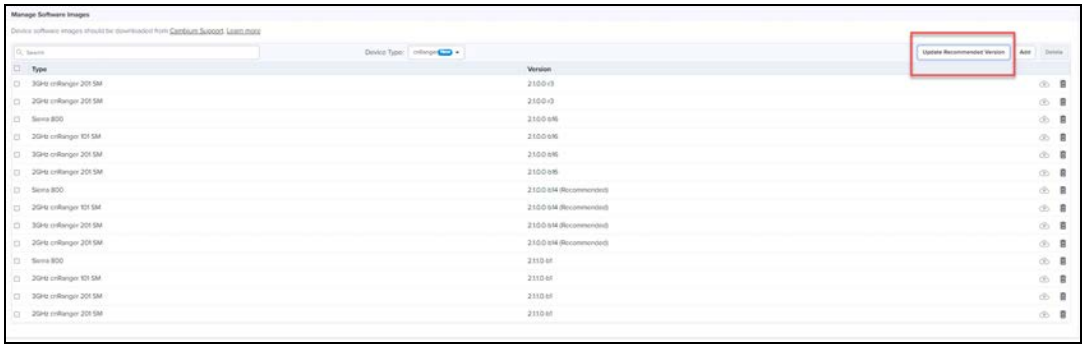


Update Recommended Version

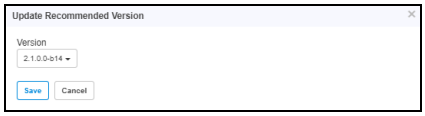
Update recommended version allows the user to update the Version with the recommended version available from the drop-down.

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:

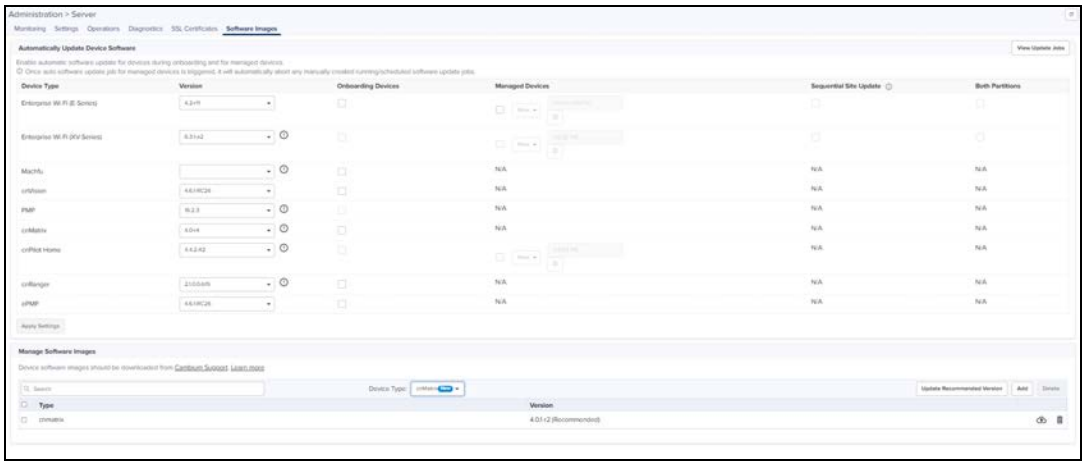
1. Navigate to **Administration > Server > Software Images > Automatically Update Device Software** tab.
2. Select the version file and then click **onboarding/Managed Devices**.

> **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 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 179 Automatically Update Device Software



Webhooks

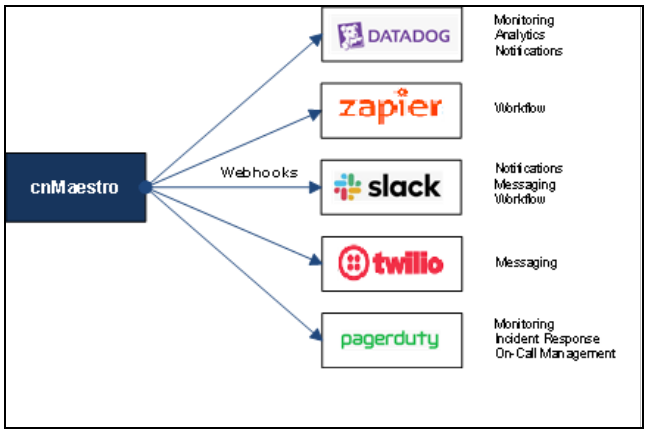
cnMaestro Webhooks provides real-time streaming for alarms using a push notification model. Webhooks data is HTTPS posted to an external Web service. They enable the following benefits:

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 180 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

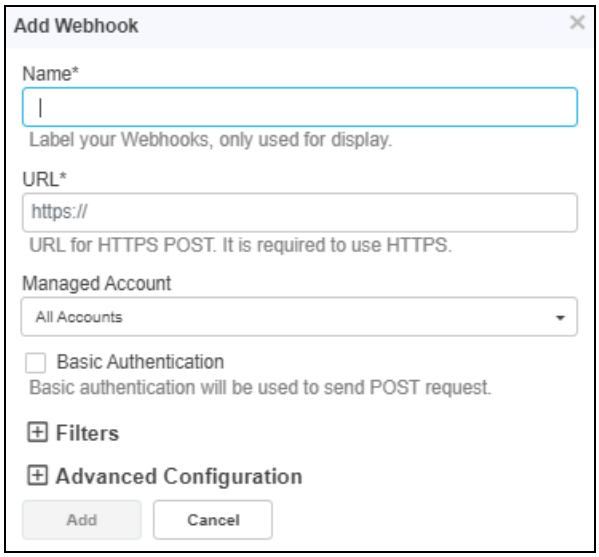
Webhooks are limited to 2 entries per account. In a managed services environment, each managed account can have two Webhooks.

cnMaestro Webhooks Configuration

1. Navigate to **Administration > Settings > Webhook**.

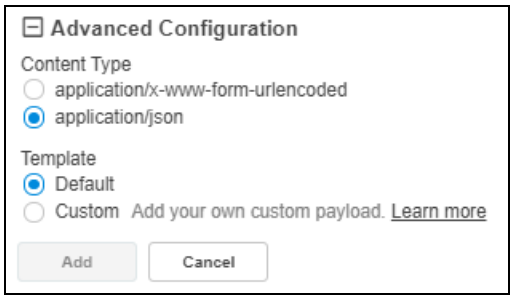
2. Click **Add Webhook**. The following window appears:

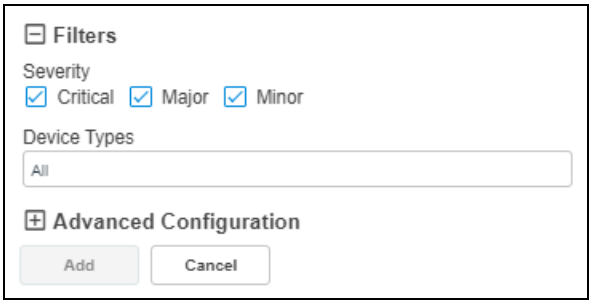
Figure 181 Configure: Add Webhook parameters Page



3. Enter the parameters as shown in the below table.

Table 52: Add Webhook parameters

Parameter	Description
Advanced Configuration - Content type and Template	You can choose content-type as JSON or URL-Encoded Form. 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. The Webhooks JSON payload follows the same format as the cnMaestro RESTful API, with a few additional Webhook-specific variables/keys. 
Basic Authentication	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. Note 1: 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. Note 2: 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)
Filters	You can filter the alarms based on severity such as Minor, Major, or Critical. You can also select multiple severities. Device type allows to select the particular device from the drop-down.

Parameter	Description
	
Managed Account	If cnMaestro is configured for MSP (Managed Service Provider), you can map the Webhooks to a Managed Account. Note A maximum of two Webhooks can be configured per Managed Account.
Name and URL	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.
Type	Type of cnMaestro notification to configure Webhook. Note cnMaestro release 2.4.0 supports only alarms as the type for Webhooks configuration.

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 53: 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 182 Viewing Configured Webhooks

cnMaestro Webhooks Configuration provide details on the parameters displayed:

Table 54: Webhook parameters

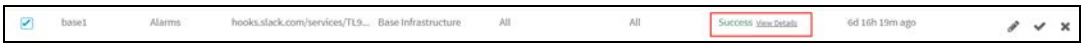
Parameter	Description
Device Type	The Device Type filter on Webhook.
Enable	Select Enable checkbox to enable the Webhook.
Last Status	Last status of Webhook
Last Status Time	Last Webhook send time.
Managed Account	If the MSP Service is enabled, this is the type of account (E.g. All Accounts, Base Infrastructure, 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

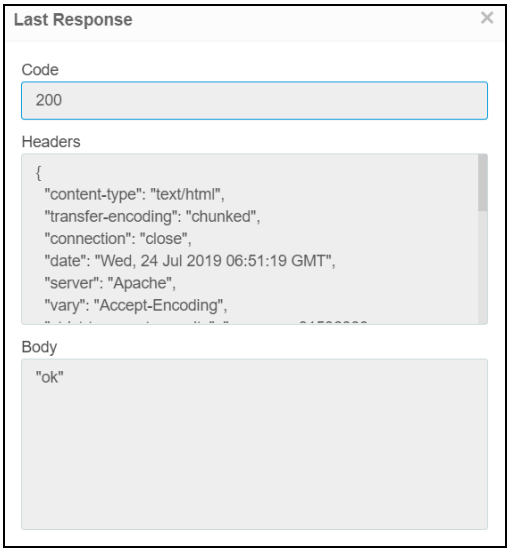
Click **View Details** to check the status of message sent last.

Figure 183 Status check view



View Details displays the response Code, Headers and Body of Webhooks endpoint.

Figure 184 Last response code



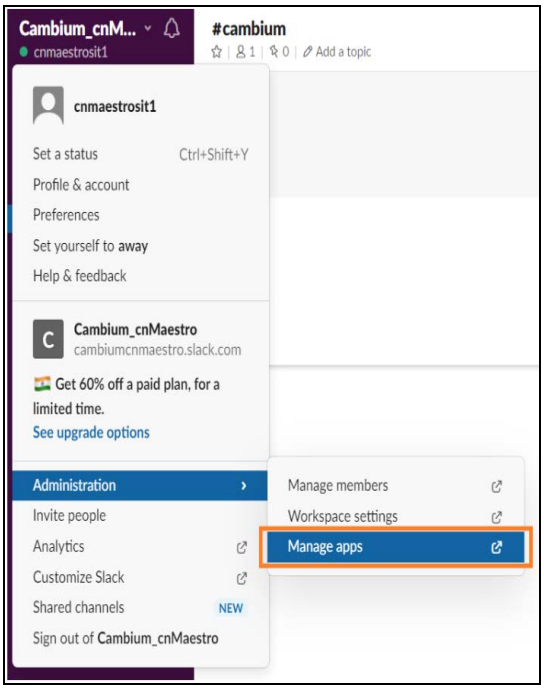
Custom Template Examples

Slack Configuration

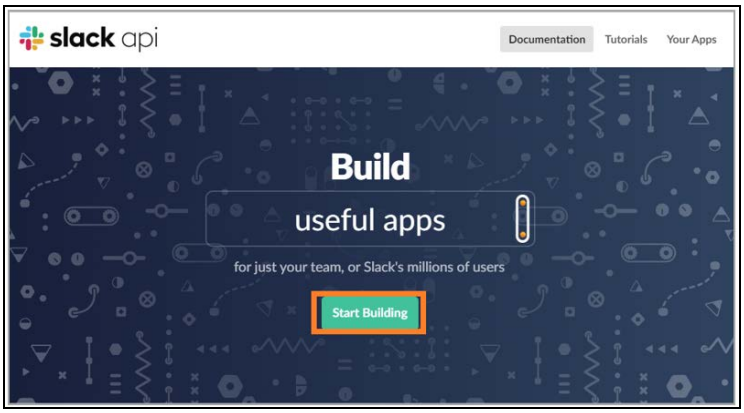
Slack is a platform for team communication, offering instant messaging, document sharing, and knowledge search.

Following is a simple example of configuring Slack integration with cnMaestro Webhooks using a custom Template.

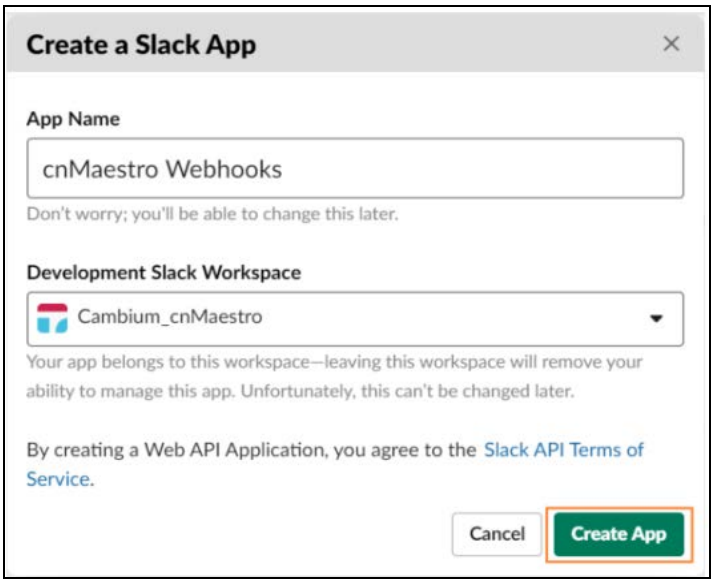
1. On your Slack Screen, click on your workspace name at the top of the left-hand menu and open **Administration** > **Manage** apps.



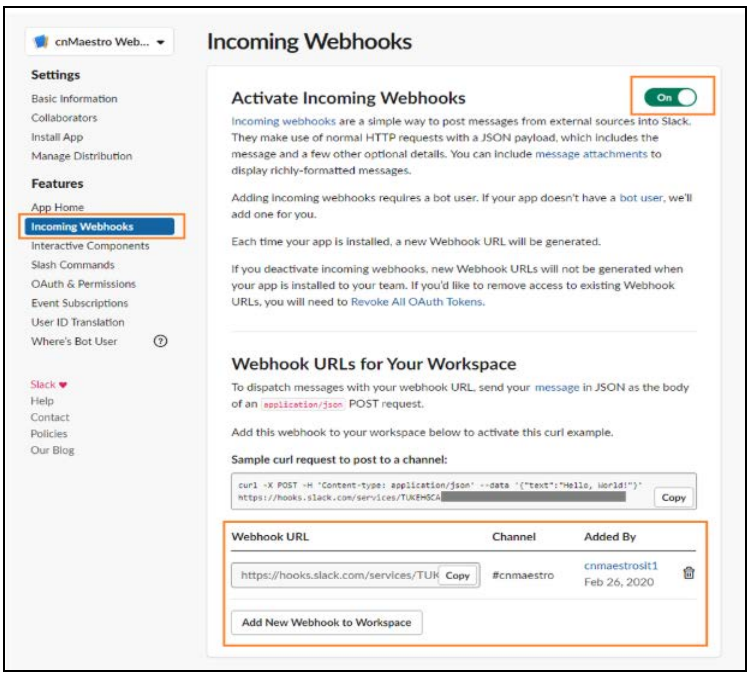
2. In the apps screen, click the Build and then the **Start Building**.



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**.



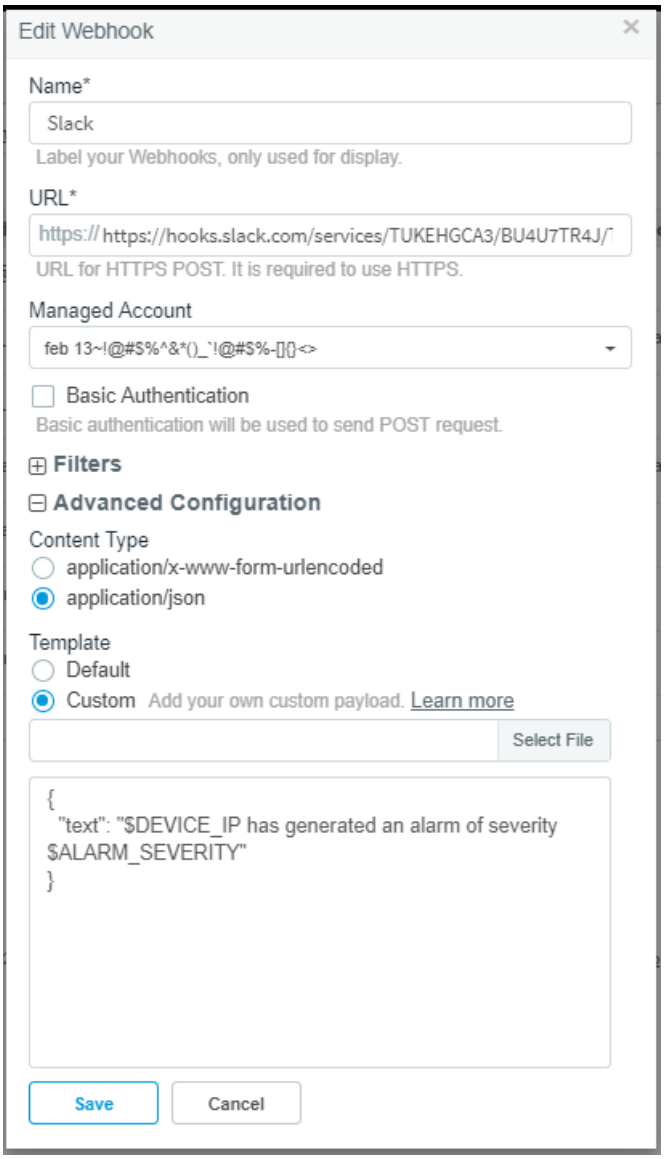
4. In the **Basic Information** tab, select **Incoming Webhooks** from the left menu and create a webhook, providing all the permission and targeted Slack Channel details.



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**.



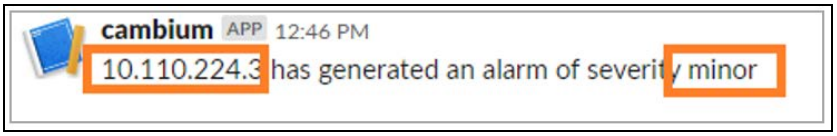
Slack expects a custom JSON payload (https://api.slack.com/incoming-webhooks), The simple one is as follows:

```
{
"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"
}
```

8. Once an alarm occurs, the following message appears in the configured Slack channel. Notice the variables have been replaced with actual values.



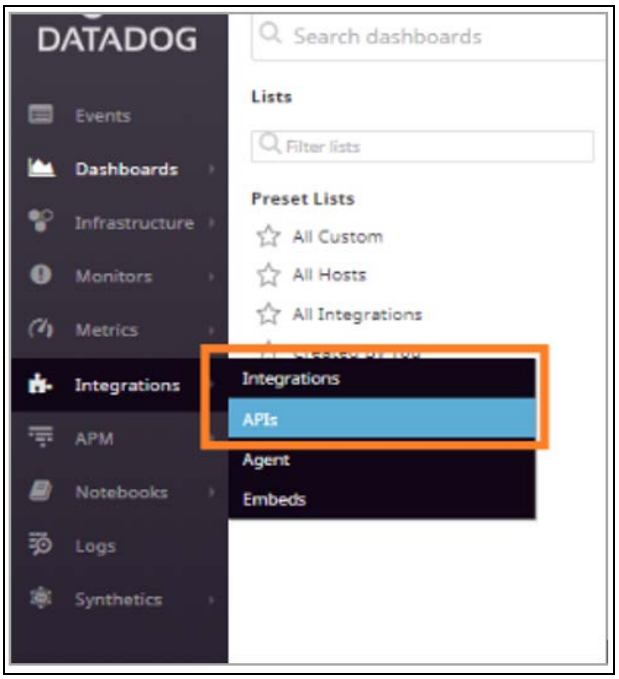
Datadog Configuration

Datadog is a service for IT, Operations and Development teams who write and run applications at scale.

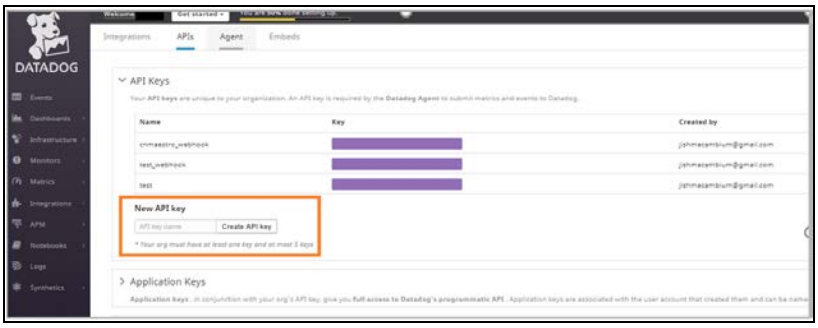
Following is an example of how to create Datadog events using cnMaestro Webhooks and custom templates.

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.

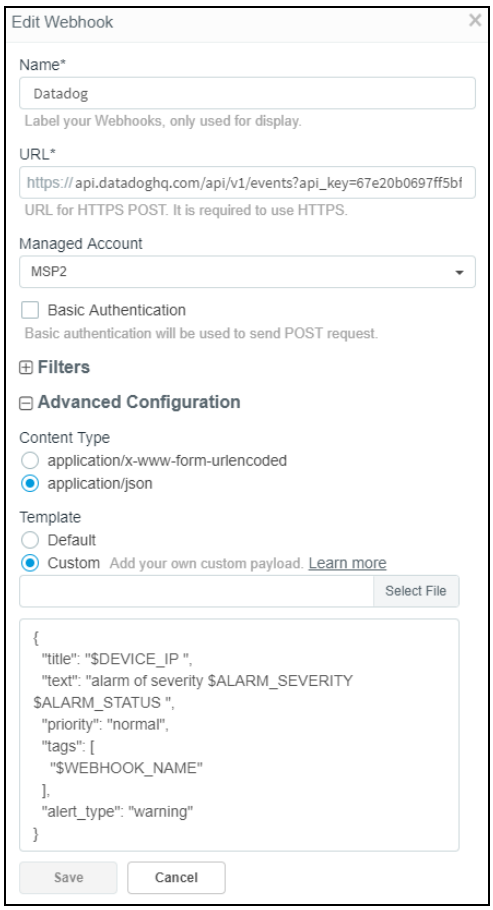
3. Datadog expects a custom JSON payload, following is a simple Datadog specific payload format using cnMaestro Webhook variables.

```
{
"title": "$DEVICE IP",
"text": "Alarm of severity $ALARM_SEVERITY $ALARM_STATUS",
"priority": "normal",
"tags": ["$WEBHOOK_NAME"],
"alert_type": "warning"
}
```

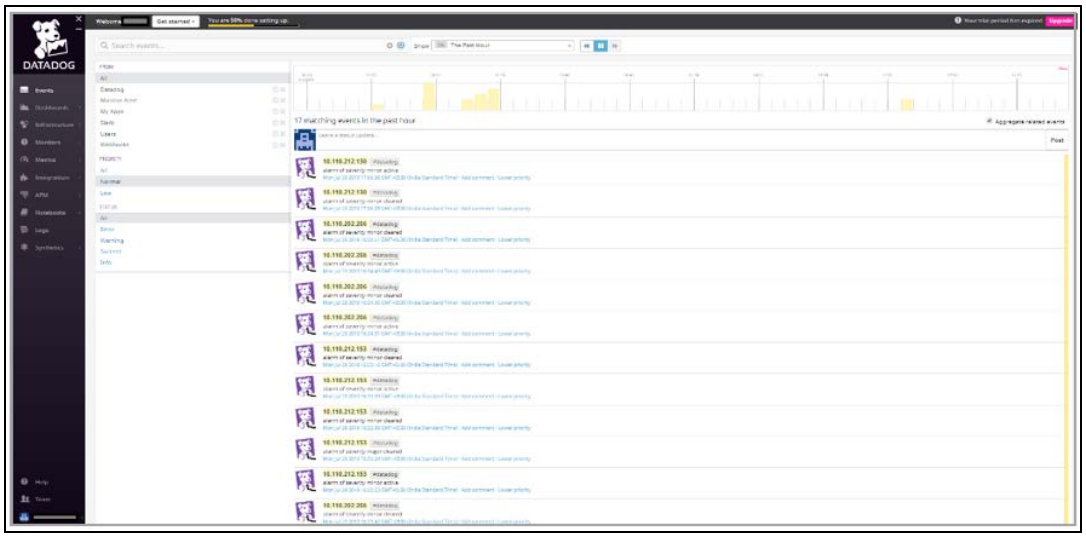
Note

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**.



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.

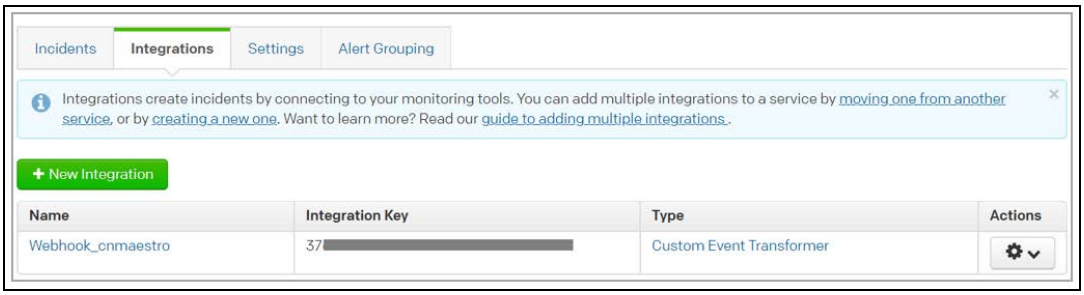
To begin, login to PagerDuty or create a new account.

https://app.pagerduty.com/

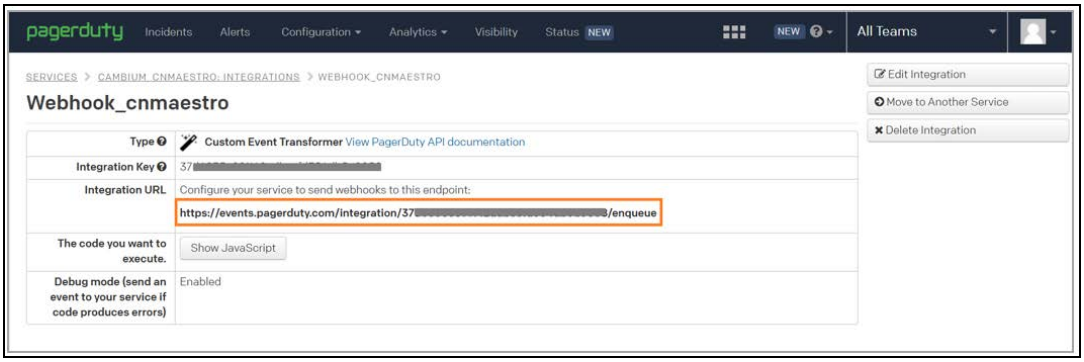
To capture the cnMaestro alarms you need to add a new integration into PagerDuty using a Transformer tool.

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.



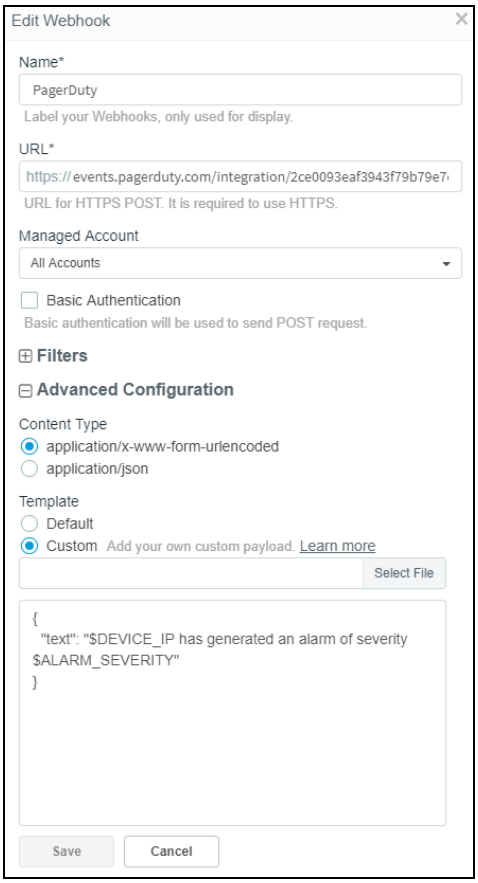
4. Click on the Name of your new integration to view the details.



Integration URL is used in configuration of cnMaestro Webhooks.

https://events.pagerduty.com/integration/<integartion_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”
}
```

Note

Learn more about PagerDuty and different integrations at https://support.pagerduty.com/docs/webhooks.

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

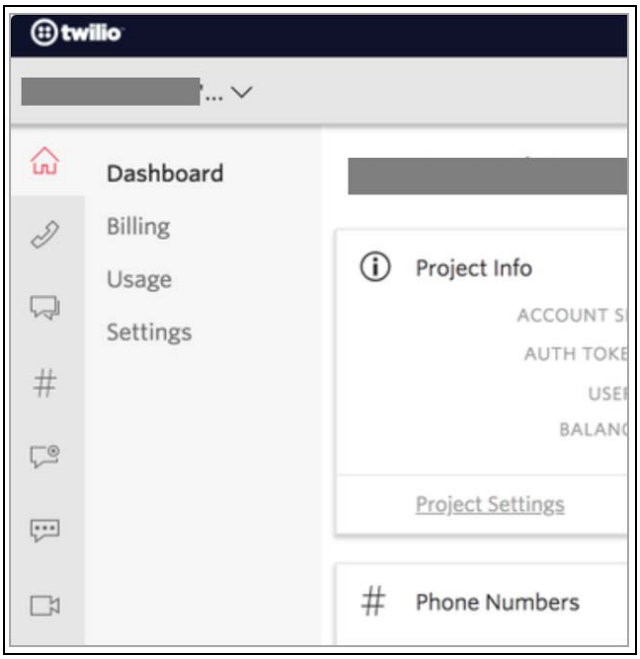
Twilio is a developer platform for communications. Software teams use the Twilio API to add capabilities like voice, video, and messaging to their applications. Twilio is mainly used as an SMS service provider for websites and apps.

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.

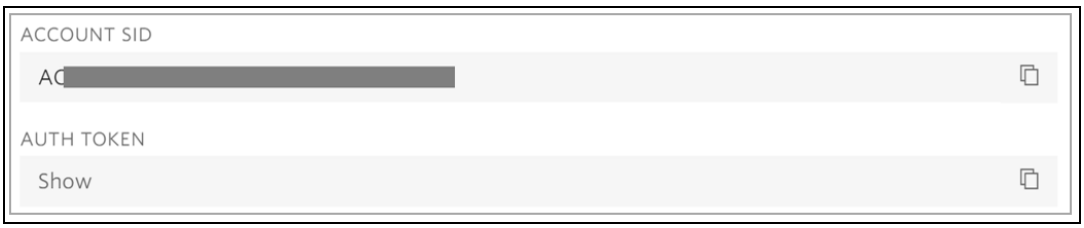
To send a cnMaestro alarm as an SMS directly to a phone, we are going to use the Twilio's API to programmatically send text messages.

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**.

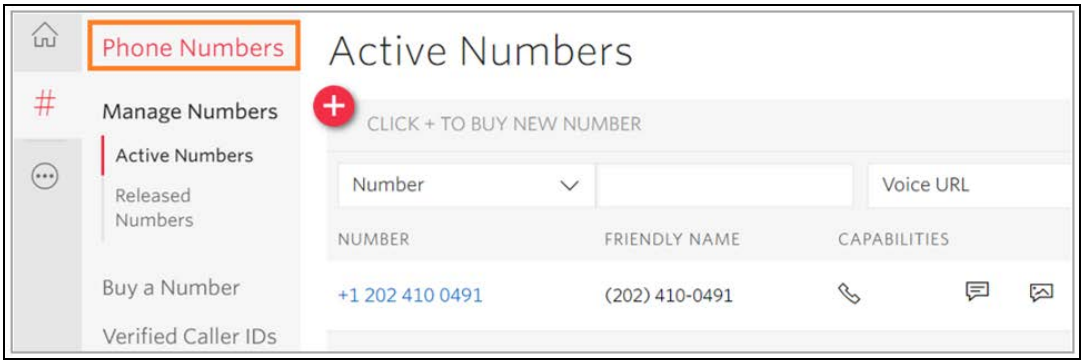


Make a note of the Account SID, Auth Token values on the main twilio.com/user/accountpage – you need it when you configure the cnMaestro Webhooks with Basic Authentication username and password.

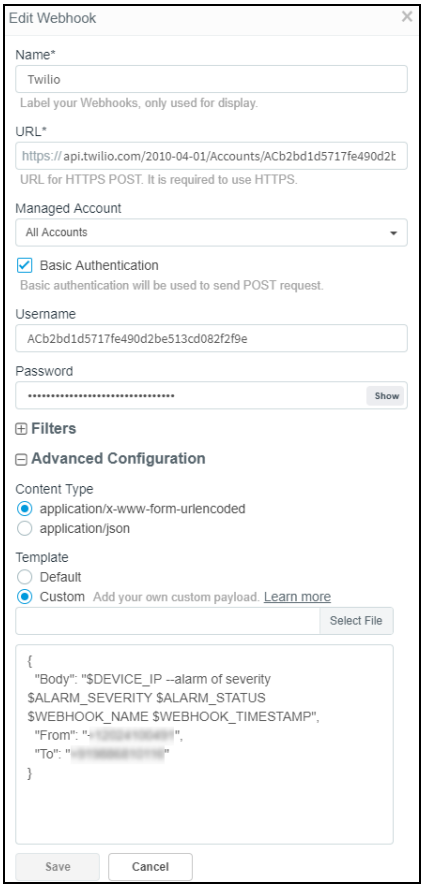
3. Add the **Account SID** to Add the Account SID to https://api.twilio.com/2010-04-01/Accounts/ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/Messages.json, this URL will be used as cnMaestro Webhook URL.



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.

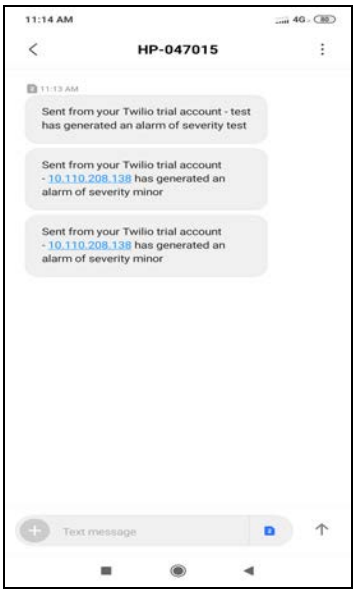
```
{
"Body": "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY",
"From": "+12024100491",
"To": "+91**********"
}
```

NOTE

To configure Twilio to cnMaestro Webhooks you should use application/x-www-form-urlencoded as content type.

Learn more about Twilio and expected JSON format at https://www.twilio.com/docs/usage/api

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.

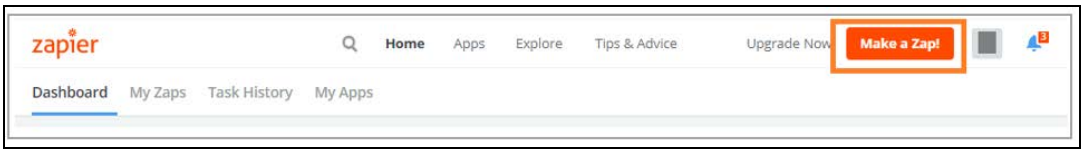
With Zapier you can build Zaps that perform your automation for you. These automations are achieved by mixing a Trigger with actions available on your favourite apps. Zapier supports hundreds of apps. You can mix and match triggers and actions to automate.

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.

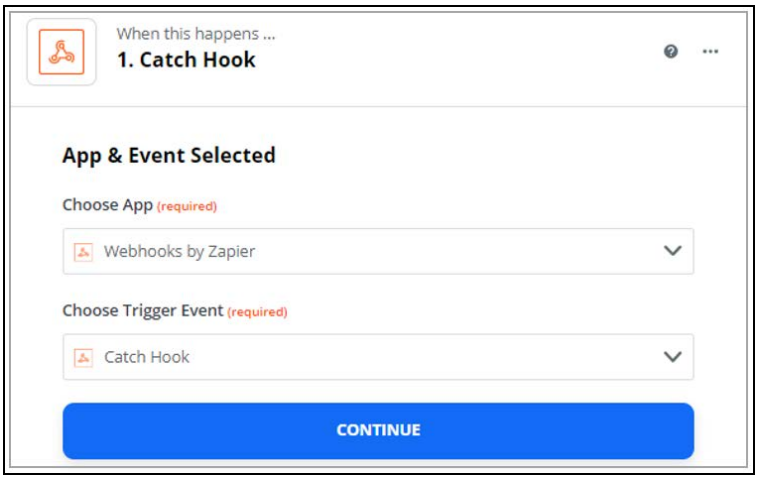
First, Login to Zapier or create a new account.

/https://zapier.com/

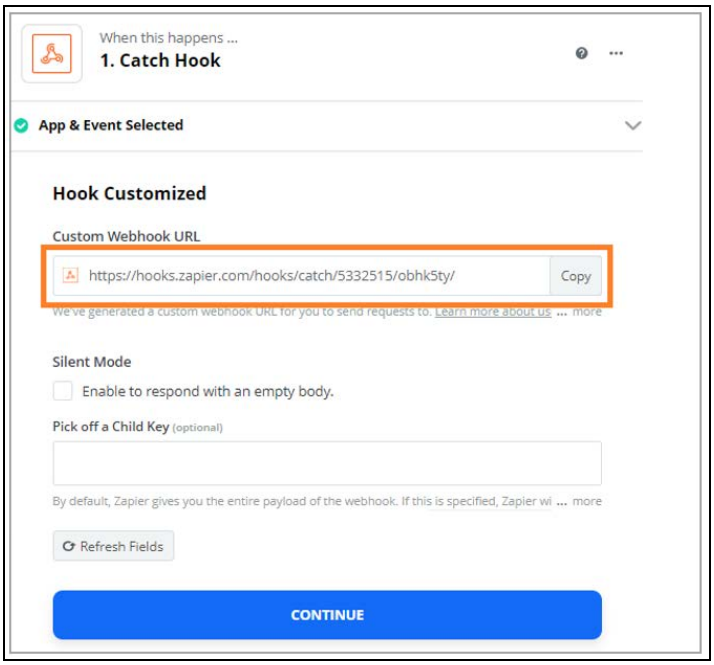
1. After login to your Zapier account, navigate to dashboard.
2. On your Zapier dashboard, click on **Make a Zap** at the top right-hand side.



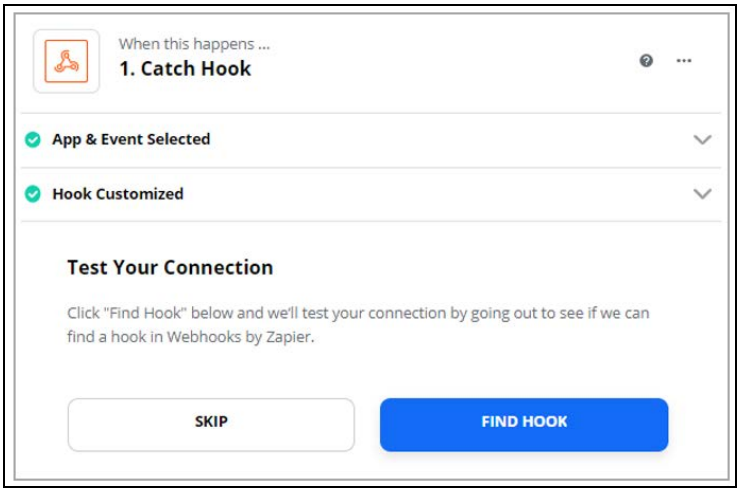
3. Choose **Webhooks by Zapier** and **Catch Hook** as the trigger app and trigger event.



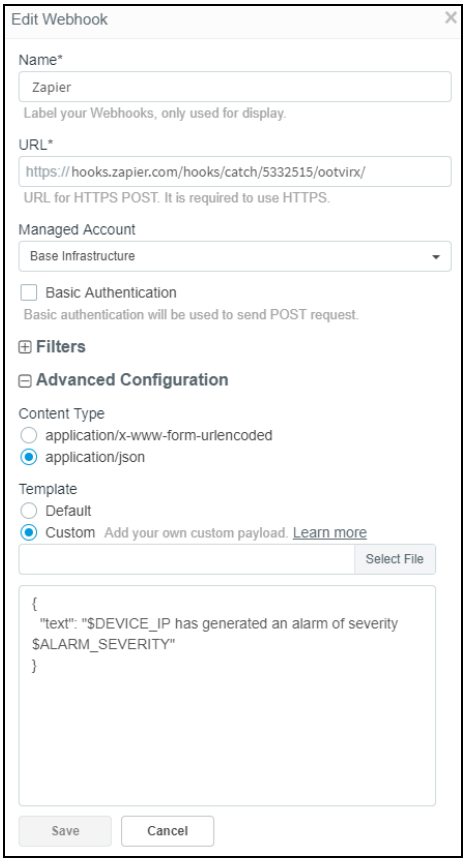
4. To customize your webhook trigger, copy the given URL and configure it in your cnMaestro Webhook.



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**.

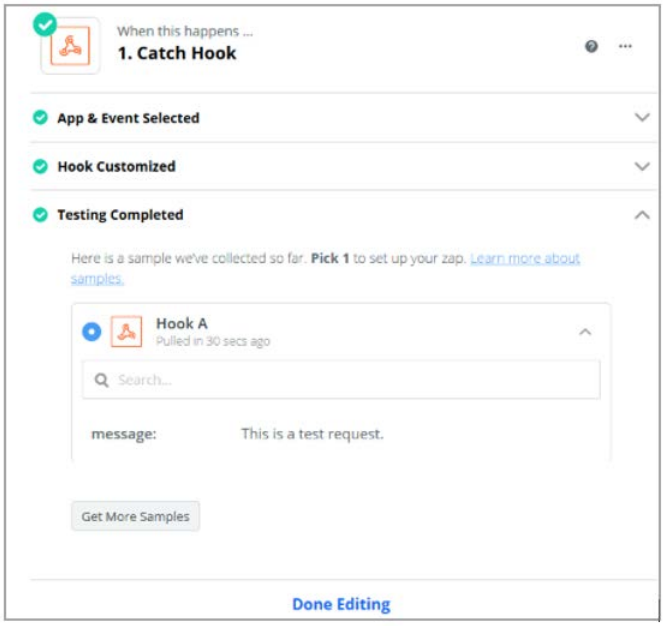


You can use the custom payload or default option in cnMaestro. For this example, we are using the following custom template with variables $DEVICE_IP and $ALARM_SEVERITY in the formatted message.

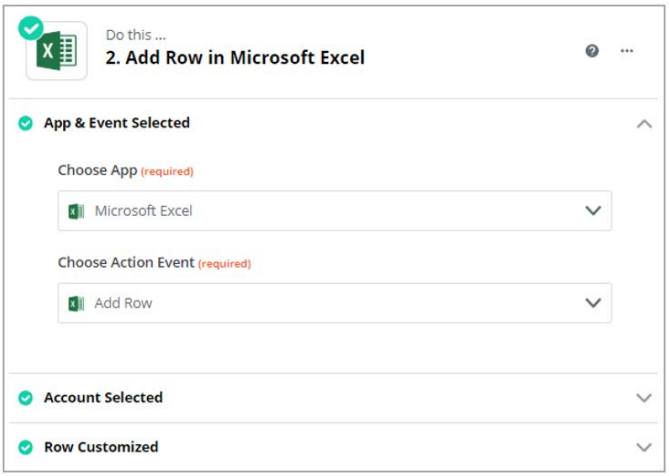
```
{
"text" : "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY”
}
```

7. Send a test webhook by clicking on the test icon on the right-hand side of the webhook table.

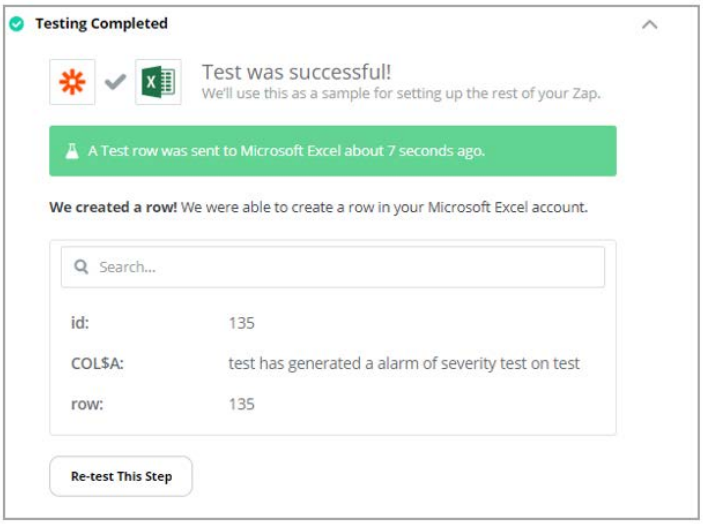
8. Now go back to Zapier and click **Find Hook** to complete the testing.



9. Set up Microsoft Excel as the action for your Zap, action event, connect your excel account and customize.



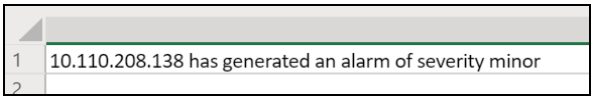
10. To check if your action works as expected. Click **Send Test** to run the action step. The next screen shows whether Zapier has been able to successfully perform the action step or not.



Note

Learn more about how Zapier supports different apps at https://zapier.com/help/.

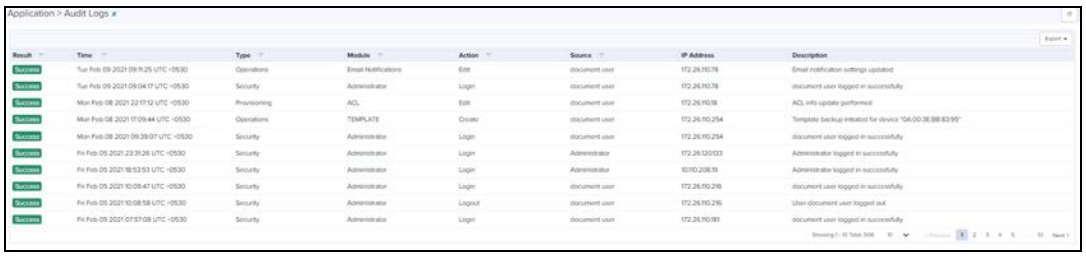
11. Once an Alarm occurs, the following message appears in the configured excel sheet. Notice the variables replaces with actual values.



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 **Administartion** > **Audit Logs** page.

Figure 185 Audit Logs



The following table describes the Audit Logs parameters and their descriptions.

Table 55: 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 56: Log Action Parameters

Parameter	Description
Claim	Claim a device in the network operator.
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
CBRS	Services	CBRS
data-tunnel	provisioning	Data Tunneling

Module	Type (s)	Description
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 **Administartion > 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 186 Syslog

The following table describes the parameters in Syslog server:

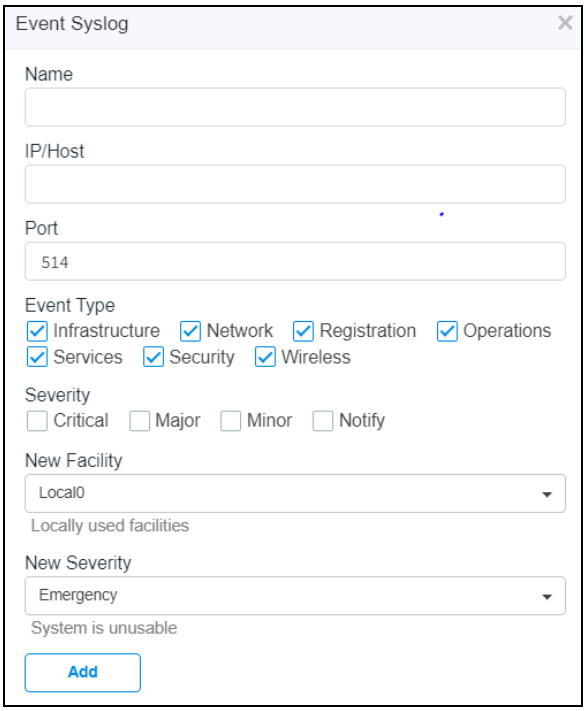
Table 57: Syslog Server Parameters

Field	Description
☑	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 pops-up.



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.

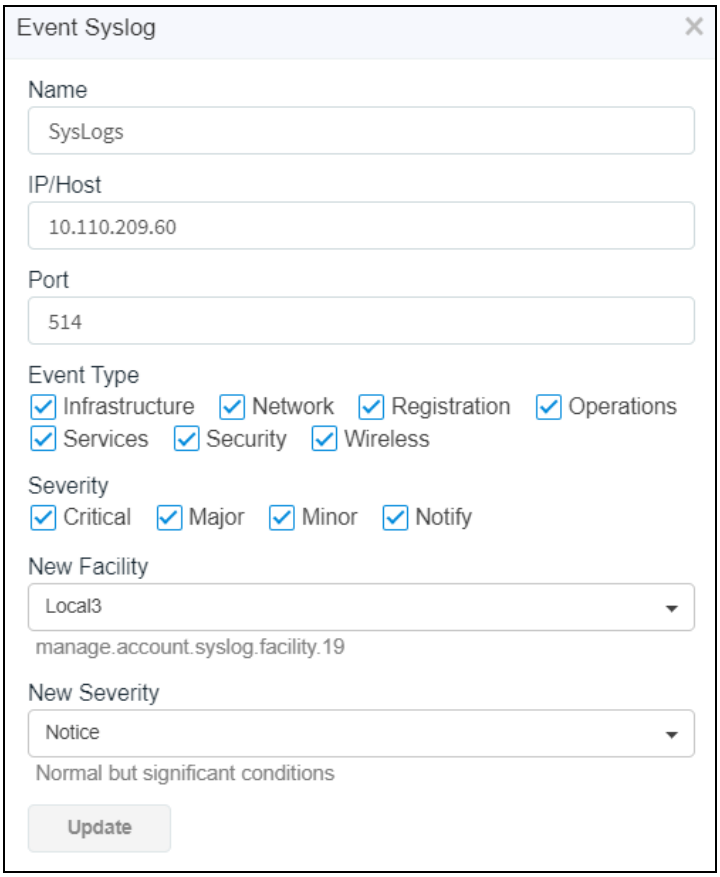
Facility	Description
Local 0-Local 7	It is the locally used facilities.

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.

Value	Severity	Description
3	Error	Error conditions
4	Warning	Warning conditions.
5	Notice	Normal but significant conditions. Conditions that are not error conditions but may require special handling.
6	Informational	Informational messages.
7	Debug	Debug-level-messages.

8. Click to edit the Event Syslog. The dialog box appears:

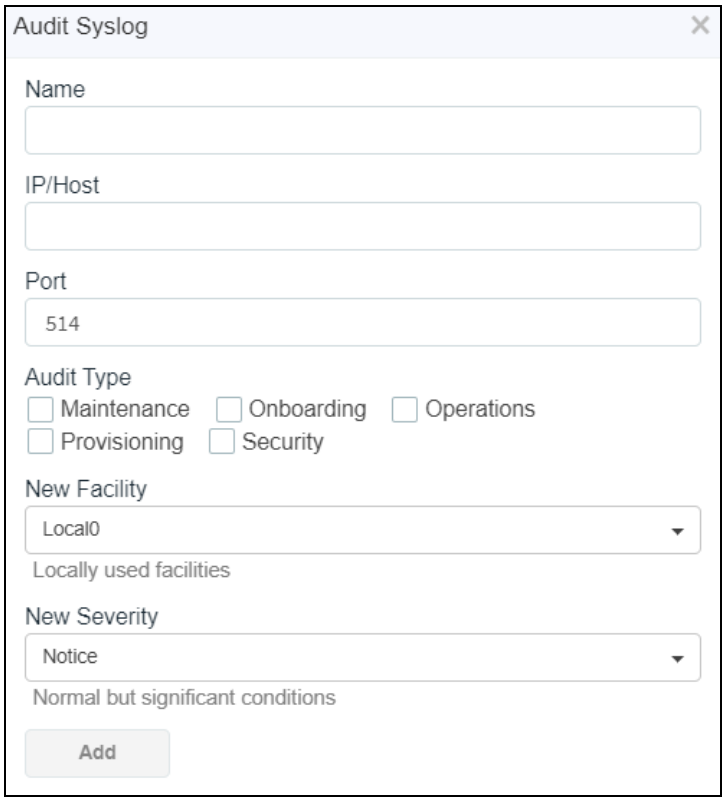


9. Repeat the above steps to update an existing Notification Syslog.

Audit Syslog

The Audit Syslog separates messages based upon Audit Type.

Click Add a new Audit Syslog window pops-up.



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

Starting in cnMaestro 3.0.0, On-Premises installations will be associated with a **Cloud Anchor** account. The Anchor account is a new type of cnMaestro account which is only mapped to On-Premises instances. A single Anchor account can support many independent On-Premises instances.

Cloud Connectivity reports the following details of On-Premises instances in the corresponding Anchor account:

- System level details of each On-Premises instance like Disk, Processor, RAM, Uptime, and Vendor (VMWare VM, KVM, and Oracle Virtual Box).
- Total managed devices, device type distribution and count, On-Premises software version (OVA and Package), user type distribution and count, Account type (Backhaul, Enterprise, and Industrial Internet), and Country.
- On-Premises features enabled like Auto Provisioning, Auto Upgrade, CBRS, MSP, Lock Wi-Fi AP/cnMatrix Configuration, SNMP, and Wi-Fi.

The Cloud Anchor account automatically pushes announcements of new device firmware and cnMaestro software images to connected On-Premises instances.

In the future, Cloud connectivity will be used to manage **cnMaestro X** subscriptions for On-Premises instances. It will also be extended to simplify the CBRS provisioning and billing by tying multiple On-Premises instances to a single Cloud account.

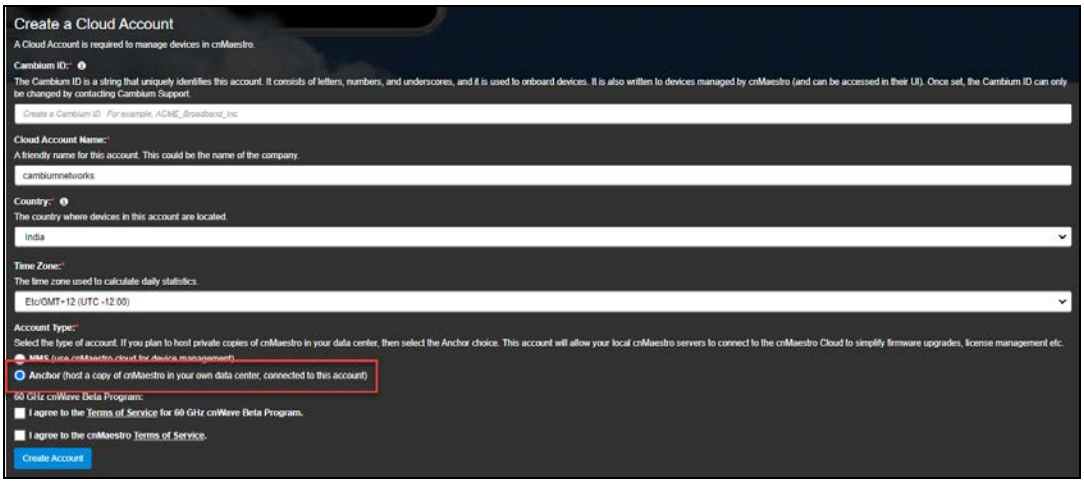
Creation of Cloud Anchor Account

The Cloud Anchor Account is created in the same way one creates a standard Cloud NMS Account. A new Type option is added allowing one to choose between NMS and Anchor.

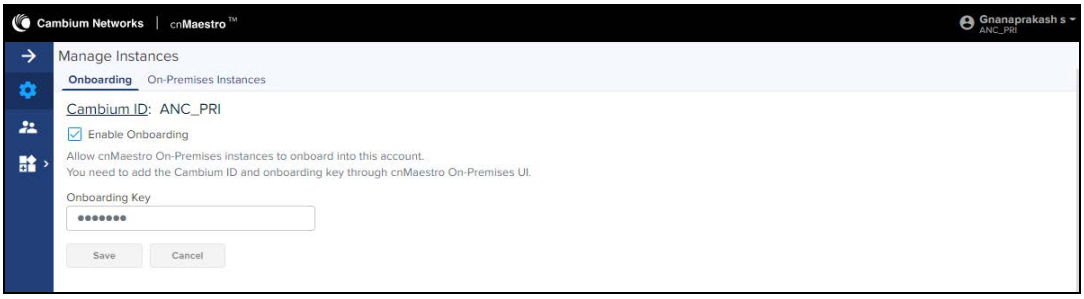
A Cloud Anchor Account should be created before installing cnMaestro On-Premises as shown below:

1. Navigate to the account page and click **Create Account**.

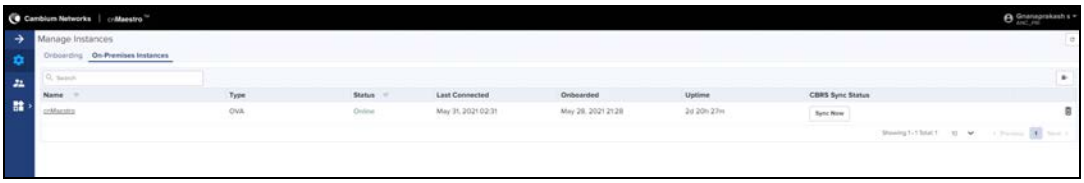
2. In account type, select **Anchor**.



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



5. Once the On-Premises server has been added, the On-Premises Instances page lists the servers.



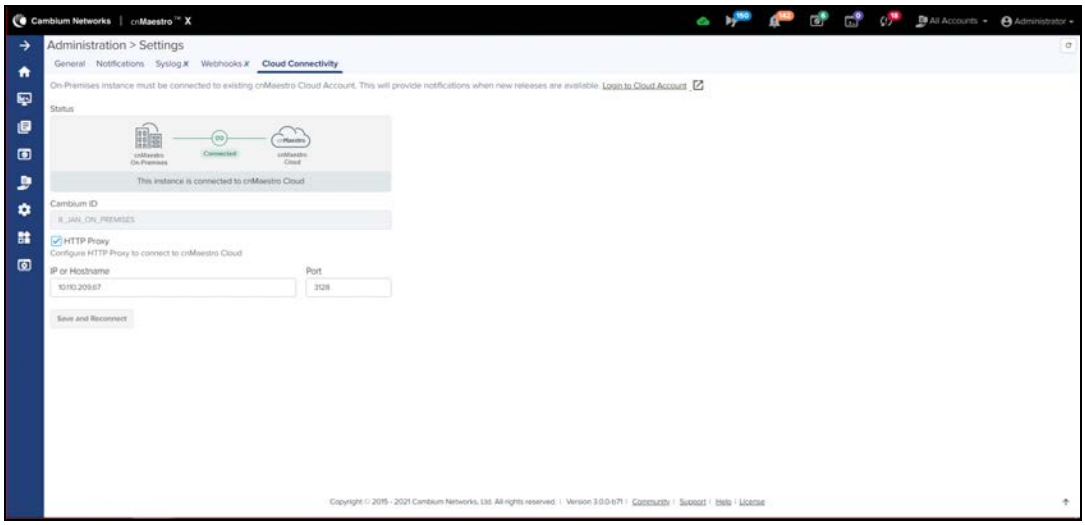
Connecting cnMaestro On-Premises to Anchor Account

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:

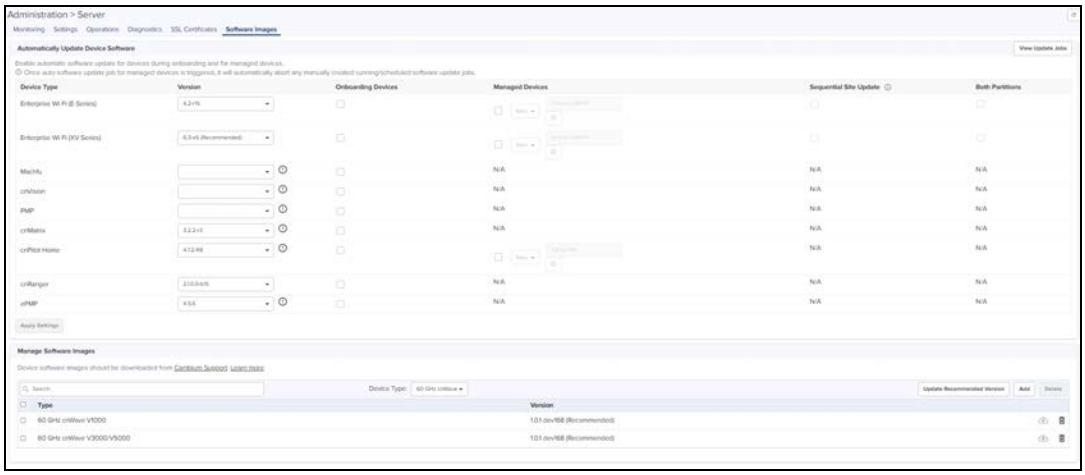
- During the retry time it will take 15 minutes to connect the On-Premises with Anchor Cloud account.
- For every 1 hour it updates the periodic inventory status of On-Premises to Cloud.

Software Images

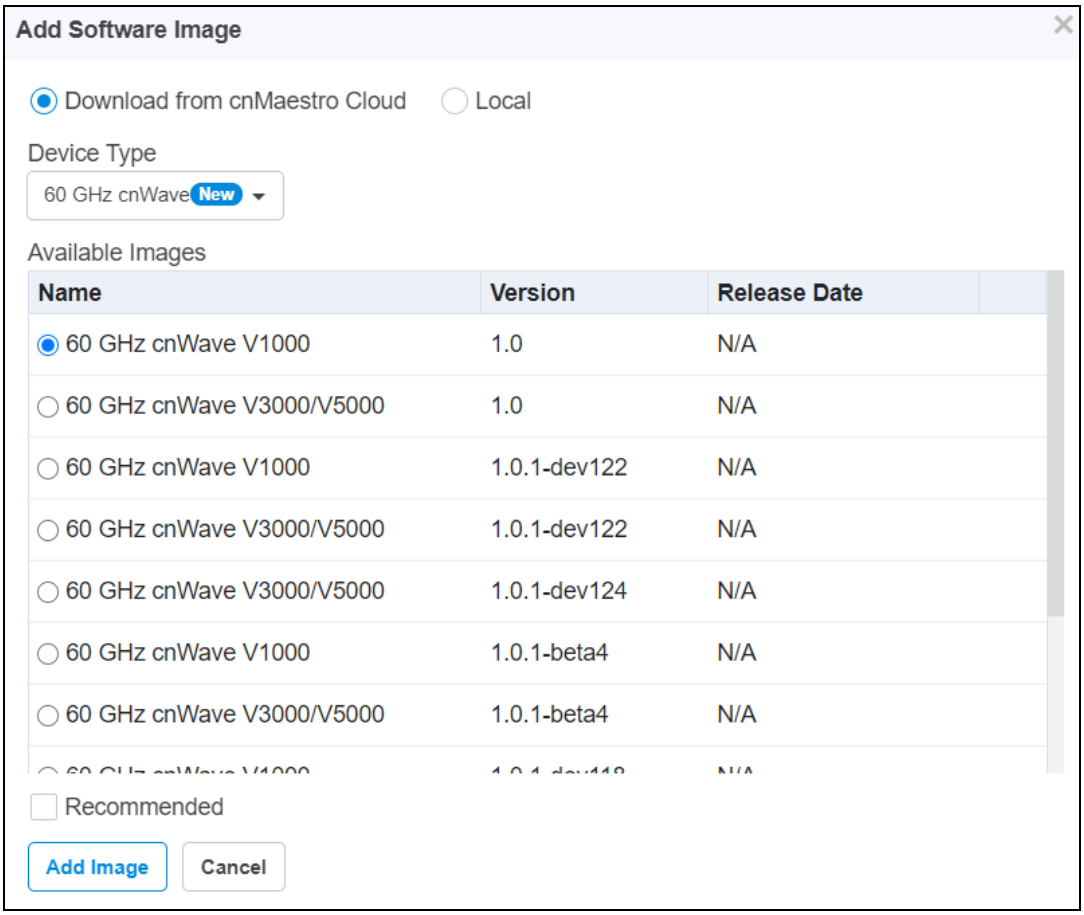
Once the On-Premises server is synced with the cloud, the user can upload the software images from cloud directly to the On-Premises.

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.**

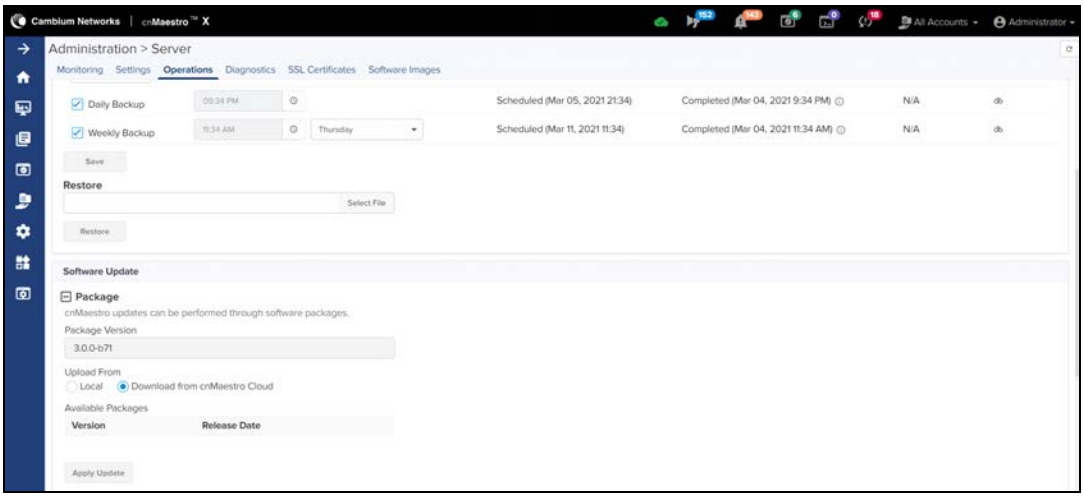
cnMaestro System Update

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**.

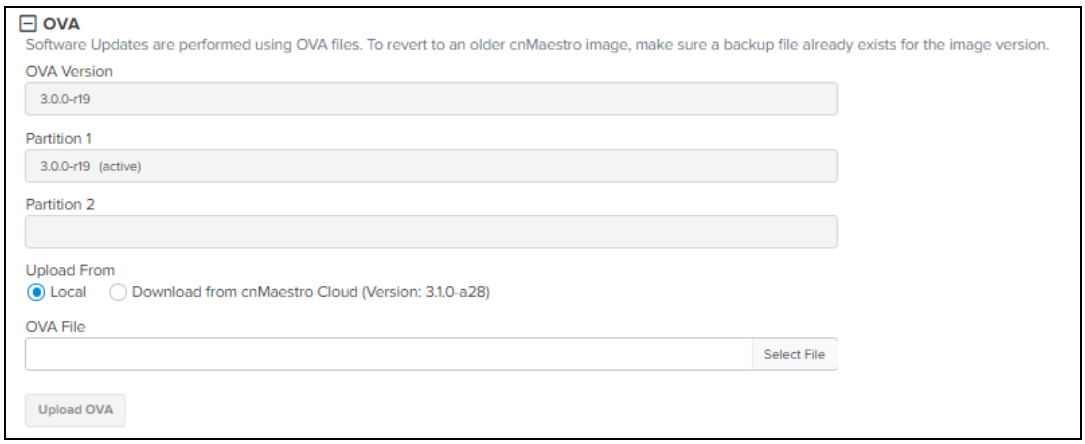


OVA

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**.



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
- Account Recovery
- Configure Network Time Protocol (NTP)
- Extending the Data Disk
- Application Account Recovery

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.

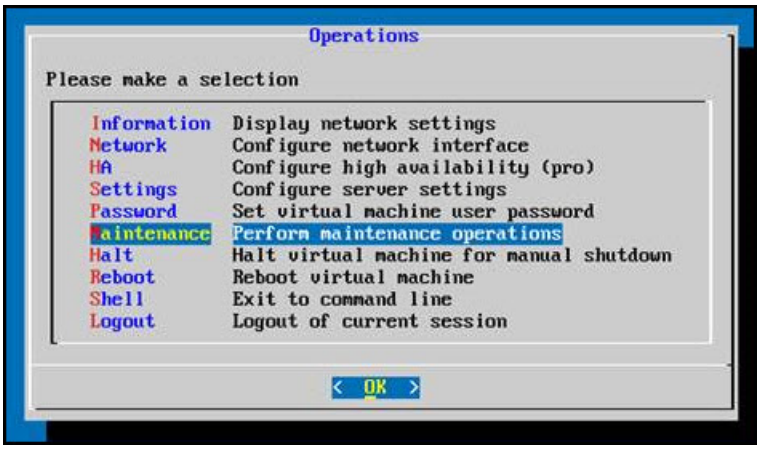
SSH Access

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.

4. A screen pops-up if SSH is enabled successfully.

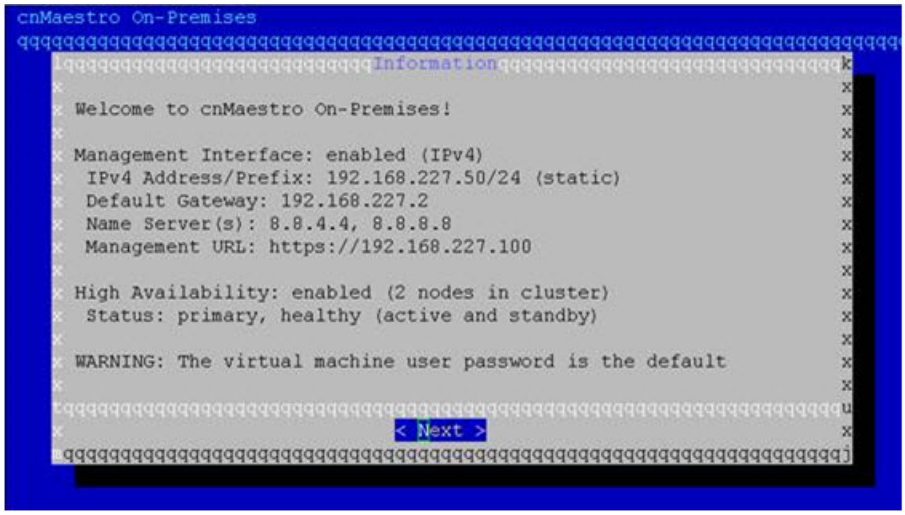
You can then log into the cnMaestro system using the same 'cambium' account used to log in through the Console.

```
# ssh cambium@192.168.127.51
```

NOTE:

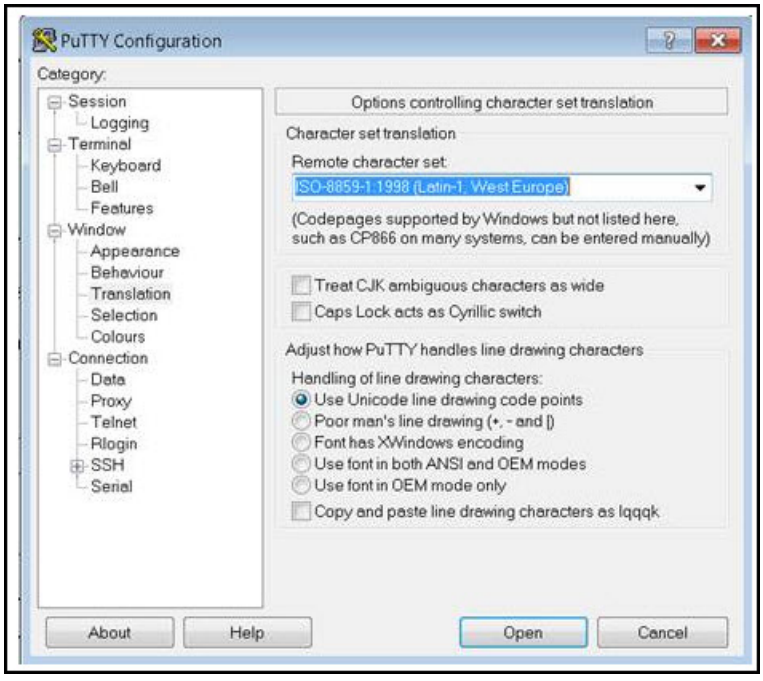
The ‘cambium’ user has sudo access, so if using SSH, be sure to change the default password of this user before enabling the feature.

The Windows application putty, by default, will not print the dialog correctly, and the customer needs to set the Translation accordingly.

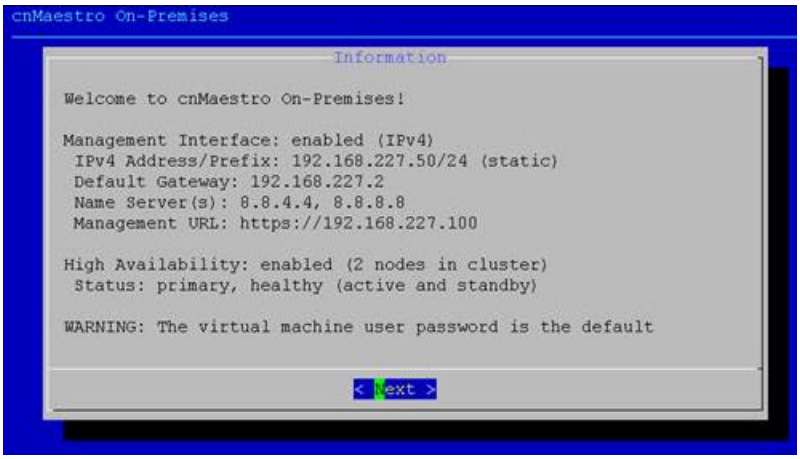


NOTE:

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:**
>
> Data bacukp taken from On-Premises instance after 3.0.0 will have current month data collections in which the data backup is generated and years collection from the day of upgrade to 3.0.0.

cnMaestro On-Premises recommends using a separate data disk for network data and using the snapshot functionality of your Virtualization infrastructure to back up this data consistently.

User will be using a backup system connected to Virtualization infrastructure, so details may differ, but if the system is based on snapshots of the disks it works. Guest-based backup agents are not supported, as consistent point-in-time backups of the entire disk are needed. Serial agent-based backups may back up one part of the disk while another is being written, and result in unusable backups.

Cambium Networks does not recommend relying only on persistent snapshots, as it may seriously degrade performance. Users are recommended to use snapshots to ensure data consistency only, not as backup storage. The recommended backup method is to create a snapshot, copy data, then delete the snapshot, and most backup software is done automatically. It is not recommended keeping of snapshots for more than 24 hours.

> **NOTE:**
>
> It is not recommended to use non-snapshot backup methods, as data is constantly being written, and backups are likely to be inconsistent or unuseable.

Virtualization System Specific

ESXi

Standard snapshot-based backups work with existing vmWare-supported backup tools, and are likely to work with your existing backup solution. We do not recommend attempting to backup snapshot or disk files directly from storage.

Hyper-V

Standard snapshot-based backups work with existing Hyper-V supported backup tools, and are likely to work with your existing backup solution. We do not recommend attempting to backup snapshot or disk files directly from storage.

OpenStack

For LVM and Ceph RBD, snapshots from the storage node should be taken and then copied to offsite storage. We recommend backing up individual volumes if possible, and restoring these. While file-based recovery from within a volume may be possible in some situations, it is not supported.

Account Recovery

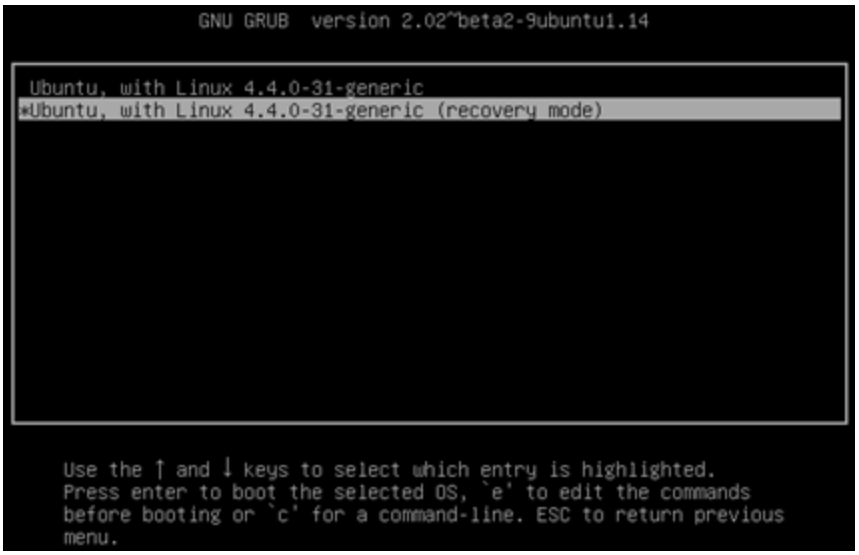
cnMaestro has two types of accounts: the Virtual Machine (Console) account and the cnMaestro Application account. Both of these can be recovered if you forget the administrator password.

Virtual Machine (Console) Account Recovery

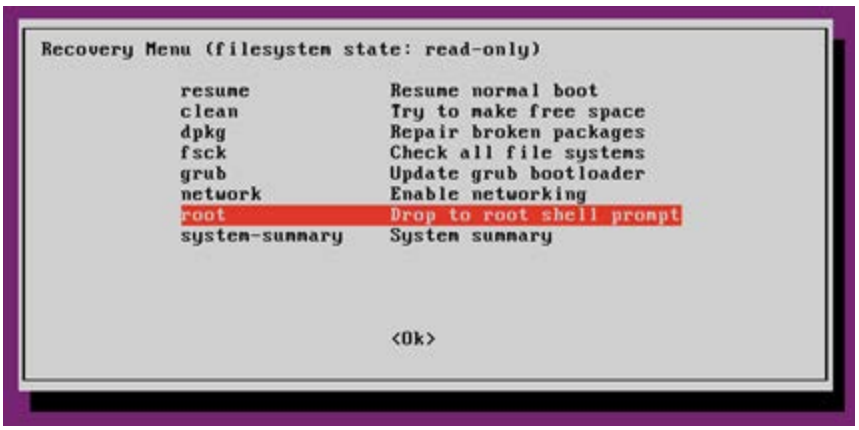
cnMaestro is installed on Ubuntu Server and can leverage the Ubuntu Recovery Mode process to reset the "Cambium Networks" Console login password. The steps are the following:

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

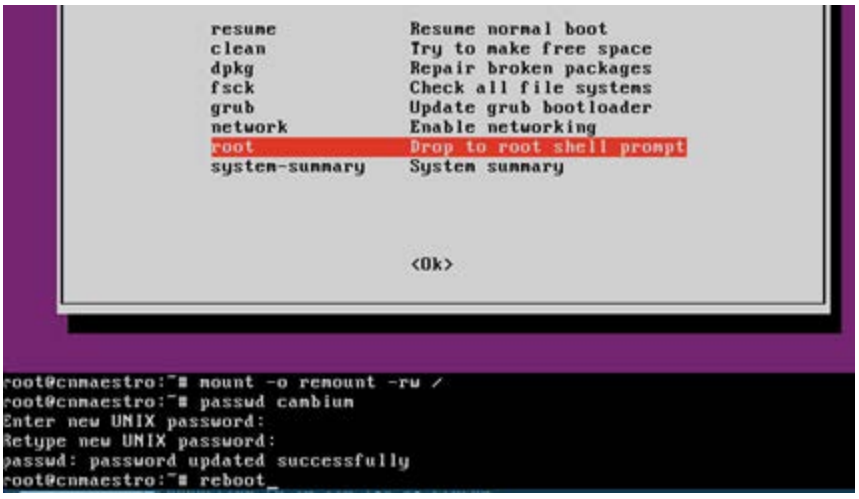


3. Once in the Recovery Menu, select the **root** option to enter a root shell

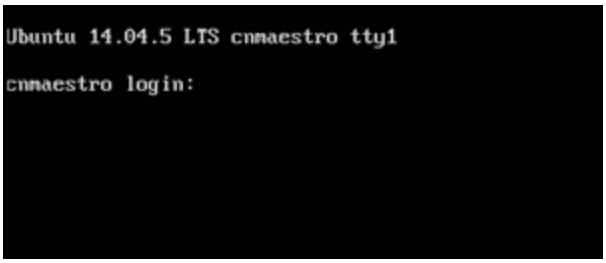


4. The shell will display a command parser along the bottom of the screen. Type the following (without the '#')to reset the password of the **cambium** user.

```
# 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.

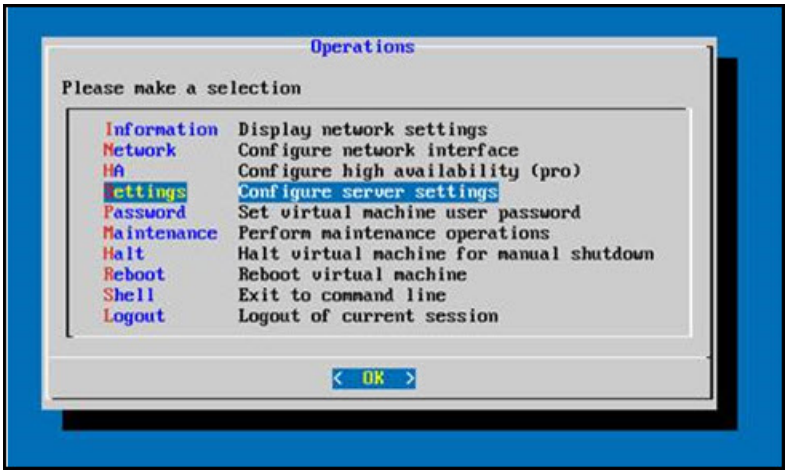
Configure Network Time Protocol (NTP)

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.

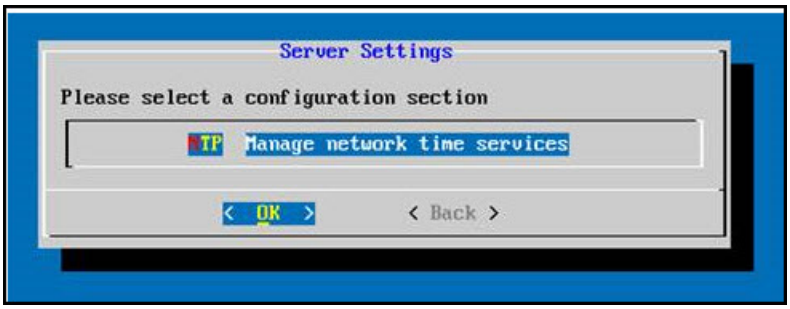
Disabling NTP Support

Follow the below steps to disable NTP Support:

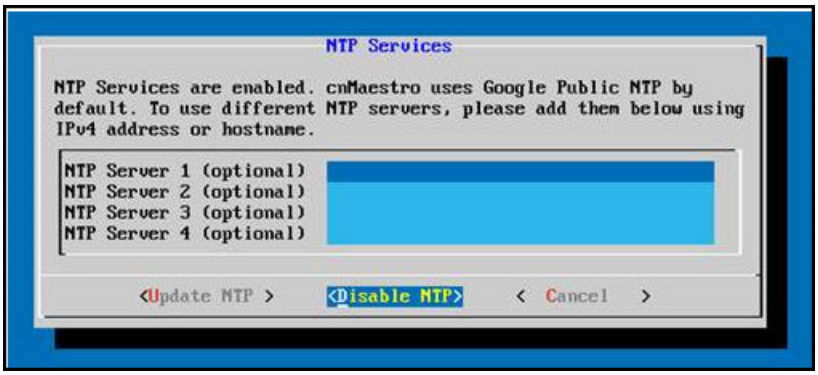
1. From the **Operations** page, select **Settings**.



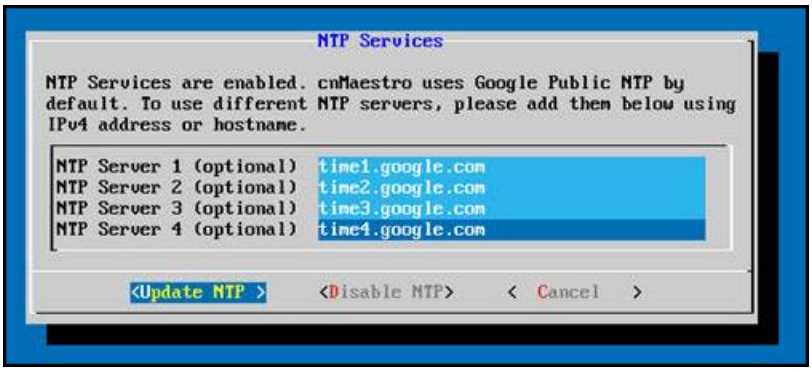
2. Select NTP to **Manage Network Time Services.**



3. To disable NTP, select the **Disable NTP** Option.



4. Set custom NTP servers and Update NTP.



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:

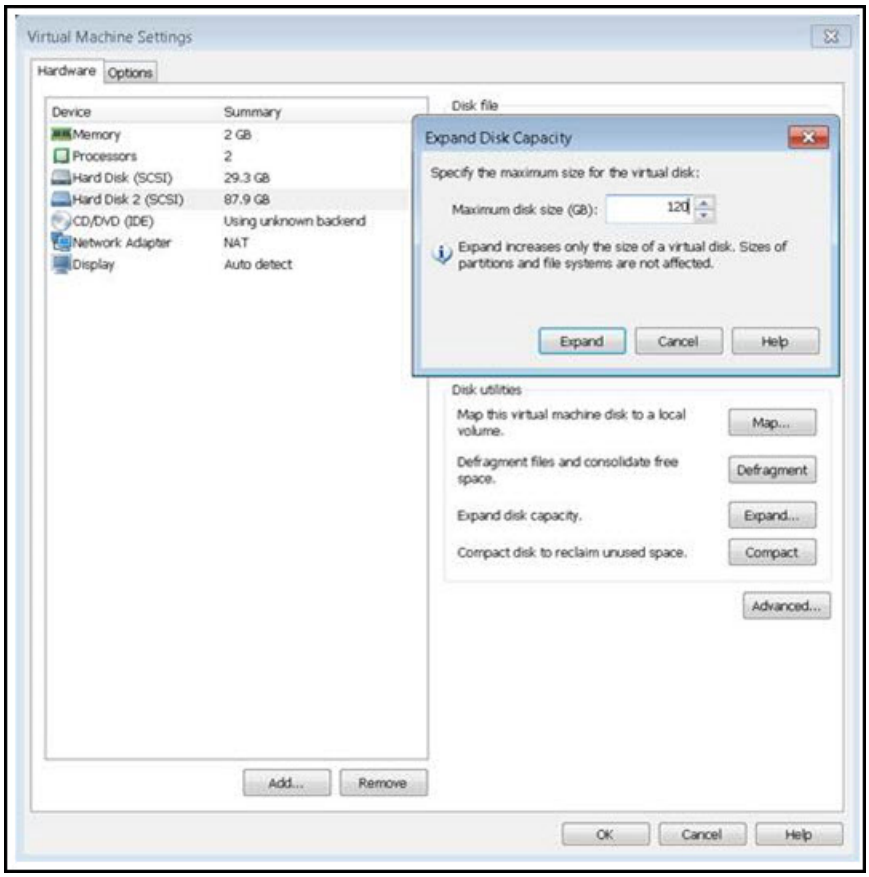
- Phase 1: Expand the virtual disk (using the virtual machine infrastructure).
- Phase 2: Extend the cnMaestro partition and file system (using the command line instructions listed below).

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).

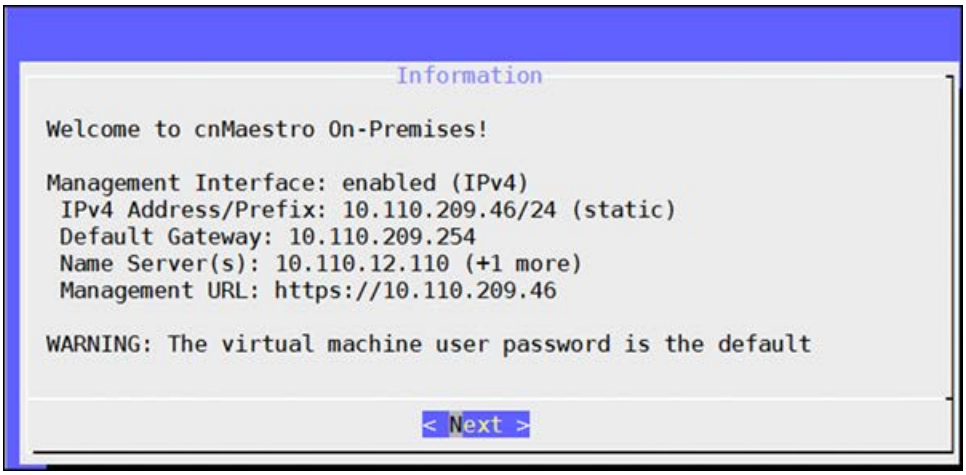
```
cambium@cnmaestro:~$ df -k
Filesystem                        1K-blocks    Used Available Use% Mounted on
udev                                1003608       0   1003608   0% /dev
tmpfs                                204800   10272    194528   6% /run
/dev/mapper/cnmaestro--vg-root     28377236 3622112  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
```

Application Account Recovery

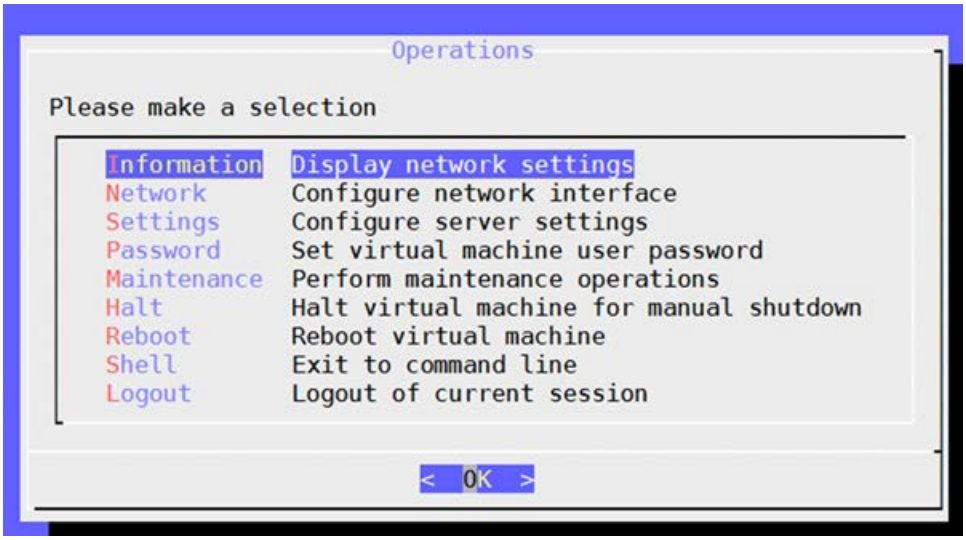
Console administrators can create a one-time password providing Super Administrator access to the cnMaestro UI for a single session (the password will expire in one hour or after a single use). This is a fail safe mechanism that allows cnMaestro access to update current authentication settings.

To create a one-time password:

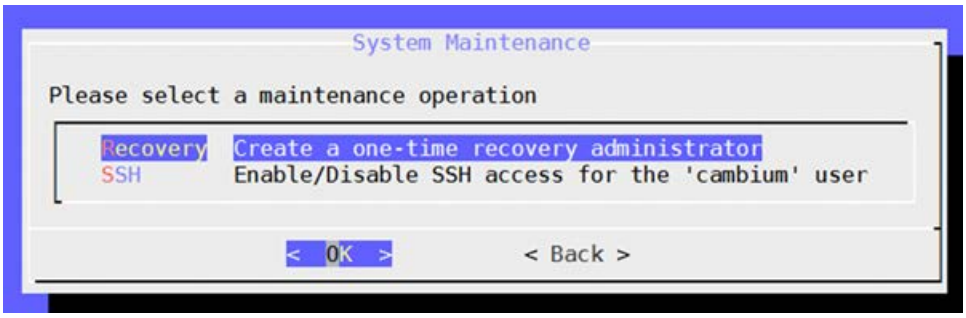
1. Log into the cnMaestro Console and following window pops-up:



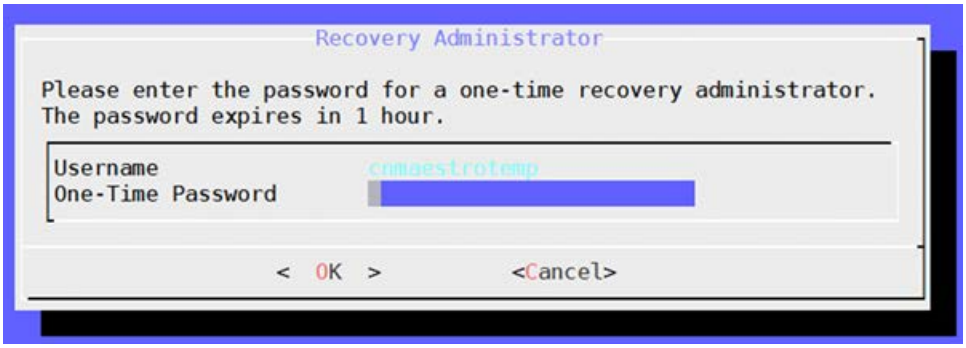
2. Click **Next**.
3. Select **Information** and click **Ok**.



4. Select **Recovery** tab and click **Ok**.

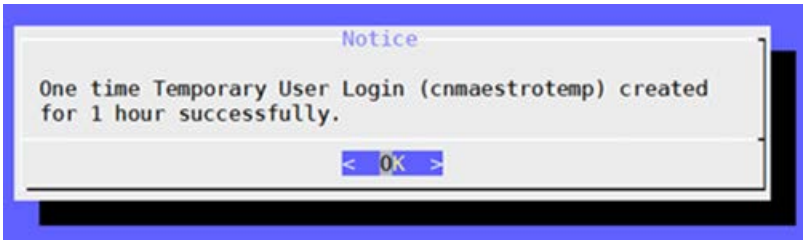


5. Enter the password in the **OneTime Password** text box.



> **NOTE:**
>
> The username for temporary user login is **cnmaestrotemp**. It cannot be changed.

6. Click **OK**. The following window is displayed:



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]
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

Name	Details	Mode
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

Name	Details	Mode
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
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
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	

Name	Details	ePMP	PMP
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.frequency	RF frequency	AP/SM	AP/SM
radio.frame_period	Frame period		AP
radio.dl_frame_utilization	Downlink frame utilization		AP

Name	Details	ePMP	PMP
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
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

Name	Details	ePMP	PMP
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

Name	Details	Mode
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

Name	Details	Mode
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
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
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

Name	Details	Mode
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
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

Name	Details	Mode
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

cnMatrix

General

Name	Details
mac	MAC address
managed_account	Managed account name
mode	Device mode
name	Device name

Name	Details
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	Details	Mode
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
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	
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

Name	Details	ePMP	PMP
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

Name	Details	Mode
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
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

Name	Details	Mode
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
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
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

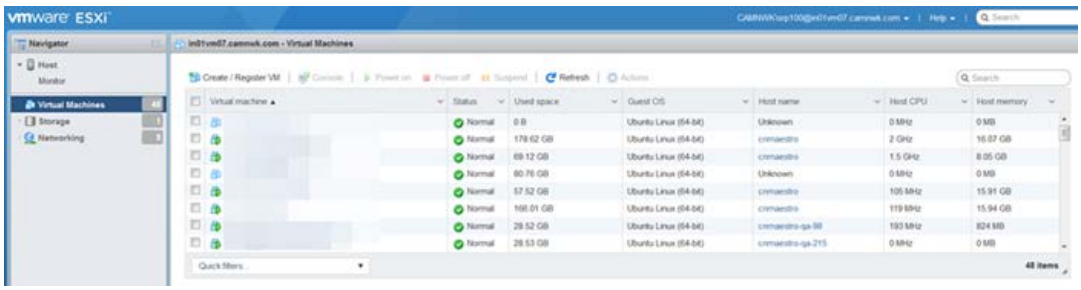
Deployments

VMware ESXi Installation

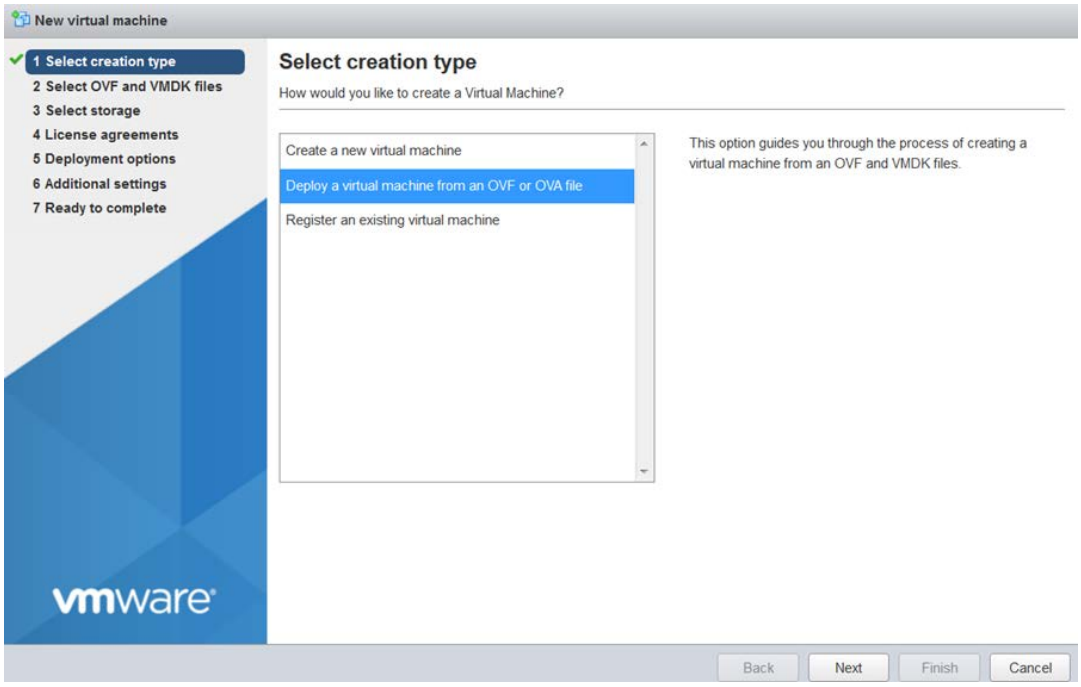
> **NOTE:**
>
> Deploying ESXi is an involved process. The steps below assume you have VMware ESXi version 6.0.0 Update 3 (Build 7967664) or higher already installed on hardware. If you don't have an ESXi hypervisor available, you can download it from VMware website. VMware provides directions for installing the ESXi ISO on a server.

cnMaestro VM Deployment

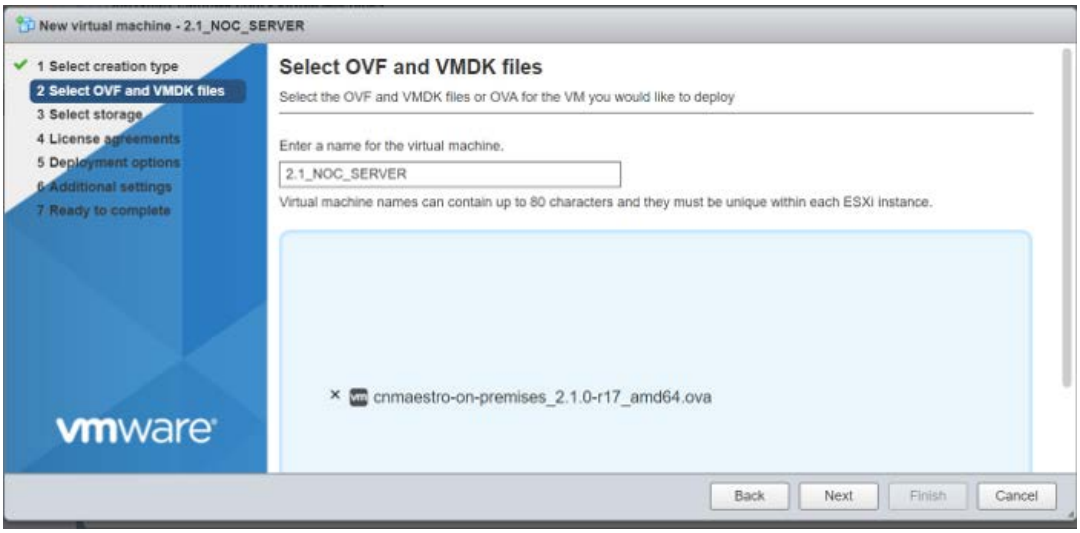
1. Login into ESXi host.
2. Click **Virtual Machines**.



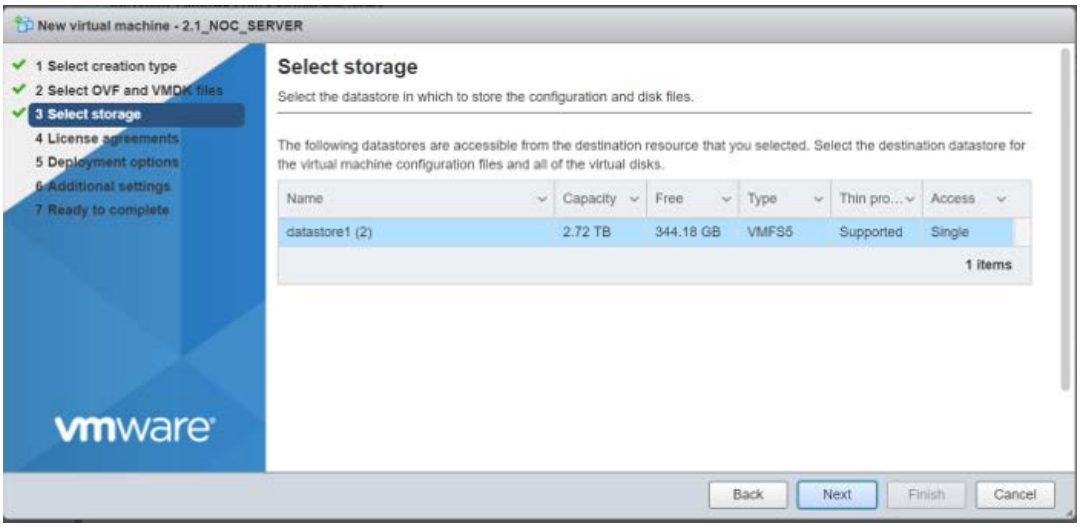
3. Click **Create/Register VM.**



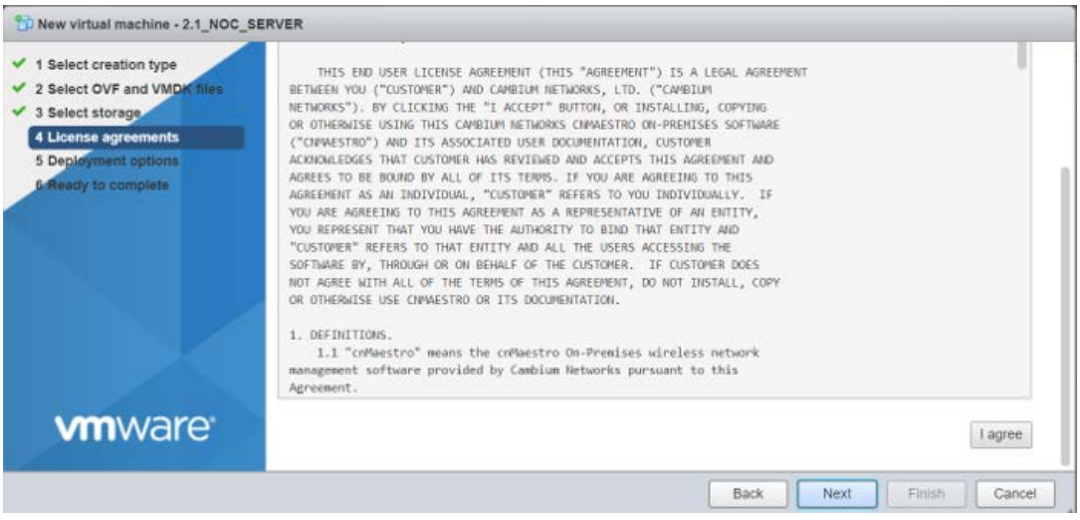
4. Click **Next**.



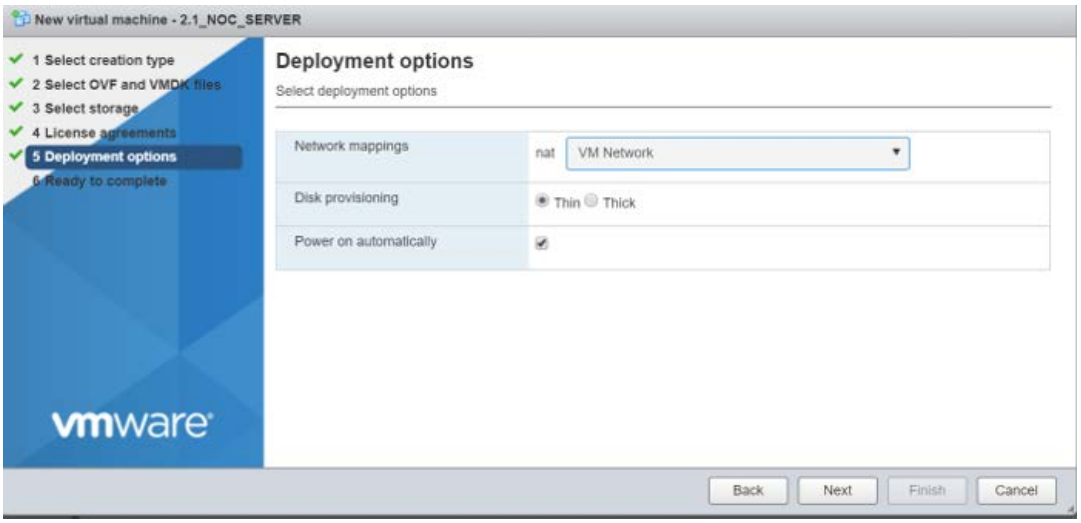
4. Select datastore which has more space



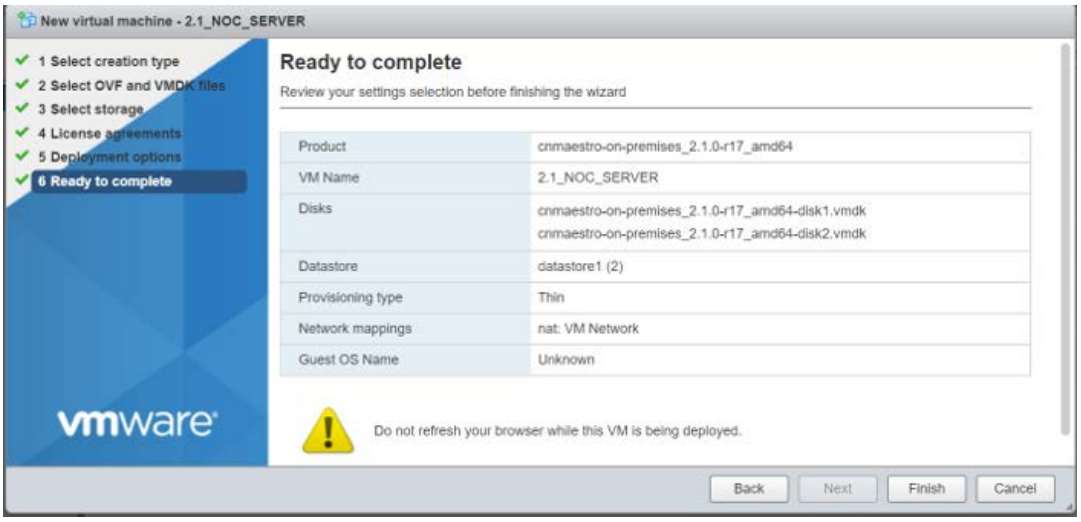
5. Click **Next**.



6. Click **I Agree** the license agreements and click **Next**.

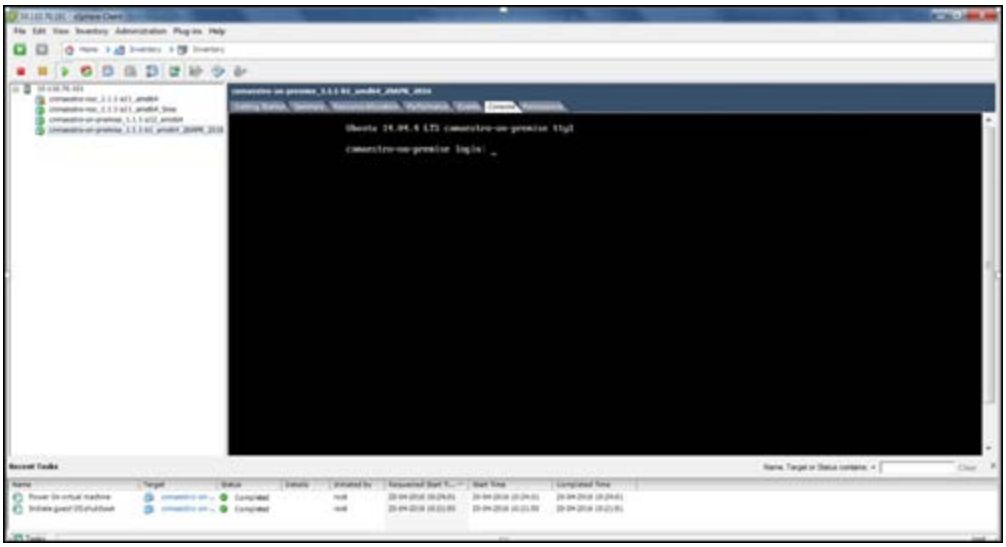


7. Select the network and click **Next.**



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.

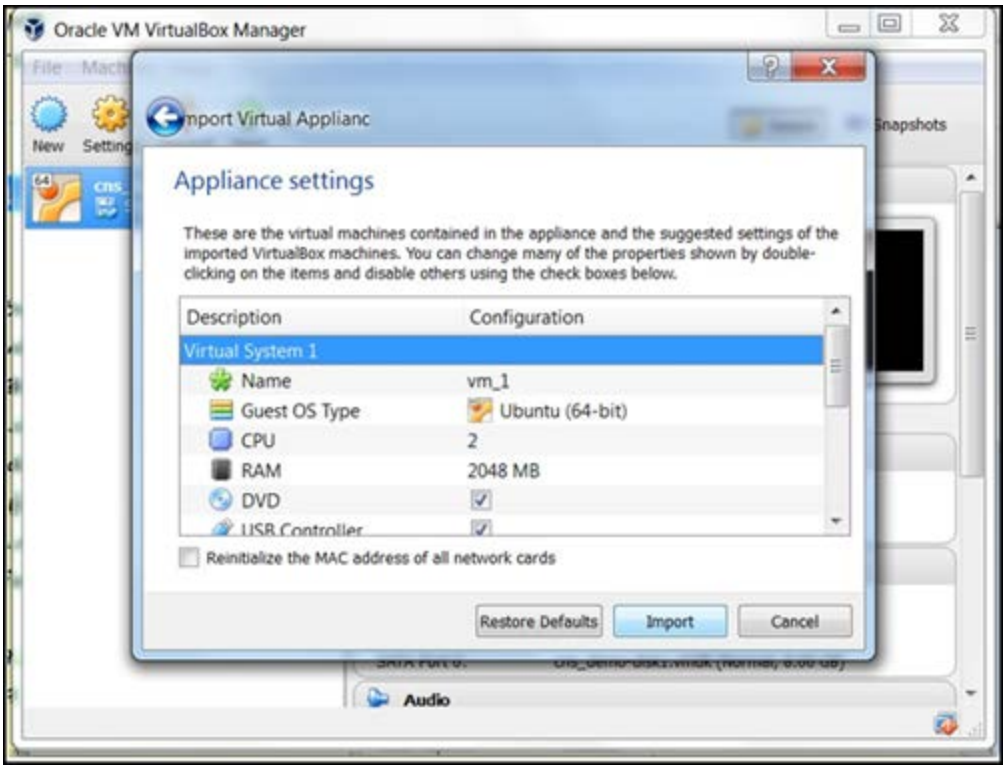
Oracle VirtualBox 5 Installation

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.

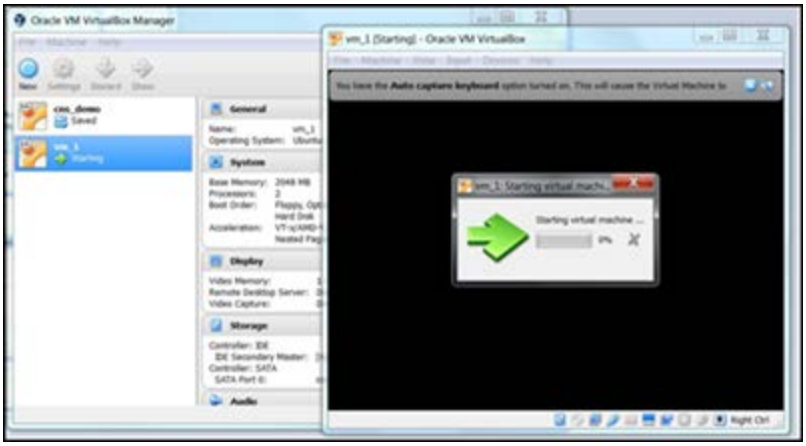
3. Configure the resources required for the VM.



4. Click **Import**.

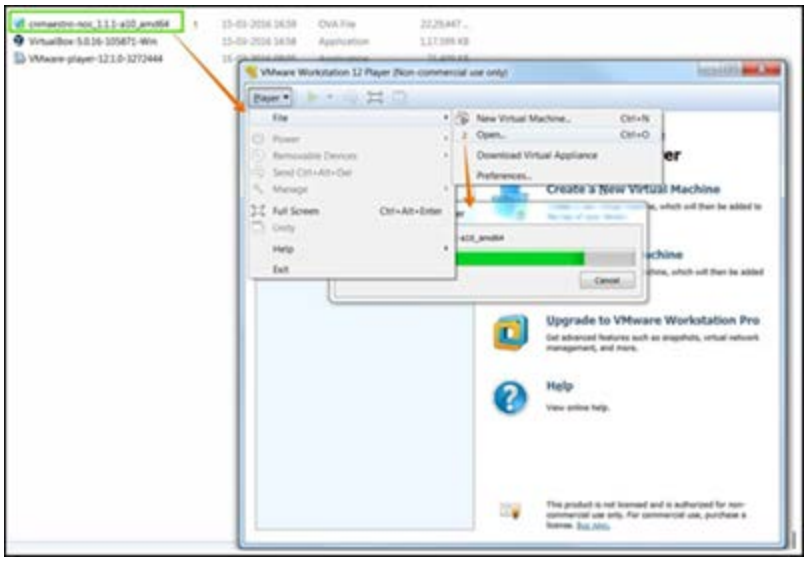
5. The new VM will appear on the left panel. Select the VM and click **start VM** and navigates to the configuration screen.

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.

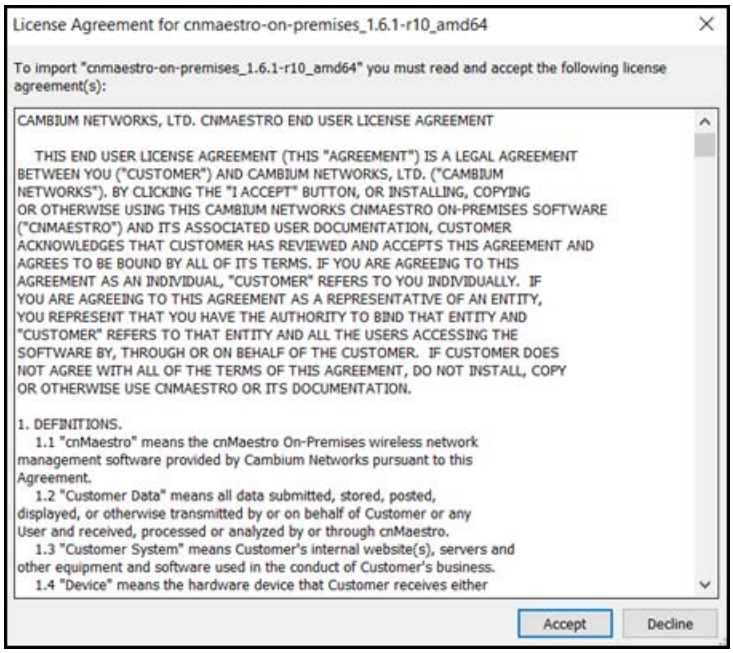


VMWare Workstation

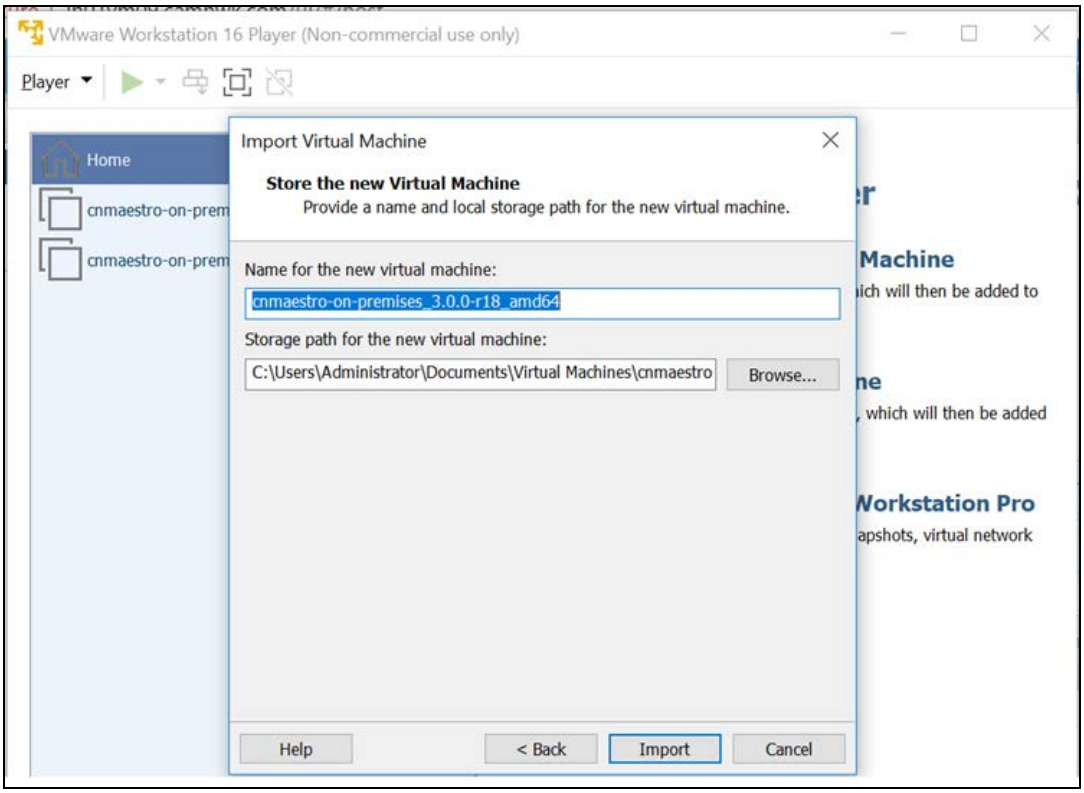
1. Open VMware workstation player. Navigate to **Player > File > Open Menu** and select CnMaestro On-Premises release OVA file.



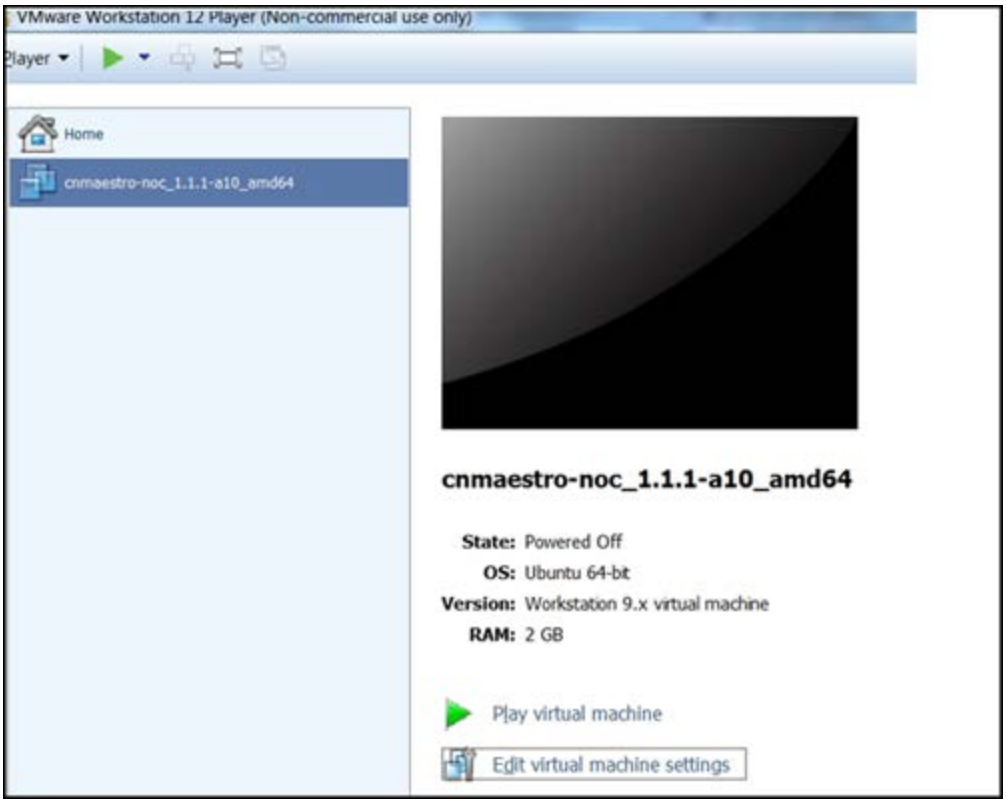
2. Accept the cnMaestro EULA, once the EULA is accepted, cnMaestro will be imported into the VM environment and it could take a couple minutes.



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

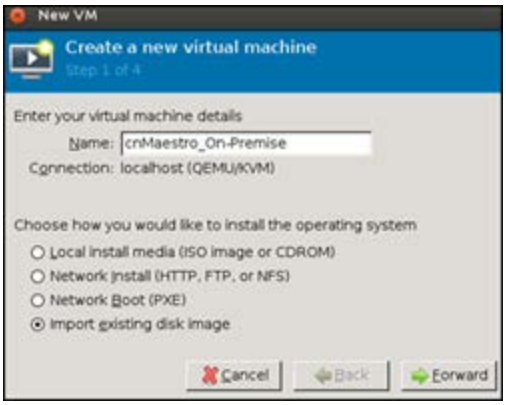
cnmaestro-on-premises_1.2.1-b19_amd64-disk1.vmd

2. **Convert vmdk image to qcow2**

$ qemu-img convert -O qcow2 cnmaestro-on-premises_1.2.1-b19_amd64-disk1.vmdk cnmaestro-on-premises_1.2.1-b19_amd64.qcow

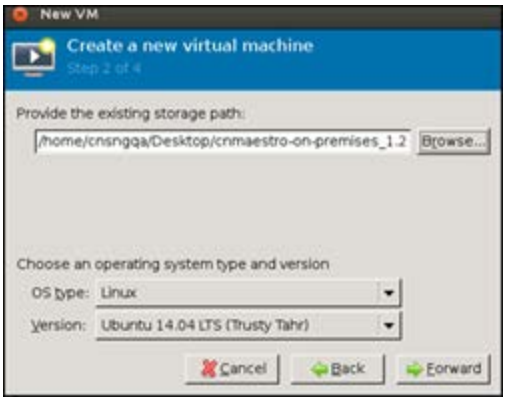
3. **Create New VM**

a. Launch Virtual Machine manager.
b. Create new VM.
c. Choose **import existing disk image**.
d. Click **Forward.**



4. Select disk image file

a. Choose **qcow2** image that is created in earlier steps.
b. Select OS type as **Linux**
c. Click **Forward.**

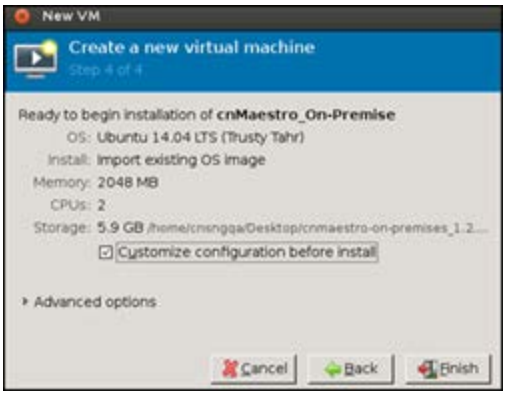


5. Configure Memory and CPU

Configure Memory and CPU settings as per the requirements.

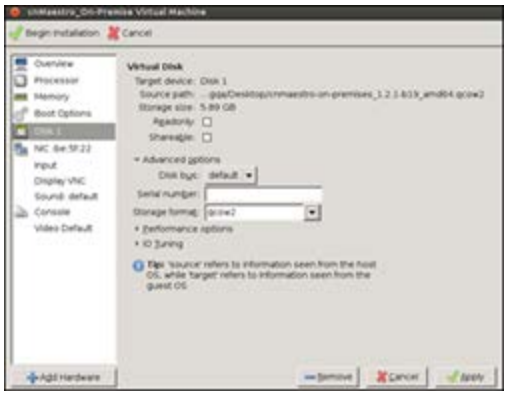
6. Customize other VM Configuration

a. Select **Customize Configuration before install** 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**.

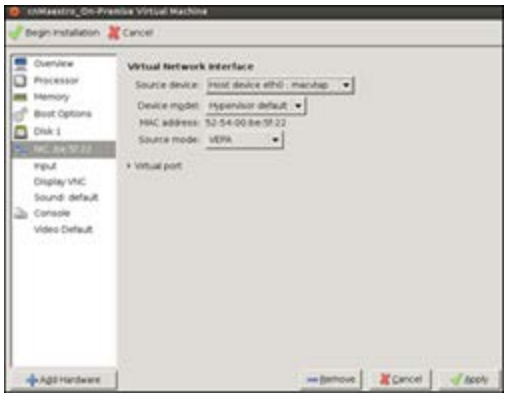


8. **Configure Network Adapter**

   a. Select NIC from the left pane.

   b. Select the appropriate source device. Default: NAT.

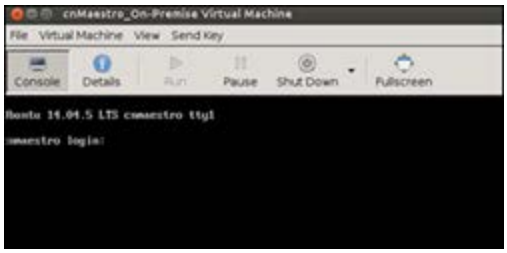
   c. Click **Apply**.



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

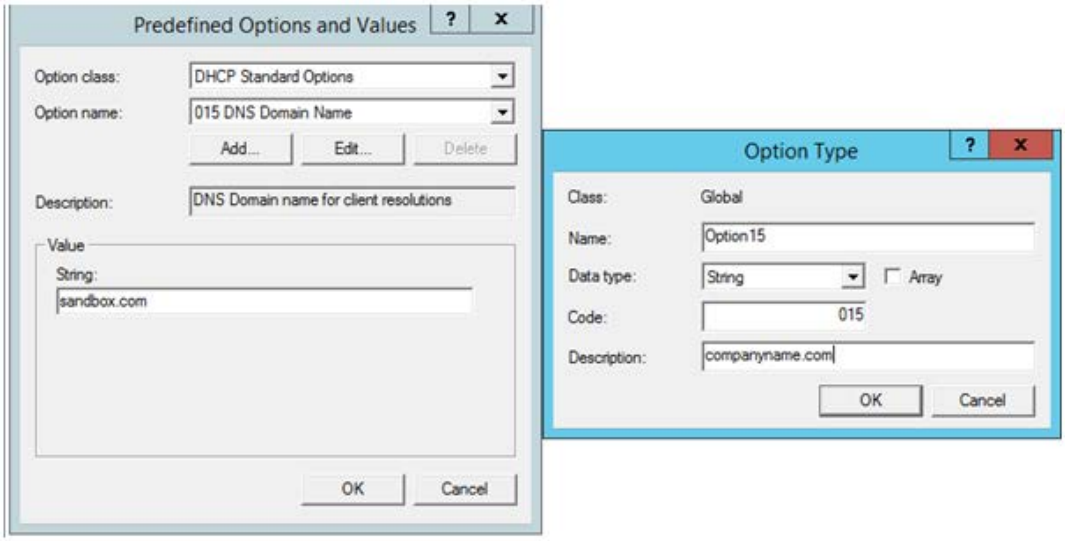
Option 15 returns the domain name to the Cambium Devices.

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.



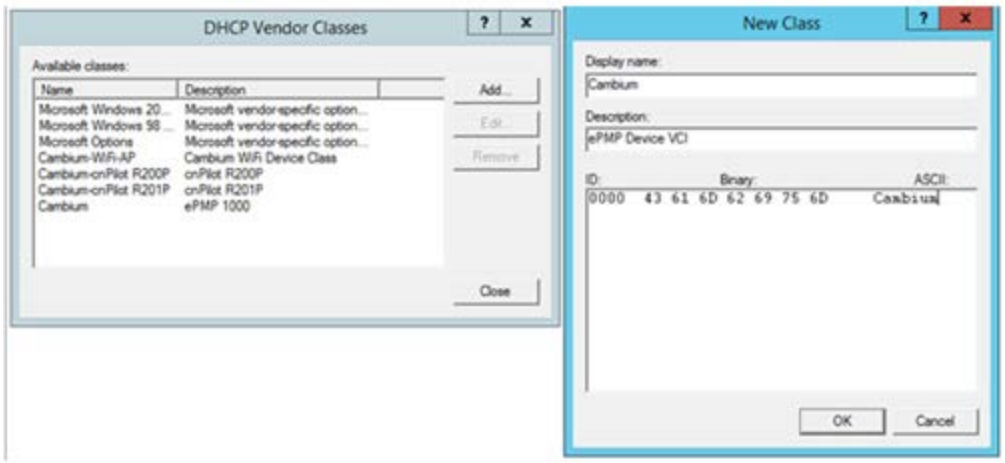
NOTE:

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**.
2. Find your server and right-click on the scope to be configured under the server name. Click on the **Define Vendor Classes** and click the **Add** button in the dialog box that appears.

3. Provide the Display name, Description and then click in the ASCII column and enter the value as Cambium as shown in the below figure, and then click **OK**.



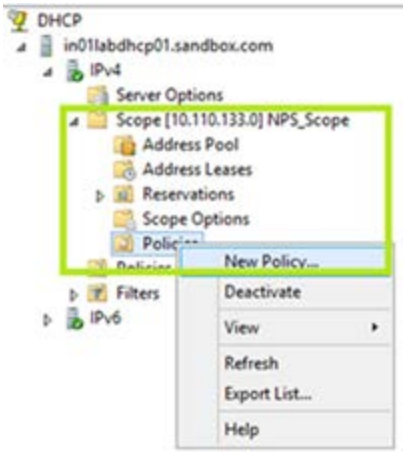
The above example is for an ePMP device. In order to create the VCI for other device types, please follow the same steps, and in the ASCII column provide the following values:

Product	VCI (DHCP Option 60)
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

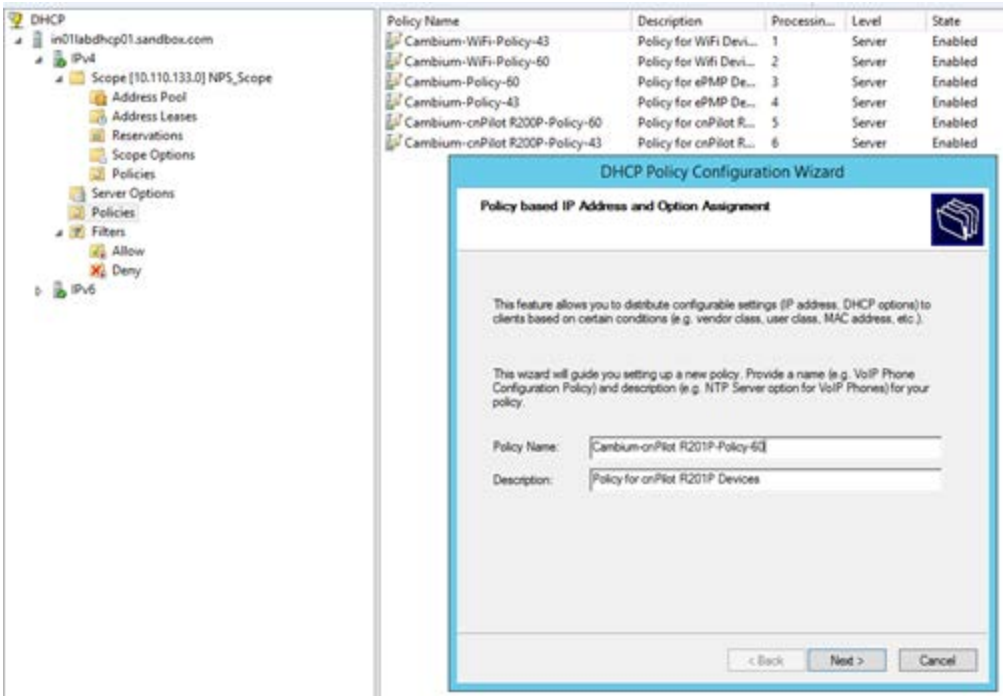
Configuring the Policies at the SCOPE Level

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.

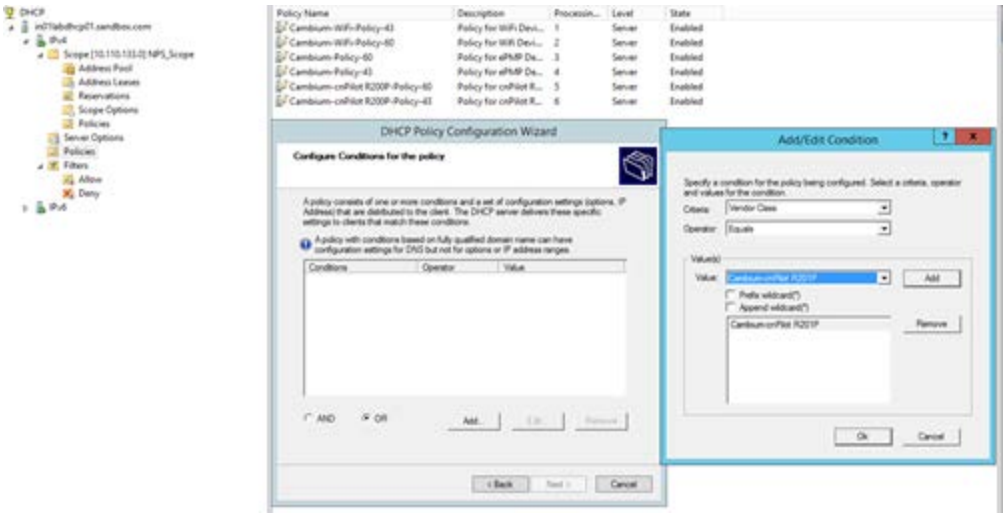
1. Select the scope in which you want to create the policy, and then right click on the Policies option. Select New Policy.



2. In the pop-up, enter the Policy Name and Description and click **Next** button.

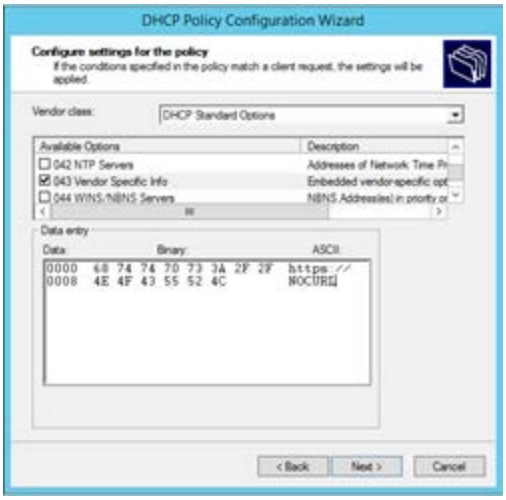


3. The Policy consists of Matching conditions based on Vendor Class, user class, MAC Address, Client Identifiers, FQDN and Relay Agent Information. For Cambium Devices we need Vendor Class based match conditions only.
   a. In the dialog, click on the **Add** button and in the pops-up select the Criteria as **Vendor Class**, the Operator as **Equals**, and the Value as the VCI created for the Cambium Device type.
   b. For example, for cnPilot R201P device the Vendor Class selection is “Cambium-cnPilot R201P”.
   c. Click **Add** and then **OK** in the pop-up. Click **Next** in the Policy Configuration Wizard.

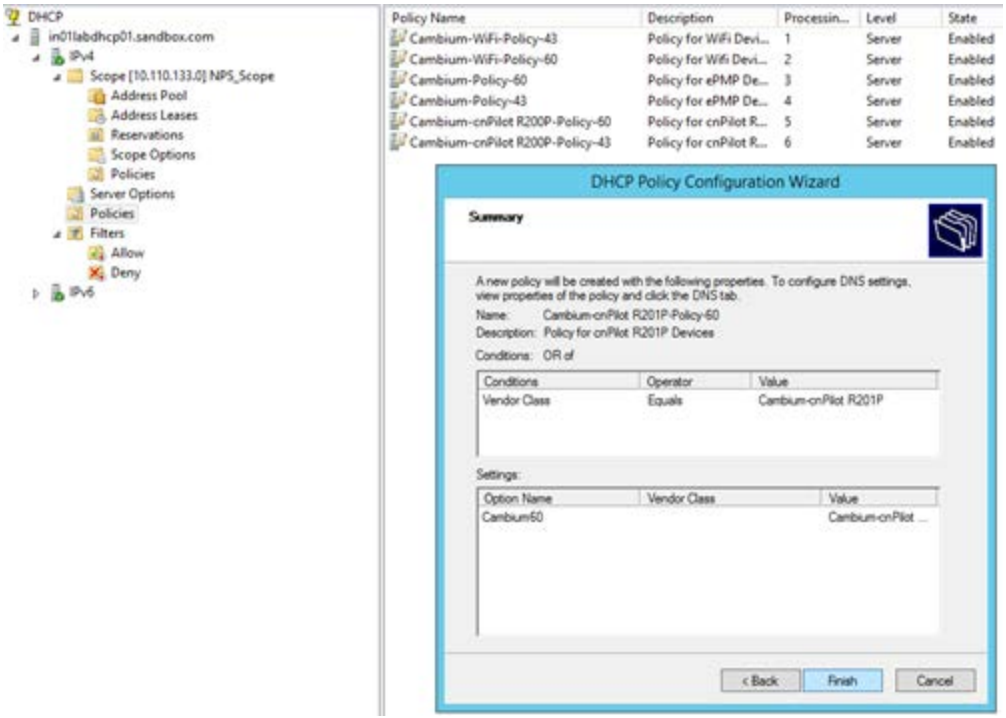


4. In the policy configuration settings wizard, select the option **No** and click **Next**.

Then select the vendor class as DHCP standard options and Select the options 43 and 60 from the available options and specify the values that need to be sent to the device. Click **Next** once the options are selected and values are specified.



5. Click Finish in the final settings page. The policy is displayed in the RHS pane.



The above Policy is a generic one. For all the device types, the policies should be created 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

Network Requirements

Inbound Ports

The following table provides information about network port requirements for inbound:

Table 58: 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 59: 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.