



RELEASE NOTES

cnMaestro™

Release 6.2.0



Contents

Introduction	3
EasyPass: Hospitality PMS Integration	3
NSE Enhancements.....	4
MarketApps: 60 GHz cnWave Installer App	8
MarketApps: Installer App Enhancements	10
Historical Clients detail at the AP level	11
Per-AP Performance Graphs for PER and Non-Wi-Fi Interference	11
PON Enhancements.....	12
Miscellaneous Enhancements	13
API Updates X.....	15
Supported Cambium Products.....	24
Supported Browsers	27
Significant Fixes	28
Known Issues	28
Where to Get Help.....	31

Introduction

The cnMaestro™ 6.2.0 release introduces a new set of exciting features and improvements.

Important: Web Browser

Restart your browser or clear the browser cache with a hard reload if you have UI problems after the 6.2.0 update.

Important: Enterprise Wi-Fi AP Version

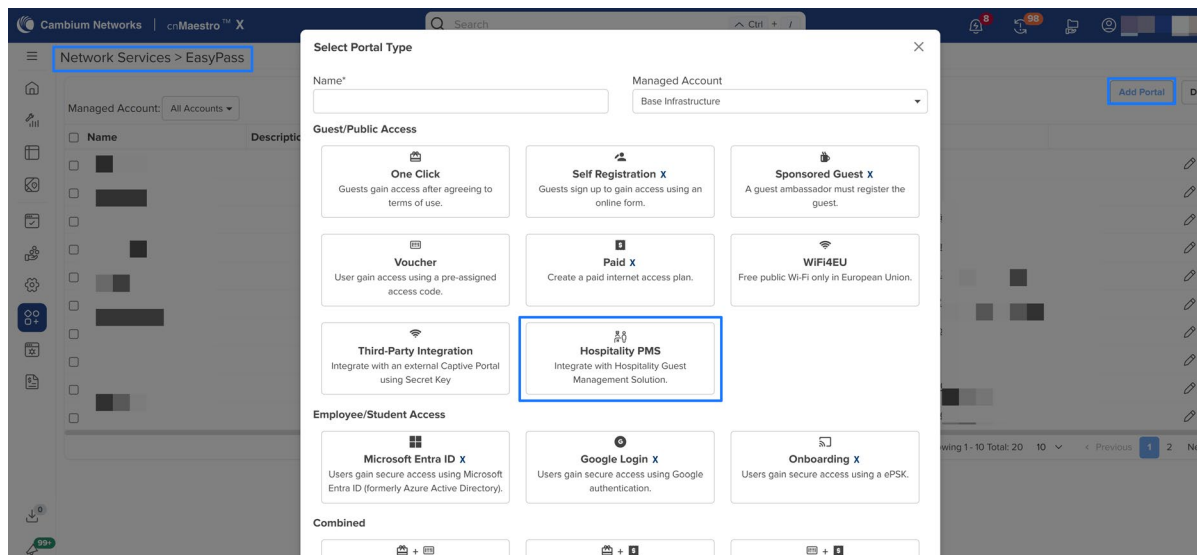
Update to the Enterprise Wi-Fi AP 6.6.1 or later if you plan to use MarketApps.

EasyPass: Hospitality PMS Integration

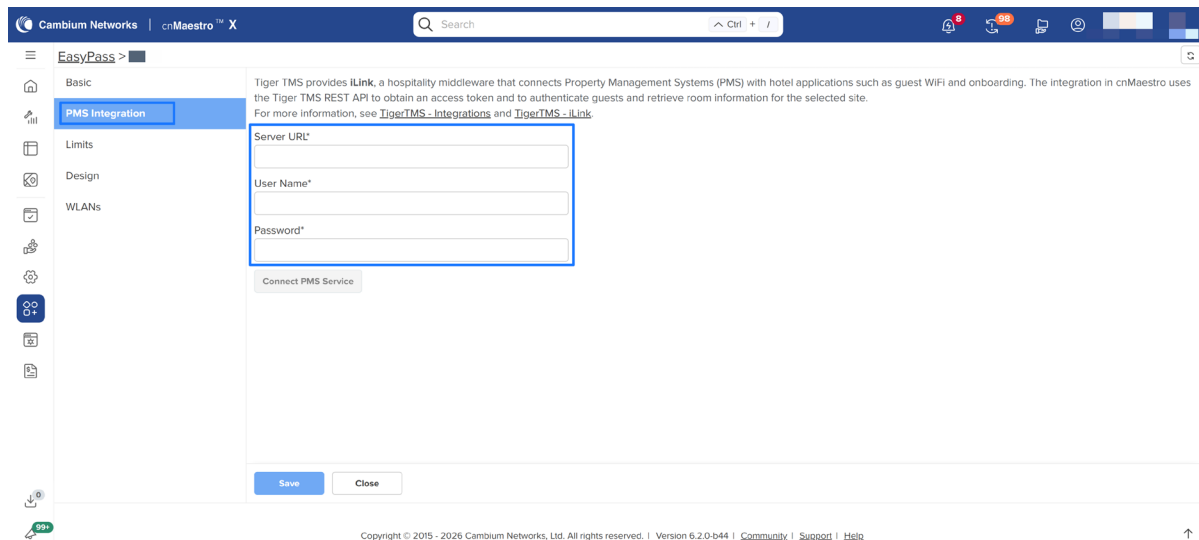
This feature is now Generally Available (GA) in 6.2.0.

TigerTMS is a PMS system service provider for Hospitality. They provide a full management system for property managers from check-in, billing, etc. They provide API for Captive Portal deployment in their systems through which guests are authenticated, and session is managed through it.

Navigate to *EasyPass* > *Add Portal* > *Hospitality PMS*



Configure Server URL, Username and Password under PMS integration page to connect with PMS service.



NSE Enhancements

Cellular WAN Integration

This feature is now Generally Available (GA) in 6.2.0.

If the NSE is connected behind a Teltonika modem, it can fetch cellular statistics from the modem and display them in cnMaestro.

To configure this:

- Set the uplink type to **Cellular** under **WAN** configuration
- Provide the required username and password

Once configured, the NSE will fetch statistics from the modem and display them in cnMaestro.

Note: This feature requires NSE devices running software version **2.2 or later**.

WAN Configurations

WAN-1 (Port 1) **WAN-2 (Port 3)** **Virtual WAN** **Add**

Assigned Port*
Port 3

The minimum device software version required for this feature is '2.0'.

IP Address Assignment
Dynamic

Uplink Type
Cellular

Cellular WAN Username*

Cellular WAN Password*

☐ Enable 802.1q VLAN tagging of frames

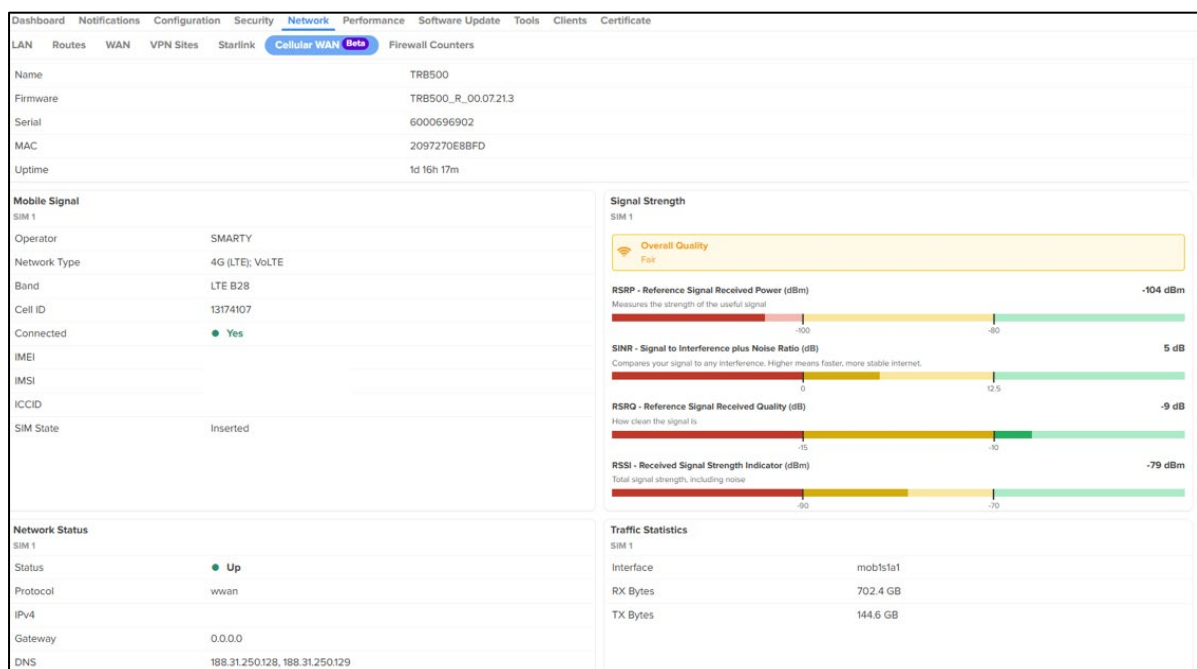
Additional IP Addresses

Additional WAN IP addresses used for Source NAT e.g. 50.11.0 or 50.11.0/29 or 50.11.0-50.11.7.

The statistics are available at *Network > Cellular WAN*.

As part of the statistics displayed, we provide the following details:

- Hardware and software version of the modem
- Mobile signal information
- Cellular signal strength details
- Network status
- Traffic statistics



Snort3 support for NSE3000, Snort2 to Snort3 VRT Category Migration

This release introduces migration of Snort VRT categories. Since Snort2 and Snort3 use different VRT category definitions, migration ensures that existing IPS policies continue to function correctly after the upgrade.

cnMaestro automatically migrates configured Snort2 VRT categories to the corresponding Snort3 VRT categories during device upgrades.

No changes are required for IPS categories other than Snort VRT categories.

IDS/IPS

☒ Enable IDS/IPS

Mode

Detection

Rule Type

snort-vrt

Rules

Balanced

Olink Code*

Procure a snort.org Olinkmaster code and paste it here. (Paste the code only and not the URL)

Category

☐ app-detect

☐ exploit-kit

☐ os

☐ server-mail

☐ browser

☐ File

☐ policy

☐ community

☐ indicator

☐ protocol

☐ content-replace

☐ Malware

☐ pua-adware

Note: This feature requires NSE devices running software version **2.3 or later**.

Tailscale Integration

This release introduces Tailscale integration for the NSE, enabling administrators to securely connect branch networks that are behind NAT to a Tailscale peer (Tailnet) or to other branches that are also behind NAT, without requiring traditional VPN configuration or port forwarding.

The integration simplifies secure site-to-site and remote connectivity by leveraging Tailscale's WireGuard®-based mesh networking, providing seamless, secure communication between distributed sites.

Configuration

Navigate to *NSE Group* → *VPN* → *Tailscale*

Configure the following settings:

Parameter	Description
Enable Tailscale	Enables or disables Tailscale on the NSE.
Authentication Key	Tailscale authentication key used to register the device with the Tailscale cloud
Enable Accept Routes	Accepts subnet routes advertised by other Tailscale nodes.

Advertise Routes Specifies the local LAN subnets to advertise to the tailnet (for example, 192.168.50.0/24).

Note: This feature requires NSE devices running software version **2.3 or later**.

Basic

Management

Network

Groups

WAN

Firewall

DNS

Threat Protection

VPN

User-Defined Overrides

demo@demo.com

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

Tailscale

☒ Enable Tailscale

Authentication Key*

.....

Tailscale pre-shared authentication key

☒ Enable Accept Routes

Accept subnet routes advertised by other tailscale nodes

Advertise Routes

192.168.1.0/24 x

192.168.2.0/24 x

192.10.1.0/24 x

192.10.10.0/24 x

192.10.110.0/24 x

192.168.203.0/24 x

Type and press Enter

List of subnets to advertise to the tailnet (e.g. 192.168.1.0/24)

The Tailnet Dashboard for NSE provides centralized visibility regarding the operational status and performance of the Tailscale client. Administrators can monitor peer connectivity, network activity, DERP latency, and client health from a single dashboard, simplifying troubleshooting and operational monitoring.

Navigate to NSE > Network > Tailnet

NSE > NSE-7039B0-India-2-DNDh

Dashboard Notifications Configuration Security Network Performance Software Update Tools Clients Certificate

LAN Routes WAN VPN Sites Tailnet Starlink Cellular WAN Firewall Counters

Tunnel Activity

Aggregate traffic across all peers

Tailnet Peers

13 8

Total Online

RX from Peers

2.38 KB

Inbound

TX to Peers

2.4 KB

Outbound

Client Stats

Version 1.96.0-dev(20260305-7943b3a2)

Interface Status Up

State Running

Network Environment

Protocol UDP

IP Port 115.110.225.242:54796

Mapping Varies by Destination IP False

Captive Portal False

Nearest DERP Bengaluru

DERP Latency

Good < 50 ms Expected 50-100 ms Poor > 150 ms

Bengaluru 20 ms

Singapore 50 ms

Hong Kong 85 ms

Tokyo 121 ms

London 145 ms

Sydney 171 ms

Paris 173 ms

Helsinki 177 ms

Frankfurt 177 ms

Amsterdam 181 ms

Tailnet Peers

Apply Filter(s)

Host Name	OS	IP Address	Relay Server	Status	Rx Bytes	Tx Bytes	Last Seen	Exit Node	Last Handshake
NSE-7003E8-Updated	linux	100.125.191.74	bit	Online	0 Bytes	0 Bytes	25 Jun 2026, 05:31 AM	False	N/A
IND-6MFMH4K3	windows	100.75.179.62	bit	Online	612 Bytes	988 Bytes	25 Jun 2026, 05:31 AM	False	25 Jun 2026, 04:12 PM
Raspberry-PiRed	linux	100.119.66.47	bit	Online	0 Bytes	0 Bytes	25 Jun 2026, 05:31 AM	False	N/A
NSE-7003D0-2	linux	100.94.194.41	bit	Offline	0 Bytes	0 Bytes	24 Jun 2026, 11:50 AM	False	N/A
NSE-000150-Beta-Rashin-Ent	linux	100.73.232.24	bit	Offline	0 Bytes	0 Bytes	19 Jun 2026, 03:18 PM	False	N/A
IND-5CD75145GG	linux	100.974.11	bit	Offline	0 Bytes	0 Bytes	20 Jun 2026, 05:46 PM	False	N/A
linetest	linux	100.122.1.35	bit	Online	0 Bytes	0 Bytes	25 Jun 2026, 05:31 AM	False	N/A
NSE-703568-US	linux	100.91.7.75	bit	Offline	0 Bytes	0 Bytes	09 Jun 2026, 07:25 PM	False	N/A
NSE-700880	linux	100.118.18.7125	bit	Online	0 Bytes	0 Bytes	-	False	N/A
IND-77CGM22	windows	100.89.58.120	bit	Online	1.77 KB	1.41 KB	25 Jun 2026, 05:31 AM	False	25 Jun 2026, 04:12 PM

DNAT counters

This release introduces the DNAT statistics page, providing real-time visibility into traffic matching Destination NAT (DNAT) rules configured on the NSE. Administrators can monitor hit count on the rule and validate that inbound traffic is being translated as expected.

Navigate to NSE Dashboard > Network > Firewall counters

NSE > NSE-701038-Bangalore

Dashboard Notifications Configuration Security **Network** Performance Software Update Tools Clients Certificate

LAN Routes WAN VPN Sites Talinet Starlink Cellular WAN **Firewall Counters**

Outbound Firewall

Apply Filter(s)

Name	Packets	Bytes	Comment
No Data Available			

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

DNAT

Apply Filter(s)

Name	Packets	Bytes	Comment
dnat_vwan_pf_rule_1	1	52 B	dnat: wan1 ip daddr 10.110.200.52 tcp dport 22 -> 192.168.200.10:22
http	4	208 B	dnat: wan1 ip daddr 10.110.200.52 tcp dport 8000 -> 192.168.10.12:8000
dnat_wan1_tto1_rule_1	0	0	dnat: wan1 ip daddr 10.110.200.51 -> 192.168.200.11
dnat_wan2_tto1_rule_2	0	0	dnat: wan2 ip daddr 10.110.200.70 -> 192.168.10.12

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

Note: This feature requires NSE devices running software version **2.3 or later**.

User Groups in Outbound Firewall

This release introduces User Group-based firewall policies, enabling administrators to define firewall rules using user groups instead of individual IP addresses or subnets.

User groups simplify policy management by allowing multiple IP subnets to be grouped under a single logical entity, making firewall rule configuration more scalable and easier to maintain.

Note: This feature requires NSE devices running software version **2.3 or later**.

Navigate to NSE group > Groups > User Group

NSE Groups > Charter_BayCity_NSE

Basic Management Network **Groups** WAN Firewall DNS Threat Protection

User Groups

Apply Filter(s)

Name	Description	IP Addresses / Source Subnets
Students	Students Group	192.168.20.0/24, 192.162.201.0/24, 192.168.202.0/24
Network-Management	network management	192.168.200.0/24
Teachers	Teaching staff	192.168.30.0/24, 192.168.40.0/24, 192.168.41.0/24
Guest	guest user	192.168.31.0/24, 192.168.32.0/24
Admin	Administration Staff	192.168.35.0/24, 192.168.36.0/24

Showing 1 - 5 Total: 5 10 < Previous 1 Next >

Navigate to NSE group > Firewall > Outbound Filter Rules

Outbound Filter Rules

Filter traffic from LAN to WAN or to other subnets

Apply Filter(s)

Precedence	Name	Description	Action	Type	Protocol	Source IP Address	Mask	Source Port	Destination...	Mask	Destination...
1	Block-student-Guest	-	Deny	IP Based	any	Students	any	any	Guest	any	any
2	Block-Guest-Admin	-	Deny	IP Based	any	Guest	any	any	Admin	any	any

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

MarketApps: 60 GHz cnWave Installer App

cnMaestro 6.2.0 introduces support for onboarding 60 GHz cnWave devices through the Installer MarketApp. This enhancement extends the existing field installation workflow,

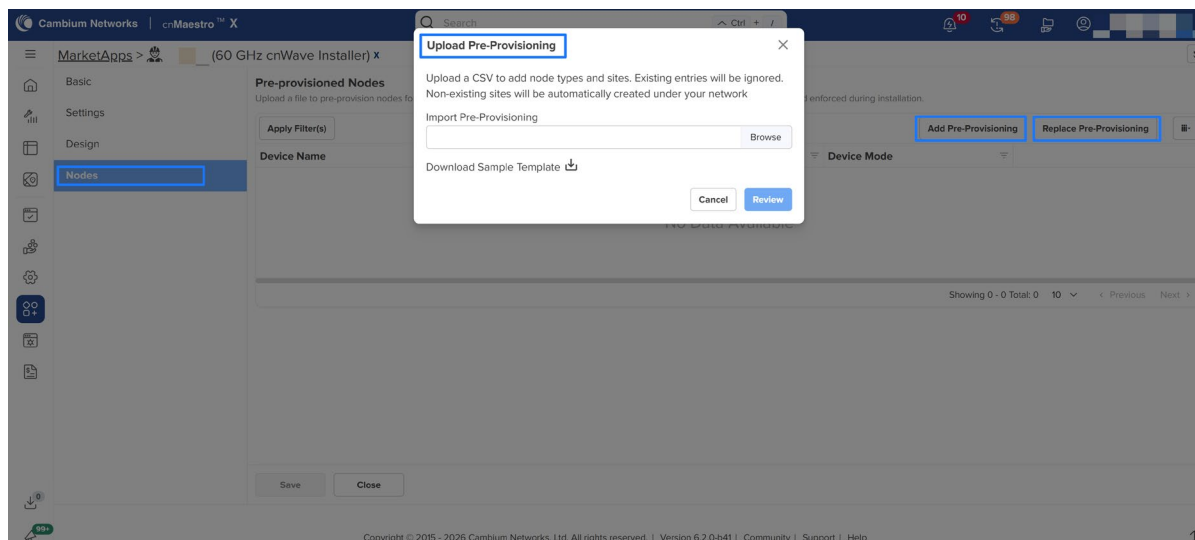
enabling installers to claim supported cnWave devices directly into cnMaestro during on-site deployment.

Using the Installer App, installers can enter the serial number or scan device details, select the deployment context configured by the MSP admin, and capture installation information as part of the onboarding process. This allows field teams to complete device installations without requiring access to the full cnMaestro administrative interface.

After onboarding, the 60 GHz cnWave device is automatically added to cnMaestro for centralized monitoring and management. Installation details captured through the Installer App are stored in the installation summary, helping administrators maintain accurate deployment records and track installation history.

Note: Before onboarding 60 GHz cnWave devices through the Installer App, the E2E controller must be onboarded first.

The top screenshot shows the 'Select App Type' dialog box in the cnMaestro interface. The dialog has fields for 'Name*' and 'Managed Account*'. Under 'Select Type', there are five app options: 'MDU Managed Wi-Fi', 'MDU Self Service Wi-Fi', 'Outdoor Hospitality Managed Wi-Fi', 'Senior Living Managed Wi-Fi', and '60 GHz cnWave Installer'. The '60 GHz cnWave Installer' app is highlighted with a blue border and a blue button. Below the dialog, a table lists installed apps: 'Enterprise Installer', 'Enterprise Installer', 'MDU Managed Wi-Fi', and 'Senior Living Managed Wi-Fi'. The bottom screenshot shows the 'Settings' page for the '60 GHz cnWave Installer' app. A search dropdown menu is open, showing a list of 60 GHz cnWave E2E-c devices. The table below the search has columns for 'User Email' and 'Validity'. The footer of the interface shows the copyright information: 'Copyright © 2015 - 2026 Cambium Networks, Ltd. All rights reserved. | Version 6.2.0-b4f | Community | Support | Help'.

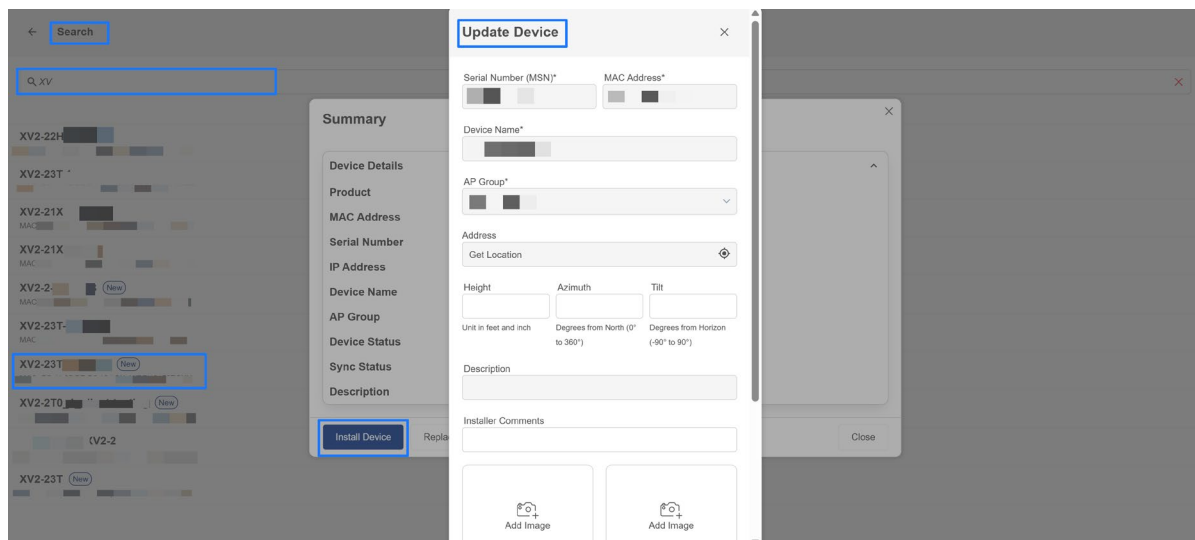


MarketApps: Installer App Enhancements

Installer App: Improved Search & Update support for existing Devices

The Installer MarketApp has been enhanced to support searching existing managed devices by Serial Number, Device Name, or MAC Address, including partial search. Administrators can now quickly locate existing devices and update installation details such as location, height, tilt, and photos.

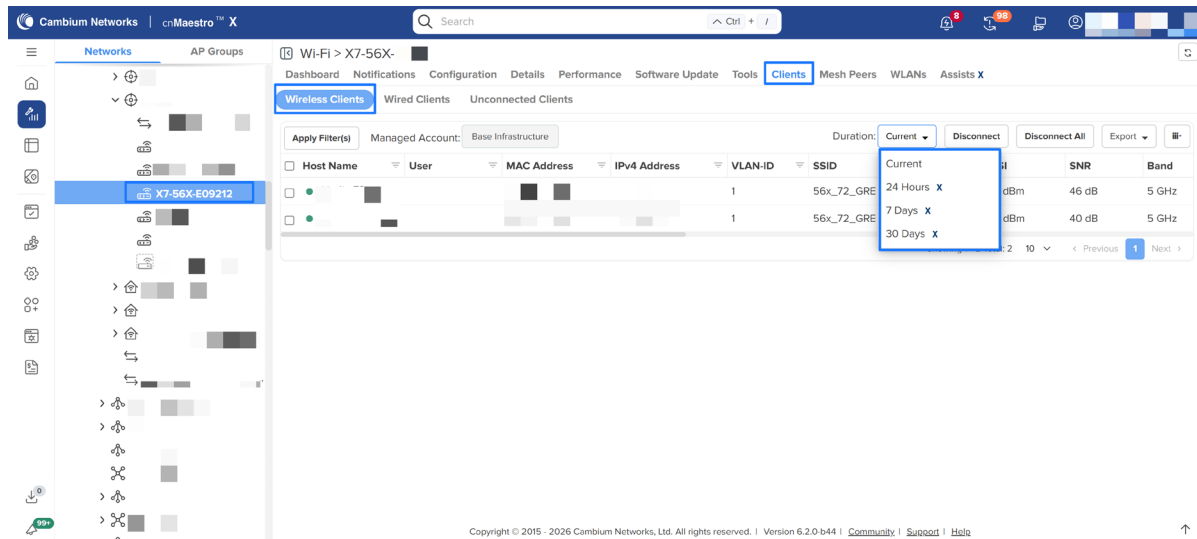
This enhancement also improves the device replacement workflow by allowing devices to be replaced while retaining the existing configuration, helping simplify installation management and ongoing maintenance.



Historical Clients detail at the AP level

This release introduces support for viewing historical client details at the individual AP level. Administrators can now review clients that were previously associated with a specific AP, helping improve visibility into past client activity and connectivity behavior.

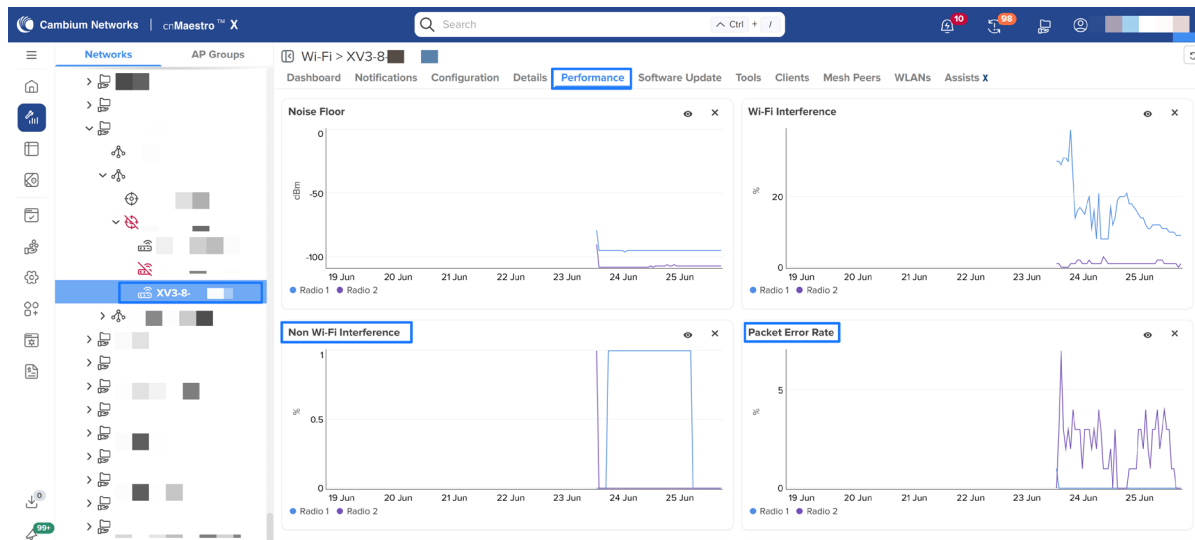
This enhancement simplifies troubleshooting by allowing administrators to investigate client history directly from the AP context, making it easier to analyze roaming, connectivity, and usage patterns over time.



Per-AP Performance Graphs for PER and Non-Wi-Fi Interference

This release introduces new RF performance information to device performance graphs, including **Packet Error Rate** and **Non-Wi-Fi Interference** time-series data.

These new graphs help administrators monitor wireless channel health over time, identify packet loss trends, and understand the impact of non-Wi-Fi interference on device performance. This enhancement improves troubleshooting visibility and helps optimize RF performance for supported devices.



Note: Wi-Fi 6 and Wi-Fi 7 devices supports Packet Error Rate, and Non-Wi-Fi Interference. Wi-Fi 5 devices support only Packet Error Rate information.

PON Enhancements

Service Profiles for ONUs

This release introduces support for viewing ONU Profiles for supported PON deployments. Administrators can review ONU profile information from cnMaestro and change the associated profile as needed, providing better visibility and control over ONU-level configuration.

This enhancement improves operational visibility and helps administrators verify and update ONU profile assignments more efficiently without needing to access the OLT directly.

Name	Serial Number	Current ONU Profile
XGS-PON-ONU		onuAnyTagProfile
G-PON-ONU		onuAnyTagProfile
XGS-PON-ONU		onuAnyTagProfile

Showing 1 - 3 Total: 3

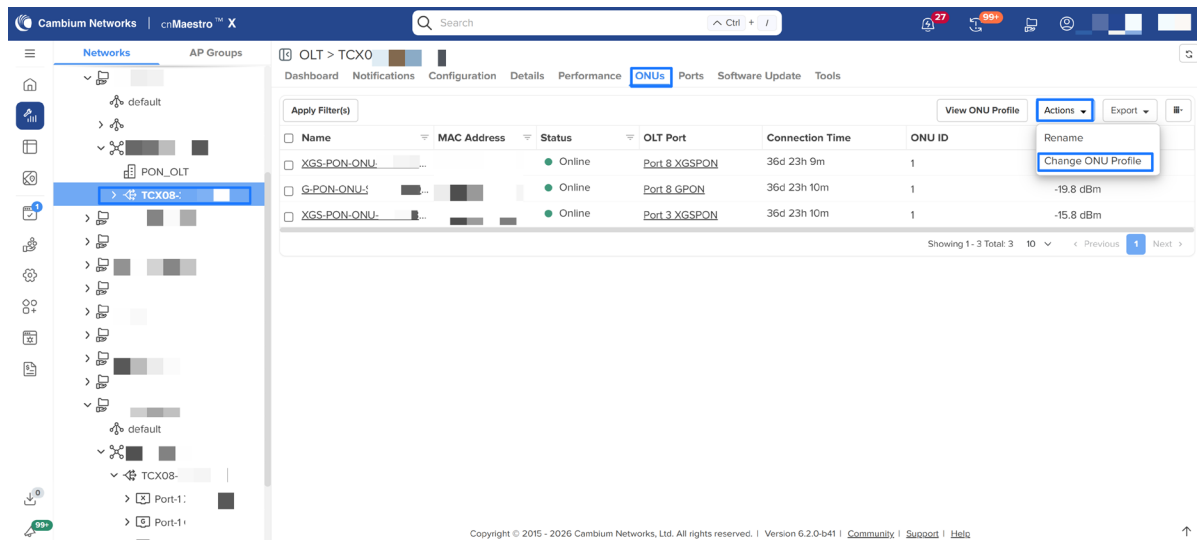
onuAnyTagProfile Profile Details

Profile Details

- Downlink: 1000
- Uplink: 1000
- Mgmt VLAN ID

Service Profile

- Eth0: anyTAGprofile(4095->4095)
- Eth0: newDefault(Untagged->Untagged)
- Eth0: VLAN2001(2001->2001)



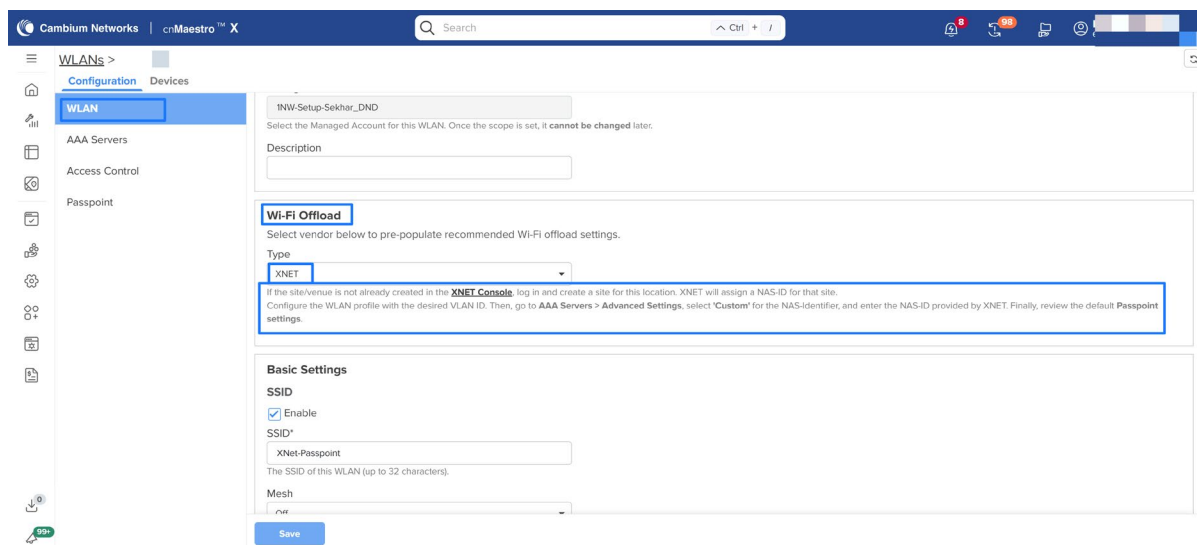
Miscellaneous Enhancements

Wi-Fi Offload - Vendor URL and Help Text

This release enhances the Wi-Fi Offload configuration workflow by adding vendor URL support and updated help text for Wi-Fi offload vendors.

Administrators can now view vendor-related URL information while configuring Wi-Fi Offload settings under WLANs, making it easier to reference vendor-specific details during setup. The updated help text provides clearer guidance for selecting and configuring supported Wi-Fi offload vendors.

This enhancement improves usability, reduces configuration ambiguity, and helps administrators complete Wi-Fi Offload setup more efficiently.

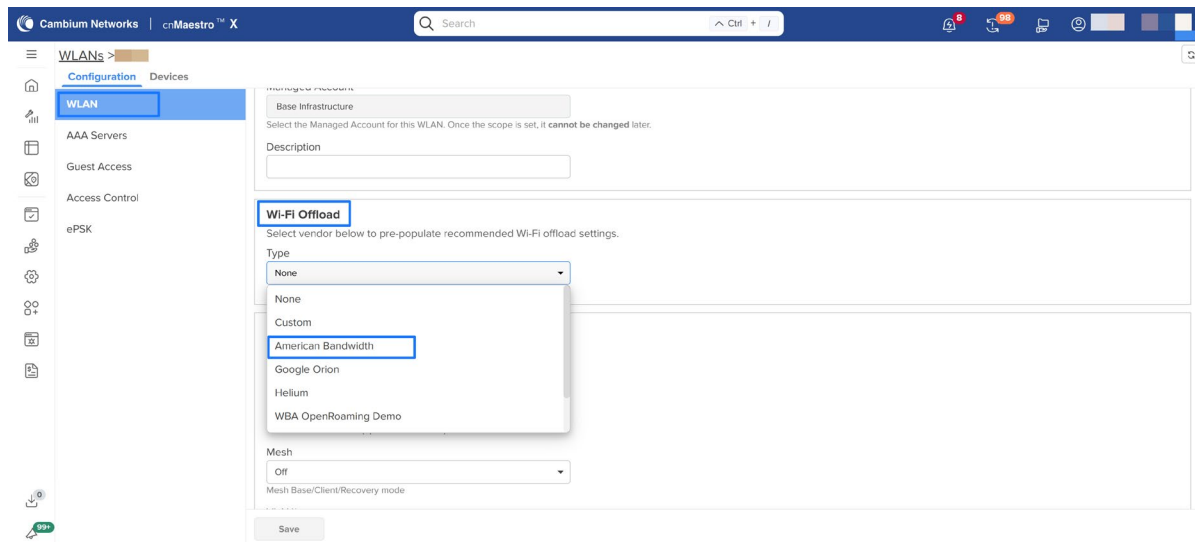


Wi-Fi Offload American Bandwidth support

This release adds a Passpoint configuration profile for **American Bandwidth** under Wi-Fi Offload settings. Administrators can select the American Bandwidth vendor profile to

populate the recommended Passpoint parameters, reducing the manual configuration required for Wi-Fi offload deployments.

This enhancement simplifies Passpoint setup, improves configuration consistency, and helps administrators onboard American Bandwidth Wi-Fi offload services more efficiently.

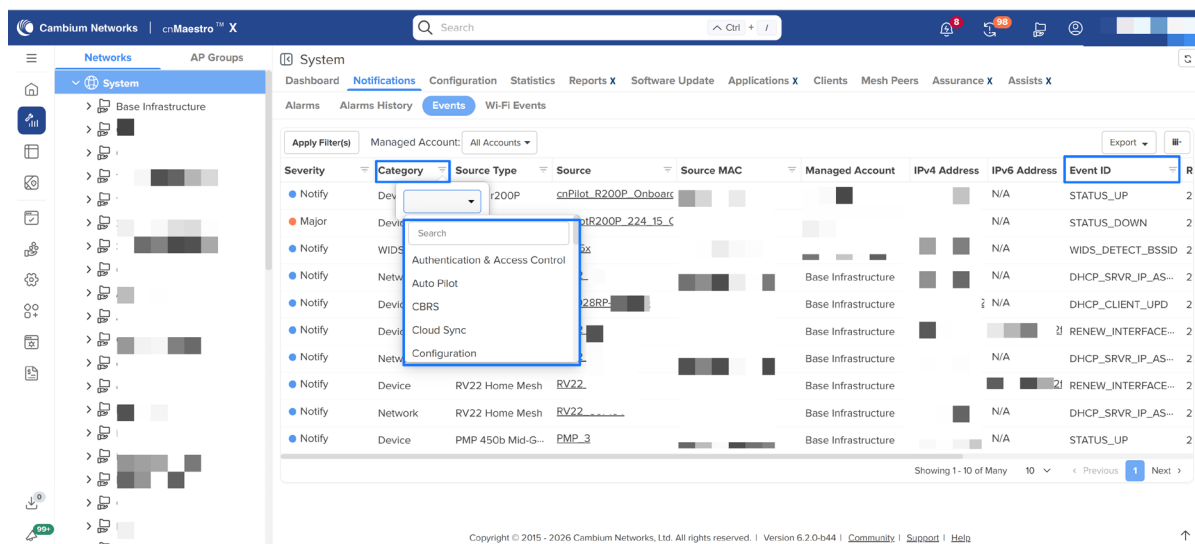


Enhancements to Notifications > Events: Grid Structure and Column Mapping

This release enhances the Notifications grids with updated column names, ordering, filtering, and mapping to improve consistency across the UI, exports, and reports.

- The **Name** column in **Alarms**, **Alarm History**, **Events**, and **Wi-Fi Events** is now renamed to **Event Type**.
- In **Alarm History**, the **Clear** column is renamed to **Cleared Time** and moved next to the **Status** column.
- The **Events** grid has also been updated with new column mapping definitions, the previous **Event Type** column has been removed where applicable, and the filters for the **Category** column have been changed.

These updates provide clearer events and alarm information, improve alignment between grid views and exported data, and make notification records easier to review and interpret.



API Updates X

Deprecated APIs

Request Method	Path	Deprecated In	Sunset In	Replacement	Details
Guest Access API					
GET	/portals	5.2.0	6.3.0	/api/v2/easypass	The Guest Access Portal feature has been deprecated, and as a result, the associated RESTful APIs have also been deprecated.
GET	/portals/{portalName}	5.2.0	6.3.0	/api/v2/easypass/{portalName}	
GET	/portals/{portalName}/events	5.2.0	6.3.0	/api/v2/easypass/{portalName}/sessions/login_events	
PUT	/portals/{portalName}/whitelist	5.2.0	6.3.0	/api/v2/easypass/{portalName}/configuration/allowed_domains	
GET	/portals/{portalName}/voucher_plans	5.2.0	6.3.0	/api/v2/easypass/{portalName}/voucher_plans	
GET	/portals/{portalName}/vouchers/{voucherPlan}	5.2.0	6.3.0	/api/v2/easypass/{portalName}/voucher_plans/{voucherPlan}/vouchers	
POST	/portals/{portalName}/vouchers/{voucherPlan}/generate	5.2.0	6.3.0	/api/v2/easypass/{portalName}/voucher_plans/{voucherPlan}/vouchers/generate	
cnArcher Installation Summary					
GET	/api/v2/cnarcher/installation/summary	6.0.0	6.3.0	/api/v2/installation/summary	Added new APIs with app type filter to retrieve installation summary details for all supported app types (cnArcher, enterprise-installer, etc.) under a site or tower.
GET	/api/v2/cnarcher/installation/summary/{mac}	6.0.0	6.3.0	/api/v2/installation/summary/{mac}	

Deprecated Fields

Request Method	Path	Field Name	Deprecate d In	Sunset In	Replacement	Details
AP Groups						
GET	/wifi_enterprise/ap_groups	auto_rf_channel_selection_mode	5.2.1	6.3.0	N/A	These fields are no longer relevant for Auto-RF configuration.
GET	/wifi_enterprise/ap_groups	channel_utilization_threshold	5.2.1	6.3.0	N/A	
POST	/wifi_enterprise/ap_groups	auto_rf_channel_selection_mode	5.2.1	6.3.0	N/A	
PUT	/wifi_enterprise/ap_groups/{ap_group_name}	auto_rf_channel_selection_mode	5.2.1	6.3.0	N/A	This field is no longer relevant for Auto-RF configuration.
POST	/api/v2/wifi_enterprise/ap_groups	shared	6.0.0	6.3.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.3.0
POST	/api/v2/wifi_xirrus/ap_groups	shared	6.0.0	6.3.0	N/A	
Wi-Fi Enterprise						
GET	/devices/clients	ap_mac	5.0.0	6.3.0	device_mac	The ap_mac field is deprecated and replaced with a new generic term, device_mac , to accommodate other non-Wi-Fi device types, such as NSE. For a similar reason, the rx_bytes and tx_bytes fields have also been taken out of the radio

Request Method	Path	Field Name	Deprecate d In	Sunset In	Replacement	Details
						property of an AP device.
GET	/devices/wired_clients	ap_mac	5.0.0	6.3.0	device_mac	The ap_mac field is deprecated and replaced with a new generic term, device_mac , to accommodate other non-Wi-Fi device types, such as NSE.
GET	/devices/clients/summary	rate	5.2.1	6.3.0	tx_rate	For consistency , the rate field has been deprecated and replaced with a new field, tx_rate, alongside the introduction of a corresponding rx_rate field.
GET	/devices/clients/summary	client_type	5.2.1	6.3.0	os	The client_type field was capturing the OS information, which was incorrect. So replaced it with a new field os.
Switch Groups						
GET	/api/v2/cnmatrix/switch_group_s_ports/{switch_group_name}	nid	5.2.5	6.3.0	network	Renamed the deprecated fields to

Request Method	Path	Field Name	Deprecate d In	Sunset In	Replacement	Details
GET	/api/v2/cnmatrix/switch_group s_ports/{switch_group_name}	tid	5.2.5	6.3.0	tower	relevant ones.
GET	/api/v2/cnmatrix/switch_group s_ports/{switch_group_name}	mcid	5.2.5	6.3.0	managed_acc ount	
GET	/api/v2/cnmatrix/switch_group s_ports/{switch_group_name}	eType	5.2.5	6.3.0	N/A	eType is redundant as the API endpoint is specific to cnMatrix itself.
POST	/api/v2/cnmatrix/switch_group s	shared	6.0.0	6.3.0	N/A	The shared field is deprecated and will be removed in version 6.3.0
Events API						
GET	/api/v2/events	offset total	6.0.0	6.3.0	continuation_t oken	The offset request parameter is deprecated in 6.0.0 and will be removed in version 6.3.0 release. Please use the continuation_token request parameter instead. The total response field is deprecated in 6.0.0 and will be removed in version 6.3.0 release.
Device Performance API						

Request Method	Path	Field Name	Deprecate d In	Sunset In	Replacement	Details
GET	/api/v2/devices/{mac}/performance	offset total	6.0.0	6.3.0	continuation_token	The offset request parameter is deprecated in 6.0.0 and will be removed in version 6.3.0 release. Please use the continuation_token request parameter instead. The total response field is deprecated in 6.0.0 and will be removed in version 6.3.0 release.
NSE Threats API						
GET	/api/v2/devices/nse/{mac}/threats	offset total	6.0.0	6.3.0	continuation_token	The offset request parameter is deprecated in 6.0.0 and will be removed in version 6.3.0 release. Please use the continuation_token request parameter instead. The total response field is deprecated in 6.0.0 and will be removed in version 6.3.0 release.

Request Method	Path	Field Name	Deprecate d In	Sunset In	Replacement	Details
WLANs						
POST	/api/v2/wifi_enterprise/wlans	ga_cn_portal_name	6.0.0	6.3.0	use /api/v2/easypass/{portalName}/wlans to attach and detach cnmaestro portal types.	The ga_cn_portal_name field is deprecated in 6.0.0 and will be removed in release 6.3.0. The cnmaestro value for the ga_portal_mode field is deprecated in 6.0.0 and will be removed in release 6.3.0. Please use /api/v2/easypass/{portalName}/wlans to attach and detach cnmaestro portal types.
PUT	/api/v2/wifi_enterprise/wlans/{wlan_name}	ga_cn_portal_name	6.0.0	6.3.0		
POST	/api/v2/wifi_enterprise/wlans	shared	6.0.0	6.3.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.3.0
Access Control Policy						
POST	/api/v2/wifi_enterprise/access_control	shared	6.0.0	6.3.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.3.0
NSE Groups						
POST	/api/v2/nse/nse_groups	shared	6.0.0	6.3.0	N/A	The shared field is deprecated in 6.0.0 and

Request Method	Path	Field Name	Deprecate d In	Sunset In	Replacement	Details
						will be removed in version 6.3.0
Configuration Templates						
POST	/api/v2/device/configuration/templates	shared	6.0.0	6.3.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.3.0
Devices Statistics						
GET	/api/v2/devices/statistics	mode	6.1.0	6.3.0	type	The mode filter is deprecated and will be removed in 6.3.0. Use type filter instead.
GET	/api/v2/devices/{mac}/statistics	mode	6.1.0	6.3.0	type	
60 GHz cnWave Software Upgrade						
POST	/api/v2/cnwave60/networks/{network_id}/jobs/device/update	Torrent option in download_protocol	6.1.0	6.1.0	Use http option under download_protocol	The torrent option has been removed from the download_protocol field. Only http is now supported. Requests specifying torrent will be rejected with an error. If download_protocol is not specified, it defaults to http.

Update notice for existing APIs

Request Method	Path	Details
Device Performance API		

Request Method	Path	Details
GET	/api/v2/devices/{mac}/performance	Added support for noise_floor, interference, non_wifi_interference, packet_error_rate for Enterprise Wi-Fi devices
Devices API		
GET	/api/v2/devices	Added profile_attached query parameter to filter devices by Profile name. The attached profile name is returned in the profile_attached response field.
Installation Summary API		
GET	/api/v2/installation/summary	Added support to retrieve installation summary details for cnwave60-installer app type. Optionally filter by app type using the type=cnwave60-installer query parameter.
GET	/api/v2/installation/summary/{mac}	Added support to retrieve installation summary details for a specific cnWave60 device.
NSE Groups API		
POST	/api/v2/nse/nse_groups	The snort_vrt_rule_category field now uses the unified Snort 3 category set for both NSE 3000 and NSE 4000. Legacy Snort 2-only category names (e.g. backdoor, bad-traffic, botnet-cnc) are no longer accepted and will return a validation error. Added support for tailscale configuration (enable, auth_key, accept_routes, advertise_routes) under NSE Groups. The user groups are supported in src and dest fields and comma separated ports are allowed for outbound firewall filter rules only. The name field is now mandatory in Port Forward, NAT One-to-One, and NAT One-to-Many rules. The name must be globally unique across all three rule types, start with a letter or underscore, and contain only alphanumeric characters and underscores. Requests missing the name field or containing duplicate names will be rejected with a validation error.
PUT	/api/v2/nse/nse_groups/{nse_group_name}	
GET	/api/v2/nse/nse_groups	The snort_vrt_rule_category field in responses now reflects the unified Snort 3 category set. Existing NSE 3000 profiles have been automatically migrated. Added support for tailscale configuration (enable, auth_key, accept_routes, advertise_routes) under NSE Groups. The user groups are supported in src and dest fields and comma separated ports are allowed for outbound firewall filter rules only. The name field is now returned for Port Forward, NAT One-to-One, and NAT One-to-Many rules. Existing rules without a name have been back-filled by migration using auto-generated names (e.g. dnat_wan1_pf_rule_1).
GET	/api/v2/nse/nse_groups/{nse_group_name}	

New APIs added in 6.2.0

Request Method	Path	Details
Market Apps API		
GET	/api/v2/marketapps	Added API to retrieve a list of all market apps. Optionally filter by managed account and app type.
POST	/api/v2/marketapps	Added API to create a new market app. Supports managed-wifi, self-service-wifi, senior-living, and outdoor-hospitality app types.
GET	/api/v2/marketapps/{app_name}	Added API to retrieve the full configuration of a specific market app including branding and type-specific settings.
PUT	/api/v2/marketapps/{app_name}	Added API to update market app configuration including description, branding, and type-specific settings.
DELETE	/api/v2/marketapps/{app_name}	Added API to delete a market app by name.
DELETE	/api/v2/msp/managed_accounts/{managed_account}/marketapps/{app_name}	Added MSP API to delete a market app for a managed account.
PUT	/api/v2/marketapps/{app_name}/logo	Added API to upload a logo image for a market app. Supports PNG and JPEG formats up to 100 KB.
GET	/api/v2/marketapps/{app_name}/units	Added API to retrieve all units associated with a market app, including device mapping, VLAN, and state information.
PUT	/api/v2/marketapps/{app_name}/units	Added API to add or replace units in a market app. Supports bulk add and replace operations.
PUT	/api/v2/marketapps/{app_name}/units/{unit}	Added API to update the VLAN or device mapping for a specific unit in a market app.
GET	/api/v2/marketapps/{app_name}/members	Added API to retrieve all members (property managers) associated with a market app.
POST	/api/v2/marketapps/{app_name}/members	Added API to add or remove members from a market app by email.
PUT	/api/v2/marketapps/{app_name}/members/resend-invite	Added API to send invitation emails to all users or resend them to specific users.
PUT	/api/v2/marketapps/{app_name}/units/{unit}/resend-invite	Added API to resend the invitation email with credentials for a specific unit.

Supported Cambium Products

cnMaestro supports the following Cambium Networks products. The software versions are the **minimum required** to use cnMaestro (not the recommended versions).

Family	Model	Version
60 GHz cnWave	V1000	1.0
	V2000	1.2.2-beta3
	V3000	1.0
	V5000	1.0
	V5000i	1.8
	V2000i	1.8
cnMatrix	EX2000/EX1000	2.0.4-r1
	EX3000	5.0.1
	EX3024-F	6.0-r2
	EX3030RM-P	6.2.0
	EX3052RM-P	6.2.0
cnPilot Home	cnPilot R200, R200P	4.4.2-R2
	cnPilot R201, R201P	4.4.2-R2
	cnPilot R190V, R190W	4.4.2-R2
	cnPilot R195P	4.5.2
	cnPilot R195W	4.7
cnRanger	Sierra 800	1.0.1.0-r1
	Tyndall 101	1.0.1.0-r1
	Tyndall 201	2.0.0.0-r1
cnReach	N500	5.2.17e
cnVision	Hub 360r, FLEXr	4.6
	Client Micro, Mini, Maxr	4.6
cnWave 5G Fixed	B1000 (BTS)	2.0
	C100 (CPE)	2.0
Edge Controller	N/A	1.0.0
Enterprise Wi-Fi	cnPilot e400/e500	2.5.2-r3
	cnPilot e410/e430w/e600	3.5.2-R4
	cnPilot e501S/e502S	3.2.1-r6
	cnPilot e700	3.8
	cnPilot e425/e505	4.0-r17
	cnPilot e510	3.11.4-r9
	XE3-4	6.4
	XE3-4TN	6.5.1
	XE5-8	6.4.1-r15

Family	Model	Version
	XV2-2X	6.1
	XV2-2T0	6.4
	XV2-2T1	6.4.1-r15
	XV2-21X	6.5
	XV2-22H	6.5
	XV2-23T	6.5
	XV3-8	6.0
	X7-35X	7.0-b14
	X7-53X	7.1.1
	X7-55X	7.1.1
	X7-56X	7.1.2
ePMP 1000 Hotspot	ePMP 1000 Hotspot	2.5.2-r3
ePMP	ePMP 1000, Force 180/200	2.6.2
	ePMP 2000	3.0.1
	ePMP Elevate XM/XW	3.2
	ePMP Force 190	3.5
	ePMP Force 300	4.1
	ePMP PTP 550	4.1.1
	ePMP Force 130 5 GHz	4.3.2
	ePMP 3000L	4.3.2
	ePMP Elevate SXGLITE5, LHG5	4.3.2.1
	ePMP Force 130 2.4 GHz	4.4
	ePMP Force 300-19, 19R, 13	4.4
	ePMP 3000	4.4.1
	ePMP PTP 550 E	4.4.2
	ePMP MP 3000	4.5
	ePMP Force 300-13L	4.5.2
	ePMP Force 300-13LC, 22L, 25L	4.6
	ePMP Force 200L	4.7.0
	ePMP 4000, Force 400 GPS, 400 CSM, 425	5.1.0
	ePMP 4600, ePMP4600L, ePMP Force 4600C, ePMP Force 4525, ePMP Force 4500, ePMP Force 4625	5.4.0
NSE	NSE3000	1.2-b5
	NSE4000	2.0-r13
PMP	PMP 450i, PMP 450, PMP 450m, PMP 430 SM	22.1.2
	PTP 450, and PTP 450i	22.1.2

Family	Model	Version
	MicroPoP Omni/Sector	22.1.2
	PMP 450v	23.0
PON	TCX16 - 16 port OLT	1.1.0
	TCX08 - 8 port OLT	
	SGX00 - Indoor GPON ONT	
	SXX00 - Indoor XGSPON ONT	
	SGT00 - Outdoor GPON ONT	
	SXT00 - Outdoor XGSPON ONT	
PTP	PTP 650	01-47
	PTP 670 (650 Emulation)	01-47
	PTP 670, PTP 700	02-67
PTP 820/850	PTP 820C, 820E, 820F, 820G, 820S	11.9
	PTP 850C, 850E	11.9
RV22 Home Mesh	RV22 Home Mesh	1.0
Xirrus (Enterprise Wi-Fi)	XA4-240	8.7.0
	XD2-230	8.7.0
	XD2-240	8.7.0
	XD4-130	8.7.0
	XH2-120	8.7.0
	XH2-240	8.7.0
	XR-620	8.7.0
	XR-630	8.7.0
	XR-2226	8.7.0
	XR-2236	8.7.0
	XR-2247	8.7.0
	XR-2426	8.7.0
	XR-2436	8.7.0
	XR-2447	8.7.0
	XR-4426	8.7.0
	XR-4436	8.7.0
	XR-4447	8.7.0

Supported Browsers

cnMaestro supports the following browsers:

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

Significant Fixes

The following issues have been fixed:

ID	Details
CNSSNG-53351	Incorrect product naming for ePMP 4500L AP
CNSSNG-50157	[Radio Modes] The help text for the radio mode is displaying incorrect information.
CNSSNG-49996	EasyPass Azure login show username in clients info
CNSSNG-46305	Spanning Tree Overrides not working for the switch groups created using RESTful API
CNSSNG-38730	Device Tools Wi-Fi Analyzer report SNR Column Sorting does not work

Known Issues

This section lists the known issues in the cnMaestro releases:

** Reported in Release 6.1.0*

ID	Details
CNSSNG-52711*	Bulk edit on hybrid ports with VLAN append and delete operations are not reflecting the VLANs immediately under <i>Switch groups > Configuration > Ports</i> .
CNSSNG-52602*	Sign In Message, Access Granted Message, Authentication failed and Logout failed to be removed from cnMaestro as they are not supported in NSE device UI.
CNSSNG-52570*	NSE Network LAN page is loading slow when the Cellular WAN is enabled.
CNSSNG-52453*	Switch Group save failed after deleting an additional port channel on a cnMatrix device.
CNSSNG-52196*	VLANs are not reflected in Switch ports grid upon adding/deleting VLANs from switch group in Onboarding page.
CNSSNG-52043*	Inter-VLAN Routing column incorrectly showed Disabled for newly added VLANs, even when Enabled was selected during bulk VLAN configuration in NSE group.
CNSSNG-52003*	Restrict AP replacement when source AP is associated with MarketApp (MDU Wi-Fi).
CNSSNG-51217	Intermittently DNS events not getting unblocked automatically and events not generated.
CNSSNG-51123	Virtual WAN configuration not removed from View Device Configuration after NSE downgrade from 2.1.
CNSSNG-51033	Selected switch filter not applied when navigating to Statistics tab from Switch Groups dashboard.

ID	Details
CNSSNG-50422	Email Notifications take more than 10 minutes for processing after generating the alarms.
CNSSNG-50282	Switches tab is listing device of another switch group with same name but different scope.
CNSSNG-49936	Port configuration from onboarding page is not reflected after the device is onboarded.
CNSSNG-49866	Unable to search devices using IPv6 addresses from the Search Devices option.
CNSSNG-49726	Installer MarketApp: Device Overrides are not getting applied if different device model is replaced.
CNSSNG-47877	Inconsistent Component Carrier sequence across cnMaestro.
CNSSNG-47773	In Enterprise view, restrict alarms related to Enterprise AP, NSE, and cnMatrix devices only.
CNSSNG-47698	Notification template name should update with email ID after migration.
CNSSNG-47207	Switch Group rename causes cnMatrix devices to go Not In Sync.
CNSSNG-46593	Unsupported alarms are displaying for devices for cnMatrix, Wi-Fi AP and PON.
CNSSNG-46051	When two devices are added as a hub and use the same NSE groups, both devices get a role as a responder.
CNSSNG-45803	Changing the 'Time Range' from NSE Site level > Applications does not update the dashboard results when the Network with special characters.
CNSSNG-45149	Golay config is set to Auto configuration when we change Golay from Maps.
CNSSNG-45087	cnMaestro shows IoT Device Identification in Security mode, even if the device is not reporting any stats.
CNSSNG-45063	Error "Incompatible assigned channel for link" is seen when trying to change the channel of the DN-DN offline link.
CNSSNG-45062	Error "Given link Name is not in any group" is seen when trying to change channel for the CN offline link.
CNSSNG-44989	The Site to site VPN checkbox should be disabled for old customers if they have not enabled it earlier.
CNSSNG-44758	"Previous CH req in progress" error is seen when the change channel operation is done from maps with an offline link included in the group.
CNSSNG-44756	The backup link is not included in the group channel of a sector, even though it is in the same sector.
CNSSNG-44747	Error messages need to be modified for the change channel operation of the offline link.

ID	Details
CNSSNG-44623	Operator User in both Main and MSP should be able to view the Auto VPN Config and Dashboards, as well as the NSE Groups.
CNSSNG-44564	Handling config sync failures in Auto VPN config push.
CNSSNG-41787	Spare device showing duplicate vulnerability data at the system level.
CNSSNG-41600	HA State goes to fault when no clients are connected.
CNSSNG-41503	Unable to see "POWER BOOTLOOP detected" event.
CNSSNG-40814	Port 6 should be shown as HA in the dashboard port status.
CNSSNG-36782	Home sites are not listed while moving devices from the inventory page.
CNSSNG-30927	Modify the remote subnet and local subnet fields under IPsec to have the option to enter the subnet in list form.
CNSSNG-21396	Issues related to cnMatrix onboarding overrides.

Where to Get Help

There are several places to get help with cnMaestro.

- **[Cambium Community](#)**: The cnMaestro Forum provides the best place to ask questions and get up-to-date information.
- **[Cambium Support](#)**: The Cambium Support team is available 24/7 to answer questions and resolve issues.