Cambium Networks™

RELEASE NOTES

cnMaestro™

Release 6.1.0

Contents

Introduction

The cnMaestro™ 6.1.0 release introduces a new set of exciting features and improvements.

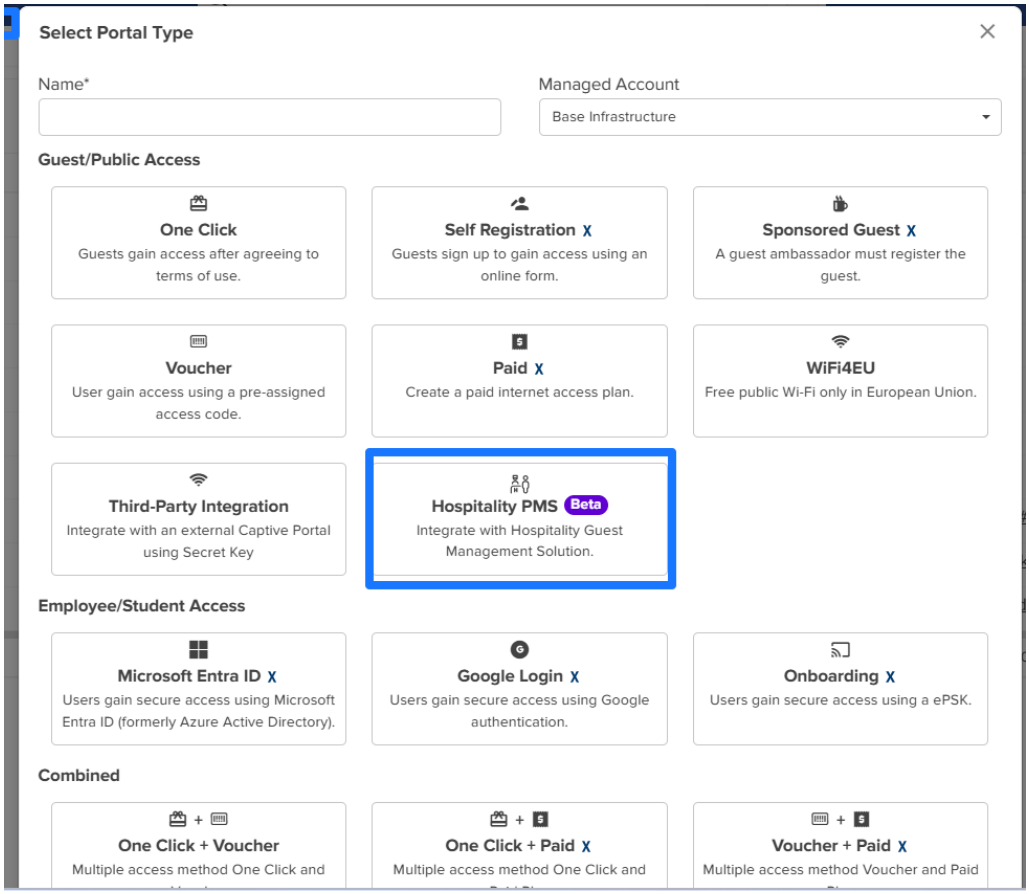
Important: Web Browser
Restart your browser or clear the browser cache with a hard reload if you have UI problems after the 6.1.0 update.

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

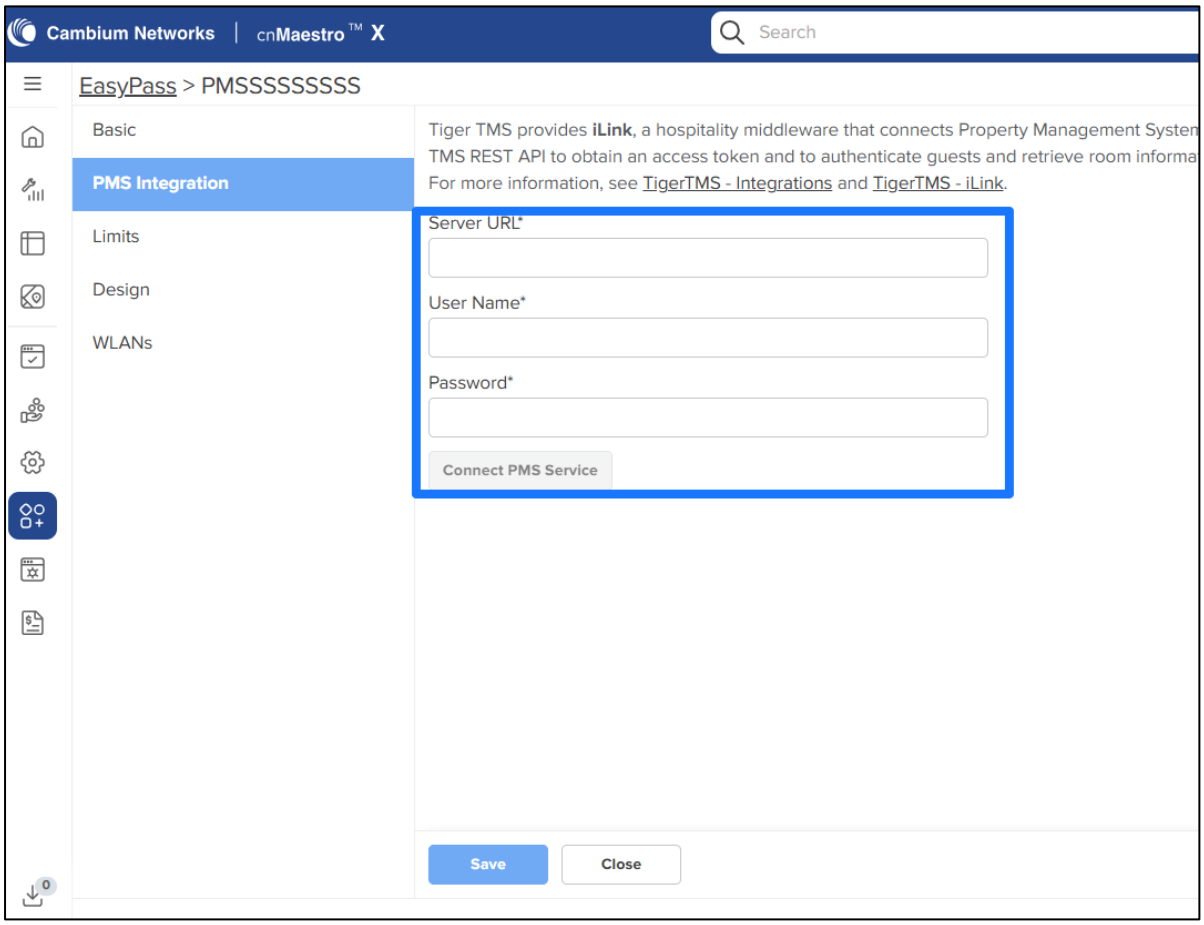
EasyPass: Hospitality PMS Integration Beta

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 Beta

This release introduces integration with Teltonika LTE modems.

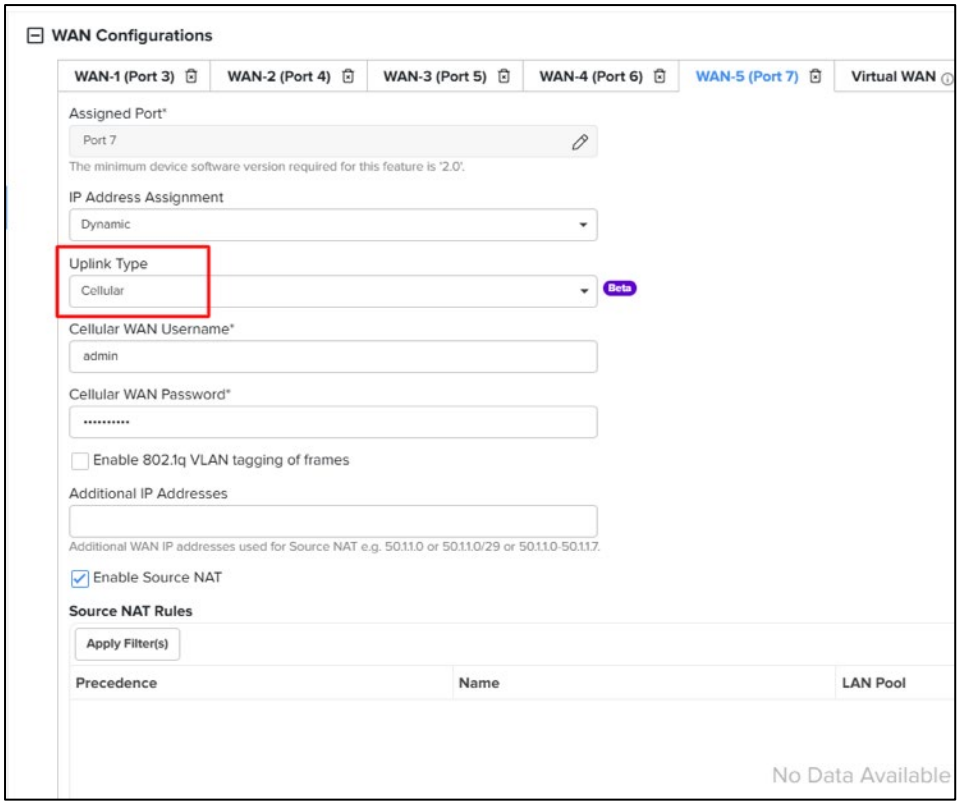
If the NSE is connected behind a Teltonika modem, it can fetch cellular statistics from the modem and display them in cnMaestro.

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.

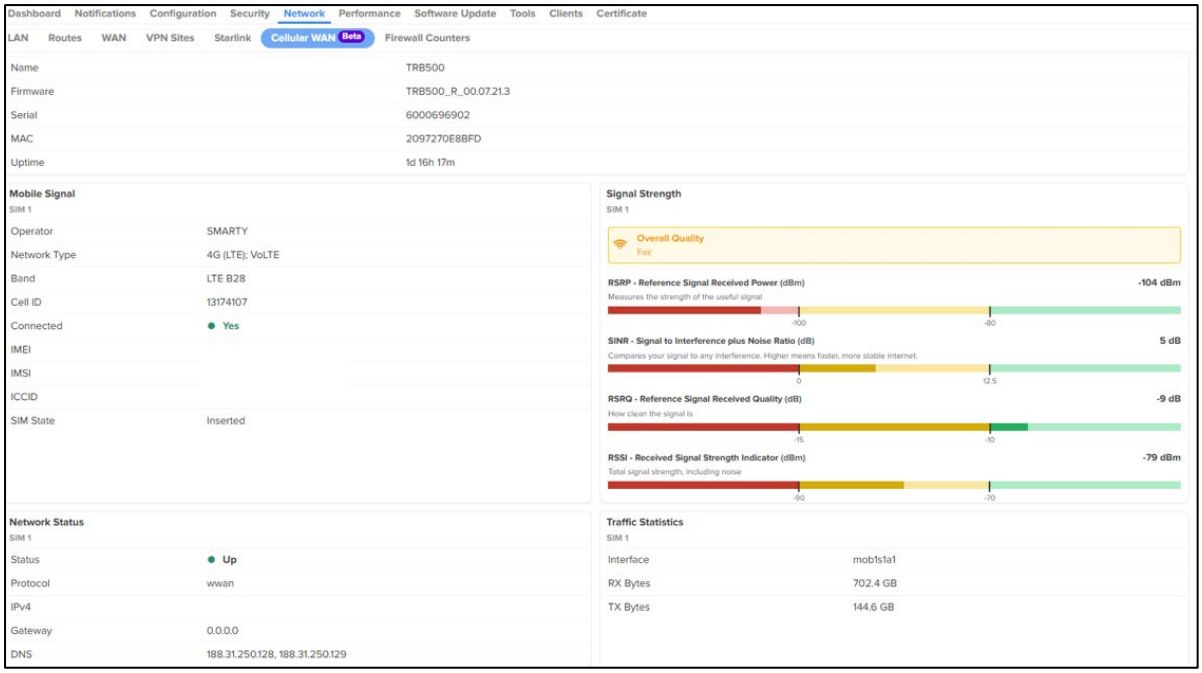
Note: This feature requires NSE devices running software version **2.2 or later.**



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



2FA over Wireguard

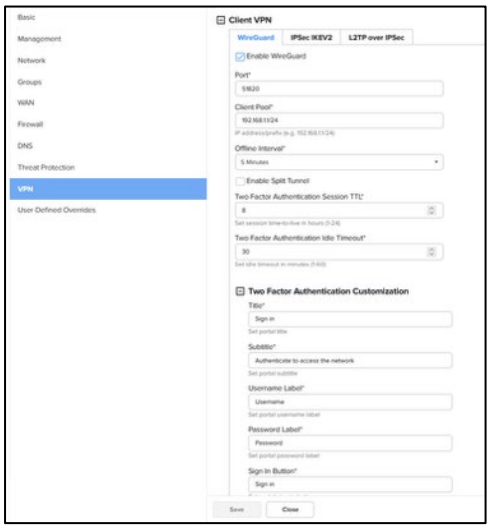
This release introduces two-factor authentication for WireGuard.

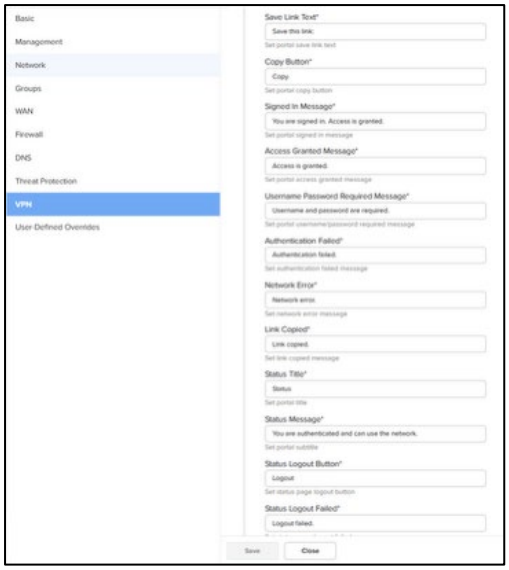
The NSE WireGuard remote VPN solution implements two-factor authentication in two steps:

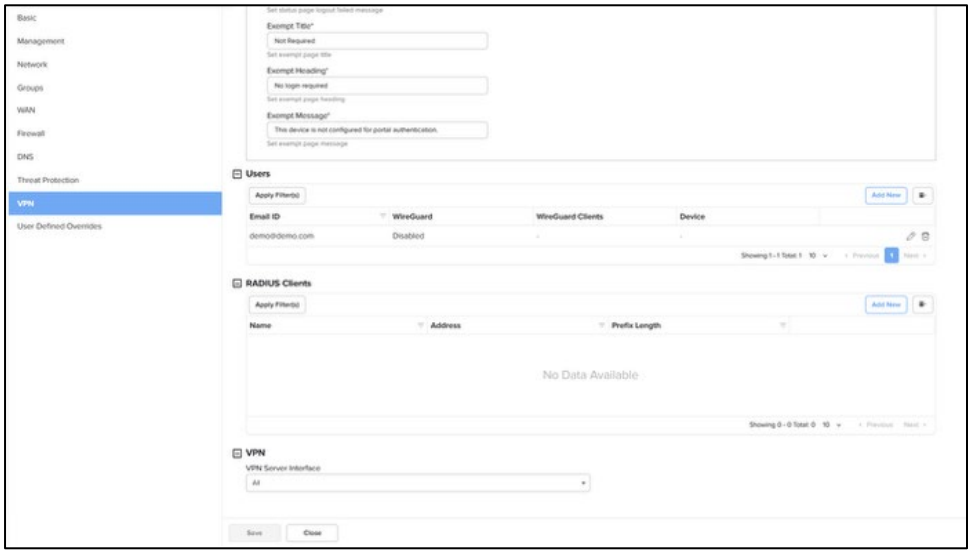
1. WireGuard cryptographic keys are required to establish the VPN tunnel (something you have).
2. After the tunnel is established, the user must authenticate using a username and password before traffic forwarding is allowed (something you know).

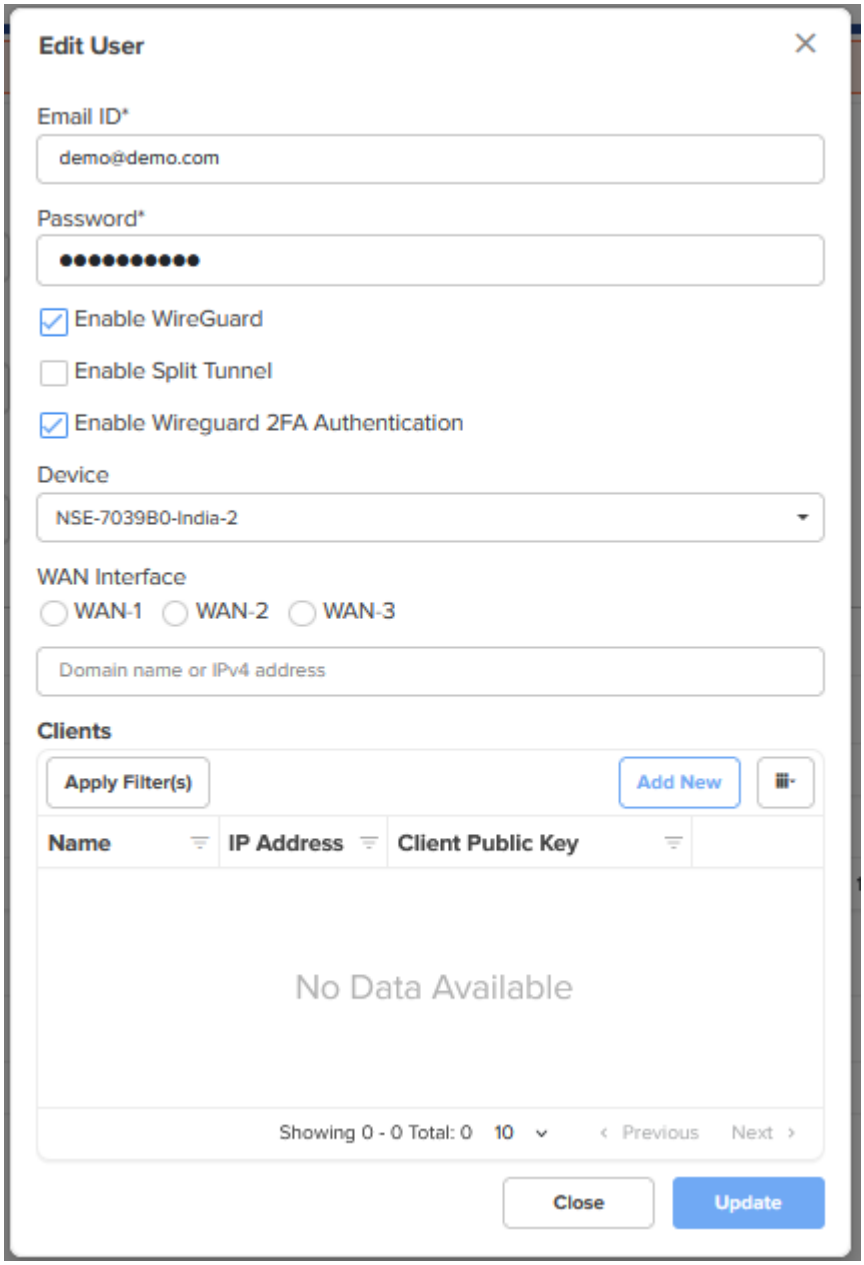
By requiring both the VPN configuration with keys and user credentials, the NSE ensures that access is granted only after two independent authentication factors are verified.

The user can enable two-factor authentication on a per-client basis.



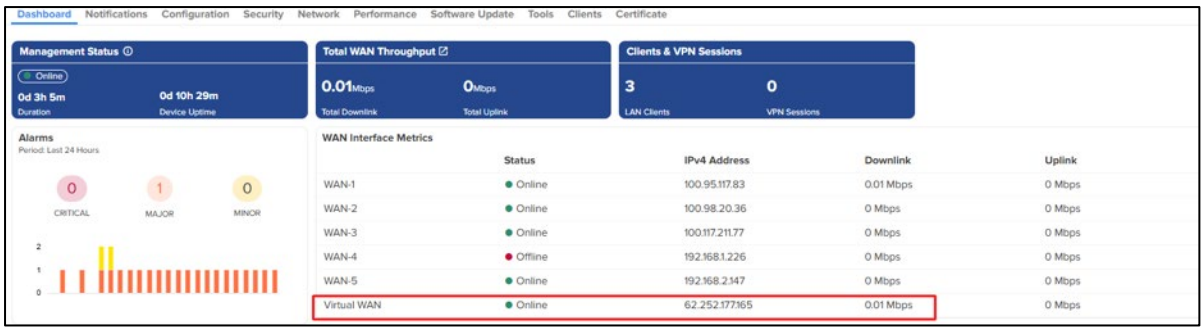

Basic
Management
Network
Groups
WAN
Firewall
DNS
Threat Protection
VPN
User Defined Overrides
Save Link Text*
Save this link:
Copy Button*
Copy
Signed In Message*
You are signed in. Access is granted.
Access Granted Message*
Access is granted.
Username Password Required Message*
Username and password are required.
Authentication Failed*
Authentication failed.
Network Error*
Network error.
Link Copied*
Link copied.
Status Title*
Status
Status Message*
You are authenticated and can use the network.
Status Logout Button*
Logout
Status Logout Failed*
Logout failed.
Save
Close


Basic
Management
Network
Groups
WAN
Firewall
DNS
Threat Protection
VPN
User Defined Overrides
Exempt Title*
Not Required
Exempt Heading*
No login required
Exempt Message*
This device is not configured for portal authentication.
Users
Apply Filter(s)
Add New
Email ID
WireGuard
WireGuard Clients
Device
demo@demo.com
Disabled
RADIUS Clients
Apply Filter(s)
Add New
Name
Address
Prefix Length
No Data Available
VPN
VPN Server Interface
All
Save
Close

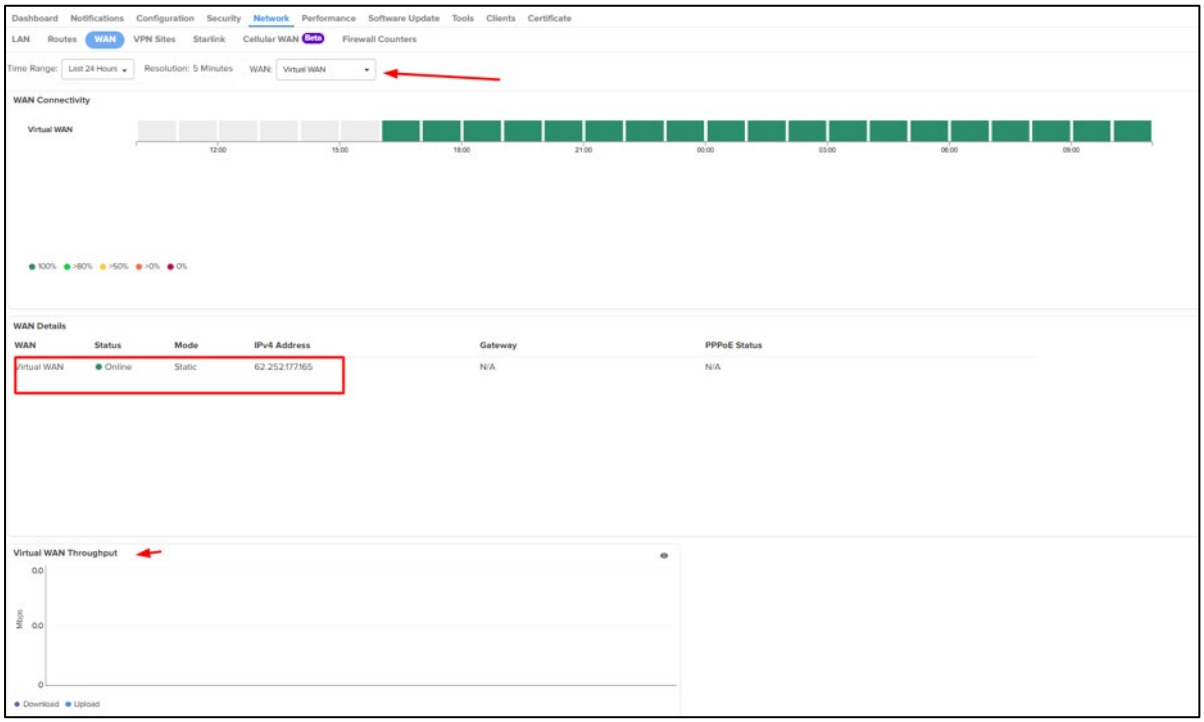


Virtual WAN Status

- In the previous release, we introduced the Virtual WAN feature on NSE. In this release, we have added Virtual WAN statistics.
- On the NSE dashboard, users can now view the status of the Virtual WAN interface, verify whether it is up or down, and confirm if traffic is being forwarded by checking the uplink and downlink counters.



On the network WAN page, you can view the usage of the virtual WAN link



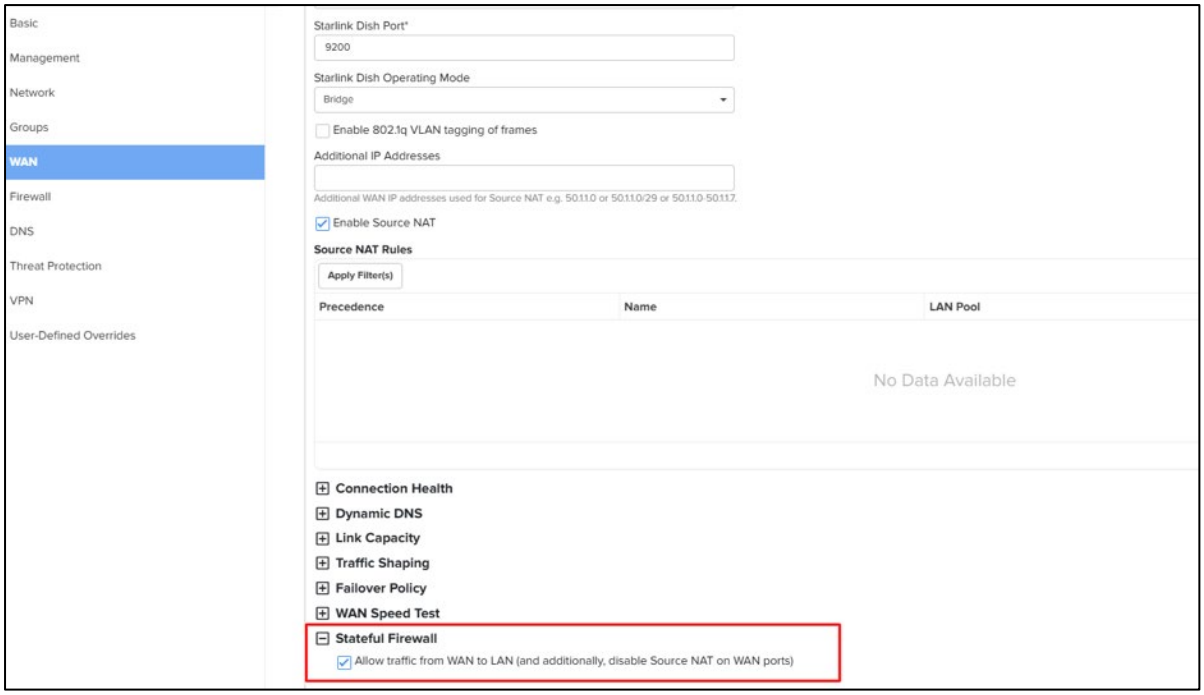
Per-WAN Firewall

In some deployments, the uplink router handles NAT, and the NSE operates mainly as a router.

If the firewall remains enabled on the NSE, the uplink router may not be able to reach the LAN subnets behind the NSE

To address this, in **6.1.0,** we introduced an option to disable the firewall on a per-WAN interface, allowing traffic from WAN to LAN.

By default, stateful firewalls are enabled on every WAN interface.



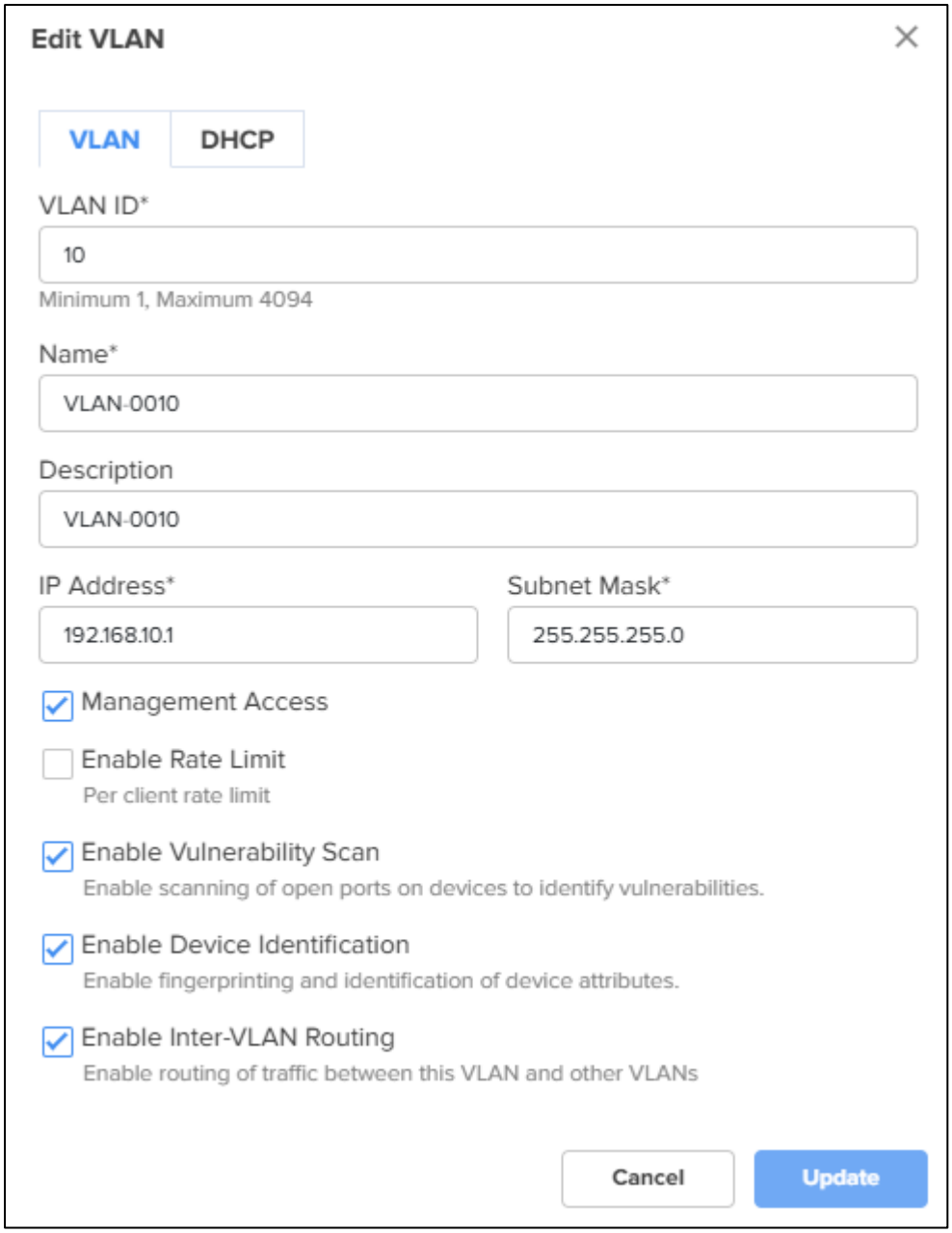
Inter-VLAN Routing

This release introduces an option to disable inter-VLAN routing, preventing communication between VLANs.

This is useful in scenarios such as a guest VLAN, where users should have internet access only but must be restricted from accessing devices in other local VLANs.

By enabling inter-VLAN blocking, traffic between VLANs is prevented while still allowing internet access, meeting this requirement effectively

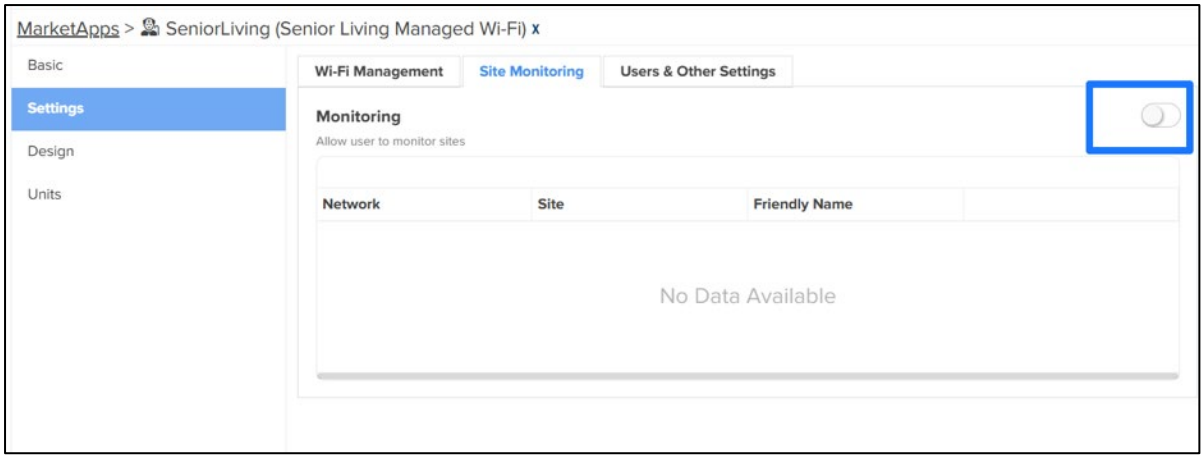
The option to disable inter-VLAN routing is available while creating the VLAN interface. By default, inter-VLAN routing is enabled.



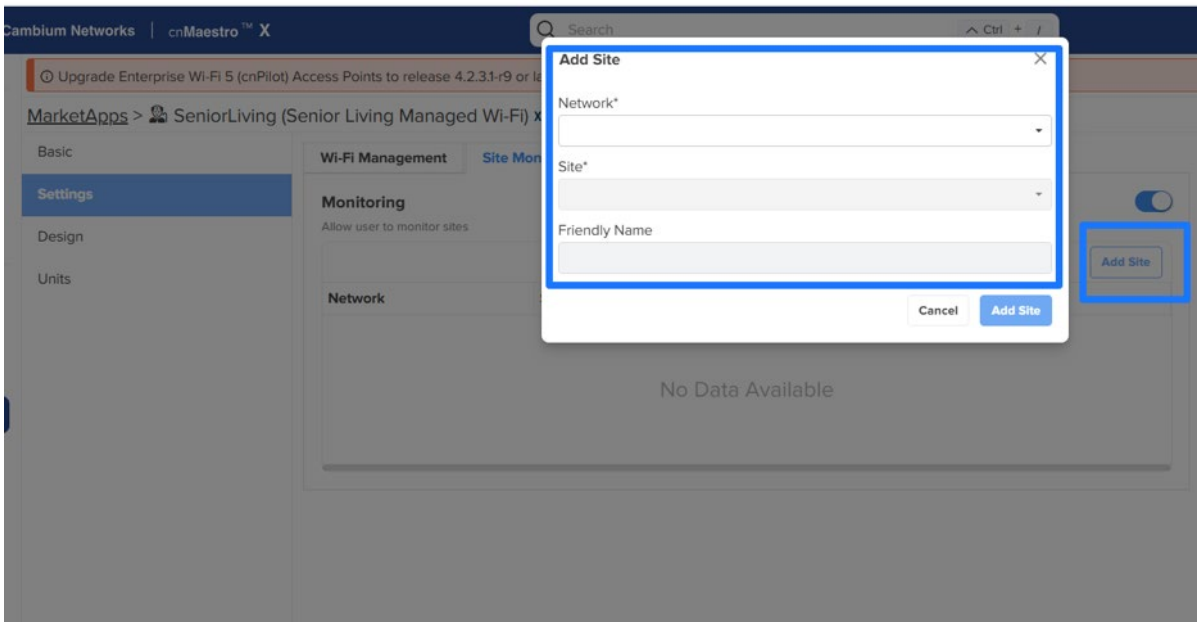
MarketApps: Simple Monitoring Dashboards

This feature enhances MarketApps by enabling property managers to configure which sites they wish to monitor within their network infrastructure. This feature is available for MDU Managed WiFi, Outdoor Hospitality Managed WiFi, and Senior Living Managed WiFi.

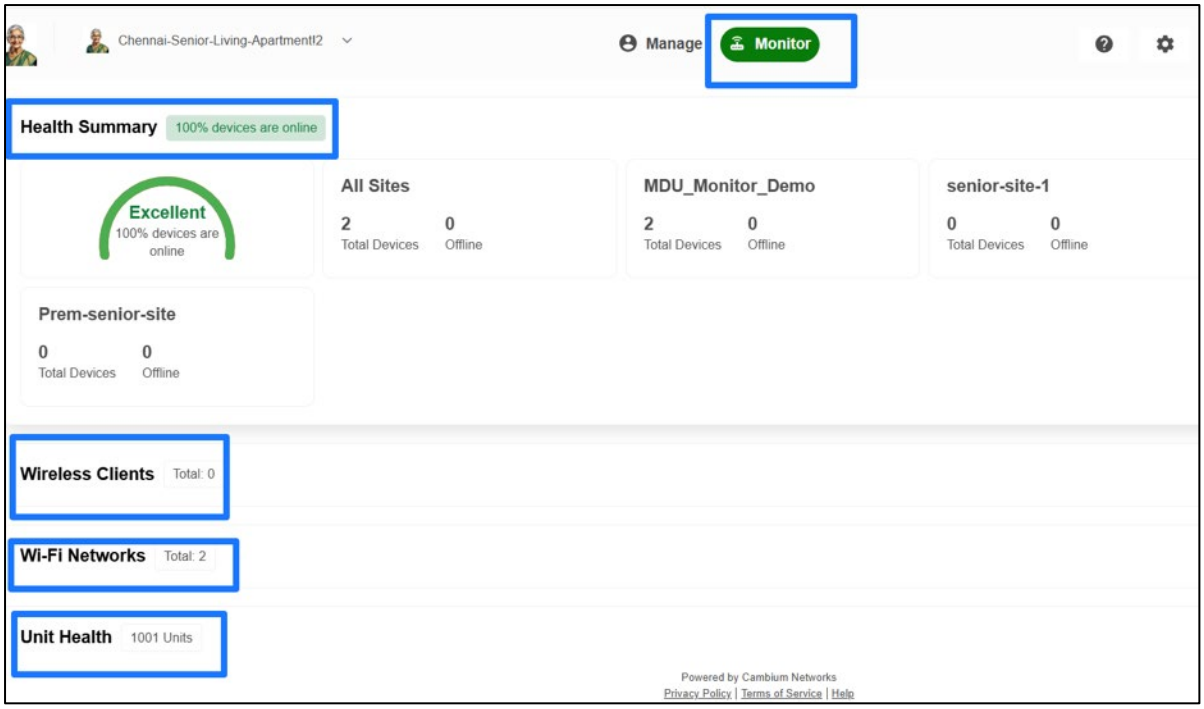
Navigate to *MarketApps* > *Settings* > *Site Monitoring* > *Enable* and add the sites that need to be monitored.



Once enabled, navigate to *Add Site* and select the intended Networks and Sites.



Once enabled, navigate to the manager portal to see the monitoring details like Health Summary, Wireless Clients, WiFi networks, and Unit Health.

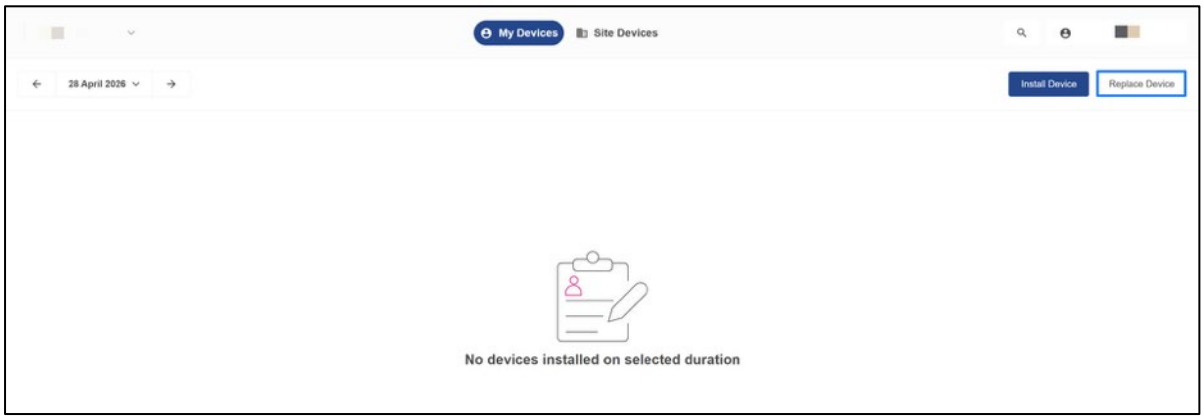


MarketApps: cnMatrix Device Replacement Support in Installer App

This feature enhances the Installer App by enabling streamlined workflows for replacing existing cnMatrix switches.

With this capability, installers can efficiently replace switches as part of upgrade or maintenance activities without complex manual steps. The workflow is designed to simplify hardware replacement in the field while ensuring continuity of deployment processes and preventing unsupported replacements, cross-site mismatches, and switch model mismatches.

This results in faster device replacement, reduced operational effort, and minimized network downtime, ultimately improving overall deployment efficiency.



MarketApps: Installer App Enhancements

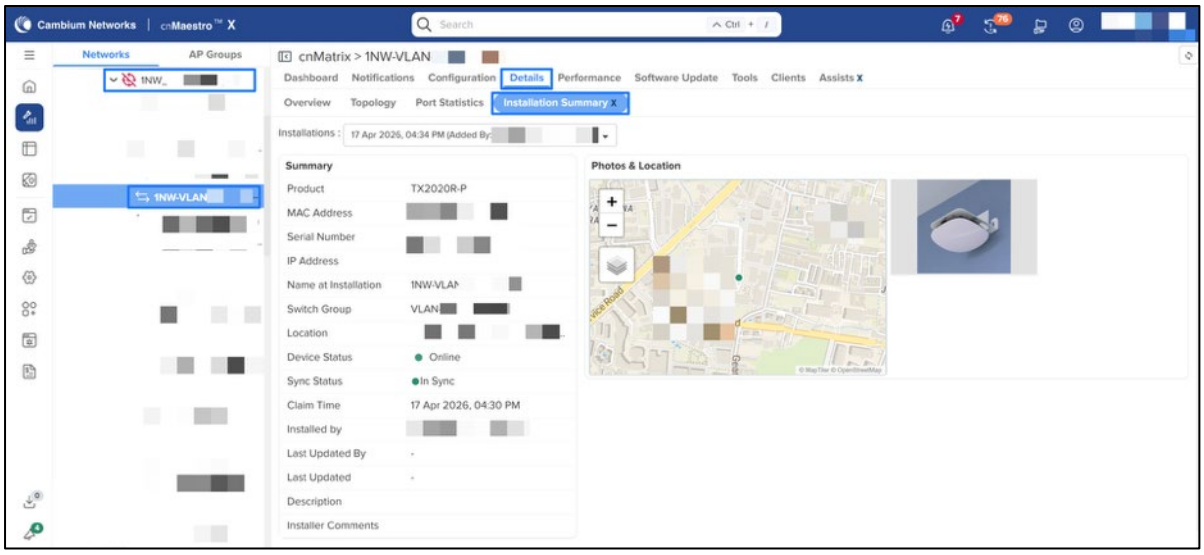
Installer App: Streamlined Installation Workflow for Pre-configured Devices

This feature enables installers to capture and submit installation details for devices that are already claimed or pre-configured in cnMaestro.

With this enhancement, installers can use the existing **Assign** workflow to scan a QR code or manually enter a device serial number, then proceed directly with installation data collection. They can enter key installation parameters such as height, elevation, azimuth, and tilt, upload up to four site photos, run a speed test, and save the details as an Installation Summary.

This workflow does not require installers to search for the device or modify existing configuration, such as AP Groups, device name, or description. If the device is already configured by an MSP, those values are preserved and skipped during the installation flow.

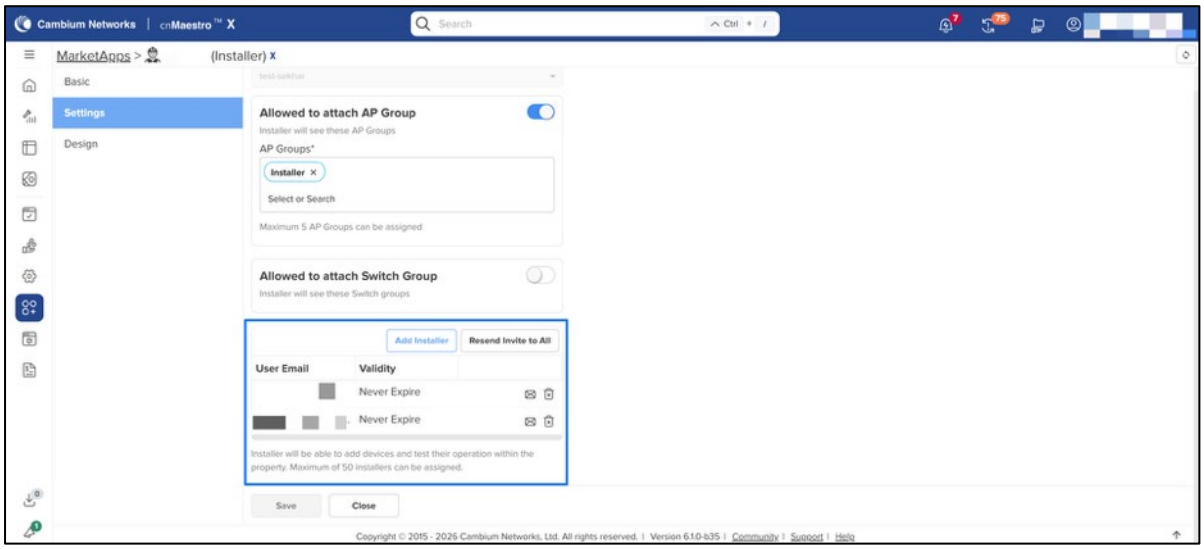
The saved Installation Summary is associated with the device and becomes visible in cnMaestro. This provides simpler field installation experience for both APs and switches while maintaining the existing device configuration.



Installer App Improvements

The enhancements below are introduced to improve scalability and usability for field deployments.

With this update, the Installer App now supports up to **50 users,** an increase from the previous limit of 10, enabling better handling of larger teams and deployments.



Additionally, the session duration has been extended from **24 hours to 7 days**, reducing the need for frequent logins during ongoing installation activities.

These improvements enhance operational efficiency, provide a smoother user experience for installers, reduce login interruptions, and better suit the app for large-scale field operations.

Switch Groups Enhanced with Port Configuration

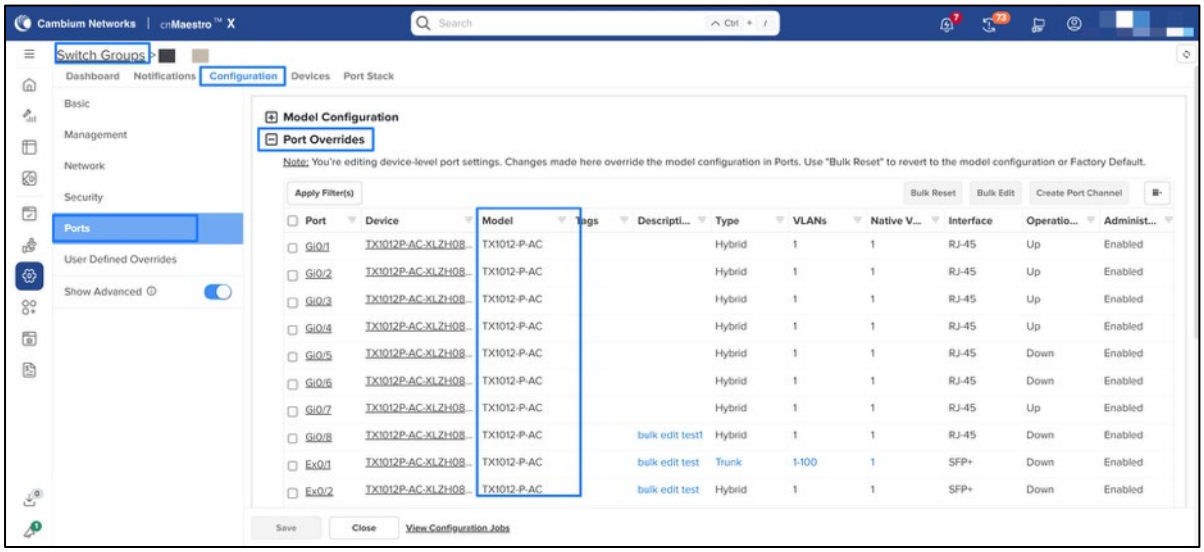
This **feature** improves the Switch Group user experience by simplifying port configuration and reducing confusion between model-level and device-level changes.

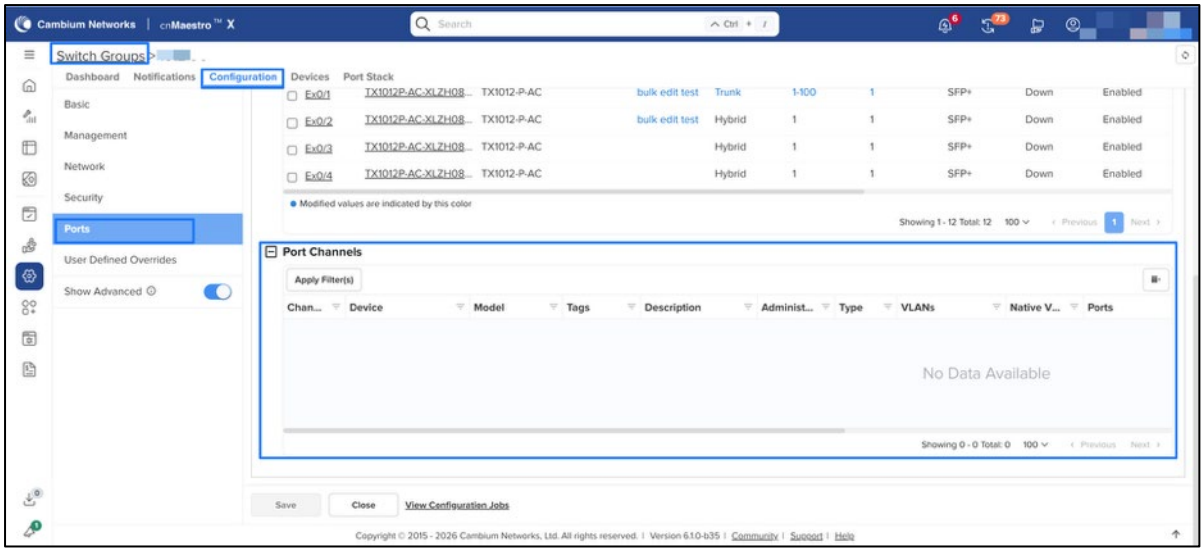
With this enhancement, port configuration (Port overrides and Port channels) is moved under *Switch Groups* > *Configuration* > *Ports*, while the existing model baseline configuration is available in a collapsible section.

The switch group clearly distinguishes between **model configuration changes**, which apply to all matching switches in the group, and **port override changes**, which apply only to the applicable switch. The Devices and Statistics views are also consolidated to provide a cleaner experience, and users can jump directly from port statistics to the related port configuration.

When saving changes, the system provides clear feedback about the scope of the changes and the impacted switches.

This enhancement makes switch port configuration easier to understand, reduces accidental bulk edits, and improves the overall configuration workflow.





Device Replacement Support for cnMatrix and Wi-Fi Access Points

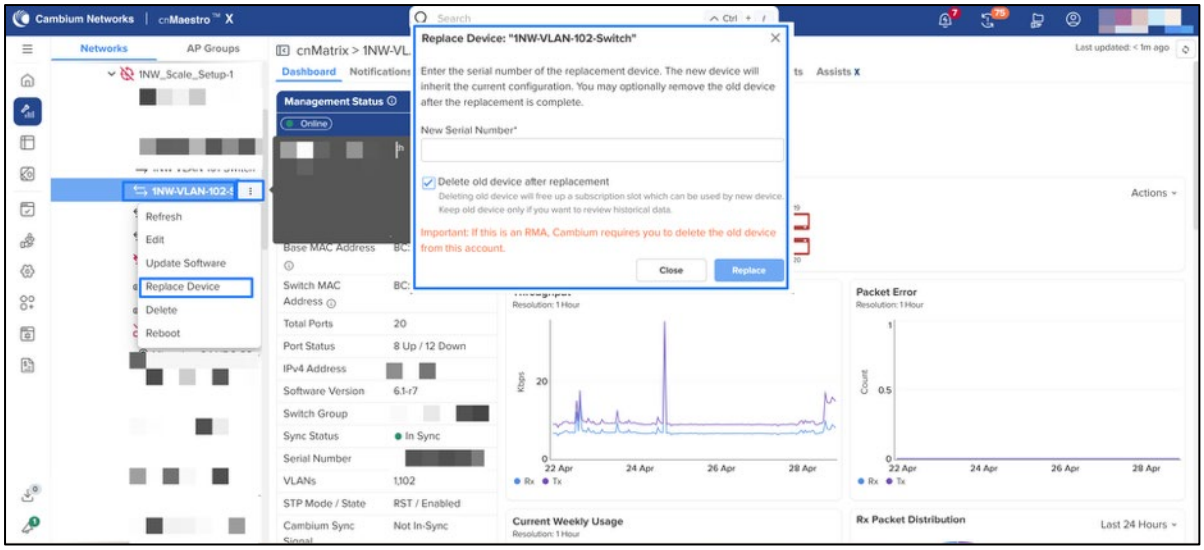
This release introduces the replace AP and cnMatrix switch feature which simplifies the replacement of cloud-managed APs and cnMatrix switches while preserving key device context.

With this enhancement, administrators can replace a managed device by entering the new device serial number. cnMaestro claims the replacement device into the same account, network, and site, then copies supported configuration such as device name, description, profile, configuration overrides, rules, and related metadata. For cnMatrix switches, port-level configuration is also copied when the old and new switch models match.

The old device is renamed with a replacement suffix, and administrators can optionally delete it after the replacement is successful to free the subscription slot. The workflow includes validations to prevent unsupported replacements, cross-site or cross-network moves, failed claims, and switch model mismatches.

This feature reduces manual reconfiguration, simplifies RMA and hardware replacement workflows, and helps minimize service disruption during device replacement.

NOTE: If this is an RMA, Cambium requires you to delete the old device from this account.

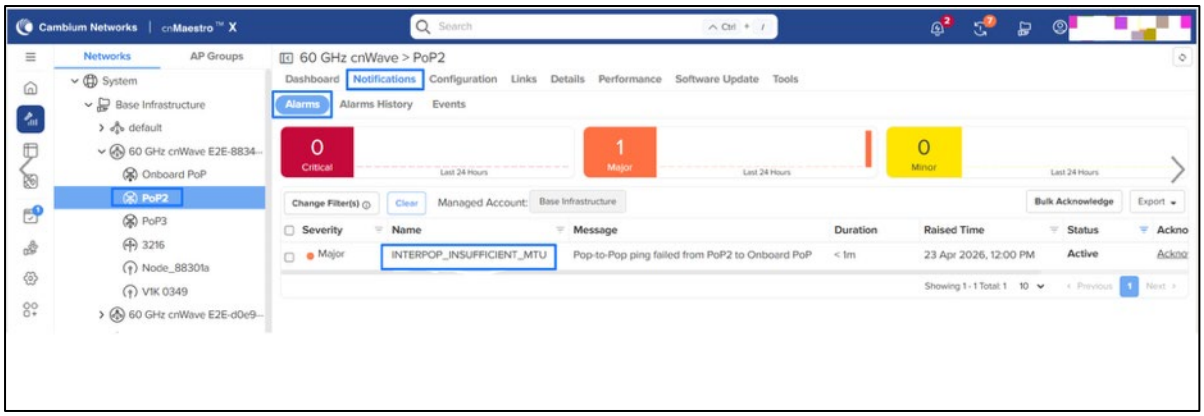


60 GHz cnWave Enhancements

Inter-POP Insufficient Path MTU alarm

This feature introduces the INTERPOP_INSUFFICIENT_MTU alarm in cnMaestro for cnWave deployments. The alarm is triggered when the effective path MTU between two cnWave PoP nodes is less than 1934 bytes, typically due to an intermediate managed switch configured with the default MTU of 1500.

This enhancement helps operators quickly identify misconfigured MTU settings on switches between PoP nodes, preventing potential fragmentation or loss of subscriber traffic. If the issue is not resolved, the alarm automatically clears after 7 days.



Note: This feature is supported by 60 GHz cnWave PoP devices running firmware version 1.8 or later.

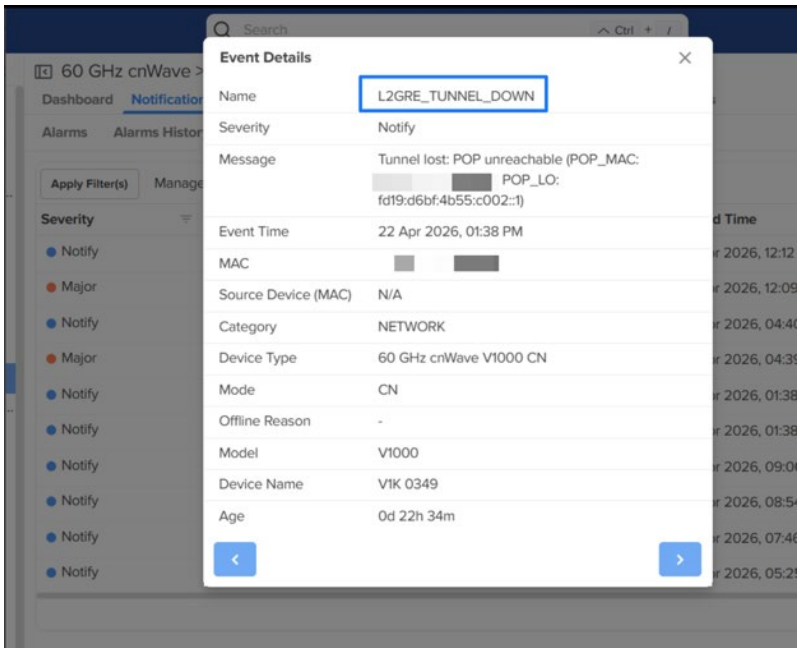
L2GRE Events

The L2GRE Tunnel Events in Notifications feature adds support for displaying cnWave L2GRE tunnel state changes in the *Notifications* > *Events* page.

With this enhancement, users can track L2GRE tunnel state changes directly from cnMaestro and review when tunnels go up or down using the following event names:

- **L2GRE_TUNNEL_UP**

- **L2GRE_TUNNEL_DOWN**



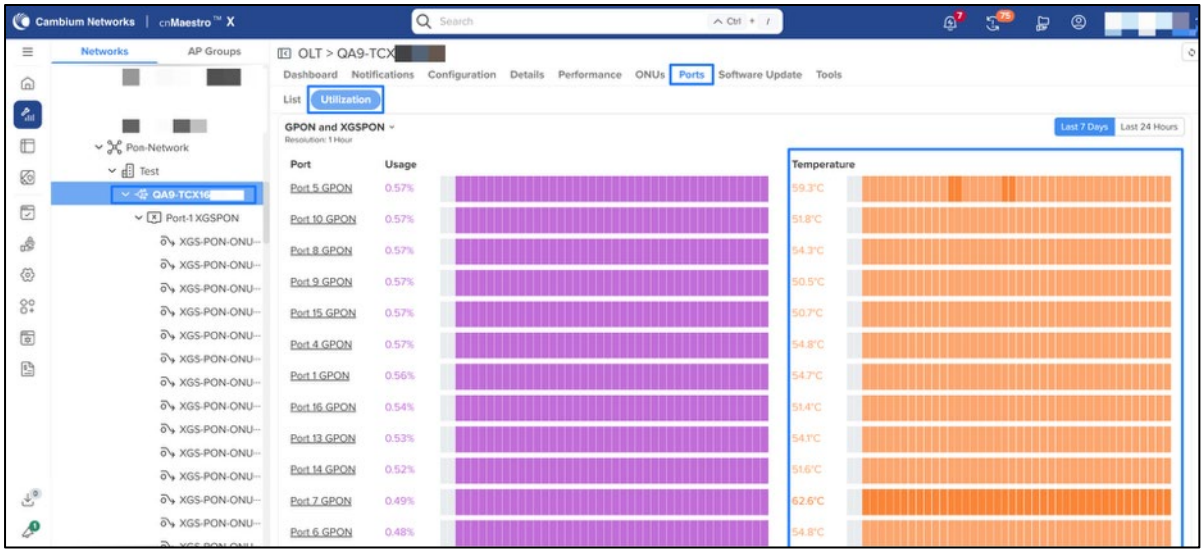
Note: This feature is supported by 60 GHz cnWave devices running firmware 1.8 or later.

PON Enhancements

Temperature graph for PON Ports

The Temperature graph for PON ports feature adds temperature trend visibility for PON ports in the OLT dashboard.

With this enhancement, temperature data already available in OLT Dashboard > *Ports* > *List* is now also plotted in OLT Dashboard > *Ports* > *Utilization*. Users can view real-time and historical temperature values for each PON port in a graph format.



Overdraft Reordering

This feature improves how devices are handled when subscription capacity is unavailable and how they transition back to paid subscription slots.

When a device is onboarded for the first time without an active subscription, it is placed in overdraft to prevent onboarding from being blocked. If the same device is re-onboarded later and no subscription is available, it is marked as a slot deficit instead of being allowed into overdraft again, ensuring fair usage.

When subscription capacity becomes available, devices in overdraft are automatically moved to paid subscriptions after completing their overdraft duration in the order they entered overdraft.

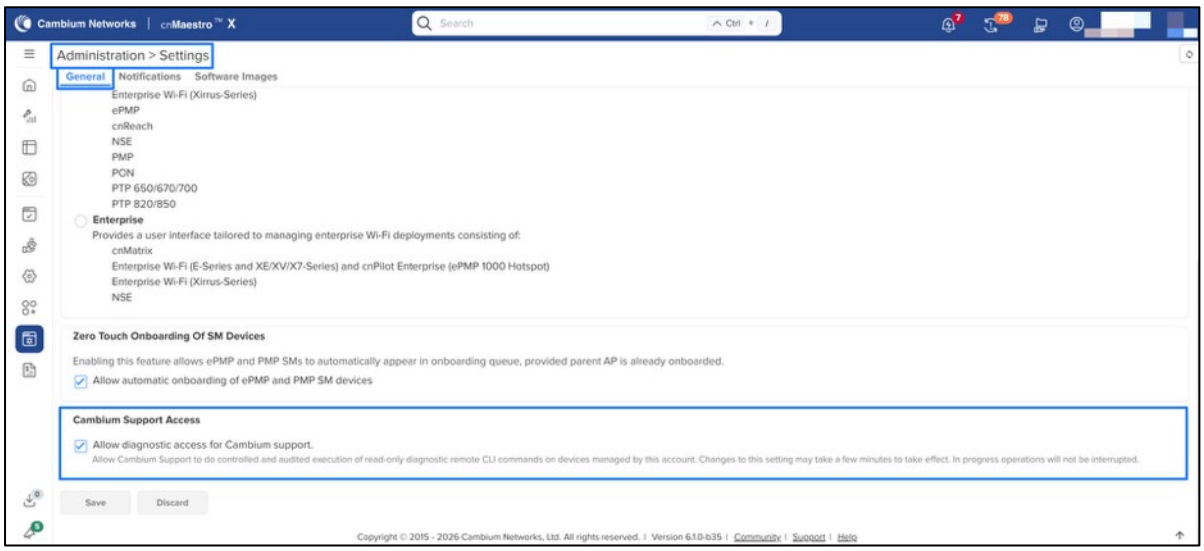
These changes make subscription allocation more predictable, fair, and efficient, while improving overall user visibility and experience.

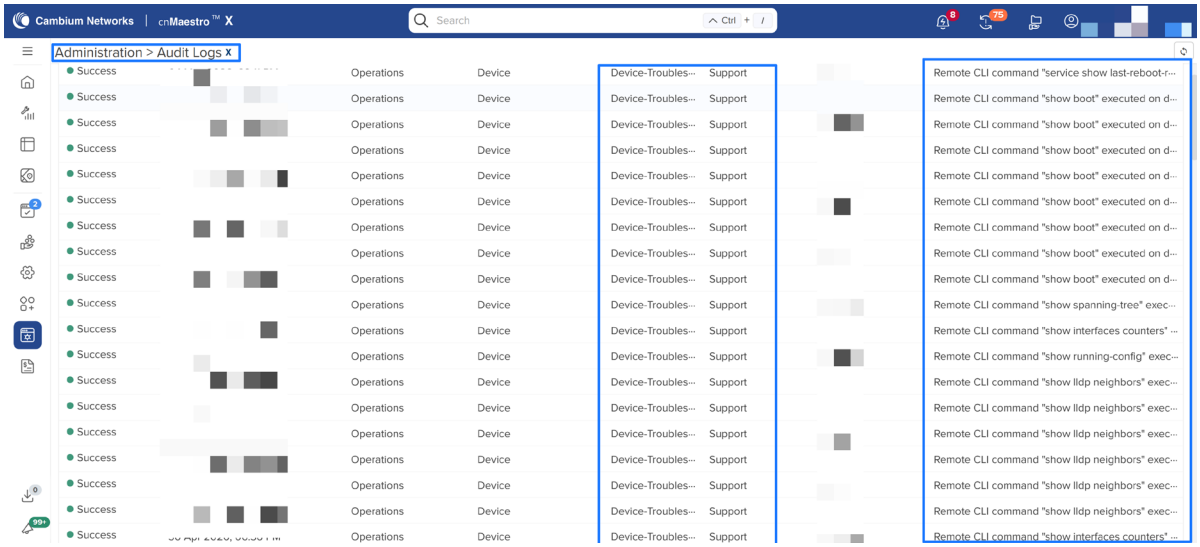
Remote CLI Access Opt-In Consent

This feature adds customer-controlled consent for Cambium Support to execute diagnostic remote CLI commands on Cloud-managed devices.

A new system-level administrative setting, **Allow diagnostic access for Cambium support**, is disabled by default. Customers can turn it ON from the *Administration* > *Settings* > *General* page. When enabled, Cambium Support can perform controlled and audited execution of read-only, allow-listed diagnostic CLI commands for troubleshooting. If disabled, remote CLI operations are blocked.

Only Super Administrators have the ability to enable or disable this setting. All changes to consent and executions of remote CLI commands are recorded in the Audit Logs for tracking and auditing purposes. This provides customers with better control and transparency while still enabling faster support diagnostics.



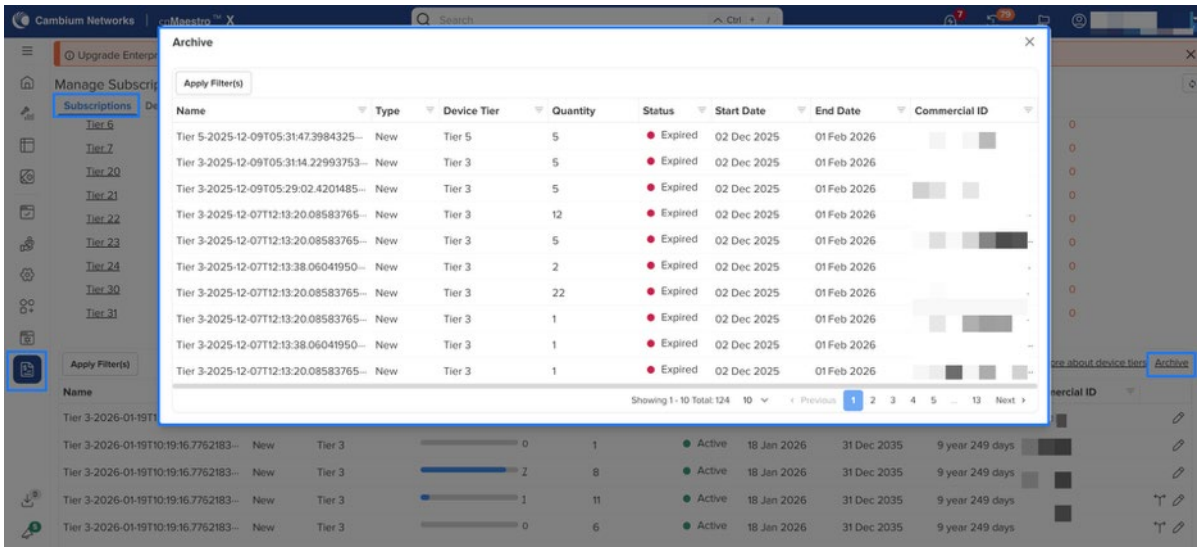


Miscellaneous Enhancements

Archive Expired Subscriptions

This feature improves how expired subscriptions are managed and displayed within the system. With this enhancement, expired subscriptions are automatically moved out of the active subscription view and archived. This reduces clutter in the user interface and ensures that only relevant, active subscriptions are prominently displayed.

By separating expired subscriptions from active ones, the system improves performance, especially for accounts with many subscriptions, and makes it easier for administrators to manage and review current entitlements.



Enhanced Ethernet Port Statistics

Previously, the system displayed only generic Ethernet or uplink speeds, without indicating which physical port was used for the uplink. This made it difficult to troubleshoot connectivity issues, especially for multi-port access points.

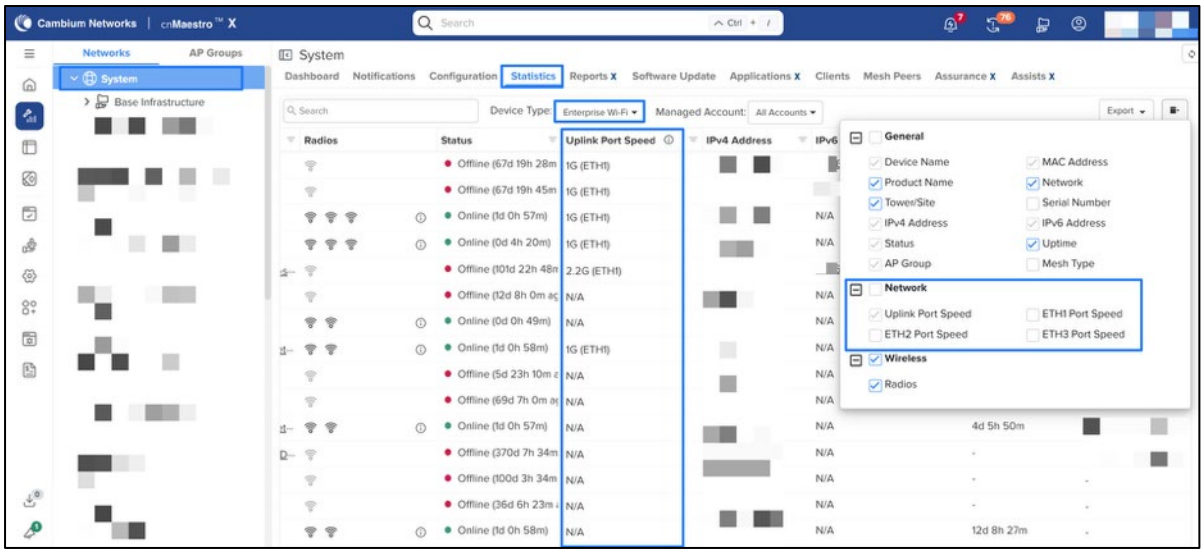
With this enhancement, a new default column **Uplink Port Speed** is introduced, showing both the port and its speed (for example, *1G (ETH1)*). This allows users to quickly identify

which port serves as the uplink and its operating speed. The column also includes filtering options based on speed (10M, 100M, 1G, and above), making it easier to analyze network performance across devices.

For more detailed analysis, individual Ethernet ports (ETH1, ETH2, ETH3) are available as optional columns through the column chooser. These columns provide port-specific speeds with filtering and sorting capabilities, enabling deeper troubleshooting when required.

Additionally, the feature includes guidance on applicability, indicating that uplink port visibility is supported on newer firmware versions, while legacy devices can still be analyzed using individual port columns.

Overall, this enhancement provides a clearer, more flexible view of Ethernet Ports performance, helping administrators quickly identify uplink behavior and troubleshoot connectivity issues more effectively.



Note: This feature is supported on APs running firmware 7.1.1 or later.

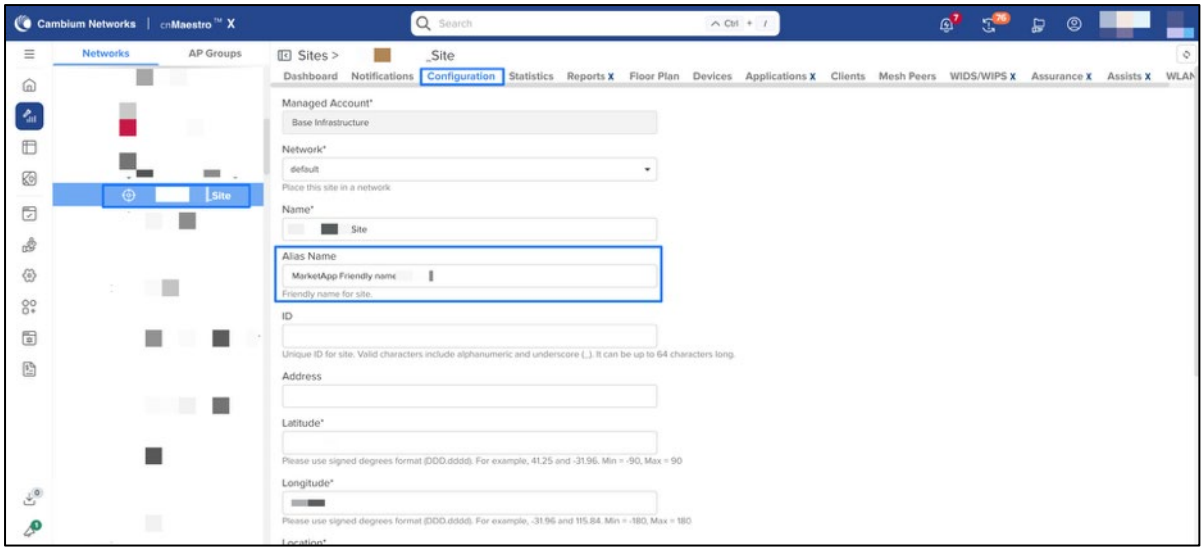
Site Alias Support

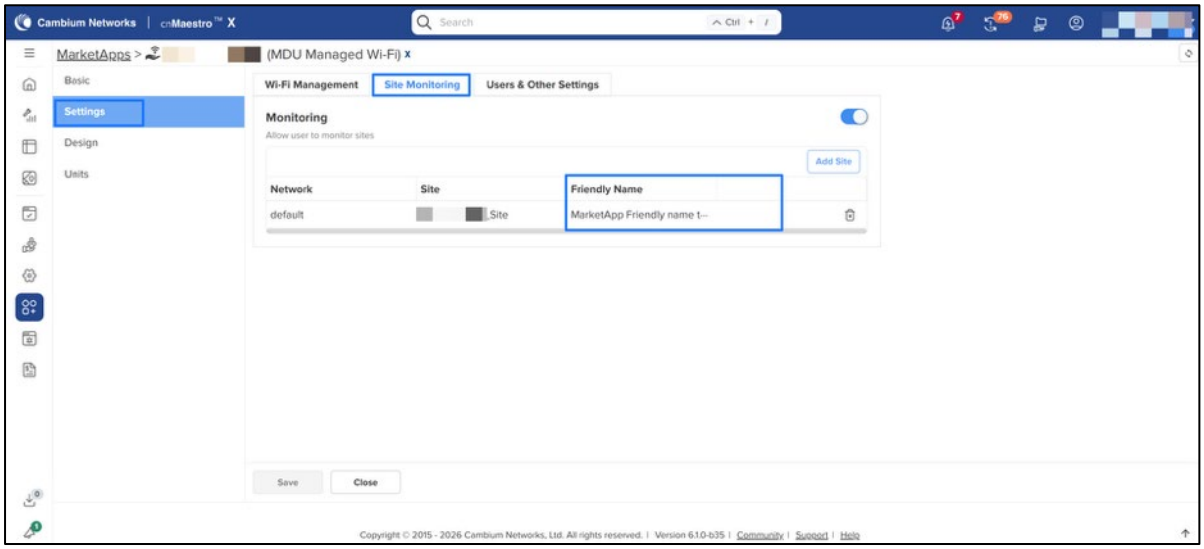
This feature enables assigning a friendly name (alias) to a site, improving usability and integration with applications such as MarketApps.

This enhancement allows administrators to define an optional alias for each site, improving readability and usability, especially in large deployments. The alias can be used alongside the existing site name to make identification more intuitive and aligned with business or operational needs.

In addition, safeguards have been introduced to prevent deletion of sites that are currently associated with applications such as MarketApps, ensuring system integrity.

Overall, this feature enables easier site identification, improves operational efficiency, and reduces the chances of misconfiguration.



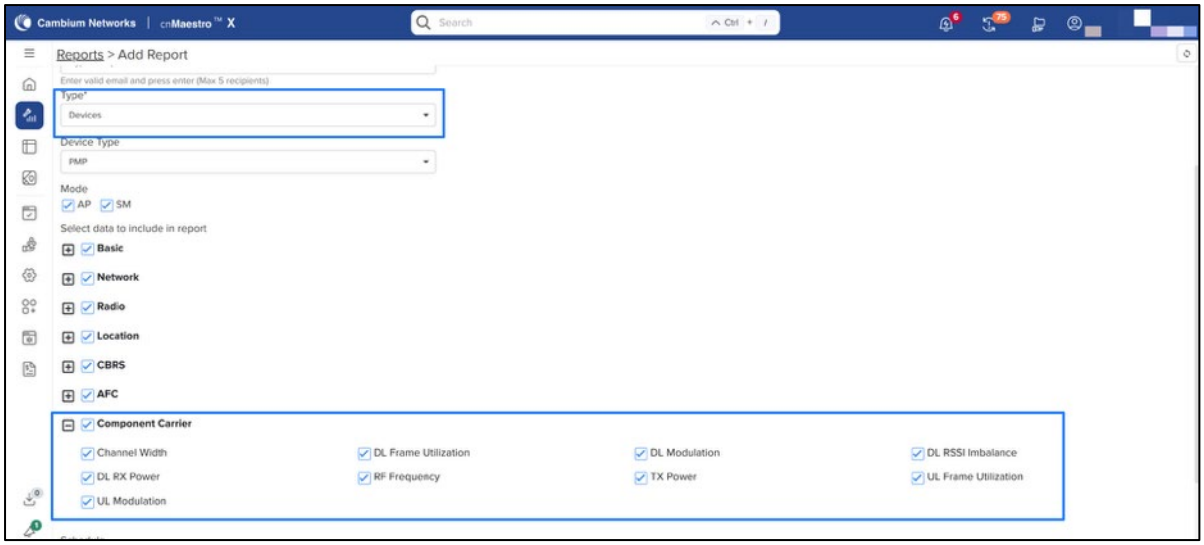


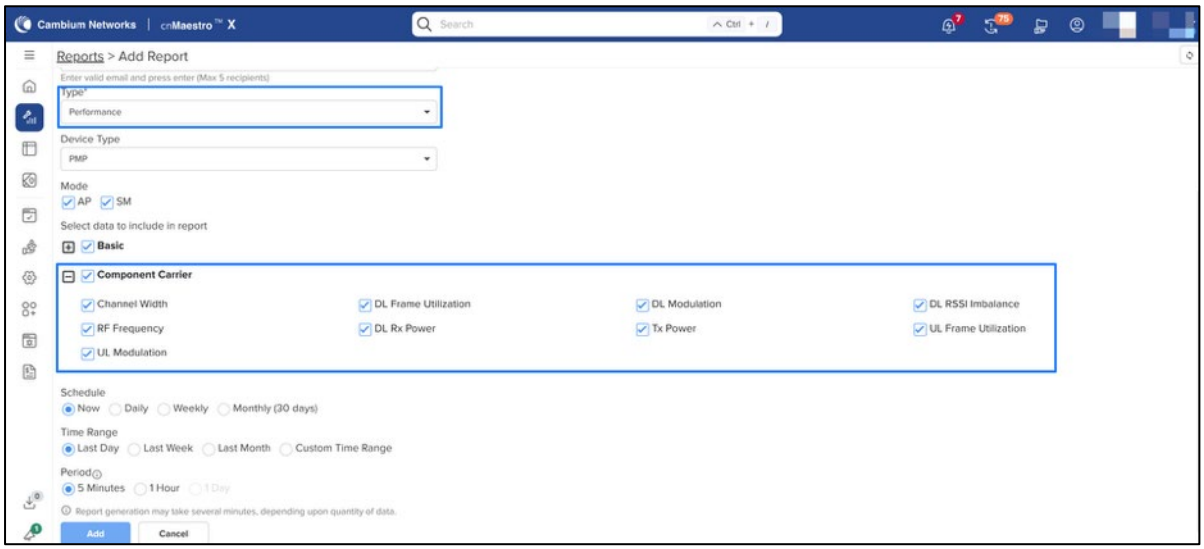
PMP 450v Report Enhancements

This release adds new reporting fields for PMP 450v 4x4 and 2x2 devices in the Performance and Device reports.

With this enhancement, reports now include additional RF and performance details such as **RF frequency, channel width, and Tx power**. AP reports include **DL frame utilization** and **UL frame utilization**, while SM reports include **RSSI imbalance, DL Rx power, UL modulation, and DL modulation**.

These fields are generated for all three component carriers, giving users more complete visibility into PMP 450v device performance and radio characteristics directly from reporting workflows.





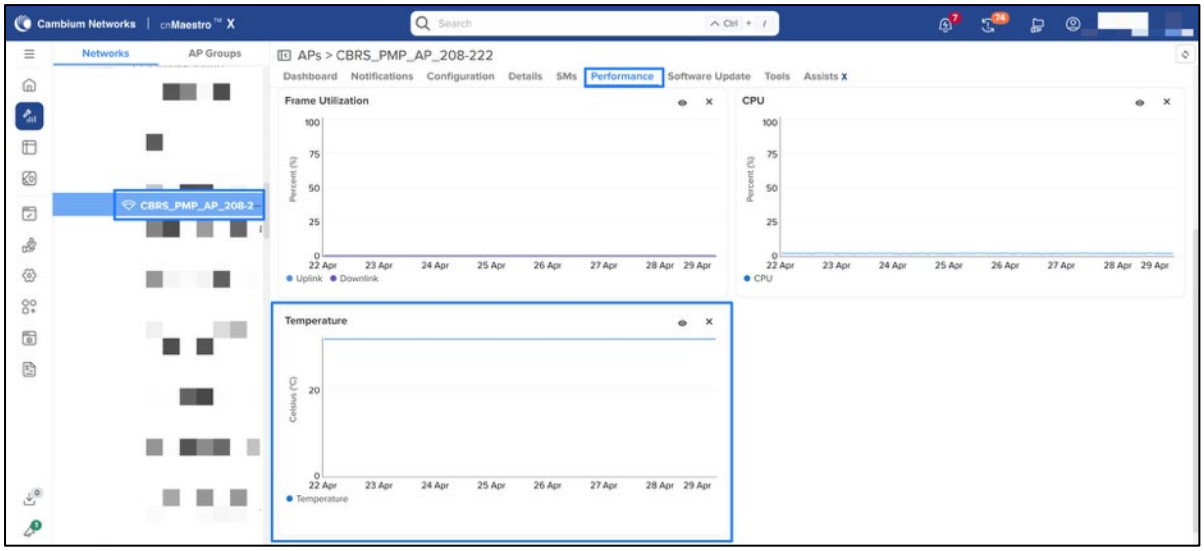
Temperature Graph for PMP Devices

This release adds temperature monitoring and visualization for PMP devices, including 450m, 450i, and 450b.

With this enhancement, supported PMP APs and SMs periodically report temperature data to cnMaestro. cnMaestro stores the temperature values over time and displays them graphically in the **Performance** section for both APs and SMs.

For devices that report multiple temperature values, such as 450m devices with per-chain temperature data, each value is plotted separately and clearly labeled within the same graph.

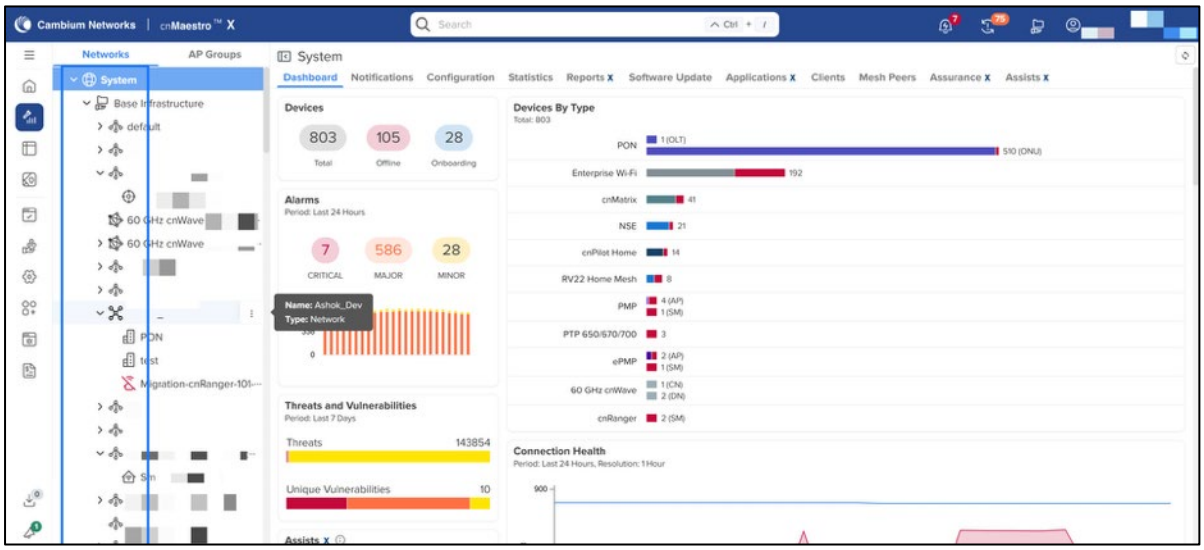
This helps users monitor device temperature trends, identify thermal issues, and troubleshoot performance or hardware-related problems more effectively.



Updated Device and Data Grid Icons

In this release icons across cnMaestro are refreshed to provide a more consistent and modern user experience.

With this update, icons in the network tree, enhanced search, and data grid tables have been revamped for improved visual consistency and easier recognition. This helps users quickly identify device types and actions across different areas of the application.



Tree Search Removal

The older Tree search has been retired. Enhanced search is now the default, offering improved speed, accuracy, and advanced search.

Events Delete Option Removal

The **Delete Option Removal** under *Notifications* > *Events* tab enhancement removes the single and bulk delete actions from the **Events** tab across all levels.

Notifications Alarm Selection Improvements

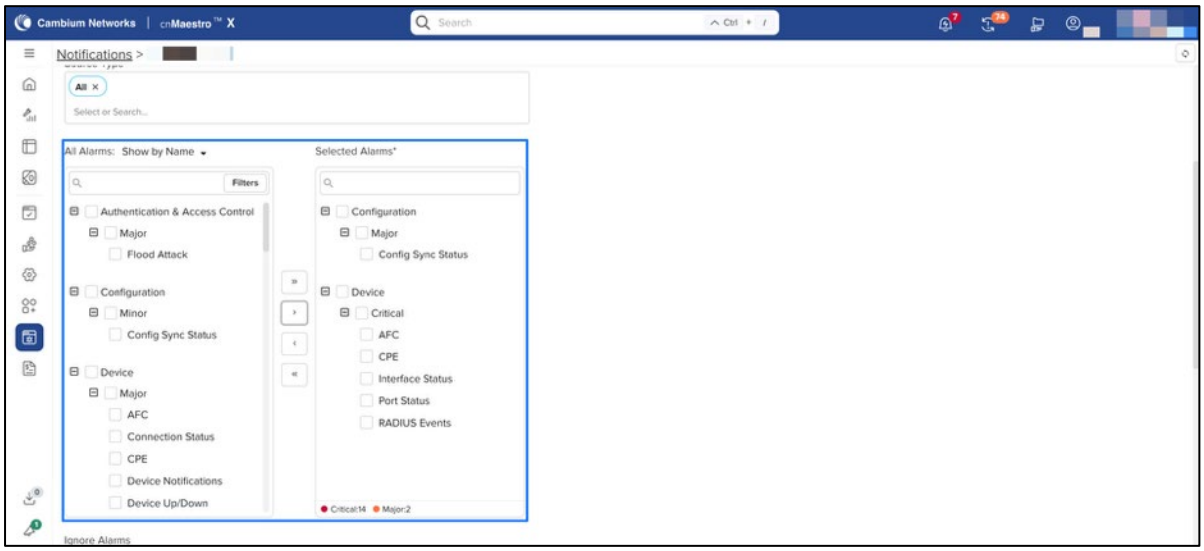
This release improves the alarm selection experience while configuring webhook notifications.

With this update, webhook alarm selection uses a clearer **dual-list selection interface**, making it easier for users to choose which alarms should trigger webhook notifications. The alarm filter experience has been simplified by adding **Select All** and **Deselect All** options, while removing unnecessary filtering from the selected alarms list.

The **Notify** option has also been removed from the selection workflow to reduce confusion and keep the configuration focused on alarm selection.

The update also improves clarity by separating display preferences from filtering behavior and by refining alarm options, such as listing only relevant alarm conditions (e.g., Offline) rather than including both Online and Offline states.

These changes make webhook notification configuration easier to understand, faster to manage, and less prone to selection errors.



API Updates X

Deprecated APIs

Request Method	Path	Deprecated In	Sunset In	Replacement	Details
Guest Access API					
GET	/portals	5.2.0	6.2.0	/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	6.2.0	/api/v2/easypass/{portalName}	
GET	/portals/{portalName}/events	5.2.0	6.2.0	/api/v2/easypass/{portalName}/sessions/login_events	
PUT	/portals/{portalName}/whitelist	5.2.0	6.2.0	/api/v2/easypass/{portalName}/configuration/allowed_domains	
GET	/portals/{portalName}/voucher_plans	5.2.0	6.2.0	/api/v2/easypass/{portalName}/voucher_plans	
GET	/portals/{portalName}/vouchers/{voucherPlan}	5.2.0	6.2.0	/api/v2/easypass/{portalName}/voucher_plans/{voucherPlan}/vouchers	
POST	/portals/{portalName}/vouchers/{voucherPlan}/generate	5.2.0	6.2.0	/api/v2/easypass/{portalName}/voucher_plans/{voucherPlan}/vouchers/generate	
cnArcher Installation Summary					
GET	/api/v2/cnarcher/installation/summary	6.0.0	6.2.0	/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	6.2.0	/api/v2/installation/summary/{mac}	

Deprecated Fields

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
AP Groups						
GET	/wifi_enterprise/ap_groups	auto_rf_channel_selection_mode	5.2.1	6.2.0	N/A	These fields are no longer relevant for Auto-RF configuration.
GET	/wifi_enterprise/ap_groups	channel_utilization_threshold	5.2.1	6.2.0	N/A	
POST	/wifi_enterprise/ap_groups	auto_rf_channel_selection_mode	5.2.1	6.2.0	N/A	This field is no longer relevant for Auto-RF configuration.
PUT	/wifi_enterprise/ap_groups/{ap_group_name}	auto_rf_channel_selection_mode	5.2.1	6.2.0	N/A	
POST	/api/v2/wifi_enterprise/ap_groups	shared	6.0.0	6.2.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.2.0
POST	/api/v2/wifi_xirrus/ap_groups	shared	6.0.0	6.2.0	N/A	
Wi-Fi Enterprise						
GET	/devices/clients	ap_mac	5.0.0	6.2.0	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	Deprecated In	Sunset In	Replacement	Details
						property of an AP device.
GET	/devices/wired_clients	ap_mac	5.0.0	6.2.0	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	6.2.0	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	6.2.0	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_groups_ports/{switch_group_name}	nid	5.2.5	6.2.0	network	Renamed the deprecated fields to

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
GET	/api/v2/cnmatrix/switch_groups_ports/{switch_group_name}	tid	5.2.5	6.2.0	tower	relevant ones.
GET	/api/v2/cnmatrix/switch_groups_ports/{switch_group_name}	mcid	5.2.5	6.2.0	managed_account	
GET	/api/v2/cnmatrix/switch_groups_ports/{switch_group_name}	eType	5.2.5	6.2.0	N/A	eType is redundant as the API endpoint is specific to cnMatrix itself.
POST	/api/v2/cnmatrix/switch_groups	shared	6.0.0	6.2.0	N/A	The shared field is deprecated and will be removed in version 6.2.0
Events API						
GET	/api/v2/events	offset total	6.0.0	6.2.0	continuation_token	The offset request parameter is deprecated in 6.0.0 and will be removed in version 6.2.0 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 6.2.0 release.
Device Performance API						

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
GET	/api/v2/devices/{mac}/performance	offset total	6.0.0	6.2.0	continuation_token	The offset request parameter is deprecated in 6.0.0 and will be removed in version 6.2.0 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 6.2.0 release.
NSE Threats API						
GET	/api/v2/devices/nse/{mac}/threats	offset total	6.0.0	6.2.0	continuation_token	The offset request parameter is deprecated in 6.0.0 and will be removed in version 6.2.0 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 6.2.0 release.

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
WLANs						
POST	/api/v2/wifi_enterprise/wlans	ga_cn_portal_name	6.0.0	6.2.0	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 6.2.0. The cnmaestro value for the ga_portal_mode field is deprecated in 6.0.0 and will be removed in release 6.2.0. 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	6.2.0		
POST	/api/v2/wifi_enterprise/wlans	shared	6.0.0	6.2.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.2.0
Access Control Policy						
POST	/api/v2/wifi_enterprise/access_control	shared	6.0.0	6.2.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.2.0
NSE Groups						
POST	/api/v2/nse/nse_groups	shared	6.0.0	6.2.0	N/A	The shared field is deprecated in 6.0.0 and

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
						will be removed in version 6.2.0
Configuration Templates						
POST	/api/v2/device/configuration/templates	shared	6.0.0	6.2.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.2.0
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 Statistics API		
GET	/api/v2/devices/statistics	

Request Method	Path	Details
GET	/api/v2/devices/{mac}/statistics	Added support for packet_error_rate field under radios. New Type filter is also added. Added tunnels statistics for the supported W-Fi enterprise device types.
AP Groups API		
POST	/api/v2/wifi_enterprise/ap_group	Added support for Auto-RF Dynamic Power fields (Dynamic Power Mode, Minimum Transmit Power, Maximum Transmit Power, Minimum Neighbour Threshold, Cell Size Overlap Threshold). The data rate fields minimum_unicast_rate and multicast_rate are supported exclusively for cnPilot devices. data rate fields min_unicast_rate, mcast_rate, and mgmt_rate are supported exclusively for XE/XV/X7 series devices.
PUT	/api/v2/wifi_enterprise/ap_group/{ap_group_name}	
GET	/api/v2/wifi_enterprise/ap_group	
Sites API		
POST	/api/v2/networks/{network_name}/sites	Added new site alias optional field.
PUT	/api/v2/networks/{network_name}/sites/{site_name}	
GET	/api/v2/networks/{network_name}/sites	
Alarms API		
GET	/api/v2/alarms	Added support for filtering alarms by network/tower/site.
GET	/api/v2/alarms/history	Added support for filtering alarms history by network/tower/site.
WLANs API		
POST	/api/v2/wifi_enterprise/wlans	Added support for dhcpopt82_cid_custom_delimiter, dhcpopt82_rid_custom_delimiter, and dhcpopt82_mac_addr_delimiter fields under advanced settings.
PUT	/api/v2/wifi_enterprise/wlans/{wlan_name}	
GET	/api/v2/wifi_enterprise/wlans	
GET	/api/v2/wifi_enterprise/wlans/{wlan_name}	

New APIs added in 6.1.0

No new APIs added in 6.1.0

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

Family	Model	Version
	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
	XV2-2X	6.1
	XV2-2T0	6.4
	XV2-2T1	6.4.1-r15
	XV2-21X	6.5
	XV2-22H	6.5

Family	Model	Version
	XV2-23T	6.5
	XV3-8	6.0
	X7-35X	7.0-b14
	X7-53X	7.1.1
	X7-55X	7.1.1
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
	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	

Family	Model	Version
	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:

** Known issues in Release 6.0.0 and below are resolved in Release 6.1.0*

ID	Details
CNSSNG-52484	Non-deterministic pagination in Networks API due to unsorted data retrieval.
CNSSNG-52183	Redirection to 60 GHz cnWave device dashboard is not working when clicking on hyperlink of node name from *Network* > *Links* tab if node name contains only numbers.
CNSSNG-52159	Management VLAN was not updated correctly in Advanced Settings of Enterprise Wi-Fi device overrides after changing the management VLAN from VLAN 1 to another VLAN.
CNSSNG-52057	WLAN details retrieved through the API returned an incorrect PMF value.
CNSSNG-52037	EasyPass Splash Page Connect button turned white after selecting a checkbox for Apple devices.
CNSSNG-51948	EasyPass Self Registration clients did not show the username in the client table.
CNSSNG-51859	Exporting EasyPass vouchers as PDF generated a zero-byte file.
CNSSNG-51744*	Upgrade timeout messages appear even when the upgrade succeeds.
CNSSNG-51521*	Exporting selected ePSK entries exported all ePSK entries instead of only the selected ones.
CNSSNG-51455*	Custom delimiter and MAC delimiter settings could not be configured through the API.
CNSSNG-51337*	Unable to export installation summary as PDF when 500+ APs are installed via the Installer App.
CNSSNG-51299*	Bulk config: VLAN and Status not updating under WLAN overrides.
CNSSNG-51245*	Optimization API not working for E2E network under MSP account.
CNSSNG-51148*	Importing a Switch Group failed during the import process.
CNSSNG-51118*	Sending an ePSK by email used a default duration of 1440 hours instead of the configured session duration.
CNSSNG-50856*	Device Type incorrectly identified for cnMatrix's Wired Clients.
CNSSNG-50762*	Images in custom reports were not displayed properly.
CNSSNG-50581*	Same alarm name displayed under Major and Notify severity.
CNSSNG-50277*	Config push failed with error when port channel with hybrid mode has multiple VLANs.

ID	Details
CNSSNG-50177*	DL and UL values in WLANs tab updating with delay during 5-minute interval.
CNSSNG-49919*	RV22 devices could not be moved across networks and sites.
CNSSNG-49299*	APs without configured NTP servers used UTC time instead of applying the time zone configured in cnMaestro.
CNSSNG-47881*	MarketApps: Residents could still connect clients after being terminated or after their scheduled checkout time.
CNSSNG-45119*	Channel number is not updated to the new channel when the Primary controller comes back to active state, if we change the channel from Maps when the Backup controller is active.
CNSSNG-45116*	Channel Number is showing '0' in node>dashboard channel widget if we change the channel when the Backup controller is active.

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 *Switch groups* > *Configuration* > *Ports*.
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.