Cambium Networks™

RELEASE NOTES

cnMaestro™

Release 6.0.0

Contents

Introduction

The cnMaestro™ 6.0.0 release introduces a new advanced DPI engine for improved application recognition and traffic classification, enhanced security visibility including DNS filtering insights and IPS updates, and new Virtual WAN capabilities with WireGuard support. It also strengthens wired client visibility for cnMatrix switches, expands dashboard analytics to 30 days, and streamlines configuration and reporting workflows.

Additional UI refinements, API updates, and platform improvements further enhance scalability, performance, and overall user experience.

Important: Web Browser
Restart your browser or clear the browser cache with a hard reload if you have UI problems after the 6.0.0 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.

Enterprise Wi-Fi, NSE: New Advanced DPI Engine

This release introduces an upgrade to the Deep Packet Inspection (DPI) engine used on Cambium NSE and Wi-Fi solutions for Application Visibility and Control. The upgraded engine utilizes an industry leading modern, advanced technology stack.

The updated DPI engine delivers improved application recognition accuracy, enhanced traffic classification, and better performance and scalability across Cambium enterprise Wi-Fi and/or NSE deployments. Customers will benefit from a much larger number of identified applications, stronger policy enforcement, and greater precision in analytics.

The updated DPI engine increases application recognition capacity to 5,000+ distinct applications, significantly expanding visibility compared to the legacy engine's ~2,000 application support.

This enhancement maintains seamless DPI functionality while strengthening overall system performance and scalability across supported configurations.

Note: The new DPI engine is supported by Enterprise Wi-Fi APs running version 7.2 or later and on NSE devices running version 2.1 or later.

Important: Upgrade/Downgrade Impact to Access Control Policy (ACP)/ Firewall Configuration

For NSE

- **Downgrade (to versions below 2.1):**
  Downgrading may result in the loss of certain firewall configurations. After the downgrade, manually re-sync the configuration from the Device Configuration page to ensure proper firewall operation.

- **Upgrade (to version 2.1 and above):**
  The configured **NSE Groups** may contain settings that are not applicable to the upgraded version. Review the NSE Group configuration after the upgrade.

For Enterprise Wi-Fi APs

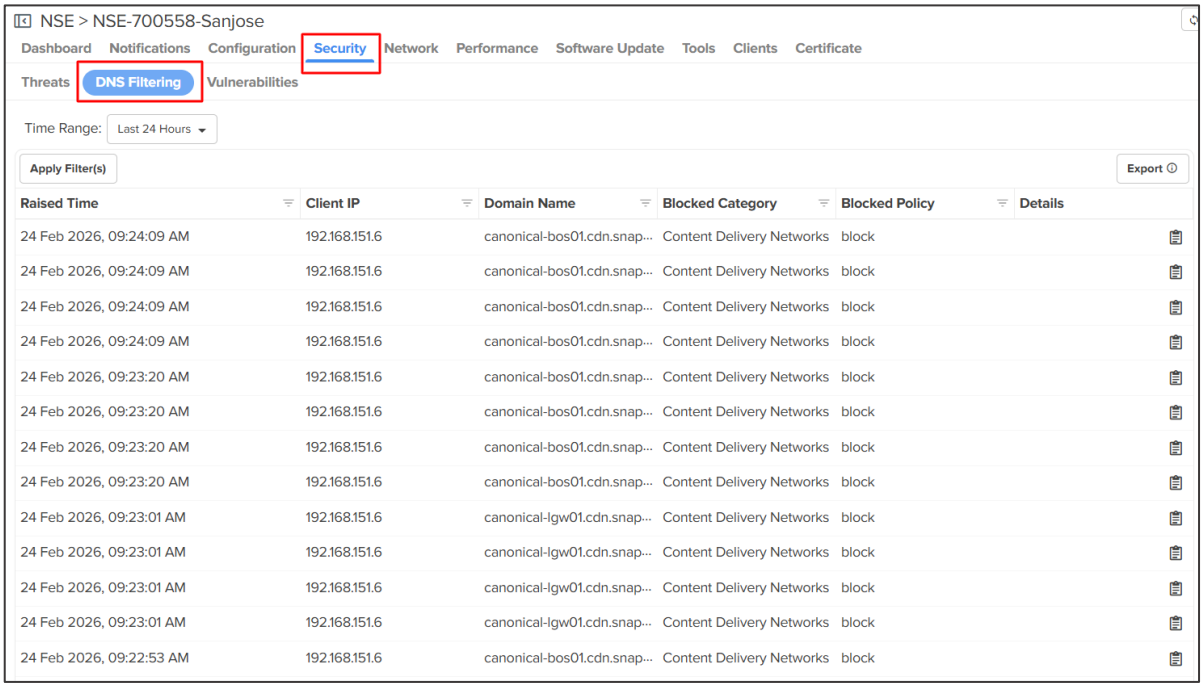
- During **upgrade (to version 7.2 and above) or downgrade (to versions below 7.2)**, the **Access Control Policy (ACP)** associated with the configured **AP Groups or WLAN** may include **application-based rule configurations** that are not supported by the selected version.
  Review and update the associated ACP rules after the version change.

NSE Enhancements

DNS Filter Events

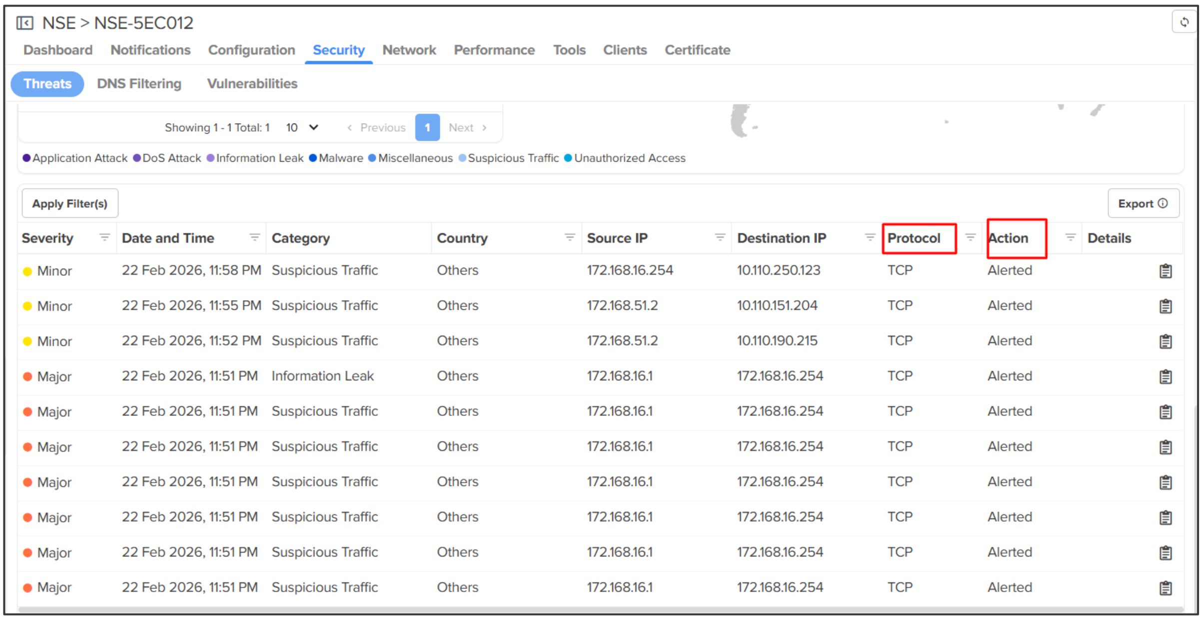
This release introduces a new DNS Filtering tab at the device level under the Security page.

This enhancement provides detailed visibility into DNS-based security events, including client IP address, blocked domain, blocked category, and the associated policy under which the action was enforced. The new view enables more efficient monitoring, improved troubleshooting, and clearer insight into DNS security policy enforcement at the device level.



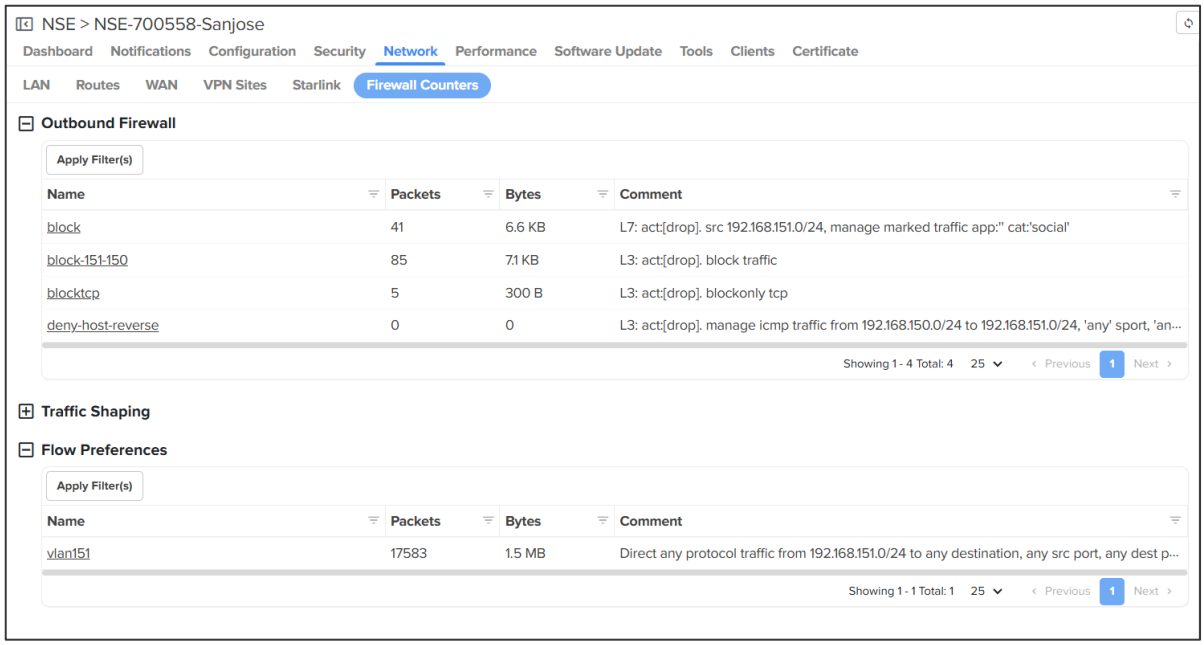
Additional Fields under the IPS Threat Events

- Under the *Security > Threats page,* two additional columns have been introduced to the table: Protocol and Action.
- The Protocol column indicates whether the threat originated from a TCP, UDP or ICMP flow.
  The Action column shows how the event was handled — Alerted (IDS in detection mode) or Dropped (IDS in protection mode).



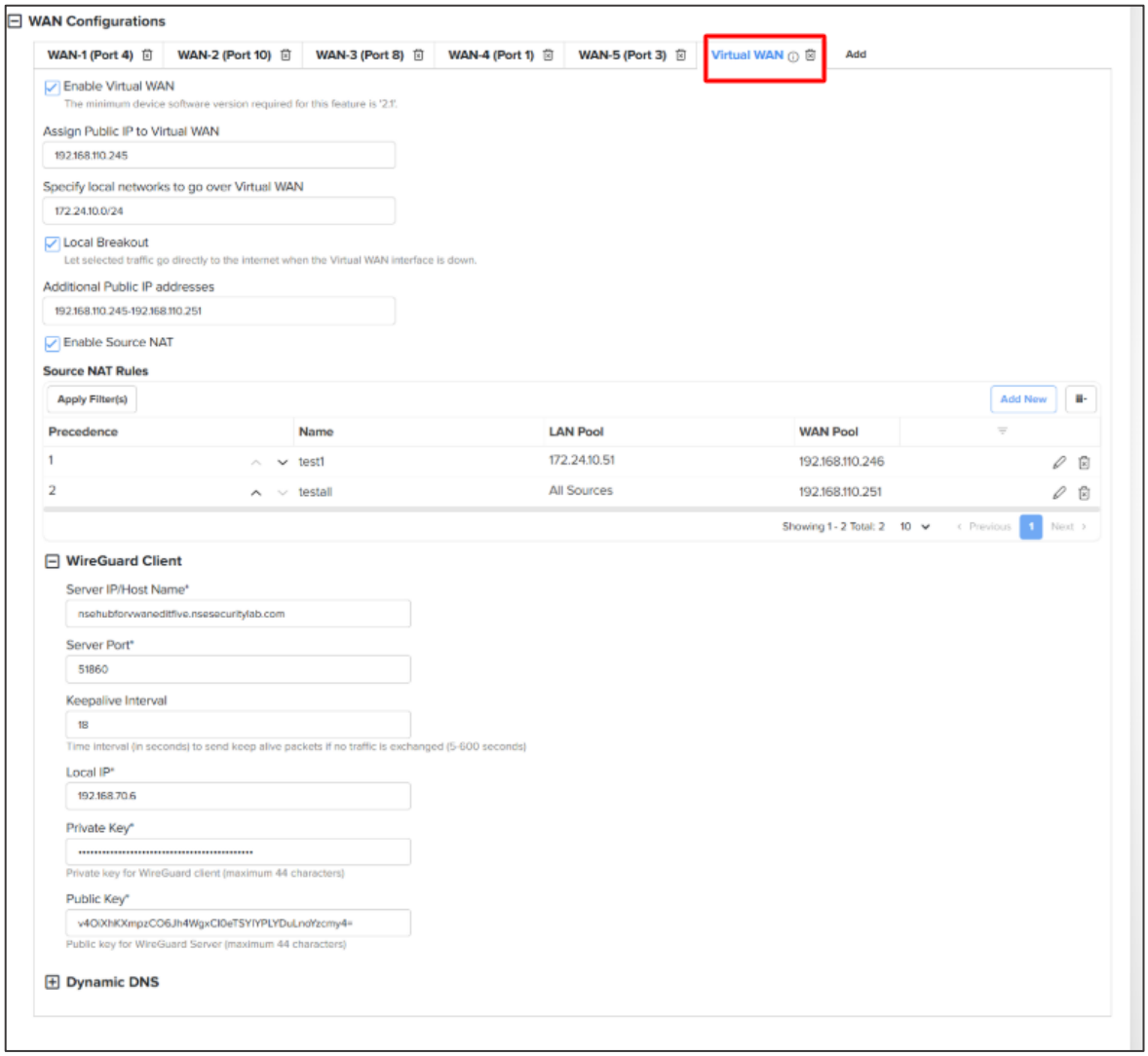
Firewall Counters

- The **Firewall Counters** page provides visibility into firewall rule activity on the device. It displays rule hit counts in terms of packets and bytes for configured Outbound Firewall rules, Traffic Shaping rules, and Flow Preferences, helping administrators verify rule matches.
- This page is particularly useful for confirming whether specific rules are being triggered.



Virtual WAN

- Virtual WAN is a new feature introduced in this release. It enables the creation of an additional WAN interface for forwarding user traffic.
- The virtual interface establishes a WireGuard tunnel with a peer, and user traffic is routed through this secure tunnel.
- All features available on the physical WAN interface such as assigning a public IP, Source NAT, Destination NAT and Dynamic DNS are also supported on Virtual WAN.
- In addition, users can enable **Local Breakout**, which monitors the status of the Virtual WAN interface. If Virtual WAN goes down, traffic is automatically routed over the underlying connection.
- We also allow a remote VPN WireGuard client to connect via the Virtual WAN interface.



Support for cnMatrix Wired Clients

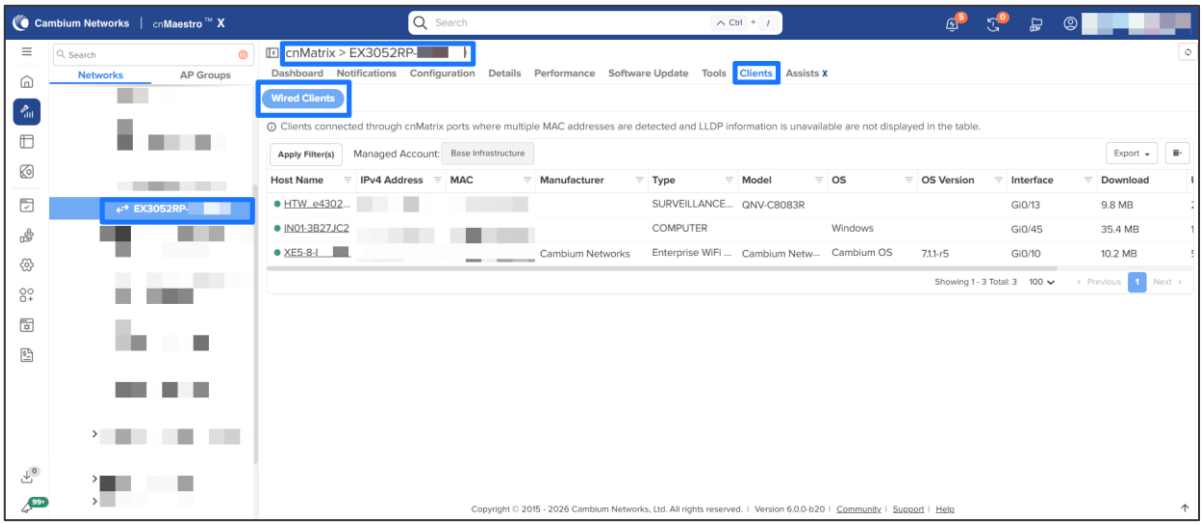
cnMaestro now delivers enhanced visibility and reporting for wired clients connected directly to Ethernet ports on cnMatrix switches.

Wired clients are uniquely identified by their MAC address and include detailed attributes such as IP address, device category, operating system, and connection statistics. cnMaestro intelligently aggregates client information from multiple sources to deliver comprehensive, accurate client insights across the network. This feature improves network visibility, strengthens client-level monitoring, and enables administrators to better analyze and manage wired client devices across the network.

This enhancement also includes:

- Accurate client identification using LLDP, DHCP snooping, and traffic analysis
- Reporting of client properties, connection age, and port-level statistics
- Support for advanced client insights such as device fingerprinting, application usage, and vulnerability information (when NSE is present in the same network)

NOTE: For cnMatrix switches, wired client information is available only for currently connected clients; historical data is not supported.

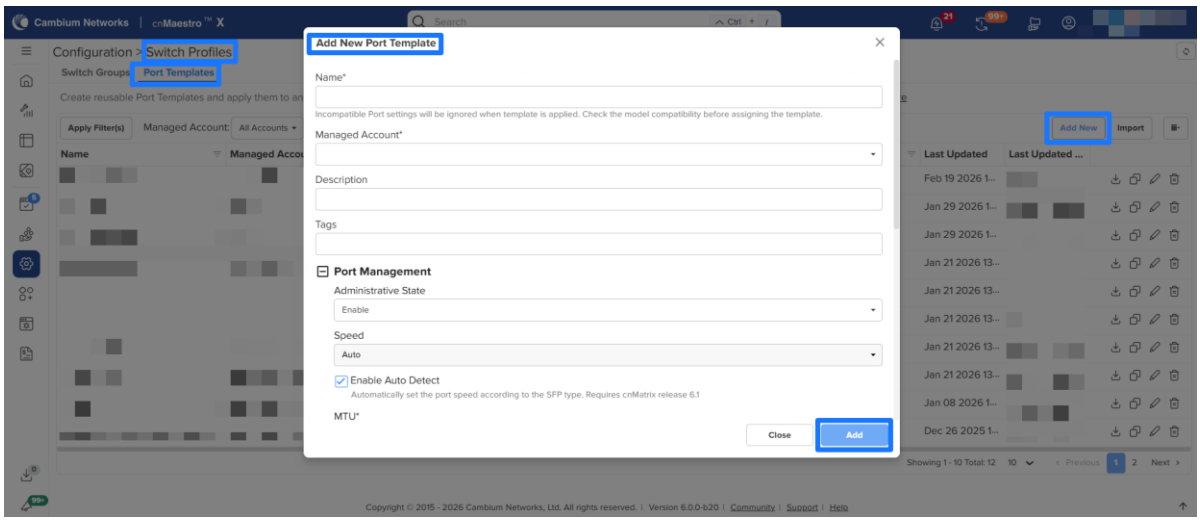


cnMatrix: Port Templates and Model based Port Configuration

This release introduces significant improvements to port-level configuration within Switch Profiles, enabling administrators to streamline switch provisioning and maintain consistent configurations across cnMatrix models using Port Templates and Ports Configuration.

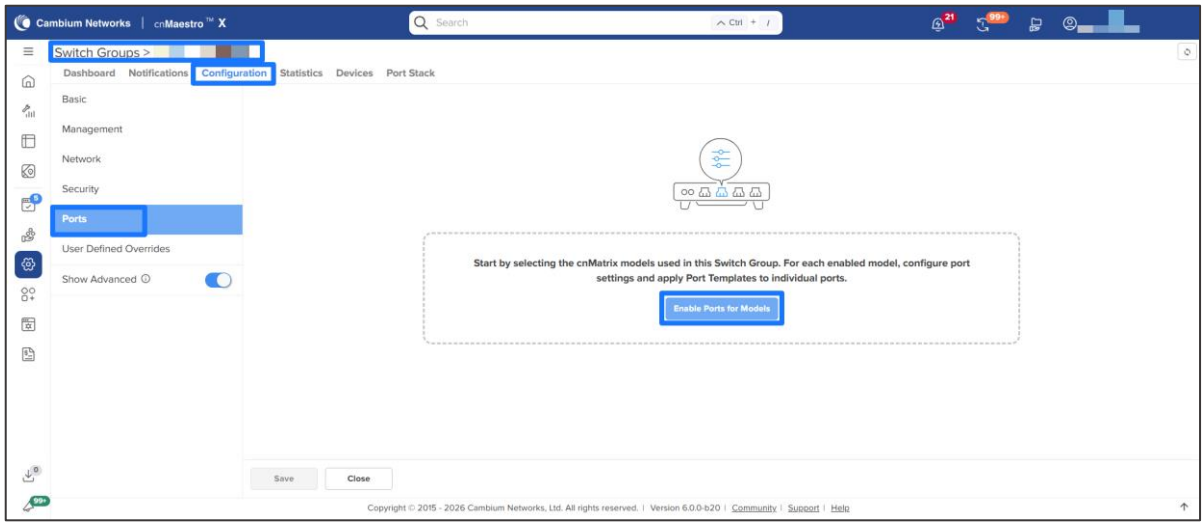
Port Templates

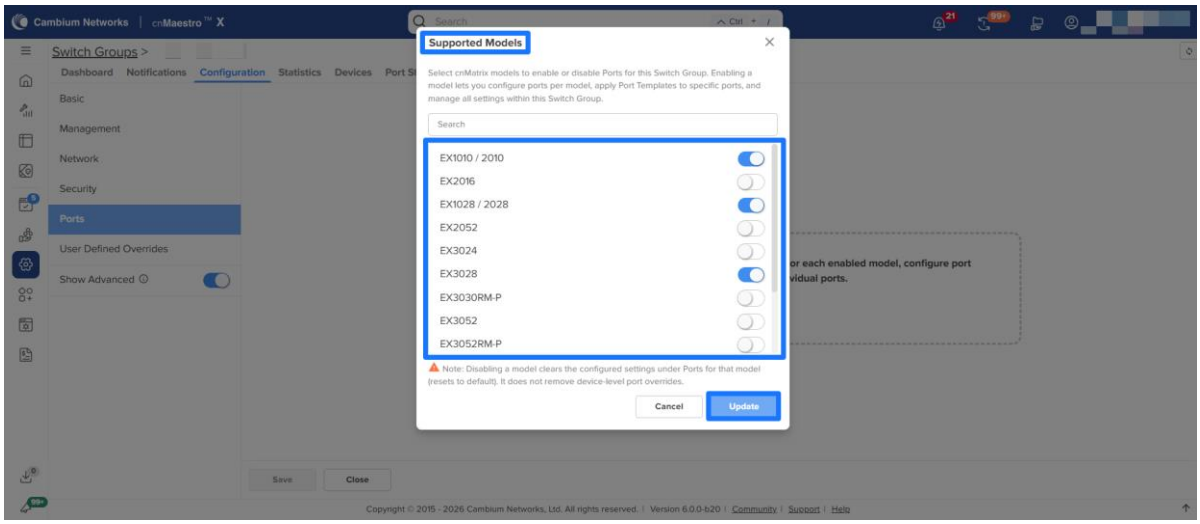
Port Templates allow administrators to create reusable, predefined port configurations and apply them to one or more ports within a Switch Group. When a template includes model-specific settings, the system automatically ignores unsupported parameters for switch models that do not support them.

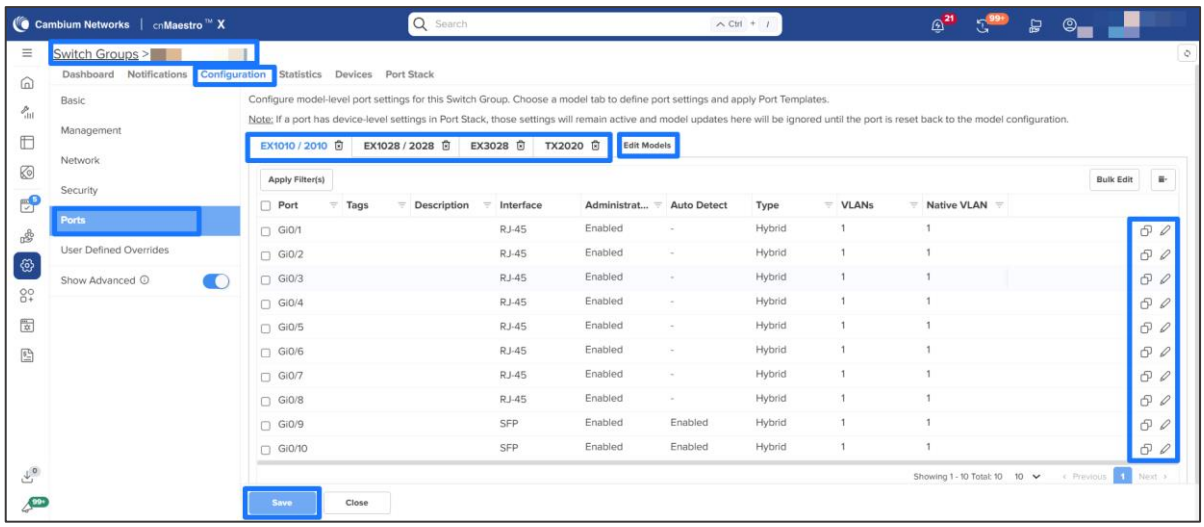


Model based Port Configuration

The new Ports Configuration feature provides centralized management of port-level settings for different cnMatrix switch models within a Switch Group. Administrators can enable or disable Ports Configuration by model and define consistent, model-specific configurations across large or distributed deployments.







Key Capabilities

Model-Based Configuration: Select supported cnMatrix models to activate Ports and manage configurations per model.

Template Assignment: Apply Port Templates to individual ports for faster setup and uniform behavior.

Granular Port Control: Configure VLANs, PoE, STP, rate limits, 802.1X, ACLs, and other port attributes at a per-port level.

Bulk Management: Update multiple ports simultaneously to accelerate deployment and configuration changes.

Safe Defaults: Disabling Port Mapping returns ports to their default configuration, ensuring a consistent baseline.

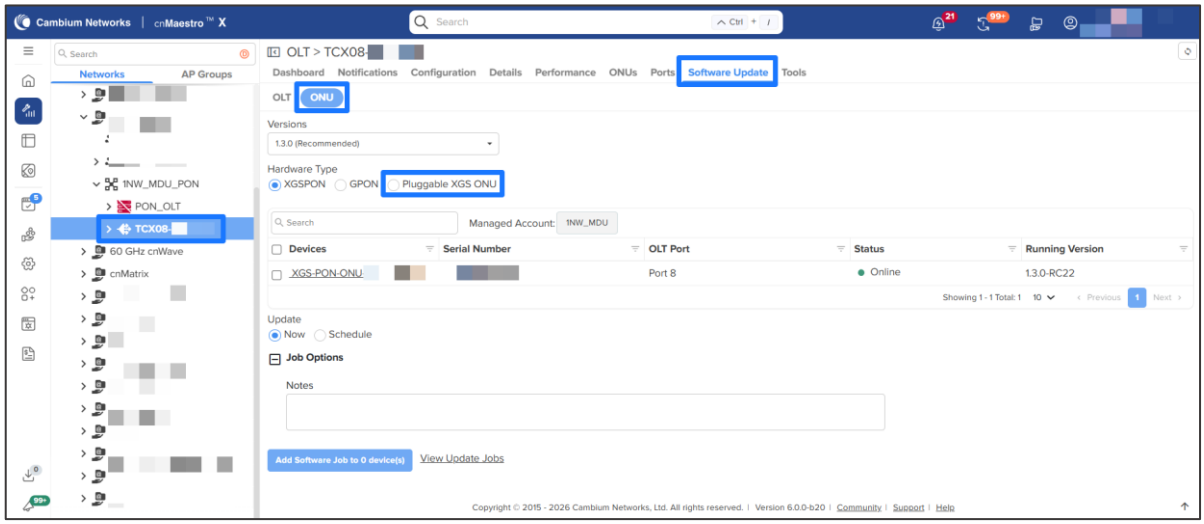
These enhancements support zero-touch provisioning, reduce configuration time, and help standardize switch behavior across diverse cnMatrix models.

Behavior Notes

Ports can be configured per model by selecting the appropriate switch model tab and assigning Port Templates to each port. Device-level changes made directly on the Ports tab take precedence over Port Configuration.

PON: Software Upgrade Support for Pluggable XGS ONUs

cnMaestro now supports software upgrades for **Pluggable XGS ONU devices**. Administrators can initiate and manage firmware upgrades, ensuring devices run the latest supported version of software.

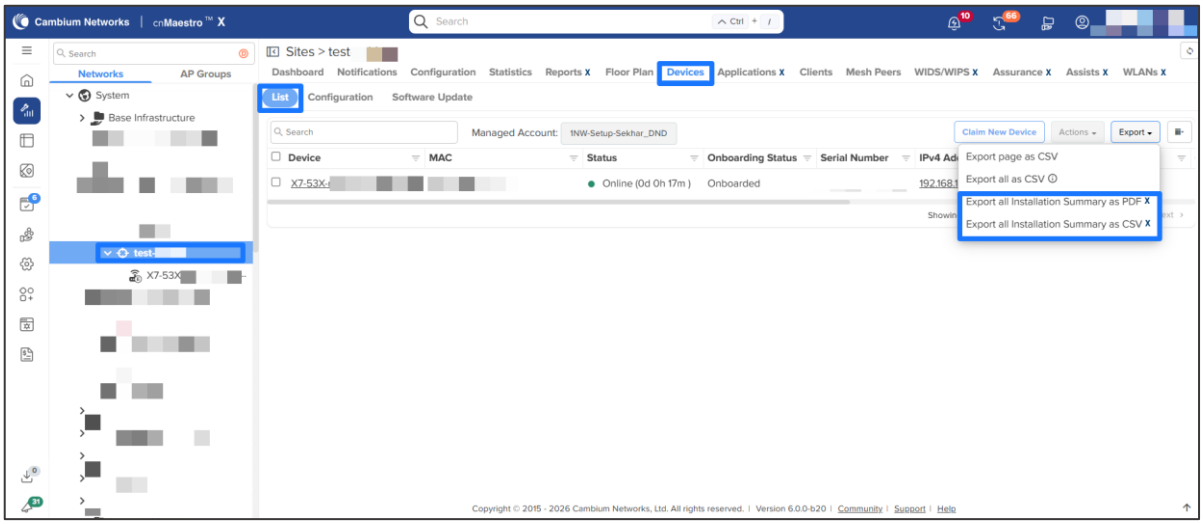


MarketApps Enhancements

Export Installation Summary per Site

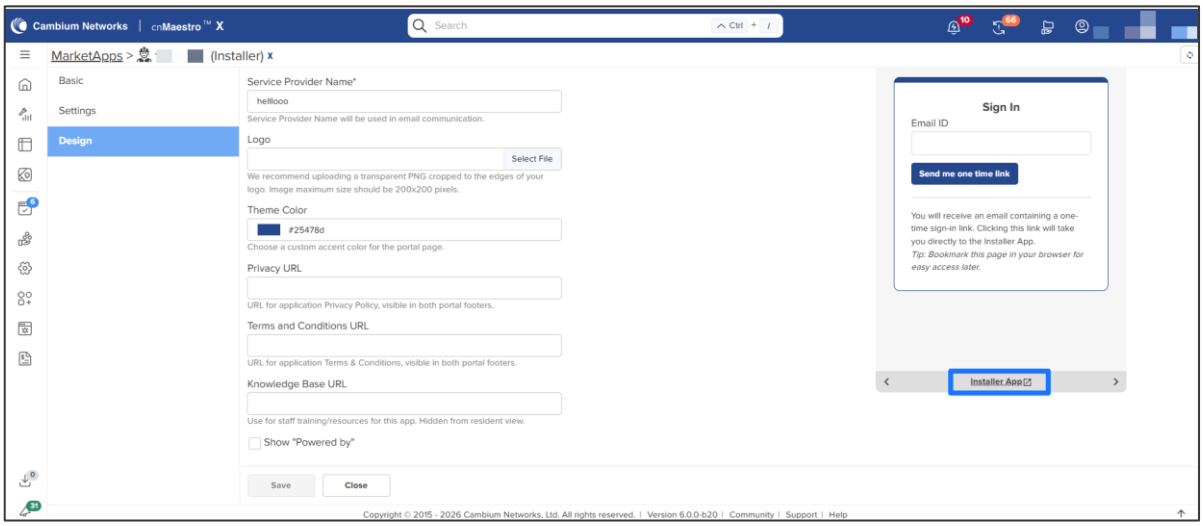
cnMaestro now supports exporting Installation Summary reports at the Site level. Users can export installation summaries for all devices within a selected Site in PDF or CSV format directly from ***Devices > List > Export***.

This enhancement streamlines reporting workflows and enables more efficient analysis and sharing of installation details.



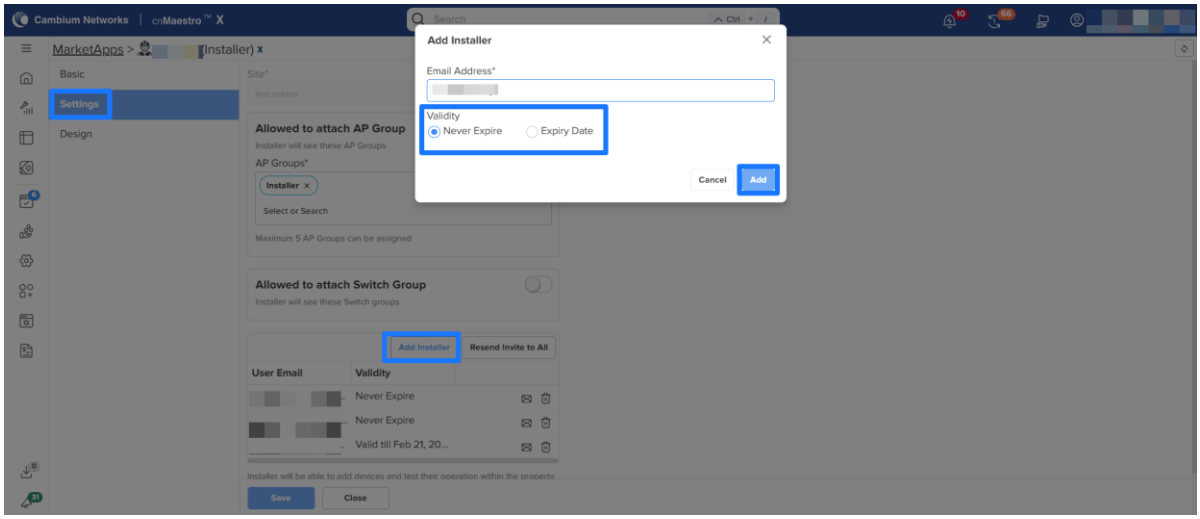
Single Sign In Support for Installer App

cnMaestro Admins can now navigate directly from cnMaestro to the Installer App and edit permitted installation-related fields as needed. This enhancement improves operational flexibility and reduces workflow friction.



Allow MSP admin to invite an installer with an expiry date

A new **expiry date field** is introduced while inviting Installer users. Administrators can now define a validity period during user invitation. Once the specified expiry date is reached, the Installer user account will be **automatically deleted** from the system.

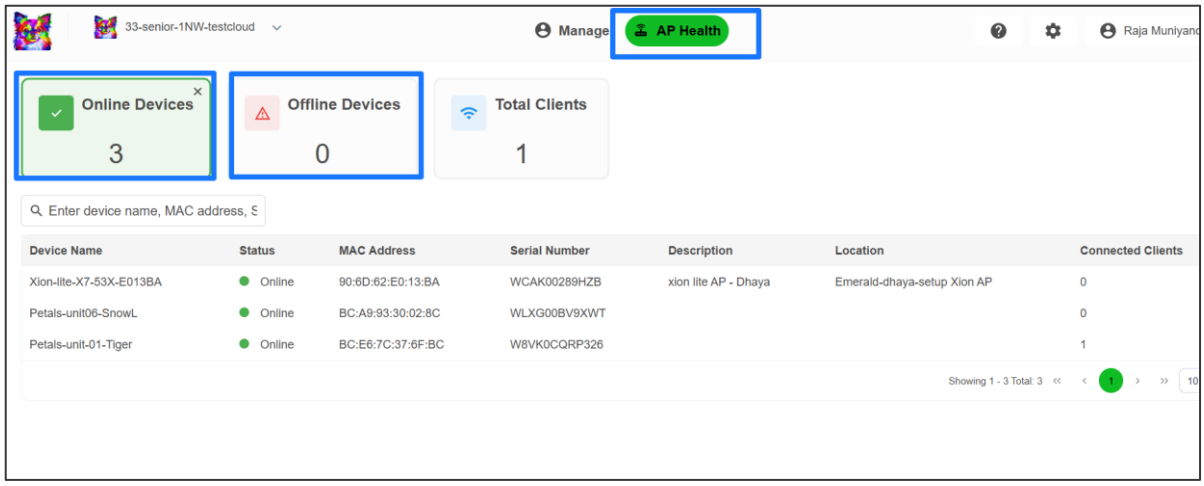


Installer App – Installation Summary Popup Enhanced for Desktop View

The Installation Summary pop-up in the Installer App has been enhanced to provide an optimized desktop viewing experience, improving usability and readability on larger screens.

Online/Offline filter for AP Health in MarketApps

Added support for Online/Offline filter in AP Health under the manager portal.



Miscellaneous Enhancements

Extended Time Range Support for Site Dashboard Metrics

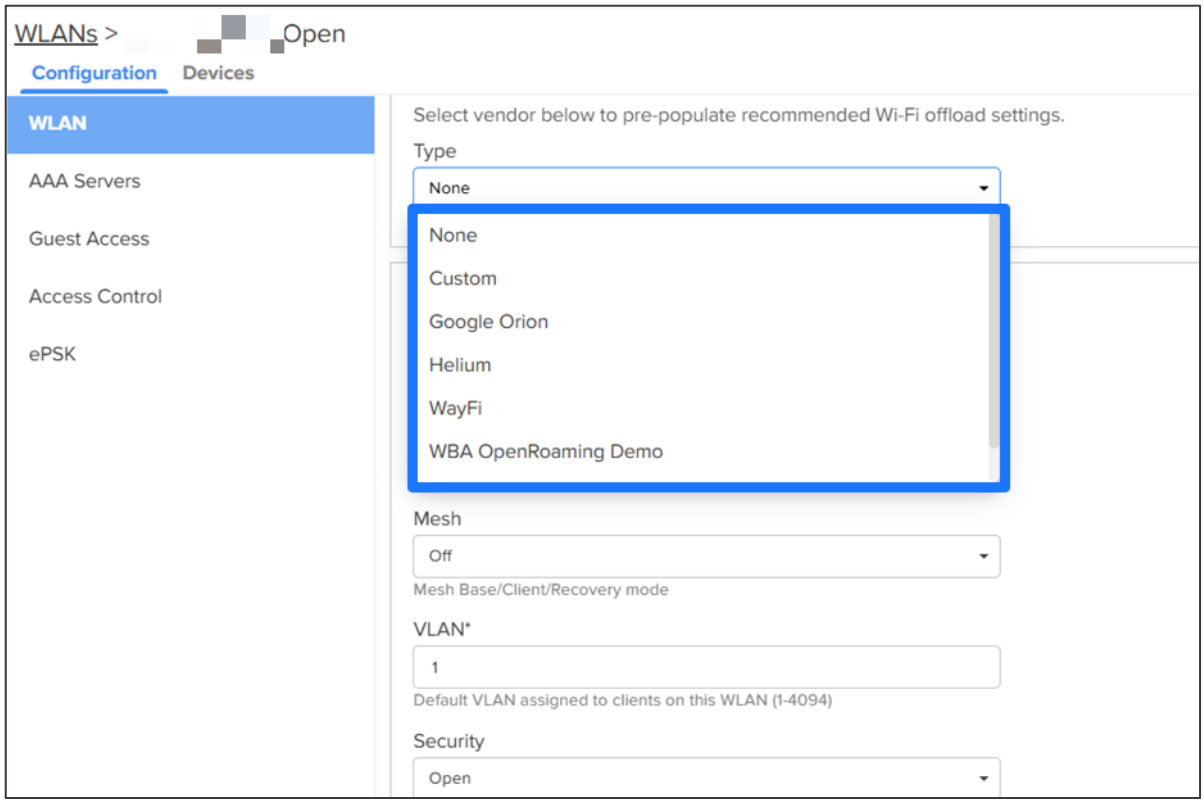
The Site Dashboard now supports an expanded time range of up to 30 days (previously 7 days) for the **Clients Stacked by Band** and **Throughput** widgets. This enhancement provides improved historical visibility and enables more comprehensive performance analysis at the site level.

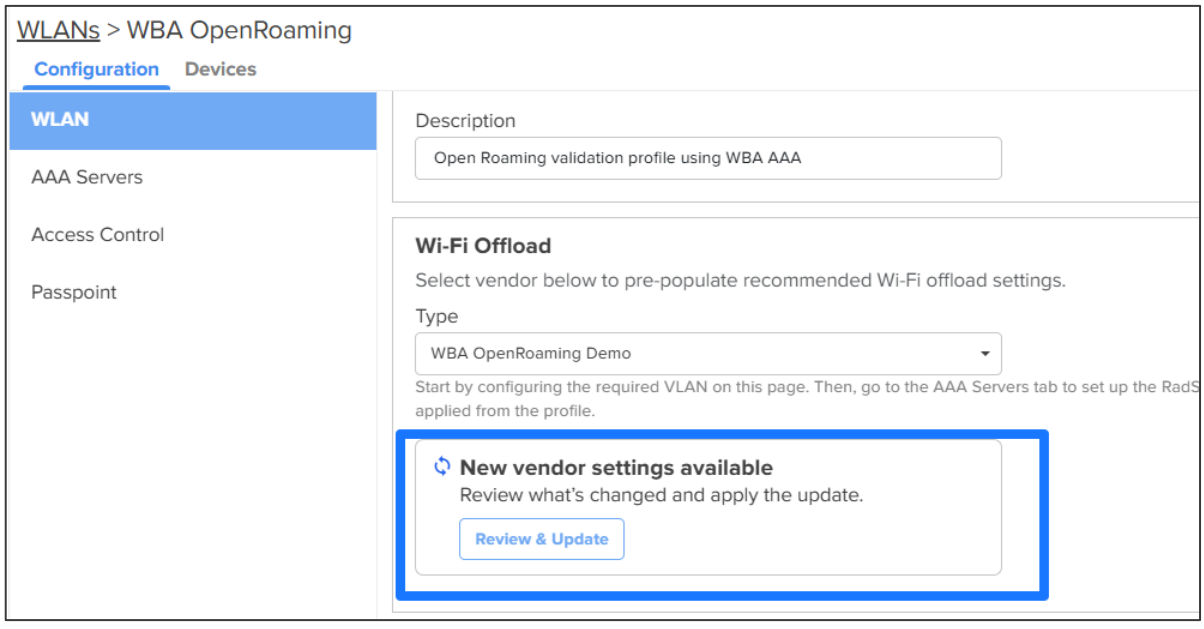
Wi-Fi Offload Enhancement

Added support for new Wi-Fi offload vendors, including Google Orion and Helium.

Additionally, when a configuration update is made to a Wi-Fi offload vendor in the backend, a trigger is generated to notify the system. Upon receiving the trigger, the system identifies WLANs associated with the updated offload vendor. Users can then review and apply the latest configuration as needed.

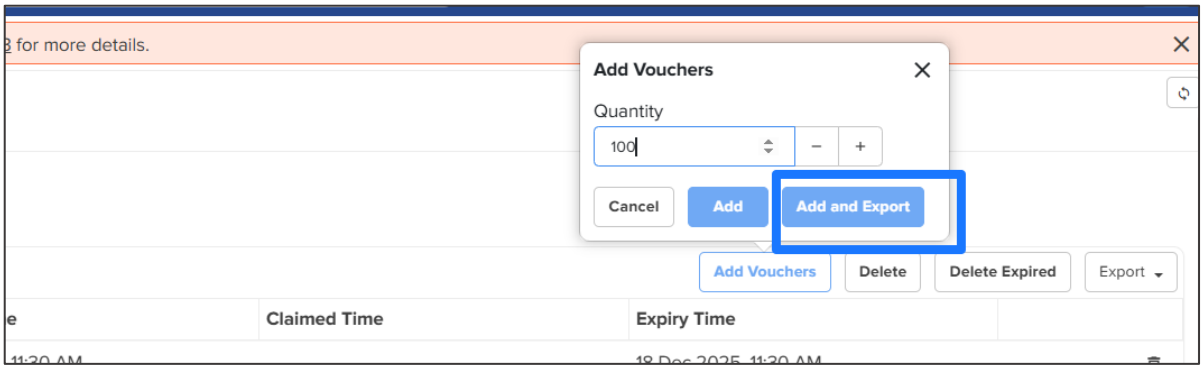
This enhancement improves configuration accuracy and ensures the timely synchronization of Wi-Fi offload settings.





Generate and Export the Vouchers

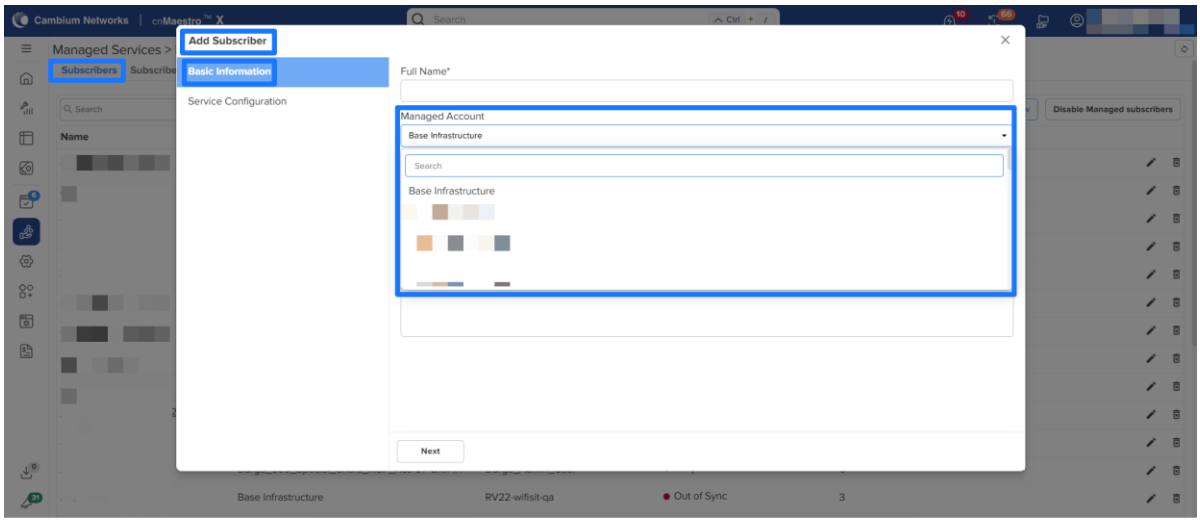
This option allows Users to “Generate and Export” Vouchers at the time of voucher generation.



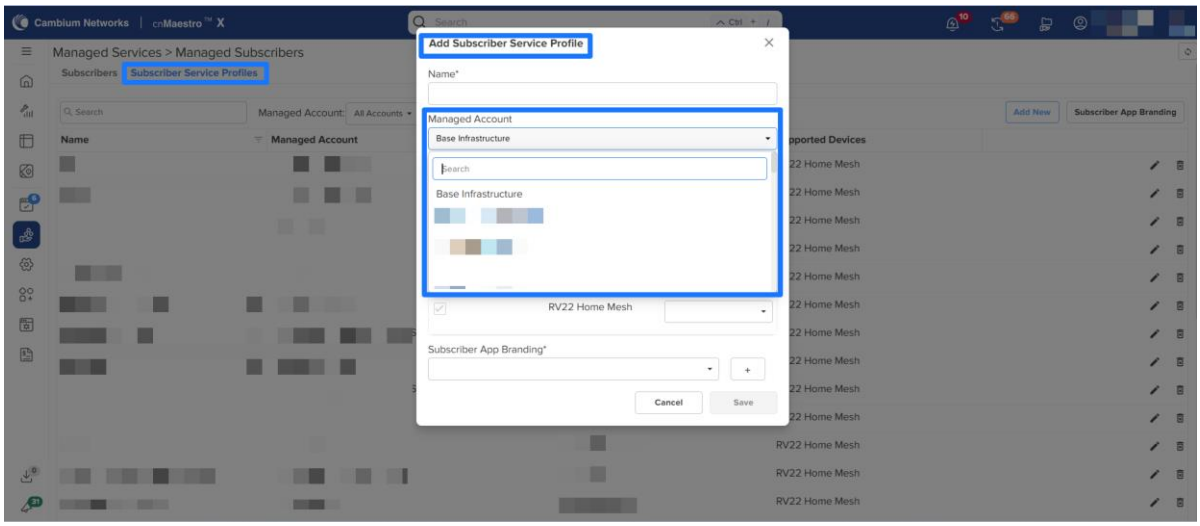
Managed Account Selection Support for Managed Subscribers (RV22)

Managed Account selection is now enabled for Managed Subscribers on RV22 devices. Administrators can select the appropriate Managed Account while managing Subscribers, Subscriber Profiles, and Branding configurations using a dropdown available on both listing and detail pages. Added **Managed Account dropdown** in the following screens:

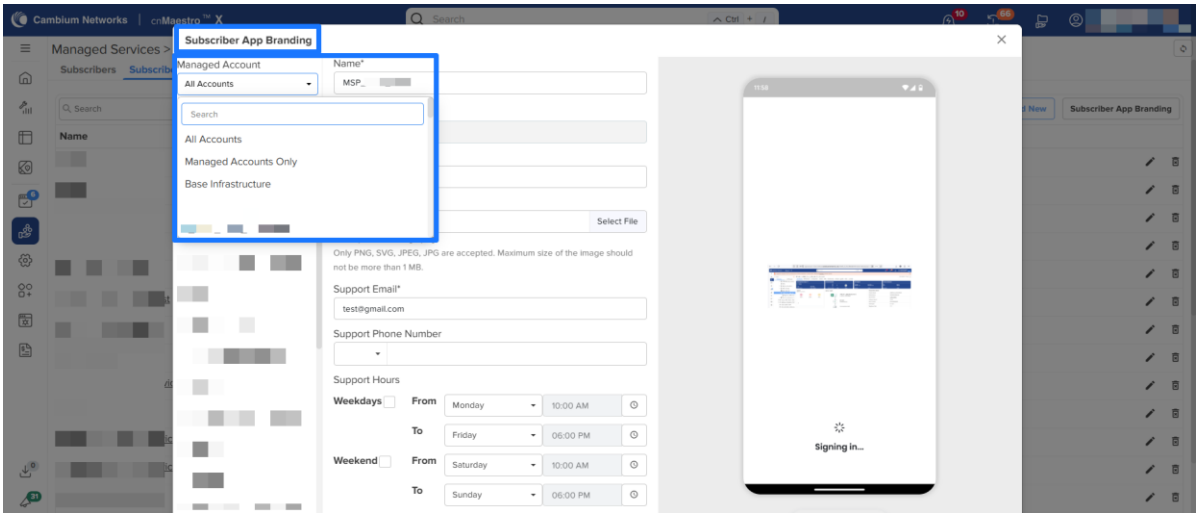
- Subscriber Listing and Details



- Subscriber Profile Listing and Details



- Branding Listing and Details

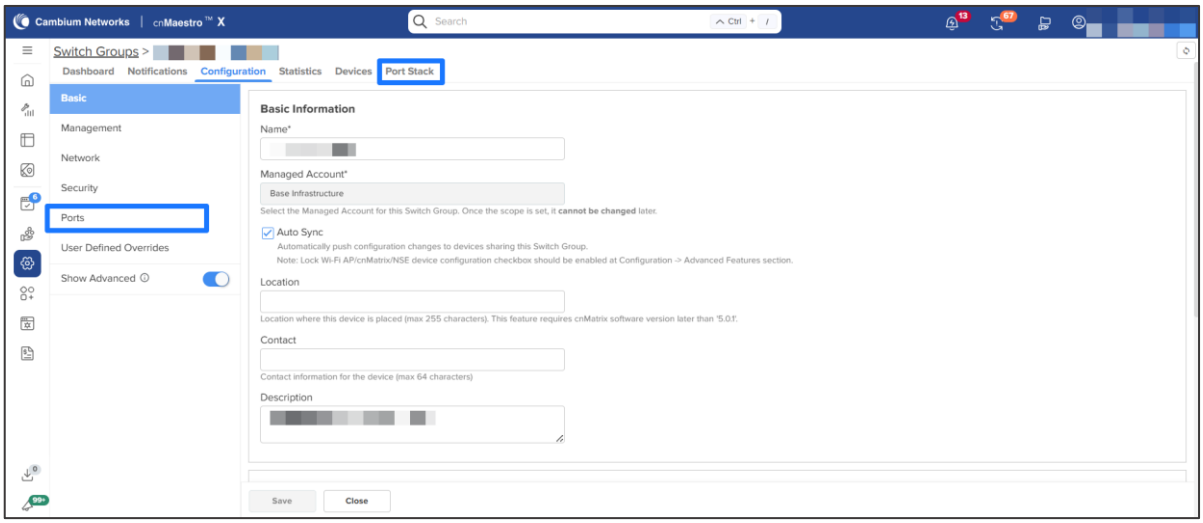


Switch Group UI Terminology Updates

Certain tabs and sections within **Switch Group** have been renamed to improve clarity and consistency:

- **Port Mapping** is now renamed to **Ports**
- **Ports** tab is now renamed to **Port Stack**

All related help text, tooltips, and pop-up information messages have been updated accordingly to reflect the new terminology.

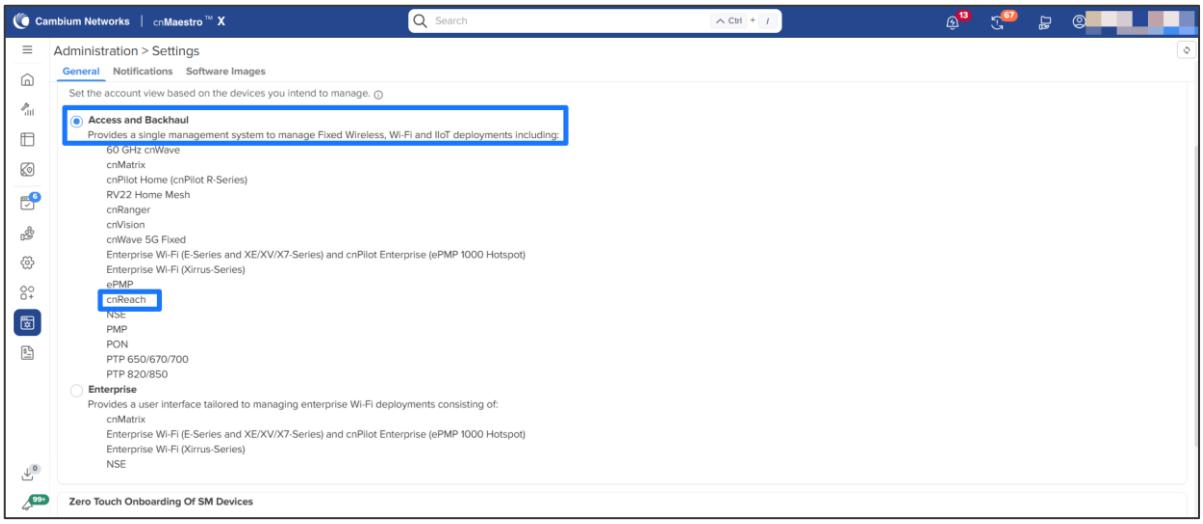


Removal of Industrial Internet Account Type

Starting with the **6.0.0 release**, the **Industrial Internet account type** has been completely removed from cnMaestro and now supports only the following account types:

- **Access & Backhaul**
- **Enterprise**

Creation of new Industrial Internet accounts is no longer supported, and existing accounts have been migrated to the **Access & Backhaul account type**. To ensure continuity, **cnReach device** management has been migrated to the **Access & Backhaul account type**, preserving full functionality and device management capabilities.



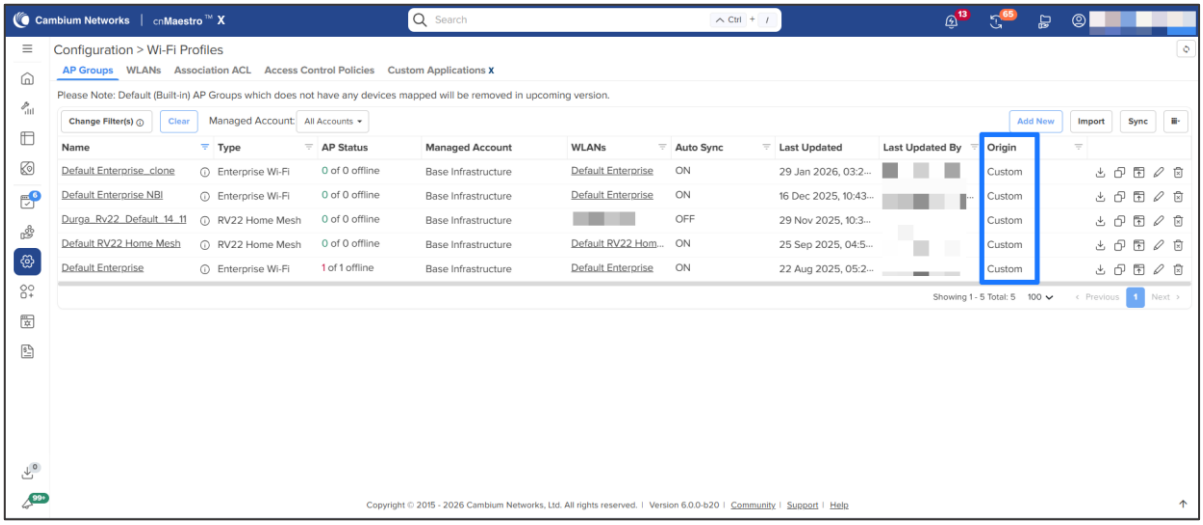
Removal of Default Group and Shared Scope Support

Starting with the **6.0.0 release**, cnMaestro no longer supports the **Default Group** for Enterprise AP, Switch, NSE, and RV22 device types. Devices must now be associated with explicitly created groups to ensure clearer configuration management and policy control.

In addition, the **"Shared" scope** is no longer supported for new configurations. The Shared scope option has been removed from configuration workflows and is no longer available for Templates.

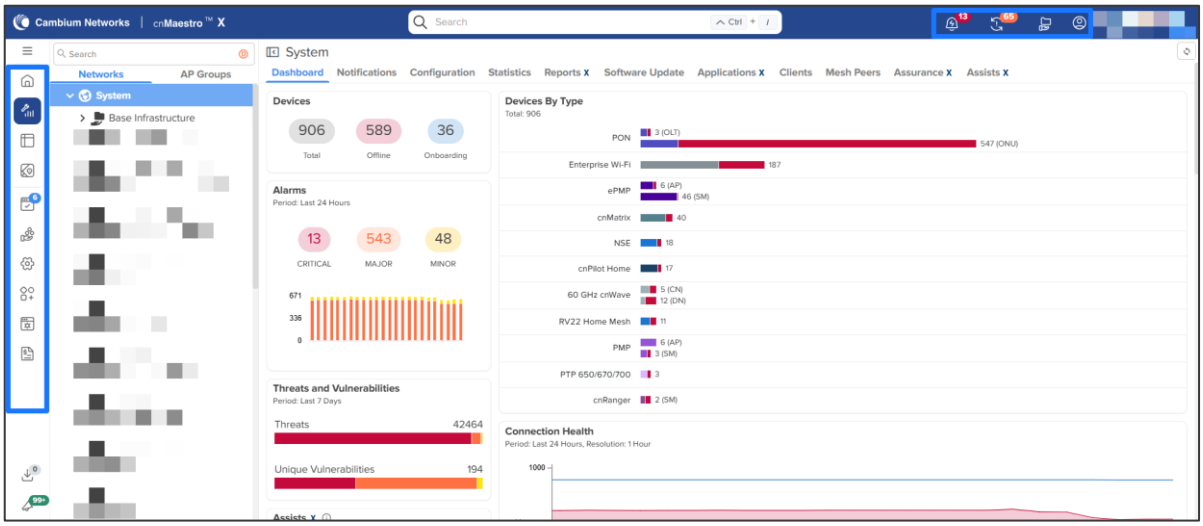
As part of this change, built-in configurations are now handled as follows:

- Built-in configurations mapped to devices are automatically converted to **custom** configurations.
- Built-in configurations previously modified by users are converted to **custom** configurations.
- Built-in configurations can now be deleted if no longer required



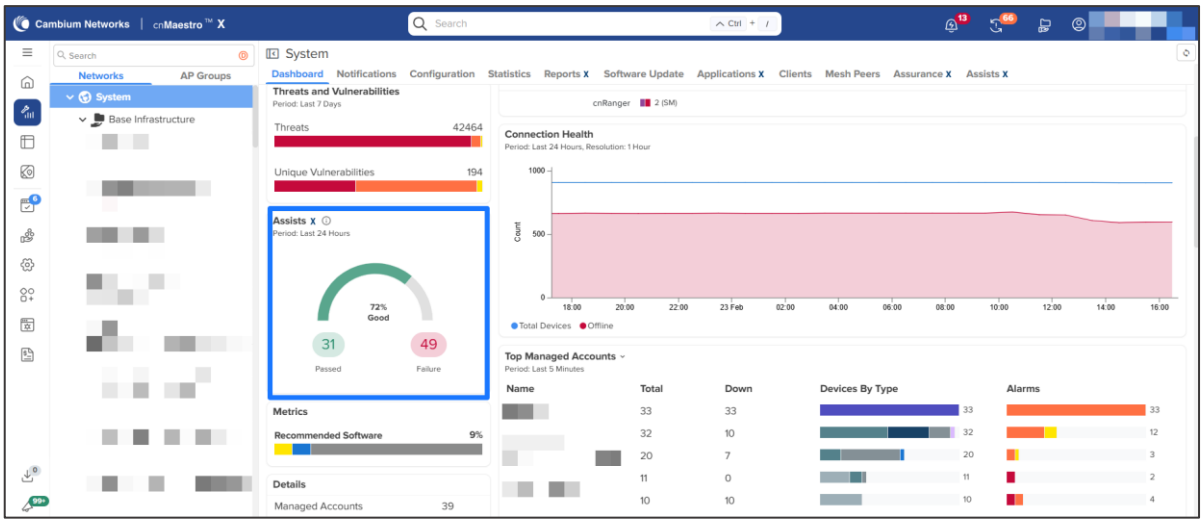
Side Navigation and Header Icons Revamp

cnMaestro has refreshed the side navigation and header icons by replacing legacy Font Awesome icons with modern SVG-based icons. This update enhances visual clarity, improves design consistency, and provides better scalability across the user interface for a more polished user experience.



Assists – KPI Visualization Enhancement Across All Levels

Assists KPI visualization has been updated across all hierarchy levels to align with standard health indicator conventions. Success metrics are now displayed on the left (green), and failure metrics are shown on the right (red)



API Updates X

Deprecated APIs

Request Method	Path	Deprecated In	Sunset In	Replacement	Details
Guest Access API					
GET	/portals	5.2.0	6.1.0	/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	6.1.0	/api/v2/easypass/{portalName}	
GET	/portals/{portalName}/events	5.2.0	6.1.0	/api/v2/easypass/{portalName}/sessions/login_events	
PUT	/portals/{portalName}/whitelist	5.2.0	6.1.0	/api/v2/easypass/{portalName}/configuration/allowed_domains	
GET	/portals/{portalName}/voucher_plans	5.2.0	6.1.0	/api/v2/easypass/{portalName}/voucher_plans	
GET	/portals/{portalName}/vouchers/{voucherPlan}	5.2.0	6.1.0	/api/v2/easypass/{portalName}/voucher_plans/{voucherPlan}/vouchers	
POST	/portals/{portalName}/vouchers/{voucherPlan}/generate	5.2.0	6.1.0	/api/v2/easypass/{portalName}/voucher_plans/{voucherPlan}/vouchers/generate	
cnArcher Installation Summary					
GET	/api/v2/cnarcher/installation/summary	6.0.0	6.1.0	/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	6.1.0	/api/v2/installation/summary/{mac}	

Deprecated Fields

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
AP Groups						

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
GET	/wifi_enterprise/ap_groups	auto_rf_channel_selection_mode	5.2.1	6.1.0	N/A	These fields are no longer relevant for Auto RF configuration.
GET	/wifi_enterprise/ap_groups	channel_utilization_threshold	5.2.1	6.1.0	N/A	
POST	/wifi_enterprise/ap_groups	auto_rf_channel_selection_mode	5.2.1	6.1.0	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	6.1.0	N/A	
POST	/api/v2/wifi_enterprise/ap_groups	shared	6.0.0	6.1.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.1.0
POST	/api/v2/wifi_xirrus/ap_groups	shared	6.0.0	6.1.0	N/A	
Wi-Fi Enterprise						
GET	/devices/clients	ap_mac	5.0.0	6.1.0	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 property of an AP device.

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
GET	/devices/wired_clients	ap_mac	5.0.0	6.1.0	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	6.1.0	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	6.1.0	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	6.1.0	network	Renamed the deprecated fields to relevant ones.
GET	/api/v2/cnmatrix/switch_group	tid	5.2.5	6.1.0	tower	

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
	s_ports/{switch_group_name}					
GET	/api/v2/cnmatrix/switch_groups_ports/{switch_group_name}	mcid	5.2.5	6.1.0	managed_account	
GET	/api/v2/cnmatrix/switch_groups_ports/{switch_group_name}	eType	5.2.5	6.1.0	N/A	eType is redundant as the API endpoint is specific to cnMatrix itself.
POST	/api/v2/cnmatrix/switch_groups	shared	6.0.0	6.1.0	N/A	The shared field is deprecated and will be removed in version 6.1.0
Events API						
GET	/api/v2/events	offset total	6.0.0	6.1.0	continuation_token	The offset request parameter is deprecated in 6.0.0 and will be removed in version 6.1.0 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 6.1.0 release.
Device Performance API						
GET	/api/v2/devices/{mac}/performance	offset total	6.0.0	6.1.0	continuation_token	The offset request parameter is deprecated

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
						in 6.0.0 and will be removed in version 6.1.0 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 6.1.0 release.
NSE Threats API						
GET	/api/v2/devices/nse/{mac}/threats	**offset** **total**	**6.0.0**	**6.1.0**	continuation_token	The offset request parameter is deprecated in 6.0.0 and will be removed in version 6.1.0 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 6.1.0 release.
WLANs						
POST	/api/v2/wifi_enterprise/wlans	ga_cn_portal_name	6.0.0	6.1.0	use /api/v2/easypa	The ga_cn_port

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
PUT	/api/v2/wifi_enterprise/wlans/{wlan_name}	ga_cn_portal_name	6.0.0	6.1.0	ss/{portalName}/wlans to attach and detach cnmaestro portal types.	al_name field is deprecated in 6.0.0 and will be removed in release 6.1.0. The cnmaestro value for the ga_portal_mode field is deprecated in 6.0.0 and will be removed in release 6.1.0. Please use /api/v2/easypass/{portalName}/wlans to attach and detach cnmaestro portal types.
POST	/api/v2/wifi_enterprise/wlans	shared	6.0.0	6.1.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.1.0
Access Control Policy						
POST	/api/v2/wifi_enterprise/access_control	shared	6.0.0	6.1.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.1.0
NSE Groups						
POST	/api/v2/nse/nse_groups	shared	6.0.0	6.1.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in

Request Method	Path	Field Name	Deprecated In	Sunset In	Replacement	Details
						version 6.1.0
Configuration Templates						
POST	/api/v2/device/configuration/templates	shared	6.0.0	6.1.0	N/A	The shared field is deprecated in 6.0.0 and will be removed in version 6.1.0

Update notice for existing APIs

Request Method	Path	Details
Device Performance API		
GET	/api/v2/devices/{mac}/performance	Enhanced pagination support with continuation token-based pagination. In the current version, offset and total fields are returned in responses for backward compatibility when using offset pagination. When using continuation_token pagination, continue pagination until next_continuation_token is absent. Note: offset and total fields will be completely removed in version 6.1.0 release.
Events API		
GET	/api/v2/events	Enhanced pagination support with continuation token-based pagination. In the current version, offset and total fields are returned in responses for backward compatibility when using offset pagination. When using continuation_token pagination, continue pagination until next_continuation_token is absent. Note: offset and total fields will be completely removed in 6.1.0 release.
NSE Threats API		
GET	/api/v2/devices/nse/{mac}/threats	Enhanced pagination support with continuation token-based pagination. In the current version, offset and total fields are returned in responses for backward compatibility when using offset pagination. When using continuation_token pagination, continue pagination until next_continuation_token is absent. **Note**: offset and total fields will be completely removed in version 6.1.0 release.
GET	/api/v2/devices/nse/{mac}/threats	Added rule_description, action, protocol and client_mac fields.

Request Method	Path	Details
NSE Groups		
POST	/api/v2/nse/nse_groups	Applications list is now defined in schema with explicit distinction between legacy and new apps. Unsupported apps will return an error — verify allowed apps against the updated schema. Using new apps will return a warning, as they may not function correctly on NSE versions less than 2.1
PUT	/api/v2/nse/nse_groups/{nse_group_name}	Applications list is now defined in schema with explicit distinction between legacy and new apps. Unsupported apps will return an error — verify allowed apps against the updated schema. Using new apps will return a warning, as they may not function correctly on NSE versions less than 2.1
POST	/api/v2/nse/nse_groups	Added validation to not allow spaces and not to start with a non-alphabetical character in the name of traffic shapping, failover policy and outbound filter rules in NSE Groups.
PUT	/api/v2/nse/nse_groups/{nse_group_name}	Added validation to not allow spaces and not to start with a non-alphabetical character in the name of traffic shapping, failover policy and outbound filter rules in NSE Groups.
POST	/api/v2/nse/nse_groups	Added name field for flow preferences in NSE Groups and it is mandatory.
PUT	/api/v2/nse/nse_groups/{nse_group_name}	Added name field for flow preferences in NSE Groups and it is mandatory.
Access Control Policy		
POST	/api/v2/wifi_enterprise/access_control/	Applications list is now defined in schema with explicit distinction between legacy and new apps. Unsupported apps will return an error — verify allowed apps against the updated schema. Using new apps will return a warning, as they may not function correctly on Wi-Fi versions below 7.2.
PUT	/api/v2/wifi_enterprise/access_control/{acp_name}	Applications list is now defined in schema with explicit distinction between legacy and new apps. Unsupported apps will return an error — verify allowed apps against the updated schema. Using new apps will return a warning, as they may not function correctly on Wi-Fi versions below 7.2.
60 GHz cnWave Network Config Optimization		
POST	/api/v2/cnwave60/networks/{network_id}/optimization/triggerGolayOptimization	Added support to trigger golay optimization for 60 GHz cnWave networks.
POST	/api/v2/cnwave60/networks/{network_id}/optimization/triggerChannelOptimization	Added support to trigger channel optimization for 60 GHz cnWave networks.
POST	/api/v2/cnwave60/networks/{network_id}/optimization/triggerPolarityOptimization	Added support to trigger polarity optimization for 60 GHz cnWave networks.

New APIs added in 6.0.0

Request Method	Path	Details
Installation Summary		
GET	/api/v2/installation/summary	Added support to retrieve installation summary details for all supported app types (cnArcher, enterprise-installer, etc.) under a site or tower. Optionally filter by specific app type using the type query parameter.
GET	/api/v2/installation/summary/{mac}	Added support to retrieve installation summary details for all supported app types (cnArcher, enterprise-installer, etc.) under a site or tower. Optionally filter by specific app type using the type query parameter.
60 GHz cnWave		
POST	/api/v2/cnwave60/devices/{mac}/ping	Added support to initiate ping tests on cnWave60 devices. Supports three modes: node-to-node ping (using device names), IPv4 address ping, and IPv6 address ping.
GET	/api/v2/cnwave60/devices/{mac}/ping	Added support to retrieve ping test results using the action ID. Returns ping statistics including packets sent, received, loss percentage, and RTT (min/avg/max).
POST	/api/v2/cnwave60/networks/onboard_controller	Added support to claim and onboard an E2E Controller Network (only supports onboard controllers).
EasyPass WLANs		
PUT	/api/v2/easypass/{portalName}/wlans	Added support to manage WLAN assignments for EasyPass portals. Allows assigning and unassigning WLANs.
Security		
GET	/api/v2/devices/{mac}/dns_filtering	Added support to retrieve DNS filtering events details for NSE devices

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
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	

Family	Model	Version
	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:

** Known issues in Release 5.2.5 and resolved in Release 6.0.0*

ID	Details
CNSSNG-51288	DHCP Option-82 – Custom messages did not work when keywords such as APMAC, BSSID, and SSID were entered in uppercase.
CNSSNG-51283	Workflow for Teams – Update the Webhooks syntax checker to allow duplicate keys when they exist in different JSON scopes, ensuring valid nested structures are accepted without validation errors.
CNSSNG-51231	Easypass Onboarding – Users who reached the device limit were redirected to the splash page but unable to release or remove existing devices
CNSSNG-51118	ePSK – Send ePSK email shows default duration as 1440 hours instead of configured session duration.
CNSSNG-50972	Unable to save Switch Group configuration after creating a PBA rule with the DEFAULT type.
CNSSNG-50464	Connection Events under Assurance intermittently display the client MAC address instead of the AP name.
CNSSNG-50442*	Invalid JSON error occurs when selecting a specific account under Manage Subscription Scope.
CNSSNG-50327	EasyPass onboarding users imported via CSV without Activation and Expiration values are displayed with a default 7-day expiration, even though the backend values are set to 0
CNSSNG-50317*	MTU value set on the network section of the switch group is not reflecting on port mapping and ports tab correctly
CNSSNG-50242	Device search fails when more than 20 unmanaged devices are present in a network, site, or AP group.
CNSSNG-50072*	When switch group has multiple switches, Switch name filter is not working properly after applying ACL on port
CNSSNG-49872*	Upgrade to Security Plus fails without a clear Tier 31 deficit message (required for NSE4000).
CNSSNG-49854*	Senior Living MarketApp: Wi-Fi support app and Front desk app link is not accessible from Safari browser
CNSSNG-47958	Clicking Edit Ports in cnMaestro for cnMatrix navigates to the wrong switch
CNSSNG-47809	Error occurs while adding a user; user not visible under Administrators > Users but appears in Account Lookup.
CNSSNG-46218	Displays an IPv6 address in the IPv4 address field on the AP Dashboard

ID	Details
CNSSNG-30412	NBI does not display proper error messages when testing boundary limit values for band parameters.

Known Issues

This section lists the known issues in the cnMaestro releases:

** Reported in Release 6.0.0*

ID	Details
CNSSNG-51337*	Unable to do export as installation summary as PDF when 500+ APs are installed via 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-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
CNSSNG-50856*	Device Type incorrectly identified for cnMatrix's Wired Clients
CNSSNG-50581*	Same alarm name displayed under Major and Notify severity
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-50277	Config push is failed with error when port channel with hybrid mode has multiple VLANs
CNSSNG-50177	DL and UL values in WLANs tab updating with delay during 5-minute interval
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-49799	Managed Account displays as 'N/A' in reports when a newly created managed account is used
CNSSNG-49726	Installer MarketApp: Device Overrides are not getting applied if different device model is replaced
CNSSNG-48159	'Component Carrier Properties' are not included in the exported report from PMP AP level > SMs tab > Export

ID	Details
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-46593	Unsupported alarms are displaying for devices for cnMatrix, Wi-Fi AP and PON
CNSSNG-47207	Switch Group rename causes cnMatrix devices to go Not In Sync
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-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
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.
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

ID	Details
CNSSNG-41870	Reboot from the tree menu displays an error: "Failed to send Reboot command to device(s)" for PTP 8xx devices.
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-39026	The remaining time is wrong for End of Day (Midnight) and End of Week (Saturday) for the session duration.
CNSSNG-38801	Device not moving to the correct site/SM when changing subscriber.
CNSSNG-36850	Issue with the Device going out of sync with the PPPoE connection.
CNSSNG-36849	The Chile time zone is missing.
CNSSNG-36782	Home sites are not listed while moving devices from the inventory page.
CNSSNG-36723	Enabling the Show Interfering Sectors should not display all the towers under the network.
CNSSNG-36483	Application and Vulnerability tabs are missing for the wireless clients when NSE is offline.
CNSSNG-33861	Completed reports should be transferred to the Completed Column immediately when the jobs are complete.
CNSSNG-33660	The template should have a scroll bar.
CNSSNG-31613	Reporting layer memory usage.
CNSSNG-31029	For the responder role, the Site-to-Site VPN tunnel, the remote address field is not present.
CNSSNG-31006	If the site contains NSE, cnMatrix, and Wi-Fi AP, the devices are not sorted correctly.
CNSSNG-30927	Modify the remote subnet and local subnet fields under IPsec to have the option to enter the subnet in list form.
CNSSNG-30696	Changes are required if the IKE version 1 is selected.
CNSSNG-30691	Should not allow configuration of duplicate subnets in the remote subnet and the local subnet.
CNSSNG-28326	AP Groups/Sites/Towers list all types of devices while generating reports.
CNSSNG-28282	Scheduled Reports for the Expired device are completed.
CNSSNG-28151	The total device count and count displayed in the Recommended Software metrics do not match.

ID	Details
CNSSNG-26911	The NSE configuration page should use the Management IP as a clickable link, not the WAN Address.
CNSSNG-26188	Error on deleting the NSE device from the inventory page.
CNSSNG-25758	Able to see cnPilot R-series AP Groups in Enterprise View.
CNSSNG-25238	AOS device WebSocket does not disconnect for an X account downgraded to Pure ESS after Retention expired.
CNSSNG-25150	AOS device Configuration Job times out if the Device is in DHCP.
CNSSNG-24529	Multi-floor issue with Firefox browser.
CNSSNG-21396	Issues related to cnMatrix onboarding overrides.
CNSSNG-21271	SM status is missing in the AP details on the map.
CNSSNG-21264	Auto refresh does not work when Site/Tower/Device details are updated in the Network level map.
CNSSNG-20745	AP Count is -1 in Anchor when deregistering the device from Anchor.
CNSSNG-19275	Issues related to offline alarms of expired devices.
CNSSNG-19264	The unmanaged expired device approve button is not disabled.
CNSSNG-18923	After migration Reports Job page is empty due to cached data. **Workaround**: Clear Cache and Cookies after migration.
CNSSNG-16197	CBSDID search will not work when the device was synced from a tool without obtaining a grant first. **Workaround**: Perform a CBSDID search from domain proxy view on Cloud to obtain mac address, then perform MAC address search on tool to find the device.
CNSSNG-15595	cnMatrix Hostname falls back to old Hostname if the template is pushed for the first time (if a Switch Group already exists).
CNSSNG-15356	If a device has a weak serial number in a non-CBRS build, and the sector is imported first, the device will not contact cnMaestro.
CNSSNG-14030	CBRS race condition: SM “stuck” in cnMaestro during reparenting if import and start occur as SMs arrive in the onboarding queue. **Workaround**: To avoid this issue, follow the suggested SM reparenting procedures listed in the latest version of the Cambium CBRS standalone procedures document.
CNSSNG-12812	cnPilot R-series dual radio devices (r-201P, r-195W) AP Group country code/SSID configured from overrides getting applied only to the 2.4 GHz radio.

ID	Details
CNSSNG-11389	Microsoft Edge Browser does not support system OVA file upgrade. **Workaround**: Use Google Chrome browser
CNSSNG-11299	AP Regulatory Channel list support check needed for checking valid channels.

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.