User’s Guide

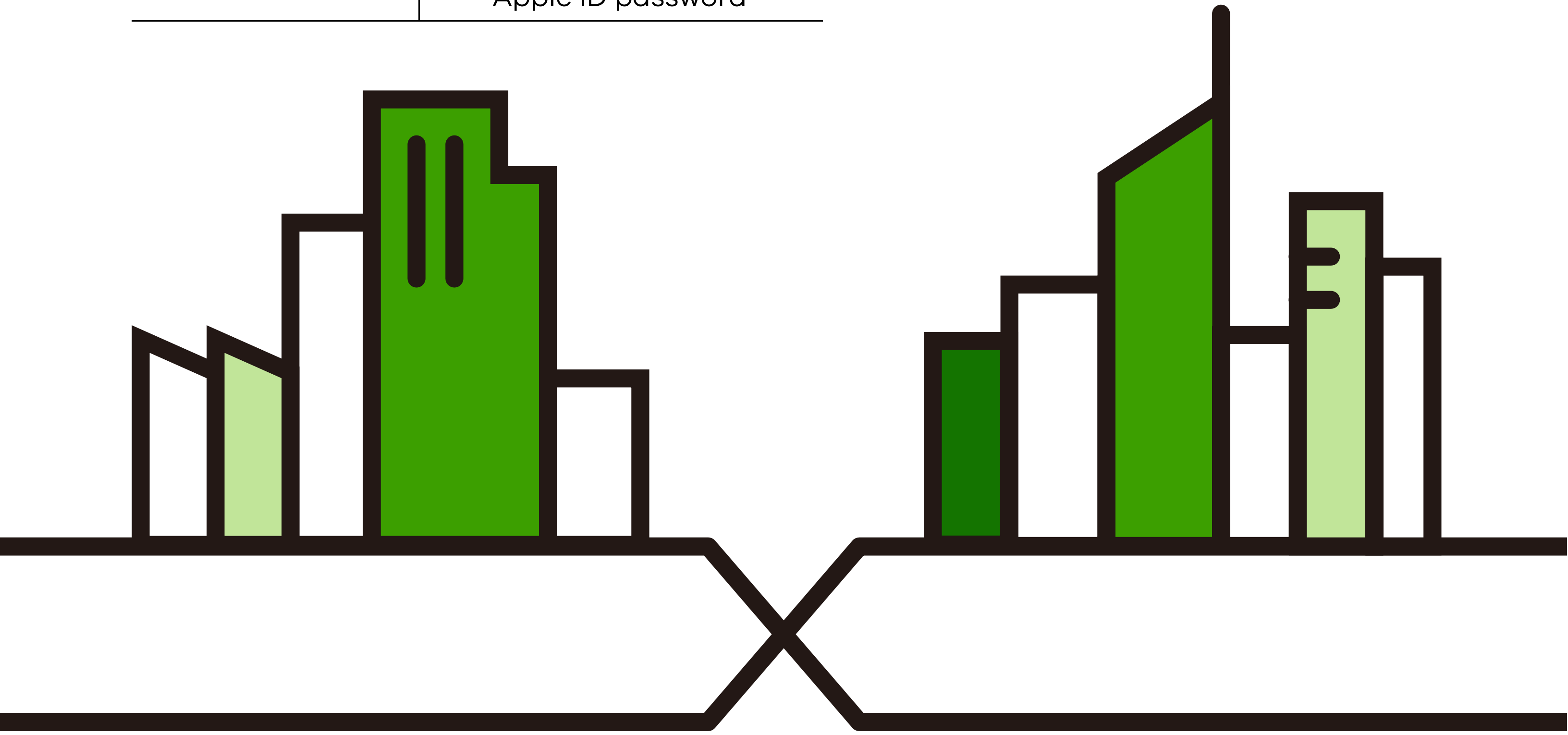
NCC

Nebula Control Center

Default Login Details

NCC URL	https://nebula.zyxel.com
User Name	Zyxel Account email Google Account email Apple ID email
Password	Zyxel Account password Google Account password Apple ID password

Version 18.30 Edition 1, 01/2025



Copyright © 2025 Zyxel and/or its affiliates. All Rights Reserved.

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a system managing a series of products. Not all products support all features. Screenshots and graphics in this book may differ slightly from what you see due to differences in release versions or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Note: The Nebula Device on each chapter refers to the Nebula AP, Switch, Security Appliance, Mobile Router, or Accessory respectively.

Related Documentation

- Nebula Device Quick Start Guide

  The Quick Start Guide shows how to connect the managed device, such as the Nebula AP, Switch, Security Appliance, or Mobile Router.

- Nebula Device User's Guide

  Refer to the individual Nebula managed device's User's Guide for information about how to set the device to be managed by the NCC and/or configure the device using its built-in Web Configurator,

- More Information

  Go to the **Nebula Control Center** to find other information on the NCC.

Table of Contents

PART I

Introduction & Getting Started Tutorials

CHAPTER 1 Introduction

1.1 NCC Overview

The Zyxel Nebula Control Center (NCC) is a cloud-based network management system that allows you to remotely manage and monitor Zyxel Nebula Mobile Routers, Access Points, Ethernet Switches, Security Appliances, and Accessories. A Nebula Mobile Router is an LTE or NR cellular 5G indoor or outdoor router that can be managed by Nebula. You need to set up a Zyxel Account in order to log into the NCC and manage your Nebula Devices, as discussed in Section 1.2.2 on page 25.

NCC feature support includes:

- System accounts with different privilege levels
  - Site Administrator: manage one site, which is a network that contains Nebula Devices
  - Organization Administrator: manage one or more organizations, which are sets of sites
- Multi-tenant management
- Inventory and license management
- Alerts to view events, such as when a device goes down
- Graphically monitor individual devices
- Securely manage Nebula Devices by using the Network Configuration Protocol (NETCONF) over TLS

Note: NCC supports IPv4 address only.

The following table describes the supported Nebula Devices.

Table 1 Supported Nebula Devices

CATEGORY	INCLUDED ZYXEL DEVICES
Hybrid Mobile Routers	LTE/NR Indoor/Outdoor Models
Security Router	SCR 50AXE, USG LITE 60AX
Security Gateways	NSG Series
Hybrid Security Firewalls	ZyWALL ATP / USG FLEX / USG FLEX H / USG20(W)-VPN Series Note: The following Nebula Devices do NOT have a P1 port: • USG FLEX 50 • USG FLEX 100 rev 2.0 • ATP100 rev 2.0
Hybrid Switches	NSW / GS / XGS / XS Series
Hybrid APs (Access Point)	NAP / NWA / WAC / WAX Series
Accessories	PoE12-3PD

Note: To view the list of Nebula Devices that can be managed through NCC, go to **Help** > **Device function table**.

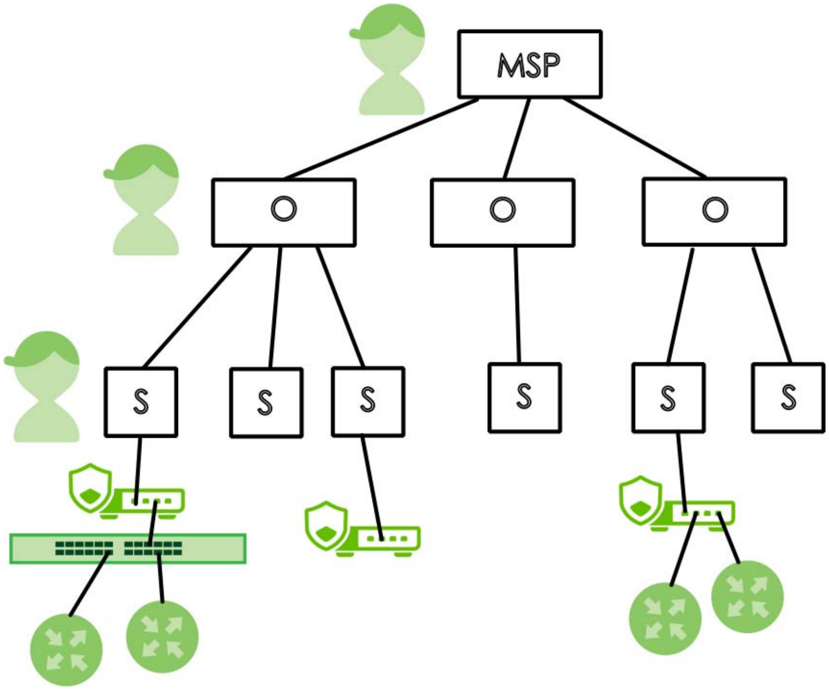
A hybrid device can operate in either standalone or Nebula cloud management mode. When the hybrid device is in standalone mode, it can be configured and managed by the Web Configurator. When the hybrid device is in Nebula cloud management mode, it can be managed and provisioned by the Zyxel Nebula Control Center (NCC).

1.1.1 MSP (Managed Services Provider) Portal

If you have an MSP license (as discussed in Section 14.1 on page 741), use the MSP menus for cross-organization management and branding.

A Managed Service Provider (MSP) network is a group of organizations that belong to the same organization administrator. With MSP, you can:

- View the organization summary and transfer licenses
- Copy the settings from a source organization to a destination organization
- Create administrators or groups of administrators (teams) and view their login details
- Assign administrators to multiple organizations
- Upload/replace/remove the dashboard logo on NCC
- Set the support contact details
- Configure MSP alerts to monitor Nebula Devices for unexpected events (for example, online/offline events)



1.1.2 Sites, Organizations, and Groups

To manage by how Nebula Devices are deployed, use the Site-wide, Organization-wide and Group-wide menus.

In the NCC, a site is a group of Nebula-managed devices in the same network. An organization is a group of sites. A group is a collection of two or more organizations. To use the NCC to manage your

Nebula Devices, each Nebula Device should be assigned to a site and the site must belong to an organization.

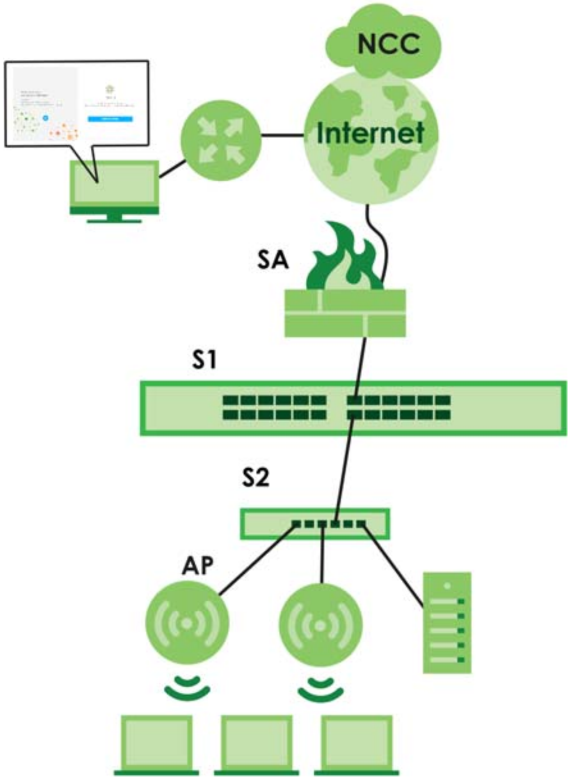
- A site can have multiple Nebula Devices, but can only belong to one organization.
- A site can be managed by more than one site or organization administrator.
- An organization can contain multiple sites and can be managed by more than one organization administrator.
- A Zyxel Account can be an organization administrator and/or site administrator in the NCC (see Section 12.3 on page 676).
- A site administrator can manage more than one site.

1.1.3 Mobile Router, Security Appliance, Switches, Access Points, and Accessories

To manage by Nebula Device type, use the Security Router, Mobile Router, Firewall, Security Gateway, Switch or Access Point menus.

In the following example, with an NCC organization administrator account, you can use NCC to remotely manage and monitor the Zyxel Nebula Security Appliances (**SA**), Ethernet Switches (**S**), and Access Points (**AP**).

Figure 1 NCC Example Network Topology



1.1.4 License Concept

The following section describes license concepts in NCC. Licenses unlock additional features in NCC. This means you purchase a license, assign the license to a Nebula Device, and you can then use the service in the site or organization that the Nebula Device is in.

1.1.4.1 Summary of NCC Licenses

There are three categories of licenses in NCC:

- Organization: These licenses unlock advanced features for sites and organizations.
- Security Service: These licenses unlock advanced security features on a Security Appliance/Firewall device.
- MSP: This license unlocks the MSP menu for an NCC user account.

The following table gives a summary of all licenses in NCC at the time of writing.

Table 2 Licenses Summary

LICENSE	CATEGORY	ASSIGN TO	DESCRIPTION
Nebula Professional Pack	Organization	Any NCC-managed devices	Unlocks all advanced features within the Nebula Device's organization. For details on Pro features, see Section 1.1.4.2 on page 19.
Nebula Plus Pack	Organization	Any NCC-managed devices	Unlocks certain advanced features within the Nebula Device's organization. Note: Upgrade to Nebula Professional Pack to get all the advanced features. For details on Plus features, see Section 1.1.4.2 on page 19.
MSP	MSP	NCC user account	Unlocks the MSP menu and MSP features for an NCC user account.
MSP Trial	MSP	NCC user account	Unlocks the MSP menu and MSP features but is available only once per NCC account for 30 days. Go to **More** > **My devices & services** > **Services: Activate trial for MSP**. Note: An MSP Trial license may not be transferred to a different account. A deactivated trial license ends the service and cannot be re-claimed.
Organization Trial	Organization	Organization	Available when creating a new organization. Unlocks all **Nebula Professional Pack** and **Nebula Security Pack (NSS)** features in the organization for 30 days. There are no restrictions on the allowed number of Nebula Devices or sites. Note: Each Nebula user account can create 10 new organizations with trial licenses every 90 days.

Table 2 Licenses Summary (continued)

LICENSE	CATEGORY	ASSIGN TO	DESCRIPTION
Nebula Security Pack (Nebula Security Service)	Security Service	Nebula Security Gateway (NSG) devices	Unlocks security services, such as anti-virus and anti-malware. You can use these security services within the NSG's site.
UTM Security Pack	Security Service	USG FLEX devices	Unlocks security services, such as anti-malware, content filter, URL threat filter, IP reputation, sandboxing, IPS (Intrusion Prevention System), application patrol, SecuReporter, CDR (Collaborative Detection & Response), and security profile sync (see Section 12.4.5 on page 695 for more information), on a Security Firewall. You can then use these security services within the Security Firewall's site.
Gold Security Pack	Organization and Security Service	ATP devices	Unlocks security services, such as content filter, application patrol, DNS/URL threat filter, IPS (Intrusion Prevention System), Reputation filter, anti-malware with hybrid mode, sandboxing, CDR (Collaborative Detection & Response), security profile sync, Secure WiFi, SecuReporter, and all advanced features of a Nebula Professional Pack license. For details on Pro features, see Section 1.1.4.2 on page 19.
Gold Security Pack	Organization and Security Service	USG FLEX devices except USG20-VPN / USG20W-VPN / USG FLEX 50	Unlocks security services, such as content filter, application patrol, DNS/URL threat filter, IPS (Intrusion Prevention System), Reputation filter, anti-malware, sandboxing, CDR (Collaborative Detection & Response), security profile sync, Secure WiFi, SecuReporter, and all advanced features of a Nebula Professional Pack license.
Secure WiFi	Security Service	USG FLEX devices except USG FLEX 50	Unlocks the Remote AP feature.
Content Filter Pack	Security Service	USG VPN devices	Unlocks security services, such as content filter, SecuReporter, and security profile sync on USG FLEX 50 / USG20-VPN / USG20W-VPN devices.
Connect & Protect (CNP)	Security Service	NWA1123-ACv3, WAC500, WAC500H	Unlocks security services, such as threat protection using DNS and IP reputation filters.
Connect & Protect Plus (CNP+)	Security Service	NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, WAX650S	Unlocks security services, such as application visibility and threat protection using DNS and IP reputation filters.
Elite Pack	Organization and Security Service	SCR 50AXE, USG LITE 60AX	Unlocks security services, such as web filtering, Ransomware Prevention Premium, and all advanced features of a Nebula Professional Pack license. For details on Pro features, see Section 1.1.4.2 on page 19.
Entry Defense Pack	Security Service	USG FLEX H devices	Unlocks security services, such as DNS/URL threat filter, Reputation filter, SecuReporter, and Priority support requests.

1.1.4.2 Organization License Tiers

NCC features the following license tiers for organizations: **Base, Plus, Professional**.

- The **Base** tier is free and included with every organization.
- The **Plus** and **Professional** tier licenses unlock additional features within the organization. From a **Plus** tier license, upgrade to a **Professional** tier license to unlock all the additional features. These features are marked in the user interface with a diamond icon (💎). Hover the mouse over the licensed features to view the license type.

The feature differences between the license tiers are listed below:

Table 3 NCC License Tier Differences

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
Group-wide menu (Monitor – Overview, Inventory, Change log, and Configure – Settings, Org-to-Org VPN, and Administrators)	No	No	Yes	Group-wide	To create a group, you must be an NCC admin and the owner of two or more Professional organizations.
Organization change logs	No	No	Yes	Organization-wide > Organization-wide manage > Change log	
Login IPv4 address ranges for an organization	No	No	Yes	Organization-wide > Organization-wide manage > Organization settings	
Number of admin accounts	5	8	Unlimited	Organization-wide > Administrators	
Number of cloud authentication accounts	50	100	Unlimited	Organization-wide > Organization-wide manage > Cloud authentication	
Cloud authentication users with VLAN attribute	No	No	Yes	Organization-wide > Organization-wide manage > Cloud authentication (Account type: User)	
Cloud Authentication DPPSK account type	No	No	Yes	Organization-wide > Organization-wide manage > Cloud authentication (Account type: DPPSK)	
Site-wide settings sync	No	No	Yes	Organization-wide > Organization-wide manage > Configuration management	
Switch settings clone	No	No	Yes	Organization-wide > Organization-wide manage > Configuration management	

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
Site/Switch configuration backup and restore	No	No	Yes	Organization-wide > Organization-wide manage > Configuration management	
Configuration templates	No	No	Yes	Organization-wide > Organization-wide manage > Configuration templates	At the time of writing, gateway and mobile router configuration templates are not available
Add client to block list/allow list	No	No	Yes	Site-wide > Clients	
WiFi aid	No	No	Yes	Site-wide > Clients	
Connection log	No	No	Yes	Site-wide > Clients	
Site-wide topology	No	Yes	Yes	Site-wide > Topology	
Summary report email & schedule	No	Yes	Yes	Site-wide > Summary report Site-wide > Monitor > Access point / Switch / Security gateway / Firewall > Summary report	
Time period for summary reports	24 hours	7 days	365 days	Site-wide > Summary report Site-wide > Monitor > Access point / Switch / Security gateway / Firewall > Summary report	
Time period for device monitoring statistics	24 hours	7 days	365 days	Site-wide > Devices > Access point / Switches / Security router / Security gateway / Firewall > [Select Access Points / Switches]	
Time period for client monitoring statistics	24 hours	7 days	365 days	Site-wide > Clients > [Select client]	
Time period for device event log access	24 hours	7 days	365 days	Site-wide > Monitor > Site features logs	
Export data to CSV/XML file	No	No	Yes	All monitoring pages with tables	
Open API	No	No	Yes	All monitoring information	
API access (for example, DPPSK third-party integration)	No	No	Yes	Site-wide > Configure > Site settings	
Smart email alerts	Yes	Yes	Yes	Site-wide > Configure > Alert settings	

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
Per-device firmware upgrade schedules	No	Yes	Yes	Site-wide > Configure > Firmware management	
Org-wide firmware upgrade	No	Yes	Yes	Organization-wide > Organization-wide manage > Firmware management	
Priority support requests from NCC portal or Nebula app	Yes	No	Yes	Help center > Support request	
Web chat with tech support directly from NCC portal	No	No	Yes	Website footer	
Maximum uploaded photos from phone through NCC app	1	1	5	Site-wide > Devices > [select Nebula Device for example, Access points] > Photo	
Remote CLI access	No	No	Yes	Site-wide > Devices > Access Points / Security gateway / Firewall [Select AP] Live tools	
Wireless health monitor and report	No	No	Yes	Site-wide > Monitor > Access points > Wireless health	
Programmable SSID/PSK	No	No	Yes	Site-wide > Configure > SSID settings	
Dynamic Personal Pre-Shared Key (DPPSK)	No	No	Yes	Site-wide > Configure > Access points > SSID advanced settings	
Vouchers as WiFi authentication credentials	No	Yes	Yes	Site-wide > Monitor > Access points > Vouchers Site-wide > Configure > Site settings Site-wide > Configure > Access points > SSID advanced settings Site-wide > Configure > Access points > Captive portal customization > [portal theme]	
RADIUS accounting for captive portal	No	No	Yes	Site-wide > Configure > Access points > SSID advanced settings	

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
Customize RADIUS NAS ID	No	No	Yes	Site-wide > Configure > Access points > SSID advanced settings	
Customize portal redirect URL parameter	No	No	Yes	Site-wide > Configure > Access points > Captive portal customization	
Smart steering per AP	No	No	Yes	Site-wide > Configure > Access points > Radio settings > [Edit the selected Access Point]	
Bandwidth Management by VLAN interface	No	No	Yes	Site-wide > Configure > Access points > Traffic shaping	Currently supported on NWA1123ACv3, WAC500, WAC500H, NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, WAX650S
AP traffic log	No	No	Yes	Site-wide > Configure > Site settings	
IPTV report	No	No	Yes	Site-wide > Monitor > Switches > IPTV report	
Advanced IGMP	No	No	Yes	Site-wide > Configure > Switches > Advanced IGMP	
Switch Surveillance Monitoring with ONVIF	No	No	Yes	Site-wide > Monitor > Switches > Surveillance	Currently only supported on GS1350 series switches
Extended PoE range	Yes	Yes	Yes	Site-wide > Configure > Switches > Switch ports > [select port]	Currently only supported on GS1350 series switches
Automatic PoE device recovery	No	Yes	Yes	Site-wide > Configure > Switches > Switch ports > [select port]	
Port bandwidth control	Yes	Yes	Yes	Site-wide > Configure > Switches > Switch ports > [edit the selected port]	
Vendor ID-based VLAN	No	Yes	Yes	Site-wide > Configure > Switches > Switch settings	

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
IP interface and static route	No	No	Yes	Site-wide > Configure > Switches > IP & routing	
Remote SSH in Live tools	No	No	Yes	Site-wide > Devices > Switches: Switch Details > Live tools > Remote SSH	
IP Source Guard	No	No	Yes	Site-wide > Configure > Switches > Switch settings	
Nebula cloud authentication	Yes	Yes	Yes	Site-wide > Configure > Switches > Authentication	
Cloud Stacking	No	No	Yes	Site-wide > Configure > Switches > Stacking management	
Time period for security service (AV/App Patrol/CF/IDP/NSS) analysis report	24 hours	7 days	365 days	Site-wide > Monitor > Security gateway > NSS analysis report	Requires Nebula Security Gateway (NSG) Nebula Security Service (NSS) – Security Pack (SP) license
Traffic log archiving	No	No	Yes	Site-wide > Monitor > Firewall > SecuReporter	
VPN topology with traffic usage	No	No	Yes	Organization-wide > Organization-wide manage > VPN Orchestrator	
Smart VPN	No	No	Yes	Organization-wide > Organization-wide manage > VPN Orchestrator	
VPN provision script email	No	No	Yes	Site-wide > Configure > Security gateway / Firewall > Remote access VPN (L2TP/IPSec)	
Collaborative Detection & Response (CDR) with automatic respond action	No	No	Yes	Site-wide > Configure > Collaborative detection & response	Requires Security Firewall UTM Security Pack license

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
Smart mesh with manual select of mesh controller (root) and automatic fall back to auto mode	Yes	Yes	Yes	Site-wide > Devices > Access points	Currently supported on NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, WAX650S, NWA1123ACv3, WAC500, and WAC500H APs
Traffic logs to SecuReporter	No	No	Yes	Site-wide > Configure > Site settings	Also available for Gold Security Pack, UTM Security Pack, and Content Filter Pack
Home networking	Yes	Yes	Yes	Site-wide > Devices > Mobile Router > Configuration	Currently only supported on NR5101, FWA510 and LTE3301-PLUS
Cellular IP Passthrough	No	No	Yes	Site-wide > Devices > Mobile Router > Configuration	Currently only supported on NR7101 and LTE7461
Remote configurator in Live tools	No	No	Yes	Site-wide > Devices > Mobile Router > Live tools > Remote configurator	Requires LTE or NR cellular 5G indoor or outdoor router running the latest firmware
Client device heartbeat	No	No	Yes	Site-wide > Devices > Mobile Router > Client device heartbeat	Currently only supported on FWA510 and LTE3301-PLUS

Organization License Grace Period

If a Professional or Plus license expires while assigned to a Nebula Device or you add an unlicensed Nebula Device to the organization, you have a 15-day grace period during which the organization's license remains active. During the grace period, you must perform one of the following actions:

- Assign a valid Plus or Professional license to the unlicensed Nebula Device.
- Remove the unlicensed Nebula Device from the organization.

If the expired Nebula Device is still in the organization after the grace period elapses, the organization automatically downgrades to the Base tier.

The grace period status can be any of the following:

- **Near Expiring**: Any Nebula Devices with licenses expiring within 15 days before the grace period has started.
- **License Expired**: Any Nebula Devices with expired licenses after the grace period.
- **Insufficient Licenses**: Any Nebula Devices that are unlicensed, or lower tier licensed Nebula Devices added during the grace period.

1.1.4.3 General License Information

License Validity

Each license has a validity period, for example: 6 months, 1 year, 2 years. After being activated, a license also has an expiry date, which is calculated as Activation Date + Validity Period. For example, if a 1-year license is activated on January 1st 2022, then its expiry date is January 1st 2023.

Note: A license cannot be deactivated. An activated license continues counting towards its expiry date, even if its licensed service is deactivated.

Bundled and Renewal Licenses

A **bundled license** is a license that is included when you purchase a Nebula Device. The bundled license is automatically assigned to the purchased Nebula Device when you add the Nebula Device to NCC.

A **renewal license** is a license purchased separately from a Nebula Device as a license key, from Zyxel or a third-party reseller. To assign a renewal license to a Nebula Device, go to **Organization-wide** > **License & inventory** > **License** and then click **+Add**. See Section 12.2.7 on page 669 for more information.

1.2 Getting Started

You can perform network management with the NCC using a web browser. Use a browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended browser is Google Chrome.

View the browser in full screen mode to display the NCC portal properly.

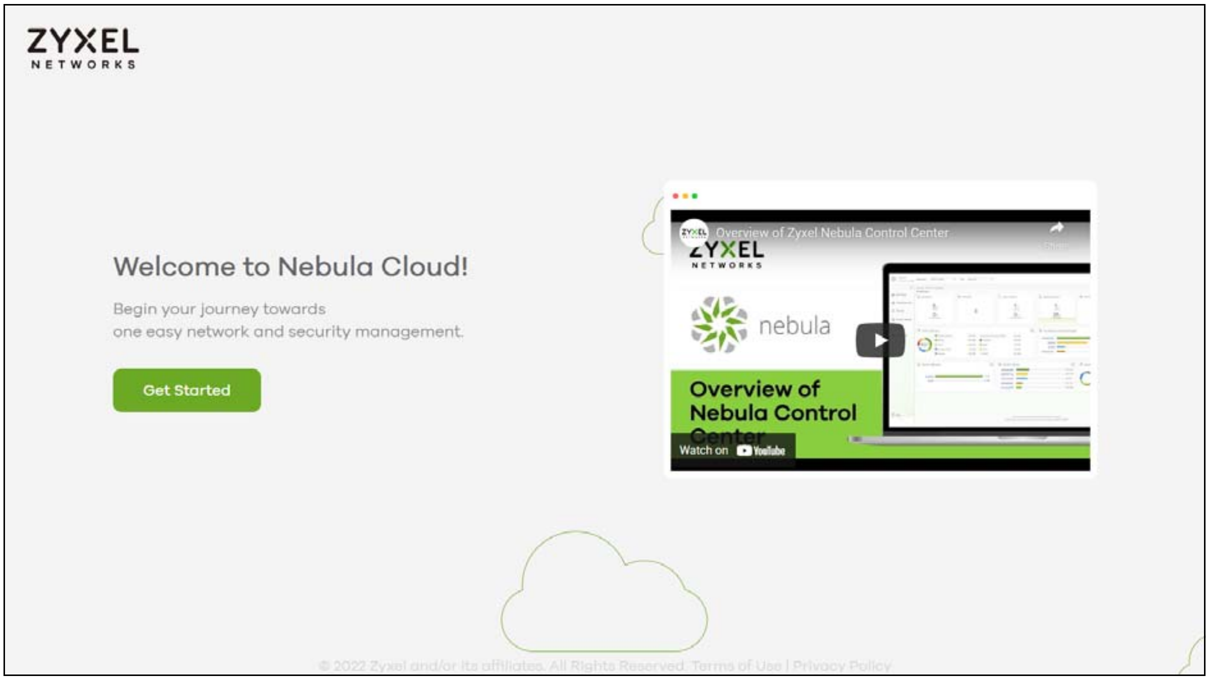
1.2.1 Connect Nebula Managed Devices

Connect your Nebula managed devices (such as the NAP102 or the NSW100-28P) to your local network. Your local network must have Internet access. See the corresponding Quick Start Guides for hardware connections.

1.2.2 Access the NCC Portal

Go to the NCC portal website.

1 Enter *http://nebula.zyxel.com* in a supported web browser. Click **Get Started**.



Welcome to Nebula Cloud!

Begin your journey towards
one easy network and security management.

Get Started

ZYXEL NETWORKS
Overview of Zyxel Nebula Control Center
ZYXEL NETWORKS
nebula
Overview of Nebula Control Center
Watch on YouTube

© 2022 Zyxel and/or its affiliates. All Rights Reserved. Terms of Use | Privacy Policy

2 To log in using your Google Account, click **Continue with Google** and then click **Sign In**.
Or, to log in using your Apple Account, click **Continue with Apple** and then click **Sign In**.
Or, enter the Zyxel Account **Email** and **Password**, and then click **Sign In**.

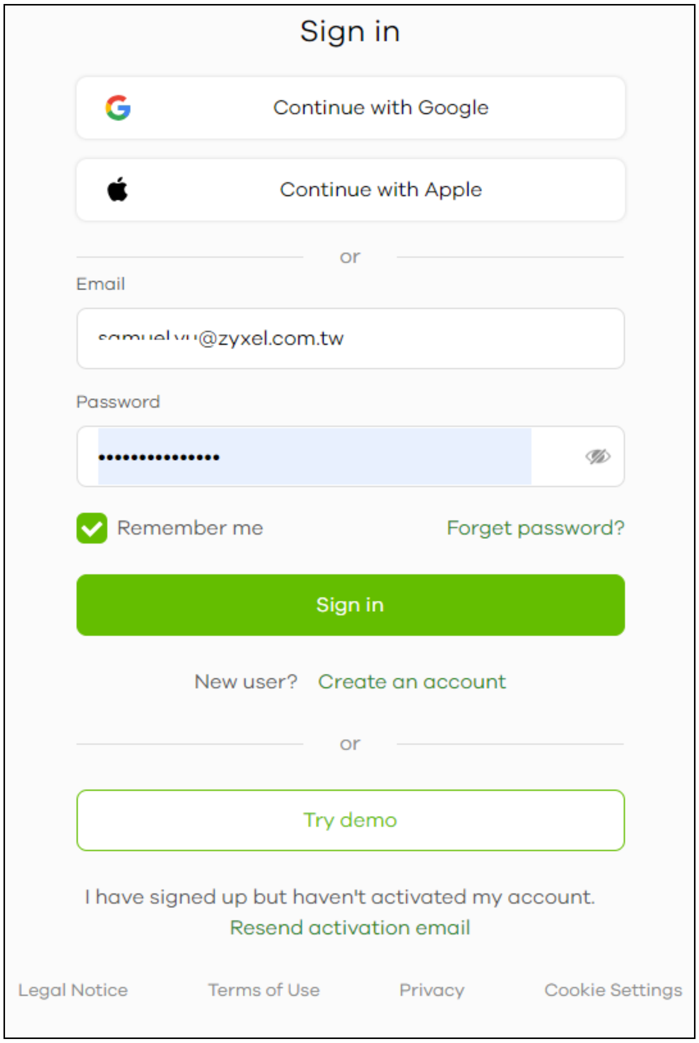
Note: To log into the NCC with your Zyxel Account., click **Create an account** with your existing email address if you do not have a Zyxel Account.

Note: The Zyxel Account does not allow account creation using disposable email addresses.

Note: When you log in using a social account (Google or Apple) but the email address was registered with a Zyxel Account, the system will prompt you to perform a login account transfer. You must agree to this before proceeding with the social account login. After the login account transfer, you can only log in using the social account method, not the Zyxel Account method.

Note: Two-factor authentication, changing password, and forget password for social account logins are managed on your social account settings.

Note: Organization-wide two-factor authentication is not allowed when you log in using a social account (Google or Apple).



Sign in

Continue with Google

Continue with Apple

or

Email

samuel.yu@zyxel.com.tw

Password

•••••••••••••••

☑ Remember me Forget password?

Sign in

New user? Create an account

or

Try demo

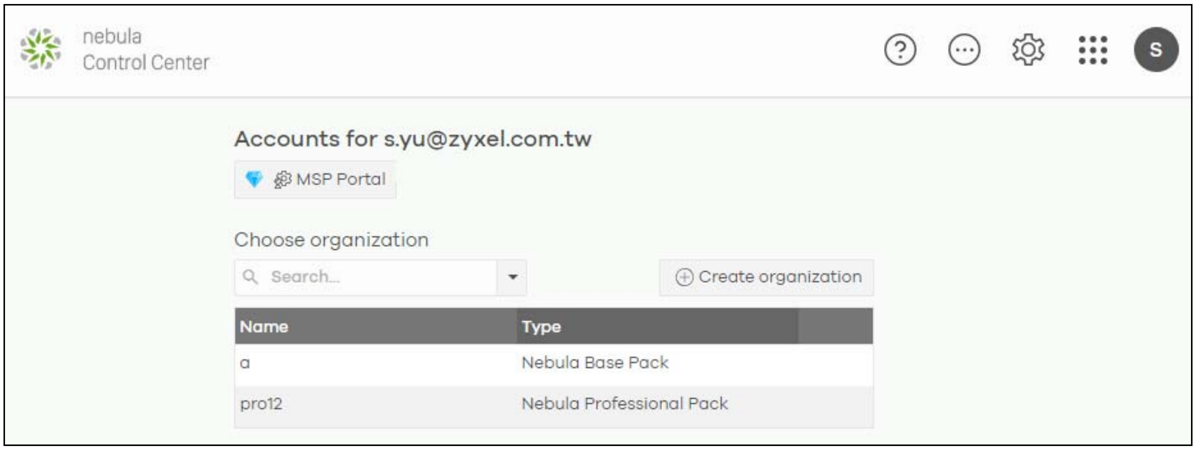
I have signed up but haven't activated my account.
Resend activation email

Legal Notice Terms of Use Privacy Cookie Settings

Note: Click **Try demo** to enter the **Demo Site**. The **Demo Site** allows you to explore the NCC Portal.

3 Click **Create organization** to create a new organization. If this is the first time you have logged into NCC, proceed to step 9.

If you have more than one organization, click a row to select the organization you want to manage.



Accounts for s.yu@zyxel.com.tw

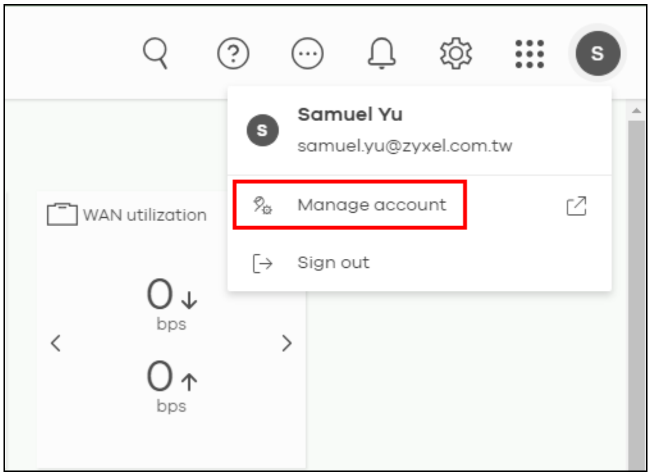
MSP Portal

Choose organization

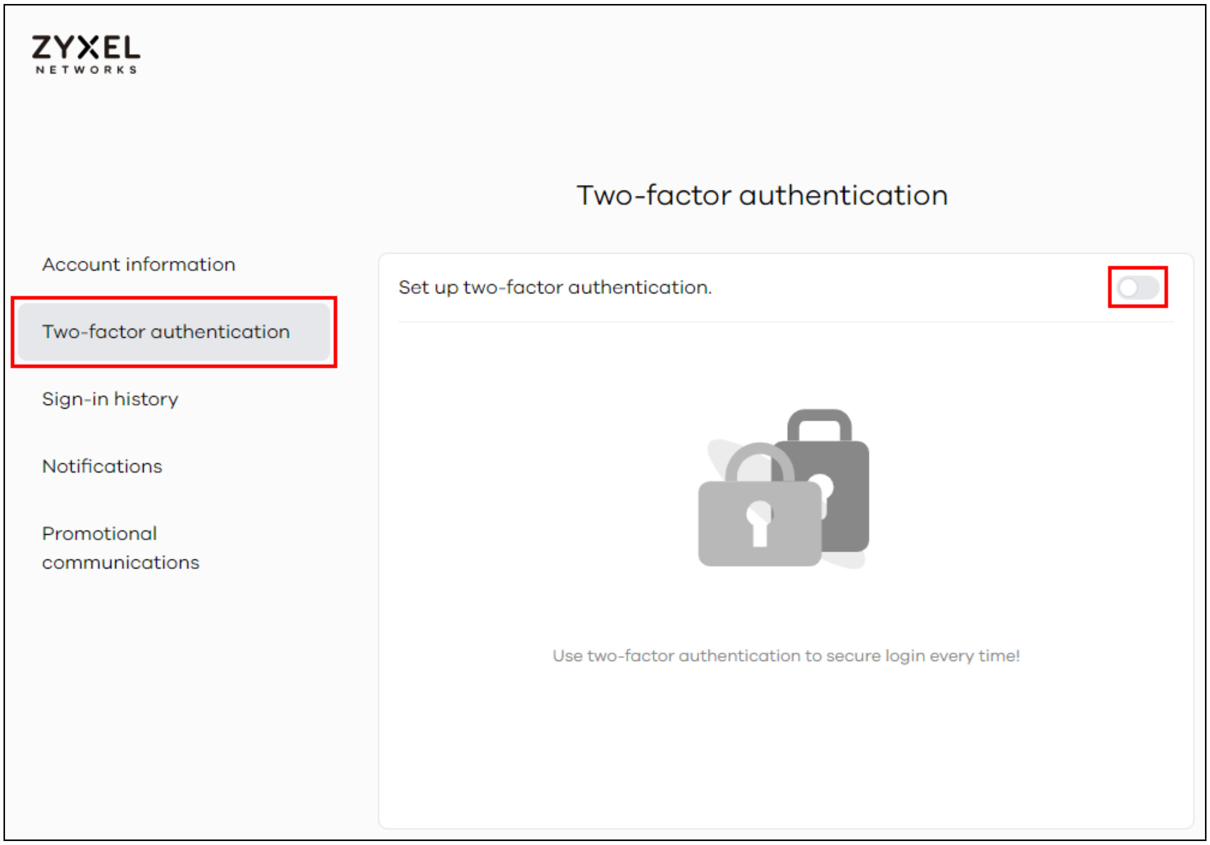
Search... Create organization

Name	Type
a	Nebula Base Pack
pro12	Nebula Professional Pack

4 The NCC supports two-factor authentication (2FA) to add a second layer of security to your account. Click **Manage account** to enable Two-factor authentication on the following page. Otherwise, you can skip 2FA and go to step 9 directly.



5 Click **Two-factor authentication** and then click the switch to enable Two-factor authentication.

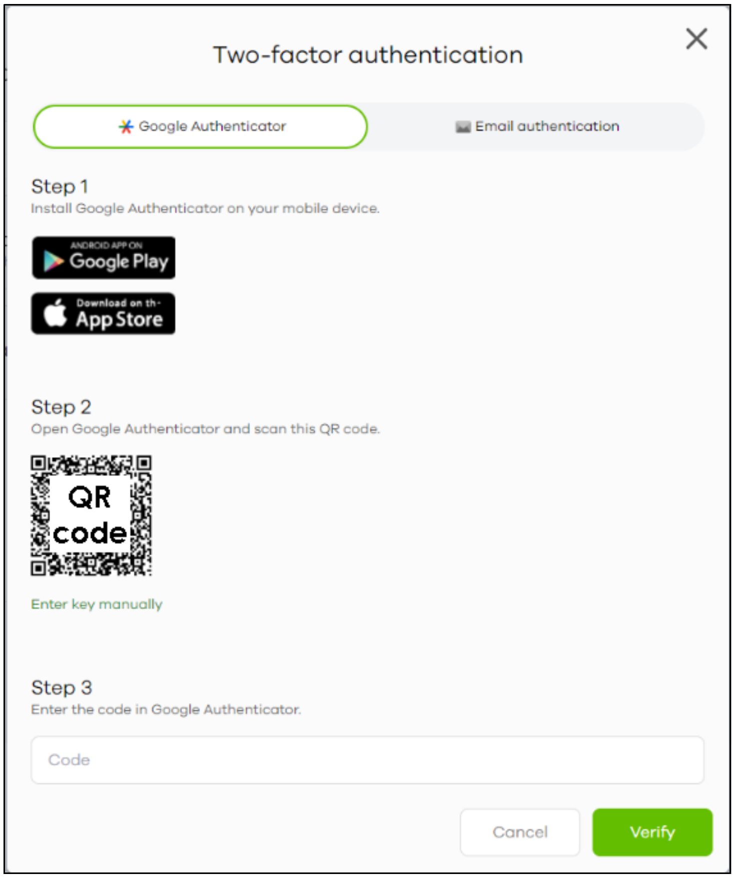


Two-factor authentication

Set up two-factor authentication.

Use two-factor authentication to secure login every time!

6 The following screen appear. Activate the two-step verification service using the Google Authenticator app or your email address. If you select **Google Authenticator**, install the app on your smartphone and scan the QR code on the NCC web screen to get a 6-digit one-time code. Then enter the code and click **Verify** to authenticate your identity.



Two-factor authentication

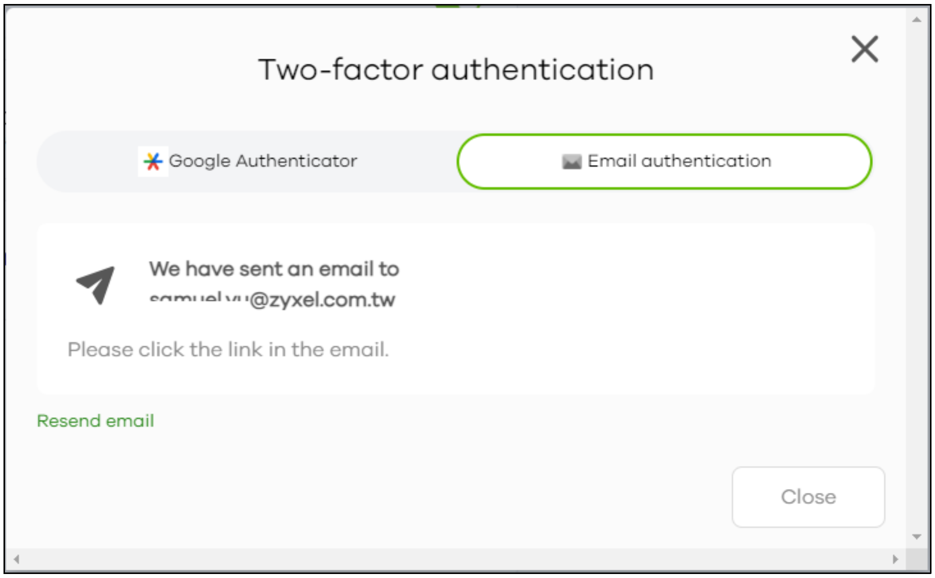
Step 1
Install Google Authenticator on your mobile device.

Step 2
Open Google Authenticator and scan this QR code.

Step 3
Enter the code in Google Authenticator.

Alternatively, click **Email authentication** to use your email to authenticate.

If you select **Email authentication**, an email is sent to your Zyxel Account's email address. Click the **Enable 2FA** link in the email.

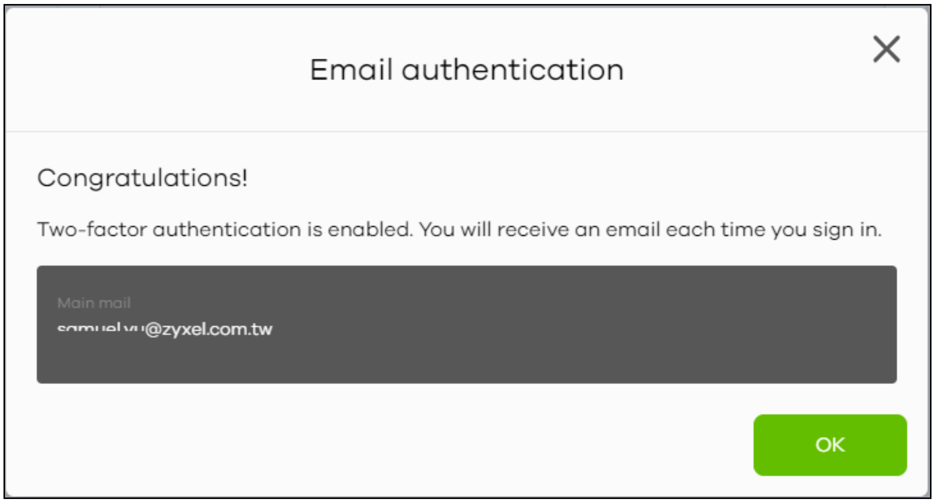


Two-factor authentication

We have sent an email to
samuel.yu@zyxel.com.tw

Please click the link in the email.

7 Click **OK** to confirm email authentication the next time you need to log in again.



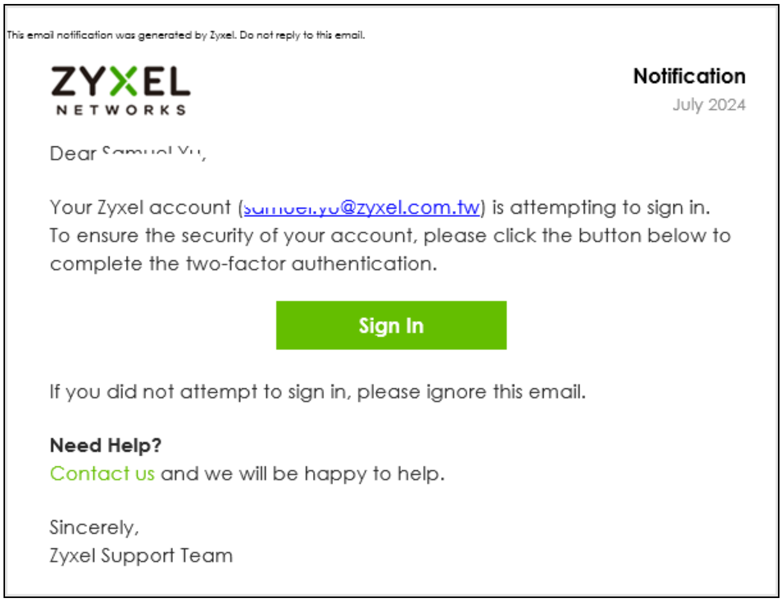
Email authentication

Congratulations!

Two-factor authentication is enabled. You will receive an email each time you sign in.

Main mail
[redacted]@zyxel.com.tw

8 To re-log in Nebula after the **Two-factor authentication** is enabled. Go to **Applications** > **Nebula** and then click the **Sign In** link on the **Zyxel Account Login Verification** email to log in your Nebula account.



This email notification was generated by Zyxel. Do not reply to this email.

Notification
July 2024

Dear [redacted],

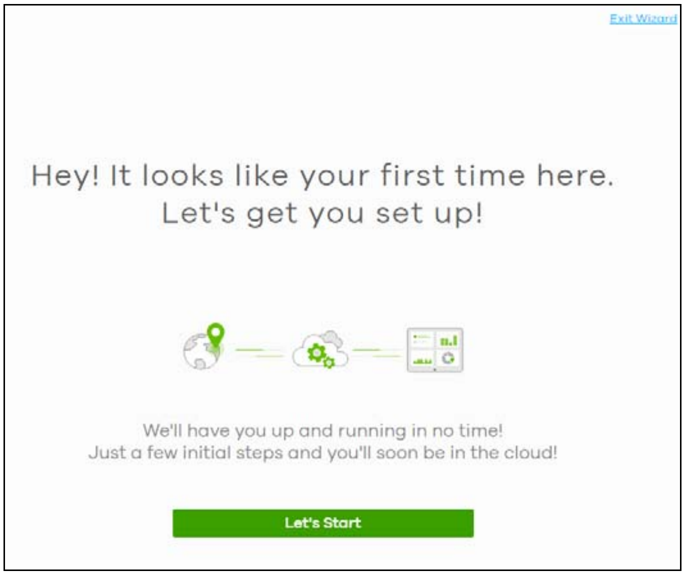
Your Zyxel account ([redacted]@zyxel.com.tw) is attempting to sign in.
To ensure the security of your account, please click the button below to complete the two-factor authentication.

If you did not attempt to sign in, please ignore this email.

Need Help?
Contact us and we will be happy to help.

Sincerely,
Zyxel Support Team

9 If this is the first time you have logged into NCC, the setup wizard welcome screen displays. You need to create your organization and sites, register Nebula Devices and associate them with a site. See Chapter 2 on page 63 for how to use the wizard.



Exit Wizard

Hey! It looks like your first time here.
Let's get you set up!

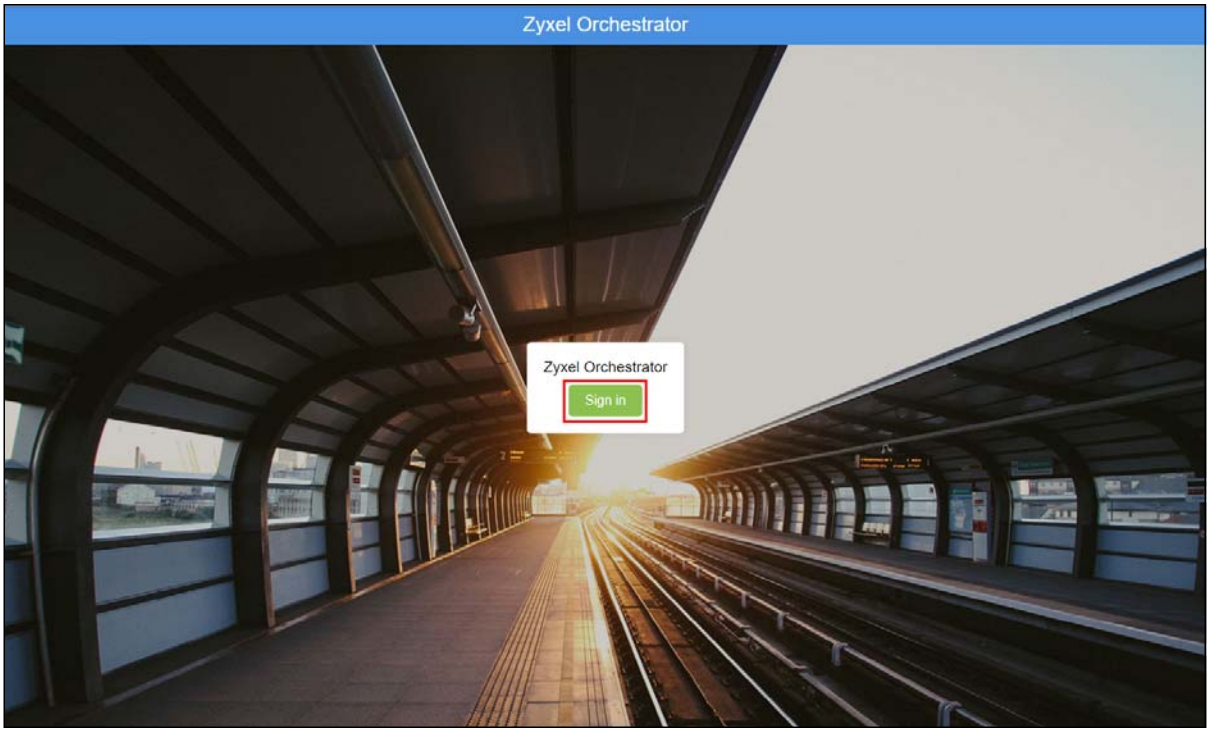
We'll have you up and running in no time!
Just a few initial steps and you'll soon be in the cloud!

Let's Start

1.2.3 Access the Nebula SD-WAN (Orchestrator) Portal

Go to the Nebula SD-WAN (Orchestrator) web portal to configure ZyWALL VPN devices. This is only available if you have purchased the SD-WAN license for Orchestrator Management.

1 Enter *https://go.sd-wan.nebula.zyxel.com* in a supported web browser. Click **Sign in**.



Zyxel Orchestrator

Zyxel Orchestrator

Sign in

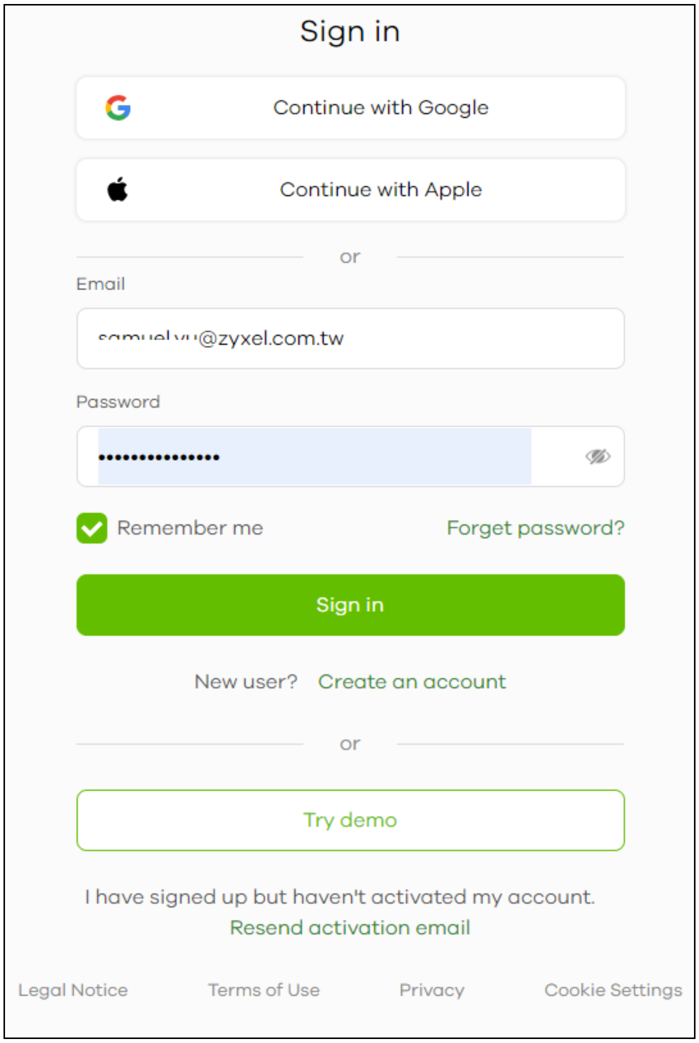
2 To log in using your Google Account, click **Continue with Google** and then click **Sign In**.
Or, to log in using your Apple Account, click **Continue with Apple** and then click **Sign In**.
Or, enter the Zyxel Account **Email** and **Password**, and then click **Sign in**.

Note: To log into the NCC with your Zyxel Account., click **Create an account** with your existing email address if you do not have a Zyxel Account.

Note: The Zyxel Account does not allow account creation using disposable email addresses.

Note: When you log in using a social account (Google or Apple) but the email address was registered with a Zyxel Account, the system will prompt you to perform a login account transfer. You must agree to this before proceeding with the social account login. After the login account transfer, you can only log in using the social account method, not the Zyxel Account method.

Note: Two-factor authentication, changing password, and forget password for social account logins are managed on your social account settings.



Sign in

Email: samuel.yu@zyxel.com.tw

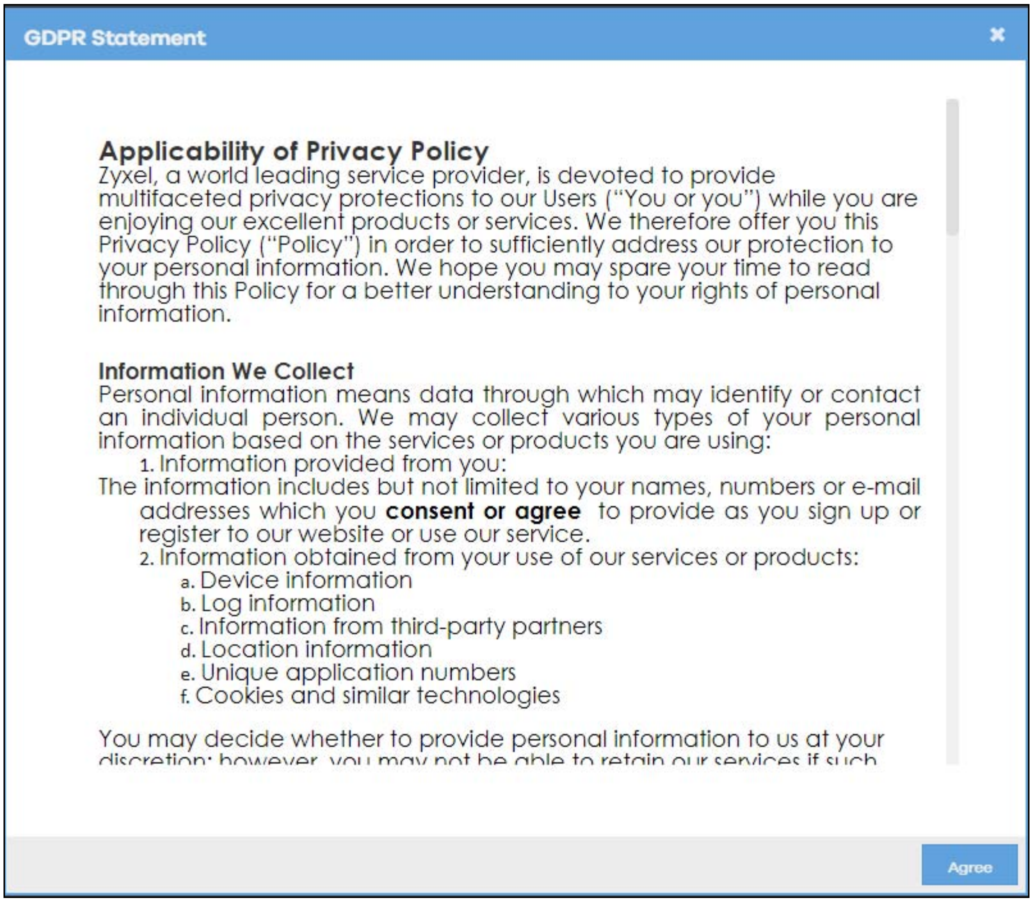
Password: •••••••••••••••

☑ Remember me

I have signed up but haven't activated my account.

Note: Click **Try demo** to enter the **Demo Site**. The **Demo Site** allows you to explore the Nebula SD-WAN (Orchestrator) portal.

3 Read the **GDPR Statement** and click **Agree** to enter the Nebula SD-WAN (Orchestrator) portal.



GDPR Statement

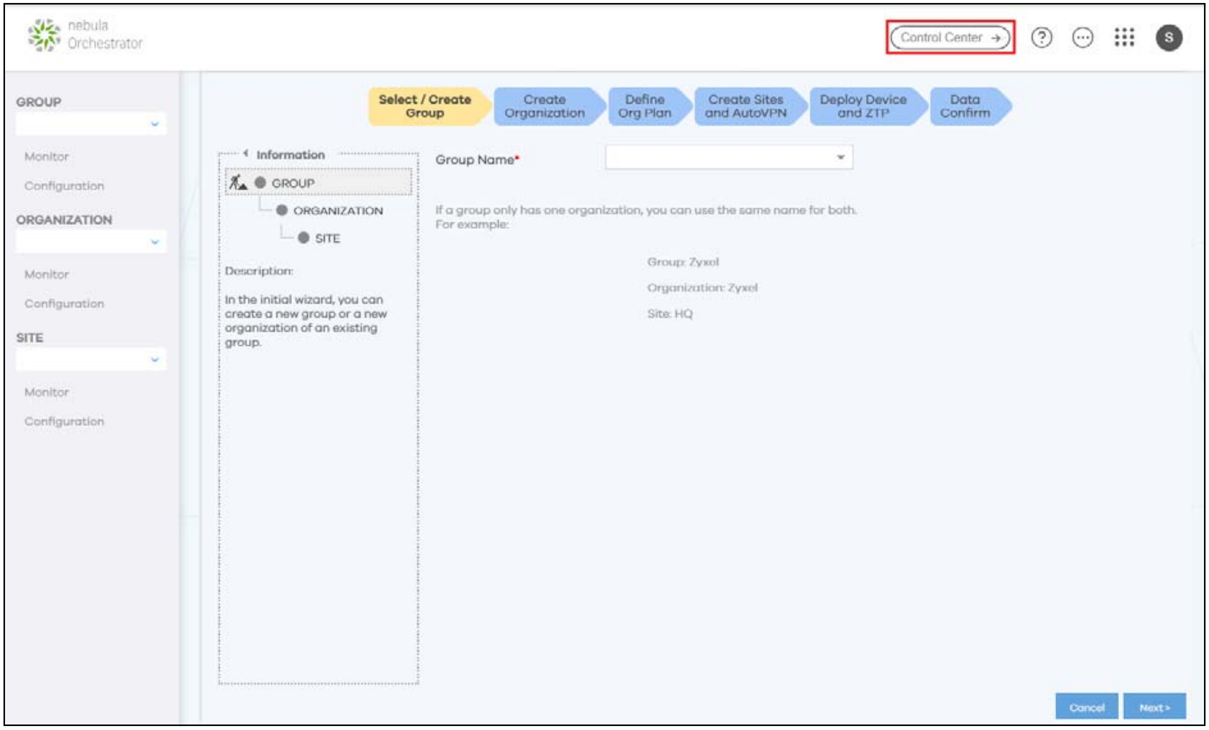
Applicability of Privacy Policy
Zyxel, a world leading service provider, is devoted to provide multifaceted privacy protections to our Users ("You or you") while you are enjoying our excellent products or services. We therefore offer you this Privacy Policy ("Policy") in order to sufficiently address our protection to your personal information. We hope you may spare your time to read through this Policy for a better understanding to your rights of personal information.

Information We Collect
Personal information means data through which may identify or contact an individual person. We may collect various types of your personal information based on the services or products you are using:

1. Information provided from you:
The information includes but not limited to your names, numbers or e-mail addresses which you **consent or agree** to provide as you sign up or register to our website or use our service.
2. Information obtained from your use of our services or products:
   a. Device information
   b. Log information
   c. Information from third-party partners
   d. Location information
   e. Unique application numbers
   f. Cookies and similar technologies

You may decide whether to provide personal information to us at your discretion; however, you may not be able to retain our services if such

Figure 2 Nebula SD-WAN (Orchestrator)



Description:

In the initial wizard, you can create a new group or a new organization of an existing group.

If a group only has one organization, you can use the same name for both. For example:

Group: Zyxel

Organization: Zyxel

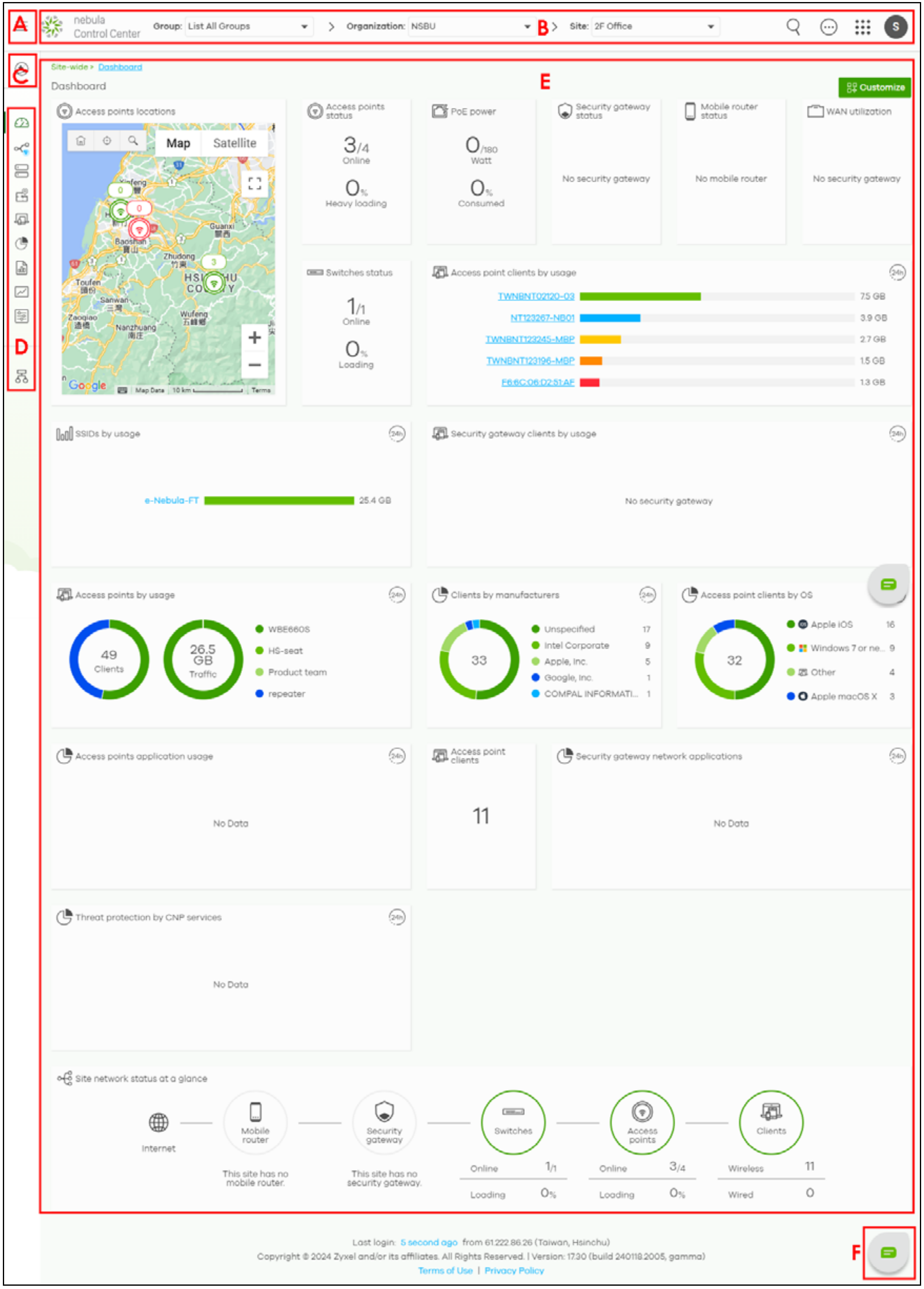
Site: HQ

You can click **Control Center** to go to the NCC platform.

1.3 NCC Portal Overview

The following summarizes how to navigate the Nebula web site from the **Dashboard** screen. The NCC portal screen is divided into these parts:

Figure 3 NCC Overview



Group: List All Groups

Organization: NSBU

Site: 2F Office

Last login: 5 second ago from 61.222.86.26 (Taiwan, Hsinchu)

Copyright © 2024 Zyxel and/or its affiliates. All Rights Reserved. | Version: 17.30 (build 240118.2005, gamma)

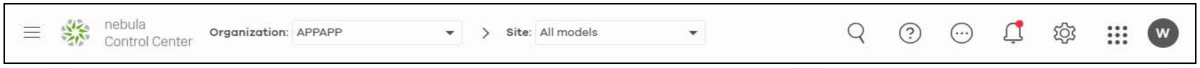
Terms of Use | Privacy Policy

- A – Expand/Collapse the Navigation Panel
- B – Title Bar
- C – Intent (Nebula AI)
- D – Navigation Panel
- E – Main Screen
- F – Chatbot AI

1.3.1 Title Bar

The title bar provides common links and is always at the top of NCC.

Figure 4 NCC Title Bar



Organization: APPAPP

Site: All models

The icons provide the following functions.

Table 4 NCC Title Bar

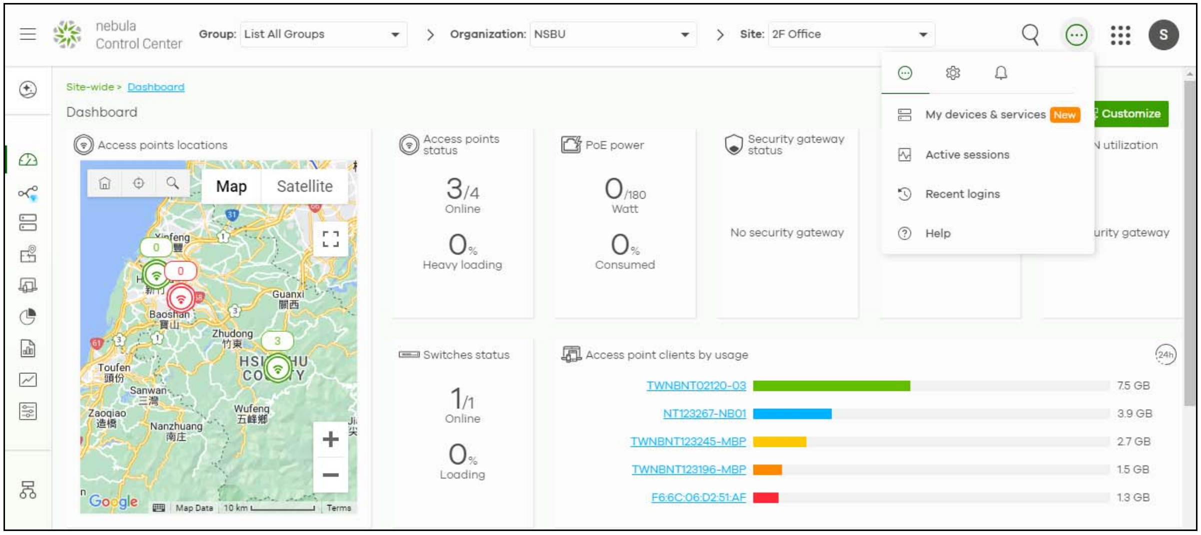
LABEL	DESCRIPTION
≡	Click this to expand or collapse the navigation panel. This allows you to show or hide the icon's label.
nebula Control Center	Click this to show the **Dashboard** screen.
Group	This shows the name of the groups you are managing, if your NCC account has an MSP license. Click to choose another group if you have multiple groups. Note: To create a group, you must be the owner of two or more Pro pack organizations that are not currently assigned to a group, as discussed in Section 13.1.1 on page 728.
Organization	This shows the name of the organization you are managing. Click to choose another organization, access the MSP portal or create a new organization. Note: If you did not enable **Two-factor authentication** in the **Account** > **Manage account**, the organization name with two-factor authentication enabled will be grayed out.
Site	This shows the name of the site you are managing. Click to choose another site if you have multiple sites in the selected organization.
Search	Use this to search for managed Nebula Devices by model, description or MAC address.
Help	Click this to view the documentation for NCC and NCC-compatible devices. For example, to view the Security Firewall Series configuration and hardware information, locate the documents under Security Appliance.
More	Click this to view your account information, login history and active sessions. You can also view your Nebula Devices and manage NCC licenses linked to your account.
Notification	Click this to view announcements such as: • New features announcements • NCC scheduled maintenance and service disruption announcements • Nebula Device offline/online status updates • Firmware upgrades availability A red dot on the icon signifies an unread announcement(s).
Settings	Click this to select a display language for the screens, or change the theme between dark and light mode.

Table 4 NCC Title Bar (continued)

LABEL	DESCRIPTION
Applications	Click this to open a list of links to different Zyxel sites, such as myZyxel, Nebula, SecuReporter, Astra, Circle, Marketplace, Store, Education, and the Community.
Account	Click this to manage your NCC account settings, or to sign out of NCC.

Note: If the browser window is too narrow, the layout of the title bar changes and some settings are hidden under the More menu.

Figure 5 Layout of the Title Bar



1.3.1.1 Site/Organization/Group

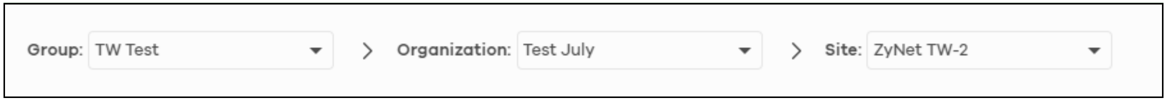
Select the site, organization and group that you want to manage.

- If you select a group, you can only select organization in that group. Select **List all Groups** from the Group drop-down list to view all organizations and group.
- If you have multiple organizations, select **MSP Portal** from the **Organization** drop-down list box to view your organization summary (see Section 14.2 on page 741).

Note: You need to have an MSP license to view the **MSP Portal**.

- If you need to have more organizations, select **Create organization** from the **Organization** drop-down list box to create a new one (see Section 1.4 on page 57).
- If you need to have more sites, select **Create site** from the **Site** drop-down list box to create a new one (see Section 1.6 on page 59).

Figure 6 NCC Title Bar: Group/Organization/Site

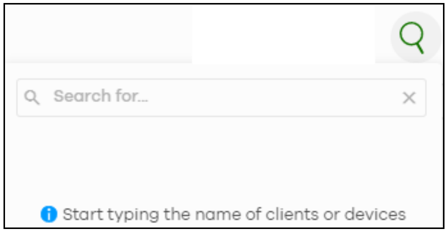


Group: TW Test > Organization: Test July > Site: ZyNet TW-2

1.3.1.2 Search

Click this to search for NCC-managed devices by model, description or MAC address. You can enter partial search criteria.

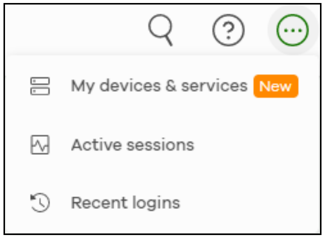
Figure 7 Search



1.3.1.3 More

Click the More icon at the top right-hand corner of the **Dashboard** screen to view and configure account settings.

Figure 8 More



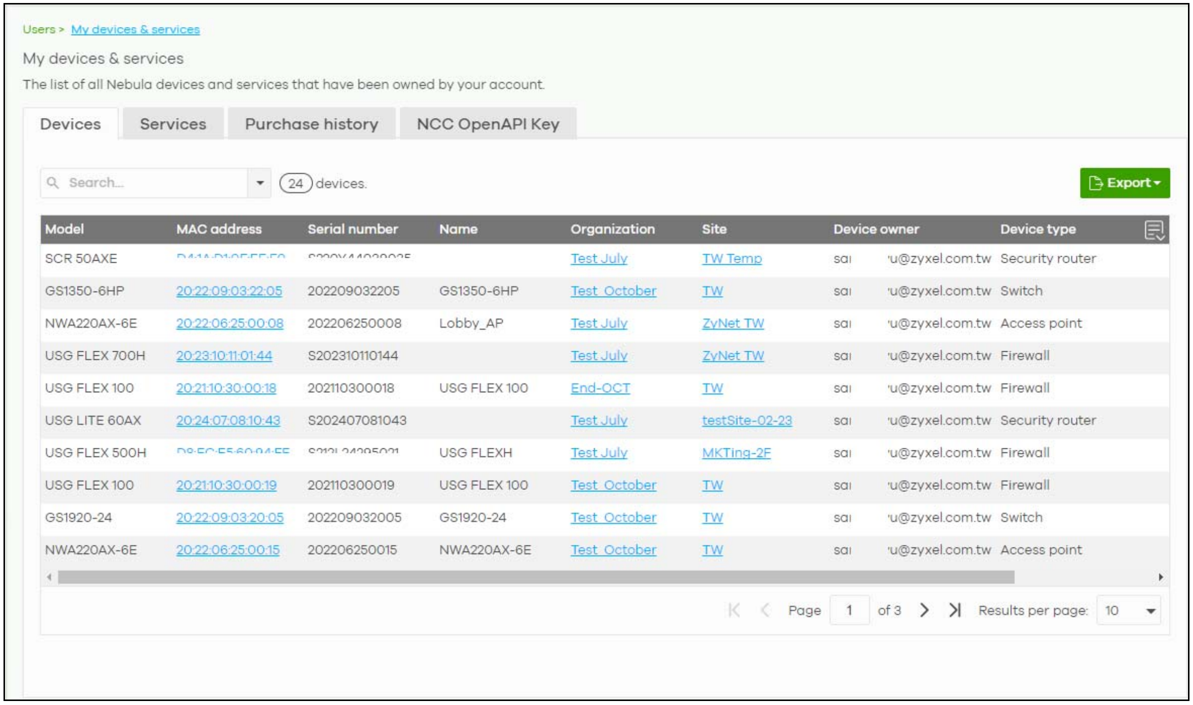
The following table describes this menu.

Table 5 Login Account Menu

LABEL	DESCRIPTION
Profile	This shows account information, such as name, address, and phone number.
My devices & services	This shows a list of all Nebula Devices in NCC that have your login account as the owner. You can filter the list of Nebula Devices by name, serial number, model, or organization. You can also register licenses to your account, such as an MSP license.
Active sessions	Shows all active web browser sessions for this login account. Click **End Session** to close a session and force the user to log into NCC again in that browser.
Recent logins	Shows the login history for this user account, including IPv4 address, location, and time.

Click **My devices & services** and the following screen appears. Click **Devices** to view all Nebula Devices of the user account which can be managed by NCC, MSP ID and organization notes, and/or all Nebula Devices not registered to this user account but with a Full (Delegated) administrator privilege. See the table on **MSP cross-org manage** > **MSP cross-org manage** > **Admins & teams** > **Admins** in Section 14.3.2 on page 746 for details on the organization privileges. See the table on **MSP cross-org manage** > **MSP cross-org manage** > **MSP portal** in Section 14.2 on page 741 for details on the MSP ID and organization notes.

Figure 9 Devices



Users > My devices & services

My devices & services

The list of all Nebula devices and services that have been owned by your account.

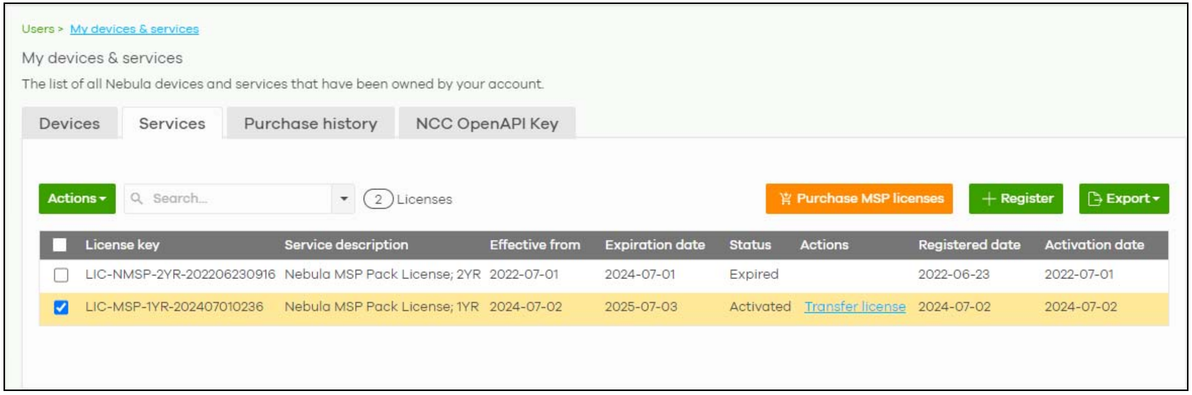
24 devices.

Model	MAC address	Serial number	Name	Organization	Site	Device owner	Device type
SCR 50AXE	[illegible]	[illegible]		Test July	TW Temp	sai 'u@zyxel.com.tw	Security router
GS1350-6HP	20:22:09:03:22:05	202209032205	GS1350-6HP	Test October	TW	sai 'u@zyxel.com.tw	Switch
NWA220AX-6E	20:22:06:25:00:08	202206250008	Lobby_AP	Test July	ZyNet TW	sai 'u@zyxel.com.tw	Access point
USG FLEX 700H	20:23:10:11:01:44	S202310110144		Test July	ZyNet TW	sai 'u@zyxel.com.tw	Firewall
USG FLEX 100	20:21:10:30:00:18	202110300018	USG FLEX 100	End-OCT	TW	sai 'u@zyxel.com.tw	Firewall
USG LITE 60AX	20:24:07:08:10:43	S202407081043		Test July	testSite-02-23	sai 'u@zyxel.com.tw	Security router
USG FLEX 500H	[illegible]	[illegible]	USG FLEXH	Test July	MKTing-2F	sai 'u@zyxel.com.tw	Firewall
USG FLEX 100	20:21:10:30:00:19	202110300019	USG FLEX 100	Test October	TW	sai 'u@zyxel.com.tw	Firewall
GS1920-24	20:22:09:03:20:05	202209032005	GS1920-24	Test October	TW	sai 'u@zyxel.com.tw	Switch
NWA220AX-6E	20:22:06:25:00:15	202206250015	NWA220AX-6E	Test October	TW	sai 'u@zyxel.com.tw	Access point

Page 1 of 3 Results per page: 10

Click **Services** to view and configure the start dates, end dates, registered dates, activated dates and statuses of an MSP license, purchase or register a license key, and export the list of MSP licenses in CSV/ XML format.

Figure 10 Services



Users > My devices & services

My devices & services

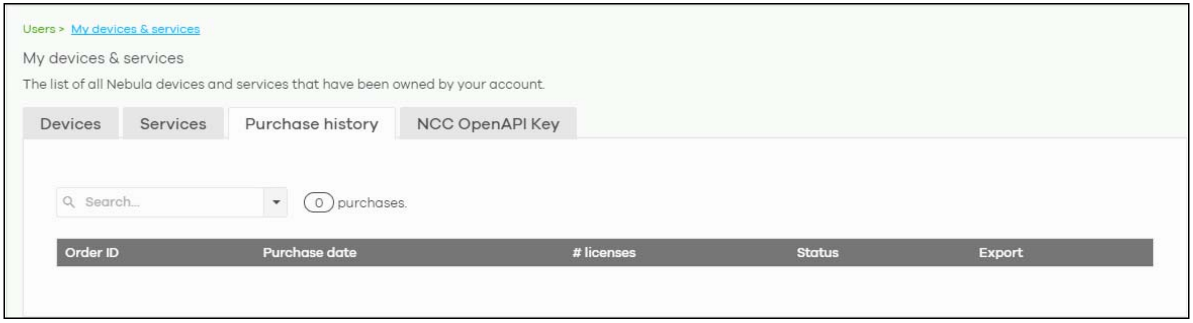
The list of all Nebula devices and services that have been owned by your account.

2 Licenses

☐	License key	Service description	Effective from	Expiration date	Status	Actions	Registered date	Activation date
☐	LIC-NMSP-2YR-202206230916	Nebula MSP Pack License; 2YR	2022-07-01	2024-07-01	Expired		2022-06-23	2022-07-01
☑	LIC-MSP-1YR-202407010236	Nebula MSP Pack License; 1YR	2024-07-02	2025-07-03	Activated	Transfer license	2024-07-02	2024-07-02

Click **Purchase history** to view the order ID, purchase date, number of licenses, statuses of purchased MSP license(s), and export the information in CSV / XML format.

Figure 11 Purchase History



My devices & services

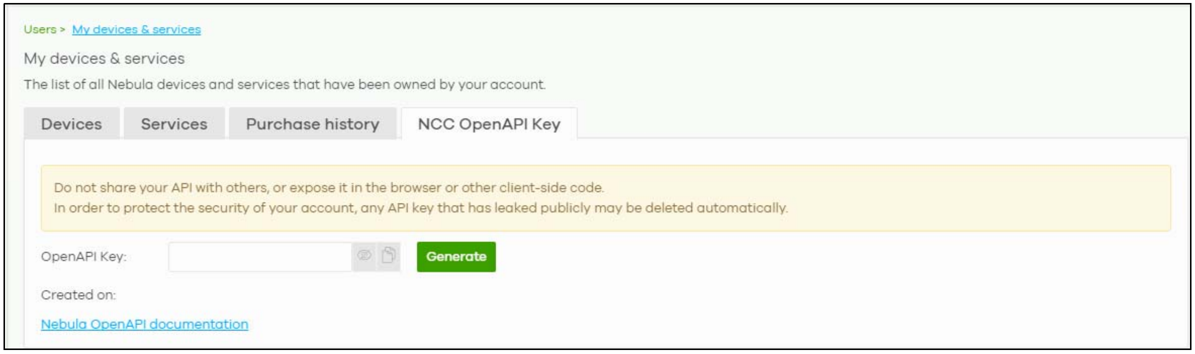
The list of all Nebula devices and services that have been owned by your account.

0 purchases.

Order ID	Purchase date	# licenses	Status	Export

Click **NCC OpenAPI Key** tab to manage your API key. An API key is required by third-party for access to information and logs from NCC. Click **Generate** to create a key. Click **Delete** to invalidate the key. Then, click **Generate** again to create a new key.

Figure 12 NCC OpenAPI Key (Generate Key)



My devices & services

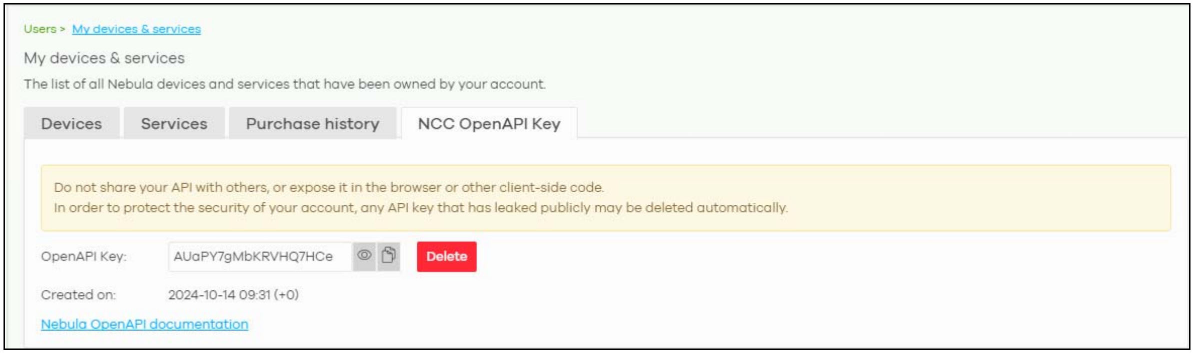
The list of all Nebula devices and services that have been owned by your account.

Do not share your API with others, or expose it in the browser or other client-side code.
In order to protect the security of your account, any API key that has leaked publicly may be deleted automatically.

OpenAPI Key:

Created on:

Figure 13 NCC OpenAPI Key (Delete Key)



My devices & services

The list of all Nebula devices and services that have been owned by your account.

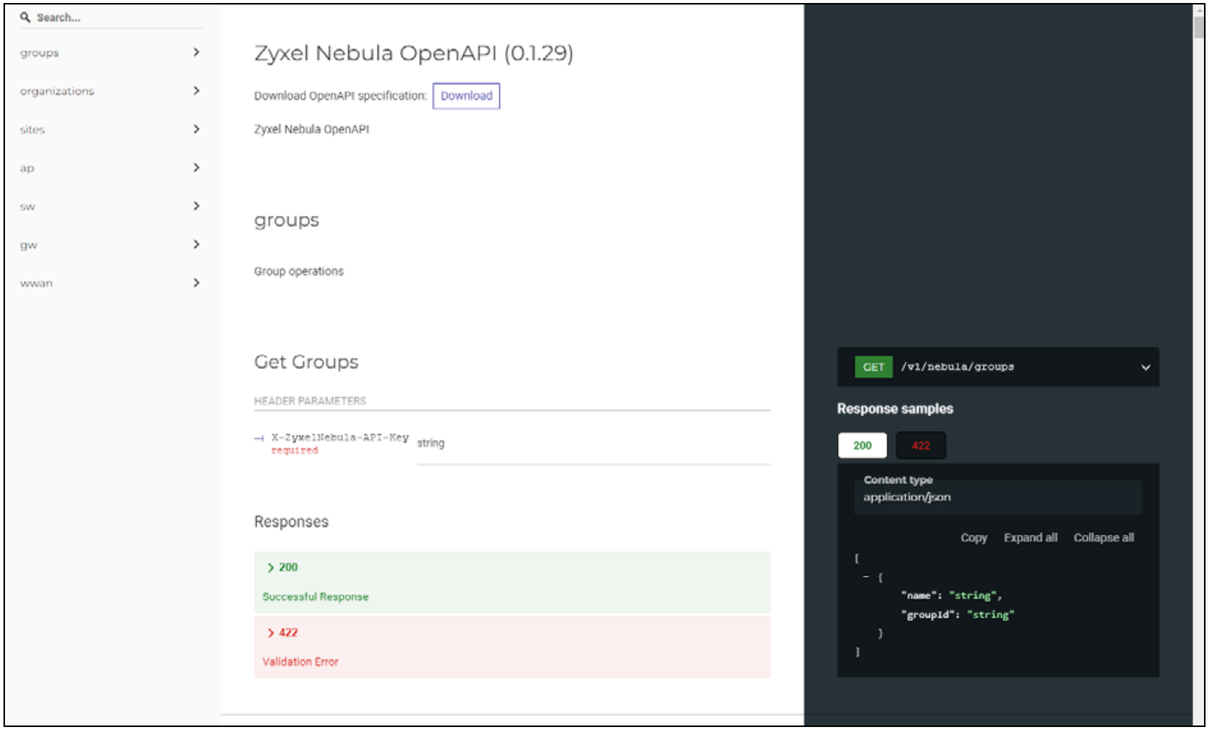
Do not share your API with others, or expose it in the browser or other client-side code.
In order to protect the security of your account, any API key that has leaked publicly may be deleted automatically.

OpenAPI Key: AUaPY7gMbKRVHQ7HCe

Created on: 2024-10-14 09:31 (+0)

Click **Nebula OpenAPI documentation** to search for available Nebula OpenAPI commands. For example, **Get Groups**, **Get Organizations From A Group**, **Get Organizations**, and so on.

Figure 14 Nebula OpenAPI Documentation



Zyxel Nebula OpenAPI (0.1.29)

Download OpenAPI specification: Download

Zyxel Nebula OpenAPI

groups

Group operations

Get Groups

HEADER PARAMETERS

X-ZyxelNebula-API-Key required string

Responses

> 200 Successful Response

> 422 Validation Error

GET /v1/nebula/groups

Response samples

200 422

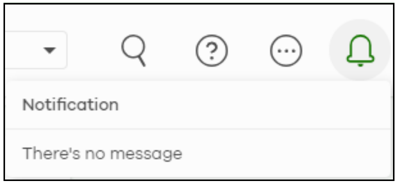
Content type application/json

```
[
  - {
      "name": "string",
      "groupId": "string"
    }
]
```

1.3.1.4 Notifications

Click this alert icon to view log messages for the selected site.

Figure 15 NCC Notification



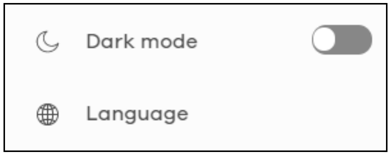
Notification

There's no message

1.3.1.5 Settings

Click the **Settings** icon at the top right-hand corner of the screen to view and configure NCC settings.

Figure 16 Settings



Dark mode

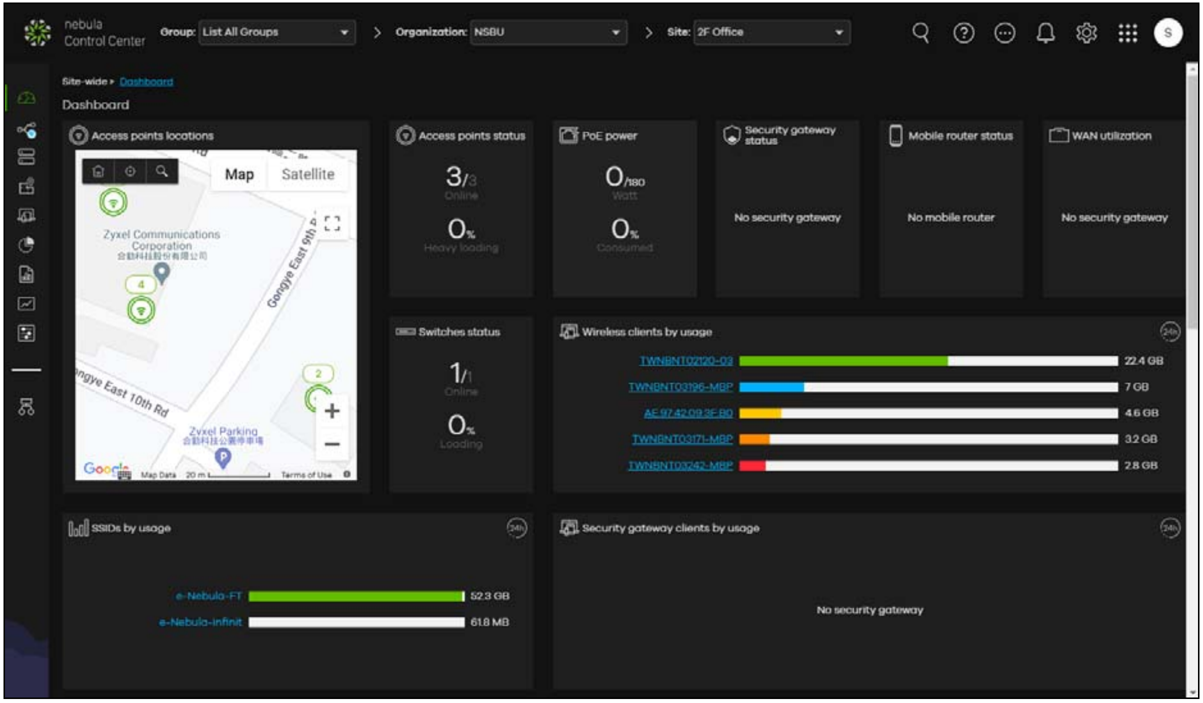
Language

The following table describes this menu.

Table 6 Settings Menu

LABEL	DESCRIPTION
Dark mode	Click this to apply a black background and white text to the white background and black text on the NCC screen.
Language	Select the NCC display language. At the time of writing, the following languages are available: English, Chinese, Japanese, German, Russian, French.

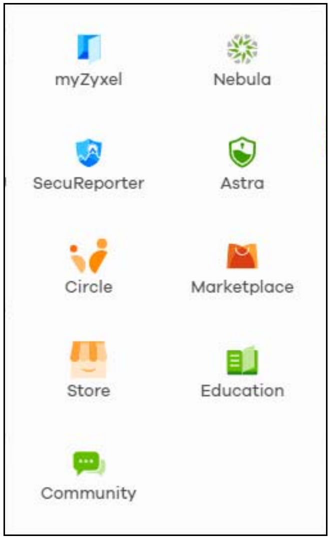
Figure 17 Dark Mode



1.3.1.6 Applications

Click this to display a list of related Zyxel Account links.

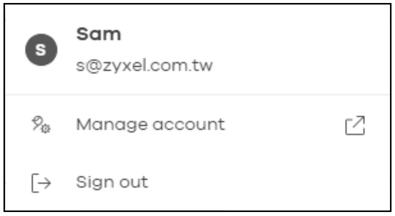
Figure 18 Related Zyxel Account Links



1.3.1.7 Account

Click the **Account** icon at the top right-hand corner of the screen to view and configure Zyxel Account settings.

Figure 19 Account



The following table describes this menu.

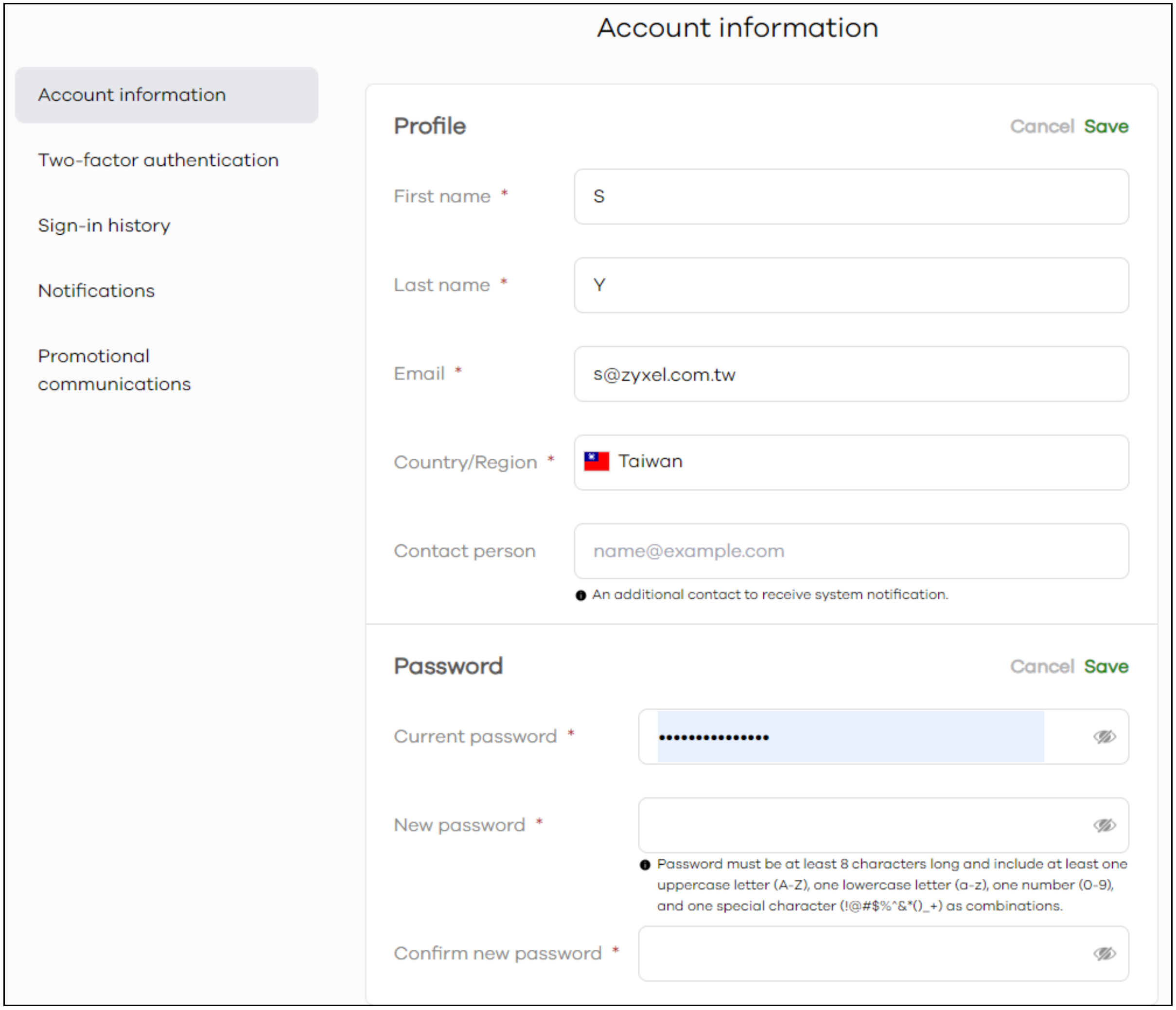
Table 7 Account Menu

LABEL	DESCRIPTION
Manage account	Click this to edit your account settings at Zyxel.
Sign out	Sign out of the Zyxel Account.

Account Information

Click **Account information** to add/change your account information and the login password.

Figure 20 Account Information



Account information

Profile

First name * S

Last name * Y

Email * s@zyxel.com.tw

Country/Region * Taiwan

Contact person name@example.com

An additional contact to receive system notification.

Password

Current password * •••••••••••••••

New password *

Password must be at least 8 characters long and include at least one uppercase letter (A-Z), one lowercase letter (a-z), one number (0-9), and one special character (!@#$%^&*()_+) as combinations.

Confirm new password *

The following table describes this menu.

Table 8 Account Information Menu

LABEL	DESCRIPTION
Account information	Click **Edit profile** to add/change the following account information:
First name Last name	Enter your first and last names. Both names must consist of 1 – 64 alphanumeric characters.
Email	Enter the email address you use to log in to the Zyxel Account. Note: The Zyxel Account does not allow disposable email addresses (for example, example@zevars.com). A disposable email is an email address that is temporary. It expires after a set amount of time or a set number of uses.
Country/Region	Select where you are located.
Contact person	Enter another person's email address to receive notifications about your Nebula Device.
Password	Click **Change password** to change your current password.
Current Password	Enter the current password you use to log in to the Zyxel Account.

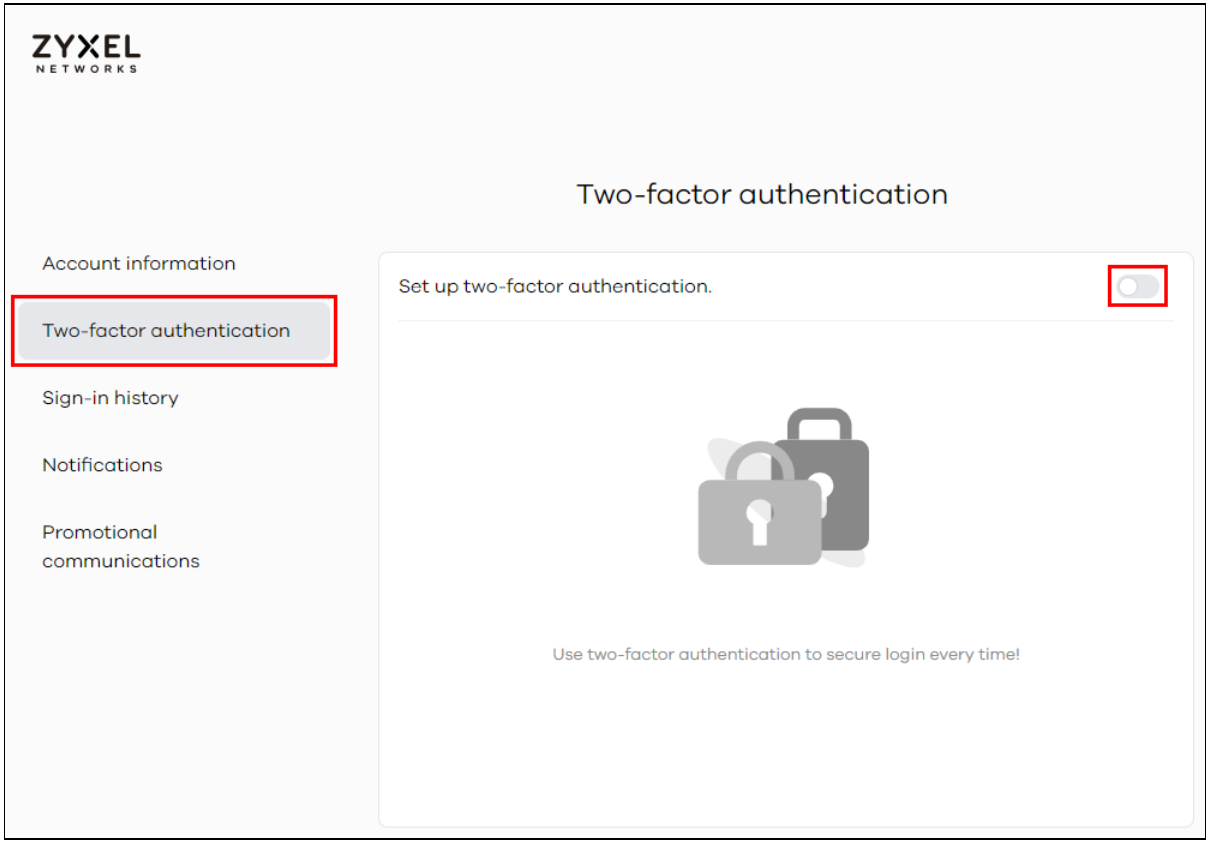
Table 8 Account Information Menu

LABEL	DESCRIPTION
New Password	Enter the **New Password**. Use a minimum of 8 characters, including 0–9 a–z A–Z `~!@#$%&*(_+-={} | [];"'./<> ?).
Confirm new password	Enter the **New Password** to confirm.
Cancel	Click **Cancel** to exit this screen without saving.
Save	Click **Save** to save your changes back to the Zyxel Account.

Two-factor Authentication

Click the **Set up two-factor authentication** switch to the right to add a second layer of security to your Zyxel Account.

Figure 21 Two-factor Authentication



Two-factor authentication

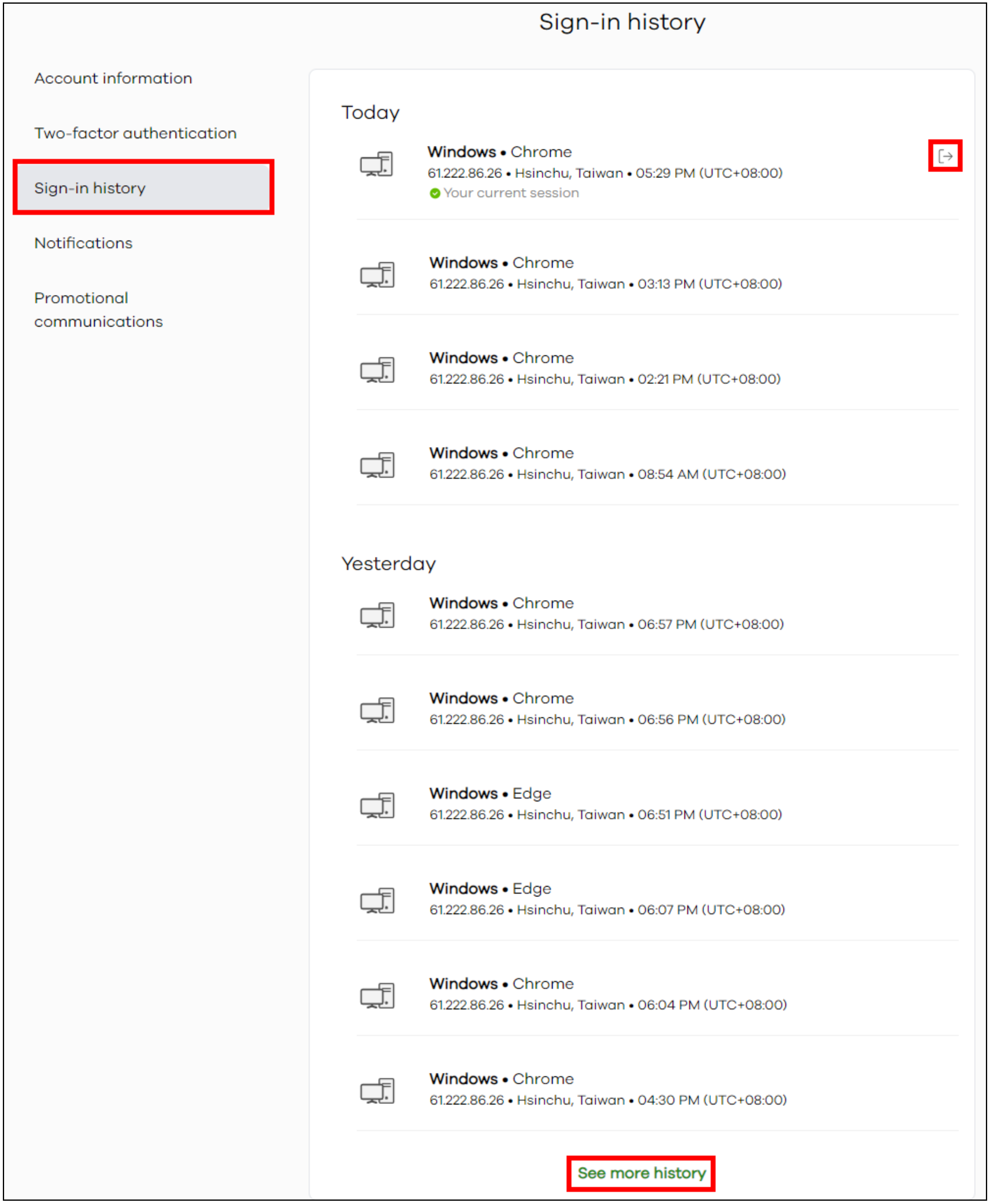
Set up two-factor authentication.

Use two-factor authentication to secure login every time!

Sign-in History

Use the **Sign-in history** screen to view a log of the last 10 sign-ins to your Zyxel Account. Click **See more history** to view a log of sign-ins to your Zyxel Account for up to the last 60 days. Click the Sign out icon to log out of your Zyxel Account session.

Figure 22 Sign-in History



Sign-in history

Today

Windows • Chrome
61.222.86.26 • Hsinchu, Taiwan • 05:29 PM (UTC+08:00)
Your current session

Windows • Chrome
61.222.86.26 • Hsinchu, Taiwan • 03:13 PM (UTC+08:00)

Windows • Chrome
61.222.86.26 • Hsinchu, Taiwan • 02:21 PM (UTC+08:00)

Windows • Chrome
61.222.86.26 • Hsinchu, Taiwan • 08:54 AM (UTC+08:00)

Yesterday

Windows • Chrome
61.222.86.26 • Hsinchu, Taiwan • 06:57 PM (UTC+08:00)

Windows • Chrome
61.222.86.26 • Hsinchu, Taiwan • 06:56 PM (UTC+08:00)

Windows • Edge
61.222.86.26 • Hsinchu, Taiwan • 06:51 PM (UTC+08:00)

Windows • Edge
61.222.86.26 • Hsinchu, Taiwan • 06:07 PM (UTC+08:00)

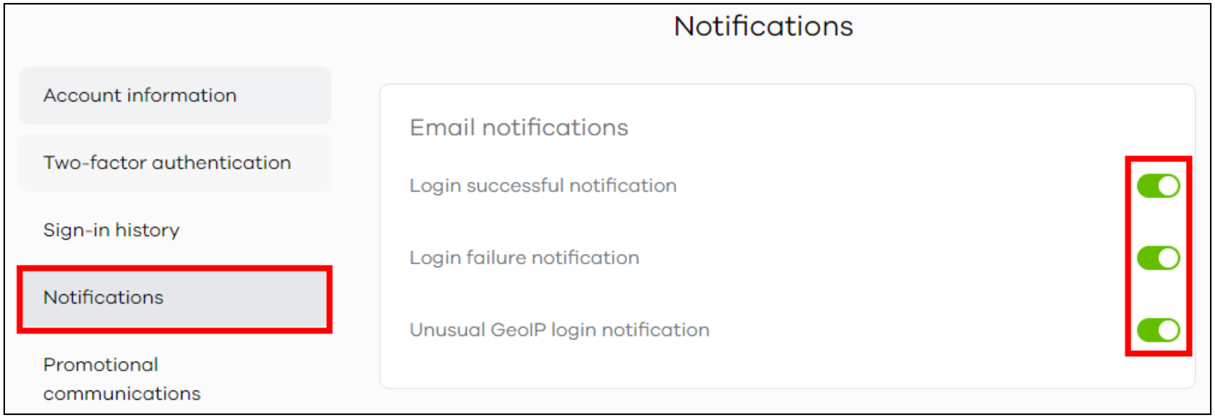
Windows • Chrome
61.222.86.26 • Hsinchu, Taiwan • 06:04 PM (UTC+08:00)

Windows • Chrome
61.222.86.26 • Hsinchu, Taiwan • 04:30 PM (UTC+08:00)

Notifications

Use the **Notifications** screen to enable email notifications for each successful or unsuccessful login to your Zyxel Account.

Figure 23 Notifications



Notifications

Email notifications

Login successful notification

Login failure notification

Unusual GeoIP login notification

The following table describes this menu.

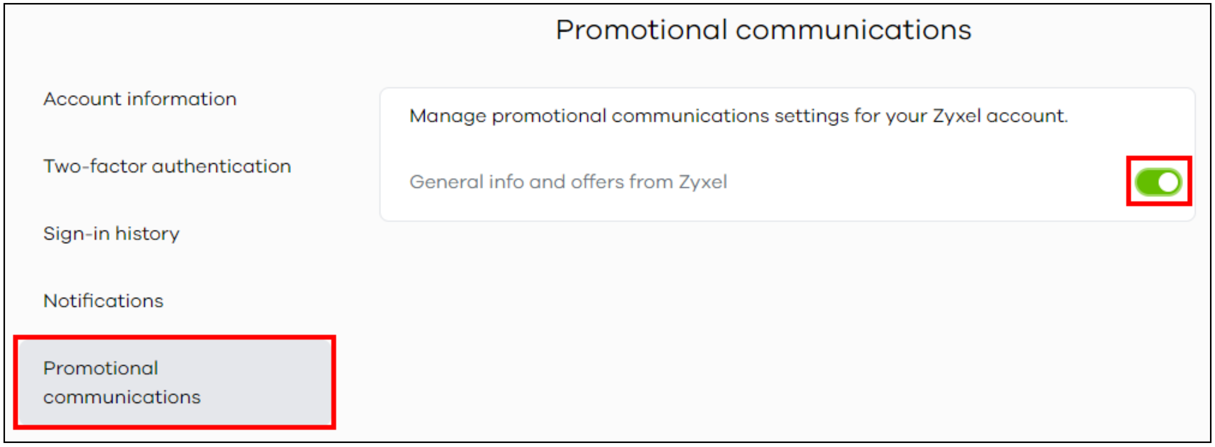
Table 9 Notifications Menu

LABEL	DESCRIPTION
Email notifications	Click the switch to the right to receive an email alert when the following events occur.
Login successful notification	A notification is sent by email for each successful login to your Zyxel Account.
Login failure notification	A notification is sent by email for each unsuccessful login attempt to your Zyxel Account.
Unusual GeoIP login notification	A notification is sent by email for each login attempt to your Zyxel Account from a location you have not logged in from in the past 60 days.

Promotional Communications

Click the **General info and offers from Zyxel** switch to the right to receive emails containing general information and promotional offers from Zyxel.

Figure 24 Promotional Communications



Promotional communications

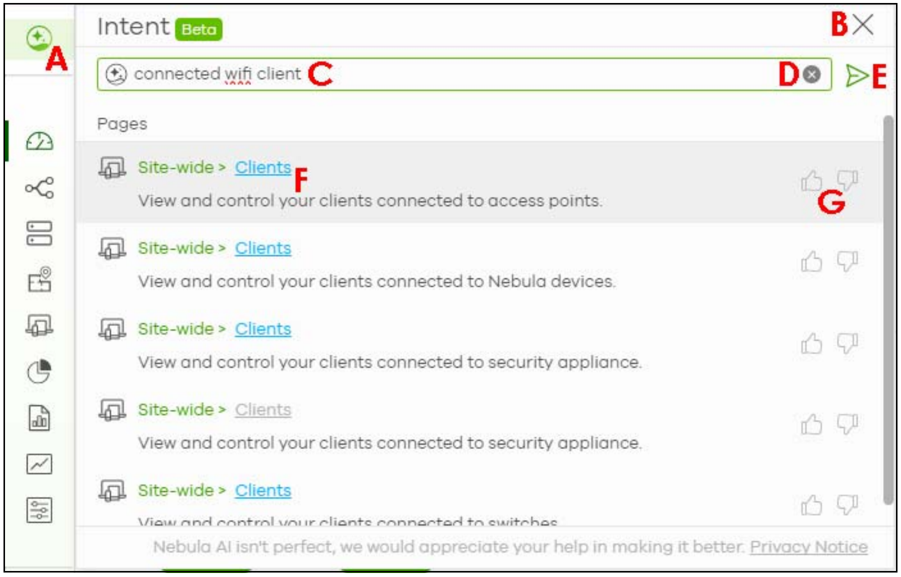
Manage promotional communications settings for your Zyxel account.

General info and offers from Zyxel

1.3.2 Intent

Click the **Intent** icon at the top left-hand corner of the screen to search for pages about where to configure an NCC feature.

Figure 25 Intent



connected wifi client

View and control your clients connected to access points.

View and control your clients connected to Nebula devices.

View and control your clients connected to security appliance.

View and control your clients connected to security appliance.

View and control your clients connected to switches

Nebula AI isn't perfect, we would appreciate your help in making it better. Privacy Notice

The following table describes this menu.

Table 10 Intent Menu

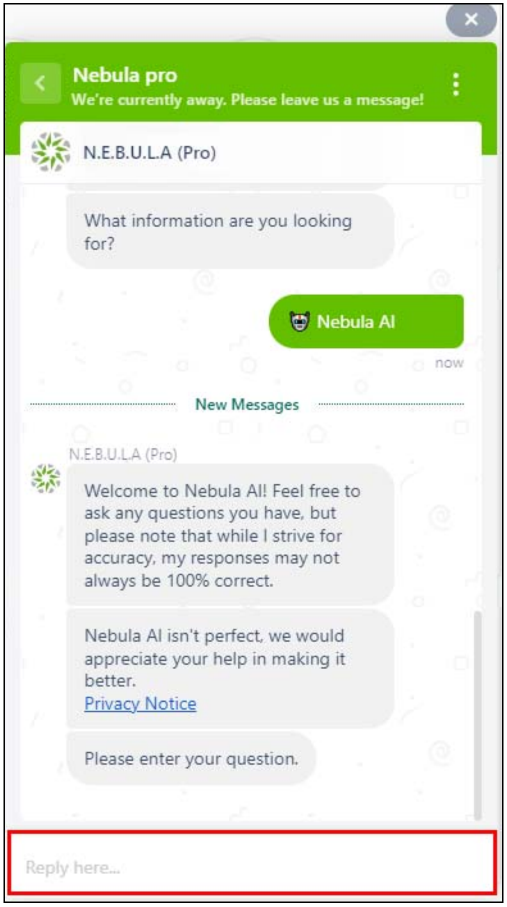
LABEL	DESCRIPTION
A	Click this to display/hide the **Intent** window.
B	Click this to hide the **Intent** window.
C	Enter your query here. You can enter a complete sentence to search for information instead of a keyword. Press **Enter** on your keyboard or click the Send button (**E**) to send your query to Nebula AI. Note: You can use up to 4096 alphanumeric characters.
D	Click this to remove the text and start another query.
E	Click this to send your query to Nebula AI.
F	By default, this displays the popular topics. After entering your query and clicking send, the AI-generated page links appear. Click on an AI-generated link to go to the page in NCC.
G	Click the thumbs up icon if the AI-generated link is helpful. This increases Nebula AI's association of your query to the page in NCC. Alternatively, click the thumbs down icon if the AI-generated link is unhelpful. This decreases Nebula AI's association of your query to the page in NCC.

1.3.3 Chatbot AI

Click the **Chatbot AI** icon at the lower right of the screen to answer your NCC queries.

Note: The Chatbot AI is a Nebula Base tier feature. You need a Nebula Professional Pack license to have the following features:
– direct your query to a live Zyxel Support team member from 09:00 to 17:00 (UTC+8)
– submit a support ticket (see Section 15.5 on page 776 for more information).

Figure 26 Chatbot AI – Enter Your Query



Nebula pro

We're currently away. Please leave us a message!

N.E.B.U.L.A (Pro)

What information are you looking for?

Nebula AI

now

New Messages

N.E.B.U.L.A (Pro)

Welcome to Nebula AI! Feel free to ask any questions you have, but please note that while I strive for accuracy, my responses may not always be 100% correct.

Nebula AI isn't perfect, we would appreciate your help in making it better.
Privacy Notice

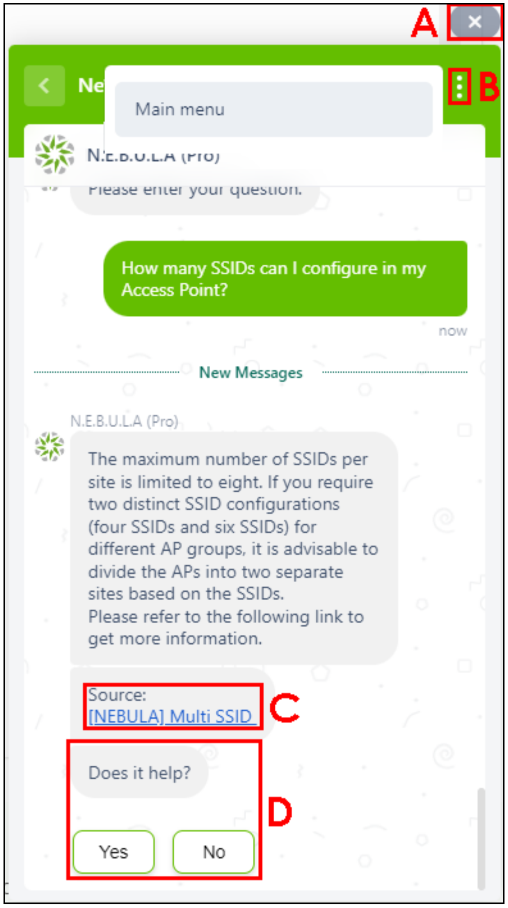
Please enter your question.

Reply here...

Enter your query on **Reply here...** and press **Enter** on your keyboard to send your query to Chatbot AI. The AI-generated answer appears.

Note: You can enter up to 4,096 keyboard characters.

Figure 27 Chatbot AI



Please enter your question.

How many SSIDs can I configure in my Access Point?

now

New Messages

N.E.B.U.L.A (Pro)

The maximum number of SSIDs per site is limited to eight. If you require two distinct SSID configurations (four SSIDs and six SSIDs) for different AP groups, it is advisable to divide the APs into two separate sites based on the SSIDs.
Please refer to the following link to get more information.

Source:
[NEBULA] Multi SSID

Does it help?

The following table describes this menu.

Table 11 Chatbot AI Menu

LABEL	DESCRIPTION
A	Click this to close the **Chatbot AI** window.
B	Click this to show the main menu.
C	For more information, click the link to the source of the AI-generated answer on the Zyxel Community site.
D	Click **Yes** if the AI-generated answer is helpful. This increases Chatbot AI's association of your query to the topic in the Chatbot source. Alternatively, click **No** if the AI-generated answer is unhelpful.

1.3.4 Navigation Panel

Use the NCC menu items to configure network management for each site, organization and/or Nebula Device.

Table 12 Navigation Menus Overview

LABEL	DESCRIPTION
Use these menus to set up customer networks.	
Site-wide	Manage Nebula Devices in a site.

Table 12 Navigation Menus Overview (continued)

LABEL	DESCRIPTION
Organization-wide	Manage multiple network sites within an organization.
Group-wide	Manage settings for multiple organizations and create VPN links between groups in the organization. Two or more Pro tier organizations can be a group.
MSP	Create multiple organizations and change the branding and assign administrators to multiple organizations.
Use these menus to set up customer Nebula Devices.	
Access points	Manage the Zyxel APs (Access Points).
Switches	Manage the Zyxel Switches.
Security router	Manage the SCR 50AXE and USG LITE 60AX.
Firewall	Manage the ZyWALL ATP, USG FLEX, USG FLEX H and USG20(W)-VPN devices (firewalls).
Security gateway	Manage the ZyWALL NSG devices.
Mobile router	Manage the Zyxel LTE/NR devices.
Help center	Access the Zyxel community forum, submit a support ticket, view User Guides for Nebula managed devices, view ports used by Nebula, view Nebula privacy policies, and view devices/features that can be managed by Nebula.

This is a summary of the menu details.

Table 13 NCC Menu Summary

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
Site-wide	Intent	Use this menu to search for pages in the NCC portal where to configure a particular feature.
	Dashboard	Use this menu to view Nebula Device connection status and traffic summary.
	Topology	Use this menu to view Nebula managed-device connections in your network.
	Devices	
	Add devices	Click + to register a Nebula Device and add it to the site.
	Access points / Switches / Security router / Firewall / Security gateway / Mobile router / Accessories	Use this menu to view Nebula Device connection status and traffic summary.
	Map & floor plans	Use this menu to locate Nebula Devices on a world map or on a floor plan.
	Clients	
	Client list	Use this menu to view the connection status and detailed information of all wired and WiFi clients connected to Nebula Devices (Access Points, Switches, Security Appliances) in the site.
	WiFi Aid	Use this menu to display an overview of the AP's WiFi clients connection issues, as an aid to troubleshooting.
	Connection log	Use this menu to view all related event logs between Access Points and WiFi clients, and DHCP logs of Nebula Security Appliances (NSG, ZyWALL USG FLEX, ATP, and USG20(W)-VPN). Association, Authentication, Disconnection, and DHCP event logs that occur are summarized in chronological order to aid in troubleshooting.
	Applications usage	Use this menu to view usage of applications such as Social Network, Telephony (VoIP), Advertising, News, Web Services in the network.
	Summary report	Use this menu to view network statistics for a site, such as bandwidth usage, power usage, top Nebula Devices, top clients and/or top SSIDs.
	Monitor	
	Access points	
	Event log	Use this menu to view all events on the Access Point. An event is something that has happened to a Nebula managed device.
	Vouchers	Use this menu to create and manage vouchers that allow WiFi network access.
	Wireless health	Use this menu to view health of the WiFi networks for the supported Access Points and connected clients.
	WiFi Aid	Use this menu to display an overview of the AP's WiFi clients connection issues, as an aid to troubleshooting.
	Summary report	Use this menu to view network statistics specific to Access Points in the site.

Table 13 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
	Switches	
	Event log	Use this menu to view all events on the Switch. An event is something that has happened to a Nebula managed device.
	Surveillance	Use this screen to view information about Powered Devices (PDs) connected to ports on the Switch.
	IPTV report	Use this menu to view available IPTV channels and client information.
	Summary report	Use this menu to view network statistics specific to Switches in the site.
	Security router	
	Event log	Use this menu to view all events on the Security router. An event is something that has happened to a Nebula managed device.
	VPN connections	Use this menu to view status of the site-to-site VPN connections.
	Threat report	Use this menu to view statistics for threat management categories.
	Content Filter report	Use this screen to view statistics for content filter categories.
	Firewall	
	Event log	Use this menu to view all events on the Security Firewall. An event is something that has happened to a Nebula managed device.
	VPN connections	Use this menu to view status of the site-to-site VPN connections.
	SecuReporter	Use this menu to view the statistics report for NSS (Nebula Security Service), such as content filter, Intrusion Detection and Prevention (IDP), application patrol, and anti-virus.
	Summary report	Use this menu to view network statistics specific to the Security Firewall in the site.
	Security gateway	
	Event log	Use this menu to view all events on the security gateway. An event is something that has happened to a Nebula managed device.
	VPN connections	Use this menu to view status of the site-to-site VPN connections.
	NSS analysis report	Use this menu to view the statistics report for NSS (Nebula Security Service), such as content filter, Intrusion Detection and Prevention (IDP), application patrol, and anti-virus.
	Summary report	Use this menu to view network statistics specific to the security gateway in the site.
	Containment list	Use this menu to view and manage Nebula Devices contained by CDR (Collaborative Detection & Response).
	Site feature logs	Use this menu to view log messages about configuration changes made by the NCC for the site.

Table 13 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
	Configure	
	Access points	
	SSID settings	Use this menu to view and configure SSID settings and authentication methods.
	SSID advanced settings	Use this menu to configure network access, traffic options, advanced settings for SSID profiles, SSID visibility settings, and set whether the SSID is enabled or disabled on each day of the week.
	Captive portal customization	Use this menu to configure captive portal settings for SSID profiles.
	Radio settings	Use this menu to configure global radio settings, such as maximum output power or channel width, and enable smart client steering for all Access Points in the site.
	Traffic shaping	Use this menu to configure the maximum bandwidth and load balancing.
	Security service	Use this menu to enable application visibility and optimization, and IP reputation filter on the managed Access Point.
	AP & port settings	Use this menu to configure load balancing settings and enable or disable a port on the managed Access Point and configure the port's VLAN settings.
	Switches	
	Switch ports	Use this menu to view the Switch port statistics and configure Switch settings for the ports.
	Port profiles	Use this menu to create profiles that can be applied to each port on the Nebula Device. A port profile can enable the following features such as RSTP, STP guard, port isolation, loop guard, storm control, and PoE.
	Stacking management	Use this menu to create a stacking system, configure the stacking settings, and view the stacking status.
	ACL	Use this menu to configure the access control list in order to control access to the Switches.
	IP & Routing	Use this menu to configure layer 3 features such as creating IP interfaces and static routes on the Switch.
	ONVIF discovery	Use this menu to enable ONVIF and configure ONVIF VLAN ID for the selected Switch.
	Advanced IGMP	Use this menu to enable and configure IGMP snooping and create IGMP filtering profiles.
	Authentication	Use this menu to configure authentication servers and policies.
	PoE schedules	Use this menu to set the schedule for Switches in distributing power to powered devices.
	Switch settings	Use this menu to configure global Switch settings, such as (R)STP, QoS, port mirroring, voice VLAN and DHCP white list.

Table 13 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
	Security router	
	Interface	Use this menu to configure interface address, subnet mask and VLAN ID settings on the Security Router.
	Threat management	Use this menu to enable threat management categories, configure exception list using client's name/IP address, and allowed/blocked domain name list.
	Traffic management	Use this menu to manage the use of various applications on the network and control access to specific web sites or web content.
	Firewall	Use this menu to configure firewall rules for outbound traffic, create new NAT rules and edit/delete existing NAT rules.
	Site-to-Site VPN	Use this menu to configure VPN rules between Security Routers.
	Remote access VPN	Use this menu to enable and configure IPsec VPN rule from off-site clients to an on-site Security Router. Note: The SCR 50AXE does not support Remote access VPN.
	SSID settings	Use this menu to view and configure SSID settings and authentication methods.
	SSID advanced settings	Use this menu to configure WiFi security, band selection, assisted roaming and U-APSD (Unscheduled automatic power save delivery) settings for the SSID profiles.
	Radio settings	Use this menu to configure global radio settings, such as maximum output power or channel width, and enable smart client steering for all Security Routers in the site.
	Router settings	Use this menu to configure DNS settings.
	Firewall	
	Port	Use this menu to configure network mode and port grouping on the Security Firewall (USG Flex / ATP Series).
	Interface	Use this menu to configure interface address, subnet mask and VLAN ID settings on the Security Firewall (USG Flex / ATP Series).
	Port and Interface	Use this menu to configure port groups and network interfaces on the Security Firewall (USG FLEX H Series).
	Routing	Use this menu to view and configure policy routes, static routes and WAN load balancing.
	NAT	Use this menu to view and configure virtual servers and NAT settings.
	Site-to-Site VPN	Use this menu to configure VPN rules between Security Firewalls.
	Remote access VPN	Use this menu to enable and configure IPsec VPN or L2TP VPN rules from off-site clients to an on-site Security Firewall.
	Security policy	Use this menu to configure firewall rules for outbound traffic, application patrol, schedule profiles and port forwarding rules for inbound traffic.
	Security service	Use this menu to enable content filter and block access to specific web sites. You can also enable Anti-virus and Intrusion Detection and Prevention (IDP) on the Security Firewall.
	Captive portal	Use this menu to configure captive portal settings for each Security Firewall interface.
	Authentication method	Use this menu to configure network access settings through a captive portal or Nebula Cloud Authentication.

Table 13 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
	Wireless	Use this menu to configure different SSID profiles for your ZyWALL USG FLEX 100W and USG20W-VPN. Note: This menu only appears for the ZyWALL USG FLEX 100W and USG20W-VPN.
	Firewall settings	Use this menu to configure the DNS server and address records and also set the external AD (Active Directory) server or RADIUS server that the Security Firewall can use in authenticating users. You can also specify walled garden web site links for all interfaces on the Security Firewall.
	Security gateway	
	Interface addressing	Use this menu to configure network mode, port grouping, interface address, static route and DDNS settings on the security gateway.
	Policy route	Use this menu to view and configure policy routes.
	Firewall	Use this menu to configure firewall rules for outbound traffic, application patrol, schedule profiles and port forwarding rules for inbound traffic.
	Security service	Use this menu to enable content filter and block access to specific web sites. You can also enable Anti-virus and Intrusion Detection and Prevention (IDP) on the security gateway.
	Site-to-Site VPN	Use this menu to configure VPN rules.
	Remote access VPN	Use this menu to enable and configure IPsec VPN or L2TP VPN settings.
	Captive portal	Use this menu to configure captive portal settings for each security gateway interface.
	Network access method	Use this menu to enable or disable web authentication on an interface.
	Traffic shaping	Use this menu to configure the maximum bandwidth and load balancing.
	Gateway settings	Use this menu to configure the DNS server and address records and also set the external AD (Active Directory) server or RADIUS server that the security gateway can use in authenticating users. You can also specify walled garden web site links for all interfaces on the security gateway.
	Alert settings	Use this menu to set which alerts are created and emailed or sent by the Zyxel Nebula Mobile app. You can also set the email addresses to which an alert is sent.
	Firmware management	Use this menu to upgrade firmware or schedule firmware upgrades for Nebula Devices in the site.
	Cloud authentication	Use this menu to add user accounts and grant user access to the selected site through different authentication methods, such as the MAC-based authentication, captive portal or the IEEE 802.1x authentication method.
	Collaborative detection & response	Use this menu to view and configure the policies and notification settings for malware, IDP and web threats and corresponding containment actions to quarantine, alert or block. This is only available for ZyWALL USG Flex Series and ZyWALL ATP Series at the time of writing.
	Site settings	Use this menu to change the general settings for the site, such as the site name, Nebula Device login password, captive portal reauthentication, SNMP, AP traffic logs to a Syslog server, traffic logs to SecuReporter, WiFi network authentication voucher settings, and API access for DPPSK third-party integration.

Table 13 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
Organization-wide	License & inventory	Use this menu to manage your licenses and view the summary of Nebula Devices which have been registered and assigned to the sites in the selected organization.
	Administrators	Use this menu to view, remove, or create a new administrator account for this organization.
	Organization-wide manage	
	Organization portal	Use this menu to view a list of sites belonging to the selected organization and detailed information about the Nebula Devices connected to the sites.
	Configuration management	Use this menu to synchronize the configuration between sites or switch ports and back up or restore a configuration file.
	Configuration templates	Use this menu to create or delete a configuration template or bind a site to the template.
	VPN orchestrator	Use this menu to view and manage VPNs created for the selected organization.
	Security profile sync	Use this menu to synchronize the settings of URL threat filter, anti-malware and content filter on the selected gateways.
	Firmware management	Use this menu to upgrade firmware or schedule firmware upgrades for Nebula Devices in the organization.
	Cloud authentication	Use this menu to create or remove user accounts and grant user access to all sites in the selected organization through different authentication methods, such as MAC-based authentication, captive portal, or the IEEE 802.1x authentication method.
	Change log	Use this menu to view log messages about configuration changes in this organization.
	Organization settings	Use this menu to configure security settings or delete the organization.
Group-wide	Group-wide manage	
	Group portal	Use this menu to view organization and license details of a selected group.
	Org-to-Org VPN	Use this menu to view and manage VPNs between members in the group.
	Inventory	Use this menu to view Nebula Devices belonging to organizations. You may also export the list of Nebula Devices found to your computer.
	Administrators	Use this menu to view, remove, or create a new administrator account for the selected group.
	Change log	Use this menu to view log messages about configuration changes in the group.
	Group settings	Use this menu to configure group information and group members.

Table 13 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
MSP	MSP cross-org manage	
	MSP portal	Use this menu to create multiple organizations and change the branding and assign administrators to multiple organizations.
	Admins & teams	Use this menu to create administrators or groups of administrators (teams) and view their login details.
	Cross-org synchronization	Use this menu to sync or clone organization-wide settings from a source organization to a destination organization.
	Backup & restore	Use this menu to back up your current Security Firewall's configurations to NCC, or restore a previously saved configuration to the site.
	Alert templates	Use this menu to configure **MSP alert template**s to monitor Nebula Devices for unexpected events (for example, online or offline events).
	Firmware upgrades	Use this menu to check the Nebula Devices' firmware status across organizations and schedule firmware upgrades.
	Change log	Use this menu to view log messages about configuration changes in the **Admins & teams** and **Cross-org synchronization** screens.
	MSP branding	Use this menu to upload/replace/remove the dashboard logo. You can also set the support contact details.

1.4 Create Organization

Use this screen to first create an organization, then create a site (network) in the organization, and finally add Nebula Devices to the site.

Note: You have to contact Zyxel customer support if you need to change the device owner or remove an Organization from the NCC. But an administrator can remove sites without customer support. Configure your Nebula Device owners and organizations carefully. See also Section 12.2 on page 659.

Note: There is no limit as to how many organizations you can create, but you can only activate a trial license up to 10 new organizations every 90 days. The expiration date of the organization created using a trial license is shown.

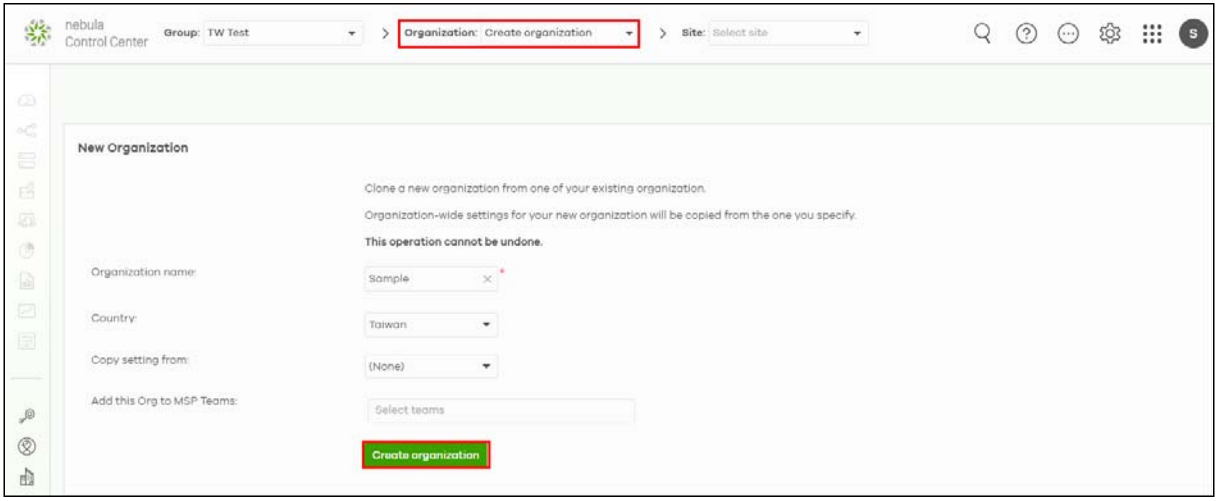
1 Click **Create Organization** from the **Organization** drop-down list box in the title bar. The Wizard starts. See Chapter 2 on page 63 for detailed information about how to use the wizard to create an organization and site. Otherwise, click **Exit Wizard** to close the wizard and display the **Create organization** screen.

2 Enter a name for your organization.

3 If you already have one or more than one organization under your account and you want to copy the organization settings of an existing one, select the organization name from the **Copy setting from** field and also **Add this Org to MSP Teams** by selecting existing teams before clicking the **Create organization** button.

4 Click the **Create organization** button to add a new organization.

Figure 28 Create Organization



New Organization

Clone a new organization from one of your existing organization.

Organization-wide settings for your new organization will be copied from the one you specify.

This operation cannot be undone.

Organization name: Sample *

Country: Taiwan

Copy setting from: (None)

Add this Org to MSP Teams: Select teams

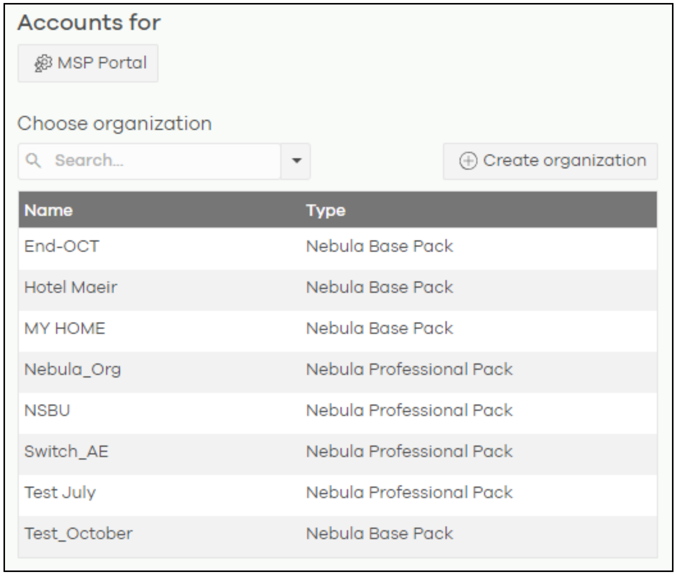
5 Choose whether to activate a one-month trial of Nebula Pro Pack and Nebula Security Services for the organization. For example, USG FLEX 700, Secure WiFi License, 1MO; USG FLEX 700, UTM Security Pack License, 1MO; Nebula Professional Pack License, 1MO.

1.5 Choose Organization

When you have more than one organization on your account, the following screen displays right after you log in. Select the organization you want to manage now, access the **MSP Portal** or click **Create organization** to add a new one.

Note: You need to purchase an MSP license to see the MSP Portal menu.

Figure 29 Choose Organization

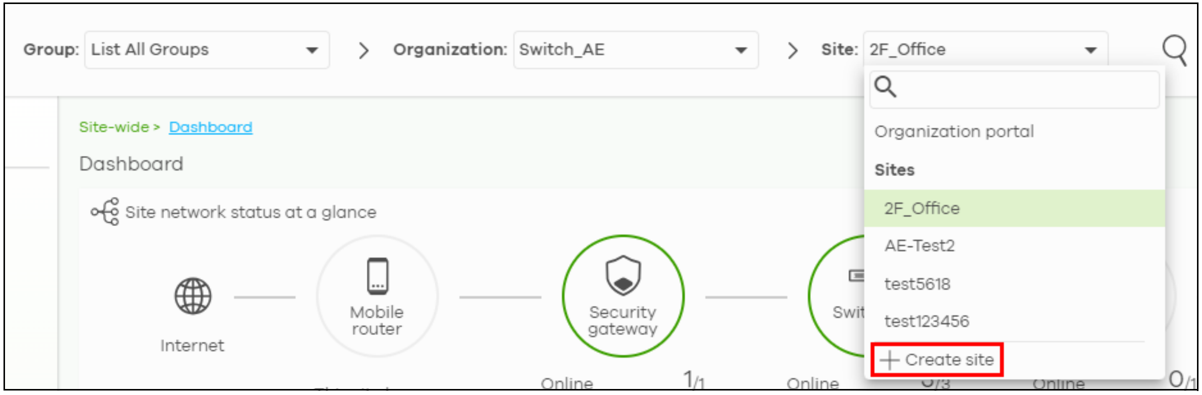


Name	Type
End-OCT	Nebula Base Pack
Hotel Maeir	Nebula Base Pack
MY HOME	Nebula Base Pack
Nebula_Org	Nebula Professional Pack
NSBU	Nebula Professional Pack
Switch_AE	Nebula Professional Pack
Test July	Nebula Professional Pack
Test_October	Nebula Base Pack

1.6 Create Site

To add more sites to an organization, select **Create site** from the **Site** drop-down list box to create a new one.

Figure 30 NCC Title Bar: Group/Organization/Site: Create site



Create One Site

If you need to create a site in your organization, do the following:

1 To create a single site, select the **One site** tab.

2 Enter a descriptive name, 1 – 64 characters including 0–9 a–z A–Z `~!@#$%&*(_+-={} | [];'"./<> ?) in the **Site name**.

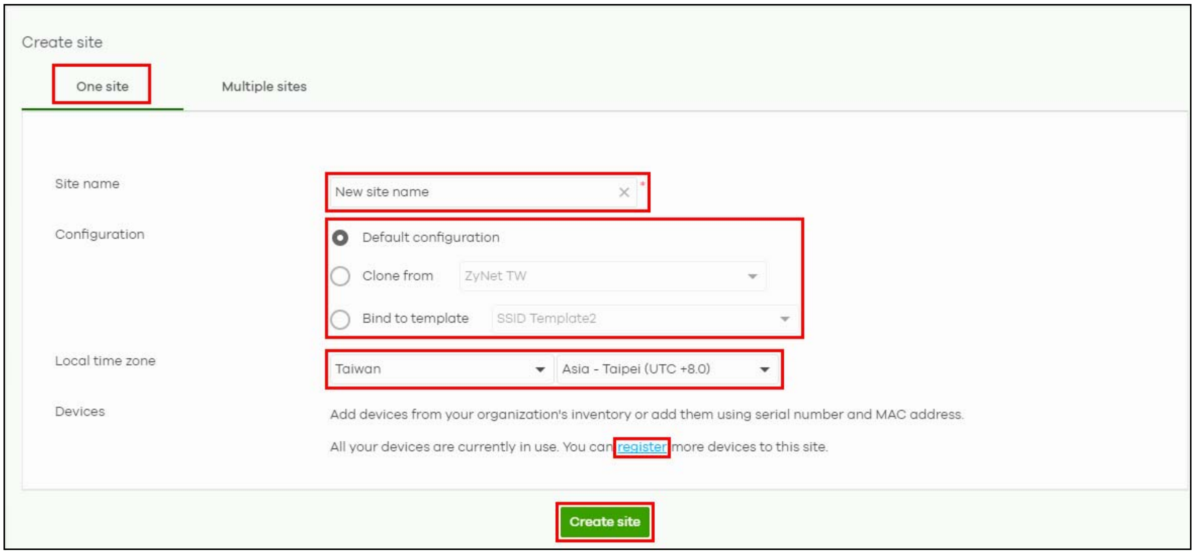
3 Set the site's configuration:

- Select **Clone from** if you want to copy the configuration from another site.
- Select **Bind to template** if you want to bind the site to a configuration template created in **Organization-wide** > **Organization-wide manage** > **Configuration templates**. A configuration template is a virtual site. The settings you configured in a template will apply to the real sites which are bound to the template.
- Otherwise, select **Default configuration**.

4 Select the **Local time zone** of the site's location.

5 Click the **register** link in **You can register more devices to this site.** to add device(s) to your site. See Section 12.2.2 on page 662 for more details.

6 Click the **Create site** button to add a new site.



Create site

One site | Multiple sites

Site name: New site name ×

Configuration:
● Default configuration
○ Clone from ZyNet TW
○ Bind to template SSID Template2

Local time zone: Taiwan | Asia - Taipei (UTC +8.0)

Devices: Add devices from your organization's inventory or add them using serial number and MAC address.

All your devices are currently in use. You can register more devices to this site.

Create site

Create Multiple Sites

If you need to create multiple sites and even add Nebula Device(s) to the site at the same time, do the following:

1 To create more than one site, select the **Multiple sites** tab.

2 Set the sites' configuration:

- Select **Clone from** if you want to copy the configuration from another site.
- Select **Bind to template** if you want to bind the sites to a template created in **Organization-wide** > **Organization-wide manage** > **Configuration templates**. A configuration template is a virtual site. The settings you configured in a template will apply to the real sites which are bound to the template.
- Otherwise, select **Default configuration**.

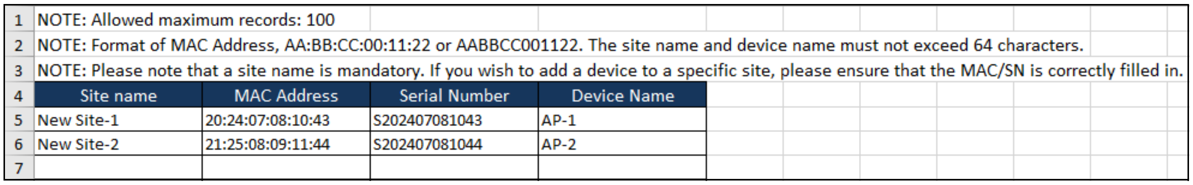
3 Select the **Local time zone** of the site administrator's location.

4 Click the **Download sample import file** link to download a blank Excel file template, edit it accordingly, and save it. The Excel file template can contain the following, maximum of 100 rows:

- **Site name**. Enter a descriptive name, up to 64 characters including 0–9 a–z A–Z `~!@#$%&*(_+-={} | [];"'./<> ?). You can enter multiple rows with the same site name when adding Nebula Devices to the same site.

Note: NCC does not allow duplicate same site.

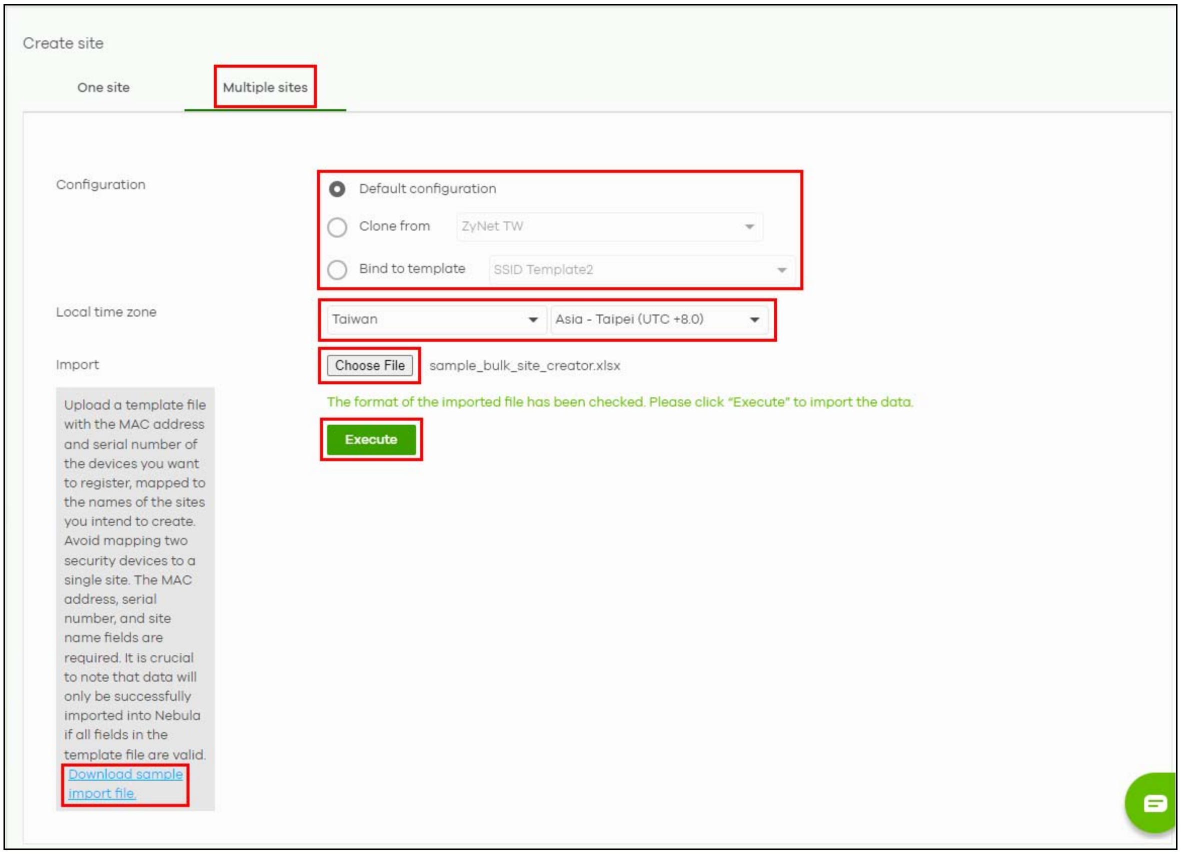
- **MAC address** (optional). Enter the unique MAC address of the Nebula Device(s) to add to the new site. Make sure to use the correct format AA:BB:CC:00:11:22 or AABBCC001122.
- **Serial number** (optional). Enter the unique serial number of the Nebula Device(s) to add to the new site.
- **Device name** (optional). Assign a unique name to the Nebula Device, up to 64 characters including 0–9 a–z A–Z `~!@#$%&*(_+-={} | [];"'./<> ?).



1	NOTE: Allowed maximum records: 100			
2	NOTE: Format of MAC Address, AA:BB:CC:00:11:22 or AABBCC001122. The site name and device name must not exceed 64 characters.			
3	NOTE: Please note that a site name is mandatory. If you wish to add a device to a specific site, please ensure that the MAC/SN is correctly filled in.			
4	Site name	MAC Address	Serial Number	Device Name
5	New Site-1	20:24:07:08:10:43	S202407081043	AP-1
6	New Site-2	21:25:08:09:11:44	S202407081044	AP-2
7				

5 Click **Choose file** to locate the Excel file you wish to upload to NCC.

6 Click the **Execute** button to add new sites and optional Nebula Devices.



Create site

Configuration

● Default configuration

○ Clone from ZyNet TW

○ Bind to template SSID Template2

Local time zone: Taiwan | Asia - Taipei (UTC +8.0)

Import: Choose File sample_bulk_site_creator.xlsx

The format of the imported file has been checked. Please click "Execute" to import the data.

Upload a template file with the MAC address and serial number of the devices you want to register, mapped to the names of the sites you intend to create. Avoid mapping two security devices to a single site. The MAC address, serial number, and site name fields are required. It is crucial to note that data will only be successfully imported into Nebula if all fields in the template file are valid. Download sample import file.

Note: NCC will check and display an error message when:

The Nebula Device has already been added to NCC or registered to an organization

Entry format error in the Excel file template

Duplicate site name.

1.7 Cloud-Saving Mode

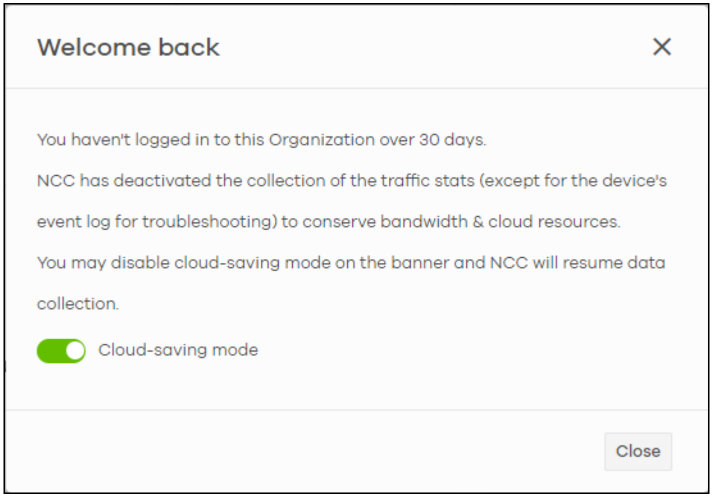
If you do not log into a base (free) license tier organization for over 30 days, the organization automatically enters Cloud-saving mode to save your network bandwidth and cloud resources.

When Cloud-saving is enabled, NCC does not record any data traffic statistics, except the following:

- Event logs
- Security Appliance WAN interface logs between the Nebula Device and NCC, and
- NSS (Nebula Security Service) analysis report (requires Nebula Security Pack (Nebula Security Service) license).

To disable Cloud-saving mode, click the **Cloud-saving mode** switch or click the link in the NCC banner when notified.

Figure 31 Cloud-saving mode



Welcome back

You haven't logged in to this Organization over 30 days.

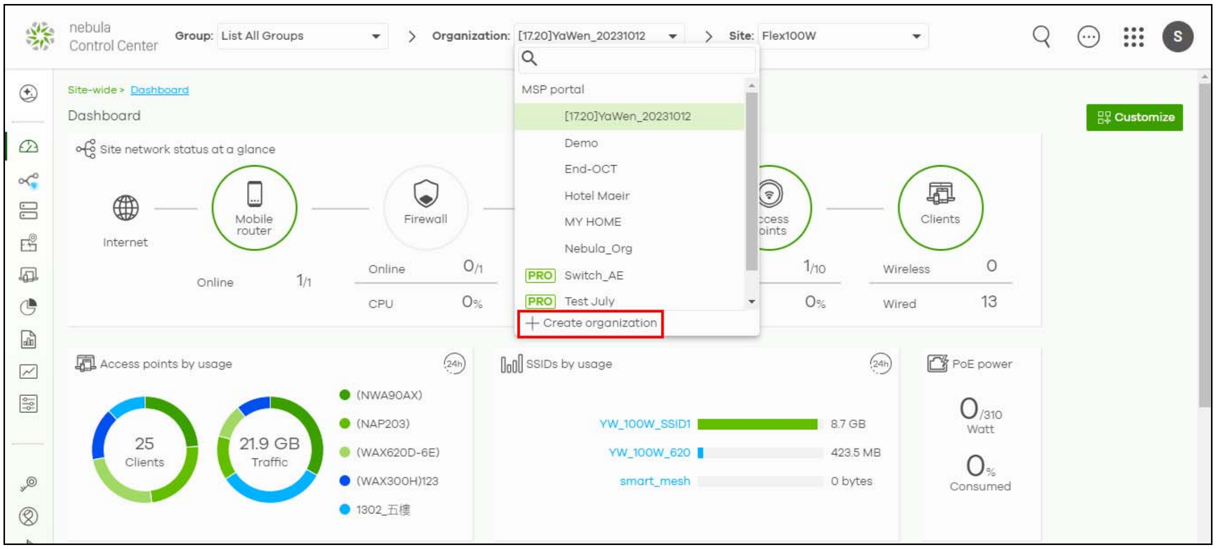
NCC has deactivated the collection of the traffic stats (except for the device's event log for troubleshooting) to conserve bandwidth & cloud resources.

You may disable cloud-saving mode on the banner and NCC will resume data collection.

CHAPTER 2
Setup Wizard

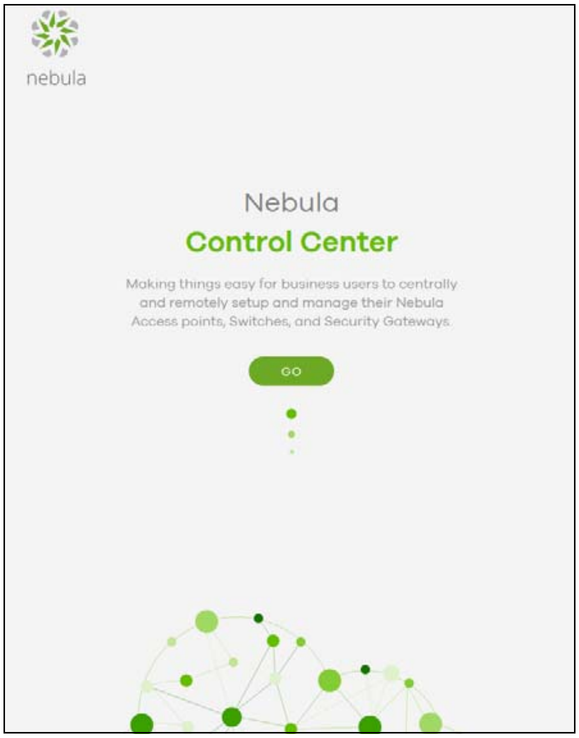
2.1 Setup Wizard

- The setup wizard helps you create an organization and site, add Nebula Devices, upgrade your Nebula Device firmware, and set up WiFi networks quickly.
- The wizard appears automatically after you log in the first time or if there is no organization created under your account.
- The wizard also starts when you click **Create Organization** from the **Organization** drop-down list box in the title bar.



2.1.1 Step1: Run the Wizard

1 After logging in to *https://nebula.zyxel.com*, the following screen appears. Click **GO** to start the NCC wizard.

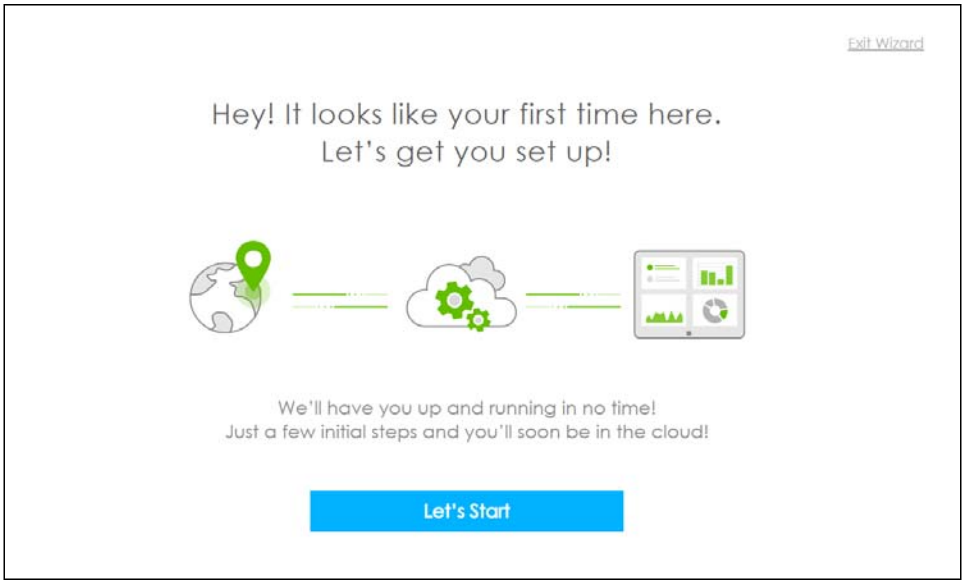

nebula

Nebula

Control Center

Making things easy for business users to centrally and remotely setup and manage their Nebula Access points, Switches, and Security Gateways.

2 The welcome screen displays when you are creating the first organization under your account. Click **Let's Start** to begin.



Hey! It looks like your first time here.
Let's get you set up!

We'll have you up and running in no time!
Just a few initial steps and you'll soon be in the cloud!

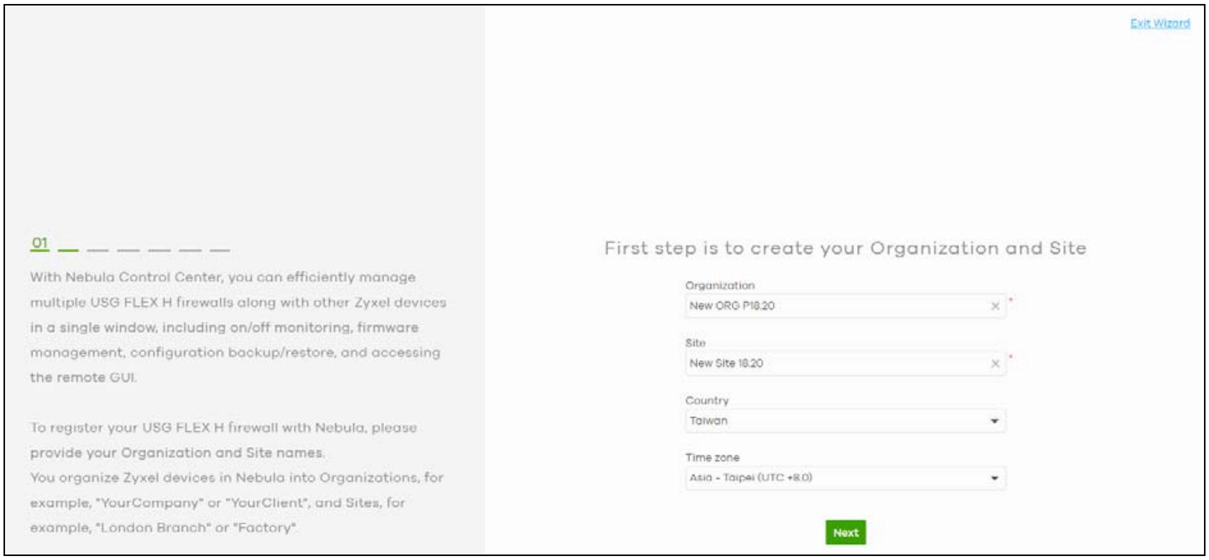
Note: This screen will appear only if you have not created a new organization.

2.1.2 Step 2: Create an Organization and Site

1 Enter a descriptive name for your organization and site. Both names must consist of 1 – 64 characters.

2 Select the time zone of your location. This will set the time difference between your time zone and Coordinated Universal Time (UTC).

3 Click **Next** to continue.



01

With Nebula Control Center, you can efficiently manage multiple USG FLEX H firewalls along with other Zyxel devices in a single window, including on/off monitoring, firmware management, configuration backup/restore, and accessing the remote GUI.

To register your USG FLEX H firewall with Nebula, please provide your Organization and Site names.
You organize Zyxel devices in Nebula into Organizations, for example, "YourCompany" or "YourClient", and Sites, for example, "London Branch" or "Factory".

First step is to create your Organization and Site

Organization: New ORG P18.20 *

Site: New Site 18.20 *

Country: Taiwan

Time zone: Asia - Taipei (UTC +8.0)

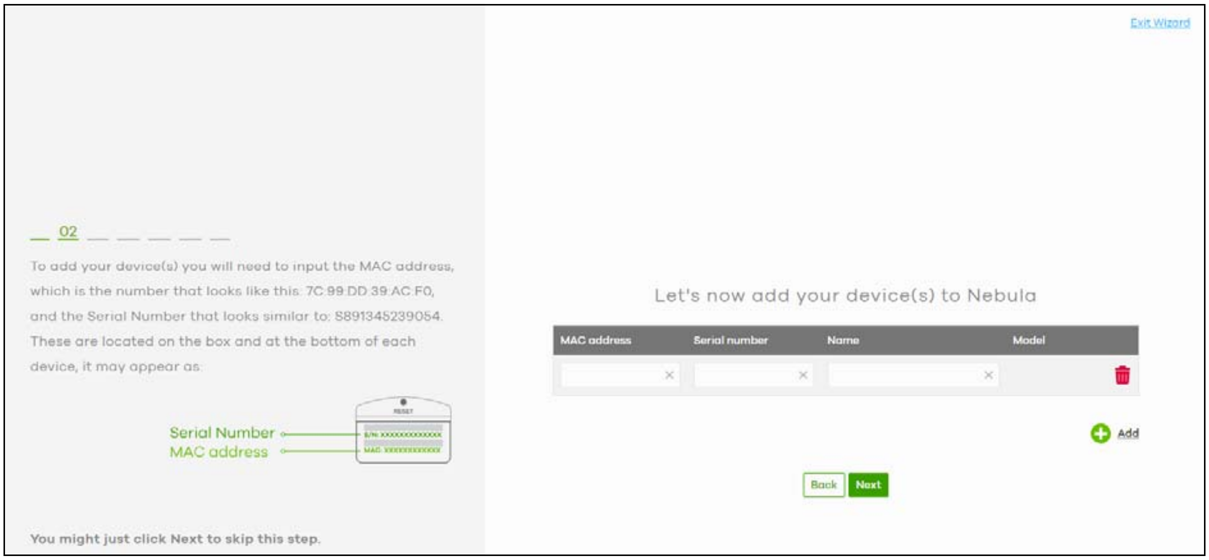
2.1.3 Step 3: Add Your Nebula Devices

1 Enter your device's MAC address and serial number.

You can also leave the fields blank and click **Next** to move on to the next step without adding a Nebula Device.

2 Click the **+ Add** button to register and add the Nebula Device to the site. You can register multiple Nebula Devices at a time.

3 Click **Next** to proceed.



02

To add your device(s) you will need to input the MAC address, which is the number that looks like this: 7C:99:DD:39:AC:F0, and the Serial Number that looks similar to: S891345239054. These are located on the box and at the bottom of each device, it may appear as:

You might just click Next to skip this step.

Let's now add your device(s) to Nebula

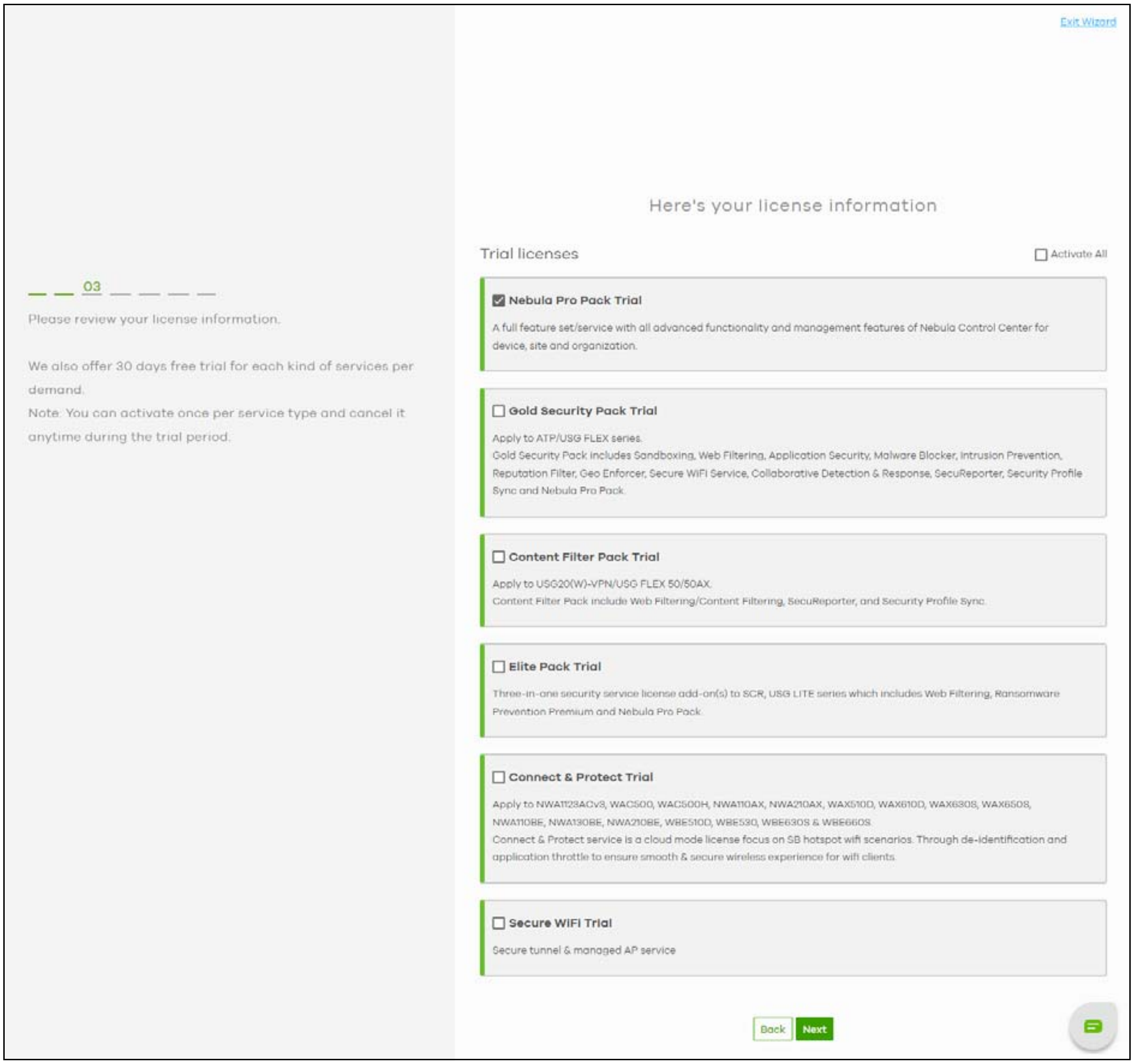
MAC address	Serial number	Name	Model

2.1.4 Step 4: Activate the Trial License(s)

You can decide if you want to activate a one-month trial period of Nebula Pro Pack and Nebula Security Services for the organization. Before deciding on the trial license to activate, see Section 12.2.8 on page 672 for more information.

Note: Before activating a trial license, make sure the services in the license can be used by a Nebula Device in the organization.

If you choose to activate a trial license, click to select the trial license(s) and then click **Next**. NCC will send you an email reminding you to purchase the full license when the trial is close to expiring.



Please review your license information.

We also offer 30 days free trial for each kind of services per demand.

Note: You can activate once per service type and cancel it anytime during the trial period.

Here's your license information

Trial licenses

□ Activate All

☑ **Nebula Pro Pack Trial**

A full feature set/service with all advanced functionality and management features of Nebula Control Center for device, site and organization.

□ **Gold Security Pack Trial**

Apply to ATP/USG FLEX series.
Gold Security Pack includes Sandboxing, Web Filtering, Application Security, Malware Blocker, Intrusion Prevention, Reputation Filter, Geo Enforcer, Secure WiFi Service, Collaborative Detection & Response, SecuReporter, Security Profile Sync and Nebula Pro Pack.

□ **Content Filter Pack Trial**

Apply to USG20(W)-VPN/USG FLEX 50/50AX.
Content Filter Pack include Web Filtering/Content Filtering, SecuReporter, and Security Profile Sync.

□ **Elite Pack Trial**

Three-in-one security service license add-on(s) to SCR, USG LITE series which includes Web Filtering, Ransomware Prevention Premium and Nebula Pro Pack.

□ **Connect & Protect Trial**

Apply to NWA1123ACv3, WAC500, WAC500H, NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, WAX650S, NWA110BE, NWA130BE, NWA210BE, WBE510D, WBE530, WBE630S & WBE660S.
Connect & Protect service is a cloud mode license focus on SB hotspot wifi scenarios. Through de-identification and application throttle to ensure smooth & secure wireless experience for wifi clients.

□ **Secure WiFi Trial**

Secure tunnel & managed AP service

2.1.5 Step 5: Upgrade your Nebula Device Firmware

You should always use the most recent firmware to get the latest features, improvements, and bug fixes by clicking **Yes** (default setting).

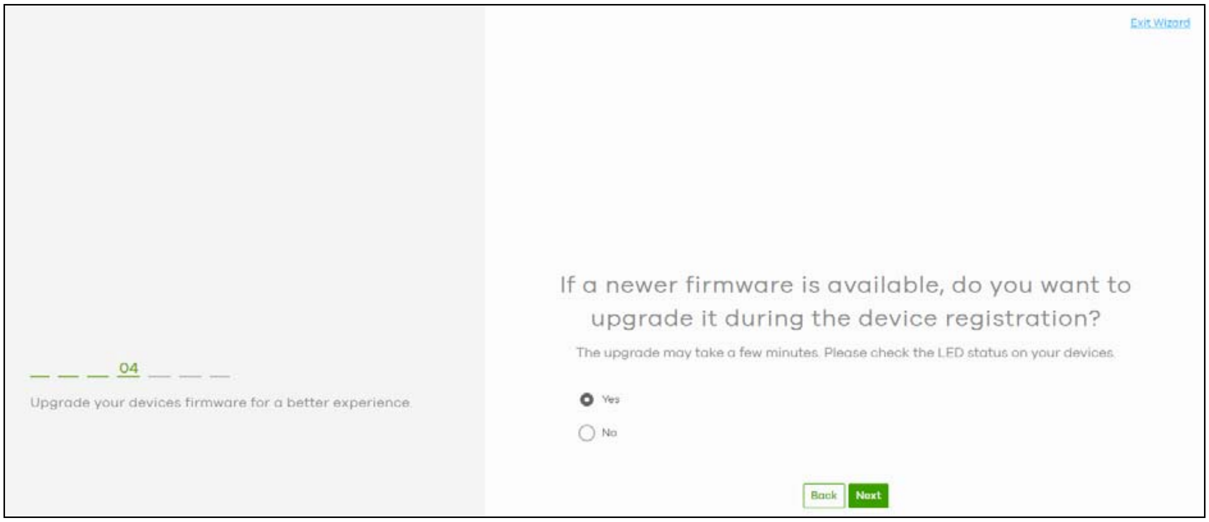
Even if you choose not to upgrade the firmware, NCC will still perform a mandatory upgrade to **Stable** firmware version if the Nebula Device's firmware have security vulnerabilities, and/or lack key performance improvements. See Table 203 on page 707 for the description of a **Stable** firmware.

The following table shows when a mandatory firmware upgrade occurs for the different Nebula Device types.

Table 14 Mandatory Firmware Upgrade Behavior

NEBULA DEVICE TYPE	MANDATORY FIRMWARE UPGRADE TIME
Access Points	The mandatory firmware upgrade occurs when the Nebula Device is online with NCC.
Switches / Security Appliances	The mandatory firmware upgrade occurs after registering the Nebula Device on NCC.

Click **Next** to proceed.



04

Upgrade your devices firmware for a better experience.

If a newer firmware is available, do you want to upgrade it during the device registration?

The upgrade may take a few minutes. Please check the LED status on your devices.

● Yes

○ No

2.1.6 Step 6: Set up your WiFi Network

1 Configure the WiFi settings for the managed APs. Enter the WiFi network name (SSID) and the WiFi password.

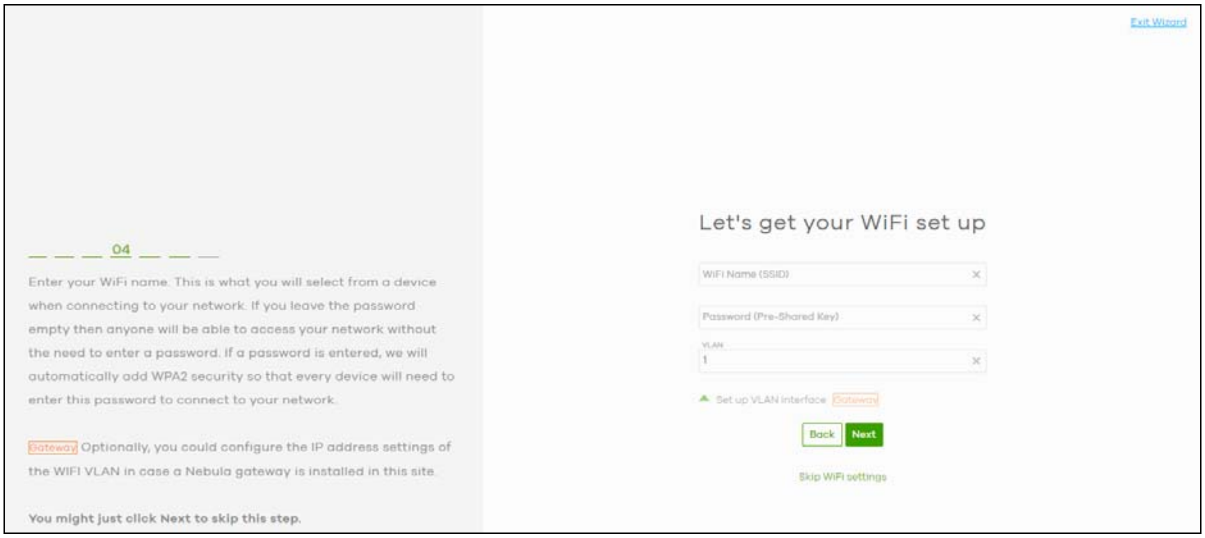
You can also leave the fields blank and click **Next** to move on to the next step without setting up the main WiFi network.

2 Configure the ID number of the VLAN to which the SSID belongs.

The VLAN ID 1 is generated automatically by the NCC and reserved for a gateway's LAN 1 and LAN 2 by default. The IPv4 subnets 192.168.1.0/24 and 192.168.2.0/24 are also reserved for these two LAN interfaces.

If you enter a different VLAN ID other than the default one ("1") in the **VLAN** field, click the **Set up VLAN interface** link to create a gateway interface with the specified VLAN ID. You need to configure an IPv4 address and subnet mask and enable the DHCP server function for this interface.

3 Click **Next** to proceed.



04

Enter your WiFi name. This is what you will select from a device when connecting to your network. If you leave the password empty then anyone will be able to access your network without the need to enter a password. If a password is entered, we will automatically add WPA2 security so that every device will need to enter this password to connect to your network.

Gateway Optionally, you could configure the IP address settings of the WIFI VLAN in case a Nebula gateway is installed in this site.

You might just click Next to skip this step.

Let's get your WiFi set up

WiFi Name (SSID)

Password (Pre-Shared Key)

VLAN: 1

2.1.7 Step 7: Set up a Guest WiFi Network

1 Configure WiFi and VLAN settings for guest users who can wirelessly access the Internet or networks through Nebula Devices.

You can also leave the fields blank and click **Next** to move on to the next step without setting up the guest WiFi network.

2 If you want to enable web authentication, select **Clicking "Agree" to access the network** to block network traffic until a client agrees to the policy of user agreement. Otherwise, select **Using their Facebook account to join the network** to block network traffic until the client logs in using his/her existing Facebook account.

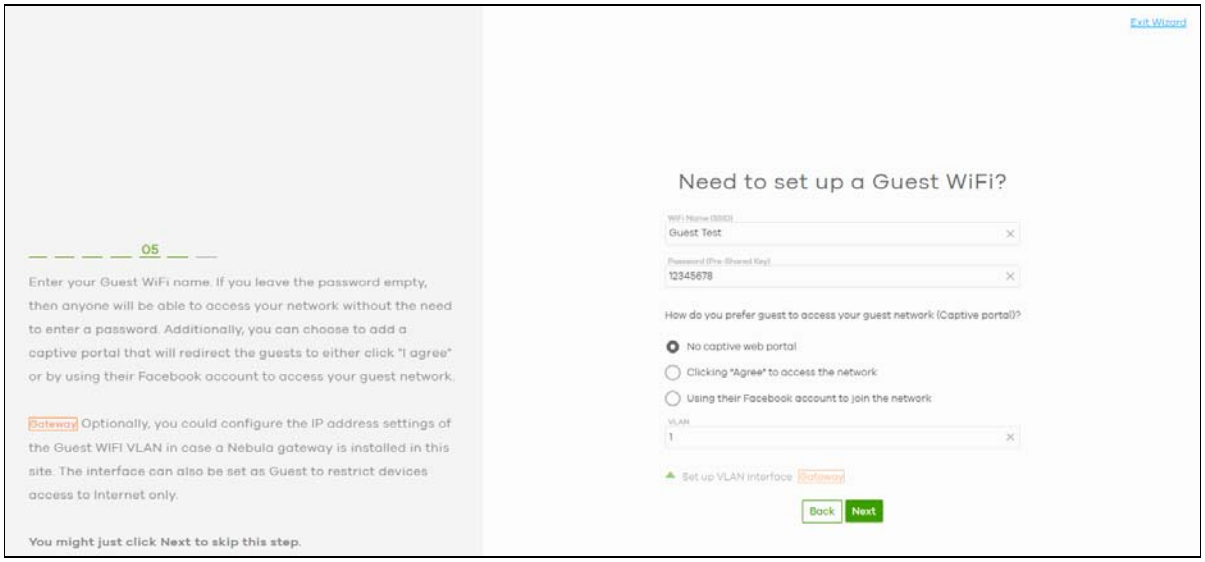
Note: If you do not enable any WiFi security, your network is accessible to any WiFi networking device that is within range.

Note: The guest network function and Layer 2 isolation between clients are enabled on this WiFi network by default.

If you enter a different VLAN ID other than the default one ("1") in the **VLAN** field, click the **Set up VLAN interface** link to create a gateway interface with the specified VLAN ID. You can set the gateway interface as a guest interface, configure the IPv4 address and subnet mask and enable the DHCP server function for this interface.

Note: If you set the guest WiFi network to use the same VLAN ID as the WiFi network and have already configured the gateway interface, the gateway interface configuration fields will be grayed out in this screen.

3 Click **Next** to proceed.



05

Enter your Guest WiFi name. If you leave the password empty, then anyone will be able to access your network without the need to enter a password. Additionally, you can choose to add a captive portal that will redirect the guests to either click "I agree" or by using their Facebook account to access your guest network.

Gateway Optionally, you could configure the IP address settings of the Guest WIFI VLAN in case a Nebula gateway is installed in this site. The interface can also be set as Guest to restrict devices access to Internet only.

You might just click Next to skip this step.

Exit Wizard

Need to set up a Guest WiFi?

WiFi Name (SSID): Guest Test

Password (Pre-Shared Key): 12345678

How do you prefer guest to access your guest network (Captive portal)?

● No captive web portal

○ Clicking "Agree" to access the network

○ Using their Facebook account to join the network

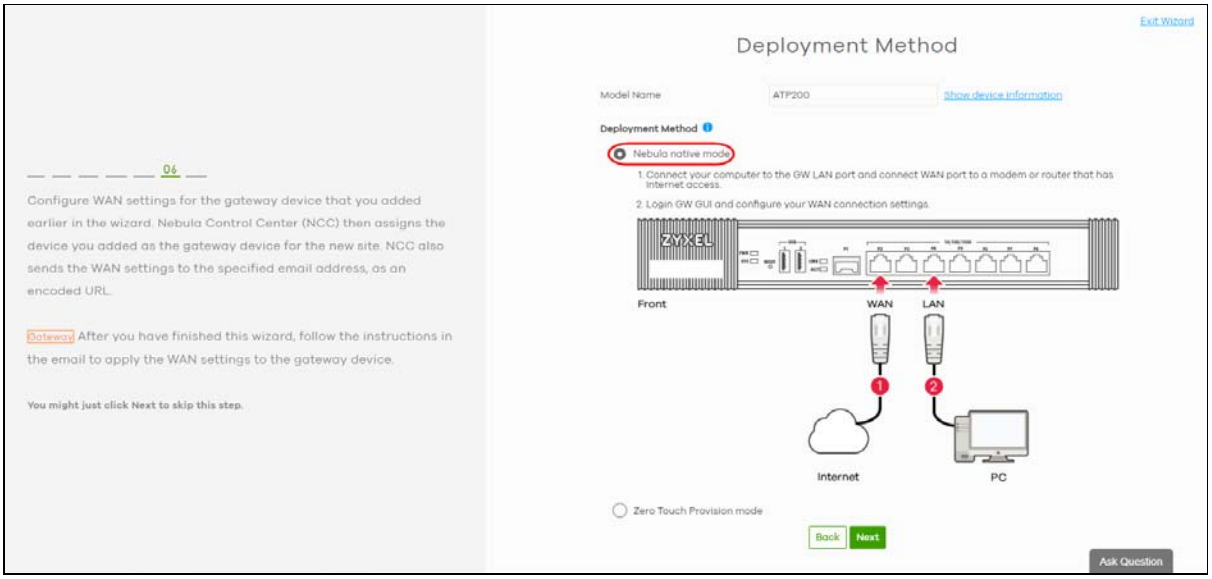
VLAN: 1

Set up VLAN interface Gateway

Back Next

2.1.8 Step 8: Set up the Deployment Method

If you added a ZyWALL USG FLEX / ATP / USG20(W)-VPN Series device in step 3, you need to select a deployment method for management by Nebula. Select **Nebula native mode** if available. If not, select **Zero Touch Provision mode** and configure an email address to send an activation link to the administrator who is in charge of managing the Nebula Device.



06

Configure WAN settings for the gateway device that you added earlier in the wizard. Nebula Control Center (NCC) then assigns the device you added as the gateway device for the new site. NCC also sends the WAN settings to the specified email address, as an encoded URL.

Gateway After you have finished this wizard, follow the instructions in the email to apply the WAN settings to the gateway device.

You might just click Next to skip this step.

Exit Wizard

Deployment Method

Model Name: ATP200 Show device information

Deployment Method

● Nebula native mode

1. Connect your computer to the GW LAN port and connect WAN port to a modem or router that has Internet access.
2. Login GW GUI and configure your WAN connection settings.

○ Zero Touch Provision mode

Back Next

Ask Question

2.1.8.1 Nebula Native Mode

To use the Nebula native mode deployment method, perform the steps described in On the Nebula Device.

2.1.8.2 Zero Touch Provision Mode

To configure the Zero Touch Provisioning (ZTP) settings, do the following in NCC:

1 Enable **VLAN Tag** and configure the **VLAN ID** (1 – 4094) for the WAN port.

2 Select **Static**/**DHCP**/**PPPoE**/**PPPoE with static IP** for the WAN type of the Nebula Device.

3 If you select **DHCP**, enter the **MTU** (Maximum Transmission Unit) to set the maximum size (1280 – 1500) of each data packet, in bytes, that can move through this interface.

If you select **Static**, enter the **IP Address**, **Subnet Mask**, **Default Gateway**, **First**/**Second DNS Server**, and **MTU** (1280 – 1500).

If you select **PPPoE**, select the **Authentication Type**, enter the **Username**, **Password**, and **MTU** (1280 – 1492).

If you select **PPPoE with static IP**, select the **Authentication Type**, enter the **Username**, **Password**, **IP Address**, **Default Gateway**, **First DNS Server** and **MTU** (1280 – 1492).

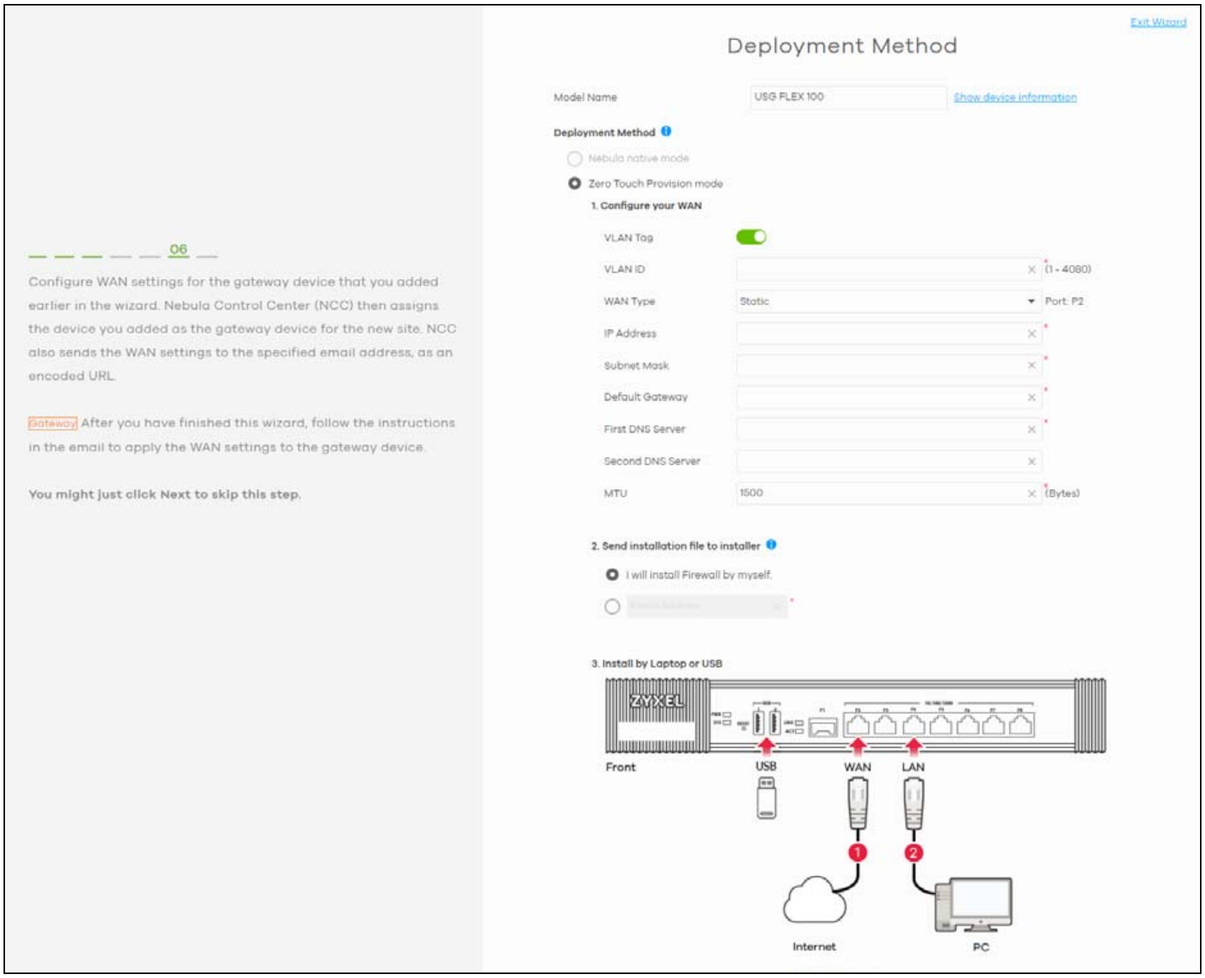
Note: Configure the VLAN ID and WAN interface for the Nebula Device exactly as your ISP gave it to you.

4 Click **Next**.

5 Select **I will install Firewall by myself** to receive an activation email and activation link/file. Alternatively, if you want another administrator to activate the Nebula Device, enter the recipient's **Email Address**.

6 Click **Next**.

7 Select where the Nebula Device will get and install the activation file, from a computer or through a USB drive.



06

Configure WAN settings for the gateway device that you added earlier in the wizard. Nebula Control Center (NCC) then assigns the device you added as the gateway device for the new site. NCC also sends the WAN settings to the specified email address, as an encoded URL.

Gateway After you have finished this wizard, follow the instructions in the email to apply the WAN settings to the gateway device.

You might just click Next to skip this step.

Exit Wizard

Deployment Method

Model Name: USG FLEX 100 Show device information

Deployment Method

○ Nebula native mode

● Zero Touch Provision mode

1. Configure your WAN

VLAN Tag	On	
VLAN ID		* (1 - 4080)
WAN Type	Static	Port: P2
IP Address		*
Subnet Mask		*
Default Gateway		*
First DNS Server		*
Second DNS Server		
MTU	1500	* (Bytes)

2. Send installation file to installer

● I will install Firewall by myself.

○ *

3. Install by Laptop or USB

On the Nebula Device

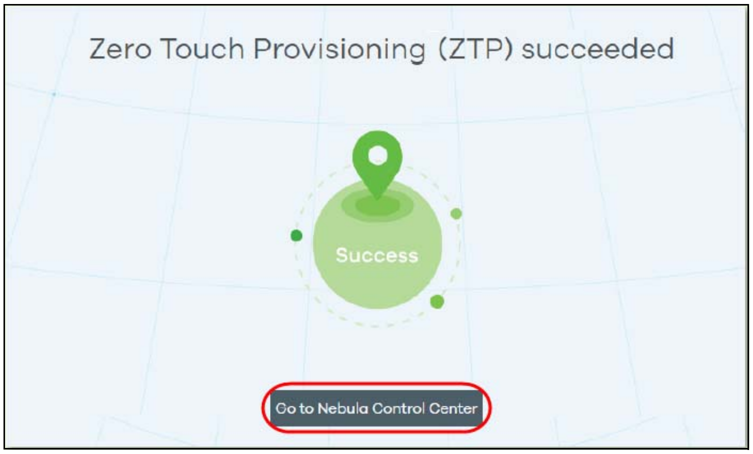
1 Back up the current configuration (in case you want to return to On Premises mode later).

2 Reset the Nebula Device if it was previously configured.

3 Connect the Nebula Device’s WAN port to a modem/router that has Internet access.

4 Connect your computer to the Nebula Device’s LAN port.

5 If you select **Nebula native mode**, go directly to step 7.
Click the activation link in the email.
Alternatively, save the activation file in the root directory of a USB drive. Then insert the USB drive into your Nebula Device.
Wait until Nebula Zero Touch Provisioning is successful.



Zero Touch Provisioning (ZTP) succeeded

6 Click **Go to Nebula Control Center** to configure the Nebula Device using NCC.

7 When you log into the Web Configurator for the first time or when you reset the Nebula Device to its default configuration, the **Initial Setup Wizard** screen displays. Choose **Nebula Mode** to manage your Nebula Device remotely using Nebula Control Center (NCC).

8 Follow the wizard to configure the Nebula Device network settings to connect to NCC.
The screens vary depending on the encapsulation type. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you do not have that information.

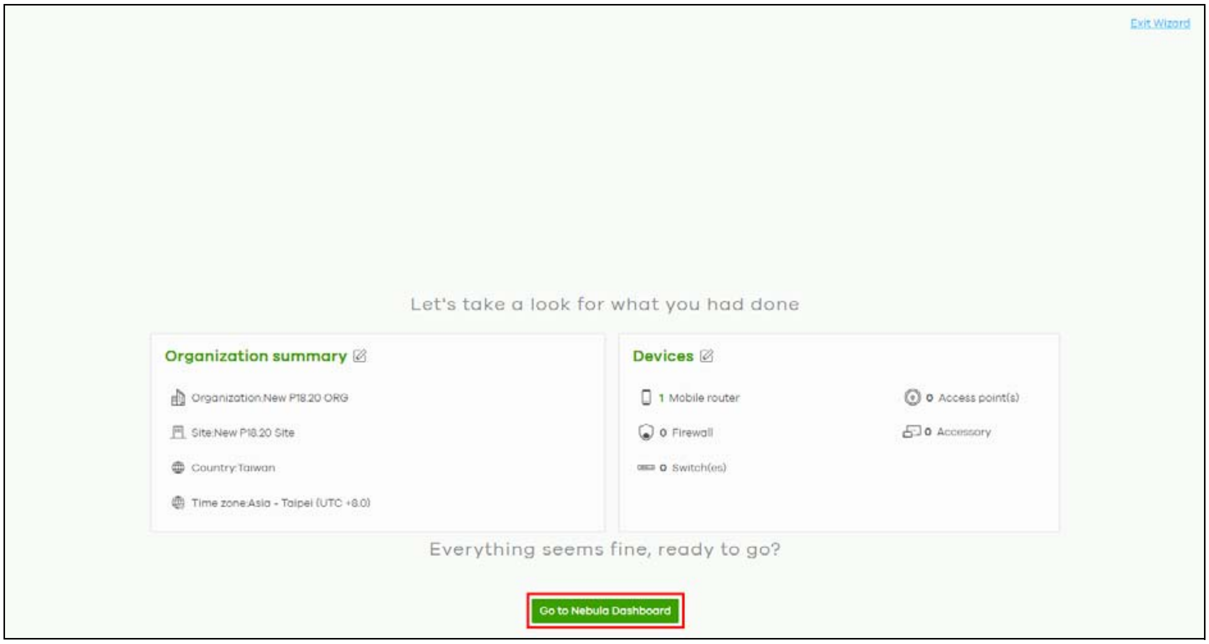
Note: Refer to the Nebula Device User’s Guide for more information.

2.1.9 Step 9: View the Summary

1 A summary of the wizard configuration will display after you complete the deployment method.

2 You can click a section’s edit icon (✎) to modify its setting.

3 You must click **Go to Nebula Dashboard** to save your changes in the wizard; otherwise click **Exit Wizard** to close the wizard screen without saving the settings.



Let's take a look for what you had done

Organization summary

Organization:New P18.20 ORG

Site:New P18.20 Site

Country:Taiwan

Time zone:Asia - Taipei (UTC +8.0)

Devices

1 Mobile router

0 Firewall

0 Switch(es)

0 Access point(s)

0 Accessory

Everything seems fine, ready to go?

Note: To set the administrator privileges, see Section 14.3.1 on page 746 for more information.

CHAPTER 3 Tutorials

3.1 Overview

This chapter shows you how to use the NCC's various features.

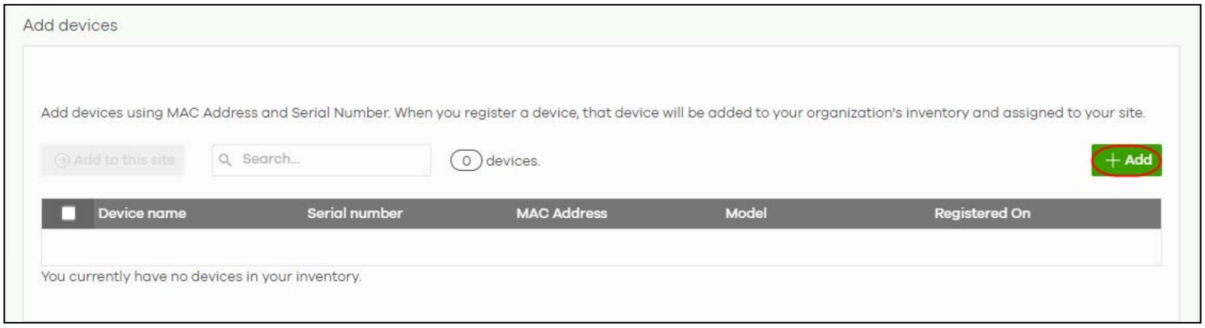
- Add a Nebula Device
- Activate and Assign a License for a Nebula Device, Site, or Organization
- Monitor a Site
- Know What Licenses are Set to Expire in My Site or Organization
- Renew an Expired License
- Transfer Licenses
- Change an Organization and/or Site Name
- Reset the Nebula Password
- Maintain Firmware
- Backup Current Configurations in NCC
- Assign an Administrator to Manage a Nebula Device
- Transfer the Ownership of the Organization
- Manage a Configuration Template
- Activate an MSP License
- Configure CNP/CNP Plus Security Services
- Delete an Organization
- Remote Access VPN Setup
- Route L2TP VPN Traffic
- Configure Guest Isolation on your WiFi Network
- Configure Content Filter to Block Access to Certain Websites
- Configure Schedule to Allow WiFi Access Only at Certain Times
- How to Position Multiple Nebula Devices (for Nebula Access Points only)
- Change the Default SSID and Password
- Change the WiFi Band Mode
- Check What Clients are Connected to Nebula Devices in your Network
- Find the SSID of the WiFi Client (for Nebula Access Points only)
- Use Tags to Assign SSIDs for Nebula Devices (for Nebula Access Points only)
- Resolve WiFi Connection Problems (for Nebula Access Points only)
- Configure WiFi Security with WPA2 Personal (for Nebula Access Points only)
- Configure WiFi Security with WPA2 Enterprise (for Nebula Access Points only)
- Configure a Captive Portal

- Create a Custom Captive Portal Page
- Limit Applications Usage or Block Applications
- Find the LAN Port Used by Connected Wired Client Devices (for Nebula Switches only)
- Configure Voice VLAN (for Nebula Switches only)
- Manage IPTV (for Nebula Switches only)
- Enable IP Source Guard (for Nebula Switches only)
- Set Up MAC Authentication With NCAS (for Nebula Switches only)
- Set Up Dynamic VLAN With RADIUS (for Nebula Switches only)
- Monitor Dynamic VLAN Using Event Logs (for Nebula Switches only)
- Register a Nebula Device (mobile router) in Nebula
- Using Collaborative Detection and Response (CDR)
- Deploy With Nebula Native Mode (for Security Firewalls in Nebula only)
- Configure DHCP Domain Name (for Security Firewalls in Nebula only)
- Monitor Client Bandwidth Usage (for Security Firewalls in Nebula only)
- Configure a Primary and Backup WAN (for Security Firewalls in NCC only)
- Enable Smart Mesh on a Security Router

3.2 Add a Nebula Device

This section shows you how to add a Mobile Router, Security Gateway, Nebula Firewall, Access Point or Switch to a selected organization and site on NCC for management.

1 Go to the **Site-wide** > **Devices** > **+** > **Add devices** screen. Click **+Add**.



Add devices

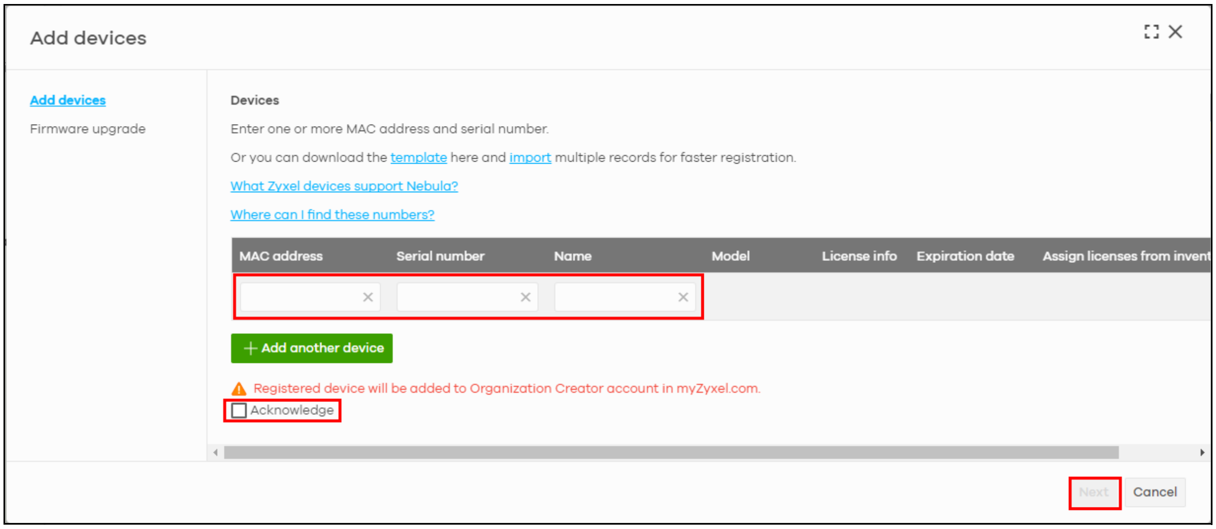
Add devices using MAC Address and Serial Number. When you register a device, that device will be added to your organization's inventory and assigned to your site.

□	Device name	Serial number	MAC Address	Model	Registered On

You currently have no devices in your inventory.

2 Enter the **Serial number**, **MAC address**, and a descriptive **Name** of the Nebula Device you want to add. Click the **Finish** button to save the changes.

Note: When a Nebula Device is added to a site other than a Nebula Device owner, the **Acknowledge** button appears. Click this button first to confirm that the **Serial number** and **MAC Address** information are correct. Then click the **Next** button to check the Nebula Device firmware.



Devices

Enter one or more MAC address and serial number.

Or you can download the template here and import multiple records for faster registration.

What Zyxel devices support Nebula?

Where can I find these numbers?

MAC address	Serial number	Name	Model	License info	Expiration date	Assign licenses from invent

Registered device will be added to Organization Creator account in myZyxel.com.

□ Acknowledge

3.3 Activate and Assign a License for a Nebula Device, Site, or Organization

This section shows you how to activate and assign a license for a Nebula Device, site, or organization. See Section 1.1.4.2 on page 19 for a summary of NCC licenses.

The following table describes the license types at the time of writing.

Table 15 License Types

LOCATION	LICENSE TYPE	APPLICATION
MSP (Managed Services Provider)	MSP	NCC (Nebula Control Center) user account
Organization-wide	Professional / PLUS	AP (Access Point) / NSG (Nebula Security Gateway) / Switch / USG FLEX device
Organization-wide	Gold Security	ATP device / USG FLEX device
Site-wide	NSS (Nebula Security Service)	NSG device
Site-wide	UTM (Unified Threat Management) Security / Secure WiFi	USG FLEX device
Site-wide	Content Filter	USG FLEX 50 / USG20-VPN / USG20W-VPN device
Site-wide	Connect & Protect (CNP) / Connect & Protect Plus (CNP+)	NWA1123ACv3, WAC500, WAC500H / NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, WAX650S, USG LITE 60AX device
Site-wide	Elite	SCR 50AXE, USG LITE 60AX

3.3.1 Bundled License and Add-on License

A bundled license is a license that is included when you purchase a Nebula Device (Mobile Router, Access Point, Switch, NSG, USG FLEX, ATP, and USG20(W)-VPN). The bundled license is automatically assigned to the purchased Nebula Device when you add the Nebula Device to NCC. A bundled license cannot be transferred to another Nebula Device.

An add-on license is a license purchased separately from a Nebula Device as a license key, from Zyxel or another vendor. An add-on license can be applied to any Nebula Device.

3.3.2 License States

The following are the license states in NCC.

- **Active** – This displays when the license pack assigned to a Nebula Device, is activated, and is in use (expiration countdown/timer has started).
- **Queued** – This displays when the same license pack assigned to a Nebula Device, is activated, but not yet in use (expiration countdown/timer has not started).
- **Deferred** – This displays when you bought a Gold Security pack license and a new UTM Security pack license. The new UTM Security pack license services are deferred as the Gold Security pack license has priority, so the new UTM Security pack license services will not become active until the Gold Security pack license services first become active, then expire.

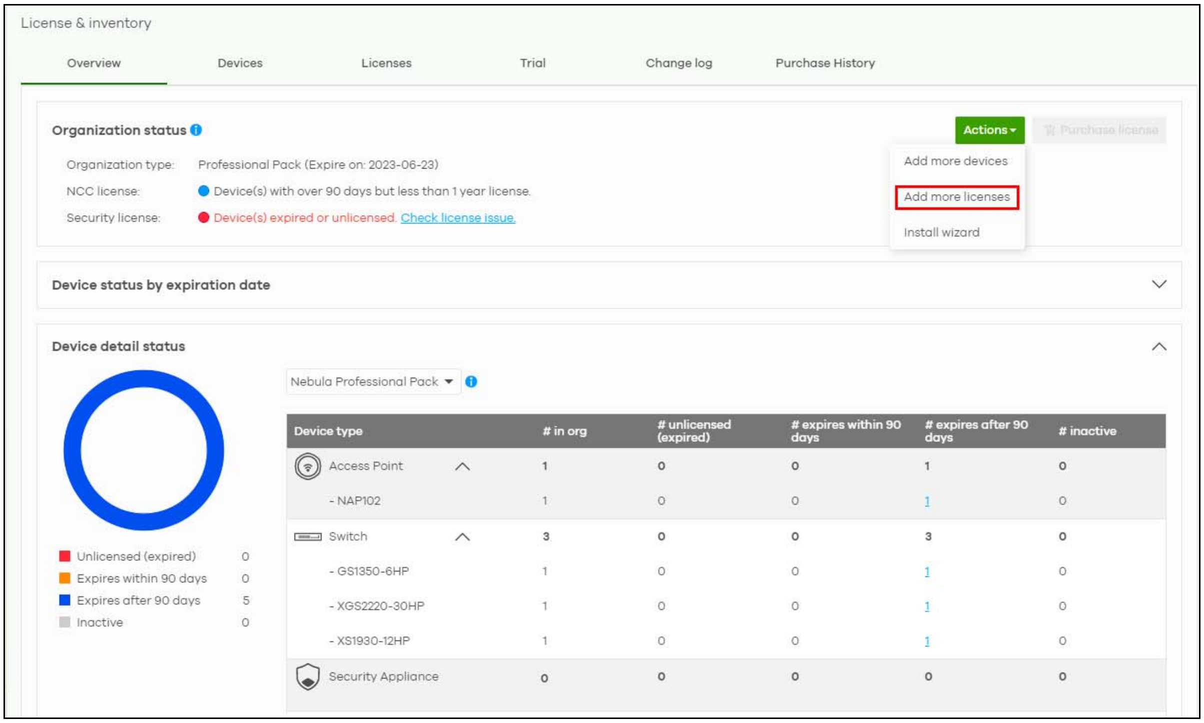
Note: A bundled license pack has priority over other license pack.
For example, a Gold Security pack license will become **Deferred** when assigned to a Nebula Device with an **Active** bundled UTM Security pack license.

- **Inactive** – This displays when the license pack assigned to a Nebula Device, is not activated in NCC.
- **Unused** – This displays when the license pack assigned to an organization, is not assigned to a Nebula Device and not activated in NCC.
- **Expired** – This displays when the license pack assigned to a Nebula Device is past its validity.

3.3.3 License Activation Process

You must have a Nebula Device and a license pack to activate a license. Perform the following to activate a license.

1 In the **Organization-wide** > **License & inventory**, click **Action** > **Add more licenses**.



License & inventory

Overview | Devices | Licenses | Trial | Change log | Purchase History

Organization status

Actions ▾ | Purchase license

- Add more devices
- Add more licenses
- Install wizard

Organization type:	Professional Pack (Expire on: 2023-06-23)
NCC license:	● Device(s) with over 90 days but less than 1 year license.
Security license:	● Device(s) expired or unlicensed. Check license issue.

Device status by expiration date

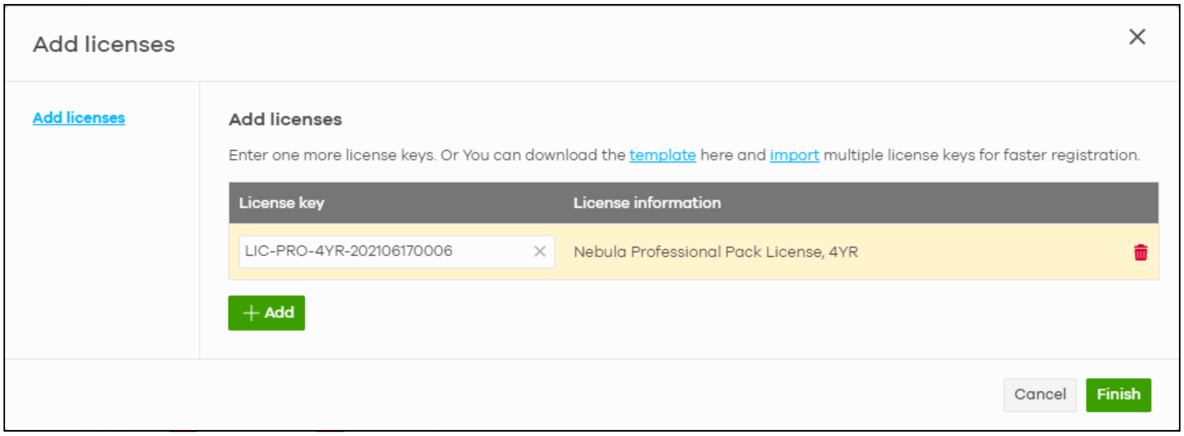
Device detail status

Nebula Professional Pack ▾

🟥 Unlicensed (expired)	0
🟧 Expires within 90 days	0
🟦 Expires after 90 days	5
⬜ Inactive	0

Device type	# in org	# unlicensed (expired)	# expires within 90 days	# expires after 90 days	# inactive
Access Point	1	0	0	1	0
- NAP102	1	0	0	1	0
Switch	3	0	0	3	0
- GS1350-6HP	1	0	0	1	0
- XGS2220-30HP	1	0	0	1	0
- XS1930-12HP	1	0	0	1	0
Security Appliance	0	0	0	0	0

2 Enter the **License key** and the **License information** will display.



Add licenses

Add licenses

Add licenses

Enter one more license keys. Or You can download the template here and import multiple license keys for faster registration.

License key	License information
LIC-PRO-4YR-202106170006	Nebula Professional Pack License, 4YR

+ Add

Cancel | Finish

3 Click **Finish**. The license is now assigned to your organization and site.

Note: A newly assigned license will not start its expiration countdown/timer until activated. Multiple add-on Plus Pack and Pro Pack licenses can be assigned to the same Nebula Device managed by NCC.

4 In the **Organization-wide** > **License & inventory**, select the **Devices** tab.

5 Locate the Nebula Device to assign a license(s). Click the **Actions** button and select **Assign license** on the device row.

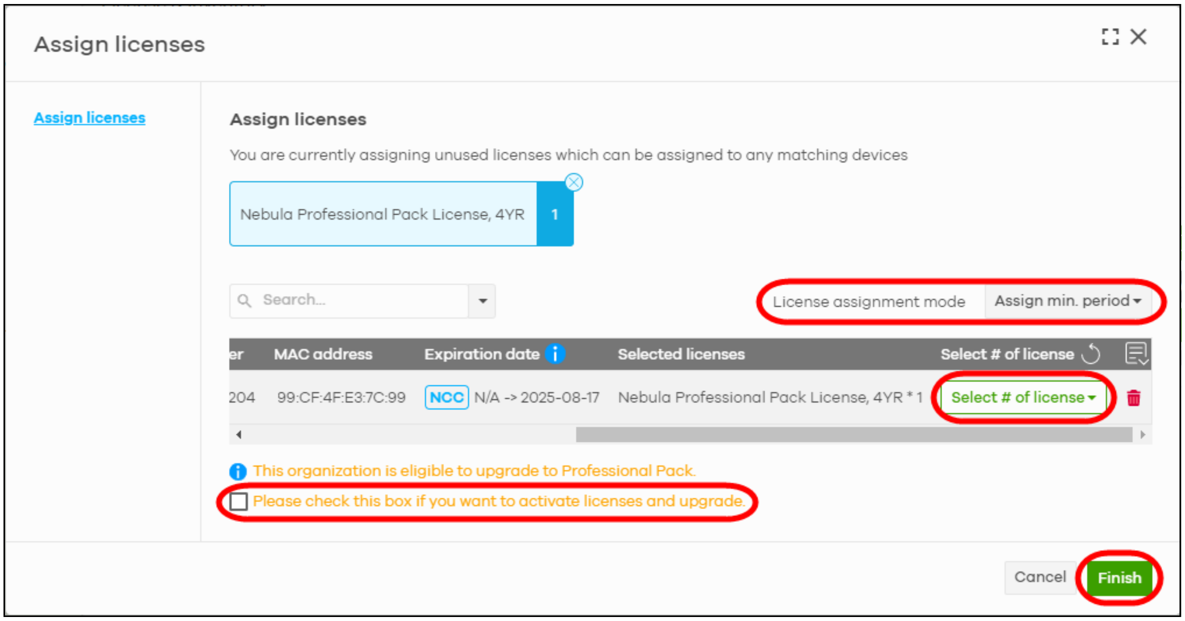
6 Clear any license that you do not want added to the Nebula Device.

7 For multiple licenses of the same type to be added to the Nebula Device, set the number of licenses in the **Select # of license** field.

8 Set the expected expiration date criteria from the **License assignment mode**.

- **Assign min. period** – NCC assigns one of each license type with the shortest duration to each Nebula Devices.
- **Assign all** – NCC assigns all selected license type equally to each Nebula Device.
- **Target expiration date** – Set a future date. NCC assigns an equal number of licenses to each Nebula Devices until the expiration date (future date) is reached or exceeded.

9 Click **Please check this box if you want to activate licenses and upgrade**. Then, click **Finish**.



Assign licenses

Assign licenses

You are currently assigning unused licenses which can be assigned to any matching devices

Nebula Professional Pack License, 4YR 1

License assignment mode: Assign min. period

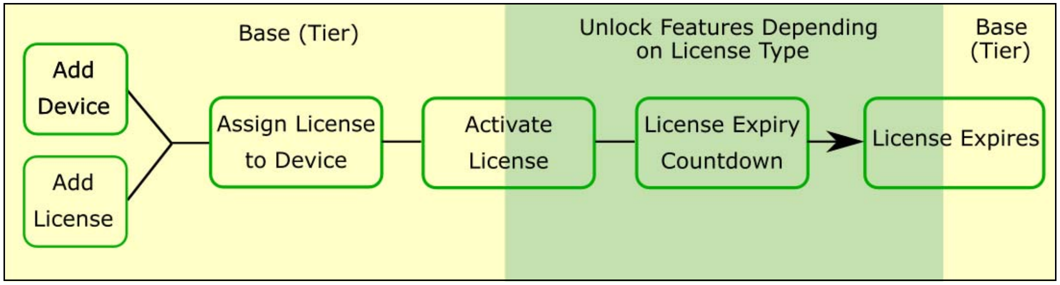
er	MAC address	Expiration date	Selected licenses	Select # of license
204	99:CF:4F:E3:7C:99	NCC N/A -> 2025-08-17	Nebula Professional Pack License, 4YR * 1	Select # of license

This organization is eligible to upgrade to Professional Pack.

□ Please check this box if you want to activate licenses and upgrade.

The features that will be unlocked depends on the license type purchased.

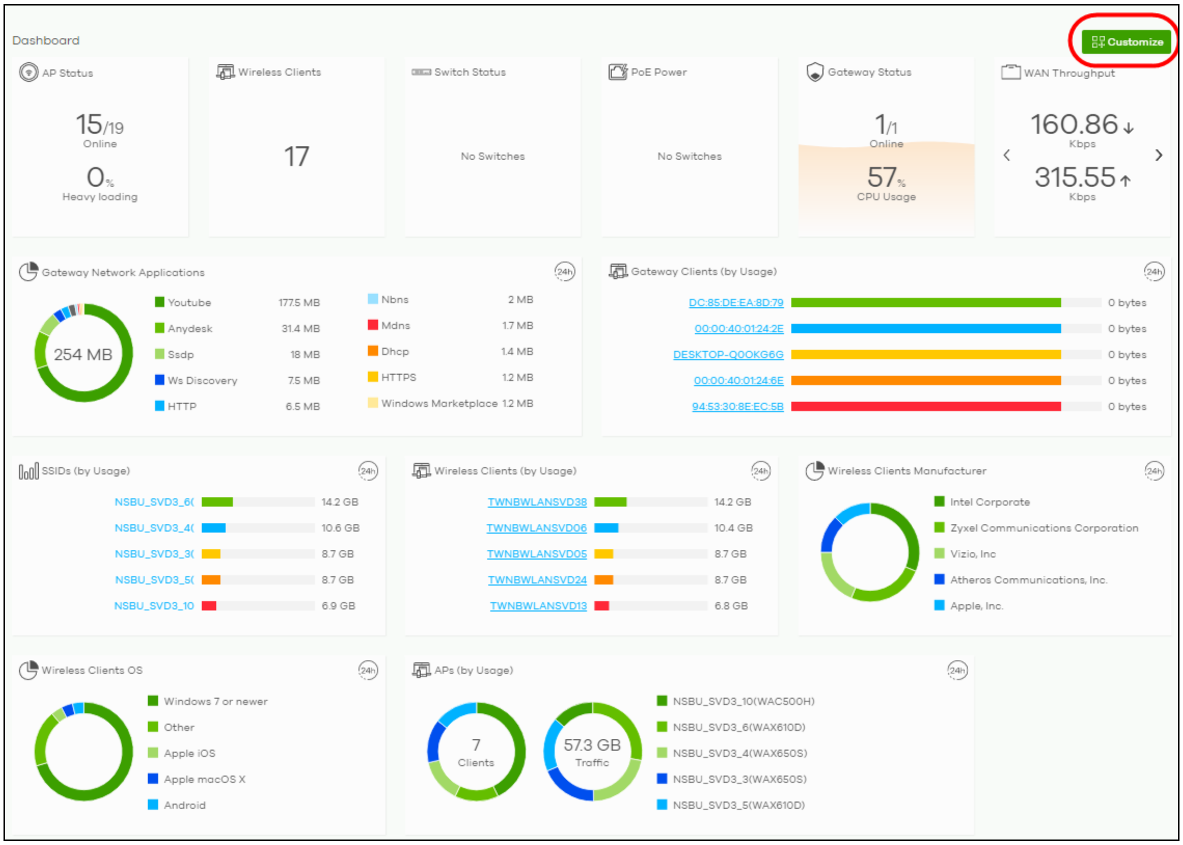
Figure 32 License Activation Process



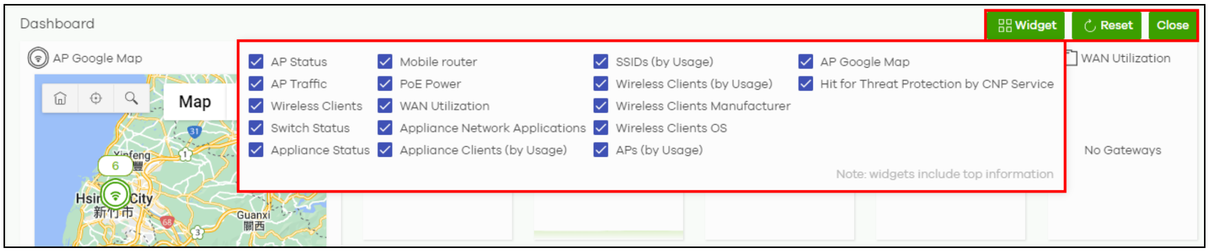
3.4 Monitor a Site

This section shows you how to view and monitor your Nebula Devices and WiFi/wired networks within a site.

1 Go to the **Site-wide** > **Dashboard** screen. To change the default view, click **Customize** to show the **Widget**, **Reset,** and **Close** buttons.



2 Click **Widget** to select which widgets to display. For example, clicking **SSIDs (by Usage)** will show the top 5 SSIDs with the highest percentage of bandwidth usage in the past 24 hours.
Click **Reset** to restore the dashboard back to the default view.
Click **Close** to hide the **Widget**. **Reset**, and **Close** buttons and show the **Customize** button.

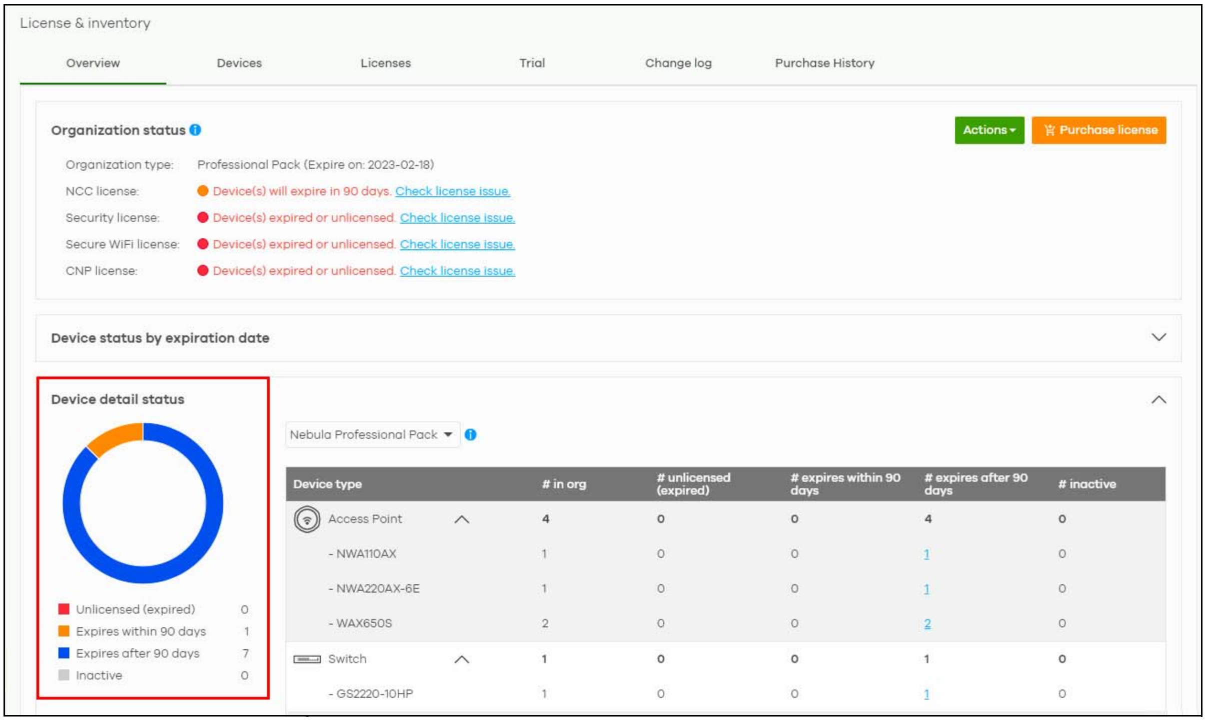


☑ AP Status
☑ AP Traffic
☑ Wireless Clients
☑ Switch Status
☑ Appliance Status
☑ Mobile router
☑ PoE Power
☑ WAN Utilization
☑ Appliance Network Applications
☑ Appliance Clients (by Usage)
☑ SSIDs (by Usage)
☑ Wireless Clients (by Usage)
☑ Wireless Clients Manufacturer
☑ Wireless Clients OS
☑ APs (by Usage)
☑ AP Google Map
☑ Hit for Threat Protection by CNP Service

Note: widgets include top information

3.5 Know What Licenses are Set to Expire in My Site or Organization

Use the **Overview** tab in the **Organization-wide** > **License & inventory** to keep track of what licenses are set to expire to prevent a cut in services.



Organization status

Organization type:	Professional Pack (Expire on: 2023-02-18)
NCC license:	● Device(s) will expire in 90 days. Check license issue.
Security license:	● Device(s) expired or unlicensed. Check license issue.
Secure WiFi license:	● Device(s) expired or unlicensed. Check license issue.
CNP license:	● Device(s) expired or unlicensed. Check license issue.

Device status by expiration date

Device detail status

🟥 Unlicensed (expired)	0
🟧 Expires within 90 days	1
🟦 Expires after 90 days	7
⬜ Inactive	0

Nebula Professional Pack

Device type	# in org	# unlicensed (expired)	# expires within 90 days	# expires after 90 days	# inactive
Access Point	4	0	0	4	0
- NWA110AX	1	0	0	1	0
- NWA220AX-6E	1	0	0	1	0
- WAX650S	2	0	0	2	0
Switch	1	0	0	1	0
- GS2220-10HP	1	0	0	1	0

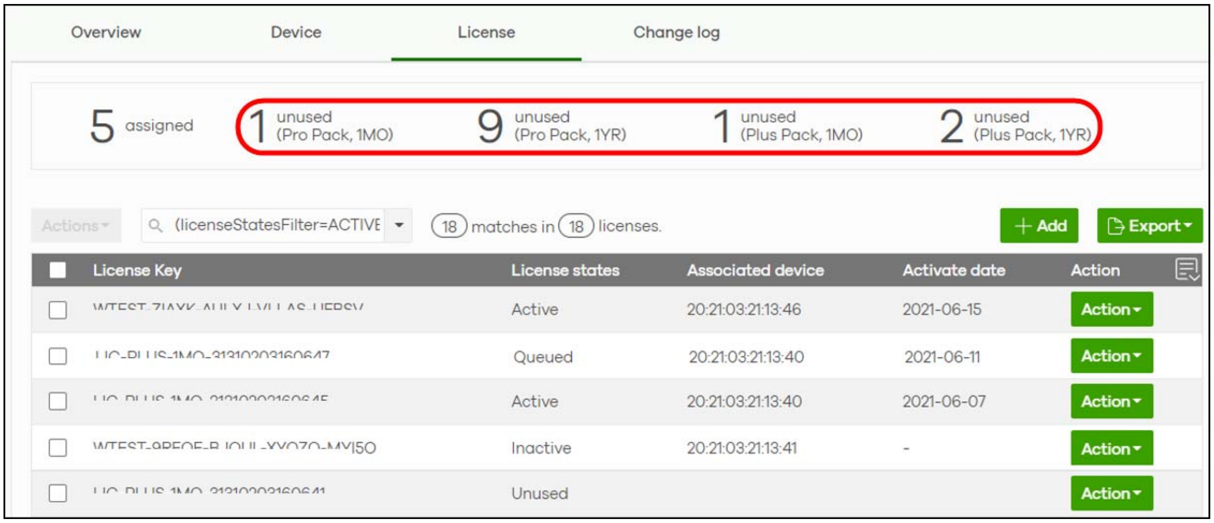
The license health is shown in the **Device detail status** and the following are the definition:

- Red – Nebula Device with expired license.
- Orange – Nebula Device with license that will expire in 90 days.
- Blue – Nebula Device with license that will expire in less than a year but over 90 days.
- Green – Nebula Device with license that will not expire within a year.

If a Pro or Plus tier license expires while assigned to a Nebula Device or you add an unlicensed Nebula Device to the organization, you have a 15-day grace period during which the organization's license remains active. See Section on page 24 for details on a Nebula Device entering the grace period and what actions you must take.

3.6 Renew an Expired License

An administrator account should have read and write (Full) access privilege to add or renew licenses for Nebula Devices in the organization. Go to **Organization-wide** > **License & inventory** to view the available (unused) licenses assigned to your organization.



5 assigned | 1 unused (Pro Pack, 1MO) | 9 unused (Pro Pack, 1YR) | 1 unused (Plus Pack, 1MO) | 2 unused (Plus Pack, 1YR)

18 matches in 18 licenses.

□	License Key	License states	Associated device	Activate date	Action
□	WTEST-ZIAYK-AUIJY-LVLLAS-UFPSV	Active	20:21:03:21:13:46	2021-06-15	Action
□	LIC-PLUS-1MO-31310203160647	Queued	20:21:03:21:13:40	2021-06-11	Action
□	LIC-PLUS-1MO-31310203160645	Active	20:21:03:21:13:40	2021-06-07	Action
□	WTEST-9PEOE-BJQUL-XYOZO-MYI5O	Inactive	20:21:03:21:13:41	-	Action
□	LIC-PLUS-1MO-31310203160641	Unused			Action

In the example figure above, four kinds of licenses are available for assigning to your Nebula Device: Pro Pack 1MO / 1YR and Plus Pack 1MO / 1YR. Click any one of the license. For example, if you click Plus Pack 1YR, then only the two Plus Pack **License Key**s with 1-year validity will display in the table.

Select the checkbox and click **Action**. Then click **Assign license**. See Section 3.3.3 on page 77 for details on assigning a license to a Nebula Device.

If the expired Nebula Device is still in the organization after the grace period elapses, the organization automatically downgrades to the Base tier. See Section on page 24 for details on a Nebula Device entering the grace period and what actions you must take.

3.7 Transfer Licenses

A license assigned to an organization and Nebula Device can be transferred to another Nebula Device in the same or different organization. The following guidelines apply when transferring licenses:

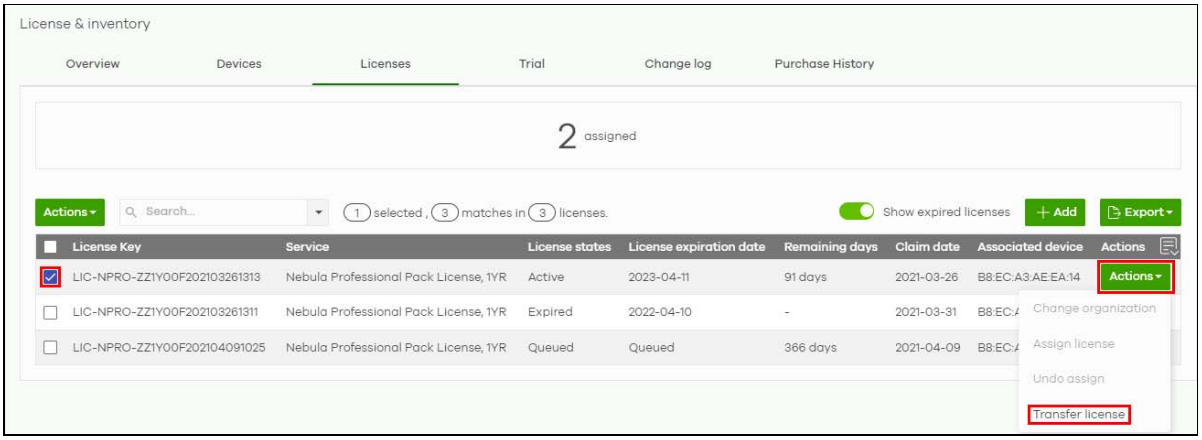
- The Nebula Devices must have the same owner.
- Bundled, Trial, and Promotion licenses cannot be transferred. (See Table 186 for more information.)
- If the license transfer causes the Nebula Devices in the organization to be without a valid license, the organization automatically downgrades to the Base tier.

3.7.1 Select Transferable Licenses

To select a transferable license(s), do the following:

1 Go to the **Organization-wide** > **License & inventory** > **Licenses** screen.

2 Select the license you want to transfer. Click **Actions**, and then click **Transfer license**.



License & inventory

Overview | Devices | Licenses | Trial | Change log | Purchase History

2 assigned

Actions ▾ | Search... | 1 selected , 3 matches in 3 licenses. | Show expired licenses | + Add | Export ▾

☐	License Key	Service	License states	License expiration date	Remaining days	Claim date	Associated device	Actions
☑	LIC-NPRO-ZZ1Y00F202103261313	Nebula Professional Pack License, 1YR	Active	2023-04-11	91 days	2021-03-26	B8:EC:A3:AE:EA:14	Actions ▾
☐	LIC-NPRO-ZZ1Y00F202103261311	Nebula Professional Pack License, 1YR	Expired	2022-04-10	-	2021-03-31	B8:EC:A	
☐	LIC-NPRO-ZZ1Y00F202104091025	Nebula Professional Pack License, 1YR	Queued	Queued	366 days	2021-04-09	B8:EC:A	

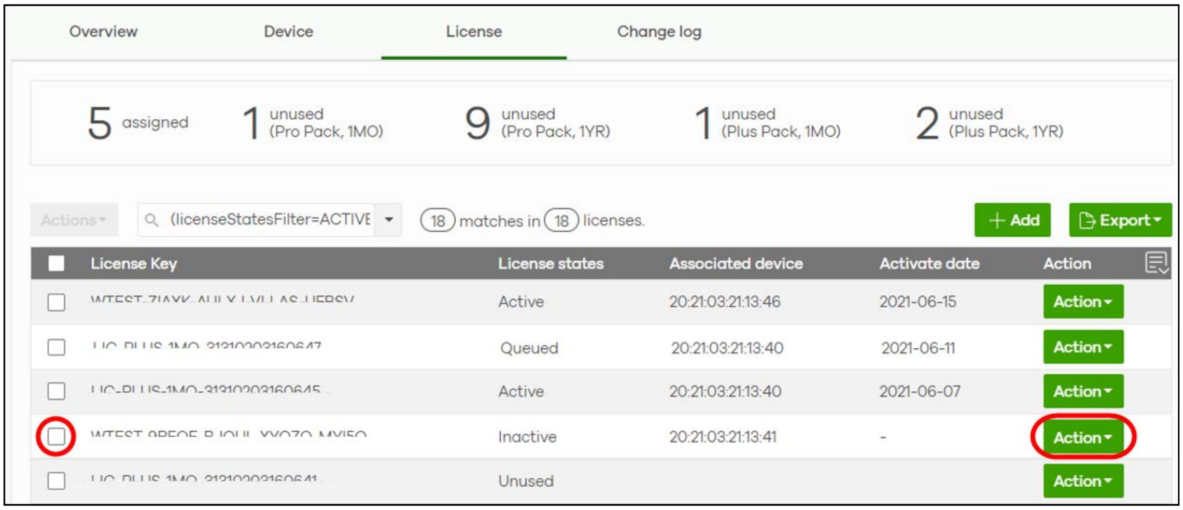
3.7.2 Undo Assigning a License

An administrator account should have read and write (Full) access privilege to un-assign licenses. Only an **Inactive** license (license is assigned to a specific Nebula Device but not activated) can be un-assigned.

To un-assign a license, do the following:

1 Go to the **Organization-wide** > **Configure** > **License & inventory** > **License** screen.

2 Select the **License Key** with an **Inactive** license state that you want to undo assign. Click **Action**, then click **Undo assign**. The license will return to the **Unused** license state.



Overview | Device | License | Change log

5 assigned | 1 unused (Pro Pack, 1MO) | 9 unused (Pro Pack, 1YR) | 1 unused (Plus Pack, 1MO) | 2 unused (Plus Pack, 1YR)

Actions ▾ | (licenseStatesFilter=ACTIVE | 18 matches in 18 licenses. | + Add | Export ▾

☐	License Key	License states	Associated device	Activate date	Action
☐	WTEST-ZIAYK-AULY-LVLLAS-UERSV	Active	20:21:03:21:13:46	2021-06-15	Action ▾
☐	LIC-PLUS-1MO-31310203160647	Queued	20:21:03:21:13:40	2021-06-11	Action ▾
☐	LIC-PLUS-1MO-31310203160645	Active	20:21:03:21:13:40	2021-06-07	Action ▾
☐	WTEST-9REOE-RJOUL-XYOZO-MYIEO	Inactive	20:21:03:21:13:41	-	Action ▾
☐	LIC-PLUS-1MO-31310203160641	Unused			Action ▾

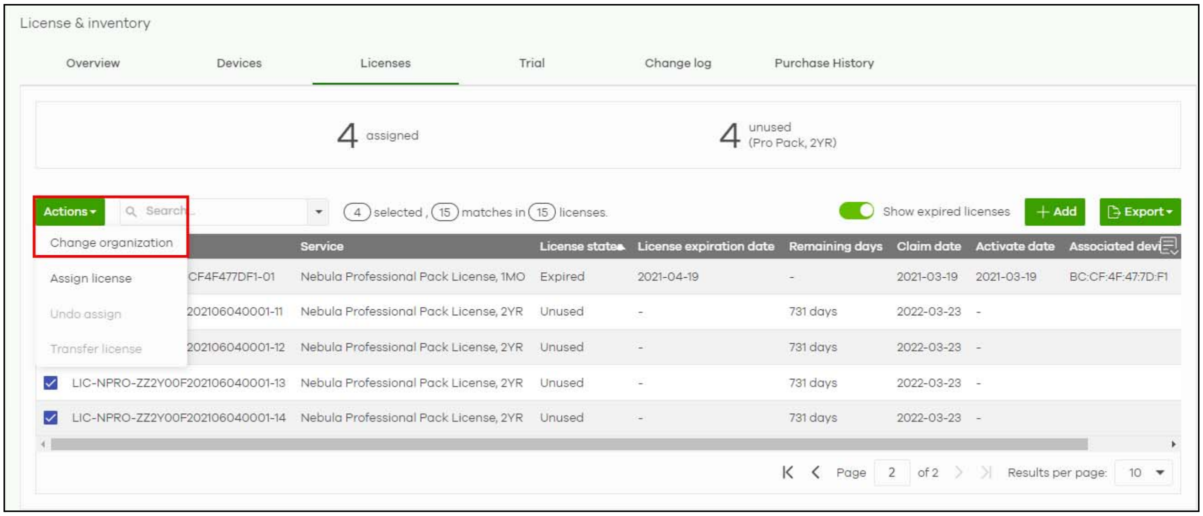
3.7.3 Transfer a License to a Different Organization

Only an **Unused** license (a license which is assigned to an organization but not assigned to a specific Nebula Device) can be transferred. Both source and destination organizations should belong to the same owner.

To transfer a license to another organization, do the following:

1 Perform the steps described in Select Transferable Licenses.

2 With the licenses you want to transfer selected, click **Actions** and then click **Change organization**.



License & inventory

4 assigned

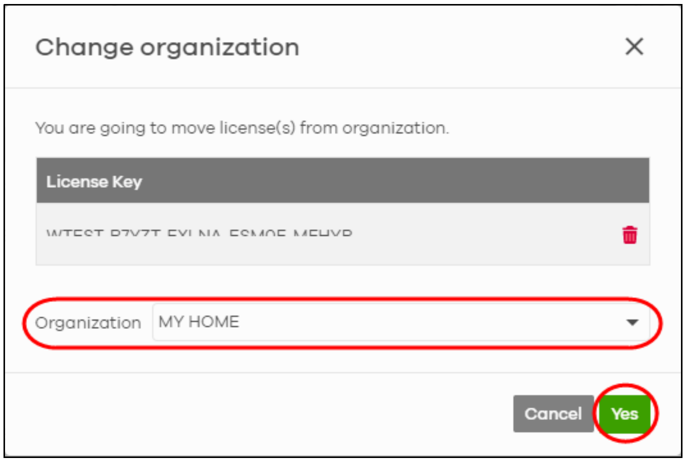
4 unused (Pro Pack, 2YR)

4 selected , 15 matches in 15 licenses.

	Service	License state	License expiration date	Remaining days	Claim date	Activate date	Associated devi
CF4F477DF1-01	Nebula Professional Pack License, 1MO	Expired	2021-04-19	-	2021-03-19	2021-03-19	BC:CF:4F:47:7D:F1
202106040001-11	Nebula Professional Pack License, 2YR	Unused	-	731 days	2022-03-23	-	
202106040001-12	Nebula Professional Pack License, 2YR	Unused	-	731 days	2022-03-23	-	
☑ LIC-NPRO-ZZ2Y00F202106040001-13	Nebula Professional Pack License, 2YR	Unused	-	731 days	2022-03-23	-	
☑ LIC-NPRO-ZZ2Y00F202106040001-14	Nebula Professional Pack License, 2YR	Unused	-	731 days	2022-03-23	-	

Page 2 of 2 Results per page: 10

3 Select the **Organization** you want to transfer the licenses to. The current organization will be excluded from the list. Then click **Yes**.



Change organization

You are going to move license(s) from organization.

License Key
WTEST-P7VZT-FXLNA-ESMQE-MEHXP

Organization: MY HOME

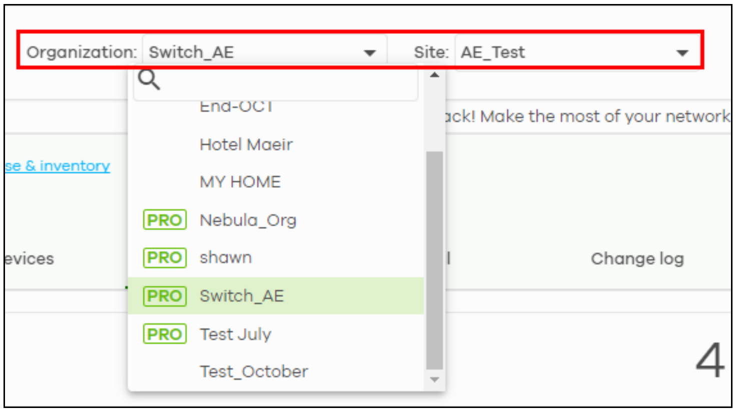
You have successfully transferred a license to another organization, but without assigning it to a Nebula Device yet.

3.7.4 Assign a License to a Nebula Device in the New Organization

To assign a license(s) to a Nebula Device in the new organization, do the following:

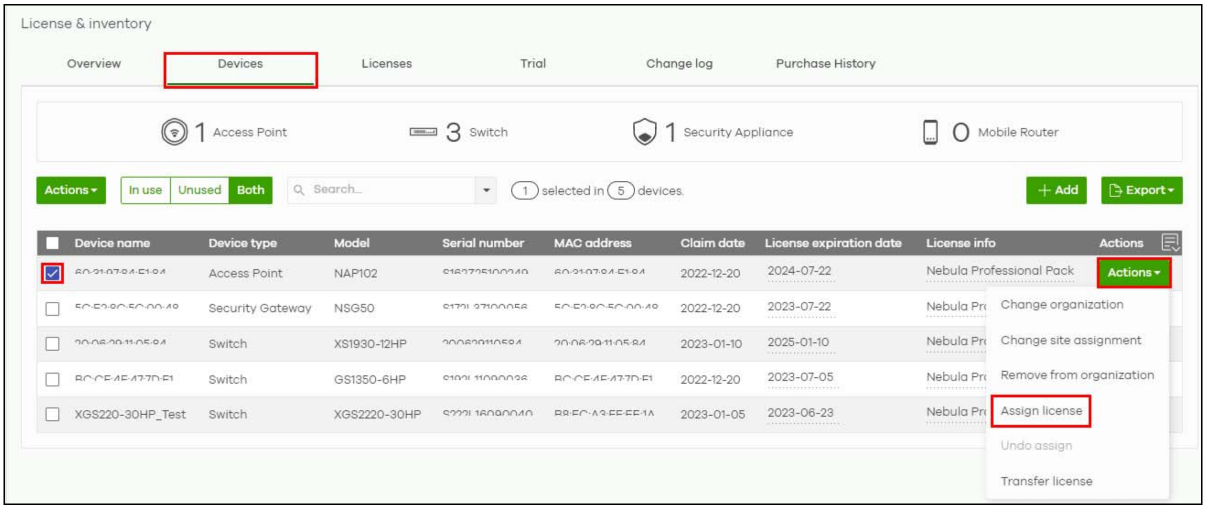
1 Perform the steps mentioned in Transfer a License to a Different Organization.

2 Select the **Organization** and **Site** where the license is transferred.



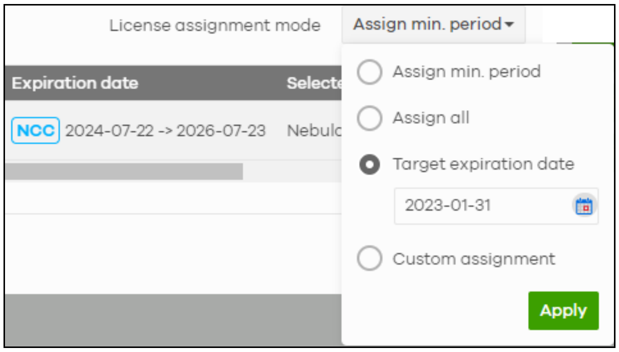
3 Go to the **Organization-wide** > **Configure** > **License & inventory** > **Device** screen.

4 Select the **Devices**, click **Actions**, then click **Assign license**.



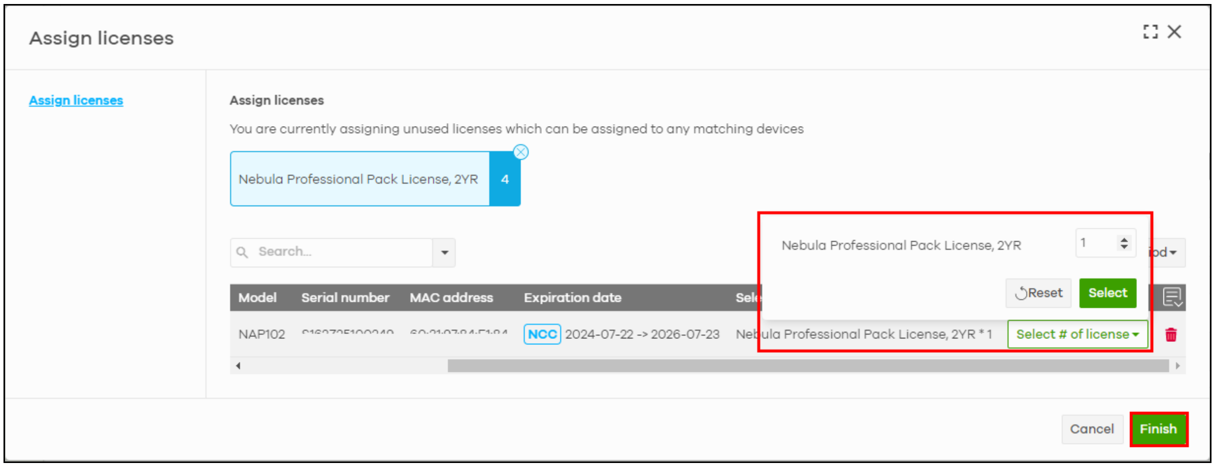
	Device name	Device type	Model	Serial number	MAC address	Claim date	License expiration date	License info	Actions
☑	60:31:97:84:E1:84	Access Point	NAP102	S162725100249	60:31:97:84:E1:84	2022-12-20	2024-07-22	Nebula Professional Pack	Actions
□	5C:E2:8C:5C:00:48	Security Gateway	NSG50	S172L37100056	5C:E2:8C:5C:00:48	2022-12-20	2023-07-22	Nebula Pro	
□	20:06:29:11:05:84	Switch	XS1930-12HP	200629110584	20:06:29:11:05:84	2023-01-10	2025-01-10	Nebula Pro	
□	BC:CF:4F:47:7D:F1	Switch	GS1350-6HP	S192L11090036	BC:CF:4F:47:7D:F1	2022-12-20	2023-07-05	Nebula Pro	
□	XGS220-30HP_Test	Switch	XGS2220-30HP	S222L16090040	B8:EC:A3:EF:EE:1A	2023-01-05	2023-06-23	Nebula Pro	

5 Select the **License assignment mode** to have NCC filter licenses that can be assigned.



- **Assign min. period** – one month license packs for your Nebula Device will be picked and displayed.
- **Assign all** – all licenses that can be assigned are displayed.
- **Target expiration date** – all licenses that meet the expiry criteria you set and can be assigned are displayed.
- **Custom assignment** – any change in value to **Assign min period** and **Assign all** licenses above will become a **Custom assignment** and are displayed.

6 Click **Select # of license**. In the pop-up window, confirm or edit the value appearing beside the license type based on the criteria set in **License assignment mode**. Click **Select** to confirm. Then click **Finish**.



Assign licenses

Assign licenses

Assign licenses

You are currently assigning unused licenses which can be assigned to any matching devices

Nebula Professional Pack License, 2YR 4

Nebula Professional Pack License, 2YR 1

Model	Serial number	MAC address	Expiration date	Sel
NAP102	[illegible]	[illegible]	NCC 2024-07-22 -> 2026-07-23	Nebula Professional Pack License, 2YR * 1

3.7.5 Transfer a License to a Nebula Device in a New Organization

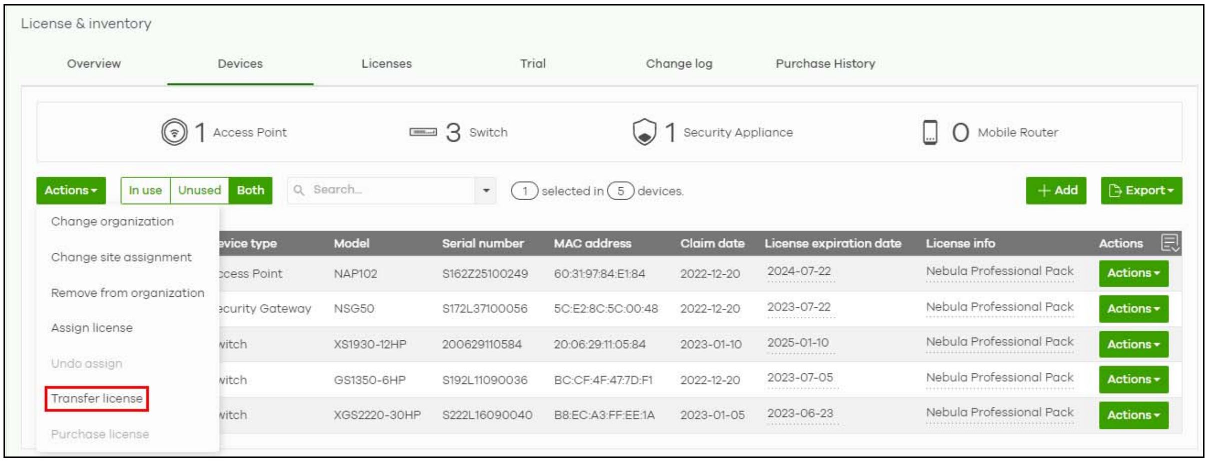
To transfer a license(s) to a Nebula Device in the new organization, do the following:

1 Perform the steps mentioned in Assign a License to a Nebula Device in the New Organization.

2 Click **Organization-wide** > **License & inventory** > **Device** tab.

3 Select the devices with the license to be transferred.

4 Click **Actions** and select **Transfer License**.



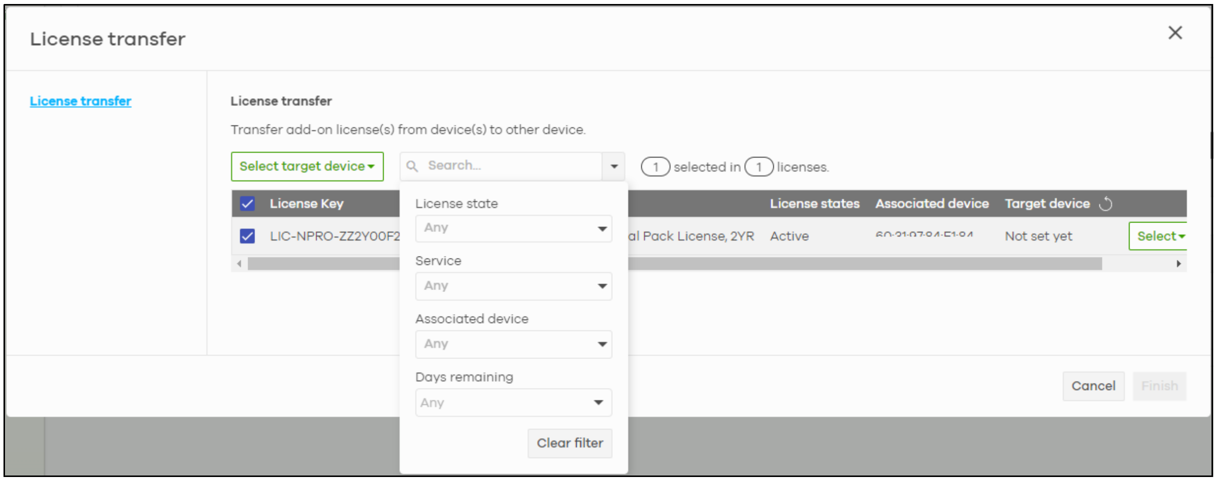
License & inventory

1 Access Point 3 Switch 1 Security Appliance 0 Mobile Router

1 selected in 5 devices.

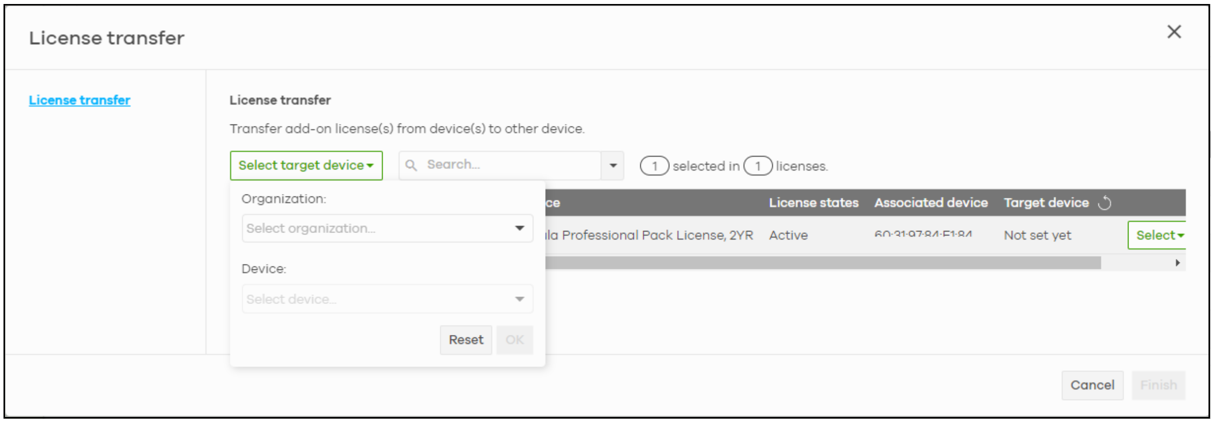
evice type	Model	Serial number	MAC address	Claim date	License expiration date	License info	Actions
ccess Point	NAP102	S162Z25100249	60:31:97:84:E1:84	2022-12-20	2024-07-22	Nebula Professional Pack	Actions
ecurity Gateway	NSG50	S172L37100056	5C:E2:8C:5C:00:48	2022-12-20	2023-07-22	Nebula Professional Pack	Actions
witch	XS1930-12HP	200629110584	20:06:29:11:05:84	2023-01-10	2025-01-10	Nebula Professional Pack	Actions
witch	GS1350-6HP	S192L11090036	BC:CF:4F:47:7D:F1	2022-12-20	2023-07-05	Nebula Professional Pack	Actions
witch	XGS2220-30HP	S222L16090040	B8:EC:A3:FF:EE:1A	2023-01-05	2023-06-23	Nebula Professional Pack	Actions

5 The **License transfer** window appears. Click **Search** to set the filter to select the licenses.



☑ License Key		License states	Associated device	Target device	
☑ LIC-NPRO-ZZ2Y00F2	al Pack License, 2YR	Active	60:31:97:84:E1:84	Not set yet	Select

6 Click **Select target device** to transfer all licenses to one Nebula Device by selecting the same/different **Organization** and target **Device**. Then click **OK**. Or select the devices individually.



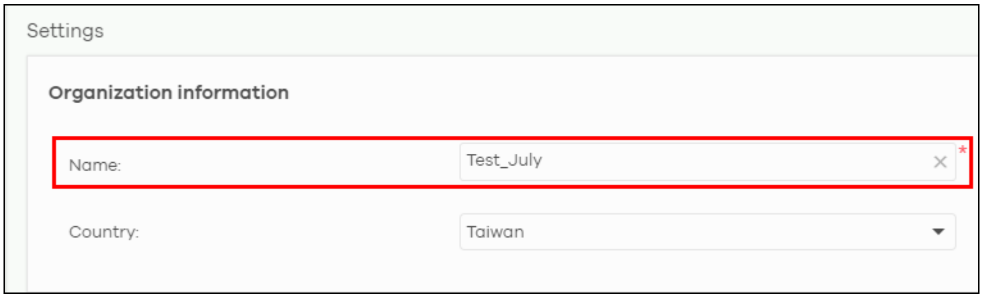
ce	License states	Associated device	Target device	
ıla Professional Pack License, 2YR	Active	60:31:97:84:E1:84	Not set yet	Select

3.8 Change an Organization and/or Site Name

To change your organization name or site name, do the following:

Organization Name

1 Go to **Organization-wide** > **Organization-wide manage** > **Organization settings**.



Name: Test_July

Country: Taiwan

2 Enter a new descriptive name, 1 – 64 characters including 0–9 a–z A–Z `~!@#$%&*(_+-={} | [];'"./<> ?) in **Name**.

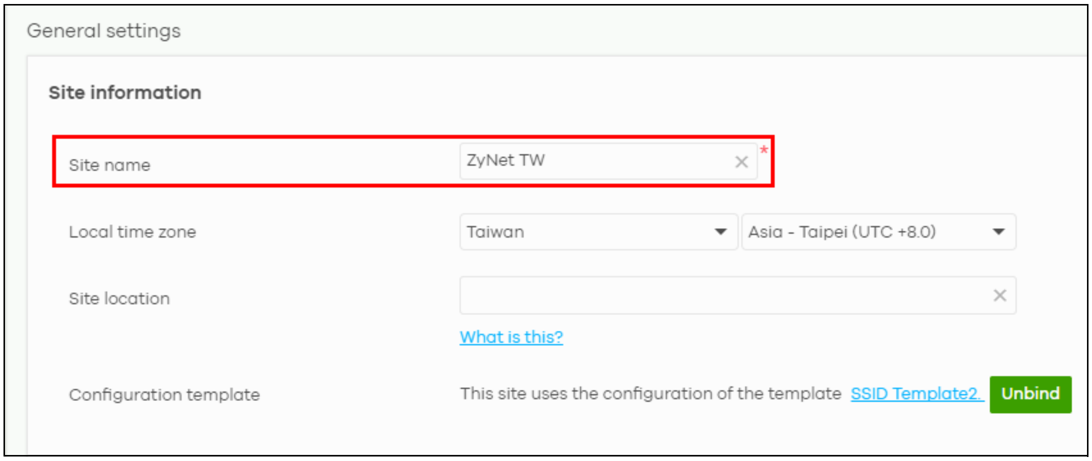
Note: NCC does not allow duplicate organization name.

Note: Changing the organization name will not affect the Nebula Devices configuration in NCC.

3 Then, click **Save** at the bottom of the screen.

Site Name

1 Go to **Site-wide** > **Configure** > **Site settings**.



General settings

Site information

Site name: ZyNet TW

Local time zone: Taiwan | Asia - Taipei (UTC +8.0)

Site location:

Configuration template: This site uses the configuration of the template SSID Template2.

2 Enter a descriptive name, 1 – 64 characters including 0–9 a–z A–Z `~!@#$%&*(_+-={} | [];'"./<> ?) in **Site name**.

Note: NCC does not allow duplicate site name.

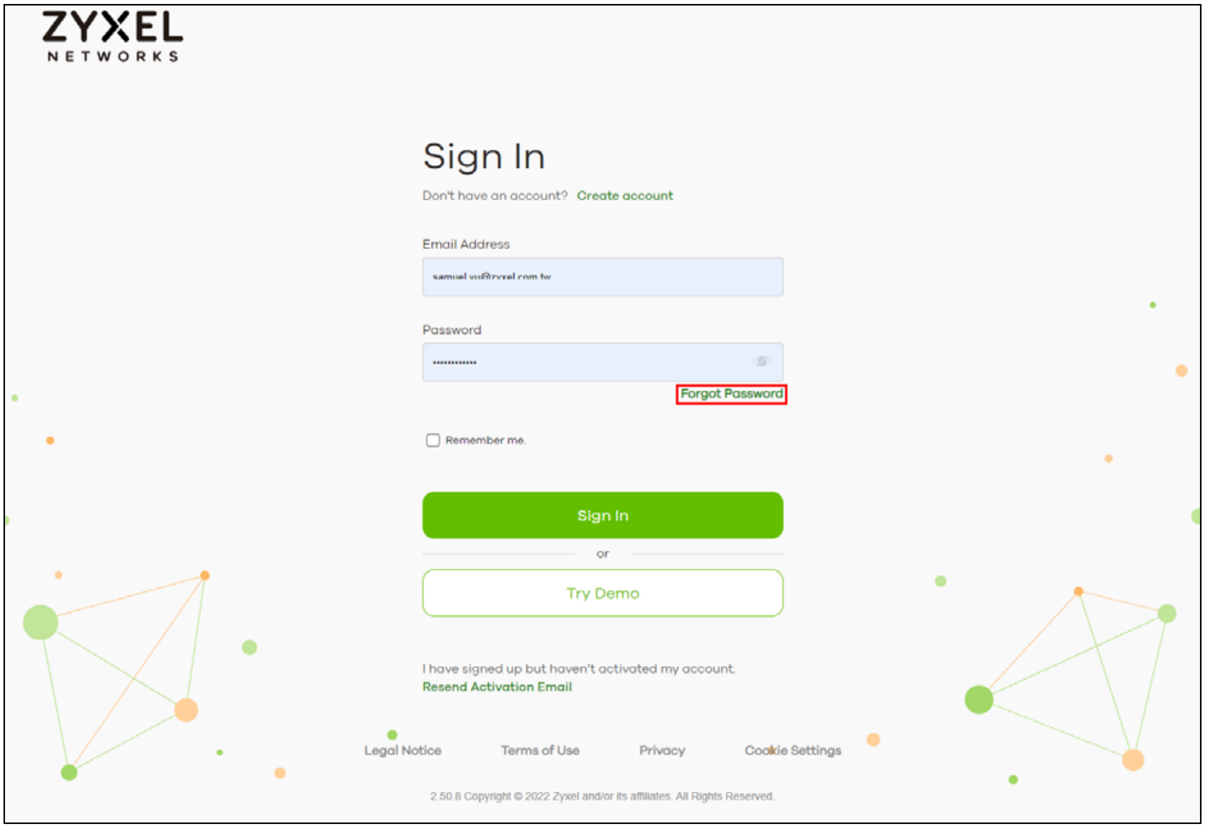
Note: Changing the site name will not affect the Nebula Devices configuration in NCC.

3 Then, click **Save** at the bottom of the screen.

3.9 Reset the Nebula Password

If you forget your Nebula portal login password and need to reset it, do the following:

1 In the Nebula portal **Sign In** page, click **Forgot Password**.



Sign In

Don't have an account? Create account

Email Address

samuel.yu@zyxel.com.tw

Password

••••••••••••

Forgot Password

□ Remember me.

Sign In

or

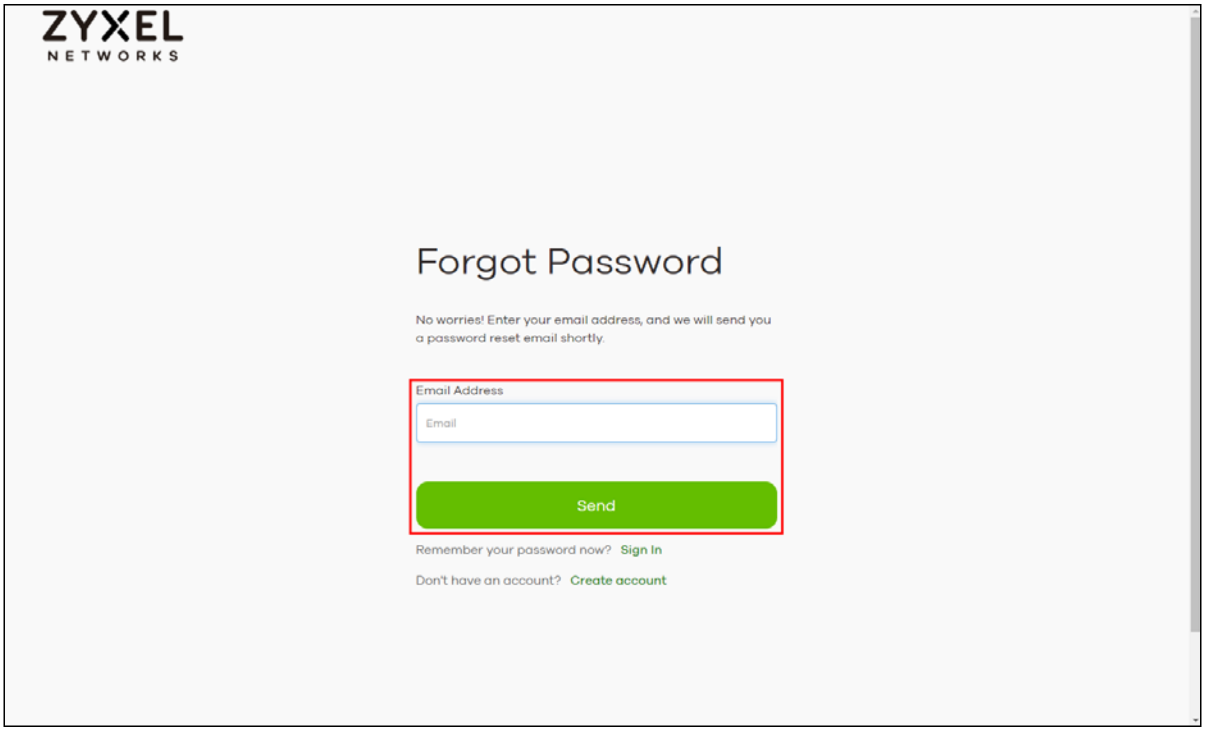
Try Demo

I have signed up but haven't activated my account.
Resend Activation Email

Legal Notice Terms of Use Privacy Cookie Settings

2.50.8 Copyright © 2022 Zyxel and/or its affiliates. All Rights Reserved.

2 Enter your Zyxel Account's email address, and then click **Send**.



Forgot Password

No worries! Enter your email address, and we will send you a password reset email shortly.

Email Address

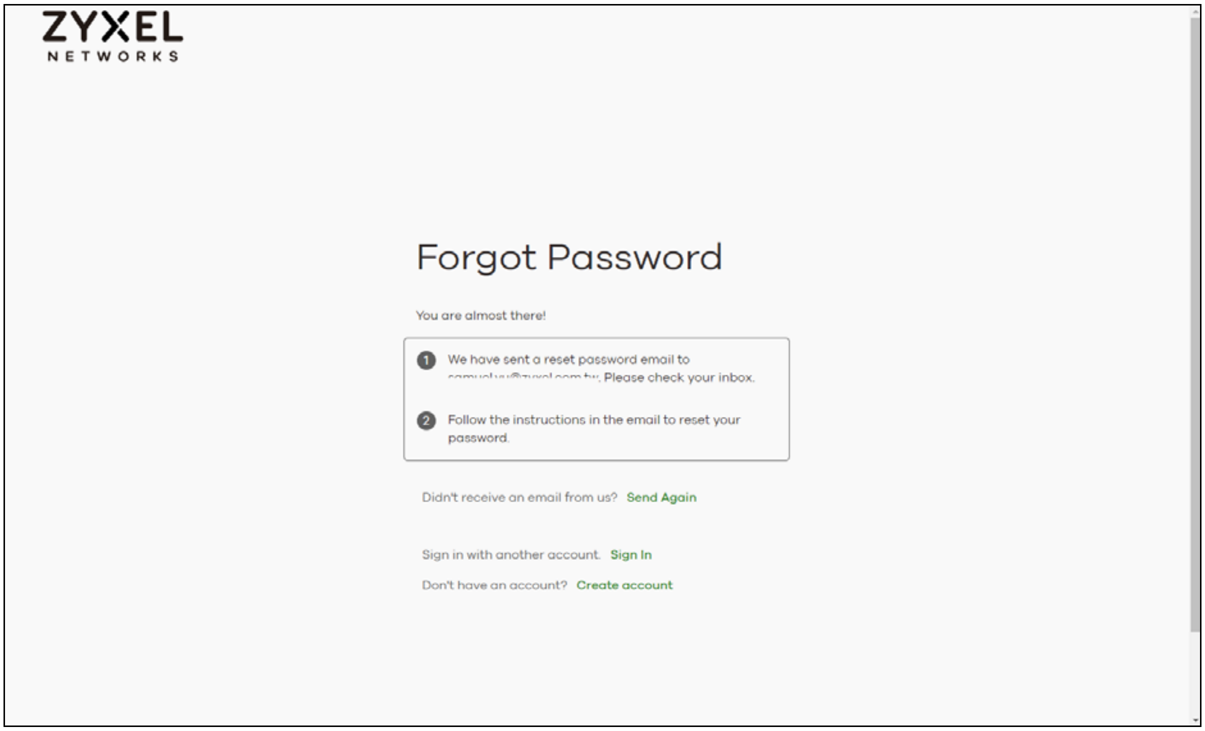
Email

Send

Remember your password now? Sign In

Don't have an account? Create account

A reset password email has been sent notification appears.



Forgot Password

You are almost there!

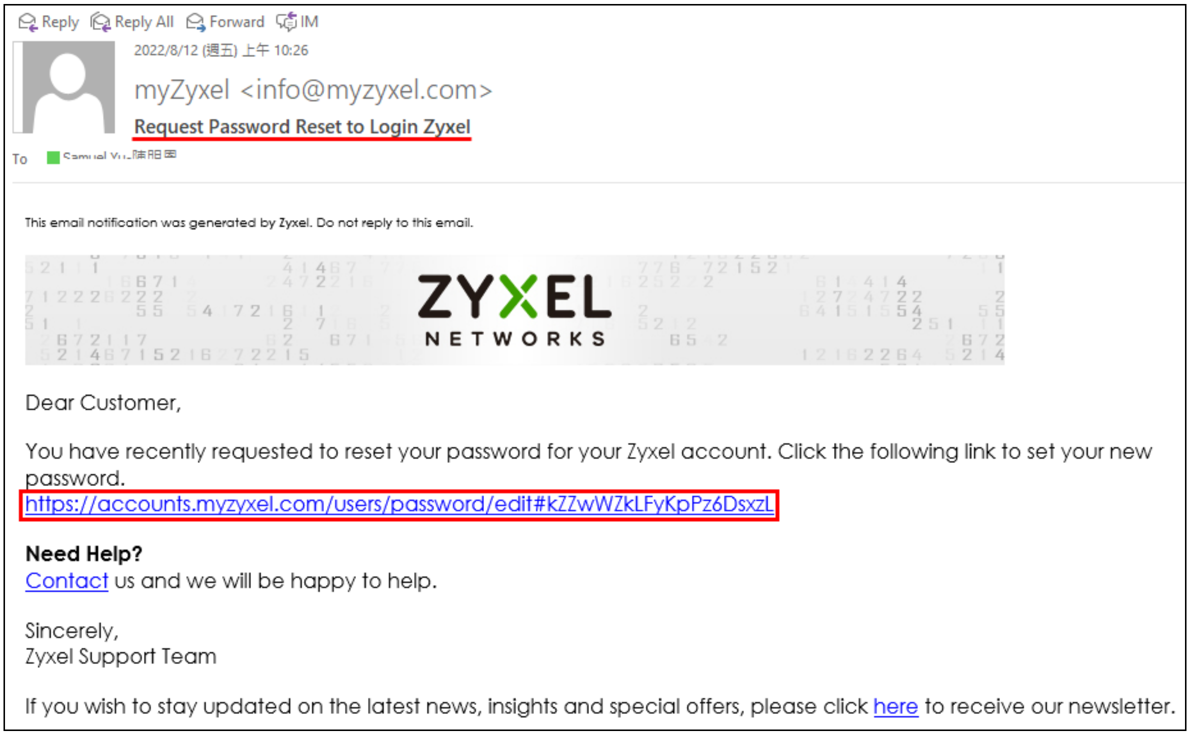
1. We have sent a reset password email to samuel.yu@zyxel.com.tw. Please check your inbox.
2. Follow the instructions in the email to reset your password.

Didn't receive an email from us? Send Again

Sign in with another account. Sign In

Don't have an account? Create account

3 Click the link in the **Request Password Reset to Login Zyxel** email.



2022/8/12 (週五) 上午 10:26

myZyxel <info@myzyxel.com>

Request Password Reset to Login Zyxel

To Samuel Yu-[illegible]

This email notification was generated by Zyxel. Do not reply to this email.

Dear Customer,

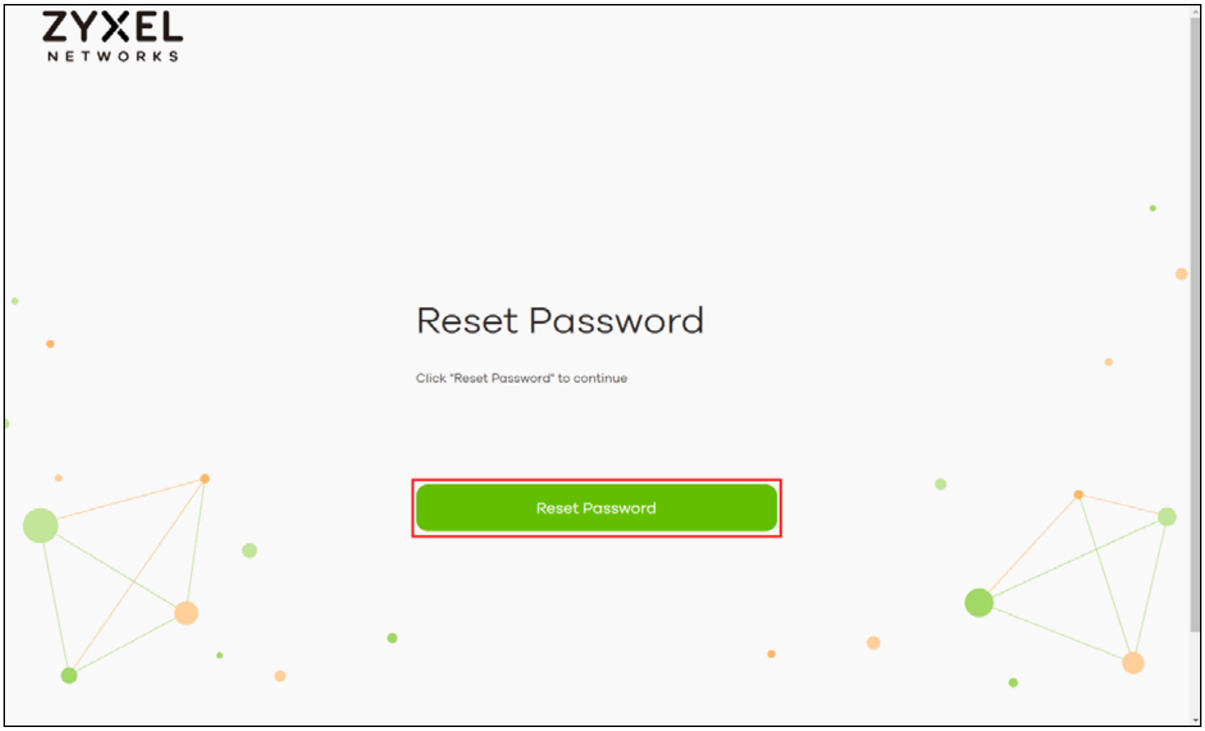
You have recently requested to reset your password for your Zyxel account. Click the following link to set your new password.
https://accounts.myzyxel.com/users/password/edit#kZZwWZkLFyKpPz6DsxzL

Need Help?
Contact us and we will be happy to help.

Sincerely,
Zyxel Support Team

If you wish to stay updated on the latest news, insights and special offers, please click here to receive our newsletter.

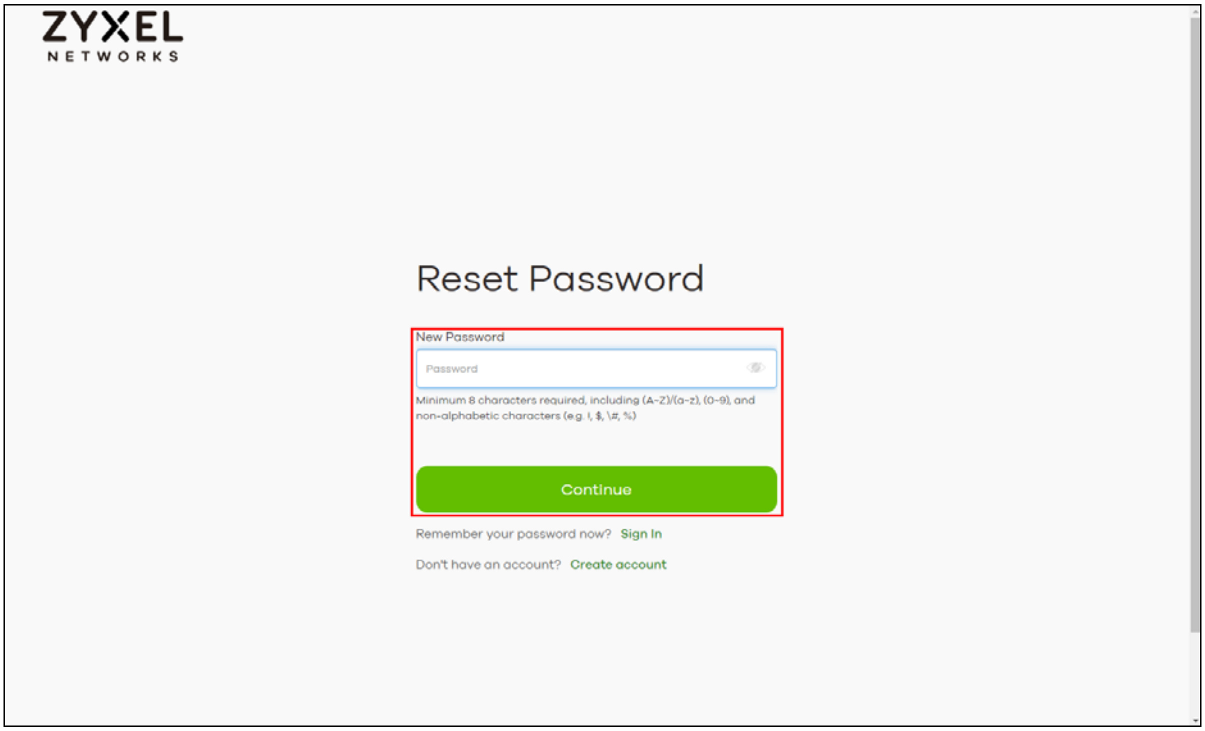
4 The following screen appears. Click **Reset Password**.



Reset Password

Click "Reset Password" to continue

5 Enter the **New Password**. Use a minimum of 8 characters, including 0–9 a–z A–Z `~!@#$%&*(_+-={} | [];'"./ <> ?). Then click **Continue**.



Reset Password

New Password

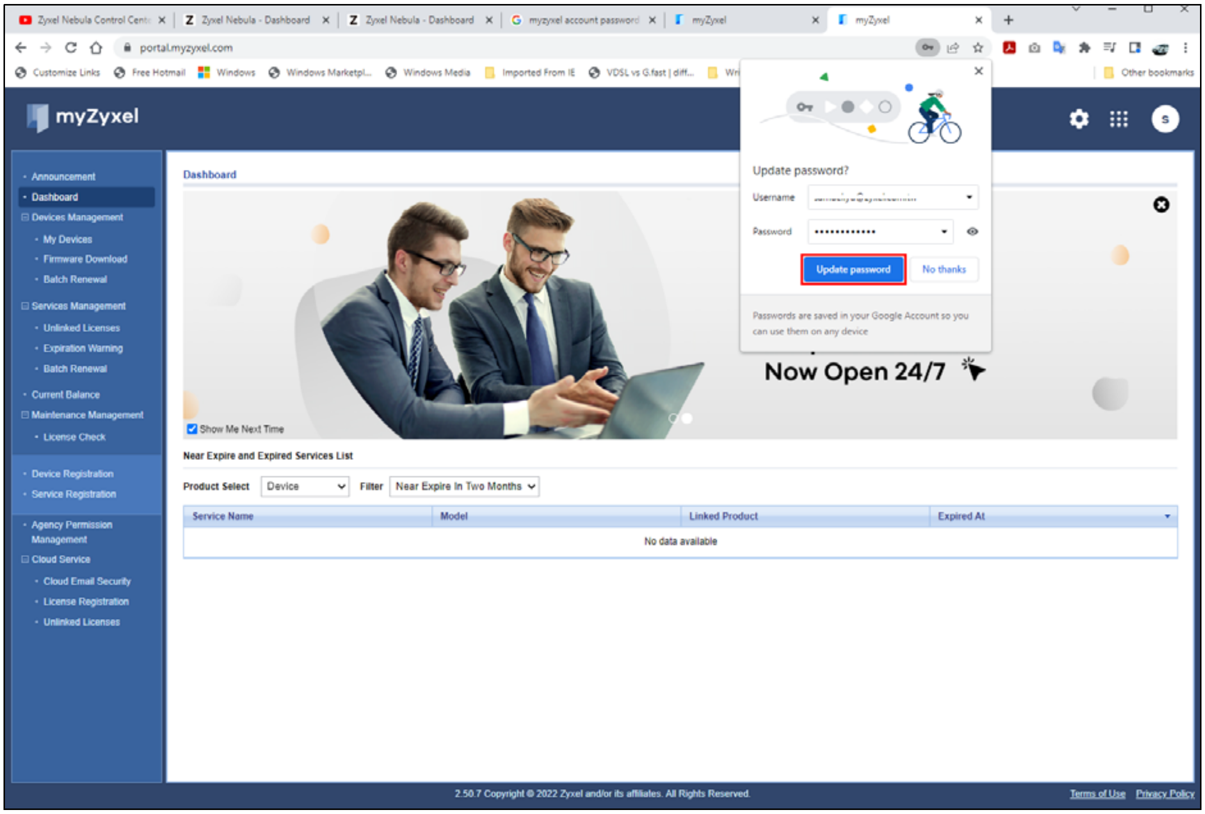
Password

Minimum 8 characters required, including (A-Z)/(a-z), (0-9), and non-alphabetic characters (e.g. !, $, \#, %)

Remember your password now? Sign In

Don't have an account? Create account

6 You will be transferred to the myZyxel portal. Click **Update password**.



Update password?

Username

Password ••••••••••••

Passwords are saved in your Google Account so you can use them on any device

☑ Show Me Next Time

Near Expire and Expired Services List

Product Select: Device Filter: Near Expire In Two Months

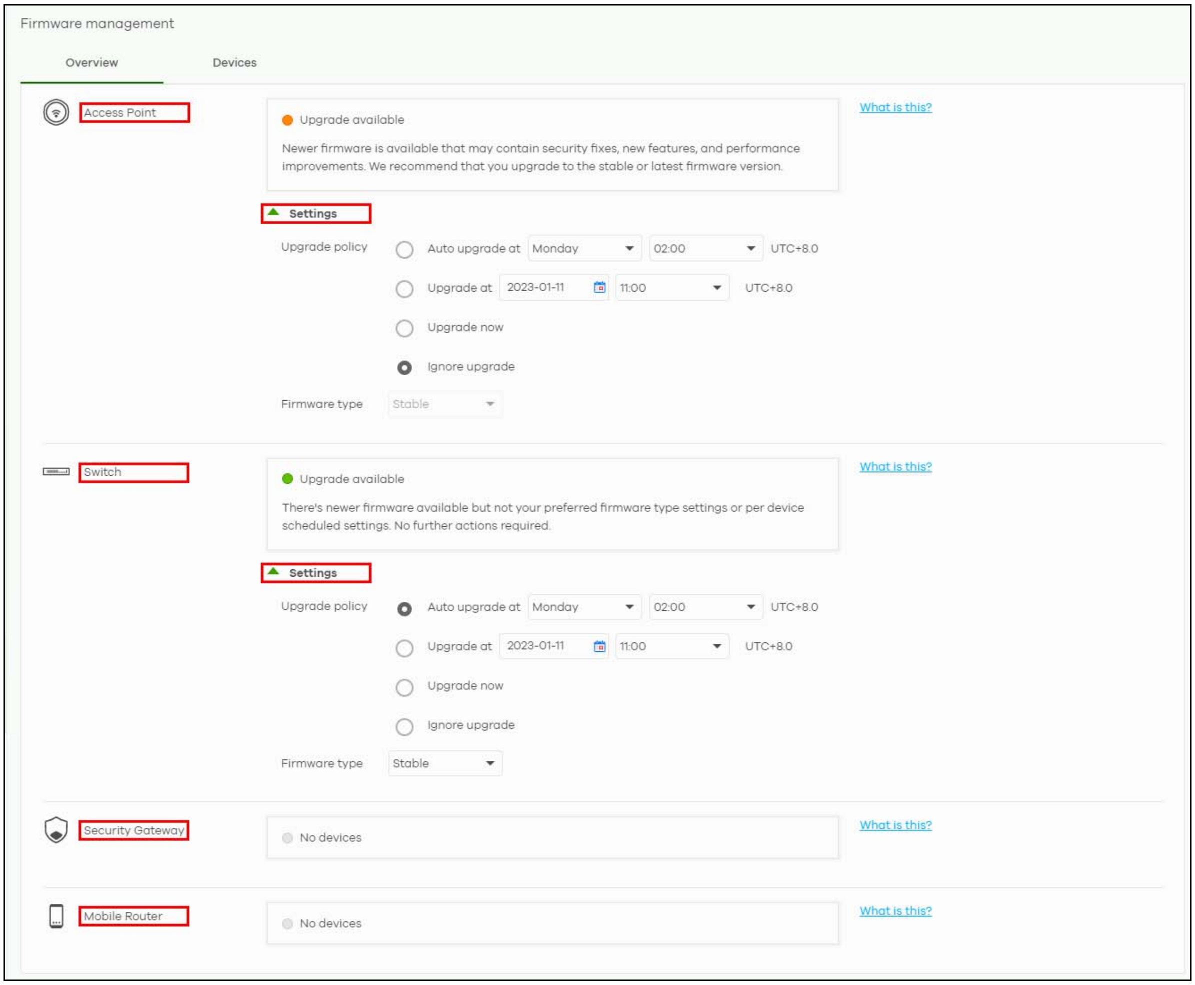
Service Name	Model	Linked Product	Expired At
No data available			

2.50.7 Copyright © 2022 Zyxel and/or its affiliates. All Rights Reserved.

3.10 Maintain Firmware

This section shows you how to update and maintain a Nebula Device's firmware.

1 Go to the **Site-wide** > **Configure** > **Firmware management** > **Overview** screen. Under **Settings**, you can set different times to upgrade firmware for your Access Points, Switches, Security Routers, Firewalls, Security Gateways, and Mobile Routers in your site. Select the day and time of the week when NCC will detect if any new firmware is available. NCC will send out a reminder email to the administrator for the available updates. If the administrator does NOT perform the update, after the set period of time is over, NCC will automatically upgrade the firmware for the Nebula Devices in the site. Or select **Upgrade now** to upgrade immediately.



Firmware management

Overview | Devices

Access Point

● Upgrade available

Newer firmware is available that may contain security fixes, new features, and performance improvements. We recommend that you upgrade to the stable or latest firmware version.

What is this?

Settings

Upgrade policy
- ○ Auto upgrade at Monday 02:00 UTC+8.0
- ○ Upgrade at 2023-01-11 11:00 UTC+8.0
- ○ Upgrade now
- ● Ignore upgrade

Firmware type: Stable

Switch

● Upgrade available

There's newer firmware available but not your preferred firmware type settings or per device scheduled settings. No further actions required.

What is this?

Settings

Upgrade policy
- ● Auto upgrade at Monday 02:00 UTC+8.0
- ○ Upgrade at 2023-01-11 11:00 UTC+8.0
- ○ Upgrade now
- ○ Ignore upgrade

Firmware type: Stable

Security Gateway

No devices

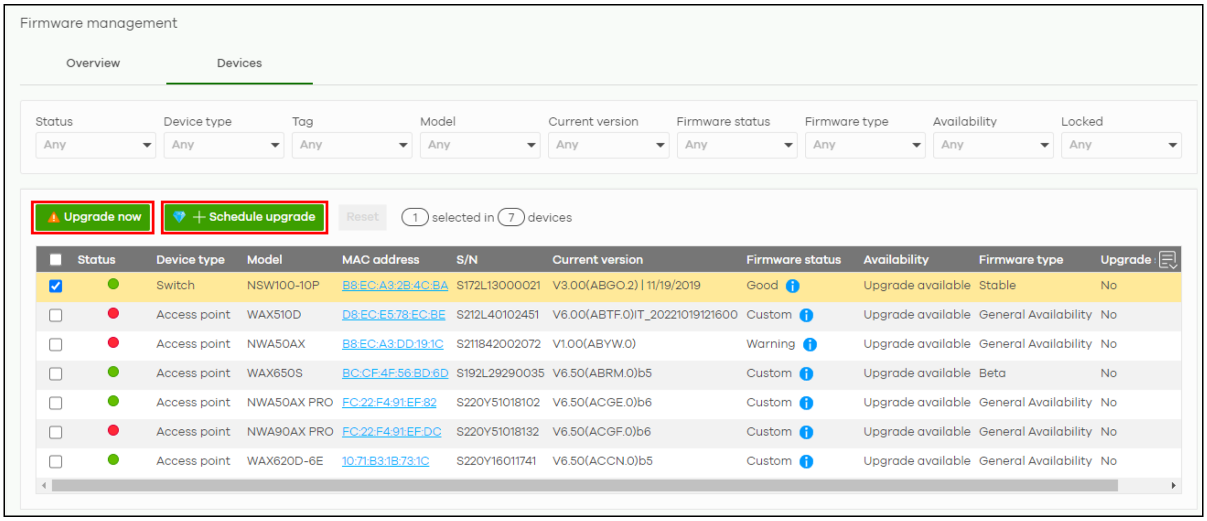
What is this?

Mobile Router

No devices

What is this?

2 You can set different times to upgrade firmware for your Nebula Devices to overwrite the site-wide **Settings** by going to the **Site-wide** > **Configure** > **Firmware management** > **Devices** screen. Or select **Upgrade now** to upgrade immediately.



Firmware management

Overview | Devices

Status: Any | Device type: Any | Tag: Any | Model: Any | Current version: Any | Firmware status: Any | Firmware type: Any | Availability: Any | Locked: Any

Upgrade now | Schedule upgrade | Reset | 1 selected in 7 devices

☐	Status	Device type	Model	MAC address	S/N	Current version	Firmware status	Availability	Firmware type	Upgrade
☑	🟢	Switch	NSW100-10P	B8:EC:A3:2B:4C:BA	S172L13000021	V3.00(ABGO.2) | 11/19/2019	Good	Upgrade available	Stable	No
☐	🔴	Access point	WAX510D	D8:EC:E5:78:EC:BE	S212L40102451	V6.00(ABTF.0)IT_20221019121600	Custom	Upgrade available	General Availability	No
☐	🔴	Access point	NWA50AX	B8:EC:A3:DD:19:1C	S211842002072	V1.00(ABYW.0)	Warning	Upgrade available	General Availability	No
☐	🟢	Access point	WAX650S	BC:CF:4F:56:BD:6D	S192L29290035	V6.50(ABRM.0)b5	Custom	Upgrade available	Beta	No
☐	🟢	Access point	NWA50AX PRO	FC:22:F4:91:EF:82	S220Y51018102	V6.50(ACGE.0)b6	Custom	Upgrade available	General Availability	No
☐	🔴	Access point	NWA90AX PRO	FC:22:F4:91:EF:DC	S220Y51018132	V6.50(ACGF.0)b6	Custom	Upgrade available	General Availability	No
☐	🟢	Access point	WAX620D-6E	10:71:B3:1B:73:1C	S220Y16011741	V6.50(ACCN.0)b5	Custom	Upgrade available	General Availability	No

3 If you do not want to upgrade the firmware immediately, you can click **+Schedule Upgrade** to create a schedule for your Nebula Device.

- Select **Follow device type settings** to upgrade the Nebula Device according to the site-wide schedule configured for all Nebula Devices in the site.
- Select **Auto upgrade at every Week**/**Month on Sunday**–**Saturday at hh:mm** to set up a routine schedule for upgrades.
- Select **Upgrade at** to set up a specific date and time for a one time upgrade. This option can be enabled only when the selected Nebula Devices have a new firmware available.

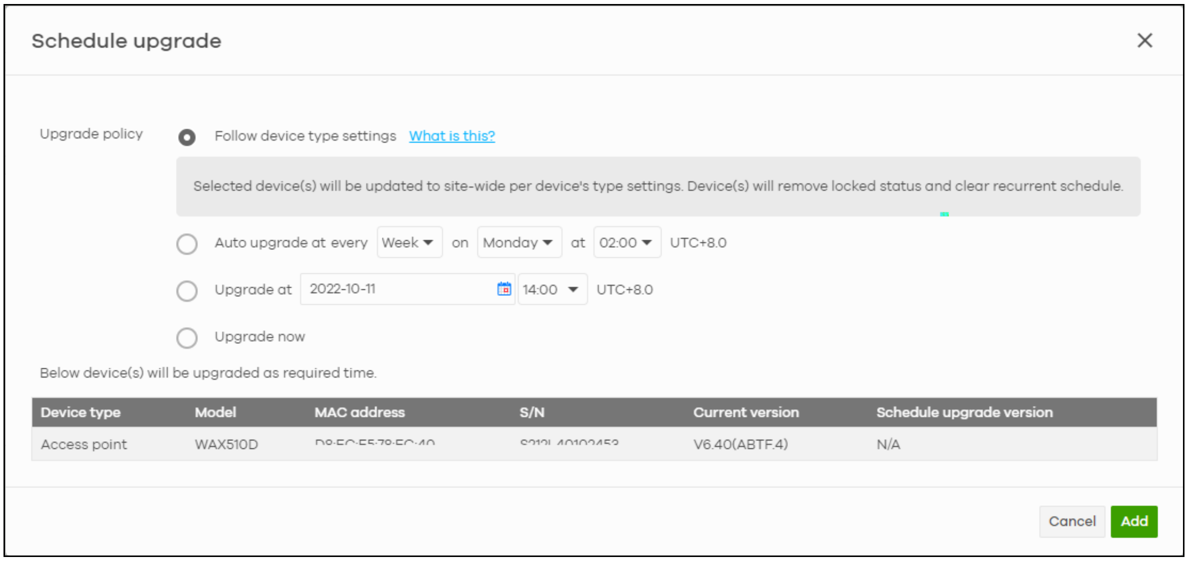
Note: Due to network bandwidth and number of Nebula Devices per site, not all Nebula Devices may get the firmware upgrade on the specified date/time.

- Select **Upgrade now** to immediately install the firmware. Then select the **Firmware type** (**Stable** or **Latest** (default)).

Note: When a firmware is officially released by Zyxel, it is the **Latest** firmware. For example, V6 is the **Latest** firmware. When the next firmware, V7, is released by Zyxel, V7 becomes the **Latest** firmware, and V6 will be classified as **General Availability**. Your Nebula Device firmware can be upgraded to V7 to use the new features. Zyxel will select a previous version (for example, V3) as a **Stable** release if no major issues have been reported by users.

Note: The **Upgrade at** and **Upgrade now** options can be enabled only when the selected Nebula Devices have a new firmware available.

4 Click **Add** to save the settings.



Schedule upgrade

Upgrade policy

● Follow device type settings What is this?

Selected device(s) will be updated to site-wide per device's type settings. Device(s) will remove locked status and clear recurrent schedule.

○ Auto upgrade at every Week on Monday at 02:00 UTC+8.0

○ Upgrade at 2022-10-11 14:00 UTC+8.0

○ Upgrade now

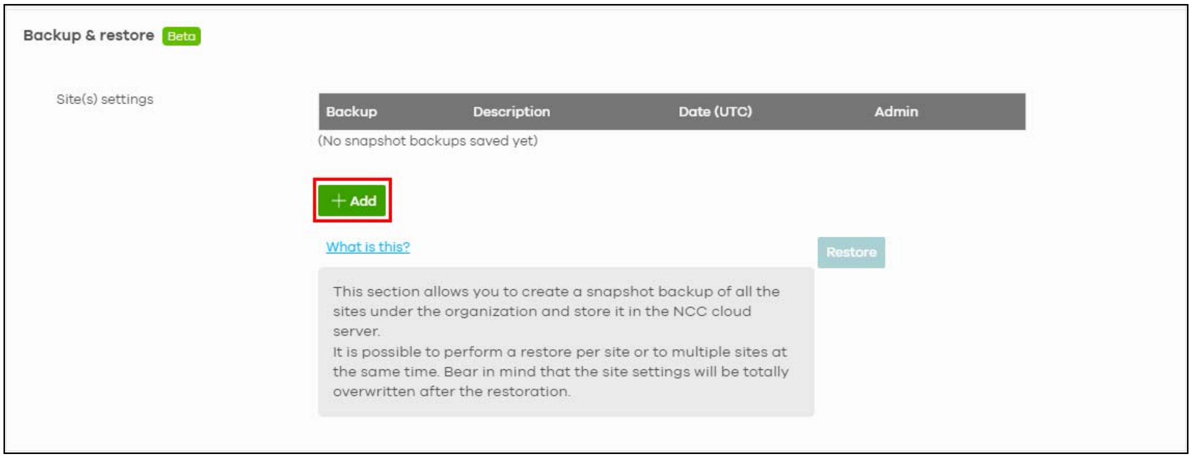
Below device(s) will be upgraded as required time.

Device type	Model	MAC address	S/N	Current version	Schedule upgrade version
Access point	WAX510D	D8:EC:E5:78:EC:40	S212L40102453	V6.40(ABTF.4)	N/A

3.11 Backup Current Configurations in NCC

This section shows you how to back up the current configurations for sites to the NCC, You may go back to this configuration if future configuration changes causes problems.

1 Go to the **Organization-wide** > **Organization-wide manage** > **Configuration management**: **Backup & restore**: **Site(s) settings** screen, then click **+Add**.



Backup & restore Beta

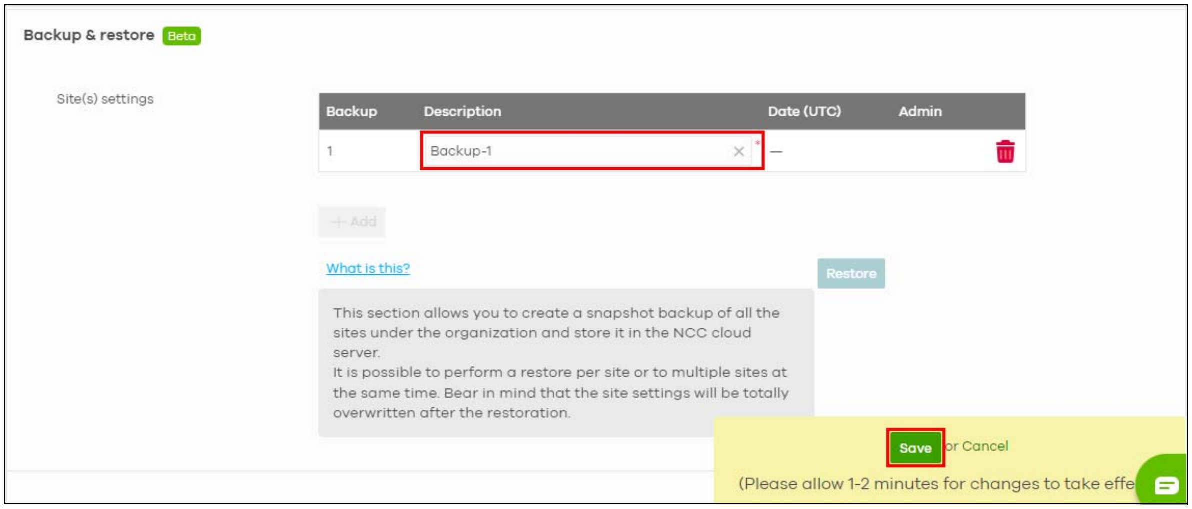
Site(s) settings

Backup	Description	Date (UTC)	Admin

(No snapshot backups saved yet)

This section allows you to create a snapshot backup of all the sites under the organization and store it in the NCC cloud server.
It is possible to perform a restore per site or to multiple sites at the same time. Bear in mind that the site settings will be totally overwritten after the restoration.

2 Enter a name for the backup in **Description** in order to save it to the NCC. You can use alphanumeric and ()+/:=?!*#@$_%- characters, up to 512 characters. Then click **Save**.



Backup & restore Beta

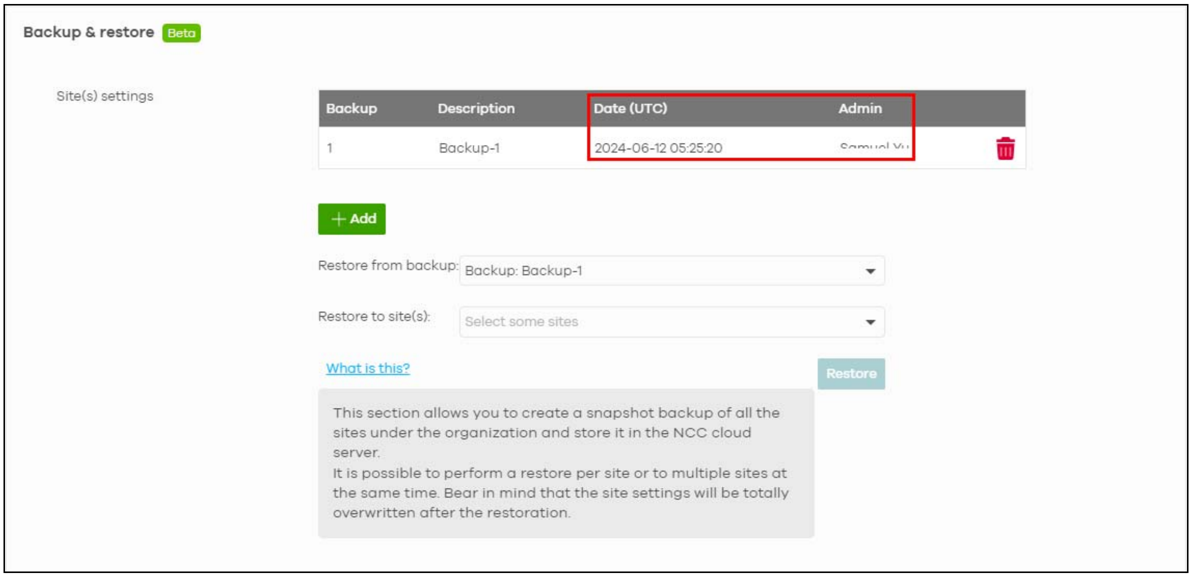
Site(s) settings

Backup	Description	Date (UTC)	Admin
1	Backup-1	—	

This section allows you to create a snapshot backup of all the sites under the organization and store it in the NCC cloud server.
It is possible to perform a restore per site or to multiple sites at the same time. Bear in mind that the site settings will be totally overwritten after the restoration.

(Please allow 1-2 minutes for changes to take effe

The **Date** of the backup and the name of the **Admin**istrator account who performed the backup will appear on the table.



Backup & restore Beta

Site(s) settings

Backup	Description	Date (UTC)	Admin
1	Backup-1	2024-06-12 05:25:20	Samuel Yu

Restore from backup: Backup: Backup-1

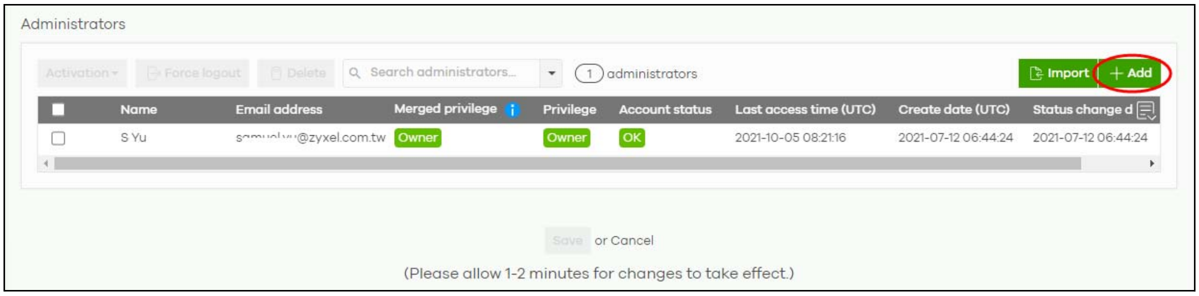
Restore to site(s): Select some sites

This section allows you to create a snapshot backup of all the sites under the organization and store it in the NCC cloud server.
It is possible to perform a restore per site or to multiple sites at the same time. Bear in mind that the site settings will be totally overwritten after the restoration.

3.12 Assign an Administrator to Manage a Nebula Device

This section shows you how to assign an administrator to manage your Nebula Device.

1 Go to the **Organization-wide** > **Administrators** screen. Click **+Add**.



Administrators

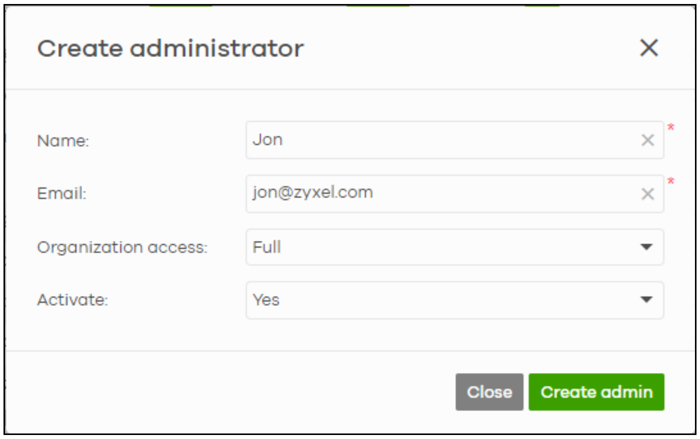
☐	Name	Email address	Merged privilege	Privilege	Account status	Last access time (UTC)	Create date (UTC)	Status change d
☐	S Yu	samuel.yu@zyxel.com.tw	Owner	Owner	OK	2021-10-05 08:21:16	2021-07-12 06:44:24	2021-07-12 06:44:24

(Please allow 1-2 minutes for changes to take effect.)

2 Enter the **Name** and **Email** of a Zyxel Account. Assign the **Organization access** (**Full**, **Read-Only**, **None**). See Table 225 on page 746 for information on organization privileges.

If you select **Full** for **Organization access**, select **Delegate owner's authority** to grant owner privileges to the new administrator except deleting/transferring organization ownership. Otherwise, do not select this option.

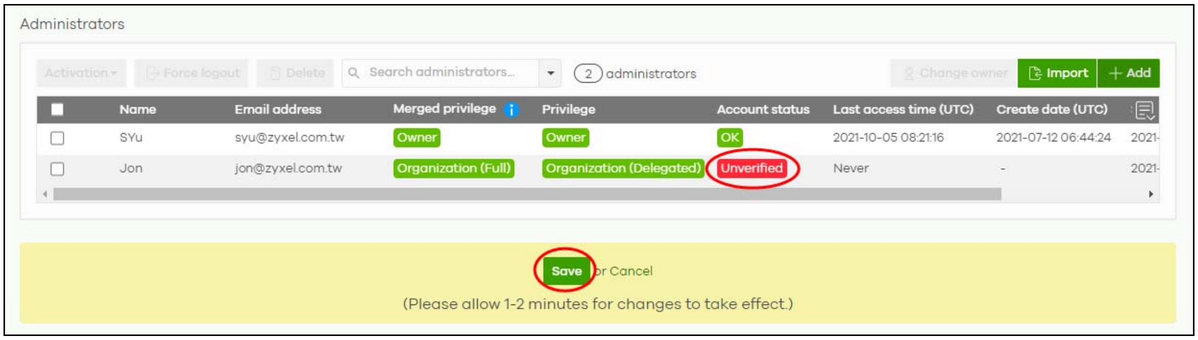
Select **Yes** if you wish to **Activate** the account administrator. Alternatively, select **No** if you wish to create an account administrator, but activate at a later time. The click **Create admin**.



Create administrator

Name:	Jon
Email:	jon@zyxel.com
Organization access:	Full
Activate:	Yes

3 The **Account status** field will show **Unverified**. Click **Save**.

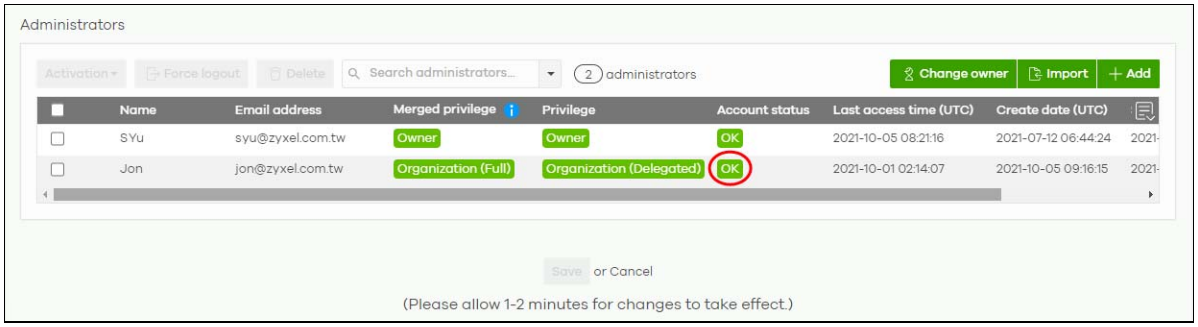


Administrators

□	Name	Email address	Merged privilege	Privilege	Account status	Last access time (UTC)	Create date (UTC)	
□	SYu	syu@zyxel.com.tw	Owner	Owner	OK	2021-10-05 08:21:16	2021-07-12 06:44:24	2021-
□	Jon	jon@zyxel.com.tw	Organization (Full)	Organization (Delegated)	Unverified	Never	-	2021-

(Please allow 1-2 minutes for changes to take effect.)

The **Account status** field will show **OK** after saving. The new administrator will receive an email notification.



Administrators

□	Name	Email address	Merged privilege	Privilege	Account status	Last access time (UTC)	Create date (UTC)	
□	SYu	syu@zyxel.com.tw	Owner	Owner	OK	2021-10-05 08:21:16	2021-07-12 06:44:24	2021-
□	Jon	jon@zyxel.com.tw	Organization (Full)	Organization (Delegated)	OK	2021-10-01 02:14:07	2021-10-05 09:16:15	2021-

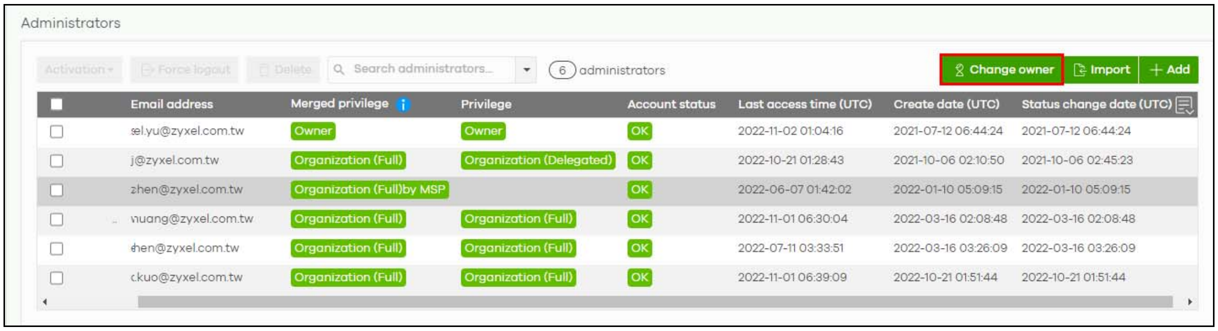
(Please allow 1-2 minutes for changes to take effect.)

3.13 Transfer the Ownership of the Organization

This section shows you how to transfer an organization's ownership, which includes transfer ownership of the Nebula Devices.

Note: Only the owner can transfer ownership of an organization to another administrator. See Section 3.12 on page 96 if you want to transfer management of your Nebula Devices only.

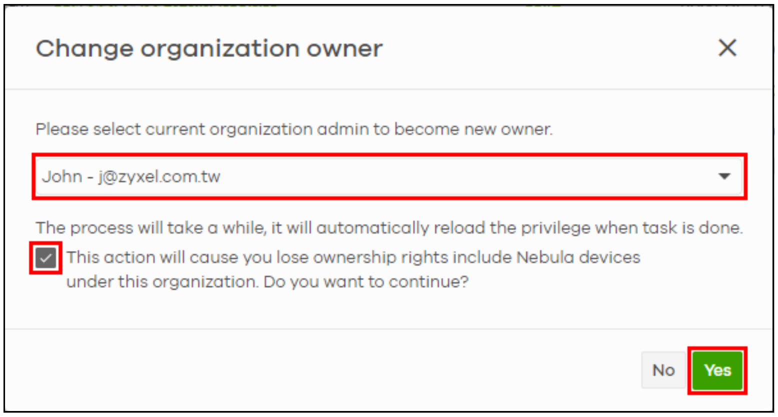
1 The new owner must be an administrator in the same organization. Go to the **Organization-wide** > **Administrators** screen. Click **Change owner**.



Administrators

□	Email address	Merged privilege	Privilege	Account status	Last access time (UTC)	Create date (UTC)	Status change date (UTC)
□	sel.yu@zyxel.com.tw	Owner	Owner	OK	2022-11-02 01:04:16	2021-07-12 06:44:24	2021-07-12 06:44:24
□	j@zyxel.com.tw	Organization (Full)	Organization (Delegated)	OK	2022-10-21 01:28:43	2021-10-06 02:10:50	2021-10-06 02:45:23
□	zhen@zyxel.com.tw	Organization (Full)by MSP		OK	2022-06-07 01:42:02	2022-01-10 05:09:15	2022-01-10 05:09:15
□	huang@zyxel.com.tw	Organization (Full)	Organization (Full)	OK	2022-11-01 06:30:04	2022-03-16 02:08:48	2022-03-16 02:08:48
□	hen@zyxel.com.tw	Organization (Full)	Organization (Full)	OK	2022-07-11 03:33:51	2022-03-16 03:26:09	2022-03-16 03:26:09
□	ckuo@zyxel.com.tw	Organization (Full)	Organization (Full)	OK	2022-11-01 06:39:09	2022-10-21 01:51:44	2022-10-21 01:51:44

2 Select the new owner from the other administrators in this organization from the drop-down menu. Select the checkbox to continue, and click **Yes** to confirm transfer of ownership.



Change organization owner

Please select current organization admin to become new owner.

John - j@zyxel.com.tw

The process will take a while, it will automatically reload the privilege when task is done.

☑ This action will cause you lose ownership rights include Nebula devices under this organization. Do you want to continue?

The new owner will be notified by email and must accept ownership of the organization.

3.14 Manage a Configuration Template

This section shows you how to use a configuration template to manage sites for your organization. Create a site and then bind a site to a template. You may enable the local override function if you want to configure some specific settings directly in a site after a site is bound to a template.

Note: This feature is available to an organization administrator with full privileges only (see Table 225 on page 746 for details on organization privileges).

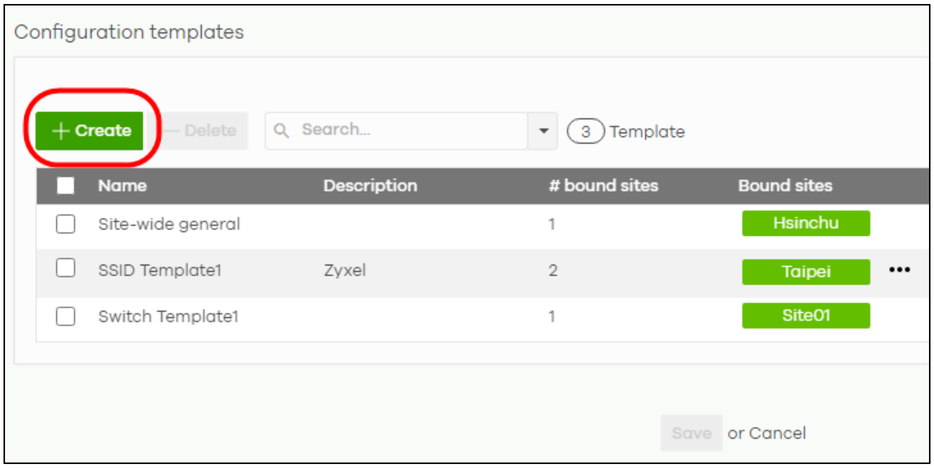
1 Create and Bind a Template Site/Setting

2 Duplicate and Import a Template Setting to a Site

3 Enable the Override Site-wide Configuration (Local Override) Feature

3.14.1 Create and Bind a Template Site/Setting

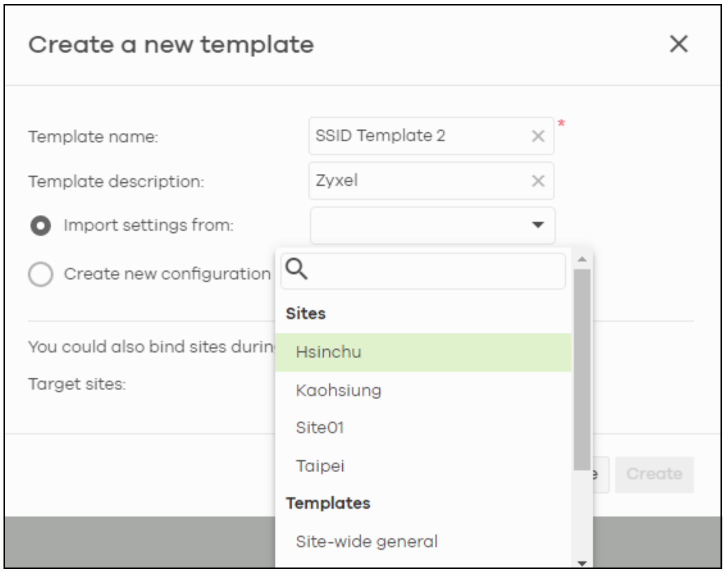
1 Go to the **Organization-wide** > **Organization-wide manage** > **Configuration templates** screen. Click **+Create**.



Configuration templates

Name	Description	# bound sites	Bound sites
□ Site-wide general		1	Hsinchu
□ SSID Template1	Zyxel	2	Taipei •••
□ Switch Template1		1	Site01

2 The following screen appears. Enter a **Template name** and **Template description** for the template site or setting you want to create.
To create a new configuration template, select **Create new configuration template**.
To import an existing template from a site or template, select **Import settings from**.



Template name: SSID Template 2 *

Template description: Zyxel

● Import settings from:

○ Create new configuration

You could also bind sites durin

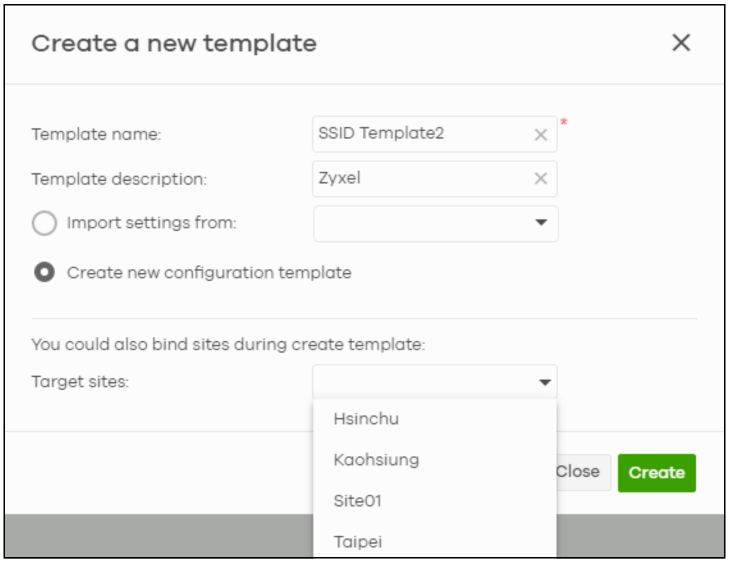
Target sites:

Sites
- Hsinchu
- Kaohsiung
- Site01
- Taipei

Templates
- Site-wide general

Note: Under **Import settings from**, select a site from **Sites** to copy a site's settings. Under **Import setting from**, select a template from **Templates** to copy a site's site-wide general setting, an Access Point's SSIDs setting or a Switch's port setting.

3 Select a site from the **Target sites** drop-down list box to bind the template to a site.
Click **Create** and then click **Save** to save the changes.



Template name: SSID Template2 *

Template description: Zyxel

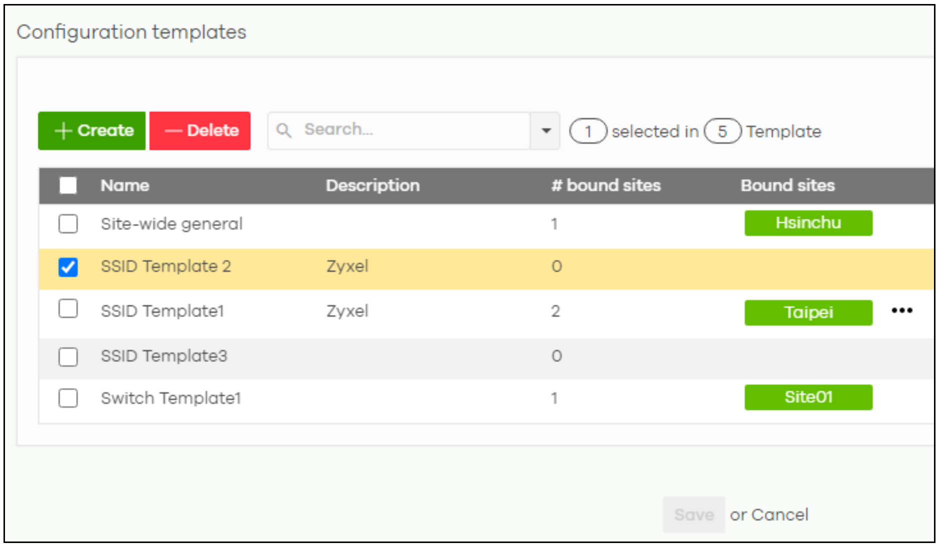
○ Import settings from:

● Create new configuration template

You could also bind sites during create template:

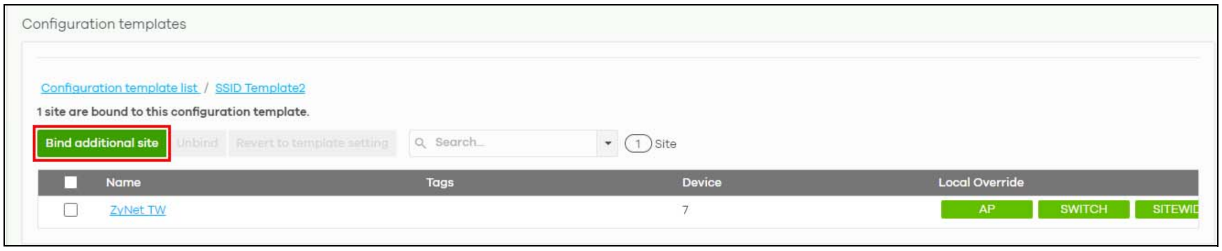
Target sites:
- Hsinchu
- Kaohsiung
- Site01
- Taipei

If you skip this step, you can bind a template to a site later. Go to the **Organization-wide** > **Organization-wide manage** > **Configuration templates** screen. Select the template you want to use and then click the row with the template that you want to bind to a site.



☐	Name	Description	# bound sites	Bound sites
☐	Site-wide general		1	Hsinchu
☑	SSID Template 2	Zyxel	0	
☐	SSID Template1	Zyxel	2	Taipei •••
☐	SSID Template3		0	
☐	Switch Template1		1	Site01

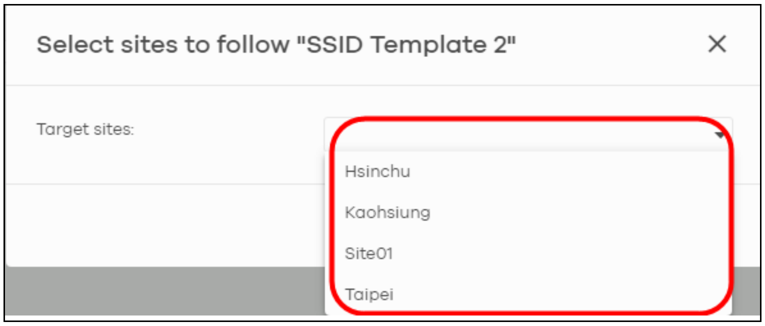
4 The following screen appears. Click **Bind additional site** to select the site you want to bind the template to.


Configuration templates
Configuration template list / SSID Template2
Bind additional site
Unbind
Revert to template setting
Search...
1 Site

1 site are bound to this configuration template.

☐	Name	Tags	Device	Local Override
☐	ZyNet TW		7	AP SWITCH SITEWID

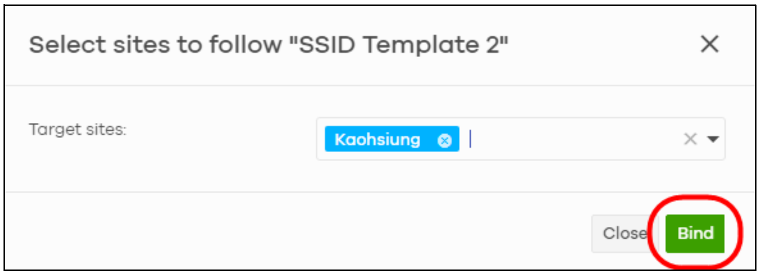
5 The following screen appears. Click the **Target sites** drop-down list box.



Select sites to follow "SSID Template 2"

Target sites:

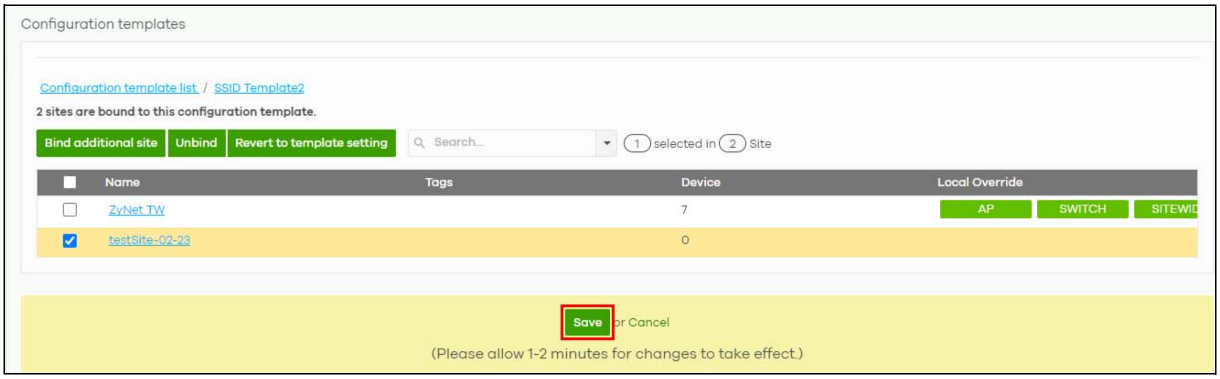
6 Select a site from the **Target sites** drop-down box list and then click **Bind**.



Select sites to follow "SSID Template 2"

Target sites: Kaohsiung

7 Click **Save** to save the changes.



Configuration templates

Configuration template list / SSID Template2

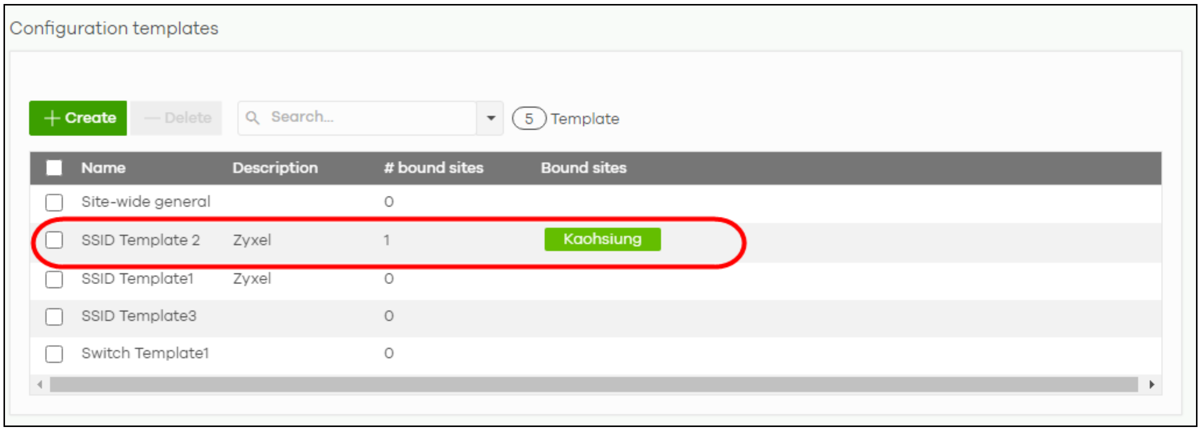
2 sites are bound to this configuration template.

1 selected in 2 Site

□	Name	Tags	Device	Local Override
□	ZyNet TW		7	AP SWITCH SITEWID
☑	testSite-02-23		0	

(Please allow 1-2 minutes for changes to take effect.)

8 A configuration template is created as shown in the **Organization-wide** > **Organization-wide manage** > **Configuration templates** screen.

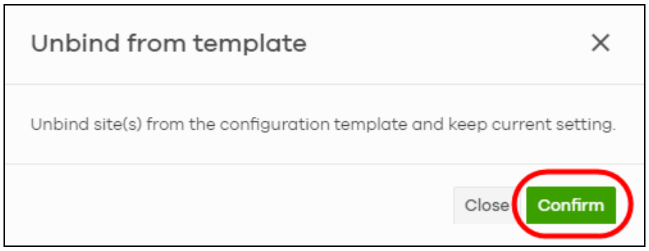


Configuration templates

5 Template

□	Name	Description	# bound sites	Bound sites
□	Site-wide general		0	
□	SSID Template 2	Zyxel	1	Kaohsiung
□	SSID Template1	Zyxel	0	
□	SSID Template3		0	
□	Switch Template1		0	

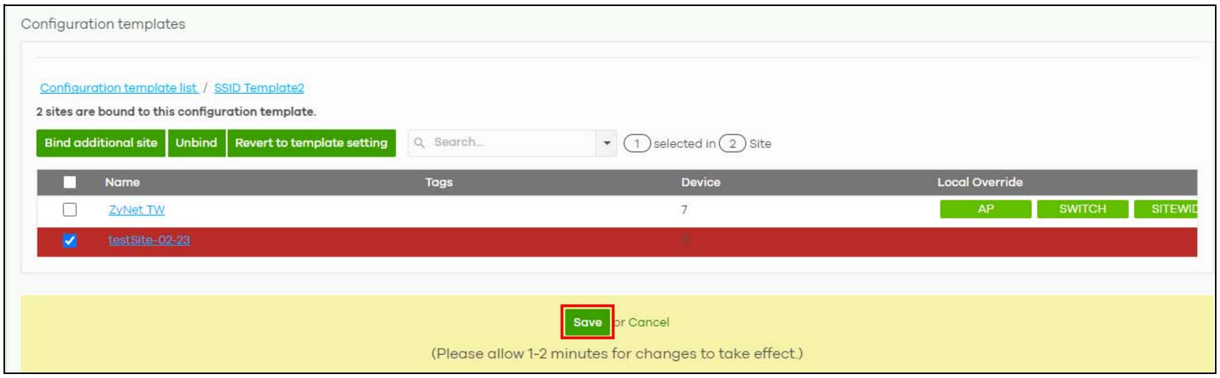
9 To release a site from using a configuration template, select a site and then click **Unbind** to unbind the site. The site which is unbound from the template still retains the settings applied from the template. The following screen appears. Click **Confirm** to confirm the changes.



Unbind from template

Unbind site(s) from the configuration template and keep current setting.

10 Click **Save** to save the changes.



Configuration templates

Configuration template list / SSID Template2

2 sites are bound to this configuration template.

1 selected in 2 Site

□	Name	Tags	Device	Local Override
□	ZyNet TW		7	AP SWITCH SITEWID
☑	testSite-02-23			

or Cancel

(Please allow 1-2 minutes for changes to take effect.)

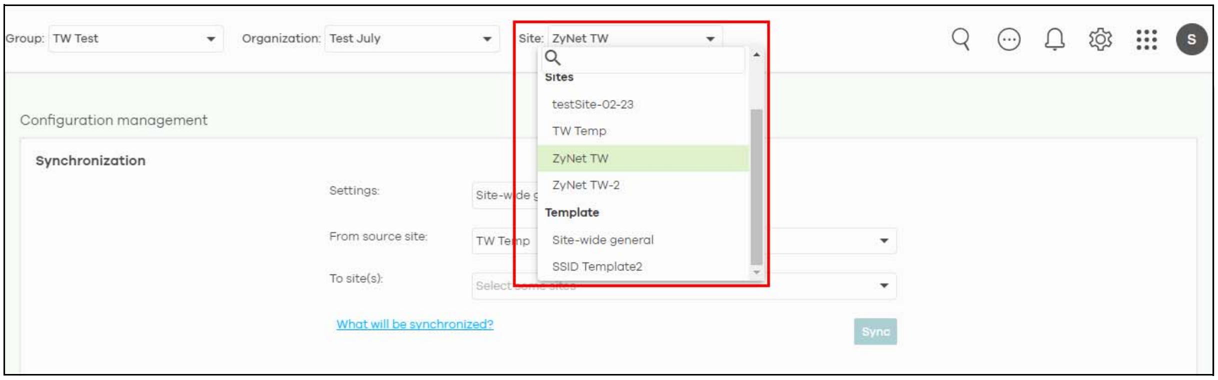
3.14.2 Duplicate and Import a Template Setting to a Site

This section shows you how to duplicate and then import the following template settings to a site:

- The site-wide general setting includes the device configuration, SNMP and captive portal re-authentication.
- An Access Point's SSID setting.
- A Switch's port setting.

The site-wide general setting

1 Select a bound site from the **Site** drop-down list box.



Group: TW Test

Organization: Test July

Site: ZyNet TW

Configuration management

Synchronization

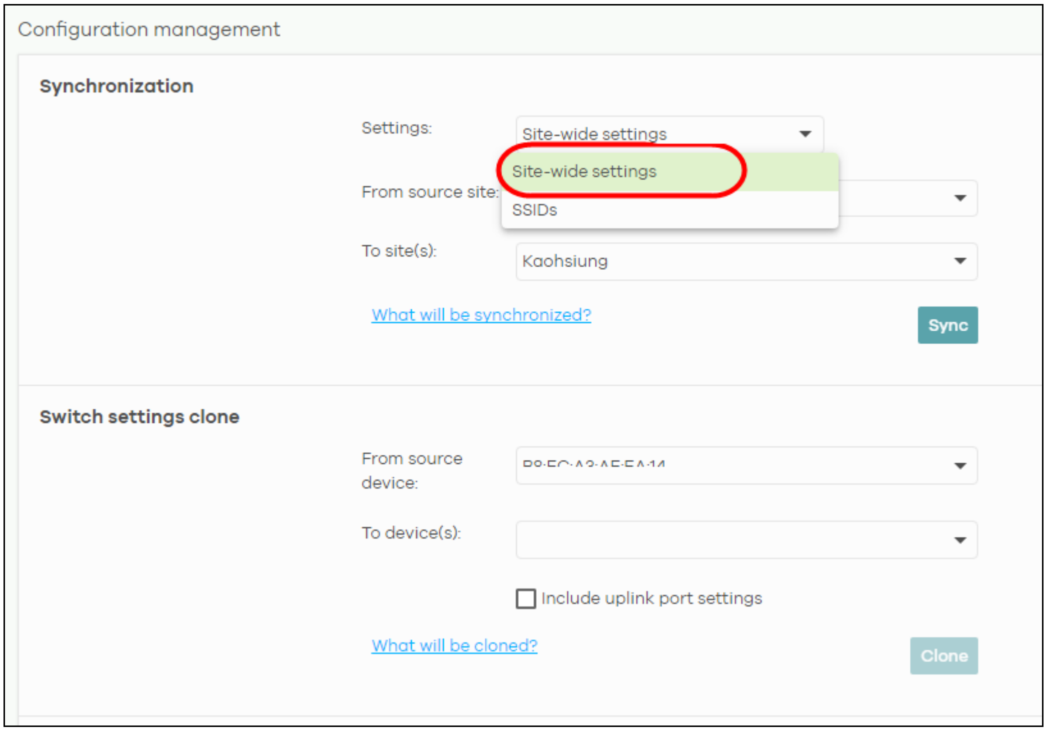
Settings: Site-wide g

From source site: TW Temp

To site(s): Select some sites

What will be synchronized?

2 Go to the **Organization-wide** > **Organization-wide manage** > **Configuration management** screen. Under **Synchronization**, select the **Site-wide settings** in **Settings** to copy a site's general setting to another site.



Configuration management

Synchronization

Settings: Site-wide settings

Site-wide settings

SSIDs

From source site:

To site(s): Kaohsiung

What will be synchronized?

Sync

Switch settings clone

From source device: B8:EC:A3:AE:EA:14

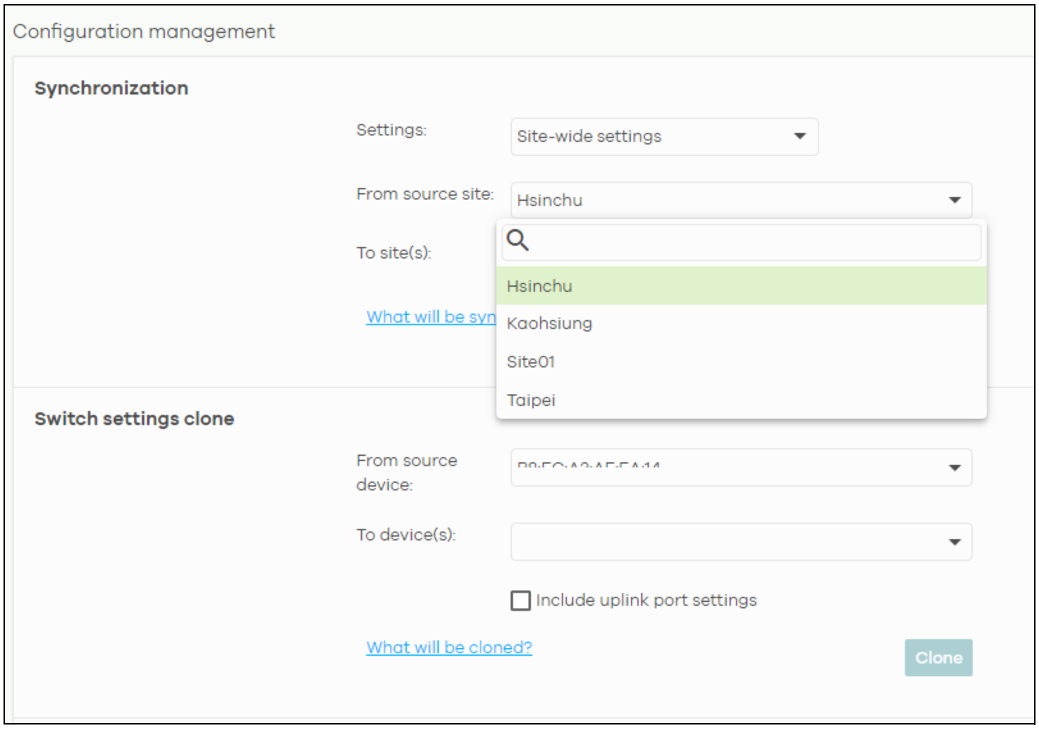
To device(s):

□ Include uplink port settings

What will be cloned?

Clone

3 From the **From source site** drop-down list box, select the site you want to copy the **Site-wide settings** from.



Configuration management

Synchronization

Settings: Site-wide settings

From source site: Hsinchu

Hsinchu

Kaohsiung

Site01

Taipei

To site(s):

What will be syn

Switch settings clone

From source device: B8:EC:A3:AE:EA:14

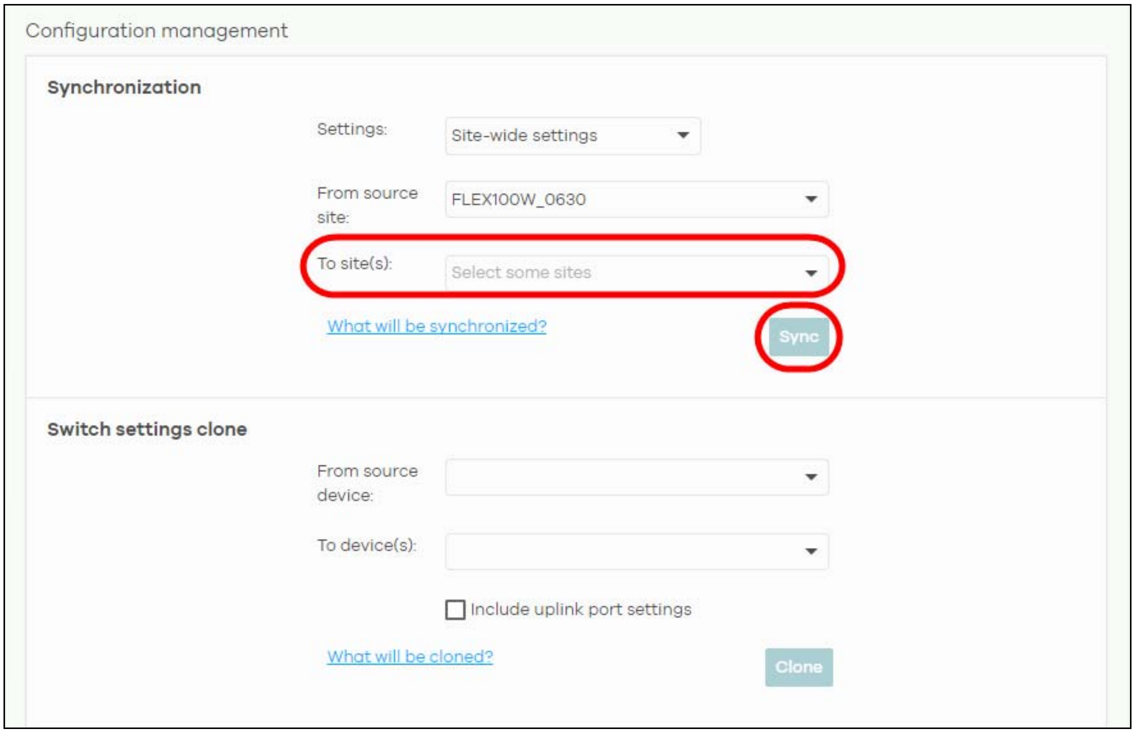
To device(s):

□ Include uplink port settings

What will be cloned?

Clone

4 From the **To site(s)** drop-down list box, select the site you want to import the **Site-wide settings** to. Click **Sync** to save the changes.



Configuration management

Synchronization

Settings: Site-wide settings

From source site: FLEX100W_0630

To site(s): Select some sites

What will be synchronized?

Sync

Switch settings clone

From source device:

To device(s):

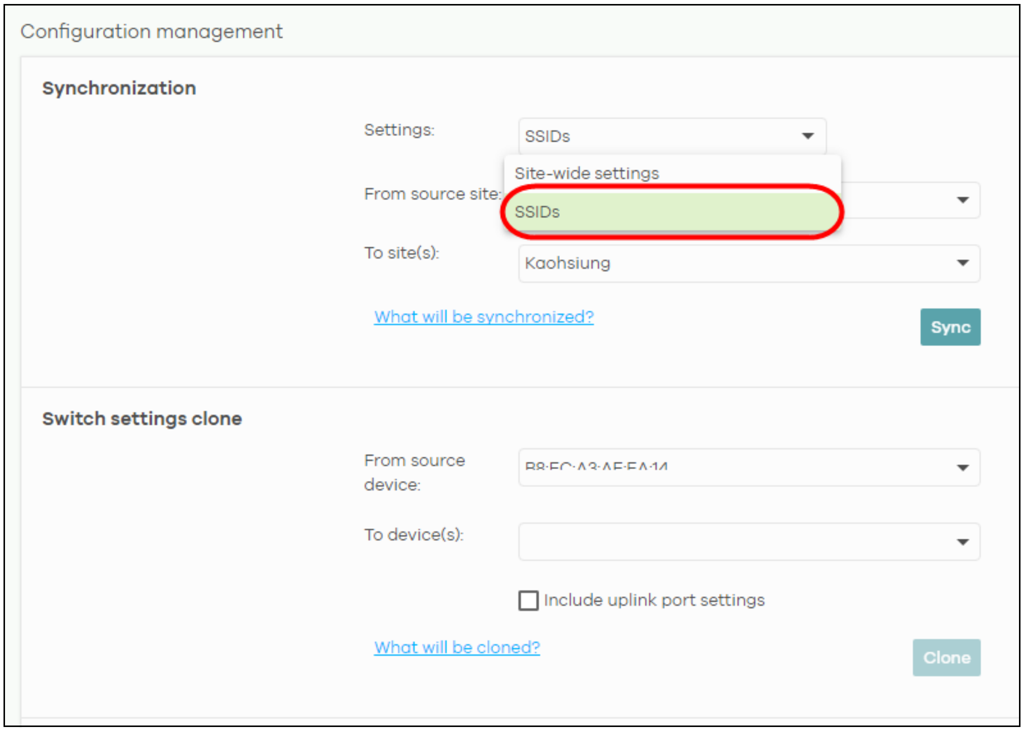
□ Include uplink port settings

What will be cloned?

Clone

An Access Point's SSID Setting

1 Go to **Organization-wide** > **Organization-wide manage** > **Configuration management** screen. Under **Synchronization,** select **SSIDs** to copy a site's SSIDs settings to another site. The duplicated **SSIDs** include the authentication and captive portal settings.



Configuration management

Synchronization

Settings: SSIDs

Site-wide settings

SSIDs

From source site:

To site(s): Kaohsiung

What will be synchronized?

Sync

Switch settings clone

From source device: B8:EC:A3:AE:EA:14

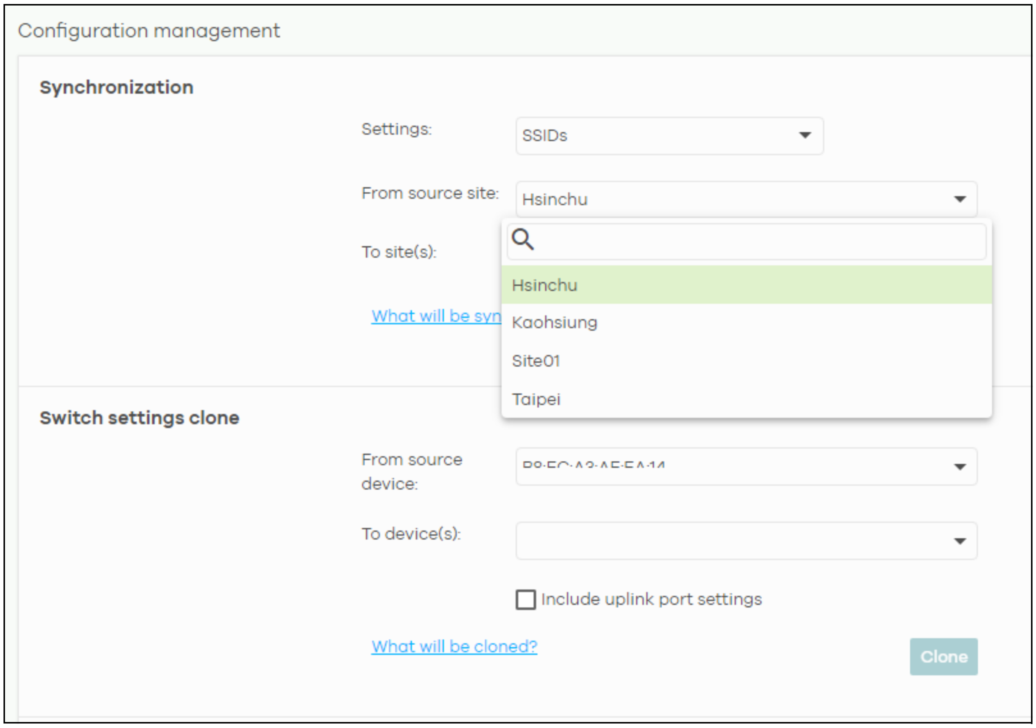
To device(s):

□ Include uplink port settings

What will be cloned?

Clone

2 From the **From source site** drop-down list box, select the site you want to copy the **SSIDs** from.



Configuration management

Synchronization

Settings: SSIDs

From source site: Hsinchu

To site(s):

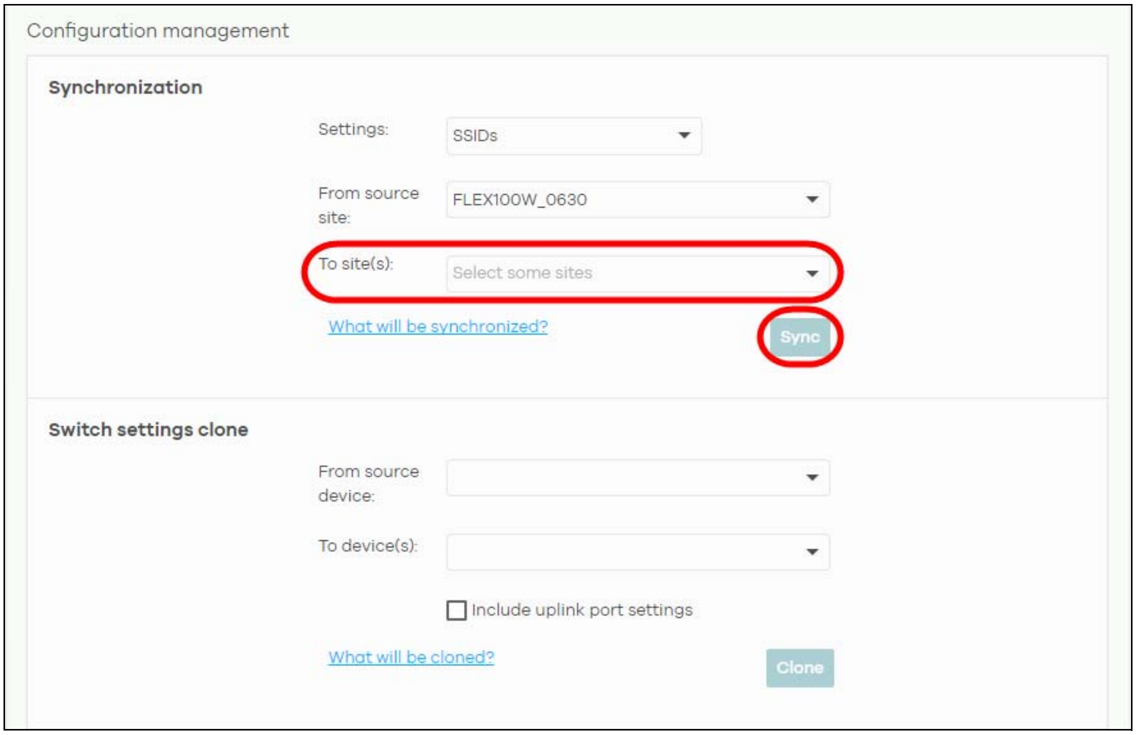
Switch settings clone

From source device: B8:EC:A3:AE:EA:14

To device(s):

□ Include uplink port settings

3 From the **To site(s)** drop-down list box**,** select the site you want to import the **SSIDs** to. Click **Sync** to save the changes.



Configuration management

Synchronization

Settings: SSIDs

From source site: FLEX100W_0630

To site(s): Select some sites

Switch settings clone

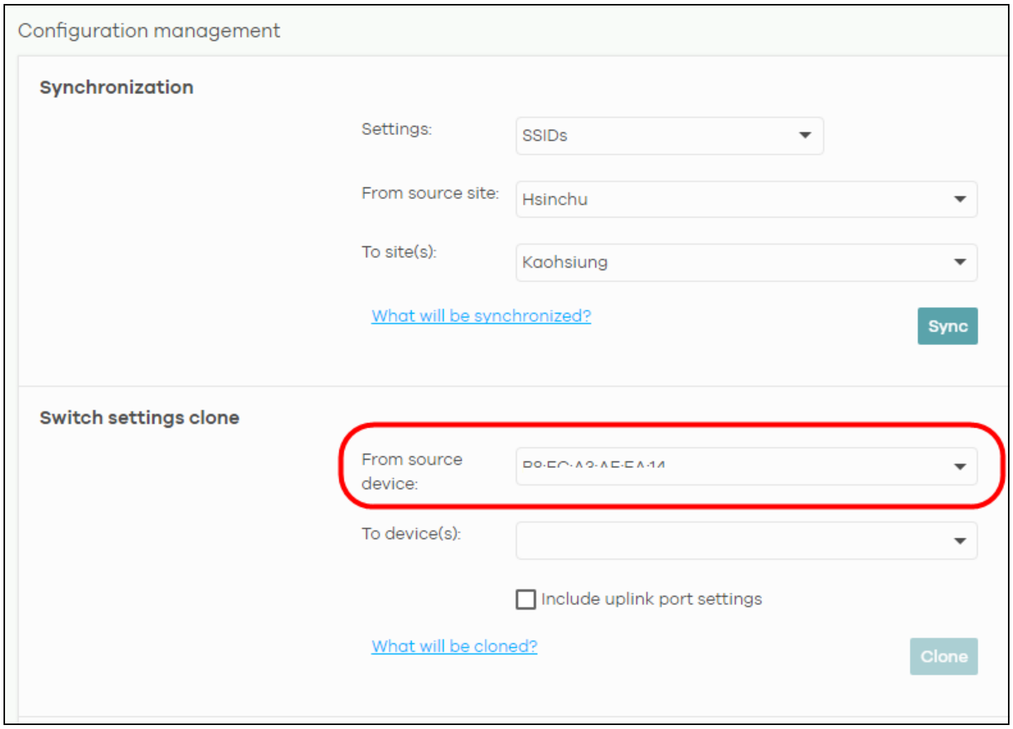
From source device:

To device(s):

□ Include uplink port settings

A Switch's Port Setting

1 Go to the **Organization-wide** > **Organization-wide manage** > **Configuration management** screen. Under **Switch settings clone**, select the Nebula Device's MAC address from the **From source device** drop-down list box. The cloned switch setting includes the port setting, IGMP advanced settings and STP bridge priority.



Configuration management

Synchronization

Settings: SSIDs

From source site: Hsinchu

To site(s): Kaohsiung

What will be synchronized?

Switch settings clone

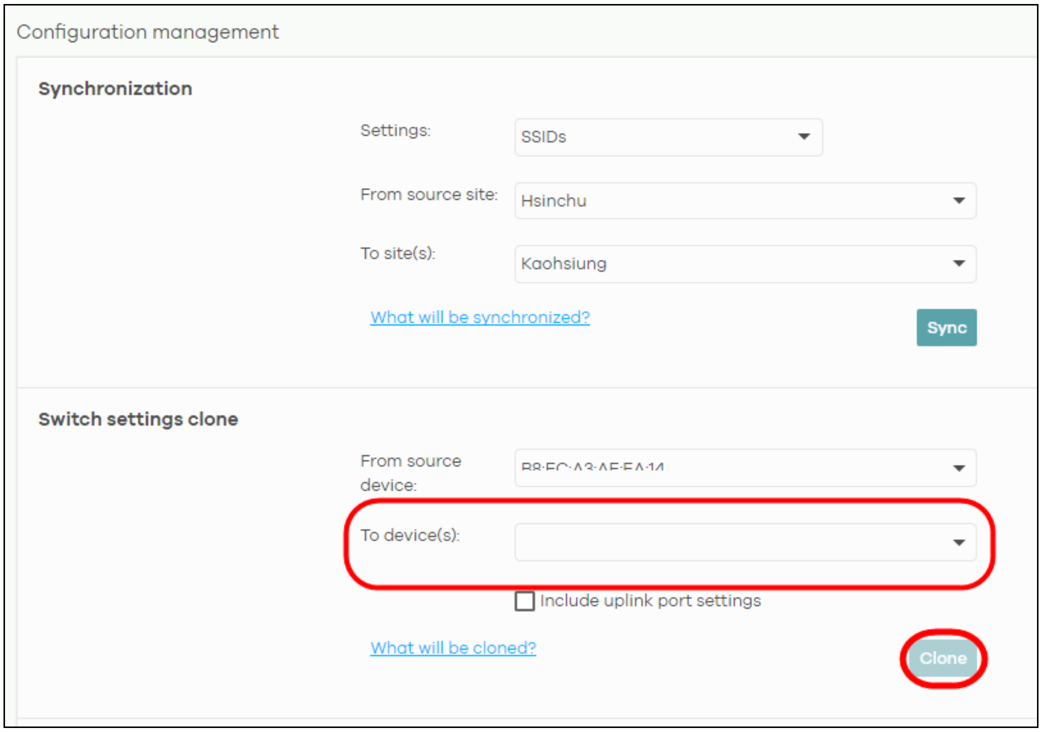
From source device: B8:EC:A3:AE:EA:14

To device(s):

□ Include uplink port settings

What will be cloned?

2 From the **To device(s)** drop-down list box, select the Nebula Device's MAC address you want to import the Switch setting to. Click **Clone** to save the changes.



Configuration management

Synchronization

Settings: SSIDs

From source site: Hsinchu

To site(s): Kaohsiung

What will be synchronized?

Sync

Switch settings clone

From source device: B8:EC:A3:AE:EA:14

To device(s):

□ Include uplink port settings

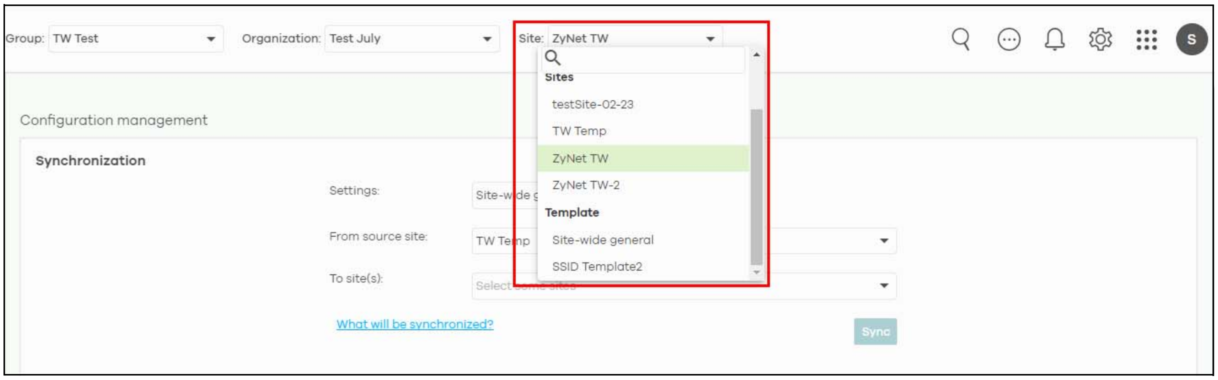
What will be cloned?

Clone

3.14.3 Enable the Override Site-wide Configuration (Local Override) Feature

A configuration template is a list of common settings that you can bind (apply) to a site. If you do not want to apply any new settings from the template to a site, just unbind that site. If you want to configure some specific settings directly in a site after the site is bound to a template, turn on the local override function. This feature is available to an organization administrator with full privileges only.

This section shows you how to enable the **Override site-wide configuration** feature to update site information. Select a bound site from the **Site** drop-down list box to edit the details of the selected site.



Group: TW Test

Organization: Test July

Site: ZyNet TW

Sites

testSite-02-23

TW Temp

ZyNet TW

ZyNet TW-2

Template

Site-wide general

SSID Template2

Configuration management

Synchronization

Settings: Site-wide g

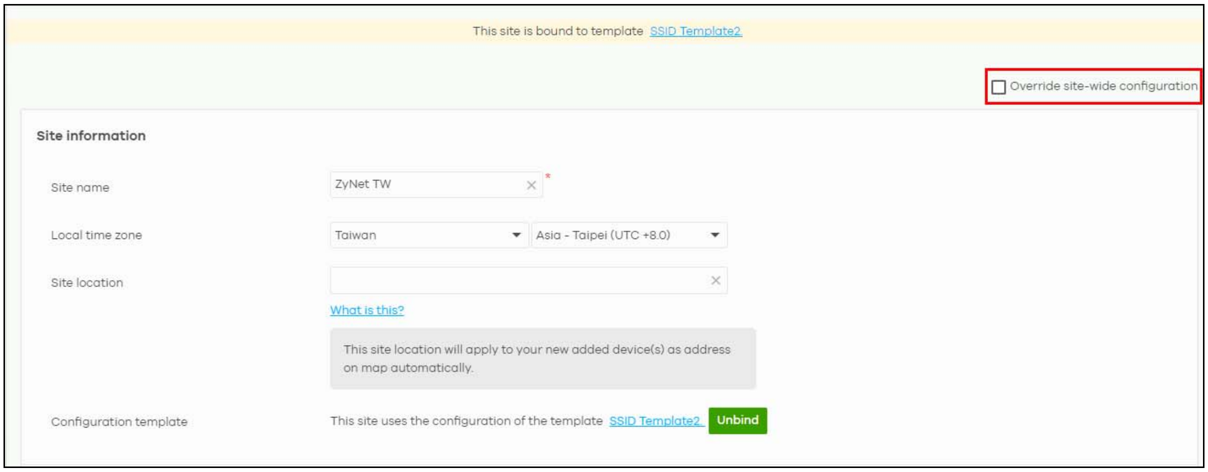
From source site: TW Temp

To site(s): Select some sites

What will be synchronized?

Sync

1 Go to a page under **Site-wide** > **Configure** and then select the **Override site-wide configuration** box. The **Configuration** page of a bound site contains an **Override site-wide configuration** box.



This site is bound to template SSID Template2

☐ Override site-wide configuration

Site information

Site name: ZyNet TW

Local time zone: Taiwan; Asia - Taipei (UTC +8.0)

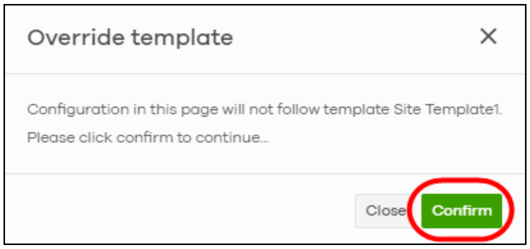
Site location:

What is this?

This site location will apply to your new added device(s) as address on map automatically.

Configuration template: This site uses the configuration of the template SSID Template2 Unbind

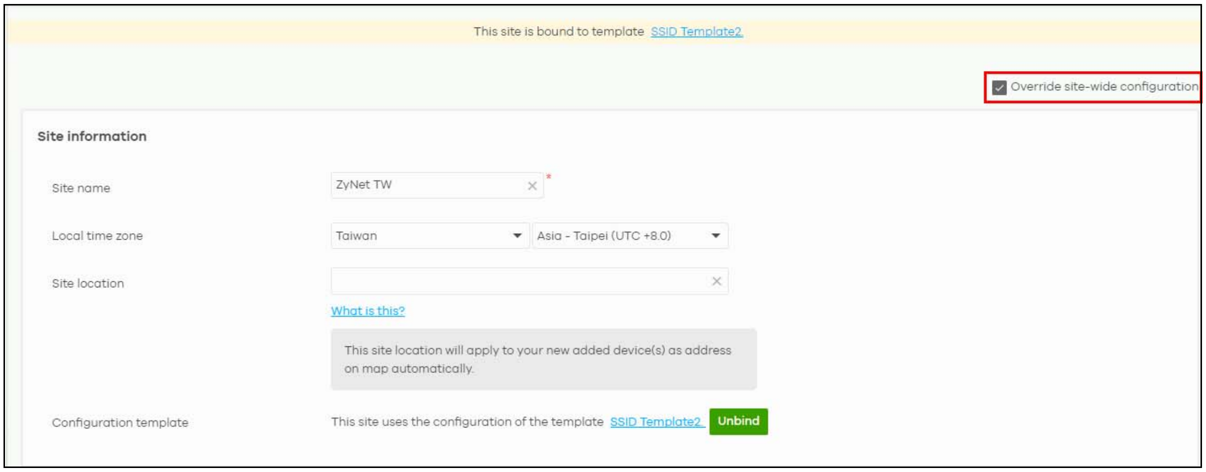
2 The following screen appears. Click **Confirm** to continue.



Override template

Configuration in this page will not follow template Site Template1.
Please click confirm to continue...

3 In the **Site-wide** > **Configure** > **Site settings** screen, edit the **Site information**, **Device configuration**, **Captive portal reauthentication**, **SNMP** and **Voucher settings** on the following page. Click **Save** to save the changes.



This site is bound to template SSID Template2

☑ Override site-wide configuration

Site information

Site name: ZyNet TW

Local time zone: Taiwan; Asia - Taipei (UTC +8.0)

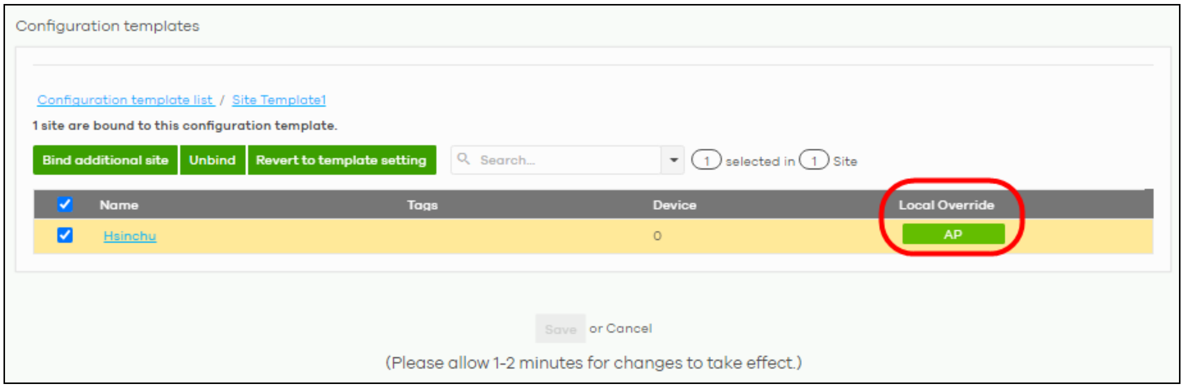
Site location:

What is this?

This site location will apply to your new added device(s) as address on map automatically.

Configuration template: This site uses the configuration of the template SSID Template2 Unbind

4 To verify the local override setting of a site, go to **Organization-wide** > **Organization-wide manage** > **Configuration templates**. The **Local Override** field may show that **AP/SWITCH/GATEWAY/SITE-WIDE** settings in the template do not apply to the site. A tag for **AP**, as shown in the following figure, indicates that Access Point settings have a local override and any further changes in the template's AP settings will not be synchronized to the site.



Configuration templates

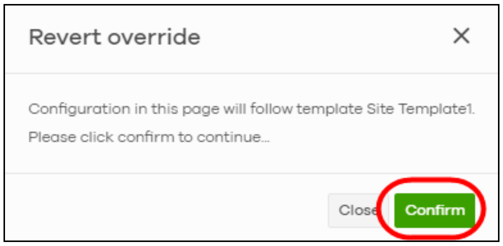
Configuration template list / Site Template1

1 site are bound to this configuration template.

☑	Name	Tags	Device	Local Override
☑	Hsinchu		0	AP

(Please allow 1-2 minutes for changes to take effect.)

5 If you decide to go back to the original template settings, clear the **Override site-wide configuration** box on any page under **Site-wide** > **Configuration**. The following screen appears. Click **Confirm** to continue.



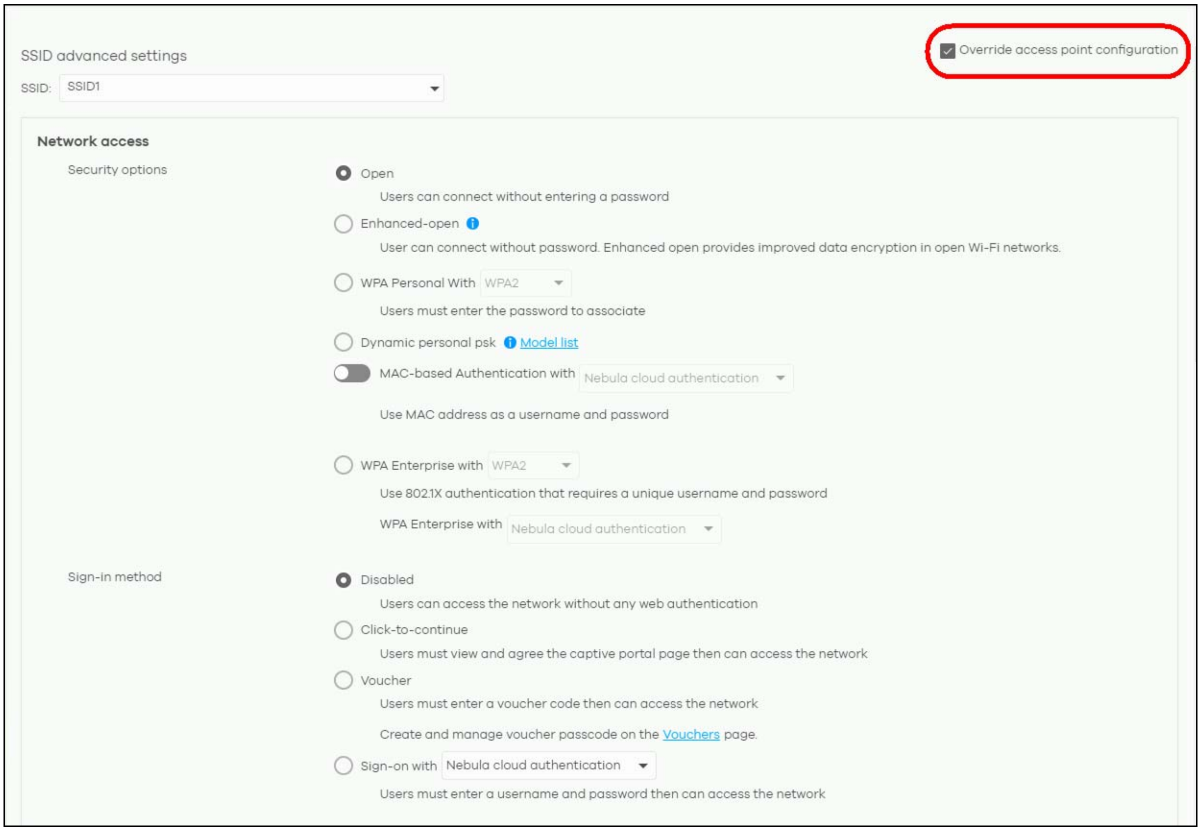
Revert override

Configuration in this page will follow template Site Template1.
Please click confirm to continue...

Overwrite the Access Point / Switch Setting

1 Go to any page under **Site-wide** > **Configure > Access points** / **Switch** and then select the **Override access point configuration** box. Every **Configuration** page of a bound site contains an **Override site-wide configuration** box.

Note: If the local override configuration is enabled on one page, all configuration pages of the Nebula Devices in the selected site will be enabled.



SSID advanced settings

SSID: SSID1

☑ Override access point configuration

Network access

Security options

● Open
Users can connect without entering a password

○ Enhanced-open
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.

○ WPA Personal With WPA2
Users must enter the password to associate

○ Dynamic personal psk Model list

MAC-based Authentication with Nebula cloud authentication
Use MAC address as a username and password

○ WPA Enterprise with WPA2
Use 802.1X authentication that requires a unique username and password
WPA Enterprise with Nebula cloud authentication

Sign-in method

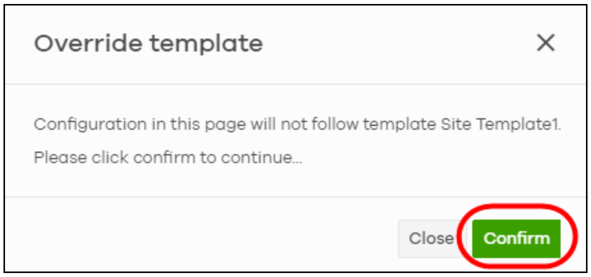
● Disabled
Users can access the network without any web authentication

○ Click-to-continue
Users must view and agree the captive portal page then can access the network

○ Voucher
Users must enter a voucher code then can access the network
Create and manage voucher passcode on the Vouchers page.

○ Sign-on with Nebula cloud authentication
Users must enter a username and password then can access the network

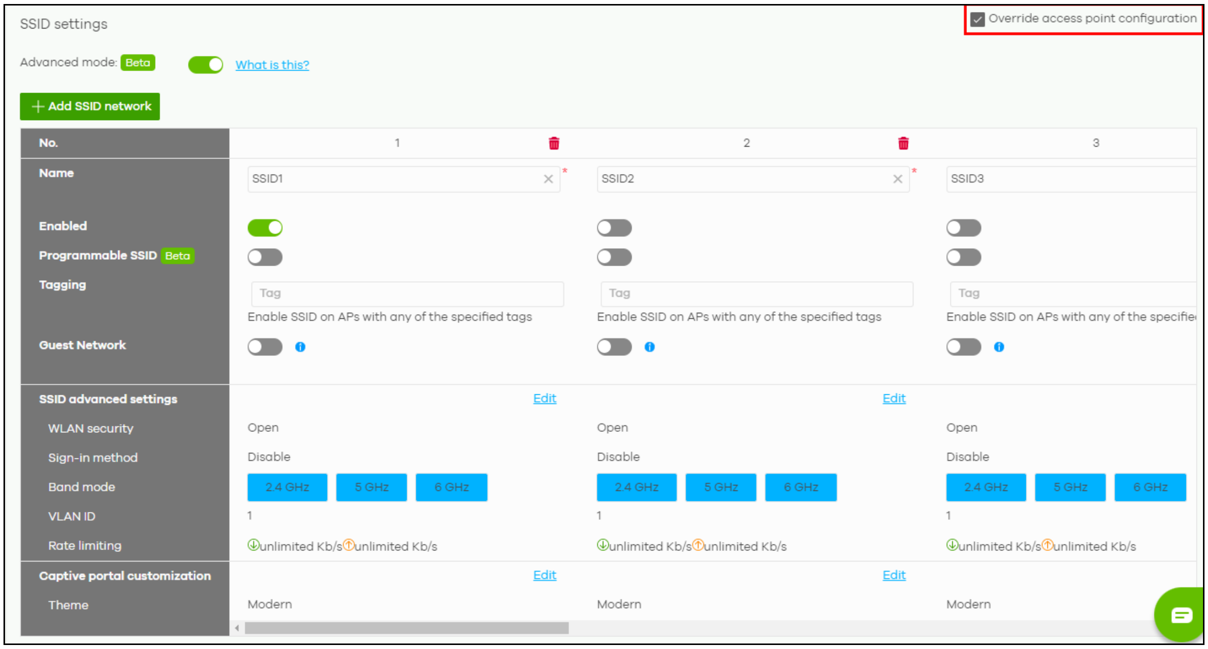
2 This allows a specific type of Nebula Device setting override. The following screen appears. Click **Confirm** to continue.



Override template

Configuration in this page will not follow template Site Template1.
Please click confirm to continue...

3 In **Site-wide** > **Configure** > **Access point** > **SSID settings**, edit your SSIDs, authentication or captive portal settings on the following page. Click **Save** to save the changes.


SSID settings

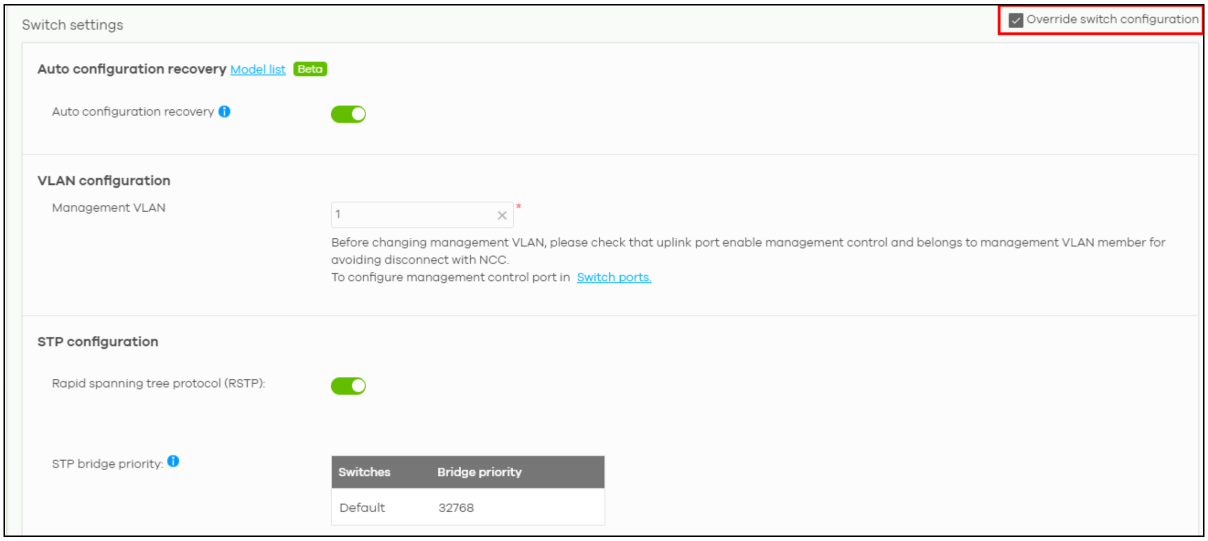
☑ Override access point configuration

Advanced mode: Beta   What is this?

+ Add SSID network

No.	1	2	3
Name	SSID1	SSID2	SSID3
Enabled	●	○	○
Programmable SSID Beta	○	○	○
Tagging	Tag Enable SSID on APs with any of the specified tags	Tag Enable SSID on APs with any of the specified tags	Tag Enable SSID on APs with any of the specifie
Guest Network	○	○	○
SSID advanced settings	Edit	Edit	
WLAN security	Open	Open	Open
Sign-in method	Disable	Disable	Disable
Band mode	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
VLAN ID	1	1	1
Rate limiting	unlimited Kb/s unlimited Kb/s	unlimited Kb/s unlimited Kb/s	unlimited Kb/s unlimited Kb/s
Captive portal customization	Edit	Edit	
Theme	Modern	Modern	Modern

4 In the **Site-wide** > **Configuration** > **Switches** > **Switch settings** screen, edit **VLAN configuration**, **STP configuration**, **Quality of service**, or **Port mirroring** settings on the following page. Click **Save** to save the changes.


Switch settings

☑ Override switch configuration

Auto configuration recovery Model list Beta

Auto configuration recovery ●

VLAN configuration

Management VLAN: 1

Before changing management VLAN, please check that uplink port enable management control and belongs to management VLAN member for avoiding disconnect with NCC.
To configure management control port in Switch ports.

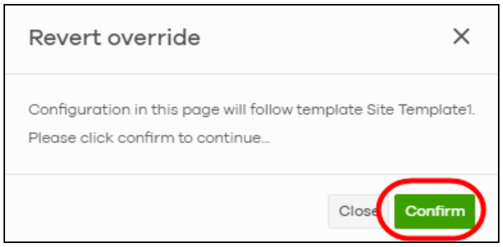
STP configuration

Rapid spanning tree protocol (RSTP): ●

STP bridge priority:

Switches	Bridge priority
Default	32768

5 To go back to the original template settings, clear the **Override switch configuration** box on any page under **Site-wide** > **Configuration > Access points** / **Switches**. The following screen appears. Click **Confirm** to continue.


Revert override

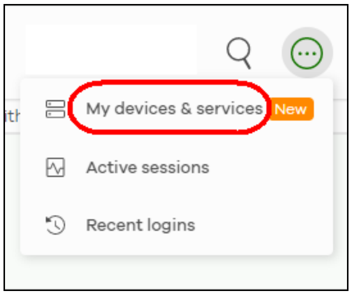
Configuration in this page will follow template Site Template1.
Please click confirm to continue...

3.15 Activate an MSP License

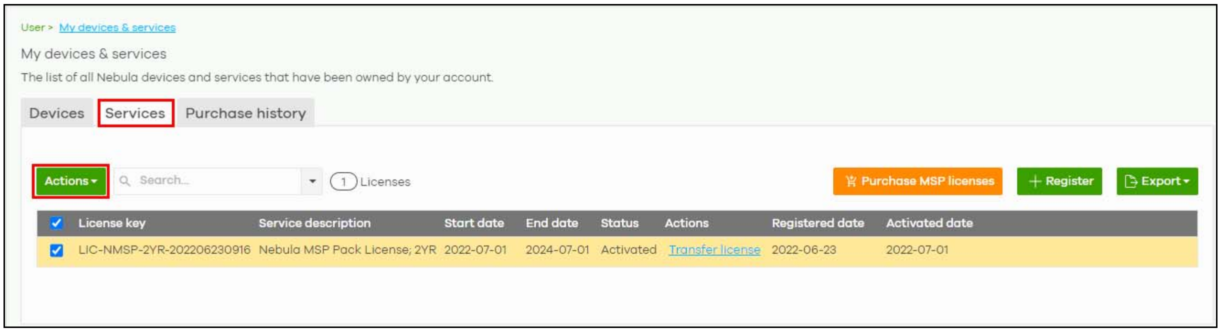
You must have an NCC account and an MSP license pack to activate an MSP license.

To activate an MSP pack, do the following:

1 Click the More icon (upper right) and select **My devices & services**.



2 Select the **Services** tab.


User > My devices & services

My devices & services

The list of all Nebula devices and services that have been owned by your account.

☑	License key	Service description	Start date	End date	Status	Actions	Registered date	Activated date
☑	LIC-NMSP-2YR-202206230916	Nebula MSP Pack License; 2YR	2022-07-01	2024-07-01	Activated	Transfer license	2022-06-23	2022-07-01

3 Select the MSP Pack license, click **Actions**, and select **Activate**. The MSP menus can now unlock the MSP branding, Admins & teams, Cross-org synchronization, and MSP alerts features (see Chapter 14 on page 741 for details on the MSP menus).

3.16 Configure CNP/CNP Plus Security Services

Different features are enabled depending on the type of trial license you purchased.

If you activate the CNP trial license, only the IP reputation filter is enabled. If you activate the CNP Plus trial license, IP reputation filter and application visibility & optimization are enabled.

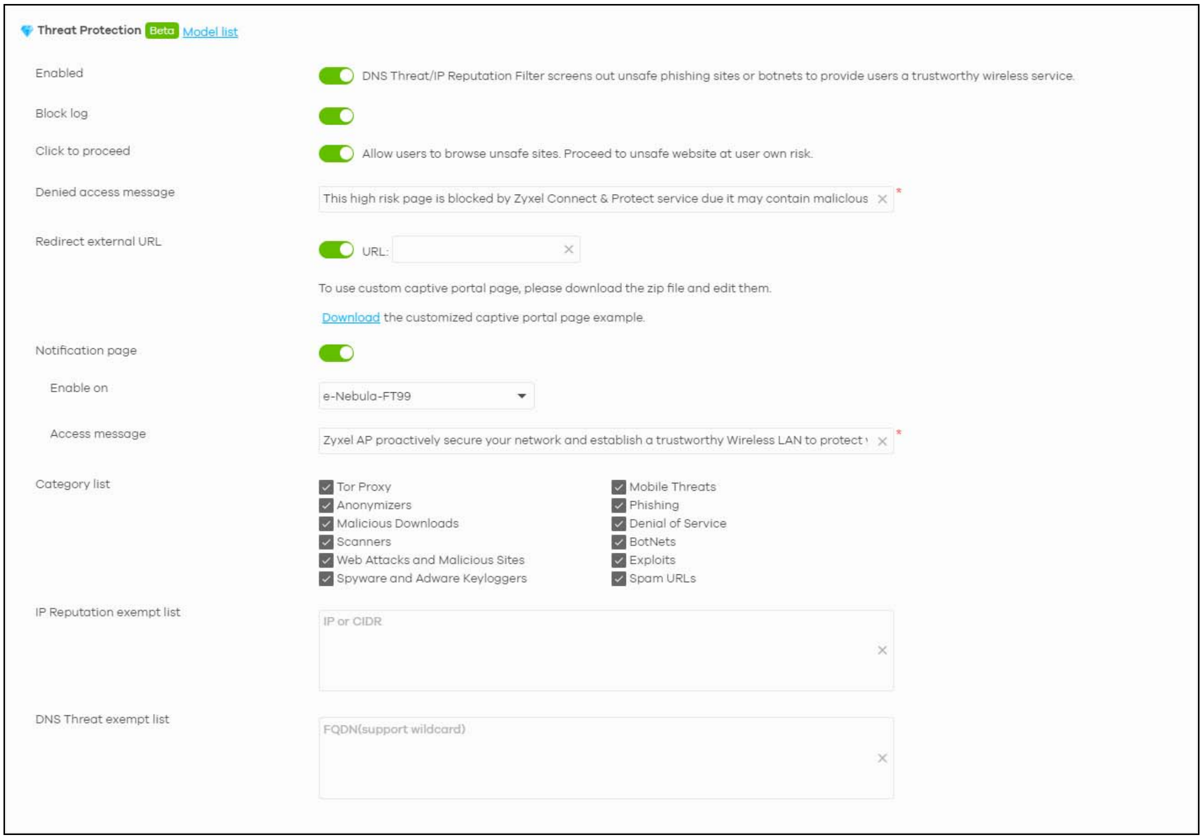
3.16.1 Threat Protection

An IP address with a bad reputation is an IP address associated with suspicious activities, such as spam, virus, and phishing. These are stored in a database. IP reputation checks the reputation of an IPv4 (only) IP address from the database. When there are packets coming from an IPv4 address with bad reputation, you can set the Nebula Device to respond by blocking these packets. You can change the response action set in NCC. You can also configure an exempt list to allow packets from specific IP addresses regardless of their content rating.

Both the CNP/CNP Plus licenses enable the IP reputation filter feature. To configure IP reputation filter, do the following:

1 Go to **Site-wide** > **Configure** > **Access points** > **Security service**.

2 Refer to Section 5.3.6 on page 341 for details on how to configure the **Threat Protection** fields.



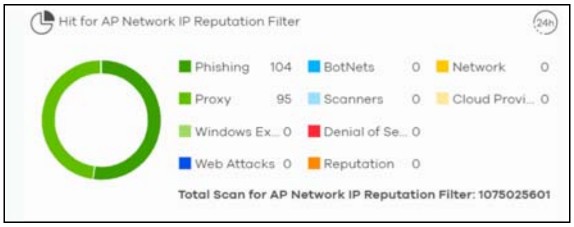
Threat Protection Beta Model list

Enabled	● DNS Threat/IP Reputation Filter screens out unsafe phishing sites or botnets to provide users a trustworthy wireless service.
Block log	●
Click to proceed	● Allow users to browse unsafe sites. Proceed to unsafe website at user own risk.
Denied access message	This high risk page is blocked by Zyxel Connect & Protect service due it may contain malicious × *
Redirect external URL	● URL: ×
	To use custom captive portal page, please download the zip file and edit them.
	Download the customized captive portal page example.
Notification page	●
Enable on	e-Nebula-FT99 ▾
Access message	Zyxel AP proactively secure your network and establish a trustworthy Wireless LAN to protect × *
Category list	☑ Tor Proxy ☑ Anonymizers ☑ Malicious Downloads ☑ Scanners ☑ Web Attacks and Malicious Sites ☑ Spyware and Adware Keyloggers ☑ Mobile Threats ☑ Phishing ☑ Denial of Service ☑ BotNets ☑ Exploits ☑ Spam URLs
IP Reputation exempt list	IP or CIDR ×
DNS Threat exempt list	FQDN(support wildcard) ×

3 Then click **Save**.

Go to **Site-wide** > **Dashboard**: **Hit for Threat Protection by CNP Service** to view the following:

- total number of times packets coming from an IPv4 address with a bad reputation occur, and
- the number of times connection attempts to an IPv4 address with a bad reputation occur.



3.16.2 Application Visibility & Optimization

Application visibility provides a way for a Nebula-managed Access Point to manage applications in WiFi network. It can detect the type of applications used by WiFi clients and how much bandwidth they use.

Application optimization is a way to limit the bandwidth usage of applications in the WiFi network. For example, applications that need real time traffic such as video streaming may use more resources. Use application optimization to limit the bandwidth used to stream video to prevent it from slowing down your WiFi network. Application optimization limits the applications bandwidth usage by their categories. You can manage and view the applications and their categories in **Site-wide** > **Applications usage** > **Application View by Access Point**.

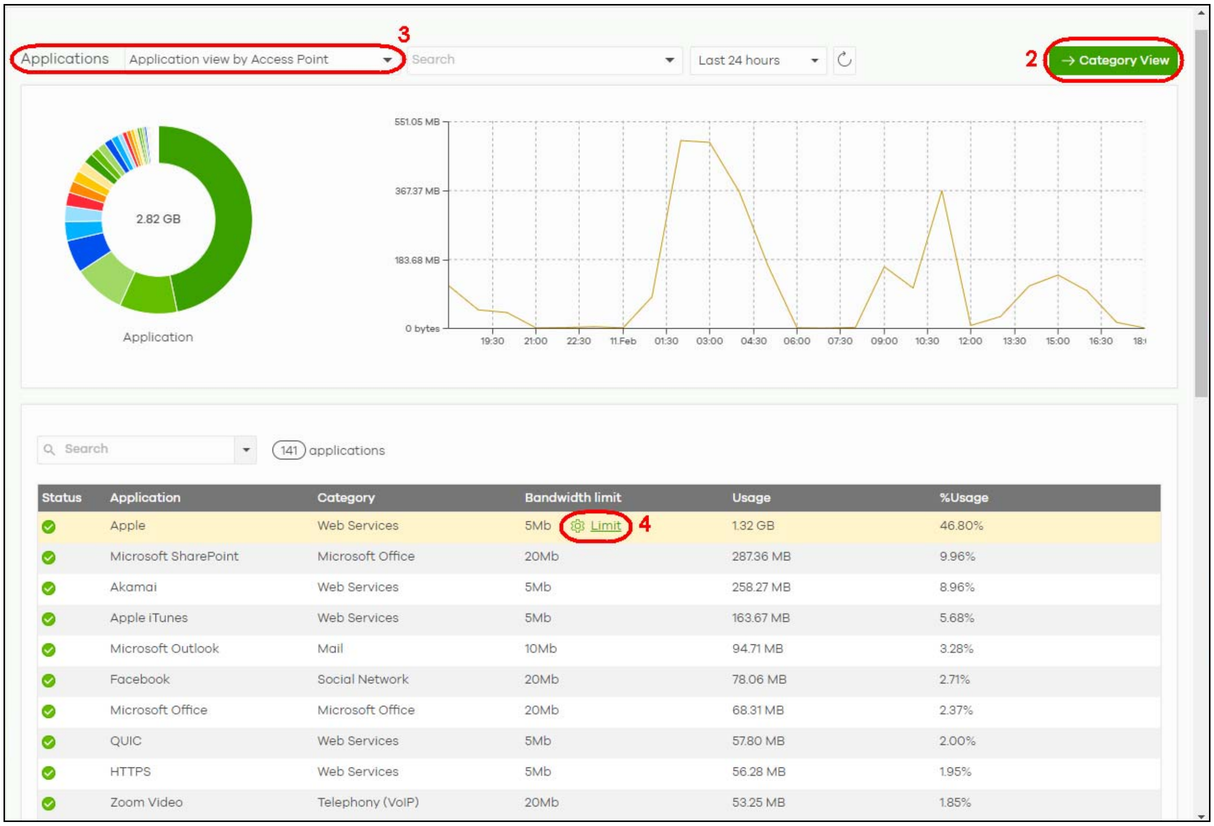
You need to purchase the CNP Plus license to enable application visibility & optimization. To configure application visibility & optimization, do the following:

1 Go to **Site-wide** > **Applications usage**.

2 Make sure you are in **Application View** (**--> Category View** is displayed)

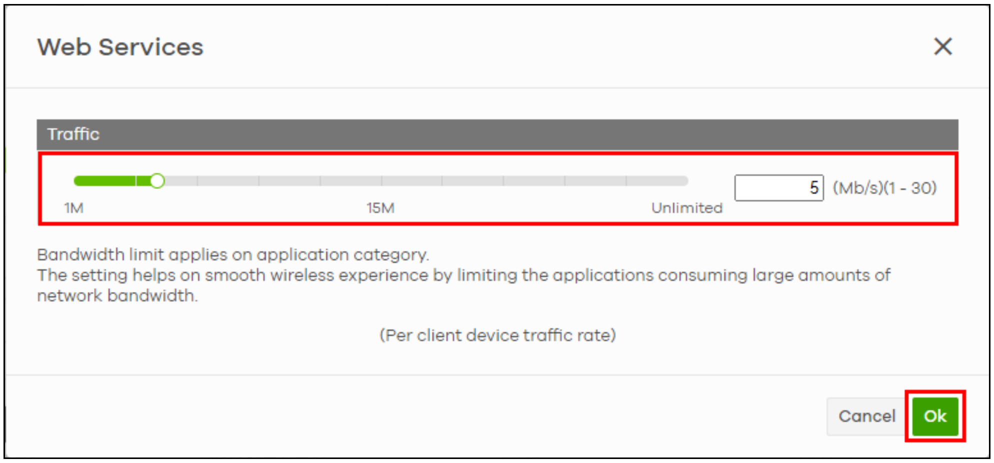
3 Select **Application View by Access Point** in the **Applications** field.

4 Hover the mouse pointer anywhere on an application row. Click the **Limit** icon to set its **Bandwidth limit**.



Status	Application	Category	Bandwidth limit	Usage	%Usage
✓	Apple	Web Services	5Mb Limit	1.32 GB	46.80%
✓	Microsoft SharePoint	Microsoft Office	20Mb	287.36 MB	9.96%
✓	Akamai	Web Services	5Mb	258.27 MB	8.96%
✓	Apple iTunes	Web Services	5Mb	163.67 MB	5.68%
✓	Microsoft Outlook	Mail	10Mb	94.71 MB	3.28%
✓	Facebook	Social Network	20Mb	78.06 MB	2.71%
✓	Microsoft Office	Microsoft Office	20Mb	68.31 MB	2.37%
✓	QUIC	Web Services	5Mb	57.80 MB	2.00%
✓	HTTPS	Web Services	5Mb	56.28 MB	1.95%
✓	Zoom Video	Telephony (VoIP)	20Mb	53.25 MB	1.85%

5 Use the slider or enter the **Traffic** allowed in **Mb/s** (**1** – **30** or **Unlimited**).



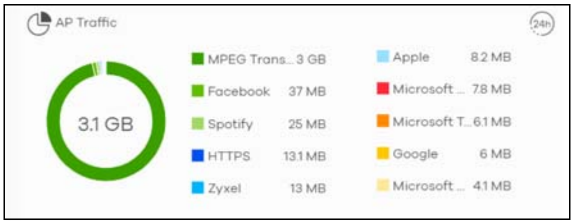
5 (Mb/s)(1 - 30)

Bandwidth limit applies on application category.
The setting helps on smooth wireless experience by limiting the applications consuming large amounts of network bandwidth.

(Per client device traffic rate)

6 Then click **Ok**.

To monitor the application bandwidth usage, go to **Site-wide** > **Dashboard**: **Access points application usage** to view the top ten applications that use the most bandwidth in the site.



3.17 Delete an Organization

Only the Organization owner can delete an Organization. An Organization can be deleted only when it has no site(s), administrator(s), user(s), license(s), or Nebula Device(s) in the Organization.

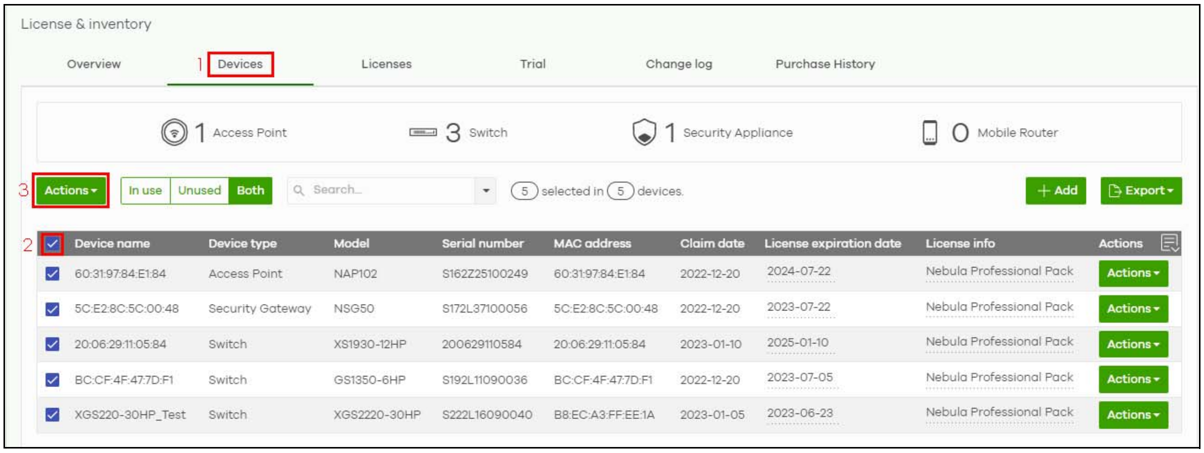
To delete an Organization from the NCC, do the following:

3.17.1 Remove All Nebula Devices

1 Go to **Organization-wide** > **License & inventory** > **Devices** tab (1).

2 Click the checkbox (2) to select all Nebula Devices.

3 Click the **Actions** button (3).

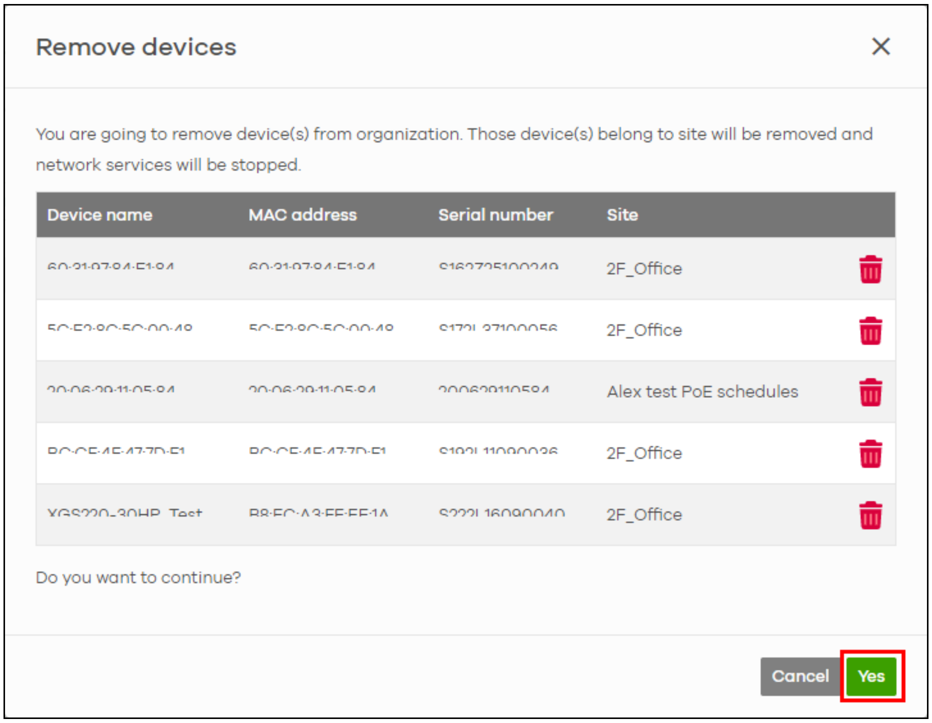


5 selected in 5 devices.

☑	Device name	Device type	Model	Serial number	MAC address	Claim date	License expiration date	License info	Actions
☑	60:31:97:84:E1:84	Access Point	NAP102	S162Z25100249	60:31:97:84:E1:84	2022-12-20	2024-07-22	Nebula Professional Pack	Actions
☑	5C:E2:8C:5C:00:48	Security Gateway	NSG50	S172L37100056	5C:E2:8C:5C:00:48	2022-12-20	2023-07-22	Nebula Professional Pack	Actions
☑	20:06:29:11:05:84	Switch	XS1930-12HP	200629110584	20:06:29:11:05:84	2023-01-10	2025-01-10	Nebula Professional Pack	Actions
☑	BC:CF:4F:47:7D:F1	Switch	GS1350-6HP	S192L11090036	BC:CF:4F:47:7D:F1	2022-12-20	2023-07-05	Nebula Professional Pack	Actions
☑	XGS220-30HP_Test	Switch	XGS2220-30HP	S222L16090040	B8:EC:A3:FF:EE:1A	2023-01-05	2023-06-23	Nebula Professional Pack	Actions

4 Click **Remove from organization**.

5 Click the **Yes** button to confirm, or click the delete icon to remove each devices individually.



You are going to remove device(s) from organization. Those device(s) belong to site will be removed and network services will be stopped.

Device name	MAC address	Serial number	Site
60:31:97:84:E1:84	60:31:97:84:E1:84	S162Z25100249	2F_Office
5C:E2:8C:5C:00:48	5C:E2:8C:5C:00:48	S172L37100056	2F_Office
20:06:29:11:05:84	20:06:29:11:05:84	200629110584	Alex test PoE schedules
BC:CF:4F:47:7D:F1	BC:CF:4F:47:7D:F1	S192L11090036	2F_Office
XGS220-30HP_Test	B8:EC:A3:FF:EE:1A	S222L16090040	2F_Office

Do you want to continue?

3.17.2 Transfer All Licenses

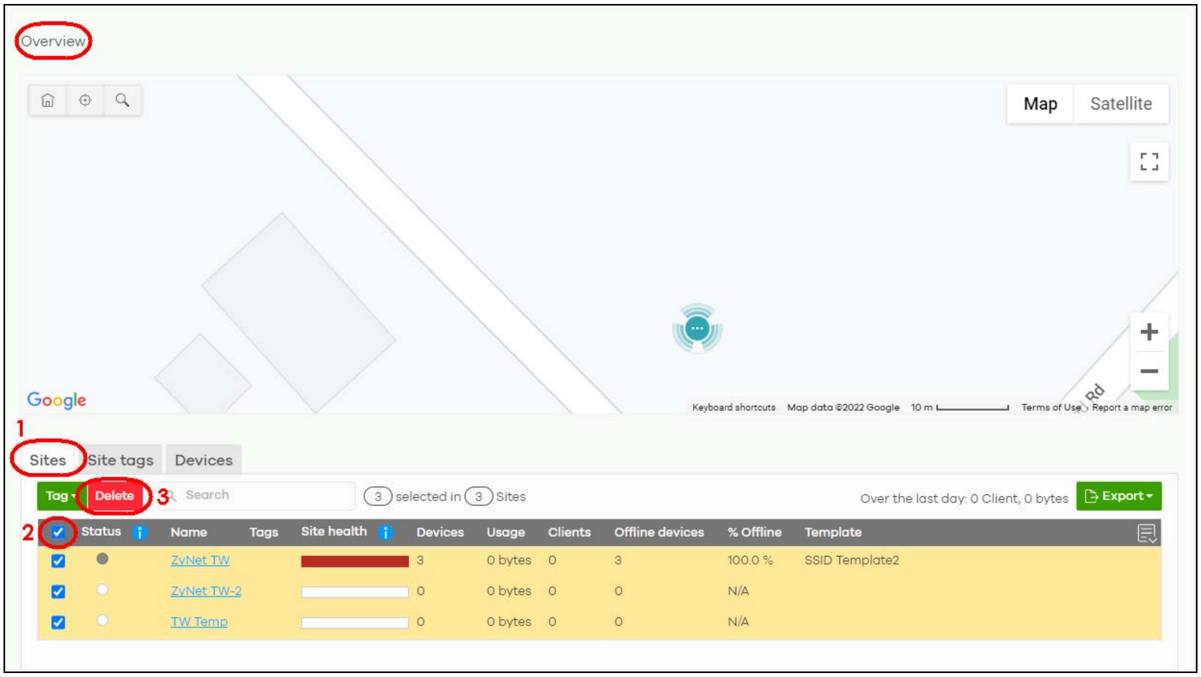
See Section 3.7 on page 82 in this chapter for information on how to transfer licenses assigned to an organization and Nebula Device to another Nebula Device in a different organization.

3.17.3 Delete All Sites

1 Go to **Organization-wide** > **Organization-wide manage** > **Organization portal** > **Sites** tab (1).

2 Click the checkbox (2) to select all sites.

3 Click the **Delete** button (3) to remove all sites.

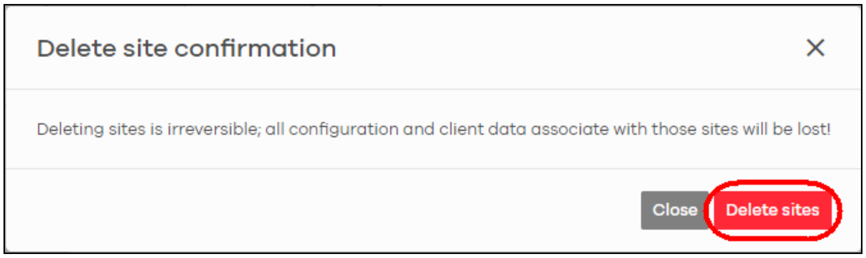


3 selected in 3 Sites

Over the last day: 0 Client, 0 bytes

☑	Status	Name	Tags	Site health	Devices	Usage	Clients	Offline devices	% Offline	Template
☑	●	ZyNet TW			3	0 bytes	0	3	100.0 %	SSID Template2
☑	○	ZyNet TW-2			0	0 bytes	0	0	N/A	
☑	○	TW Temp			0	0 bytes	0	0	N/A	

4 Click the **Delete sites** button to confirm.



Delete site confirmation

Deleting sites is irreversible; all configuration and client data associate with those sites will be lost!

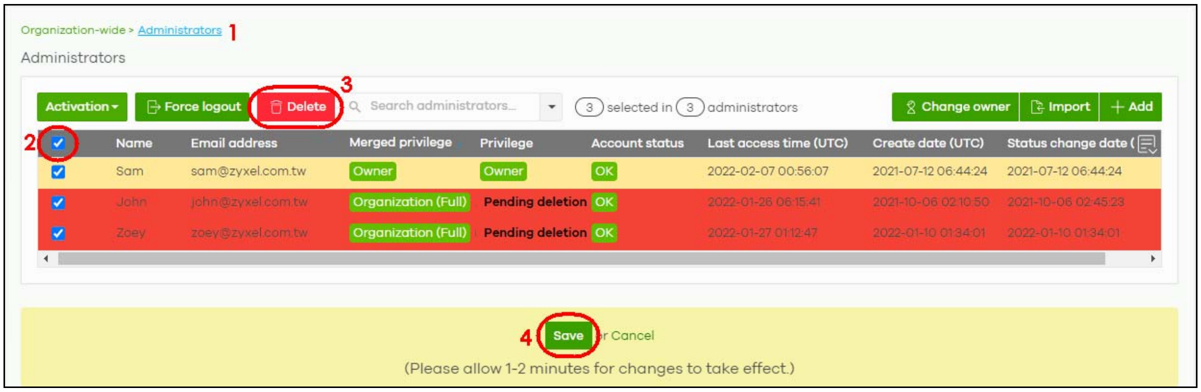
3.17.4 Delete All Administrators

1 Go to **Organization-wide** > **Administrators** (1).

2 Click the checkbox to select all administrators (2).

3 Click the **Delete** button (3).

4 Click the **Save** button (4) to confirm.



Organization-wide > Administrators

Administrators

3 selected in 3 administrators

☑	Name	Email address	Merged privilege	Privilege	Account status	Last access time (UTC)	Create date (UTC)	Status change date (
☑	Sam	sam@zyxel.com.tw	Owner	Owner	OK	2022-02-07 00:56:07	2021-07-12 06:44:24	2021-07-12 06:44:24
☑	John	john@zyxel.com.tw	Organization (Full)	Pending deletion	OK	2022-01-26 06:15:41	2021-10-06 02:10:50	2021-10-06 02:45:23
☑	Zoey	zoey@zyxel.com.tw	Organization (Full)	Pending deletion	OK	2022-01-27 01:12:47	2022-01-10 01:34:01	2022-01-10 01:34:01

(Please allow 1-2 minutes for changes to take effect.)

3.17.5 Remove All Users

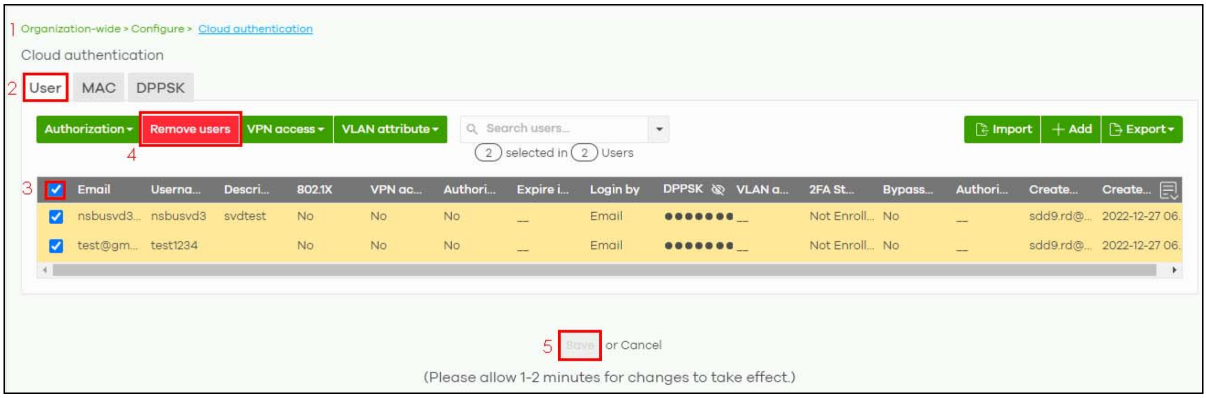
1 Go to **Organization-wide** > **Organization-wide manage** > **Cloud authentication** (1).

2 Select the **User** tab (2).

3 Click the checkbox to select all users (3).

4 Click the **Remove users** button (4).

5 Click the **Save** button (5) to confirm.



Organization-wide > Configure > Cloud authentication

Cloud authentication

2 selected in 2 Users

☑	Email	Userna...	Descri...	802.1X	VPN ac...	Authori...	Expire i...	Login by	DPPSK	VLAN a...	2FA St...	Bypass...	Authori...	Create...	Create...
☑	nsbusvd3...	nsbusvd3	svdtest	No	No	No	__	Email	●●●●●●●	__	Not Enroll...	No	__	sdd9.rd@...	2022-12-27 06.
☑	test@gm...	test1234		No	No	No	__	Email	●●●●●●●	__	Not Enroll...	No	__	sdd9.rd@...	2022-12-27 06.

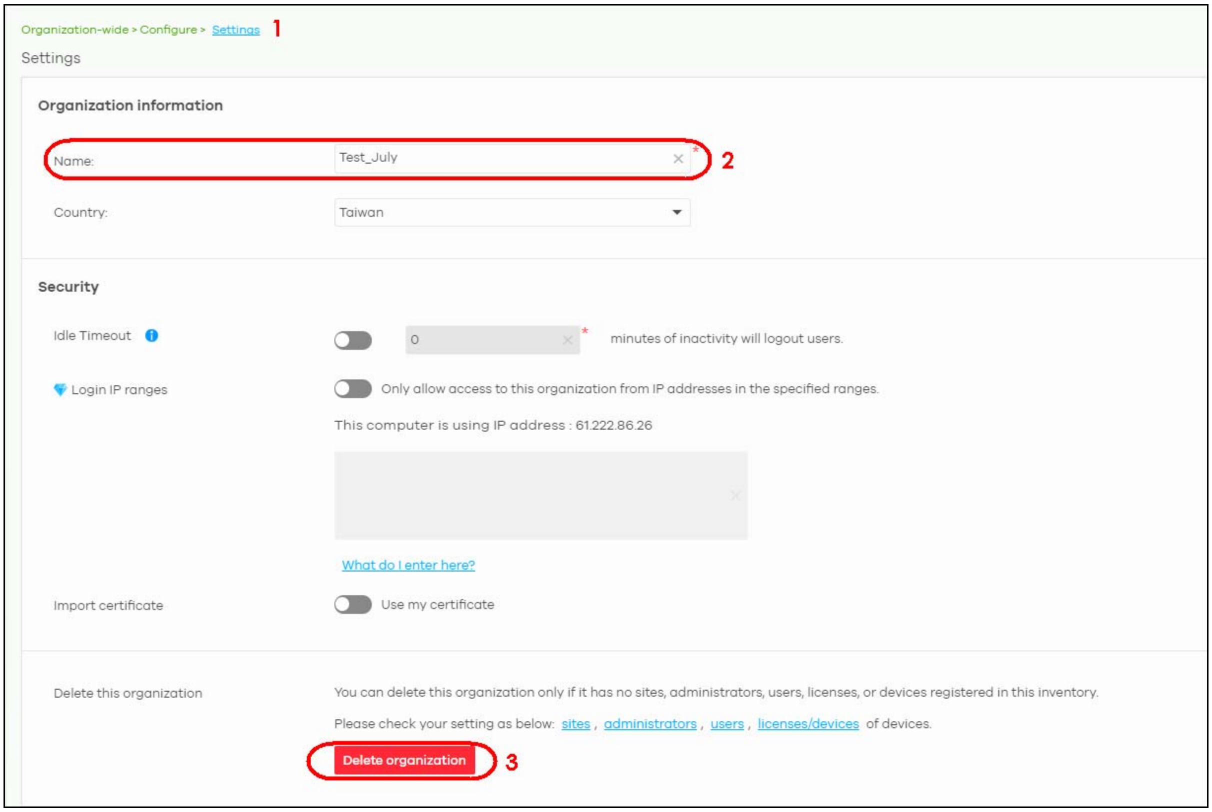
(Please allow 1-2 minutes for changes to take effect.)

3.17.6 Delete the Organization

1 Go to **Organization-wide** > **Organization-wide manage** > **Organization settings** (1).

2 Enter the **Name** of the organization you wish to remove (2).

3 Click the **Delete organization** button (3).



Organization-wide > Configure > Settings

Settings

Organization information

Name: Test_July

Country: Taiwan

Security

Idle Timeout: 0 minutes of inactivity will logout users.

Login IP ranges: Only allow access to this organization from IP addresses in the specified ranges.

This computer is using IP address : 61.222.86.26

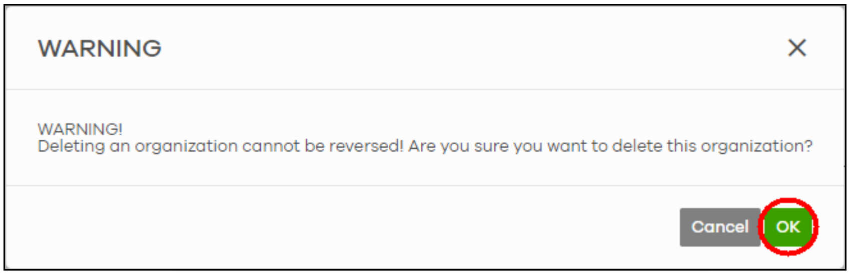
What do I enter here?

Import certificate: Use my certificate

Delete this organization: You can delete this organization only if it has no sites, administrators, users, licenses, or devices registered in this inventory.

Please check your setting as below: sites , administrators , users , licenses/devices of devices.

4 Click the **OK** button to confirm.

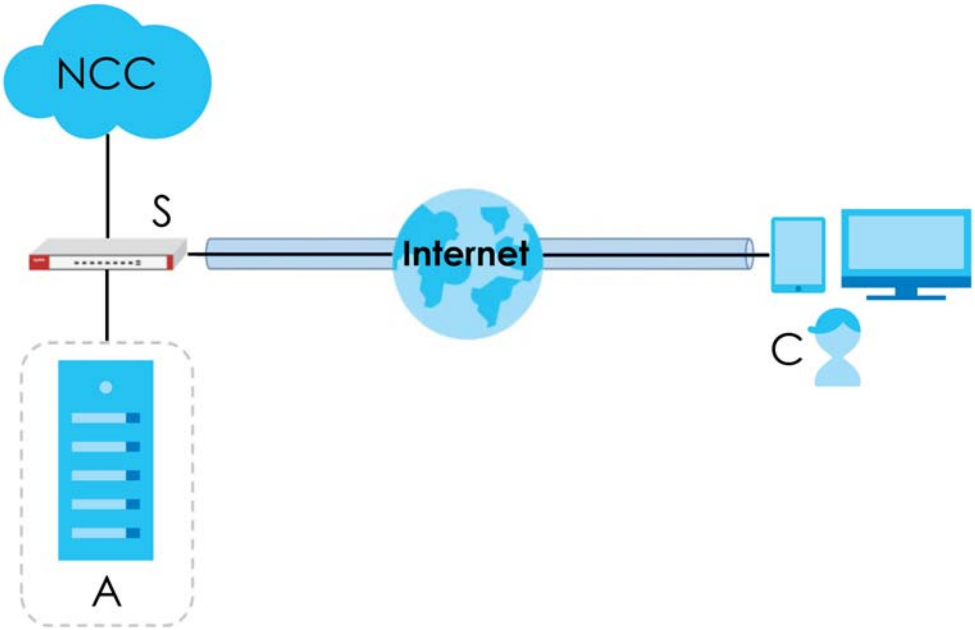


WARNING

WARNING!
Deleting an organization cannot be reversed! Are you sure you want to delete this organization?

3.18 Remote Access VPN Setup

The following figure illustrates a secure VPN channel configured through NCC. The VPN client (C) remotely accesses the office server (A) through the Nebula Device (S) in a typical work from home scenario.



To set up a remote access VPN on Nebula, do the following:

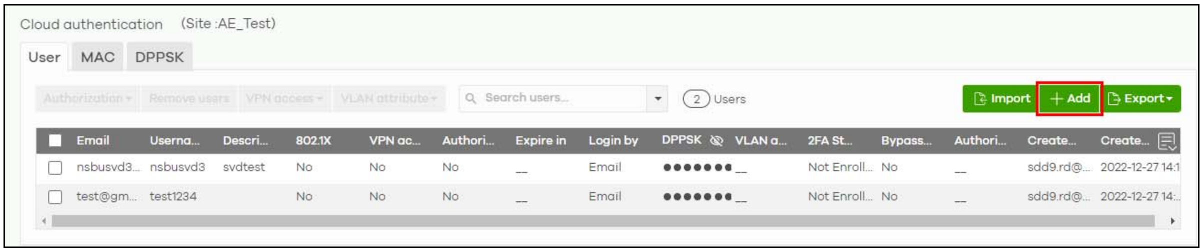
- Create a VPN user
- Enable the remote access VPN rule for IPSec VPN client
- Check the connection in Nebula.

The user needs to do the following:

- Set up the VPN using Zyxel's SecuExtender (only), a VPN client software
- Import the VPN configuration file
- Open the VPN tunnel
- Set up two Factor Authentication on a mobile device to bind the user account.

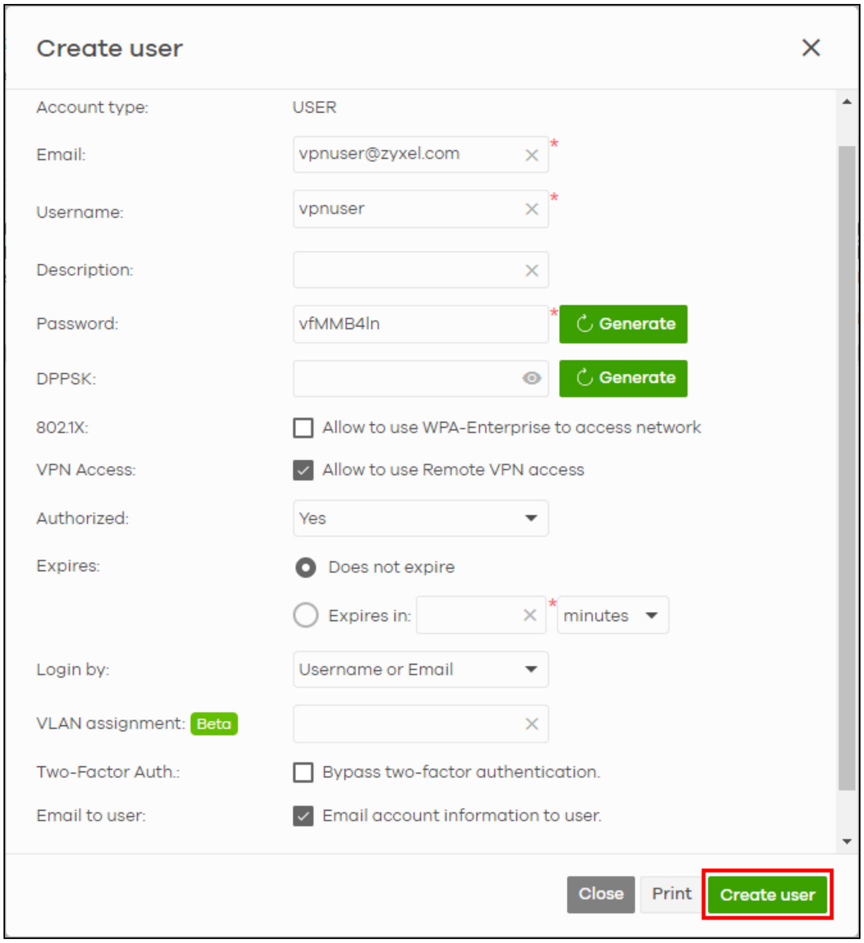
3.18.1 Create a VPN User

1 Go to the **Site-wide** > **Configure** > **Cloud authentication** screen. Click **+Add** to create a user.



□	Email	Userna...	Descri...	802.1X	VPN ac...	Authori...	Expire in	Login by	DPPSK	VLAN a...	2FA St...	Bypass...	Authori...	Create...	Create...
□	nsbusvd3...	nsbusvd3	svdtest	No	No	No	_	Email	●●●●●●●	_	Not Enroll...	No	_	sdd9.rd@...	2022-12-27 14:1
□	test@gm...	test1234		No	No	No	_	Email	●●●●●●●	_	Not Enroll...	No	_	sdd9.rd@...	2022-12-27 14:...

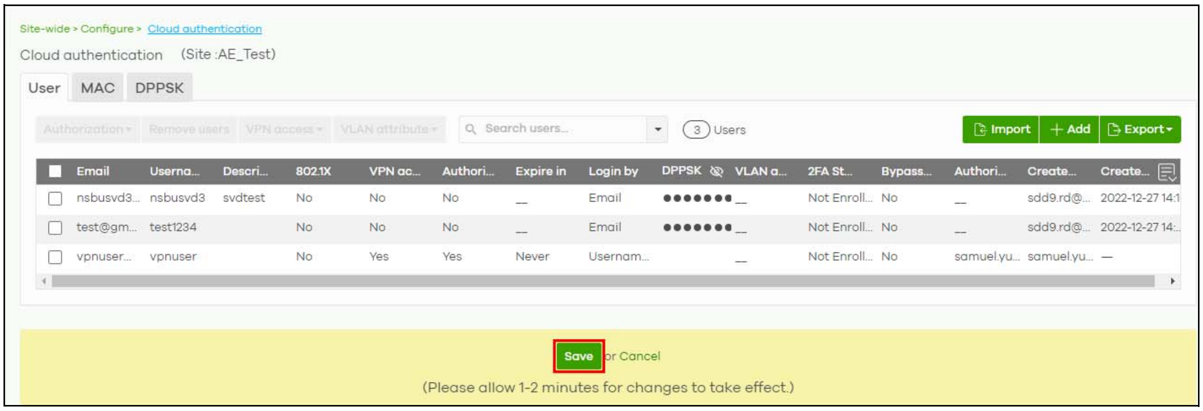
2 Enter an **Email**, **Username**, generate or enter a **Password** (4 – 31 characters, including 0–9 a–z A–Z `~!@#$%&*(_+-={} | [];'"./<> ?). Click **Allow to use Remote VPN access**. Click **Does not expire** to set no time limit for this user account. Select **Username or Email** in **Login by**. Click to select **Email account information to user**. Then click **Create user**.



Create user

Account type:	USER
Email:	vpnuser@zyxel.com *
Username:	vpnuser *
Description:	
Password:	vfMMB4ln *
DPPSK:	
802.1X:	□ Allow to use WPA-Enterprise to access network
VPN Access:	☑ Allow to use Remote VPN access
Authorized:	Yes
Expires:	● Does not expire ○ Expires in: * minutes
Login by:	Username or Email
VLAN assignment: Beta	
Two-Factor Auth.:	□ Bypass two-factor authentication.
Email to user:	☑ Email account information to user.

3 Click **Save**.



Site-wide > Configure > Cloud authentication

Cloud authentication (Site :AE_Test)

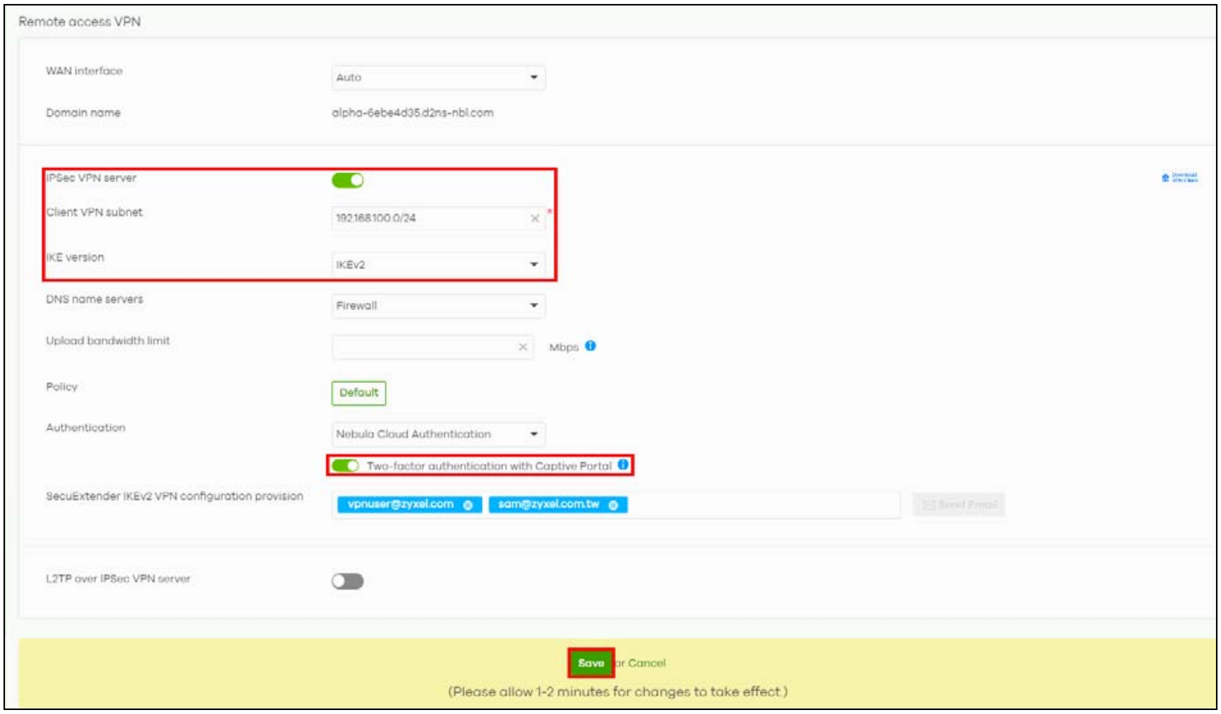
□	Email	Userna...	Descri...	802.1X	VPN ac...	Authori...	Expire in	Login by	DPPSK	VLAN a...	2FA St...	Bypass...	Authori...	Create...	Create...
□	nsbusvd3...	nsbusvd3	svdtest	No	No	No	_	Email	●●●●●●●	_	Not Enroll...	No	_	sdd9.rd@...	2022-12-27 14:1
□	test@gm...	test1234		No	No	No	_	Email	●●●●●●●	_	Not Enroll...	No	_	sdd9.rd@...	2022-12-27 14:...
□	vpnuser...	vpnuser		No	Yes	Yes	Never	Usernam...		_	Not Enroll...	No	samuel.yu...	samuel.yu...	—

(Please allow 1-2 minutes for changes to take effect.)

3.18.2 Enable the Remote Access VPN Rule for IPSec VPN Client

1 Go to the **Site-wide** > **Configure** > **Firewall** > **Remote access VPN** screen. Click **IPSec VPN server** to enable VPN. Enter the IP address range in **Client VPN subnet**. Select **IKEv2** in **IKE version**.

Click **Two-factor authentication with Captive Portal** to enable two-factor authentication with the Google authenticator app. The VPN client will be asked to provide a Google authenticator verification code, so must install the Google Authenticator app. Then click **Save**.



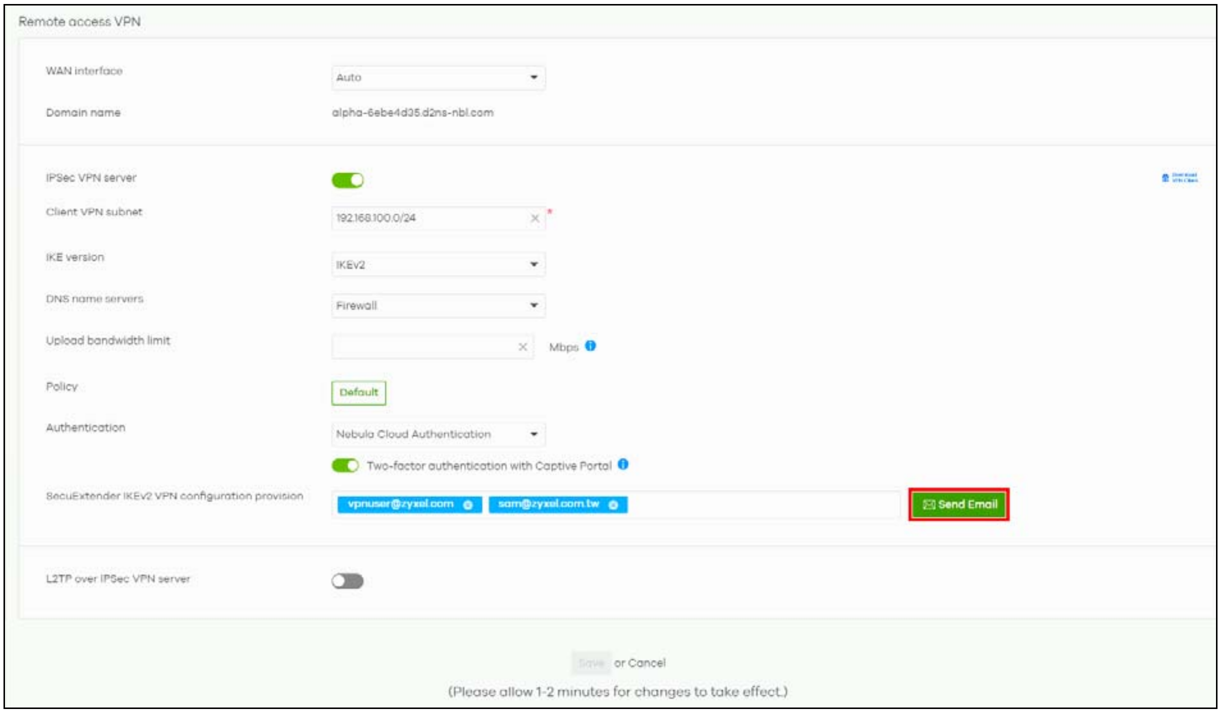
Remote access VPN

WAN interface	Auto
Domain name	alpha-6ebe4d35.d2ns-nbl.com
IPSec VPN server	●
Client VPN subnet	192.168.100.0/24
IKE version	IKEv2
DNS name servers	Firewall
Upload bandwidth limit	Mbps
Policy	Default
Authentication	Nebula Cloud Authentication
	● Two-factor authentication with Captive Portal
SecuExtender IKEv2 VPN configuration provision	vpnuser@zyxel.com, sam@zyxel.com.tw Send Email
L2TP over IPSec VPN server	○

Save or Cancel

(Please allow 1-2 minutes for changes to take effect.)

2 Click **Send Email** to give your VPN client the configuration instructions through email.



Remote access VPN

WAN interface	Auto
Domain name	alpha-6ebe4d35.d2ns-nbl.com
IPSec VPN server	●
Client VPN subnet	192.168.100.0/24
IKE version	IKEv2
DNS name servers	Firewall
Upload bandwidth limit	Mbps
Policy	Default
Authentication	Nebula Cloud Authentication
	● Two-factor authentication with Captive Portal
SecuExtender IKEv2 VPN configuration provision	vpnuser@zyxel.com, sam@zyxel.com.tw Send Email
L2TP over IPSec VPN server	○

Save or Cancel

(Please allow 1-2 minutes for changes to take effect.)

3.18.3 VPN Setup by the VPN Client

1 The VPN client should receive the following emails:

- **Configuration for SecuExtender IPSec VPN Client** email with attached VPN configuration file (.tgb). Save the configuration file in your computer.
- **Nebula Cloud Account Information** email with the following login information: **Email**, **Username**, **Password**, and **Expired time** (validity = **NEVER**).

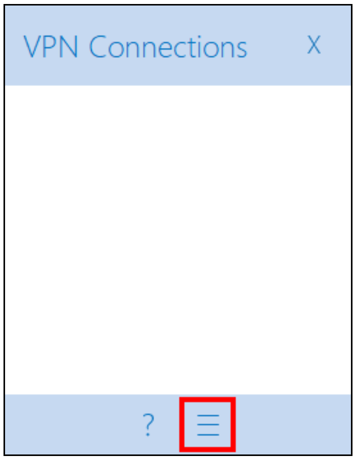
2 Click the link in the **Configuration for SecuExtender IPSec VPN Client** email for instructions on installing the SecuExtender and activating the license key. The **How to activate SecuExtender license key after your online purchase** webpage appears.

- Click **Download**.
- Select the SecuExtender app based on your computer's operating system to install it.
- Follow the online prompts to activate the SecuExtender license.

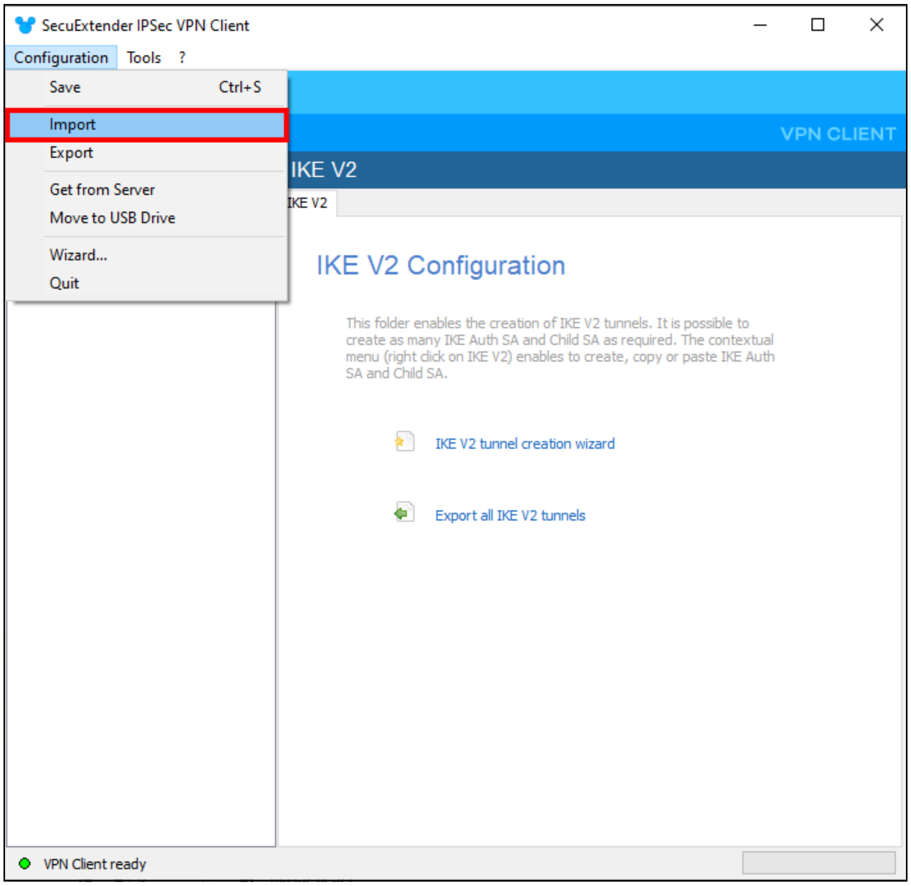
3.18.4 Import the VPN Configuration File

1 Save the attached VPN configuration file (.tgb) from the **Configuration for SecuExtender IPSec VPN Client** email on the VPN user's computer.

2 On your computer, open SecuExtender. Click the menu icon.

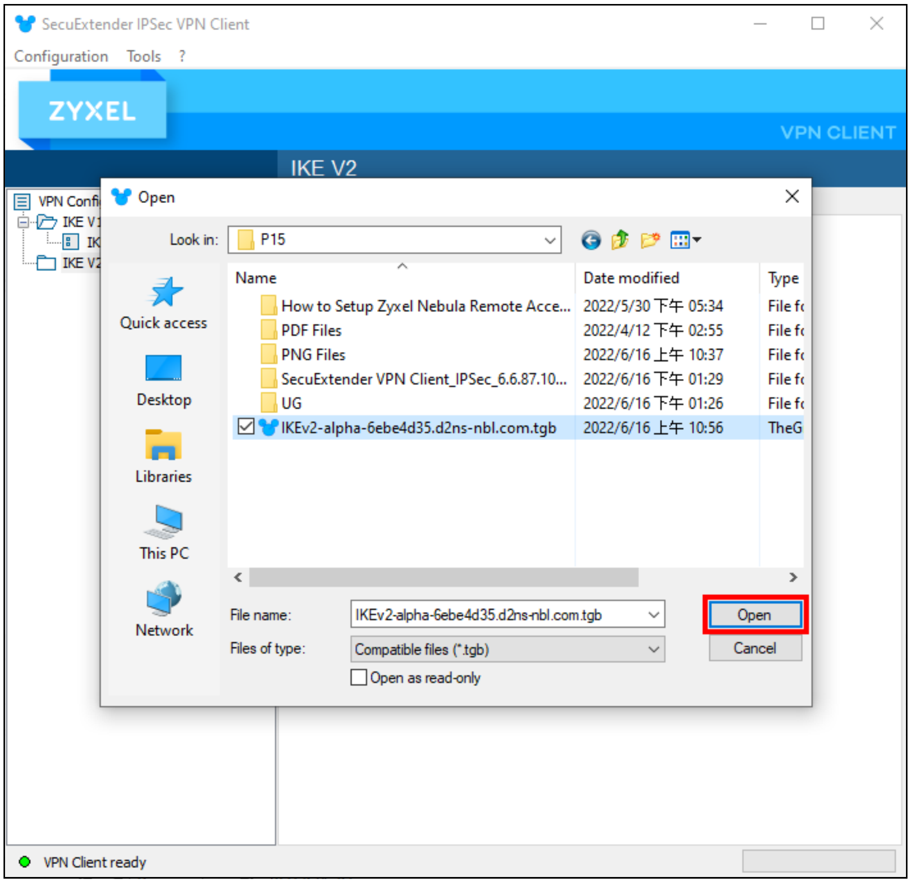


3 Click **Configuration** > **Import**.



This folder enables the creation of IKE V2 tunnels. It is possible to create as many IKE Auth SA and Child SA as required. The contextual menu (right click on IKE V2) enables to create, copy or paste IKE Auth SA and Child SA.

4 Locate in your computer and click **Open** to import the VPN configuration file from the Configuration for SecuExtender IPSec VPN Client email.



Look in: P15

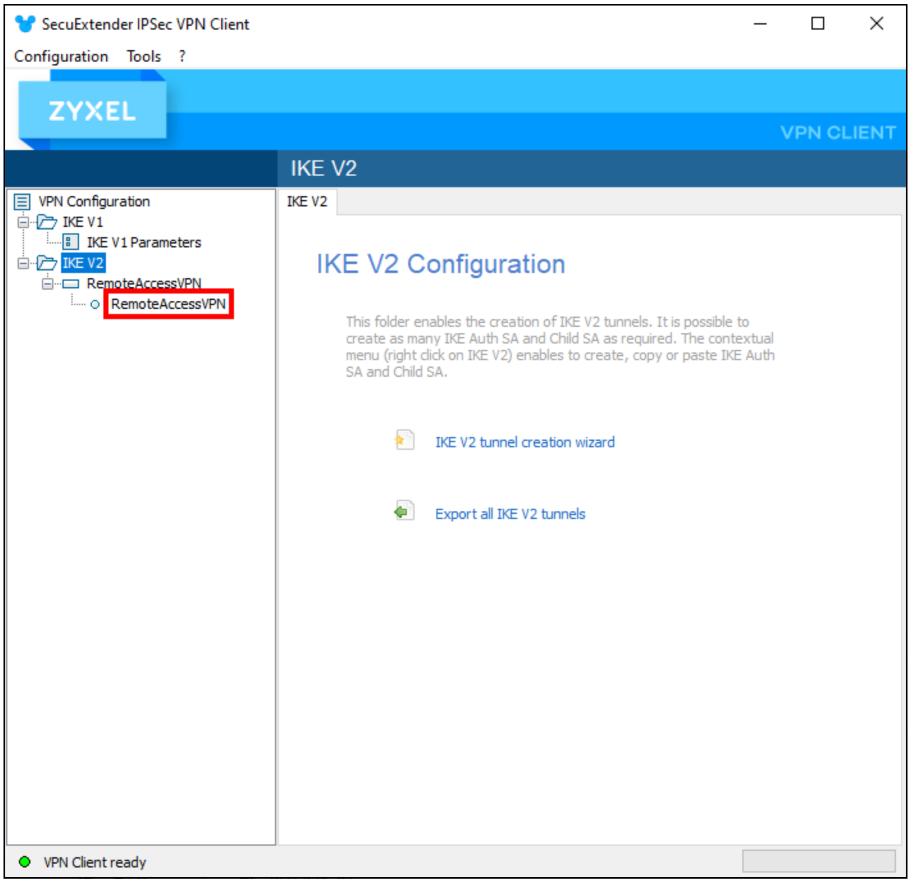
Name	Date modified	Type
How to Setup Zyxel Nebula Remote Acce...	2022/5/30 下午 05:34	File fo
PDF Files	2022/4/12 下午 02:55	File fo
PNG Files	2022/6/16 上午 10:37	File fo
SecuExtender VPN Client_IPSec_6.6.87.10...	2022/6/16 下午 01:29	File fo
UG	2022/6/16 下午 01:26	File fo
☑ IKEv2-alpha-6ebe4d35.d2ns-nbl.com.tgb	2022/6/16 上午 10:56	TheG

File name: IKEv2-alpha-6ebe4d35.d2ns-nbl.com.tgb

Files of type: Compatible files (*.tgb)

□ Open as read-only

5 Click **RemoteAccessVPN** in **VPN Configuration** > **IKE V2** > **RemoteAccessVPN**.

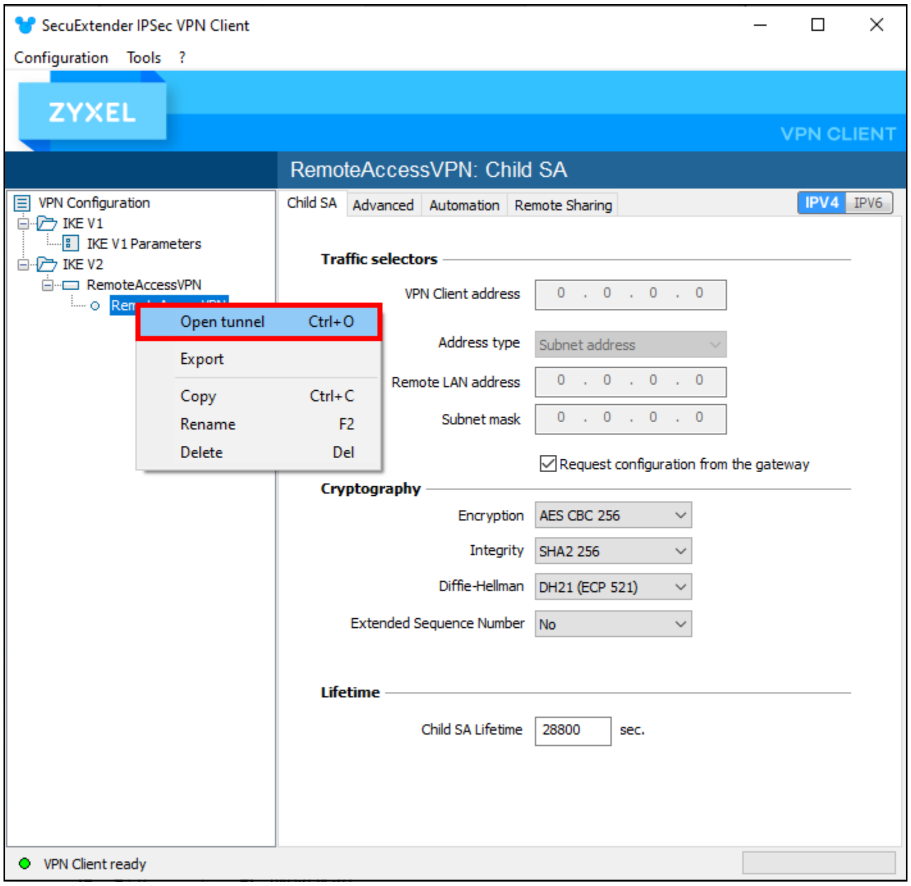


IKE V2 Configuration

This folder enables the creation of IKE V2 tunnels. It is possible to create as many IKE Auth SA and Child SA as required. The contextual menu (right click on IKE V2) enables to create, copy or paste IKE Auth SA and Child SA.

3.18.5 Open the VPN Tunnel

1 Right-click **RemoteAccessVPN** in **VPN Configuration** > **IKE V2** > **RemoteAccessVPN** and click **Open tunnel**.



RemoteAccessVPN: Child SA

Traffic selectors

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 0 . 0 . 0 . 0

Subnet mask: 0 . 0 . 0 . 0

☑ Request configuration from the gateway

Cryptography

Encryption: AES CBC 256

Integrity: SHA2 256

Diffie-Hellman: DH21 (ECP 521)

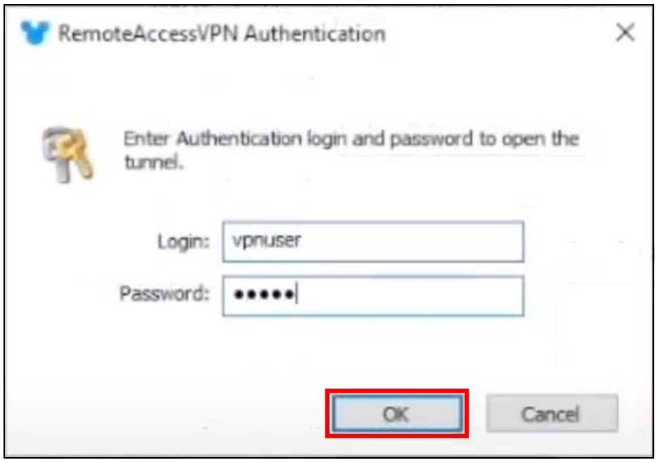
Extended Sequence Number: No

Lifetime

Child SA Lifetime: 28800 sec.

VPN Client ready

2 On the next screen, enter the **Login: Username** and **Password** from the **Nebula Cloud Account Information** email. Then click **OK**.



Enter Authentication login and password to open the tunnel.

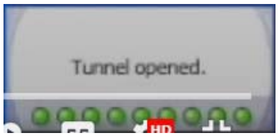
Login: vpnuser

Password: •••••

IKEV2 Auth sent will appear on the lower right of the screen.

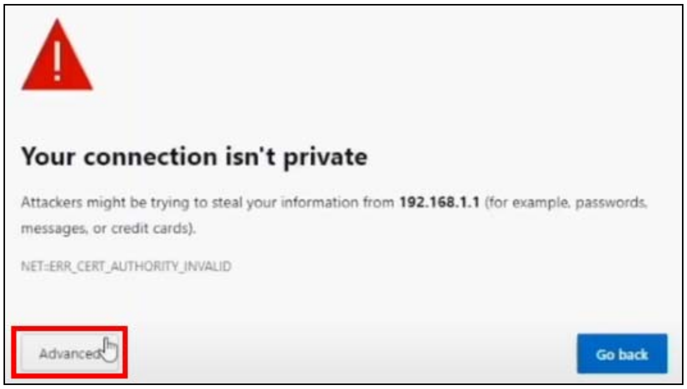
IKE V2 Auth sent

Wait until **Tunnel opened** appears on the lower right of the screen.


Tunnel opened.

An IP address will now appear in **VPN Client address** to replace the previous **0.0.0.0**. The button lights green in front of **RemoteAccessVPN** in **VPN Configuration** > **IKE V2** > **RemoteAccessVPN**.

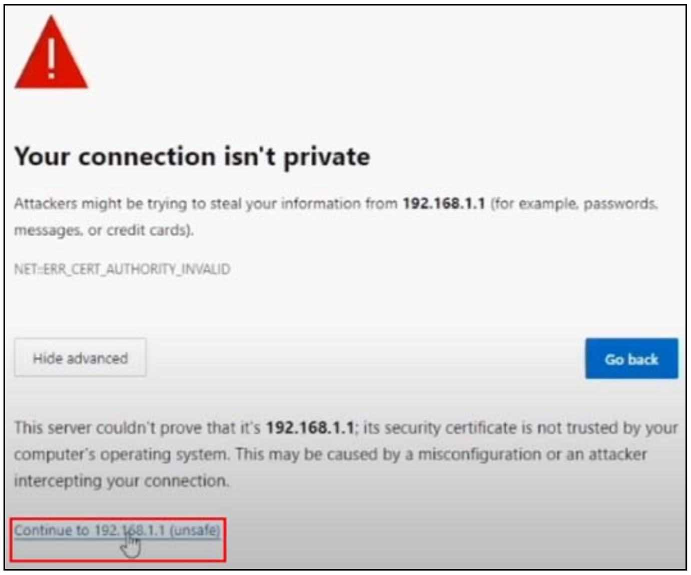
3 When **Your connection isn't private** appears on the web browser, click **Advanced** to continue.


Your connection isn't private

Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

4 Click the **Continue to xxx.xxx.x.x (unsafe)** link on the bottom of the screen.


Your connection isn't private

Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards).

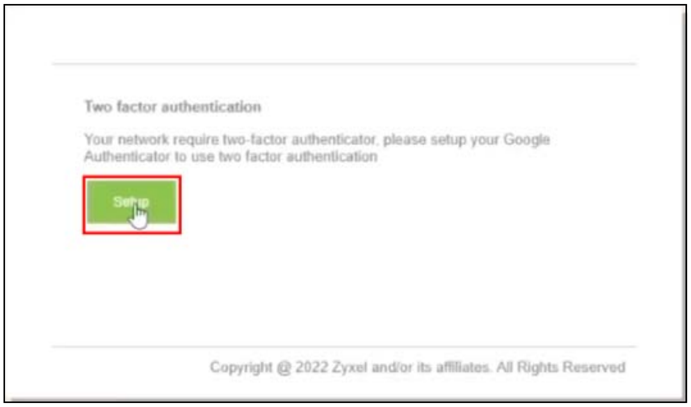
NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **192.168.1.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Continue to 192.168.1.1 (unsafe)

3.18.6 Set Up Two Factor Authentication to Bind the User Account

1 On the **Two factor authentication** screen, click **Setup**.

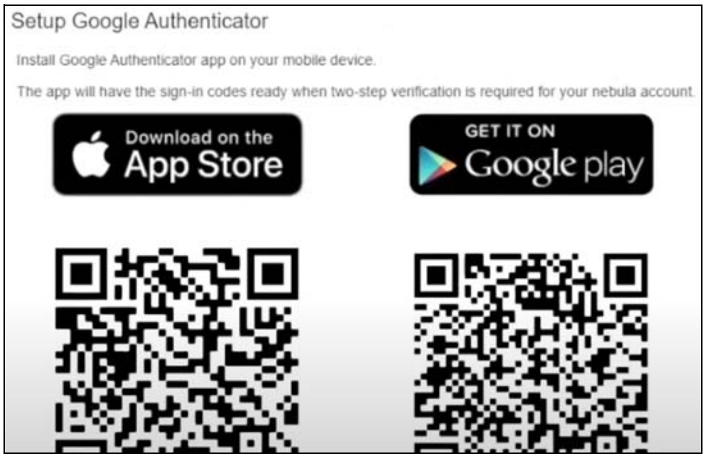


Two factor authentication

Your network require two-factor authenticator, please setup your Google Authenticator to use two factor authentication

Copyright @ 2022 Zyxel and/or its affiliates. All Rights Reserved

The prompt to download and install the **Google Authenticator** app on a mobile device appears. Install the **Google Authenticator** app. Then click **Next**.

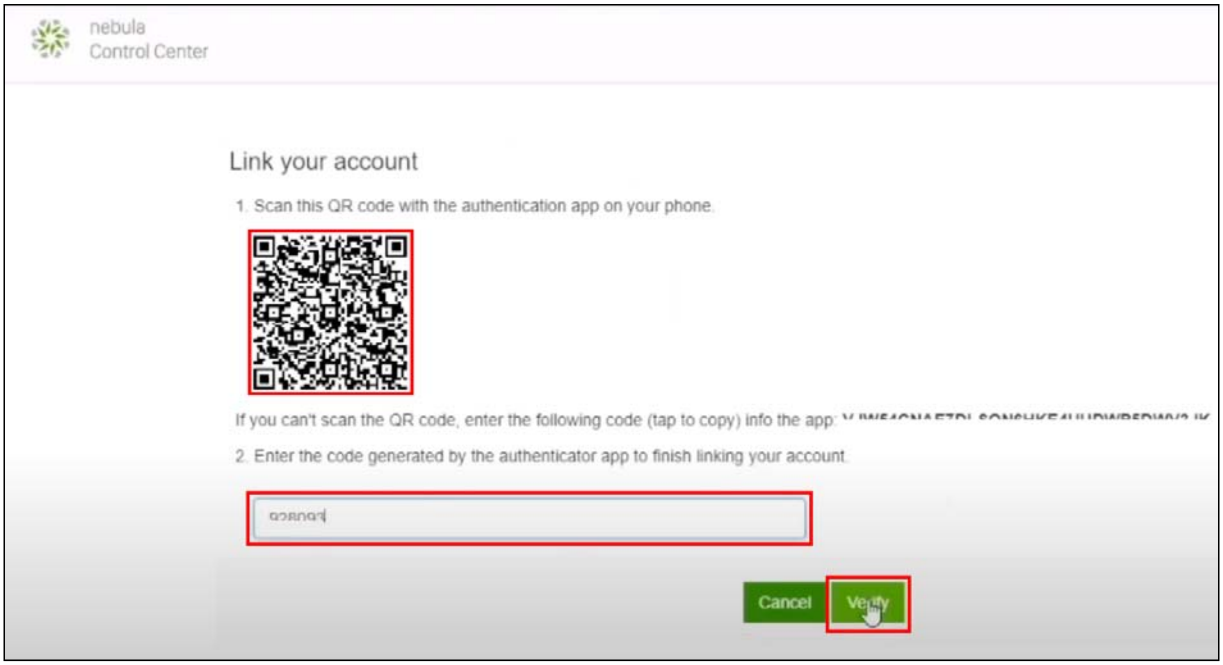


Setup Google Authenticator

Install Google Authenticator app on your mobile device.

The app will have the sign-in codes ready when two-step verification is required for your nebula account.

2 Use the **Google Authenticator** app to scan the QR code. The QR code contains the user account information created in step 2 of Create a VPN User. Enter the code. Then click **Verify**.



nebula Control Center

Link your account

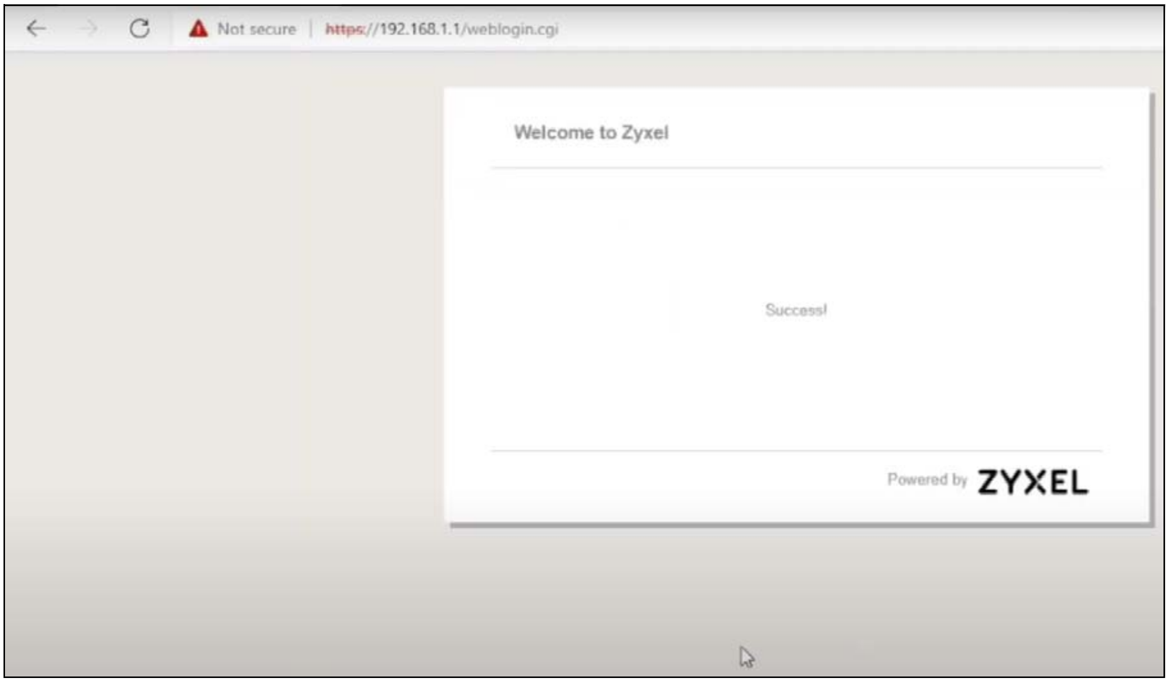
1. Scan this QR code with the authentication app on your phone.

If you can't scan the QR code, enter the following code (tap to copy) info the app:

2. Enter the code generated by the authenticator app to finish linking your account.

Note: Two Factor Authentication needs to be set up by the user only once. On the next login, just enter the Two Factor Authentication passcode.

The following screen will appear in the user's web browser.



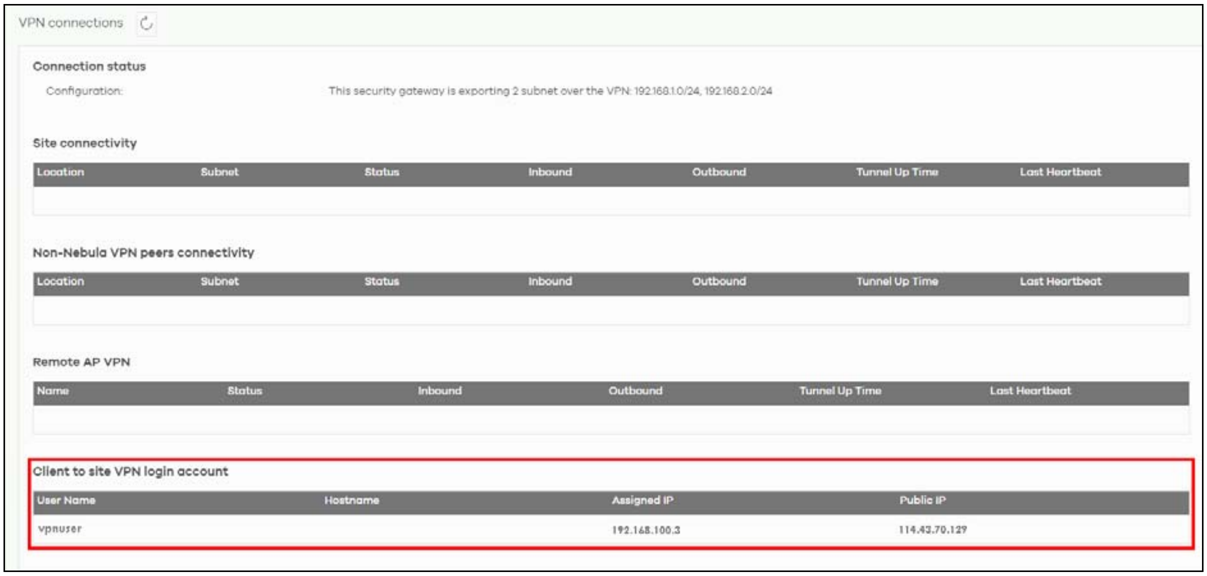
Welcome to Zyxel

Success!

Powered by ZYXEL

3.18.7 Check the Connection in Nebula by the Administrator

Go to the **Site-wide** > **Monitor** > **Firewall** > **VPN connections** screen. The remote VPN connection should appear in **Client to site VPN login account** table.



VPN connections

Connection status

Configuration: This security gateway is exporting 2 subnet over the VPN: 192.168.1.0/24, 192.168.2.0/24

Site connectivity

Location	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat

Non-Nebula VPN peers connectivity

Location	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat

Remote AP VPN

Name	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat

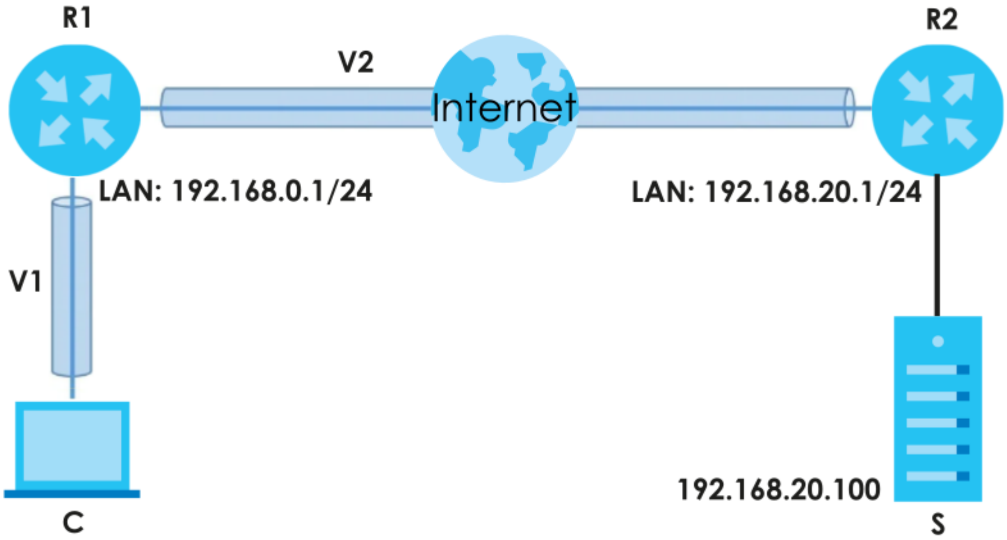
Client to site VPN login account

User Name	Hostname	Assigned IP	Public IP
vpnuser		192.168.100.3	114.43.70.129

3.19 Route L2TP VPN Traffic

L2TP (Layer 2 Tunneling Protocol) is a tunneling protocol used to support virtual private networks (VPNs). L2TP works at layer 2 (the data link layer) to tunnel network traffic between two Nebula Devices over another network (like the Internet). In L2TP VPN, establish an IPSec (Internet Protocol Security) VPN tunnel first and then build an L2TP tunnel inside it. IPSec VPN connects IPSec routers or remote users using an IPSec software such as SecuExtender.

The following example figure shows a VPN client (C) connecting to a Nebula Device (R1) through an L2TP VPN (V1). Nebula Device (R1) connects to Nebula Device (R2) using site-to-site VPN (V2). The VPN client (C) can access a server (S) inside the Nebula Device (R2) through the two VPN tunnels (V1, V2).



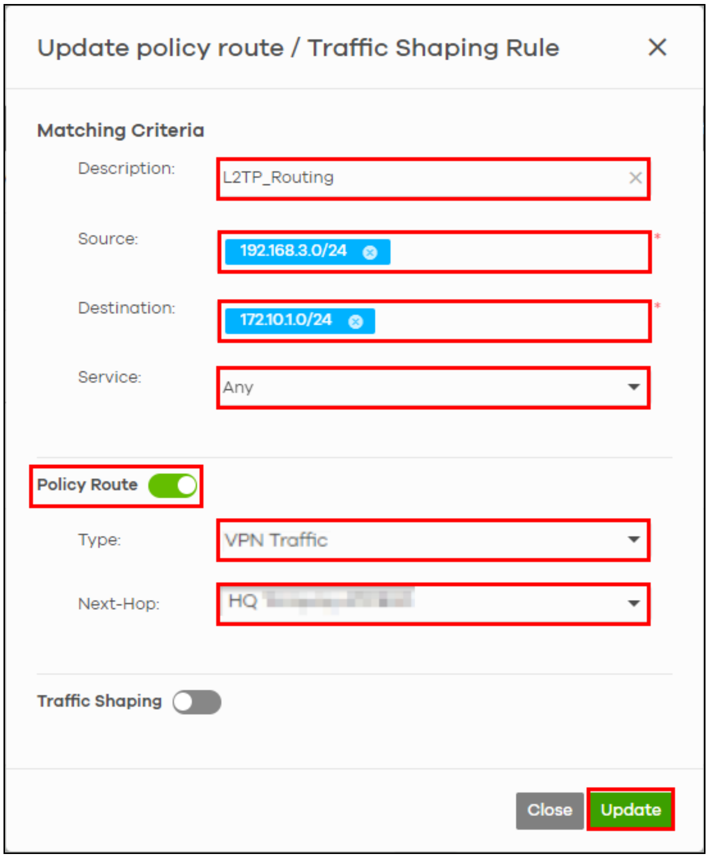
You can set up a VPN site-to-site tunnel to a cloud computing service like Microsoft Azure. To route L2TP traffic between your site and Microsoft Azure site, do the following:

Nebula Device (Firewall device) IP address	192.168.1.1
L2TP VPN (source site)	192.168.3.0/24
Microsoft Azure network (destination site)	172.10.1.0/24

Go to **Site-wide** > **Configure** > **Firewall** > **Routing**: **Policy Route/Traffic Shaping**: **Add**.

- Enter a definition for the rule in **Description**: for example, L2TP_Routing.
- Enter the L2TP IP address range to which this rule applies in **Source** IP: 192.168.3.0/24.
- Enter the **Destination** IP address range to which this rule applies: 172.10.1.0/24.
- Select **Any** protocol to apply the policy route to in **Service**.
- Click to enable **Policy Route**.
- Select **VPN Traffic** in **Type** to route the matched packets through the VPN tunnel you specified in the **Next-Hop** field.
- Select the remote VPN gateway's site name in **Next-Hop**.

Then click **Update**. Network traffic can now pass between your site and Microsoft Azure site through the L2TP tunnel.



Update policy route / Traffic Shaping Rule

Matching Criteria

Description: L2TP_Routing

Source: 192.168.3.0/24

Destination: 172.10.1.0/24

Service: Any

Policy Route

Type: VPN Traffic

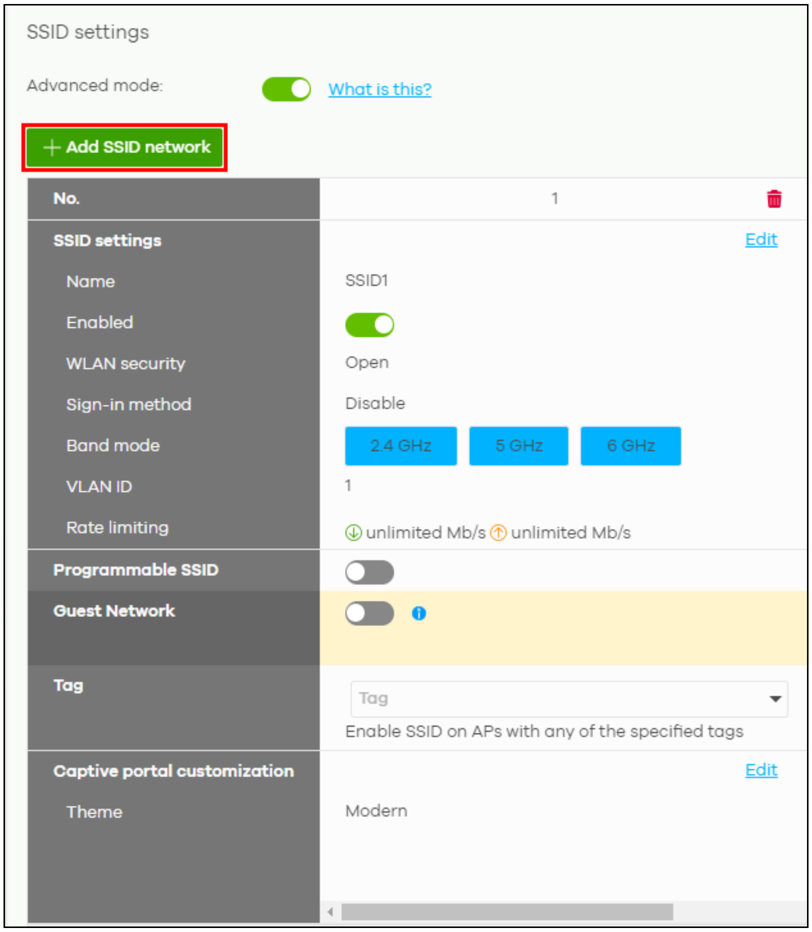
Next-Hop: HQ [redacted]

Traffic Shaping

3.20 Configure Guest Isolation on your WiFi Network

To enhance security for both host network and guest users, configure guest isolation on your WiFi network. This prevents the guest users from seeing each other on your WiFi network.

1 Go to **Site-wide** > **Configure** > **Access points** > **SSID settings** and click **+ Add SSID network**.



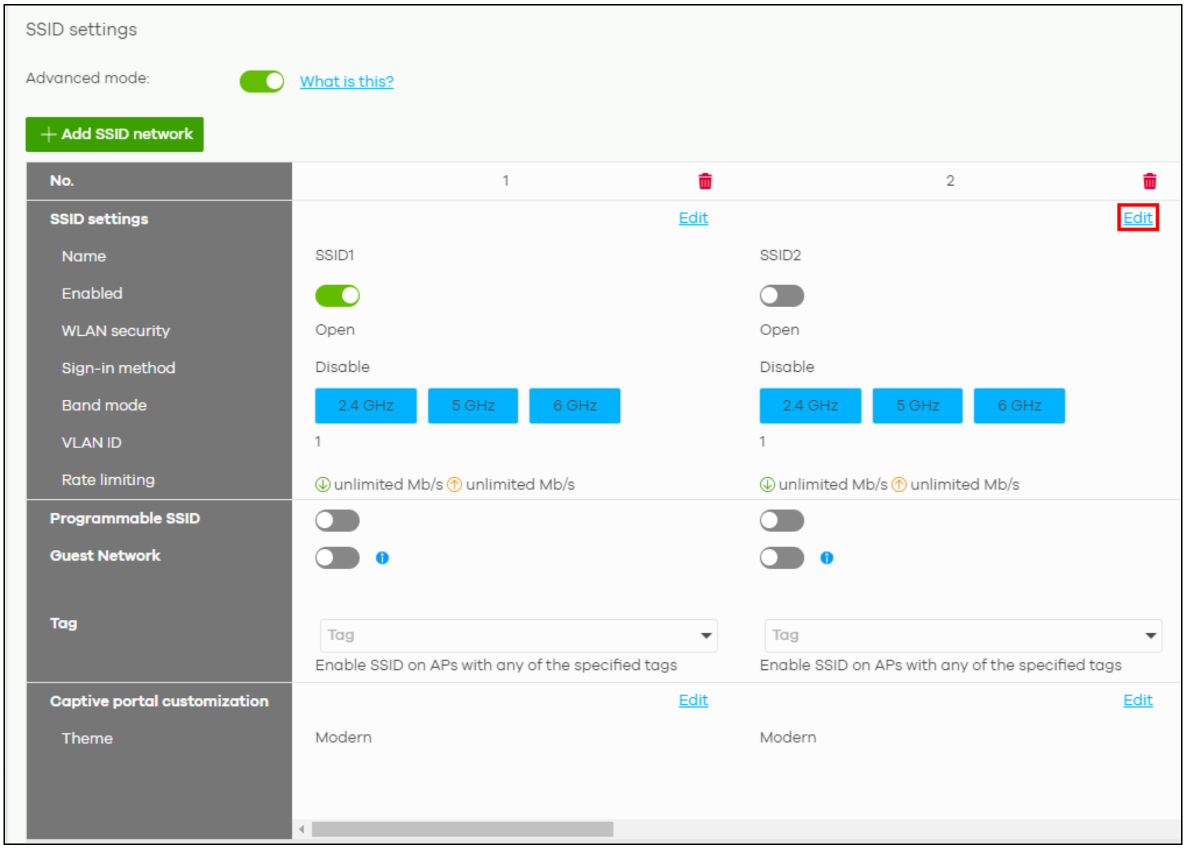
SSID settings

Advanced mode: What is this?

+ Add SSID network

No.	1
SSID settings	Edit
Name	SSID1
Enabled	●
WLAN security	Open
Sign-in method	Disable
Band mode	2.4 GHz 5 GHz 6 GHz
VLAN ID	1
Rate limiting	unlimited Mb/s unlimited Mb/s
Programmable SSID	○
Guest Network	○
Tag	Tag Enable SSID on APs with any of the specified tags
Captive portal customization	Edit
Theme	Modern

2 Click **Edit** on **SSID2** to go to the **Site-wide** > **Configure** > **Access points** > **SSID advanced settings** screen.



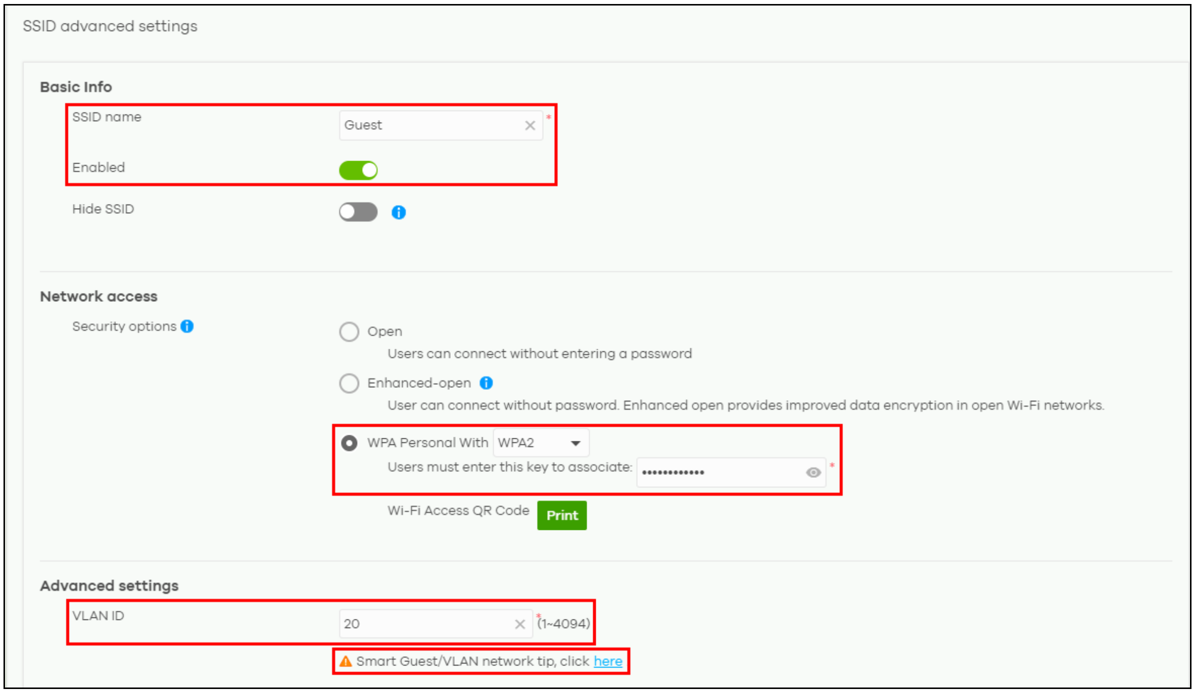
SSID settings

Advanced mode: ● What is this?

+ Add SSID network

No.	1	2
SSID settings	Edit	Edit
Name	SSID1	SSID2
Enabled	On	Off
WLAN security	Open	Open
Sign-in method	Disable	Disable
Band mode	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
VLAN ID	1	1
Rate limiting	unlimited Mb/s unlimited Mb/s	unlimited Mb/s unlimited Mb/s
Programmable SSID	Off	Off
Guest Network	Off	Off
Tag	Tag Enable SSID on APs with any of the specified tags	Tag Enable SSID on APs with any of the specified tags
Captive portal customization	Edit	Edit
Theme	Modern	Modern

3 Enter a name for this WiFi network for identification purposes (for example, Guest). Click **Enabled** to turn on this WiFi network. Select **WPA Personal With** (**WPA2**) and enter a pre-shared key from 8 to 63 case-sensitive keyboard characters in **Users must enter this key to associate** to enable WPA2-PSK data encryption. Enter the ID number of the VLAN to which the SSID belongs (for example, 20).



SSID advanced settings

Basic Info

SSID name: Guest *

Enabled: On

Hide SSID: Off

Network access

Security options

○ Open
Users can connect without entering a password

○ Enhanced-open
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.

● WPA Personal With WPA2
Users must enter this key to associate: •••••••••••• *

Wi-Fi Access QR Code Print

Advanced settings

VLAN ID: 20 (1~4094)

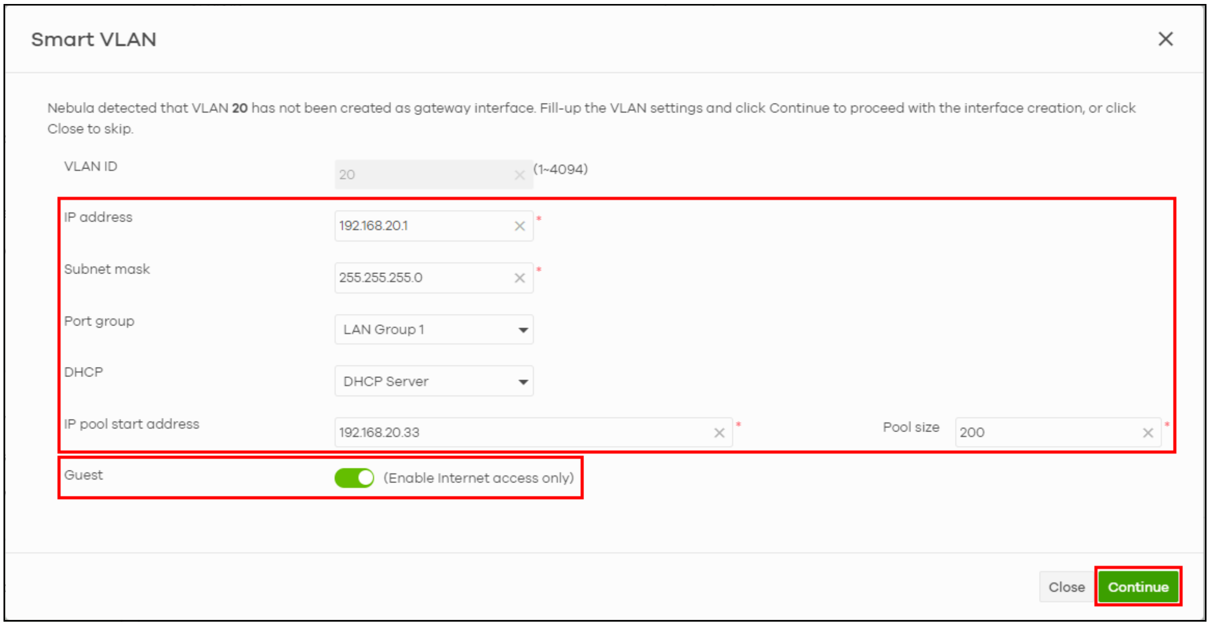
⚠ Smart Guest/VLAN network tip, click here

Note: If you have a Nebula Security Appliance installed in the site but did not configure the VLAN ID on the gateway, **Smart Guest/VLAN network tip, click here** displays. Click here to open a screen where you can create a gateway interface with the new VLAN ID.

4 On the Smart VLAN screen:

- Enter the **IP address** and **Subnet mask**, and select the **Port group** to which the Security Firewall interface belongs. Go to **Site-wide** > **Configure** > **Firewall** > **Interface** to get the **Port group** information.
- In **DHCP**, select **DHCP Server** to allow the Nebula Device to assign IP addresses and provide subnet mask, gateway, and DNS server information to the network.
- In **IP pool start address**, enter the IP address from which the Nebula Device begins allocating IP addresses.
- In **Pool size**, enter the number of IP addresses to allocate. For example, 200. This number must be at least one and is limited by the interface's **Subnet mask**. If the **Subnet mask** is 255.255.255.0 and the **IP pool start address** is 192.168.20.33, the Nebula Device can allocate 192.168.20.33 to 192.168.20.232, or 200 IP addresses.
- Click the **Guest** switch to the right to configure the interface as a Guest interface. Client devices connected to a Guest interface have Internet access but cannot communicate with each other directly or access networks behind the Nebula Device.

Then click **Continue** to save your settings for the VLAN to the NCC and return to the **Site-wide** > **Configure** > **Access points** > **SSID advanced settings** screen.



Smart VLAN

Nebula detected that VLAN **20** has not been created as gateway interface. Fill-up the VLAN settings and click Continue to proceed with the interface creation, or click Close to skip.

VLAN ID: 20 (1~4094)

IP address: 192.168.20.1 *

Subnet mask: 255.255.255.0 *

Port group: LAN Group 1

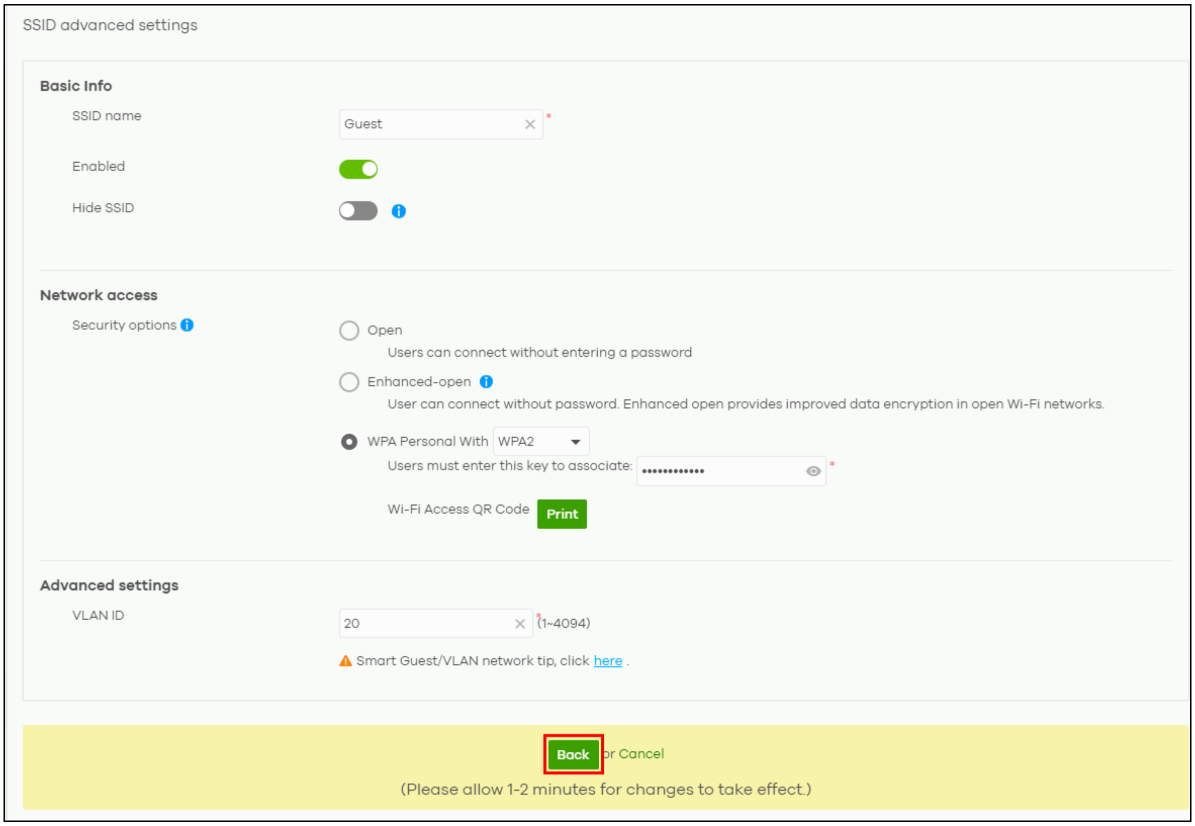
DHCP: DHCP Server

IP pool start address: 192.168.20.33 *

Pool size: 200 *

Guest: (Enable Internet access only)

5 Click **Back** to save your settings for the Guest SSID to the NCC and return to the **Site-wide** > **Configure** > **Access points** > **SSID settings** screen.



SSID advanced settings

Basic Info

SSID name: Guest *

Enabled: on

Hide SSID: off

Network access

Security options

○ Open
Users can connect without entering a password

○ Enhanced-open
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.

● WPA Personal With WPA2
Users must enter this key to associate: •••••••••••• *

Wi-Fi Access QR Code

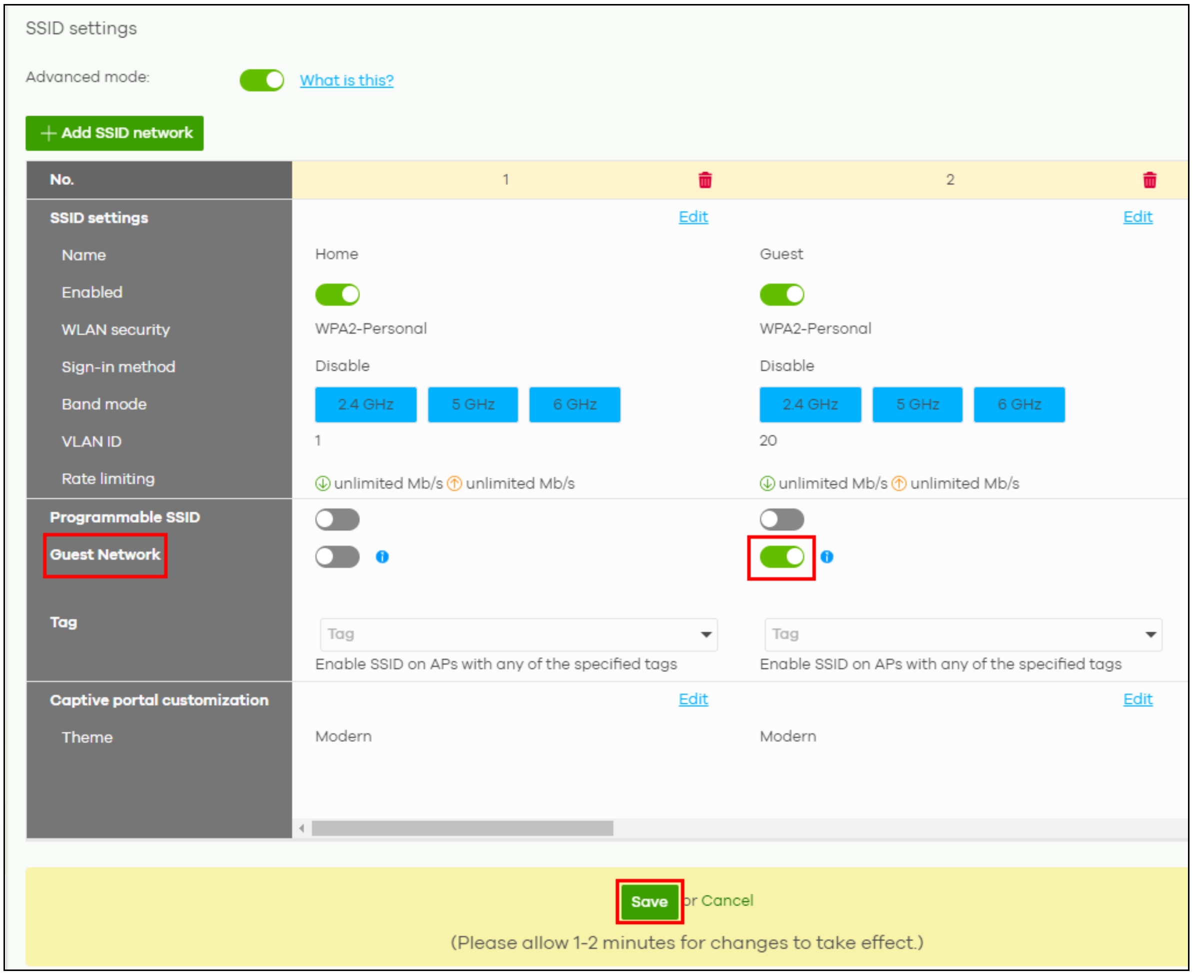
Advanced settings

VLAN ID: 20 * (1~4094)

Smart Guest/VLAN network tip, click here .

(Please allow 1-2 minutes for changes to take effect.)

6 Activate the **Guest Network** for the Guest SSID and click **Save**.



SSID settings

Advanced mode: ● What is this?

+ Add SSID network

No.	1	2
SSID settings	Edit	Edit
Name	Home	Guest
Enabled	●	●
WLAN security	WPA2-Personal	WPA2-Personal
Sign-in method	Disable	Disable
Band mode	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
VLAN ID	1	20
Rate limiting	⇓ unlimited Mb/s ⇑ unlimited Mb/s	⇓ unlimited Mb/s ⇑ unlimited Mb/s
Programmable SSID	○	○
Guest Network	○	●
Tag	Tag Enable SSID on APs with any of the specified tags	Tag Enable SSID on APs with any of the specified tags
Captive portal customization	Edit	Edit
Theme	Modern	Modern

Save or Cancel

(Please allow 1-2 minutes for changes to take effect.)

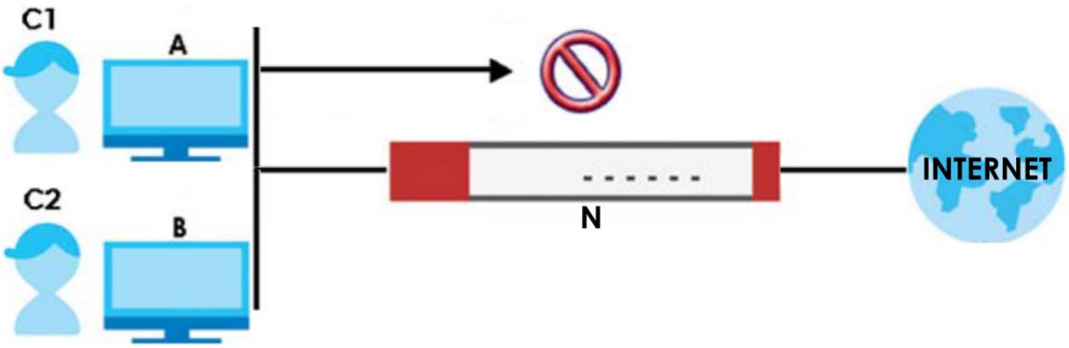
To test the configuration:

1. Connect a WiFi client to the Guest SSID. The WiFi client should get an IP address from the Guest SSID.
2. Have the Guest WiFi client access the www.zyxel.com website to test Internet connectivity.
3. Then, have the WiFi client connected to the Guest SSID ping another WiFi client connected to the Home SSID. The ping attempt should fail as the WiFi client connected to the Guest SSID can only access the Internet.

3.21 Configure Content Filter to Block Access to Certain Websites

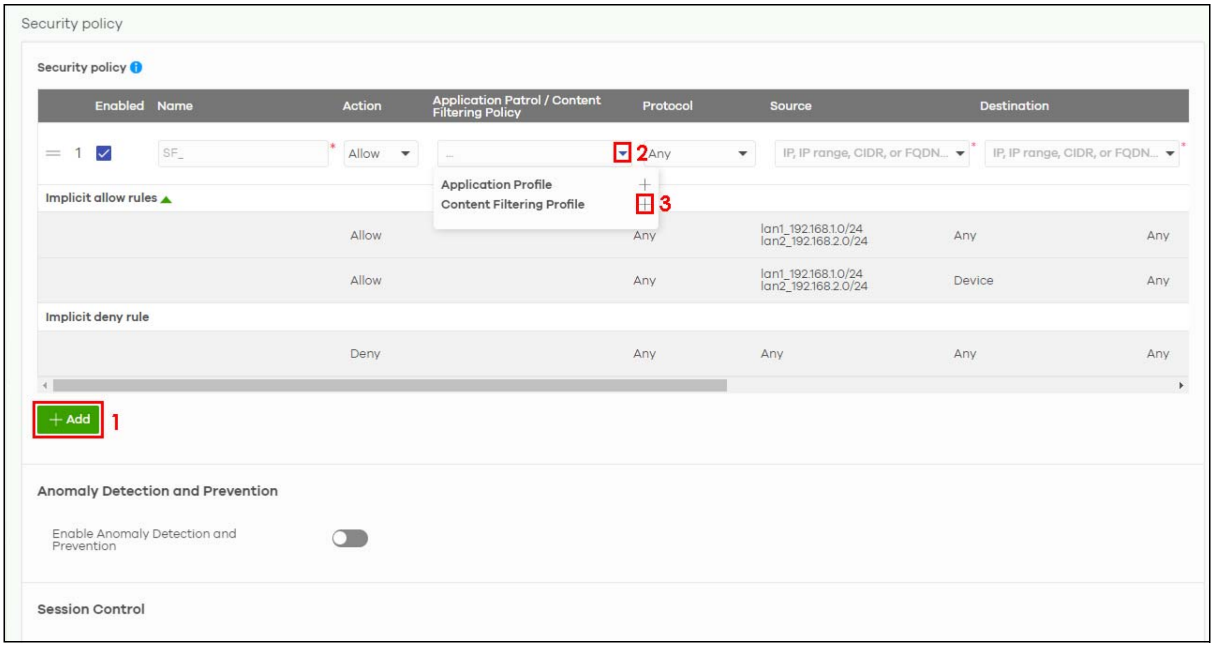
This example shows how to block clients from accessing social media websites like Facebook.

The following example figure shows client **C1** using computer **A** and client **C2** using computer **B** to access the Internet through the Nebula Device **N**.



You want to block the LAN clients **C1** and **C2** from accessing social media websites such as Facebook. Create a content filter profile that includes the social media category.

1 Go to **Site-wide** > **Configure** > **Firewall** > **Security policy: Security policy** and click **+ Add** (1).



Security policy

Security policy

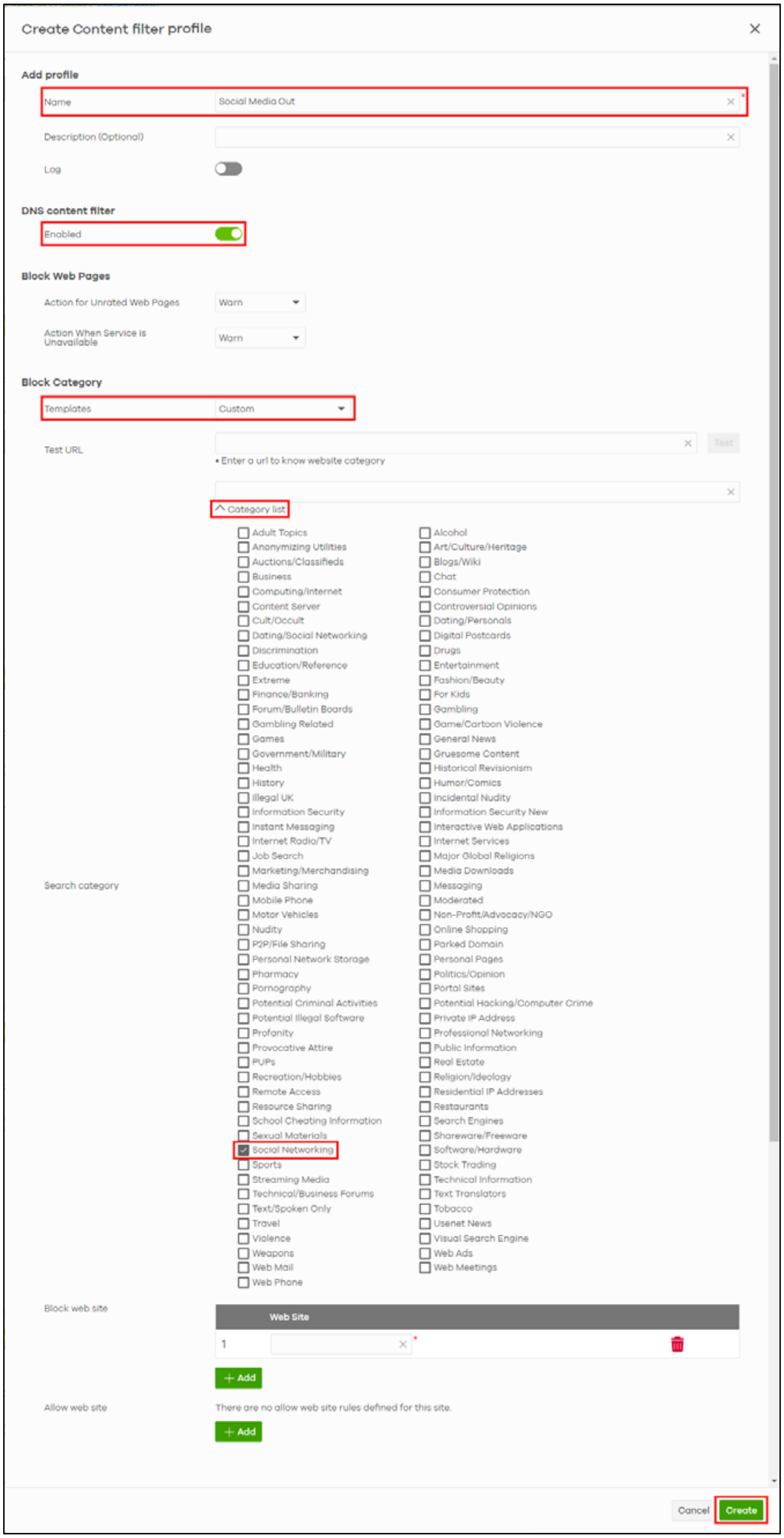
	Enabled	Name	Action	Application Patrol / Content Filtering Policy	Protocol	Source	Destination	
═ 1	☑	SF_ *	Allow	...	Any	IP, IP range, CIDR, or FQDN... *	IP, IP range, CIDR, or FQDN... *	
Implicit allow rules ▲								
			Allow		Any	lan1_192.168.1.0/24 lan2_192.168.2.0/24	Any	Any
			Allow		Any	lan1_192.168.1.0/24 lan2_192.168.2.0/24	Device	Any
Implicit deny rule								
			Deny		Any	Any	Any	Any

Anomaly Detection and Prevention

Enable Anomaly Detection and Prevention ○

Session Control

2 Click the drop-down menu button (2) and then click '**+**' (3) for **Content Filtering Profile** to add a Content Filter profile. The Nebula Device takes the action set in the profile when traffic matches the profile's policy. The following screen appears. See Table 125 on page 522 for a description of the fields in the **Create content filter profile** screen.



Create Content filter profile

Add profile

Name: Social Media Out

Description (Optional):

Log

DNS content filter

Enabled

Block Web Pages

Action for Unrated Web Pages: Warn

Action When Service is Unavailable: Warn

Block Category

Templates: Custom

Test URL

- Enter a url to know website category

Search category

Category list

- □ Adult Topics
- □ Anonymizing Utilities
- □ Auctions/Classifieds
- □ Business
- □ Computing/Internet
- □ Content Server
- □ Cult/Occult
- □ Dating/Social Networking
- □ Discrimination
- □ Education/Reference
- □ Extreme
- □ Finance/Banking
- □ Forum/Bulletin Boards
- □ Gambling Related
- □ Games
- □ Government/Military
- □ Health
- □ History
- □ Illegal UK
- □ Information Security
- □ Instant Messaging
- □ Internet Radio/TV
- □ Job Search
- □ Marketing/Merchandising
- □ Media Sharing
- □ Mobile Phone
- □ Motor Vehicles
- □ Nudity
- □ P2P/File Sharing
- □ Personal Network Storage
- □ Pharmacy
- □ Pornography
- □ Potential Criminal Activities
- □ Potential Illegal Software
- □ Profanity
- □ Provocative Attire
- □ PUPs
- □ Recreation/Hobbies
- □ Remote Access
- □ Resource Sharing
- □ School Cheating Information
- □ Sexual Materials
- ☑ Social Networking
- □ Sports
- □ Streaming Media
- □ Technical/Business Forums
- □ Text/Spoken Only
- □ Travel
- □ Violence
- □ Weapons
- □ Web Mail
- □ Web Phone
- □ Alcohol
- □ Art/Culture/Heritage
- □ Blogs/Wiki
- □ Chat
- □ Consumer Protection
- □ Controversial Opinions
- □ Dating/Personals
- □ Digital Postcards
- □ Drugs
- □ Entertainment
- □ Fashion/Beauty
- □ For Kids
- □ Gambling
- □ Game/Cartoon Violence
- □ General News
- □ Gruesome Content
- □ Historical Revisionism
- □ Humor/Comics
- □ Incidental Nudity
- □ Information Security New
- □ Interactive Web Applications
- □ Internet Services
- □ Major Global Religions
- □ Media Downloads
- □ Messaging
- □ Moderated
- □ Non-Profit/Advocacy/NGO
- □ Online Shopping
- □ Parked Domain
- □ Personal Pages
- □ Politics/Opinion
- □ Portal Sites
- □ Potential Hacking/Computer Crime
- □ Private IP Address
- □ Professional Networking
- □ Public Information
- □ Real Estate
- □ Religion/Ideology
- □ Residential IP Addresses
- □ Restaurants
- □ Search Engines
- □ Shareware/Freeware
- □ Software/Hardware
- □ Stock Trading
- □ Technical Information
- □ Text Translators
- □ Tobacco
- □ Usenet News
- □ Visual Search Engine
- □ Web Ads
- □ Web Meetings

Block web site

	Web Site
1	

Allow web site

There are no allow web site rules defined for this site.

3 Enter a name for this profile for identification purposes. For example, Social Media Out.

4 Make sure to click the switch to the right for **DNS content filter**: **Enabled**.

5 Select **Custom** for **Templates**.

6 To control access to the social networking type of Internet content, click **Category list** to open the list and select **Social Networking** in the **Search category**. This allows you to block access to social networking sites including Facebook.

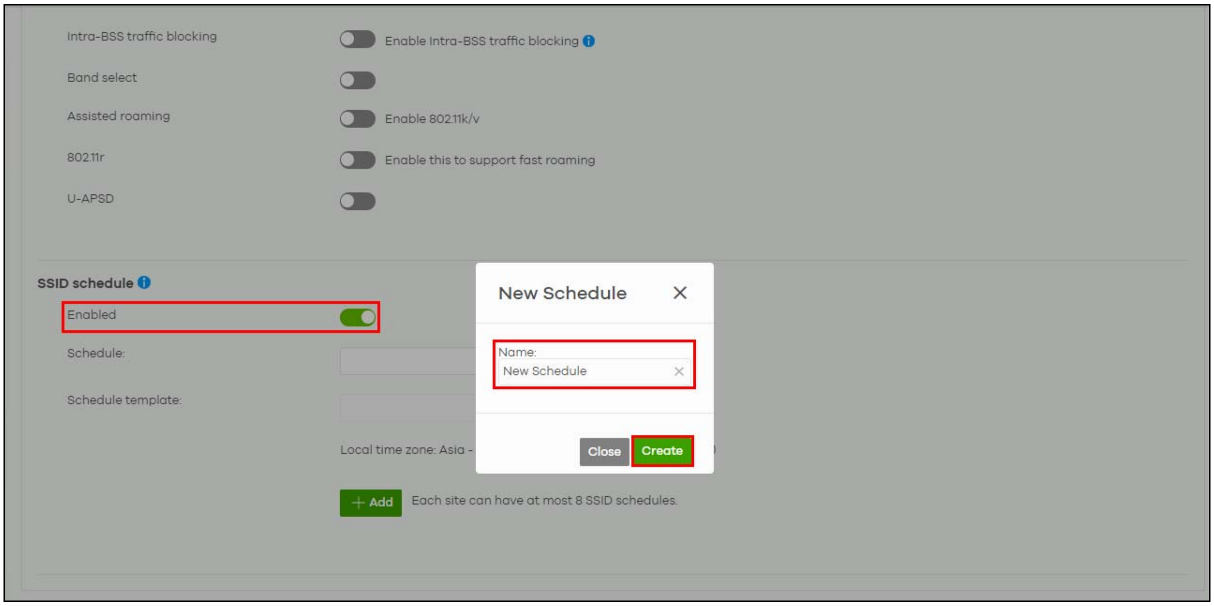
7 Then, click **Create** to save and exit.

3.22 Configure Schedule to Allow WiFi Access Only at Certain Times

This example shows you how to allow WiFi Internet access only at certain times.

To configure a schedule to control when a WiFi network (SSID) is enabled or disabled, do the following:

1 Go to **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**. Click the **Enabled** switch in **SSID schedule** to the right to configure a schedule. The **New Schedule** window appears. Enter a descriptive **Name** for the schedule of up to 127 characters (0 – 9 a – z). The casing does not matter. Then, click **Create**.



Intra-BSS traffic blocking: Enable Intra-BSS traffic blocking

Band select

Assisted roaming: Enable 802.11k/v

802.11r: Enable this to support fast roaming

U-APSD

SSID schedule

Enabled

Schedule:

Schedule template:

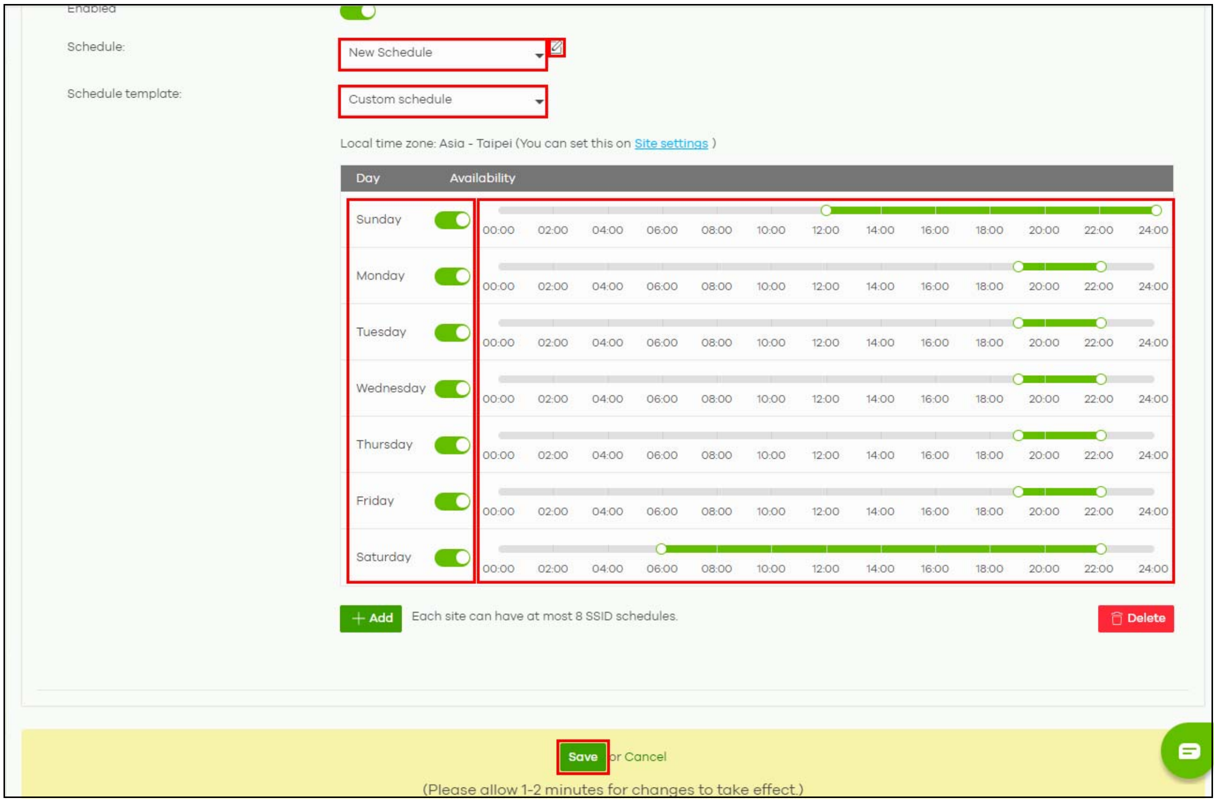
Local time zone: Asia -

Each site can have at most 8 SSID schedules.

New Schedule

Name: New Schedule

2 The schedule **Name** appears on **Schedule**. To change it, click the edit icon (✎) . Select **Custom schedule** in **Schedule template** to manually configure the **Day** and time at which the WiFi network (SSID) is enabled. Click the **Availability** switch to the right to enable the WiFi network (SSID) at the specified time on this day. Specify the hour and minute when the schedule begins and ends each day. Then click **Save**.



Enabled

Schedule: New Schedule

Schedule template: Custom schedule

Local time zone: Asia - Taipei (You can set this on Site settings)

Day	Availability
Sunday	12:00 – 24:00
Monday	19:00 – 22:00
Tuesday	19:00 – 22:00
Wednesday	19:00 – 22:00
Thursday	19:00 – 22:00
Friday	19:00 – 22:00
Saturday	06:00 – 22:00

Each site can have at most 8 SSID schedules.

Save or Cancel

(Please allow 1-2 minutes for changes to take effect.)

3.23 How to Position Multiple Nebula Devices (for Nebula Access Points only)

To select the best position to minimize signal interference for multiple Nebula access points, do the following:

1. Avoid positioning the Nebula Devices too close to each other. This can cause interference.

2. In case it may be necessary to position Nebula Devices in direct line of sight of each other, adjust the transmission power of each Nebula Device so that they are not overlapping each other. This can reduce signal interference. Go to **Site-wide** > **Configure** > **Access points** > **Radio settings** and select the **Deployment selection** and **Maximum output power**. See Section 5.3.4 on page 335 for more information.

3. Enable DCS (Dynamic Channel Selection) to let the Nebula Devices scan the best channel to use. This will minimize co-channel interference between the Nebula Devices. Go to **Site-wide** > **Configure** > **Access points** > **Radio settings** > **DCS setting**.

   Note: When **DCS client aware** is enabled in **Site-wide** > **Configure** > **Access points** > **Radio settings** > **DCS setting** and there are WiFi clients connected to the Nebula Device, the channel will not be changed after a DCS scan.

4. Configure the Nebula Devices in **Site-wide** > **Configure** > **Access points** > **Radio settings** > **DCS setting** to operate on non-overlapping channels.

   - For the **2.4 GHz channel deployment**, select **Manual**. Then, select the **Channel ID**s 1, 6, 11.

- For the **5 GHz channel deployment**, select **Manual**. Then, select the **Channel ID**s 36 to 165.

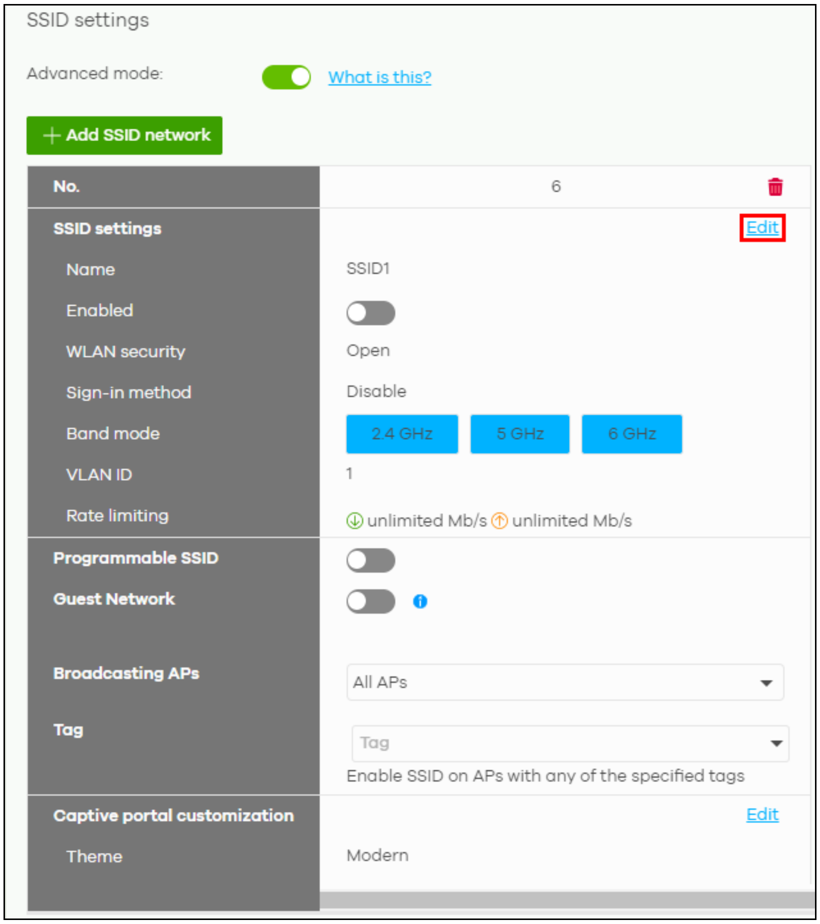
Note: The **Channel ID**s available will depend on your **Country** field selection.

3.24 Change the Default SSID and Password

To distinguish between different APs in your network, you should change the default name of the Access Point's WiFi network to which clients are connected (also known as SSID) and password.

To change the default SSID and password:

1 Go to the **Site-wide** > **Configure** > **Security router** / **Access points** > **SSID settings** tab and click **Edit**.

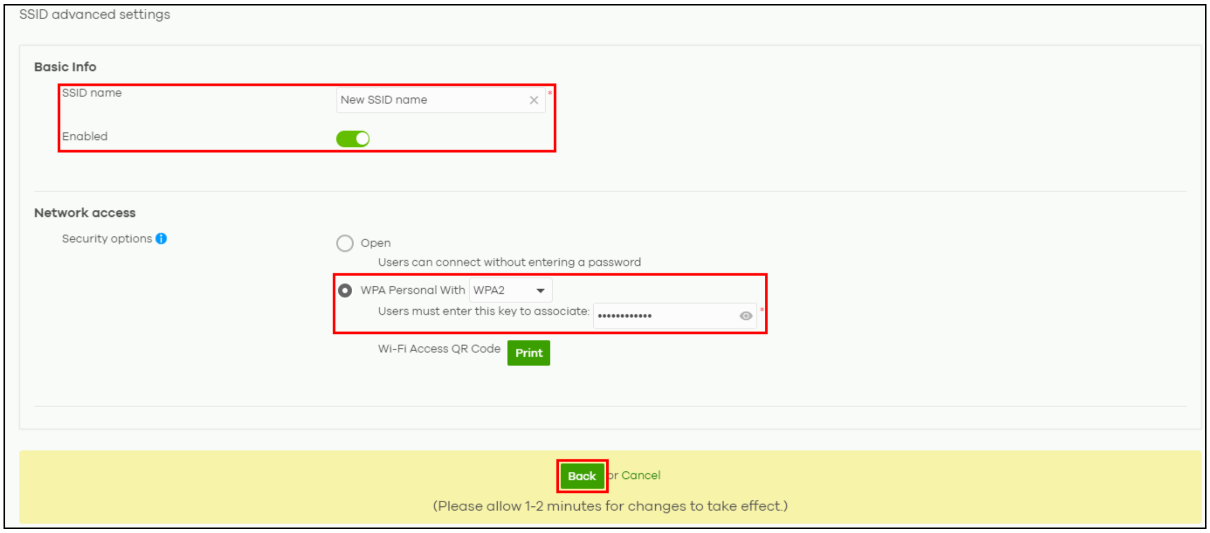


SSID settings

Advanced mode: What is this?

No.	6
SSID settings	Edit
Name	SSID1
Enabled	
WLAN security	Open
Sign-in method	Disable
Band mode	2.4 GHz 5 GHz 6 GHz
VLAN ID	1
Rate limiting	unlimited Mb/s unlimited Mb/s
Programmable SSID	
Guest Network	
Broadcasting APs	All APs
Tag	Tag Enable SSID on APs with any of the specified tags
Captive portal customization	Edit
Theme	Modern

2 Enter a descriptive name of up to 32 printable characters in **SSID name**.



SSID advanced settings

Basic Info

SSID name: New SSID name

Enabled

Network access

Security options

○ Open

Users can connect without entering a password

● WPA Personal With WPA2

Users must enter this key to associate: ••••••••••••

Wi-Fi Access QR Code

(Please allow 1-2 minutes for changes to take effect.)

3 Click the **Enabled** switch to the right to apply this SSID profile.

4 Select **WPA3** for the strongest security if the connected WiFi clients support it, otherwise select **WPA2** to add security on this WiFi network.

5 Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters in **Users must enter this key to associate**.

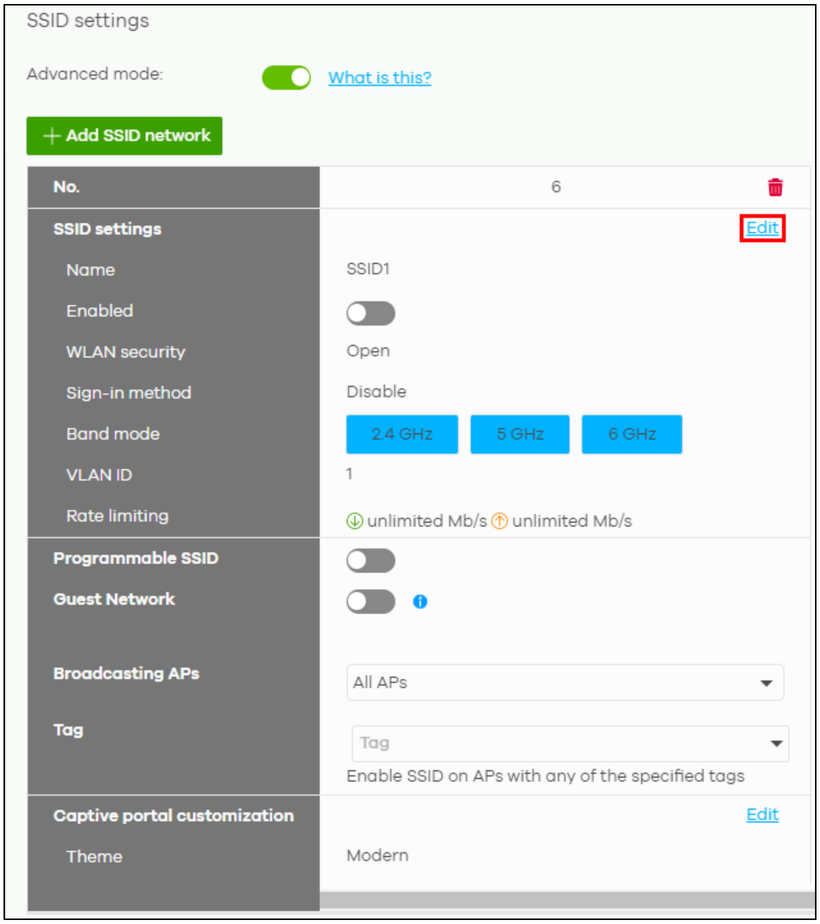
6 Click **Back** to proceed.

3.25 Change the WiFi Band Mode

If your WiFi network is slow, change the WiFi band mode. Choose 6G if the connected WiFi clients support it. Choose 5G for WiFi clients within range that require higher speeds such as video streaming.

To change the WiFi network band mode:

1 Go to the **Site-wide** > **Configure** > **Security router** / **Access points** > **SSID settings** tab and click **Edit**.

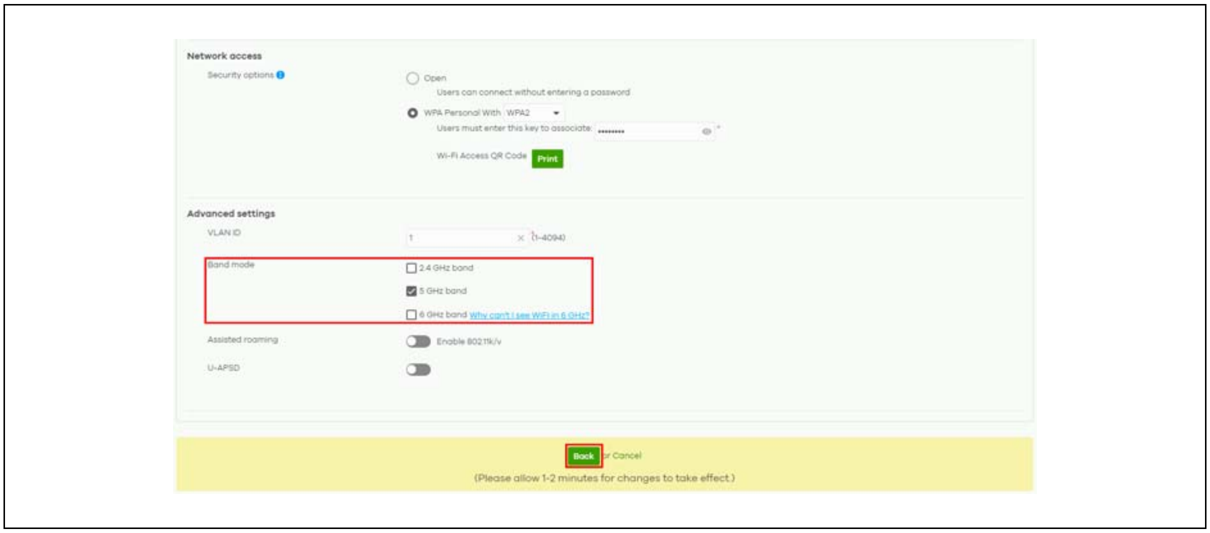


SSID settings

Advanced mode: What is this?

No.	6
SSID settings	Edit
Name	SSID1
Enabled	
WLAN security	Open
Sign-in method	Disable
Band mode	2.4 GHz 5 GHz 6 GHz
VLAN ID	1
Rate limiting	unlimited Mb/s unlimited Mb/s
Programmable SSID	
Guest Network	
Broadcasting APs	All APs
Tag	Tag Enable SSID on APs with any of the specified tags
Captive portal customization	Edit
Theme	Modern

2 In the **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**: **Advanced settings**: **Band mode**; select to have the SSID use a different band (**2.4 GHZ band**, **5 GHz band**, or **6 GHz band**).



Network access

Security options

○ Open

Users can connect without entering a password

● WPA Personal With WPA2

Users must enter this key to associate: ••••••••

Wi-Fi Access QR Code Print

Advanced settings

VLAN ID: 1 (1-4094)

Band mode: □ 2.4 GHz band ☑ 5 GHz band □ 6 GHz band Why can't I see WiFi in 6 GHz?

Assisted roaming: Enable 802.11k/v

U-APSD

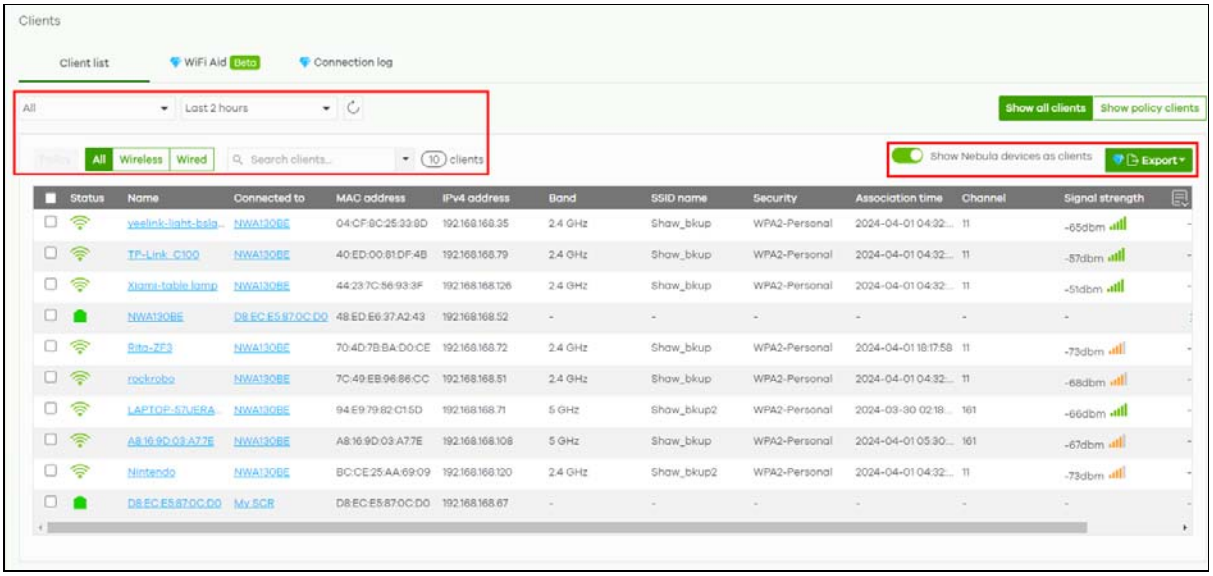
(Please allow 1-2 minutes for changes to take effect.)

3 Click **Back** to proceed.

3.26 Check What Clients are Connected to Nebula Devices in your Network

To see a list of all wired and WiFi clients connected to Nebula Devices in the site, do the following:

1 Go to the **Site-wide** > **Clients** > **Client list** screen.



☐	Status	Name	Connected to	MAC address	IPv4 address	Band	SSID name	Security	Association time	Channel	Signal strength
☐	📶	yeelink-light-bslg...	NWA130BE	04:CF:8C:25:33:8D	192.168.168.35	2.4 GHz	Shaw_bkup	WPA2-Personal	2024-04-01 04:32:...	11	-65dbm
☐	📶	TP-Link_C100	NWA130BE	40:ED:00:81:DF:4B	192.168.168.79	2.4 GHz	Shaw_bkup	WPA2-Personal	2024-04-01 04:32:...	11	-57dbm
☐	📶	Xiami-table lamp	NWA130BE	44:23:7C:56:93:3F	192.168.168.126	2.4 GHz	Shaw_bkup	WPA2-Personal	2024-04-01 04:32:...	11	-51dbm
☐	●	NWA130BE	D8:EC:E5:87:0C:D0	48:ED:E6:37:A2:43	192.168.168.52	-	-	-	-	-	-
☐	📶	Rita-ZF3	NWA130BE	70:4D:7B:BA:D0:CE	192.168.168.72	2.4 GHz	Shaw_bkup	WPA2-Personal	2024-04-01 18:17:58	11	-73dbm
☐	📶	rockrobo	NWA130BE	7C:49:EB:96:86:CC	192.168.168.51	2.4 GHz	Shaw_bkup	WPA2-Personal	2024-04-01 04:32:...	11	-68dbm
☐	📶	LAPTOP-57UERA...	NWA130BE	94:E9:79:82:C1:5D	192.168.168.71	5 GHz	Shaw_bkup2	WPA2-Personal	2024-03-30 02:18:...	161	-66dbm
☐	📶	A8:16:9D:03:A7:7E	NWA130BE	A8:16:9D:03:A7:7E	192.168.168.108	5 GHz	Shaw_bkup	WPA2-Personal	2024-04-01 05:30:...	161	-67dbm
☐	📶	Nintendo	NWA130BE	BC:CE:25:AA:69:09	192.168.168.120	2.4 GHz	Shaw_bkup2	WPA2-Personal	2024-04-01 04:32:...	11	-73dbm
☐	●	D8:EC:E5:87:0C:D0	My SCR	D8:EC:E5:87:0C:D0	192.168.168.67	-	-	-	-	-	-

2 Select to filter the list of clients, based on what type of Nebula Device (Access point, Switch, Security router) the client is connected to. Alternatively, select **All Clients**.

3 You can also set a time; the list shows each client's connection status in the past two hours, past 24 hours, past 7 days, past 30 days, or custom range. The maximum custom range is 30 days within the past 365 days. You can only show each client's connection status in the past two hours and past 24 hours only when you select **All Clients**.

4 You can select the type of clients that have been online during the selected time period: **All** (both WiFi and wired clients), **Wireless** (WiFi clients only), and **Wired** (wired clients only).

Note: Click **Show Nebula devices as clients** to show or hide the client Nebula Device(s) in the client list table. By default, this switch is ON for the sites created before the NCC 18.00 release. Otherwise, this switch is OFF for the sites created after the NCC 18.00 release.

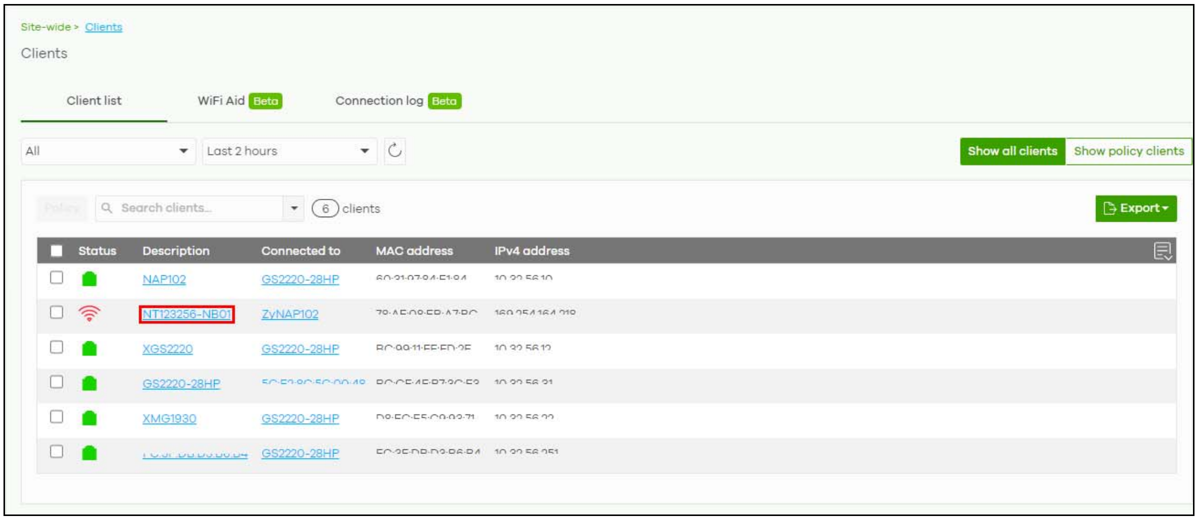
Click the **Export** button to save the client list as a CSV or XML file to your computer.

3.27 Find the SSID of the WiFi Client (for Nebula Access Points only)

You can view a list of all wired and WiFi clients connected to the Nebula Device in the site and the corresponding details. The details include the name of the Access Point's WiFi network to which the client is connected (also known as SSID).

To find the SSID of the WiFi client:

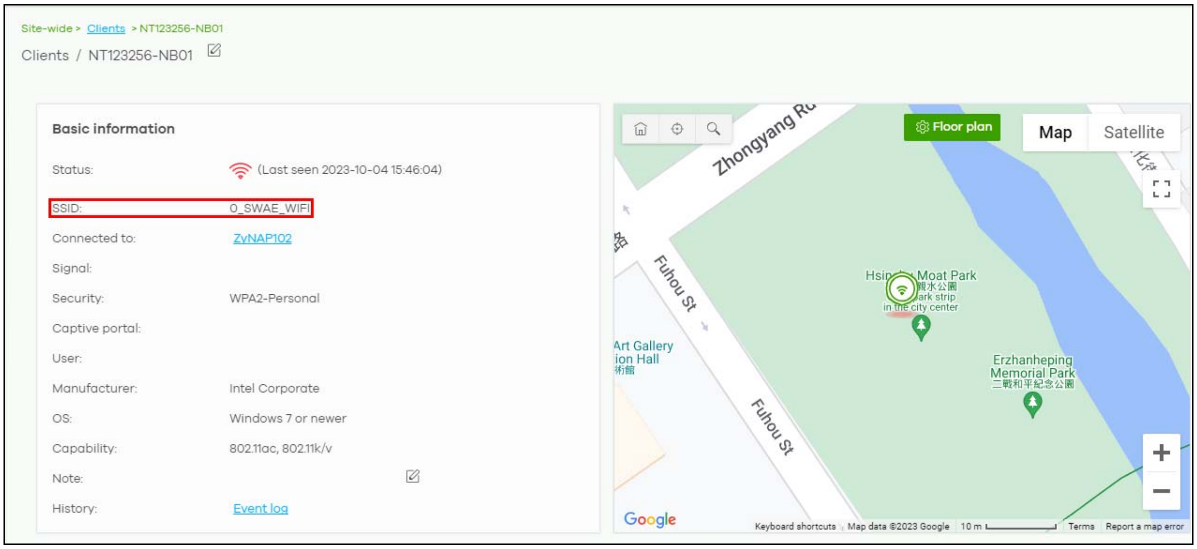
1 Go to **Site-wide** > **Clients** > **Client list** tab and click the **Description** of the WiFi client.


Site-wide > Clients

Clients

□	Status	Description	Connected to	MAC address	IPv4 address
□	🟩	NAP102	GS2220-28HP	60:31:97:84:E1:84	10.32.56.10
□	📶	NT123256-NB01	ZyNAP102	78:AF:08:EB:A7:BC	169.254.164.218
□	🟩	XGS2220	GS2220-28HP	BC:99:11:FE:ED:2F	10.32.56.12
□	🟩	GS2220-28HP	5C:E2:8C:5C:00:48	BC:CF:4F:B7:3C:E3	10.32.56.31
□	🟩	XMG1930	GS2220-28HP	D8:EC:E5:C9:93:71	10.32.56.22
□	🟩	FC:3F:DB:D3:B6:B4	GS2220-28HP	EC:3F:DB:D3:B6:B4	10.32.56.251

2 Locate the **SSID** in **Basic information** to know the name of the Access Point's WiFi network to which the client is connected.


Site-wide > Clients > NT123256-NB01

Clients / NT123256-NB01

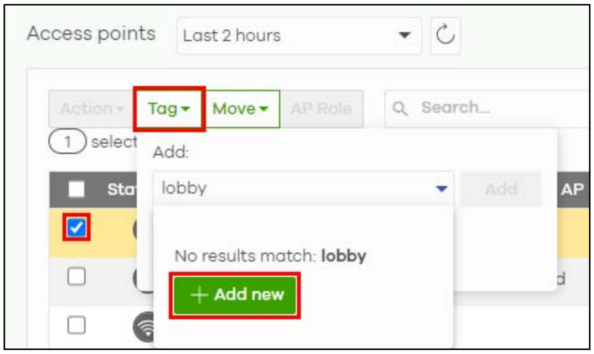
Basic information

Status:	📶 (Last seen 2023-10-04 15:46:04)
SSID:	0_SWAE_WIFI
Connected to:	ZyNAP102
Signal:	
Security:	WPA2-Personal
Captive portal:	
User:	
Manufacturer:	Intel Corporate
OS:	Windows 7 or newer
Capability:	802.11ac, 802.11k/v
Note:	
History:	Event log

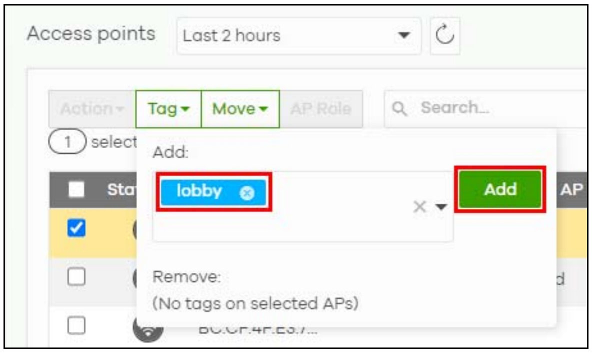
3.28 Use Tags to Assign SSIDs for Nebula Devices (for Nebula Access Points only)

When you have 2 Nebula Devices in different locations (for example, one in the lobby and one in the office), and you want Nebula Device A to only broadcast the SSID "SSID_lobby" and Nebula Device B "SSID_office" then do the following:

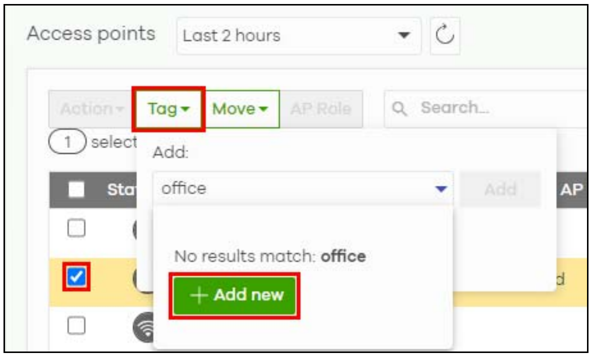
1 Go to **Site-wide** > **Devices** > **Access points**. Select the "Lobby_AP" and click **Tag**. Enter "lobby" and click **+ Add new**.



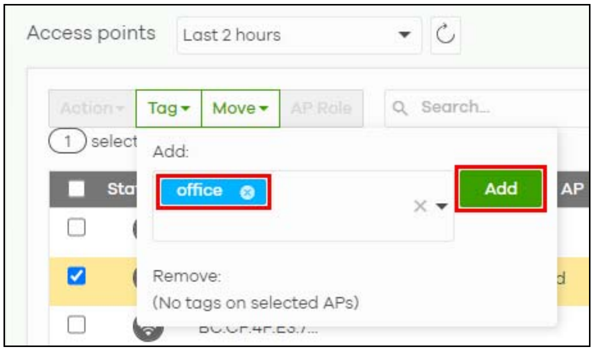
2 Click **Add** to assign the "lobby" tag to the "Lobby_AP".



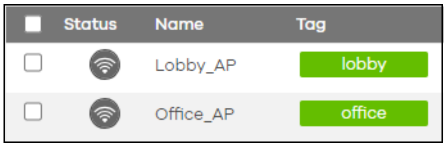
3 Select the "Office_AP" and click **Tag**. Enter "office" and click **+ Add new**.



4 Click **Add** to assign the "office" tag to the "Office_AP".

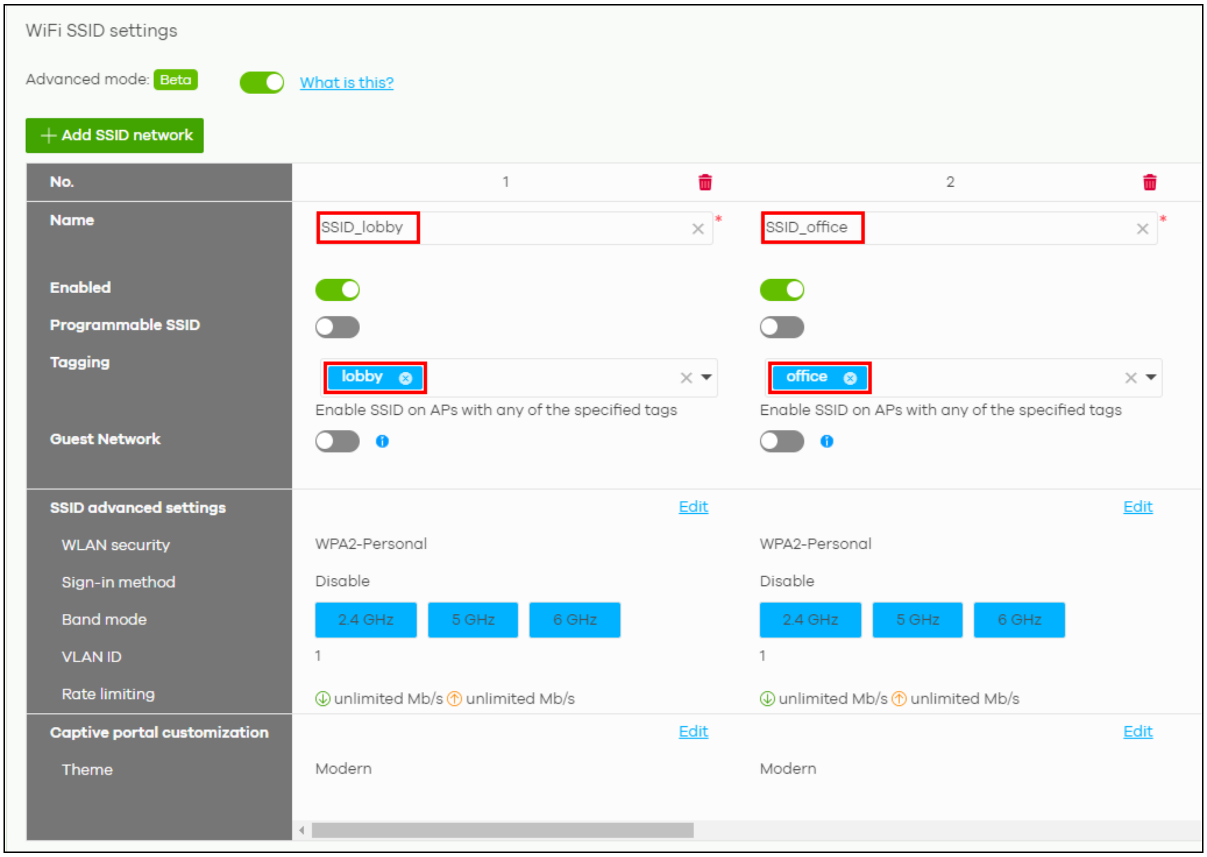


The new **Tag**s appear on the lobby and office APs in **Site-wide** > **Devices** > **Access points**.



□	Status	Name	Tag
□		Lobby_AP	lobby
□		Office_AP	office

5 Go to **Site-wide** > **Configure** > **SSID settings**. Select the “lobby” tag for the previously configured “SSID_lobby”. Select the “office” tag for the previously configured “SSID_office”.

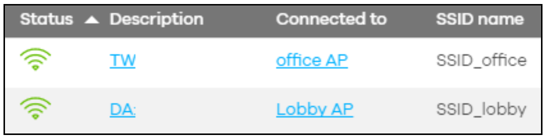


WiFi SSID settings

Advanced mode: Beta

No.	1	2
Name	SSID_lobby	SSID_office
Enabled	On	On
Programmable SSID	Off	Off
Tagging	lobby Enable SSID on APs with any of the specified tags	office Enable SSID on APs with any of the specified tags
Guest Network	Off	Off
SSID advanced settings	Edit	Edit
WLAN security	WPA2-Personal	WPA2-Personal
Sign-in method	Disable	Disable
Band mode	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
VLAN ID	1	1
Rate limiting	unlimited Mb/s unlimited Mb/s	unlimited Mb/s unlimited Mb/s
Captive portal customization	Edit	Edit
Theme	Modern	Modern

The Nebula Devices will broadcast SSIDs according to the assigned tags. Go to **Site-wide** > **Clients** to check the WiFi clients connection status.



Status ▲	Description	Connected to	SSID name
	TW	office AP	SSID_office
	DA	Lobby AP	SSID_lobby

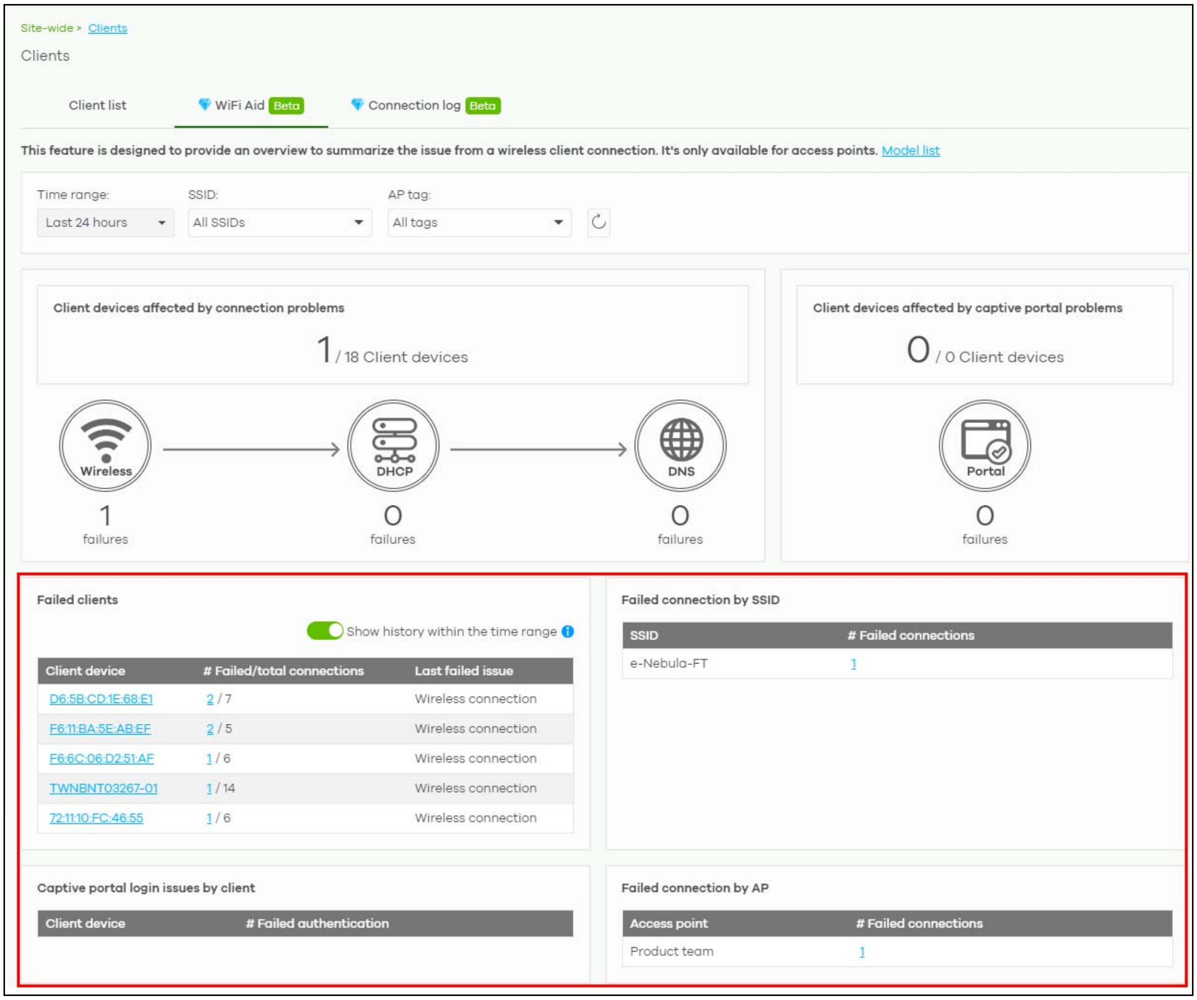
3.29 Resolve WiFi Connection Problems (for Nebula Access Points only)

The **WiFi Aid** tab in **Site-wide** > **Clients** helps you identify connection problems between WiFi clients and supported AP(s) for a selected time range.

Note: Make sure your Nebula AP is using the latest firmware.

The following tables allow you to view and identify connection problems using the following categories.

- Connection Issues by SSID
- Connection Issues by Client
- Connection Issues by Access Point
- Captive Portal Login Issues by Client



This feature is designed to provide an overview to summarize the issue from a wireless client connection. It's only available for access points. Model list

Time range: Last 24 hours

SSID: All SSIDs

AP tag: All tags

Client devices affected by connection problems

1 / 18 Client devices

Wireless: 1 failures

DHCP: 0 failures

DNS: 0 failures

Client devices affected by captive portal problems

0 / 0 Client devices

Portal: 0 failures

Failed clients

Show history within the time range

Client device	# Failed/total connections	Last failed issue
D6:5B:CD:1E:68:E1	2 / 7	Wireless connection
F6:11:BA:5E:AB:EF	2 / 5	Wireless connection
F6:6C:06:D2:51:AF	1 / 6	Wireless connection
TWNBNT03267-01	1 / 14	Wireless connection
72:11:10:FC:46:55	1 / 6	Wireless connection

Failed connection by SSID

SSID	# Failed connections
e-Nebula-FT	1

Captive portal login issues by client

Client device	# Failed authentication

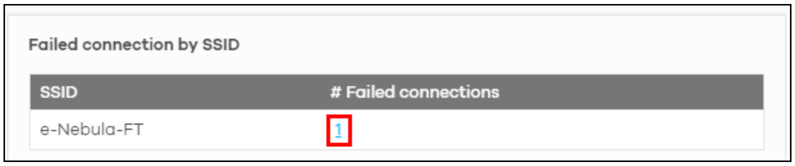
Failed connection by AP

Access point	# Failed connections
Product team	1

Connection Issues by SSID

This table displays the number of WiFi clients with WiFi connection/DHCP failures/DNS failures in each WiFi network. The list displays the WiFi network with the most connection failures first, in descending order.

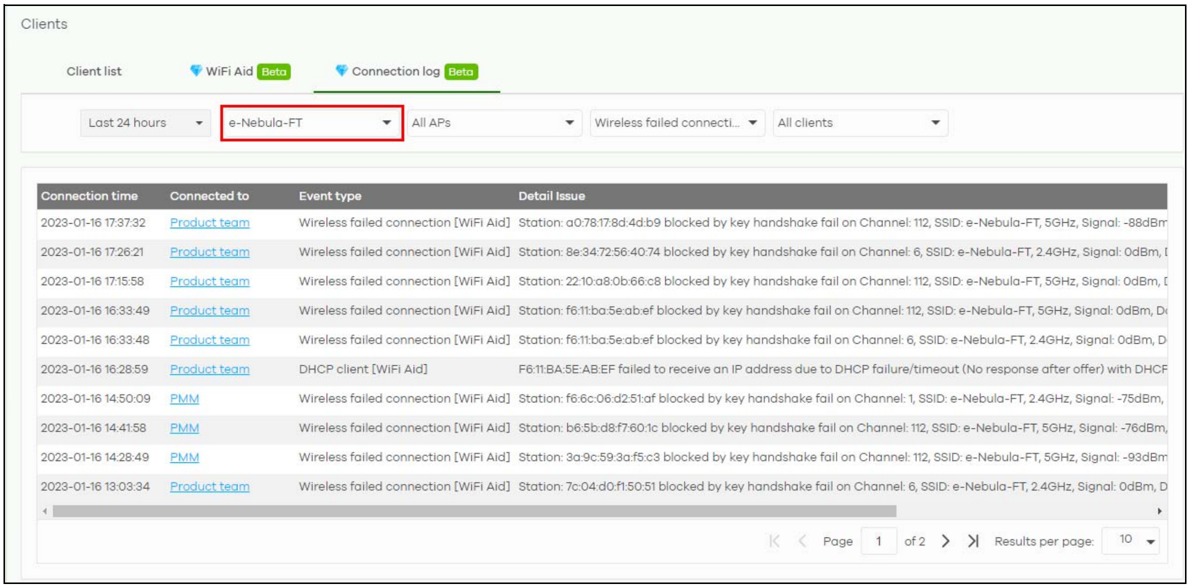
1 Click a hyperlink in the **# Failed connections** column.



Failed connection by SSID

SSID	# Failed connections
e-Nebula-FT	1

The **Site-wide** > **Clients** > **Connection log** screen appears showing all related event logs for WiFi clients in the e-Nebula-FT WiFi network in the last 24 hours.



Connection time	Connected to	Event type	Detail Issue
2023-01-16 17:37:32	Product team	Wireless failed connection [WiFi Aid]	Station: a0:78:17:8d:4d:b9 blocked by key handshake fail on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -88dBm
2023-01-16 17:26:21	Product team	Wireless failed connection [WiFi Aid]	Station: 8e:34:72:56:40:74 blocked by key handshake fail on Channel: 6, SSID: e-Nebula-FT, 2.4GHz, Signal: 0dBm,
2023-01-16 17:15:58	Product team	Wireless failed connection [WiFi Aid]	Station: 22:10:a8:0b:66:c8 blocked by key handshake fail on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: 0dBm,
2023-01-16 16:33:49	Product team	Wireless failed connection [WiFi Aid]	Station: f6:11:ba:5e:ab:ef blocked by key handshake fail on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: 0dBm, D
2023-01-16 16:33:48	Product team	Wireless failed connection [WiFi Aid]	Station: f6:11:ba:5e:ab:ef blocked by key handshake fail on Channel: 6, SSID: e-Nebula-FT, 2.4GHz, Signal: 0dBm, D
2023-01-16 16:28:59	Product team	DHCP client [WiFi Aid]	F6:11:BA:5E:AB:EF failed to receive an IP address due to DHCP failure/timeout (No response after offer) with DHCP
2023-01-16 14:50:09	PMM	Wireless failed connection [WiFi Aid]	Station: f6:6c:06:d2:51:af blocked by key handshake fail on Channel: 1, SSID: e-Nebula-FT, 2.4GHz, Signal: -75dBm,
2023-01-16 14:41:58	PMM	Wireless failed connection [WiFi Aid]	Station: b6:5b:d8:f7:60:1c blocked by key handshake fail on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -76dBm,
2023-01-16 14:28:49	PMM	Wireless failed connection [WiFi Aid]	Station: 3a:9c:59:3a:f5:c3 blocked by key handshake fail on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -93dBm
2023-01-16 13:03:34	Product team	Wireless failed connection [WiFi Aid]	Station: 7c:04:d0:f1:50:51 blocked by key handshake fail on Channel: 6, SSID: e-Nebula-FT, 2.4GHz, Signal: 0dBm, D

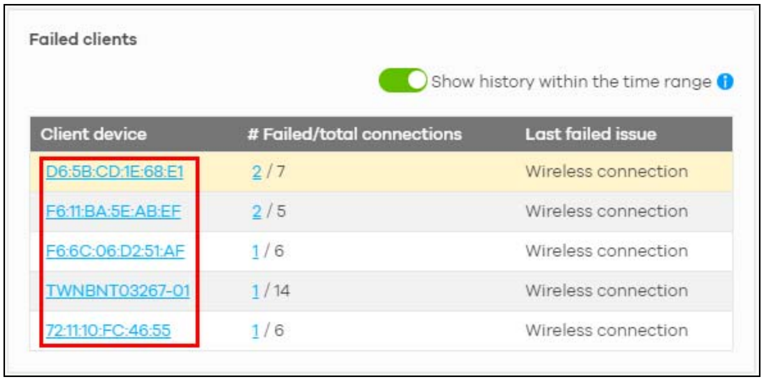
2 Use the following information listed in chronological order to resolve WiFi connection issues.

- **Connection time**. This shows the starting time period from which the event log occurred.
- **Connected to**. This shows the name (if available) or MAC address of the connected client.
- **Event type**. This shows the event type (**Association**, **Authentication**, **Disconnection**, **DHCP server**, **Wireless failed connection**, **DHCP client**, **DNS failure**, **Captive portal**) that occurred.
- **Detail issue**. This shows a summary of the APs event logs in chronological order.

Connection Issues by Client

This table displays the number of WiFi clients with failed connection attempts (WiFi connection/DHCP failures/DNS failures) and the number of total connection attempts. The list displays the WiFi client with the most connection failures first, in descending order.

1 Click a hyperlink in the **Client device** column.

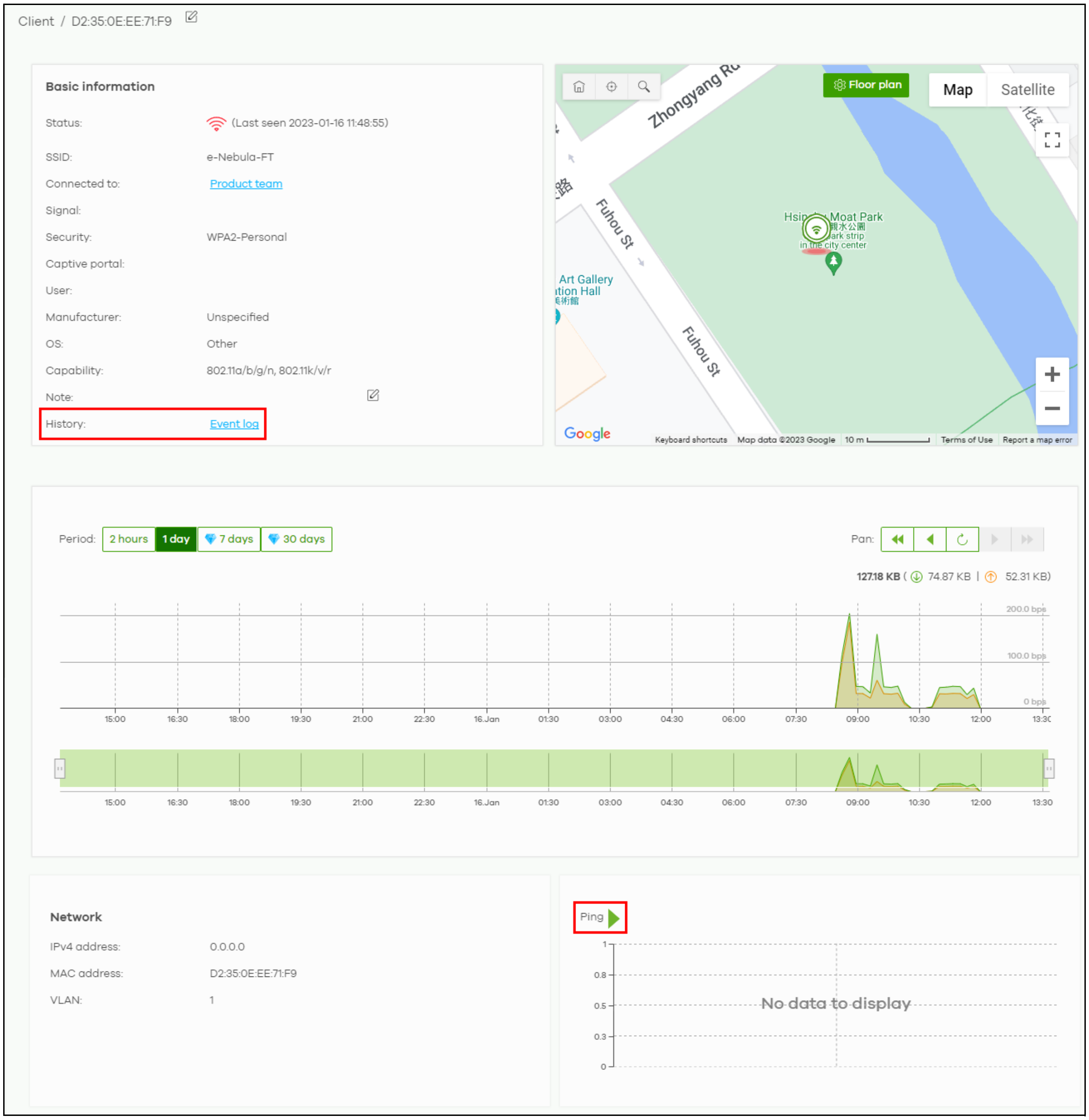


Failed clients

Show history within the time range

Client device	# Failed/total connections	Last failed issue
D6:5B:CD:1E:68:E1	2 / 7	Wireless connection
F6:11:BA:5E:AB:EF	2 / 5	Wireless connection
F6:6C:06:D2:51:AF	1 / 6	Wireless connection
TWNBNT03267-01	1 / 14	Wireless connection
72:11:10:FC:46:55	1 / 6	Wireless connection

The **Site-wide** > **Clients** > **Client list: WiFi client details** screen appears showing individual client statistics.



Client / D2:35:0E:EE:71:F9

Basic information

Status:	(Last seen 2023-01-16 11:48:55)
SSID:	e-Nebula-FT
Connected to:	Product team
Signal:	
Security:	WPA2-Personal
Captive portal:	
User:	
Manufacturer:	Unspecified
OS:	Other
Capability:	802.11a/b/g/n, 802.11k/v/r
Note:	
History:	Event log

Period: 2 hours | 1 day | 7 days | 30 days

Pan:

127.18 KB (74.87 KB | 52.31 KB)

Network

IPv4 address:	0.0.0.0
MAC address:	D2:35:0E:EE:71:F9
VLAN:	1

Ping

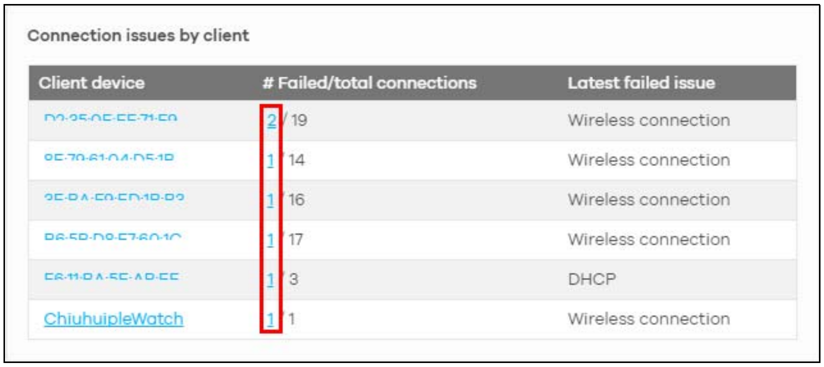
No data to display

2 Use the information in this screen to identify the WiFi client with connection issues. See Table 29 on page 263 for the description of the fields.

3 Click **History**: **Event log** to view Nebula AP log messages. Enter the Nebula AP's name or a key word, select one or multiple event types, or specify a date/time or even a time range to display only the log messages related to it.

4 Click **Ping** to ping the client's IP address from the Nebula AP to test connectivity.

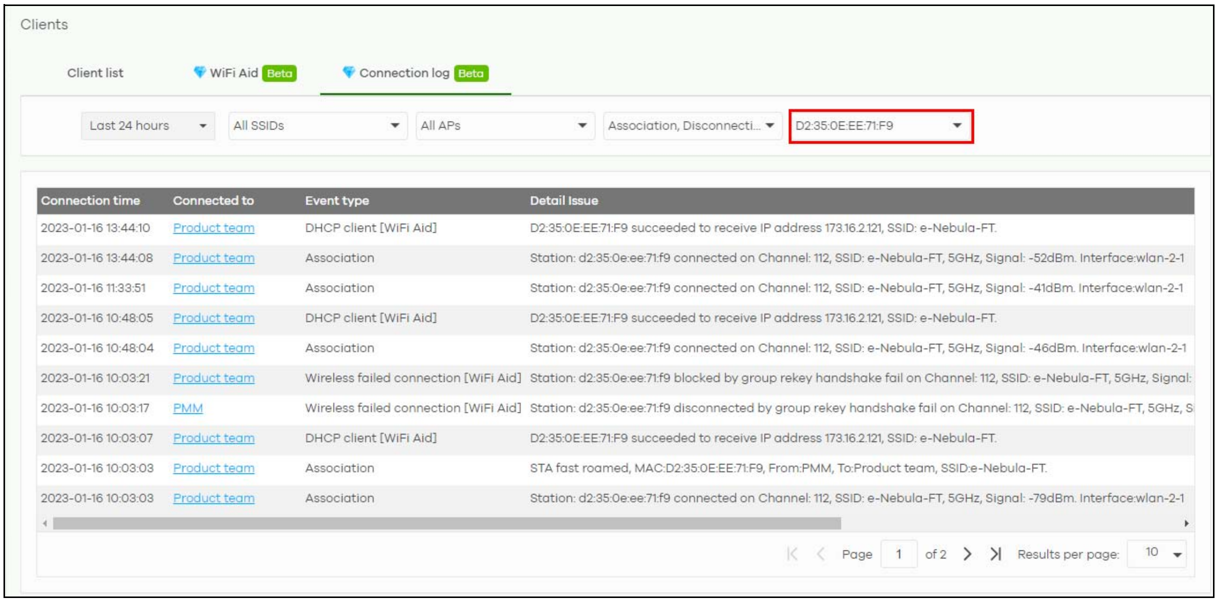
5 Click the numerator hyperlink in the **# Failed/total connections** column.



Connection issues by client

Client device	# Failed/total connections	Latest failed issue
D2:35:0E:EE:71:F9	2/ 19	Wireless connection
9E:70:61:04:D5:1B	1/ 14	Wireless connection
2E:BA:E0:ED:1B:B2	1/ 16	Wireless connection
B6:5B:D9:E7:60:1C	1/ 17	Wireless connection
E6:11:BA:5E:AB:EE	1/ 3	DHCP
ChiuhuipleWatch	1/ 1	Wireless connection

The **Site-wide** > **Clients** > **Connection log** screen appears showing all related event logs between APs and WiFi clients. See Section on page 149 on using the information listed in chronological order to resolve WiFi connection issues.



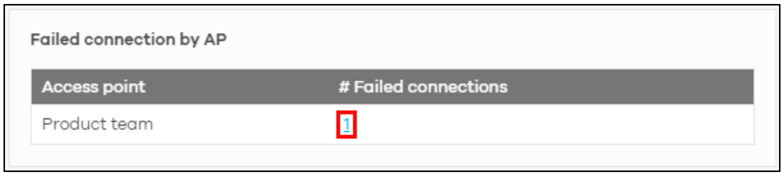
Last 24 hours ▾ All SSIDs ▾ All APs ▾ Association, Disconnecti... ▾ D2:35:0E:EE:71:F9 ▾

Connection time	Connected to	Event type	Detail Issue
2023-01-16 13:44:10	Product team	DHCP client [WiFi Aid]	D2:35:0E:EE:71:F9 succeeded to receive IP address 173.16.2.121, SSID: e-Nebula-FT.
2023-01-16 13:44:08	Product team	Association	Station: d2:35:0e:ee:71:f9 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -52dBm. Interface:wlan-2-1
2023-01-16 11:33:51	Product team	Association	Station: d2:35:0e:ee:71:f9 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -41dBm. Interface:wlan-2-1
2023-01-16 10:48:05	Product team	DHCP client [WiFi Aid]	D2:35:0E:EE:71:F9 succeeded to receive IP address 173.16.2.121, SSID: e-Nebula-FT.
2023-01-16 10:48:04	Product team	Association	Station: d2:35:0e:ee:71:f9 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -46dBm. Interface:wlan-2-1
2023-01-16 10:03:21	Product team	Wireless failed connection [WiFi Aid]	Station: d2:35:0e:ee:71:f9 blocked by group rekey handshake fail on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal:
2023-01-16 10:03:17	PMM	Wireless failed connection [WiFi Aid]	Station: d2:35:0e:ee:71:f9 disconnected by group rekey handshake fail on Channel: 112, SSID: e-Nebula-FT, 5GHz, S
2023-01-16 10:03:07	Product team	DHCP client [WiFi Aid]	D2:35:0E:EE:71:F9 succeeded to receive IP address 173.16.2.121, SSID: e-Nebula-FT.
2023-01-16 10:03:03	Product team	Association	STA fast roamed, MAC:D2:35:0E:EE:71:F9, From:PMM, To:Product team, SSID:e-Nebula-FT.
2023-01-16 10:03:03	Product team	Association	Station: d2:35:0e:ee:71:f9 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -79dBm. Interface:wlan-2-1

Connection Issues by Access Point

This table displays the number of WiFi clients with WiFi connection/DHCP failures/DNS failures listed according to access point. The list displays the access point with the most connection failures first, in descending order.

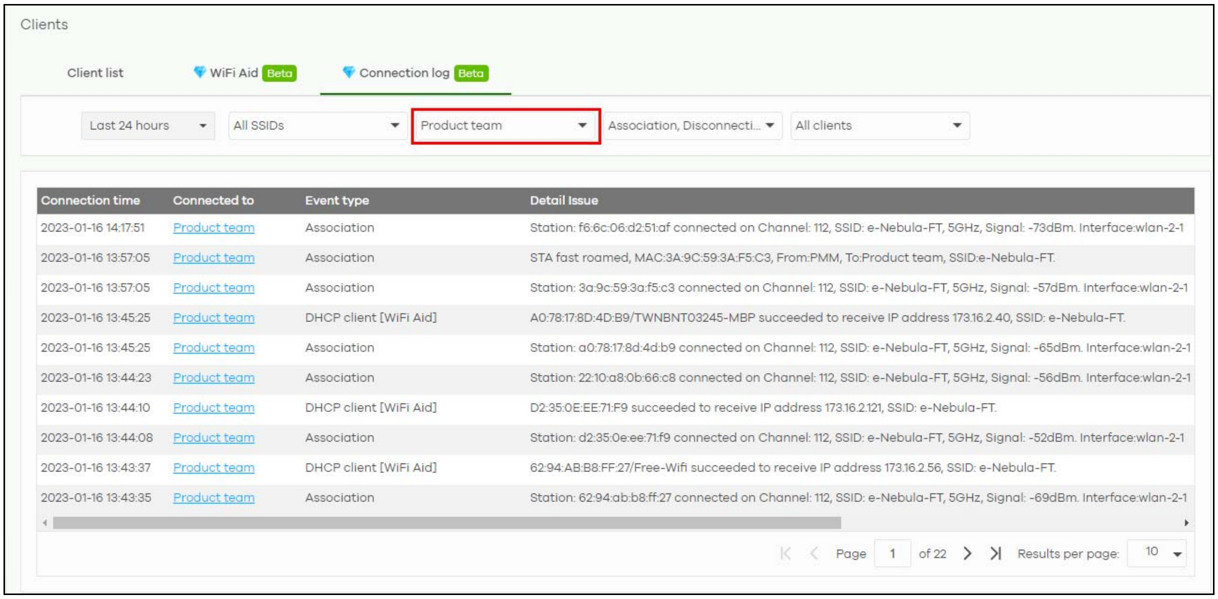
1 Click a hyperlink in the # **Failed connections** column of a specific AP.



Failed connection by AP

Access point	# Failed connections
Product team	1

The **Site-wide** > **Clients** > **Connection log** screen appears showing all related event logs between a specific AP (for example, Product team) and its WiFi clients. See Section on page 149 on using the information listed in chronological order to resolve WiFi connection issues.

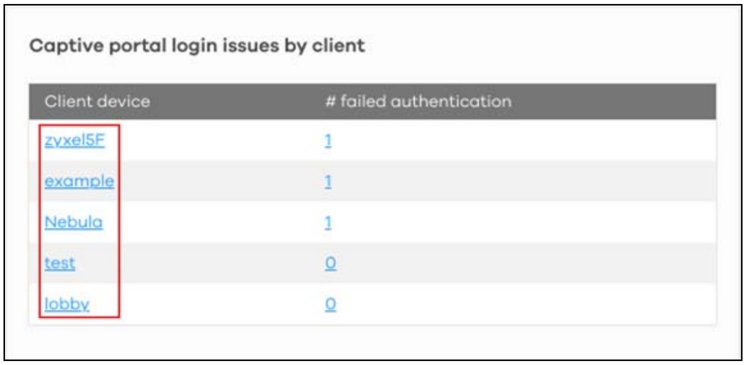


Connection time	Connected to	Event type	Detail Issue
2023-01-16 14:17:51	Product team	Association	Station: f6:6c:06:d2:51:af connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -73dBm. Interface:wlan-2-1
2023-01-16 13:57:05	Product team	Association	STA fast roamed, MAC:3A:9C:59:3A:F5:C3, From:PMM, To:Product team, SSID:e-Nebula-FT.
2023-01-16 13:57:05	Product team	Association	Station: 3a:9c:59:3a:f5:c3 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -57dBm. Interface:wlan-2-1
2023-01-16 13:45:25	Product team	DHCP client [WiFi Aid]	A0:78:17:8D:4D:B9/TWNBNT03245-MBP succeeded to receive IP address 173.16.2.40, SSID: e-Nebula-FT.
2023-01-16 13:45:25	Product team	Association	Station: a0:78:17:8d:4d:b9 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -65dBm. Interface:wlan-2-1
2023-01-16 13:44:23	Product team	Association	Station: 22:10:a8:0b:66:c8 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -56dBm. Interface:wlan-2-1
2023-01-16 13:44:10	Product team	DHCP client [WiFi Aid]	D2:35:0E:EE:71:F9 succeeded to receive IP address 173.16.2.121, SSID: e-Nebula-FT.
2023-01-16 13:44:08	Product team	Association	Station: d2:35:0e:ee:71:f9 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -52dBm. Interface:wlan-2-1
2023-01-16 13:43:37	Product team	DHCP client [WiFi Aid]	62:94:AB:B8:FF:27/Free-Wifi succeeded to receive IP address 173.16.2.56, SSID: e-Nebula-FT.
2023-01-16 13:43:35	Product team	Association	Station: 62:94:ab:b8:ff:27 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -69dBm. Interface:wlan-2-1

Captive Portal Login Issues by Client

This table displays the list of WiFi clients with the corresponding number of failed connection to the Nebula Device acting as a hotspot. The list displays the WiFi client that could not connect to the Nebula Device acting as a hotspot the most number of times first, in descending order.

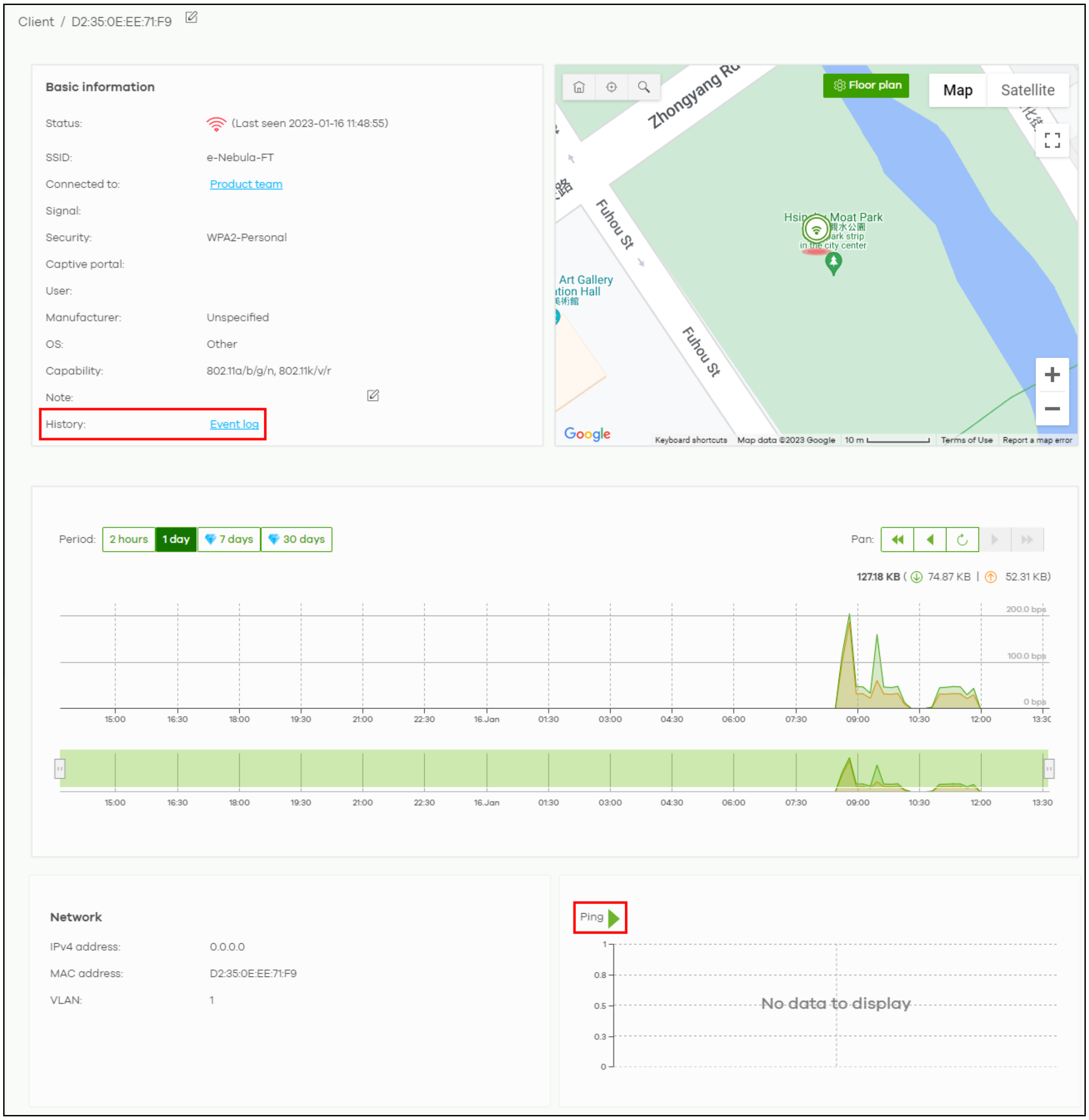
1 Click a hyperlink in the **Client device** column.



Captive portal login issues by client

Client device	# failed authentication
zyxel5F	1
example	1
Nebula	1
test	0
lobby	0

The **Site-wide** > **Clients** > **Client list: WiFi client details** screen appears showing individual client statistics. See Section on page 150 on setting the filters and using the information listed in chronological order to resolve WiFi connection issues.



Client / D2:35:0E:EE:71:F9

Basic information

Status:	(Last seen 2023-01-16 11:48:55)
SSID:	e-Nebula-FT
Connected to:	Product team
Signal:	
Security:	WPA2-Personal
Captive portal:	
User:	
Manufacturer:	Unspecified
OS:	Other
Capability:	802.11a/b/g/n, 802.11k/v/r
Note:	
History:	Event log

Period: 2 hours | 1 day | 7 days | 30 days

Pan:

127.18 KB (74.87 KB | 52.31 KB)

Network

IPv4 address:	0.0.0.0
MAC address:	D2:35:0E:EE:71:F9
VLAN:	1

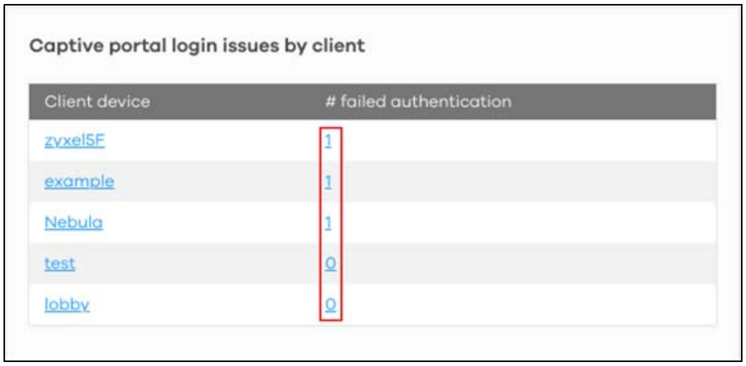
Ping

2 Use the information in this screen to identify the WiFi client with connection issues. See Table 29 on page 263 for the description of the fields.

3 Click **History**: **Event log** to view Nebula AP log messages. Enter the Nebula AP's name or a key word, select one or multiple event types, or specify a date/time or even a time range to display only the log messages related to it.

4 Click **Ping** to ping the client's IP address from the Nebula AP to test connectivity.

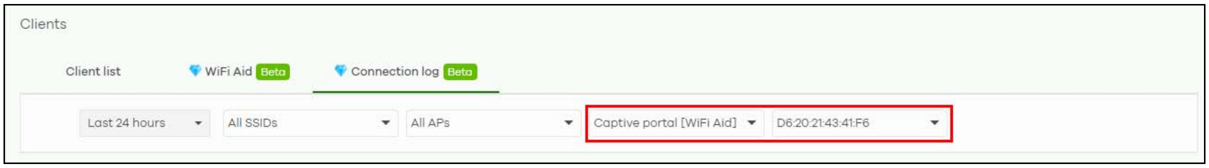
5 Click the hyperlink in the **# Failed authentication** column.



Captive portal login issues by client

Client device	# failed authentication
zyxel5F	1
example	1
Nebula	1
test	0
lobby	0

The **Site-wide** > **Clients** > **Connection log** screen appears showing all related event logs of a specific client device that could not connect to the Nebula Device acting as a hotspot.



Clients

Last 24 hours ▾ | All SSIDs ▾ | All APs ▾ | Captive portal [WiFi Aid] ▾ | D6:20:21:43:41:F6 ▾

6 Use the following information listed in chronological order to resolve WiFi clients that could not connect to the Nebula Device acting as a hotspot.

- **Connection time**. This shows the starting time period from which the event log occurred.
- **Detail issue**. This shows a summary of the APs event logs in chronological order.

3.30 Configure WiFi Security with WPA2 Personal (for Nebula Access Points only)

This tutorial shows you how to configure WPA2 Personal for an SSID.

An SSID (Service Set IDentifier) is the name of the WiFi network to which a WiFi client can connect.

WPA2 Personal uses pre-shared keys (PSK) for authentication of not so many users such as in a small office. IEEE 802.1X is an IEEE Standard for port-based network access control.

1 Create a WPA2 Personal QR code.

2 Allow WPA2 Personal authentication for this user.

3 Give the user the QR code.

3.30.1 Configure WPA2 Personal

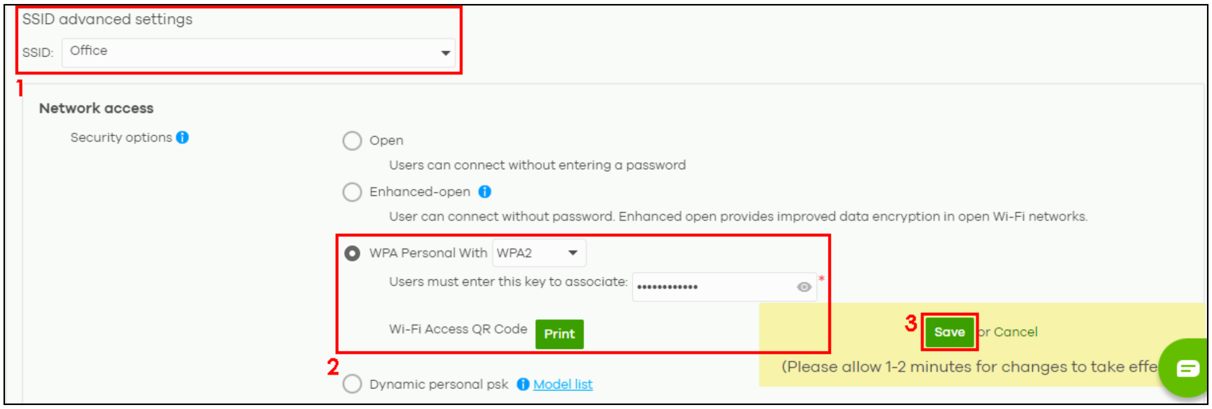
1 Go to **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**.

2 Select the **SSID** to which the settings you configure here will be applied.

3 In **Security options**, select **WPA2** in **WPA Personal With**.

4 To enable WPA2-PSK data encryption, enter a pre-shared key in **Users must enter this key to associate**. The allowed characters are 8 to 63 case-sensitive keyboard characters.

5 Click **Print** to display the QR code that includes the password for access to the WiFi network. You can save the QR code as PDF and pass it to users who are allowed to access this WiFi network. Note that anyone with this QR code can access the WiFi network.



SSID advanced settings

SSID: Office

Network access

Security options

○ Open
Users can connect without entering a password

○ Enhanced-open
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.

● WPA Personal With WPA2
Users must enter this key to associate: ••••••••••••
Wi-Fi Access QR Code Print

○ Dynamic personal psk Model list

Save or Cancel

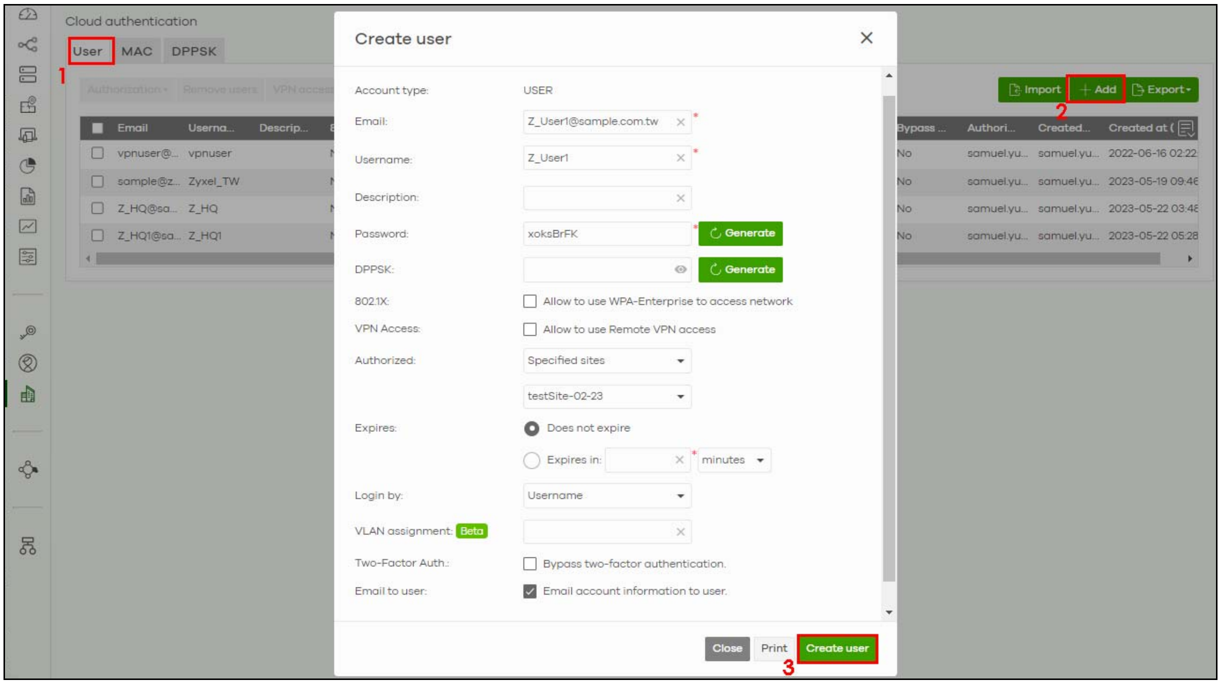
(Please allow 1-2 minutes for changes to take effe

6 Then click **Save**.

Manage User Accounts

1 Go to **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **User** to view and manage the specific user accounts which are authenticated using a pre-shared key.

2 Click **+Add** to create a new user account and fill in the user's information in the **Create user** window. Then click **Create user** to save your changes and close the screen.



Cloud authentication

User MAC DPPSK

Authorization ▾ Remove users VPN access

Email	Userna...	Descrip...	Bypass ...	Authori...	Created...	Created at (
vpnuser@...	vpnuser		No	samuel.yu...	samuel.yu...	2022-06-16 02:22
sample@z...	Zyxel_TW		No	samuel.yu...	samuel.yu...	2023-05-19 09:46
Z_HQ@sa...	Z_HQ		No	samuel.yu...	samuel.yu...	2023-05-22 03:48
Z_HQ1@sa...	Z_HQ1		No	samuel.yu...	samuel.yu...	2023-05-22 05:28

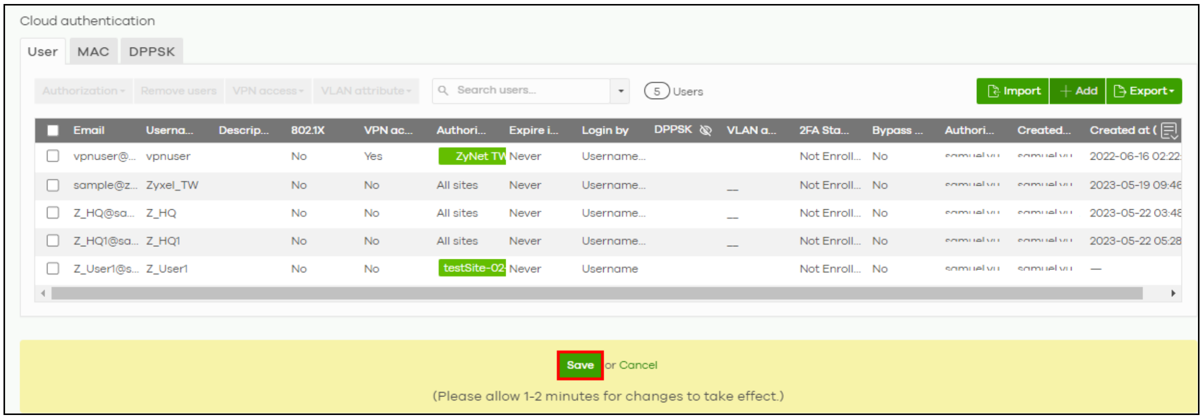
Import + Add Export ▾

Create user

Account type:	USER
Email:	Z_User1@sample.com.tw
Username:	Z_User1
Description:	
Password:	xoksBrFK Generate
DPPSK:	Generate
802.1X:	□ Allow to use WPA-Enterprise to access network
VPN Access:	□ Allow to use Remote VPN access
Authorized:	Specified sites testSite-02-23
Expires:	● Does not expire ○ Expires in: minutes
Login by:	Username
VLAN assignment Beta	
Two-Factor Auth.:	□ Bypass two-factor authentication.
Email to user:	☑ Email account information to user.

Close Print Create user

3 The click **Save**.



Cloud authentication

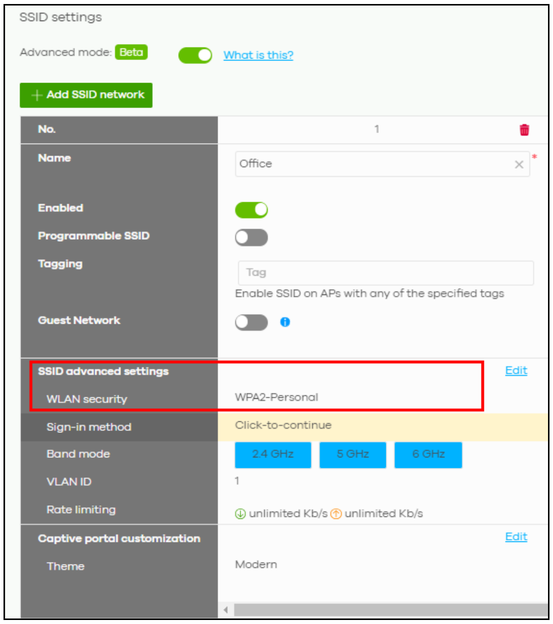
User | MAC | DPPSK

□	Email	Userna...	Descrip...	802.1X	VPN ac...	Authori...	Expire i...	Login by	DPPSK	VLAN a...	2FA Sta...	Bypass ...	Authori...	Created...	Created at (
□	vpnuser@...	vpnuser		No	Yes	ZyNet TW	Never	Username...			Not Enroll...	No	samuel yu	samuel yu	2022-06-16 02:22
□	sample@z...	Zyxel_TW		No	No	All sites	Never	Username...		_	Not Enroll...	No	samuel yu	samuel yu	2023-05-19 09:46
□	Z_HQ@sa...	Z_HQ		No	No	All sites	Never	Username...		_	Not Enroll...	No	samuel yu	samuel yu	2023-05-22 03:48
□	Z_HQ1@sa...	Z_HQ1		No	No	All sites	Never	Username...		_	Not Enroll...	No	samuel yu	samuel yu	2023-05-22 05:28
□	Z_User1@s...	Z_User1		No	No	testSite-02	Never	Username			Not Enroll...	No	samuel yu	samuel yu	—

(Please allow 1-2 minutes for changes to take effect.)

4 To check your settings, go to **Site-wide** > **Configure** > **SSID settings**.

WPA2-Personal is the encryption method shown on **SSID advanced settings**: **WLAN security**.



SSID settings

No.	1
Name	Office
Enabled	
Programmable SSID	
Tagging	Tag Enable SSID on APs with any of the specified tags
Guest Network	
SSID advanced settings	
WLAN security	WPA2-Personal
Sign-in method	Click-to-continue
Band mode	2.4 GHz 5 GHz 6 GHz
VLAN ID	1
Rate limiting	unlimited Kb/s unlimited Kb/s
Captive portal customization	
Theme	Modern

5 Give the user the QR code.

3.31 Configure WiFi Security with WPA2 Enterprise (for Nebula Access Points only)

This tutorial shows you how to configure WPA2 Enterprise for an SSID using any of the following authentication servers:

- Nebula Cloud server
- RADIUS server.

WPA2 Enterprise uses IEEE 802.1X for authentication of many users such as in a large organization.

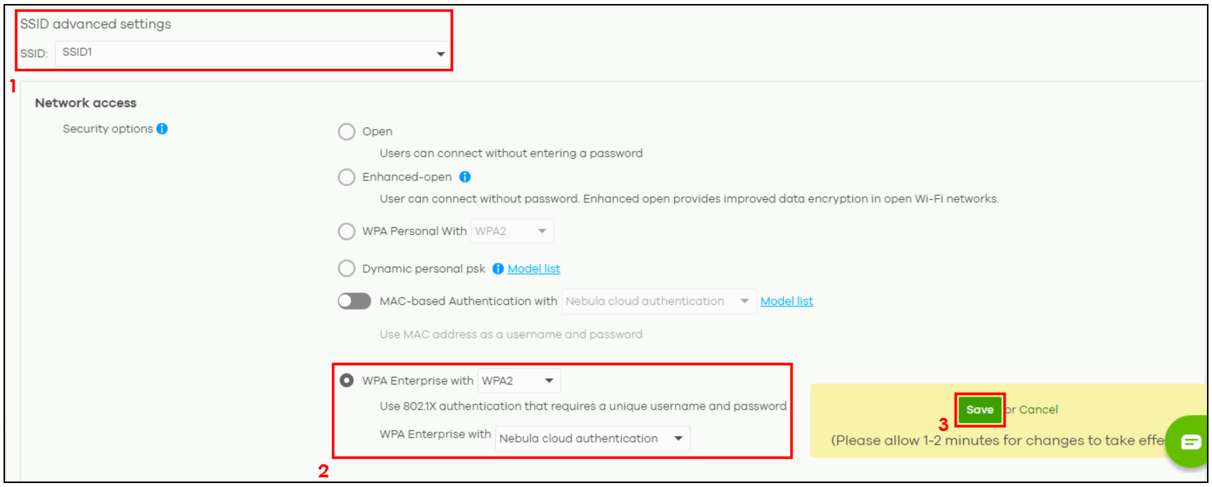
3.31.1 Configure WPA2 Enterprise with Nebula Cloud Authentication / RADIUS Server Authentication

1 Go to **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**.

2 Select the **SSID** to which the settings you configure here will be applied.

3 In **Security options**, select **WPA2** in **WPA Enterprise with**.

4 To use NCC's user database, select **Nebula cloud authentication** in **WPA Enterprise with**.

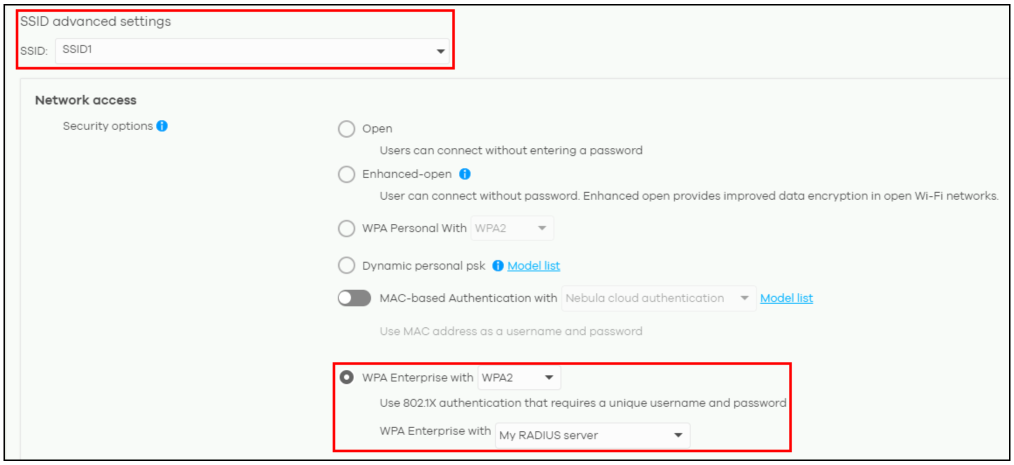


SSID advanced settings
SSID: SSID1

Network access
Security options
○ Open
Users can connect without entering a password
○ Enhanced-open
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.
○ WPA Personal With WPA2
○ Dynamic personal psk Model list
MAC-based Authentication with Nebula cloud authentication Model list
Use MAC address as a username and password
● WPA Enterprise with WPA2
Use 802.1X authentication that requires a unique username and password
WPA Enterprise with Nebula cloud authentication

Save or Cancel
(Please allow 1-2 minutes for changes to take effe

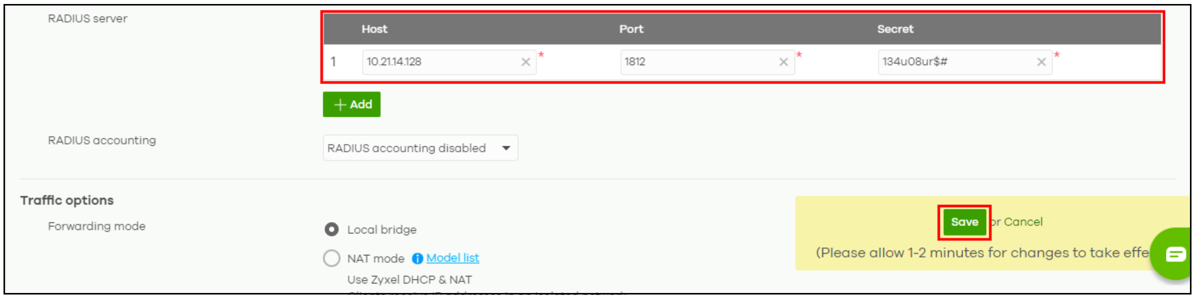
If your network has a RADIUS server for authentication, select **My RADIUS server** in **WPA Enterprise with**.



SSID advanced settings
SSID: SSID1

Network access
Security options
○ Open
Users can connect without entering a password
○ Enhanced-open
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.
○ WPA Personal With WPA2
○ Dynamic personal psk Model list
MAC-based Authentication with Nebula cloud authentication Model list
Use MAC address as a username and password
● WPA Enterprise with WPA2
Use 802.1X authentication that requires a unique username and password
WPA Enterprise with My RADIUS server

If you select **My RADIUS server** in step 4, enter the **RADIUS server**'s IP address/domain name in **RADIUS server**'s **Host**. Enter the **Port** number of the RADIUS server; the default is 1812. Enter up to 32 alphanumeric characters for the **Secret** password, which is the key to be shared between the external RADIUS server and the Nebula Device.



RADIUS server

	Host	Port	Secret
1	10.21.14.128	1812	134u08ur$#

RADIUS accounting: RADIUS accounting disabled

Traffic options

Forwarding mode: ● Local bridge ○ NAT mode Model list

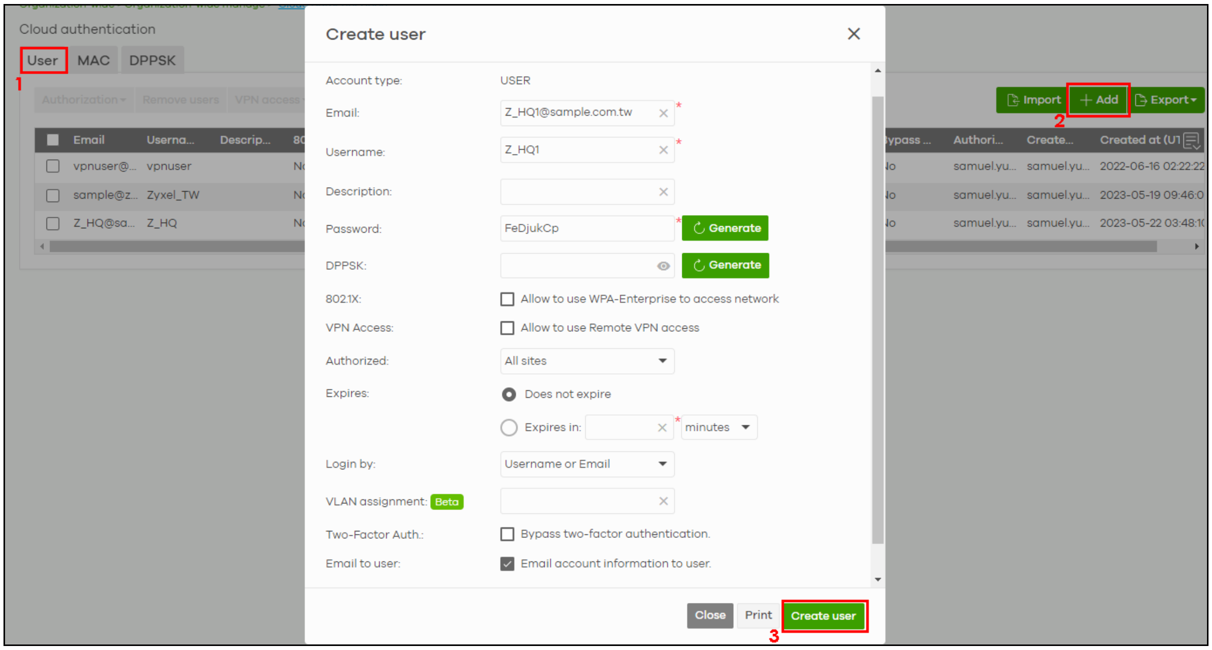
Use Zyxel DHCP & NAT

5 Then click **Save**.

Manage User Accounts

1 Go to **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **User** to view and manage the user accounts which are authenticated using the NCC user database or external RADIUS server.

2 Click **+Add** to create a new user account and fill in the user's information in the **Create user** window. Then click **Create user** to save your changes and close the screen.



Create user

Account type: USER

Email: Z_HQ1@sample.com.tw

Username: Z_HQ1

Description:

Password: FeDjukCp Generate

DPPSK: Generate

802.1X: □ Allow to use WPA-Enterprise to access network

VPN Access: □ Allow to use Remote VPN access

Authorized: All sites

Expires: ● Does not expire ○ Expires in: minutes

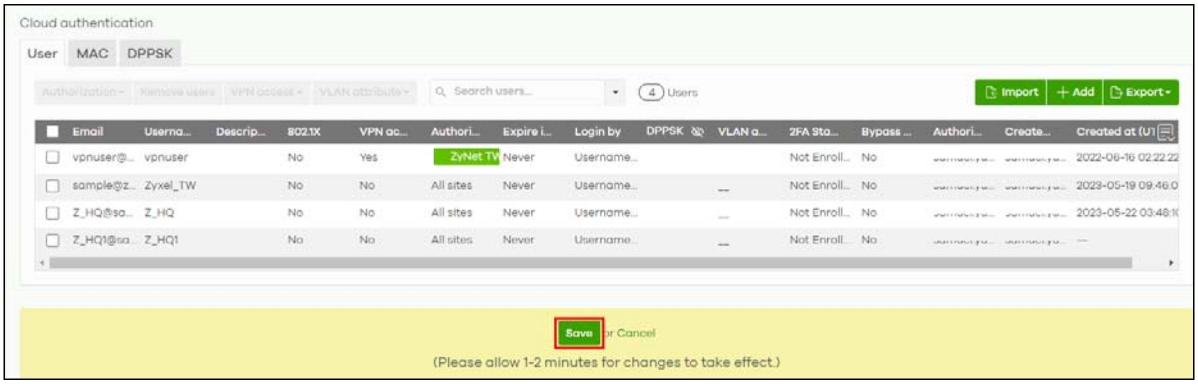
Login by: Username or Email

VLAN assignment: Beta

Two-Factor Auth.: □ Bypass two-factor authentication.

Email to user: ☑ Email account information to user.

3 The click **Save**.



Cloud authentication

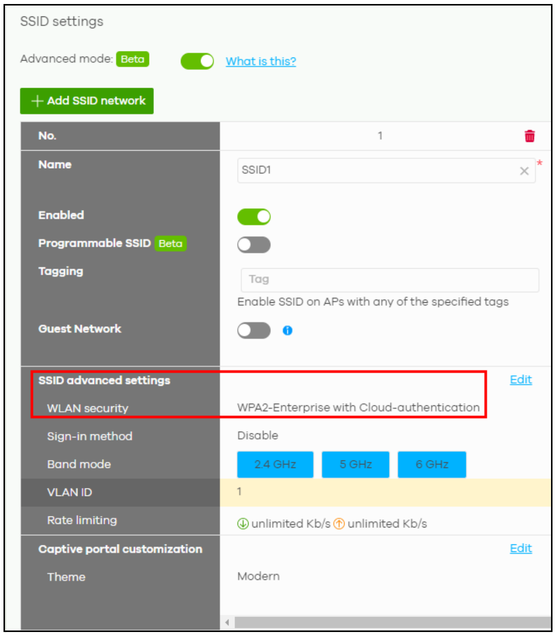
□	Email	Userna...	Descrip...	802.1X	VPN ac...	Authori...	Expire i...	Login by	DPPSK	VLAN a...	2FA Sta...	Bypass ...	Authori...	Create...	Created at (U1
□	vpnuser@...	vpnuser		No	Yes	ZyNet TV	Never	Username...			Not Enroll...	No	[illegible]	[illegible]	2022-06-16 02:22:22
□	sample@z...	Zyxel_TW		No	No	All sites	Never	Username...		—	Not Enroll...	No	[illegible]	[illegible]	2023-05-19 09:46:0
□	Z_HQ@sa...	Z_HQ		No	No	All sites	Never	Username...		—	Not Enroll...	No	[illegible]	[illegible]	2023-05-22 03:48:1
□	Z_HQ1@sa...	Z_HQ1		No	No	All sites	Never	Username...		—	Not Enroll...	No	[illegible]	[illegible]	—

(Please allow 1-2 minutes for changes to take effect.)

4 To check your settings, go to **Site-wide** > **Configure** > **SSID settings**.

For Nebula Cloud authentication, **WPA2-Enterprise with Cloud-authentication** is the encryption method shown on **SSID advanced settings: WLAN security**.

For RADIUS Server authentication, **WPA2-Enterprise with MyRADIUS** is the encryption method shown on **SSID advanced settings: WLAN security**.



SSID settings

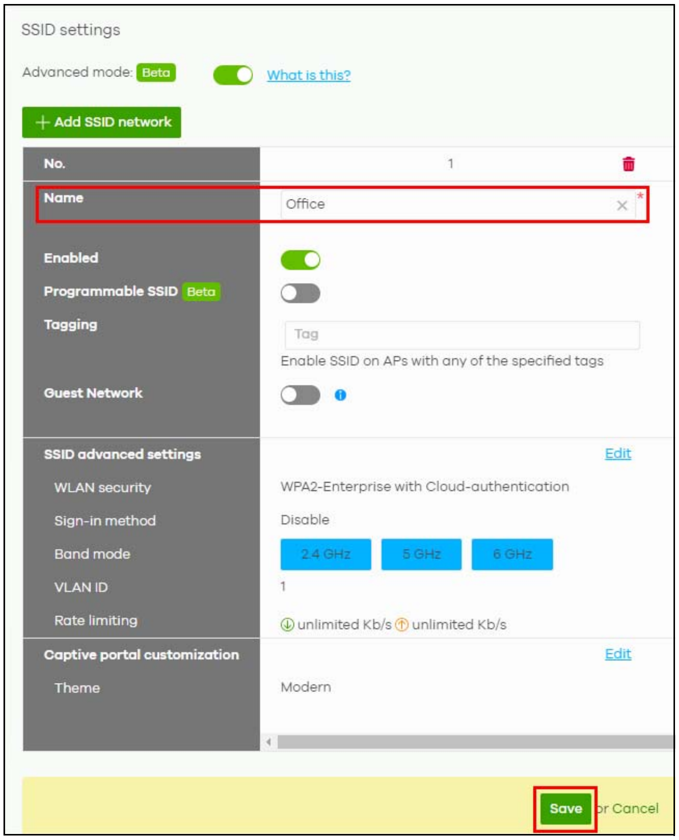
No.	1
Name	SSID1
Enabled	●
Programmable SSID Beta	○
Tagging	Tag Enable SSID on APs with any of the specified tags
Guest Network	○
SSID advanced settings	Edit
WLAN security	WPA2-Enterprise with Cloud-authentication
Sign-in method	Disable
Band mode	2.4 GHz 5 GHz 6 GHz
VLAN ID	1
Rate limiting	unlimited Kb/s unlimited Kb/s
Captive portal customization	Edit
Theme	Modern

3.32 Configure a Captive Portal

A captive portal is a login web page where a network user has to be authenticated before they can access the network.

This tutorial shows you how to configure captive portal settings for an SSID profile.

1 Go to **Site-wide** > **Configure** > **SSID settings** and enter the SSID **Name**. See Section 4.9.1 on page 277 for more information on configuring this screen. Then click **Save**.



SSID settings

Advanced mode: Beta ● What is this?

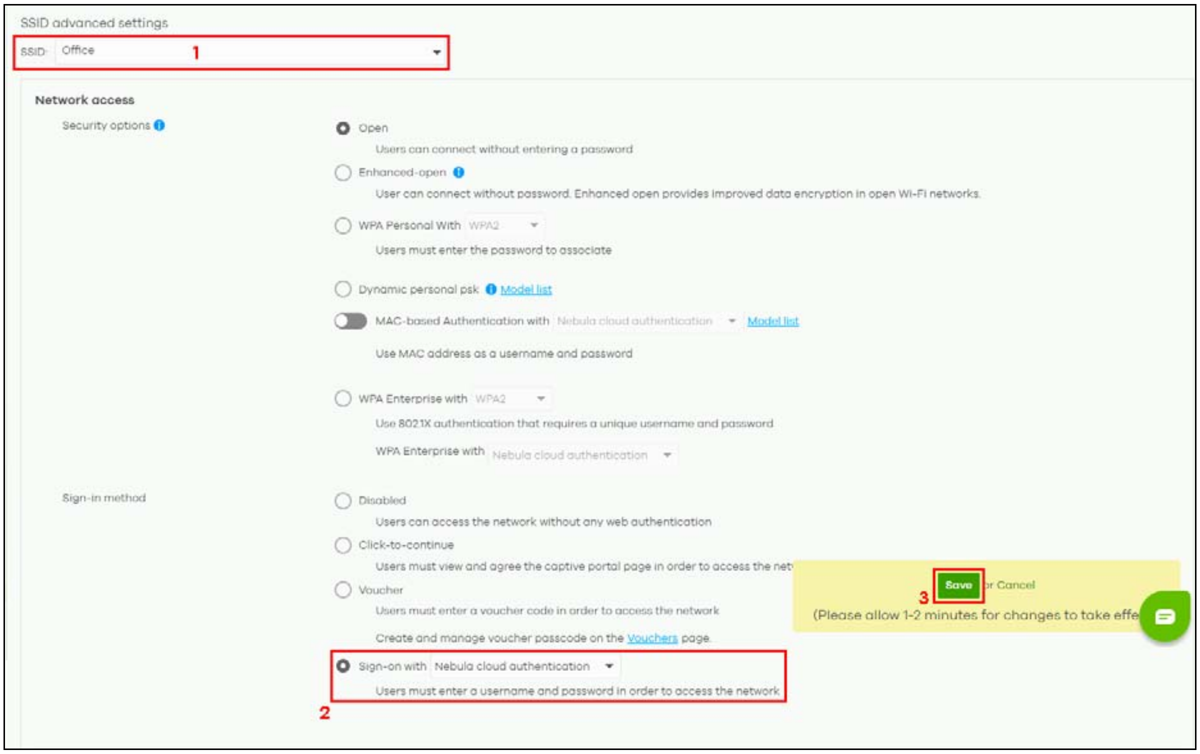
+ Add SSID network

No.	1
Name	Office
Enabled	●
Programmable SSID Beta	○
Tagging	Tag Enable SSID on APs with any of the specified tags
Guest Network	○
SSID advanced settings	Edit
WLAN security	WPA2-Enterprise with Cloud-authentication
Sign-in method	Disable
Band mode	2.4 GHz 5 GHz 6 GHz
VLAN ID	1
Rate limiting	unlimited Kb/s unlimited Kb/s
Captive portal customization	Edit
Theme	Modern

Save or Cancel

2 Go to **Site-wide** > **Configure** > **Access points** > **SSID advanced settings** and select the SSID **Name**: Office. Select the **Sign-on with**: **Nebula cloud authentication** to use the NCC user database to authenticate users. Then click **Save**.

Alternatively, select **My RADIUS server** to use a RADIUS server that will authenticate users. See Section 5.3.2 on page 320 for more information on configuring this screen.



SSID advanced settings

SSID: Office

Network access

Security options

● Open
Users can connect without entering a password

○ Enhanced-open
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.

○ WPA Personal With WPA2
Users must enter the password to associate

○ Dynamic personal psk Model list

MAC-based Authentication with Nebula cloud authentication Model list
Use MAC address as a username and password

○ WPA Enterprise with WPA2
Use 802.1X authentication that requires a unique username and password
WPA Enterprise with Nebula cloud authentication

Sign-in method

○ Disabled
Users can access the network without any web authentication

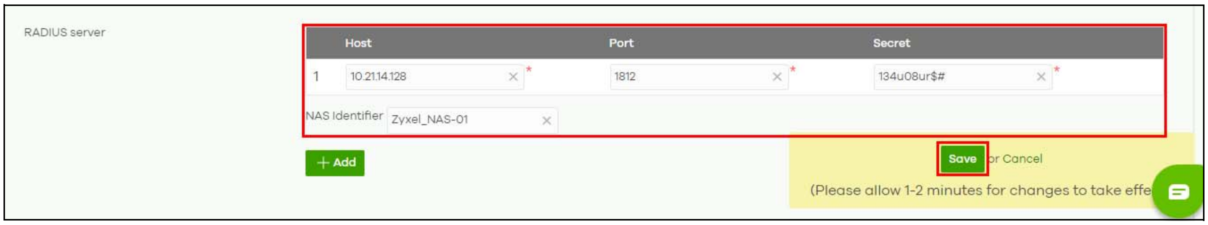
○ Click-to-continue
Users must view and agree the captive portal page in order to access the net

○ Voucher
Users must enter a voucher code in order to access the network
Create and manage voucher passcode on the Vouchers page.

● Sign-on with Nebula cloud authentication
Users must enter a username and password in order to access the network

Save or Cancel
(Please allow 1-2 minutes for changes to take effe

If you select **My RADIUS server** in step 2, enter the **RADIUS server**'s **Host**, **Port**, and **Secret**. Enter the Network Access Server (**NAS**) **identifier** on the Nebula Device to identify the Nebula Device to the RADIUS server, if required. This might be necessary if there are multiple Nebula Devices behind NAT using the same public WAN IP address for the RADIUS server. Then click **Save**.



RADIUS server

	Host	Port	Secret
1	10.2.114.128	1812	134u08ur$#

NAS Identifier: Zyxel_NAS-01

Save or Cancel
(Please allow 1-2 minutes for changes to take effe

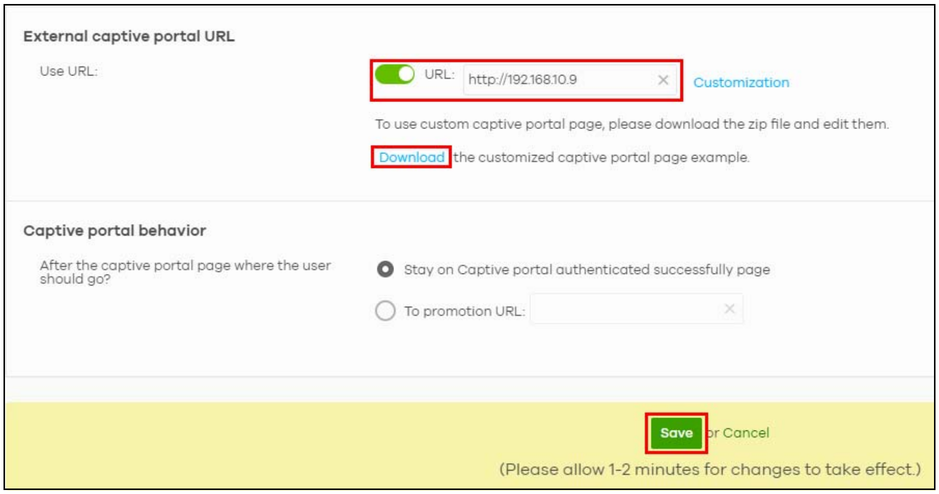
Note: Make sure to add the Nebula Device (AP) to the trusted device list in the RADIUS server.

3.33 Create a Custom Captive Portal Page

1 Go to **Site-wide** > **Configure** > **Access points** > **Captive portal customization**. Click the switch to the right to use a custom login page from an external web portal instead of the one built into the NCC. See Section 5.3.3 on page 330 for more information on configuring this screen.

2 Specify the login page's URL; for example, http://IIS server IP Address/login.asp. The Internet Information Server (IIS) is the web server on which the web portal files are installed.

3 Click **Download** to download a ZIP file containing example captive port HTML files. Unzip and edit these HTML files to upload to a webserver that is accessible from NCC.



External captive portal URL

Use URL: ● URL: http://192.168.10.9 Customization

To use custom captive portal page, please download the zip file and edit them.

Download the customized captive portal page example.

Captive portal behavior

After the captive portal page where the user should go?

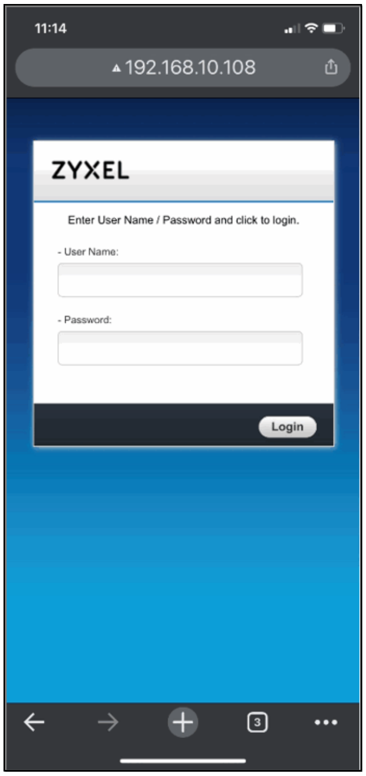
● Stay on Captive portal authenticated successfully page

○ To promotion URL:

(Please allow 1-2 minutes for changes to take effect.)

4 Then click **Save**.

5 To check your captive portal settings, enter the URL http://<server IP address>/<page name> in your browser on your smartphone or PC to confirm the login page.



Enter User Name / Password and click to login.

- User Name:

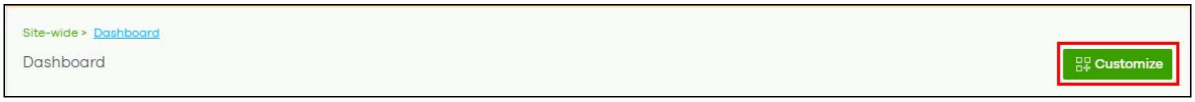
- Password:

3.34 Limit Applications Usage or Block Applications

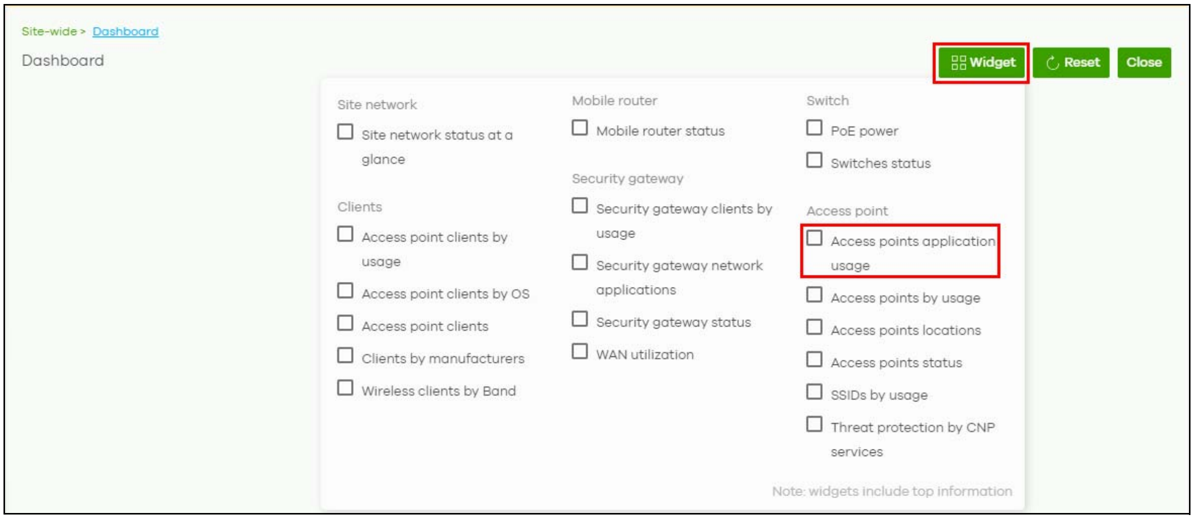
To control network traffic throughput by limiting or blocking specific applications using too much bandwidth, do the following:

Limit Applications Usage

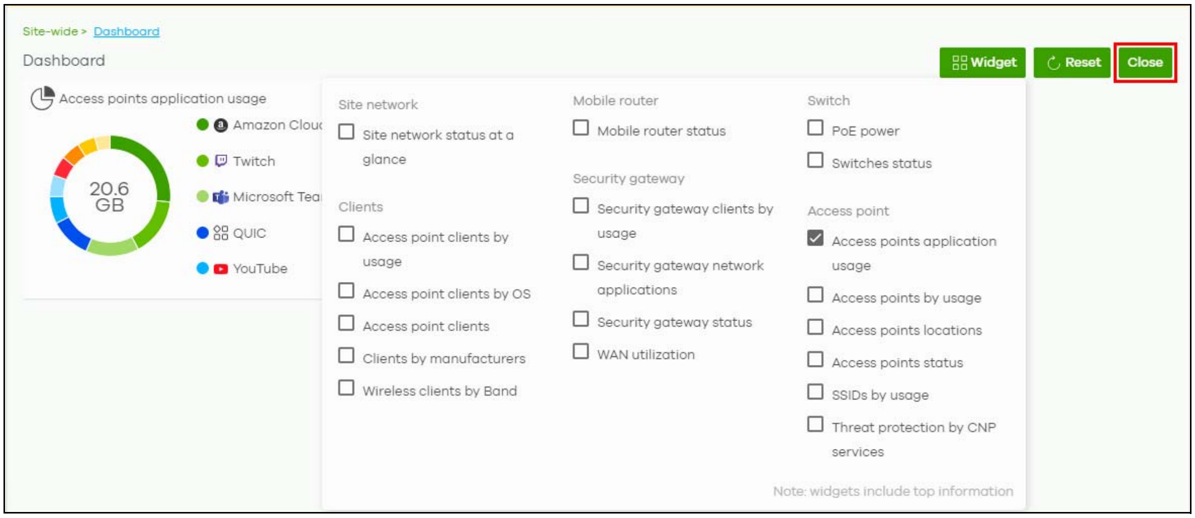
1 To filter the list of widgets to display on the **Dashboard** screen, go to **Site-wide** > **Dashboard** and click **Customize** to show the **Widget**, **Reset** and **Close** buttons.



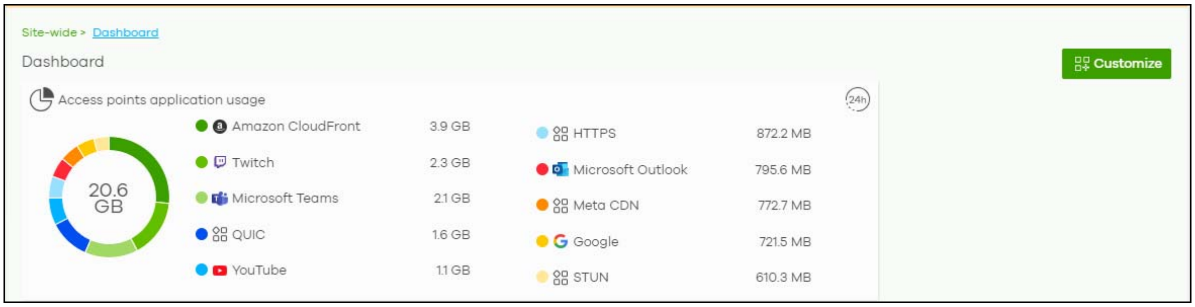
2 Click **Widget** to filter the list of widgets to display on the **Dashboard** screen and select **Access points application usage**.


Site-wide > Dashboard
Dashboard
Widget
Reset
Close
Site network
□ Site network status at a glance
Clients
□ Access point clients by usage
□ Access point clients by OS
□ Access point clients
□ Clients by manufacturers
□ Wireless clients by Band
Mobile router
□ Mobile router status
Security gateway
□ Security gateway clients by usage
□ Security gateway network applications
□ Security gateway status
□ WAN utilization
Switch
□ PoE power
□ Switches status
Access point
□ Access points application usage
□ Access points by usage
□ Access points locations
□ Access points status
□ SSIDs by usage
□ Threat protection by CNP services
Note: widgets include top information

3 Then click **Close**.


Site-wide > Dashboard
Dashboard
Access points application usage
20.6 GB
Amazon Clou
Twitch
Microsoft Tea
QUIC
YouTube
Widget
Reset
Close
Site network
□ Site network status at a glance
Clients
□ Access point clients by usage
□ Access point clients by OS
□ Access point clients
□ Clients by manufacturers
□ Wireless clients by Band
Mobile router
□ Mobile router status
Security gateway
□ Security gateway clients by usage
□ Security gateway network applications
□ Security gateway status
□ WAN utilization
Switch
□ PoE power
□ Switches status
Access point
☑ Access points application usage
□ Access points by usage
□ Access points locations
□ Access points status
□ SSIDs by usage
□ Threat protection by CNP services
Note: widgets include top information

The **Access points application usage** widget appears. This allows you to view the top ten applications used by the Nebula access points in the site in the past 24 hours.



Site-wide > Dashboard

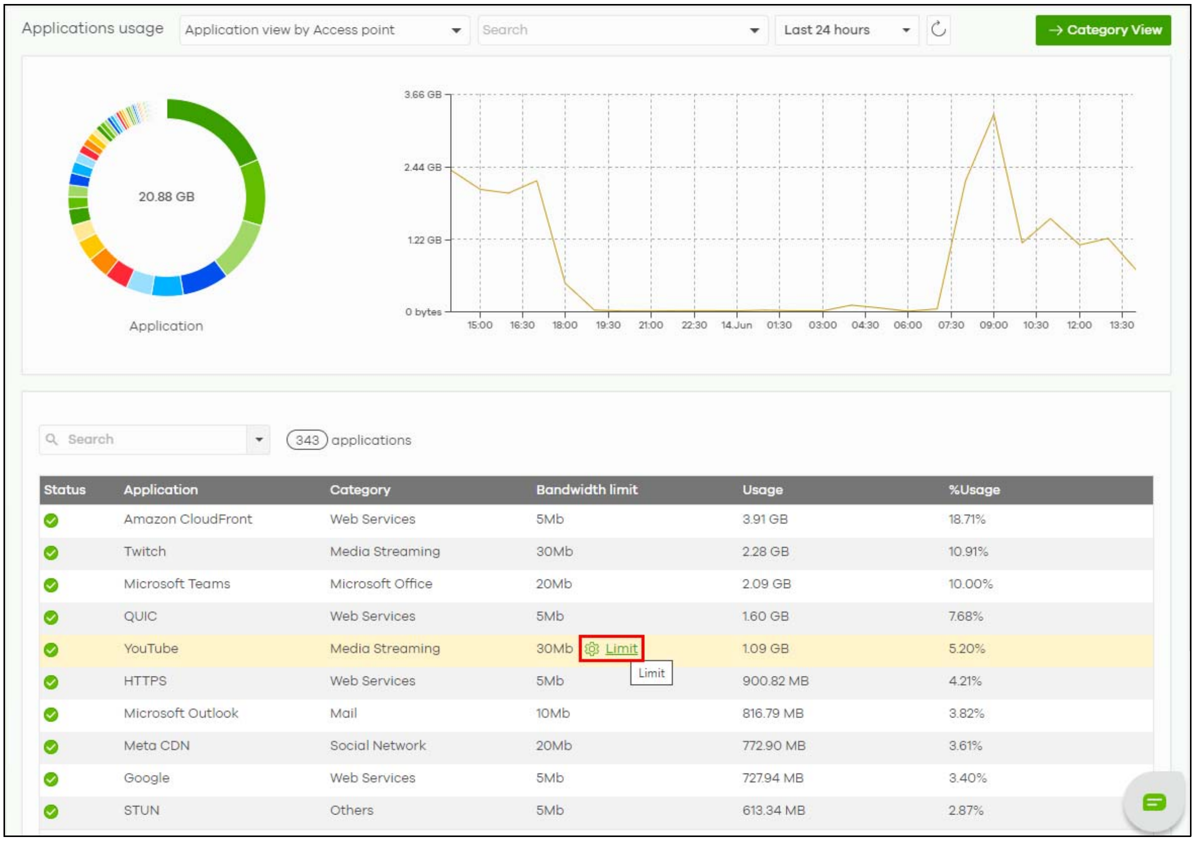
Dashboard

Customize

Access points application usage

Amazon CloudFront	3.9 GB	HTTPS	872.2 MB
Twitch	2.3 GB	Microsoft Outlook	795.6 MB
Microsoft Teams	2.1 GB	Meta CDN	772.7 MB
QUIC	1.6 GB	Google	721.5 MB
YouTube	1.1 GB	STUN	610.3 MB

4 Go to **Site-wide** > **Applications usage** to view the usage statistics for applications used in the site. Hover the mouse on the application (for example, YouTube) you wish to limit the bandwidth and click **Limit**.



Applications usage | Application view by Access point | Search | Last 24 hours | Category View

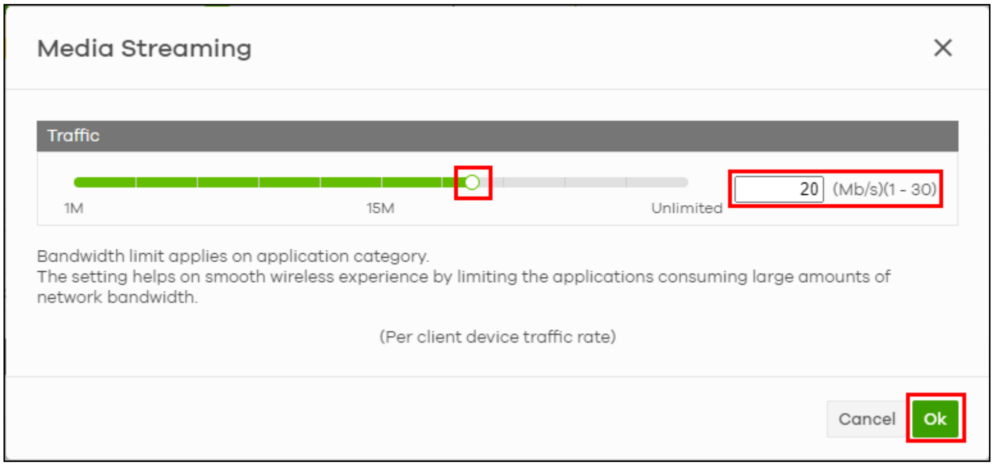
Search | 343 applications

Status	Application	Category	Bandwidth limit	Usage	%Usage
✓	Amazon CloudFront	Web Services	5Mb	3.91 GB	18.71%
✓	Twitch	Media Streaming	30Mb	2.28 GB	10.91%
✓	Microsoft Teams	Microsoft Office	20Mb	2.09 GB	10.00%
✓	QUIC	Web Services	5Mb	1.60 GB	7.68%
✓	YouTube	Media Streaming	30Mb Limit	1.09 GB	5.20%
✓	HTTPS	Web Services	5Mb	900.82 MB	4.21%
✓	Microsoft Outlook	Mail	10Mb	816.79 MB	3.82%
✓	Meta CDN	Social Network	20Mb	772.90 MB	3.61%
✓	Google	Web Services	5Mb	727.94 MB	3.40%
✓	STUN	Others	5Mb	613.34 MB	2.87%

5 On the **Media Streaming** screen that appears, set the maximum bandwidth by:

- using the slider, or
- entering the bandwidth limit (1 to 30 Mb/s).

Then click **Ok**.



Media Streaming

Traffic

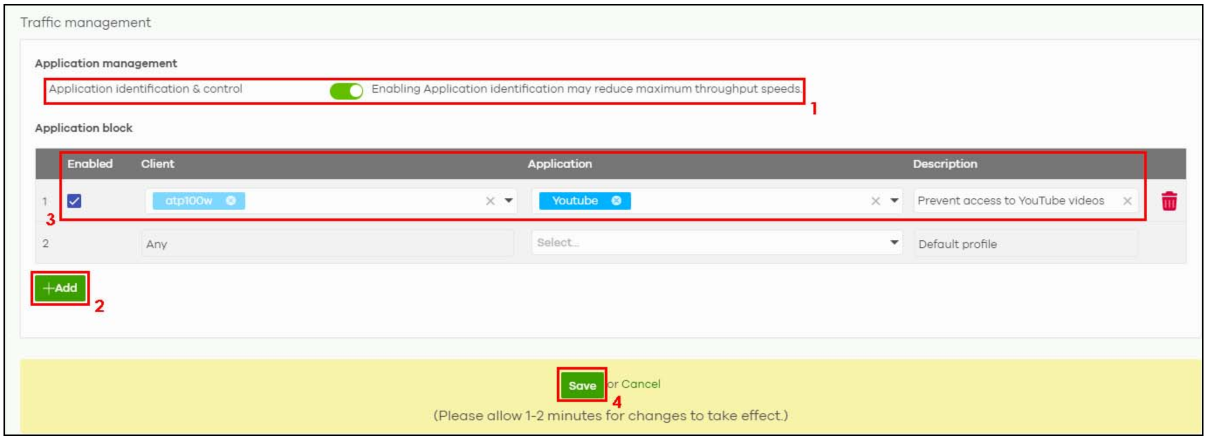
Bandwidth limit applies on application category.
The setting helps on smooth wireless experience by limiting the applications consuming large amounts of network bandwidth.

(Per client device traffic rate)

Block Applications

Go to the **Site-wide** > **Configure** > **Security router** > **Traffic management** screen and do the following:

- Click the **Application identification & control** switch to the right to control usage of applications.
- Click **+Add** to create up to 5 application management profiles.
- Select the **Enabled** checkbox to turn on the rule. Select the **Client** to which this rule applies. Select the YouTube **Application** to apply the rule. Then enter a **Description** for this profile (up to 512 characters long).
- Then click **Save** to create a new application management profile.



Traffic management

Application management

Application identification & control — Enabling Application identification may reduce maximum throughput speeds

Application block

	Enabled	Client	Application	Description
1	☑	atp100w	Youtube	Prevent access to YouTube videos
2		Any	Select...	Default profile

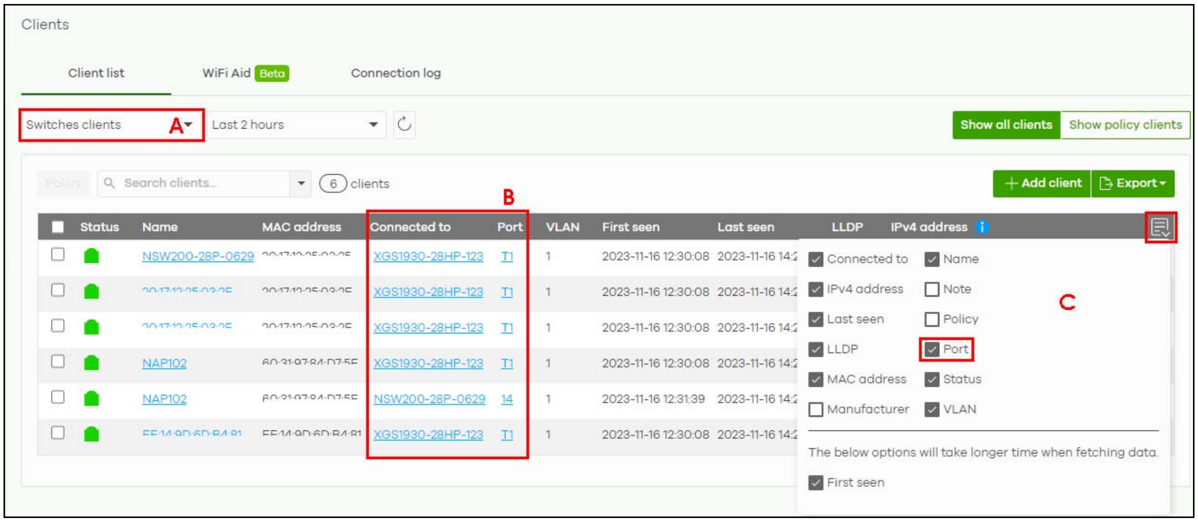
(Please allow 1-2 minutes for changes to take effect.)

3.35 Find the LAN Port Used by Connected Wired Client Devices (for Nebula Switches only)

To view a list of all wired clients connected to the Nebula Device in a site and also see the corresponding port connection, do the following:

Method 1:

1 Go to **Site-wide** > **Clients** > **Client list** tab and select **Switches clients** (A) to filter the list of clients based on the type of Nebula Device.



Clients

Client list | WiFi Aid Beta | Connection log

Switches clients A | Last 2 hours | Show all clients | Show policy clients

Policy | Search clients... | 6 clients | + Add client | Export

B

□	Status	Name	MAC address	Connected to	Port	VLAN	First seen	Last seen	LLDP	IPv4 address
□	🟩	NSW200-28P-0629	20:17:12:25:03:25	XGS1930-28HP-123	T1	1	2023-11-16 12:30:08	2023-11-16 14:2		
□	🟩	20:17:12:25:03:25	20:17:12:25:03:25	XGS1930-28HP-123	T1	1	2023-11-16 12:30:08	2023-11-16 14:2		
□	🟩	20:17:12:25:03:25	20:17:12:25:03:25	XGS1930-28HP-123	T1	1	2023-11-16 12:30:08	2023-11-16 14:2		
□	🟩	NAP102	60:31:07:84:D7:5F	XGS1930-28HP-123	T1	1	2023-11-16 12:30:08	2023-11-16 14:2		
□	🟩	NAP102	60:31:07:84:D7:5F	NSW200-28P-0629	14	1	2023-11-16 12:31:39	2023-11-16 14:2		
□	🟩	FE:14:9D:6D:B4:81	FE:14:9D:6D:B4:81	XGS1930-28HP-123	T1	1	2023-11-16 12:30:08	2023-11-16 14:2		

☑ Connected to ☑ Name
☑ IPv4 address □ Note
☑ Last seen □ Policy
☑ LLDP ☑ Port
☑ MAC address ☑ Status
□ Manufacturer ☑ VLAN

The below options will take longer time when fetching data.

☑ First seen

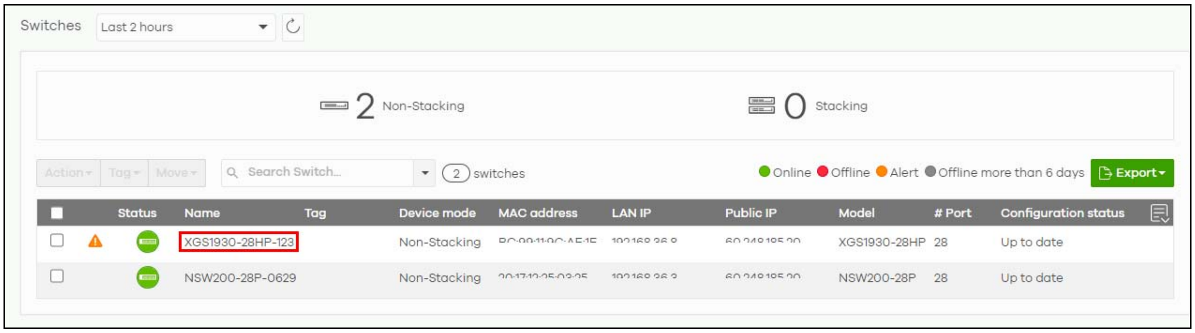
C

2 Locate the **Port** column (B) to know the port to which the client is connected.

Note: If you do not find the **Port** column (B), click the icon (C) and select **Port** to display the **Port** column (B).

Method 2:

1 Go to **Site-wide** > **Devices** > **Switches** and click the **Name** of the Switch to go to the Switch details screen.



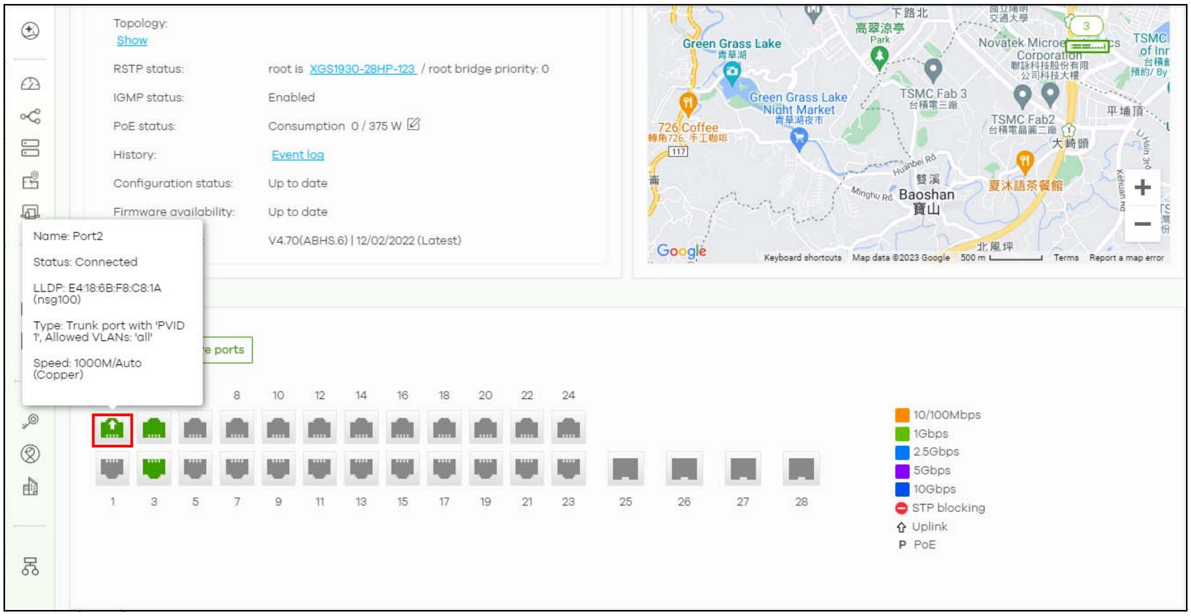
Switches | Last 2 hours

2 Non-Stacking | 0 Stacking

Action | Tag | Move | Search Switch... | 2 switches | ● Online ● Offline ● Alert ● Offline more than 6 days | Export

□		Status	Name	Tag	Device mode	MAC address	LAN IP	Public IP	Model	# Port	Configuration status
□	⚠	●	XGS1930-28HP-123		Non-Stacking	BC:99:11:9C:AE:1E	192.168.36.8	60.248.185.20	XGS1930-28HP	28	Up to date
□		●	NSW200-28P-0629		Non-Stacking	20:17:12:25:03:25	192.168.36.3	60.248.185.20	NSW200-28P	28	Up to date

2 Scroll down to the **Ports** section and hover the mouse over a port to know which client is connected.



Topology: Show

RSTP status: root is XGS1930-28HP-123 / root bridge priority: 0

IGMP status: Enabled

PoE status: Consumption 0 / 375 W

History: Event log

Configuration status: Up to date

Firmware availability: Up to date

V4.70(ABHS.6) | 12/02/2022 (Latest)

Name: Port2

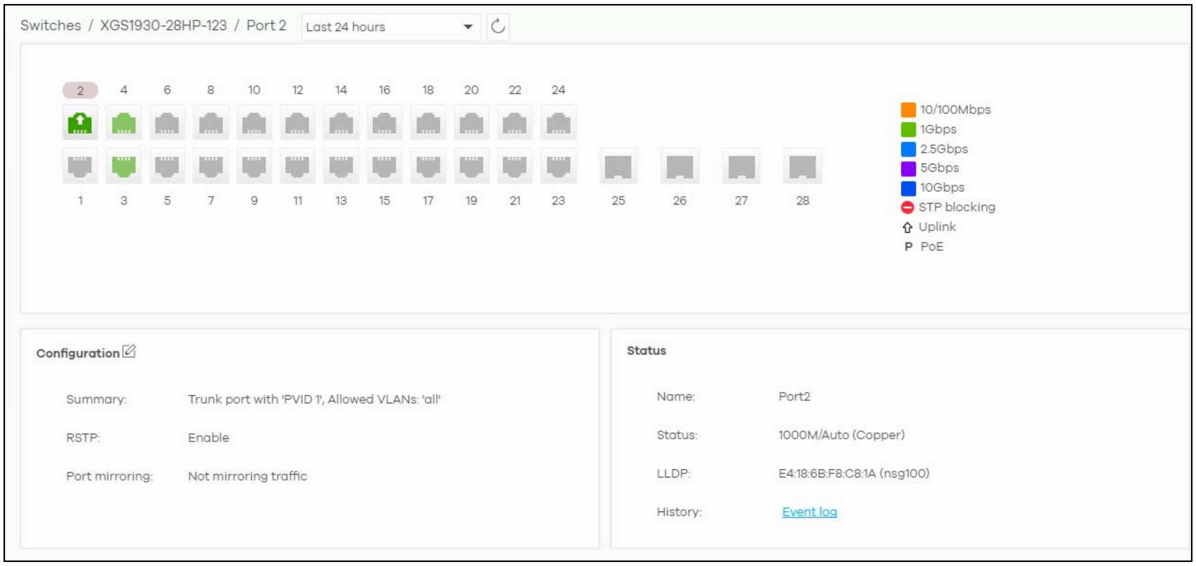
Status: Connected

LLDP: E4:18:6B:F8:C8:1A (nsg100)

Type: Trunk port with 'PVID 1', Allowed VLANs: 'all'

Speed: 1000M/Auto (Copper)

3 Click the port to go to the Switch port details screen to view the individual Nebula Device port statistics.



Switches / XGS1930-28HP-123 / Port 2 Last 24 hours

Configuration

Summary: Trunk port with 'PVID 1', Allowed VLANs: 'all'

RSTP: Enable

Port mirroring: Not mirroring traffic

Status

Name: Port2

Status: 1000M/Auto (Copper)

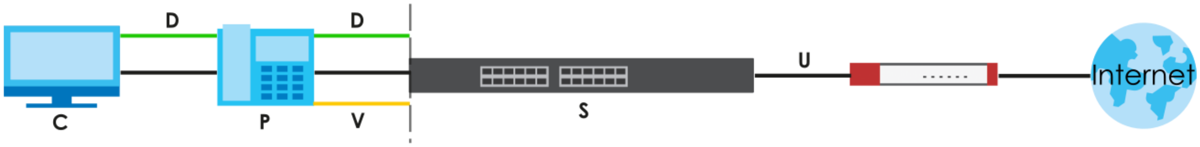
LLDP: E4:18:6B:F8:C8:1A (nsg100)

History: Event log

3.36 Configure Voice VLAN (for Nebula Switches only)

VoIP (voice over Internet protocol) devices are commonly in use in office environments. When designing a network, assign a higher priority to voice traffic. Use voice VLAN to prioritize voice packets from a VoIP device, and separate data packets from a computer.

As shown in the next figure, connect the VoIP device (P) to the Nebula Device (S) on one end. Connect the computer (C) to the VoIP device (P) on the other end. The VoIP device (P) serves as a bridge for both the Nebula Device (S) and computer (C).



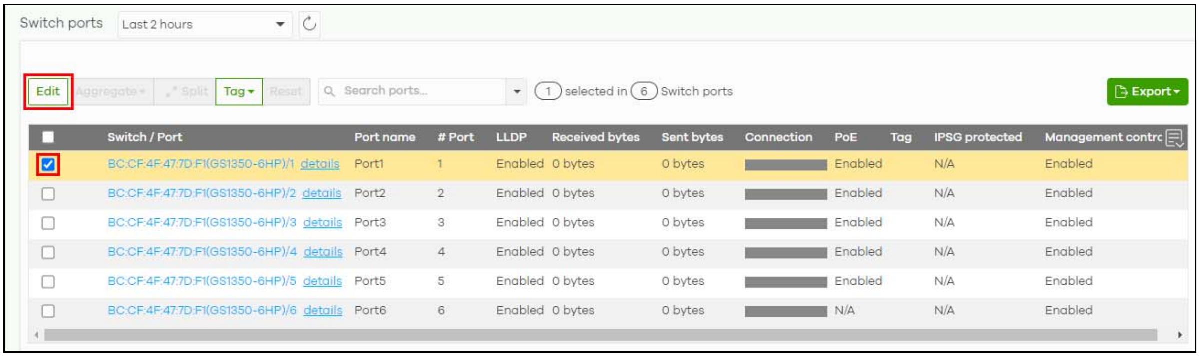
The Nebula Device will add a VLAN tag for voice packets (V) and data packets (D) separately after receiving them. Then forward the voice packets (V) and data packets (D) to the uplink port (U). This section shows you how to separate data packets (D) and voice packets (V) between a VoIP device (P) and computer (C), without having to assign a VLAN tag.

- Configure the Nebula Device Ports
- Configure the Voice VLAN

3.36.1 Configure the Nebula Device Ports

1 Go to **Site-wide** > **Configure** > **Switches** > **Switch ports**.

2 Select the port that connects to a VoIP device and click **Edit**.



1 selected in 6 Switch ports

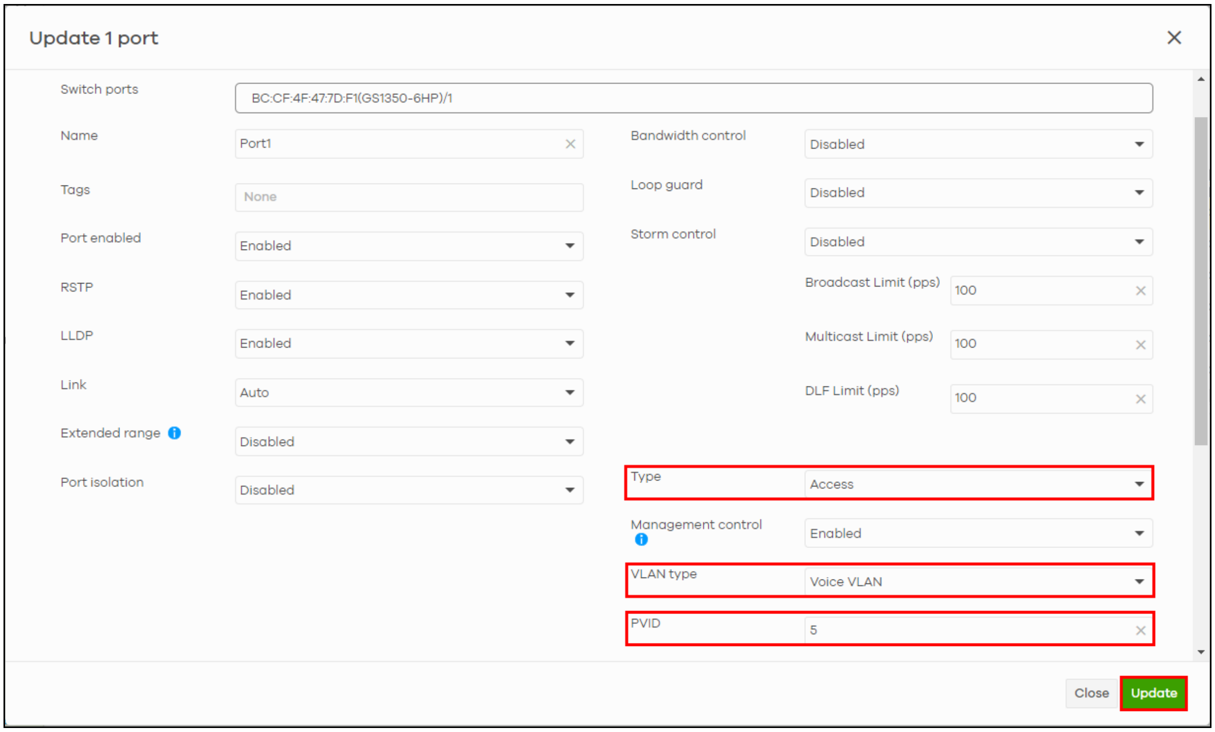
☐	Switch / Port	Port name	# Port	LLDP	Received bytes	Sent bytes	Connection	PoE	Tag	IPSG protected	Management contrc
☑	BC:CF:4F:47:7D:F1(GS1350-6HP)/1 details	Port1	1	Enabled	0 bytes	0 bytes	▬	Enabled		N/A	Enabled
☐	BC:CF:4F:47:7D:F1(GS1350-6HP)/2 details	Port2	2	Enabled	0 bytes	0 bytes	▬	Enabled		N/A	Enabled
☐	BC:CF:4F:47:7D:F1(GS1350-6HP)/3 details	Port3	3	Enabled	0 bytes	0 bytes	▬	Enabled		N/A	Enabled
☐	BC:CF:4F:47:7D:F1(GS1350-6HP)/4 details	Port4	4	Enabled	0 bytes	0 bytes	▬	Enabled		N/A	Enabled
☐	BC:CF:4F:47:7D:F1(GS1350-6HP)/5 details	Port5	5	Enabled	0 bytes	0 bytes	▬	Enabled		N/A	Enabled
☐	BC:CF:4F:47:7D:F1(GS1350-6HP)/6 details	Port6	6	Enabled	0 bytes	0 bytes	▬	N/A		N/A	Enabled

3 Select **Access** for the port **Type**.

4 Select **Voice VLAN** for the **VLAN type**.

5 Assign a **PVID** for the port. Use the PVID to tag data packets with the VLAN ID.

6 Then click **Update**.



Update 1 port

Switch ports	BC:CF:4F:47:7D:F1(GS1350-6HP)/1		
Name	Port1	Bandwidth control	Disabled
Tags	None	Loop guard	Disabled
Port enabled	Enabled	Storm control	Disabled
RSTP	Enabled	Broadcast Limit (pps)	100
LLDP	Enabled	Multicast Limit (pps)	100
Link	Auto	DLF Limit (pps)	100
Extended range	Disabled	Type	Access
Port isolation	Disabled	Management control	Enabled
		VLAN type	Voice VLAN
		PVID	5

3.36.2 Configure the Voice VLAN

1 Go to **Site-wide** > **Configure** > **Switches** > **Switch settings**.

2 Scroll to the **Voice VLAN** part of the screen.

3 Click the switch to enable the voice VLAN feature in the Nebula Device.

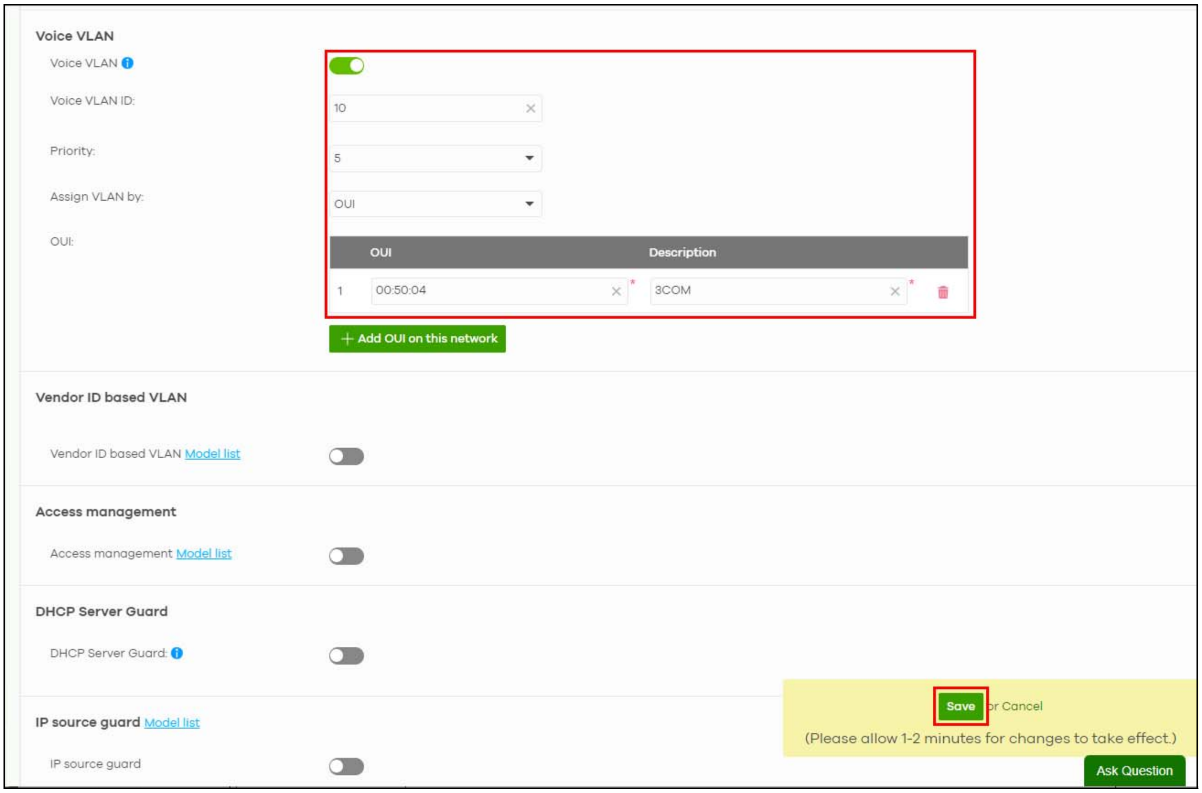
4 Enter a **Voice VLAN ID**.

5 Select the **Priority** of the voice VLAN from 1 to 6.

6 Select **OUI** in **Assign VLAN by**. The Nebula Device assigns the port connected to the VoIP device to the voice VLAN if the connected VoIP device's OUI matches any OUI in the list.

7 Enter the **OUI** address of the VoIP device. The OUI (Organizationally Unique Identifier) is the first three octets of the VoIP device's MAC address. By specifying the MAC address, the Nebula Device can identify voice traffic accordingly.

Note: The Nebula Device supports up to six vendor OUIs.



Voice VLAN

Voice VLAN: ●

Voice VLAN ID: 10

Priority: 5

Assign VLAN by: OUI

OUI:

	OUI	Description
1	00:50:04	3COM

Vendor ID based VLAN

Vendor ID based VLAN Model list: ○

Access management

Access management Model list: ○

DHCP Server Guard

DHCP Server Guard: ○

IP source guard Model list

IP source guard: ○

(Please allow 1-2 minutes for changes to take effect.)

8 Then click **Save**.

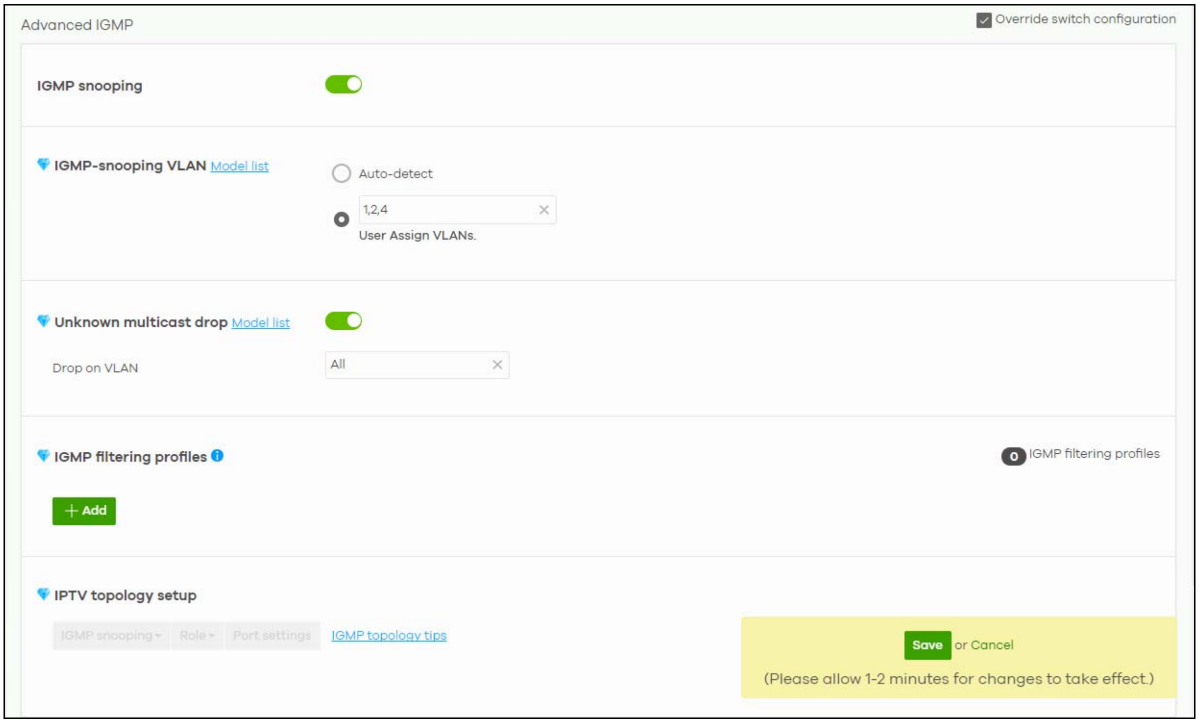
3.37 Manage IPTV (for Nebula Switches only)

This section shows you how to configure IPTV settings and view IPTV reports:

- Set up the VLAN for IPTV
- Define the Role of a Switch
- Configure the Channel Profile and Naming

3.37.1 Set up the VLAN for IPTV

1 Go to the **Site-wide** > **Configure** > **Switches** > **Advanced IGMP** screen. Click **IGMP snooping** to enable IGMP snooping on all Switches in the site. Under **IGMP-snooping VLAN**, select **Auto-detect** to automatically detect which VLANs are used for IPTV. Otherwise, manually enter the VLAN IDs (1 – 4094, up to 16 VLANs, separated by commas, no spaces) in the **User Assign VLANs** field. Click **Save** when you are finished.



Advanced IGMP

☑ Override switch configuration

IGMP snooping ●

IGMP-snooping VLAN Model list

○ Auto-detect

● 1,2,4 ×

User Assign VLANs.

Unknown multicast drop Model list ●

Drop on VLAN: All ×

IGMP filtering profiles

+ Add

0 IGMP filtering profiles

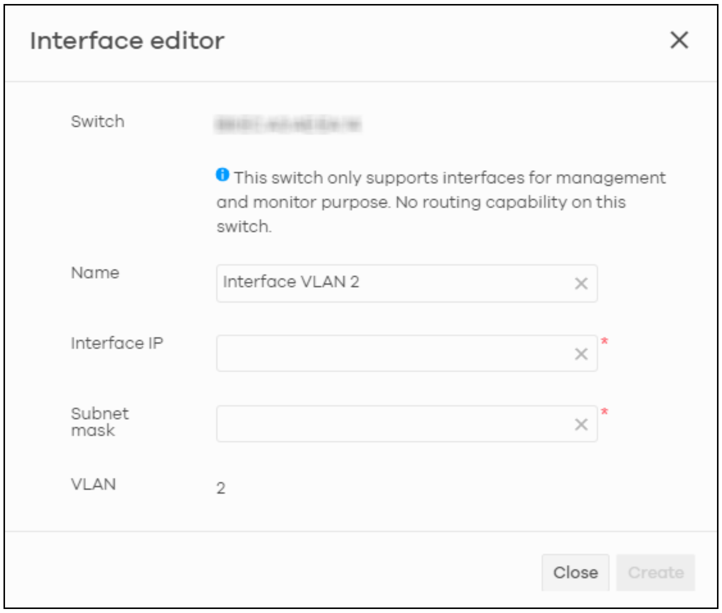
IPTV topology setup

IGMP snooping ▾ | Role ▾ | Port settings | IGMP topology tips

Save or Cancel

(Please allow 1-2 minutes for changes to take effect.)

2 If you have not defined the IP address of the Switch, go to the **Site-wide** > **Configure** > **Switches** > **IP & Routing** screen and click **+Add** under **IP interface**. The following screen appear. Enter the **Interface IP**, **Subnet mask** and ID number of the **VLAN** used for IPTV. Click **Create** to save the setting.



Interface editor ×

Switch: [redacted]

This switch only supports interfaces for management and monitor purpose. No routing capability on this switch.

Name: Interface VLAN 2 ×

Interface IP: × *

Subnet mask: × *

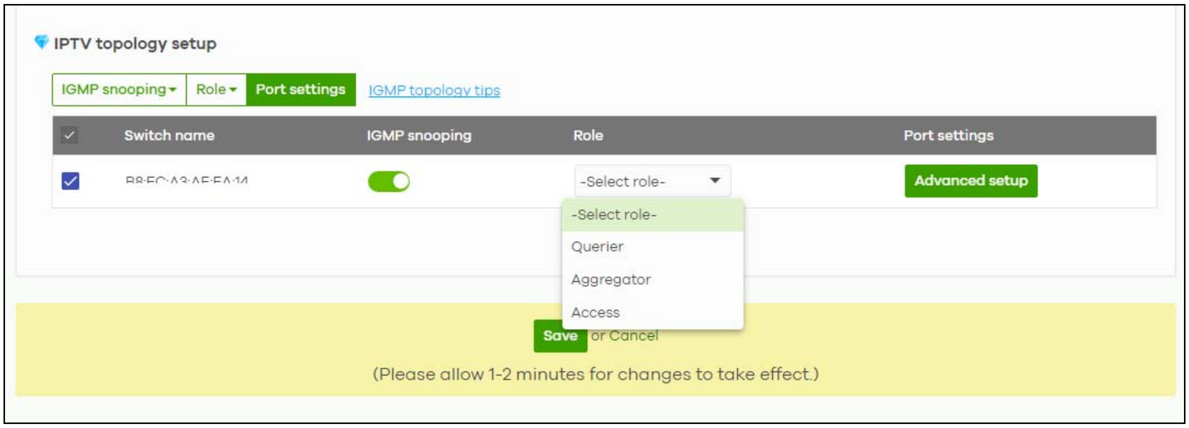
VLAN: 2

Close | Create

3.37.2 Define the Role of a Switch

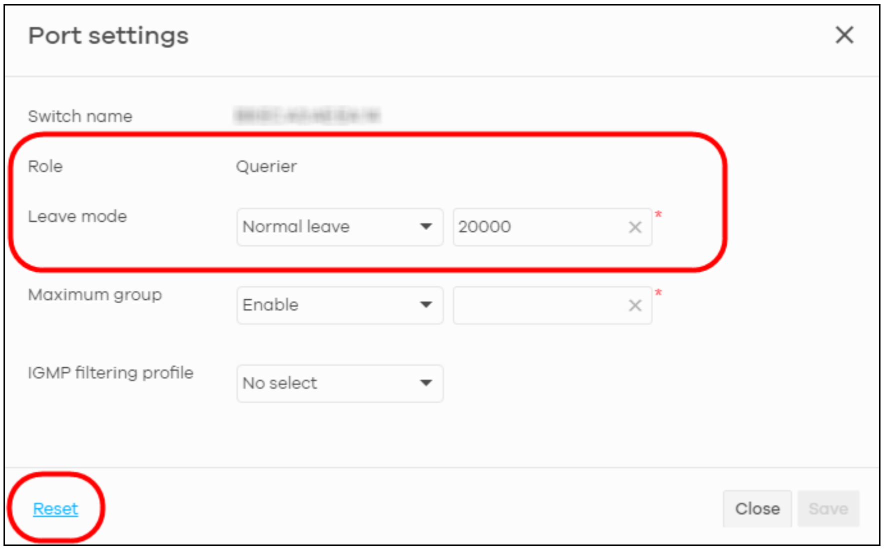
1 Go to the **Site-wide** > **Configure** > **Switches** > **Advanced IGMP** screen. Under **IPTV topology setup**, select a Switch you want to configure and select a **Role** to define the role of your Switch from the drop-down list box.

Note: Click the **IGMP topology tips** link to view information about Switch roles. If the role of the Switch is not defined accordingly, the IPTV performance will be greatly affected.



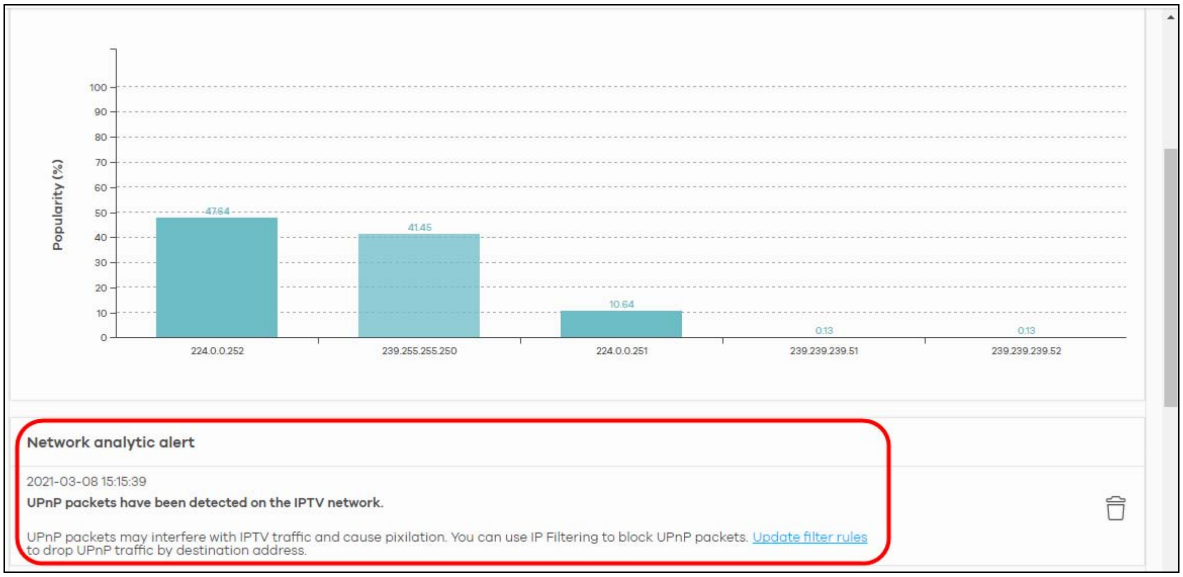
2 After you define the role of the Switch, click **Advanced setup** and the following screen appears. The **Leave mode** will show the default setting based on the role you select. But you can still go back to the **Advanced IGMP** screen to configure the **Role** and **Leave mode**. Under **Maximum group**, you can select **Enable** and enter the maximum number of channels allowed at a time. Otherwise, select **Disable**. Click **Save** to save the changes.

Note: You can click **Reset** to reset the port settings to default.



Switch name		
Role	Querier	
Leave mode	Normal leave	20000
Maximum group	Enable	
IGMP filtering profile	No select	

3 If a reminder of **Network analytic alert** appears on the **Site-wide** > **Monitor** > **Switches** > **IPTV report** page, click the **Update filter rules** link below to use the default ACL rules to block UPnP packets. In the example screen below, a **Network analytic alert** indicates that your IPTV traffic flow is affected by unneeded UPnP packets. Click the **Update filter rules** link to define IP filtering rules in the **Site-wide** > **Configure** > **Switches** > **ACL** screen to block these packets.



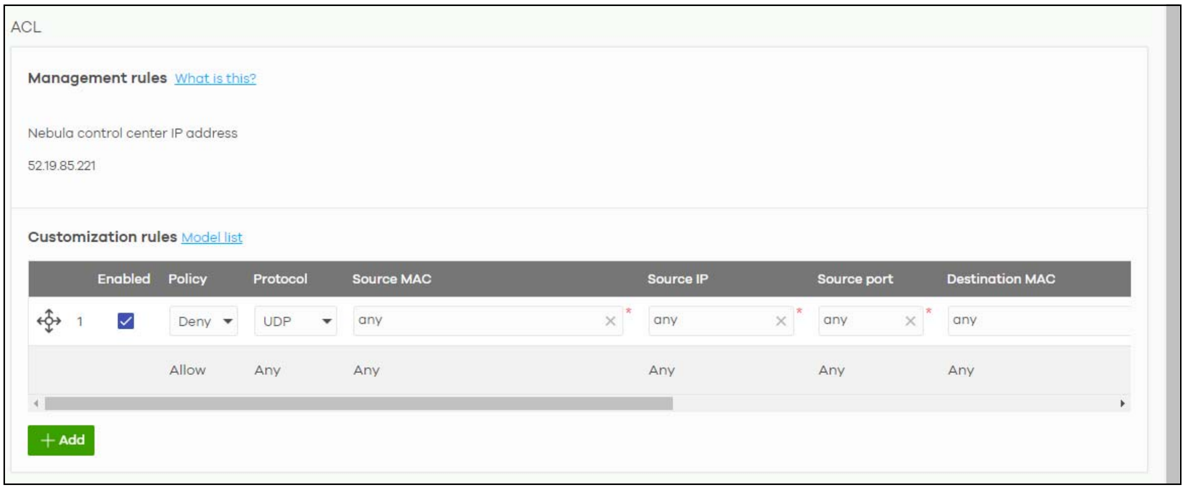
Network analytic alert

2021-03-08 15:15:39

UPnP packets have been detected on the IPTV network.

UPnP packets may interfere with IPTV traffic and cause pixilation. You can use IP Filtering to block UPnP packets. Update filter rules to drop UPnP traffic by destination address.

4 The **Update filter rules** link will lead you to the following screen. Click **Save** to save the default setting to block UPnP packets.



ACL

Management rules What is this?

Nebula control center IP address

52.19.85.221

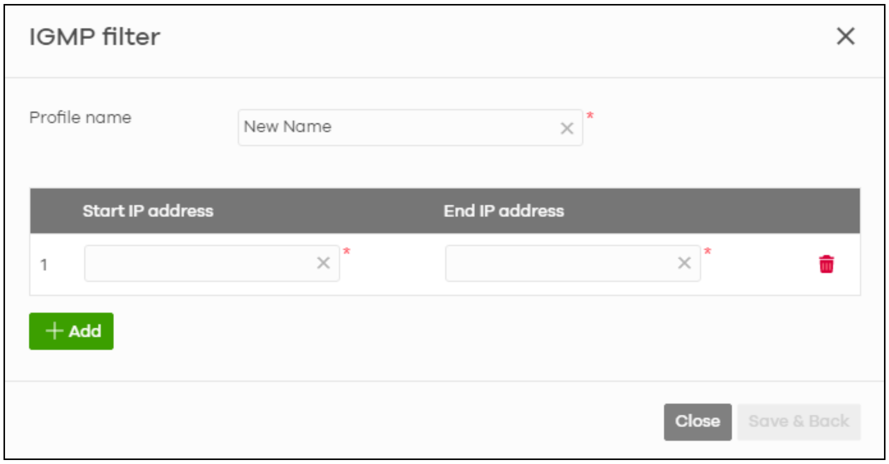
Customization rules Model list

		Enabled	Policy	Protocol	Source MAC	Source IP	Source port	Destination MAC
✥	1	☑	Deny	UDP	any	any	any	any
			Allow	Any	Any	Any	Any	Any

3.37.3 Configure the Channel Profile and Naming

A channel profile is the IP address range allowed to receive IPTV channels. An IPTV channel is used to send video traffic to the IP addresses in the channel profile.

1 To set up a range of available IPTV channels, go to the **Site-wide** > **Configure** > **Switches** > **Advanced IGMP** screen. Under **IGMP filtering profiles**, click **+Add** and the following screen appear. Enter a **Profile name** and enter the **Start IP address** and **End IP address**. Click **Save & Back** to save the changes.

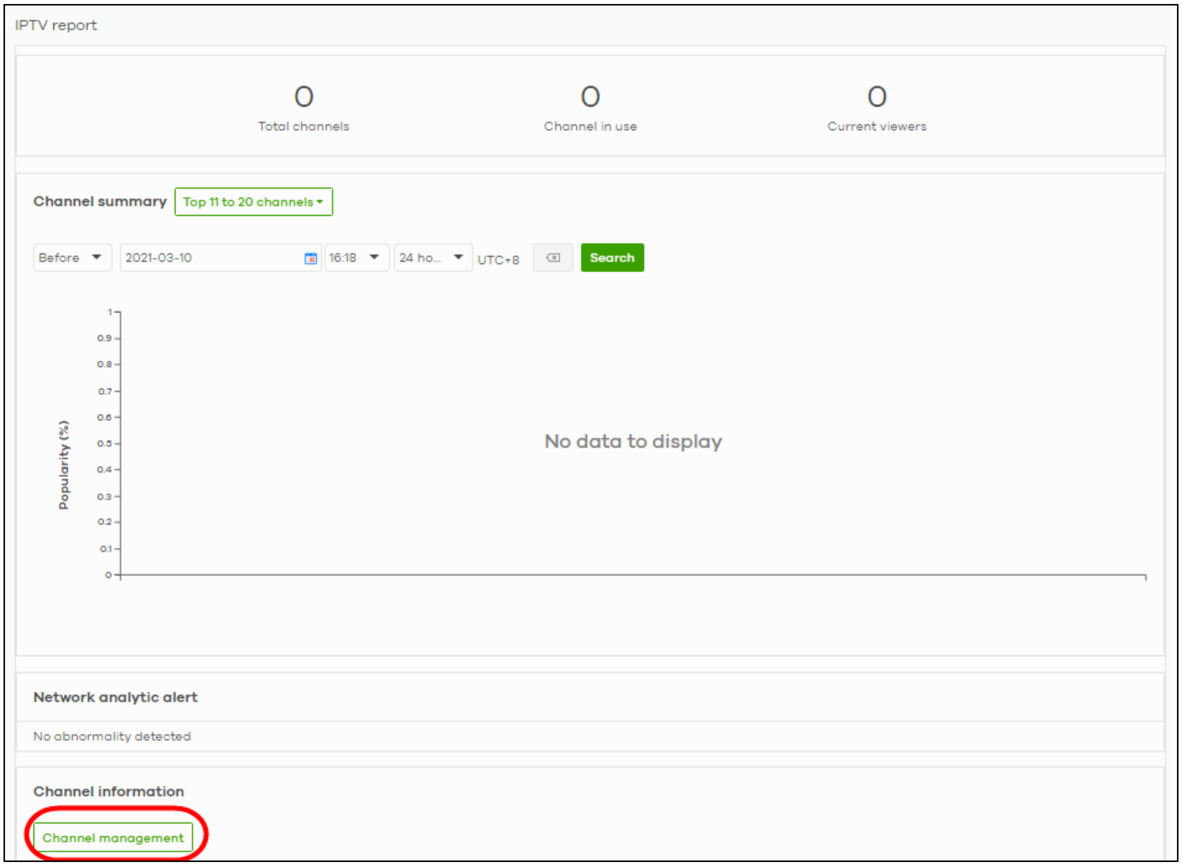


IGMP filter

Profile name: New Name *

	Start IP address	End IP address
1	*	*

2 To edit the naming of the IPTV channels, go to the **Site-wide** > **Monitor** > **Switches** > **IPTV report** screen and click **Channel management** under **Channel information**.



IPTV report

0 Total channels
0 Channel in use
0 Current viewers

Channel summary: Top 11 to 20 channels

Before 2021-03-10 16:18 24 ho... UTC+8

No data to display

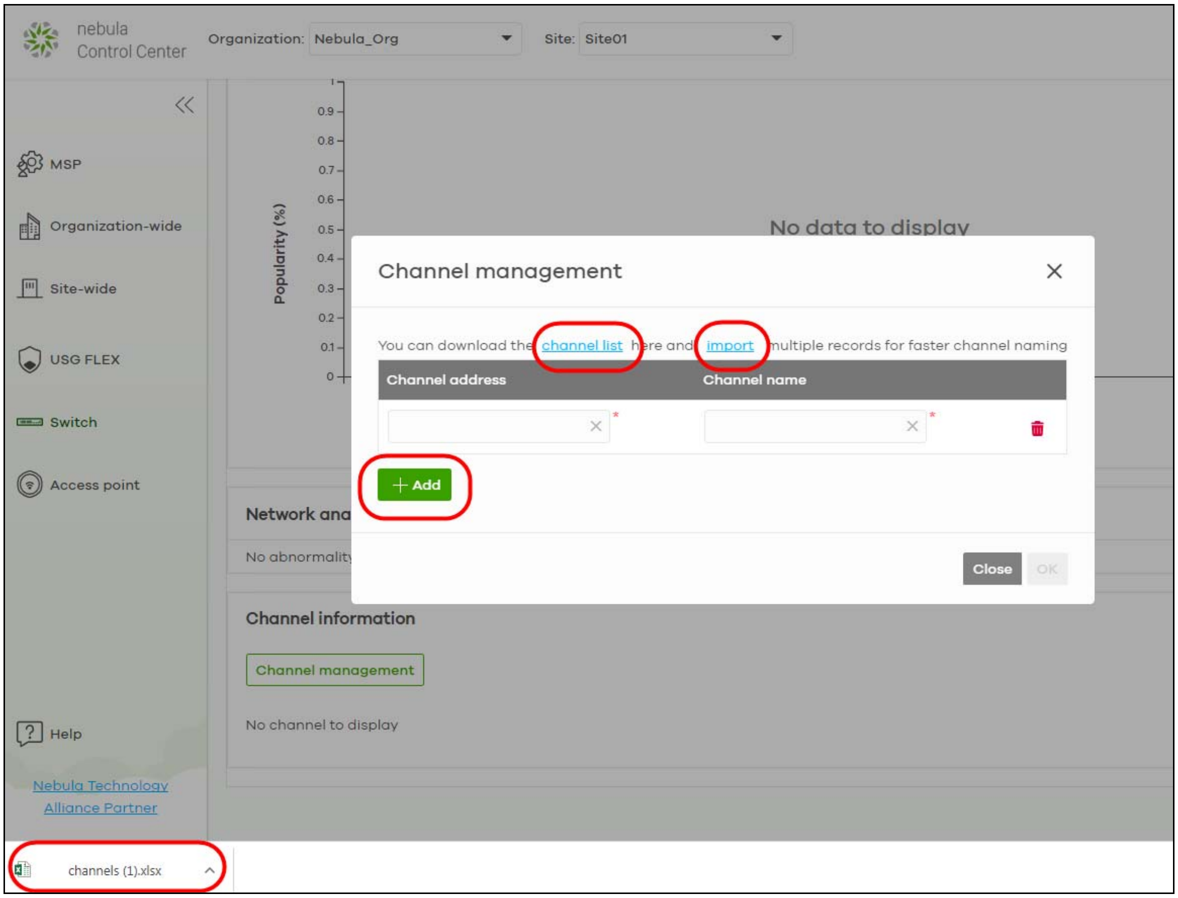
Network analytic alert

No abnormality detected

Channel information

3 You can choose to either import an updated channel list (channels.xlsx), or enter/edit each **Channel address** and **Channel name** individually.

- Under **Channel management**, click **channel list** to download a blank Excel file template, edit accordingly and save it, and then click **import** to import the complete channel list to Nebula. Or,
- Click **+Add** to add and then add/edit a **Channel address** and **Channel name** at a time.

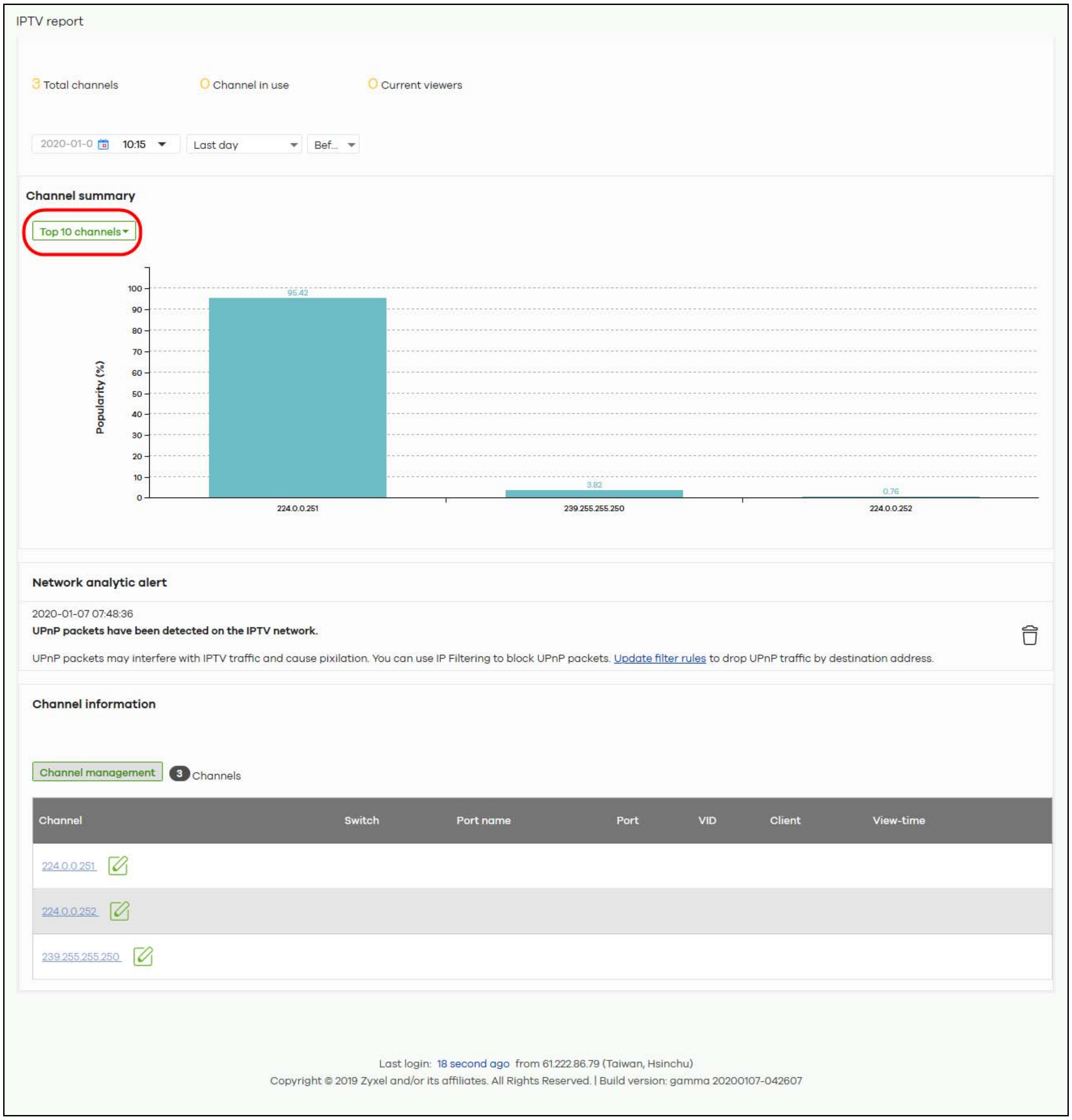


Channel management

You can download the channel list here and import multiple records for faster channel naming

Channel address	Channel name

4 To view the summary of the IPTV report, go to the **Site-wide** > **Monitor** > **Switches** > **IPTV report** screen. Click **Channel summary** to see the top or bottom viewed channels within the specified time period you choose.



IPTV report

3 Total channels

0 Channel in use

0 Current viewers

2020-01-0 10:15 ▾ Last day ▾ Bef... ▾

Channel summary

Top 10 channels ▾

Network analytic alert

2020-01-07 07:48:36

UPnP packets have been detected on the IPTV network.

UPnP packets may interfere with IPTV traffic and cause pixilation. You can use IP Filtering to block UPnP packets. Update filter rules to drop UPnP traffic by destination address.

Channel information

Channel management 3 Channels

Channel	Switch	Port name	Port	VID	Client	View-time
224.0.0.251						
224.0.0.252						
239.255.255.250						

Last login: 18 second ago from 61.222.86.79 (Taiwan, Hsinchu)

Copyright © 2019 Zyxel and/or its affiliates. All Rights Reserved. | Build version: gamma 20200107-042607

3.38 Enable IP Source Guard (for Nebula Switches only)

IP source guard consists of the following features:

- DHCP snooping. Use this to filter unauthorized DHCP server packets on the network and to build a binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.
- Static IP bindings. Use this to create static bindings in the binding table.

Binding Table

IP source guard uses a binding table to distinguish between authorized and unauthorized ARP packets in your network. The Nebula Device builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

DHCP Snooping

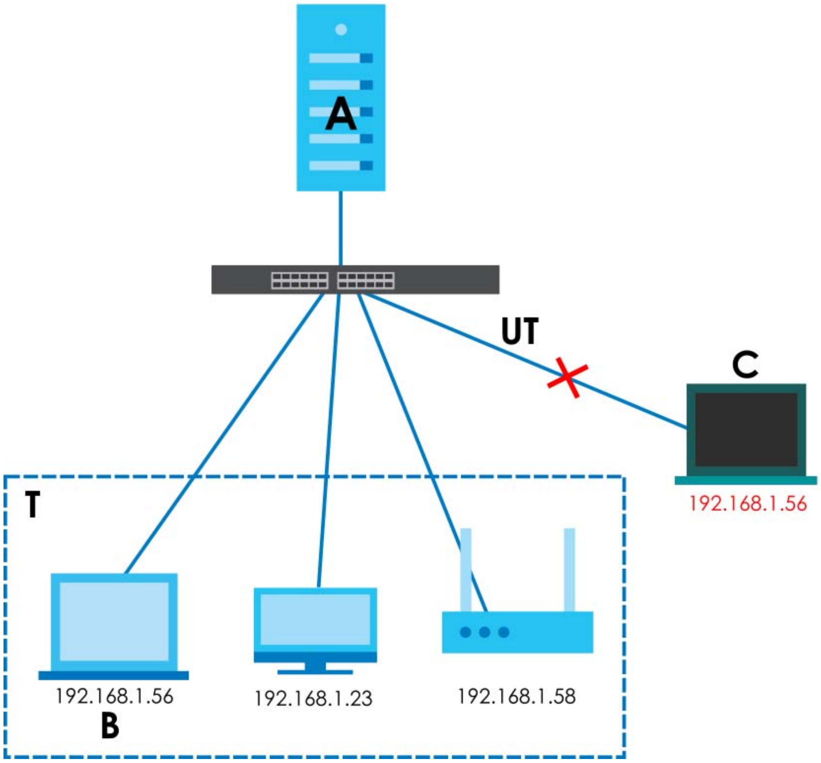
The Nebula Device only allows an authorized DHCP server on a trusted port to assign IP addresses. Unauthorized DHCP servers will not be able to assign IP addresses to network clients. When the Nebula Device receives a DHCP server packet from an authorized DHCP server, it inspects the packet and records the DHCP information in a binding table. The binding records are used in ARP inspection to filter unauthorized ARP packets.

ARP Inspection

When the Nebula Device receives an ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Nebula Device forwards the packet. Otherwise, the Nebula Device discards the packet.

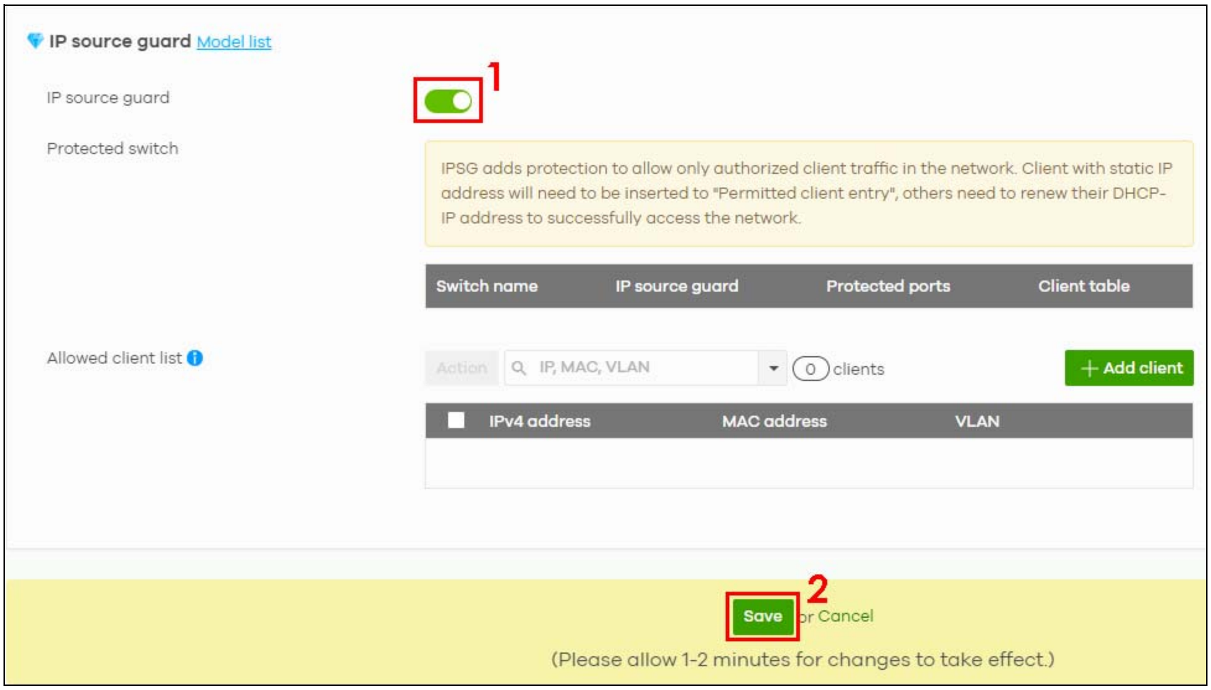
If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

The following figure demonstrates a scenario with DHCP snooping and ARP inspection enabled. In this scenario, we connect an authorized DHCP server (A) and the client devices on the ARP trusted ports (T). A client device (B) is assigned the IP address 192.168.1.56 by the authorized DHCP server (A). A malicious host (C) on an untrusted port (UT) puts a wrong MAC address with the IP address 192.168.1.56 in an ARP reply packet pretending to be client device (B) (192.168.1.56). The Nebula Device snoops DHCP packets sent from the authorized DHCP server (A) and creates bindings in the binding table. When the Nebula Device receives ARP packets from an untrusted port (UT), it compares the IP and MAC addresses with the existing bindings. Since the IP and MAC binding is different from the existing bindings, the Nebula Device blocks the unauthorized ARP packets sent from the malicious host (C). The malicious host (C) therefore cannot disguise as client device (B) to build connections with other client devices on your network.



To setup IP source guard on the Nebula, do the following:

1 Go to **Site-wide** > **Configure** > **Switches** > **Switch settings**. Slide the switch to enable **IP source guard** for the Nebula Devices in your site. Then click **Save**. The **Protected switch** and **Allowed client list** will appear. The **Protected switch** information synchronizes with the port's **IPSG Protected** setting in **Site-wide** > **Configure** > **Switches** > **Switch ports**. It will display the enabled ports.



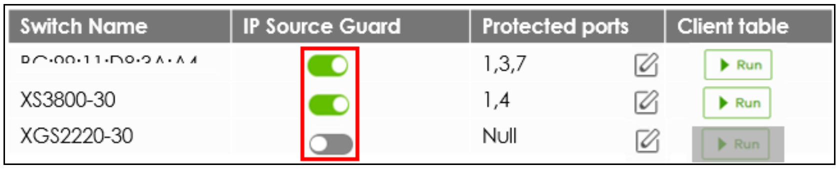
IPSG adds protection to allow only authorized client traffic in the network. Client with static IP address will need to be inserted to "Permitted client entry", others need to renew their DHCP-IP address to successfully access the network.

Switch name	IP source guard	Protected ports	Client table

□	IPv4 address	MAC address	VLAN

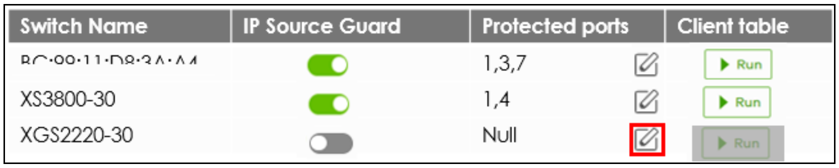
(Please allow 1-2 minutes for changes to take effect.)

2 Click the IP Source Guard switch to enable/disable **IP source guard** for the specific registered Nebula Device(s) in your site.



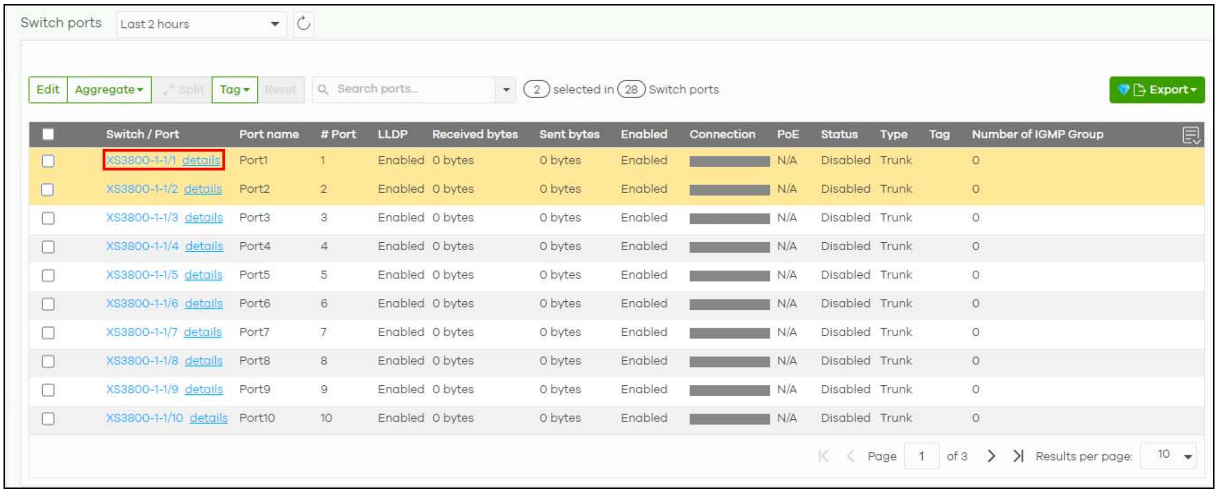
Switch Name	IP Source Guard	Protected ports		Client table
BC:99:11:D8:3A:A4	●	1,3,7	✎	▶ Run
XS3800-30	●	1,4	✎	▶ Run
XGS2220-30	○	Null	✎	▶ Run

3 Click the edit icon to go to **Site-wide** > **Configure** > **Switches** > **Switch ports** to configure **Protected ports** for the Nebula Device. A port is protected if **IPSG protected** is enabled on this port.



Switch Name	IP Source Guard	Protected ports		Client table
BC:99:11:D8:3A:A4	●	1,3,7	✎	▶ Run
XS3800-30	●	1,4	✎	▶ Run
XGS2220-30	○	Null	✎	▶ Run

4 Click to select the port you want to enable IP source guard.

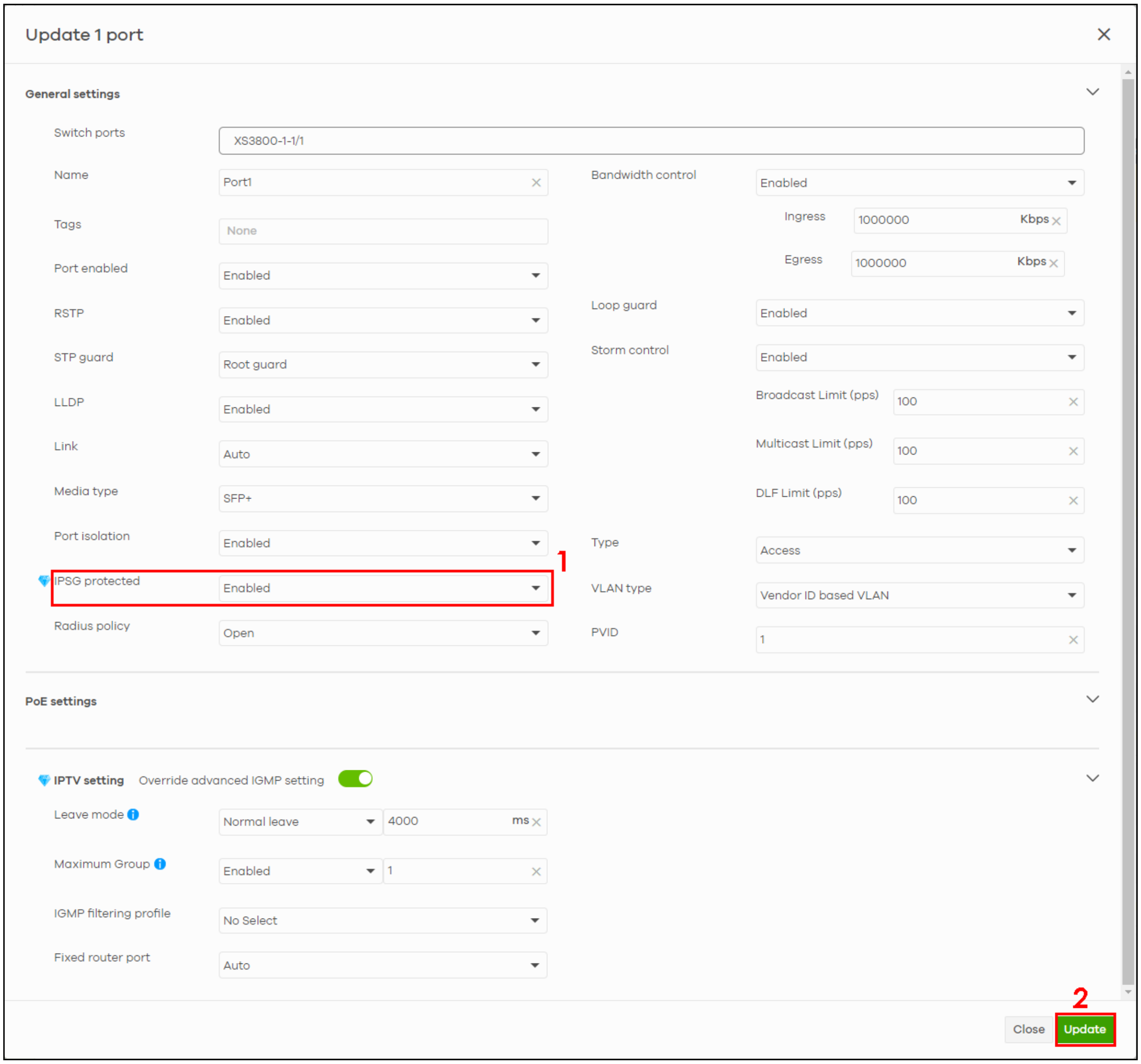


□	Switch / Port	Port name	# Port	LLDP	Received bytes	Sent bytes	Enabled	Connection	PoE	Status	Type	Tag	Number of IGMP Group
□	XS3800-1-1/1 details	Port1	1	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
□	XS3800-1-1/2 details	Port2	2	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
□	XS3800-1-1/3 details	Port3	3	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
□	XS3800-1-1/4 details	Port4	4	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
□	XS3800-1-1/5 details	Port5	5	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
□	XS3800-1-1/6 details	Port6	6	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
□	XS3800-1-1/7 details	Port7	7	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
□	XS3800-1-1/8 details	Port8	8	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
□	XS3800-1-1/9 details	Port9	9	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
□	XS3800-1-1/10 details	Port10	10	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0

Note: Do NOT configure IPSG on an uplink port as this may cause disconnection between the client device and Nebula.

To restore connection on an uplink port, go to **Site-wide** > **Configure** > **Switches** > **Switch ports** to select the uplink port. In the **Update 1 port** screen select **Disabled** in **IPSG protected**. Then reset the Nebula Device to its factory-default setting (see the Nebula Device's User's Guide for more information).

5 In the **Update port** screen, select **Enabled** in **IPSG protected**. The **IPSG protected** field in the **Site-wide** > **Configure** > **Switches** > **Switch ports** table for the updated port will display **Enabled**.



Update 1 port

General settings

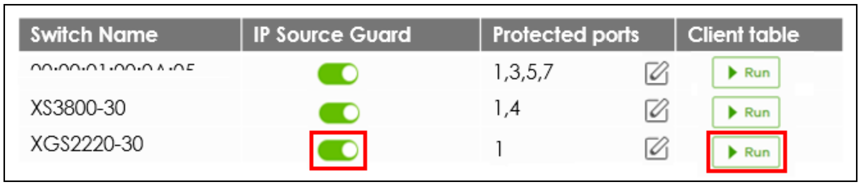
Switch ports	XS3800-1-1/1		
Name	Port1	Bandwidth control	Enabled
Tags	None	Ingress	1000000 Kbps
		Egress	1000000 Kbps
Port enabled	Enabled		
RSTP	Enabled	Loop guard	Enabled
STP guard	Root guard	Storm control	Enabled
LLDP	Enabled	Broadcast Limit (pps)	100
Link	Auto	Multicast Limit (pps)	100
Media type	SFP+	DLF Limit (pps)	100
Port isolation	Enabled	Type	Access
IPSG protected	Enabled	VLAN type	Vendor ID based VLAN
Radius policy	Open	PVID	1

PoE settings

IPTV setting Override advanced IGMP setting

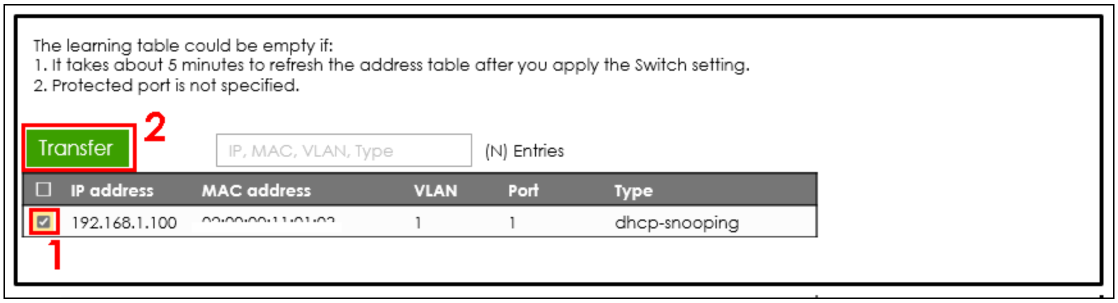
Leave mode	Normal leave	4000 ms
Maximum Group	Enabled	1
IGMP filtering profile	No Select	
Fixed router port	Auto	

6 Click **Run**.



Switch Name	IP Source Guard	Protected ports		Client table
00:00:01:00:0A:05	●	1,3,5,7	✎	▶ Run
XS3800-30	●	1,4	✎	▶ Run
XGS2220-30	●	1	✎	▶ Run

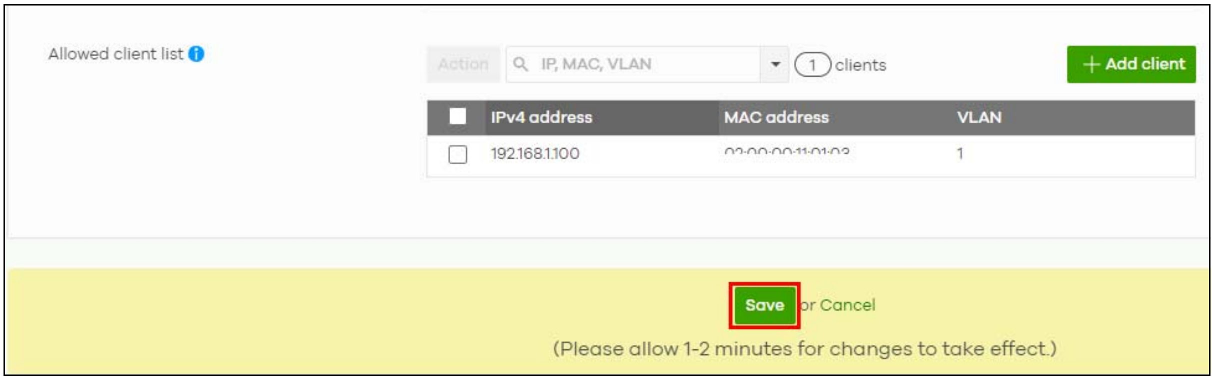
7 A merged list window appears. Click to select the port and then click **Transfer**.



The learning table could be empty if:
1. It takes about 5 minutes to refresh the address table after you apply the Switch setting.
2. Protected port is not specified.

□	IP address	MAC address	VLAN	Port	Type
☑	192.168.1.100	02:00:00:11:01:03	1	1	dhcp-snooping

8 The port with the particular IP and MAC addresses is added to the **Allowed client list**. Click **Save**.



■	IPv4 address	MAC address	VLAN
□	192.168.1.100	02:00:00:11:01:03	1

(Please allow 1-2 minutes for changes to take effect.)

3.39 Set Up MAC Authentication With NCAS (for Nebula Switches only)

To set up MAC authentication with NCAS (Nebula Cloud Authentication Server), do the following:

1 Go to **Site-wide** > **Configure** > **Switches** > **Authentication**: **Server type** to select the authentication server.

2 Click **+Add** to create the **Authentication policy**.
Enter the **Name** (for example, Trusted Device) and select **MAC-Base** in **Authentication type**.

3 Go to **Site-wide** > **Configure** > **Switches** > **Switch ports** to bind the authentication policy to the access port(s).

3a Select the port(s) and click **Edit**.

3b In the **Update # port** screen, select **Access** in **Type**.
Select **MAC-Base/Trusted Device** in **Auth. policy**. Then click **Update**.

4 Go to **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **MAC** to add MAC addresses in the cloud authentication list.

4a Click **+Add** to create to create a new user account.

4b In the **Create user** screen, enter the **MAC address** for this account.

4c In the **Authorized** field, select the user's access to **All sites** or **Specified sites**. If you select **Specified sites**, a field displays allowing you to specify the sites to which the user access is authorized.

4d Then click **Create user**.

3.40 Set Up Dynamic VLAN With RADIUS (for Nebula Switches only)

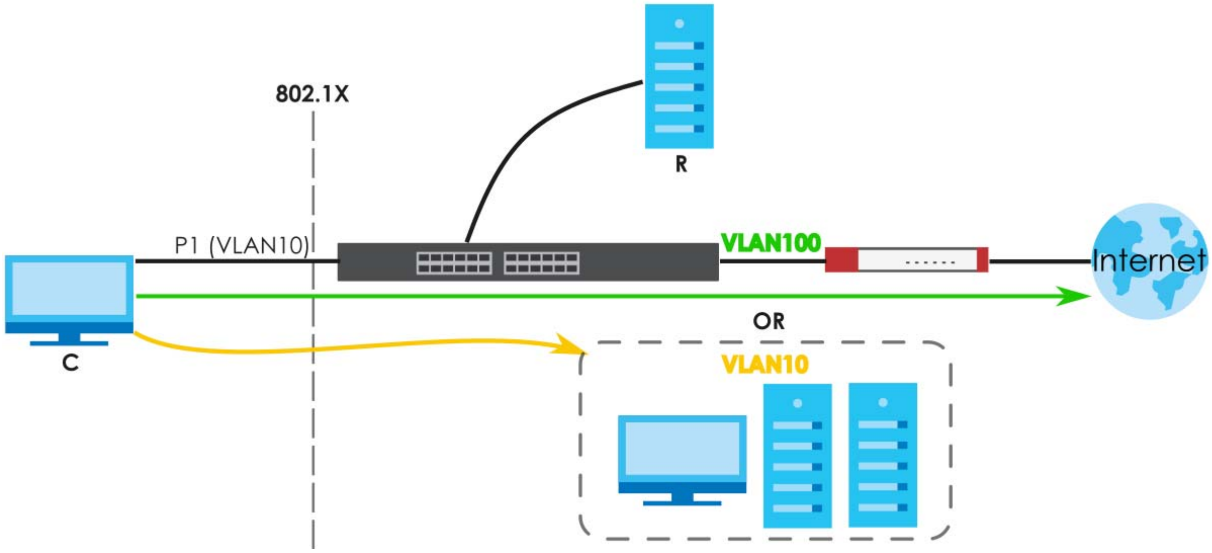
In this example, VLAN10 is configured on port 1 (P1) of the Nebula Device. The user creates the following two accounts in the RADIUS server (R):

- Account with VLAN100 assignment
- Account without VLAN assignment.

Scenario 1:
The login account passes IEEE 802.1x port authentication with dynamic VLAN assignment. Client (C) will connect to the network through VLAN100.

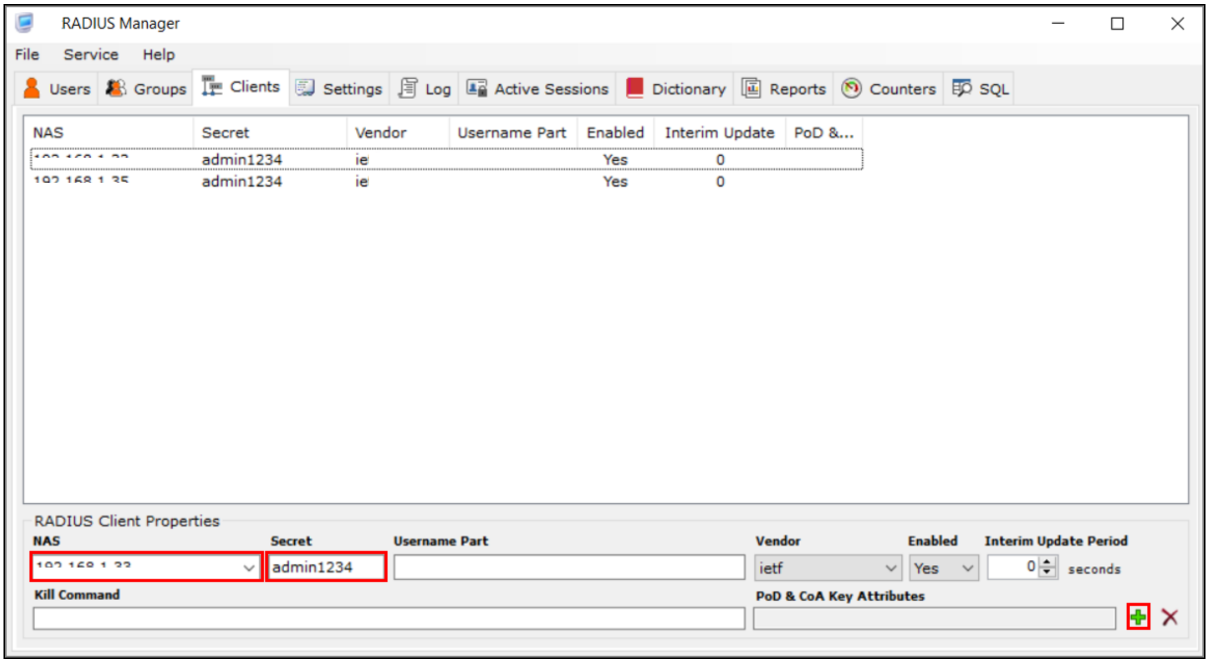
Scenario 2:
The login account passes IEEE 802.1x port authentication without dynamic VLAN assignment. Client (C) will connect to the network through VLAN10.

Figure 33 IEEE 802.1x Port Authentication With and Without Dynamic VLAN Assignment Example



To set up dynamic VLAN with RADIUS, do the following:

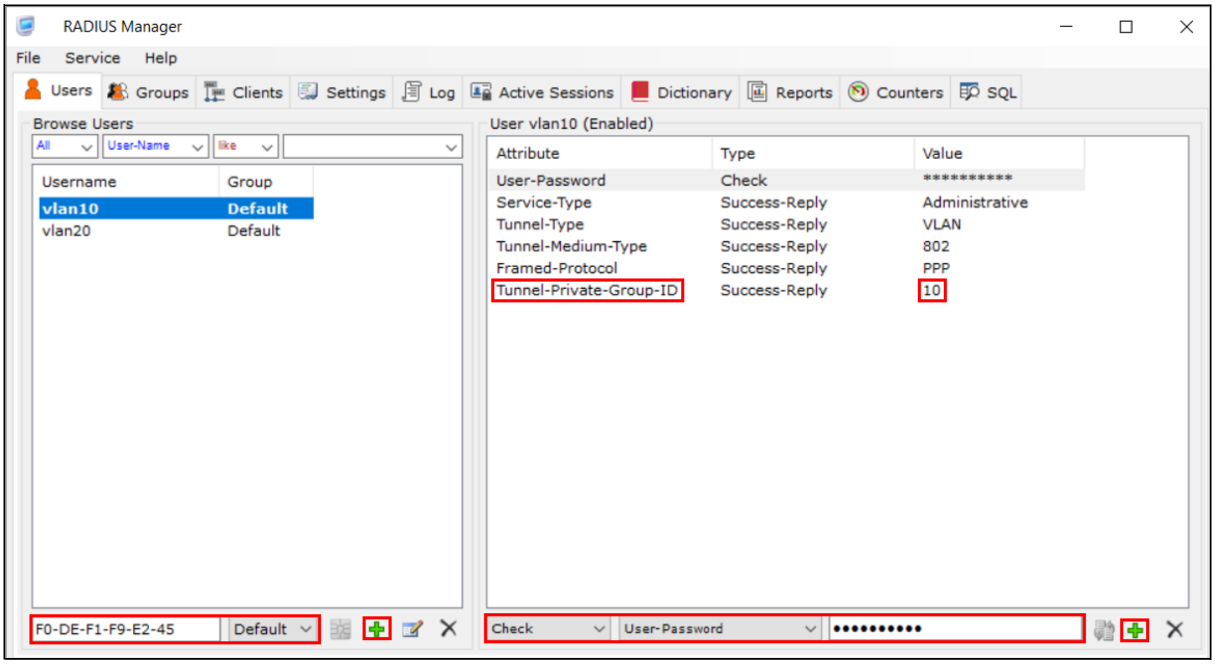
1 Configure the client list in the RADIUS server. In the example screen below, enter the management IP address of the Nebula Device in **NAS**. Enter the shared **Secret** (password) in your **Site-wide** > **Configure** > **Switches** > **Authentication** screen. Then click the add (**+**) button.



NAS	Secret	Vendor	Username Part	Enabled	Interim Update	PoD &...
192.168.1.33	admin1234	ie		Yes	0	
192.168.1.35	admin1234	ie		Yes	0	

NAS	Secret	Username Part	Vendor	Enabled	Interim Update Period
192.168.1.33	admin1234		ietf	Yes	0 seconds

2 Create a user with dynamic VLAN attributes in the RADIUS server. In the example screen below, 10 in the **Tunnel-Private-Group-ID** is the value of the dynamic VLAN of this user account.



Username	Group
vlan10	Default
vlan20	Default

User vlan10 (Enabled)

Attribute	Type	Value
User-Password	Check	**********
Service-Type	Success-Reply	Administrative
Tunnel-Type	Success-Reply	VLAN
Tunnel-Medium-Type	Success-Reply	802
Framed-Protocol	Success-Reply	PPP
Tunnel-Private-Group-ID	Success-Reply	10

F0-DE-F1-F9-E2-45 Default

Check User-Password ••••••••••

3 Go to **Site-wide** > **Configure** > **Switches** > **Authentication** to create the authentication policy.

3a Select the authentication server in **Server type**.

3b Click **+Add** in **Authentication server** to create a new RADIUS server entry.

3c Enter the IP address of the external RADIUS server in **Host**.
Enter the port of the RADIUS server for authentication (default 1812) in **Port**.

Enter a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Nebula Device in **Secret**.

3d Click **+Add** in **Authentication policy** to create a new policy.

3e Enter a descriptive name for the policy in **Name**.
Select **802.1x** in **Authentication type** to validate access to the ports based on the user name and password provided by the client.

4 Go to **Site-wide** > **Configure** > **Switches** > **Switch ports** to bind the authentication policy to the Nebula Device access ports.

4a Select the port(s) and click **Edit**.

4b In the **Update # port** screen, select **Access** in **Type**.
Select **802.1X/VLAN Assignment** in **Auth. policy**. Then click **Update**.

5 Go to **Site-wide** > **Configure** > **Switches** > **Switch ports** to add the dynamic VLAN list to the allowed VLAN list of uplink ports.

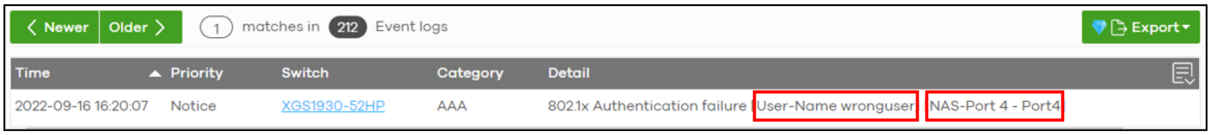
5a Select the uplink port and click **Edit**.

5b In the **Update # port** screen, select **Trunk** in **Type**.
Enter the dynamic VLAN(s) in **Allowed VLANs**. Then click **Update**.

3.41 Monitor Dynamic VLAN Using Event Logs (for Nebula Switches only)

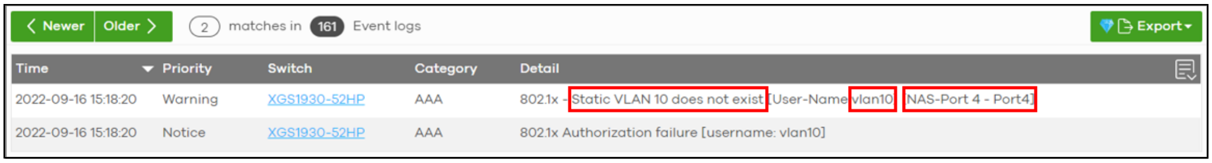
Go to **Site-wide** > **Monitor** > **Switches** > **Event log** to monitor dynamic VLANs. The following are example dynamic VLAN-related event logs:

- User submits an incorrect 802.1X credential (wrong user name on the client port ‘Port4’).



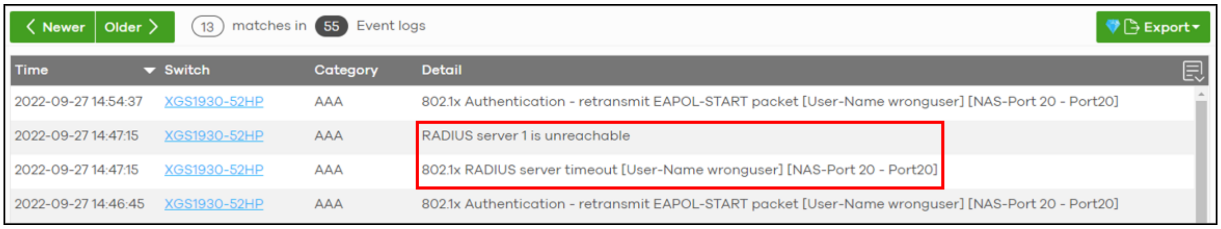
Time	Priority	Switch	Category	Detail
2022-09-16 16:20:07	Notice	XGS1930-52HP	AAA	802.1x Authentication failure [User-Name wronguser] [NAS-Port 4 - Port4]

- The dynamic VLAN attribute received is without a corresponding static VLAN (missing static VLAN 10 for the user name ‘vlan10’ on the client port ‘Port4’).



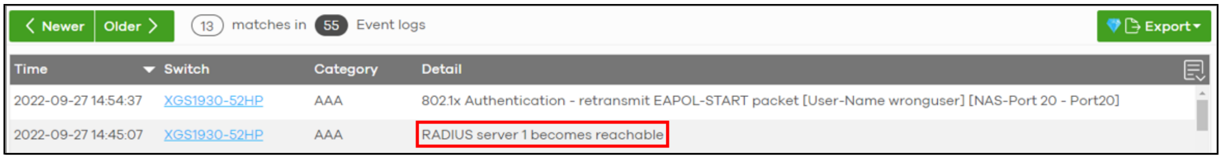
Time	Priority	Switch	Category	Detail
2022-09-16 15:18:20	Warning	XGS1930-52HP	AAA	802.1x - Static VLAN 10 does not exist [User-Name vlan10] [NAS-Port 4 - Port4]
2022-09-16 15:18:20	Notice	XGS1930-52HP	AAA	802.1x Authorization failure [username: vlan10]

- The Nebula Device cannot connect with an external RADIUS server.



Time	Switch	Category	Detail
2022-09-27 14:54:37	XGS1930-52HP	AAA	802.1x Authentication - retransmit EAPOL-START packet [User-Name wronguser] [NAS-Port 20 - Port20]
2022-09-27 14:47:15	XGS1930-52HP	AAA	RADIUS server 1 is unreachable
2022-09-27 14:47:15	XGS1930-52HP	AAA	802.1x RADIUS server timeout [User-Name wronguser] [NAS-Port 20 - Port20]
2022-09-27 14:46:45	XGS1930-52HP	AAA	802.1x Authentication - retransmit EAPOL-START packet [User-Name wronguser] [NAS-Port 20 - Port20]

- The Nebula Device re-establishes connection with an external RADIUS server.



Time	Switch	Category	Detail
2022-09-27 14:54:37	XGS1930-52HP	AAA	802.1x Authentication - retransmit EAPOL-START packet [User-Name wronguser] [NAS-Port 20 - Port20]
2022-09-27 14:45:07	XGS1930-52HP	AAA	RADIUS server 1 becomes reachable

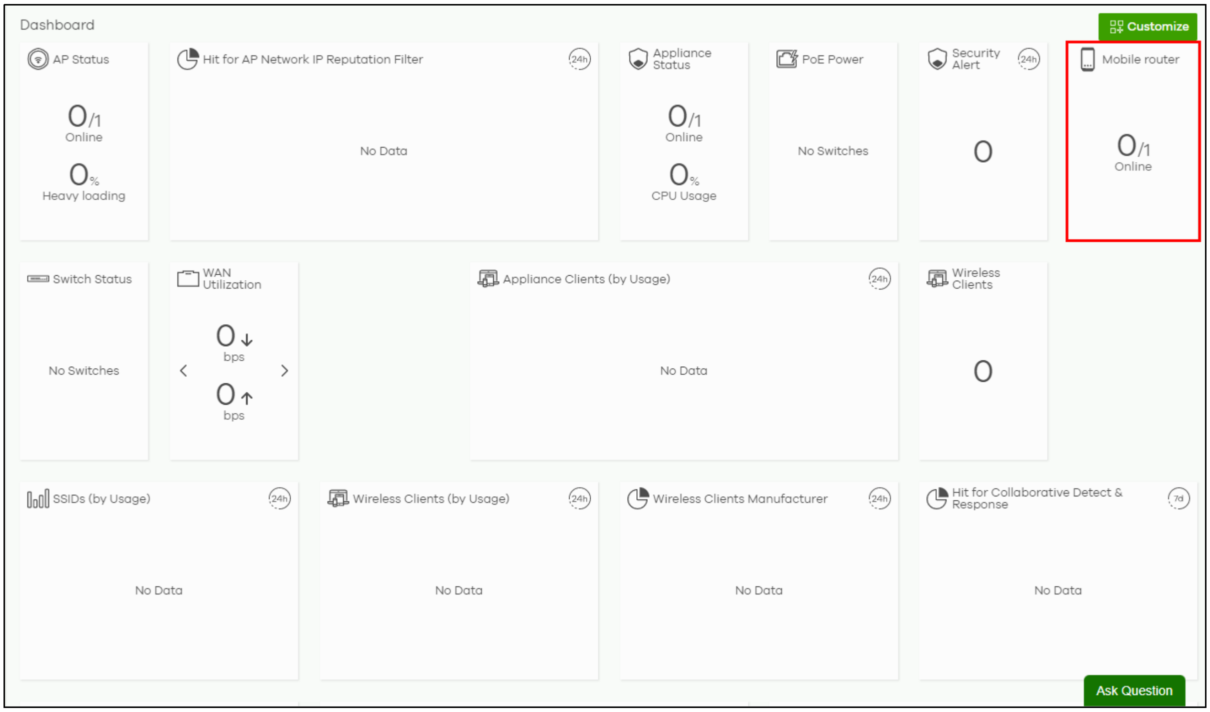
3.42 Register a Nebula Device (mobile router) in Nebula

To manage a Nebula Device (mobile router) and monitor its status in Nebula, do the following:

Nebula Configuration

1 Use the Setup Wizard to create an organization and a site, and add the Nebula Device. See Setup Wizard on page 63 for more information on using the wizard.

2 After configuring the Setup Wizard, close the Nebula Control Center welcome message to go to the Nebula portal dashboard. **0/1 Online** will show on **Mobile router**. This means that one Nebula Device (mobile router) is registered in Nebula but not yet online.

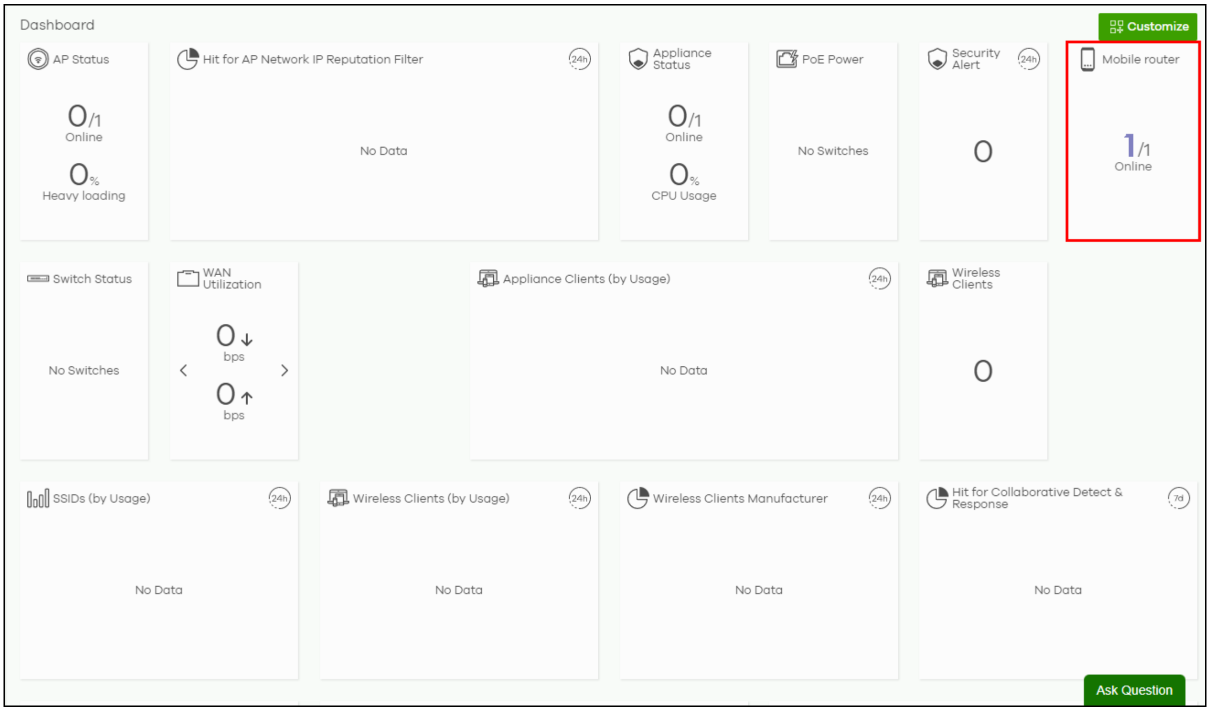


Insert the SIM Card

Insert the SIM card and do the hardware connections on the Nebula Device. Refer to the Nebula Device’s QSG (Quick Start Guide) for more information.

Check the Connection in Nebula

1 Go to **Site-wide** > **Dashboard**. **1/1 Online** will show in **Mobile router**. This means that one Nebula Device (mobile router) is registered in Nebula and is online.



2 Click **Mobile router** to monitor the Nebula Device’s status.

The Nebula Device goes into Nebula-managed mode automatically after it is successfully registered in the Nebula web portal and can be accessed there.

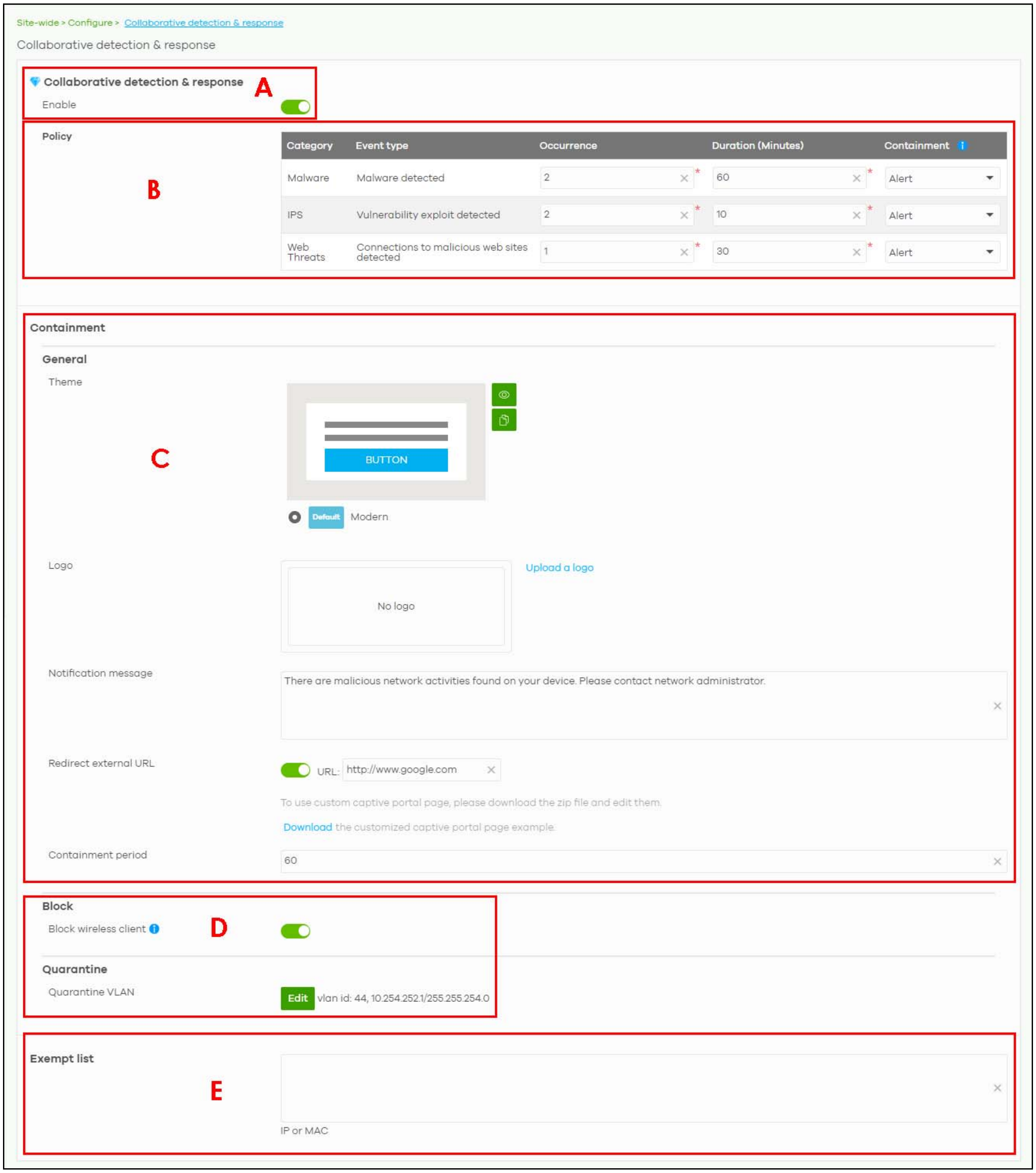
Note: Its login password and settings are then overwritten with what you have configured in the Nebula web portal. To access the Web Configurator when the Nebula Device is in Cloud mode, use the Nebula Local credentials password to login. The **Local credentials**: **Password** can be found in **Site-wide** > **Configure** > **Site settings** > **Device configuration**.

3.43 Using Collaborative Detection and Response (CDR)

Use CDR to block client IP traffic when an unsafe connection is detected and reaches the pre-set threshold. See on page 302 for more information.

To configure CDR, do the following:

1 Go to **Site-wide** > **Configure** > **Collaborative detection & response**. Click **Enable** to activate CDR (refer to the **A** part in the below figure).



Site-wide > Configure > Collaborative detection & response

Collaborative detection & response

Collaborative detection & response

Enable

Policy

Category	Event type	Occurrence	Duration (Minutes)	Containment
Malware	Malware detected	2	60	Alert
IPS	Vulnerability exploit detected	2	10	Alert
Web Threats	Connections to malicious web sites detected	1	30	Alert

Containment

General

Theme

○ Default Modern

Logo

No logo

Upload a logo

Notification message: There are malicious network activities found on your device. Please contact network administrator.

Redirect external URL: URL: http://www.google.com

To use custom captive portal page, please download the zip file and edit them.

Download the customized captive portal page example.

Containment period: 60

Block

Block wireless client

Quarantine

Quarantine VLAN: Edit vlan id: 44, 10.254.252.1/255.255.254.0

Exempt list

IP or MAC

2 Configure the criteria (**Occurrence**, **Duration**) and the **Containment** action (**Alert**, **Block**, **Quarantine**) for each **Category** (**Malware**, **IDP**, **Web Threat**) (refer to the **B** part in the above figure). See Table 43 on page 296 for more information.

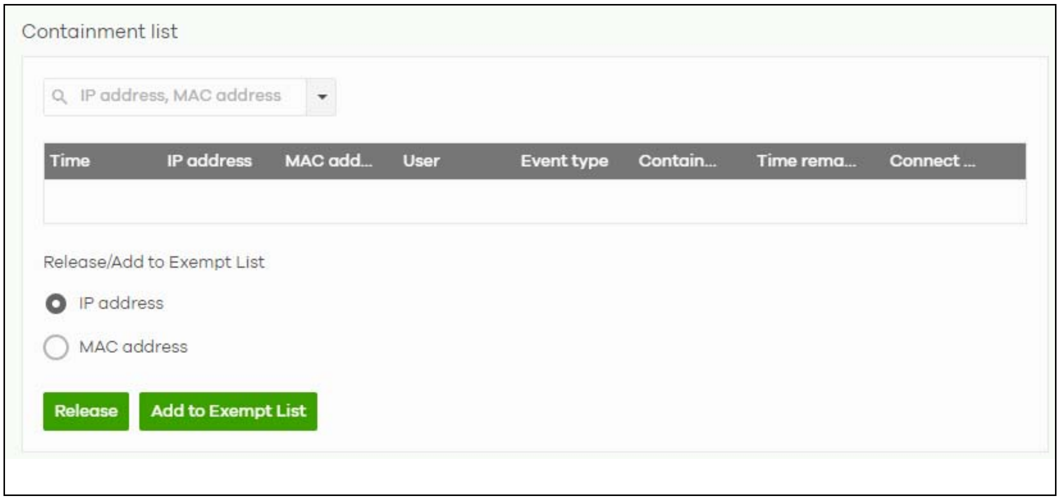
3 Configure the containment alert (**Theme**), customized pop-up (**Notification message**) for the client blocked by CDR, and the (**Containment Period**) time interval (refer to the **C** part in the above figure).

4 In **Block**, set how long a suspect client should be blocked or quarantined (1 minute to 1 day (1,440 minutes)). Enter 0 to block a suspect client until released in **Site-wide** > **Monitor** > **Containment list**. In **Quarantine**, configure a VLAN in order to isolate traffic from suspect clients (refer to the **D** part in the figure for step 1).

5 Enter the IPv4 and/or MAC addresses of client device(s) that are exempt from CDR checking in **Exempt list** (refer to the **E** part in the figure for step 1).

6 To unblock a suspect client, go to **Site-wide** > **Monitor** > **Containment list**. Select a client, then

- click **Release** to free the client from CDR containment, or
- select an IPv4 address or MAC address, click **Add to Exempt List** and then click **OK** to release the client device from CDR containment. The client device's IP or MAC address is exempt from future CDR checking.



3.44 Deploy With Nebula Native Mode (for Security Firewalls in Nebula only)

Nebula native mode means the Security Firewall has a certificate (ZTP (Zero Touch Provision) or factory) to connect with Nebula.

Note: Make sure the Nebula Device can connect to NCC through the Internet by using any of the following methods:

– DHCP WAN, or
– configure WAN through the Nebula Device's Web Configurator.

If you are adding a ZyWALL USG FLEX / ATP / USG20(W)-VPN Series Security Firewall (SF) with v5.10 and later firmware to a site, or if your SF has run ZTP before, do the following to deploy the SF using Nebula native mode:

- Reset the SF to factory-default settings
- Select the Nebula management mode.

Reset the SF to Factory-Default Settings

Note: You only need to do this if you have configured the SF before.

Press the **RESET** button on the SF panel (see the SF user's guide for more information).

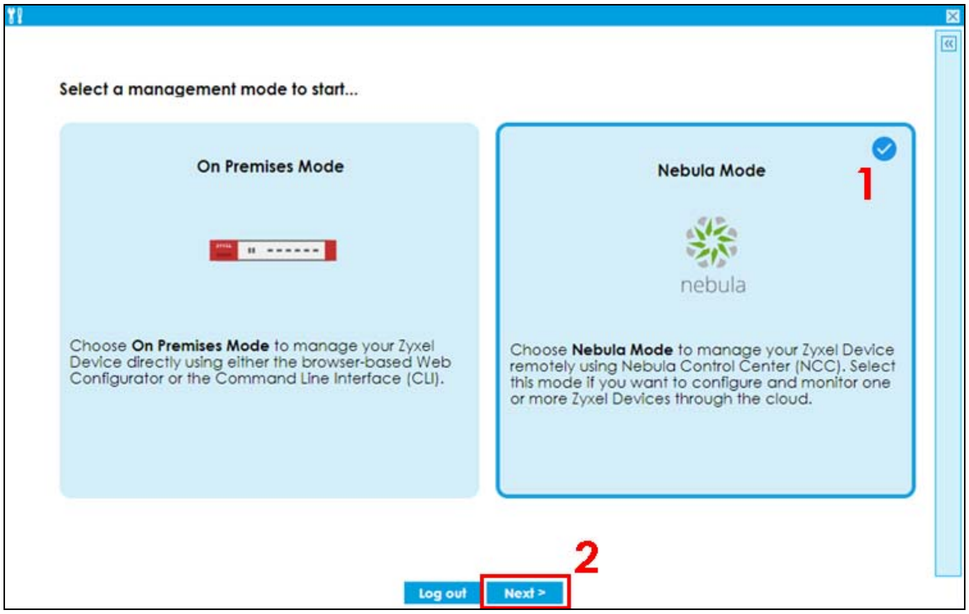
Note: Apply the factory-default settings on the SF before switching to cloud mode. Only the following two settings can be changed after resetting:

- Default administrator account password
- WAN settings

Select the Nebula Management Mode

1 Log into the SF Web Configurator (see the SF user's guide for more information). When you log into the Web Configurator, the **Initial Setup Wizard** screen displays.

2 Select **Nebula Mode** and click **Next**.



Select a management mode to start...

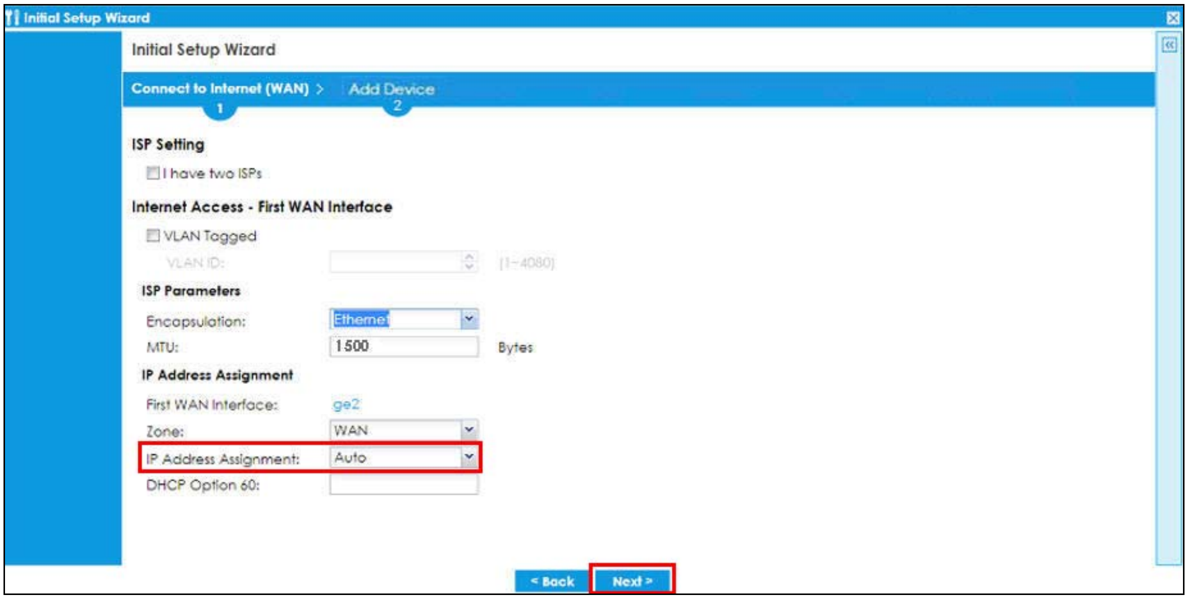
On Premises Mode

Choose **On Premises Mode** to manage your Zyxel Device directly using either the browser-based Web Configurator or the Command Line Interface (CLI).

Nebula Mode

Choose **Nebula Mode** to manage your Zyxel Device remotely using Nebula Control Center (NCC). Select this mode if you want to configure and monitor one or more Zyxel Devices through the cloud.

3 Configure the WAN settings and click **Next**.



Initial Setup Wizard

ISP Setting

□ I have two ISPs

Internet Access - First WAN Interface

□ VLAN Tagged

VLAN ID: (1~4080)

ISP Parameters

Encapsulation: Ethernet

MTU: 1500 Bytes

IP Address Assignment

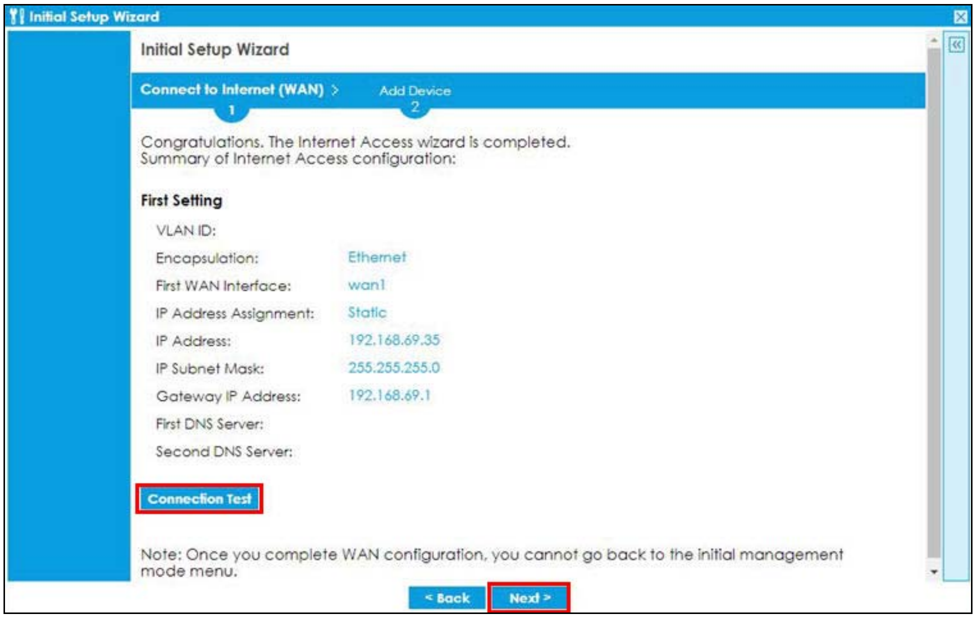
First WAN Interface: ge2

Zone: WAN

IP Address Assignment: Auto

DHCP Option 60:

4 Click **Connection Test** to check that you can access the Internet and then click **Next**.



Initial Setup Wizard

Congratulations. The Internet Access wizard is completed.
Summary of Internet Access configuration:

First Setting

VLAN ID:

Encapsulation: Ethernet

First WAN Interface: wan1

IP Address Assignment: Static

IP Address: 192.168.69.35

IP Subnet Mask: 255.255.255.0

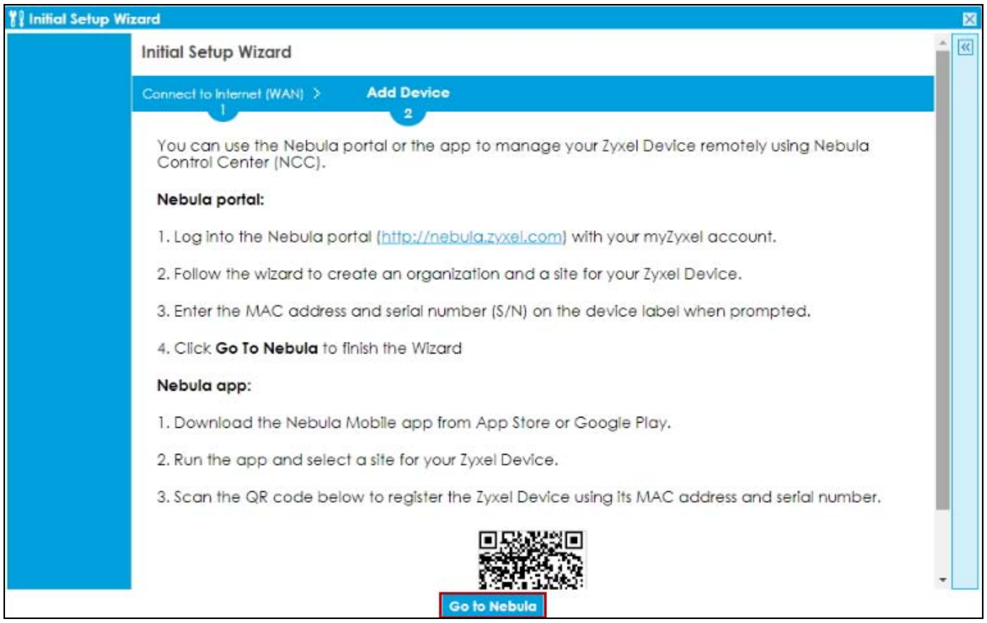
Gateway IP Address: 192.168.69.1

First DNS Server:

Second DNS Server:

Note: Once you complete WAN configuration, you cannot go back to the initial management mode menu.

5 Click **Go to Nebula**.



Initial Setup Wizard

You can use the Nebula portal or the app to manage your Zyxel Device remotely using Nebula Control Center (NCC).

Nebula portal:

1. Log into the Nebula portal (http://nebula.zyxel.com) with your myZyxel account.

2. Follow the wizard to create an organization and a site for your Zyxel Device.

3. Enter the MAC address and serial number (S/N) on the device label when prompted.

4. Click **Go To Nebula** to finish the Wizard

Nebula app:

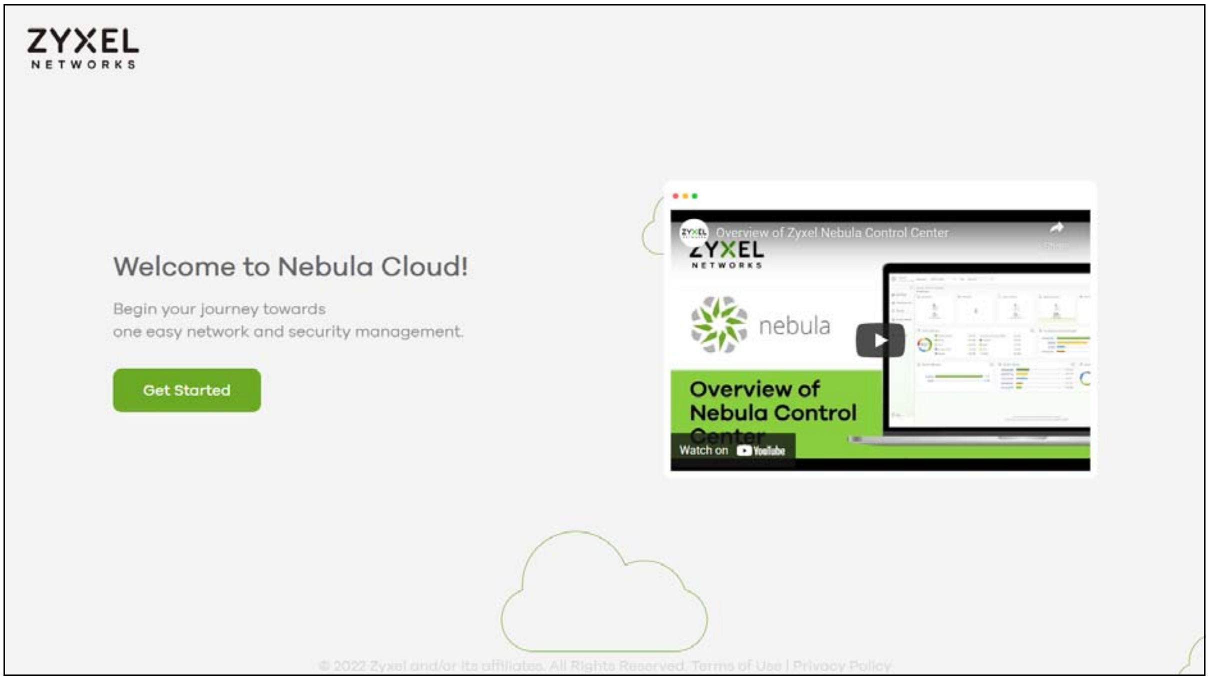
1. Download the Nebula Mobile app from App Store or Google Play.

2. Run the app and select a site for your Zyxel Device.

3. Scan the QR code below to register the Zyxel Device using its MAC address and serial number.

Nebula Configuration

1 You will be redirected to the Nebula portal. Click **Get Started**.



Welcome to Nebula Cloud!

Begin your journey towards
one easy network and security management.

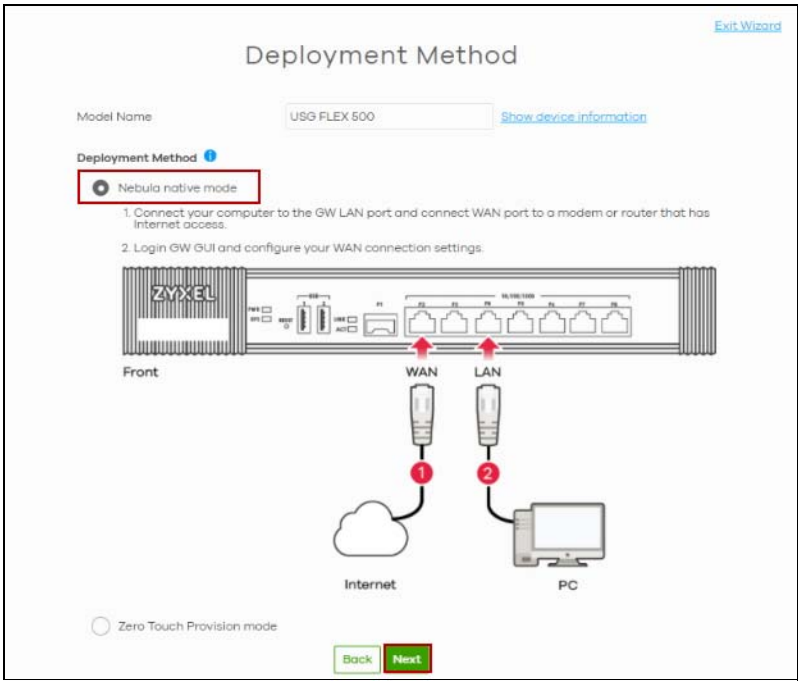
Get Started
Overview of Zyxel Nebula Control Center
ZYXEL NETWORKS
nebula
Overview of Nebula Control Center
Watch on YouTube

© 2022 Zyxel and/or its affiliates. All Rights Reserved. Terms of Use | Privacy Policy

2 Use the Setup Wizard to create an organization and a site, and add the Nebula Device. See Setup Wizard on page 63 for more information on using the wizard.

Note: Make sure to select **Nebula native mode** as the **Deployment Method** in the Setup Wizard.

Note: Nebula Devices with ZLD5.37 Patch 1 or newer firmware do not support the **Zero Touch Provision mode** (see Section 2.1.8 on page 69 for more information on the ZTP deployment method).



Exit Wizard

Deployment Method

Model Name USG FLEX 500 Show device information

Deployment Method

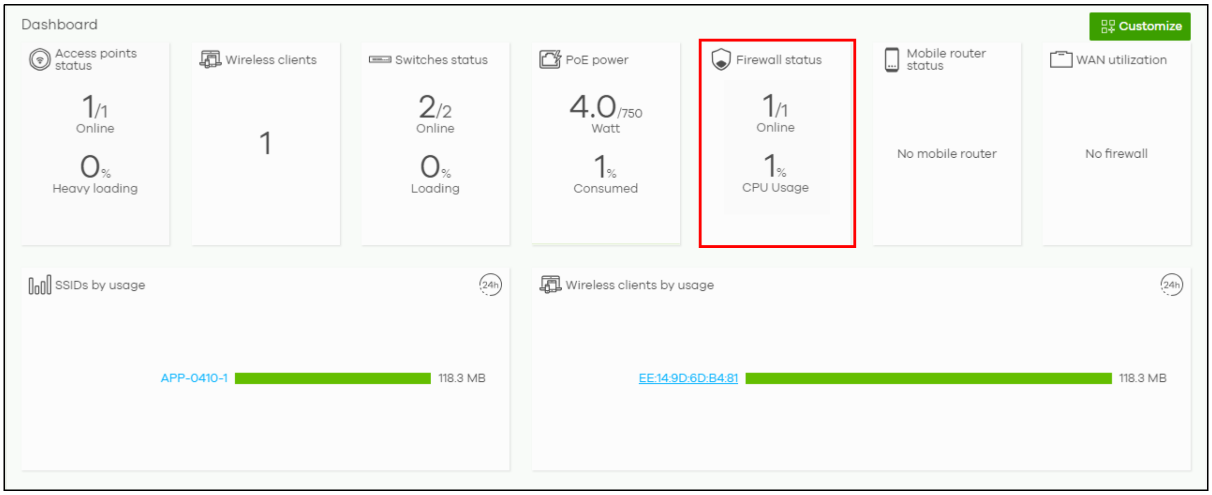
● Nebula native mode

1. Connect your computer to the GW LAN port and connect WAN port to a modem or router that has Internet access.
2. Login GW GUI and configure your WAN connection settings.

○ Zero Touch Provision mode

Back Next

3 After configuring the Setup Wizard, close the Nebula Control Center welcome message to go to the Nebula portal dashboard. **1/1 Online** will show on **Firewall Status**. This means that one SF is registered in Nebula and is online.



Dashboard

Customize

Access points status: 1/1 Online; 0% Heavy loading

Wireless clients: 1

Switches status: 2/2 Online; 0% Loading

PoE power: 4.0/750 Watt; 1% Consumed

Firewall status: 1/1 Online; 1% CPU Usage

Mobile router status: No mobile router

WAN utilization: No firewall

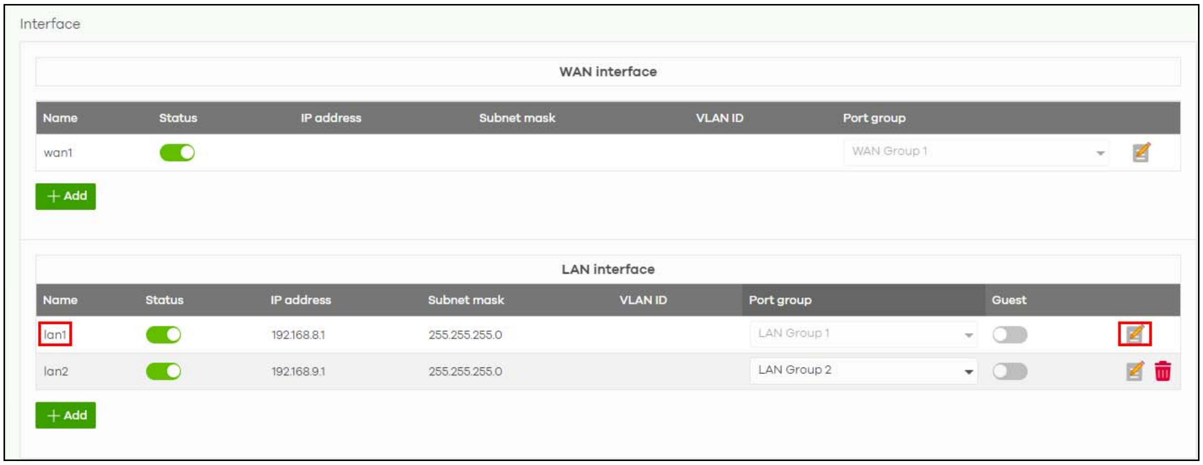
SSIDs by usage (24h): APP-0410-1 118.3 MB

Wireless clients by usage (24h): EE:14:9D:6D:B4:81 118.3 MB

3.45 Configure DHCP Domain Name (for Security Firewalls in Nebula only)

You can configure a DHCP domain name to map to a specific IP address on a specific interface. For this example, to add a domain name for the IP address 192.168.8.1 in the **lan1** interface, do the following.

1 Go to **Site-wide** > **Configure** > **Firewall** > **Interface**. Click the Edit icon for the **lan1** interface to open the **Site-wide** > **Configure** > **Firewall** > **Interface** > **LAN interface configuration** screen.



Interface

WAN interface

Name	Status	IP address	Subnet mask	VLAN ID	Port group	
wan1	●				WAN Group 1	

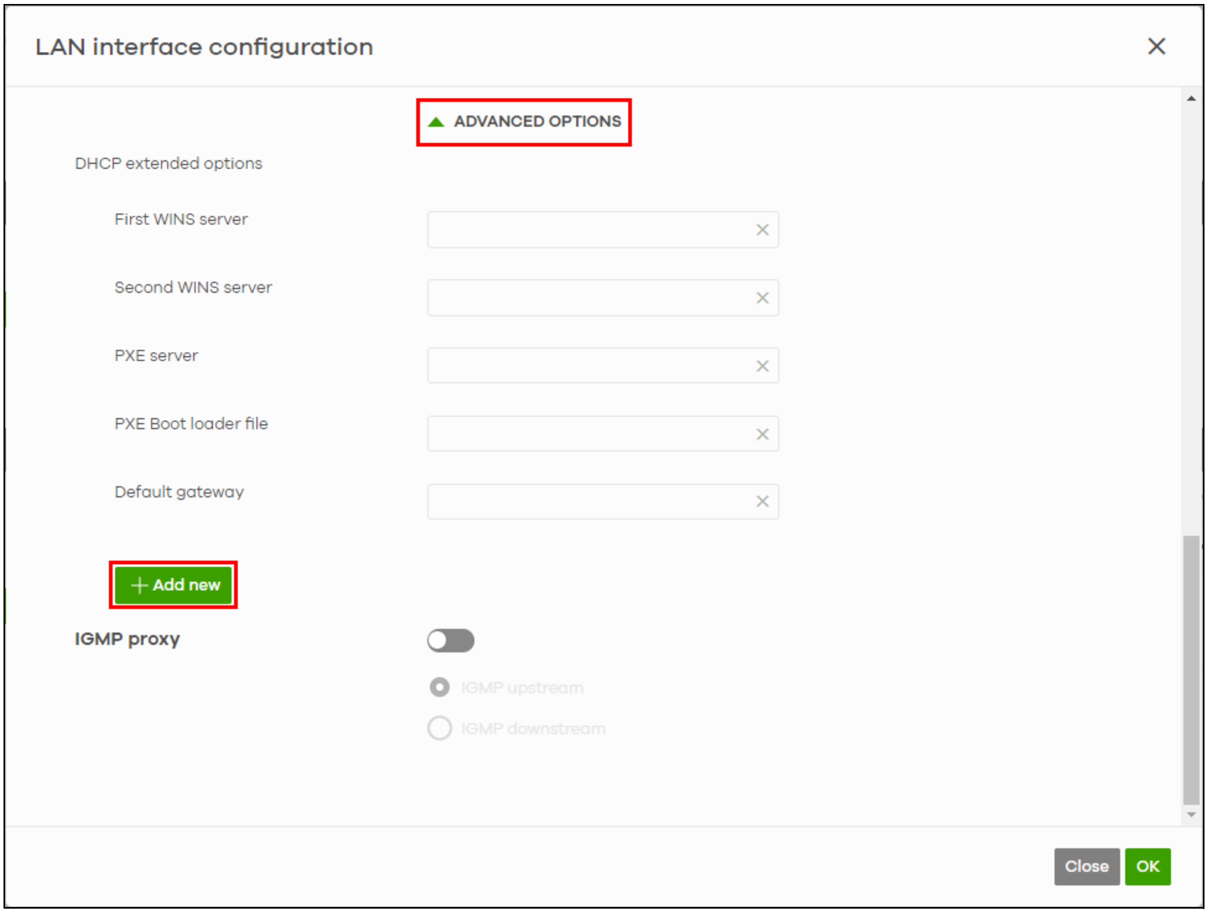
+ Add

LAN interface

Name	Status	IP address	Subnet mask	VLAN ID	Port group	Guest	
lan1	●	192.168.8.1	255.255.255.0		LAN Group 1	○	
lan2	●	192.168.9.1	255.255.255.0		LAN Group 2	○	

+ Add

2 Click **ADVANCED OPTIONS**. Then click **+Add new** to open the **Site-wide** > **Configure** > **Firewall** > **Interface** > **LAN interface configuration**: **DHCP option** screen.



LAN interface configuration

DHCP extended options

First WINS server

Second WINS server

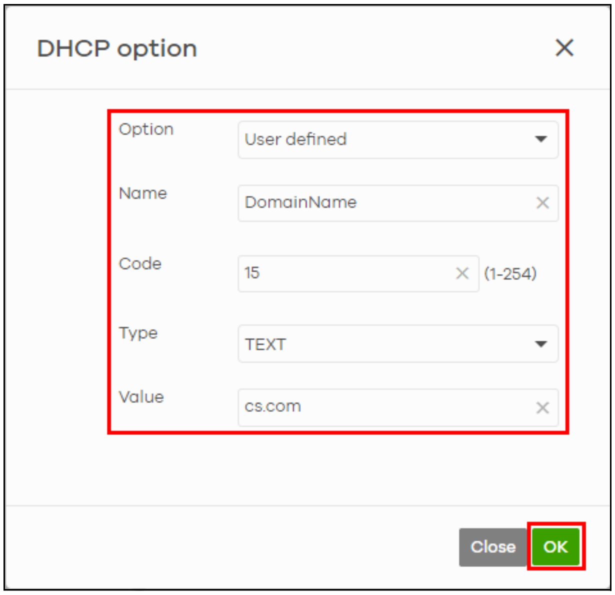
PXE server

PXE Boot loader file

Default gateway

IGMP proxy

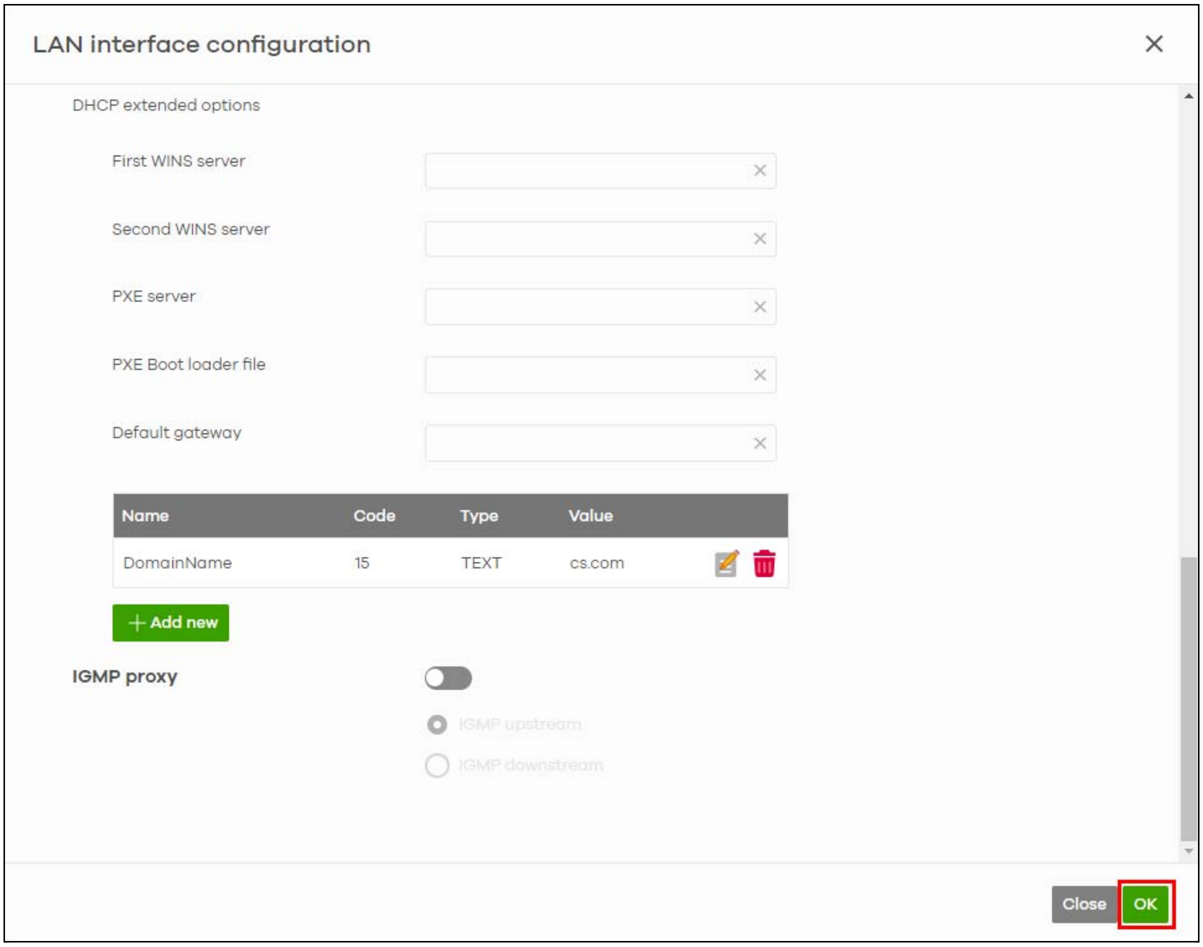
3 Select **User defined** as the DHCP **Option** that you want to add in the DHCP packets sent through the LAN interface. Select **TEXT** for the **Type**, enter a descriptive **Name** to identify and the **Code** number of the selected DHCP option (**15**, for setting the Domain Name). See *https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml* for the list of code numbers. Enter the DNS domain name of the IP address in **Value**. Then click **OK**.



DHCP option

Option	User defined
Name	DomainName
Code	15 (1-254)
Type	TEXT
Value	cs.com

4 A new user-defined DHCP option appears in **LAN interface configuration**. Click **OK**.



LAN interface configuration

DHCP extended options

First WINS server

Second WINS server

PXE server

PXE Boot loader file

Default gateway

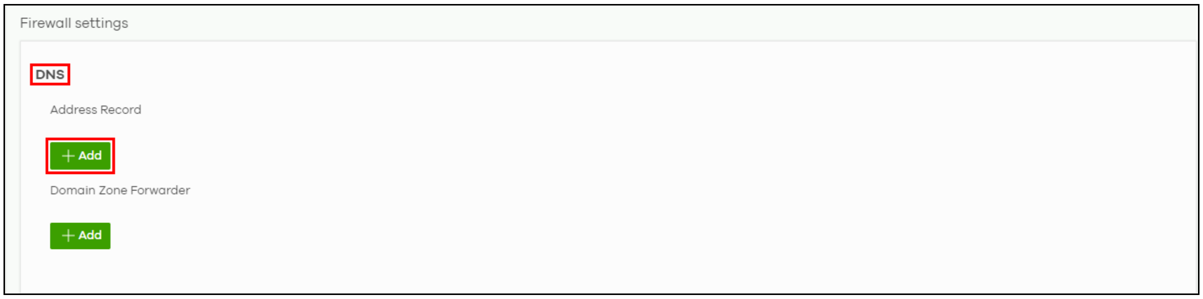
Name	Code	Type	Value
DomainName	15	TEXT	cs.com

IGMP proxy

○ IGMP upstream

○ IGMP downstream

5 Go to **Site-wide** > **Configure** > **Firewall** > **Firewall settings** and click **+Add** in **DNS** to create an **Address Record**. This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address.



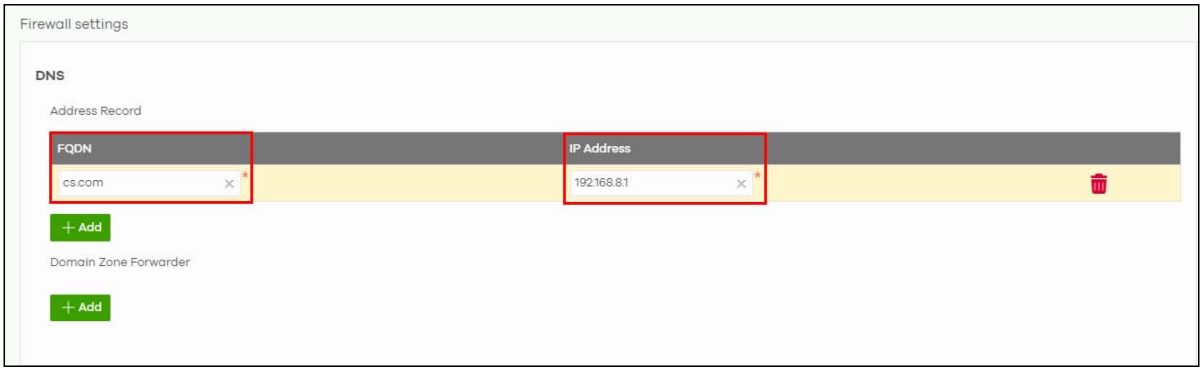
Firewall settings

DNS

Address Record

Domain Zone Forwarder

6 Enter the **FQDN** (cs.com) and **IP Address** (192.168.8.1). Then click **Save** to finish mapping the FQDN to the IP address.

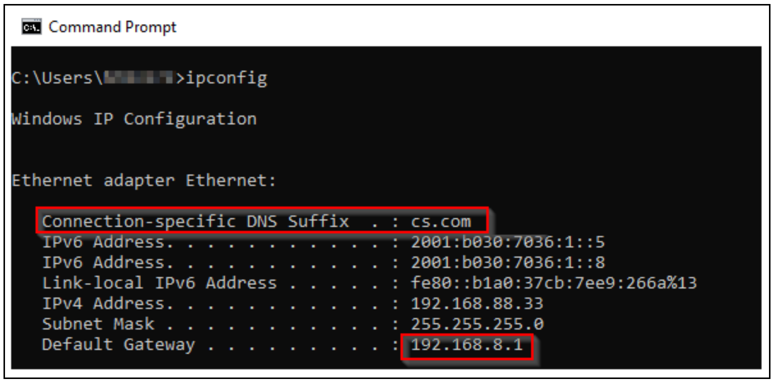


FQDN	IP Address
cs.com	192.168.8.1

To check if the domain name configuration is successful.

1 Connect a computer to the **lan1** interface (with IP address 192.168.8.1).

2 Run the **Command Prompt** and enter **ipconfig**. Check the value for **Connection-specific DNS Suffix** to confirm.

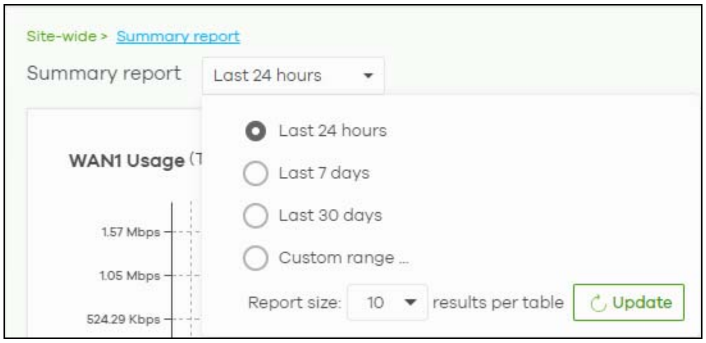


```
C:\Users\[redacted]>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : cs.com
   IPv6 Address. . . . . . . . . . . : 2001:b030:7036:1::5
   IPv6 Address. . . . . . . . . . . : 2001:b030:7036:1::8
   Link-local IPv6 Address . . . . . : fe80::b1a0:37cb:7ee9:266a%13
   IPv4 Address. . . . . . . . . . . : 192.168.88.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.8.1
```

3.46 Monitor Client Bandwidth Usage (for Security Firewalls in Nebula only)

To view network statistics for the Nebula Device of the selected site, such as top client bandwidth usage, do the following.

1 Go to **Site-wide** > **Monitor** > **Firewall** > **Summary report** to select to view the result for the past day, week or month. Alternatively, choose **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table. Then, click **Update**.



Site-wide > Summary report

Summary report   Last 24 hours ▾

WAN1 Usage (T

● Last 24 hours

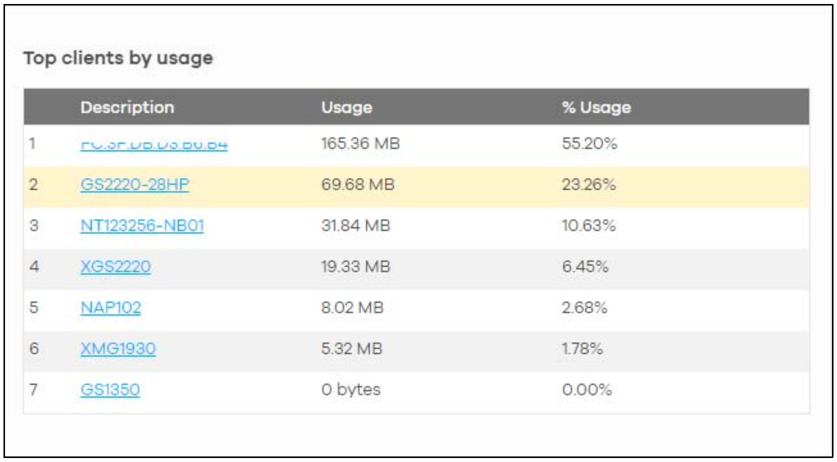
○ Last 7 days

○ Last 30 days

○ Custom range ...

Report size: 10 ▾ results per table   Update

2 Check the **Top clients by usage** widget.

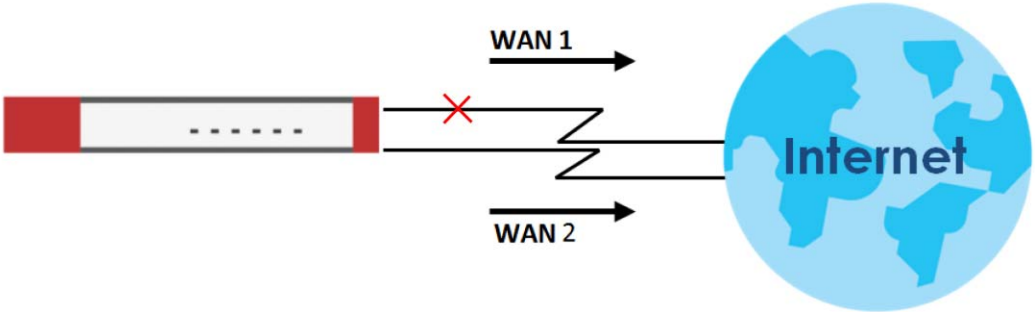


Top clients by usage

	Description	Usage	% Usage
1	FC:3F:DB:D5:B0:B4	165.36 MB	55.20%
2	GS2220-28HP	69.68 MB	23.26%
3	NT123256-NB01	31.84 MB	10.63%
4	XGS2220	19.33 MB	6.45%
5	NAP102	8.02 MB	2.68%
6	XMG1930	5.32 MB	1.78%
7	GS1350	0 bytes	0.00%

3.47 Configure a Primary and Backup WAN (for Security Firewalls in NCC only)

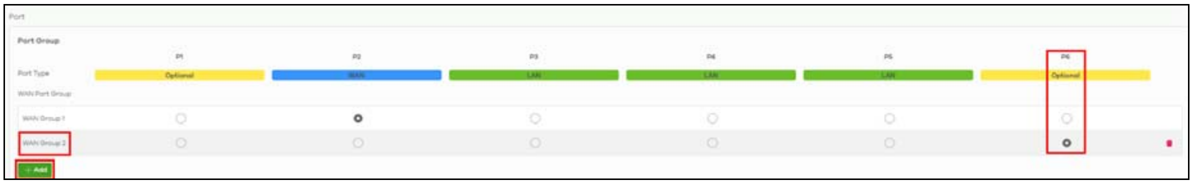
When you have 2 Internet connections, you can configure a primary connection and backup connection. For example, if the primary connection (**WAN 1**) goes offline, the Nebula Device can send its traffic through the backup connection (**WAN 2**). Traffic will use the primary connection (**WAN 1**) again when it returns online.



Note: The Nebula Device will periodically send 'Keepalive Packets' through the backup connection.

This tutorial uses the ATP100 as example. To configure a primary (**P2**) and backup connection (**P6**), do the following:

1 Click **+Add** to create **WAN Group 2**.



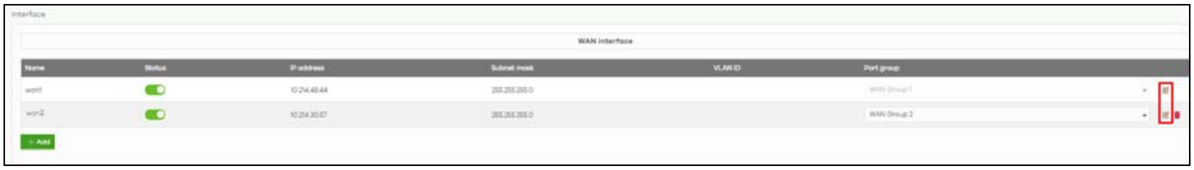
Port

Port Group

	P1	P2	P3	P4	P5	P6
Port Type	Optional	WAN	LAN	LAN	LAN	Optional
WAN Port Group						
WAN Group 1	○	●	○	○	○	○
WAN Group 2	○	○	○	○	○	●

2 Click to assign the **P6** port to **WAN Group 2**.

3 Go to **Site-wide** > **Configure** > **Firewall** > **Interface**, and click the edit icon to set an IP address for each WAN interface.

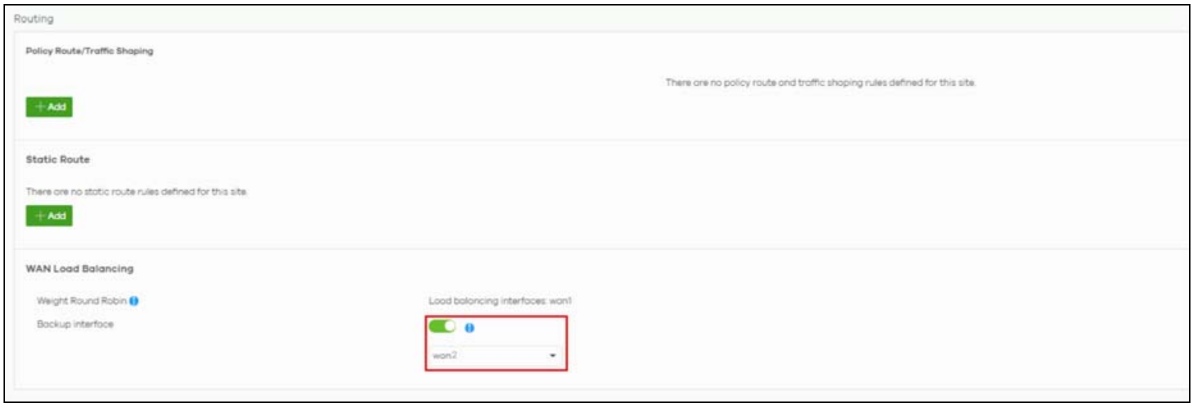


Interface

WAN interface

Name	Status	IP address	Subnet mask	VLAN ID	Port group
wan1	●	10.214.48.44	255.255.255.0		WAN Group 1
wan2	●	10.214.30.57	255.255.255.0		WAN Group 2

4 Go to **Site-wide** > **Configure** > **Firewall** > **Routing**, turn on **Backup interface** and select **wan2** as the secondary WAN.



Routing

Policy Route/Traffic Shaping

There are no policy route and traffic shaping rules defined for this site.

Static Route

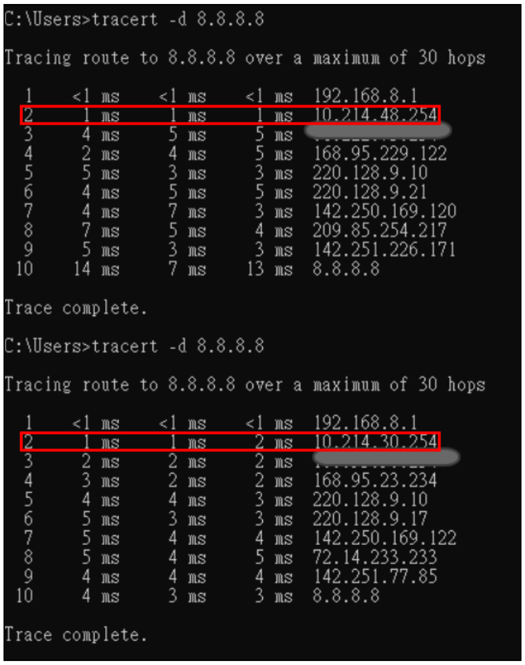
There are no static route rules defined for this site.

WAN Load Balancing

Weight Round Robin: Load balancing interfaces: wan1

Backup interface: ● wan2

5 Perform a traceroute to test if **wan2** takes over when **wan1** goes down. When both **wan1** and **wan2** connections are working, the destination of the network traffic is the **wan1** gateway (in this example, 10.214.48.254). Disconnect the **wan1** connection. Outgoing WAN traffic now goes through the **wan2** interface to gateway 10.214.30.254 in this example.



```
C:\Users>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.8.1
  2     1 ms     1 ms     1 ms  10.214.48.254
  3     4 ms     5 ms     5 ms  [redacted]
  4     2 ms     4 ms     5 ms  168.95.229.122
  5     5 ms     3 ms     3 ms  220.128.9.10
  6     4 ms     5 ms     5 ms  220.128.9.21
  7     4 ms     7 ms     3 ms  142.250.169.120
  8     7 ms     5 ms     4 ms  209.85.254.217
  9     5 ms     3 ms     3 ms  142.251.226.171
 10    14 ms     7 ms    13 ms  8.8.8.8

Trace complete.

C:\Users>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.8.1
  2     1 ms     1 ms     2 ms  10.214.30.254
  3     2 ms     2 ms     2 ms  [redacted]
  4     3 ms     2 ms     2 ms  168.95.23.234
  5     4 ms     4 ms     3 ms  220.128.9.10
  6     5 ms     3 ms     3 ms  220.128.9.17
  7     5 ms     4 ms     4 ms  142.250.169.122
  8     5 ms     4 ms     5 ms  72.14.233.233
  9     4 ms     4 ms     4 ms  142.251.77.85
 10     4 ms     3 ms     3 ms  8.8.8.8

Trace complete.
```

6 Perform a traceroute to test if **wan2** takes over when **wan1** goes down. When both **wan1** and **wan2** connections are working, the destination of the network traffic is the **wan1** gateway (in this example, 10.214.48.254). Disconnect the **wan1** connection. Outgoing WAN traffic now goes through the **wan2** interface to gateway 10.214.30.254 in this example.

3.48 Enable Smart Mesh on a Security Router

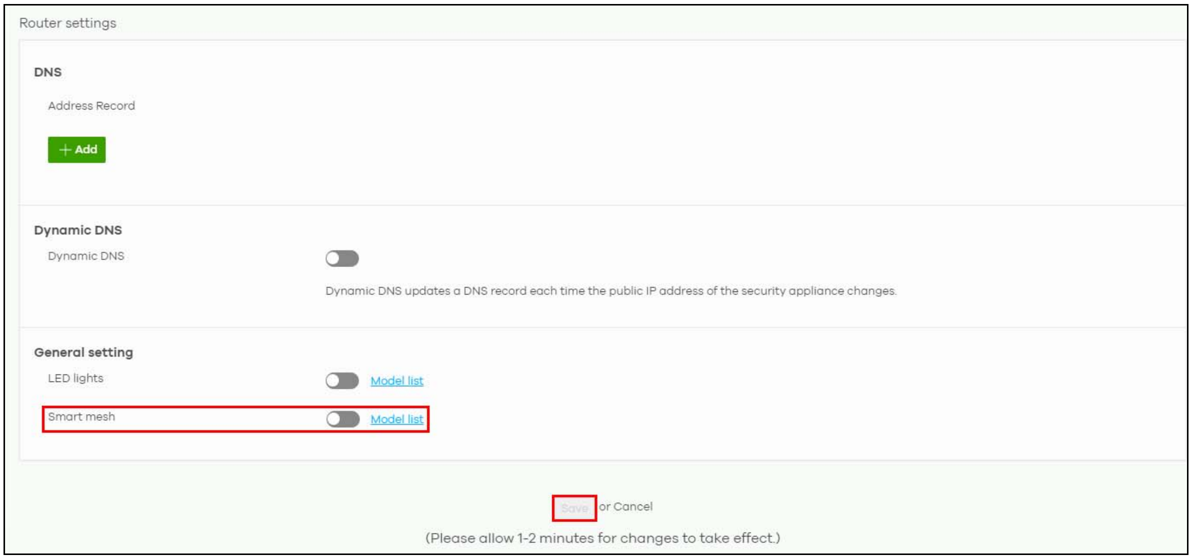
Use Smart Mesh to have two or more Nebula Devices automatically create a mesh network within your home or office, ensuring there are no areas with a weak WiFi signal. For more information on the Smart Mesh feature, see Section 5.1.1 on page 303.

Note: Only one Security Router (for example, USG LITE 60AX) is allowed per site.

Note: Make sure there is one or more supported access points (APs) in the site to use the "Smart mesh" feature.

To use the Smart Mesh feature on the USG LITE 60AX, do the following:

1 Go to **Site-wide** > **Configure** > **Security router** > **Router settings**.



Router settings

DNS

Address Record

Dynamic DNS

Dynamic DNS

Dynamic DNS updates a DNS record each time the public IP address of the security appliance changes.

General setting

LED lights

Smart mesh

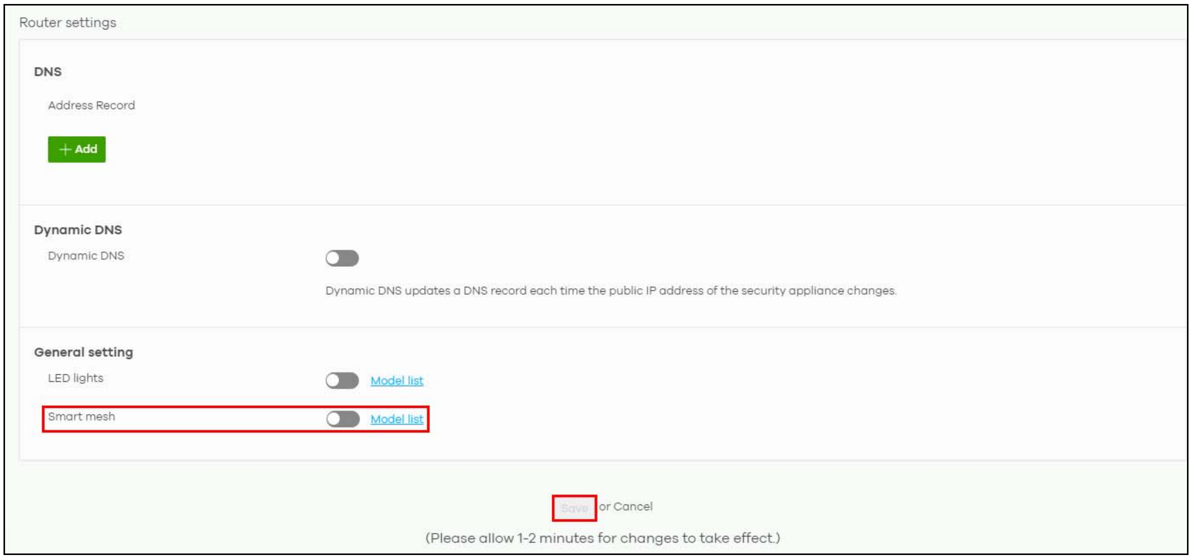
or Cancel

(Please allow 1-2 minutes for changes to take effect.)

2 In **General setting**, click the **Smart mesh** switch to the right to enable the NCC Smart Mesh feature on the USG LITE 60AX on the site.

3 Then click the **Save** button to save the changes.

4 Go to **Site-wide** > **Configure** > **Access points** > **AP & port settings**.



Router settings

DNS

Address Record

Dynamic DNS

Dynamic DNS

Dynamic DNS updates a DNS record each time the public IP address of the security appliance changes.

General setting

LED lights

Smart mesh

or Cancel

(Please allow 1-2 minutes for changes to take effect.)

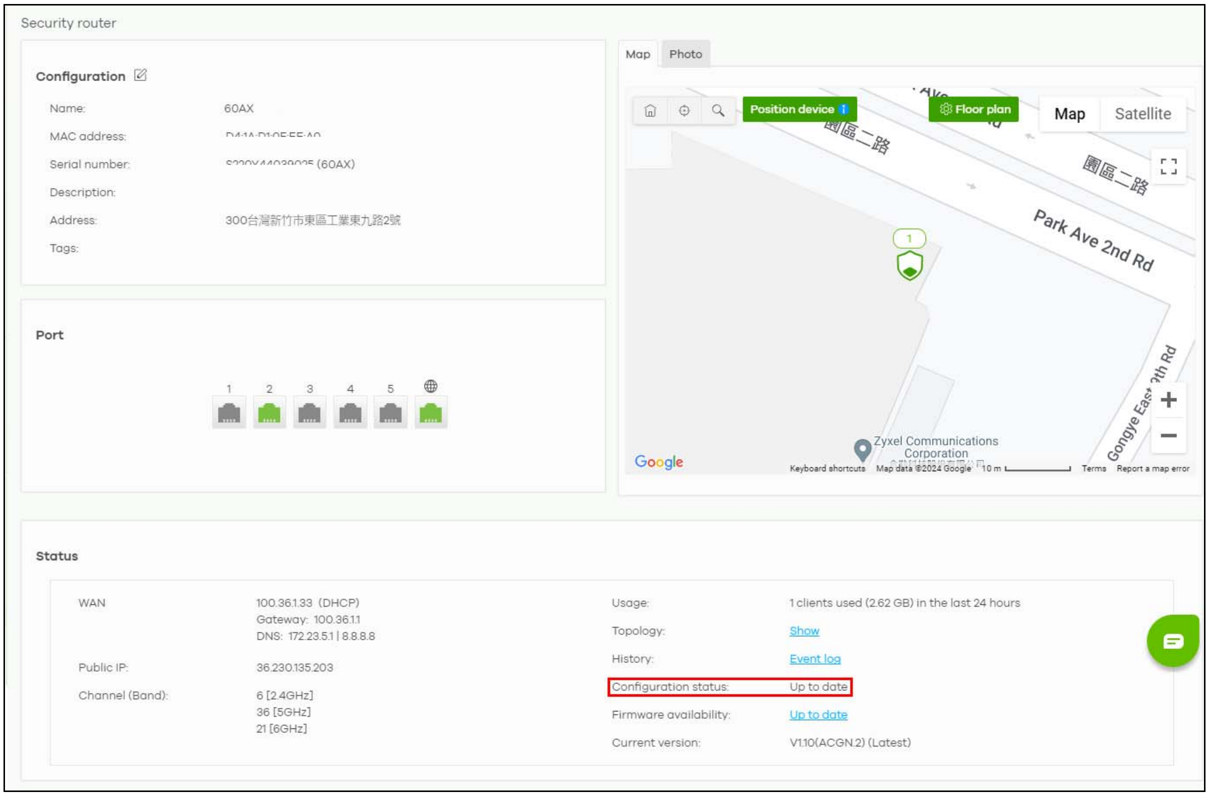
5 In **General setting**, click the **Smart mesh** switch to the right to enable the NCC Smart Mesh feature on the Nebula AP on the site.

6 Then click the **Save** button to save the changes.

7 Refer to the USG LITE 60AX User's Guide: **Hardware Connections** for connecting the Nebula Security Router to the Internet.

8 Use an Ethernet cable to connect the USG LITE 60AX to the Nebula AP. Wait until the USG LITE 60AX LED is steady green.

9 Go to **Site-wide** > **Devices** > **Security router** to check if the USG LITE 60AX shows **Up to date** on the **Configuration status**.



Security router

Configuration

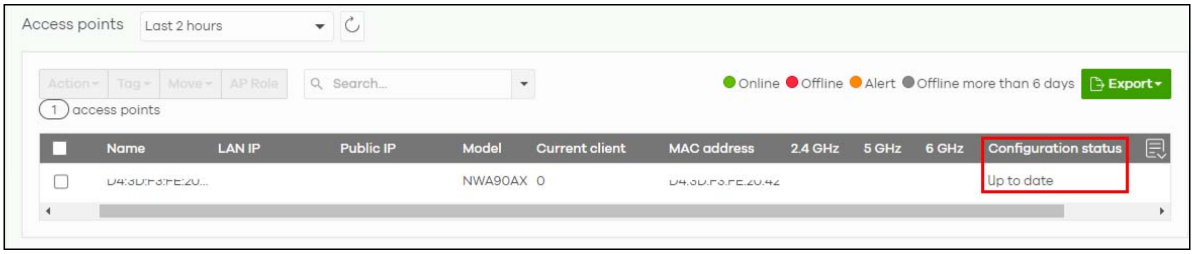
Name:	60AX
MAC address:	D4:1A:D1:0E:EE:A0
Serial number:	S220Y44039025 (60AX)
Description:	
Address:	300台灣新竹市東區工業東九路2號
Tags:	

Port

Status

WAN	100.36.1.33 (DHCP) Gateway: 100.36.1.1 DNS: 172.23.5.1 | 8.8.8.8	Usage:	1 clients used (2.62 GB) in the last 24 hours
		Topology:	Show
		History:	Event log
Public IP:	36.230.135.203	Configuration status:	Up to date
Channel (Band):	6 [2.4GHz] 36 [5GHz] 21 [6GHz]	Firmware availability:	Up to date
		Current version:	V1.10(ACGN.2) (Latest)

10 Go to the **Site-wide** > **Devices** > **Access points** screen to check if the Nebula AP shows **Up to date** on the **Configuration status**. This means that the mesh network is configured correctly.



Access points Last 2 hours

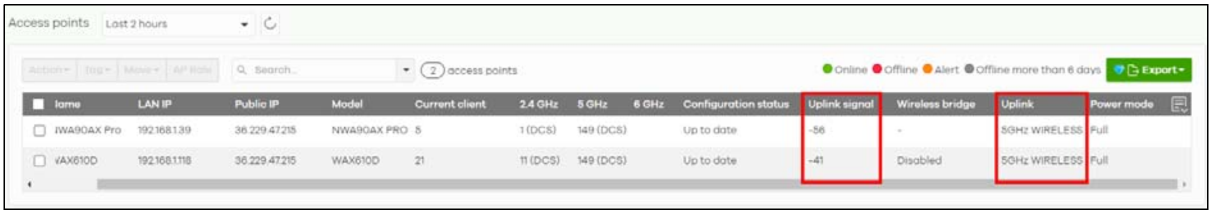
1 access points

☐	Name	LAN IP	Public IP	Model	Current client	MAC address	2.4 GHz	5 GHz	6 GHz	Configuration status
☐	D4:3D:F3:FE:20...			NWA90AX	0	D4:3D:F3:FE:20:42				Up to date

11 Unplug the Ethernet and power cable from the Nebula AP. Place the Nebula AP where you want to extend your WiFi signal, approximately 10 to 15 meters away from the USG LITE 60AX with a clear line of sight.

12 Plug in the power adapter to the Nebula AP. Make sure the LINK LED is steady green. The Nebula AP will act as a repeater AP.
Alternatively, move the Nebula AP closer to the USG LITE 60AX if the LINK LED is not steady green. For more details on the Nebula AP LEDs, please refer to the Nebula AP User's Guide.

13 Go to **Site-wide** > **Devices** > **Access points** to check the Nebula AP's Smart Mesh uplink band (**Uplink**) and the signal strength (**Uplink signal**). The Mesh link should use the 6 GHz Smart Mesh uplink band and a signal strength better than –75 dBm. See How to Position Multiple Nebula Devices (for Nebula Access Points only) for selecting the best position to minimize signal interference for multiple Nebula APs.


Access points Last 2 hours

2 access points

● Online ● Offline ● Alert ● Offline more than 6 days Export

□	lame	LAN IP	Public IP	Model	Current client	2.4 GHz	5 GHz	6 GHz	Configuration status	Uplink signal	Wireless bridge	Uplink	Power mode
□	IWA90AX Pro	192.168.1.39	36.229.47.215	NWA90AX PRO	5	1 (DCS)	149 (DCS)		Up to date	-56	-	5GHz WIRELESS	Full
□	VAX610D	192.168.1.118	36.229.47.215	WAX610D	21	11 (DCS)	149 (DCS)		Up to date	-41	Disabled	5GHz WIRELESS	Full

14 Configure an SSID for the Nebula AP. See Section 3.24 on page 142 for more information on configuring an SSID.

PART II

Manage by Site Deployment

CHAPTER 4
Site-wide

4.1 Dashboard

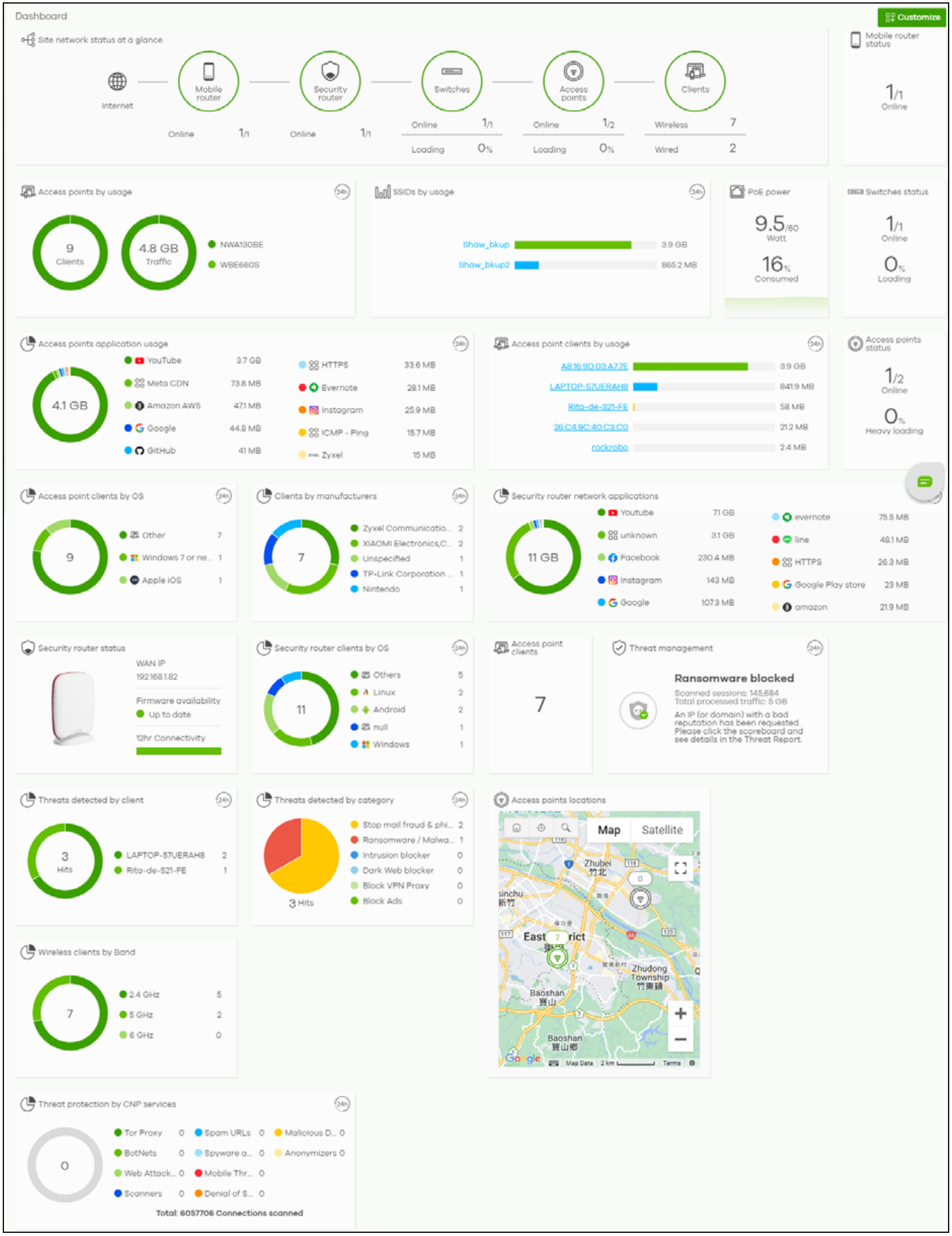
If a site is created and selected, the **Dashboard** is always the first menu you see when you log into the NCC. You can also click **Site-wide** > **Dashboard** to access this screen.

It shows the status and information for all types of Nebula Devices connected to the selected site by default.

Note: The banner **N Switches are currently protected by Auto Configuration Recovery** will display when the Nebula Switch(es) is locked by NCC. Click **N Switches** to go to **Site-wide** > **Monitor** > **Switches** for more information.

Click **Customize** to show the **Widget**, **Reset** and **Close** buttons. You can then rearrange widgets by selecting a block and holding it to move around. You can also click the **Widget** button to collapse, add and close individual widgets. Click **Reset** to return the widget settings to the defaults.

Figure 34 Site-wide > Dashboard



Dashboard

Customize

Site network status at a glance

Internet — Mobile router — Security router — Switches — Access points — Clients

Mobile router		Security router		Switches		Access points		Clients	
Online	1/1	Online	1/1	Online	1/1	Online	1/2	Wireless	7
				Loading	0%	Loading	0%	Wired	2

Mobile router status

1/1 Online

Access points by usage

9 Clients

4.8 GB Traffic

- ● NWA130BE
- ● WBE660S

SSIDs by usage

Shaw_bkup	3.9 GB
Shaw_bkup2	865.2 MB

PoE power

9.5/60 Watt

16% Consumed

Switches status

1/1 Online

0% Loading

Access points application usage

4.1 GB

● YouTube	3.7 GB	● HTTPS	33.6 MB
● Meta CDN	73.8 MB	● Evernote	28.1 MB
● Amazon AWS	47.1 MB	● Instagram	25.9 MB
● Google	44.8 MB	● ICMP - Ping	15.7 MB
● GitHub	41 MB	● Zyxel	15 MB

Access point clients by usage

A8:16:9D:03:A7:7E	3.9 GB
LAPTOP-57UERAH8	841.9 MB
Rita-de-S21-FE	58 MB
26:C4:9C:40:C3:C0	21.2 MB
rockrobo	2.4 MB

Access points status

1/2 Online

0% Heavy loading

Access point clients by OS

9

● Other	7
● Windows 7 or ne...	1
● Apple iOS	1

Clients by manufacturers

7

● Zyxel Communicatio...	2
● XIAOMI Electronics,C...	2
● Unspecified	1
● TP-Link Corporation ...	1
● Nintendo	1

Security router network applications

11 GB

● Youtube	7.1 GB	● evernote	75.5 MB
● unknown	3.1 GB	● line	48.1 MB
● Facebook	230.4 MB	● HTTPS	26.3 MB
● Instagram	143 MB	● Google Play store	23 MB
● Google	107.3 MB	● amazon	21.9 MB

Security router status

WAN IP
192.168.1.82

Firmware availability
● Up to date

12hr Connectivity

Security router clients by OS

11

● Others	5
● Linux	2
● Android	2
● null	1
● Windows	1

Access point clients

7

Threat management

Ransomware blocked

Scanned sessions: 145,684
Total processed traffic: 5 GB

An IP (or domain) with a bad reputation has been requested. Please click the scoreboard and see details in the Threat Report.

Threats detected by client

3 Hits

● LAPTOP-57UERAH8	2
● Rita-de-S21-FE	1

Threats detected by category

3 Hits

● Stop mail fraud & phi...	2
● Ransomware / Malwa...	1
● Intrusion blocker	0
● Dark Web blocker	0
● Block VPN Proxy	0
● Block Ads	0

Access points locations

Map Satellite

Wireless clients by Band

7

● 2.4 GHz	5
● 5 GHz	2
● 6 GHz	0

Threat protection by CNP services

0

● Tor Proxy	0	● Spam URLs	0	● Malicious D...	0
● BotNets	0	● Spyware a...	0	● Anonymizers	0
● Web Attack...	0	● Mobile Thr...	0		
● Scanners	0	● Denial of S...	0		

Total: 6057706 Connections scanned

The following table describes the labels in this screen.

Table 16 Site-wide > Dashboard

LABEL	DESCRIPTION
Access points status	This shows the number of assigned and connected Nebula access points, and what percentage of the access points become overloaded, that is, the number of online access points that exceed the maximum client device number (in **Site-wide** > **Configure** > **Access points** > **Traffic shaping**) by total number of online access points in the site.
Access point clients	This shows the number of WiFi clients currently connected to the managed access points.
Switches status	This shows the number of Nebula Switches assigned and connected, and what percentage of the Switches become overloaded, that is, the number of online Nebula Switches that exceed 70% of their upstream bandwidth by total number of online Nebula Switches in the site.
PoE power	This shows the total PoE power budget on the Switch and the current amount of power consumed by the powered devices.
Security router / Firewall / Security Gateway / Mobile router status	This shows the number of Nebula Security Appliances assigned and connected, and what percentage of the Security Appliance's processing capability is currently being used if the CPU goes over 93% usage. Note: The Security Firewall(s) in Cloud Monitoring mode will only show the online status but not the CPU usage.
WAN utilization	This shows the data rate of inbound/outbound traffic in Kbps (kilobits per second) or Mbps (megabits per second) that has been transmitted through the WAN interface. If the Security Appliance supports multiple WAN interfaces and more than one are active, use the arrow to switch and view the throughput of each WAN interface. Note: The Security Firewall(s) in Cloud Monitoring mode will not show.
Security alert	This shows the total number of the latest alerts sent to the administrator in the last 24 hours. Note: The Security Firewall(s) in Cloud Monitoring mode will not show.
Mobile router	This shows the number of Nebula mobile routers assigned and connected.
Security router / Firewall / Security Gateway network applications	This shows the top ten applications used by the Nebula Security Appliance in the past 24 hours. Note: The Security Firewall(s) in Cloud Monitoring mode will not show.
Security router / Firewall / Security Gateway clients by usage	This shows the top five clients of the Nebula Security Appliance with the highest percentage of bandwidth usage in the past 24 hours. Note: The Security Firewall(s) in Cloud Monitoring mode will not show.
Security router clients by OS	This shows the top five operating systems used by security router client devices in the past 24 hours. You can click an operating system to go to the **Site-wide** > **Clients** screen and view the client devices which use this operating system.
Threat management	This shows the number of threat management detections and the total volume of network traffic (GB) in the past 24 hours.
Threat detected by category	This shows the total number of times the category to which the threat belongs was detected in the past 24 hours.
Threat detected by client	This shows the name of the top five client devices who encountered a threat and the total number of threats detected in the past 24 hours.
Access point clients	This shows the number of WiFi clients connected (clients of the access points only).
SSIDs by usage	This shows the top five SSIDs with the highest percentage of bandwidth usage in the past 24 hours. You can click a WiFi network name to go to the **Site-wide** > **Monitor** > **Access Point** > **Summary report** screen.

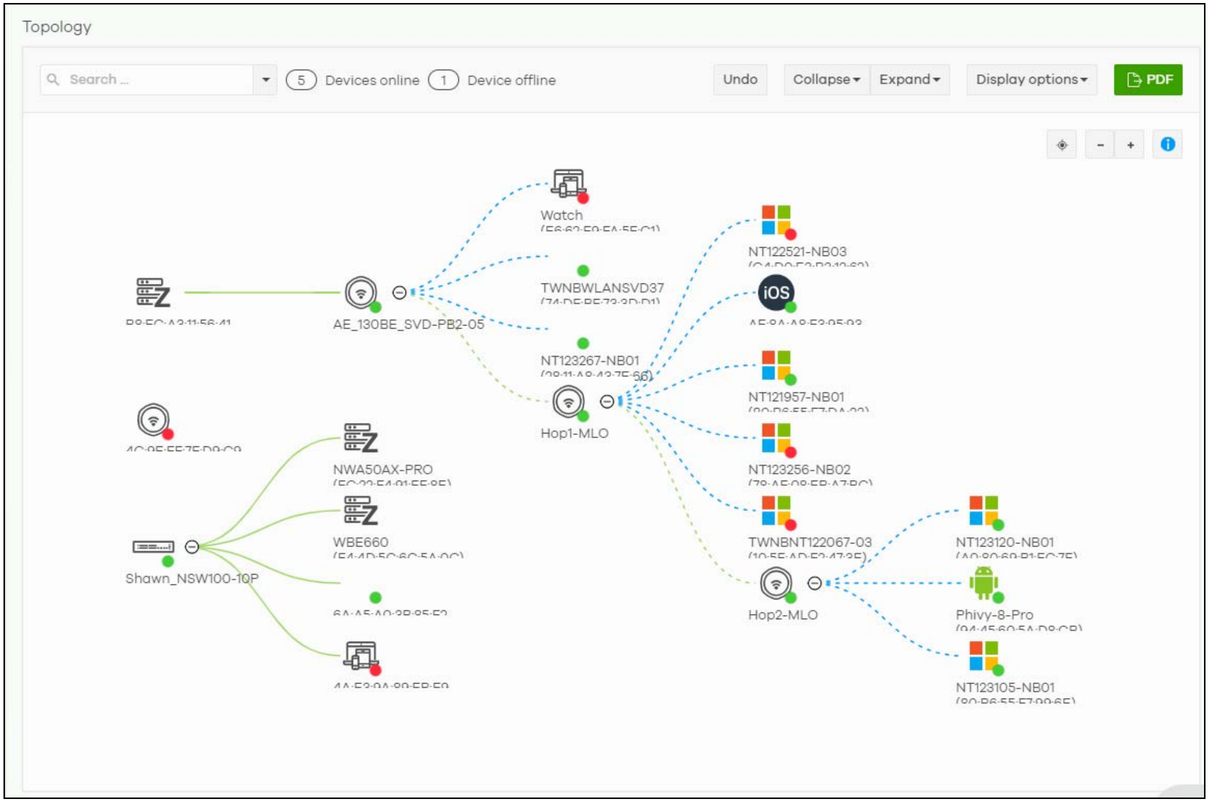
Table 16 Site-wide > Dashboard (continued)

LABEL	DESCRIPTION
Access point clients by usage	This shows the top five WiFi clients (clients of the access points only) with the highest percentage of bandwidth usage in the past 24 hours. You can click a client's name to go to the **Site-wide** > **Clients: Client list** screen.
Clients by manufacturers	This shows the top five manufacturers of WiFi client devices in the past 24 hours. You can click a manufacturer name to go to the **Site-wide** > **Clients** screen and view the client devices which are made by the manufacturer.
Collaborative detection & response hit	This shows the total number of malicious traffic detected from wired and WiFi clients that are blocked and quarantined using Collaborative Detection & Response (CDR) in the past 7 days. Note: The Security Firewall(s) in Cloud Monitoring mode will not show.
Access point clients by OS	This shows the top five operating systems used by WiFi client devices in the past 24 hours. You can click an operating system to go to the **Site-wide** > **Clients** screen and view the client devices that use this operating system.
Access points by usage	This shows the top five managed access points with the highest percentage of bandwidth usage in the past 24 hours. This also shows the number of WiFi clients associated with the access points. You can click an access point's name to go to the **Site-wide** > **Devices** > **Access Points**: **Access Points Details** screen.
Access points application usage	This shows the usage statistic of the top ten applications used in the site in the past 24 hours.
Access points locations	This shows the locations of access points on the Google map.
Threat protection by CNP services	This shows the total number of times packets coming from an IPv4 address with a bad reputation occur and the number of times connection attempts to an IPv4 address with a bad reputation occur in the past 24 hours.
Wireless client by band	This shows the total number of access points / SCR 50AXE / USG Lite 60AX WiFi client devices in the 2.4 / 5 / 6 GHz band. You can click a band to go to the **Site-wide** > **Clients** screen and view the client devices that use the respective WiFi band.

4.2 Topology

Use this screen to view the connections between Nebula Devices in the site. Click **Site-wide** > **Topology** to access this screen.

Figure 35 Site-wide > Topology



The icon of a node in the network topology indicates its Nebula Device type and the color shows whether the Nebula Device is online (green), has alerts (amber), or is offline (red). **Zyxel device** is a device manufactured by Zyxel but not registered at the NCC or unable to work in Nebula cloud management mode.

Scroll the mouse up/down to zoom in/out, or click **+** / **–** for clearer viewing. Click and hold the left mouse button while moving the mouse to change the position of the network topology diagram. Click the Center icon (⌖) to move the network topology diagram to the default position.

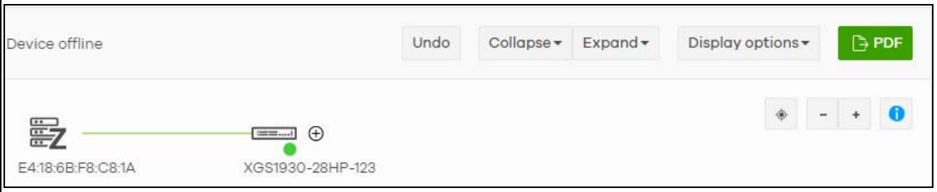
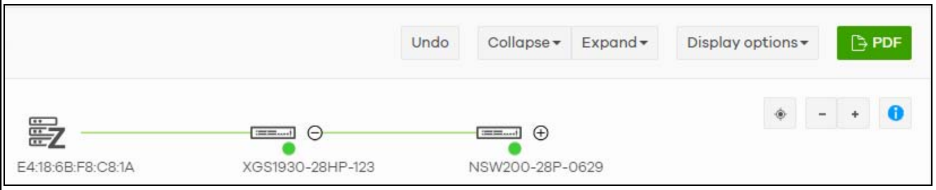
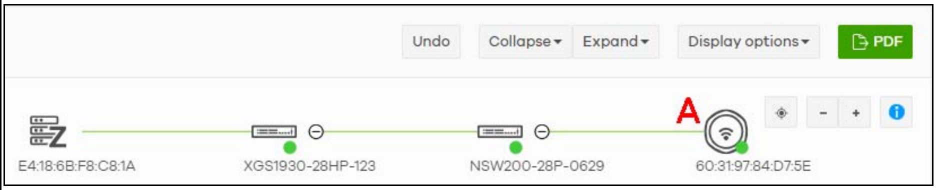
Note: Client devices must support LLDP in order to appear correctly after a Nebula accessory.

The following table describes the labels in this screen.

Table 17 Site-wide > Topology

LABEL	DESCRIPTION
Search	Set the filter to view the particular Nebula Device(s) and client device(s) in the network topology diagram. The number of matches is displayed, including the number of online/offline device(s).
Undo	Click this to cancel your action on the **Collapse** and **Expand** buttons.

Table 17 Site-wide > Topology (continued)

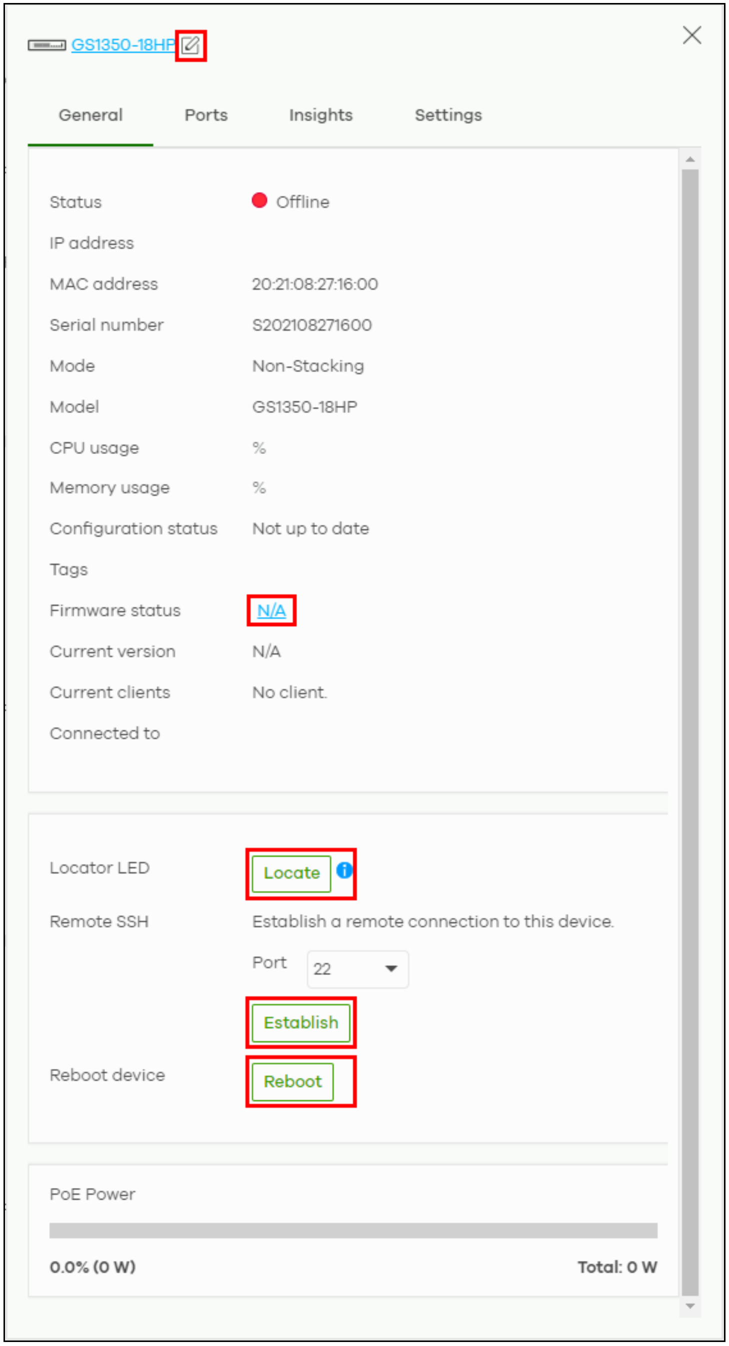
LABEL	DESCRIPTION
Collapse	Click this button and select **All** to hide all connections after the Security Appliance in the network topology diagram.  Device offline Undo Collapse Expand Display options PDF E4:18:6B:F8:C8:1A XGS1930-28HP-123 Alternatively, select **All access points** to hide all connections after the access point(s) in the network topology diagram.  Undo Collapse Expand Display options PDF E4:18:6B:F8:C8:1A XGS1930-28HP-123 NSW200-28P-0629
Expand	Click this button and select **All** to show all connections after the Security Appliance in the network topology diagram.  Undo Collapse Expand Display options PDF A E4:18:6B:F8:C8:1A XGS1930-28HP-123 NSW200-28P-0629 60:31:97:84:D7:5E Alternatively, select **All access points** to show all connections after the access point(s) in the network topology diagram if (**A**) in the above figure is hidden.
Display options	Enable **Show all clients** > **Wireless/Wired** to display the WiFi/wired client(s) that are connected to your network. Enable **Online clients** / **Offline clients** to display all client(s) that are connected to the Nebula Device / disconnected from the Nebula Device. Enable **Show device name** / **Show client name** / **Show client MAC address** to show the Nebula Device information, such as MAC address / device name and/or client device's MAC address / name in the network topology diagram. Note: NCC only displays clients connected to your network from the last 2 hours. Enable **Show redundant links** to display the secondary connection between two nodes, and also display the Nebula Device(s) that are connected to your network but cannot be identified by the NCC. The non-Nebula Device(s) installed in the network are detected by the NCC through LLDP packets. if any. Then, click **Apply**. NCC remembers the display options for each site and applies them the next time the administrator visits the **Topology** page.
PDF	Click this button to download the network topology diagram as a PDF file.

4.2.1 General

Click a Nebula Device node to view detailed Nebula Device information in the **General** tab. Click a client device node to view detailed client device information based on analytics gathered from the **Site-wide** > **Clients** pages. In the **General** tab, you can do the following:

- Click the edit icon beside the Nebula Device name to change the name of the Nebula Device.
- View the percentage of the Nebula Device's processing capability that is currently being used in **CPU usage**.
- View the percentage of the Nebula Device's RAM processing capability that is currently being used in **Memory usage**.
- Click **Firmware status** to update the Nebula Device's firmware if it is not the latest.
- Click **Locate** to turn on the **LOCATOR** LED on the Nebula Device for 5 minutes. This shows the actual location of the Nebula Device in the topology.
- Specify the **Port** number and click **Establish** using **Remote access** to establish a remote connection to this Nebula Device.
- Click **Reboot** to restart the Nebula Device.
- View the percentage of PoE power usage and the **Total** power the Nebula Device (Switches only) can provide to the connected PDs in **PoE Power**.
- View the **WAN Usage** of the Nebula Device (Security Appliances only). The y-axis shows the transmission speed of data sent or received through the WAN connection in megabits per second (Mbps). The x-axis shows the time period over which the traffic flow occurred.

Figure 36 Site-wide > Topology > General



Status ● Offline

IP address

MAC address 20:21:08:27:16:00

Serial number S202108271600

Mode Non-Stacking

Model GS1350-18HP

CPU usage %

Memory usage %

Configuration status Not up to date

Tags

Firmware status N/A

Current version N/A

Current clients No client.

Connected to

Locator LED Locate

Remote SSH Establish a remote connection to this device.

Port 22

Reboot device Reboot

PoE Power

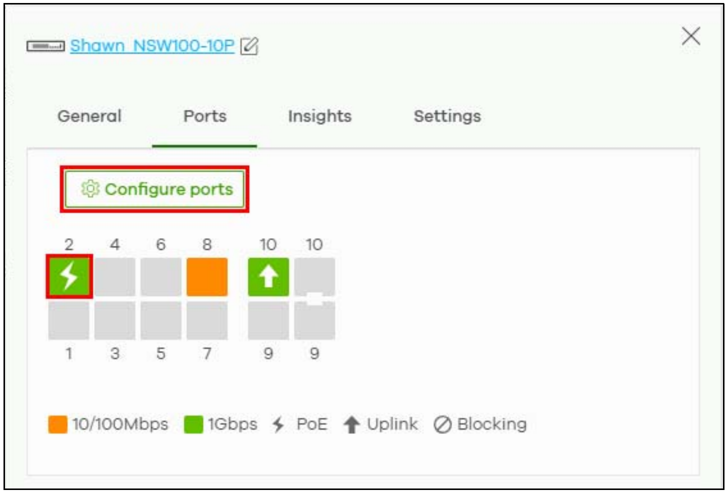
0.0% (0 W) Total: 0 W

4.2.2 Ports

Click the **Ports** tab and move the pointer over a port to view the Nebula Device's port details, such as **Name**, **Status**, **LLDP**, **Type** and **Speed**. If the port is supplying power to a node using Power over Ethernet (PoE), you can click **Power reset** to perform a power cycle on the port. This action temporarily disables PoE and then re-enables it, in order to reboot connected PoE devices. Click **LLDP** to go to the **Site-wide** > **Devices** > **Access points** > **Details** screen. See Section 4.3.1.1 on page 218 for more information. Click **Configure ports** to go to the **Site-wide** > **Devices** > (**Nebula Device**) page. See Table 21 on page 233 for more information.

Note: The **Ports** tab is not available for mobile routers and access points.

Figure 37 Site-wide > Topology > Ports

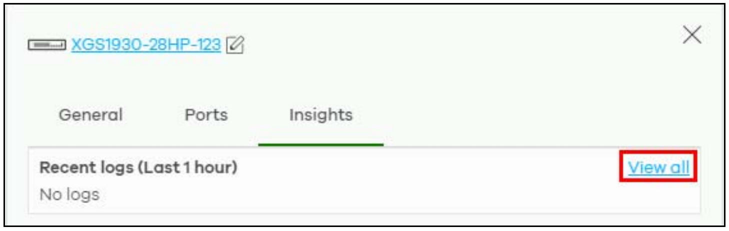


4.2.3 Insights

Click the **Insights** tab to view Nebula Device log messages for the past hour. Click **View all** to go to the **Site-wide** > **Monitor** > (Nebula Device) > **Event log** page to view more log messages. See Section 6.2.1 on page 349 for more information.

Note: The **Insights** tab is not available for mobile routers.

Figure 38 Site-wide > Topology > Insights



Recent logs (Last 1 hour)

No logs

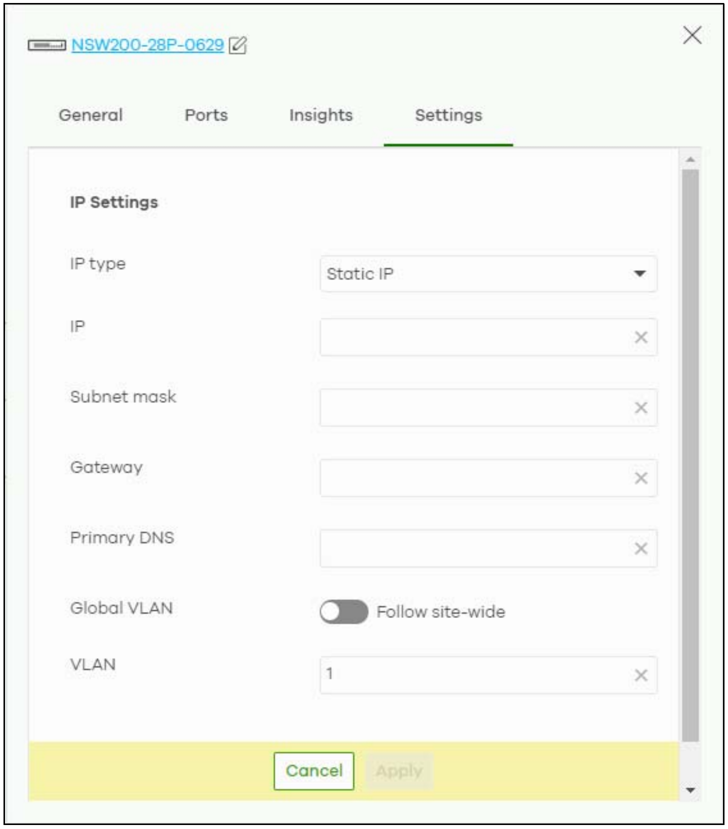
4.2.4 Settings

Click the **Settings** tab to change the IP type/address, subnet mask, gateway, primary DNS, VLAN setting. See Table 19 on page 220 for more information.

Note: The **Settings** tab is only available for Access Points and Switches.

Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.

Figure 39 Site-wide > Topology > Settings



IP Settings

IP type	Static IP
IP	
Subnet mask	
Gateway	
Primary DNS	
Global VLAN	Follow site-wide
VLAN	1

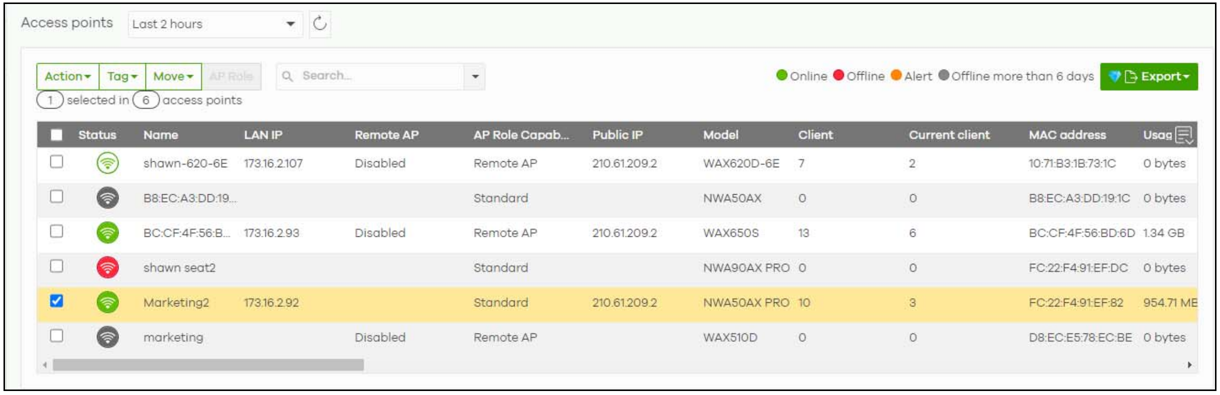
4.3 Devices

Use the **Devices** menus to check Nebula Device information, client information, event log messages and summary report for Nebula Devices in the selected site.

4.3.1 Access Points

This screen allows you to view the detailed information about a Nebula Device in the selected site. Click **Site-wide** > **Devices** > **Access points** to access this screen.

Figure 40 Site-wide > Devices > Access points



1 selected in 6 access points

☐	Status	Name	LAN IP	Remote AP	AP Role Capab...	Public IP	Model	Client	Current client	MAC address	Usag
☐		shawn-620-6E	173.16.2.107	Disabled	Remote AP	210.61.209.2	WAX620D-6E	7	2	10:71:B3:1B:73:1C	0 bytes
☐		B8:EC:A3:DD:19...			Standard		NWA50AX	0	0	B8:EC:A3:DD:19:1C	0 bytes
☐		BC:CF:4F:56:B...	173.16.2.93	Disabled	Remote AP	210.61.209.2	WAX650S	13	6	BC:CF:4F:56:BD:6D	1.34 GB
☐		shawn seat2			Standard		NWA90AX PRO	0	0	FC:22:F4:91:EF:DC	0 bytes
☑		Marketing2	173.16.2.92		Standard	210.61.209.2	NWA50AX PRO	10	3	FC:22:F4:91:EF:82	954.71 ME
☐		marketing		Disabled	Remote AP		WAX510D	0	0	D8:EC:E5:78:EC:BE	0 bytes

The following table describes the labels in this screen.

Table 18 Site-wide > Devices > Access points

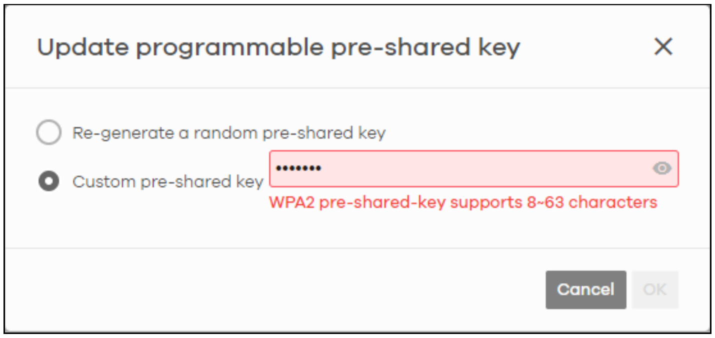
LABEL	DESCRIPTION
Access points	Select to view device information and connection status in the past 2 hours, day, week, month.
↻	Click this button to reload the data-related frames on this page.
Action	Perform an action on the selected Nebula Devices.
Reboot	Select this to restart the Nebula Device.
Upgrade	Select this to upgrade the firmware on the Nebula Device.
Change PSK	Select this to generate a random Pre-Shared Key, or use a custom Pre-Shared Key. This allows a user to access the WiFi network through the Nebula Device.  Update programmable pre-shared key ○ Re-generate a random pre-shared key ● Custom pre-shared key ••••••• WPA2 pre-shared-key supports 8~63 characters Note: **Programmable SSID** must be enabled in **Site-wide** > **Configure** > **WiFi SSID**.
Tag	Select one or multiple Nebula Devices and click this button to create a new tag for the Nebula Devices or delete an existing tag.
Move	Select one or multiple Nebula Devices and click this button to move the Nebula Devices to another site or remove the Nebula Devices from the current site.
AP Role	Select one or multiple Nebula Devices and click this button to enable or disable the **Remote AP** feature. Remote Nebula Device enables the site's Security Appliance to connect to the Nebula Device through a secure VPN tunnel. This allows you to set up VPN-enabled WiFi Nebula Devices in remote locations, such as in a branch office or at home. Clients connected to these Nebula Devices can securely access your network through the VPN tunnel. Note: Enabling Remote Nebula Device automatically enables Ethernet and wireless storm control on the Nebula Device.
Search	Specify your desired filter criteria to filter the list of Nebula Devices.
access points	This shows the number of Nebula Devices connected to the site network.
Export	Click this button to save the access point list as a CSV or XML file to your computer.
*	Click this to select all the rows in this table.
Status	This shows the status of the Nebula Device. • Green: The Nebula Device is online and has no alerts. • Amber: The Nebula Device has alerts. Hover the mouse over the icon to find the problem. • Red: The Nebula Device is offline. • Gray: The Nebula Device has been offline for 7 days or more. • 📶: The Nebula Device is acting as a repeater. For example, an alert is created and the status color is amber when the Nebula Device is transmitting data at 100 Mbps in half duplex mode or when the Nebula Device is in a **Limited Power mode**. Click the Nebula Device on this page to go to the Nebula Device's details screen for more information.

Table 18   Site-wide > Devices > Access points (continued)

LABEL	DESCRIPTION
Name	This shows the descriptive name of the Nebula Device.
LAN IP	This shows the local (LAN) IP address of the Nebula Device.
Remote AP	This shows whether the Remote Nebula Device function is **Enabled** or **Disabled**.
2.4GHz	This shows the number of WiFi clients in the 2.4 GHz band.
5GHz	This shows the number of WiFi clients in the 5 GHz band.
6GHz	This shows the number of WiFi clients in the 6 GHz band.
AP Role Capability	This displays whether the Nebula Device can act as a remote Nebula Device (**Remote AP**) or not (**Standard AP**).
Public IP	This shows the global (WAN) IP address of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Client	This shows how many clients are connected to the Nebula Device within the specified time period.
Current client	This shows how many clients are currently connecting to the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
Channel	This shows the channel ID the Nebula Device is using.
Channel Utilization 2.4GHz	This shows the percentage of the 2.4 GHz channel ID usage.
Channel Utilization 5GHz	This shows the percentage of the 5 GHz channel ID usage.
Channel Utilization 6GHz	This shows the percentage of the 6 GHz channel ID usage.
Usage	This shows the amount of data consumed by the Nebula Device's clients.
% Usage	This shows the percentage of the Nebula Device's data usage.
Description	This shows the user-specified description for the Nebula Device.
Tag	This shows the user-specified tag for the Nebula Device.
Serial number	This shows the serial number of the Nebula Device.
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
Connectivity	This shows the access point connection status. The red time slot indicates the connection to the NCC is down, and the green time slot indicates the connection is up. Move the cursor over a time slot to see the actual date and time when an Nebula Device is connected or disconnected.
Ethernet 1	This shows the speed and duplex mode of the Ethernet connection on the Nebula Device's up-link port. It shows **Down** if the Nebula Device is connected to a mesh controller wirelessly.
Neighbor Info	This shows the LLDP information received on the up-link port.
Production information	This shows the production information of the Nebula Device.
Hop	This shows the hop count of the Nebula Device. For example, "1" means the Nebula Device is connected to a mesh controller directly. "2" means there is another mesh extender between this Nebula Device and the mesh controller.
IP type	This shows whether the IP address was assigned automatically (**DHCP**), or manually (**Static IP**).

Table 18 Site-wide > Devices > Access points (continued)

LABEL	DESCRIPTION
Uplink AP	This shows the role and descriptive name of the Nebula Device to which this Nebula Device is connected wirelessly. When Smart Mesh is enabled and the mesh extender losses connection to the mesh controller, click **Reconnect** to re-establish connection. Note: Make sure to enable **Manual uplink** in **Site-wide** > **Devices** > **Access points: Details** > **Status** > **Smart mesh** > **Edit**. You also need to specify the mesh controller in **select an AP**. See Table 19 on page 220 for more information.
Uplink signal	Before the slash, this shows the signal strength the uplink Nebula Device (a mesh controller or a mesh extender) receives from this Nebula Device (in repeater mode). After the slash, this shows the signal strength this Nebula Device (in repeater mode) receives from the uplink access point.
Uplink Tx/Rx rate	This is the maximum transmission/reception rate of the mesh controller or mesh extender to which the Nebula Device is connected.
Wireless bridge	This shows whether wireless bridge is enabled on the Nebula Device. For more information about wireless bridge, see Section 5.1.2.2 on page 305.
Uplink	This shows whether the Nebula Device is connected to the gateway through a wired Ethernet connection or WiFi connection.
Power mode	This shows the Nebula Device's power status. **Full** – the Nebula Device receives power using a power adapter and/or through a PoE switch/injector using IEEE 802.3at PoE plus. The PoE device that supports IEEE 802.3at PoE Plus can supply power of up to 30W per Ethernet port. **Limited** – the Nebula Device receives power through a PoE switch/injector using IEEE 802.3af PoE even when it is also connected to a power source using a power adapter. The PoE device that supports IEEE 802.3af PoE can supply power of up to 15.4W per Ethernet port. When the Nebula Device's power mode is **Limited**, the Nebula Device throughput decreases and has just one transmitting radio chain. It always shows **Full** if the Nebula Device does not support power detection.
Firmware availability	This shows whether the firmware on the Nebula Device is **Up to date**, there is firmware update available for the Nebula Device (**Upgrade available**), or a specific version of firmware has been installed by Zyxel customer support (**Locked**).
Firmware status	This shows whether the firmware installed on the Nebula Device is up-to-date.
Firmware type	This shows **Stable** when the installed firmware may not have the latest features but has passed Zyxel internal and external testing. This shows **Latest** when the installed firmware is the most recent release with the latest features, improvements, and bug fixes. This shows **General Availability** when the installed firmware is a release before **Latest**, but is still undergoing Zyxel external testing. This shows **Dedicated** when the installed firmware is locked and Zyxel support is monitoring. Contact Zyxel customer support if you want to unlock the firmware in order to upgrade to a later one. This shows **Beta** when the installed firmware is a release version for testing the latest features and is still undergoing Zyxel internal and external testing. This shows **N/A** when the Nebula Device is offline and its firmware status is not available.
Current version	This shows the firmware version currently installed on the Nebula Device.

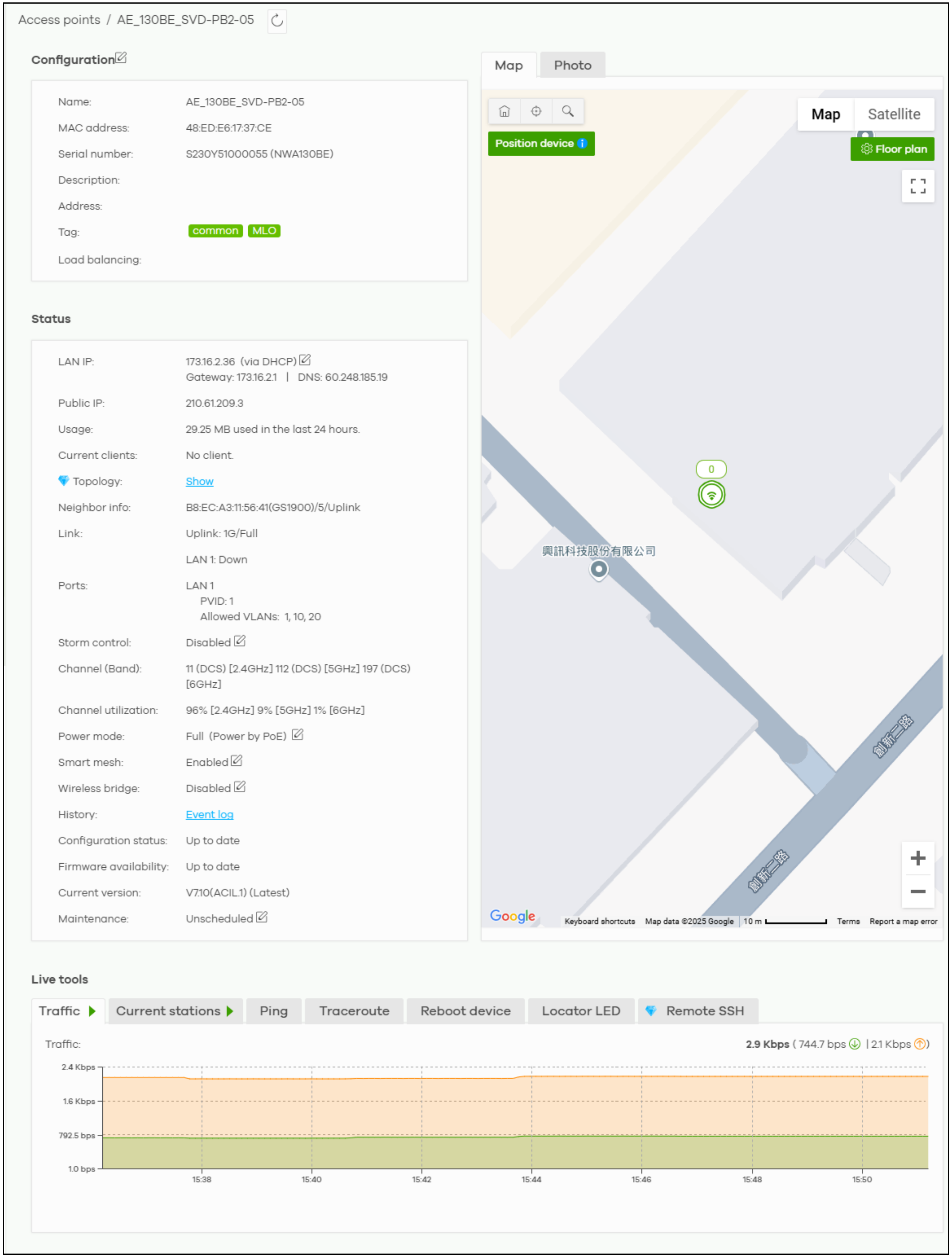
Table 18 Site-wide > Devices > Access points (continued)

LABEL	DESCRIPTION
Remote AP VPN	This shows which VPN the Remote Nebula Device tunnel is configured to use. If Remote Nebula Device is disabled, this field shows **Disconnected**.
📋	Click this icon to display a greater or lesser number of configuration fields. For faster loading of data, select only the configuration fields listed that do NOT take a long time to fetch data.

4.3.1.1 Access Point Details

Click a Nebula Device entry in the **Site-wide** > **Devices** > **Access points** screen to display individual Nebula Device statistics.

Figure 41 Site-wide > Devices > Access points: Details Part 1



Access points / AE_130BE_SVD-PB2-05

Configuration

Name:	AE_130BE_SVD-PB2-05
MAC address:	48:ED:E6:17:37:CE
Serial number:	S230Y51000055 (NWA130BE)
Description:	
Address:	
Tag:	common MLO
Load balancing:	

Status

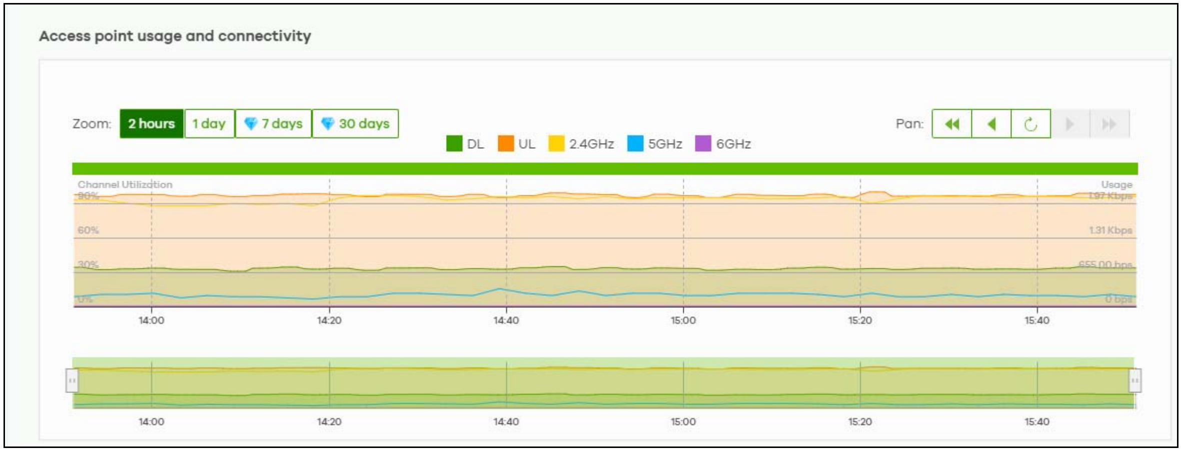
LAN IP:	173.16.2.36 (via DHCP) Gateway: 173.16.2.1 | DNS: 60.248.185.19
Public IP:	210.61.209.3
Usage:	29.25 MB used in the last 24 hours.
Current clients:	No client.
Topology:	Show
Neighbor info:	B8:EC:A3:11:56:41(GS1900)/5/Uplink
Link:	Uplink: 1G/Full
	LAN 1: Down
Ports:	LAN 1 PVID: 1 Allowed VLANs: 1, 10, 20
Storm control:	Disabled
Channel (Band):	11 (DCS) [2.4GHz] 112 (DCS) [5GHz] 197 (DCS) [6GHz]
Channel utilization:	96% [2.4GHz] 9% [5GHz] 1% [6GHz]
Power mode:	Full (Power by PoE)
Smart mesh:	Enabled
Wireless bridge:	Disabled
History:	Event log
Configuration status:	Up to date
Firmware availability:	Up to date
Current version:	V7.10(ACIL.1) (Latest)
Maintenance:	Unscheduled

Live tools

Traffic:

2.9 Kbps (744.7 bps ↓ | 2.1 Kbps ↑)

Figure 42 Site-wide > Devices > Access points: Details Part 2



The following table describes the labels in this screen.

Table 19 Site-wide > Devices > Access points: Details

<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></tr>
<tr><td>↻</td><td>Click this button to reload the data-related frames on this page.</td></tr>
<tr><td colspan="2">Configuration</td></tr>
<tr><td colspan="2">Click the edit configuration icon to change the Nebula Device name, description, tags, load balancing, and address. You can move the Nebula Device to another site or remove. You can also enter a valid <b>Address</b> and click <b>Move map marker</b> to move the Nebula Device to another location.
By default, the Nebula Device’s hostname is the MAC address. Enter a <b>Name</b> to identify the Nebula Device. You can use up to 64 alphanumeric characters including period (.) and hyphen (-). Spaces are not allowed.
Note: The period (.) and hyphen (-) cannot be the first character, last character, or appear consecutively on the <b>Name</b>. For example, -wax650, wax650-, wax650..wax650, wax650.-wax650.
The <b>Name</b> you configure here will be synchronized with the Nebula Device’s <b>System Name</b> setting when:
• The Nebula Device must have firmware version 6.60 or later
• The <b>Name</b> follows the [Hostname] or [Hostname.Domain name] format
• The domain name follows the standard DNS structure [A.B.C.D].
Then click <b>Save</b> to save your changes.</td></tr>
</table>

Table 19 Site-wide > Devices > Access points: Details (continued)

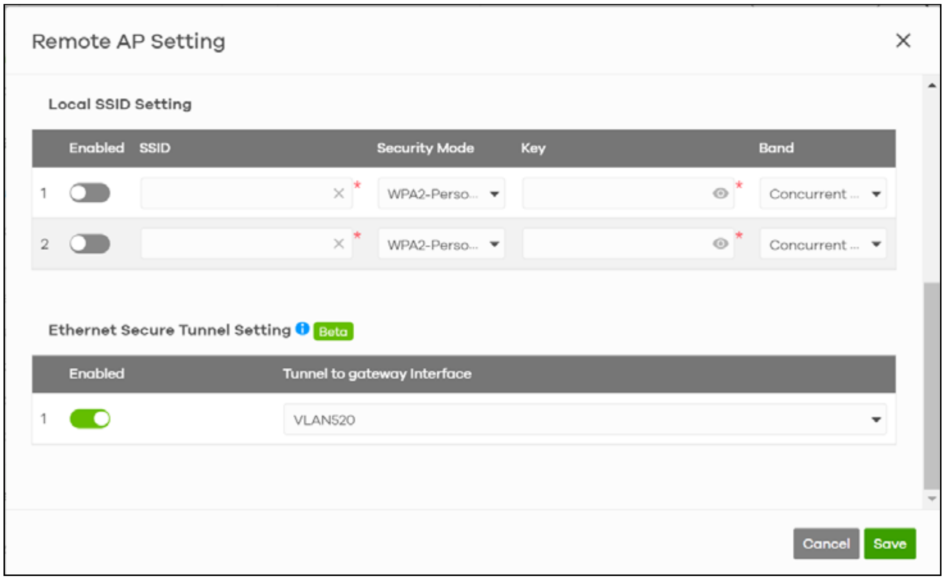
LABEL	DESCRIPTION
Remote AP	Click this to enable or disable the **Remote AP** feature. **Remote AP** enables the site's Security Appliance to connect to the Nebula Device through a secure VPN tunnel. This allows you to set up VPN-enabled WiFi Nebula Devices in remote locations, such as in a branch office or at home. Clients connected to these Nebula Devices can securely access your network through the VPN tunnel. With the **Remote AP** feature (in the Secure WiFi license) the connection is from the Nebula Device to a managed access point using NVGRE (Network Virtualization using Generic Routing Encapsulation) over IPSec tunnel. This encapsulates and encrypts traffic from the remote access point to the Nebula Device. The clients connected to the remote access point do not need IPSec client software installed. Note: Enabling **Remote AP** automatically enables Ethernet and wireless storm control on the Nebula Device. At the time of writing, **Ethernet Secure Tunnel Setting** for **Remote AP Setting** is available for WAC500H only.  Remote AP Setting Local SSID Setting Enabled | SSID | Security Mode | Key | Band 1 | ○ | | WPA2-Perso... | | Concurrent ... 2 | ○ | | WPA2-Perso... | | Concurrent ... Ethernet Secure Tunnel Setting Beta Enabled | Tunnel to gateway Interface 1 | ● | VLAN520 Cancel Save Configure and enable up to two **SSID**(s) in **Local SSID Setting**. WiFi clients connected to these SSIDs are forwarded to the local network of the remote site. The **Local SSID Setting** are different from the SSIDs you configured in **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**. See Section 5.3.2 on page 320 for the description of the fields. Select from the available LAN or VLAN interface in **Tunnel to gateway interface** to enable it, and click **Save**.
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
Serial number	This shows the serial number of the Nebula Device.
Change site	Select the new site from the drop-down menu or click **Remove** to remove the Nebula Device from the site.
Description	This shows the user-specified description for the Nebula Device.
Tags	This shows the user-specified tag for the Nebula Device.
Load balancing	This shows the load balancing group name that the Nebula Device belongs (up to two groups per access point). Nebula Devices in the same group should be within the proximity. This allows them to share the load.

Table 19 Site-wide > Devices > Access points: Details (continued)

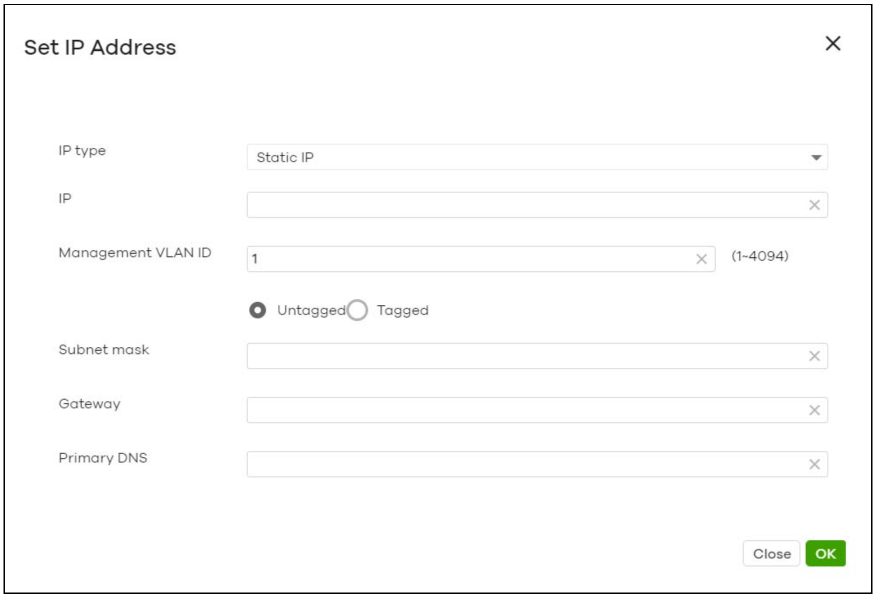
LABEL	DESCRIPTION
Address	This shows the user-specified address for the Nebula Device.
Status	
LAN IP	This shows the local (LAN) IP address of the Nebula Device. It also shows the IP addresses of the gateway and DNS server. Click the edit icon to open a screen where you can change the IP addresses, VLAN ID number and tagging setting.  Set IP Address IP type: Static IP IP: Management VLAN ID: 1 (1~4094) ● Untagged ○ Tagged Subnet mask: Gateway: Primary DNS: Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
Public IP	This shows the global (WAN) IP address of the Nebula Device.
Usage	This shows the amount of data consumed by the clients.
Current clients	This shows the number of clients which are currently connecting to the Nebula Device and its details.
Topology	Click **Show** to go to the **Site-wide** > **Topology** screen. See Section 4.2 on page 208.
Neighbor info	This shows the LLDP information received on the up-link port.
Link	This shows the speed and duplex mode of the Ethernet connection on the Nebula Device's ports. It shows **Uplink: Wireless** if the access point is an mesh extender and connected to a mesh controller wirelessly. A warning icon displays when the Nebula Device is running at 100 Mbps or a lower speed.
Ports	This is available only for the Nebula Device that has one or more than one Ethernet LAN port (except the uplink port). This shows the PVID of the LAN port and the ID number of VLANs to which the LAN port belongs. See Section 5.3.7 on page 344 for how to change the port's VLAN settings.
Storm control	Storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets received per second on the Nebula Device's Ethernet ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enabling this feature reduces broadcast, multicast and/or DLF packets in your network.

Table 19 Site-wide > Devices > Access points: Details (continued)

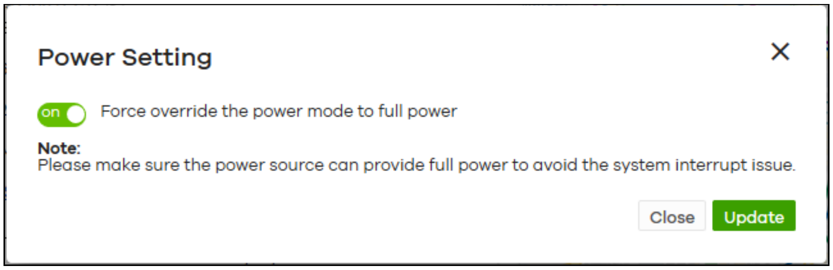
LABEL	DESCRIPTION
Channel (Band)	This shows the channel ID and WiFi frequency band currently being used by the Nebula Device.
Channel utilization	This shows the percentage of the channel ID usage.
Power mode	This shows **Full** when the Nebula Device receives power directly through a power outlet. This shows **Full (Power by DC)** when the Nebula Device receives power using a power adapter. This shows **Full (Power by PoE)** when the Nebula Device receives power through a PoE switch/injector using IEEE 802.3at PoE plus. The PoE device that supports IEEE 802.3at PoE Plus can supply power of up to 30W per Ethernet port. This shows **Limited (Require 802.3bt power)** when the Nebula Device receives power through a PoE switch/injector using IEEE 802.3bt PoE even when it is also connected to a power source using a power adapter. The PoE device that supports IEEE 802.3bt PoE can supply power of up to 71.3W per Ethernet port. This shows **Limited (Require 802.3at power)** when the Nebula Device receives power through a PoE switch/injector using IEEE 802.3at PoE even when it is also connected to a power source using a power adapter. The PoE device that supports IEEE 802.3at PoE can supply power of up to 15.4W per Ethernet port. This field is blank when the access point's firmware is older than version 5.50 or (WAX650S / WAX510D firmware is older than version 6.00P4C0). Or when the access point is offline. Click the edit icon to open a screen where you can enable full power mode.  Power Setting on Force override the power mode to full power Note: Please make sure the power source can provide full power to avoid the system interrupt issue. Note: As of this writing, the following is a list of models that will show the edit icon for enabling full power mode: NAP303, NAP353, NWA1302-AC, NWA1123-AC HD, NWA5123-AC HD, WAC6303D-S, WAC6502D-E, WAC6502D-S, WAC6503D-S, WAC6552D-S, WAC6553D-S, WAX650S, NWA110AX, WAX510D.
Antenna	This displays the antenna orientation settings for the Nebula Device that comes with internal antennas and also has an antenna switch.
Smart mesh	This shows whether Nebula Smart Mesh is enabled on the Nebula Device. For more information about Smart Mesh, see Section 5.1.1 on page 303. To view the list of Nebula Devices that support smart mesh, go to **Help** > **Device function table**.

Table 19 Site-wide > Devices > Access points: Details (continued)

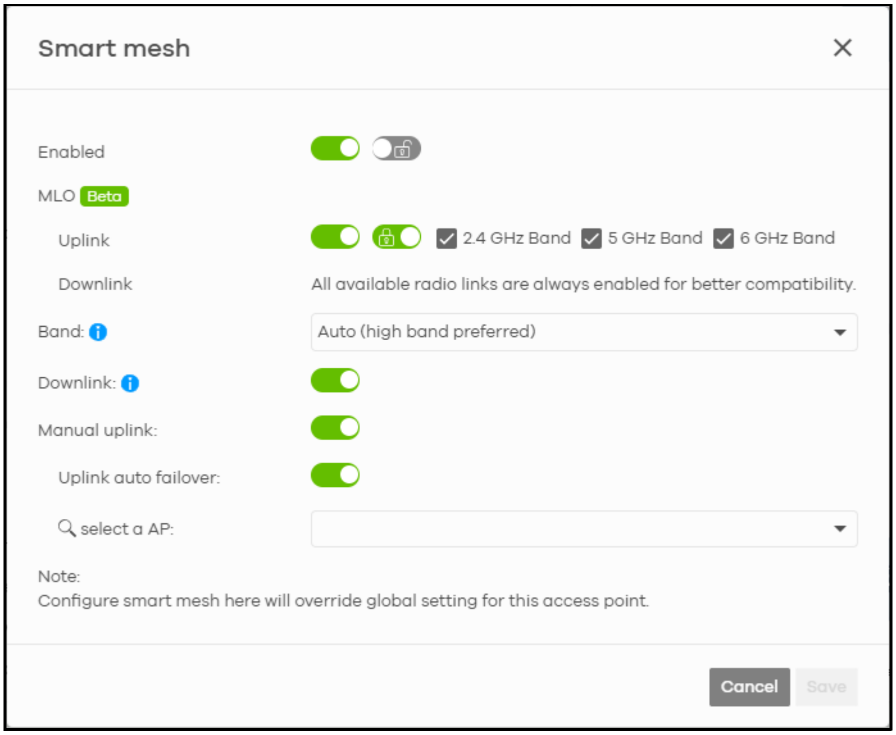
LABEL	DESCRIPTION
Edit	Edit the Nebula Device's Smart Mesh settings.  Smart mesh Enabled MLO Beta Uplink ☑ 2.4 GHz Band ☑ 5 GHz Band ☑ 6 GHz Band Downlink All available radio links are always enabled for better compatibility. Band: Auto (high band preferred) Downlink: Manual uplink: Uplink auto failover: select a AP: Note: Configure smart mesh here will override global setting for this access point. Cancel Save
Enabled	Enable or disable Smart Mesh on the Nebula Device. This setting overrides the Smart Mesh settings configured for the Nebula Device's site in NCC.
Lock	When enabled, the Nebula Device's local Smart Mesh settings overrides the Smart Mesh settings configured for the Nebula Device's site in NCC. Example 1: If Smart Mesh is enabled for the site in NCC, you can disable Smart Mesh on the Nebula Device by setting **Lock** to on and **Enabled** to off. Example 2: If Smart Mesh is disabled for the site in NCC, you can enable Smart Mesh on the Nebula Device by setting **Lock** to on and **Enabled** to on.
MLO Uplink Downlink	Select **MLO** (Multi-Link Operation) to allow a WiFi7 client to connect to the WiFi7 Nebula Device using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi7 ideal for streaming 4K / 8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Note: You need to select at least 2 frequency bands for MLO to work.
Band	This setting will apply to mesh extender. • Select **Auto (high band preferred)** to allow the mesh extender to select a higher radio band mesh controller. • Select **2.4 GHz** to use the 2.4 GHz band for regular Internet surfing and downloading. • Select **5 GHz** or **6 GHz** to use the 5 or 6 GHz band for time sensitive traffic like high-definition video, music, and gaming. Note: **6 GHz** will display only for mesh extender that support it.
Downlink	When enabled, the mesh extender can provide downlink capability to another mesh extender.
Manual uplink	When enabled, this allows you to select a mesh controller or mesh extender.

Table 19 Site-wide > Devices > Access points: Details (continued)

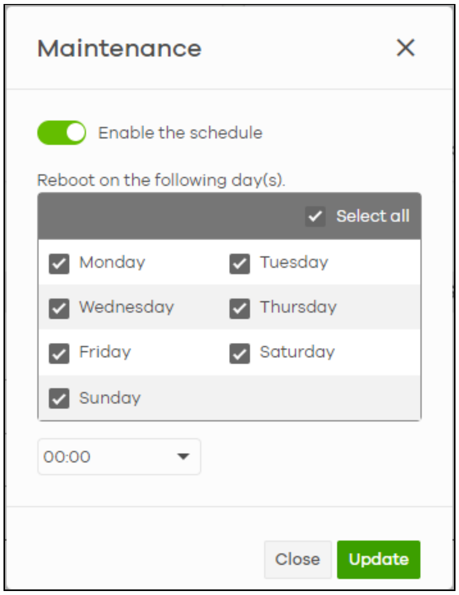
LABEL	DESCRIPTION
Uplink auto failover	When enabled, an mesh extender that cannot connect to the selected mesh controller after 5 tries, will automatically connect to another mesh controller or mesh extender.
select an AP	Select a mesh controller or mesh extender.
Wireless bridge	This shows whether wireless bridge is enabled on the Nebula Device. For more information about wireless bridge, see Section 5.1.2.2 on page 305. Note: Wireless bridge can only work when smart mesh is enabled in this screen.
Edit	Edit the Nebula Device's wireless bridge settings.
Enabled	Enable or disable wireless bridge on the Nebula Device. Note: If Smart Mesh is disabled for the site in NCC, then enabling wireless bridge automatically enables Smart Mesh on the Nebula Device.
Allowed VLANs	Enter the IDs of the VLANs that the Nebula Device will forward over the wireless bridge. By default, this field uses the VLANs allowed for LAN1 at **Site-wide** > **Configure** > **Access points** > **AP & port settings**. For details, see Section 5.3.7 on page 344.
History	Click **Event log** to go to the **Site-wide** > **Monitor** > **Access points** > **Event log** screen.
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
Firmware availability	This shows whether the firmware on the Nebula Device is up-to-date or there is firmware update available for the Nebula Device.
Current version	This shows the firmware version currently installed on the Nebula Device.
Maintenance	This shows whether automatic reboot is scheduled on the Nebula Device.
Edit	Click the **Enable the schedule** switch to the right to have the Nebula Device restart at a specific time on selected days of the week. By scheduling a reboot, you can have the Nebula Device refresh the network connections at a specified time, allowing automatic reconnection with WiFi clients in case of a connection failure. Select the day(s) of the week to have the automatic restart. Specify the time of the day (in 24-hour format) to have the Nebula Device automatically restart. For example, 23:00 is 11:00 PM.  Maintenance Enable the schedule Reboot on the following day(s). ☑ Select all ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday 00:00 Close Update

Table 19 Site-wide > Devices > Access points: Details (continued)

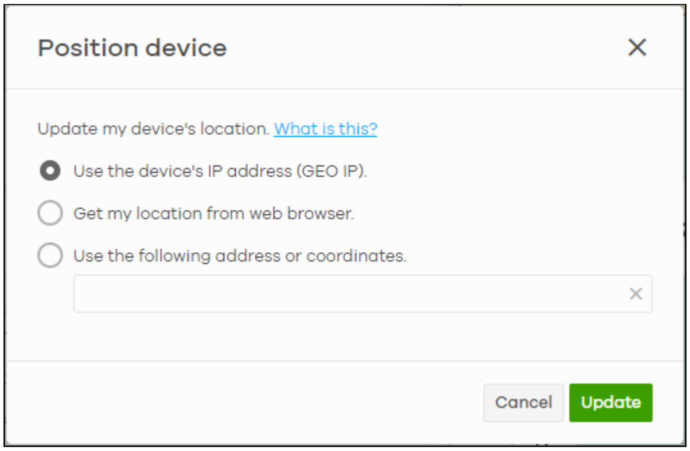
LABEL	DESCRIPTION
Map	This shows the location of the Nebula Device on Google map (**Map** view or **Satellite** imagery view) or on a floor plan. Click **Floor plan** to display a list of existing floor plans. Each floor plan has a drawing that shows the rooms scaled and viewed from above. Drag-and-drop your Nebula Device directly on the Google map or click **Position device** to update the Nebula Device's address (physical location).  Position device × Update my device's location. What is this? ● Use the device's IP address (GEO IP). ○ Get my location from web browser. ○ Use the following address or coordinates. Cancel Update - Select **GEO IP** to use the public IP address of the Nebula Device. - Select **Get my location from web browser** to use the public IP address of the computer accessing the NCC portal. - Select **Use the following address or coordinates** to enter the complete address or coordinates of the Nebula Device. Note: Nebula Devices that are offline cannot use GEO IP.
Photo	This shows the photo of the Nebula Device. Click **Add** to upload one or more photos. Click **x** to remove a photo.
Live tools	
Traffic	This shows the Nebula Device traffic statistics.
Current stations	This shows the Nebula Device's connected WiFi clients' **MAC address**, **SSID name**, **IPv4 Address**, **Signal strength**, **Security**, **Channel**, **Tx rate**, **Rx rate**, **Association time**, and **Capability**.
Ping	Enter the domain name or IP address of a computer that you want to perform ping from the Nebula Device in order to test a connection and click **Ping**. This can be used to determine if the Nebula Device and the computer are able to communicate with each other.
Traceroute	Enter the domain name or IP address of a computer that you want to perform traceroute from the Nebula Device and click **Run**. This determines the path a packet takes to the specified computer.
Reboot device	Click the **Reboot** button to restart the Nebula Device. Note: All connected clients will be temporarily disconnected during reboot.
Locator LED	Enter a time interval between 1 and 60 minutes. The locator LED will blink for the number of minutes set here once you turn on the locator LED. Click the ▶ button to turn on the locator feature, which shows the actual location of the Nebula Device between several devices in the network.
Remote SSH	This allows you to establish a remote connection to this Nebula Device by specifying the port number. Then click **Establish**. This feature is available to the organization owner, organization administrators with full privileges, and site administrators with full privileges.

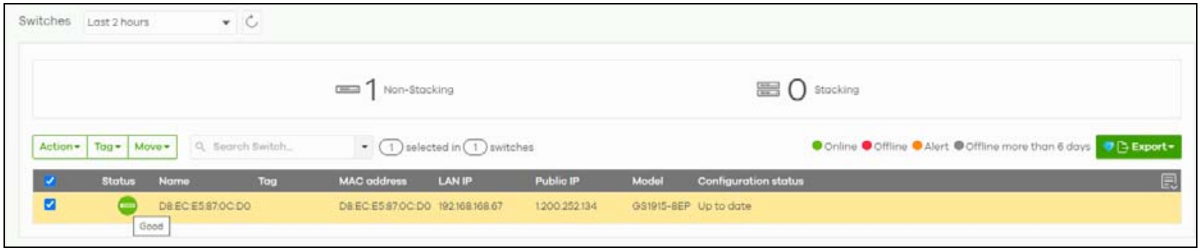
Table 19 Site-wide > Devices > Access points: Details (continued)

LABEL	DESCRIPTION
Wired stations	This shows the Nebula Device's connected wired clients' **MAC address**, **IPv4 Address**, **Port** number, and the **VLAN** ID assigned to the wired station. Note: At the time of writing **Wired stations** is available for WAC500H only.
Access point usage and connectivity Move the cursor over the chart to see the transmission rate at a specific time. Click **DL** (downlink), **UL** (uplink), **2.4GHz**, **5GHz**, or **6GHz** to hide or display the corresponding line on the chart below.	
Zoom	Select to view the statistics in the past 2 hours, day, week, or month.
Pan	Click to move backward or forward by one day or week.

4.3.2 Switches

This screen allows you to view the detailed information about a Nebula Device in the selected site. Click **Site-wide** > **Devices** > **Switches** to access this screen.

Figure 43 Site-wide > Devices > Switches



☑	Status	Name	Tag	MAC address	LAN IP	Public IP	Model	Configuration status
☑	●	D8:EC:E5:87:0C:D0		D8:EC:E5:87:0C:D0	192.168.168.67	1.200.252.134	GS1915-8EP	Up to date

The following table describes the labels in this screen.

Table 20 Site-wide > Devices > Switches

LABEL	DESCRIPTION
Switches	Select to view the Nebula Device information and connection status in the past two hours, day, week or month.
↻	Click this button to reload the data-related frames on this page.
Action	Perform an action on the selected Nebula Devices.
Reboot	Restart the Nebula Device.
Upgrade	Upgrade the firmware on the Nebula Device.
Tag	Select one or multiple Nebula Devices and click this button to create a new tag for the Nebula Devices or delete an existing tag.
Move	Select one or multiple Nebula Devices and click this button to move the Nebula Device to another site or remove the Nebula Device from the current site.
Search	Specify your desired filter criteria to filter the list of Nebula Devices.
Switch	This shows the number of Nebula Devices connected to the site network.
Export	Click this button to save the Nebula Device list as a CSV or XML file to your computer.

Table 20 Site-wide > Devices > Switches (continued)

LABEL	DESCRIPTION
Status	This shows the status of the Nebula Device. Hover the mouse over the icon for a brief description. • Green: The Nebula Device is online and has no alerts. • Amber: The Nebula Device has alerts. • Red: The Nebula Device is offline. • Gray: The Nebula Device has been offline for 7 days or more. • With lock: The Nebula Device is locked by Auto Configuration Recovery. See Table 86 on page 412 for more information. Move the cursor over an amber alert icon to view the alerts the NCC generates when an error or something abnormal is detected on the IPTV network.
Name	This shows the descriptive name of the Nebula Device.
Tag	This shows the user-specified tag for the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device. In Cloud Stacking mode, this shows the MAC address of the master Nebula Device in the stacking system.
LAN IP	This shows the local (LAN) IP address of the Nebula Device.
Public IP	This shows the global (WAN) IP address of the Nebula Device.
Model	This shows the model number of the Nebula Device.
# Port	This shows the number of the Nebula Device port which is connected to the NCC.
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
Bandwidth Utilization (Uplink port)	This shows what percentage of the upstream/downstream bandwidth is currently being used by the Nebula Device's uplink port.
Production information	This shows the Nebula Device's product description to explain what this Nebula Device is and also provides information about its features.
Connectivity	This shows the Nebula Device connection status. Nothing displays if the Nebula Device is offline. The gray time slot indicates the connection to the NCC is down, and the green time slot indicates the connection is up. Move the cursor over a time slot to see the actual date and time when a Nebula Device is connected or disconnected.
Description	This shows the user-specified description for the Nebula Device.
Device mode	This shows **Non-Stacking** when the Nebula Device is not a member of a stacking system. This shows **Stacking** when the Nebula Device is a member of a stacking system.
Serial number	This shows the serial number of the Nebula Device.
Firmware status	This shows whether the firmware installed on the Nebula Device is up-to-date.
Firmware type	This shows **Stable** when the installed firmware may not have the latest features but has passed Zyxel internal and external testing. This shows **Latest** when the installed firmware is the most recent release with the latest features, improvements, and bug fixes. This shows **General Availability** when the installed firmware is a release before **Latest**, but is still undergoing Zyxel external testing. This shows **Dedicated** when the installed firmware is locked and Zyxel support is monitoring. Contact Zyxel customer support if you want to unlock the firmware in order to upgrade to a later one. This shows **Beta** when the installed firmware is a release version for testing the latest features and is still undergoing Zyxel internal and external testing. This shows **N/A** when the Nebula Device is offline and its firmware status is not available.

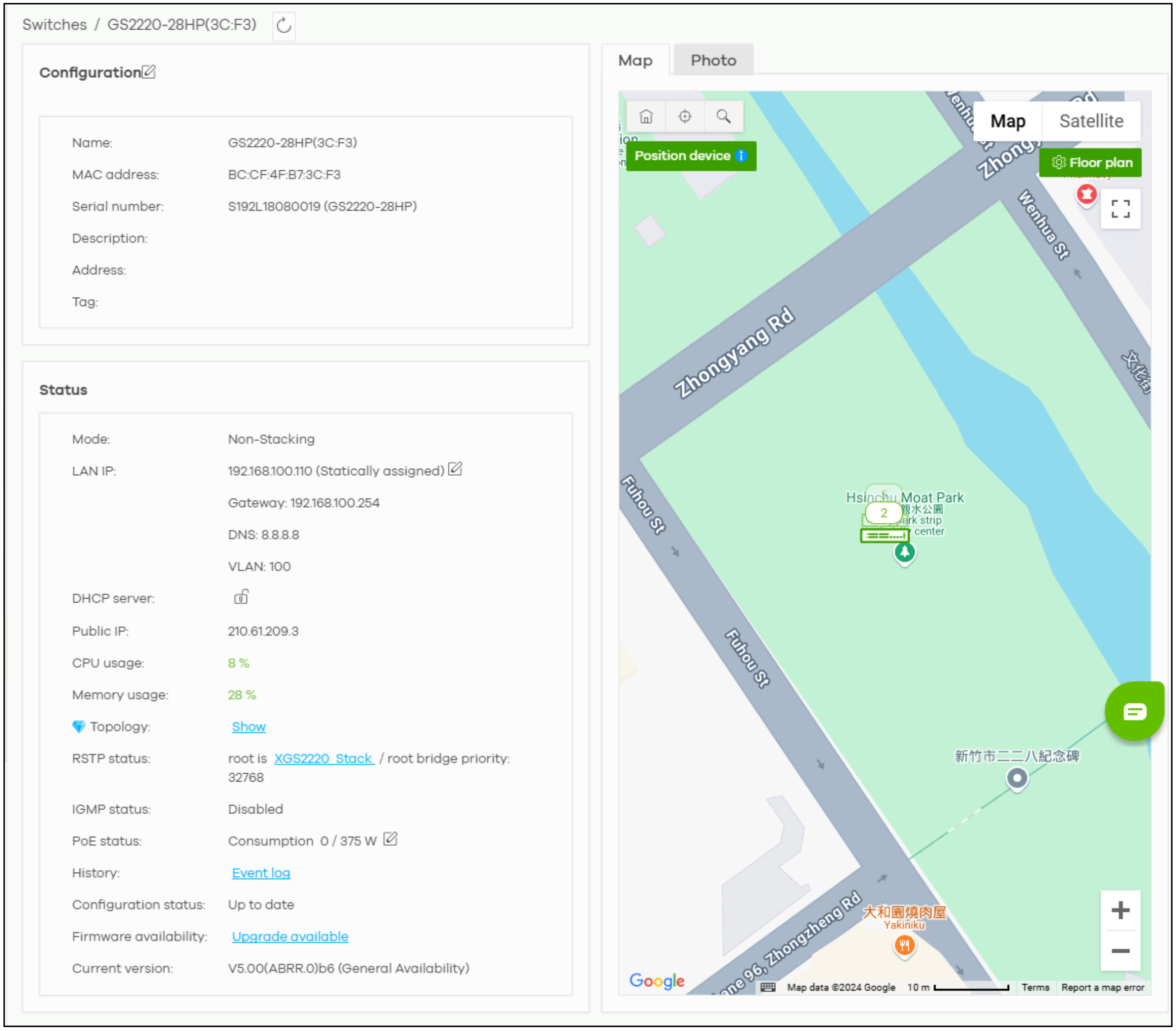
Table 20   Site-wide > Devices > Switches (continued)

LABEL	DESCRIPTION
Firmware availability	This shows whether the firmware on the Nebula Device is **Up to date**, there is firmware update available for the Nebula Device (**Upgrade available**), or a specific version of firmware has been installed by Zyxel customer support (**Locked**).
Current version	This shows the firmware version currently installed on the Nebula Device.
Usage	This shows the amount of data transmitted or received by the Nebula Device's clients.
IP type	This shows whether the IP address was assigned automatically (**DHCP**), or manually (**Static IP**).
☰	Click this icon to display a greater or lesser number of configuration fields. For faster loading of data, select only the configuration fields listed that do NOT take a long time to fetch data.

4.3.2.1 Switch Details

Click a Nebula Device entry in the **Site-wide** > **Devices** > **Switches** screen to display individual Nebula Device statistics.

Figure 44   Site-wide > Devices > Switches: Switch Details (Without Stacking)



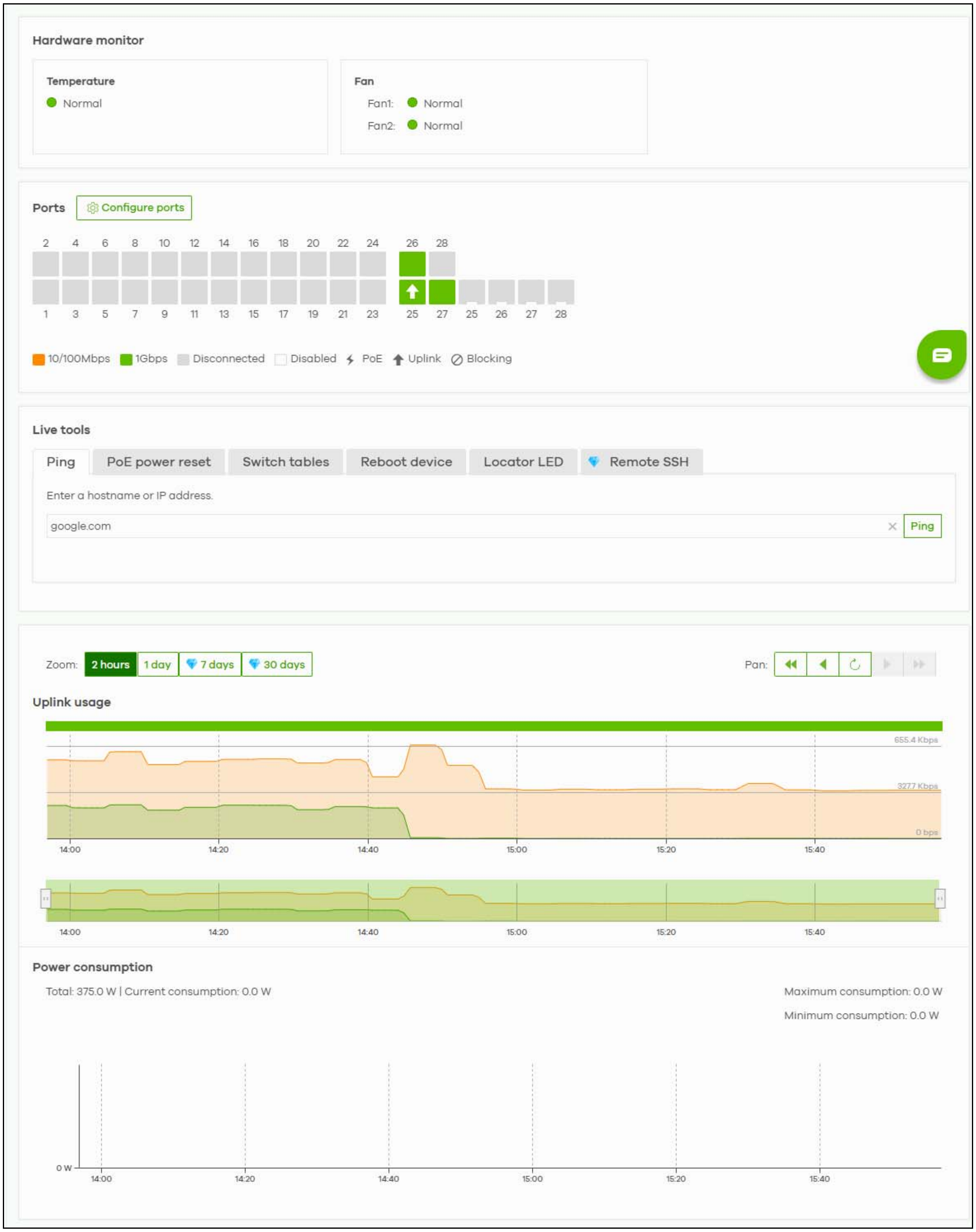
Switches / GS2220-28HP(3C:F3)

Configuration

Name: GS2220-28HP(3C:F3)
MAC address: BC:CF:4F:B7:3C:F3
Serial number: S192L18080019 (GS2220-28HP)
Description:
Address:
Tag:

Status

Mode: Non-Stacking
LAN IP: 192.168.100.110 (Statically assigned)
Gateway: 192.168.100.254
DNS: 8.8.8.8
VLAN: 100
DHCP server:
Public IP: 210.61.209.3
CPU usage: 8 %
Memory usage: 28 %
Topology: Show
RSTP status: root is XGS2220_Stack / root bridge priority: 32768
IGMP status: Disabled
PoE status: Consumption 0 / 375 W
History: Event log
Configuration status: Up to date
Firmware availability: Upgrade available
Current version: V5.00(ABRR.0)b6 (General Availability)



Enter a hostname or IP address.

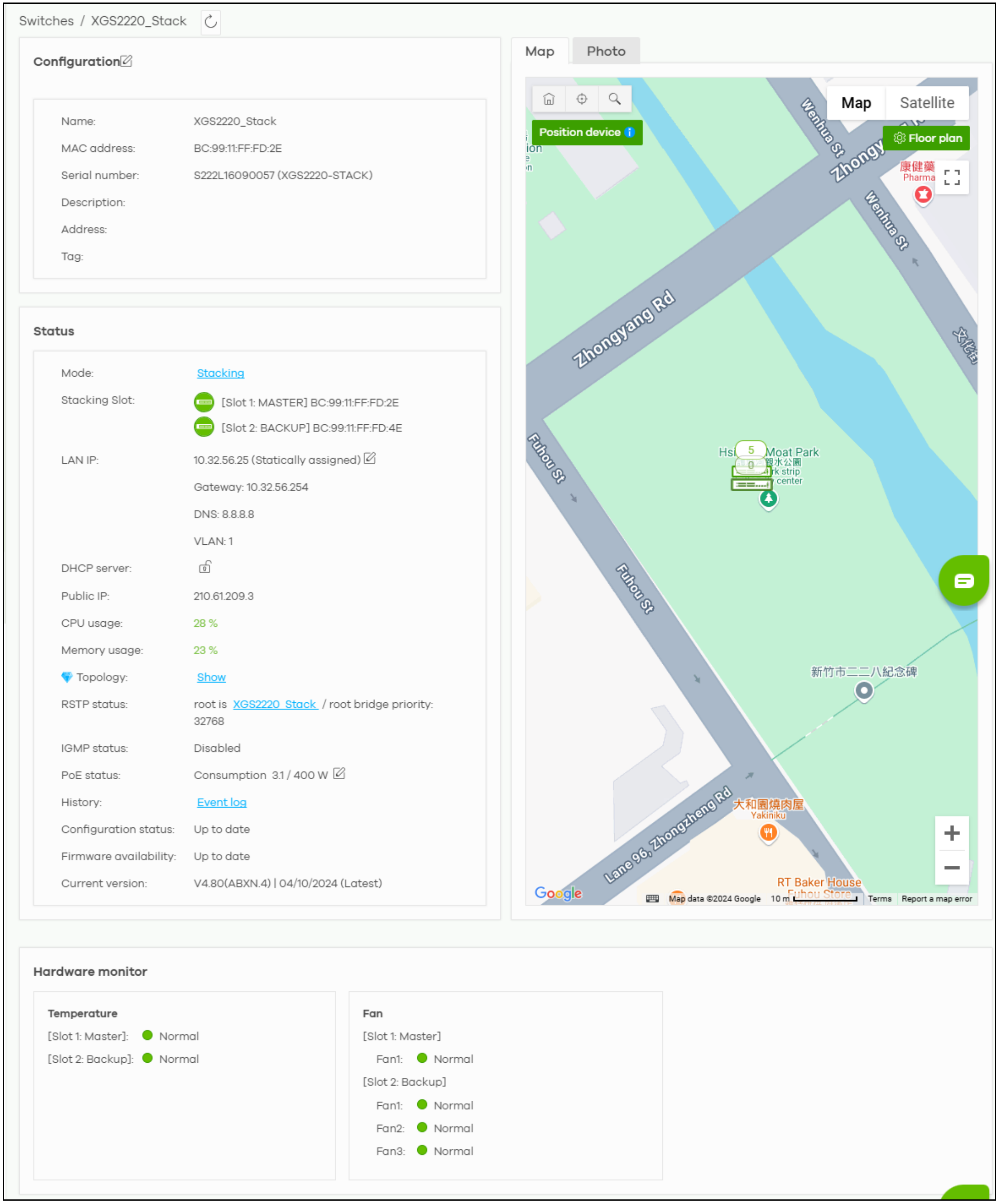
google.com

Total: 375.0 W | Current consumption: 0.0 W

Maximum consumption: 0.0 W

Minimum consumption: 0.0 W

Figure 45 Site-wide > Devices > Switches: Switch Details (With Stacking)



Switches / XGS2220_Stack

Configuration

Name: XGS2220_Stack

MAC address: BC:99:11:FF:FD:2E

Serial number: S222L16090057 (XGS2220-STACK)

Description:

Address:

Tag:

Status

Mode: Stacking

Stacking Slot: [Slot 1: MASTER] BC:99:11:FF:FD:2E

[Slot 2: BACKUP] BC:99:11:FF:FD:4E

LAN IP: 10.32.56.25 (Statically assigned)

Gateway: 10.32.56.254

DNS: 8.8.8.8

VLAN: 1

DHCP server:

Public IP: 210.61.209.3

CPU usage: 28 %

Memory usage: 23 %

Topology: Show

RSTP status: root is XGS2220_Stack / root bridge priority: 32768

IGMP status: Disabled

PoE status: Consumption 3.1 / 400 W

History: Event log

Configuration status: Up to date

Firmware availability: Up to date

Current version: V4.80(ABXN.4) | 04/10/2024 (Latest)

Hardware monitor

Temperature

[Slot 1: Master]: ● Normal

[Slot 2: Backup]: ● Normal

Fan

[Slot 1: Master]

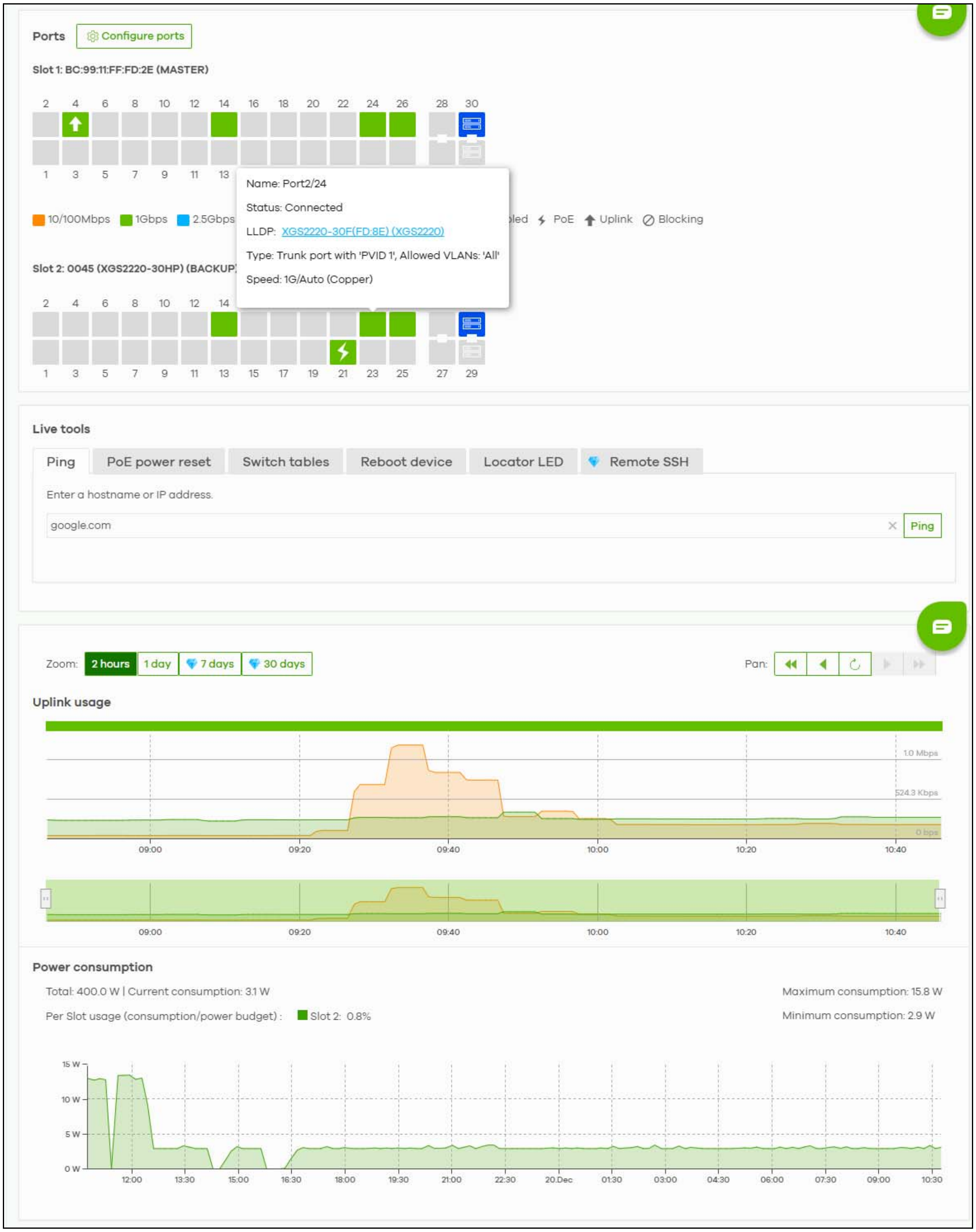
Fan1: ● Normal

[Slot 2: Backup]

Fan1: ● Normal

Fan2: ● Normal

Fan3: ● Normal



Ports ⚙ Configure ports

Slot 1: BC:99:11:FF:FD:2E (MASTER)

Name: Port2/24

Status: Connected

LLDP: XGS2220-30F(FD:8E) (XGS2220)

Type: Trunk port with 'PVID 1', Allowed VLANs: 'All'

Speed: 1G/Auto (Copper)

🟧 10/100Mbps 🟩 1Gbps 🟦 2.5Gbps ...bled ⚡ PoE ⬆ Uplink ⊘ Blocking

Slot 2: 0045 (XGS2220-30HP) (BACKUP)

Live tools

Ping | PoE power reset | Switch tables | Reboot device | Locator LED | 💎 Remote SSH

Enter a hostname or IP address.

google.com ✕ Ping

Zoom: 2 hours | 1 day | 💎 7 days | 💎 30 days   Pan:

Uplink usage

Power consumption

Total: 400.0 W | Current consumption: 3.1 W

Per Slot usage (consumption/power budget) : 🟩 Slot 2: 0.8%

Maximum consumption: 15.8 W

Minimum consumption: 2.9 W

Note: The banner **This switch is currently protected by Auto Configuration Recovery** will display when this Nebula Device is locked by NCC. Click the **Unlock** button to continue using the Nebula Device.

The following table describes the labels in this screen.

Table 21 Site-wide > Devices > Switches: Switch Details

LABEL	DESCRIPTION
↻	Click this button to reload the data-related frames on this page.
Unlock	This button only appears when the Nebula Device is locked by NCC. Click this button to continue using the Nebula Device.
Configuration Click the edit icon to change the Nebula Device name, description, tags and address. You can also move the Nebula Device to another site. After modifying a Nebula Device name, the new name will be synchronized to the Nebula Device and can be seen by protocols such as SNMP and LLDP.	
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device. In stacking mode, this shows the MAC address of the master Nebula Device in the stacking system.
Serial number	This shows the serial number of the Nebula Device.
Description	This shows the user-specified description for the Nebula Device.
Address	This shows the user-specified address for the Nebula Device.
Tag	This shows the user-specified tag for the Nebula Device.
Status	
Mode	This shows if the Nebula Device is in **Stacking** or **Non-Stacking** mode.
Stacking Slot	This shows the following information of the stacked Nebula Device: • Slot ID, • Role of the stacked Nebula Device; **MASTER**, **BACKUP** or **LINECARD**, and • MAC address.

Table 21 Site-wide > Devices > Switches: Switch Details (continued)

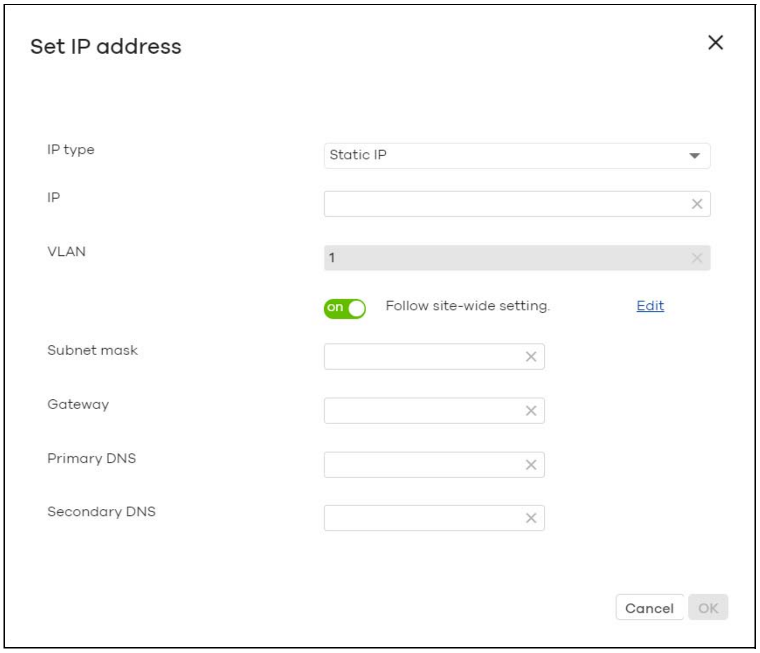
LABEL	DESCRIPTION
LAN IP	This shows the local (LAN) IP address of the Nebula Device. It also shows the IP addresses of the gateway and DNS servers. Click **Edit** to open a screen where you can change the IP address, VLAN ID number and DNS server settings.  Set IP address IP type: Static IP IP: VLAN: 1 on Follow site-wide setting. Edit Subnet mask: Gateway: Primary DNS: Secondary DNS: Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
DHCP server	This shows the IP address of the DHCP server.
Public IP	This shows the global (WAN) IP address of the Nebula Device.
CPU usage	This shows what percentage of the Nebula Device's processing capability is currently being used.
Memory usage	This shows what percentage of the Nebula Device's RAM is currently being used.
Topology	Click **Show** to go to the **Site-wide** > **Topology** screen. See Section 4.2 on page 208.
RSTP status	This shows **Disabled** when RSTP is disabled on the Nebula Device. Otherwise, it shows the name or MAC address of the Nebula Device that is the root bridge of the spanning tree, and the bridge priority.
IGMP status	This shows whether IGMP is enabled on the Nebula Device. If IGMP is enabled, it also shows the ID number of the VLAN on which the Nebula Device learns the multicast group membership and the IP address of the Nebula Device interface in IGMP querier mode.
PoE status	This shows the power management mode, the amount of power the Nebula Device is currently supplying to the connected PoE-enabled devices over the total power the Nebula Device can provide to the connected PoE-enabled devices on the PoE ports. **N/A** displays if the Nebula Device does not support PoE. In Cloud Stacking mode, this shows the total amount of power all the Nebula Devices in the stacking system are currently supplying to the connected PoE-enabled devices over the total power all the Nebula Devices in the stacking system can provide to the connected PoE-enabled devices on the PoE ports. Click the edit icon to open the **PoE Configuration** screen. See Section 4.3.2.2 on page 238.
History	Click **Event log** to go to the **Site-wide** > **Monitor** > **Switches** > **Event log** screen.

Table 21 Site-wide > Devices > Switches: Switch Details (continued)

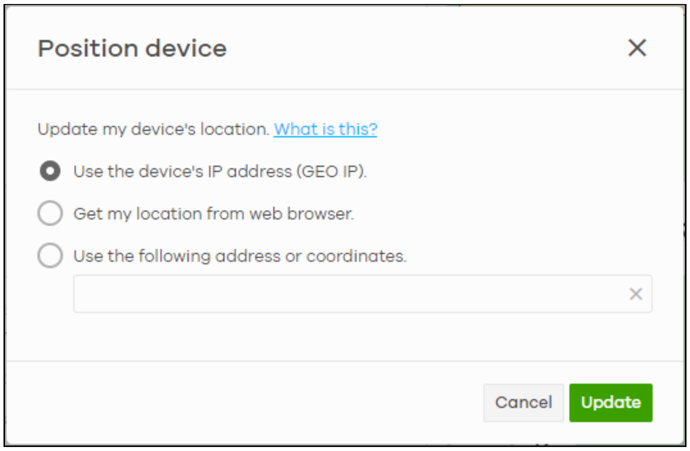
LABEL	DESCRIPTION
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
Firmware availability	This shows whether the firmware on the Nebula Device is up-to-date or there is firmware update available for the Nebula Device.
Current version	This shows the firmware version currently installed on the Nebula Device.
Map	This shows the location of the Nebula Device on Google map (**Map** view or **Satellite** imagery view) or on a floor plan. Click **Floor plan** to display a list of existing floor plans. Each floor plan has a drawing that shows the rooms scaled and viewed from above. Drag-and-drop your Nebula Device directly on the Google map or click **Position device** to update the Nebula Device's address (physical location).  Position device Update my device's location. What is this? ● Use the device's IP address (GEO IP). ○ Get my location from web browser. ○ Use the following address or coordinates. • Select **GEO IP** to use the public IP address of the Nebula Device. • Select **Get my location from web browser** to use the public IP address of the computer accessing the NCC portal. • Select **Use the following address or coordinates** to enter the complete address or coordinates of the Nebula Device. Note: Nebula Devices that are offline cannot use GEO IP.
Photo	This shows the photo of the Nebula Device. Click **Add** to upload one or more photos. Click **x** to remove a photo.
Hardware monitor	
Temperature	The Nebula Device has temperature sensors (BOARD / PHY / CPU/MAC) that are capable of detecting and reporting if the temperature rises above the threshold. BOARD / PHY / CPU/MAC refers to the location of the temperature sensor on the Switch printed circuit board. This field displays **Normal** for temperatures below the threshold and **Abnormal** for those above. Note: Make sure there is at least 2 cm of clearance on the top and bottom of the Nebula Device, and at least 5 cm of clearance on all four sides of the Nebula Device. This allows air circulation for cooling. Note: Do NOT block the ventilation holes on the Nebula Device. Allow clearance for the ventilation holes to prevent your Nebula Device from overheating. Overheating could affect the performance of your Nebula Device, or even damage it.

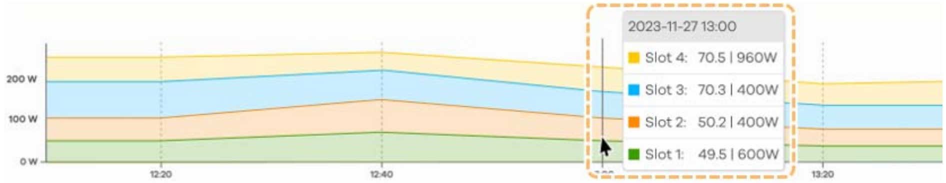
Table 21 Site-wide > Devices > Switches: Switch Details (continued)

LABEL	DESCRIPTION
Fan	**Normal** indicates that this fan is functioning at the normal speed. **High Speed** indicates that this fan is functioning above the normal speed. When the SFP+ transceiver temperature exceeds the temperature threshold (see your transceiver documentation), the Nebula Device automatically turns on the fans with maximum fan speed to cool down the system. The fans do not automatically turn off after the SFP+ transceiver temperature returns below threshold. To turn off the fans, you have to click **Reset**. **Failure** indicates that this fan is functioning below the minimum speed. Note: Go to **Help** > **Support tools** > **Device function table** to view the supported Nebula Devices.
Power source	When the Nebula Device uses two power modules, one is redundant. If one power module fails (**PSU1**) the system can operate on the remaining module (**PSU2**). **Active** indicates that the Nebula Device is currently operating from the power source to which the power module is connected. **Standby** indicates the redundant power module that is connected to a power source but the Nebula Device is NOT operating from it. **Present** is displayed when the power module is connected to the Switch, but is not connected to a power source and there is no available power. **Absent** is displayed when there is no power module connected to the Switch. **Error** indicates that this power module is functioning below the power requirement. Or, the fan in this power module is not working. Note: Go to **Help** > **Support tools** > **Device function table** to view the supported Nebula Devices.
Ports	This shows the ports on the Nebula Device. You can click a port to see the individual port statistics. See Section 4.3.2.3 on page 239. Move the pointer over a port to see additional port information. The port color indicates the connection status of the port. • Gray (#888888): The port is disconnected. • Orange (#FF8900): The port is connected and is transmitting data at 10 or 100 Mbps. • Green (#64BE00): The port is connected and is transmitting data at 1000 Mbps (1 Gbps). • Azure (#00B2FF): The port is connected and is transmitting data at 2.5 Gbps. • Violet (#8800FF): The port is connected and is transmitting data at 5 Gbps. • Blue (#004FEE): The port is connected and is transmitting data at 10000 Mbps (10 Gbps). When the port is in the STP blocking state, failed LACP negotiation state, or failed port authentication state, a blocked icon displays on top of the port (⛔ for example) in the diagram.
Configure ports	Click this button to go to the **Site-wide** > **Configure** > **Switches** > **Switch ports** screen, where you can view port summary. See Section 6.3.1 on page 362.
Name	This shows the Nebula Device name configured in NCC.
Status	This shows the connection status of the port.
LLDP	This shows the LLDP information received on the port.
Type	This shows the port type (**Trunk** or **Access**), PVID, and allowed VLANs.
Speed	This shows the current connection speed of the port. If the speed is unavailable, this displays “Ethernet”.

Table 21 Site-wide > Devices > Switches: Switch Details (continued)

LABEL	DESCRIPTION
Power reset	This button only appears when the PoE port is connected to a PD (powered device). Follow the prompt and click **Confirm** to reboot the PD connected to this port. Note: This button is not available for an uplink port.
Live tools	
Ping	Enter the host name or IP address of a computer that you want to perform ping in order to test a connection and click **Ping**.
PoE power reset	Enter the number of, or range of PoE ports and click the **Power reset** button to disable and enable the PoE ports again.
MAC table	This shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which ports. You can define how it displays and arrange the data in the summary table below. Note: This tab will appear for NSW100 and NSW200 Series only.
Switch tables	Import the following data into NCC: • **MAC table**. Click **Run** to show what device MAC address, belonging to what VLAN group (if any) is forwarded to which ports. You can define how it displays and arrange the data in the summary table. • **Routing table**. Click **Run** to show the routing destination, gateway, interface IP addresses, hop count, and routing methods. The routing table is only displayed for L3 Nebula Devices. • **ARP table**. Click **Run** to show the IP-to-MAC address mappings. The ARP table is only displayed for L3 Nebula Devices. • **IP source guard**. Click **Run** to show the static, DHCP snooping, blocked client entries, and expiration time of DHCP snooping and blocked entries on the Nebula Device. After clicking **Run** in **IP source guard**, the IPSG (IP source guard) table could be empty if: • It takes about 5 minutes to refresh the address table after you apply the Nebula Device settings • Protected port is not specified • NCC may not get completed data from Nebula Device due to unstable network. Please retry.
Reboot device	Click the **Reboot** button to restart the Nebula Device.
Locator LED	Enter a time interval between 1 and 60 minutes to stop the locator LED from blinking. The locator LED will start to blink for the number of minutes set here. Click the ⊙ button to turn on the locator feature, which shows the actual location of the Nebula Device between several Nebula Devices in the network.
Remote SSH	Select to use TCP (Transmission Control Protocol) **Port 22** or **443** to establish a remote connection to this Nebula Device. The Nebula Device will create a reverse SSH (Secure SHell) connection. Then click **Establish**. After clicking **Ok**, NCC will provide a remote connection IPv4 address and service port number. For example, Remote connection: 34.247.173.104:27086. Use this IPv4 address and port to connect to the Nebula Device using an SSH terminal emulator (for example, PuTTY). The remote session will be available for 30 minutes. In case the connection cannot be established, confirm that the network allows **Port 22** or **443**. Note: Use **Remote SSH** for troubleshooting only.
Uplink usage Move the cursor over the chart to see the transmission rate at a specific time.	
Zoom	Select to view the statistics in the past 2 hours, day, week, month, 3 months or 6 months.
Pan	Click to move backward or forward by one day or week.

Table 21 Site-wide > Devices > Switches: Switch Details (continued)

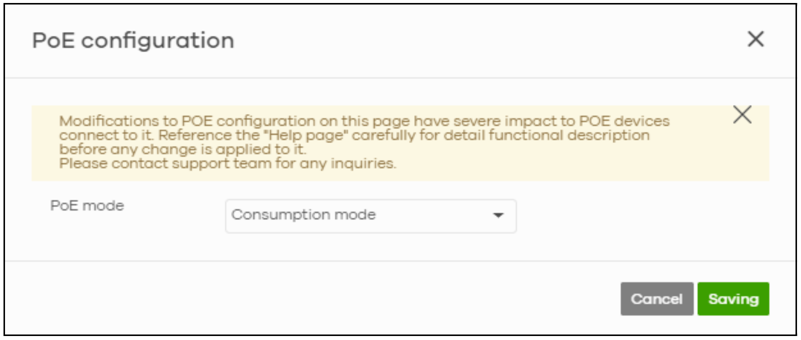
LABEL	DESCRIPTION
Power Consumption	
	Select to view the Nebula Device power consumption in the past two hours, day, week or month.
Per slot usage (consumption/power budget)	In Cloud Stacking mode, this shows the current power consumption over the total power budget (in percentage) of each Nebula Device in the stacking system.
Maximum / Minimum consumption	This shows the current, total, maximum and minimum power consumption of the Nebula Device.
y-axis	The y-axis shows the amount of power used in Watts. In Cloud Stacking mode, each stacked colored graph represents the power consumption of each Nebula Device. The highest point of the graph represents the total power consumption of the stacked Nebula Devices at the time. For example, if Nebula Device 1 = 30 W, Nebula Device 2 = 40 W, Nebula Device 3 = 50 W. The highest point in Nebula Device 2 is 70 W. The highest power consumption is 120 W at the time.
x-axis	The x-axis shows the time period over which the power consumption is recorded. Hover the mouse over the graph to view the recorded power consumption of a Nebula Device on a specific time. 

4.3.2.2 PoE Configuration

Use this screen to set the PoE settings for the Nebula Device. To access this screen, click the edit icon next to **PoE Status** in the **Site-wide** > **Devices** > **Switches: Switch Details** screen.

Note: To set PoE settings for an individual port, such as schedule, priority, and power mode, edit the Nebula Device's port settings. For details, see Section 6.3.1 on page 362.

Figure 46 Site-wide > Devices > Switches: Switch Details: PoE Configuration



PoE configuration

Modifications to POE configuration on this page have severe impact to POE devices connect to it. Reference the "Help page" carefully for detail functional description before any change is applied to it.
Please contact support team for any inquiries.

PoE mode: Consumption mode

The following table describes the labels in this screen.

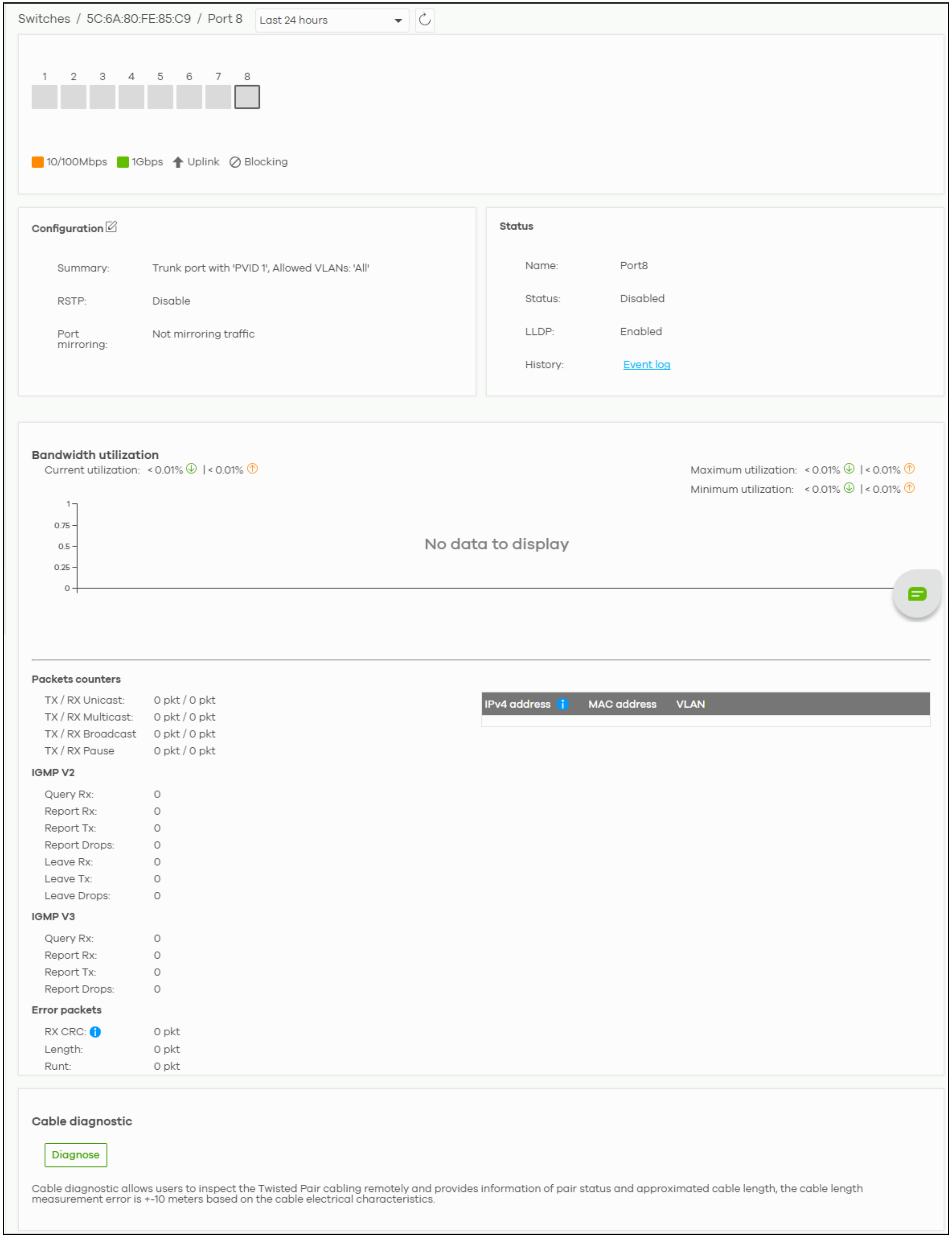
Table 22 Site-wide > Devices > Switches: Switch Details: PoE Configuration

LABEL	DESCRIPTION
PoE Mode	Select the power management mode you want the Nebula Device to use. **Classification mode** – Select this if you want the Nebula Device to reserve the Max Power (mW) to each powered device (PD) according to the priority level. If the total power supply runs out, PDs with lower priority do not get power to function. **Consumption mode** – Select this if you want the Nebula Device to manage the total power supply so that each connected PD gets a resource. However, the power allocated by the Nebula Device may be less than the Max Power (mW) of the PD. PDs with higher priority also get more power than those with lower priority levels.
Close	Click this button to exit this screen without saving.
Saving	Click this button to save your changes and close the screen.

4.3.2.3 Switch Port Details

Use this to view individual Nebula Device port statistics. To access this screen, click a port in the **Ports** section of the **Site-wide** > **Devices** > **Switches: Switch Details** screen or click the **details** link next to a port in the **Site-wide** > **Configure** > **Switches** > **Switch ports** screen.

Figure 47 Site-wide > Devices > Switches: Switch Details: Port Details



Switches / 5C:6A:80:FE:85:C9 / Port 8   Last 24 hours

🟧 10/100Mbps 🟩 1Gbps ⬆ Uplink ⊘ Blocking

Configuration

Summary:	Trunk port with 'PVID 1', Allowed VLANs: 'All'
RSTP:	Disable
Port mirroring:	Not mirroring traffic

Status

Name:	Port8
Status:	Disabled
LLDP:	Enabled
History:	Event log

Bandwidth utilization

Current utilization: < 0.01% | < 0.01%

Maximum utilization: < 0.01% | < 0.01%

Minimum utilization: < 0.01% | < 0.01%

Packets counters

TX / RX Unicast:	0 pkt / 0 pkt
TX / RX Multicast:	0 pkt / 0 pkt
TX / RX Broadcast	0 pkt / 0 pkt
TX / RX Pause	0 pkt / 0 pkt

IPv4 address	MAC address	VLAN

IGMP V2

Query Rx:	0
Report Rx:	0
Report Tx:	0
Report Drops:	0
Leave Rx:	0
Leave Tx:	0
Leave Drops:	0

IGMP V3

Query Rx:	0
Report Rx:	0
Report Tx:	0
Report Drops:	0

Error packets

RX CRC:	0 pkt
Length:	0 pkt
Runt:	0 pkt

Cable diagnostic

Cable diagnostic allows users to inspect the Twisted Pair cabling remotely and provides information of pair status and approximated cable length, the cable length measurement error is +-10 meters based on the cable electrical characteristics.

The following table describes the labels in this screen.

Table 23 Site-wide > Devices > Switches: Switch Details: Port Details

LABEL	DESCRIPTION
↻	Click this button to reload the data-related frames on this page.
Switch / Port	Select to view the port information and connection status in the past two hours, day, week or month.
Port	This figure shows the ports on the Nebula Device. Click a port to go to the corresponding port details screen. The selected port is highlighted. Move the pointer over a port to see additional port information, such as its name, MAC address, type, and connection speed. The port color indicates the connection status of the port. • Gray (#888888): The port is disconnected. • Orange (#FF8900): The port is connected and is transmitting data at 10 or 100 Mbps. • Green (#64BE00): The port is connected and is transmitting data at 1000 Mbps (1 Gbps). • Azure (#00B2FF): The port is connected and is transmitting data at 2.5 Gbps. • Violet (#8800FF): The port is connected and is transmitting data at 5 Gbps. • Blue (#004FEE): The port is connected and is transmitting data at 10000 Mbps (10 Gbps). When the port is in the STP blocking state, failed LACP negotiation state, or failed port authentication state, a blocked icon displays on top of the port (⛔ for example) in the diagram.
Name	This shows the descriptive name of the port.
Status	This shows the connection status of the port.
MAC address	This shows the MAC address of the port.
Type	This shows the port type (**Trunk** or **Access**), PVID, and allowed VLANs.
Speed	This shows the current connection speed of the port. If the speed is unavailable, this displays "Ethernet".
LLDP	This shows the LLDP information received on the port.
Configuration Click the edit icon to open the **Switch ports** screen and show the ports that match the filter criteria (the selected port number). See Section 6.3.1 on page 362.	
Summary	This shows the port's VLAN settings.
RSTP	This shows whether RSTP is disabled or enabled on the port.
Port mirroring	This shows whether traffic is mirrored on the port.
Status	
Name	This shows the name of the port.
Status	This shows the status of the port.
LLDP	This shows the LLDP (Link Layer Discovery Protocol) information received on the port.
History	Click **Event log** to go to the **Site-wide** > **Monitor** > **Switches** > **Event log** screen.
Bandwidth Utilization	
Current Utilization	This shows what percentage of the upstream/downstream bandwidth is currently being used by the port.
Maximum Utilization	This shows the maximum upstream/downstream bandwidth utilization (in percentage).
Minimum Utilization	This shows the minimum upstream/downstream bandwidth utilization (in percentage).
y-axis	The y-axis represents the transmission rate in Kbps (kilobits per second).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Power Consumption	

Table 23 Site-wide > Devices > Switches: Switch Details: Port Details (continued)

LABEL	DESCRIPTION
Total	This shows the total power consumption of the port.
Current Consumption	This shows the current power consumption of the port.
Maximum Consumption	This shows the maximum power consumption of the port.
Minimum Consumption	This shows the minimum power consumption of the port.
y-axis	The y-axis shows how much power is used in Watts.
x-axis	The x-axis shows the time period over which the power consumption is recorded.
Packets Counters	
TX/RX Unicast	This shows the number of good unicast packets transmitted/received on the port.
TX/RX Multicast	This shows the number of good multicast packets transmitted/received on the port.
TX/RX Broadcast	This shows the number of good broadcast packets transmitted/received on the port.
TX/RX Pause	This shows the number of 802.3x Pause packets transmitted/received on the port.
IGMP V2/V3	
Query Rx	This shows the number of IGMP query packets received on the port.
Report Rx	This shows the number of IGMP report packets received on the port.
Report Tx	This shows the number of IGMP report packets transmitted on the port.
Report Drops	This shows the number of IGMP report packets dropped on the port.
Leave Rx	This shows the number of IGMP leave packets received on the port.
Leave Tx	This shows the number of IGMP leave packets transmitted on the port.
Leave Drops	This shows the number of IGMP leave packets dropped on the port.
Error Packets	
RX CRC	This shows the number of packets received with CRC (Cyclic Redundant Check) errors. CRC errors indicate packet errors in the network, potentially caused by mismatching Ethernet speed/duplex, bad cables or transceivers, or malfunctioning client devices.
Length	This shows the number of packets received with a length that was out of range.
Runt	This shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
IPv4 Address	This shows the IP address of the incoming frame which is forwarded on the port. Note: The IP address is obtained using one of the following three methods: • LLDP remote information • Information collected by the Nebula Security Gateway (NSG) in this site • Information collected by NCC when the client connected to Nebula
MAC Address	This shows the MAC address of the incoming frame which is forwarded on the port.
VLAN	This shows the VLAN group to which the incoming frame belongs.
Cable Diagnostics	
Diagnose	Click **Diagnose** to perform a physical wire-pair test of the Ethernet connections on the port. The following fields display when you diagnose a port.
Channel	An Ethernet cable usually has four pairs of wires. A 10BASE-T or 100BASE-TX port only use and test two pairs, while a 1000BASE-T port requires all four pairs. This displays the descriptive name of the wire-pair in the cable.

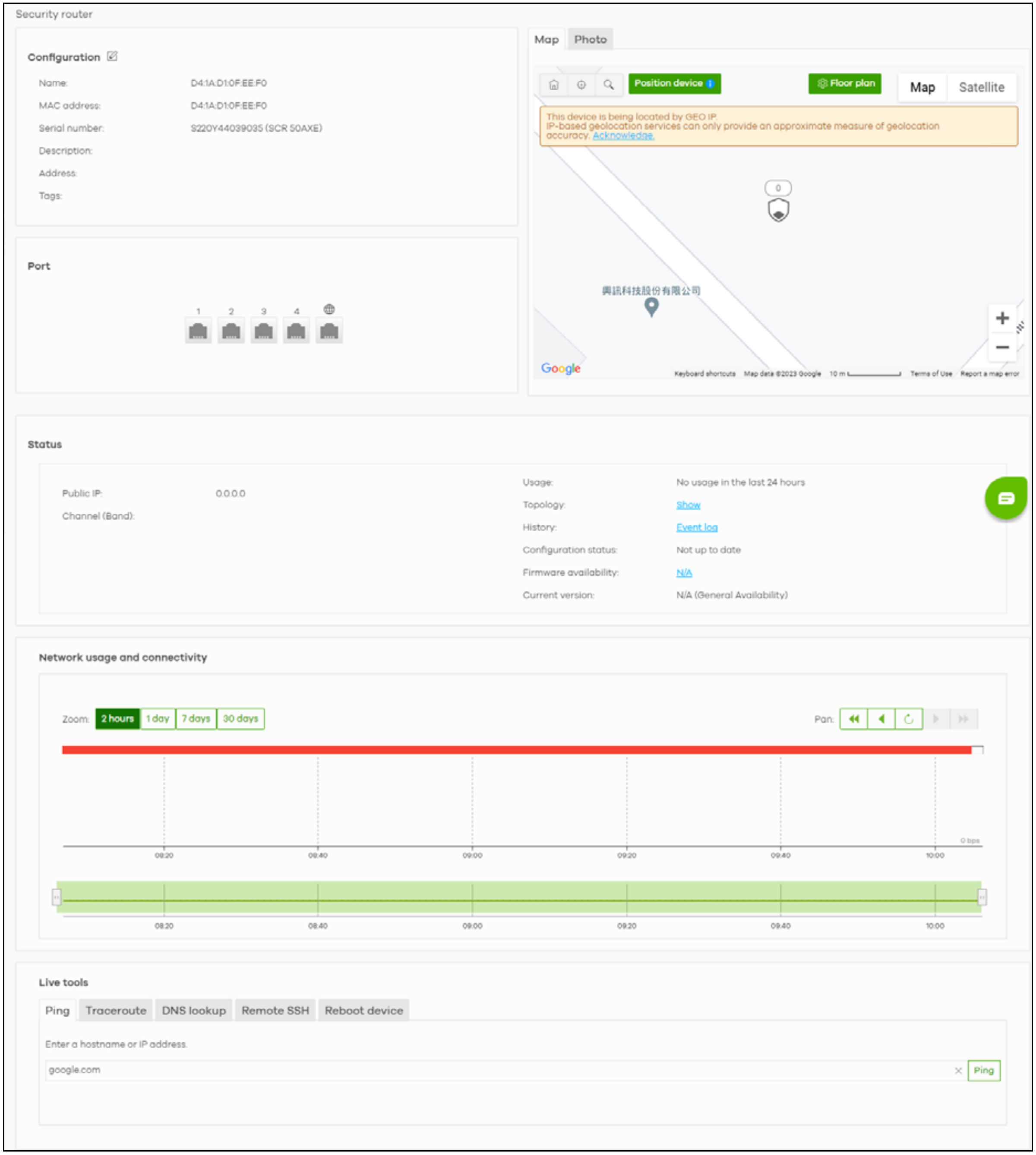
Table 23 Site-wide > Devices > Switches: Switch Details: Port Details (continued)

LABEL	DESCRIPTION
Pair Status	**OK**: The physical connection between the wire-pair is okay. **Open**: There is no physical connection (an open circuit detected) between the wire-pair. **Short**: There is a short circuit detected between the wire-pair. **Unknown**: The Nebula Device failed to run cable diagnostics on the cable connected to this port. **Unsupported**: The port is a fiber port or it is not active.
Cable Length	This displays the total length of the Ethernet cable that is connected to the port when the **Pair Status** is **OK** and the Nebula Device chipset supports this feature. This shows **N/A** if the **Pair Status** is **Open** or **Short**. Check the **Distance to fault**. This shows **Unsupported** if the Nebula Device chipset does not support to show the cable length.
Distance to fault (m)	This displays the distance between the port and the location where the cable is open or shorted. This shows **N/A** if the **Pair Status** is **OK**. This shows **Unsupported** if the Nebula Device chipset does not support to show the distance.
DDMI	This section is available only on an SFP (Small Form Factor Pluggable) port.
DDMI	Click **DDMI** (Digital Diagnostics Monitoring Interface) to display real-time SFP transceiver information and operating parameters on the port. You can also see the alarm and warning thresholds for temperature, voltage, transmission bias, transmission and receiving power.
Port	This shows the number of the port on the Nebula Device.
Vendor	This shows the vendor name of the transceiver installed in the port.
PN	This shows the part number of the transceiver installed in the port.
SN	This shows the serial number of the transceiver installed in the port.
Revision	This shows the firmware version of the transceiver installed in the port.
Date-code	This shows the date the installed transceiver's firmware was created.
Transceiver	This shows the type and the Gigabit Ethernet standard supported by the transceiver installed in the port.
Calibration	This shows whether the diagnostic information is internally calibrated or externally calibrated.
Current	This shows the current operating parameters on the port, such as transceiver temperature, laser bias current, transmitted optical power, received optical power and transceiver supply voltage.
High Alarm Threshold	This shows the high alarm threshold for temperature, voltage, transmission bias, transmission and receiving power. A trap is sent when the operating parameter is above the threshold.
High Warn Threshold	This shows the high warning threshold for temperature, voltage, transmission bias, transmission and receiving power.
Low Warn Threshold	This shows the low alarm threshold for temperature, voltage, transmission bias, transmission and receiving power. A trap is sent when the operating parameter is below the threshold.
Low Alarm Threshold	This shows the low warning threshold for temperature, voltage, transmission bias, transmission and receiving power.

4.3.3 Security Router

This screen allows you to view the detailed information about the Nebula Device in the selected site. Click **Site-wide** > **Devices** > **Security router** to access this screen.

Figure 48 Site-wide > Devices > Security router



Security router

Configuration

Name: D4:1A:D1:0F:EE:F0

MAC address: D4:1A:D1:0F:EE:F0

Serial number: S220Y44039035 (SCR 50AXE)

Description:

Address:

Tags:

Port

This device is being located by GEO IP.
IP-based geolocation services can only provide an approximate measure of geolocation accuracy. Acknowledge.

Status

Public IP: 0.0.0.0

Channel (Band):

Usage: No usage in the last 24 hours

Topology: Show

History: Event log

Configuration status: Not up to date

Firmware availability: N/A

Current version: N/A (General Availability)

Network usage and connectivity

Live tools

Enter a hostname or IP address.

google.com

The following table describes the labels in this screen.

Table 24   Site-wide > Devices > Security router

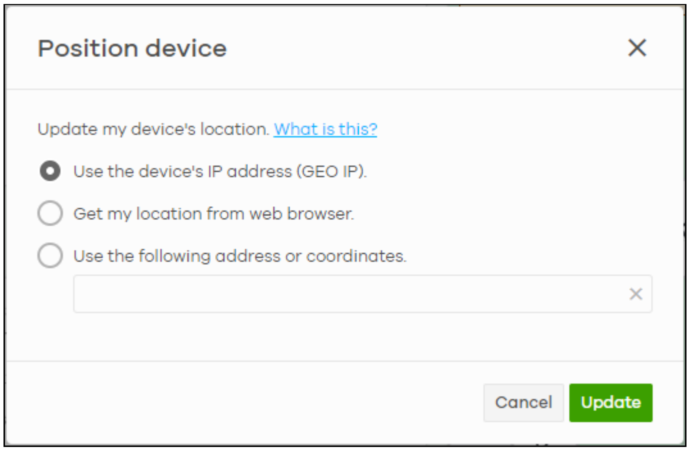
LABEL	DESCRIPTION
Configuration Click the edit icon to change the Nebula Device name, description, tags and address (physical location). You can also move the Nebula Device to another site or remove.	
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device's WAN port.
Serial number	This shows the serial number of the Nebula Device.
Description	This shows the user-specified description for the Nebula Device.
Address	This shows the user-specified address (physical location) for the Nebula Device.
Tags	This shows the user-specified tags for the Nebula Device.
Port	This shows the ports on the Nebula Device. The port is highlighted in green color when it is connected and the link is up. Move the pointer over a port to see additional port information, such as its name, connection status, MAC address, and connection speed.
Map	This shows the location of the Nebula Device on Google Maps (**Map** view or **Satellite** imagery view) or on a floor plan. Click **Floor plan** to display a list of existing floor plans. Each floor plan has a drawing that shows the rooms scaled and viewed from above. Drag-and-drop your Nebula Device directly on the Google map or click **Position device** to update the Nebula Device's address (physical location).  Position device Update my device's location. What is this? ● Use the device's IP address (GEO IP). ○ Get my location from web browser. ○ Use the following address or coordinates. Cancel Update • Select **GEO IP** to use the public IP address of the Nebula Device. • Select **Get my location from web browser** to use the public IP address of the computer accessing the NCC portal. • Select **Use the following address or coordinates** to enter the complete address or coordinates of the Nebula Device. Note: Nebula Devices that are offline cannot use GEO IP.
Photo	This shows the photo of the Nebula Device. Click **Add** to upload one or more photos. Click **x** to remove a photo.
Status	
Public IP	This shows the IPv4 address of the WAN interface, and whether it was assigned automatically (DHCP), manually (Static IP), or by PPPoE.

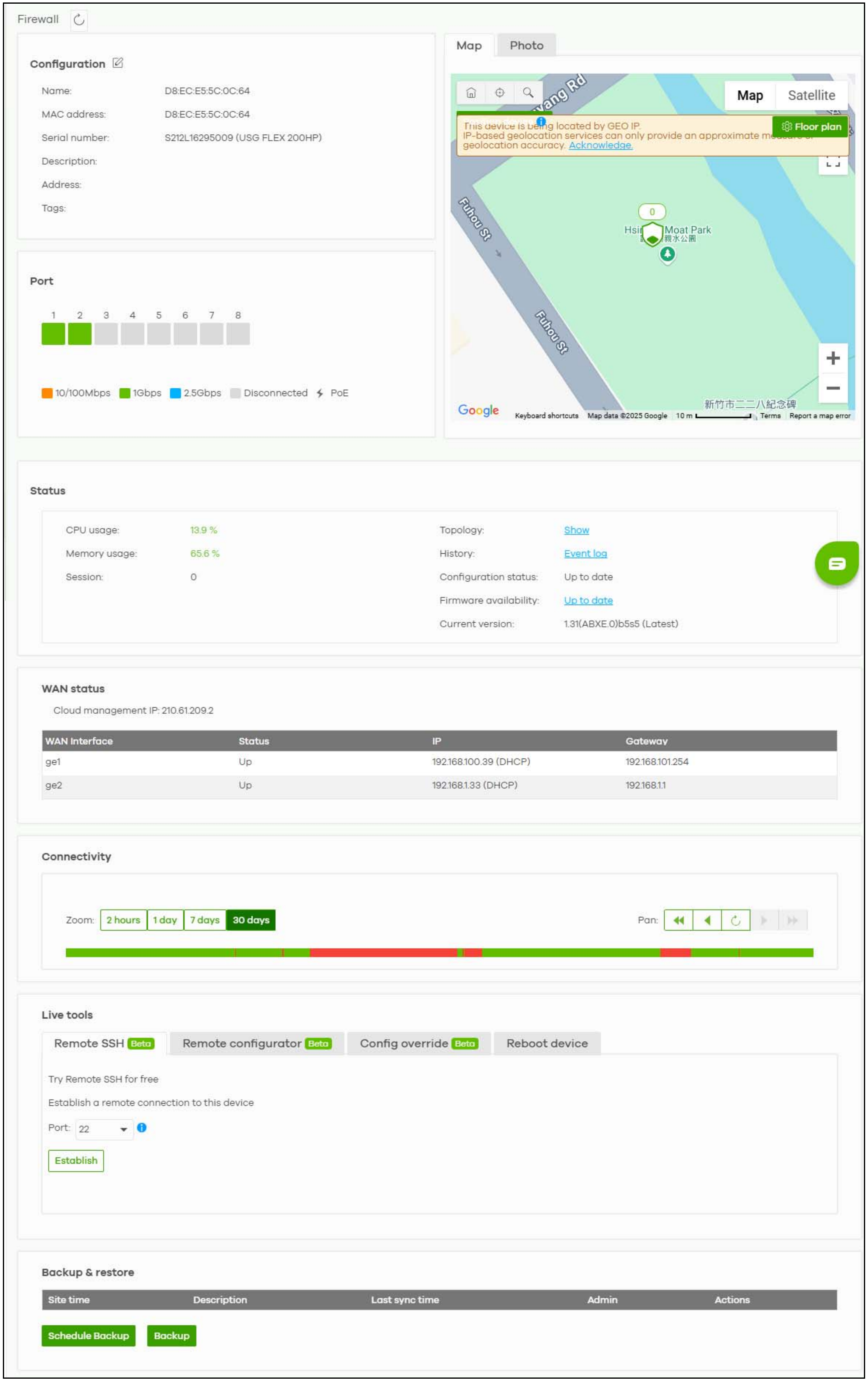
Table 24 Site-wide > Devices > Security router (continued)

LABEL	DESCRIPTION
Channel (Band)	This shows the channel ID and WiFi frequency band currently being used by the Nebula Device. Note: This field only appears for ZyWALL ATP100W, USG FLEX 100W, and USG20W-VPN.
Usage	This shows the amount of data that has been transmitted or received by the Nebula Device's clients.
Topology	Click **Show** to go to the **Site-wide** > **Topology** screen. See Section 4.2 on page 208.
History	Click **Event log** to go to the **Site-wide** > **Monitor** > **Security router** > **Event log** screen.
Configuration status	This shows whether the configuration on the Nebula Device is **Up-to-date**.
Firmware availability	This shows whether the firmware installed on the Nebula Device is **Up-to-date**.
Current version	This shows the firmware version currently installed on the Nebula Device.
Network usage and connectivity Move the cursor over the chart to see the transmission rate at a specific time.	
Zoom	Select to view the statistics in the past 2 hours, 24 hours, 7 days, or 30 days.
Pan	Click to move backward or forward by one day or week.
Live tools	
Ping	Enter the host name or IP address of a computer that you want to perform ping in order to test a connection and click **Ping**. You can select the interface (WAN, LAN, or VLAN) through which the Security Firewall sends queries for ping. Note: • To ping for VPN/routing issues, it is not necessary to connect an end-device on the LAN interface of the Nebula Device. • A routing problem is possible if the WAN interface can reach the Internet but not the LAN interface.
Traceroute	Enter the host name or IP address of a computer that you want to perform the traceroute function. This determines the path a packet takes to the specified computer.
DNS lookup	Enter a host name and click **Run** to resolve the IP address for the specified domain name.
Remote SSH	This allows you to establish a remote connection to this Nebula Device by specifying the port number. Then click **Establish**. This feature is available to the organization owner, organization administrators with full privileges, and site administrators with full privileges.
Reboot device	Click the **Reboot** button to restart the Nebula Device.

4.3.4 Firewall

This screen allows you to view the detailed information about the Nebula Device in the selected site. Click **Site-wide** > **Devices** > **Firewall** to access this screen.

Figure 49 Site-wide > Devices > Firewall (Cloud Mode)



Firewall

Configuration

Name:	D8:EC:E5:5C:0C:64
MAC address:	D8:EC:E5:5C:0C:64
Serial number:	S212L16295009 (USG FLEX 200HP)
Description:	
Address:	
Tags:	

Port

1	2	3	4	5	6	7	8
🟩	🟩	▨	▨	▨	▨	▨	▨

🟧 10/100Mbps 🟩 1Gbps 🟦 2.5Gbps ▨ Disconnected ⚡ PoE

Map Photo

This device is being located by GEO IP.
IP-based geolocation services can only provide an approximate measure of geolocation accuracy. Acknowledge.

Status

CPU usage:	13.9 %	Topology:	Show
Memory usage:	65.6 %	History:	Event log
Session:	0	Configuration status:	Up to date
		Firmware availability:	Up to date
		Current version:	1.31(ABXE.0)b5s5 (Latest)

WAN status

Cloud management IP: 210.61.209.2

WAN Interface	Status	IP	Gateway
ge1	Up	192.168.100.39 (DHCP)	192.168.101.254
ge2	Up	192.168.1.33 (DHCP)	192.168.1.1

Connectivity

Zoom: 2 hours | 1 day | 7 days | **30 days**

Pan: ⏪ ◀ ↻ ▶ ⏩

Live tools

Remote SSH Beta | Remote configurator Beta | Config override Beta | Reboot device

Try Remote SSH for free

Establish a remote connection to this device

Port: 22

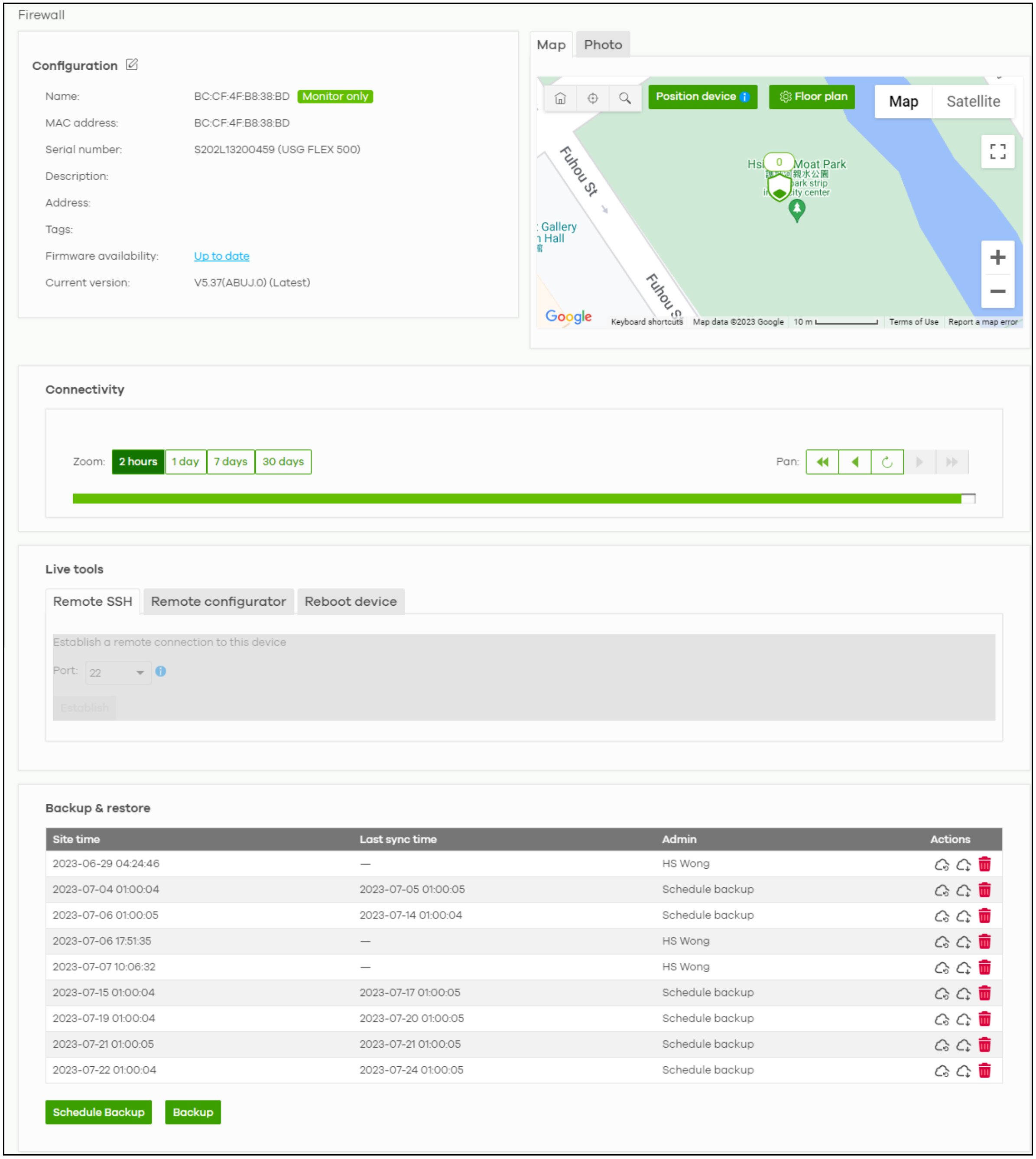
Establish

Backup & restore

Site time	Description	Last sync time	Admin	Actions

Schedule Backup | Backup

Figure 50 Site-wide > Devices > Firewall (Cloud Monitoring Mode)



Firewall

Configuration

Name: BC:CF:4F:B8:38:BD Monitor only

MAC address: BC:CF:4F:B8:38:BD

Serial number: S202L13200459 (USG FLEX 500)

Description:

Address:

Tags:

Firmware availability: Up to date

Current version: V5.37(ABUJ.0) (Latest)

Connectivity

Zoom: 2 hours | 1 day | 7 days | 30 days

Pan:

Live tools

Remote SSH | Remote configurator | Reboot device

Establish a remote connection to this device

Port: 22

Establish

Backup & restore

Site time	Last sync time	Admin	Actions
2023-06-29 04:24:46	—	HS Wong	
2023-07-04 01:00:04	2023-07-05 01:00:05	Schedule backup	
2023-07-06 01:00:05	2023-07-14 01:00:04	Schedule backup	
2023-07-06 17:51:35	—	HS Wong	
2023-07-07 10:06:32	—	HS Wong	
2023-07-15 01:00:04	2023-07-17 01:00:05	Schedule backup	
2023-07-19 01:00:04	2023-07-20 01:00:05	Schedule backup	
2023-07-21 01:00:05	2023-07-21 01:00:05	Schedule backup	
2023-07-22 01:00:04	2023-07-24 01:00:05	Schedule backup	

Schedule Backup | Backup

The following table describes the labels in this screen.

Table 25 Site-wide > Devices > Firewall

LABEL	DESCRIPTION
Configuration Click the edit icon to change the Nebula Device name, description, tags and address (physical location). You can also move the Nebula Device to another site or remove.	
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device's WAN port.

Table 25   Site-wide > Devices > Firewall (continued)

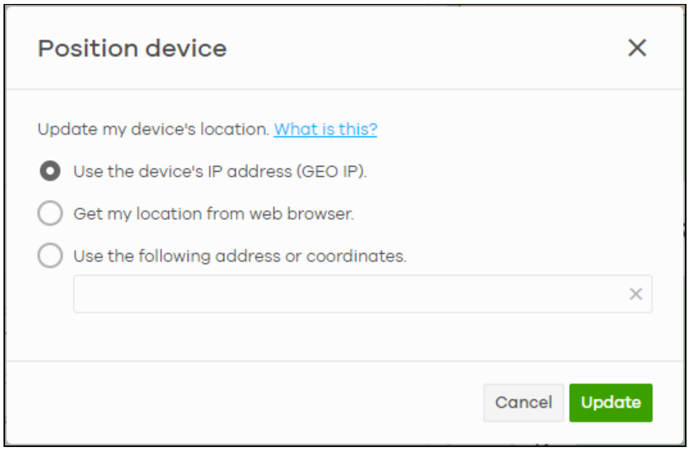
LABEL	DESCRIPTION
Serial number	This shows the serial number of the Nebula Device.
Description	This shows the user-specified description for the Nebula Device.
Address	This shows the user-specified address (physical location) for the Nebula Device.
Tags	This shows the user-specified tags for the Nebula Device.
Port	This shows the ports on the Nebula Device. The port is highlighted in green color when it is connected and the link is up. Move the pointer over a port to see additional port information, such as its name, connection status, MAC address, and connection speed. Note: These fields will not show in Cloud Monitoring mode.
Port	This shows the identity number of the selected port.
Port Group	This shows the name of the port group that the port belongs to.
Status	This shows the connection status of the port.
Map	This shows the location of the Nebula Device on Google Maps (**Map** view or **Satellite** imagery view) or on a floor plan. Click **Floor plan** to display a list of existing floor plans. Each floor plan has a drawing that shows the rooms scaled and viewed from above. Drag-and-drop your Nebula Device directly on the Google map or click **Position device** to update the Nebula Device's address (physical location).  Position device ✕ Update my device's location. What is this? ● Use the device's IP address (GEO IP). ○ Get my location from web browser. ○ Use the following address or coordinates. - Select **GEO IP** to use the public IP address of the Nebula Device. - Select **Get my location from web browser** to use the public IP address of the computer accessing the NCC portal. - Select **Use the following address or coordinates** to enter the complete address or coordinates of the Nebula Device. Note: Nebula Devices that are offline cannot use GEO IP.
Photo	This shows the photo of the Nebula Device. Click **Add** to upload one or more photos. Click **x** to remove a photo.
Status Note: These fields will not show in Cloud Monitoring mode.	
CPU usage	This shows what percentage of the Nebula Device's processing capability is currently being used.
Memory usage	This shows what percentage of the Nebula Device's RAM is currently being used.
Session	This shows how many sessions the Nebula Device currently has. A session is a unique established connection that passes through, from, to, or within the Nebula Device.

Table 25 Site-wide > Devices > Firewall (continued)

LABEL	DESCRIPTION
Channel (Band)	This shows the channel ID and WiFi frequency band currently being used by the Nebula Device. Note: This field only appears for ZyWALL ATP100W, USG FLEX 100W, and USG20W-VPN.
Usage	This shows the amount of data that has been transmitted or received by the Nebula Device's clients.
Topology	Click **Show** to go to the **Site-wide** > **Topology** screen. See Section 4.2 on page 208.
History	Click **Event log** to go to the **Site-wide** > **Monitor** > **Firewall** > **Event log** screen.
Configuration status	This shows whether the configuration on the Nebula Device is **Up-to-date**.
Firmware availability	This shows whether the firmware installed on the Nebula Device is **Up-to-date**.
Current version	This shows the firmware version currently installed on the Nebula Device.
WAN status Note: These fields will not show in Cloud Monitoring mode.	
WAN Interface	This shows the descriptive name of the active WAN connection.
Status	This shows the connection status of the WAN interface (up or down).
IP	This shows the IP address of the WAN interface, and whether it was assigned automatically (DHCP), manually (Static IP), or by PPPoE.
Gateway	This shows the IP address of the default Nebula Device assigned to the WAN interface.
DNS Server	This shows the IP addresses of the DNS servers assigned to the WAN interface.
Network usage and connectivity / Connectivity Move the cursor over the chart to see the transmission rate at a specific time.	
Zoom	Select to view the statistics in the past 2 hours, 24 hours, 7 days, or 30 days.
Pan	Click to move backward or forward by one day or week.
Live tools Note: **Traffic**, **DHCP lease**, **Ping**, **Traceroute** and **DNS lookup**, will not show in Cloud Monitoring mode.	
Traffic	This shows the WAN port statistics. The y-axis represents the transmission rate for uploads and downloads. The x-axis shows the time period over which the traffic flow occurred.
DHCP leases	This shows the IP addresses currently assigned to DHCP clients.
Ping	Enter the host name or IP address of a computer that you want to perform ping in order to test a connection and click **Ping**. You can select the interface (WAN, LAN, or VLAN) through which the Security Firewall sends queries for ping. Note: • To ping for VPN/routing issues, it is not necessary to connect an end-device on the LAN interface of the Nebula Device. • A routing problem is possible if the WAN interface can reach the Internet but not the LAN interface.
Traceroute	Enter the host name or IP address of a computer that you want to perform the traceroute function. This determines the path a packet takes to the specified computer.
DNS lookup	Enter a host name and click **Run** to resolve the IP address for the specified domain name.

Table 25   Site-wide > Devices > Firewall (continued)

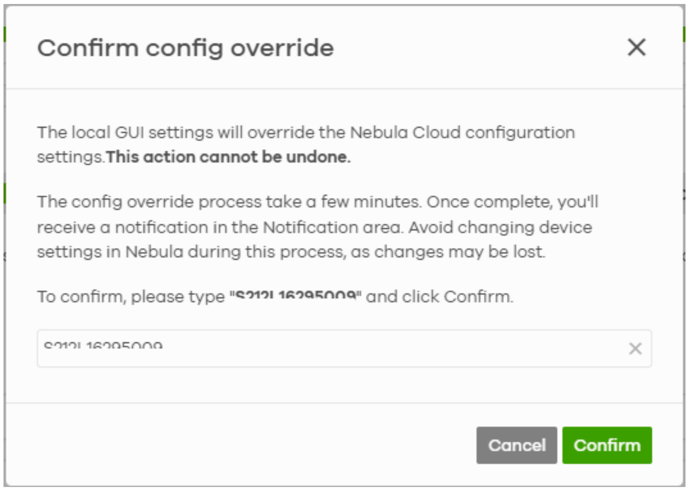
LABEL	DESCRIPTION
Remote SSH	This option is available only for the Nebula Device owner. Establish a remote command line interface (CLI) connection to the Nebula Device by specifying the **Port** number and clicking **Establish**.
Remote configurator	Click **Establish** to use TCP (Transmission Control Protocol) port 443 to establish a remote connection to this Nebula Device. The Nebula Device will create a reverse SSH (Secure SHell) connection. After clicking **Ok**, NCC will provide a remote connection IPv4 address and service port number. For example, https://63.35.218.205:31479. Use this IPv4 address and port to connect to the Nebula Device to open the Web Configurator. The remote session will be available for 30 minutes. In case the connection cannot be established, confirm that the network allows **Port 443**. Note: **Remote configurator** will only show in Cloud Monitoring mode.
Config override	Click **Config override** to apply the current Nebula Device Web Configurator setting to NCC. You will be prompted to copy and enter your Nebula Device's serial number shown on screen and click **Confirm**. The **Confirm** button is not clickable until you enter the correct serial number.  Confirm config override The local GUI settings will override the Nebula Cloud configuration settings.**This action cannot be undone.** The config override process take a few minutes. Once complete, you'll receive a notification in the Notification area. Avoid changing device settings in Nebula during this process, as changes may be lost. To confirm, please type "**S212L16295009**" and click Confirm. S212L16295009 Note: This action cannot be undone.
Reboot device	Click the **Reboot** button to restart the Nebula Device.
Backup & Restore Note: These fields will only show in Cloud Monitoring mode.	
Site time	This shows the date and time of the site, to which the change was applied, when the log was recorded.
Description	This shows the description of the backup.
Last sync time	This shows the year-month-date hour:minute:second when NCC checked the Nebula Device, but skip the scheduled backup because there is no configuration change.
Admin	This shows the name of the administrator who made the back up or **Schedule backup**.
Actions	Click the Restore icon to restore a previously saved configuration file from NCC to the Nebula Device. Click the Download icon to download the configuration file to your computer or laptop. Click the Delete icon to remove the configuration file on the Nebula Device.

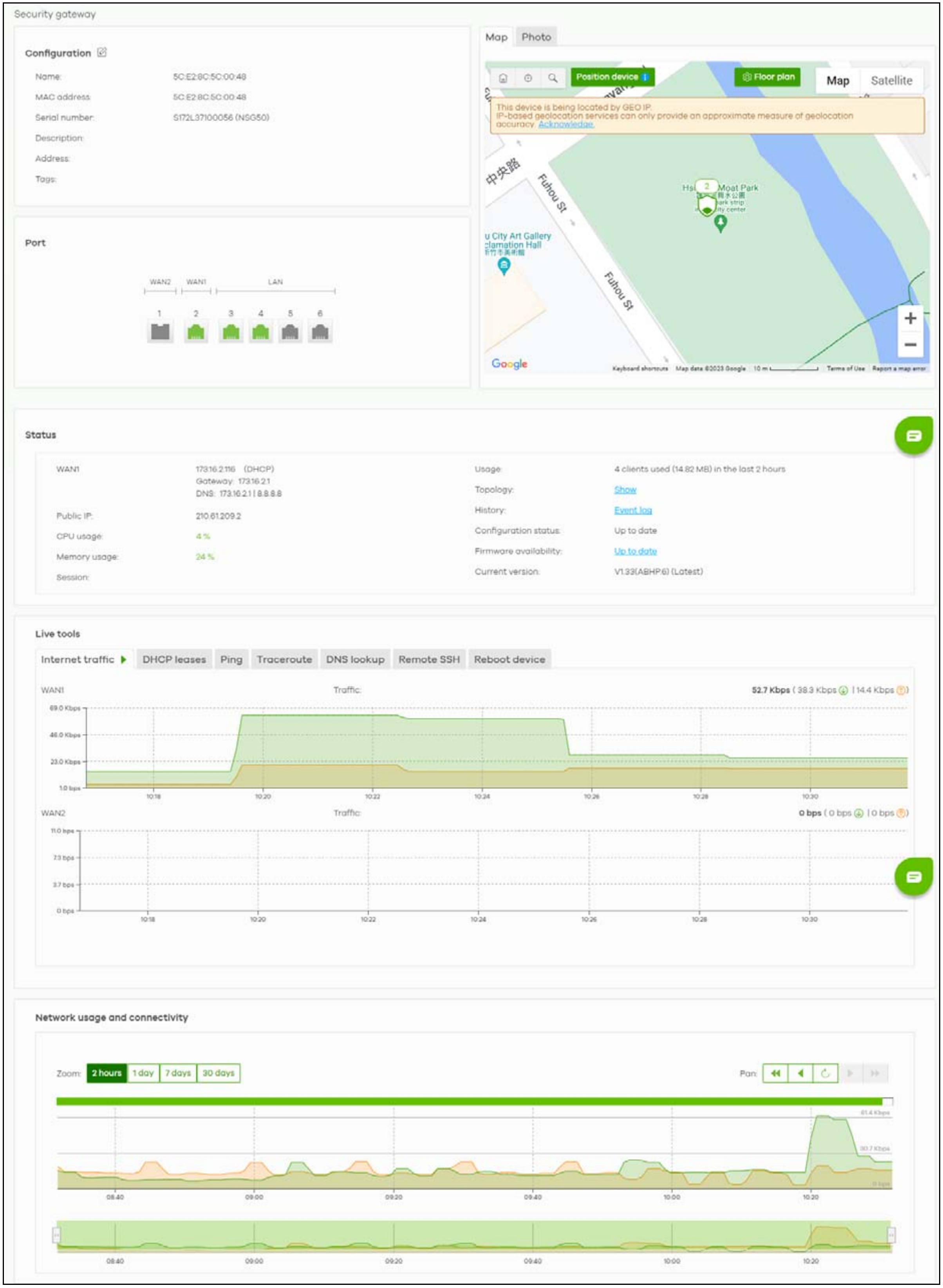
Table 25 Site-wide > Devices > Firewall (continued)

LABEL	DESCRIPTION
Schedule Backup	Select a **Monthly**, **Weekly**, or **Daily** backup of the current configuration of the Nebula Device to the NCC. Then select the **Day** of the month/week. Otherwise, select **Disable**. Then click **Confirm**. Note: • NCC will skip the scheduled backup when there is no configuration change. • NCC can retain up to 10 backup configurations per Nebula Device in this screen. When the maximum number of backup configuration per Nebula Device is reached, a new backup configuration automatically overwrites an existing backup configuration, starting with the oldest existing backup configuration first.
Backup	Click this button to create a new backup of the current configuration of the Nebula Device to the NCC.

4.3.5 Security Gateway

This screen allows you to view the detailed information about a Nebula Device in the selected site. Click **Site-wide** > **Devices** > **Security gateway** to access this screen.

Figure 51 Site-wide > Devices > Security gateway



Security gateway

Configuration

Name: 5C:E2:8C:5C:00:48

MAC address: 5C:E2:8C:5C:00:48

Serial number: S172L37100056 (NSG50)

Description:

Address:

Tags:

Port

This device is being located by GEO IP.
IP-based geolocation services can only provide an approximate measure of geolocation accuracy. Acknowledge

Status

WAN1: 173.16.2.116 (DHCP)
Gateway: 173.16.2.1
DNS: 173.16.2.1 | 8.8.8.8

Public IP: 210.61.209.2

CPU usage: 4 %

Memory usage: 24 %

Session:

Usage: 4 clients used (14.82 MB) in the last 2 hours

Topology: Show

History: Event log

Configuration status: Up to date

Firmware availability: Up to date

Current version: V1.33(ABHP.6) (Latest)

Live tools

WAN1 Traffic: 52.7 Kbps (38.3 Kbps | 14.4 Kbps)

WAN2 Traffic: 0 bps (0 bps | 0 bps)

Network usage and connectivity

The following table describes the labels in this screen.

Table 26 Site-wide > Devices > Security gateway

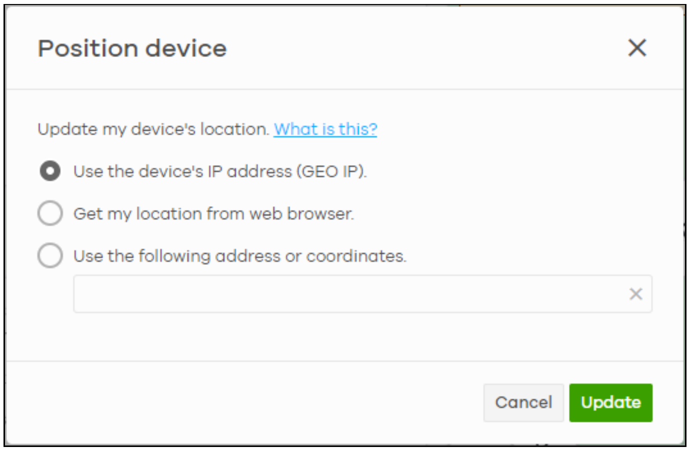
LABEL	DESCRIPTION
Configuration Click the edit icon to change the Nebula Device name, description, tags and address. You can also move the Nebula Device to another site or remove.	
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
Serial number	This shows the serial number of the Nebula Device.
Description	This shows the user-specified description for the Nebula Device.
Address	This shows the user-specified address for the Nebula Device.
Tags	This shows the user-specified tag for the Nebula Device.
Port	This shows the ports on the Nebula Device. The port is highlighted in green color when it is connected and the link is up. Move the pointer over a port to see additional port information, such as its name, connection status, MAC address, and connection speed.
Name	This shows the descriptive name of the port.
Status	This shows the connection status of the port.
MAC address	This shows the MAC address of the port.
LLDP	This shows the LLDP information received on the port.
Speed	This shows the current connection speed of the port. If the speed is unavailable, this displays "Ethernet".
Map	This shows the location of the Nebula Device on the Google map (**Map** view or **Satellite** imagery view) or on a floor plan. Click **Floor plan** to display a list of existing floor plans. Each floor plan has a drawing that shows the rooms scaled and viewed from above. Drag-and-drop your Nebula Device directly on the Google map or click **Position device** to update the Nebula Device's address (physical location).  Position device Update my device's location. What is this? ● Use the device's IP address (GEO IP). ○ Get my location from web browser. ○ Use the following address or coordinates. - Select **GEO IP** to use the public IP address of the Nebula Device. - Select **Get my location from web browser** to use the public IP address of the computer accessing the NCC portal. - Select **Use the following address or coordinates** to enter the complete address or coordinates of the Nebula Device. Note: Nebula Devices that are offline cannot use GEO IP.

Table 26 Site-wide > Devices > Security gateway (continued)

LABEL	DESCRIPTION
Photo	This shows the photo of the Nebula Device. Click **Add** to upload one or more photos. Click **x** to remove a photo.
Status	
WAN1/WAN2	This shows the IP address, gateway, DNS, and VLAN ID information for the active WAN connection.
Public IP	This shows the global (WAN) IP address of the Nebula Device.
CPU usage	This shows what percentage of the Nebula Device's processing capability is currently being used.
Memory usage	This shows what percentage of the Nebula Device's RAM is currently being used.
Security Service	This shows whether Nebula Security Services (NSS) are enabled on the Nebula Device. Click **What is this?** to view the type of enabled security services. When the gateway's NSS license expires, NSS is automatically disabled. This field displays an edit button which you can use to re-enable the services after renewing the NSS license.
Session	
Usage	This shows the amount of data that has been transmitted or received by the Nebula Device's clients.
Topology	Click **Show** to go to the **Site-wide** > **Topology** screen. See Section 4.2 on page 208.
History	Click **Event log** to go to the **Site-wide** > **Monitor** > **Security gateway** > **Event log** screen.
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
Firmware availability	This shows whether the firmware installed on the Nebula Device is up-to-date.
Current version	This shows the firmware version currently installed on the Nebula Device.
Live tools	
Internet traffic	This shows the WAN port statistics. The y-axis represents the transmission rate in Kbps (kilobits per second). The x-axis shows the time period over which the traffic flow occurred.
DHCP leases	This shows the IP addresses currently assigned to DHCP clients.
Ping	Enter the host name or IP address of a computer that you want to perform ping in order to test a connection and click **Ping**. You can select the interface through which the Nebula Device sends queries for ping.
Traceroute	Enter the host name or IP address of a computer that you want to perform the traceroute function. This determines the path a packet takes to the specified computer.
DNS lookup	Enter a host name and click **Run** to resolve the IP address for the specified domain name.
Remote SSH	This option is available only for the Nebula Device owner. Establish a remote connection by specifying the **Port** number and clicking **Establish**.
Reboot device	Click the **Reboot** button to restart the Nebula Device.
Network usage and connectivity Move the cursor over the chart to see the transmission rate at a specific time.	
Zoom	Select to view the statistics in the past 2 hours, day, week, or month.
Pan	Click to move backward or forward by one day or week.

4.3.6 Mobile Router

This screen allows you to view the detailed information about a Nebula Device in the selected site. Click **Site-wide** > **Devices** > **Mobile router** to access this screen. See the Mobile Router chapter for more information.

4.3.7 Accessories

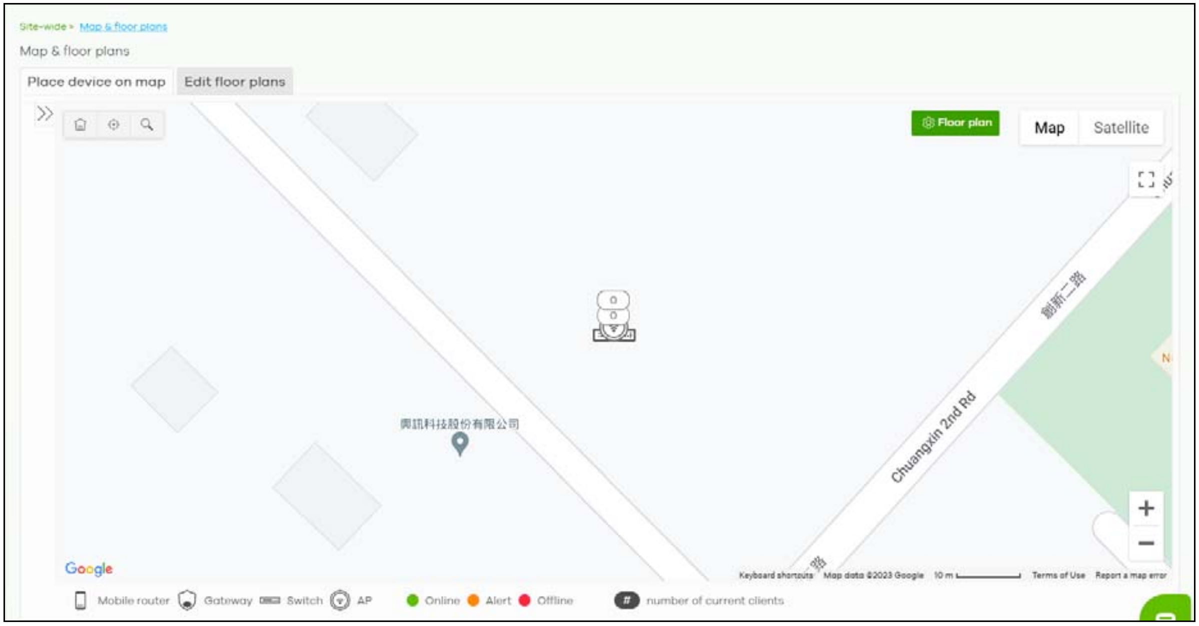
This screen allows you to view the detailed information about a Nebula Device in the selected site. Click **Site-wide** > **Devices** > **Accessories** to access this screen. See the Accessory chapter for more information.

4.4 Map & Floor Plans

This screen allows you to locate a Nebula Device on the world map and use a floor plan to show where Nebula Devices are physically located. Click **Site-wide** > **Map & floor plans** to access this screen.

Note: **Map & floor plans** do not support Nebula Accessories.

Figure 52 Site-wide > Map & floor plans



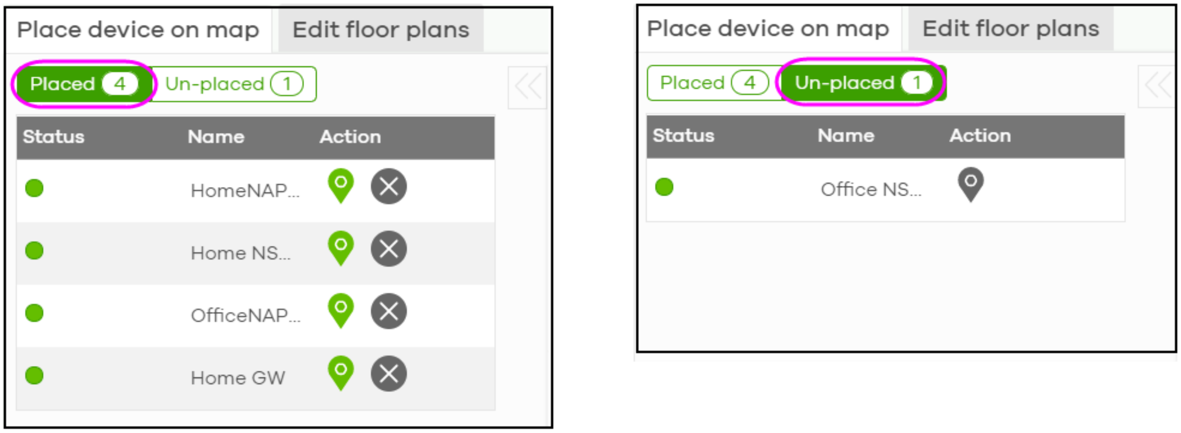
Place device on map

You can mark on the map the places where the Nebula Devices are located. Click the **Place device on map** tab to display the Nebula Device list for the selected site. Click the arrow («) on the upper left corner of the **Map & floor plans** screen to collapse or expand the list.

Click the **Placed** button to show the Nebula Devices that you have pinned on the map and/or the floor plan. Click the **Un-placed** button to show the Nebula Devices that remain to be pinned on the map. To pin a Nebula Device, select the Nebula Device from the **Un-placed** list, then drag and drop it on the map.

The pin icon next to a Nebula Device name is green (📍) if you have marked the Nebula Device on the map. Otherwise, the pin icon is gray (📍). Click the ⊗ icon to remove a Nebula Device from the map.

Figure 53 Site-wide > Map & floor plans: Place device on map



Place device on map | Edit floor plans

Placed 4 | Un-placed 1

Status	Name	Action
●	HomeNAP...	📍 ⊗
●	Home NS...	📍 ⊗
●	OfficeNAP...	📍 ⊗
●	Home GW	📍 ⊗

Place device on map | Edit floor plans

Placed 4 | Un-placed 1

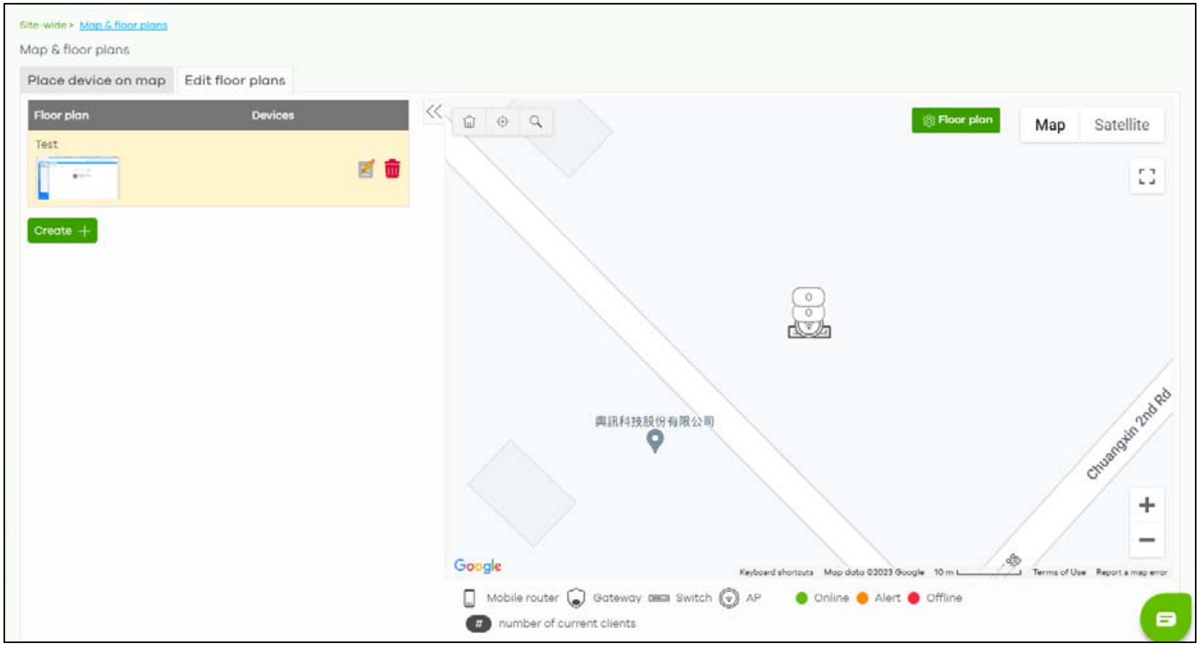
Status	Name	Action
●	Office NS...	📍

Edit floor plans

Click the **Edit floor plans** tab to display the list of existing floor plan, a drawing that shows the rooms scaled and viewed from above. Click the arrow («) on the upper left corner of the **Map & floor plans** screen to collapse or expand the list.

Use the **Create+** button to upload a new floor plan. The floor plan then shows on the Google map at the right side of the screen. Use your mouse to move the floor plan, and use the icons at the top of the map to rotate, change the transparency, resize or hide the floor plan. Click **Set position** to apply your changes. If you want to relocate the floor plan, select the floor plan from the list and click its edit icon.

Figure 54 Site-wide > Map & floor plans: Edit floor plans



The following table describes the labels in this screen.

Table 27 Site-wide > Map & floor plans: Edit floor plans

LABEL	DESCRIPTION
Floor plan	This shows the descriptive name of the floor plan.
Devices	This shows the number of Nebula Devices marked on this floor plan.
✎	Click this icon to open a screen, where you can modify the name, address and/or dimension of the floor plan.
🗑	Click this icon to delete the floor plan.

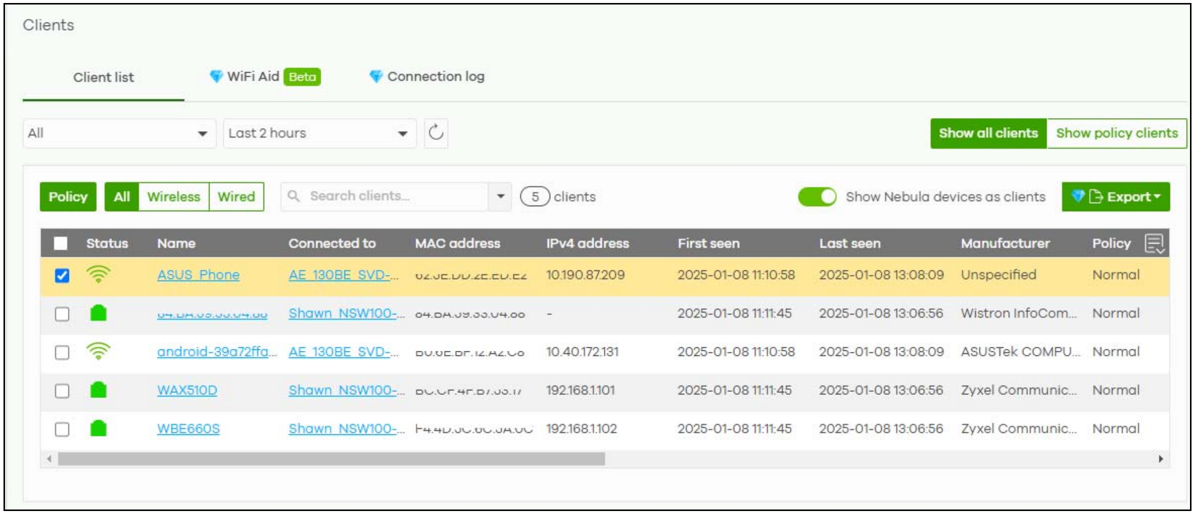
4.5 Clients

This screen shows a list of all wired and WiFi clients connected to Nebula Devices (access points, Switches, Security Appliances) in the site. You can also block or allow clients. Click **Site-wide** > **Clients** to access this screen.

Note: The blocked WiFi clients will apply to both Access Points and Security Router.

Note: NCC will not show the wired clients connected to Nebula Accessories in the site.

Figure 55 Site-wide > Clients > Client list



☐	Status	Name	Connected to	MAC address	IPv4 address	First seen	Last seen	Manufacturer	Policy
☑		ASUS_Phone	AE_130BE_SVD-...	[illegible]	10.190.87.209	2025-01-08 11:10:58	2025-01-08 13:08:09	Unspecified	Normal
☐		[illegible]	Shawn_NSW100-...	[illegible]	-	2025-01-08 11:11:45	2025-01-08 13:06:56	Wistron InfoCom...	Normal
☐		android-39a72ffa...	AE_130BE_SVD-...	[illegible]	10.40.172.131	2025-01-08 11:10:58	2025-01-08 13:08:09	ASUSTek COMPU...	Normal
☐		WAX510D	Shawn_NSW100-...	[illegible]	192.168.1.101	2025-01-08 11:11:45	2025-01-08 13:06:56	Zyxel Communic...	Normal
☐		WBE660S	Shawn_NSW100-...	[illegible]	192.168.1.102	2025-01-08 11:11:45	2025-01-08 13:06:56	Zyxel Communic...	Normal

The following table describes the labels in this screen.

Table 28 Site-wide > Clients > Client list

LABEL	DESCRIPTION
Client list	Select to filter the **Clients by device type** (**Access point clients**, **Switch clients**, **Firewall clients**, **Security gateway clients**, **Security router clients**) the client is connected to. You can also set a time; the list shows each client's connection status in the **Last 2 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, or **Custom range**. The maximum **Custom range** is 30 days within the past 365 days. When you select **Clients: All**, you can show each client's connection status in the **Last 2 hours** and **Last 24 hours** only.
↻	Click this button to reload the data-related frames on this page.
Show all clients	Click this to show all clients that have been online during the selected time period.

Table 28 Site-wide > Clients > Client list (continued)

LABEL	DESCRIPTION
Show policy clients	Click this to show clients that have a white-listed, blocked, or reserved IP policy applied to them, regardless of when they were last online. The client’s usage data is calculated according to the selected time period.
Policy	Select the clients from the table below, and then choose the security policy that you want to apply to the selected clients. Choose one of the following policies, then click **Apply policy**. • **Allow list**: The selected clients to bypass captive portal authentication. Selecting the **Allow list** policy will automatically add the **Reserve IP** policy to the security firewall clients. • **Block list**: The selected clients cannot connect to the site. How a client is blocked depends on the connected Nebula Device type selected under **Client list**. **AP**: The client is blocked by MAC address from connecting to any AP in the site. **Switch**: The client is blocked by MAC address from sending or receiving network traffic. **Gateway**: The Security Appliance will not route traffic for the client’s IP address. Selecting the **Block list** policy will automatically add the **Reserve IP** policy to the security firewall clients. • **To specific SSID:** Selectively apply captive portal authentication to specific_SSIDs on an AP. • **Normal**: The selected clients have no policies applied to them. • **Reserve IP**: The client is allowed by IPv4 address to connect to the site. This is the default policy. Select this to reserve/freeze the assigned dynamic IPv4 address to the client device. The security router client will be added to the **Static DHCP table** in the **Site-wide** > **Configure** > **Security router** > **Interface** > **LAN interface configuration**. The security firewall client will be added to the **Static DHCP table** in the **Site-wide** > **Configure** > **Firewall** > **Interface** > **LAN interface configuration**. Note: Removing the default **Reserve IP** policy will automatically show **Normal**.
All / Wireless / Wired	Select the type of clients that have been online during the selected time period. • **All:** Click this to show all clients that have been online during the selected time period. • **Wireless**: Click this to show all WiFi clients that have been online during the selected time period. • **Wired**: Click this to show all wired clients that have been online during the selected time period.
Search clients	Specify your desired filter criteria to filter the list of clients (**Status**, **Manufacturer**, **Connected to**, **Band** (for **All**, **Access point clients**, and **Security router clients**), **VLAN**, **Policy**).
N clients	This shows the number of clients (N) connected to the gateway in the site network.
Show Nebula devices as clients	This allows you to show or hide the client Nebula Device(s) in the **Client list** table (for **All** clients only). By default, this switch is ON for the sites created before the NCC 18.00 release. Otherwise, this switch is OFF for the sites created after the NCC 18.00 release.
Export	Click this button to save the client list as a CSV or XML file to your computer.
General fields Note: A ‘–’ (dash) will show on the field with no value.	
	Select an entry’s checkbox to select a specific client. Otherwise, select the checkbox in the table heading row to select all clients.
Status	This shows whether the client is online (green) or offline (red), and whether the client is wired or wireless. • Clients connected to an Access Point are reported as wireless. • Clients connected to a Switch or Security Appliance are reported as wired.

Table 28 Site-wide > Clients > Client list (continued)

LABEL	DESCRIPTION
Name	This shows the descriptive name of the client. By default, this is the client's MAC address. The client description can be obtained through the following: • User customized description • Hostname detected from client's LLDP (Link Layer Discovery Protocol) System Name • Hostname detected from the Nebula-managed access point • Hostname detected from the Nebula-managed Security Appliance. Click the name to display the individual client statistics. See wireless: Section 4.5.0.1 on page 261 and wired: Section 4.5.0.2 on page 264.
Connected to	This shows the name of the Nebula Device to which the client is connected in this site. Click the Nebula Device name to display the screen where you can view detailed information about the Nebula Device.
MAC address	This shows the MAC address of the non-WiFi7 client or the MLD MAC address of the WiFi7 client. Click the MAC address to display the individual client statistics. See wireless: Section 4.5.0.1 on page 261 and wired: Section 4.5.0.2 on page 264.
IPv4 address	This shows the IPv4 address of the client. By default, the field is blank. The client IPv4 address can be obtained through the following: • IPv4 address detected from client's LLDP (Link Layer Discovery Protocol) Management Address • IPv4 address detected from the Nebula-managed access point • IPv4 address detected from the Nebula-managed Security Appliance.
First seen	This shows the first date and time the client was discovered over the specified period of time.
Last seen	This shows the last date and time the client was discovered over the specified period of time.
Manufacturer	This shows the manufacturer of the client hardware.
Policy	This shows the security policy applied to the client.
Note	This shows additional information about the client.
User	This shows the name or the email address used to authenticate the wireless/wired clients.
Band	This shows whether the SSID use either 2.4 GHz band, 5 GHz band, or the 6 GHz band.
Capability	This shows the WiFi standards supported by the client or the supported standards currently being used by the client.
SSID name	This shows the name of the Access Point and Security Router's WiFi network to which the client is connected.
Security	This shows the encryption method used to connect to the Access Point or Security Router.
Association time	This shows the time the client first associated with the Nebula Device's WiFi network.
Authentication	This shows the authentication method used for this client.
Channel	This shows the channel number currently used by the WiFi interface.
Signal strength	This shows the RSSI (Received Signal Strength Indicator) of the client's WiFi connection, and an icon showing the signal strength. Icon default thresholds: • Green/5 blocks: signal is greater than –67 dBm, strong signal • Amber/4 blocks: signal –67 to –73 dBm, average signal • Amber/3 blocks: signal –74 to –80 dBm, below average signal • Red/2 blocks: signal is less than –80 dBm, weak signal
Port	This shows the port number of the Nebula Device the client is connected.
LLDP	This shows the LLDP (Link Layer Discovery Protocol) information received from the remote device.
VLAN	This shows the ID number of the VLAN to which the client belongs.

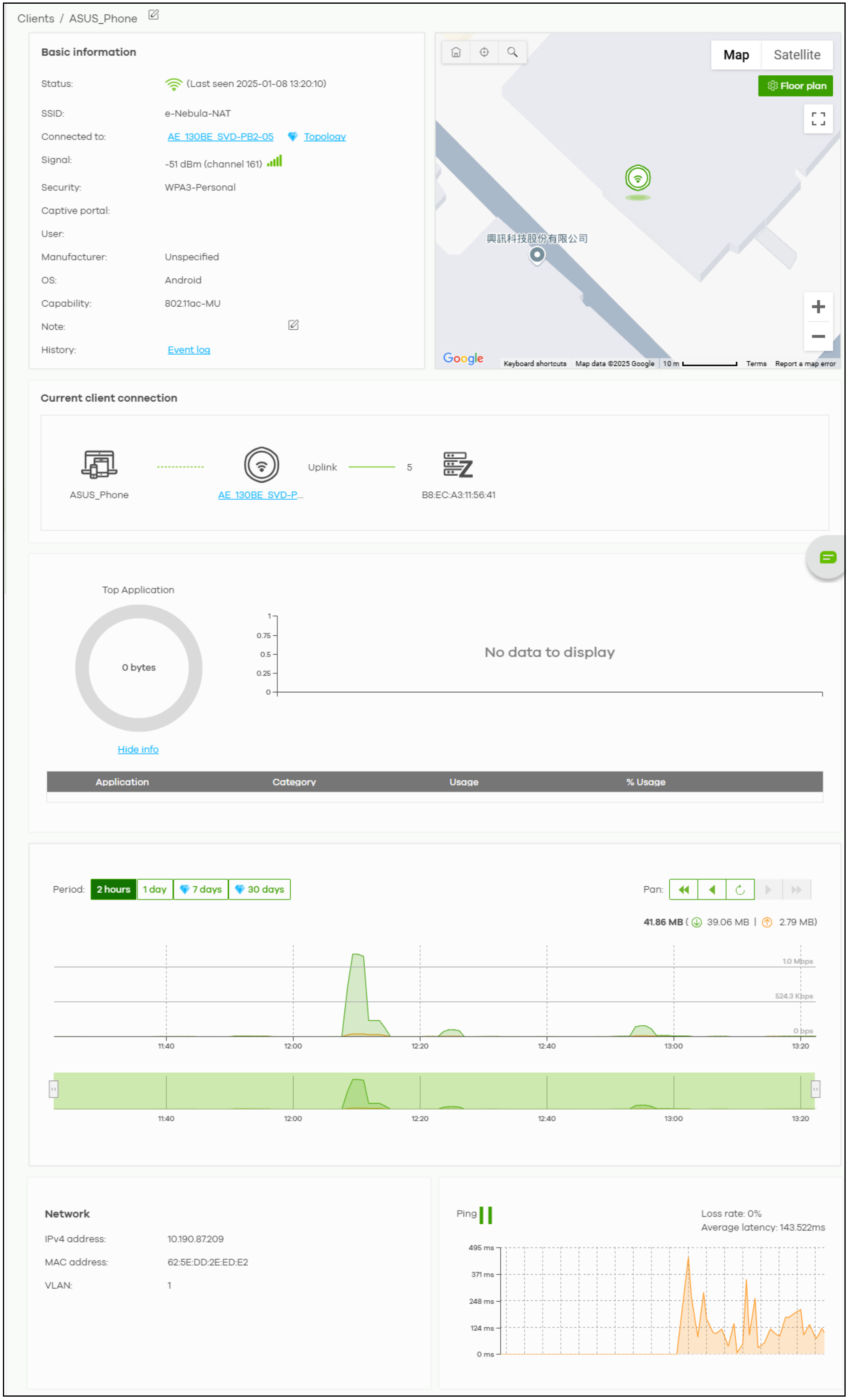
Table 28   Site-wide > Clients > Client list (continued)

LABEL	DESCRIPTION
OS	This shows the operating system running on the client device, if known.
Rx rate	This shows the maximum transmission rate of the client.
Download	This shows the amount of data received by the Nebula Device’s clients.
Upload	This shows the amount of data transmitted by the Nebula Device’s clients.
Usage	This shows the amount of data consumed by the Nebula Device’s clients.
Tx rate	This shows the maximum reception rate of the client.
☰	Click this icon to display a greater or lesser number of information about a specific client.

4.5.0.1 WiFi Client Details

Click a WiFi client entry in the **Site-wide** > **Clients** > **Clients list** screen to display individual client statistics.

Figure 56 Site-wide > Clients > Clients list: WiFi Client Details



Clients / ASUS_Phone

Basic information

Status:	(Last seen 2025-01-08 13:20:10)
SSID:	e-Nebula-NAT
Connected to:	AE_130BE_SVD-PB2-05 Topology
Signal:	-51 dBm (channel 161)
Security:	WPA3-Personal
Captive portal:	
User:	
Manufacturer:	Unspecified
OS:	Android
Capability:	802.11ac-MU
Note:	
History:	Event log

Current client connection

Top Application

No data to display

Hide info

Application	Category	Usage	% Usage

Period: 2 hours | 1 day | 7 days | 30 days

Pan:

41.86 MB (39.06 MB | 2.79 MB)

Network

IPv4 address:	10.190.87.209
MAC address:	62:5E:DD:2E:ED:E2
VLAN:	1

Ping

Loss rate: 0%
Average latency: 143.522ms

The following table describes the labels in this screen.

Table 29   Site-wide > Clients > Clients list: WiFi Client Details

LABEL	DESCRIPTION
Clients	Click the edit icon to change the client name.
Basic information	
Status	This shows whether the client is online (green), or goes offline (red). It also shows the last date and time the client was discovered.
SSID	This shows the name of the Access Point's WiFi network to which the client is connected.
Connected to	This shows the name of the Nebula managed Access Point to which the client is connected. Click the name to display the individual Access Point statistics. See Section 4.3.1.1 on page 218. Click **Topology** to go to the **Site-wide** > **Topology** screen. See Section 4.2 on page 208.
Signal	This shows the RSSI (Received Signal Strength Indicator) of the client's WiFi connection, and an icon showing the signal strength. Icon default thresholds: • Green/5 blocks: signal is greater than –67 dBm, strong signal • Amber/4 blocks: signal –67 to –73 dBm, average signal • Amber/3 blocks: signal –74 to –80 dBm, below average signal • Red/2 blocks: signal is less than –80 dBm, weak signal
Security	This shows the encryption method used to connect to the Access Point.
Captive portal	This shows the web authentication method used by the client to access the network.
User	This shows the number of users currently connected to the network through the client device.
Manufacturer	This shows the manufacturer of the device connected to the Access Point.
OS	This shows the operating system running on the client device, if known.
Capability	This shows the WiFi standards supported by the client or the supported standards currently being used by the client.
Note	This shows additional information for the client. Click the edit icon to change it.
History	Click **Event log** to go to the **Site-wide** > **Monitor** > **Access points** > **Event log** screen.
Map	This shows the location of the client on the Google map.
Current client connection	This shows the Nebula Device(s) currently connecting to the client.
Top Application	Click **Show info** to view the following fields. Alternatively, click **Hide info** to hide the following fields.
#	This shows the ranking of the application.
Application	This shows the application name.
Category	This shows the category of the application, for example email, file sharing.
Usage	This shows the amount of data consumed by the application.
% Usage	This shows the percentage of usage for the application.
Period	Select to view the statistics in the past two hours, day, week or month.
Pan	Click to move backward or forward by two hours or one day.
y-axis	The y-axis shows the transmission speed of data sent or received by the client in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Network	

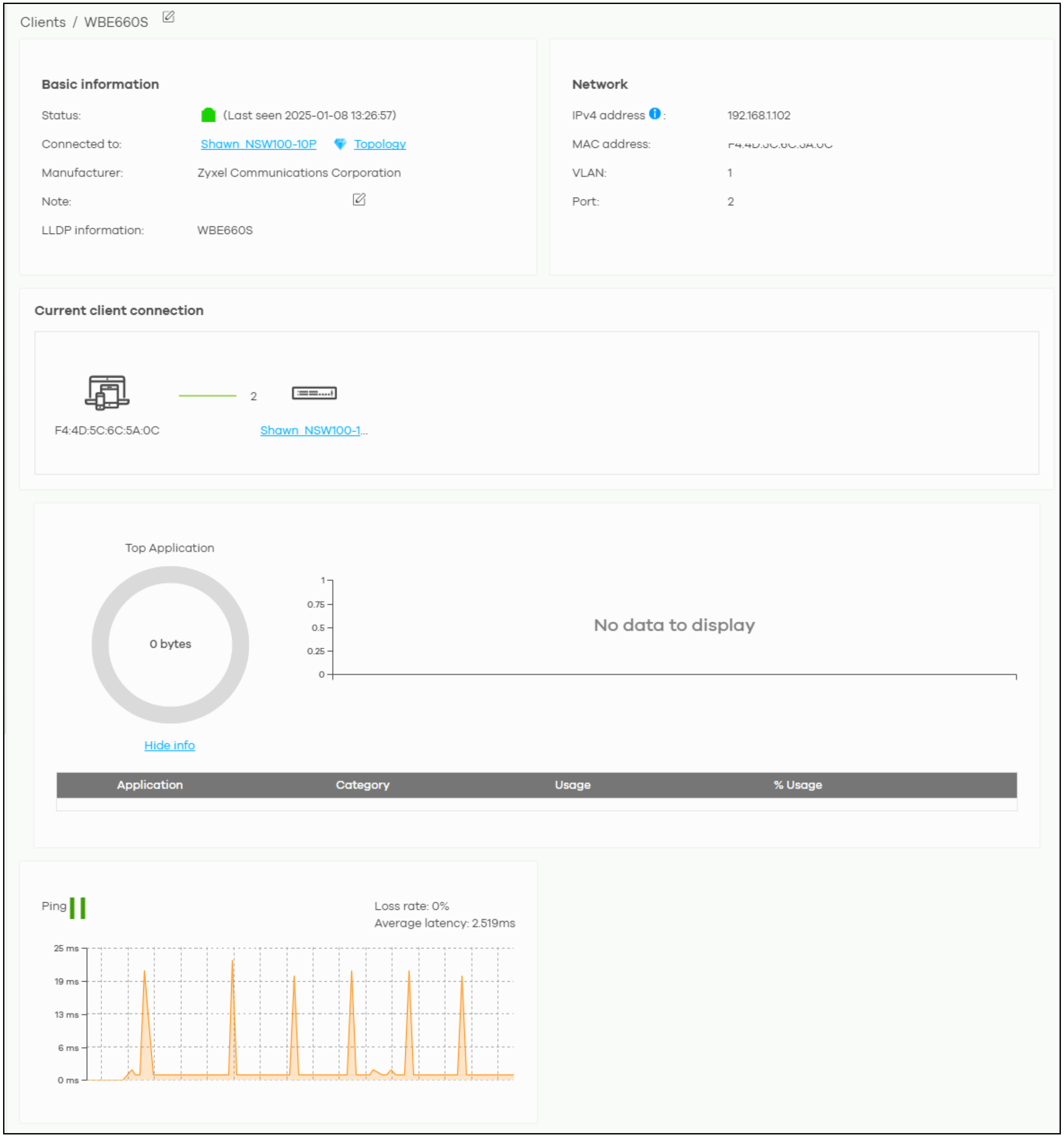
Table 29 Site-wide > Clients > Clients list: WiFi Client Details (continued)

LABEL	DESCRIPTION
IPv4 address	This shows the IP address of the client.
MAC address	This shows the MAC address of the client.
VLAN	This shows the ID number of the VLAN to which the client belongs.
Ping	Click the button to ping the client's IP address from the Nebula AP to test connectivity.
Loss rate	This shows the rate of packet loss when you perform ping.
Average latency	This shows the average latency in ms when you perform ping.

4.5.0.2 Wired Client Details

Click a wired client's descriptive name in the **Site-wide** > **Clients** > **Clients list** screen to display individual client statistics.

Figure 57 Site-wide > Clients > Clients list: Wired Client Details



Clients / WBE660S

Basic information

Status:	🟩 (Last seen 2025-01-08 13:26:57)
Connected to:	Shawn_NSW100-10P Topology
Manufacturer:	Zyxel Communications Corporation
Note:	
LLDP information:	WBE660S

Network

IPv4 address:	192.168.1.102
MAC address:	F4:4D:5C:6C:5A:0C
VLAN:	1
Port:	2

Current client connection

Application	Category	Usage	% Usage

Loss rate: 0%
Average latency: 2.519ms

The following table describes the labels in this screen.

Table 30 Site-wide > Clients > Clients list: Wired Client Details

LABEL	DESCRIPTION
Clients	Click the edit icon to change the client name.
Basic information	
Status	This shows whether the client is online (green) or offline (red). It also shows the last date and time the client was discovered, and whether the client is wired or wireless.

Table 30 Site-wide > Clients > Clients list: Wired Client Details (continued)

LABEL	DESCRIPTION
Connected to	This shows the name of the Security Appliance to which the client is connected. Click the Nebula Device name to display the screen where you can view detailed information about the Nebula Device. Click **Topology** to go to the **Site-wide** > **Topology** screen. See Section 4.2 on page 208.
User	This shows the number of users currently connected to the network through the client device.
Manufacturer	This shows the manufacturer of the client device.
OS	This shows the operating system running on the client device, if known.
Note	Enter information about this Nebula Device, for yourself or for other administrators.
History	Click **Event log** to go to the **Site-wide** > **Monitor** > **Access points** > **Event log** screen.
LLDP information	This shows the LLDP (Link Layer Discovery Protocol) information received from the remote device.
Network	
IPv4 address	This shows the IPv4 address of the client.
MAC address	This shows the MAC address of the client.
VLAN	This shows the VLAN ID for this client.
Interface	This shows the interface of the Nebula Device to which the client is connected.
Port	This shows the port number of the Nebula Device the client is connected.
Port forwarding	This shows the port forwarding rule configured for inbound traffic. Otherwise, it is **none**.
1:1 NAT IPs	This shows the local (LAN) IP address of the Nebula Device the client is connected.
Current client connection	This shows the Nebula Device(s) currently connecting to the client.
Top Application	Click **Show info** to view the following fields. Alternatively, click **Hide info** to hide the following fields.
#	This shows the ranking of the application.
Application	This shows the application name.
Category	This shows the category of the application, for example email, file sharing.
Usage	This shows the amount of data consumed by the application.
% Usage	This shows the percentage of usage for the application.
Move the cursor over the chart to see the transmission rate at a specific time.	
Zoom	Select to view the statistics in the past 2 hours, day, week, or month.
Pan	Click to move backward or forward by one day or week.
Ping	Click the button to ping the client's IP address from the gateway to test connectivity. Note: This button is grayed-out when client is not assigned an IP address.
Loss rate	This shows the rate of packet loss when you perform ping.
Average latency	This shows the average latency in ms when you perform ping.

4.5.1 WiFi Aid

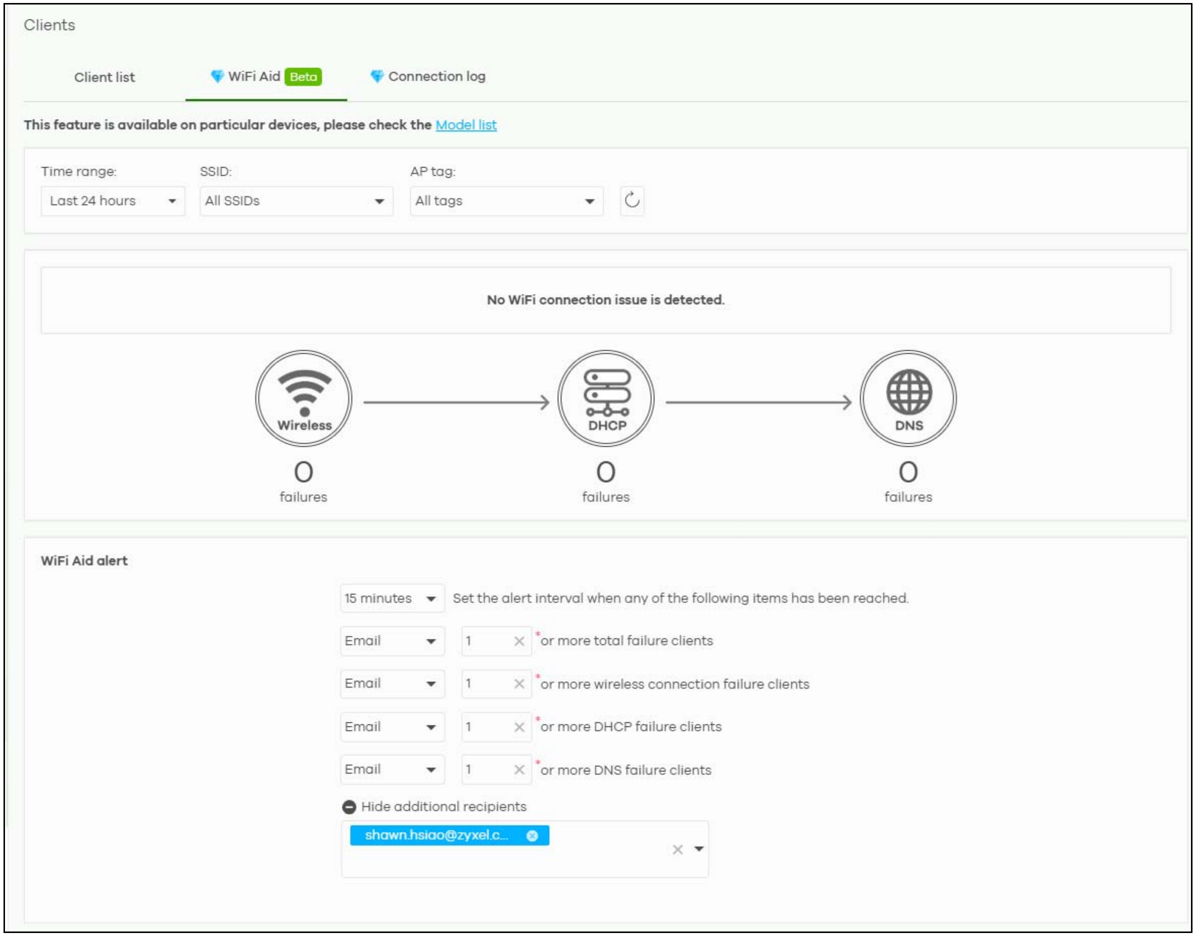
The **WiFi Aid** screen displays the number of WiFi clients that cannot connect to a Nebula Device(s) in a site. It also displays the number of WiFi clients who cannot authenticate with a Nebula Device acting as a hotspot (captive portal) or who have timed out.

Use this screen to identify connection problems between WiFi clients and supported Nebula Device(s). Click **Site-wide** > **Clients** > **WiFi Aid** to access this screen.

Note: This feature is only available if you have the Nebula Pro Pack license.

Note: After a WiFi client successfully connects to the Nebula Device, NCC erases past connection failures.

Figure 58 Site-wide > Clients > WiFi Aid



This feature is available on particular devices, please check the Model list

Time range: Last 24 hours

SSID: All SSIDs

AP tag: All tags

No WiFi connection issue is detected.

Wireless: 0 failures

DHCP: 0 failures

DNS: 0 failures

WiFi Aid alert

15 minutes Set the alert interval when any of the following items has been reached.

Email 1 *or more total failure clients

Email 1 *or more wireless connection failure clients

Email 1 *or more DHCP failure clients

Email 1 *or more DNS failure clients

Hide additional recipients

shawn.hsiao@zyxel.c...

The following table describes the labels in this screen.

Table 31 Site-wide > Clients > WiFi Aid

LABEL	DESCRIPTION
WiFi Aid	Select a **Time range**. The overview will show all WiFi clients' connection issues in the **Last hour**, **Last 12 hours**, **Last 24 hours**, or **Custom range** (from 15 minutes to one day). Select to filter the overview of the client's WiFi connection issues based on one AP WiFi network (**SSID**), or all AP WiFi networks in this site (**All SSIDs**, default). Select to filter the overview of all WiFi clients' connection issues based on one **AP tag**, or **All tags** (default). This is the tag you create in **Site-wide** > **Devices** > **Access points**. Click the Refresh icon to update this screen.
Client devices affected by connection problems	This chart displays the number of WiFi clients in this site with the following connection problems. • **Wireless** (**WiFi**) failures. This displays the number of WiFi clients that could not connect to the Nebula Device. – Make sure the WiFi client is within transmission range of the Nebula Device. – Make sure the WiFi client connects to the correct SSID and enters the correct password. – Make sure the WiFi adapter on the WiFi client is working properly. • **DHCP** failures. This displays the number of WiFi clients that failed to receive an IP address due to DHCP failure/timeout with the DHCP server. – Increase the number of IP addresses that the DHCP server can allocate. – Shorten the DHCP lease time that the WiFi client can use the assigned IP address. • **DNS** failures. This displays the number of WiFi clients that failed DNS query due to DNS timeout from a DNS server. – Make sure the DNS server is working properly. If the Nebula Device is acting as the DHCP server or DNS server in this site, check the settings. For a Security Router, see Section 7.3.1.2 on page 425 for more information. For a Security Firewall, see Section 8.3.3.2 on page 489 for more information. For a Security Gateway, see Section 9.3.1.1 on page 589 for more information. For a Mobile Router, see Section 10.4 on page 640 for more information.
Client devices affected by captive portal problems	This chart displays the number of WiFi clients that could not connect to the Nebula Device acting as a hotspot. This includes entering the wrong user credentials or an authentication timeout.
Failed clients	This table displays the number of WiFi clients with failed connection attempts (WiFi connection/DHCP failures/DNS failures) and the number of total connection attempts. The list displays the WiFi client with the most connection failures first, in descending order. Clicking the hyperlink in the **Client device** column will direct you to the **Site-wide** > **Monitor** > **Client**: **Client device** screen. See Section 4.5 on page 258 for more information on this screen. Clicking the numerator hyperlink in the **# Failed/total connections** column will direct you to the **Site-wide** > **Monitor** > **Connection log** screen. See Section 4.8 on page 274 for more information on this screen. The **Last failed issue** column displays the reason for the last connection failure.
Failed connection by SSID	This table displays the number of WiFi clients with WiFi connection/DHCP failures/DNS failures in each WiFi network. The list displays the WiFi network with the most connection failures first, in descending order. Clicking the hyperlink in the **# Failed connections** column will direct you to the **Site-wide** > **Monitor** > **Connection log** screen. See Section 4.8 on page 274 for more information on this screen.

Table 31 Site-wide > Clients > WiFi Aid (continued)

LABEL	DESCRIPTION
Captive portal login issues by client	This table displays the list of WiFi clients with the corresponding number of failed hotspot authentication or timeout. The list displays the WiFi client that could not connect to the Nebula Device acting as a hotspot the most number of times first, in descending order. Clicking the hyperlink in the **Client device** column will direct you to the **Site-wide** > **Clients** > **Client**: **Client device** screen. See Section 4.5 on page 258 for more information on this screen. Clicking the hyperlink in the **# Failed authentication** column will direct you to the **Site-wide** > **Monitor** > **Connection log** screen. See Section 4.8 on page 274 for more information on this screen.
Failed connection by AP	This table displays the number of WiFi clients with WiFi connection/DHCP failures/DNS failures to each Nebula Device. The list displays the Nebula Device with the most connection failures first, in descending order. Clicking the hyperlink in the **# Failed connection** column will direct you to the **Site-wide** > **Clients** > **Connection log** screen. See Section 4.8 on page 274 for more information on this screen.
WiFi Aid alert	Specify how long (15/30 minutes / 1 hour) the NCC waits before generating and sending an alert. Select the items to have the NCC generate and send an alert by email when the following events has reached the threshold (maximum 999): • WiFi clients with failed connection attempts (WiFi connection / DHCP failures / DNS failures). • WiFi clients with failed WiFi connection attempts. • WiFi clients with DHCP failures. • WiFi clients with DNS failures.

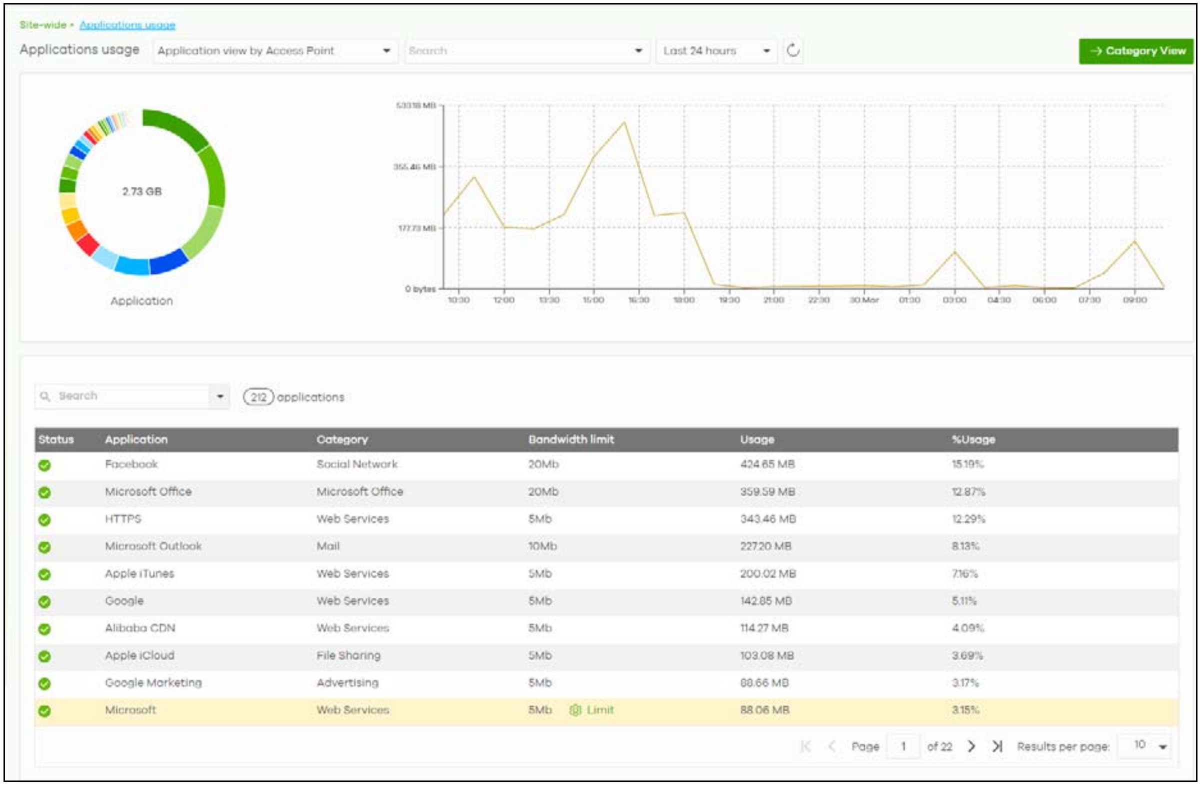
4.6 Applications Usage

This screen displays usage statistics for applications used in the site. An application can be a specific app or service (for example, Facebook) or a general protocol (for example, HTTP). You can also block or restrict bandwidth for applications at the gateway, and for multiple applications by category.

Click **Site-wide** > **Applications Usage** to access this screen.

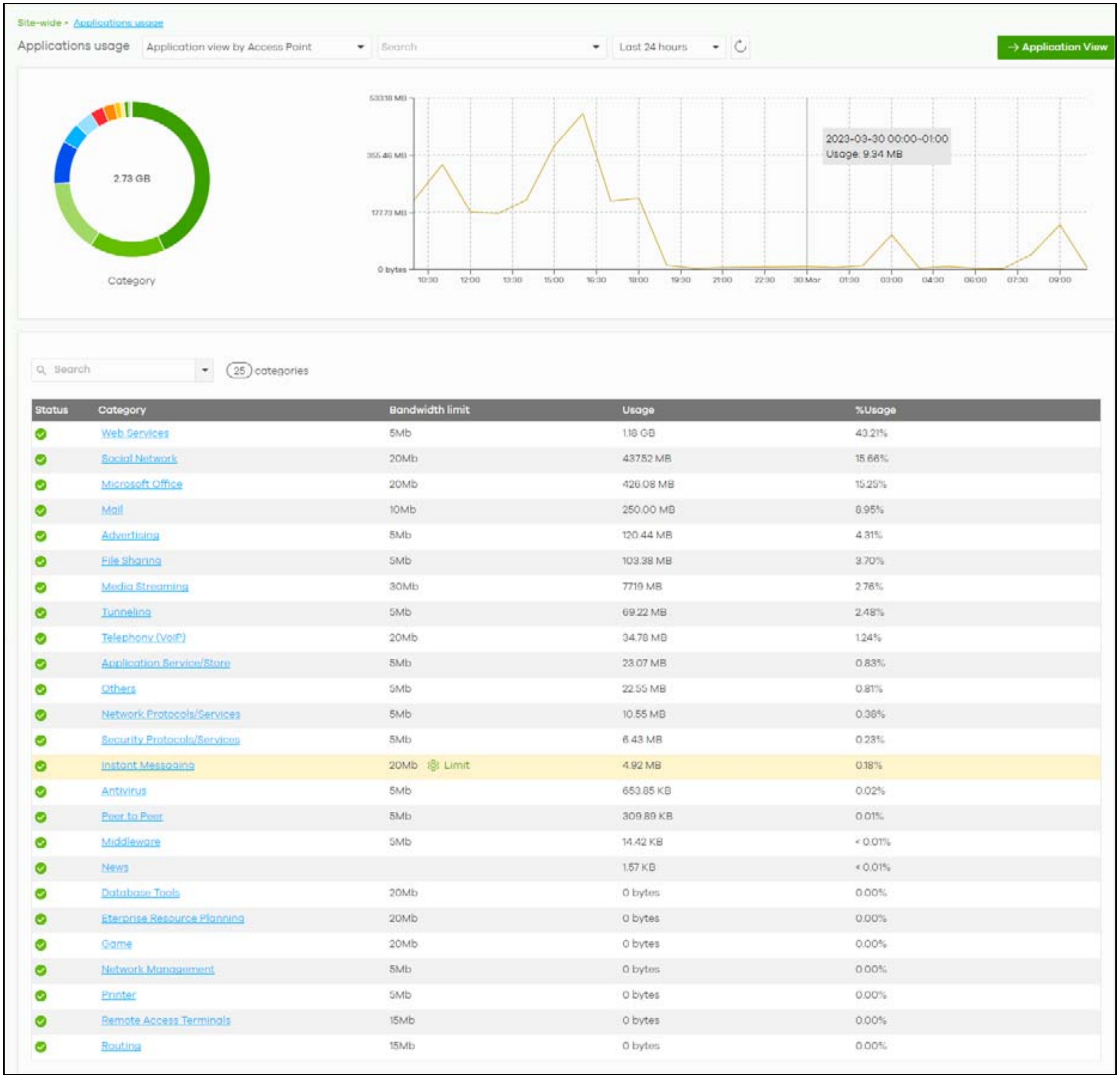
Note: You can view this screen by application or by category.

Figure 59 Site-wide > Applications usage: Application View



Status	Application	Category	Bandwidth limit	Usage	%Usage
✓	Facebook	Social Network	20Mb	424.65 MB	15.19%
✓	Microsoft Office	Microsoft Office	20Mb	359.59 MB	12.87%
✓	HTTPS	Web Services	5Mb	343.46 MB	12.29%
✓	Microsoft Outlook	Mail	10Mb	227.20 MB	8.13%
✓	Apple iTunes	Web Services	5Mb	200.02 MB	7.16%
✓	Google	Web Services	5Mb	142.85 MB	5.11%
✓	Alibaba CDN	Web Services	5Mb	114.27 MB	4.09%
✓	Apple iCloud	File Sharing	5Mb	103.08 MB	3.69%
✓	Google Marketing	Advertising	5Mb	88.66 MB	3.17%
✓	Microsoft	Web Services	5Mb Limit	88.06 MB	3.15%

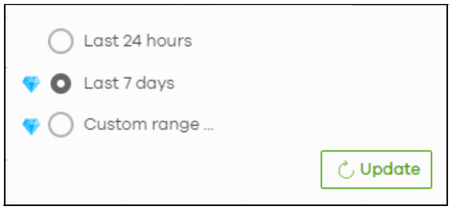
Figure 60 Site-wide > Applications usage: Category View



Status	Category	Bandwidth limit	Usage	%Usage
✓	Web Services	5Mb	1.18 GB	43.21%
✓	Social Network	20Mb	437.52 MB	15.66%
✓	Microsoft Office	20Mb	426.08 MB	15.25%
✓	Mail	10Mb	250.00 MB	8.95%
✓	Advertising	5Mb	120.44 MB	4.31%
✓	File Sharing	5Mb	103.38 MB	3.70%
✓	Media Streaming	30Mb	77.19 MB	2.76%
✓	Tunneling	5Mb	69.22 MB	2.48%
✓	Telephony (VoIP)	20Mb	34.78 MB	1.24%
✓	Application Service/Store	5Mb	23.07 MB	0.83%
✓	Others	5Mb	22.55 MB	0.81%
✓	Network Protocols/Services	5Mb	10.55 MB	0.38%
✓	Security Protocols/Services	5Mb	6.43 MB	0.23%
✓	Instant Messaging	20Mb Limit	4.92 MB	0.18%
✓	Antivirus	5Mb	653.85 KB	0.02%
✓	Peer to Peer	5Mb	309.89 KB	0.01%
✓	Middleware	5Mb	14.42 KB	< 0.01%
✓	News		1.57 KB	< 0.01%
✓	Database Tools	20Mb	0 bytes	0.00%
✓	Eterprise Resource Planning	20Mb	0 bytes	0.00%
✓	Game	20Mb	0 bytes	0.00%
✓	Network Management	5Mb	0 bytes	0.00%
✓	Printer	5Mb	0 bytes	0.00%
✓	Remote Access Terminals	15Mb	0 bytes	0.00%
✓	Routing	15Mb	0 bytes	0.00%

The following table describes the labels in this screen.

Table 32 Site-wide > Applications usage

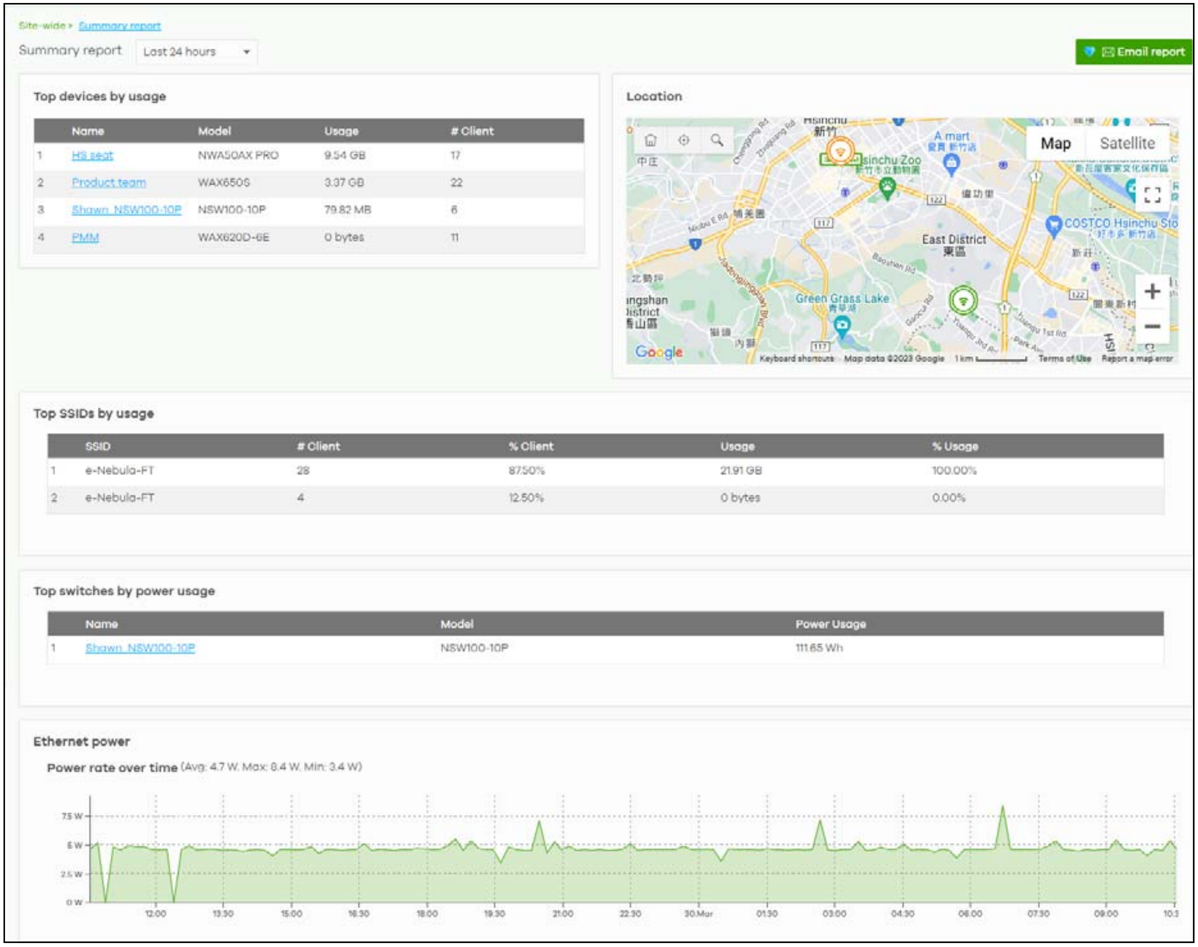
LABEL	DESCRIPTION
Applications	In Application view, select to view all applications of Nebula Security Appliances / Nebula Access Points, or only applications with bandwidth or block policies applied to Nebula Security Appliances. In Category view, select to view all applications of Nebula Security Appliances / Nebula Access Points only. Select to view the report for the past day or week. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ● Last 7 days ○ Custom range ... Update
↻	Click this button to reload the data-related frames on this page.
Category View / Application View	Click this button to view statistics by application or category.
y-axis	The y-axis shows the total amount of data used by applications or categories in the site.
x-axis	The x-axis shows the time period over which the data usage occurred.
Keyword	Enter a keyword to filter the list of log entries.
N applications/ categories	This shows the number of applications/categories (N) in the list.
Application/Category-View Fields	
Status	This shows whether the application or category is blocked or allowed within the current site.
Application	This shows the application name.
Category	This shows the name of the category to which the application belongs. Note: Click this field in Category view to see all applications in the category.
Bandwidth limit	This shows the bandwidth restriction policy for the application.
Usage	This shows the amount of data consumed by the application, or all applications in the category.
% Usage	This shows the percentage of usage for the application or category.
Limit	Click this to limit the bandwidth for the application on the site's gateway. You can apply the restrictions per gateway interface, or for all interfaces.

4.7 Summary Report

Use this screen to view statistics for the Nebula Devices and networks in the selected site.

Click **Site-wide** > **Summary report** to access this screen.

Figure 61 Site-wide > Summary report



Site-wide > Summary report

Summary report: Last 24 hours

Top devices by usage

	Name	Model	Usage	# Client
1	HS seat	NWA50AX PRO	9.54 GB	17
2	Product team	WAX650S	3.37 GB	22
3	Shawn_NSW100-10P	NSW100-10P	79.82 MB	6
4	PMM	WAX620D-6E	0 bytes	11

Top SSIDs by usage

	SSID	# Client	% Client	Usage	% Usage
1	e-Nebula-FT	28	87.50%	21.91 GB	100.00%
2	e-Nebula-FT	4	12.50%	0 bytes	0.00%

Top switches by power usage

	Name	Model	Power Usage
1	Shawn_NSW100-10P	NSW100-10P	111.65 Wh

Ethernet power

Power rate over time (Avg: 4.7 W, Max: 8.4 W, Min: 3.4 W)

The following table describes the labels in this screen.

Table 33 Site-wide > Summary report

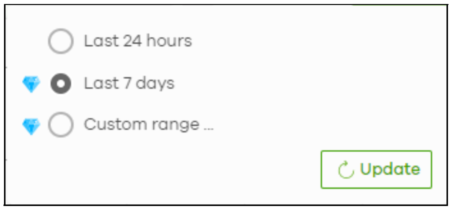
LABEL	DESCRIPTION
Summary report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ● Last 7 days ○ Custom range ... Update
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
Top devices by usage Note: The Security Firewall(s) in Cloud Monitoring mode will not show here.	
	This shows the index number of the Nebula Device.
Name	This shows the descriptive name of the Nebula Device. You can click the name to view the Nebula Device details.

Table 33 Site-wide > Summary report (continued)

LABEL	DESCRIPTION
Model	This shows the model number of the Nebula Device.
Usage	This shows the amount of data that has been transmitted by or through the Nebula Device.
Client	This shows the number of clients currently connected to the Nebula Device.
Location This shows the location of the site's gateway device on the map. Note: The Security Firewall(s) in Cloud Monitoring mode will not show here.	
Top SSIDs by usage	
#	This shows the ranking of the SSID.
SSID	This shows the SSID network name.
Encryption	This shows the encryption method use by the SSID network.
# Client	This shows how many WiFi clients are connecting to this SSID.
% Client	This shows what percentage of associated WiFi clients are connecting to this SSID.
Usage	This shows the total amount of data transmitted or received by clients connecting to this SSID.
% Usage	This shows the percentage of usage for the clients connecting to this SSID.
Top switches by power usage	
#	This shows the ranking of the Nebula Switch.
Name	This shows the descriptive name of the Nebula Switch.
Model	This shows the model number of the Nebula Switch.
Power Usage	This shows the total amount of power consumed by the Nebula Switch's connected PoE devices during the specified period of time.
Ethernet power	This graph shows power used by all PoE Switch ports in the site within the specified time, in Watts.
Avg	This shows the average power consumption for all Switch ports.
Max	This shows the maximum power consumption of the Switch ports.
Min	This shows the minimum power consumption of the Switch ports.
y-axis	The y-axis shows how much power is used by all Switches in the site, in Watts.
x-axis	The x-axis shows the time period over which power consumption is recorded.

4.8 Monitor

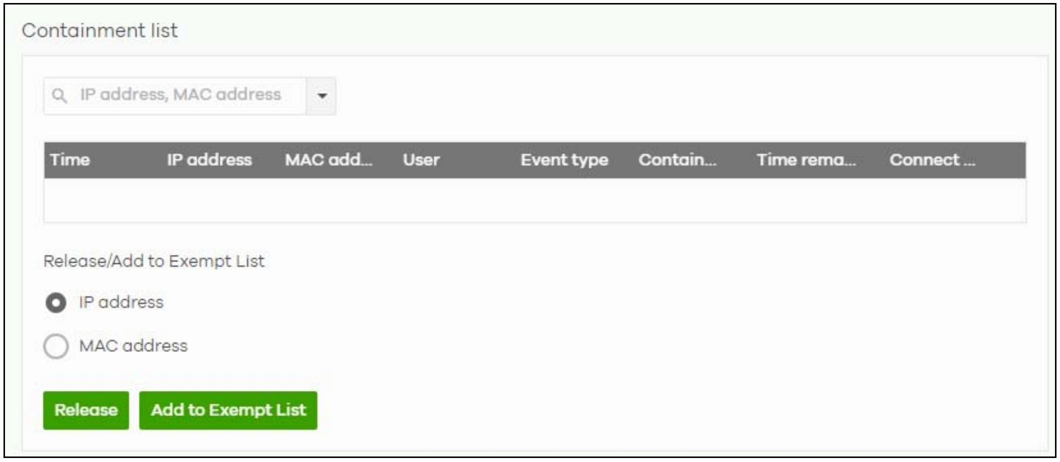
Use the **Monitor** menus to check the site features logs and containment list of the Nebula Devices for the selected site. Please click the following links to go to the respective Nebula Devices **Monitor** menus.

- Access points (Section 5.2 on page 305)
- Switches (Section 6.2 on page 349)
- Security router (Section 7.2 on page 415)
- Mobile router (Section 10.4 on page 640)
- Firewall (Section 8.2 on page 466)
- Security gateway (Section 9.2 on page 576)

4.8.1 Containment List

This screen shows a list of clients that are currently blocked in the site by the CDR security service. You can use this screen to release blocked clients. Click **Site-wide** > **Monitor** > **Containment list** to access this screen.

Figure 62 Site-wide > Monitor > Containment list



Containment list

IP address, MAC address

Time	IP address	MAC add...	User	Event type	Contain...	Time rema...	Connect ...

Release/Add to Exempt List

● IP address

○ MAC address

The following table describes the labels in this screen.

Table 34 Site-wide > Monitor > Containment list

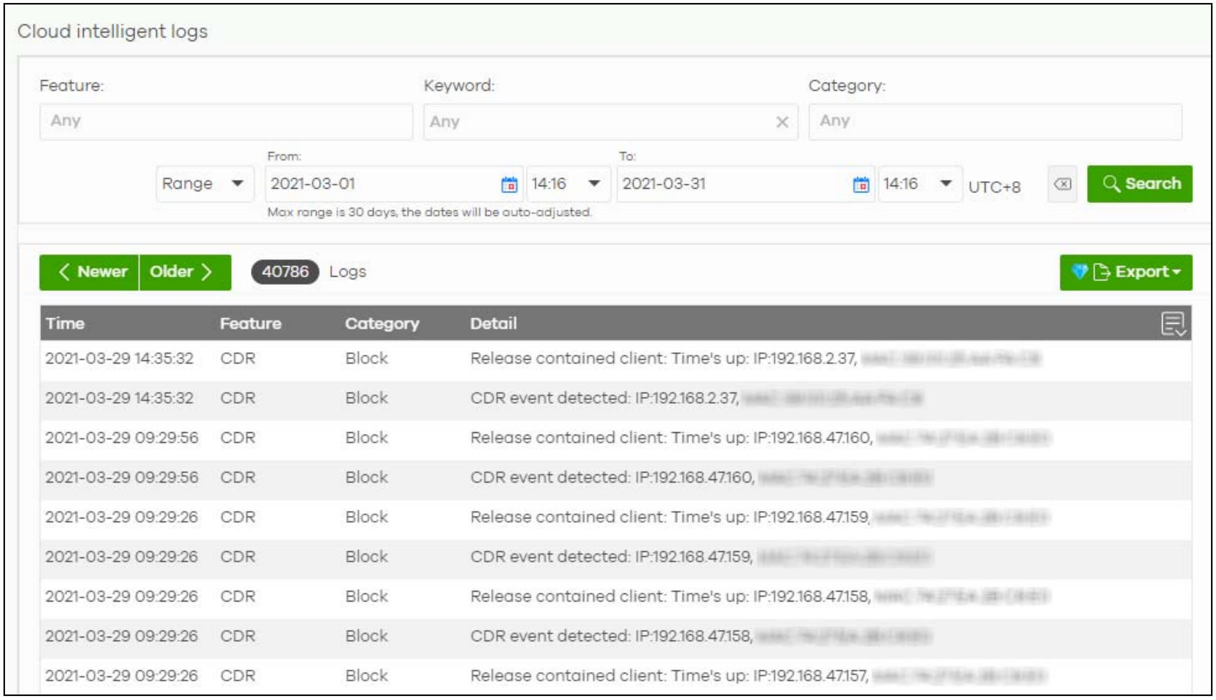
LABEL	DESCRIPTION
Search	Enter a MAC or IP address to filter the list of clients.
Time	This field displays the date and time CDR contained this client.
IP address	This field displays the IPv4 address of the client contained by CDR.
MAC address	This field displays the MAC address of the client contained by CDR.
User	This field displays the user name of a client contained by CDR who has been authenticated for Internet access. The field is blank if user authentication is not required.
Event type	This field displays details on the category of signature that triggered CDR: Web Filtering, Anti-Malware or IPS (IDP).
Containment	This field displays if the client is blocked, quarantined or just triggers an alert.
Time Remaining (mins.)	This field displays the amount of time left until this client is released by CDR.
Connect to	This field displays the description of the Access Point or the interface of the Nebula Device that the contained client is connected to.
Release/Add to Exempt List	
Release	Select a client and then click this to release this client device from CDR containment.
Add to Exempt List	Select a client, select an IPv4 address or MAC address, and then click **OK** to release this client device from CDR containment. This client device's IP or MAC address is exempt from future CDR checking.

4.8.2 Site Features Logs

This screen displays events from the Security Appliance within the selected site, such as CDR service events, alerts, and firmware management.

Click **Site-wide** > **Monitor** > **Site features logs** to access this screen.

Figure 63 Site-wide > Monitor > Site features logs



Time	Feature	Category	Detail
2021-03-29 14:35:32	CDR	Block	Release contained client: Time's up: IP:192.168.2.37, [redacted]
2021-03-29 14:35:32	CDR	Block	CDR event detected: IP:192.168.2.37, [redacted]
2021-03-29 09:29:56	CDR	Block	Release contained client: Time's up: IP:192.168.47.160, [redacted]
2021-03-29 09:29:56	CDR	Block	CDR event detected: IP:192.168.47.160, [redacted]
2021-03-29 09:29:26	CDR	Block	Release contained client: Time's up: IP:192.168.47.159, [redacted]
2021-03-29 09:29:26	CDR	Block	CDR event detected: IP:192.168.47.159, [redacted]
2021-03-29 09:29:26	CDR	Block	Release contained client: Time's up: IP:192.168.47.158, [redacted]
2021-03-29 09:29:26	CDR	Block	CDR event detected: IP:192.168.47.158, [redacted]
2021-03-29 09:29:26	CDR	Block	Release contained client: Time's up: IP:192.168.47.157, [redacted]

The following table describes the labels in this screen.

Table 35 Site-wide > Monitor > Site features logs

LABEL	DESCRIPTION
Feature	Select the features that you want to view logs for.
Keyword	Enter a keyword to filter the list of log entries.
Category	Select the type of log messages you want to view. The available categories will depend on the features you have selected under **Feature**.
Range/Before	Select filtering options, set a date, and then click **Search** to filter log entries by date. **Range**: Display log entries from the first specified date to the second specified date. **Before**: Display log entries from the beginning of the log to the selected date.
Reset filters ⌫	Click this to return the search criteria to the previously saved time setting.
Search	Click this to update the list of logs based on the search criteria.
Newer/Older	Click to sort the log messages by most recent or oldest.
N Logs	This shows the number of log messages (N) in the list.
Export	Click this button to download the log list as a CSV or XML file to your computer.
Time	This shows the date and time when the log was recorded. It uses the local time set for the site at **Site-wide** > **Configure** > **Site settings**.
Feature	Select the feature that created the log message.
Category	This shows the type of log message, for example “Block”. The available categories will depend on the feature.

Table 35 Site-wide > Monitor > Site features logs (continued)

LABEL	DESCRIPTION
Detail	This shows the details of the event. Note: Click the Nebula Device name link for an Auto configuration recovery alert to go to **Site-wide** > **Devices** > **Switches: Switch Details** screen for more information.
▤	Click this icon to display a greater or lesser number of configuration fields.

4.9 Configure

Use the **Configure** menus to set the WiFi security settings for Nebula Devices of the selected site. Please click the following links to go to the respective Nebula Devices **Configure** menus.

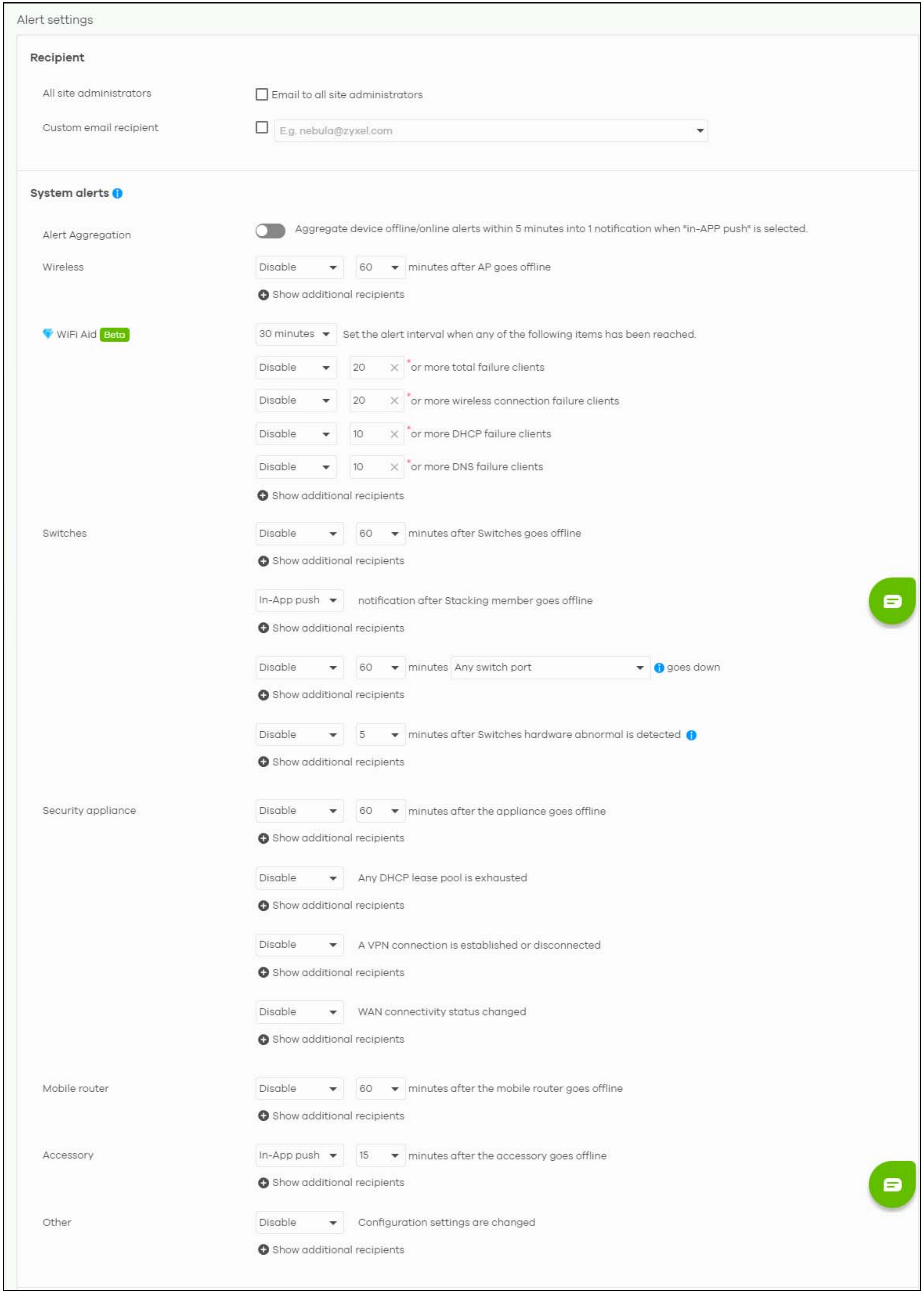
- Access points (Section 5.3 on page 317)
- Switches (Section 6.3 on page 362)
- Security router (Section 7.3 on page 420)
- Mobile router (Section 10.2 on page 632)
- Firewall (Section 8.3 on page 474)
- Security gateway (Section 9.3 on page 584)

4.9.1 Alert Settings

Use this screen to set which alerts and reports are created and emailed. You can also set the email addresses to which an alert is sent. Click **Site-wide** > **Configure** > **Alert settings** to access this screen.

Note: NCC's Smart Alert Engine uses knowledge of network topology and cross-device functionality to only generate alerts for unexpected events. This helps avoids unnecessary emails and notifications.
For example, an Access Point is receiving power from a PoE switch. If the Access Point loses power because its Ethernet cable is disconnected, NCC generates an alert. If the Access Point loses power because the Switch has a PoE schedule that disables power to the Access Point, NCC does not generate an alert.

Figure 64 Site-wide > Configure > Alert settings



Alert settings

Recipient

All site administrators □ Email to all site administrators

Custom email recipient □ E.g. nebula@zyxel.com

System alerts

Alert Aggregation ○ Aggregate device offline/online alerts within 5 minutes into 1 notification when "in-APP push" is selected.

Wireless: Disable 60 minutes after AP goes offline
Show additional recipients

WiFi Aid Beta: 30 minutes Set the alert interval when any of the following items has been reached.
Disable 20 * or more total failure clients
Disable 20 * or more wireless connection failure clients
Disable 10 * or more DHCP failure clients
Disable 10 * or more DNS failure clients
Show additional recipients

Switches: Disable 60 minutes after Switches goes offline
Show additional recipients

In-App push notification after Stacking member goes offline
Show additional recipients

Disable 60 minutes Any switch port goes down
Show additional recipients

Disable 5 minutes after Switches hardware abnormal is detected
Show additional recipients

Security appliance: Disable 60 minutes after the appliance goes offline
Show additional recipients

Disable Any DHCP lease pool is exhausted
Show additional recipients

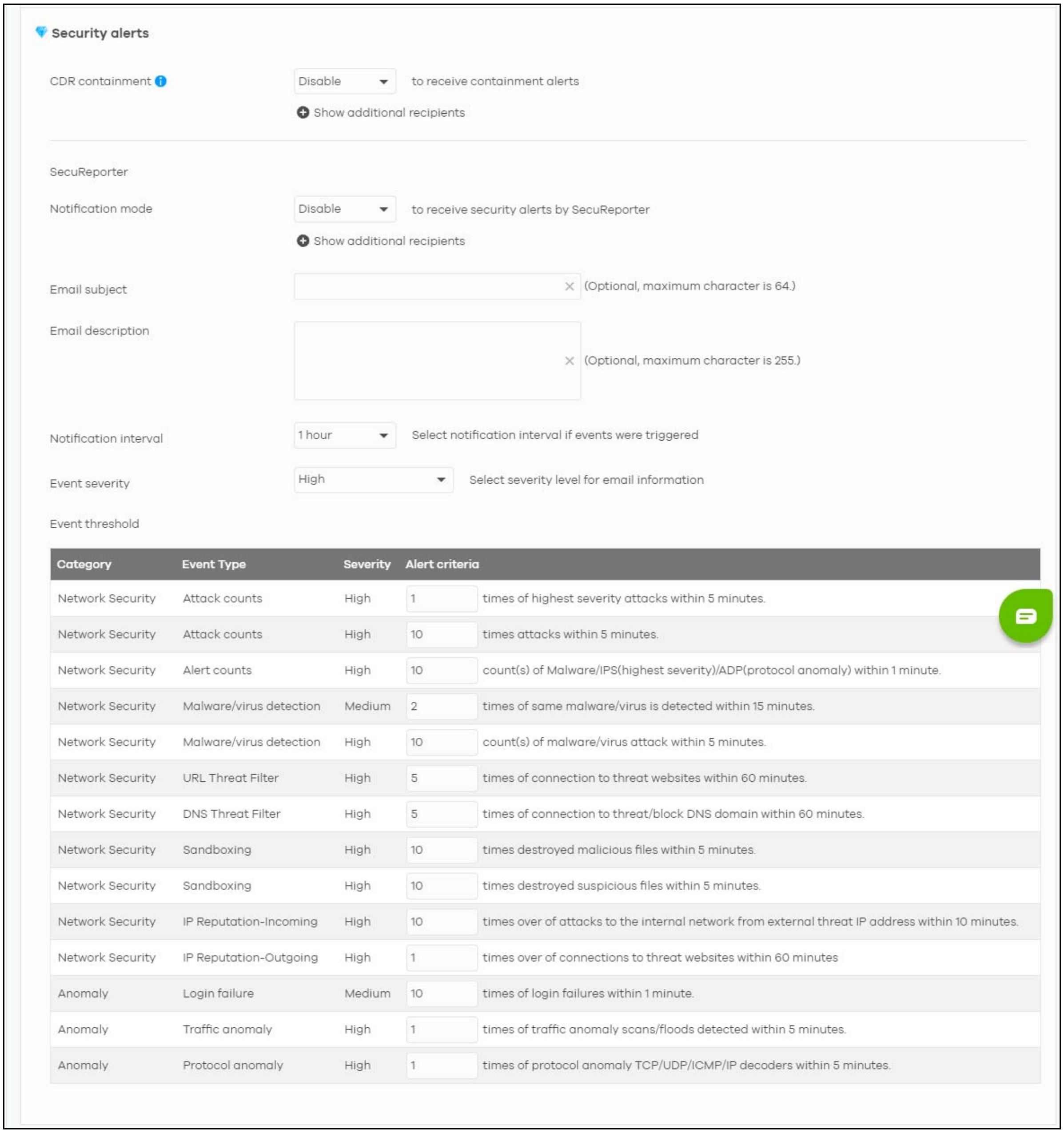
Disable A VPN connection is established or disconnected
Show additional recipients

Disable WAN connectivity status changed
Show additional recipients

Mobile router: Disable 60 minutes after the mobile router goes offline
Show additional recipients

Accessory: In-App push 15 minutes after the accessory goes offline
Show additional recipients

Other: Disable Configuration settings are changed
Show additional recipients



Security alerts

CDR containment — Disable ▾ to receive containment alerts

⊕ Show additional recipients

SecuReporter

Notification mode — Disable ▾ to receive security alerts by SecuReporter

⊕ Show additional recipients

Email subject — × (Optional, maximum character is 64.)

Email description — × (Optional, maximum character is 255.)

Notification interval — 1 hour ▾ Select notification interval if events were triggered

Event severity — High ▾ Select severity level for email information

Event threshold

Category	Event Type	Severity	Alert criteria	
Network Security	Attack counts	High	1	times of highest severity attacks within 5 minutes.
Network Security	Attack counts	High	10	times attacks within 5 minutes.
Network Security	Alert counts	High	10	count(s) of Malware/IPS(highest severity)/ADP(protocol anomaly) within 1 minute.
Network Security	Malware/virus detection	Medium	2	times of same malware/virus is detected within 15 minutes.
Network Security	Malware/virus detection	High	10	count(s) of malware/virus attack within 5 minutes.
Network Security	URL Threat Filter	High	5	times of connection to threat websites within 60 minutes.
Network Security	DNS Threat Filter	High	5	times of connection to threat/block DNS domain within 60 minutes.
Network Security	Sandboxing	High	10	times destroyed malicious files within 5 minutes.
Network Security	Sandboxing	High	10	times destroyed suspicious files within 5 minutes.
Network Security	IP Reputation-Incoming	High	10	times over of attacks to the internal network from external threat IP address within 10 minutes.
Network Security	IP Reputation-Outgoing	High	1	times over of connections to threat websites within 60 minutes
Anomaly	Login failure	Medium	10	times of login failures within 1 minute.
Anomaly	Traffic anomaly	High	1	times of traffic anomaly scans/floods detected within 5 minutes.
Anomaly	Protocol anomaly	High	1	times of protocol anomaly TCP/UDP/ICMP/IP decoders within 5 minutes.

The following table describes the labels in this screen.

Table 36 Site-wide > Configure > Alert settings

LABEL	DESCRIPTION
Recipient	
All site administrators	Select this to send alerts by email to all site administrators for the current site.
Custom email recipient	Enter the email addresses to which you want to send alerts.
System alerts	
Alert Aggregation	Alert aggregation combines offline/online alerts within a 5 minutes time frame into a single alert notification when **In-app push** in the notification type is selected.

Table 36 Site-wide > Configure > Alert settings (continued)

LABEL	DESCRIPTION
Wireless	Specify how long in minutes (5/10/15/30/60) the NCC waits before generating and sending an alert when an AP becomes offline. For each alert, you can set how to receive alert notifications: • **Email**: Alert notifications are sent by email to configured administrators, custom email recipients, and additional recipients. • **In-app push**: Alert notifications are sent to site administrators who are logged into the Nebula Mobile app. This type of notification is not available for some features. • **Both**: Alert notifications are sent by email and app notification. • **Disable**: No alerts are sent.
Show additional recipients	Depending on your configuration on the notification type, add additional user accounts who will receive email notifications for the alert.
Hide additional recipients	Do not show the additional user accounts who will receive email and/or in-app notifications for the alert.
WiFi Aid	Specify how long (15/30 minutes / 1 hour) the NCC waits before generating and sending an alert. Select the items to have the NCC generate and send an alert by email when the following events has reached the threshold (maximum 999): • WiFi clients with failed connection attempts (WiFi connection / DHCP failures / DNS failures). • WiFi clients with failed WiFi connection attempts. • WiFi clients with DHCP failures. • WiFi clients with DNS failures. For each alert, you can set to receive alert notifications through email: • **Email**: Alert notifications are sent by email to configured administrators, custom email recipients, and additional recipients. • **Disable**: No alerts are sent.
Show additional recipients	Depending on your configuration on the notification type, add additional user accounts who will receive email notifications for the alert.
Hide additional recipients	Do not show the additional user accounts who will receive email and/or in-app notifications for the alert.
Switches	Specify how long in minutes (5/10/15/30/60) the NCC waits before generating and sending an alert when a port or a Switch or a stacking member goes offline, when the Switch temperature rises above the threshold, or the fan is functioning above the normal speed. For each alert, you can set how to receive alert notifications: • **Email**: Alert notifications are sent by email to configured administrators, custom email recipients, and additional recipients. • **In-app push**: Alert notifications are sent to site administrators who are logged into the Nebula Mobile app. This type of notification is not available for some features. • **Both**: Alert notifications are sent by email and app notification. • **Disable**: No alerts are sent.
Show additional recipients	Depending on your configuration on the notification type, add additional user accounts who will receive email notifications for the alert.
Hide additional recipients	Do not show the additional user accounts who will receive email and/or in-app notifications for the alert.

Table 36 Site-wide > Configure > Alert settings (continued)

LABEL	DESCRIPTION
Security Appliance	Specify how long in minutes (5/10/15/30/60) the NCC waits before generating and sending an alert when a Security Appliance goes offline, there are more requests for IP addresses than what is available in the pool, a VPN connection is established or disconnected, or the WAN connection status has changed. For each alert, you can set how to receive alert notifications: • **Email**: Alert notifications are sent by email to configured administrators, custom email recipients, and additional recipients. • **In-app push**: Alert notifications are sent to site administrators who are logged into the Nebula Mobile app. This type of notification is not available for some features. • **Both**: Alert notifications are sent by email and app notification. • **Disable**: No alerts are sent.
Show additional recipients	Depending on your configuration on the notification type, add additional user accounts who will receive email notifications for the alert.
Hide additional recipients	Do not show the additional user accounts who will receive email and/or in-app notifications for the alert.
Mobile router / Accessory	Specify how long in minutes (5/10/15/30/60) the NCC waits before generating and sending an alert when a mobile router / accessory goes offline. For each alert, you can set how to receive alert notifications: • **Email**: Alert notifications are sent by email to configured administrators, custom email recipients, and additional recipients. • **In-app push**: Alert notifications are sent to site administrators who are logged into the Nebula Mobile app. This type of notification is not available for some features. • **Both**: Alert notifications are sent by email and app notification. • **Disable**: No alerts are sent.
Show additional recipients	Depending on your configuration on the notification type, add additional user accounts who will receive email notifications for the alert.
Hide additional recipients	Do not show the additional user accounts who will receive email and/or in-app notifications for the alert.
Other	Specify whether to send an alert each time configuration settings are changed.
Show additional recipients	Depending on your configuration on the notification type, add additional user accounts who will receive email notifications for the alert.
Hide additional recipients	Do not show the additional user accounts who will receive email and/or in-app notifications for the alert.
Security alerts	
CDR containment	Specify whether to send an email alert each time a CDR block or containment action is triggered.
Show additional recipients	Add additional user accounts who will receive email notifications for the alert.
Hide additional recipients	Do not show the additional user accounts who will receive email notifications for the alert.
SecuReporter	
Notification mode	For each alert, you can set how to receive alert notifications: • **Email**: Alert notifications are sent by email to configured administrators, custom email recipients, and additional recipients. • **In-app push**: Alert notifications are sent to site administrators who are logged into the Nebula Mobile app. This type of notification is not available for some features. • **Both**: Alert notifications are sent by email and app notification. • **Disable**: No alerts are sent.
Show additional recipients	Add additional user accounts who will receive email and in-app notifications for the alert.

Table 36 Site-wide > Configure > Alert settings (continued)

LABEL	DESCRIPTION
Hide additional recipients	Do not show the additional user accounts who will receive email and/or in-app notifications for the alert.
Email subject	Enter an email title here.
Email description	Enter a description of the emails to be sent here. For example, maybe these emails are just for high severity events.
Notification interval	Specify how often to receive a SecuReporter report. If no security events were triggered, SecuReporter will not send a report.
Event severity	Select the severity level of events that will be included in each report.
Event threshold	This table lists the events that trigger SecuReporter security alerts. You can set the alert threshold. For example, X count(s) of malware/virus attack within 5 minutes means SecuReporter includes a report in the email if the total number of combined malware and virus detection events exceed X within a 5 minute time period.

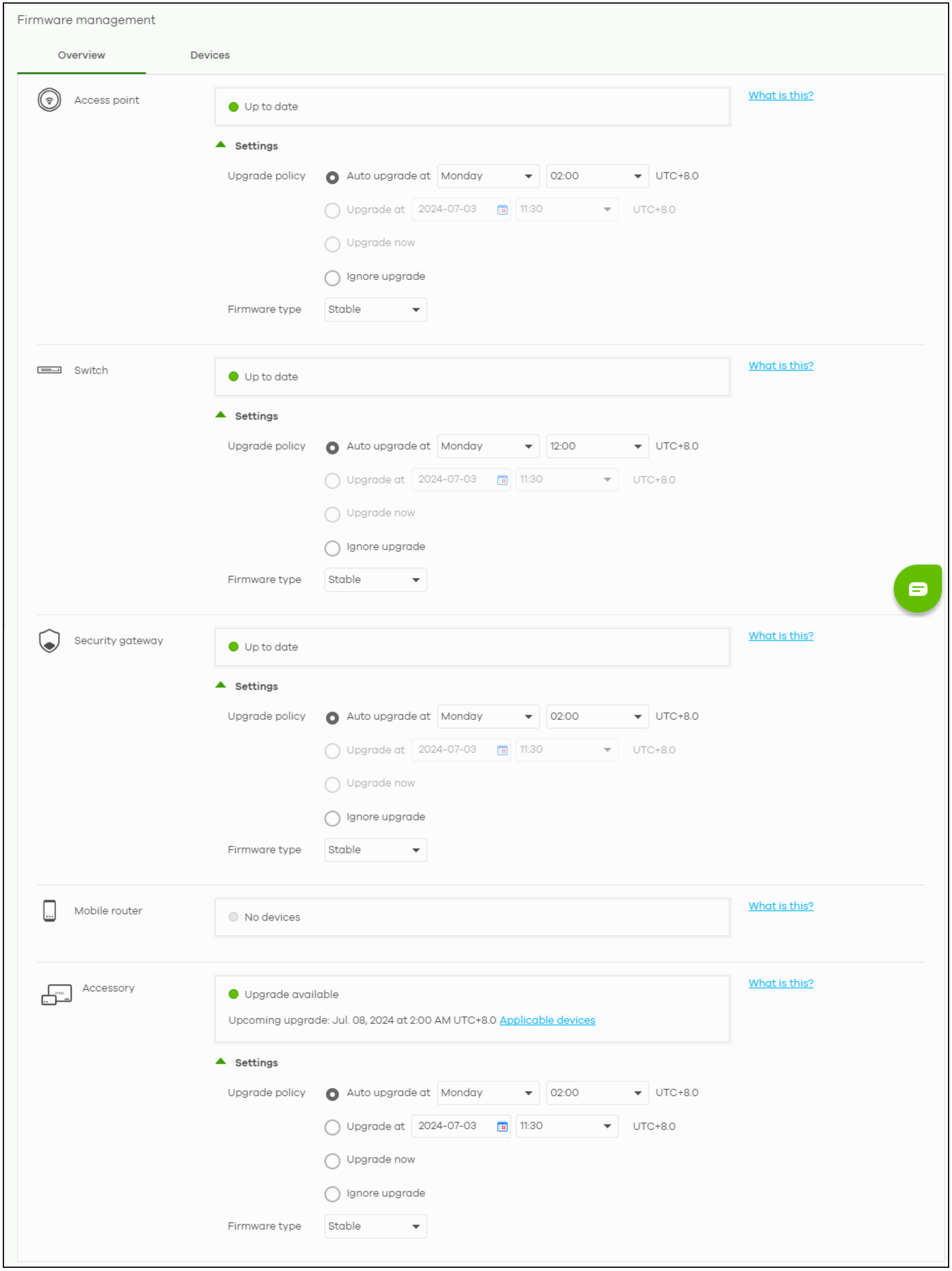
4.9.2 Firmware Management

Use this screen to schedule a firmware upgrade. You can make different schedules for different types of Nebula Devices in the site or create a schedule for a specific Nebula Device. Click **Site-wide** > **Configure** > **Firmware management** to access these screens.

4.9.2.1 Firmware Management Overview Screen

Use this screen to schedule a firmware upgrade for each Nebula Device type. You can make different schedules for different types of Nebula Devices in the site. Click **Site-wide** > **Configure** > **Firmware management** > **Overview** to access this screen.

Figure 65 Site-Wide > Configure > Firmware management > Overview



Firmware management

Overview | Devices

Access point

● Up to date

What is this?

▲ Settings

Upgrade policy
● Auto upgrade at Monday 02:00 UTC+8.0
○ Upgrade at 2024-07-03 11:30 UTC+8.0
○ Upgrade now
○ Ignore upgrade

Firmware type: Stable

Switch

● Up to date

What is this?

▲ Settings

Upgrade policy
● Auto upgrade at Monday 12:00 UTC+8.0
○ Upgrade at 2024-07-03 11:30 UTC+8.0
○ Upgrade now
○ Ignore upgrade

Firmware type: Stable

Security gateway

● Up to date

What is this?

▲ Settings

Upgrade policy
● Auto upgrade at Monday 02:00 UTC+8.0
○ Upgrade at 2024-07-03 11:30 UTC+8.0
○ Upgrade now
○ Ignore upgrade

Firmware type: Stable

Mobile router

○ No devices

What is this?

Accessory

● Upgrade available

Upcoming upgrade: Jul. 08, 2024 at 2:00 AM UTC+8.0 Applicable devices

What is this?

▲ Settings

Upgrade policy
● Auto upgrade at Monday 02:00 UTC+8.0
○ Upgrade at 2024-07-03 11:30 UTC+8.0
○ Upgrade now
○ Ignore upgrade

Firmware type: Stable

The following table describes the labels in this screen.

Table 37   Site-Wide > Configure > Firmware management > Overview

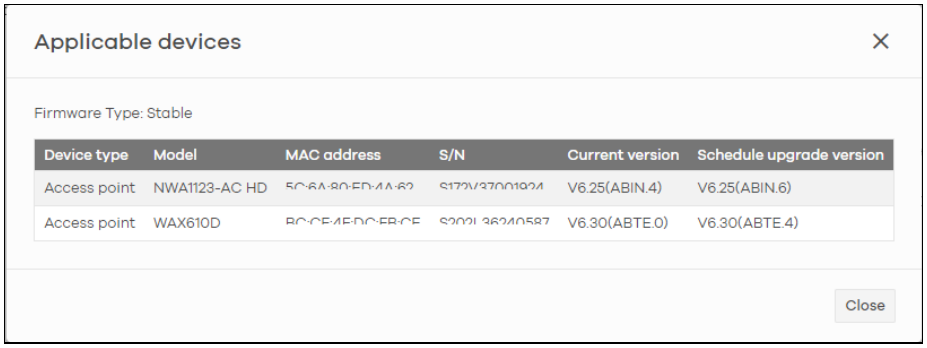
<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></tr>
<tr><td colspan="2">Access point / Switch / Security router / Firewall or Security Gateway / Mobile router / Accessory</td></tr>
<tr><td>Upgrade available</td><td>This shows the status of the Nebula Device's firmware in your site.
• **Up to date** is displayed if all the Nebula Device(s) of a particular type (for example, all Switches) in your site are using the latest firmware version.
• **Upgrade available** is displayed if there is firmware update available for any of the Nebula Device(s) of a particular type in your site. Click **Devices** to see a table list of your Nebula Device(s) that can receive this upgrade.

Applicable devices
Firmware Type: Stable
<table><tr><th>Device type</th><th>Model</th><th>MAC address</th><th>S/N</th><th>Current version</th><th>Schedule upgrade version</th></tr><tr><td>Access point</td><td>NWA1123-AC HD</td><td>5C:6A:80:ED:4A:62</td><td>S172V37001924</td><td>V6.25(ABIN.4)</td><td>V6.25(ABIN.6)</td></tr><tr><td>Access point</td><td>WAX610D</td><td>BC:CF:4F:DC:FB:CF</td><td>S202L36240587</td><td>V6.30(ABTE.0)</td><td>V6.30(ABTE.4)</td></tr></table>
• **Locked** is displayed if all the Nebula Device(s) of a particular type (for example, all Switches) in your site are using a specific version of firmware that Zyxel customer support is monitoring for troubleshooting.
• **No devices** is displayed if there is no Nebula Device of a particular type (for example, Mobile Router) registered in your site.</td></tr>
</table>

Table 37 Site-Wide > Configure > Firmware management > Overview (continued)

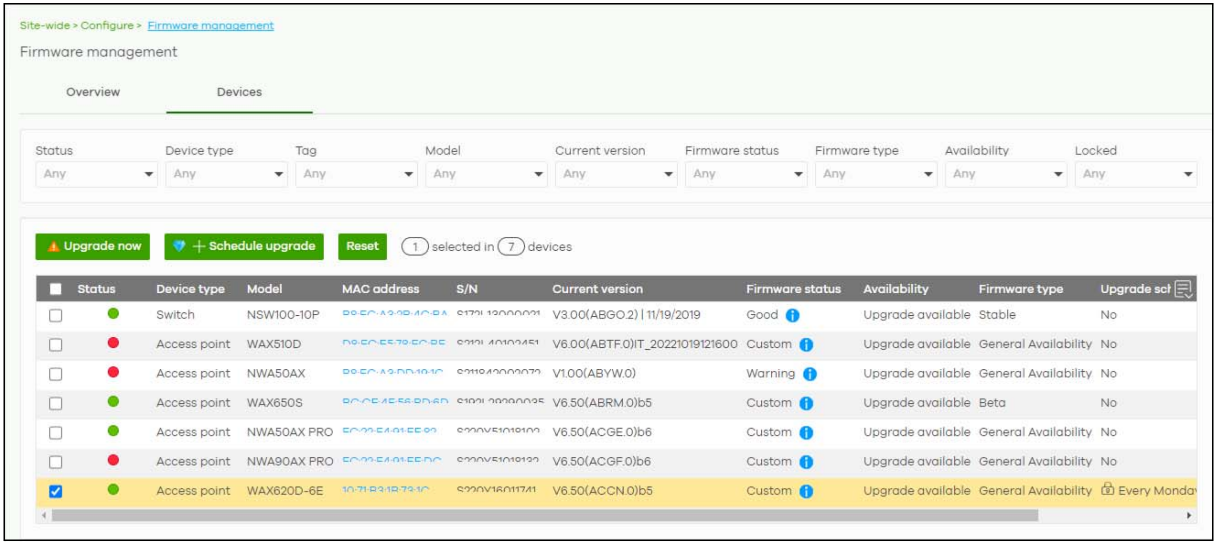
LABEL	DESCRIPTION
Settings	Create a schedule for each Nebula Device type. The following **Upgrade policy** are available: • Select **Auto upgrade at** to create a recurring schedule. With a recurring schedule, NCC will check and install the firmware when a new firmware release is available for each Nebula Device type. • Select **Upgrade at** to install the firmware at a specific date and time (up to 1 month from now) when firmware update is available for each Nebula Device type. Note: Due to network bandwidth and number of Nebula Devices per site, not all Nebula Devices may get the firmware upgrade on the specified date/ time. This field's setting will change to the **Auto upgrade at** schedule after performing the firmware update. • Select **Upgrade now** to immediately install the firmware for each Nebula Device type. Then select the **Firmware type** (**Stable** or **Latest** (default)). Note: This button is selectable only when there is firmware update available. This field's setting will return to it's previous setting (**Auto upgrade at** or **Ignore upgrade**) after performing the firmware update. • Select **Ignore upgrade** if you choose not to install the firmware. Note: NCC will still perform a mandatory upgrade if the Nebula Device's firmware have security vulnerabilities, and/or lack key performance improvements. When the schedule for **Auto upgrade at** is earlier than the mandatory upgrade schedule, then the **Auto upgrade at** schedule has priority.
Firmware type	Set the type of firmware to be installed for each Nebula Device type. • Select **Stable** to install a firmware that may not have the latest features but has passed Zyxel internal and external testing. • Select **Latest** to install the most recently release firmware with the latest features, improvements, and bug fixes. Note: This field is hidden when **Ignore upgrade** is selected in **Settings**. We generally recommend updating to the **Latest** firmware type so that you get the latest features, improvements, and bug fixes. All firmware releases are thoroughly tested internally by our engineers. If your requirements are such that you prefer fewer updates, go with the **Stable** firmware type.

4.9.2.2 Firmware Management Devices Screen

Use this screen to make different firmware upgrade schedules for different types of Nebula Devices in the site. Click **Site-wide** > **Configure** > **Firmware management** > **Devices** to access this screen.

Note: While installing a firmware update, the Nebula Device will continue to operate normally until it reboots. The reboot will take 3 to 5 minutes, so it is best to pick an upgrade time that has minimal impact on your network.

Figure 66 Site-wide > Configure > Firmware management > Devices



Site-wide > Configure > Firmware management

Firmware management

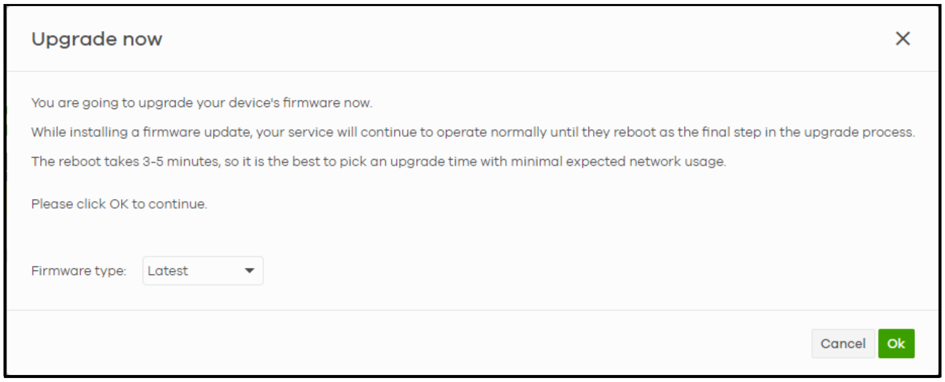
Status	Device type	Tag	Model	Current version	Firmware status	Firmware type	Availability	Locked
Any	Any	Any	Any	Any	Any	Any	Any	Any

1 selected in 7 devices

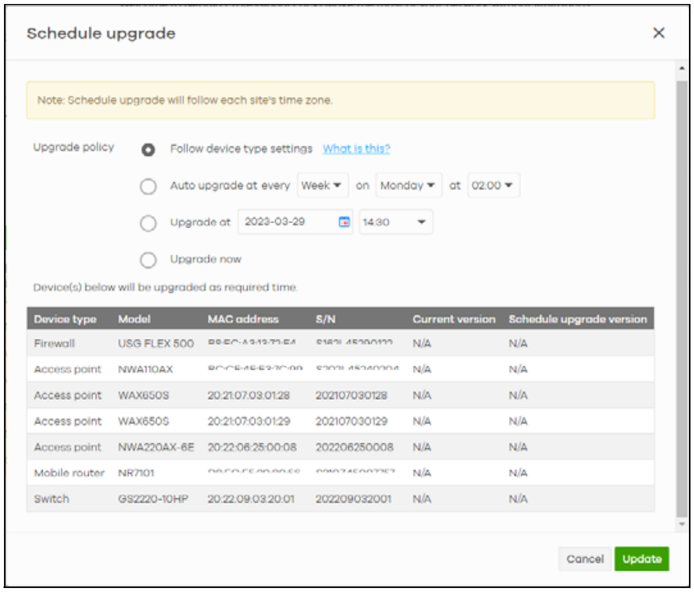
☐	Status	Device type	Model	MAC address	S/N	Current version	Firmware status	Availability	Firmware type	Upgrade sch
☐	●	Switch	NSW100-10P	[illegible]	[illegible]	V3.00(ABGO.2) | 11/19/2019	Good ⓘ	Upgrade available	Stable	No
☐	●	Access point	WAX510D	[illegible]	[illegible]	V6.00(ABTF.0)IT_20221019121600	Custom ⓘ	Upgrade available	General Availability	No
☐	●	Access point	NWA50AX	[illegible]	[illegible]	V1.00(ABYW.0)	Warning ⓘ	Upgrade available	General Availability	No
☐	●	Access point	WAX650S	[illegible]	[illegible]	V6.50(ABRM.0)b5	Custom ⓘ	Upgrade available	Beta	No
☐	●	Access point	NWA50AX PRO	[illegible]	[illegible]	V6.50(ACGE.0)b6	Custom ⓘ	Upgrade available	General Availability	No
☐	●	Access point	NWA90AX PRO	[illegible]	[illegible]	V6.50(ACGF.0)b6	Custom ⓘ	Upgrade available	General Availability	No
☑	●	Access point	WAX620D-6E	[illegible]	[illegible]	V6.50(ACCN.0)b5	Custom ⓘ	Upgrade available	General Availability	Every Monda

The following table describes the labels in this screen.

Table 38   Site-wide > Configure > Firmware management > Devices

<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></tr>
<tr><td>Upgrade Now</td><td>
Click this to immediately install the firmware on the selected Nebula Devices.
This button is selectable only when there is firmware update available for all the selected Nebula Devices.
Then, select the <b>Firmware type</b> to be installed.
• Select <b>Stable</b> to install a firmware that may not have the latest features but has passed Zyxel internal and external testing.
• Select <b>Latest</b> to install the most recently release firmware with the latest features, improvements, and bug fixes.


You are going to upgrade your device's firmware now.
While installing a firmware update, your service will continue to operate normally until they reboot as the final step in the upgrade process.
The reboot takes 3-5 minutes, so it is the best to pick an upgrade time with minimal expected network usage.
Please click OK to continue.
Firmware type: Latest

</td></tr>
<tr><td>Schedule Upgrade</td><td>
Click this to pop up a window where you can create a new schedule for the selected Nebula Devices.
You can select to upgrade firmware according to the site-wide schedule configured for the Nebula Device type in the site, create a recurring schedule, edit the schedule with a specific date and time when firmware update is available for all the selected Nebula Devices, or immediately install the firmware.
With a recurring schedule, the NCC will check and perform a firmware update when a new firmware release is available for any of the selected Nebula Devices. If the NCC service is downgraded from Nebula Professional Pack to Nebula Base, the Nebula Devices automatically changes to adhere to the site-wide schedule.


Note: Schedule upgrade will follow each site's time zone.
Upgrade policy
● Follow device type settings
○ Auto upgrade at every Week on Monday at 02:00
○ Upgrade at 2023-03-29 14:30
○ Upgrade now
Device(s) below will be upgraded as required time.
<table>
<tr><th>Device type</th><th>Model</th><th>MAC address</th><th>S/N</th><th>Current version</th><th>Schedule upgrade version</th></tr>
<tr><td>Firewall</td><td>USG FLEX 500</td><td>[illegible]</td><td>[illegible]</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Access point</td><td>NWA110AX</td><td>[illegible]</td><td>[illegible]</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Access point</td><td>WAX650S</td><td>20:21:07:03:01:28</td><td>202107030128</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Access point</td><td>WAX650S</td><td>20:21:07:03:01:29</td><td>202107030129</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Access point</td><td>NWA220AX-6E</td><td>20:22:06:25:00:08</td><td>202206250008</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Mobile router</td><td>NR7101</td><td>[illegible]</td><td>[illegible]</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Switch</td><td>GS2220-10HP</td><td>20:22:09:03:20:01</td><td>202209032001</td><td>N/A</td><td>N/A</td></tr>
</table>

</td></tr>
</table>

Table 38 Site-wide > Configure > Firmware management > Devices (continued)

LABEL	DESCRIPTION
Reset	Select one or more Nebula Devices, and then click **Reset** to allow the Nebula Devices to follow the site-wide firmware management settings.
Status	This shows the status of the Nebula Device. • Green: The Nebula Device is online and has no alerts. • Amber: The Nebula Device has alerts. • Red: The Nebula Device is offline. • Gray: The Nebula Device has been offline for 7 days or more.
Device type	This shows the type of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Tag	This shows the tag created and added to the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
S/N	This shows the serial number of the Nebula Device.
Current version	This shows the version number of the firmware the Nebula Device is currently running. It shows **N/A** when the Nebula Device goes offline and its firmware version is not available.
Firmware status	The status shows **Good** if the Nebula Device is running a **Stable** / **General Availability** / **Latest** firmware type. The status shows **Warning** if the Nebula Device is running a firmware type older than **Stable**, a newer firmware is available, and immediate action is recommended. The newer firmware may contain security enhancements, new features, and performance improvements. The status shows **Critical** if the Nebula Device is running a firmware type older than **Stable**, a newer firmware is available, and immediate action is required. The firmware may have security vulnerabilities and/or lack key performance improvements. The status shows **Custom** if the Nebula Device is running a firmware with specialized features that is not available to the general public. The status changes to **Upgrading...** after you click **Upgrade Now** to install the firmware immediately.
Firmware type	This shows **Stable** when the installed firmware may not have the latest features but has passed Zyxel internal and external testing. This shows **Latest** when the installed firmware is the most recent release with the latest features, improvements, and bug fixes. This shows **General Availability** when the installed firmware is a release before **Latest**, but is still undergoing Zyxel external testing. This shows **Dedicated** when the installed firmware is locked and Zyxel support is monitoring. Contact Zyxel customer support if you want to unlock the firmware in order to upgrade to a later one. This shows **Beta** when the installed firmware is a release version for testing the latest features and is still undergoing Zyxel internal and external testing. This shows **N/A** when the Nebula Device is offline and its firmware status is not available.
Availability	This shows whether the firmware on the Nebula Device is **Up to date**, there is firmware update available for the Nebula Device (**Upgrade available**), or a specific version of firmware has been installed by Zyxel customer support (**Locked**). Contact Zyxel customer support if you want to unlock the firmware in order to upgrade to a later one.

Table 38   Site-wide > Configure > Firmware management > Devices (continued)

LABEL	DESCRIPTION
Upgrade scheduled	This shows the date and time when a new firmware upgrade is scheduled to occur. Otherwise, it shows **Follow upgrade time** and the Nebula Device sticks to the site-wide schedule or **No** when the firmware on the Nebula Device is up-to-date or the Nebula Device goes offline and its firmware status is not available. A lock icon displays if a specific schedule is created for the Nebula Device, which means the Nebula Device firmware will not be upgraded according to the schedule configured for all Nebula Devices in the site.
Last upgrade time	This shows the last date and time the firmware was upgraded on the Nebula Device.
Schedule upgrade version	This shows the version number of the firmware which is scheduled to be installed.
☰	Click this icon to display a greater or lesser number of configuration fields.

4.9.3 Cloud Authentication

Use this screen to view and manage the user accounts which are authenticated using the NCC user database, rather than an external RADIUS server. Click **Site-wide** > **Configure** > **Cloud authentication** to access these screen.

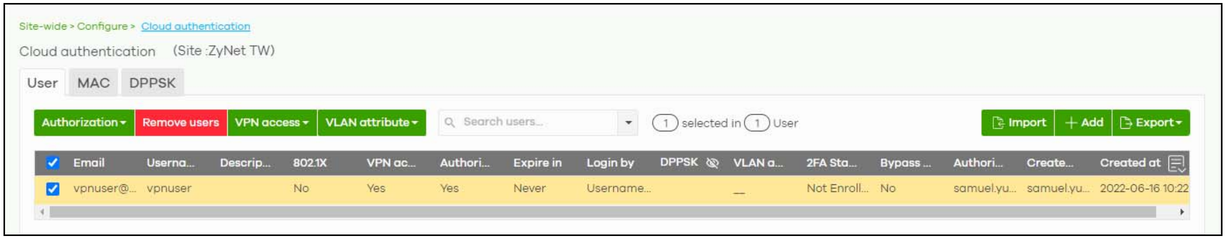
Note: The changes you made in this screen apply only to the current site. To change the cloud authentication settings for all sites in the organization, go to **Organization-wide** > **Organization-wide manage** > **Cloud Authentication** (see Section 4.9 on page 277).

Note: For more information on user account types, see Section 12.4.7.1 on page 710.

4.9.3.1 Cloud Authentication User Screen

Use this screen to view and manage regular NCC network user accounts. Click **Site-wide** > **Configure** > **Cloud Authentication** > **User** to access this screen.

Figure 67   Site-wide > Configure > Cloud Authentication > User



☑	Email	Userna...	Descrip...	802.1X	VPN ac...	Authori...	Expire in	Login by	DPPSK	VLAN a...	2FA Sta...	Bypass ...	Authori...	Create...	Created at
☑	vpnuser@...	vpnuser		No	Yes	Yes	Never	Username...		_	Not Enroll...	No	samuel.yu...	samuel.yu...	2022-06-16 10:22

The following table describes the labels in this screen.

Note: Some of the actions on this screen are only available if your administrator account has full access to the organization.

Table 39 Site-wide > Configure > Cloud Authentication > User

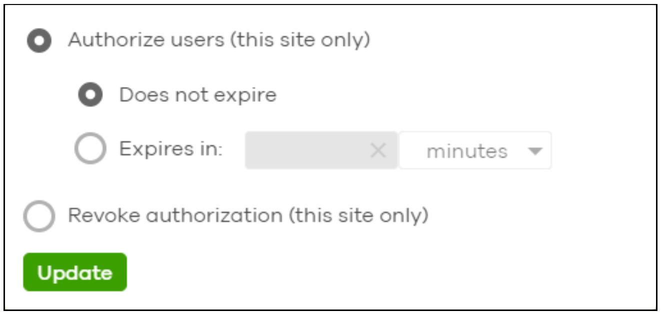
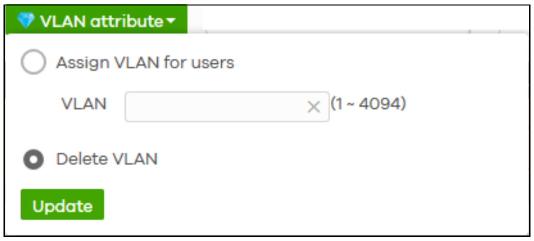
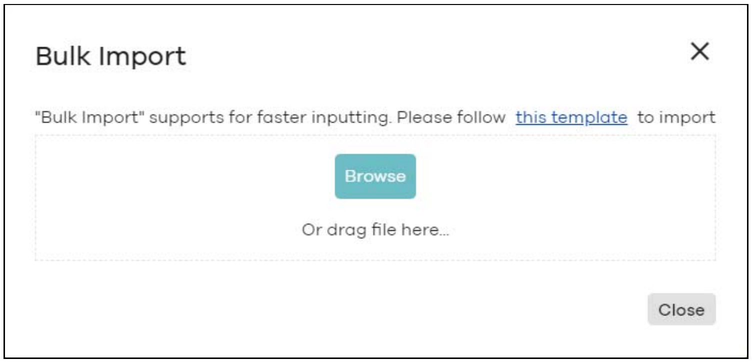
LABEL	DESCRIPTION
Authorization	Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (this site only) ● Does not expire ○ Expires in: minutes ○ Revoke authorization (this site only) Update
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
VPN access	Select one or more than one user account and click this button to configure whether the accounts can be used to connect to the organization's networks through VPN.
VLAN attribute	Select one or more than one user account and click this button to assign the users to a specific VLAN ID, or clear the VLAN ID. Then click **Update**.  VLAN attribute ○ Assign VLAN for users VLAN (1 ~ 4094) ● Delete VLAN Update
Search users	Enter a key word as the filter criteria to filter the list of user accounts.
N User	This shows how many user accounts (N) match the filter criteria and how many user accounts of the selected type are created in total.
Import	Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.  Bulk Import "Bulk Import" supports for faster inputting. Please follow this template to import Browse Or drag file here... Close
Add	Click this button to create a new user account. See Section 4.9.3.2 on page 291.
Export	Click this button to save the account list as a CSV or XML file to your computer.
Email	This shows the email address of the user account.

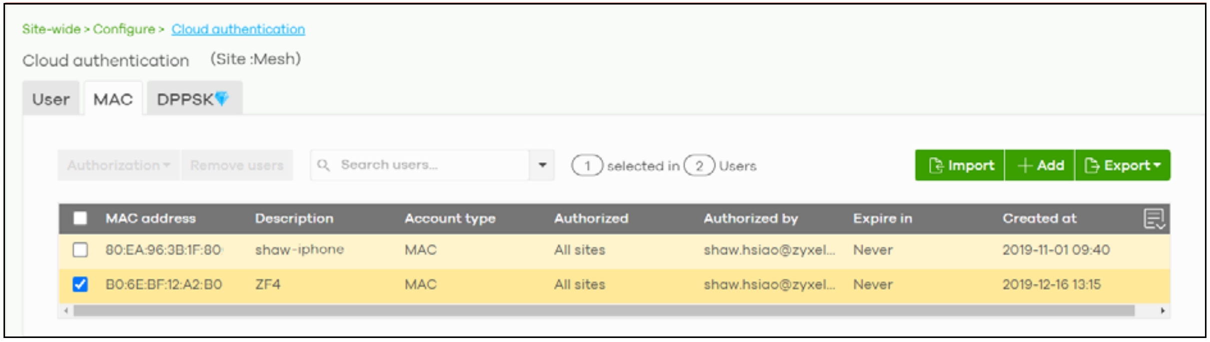
Table 39 Site-wide > Configure > Cloud Authentication > User (continued)

LABEL	DESCRIPTION
Username	This shows the user name of the user account.
Description	This shows the descriptive name of the user account.
802.1X	This shows whether 802.1X (WPA-Enterprise) authentication is enabled on the account.
VPN access	This shows whether the accounts can be used to connect to the organization's networks through VPN.
Authorized	This shows whether the user has been authorized in this site or not.
Expire in (UTC)	This shows the date and time that the account expires. This shows **--** if authentication is disabled for this account. This shows **Never** if the account never expires. This shows **Multiple value** if the account has different **Expire in** values across different sites.
Login by	This shows whether the user needs to log in with the email address and/or user name.
DPPSK	This shows the account's dynamic personal pre-shared key (DPPSK), if one is set.
VLAN assignment	This field is available only when the account type is set to **User**. This shows the VLAN assigned to the user.
2FA Status	This shows whether the account has set up two-factor authentication yet.
Bypass 2FA	This shows whether the account is allowed to bypass two-factor authentication, if two-factor authentication is enabled on a captive portal or VPN gateway.
Authorized by	This shows the email address of the administrator account that authorized the user. If the account has been authorized by different administrators across different sites, it shows **Multiple value**.
Created by	This shows the email address of the administrator account that created the user.
Created at	This shows the date and time that the account was created.
☰	Click this icon to display a greater or lesser number of configuration fields.

4.9.3.2 Cloud Authentication MAC Screen

Use this screen to view and manage Nebula Device user accounts, used for MAC-based authorization. Click **Site-wide** > **Configure** > **Cloud Authentication** > **MAC** to access this screen.

Figure 68 Site-wide > Configure > Cloud Authentication > MAC



☐	MAC address	Description	Account type	Authorized	Authorized by	Expire in	Created at
☐	80:EA:96:3B:1F:80	shaw-iphone	MAC	All sites	shaw.hsiao@zyxel...	Never	2019-11-01 09:40
☑	B0:6E:BF:12:A2:B0	ZF4	MAC	All sites	shaw.hsiao@zyxel...	Never	2019-12-16 13:15

The following table describes the labels in this screen.

Note: Some of the actions on this screen are only available if your administrator account has full access to the organization.

Table 40 Site-wide > Configure > Cloud Authentication > MAC

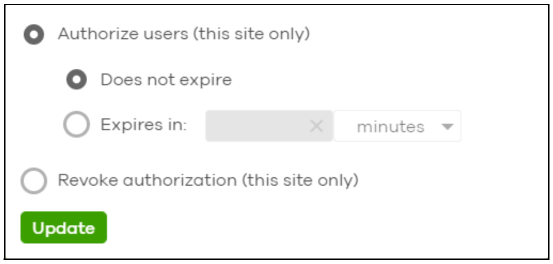
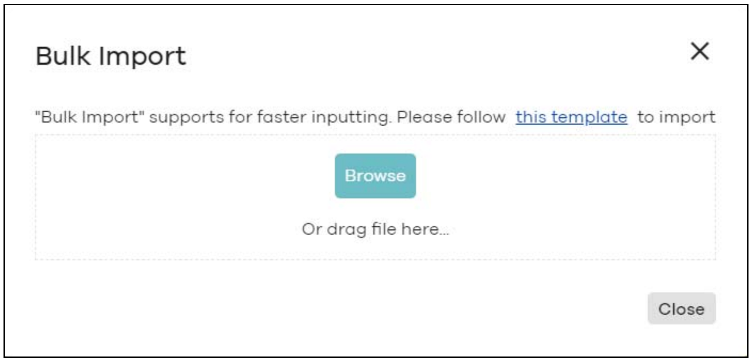
LABEL	DESCRIPTION
Authorization	Select one or more than one account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (this site only) ● Does not expire ○ Expires in: minutes ○ Revoke authorization (this site only) Update
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
Search users	Enter a key word as the filter criteria to filter the list of user accounts.
N User	This shows how many user accounts (N) match the filter criteria and how many user accounts of the selected type are created in total.
Import	Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.  Bulk Import "Bulk Import" supports for faster inputting. Please follow this template to import Browse Or drag file here... Close
Add	Click this button to create a new user account. See Section 4.9.3.3 on page 293.
Export	Click this button to save the account list as a CSV or XML file to your computer.
MAC address	This shows the MAC address of the user account.
Description	This shows the descriptive name of the user account.
Account type	This shows the type of user account: USER, MAC, or DPPSK.
Authorized	This shows whether the user has been authorized in this site or not.
Authorized by	This shows the email address of the administrator account that authorized the user. If the account has been authorized by different administrators across different sites, it shows **Multiple value**.
Expire in	This shows the date and time that the account expires. This shows **--** if authentication is disabled for this account. This shows **Never** if the account never expires. This shows **Multiple value** if the account has different **Expire in** values across different sites.

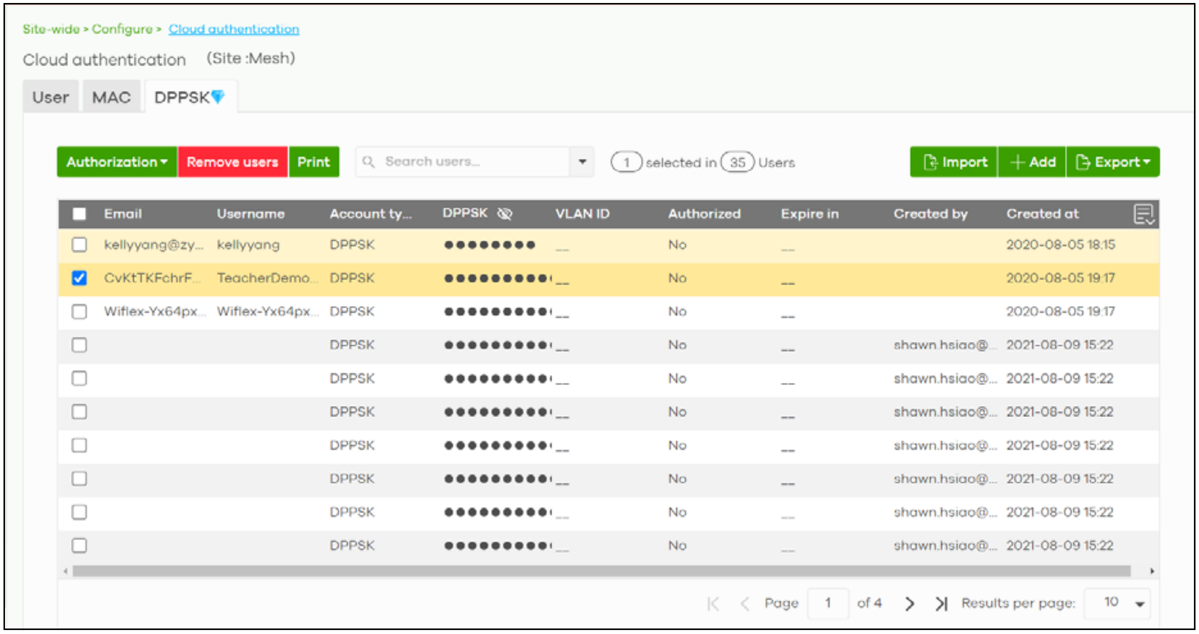
Table 40   Site-wide > Configure > Cloud Authentication > MAC (continued)

LABEL	DESCRIPTION
Created at	This shows the date and time that the account was created.
▤	Click this icon to display a greater or lesser number of configuration fields.

4.9.3.3 Cloud Authentication DPPSK Screen

Use this screen to view and manage DPPSK network user accounts. Click **Site-wide** > **Configure** > **Cloud Authentication** > **DPPSK** to access this screen.

Figure 69   Site-wide > Configure > Cloud Authentication > DPPSK



Site-wide > Configure > Cloud authentication

Cloud authentication (Site :Mesh)

User | MAC | DPPSK

Authorization ▾ | Remove users | Print | Search users... ▾ | 1 selected in 35 Users | Import | + Add | Export ▾

☐	Email	Username	Account ty...	DPPSK	VLAN ID	Authorized	Expire in	Created by	Created at
☐	kellyyang@zy...	kellyyang	DPPSK	●●●●●●●●	__	No	__		2020-08-05 18:15
☑	CvKtTKFchrF...	TeacherDemo...	DPPSK	●●●●●●●●●●	__	No	__		2020-08-05 19:17
☐	Wiflex-Yx64px...	Wiflex-Yx64px...	DPPSK	●●●●●●●●●●	__	No	__		2020-08-05 19:17
☐			DPPSK	●●●●●●●●●●	__	No	__	shawn.hsiao@...	2021-08-09 15:22
☐			DPPSK	●●●●●●●●●●	__	No	__	shawn.hsiao@...	2021-08-09 15:22
☐			DPPSK	●●●●●●●●●●	__	No	__	shawn.hsiao@...	2021-08-09 15:22
☐			DPPSK	●●●●●●●●●●	__	No	__	shawn.hsiao@...	2021-08-09 15:22
☐			DPPSK	●●●●●●●●●●	__	No	__	shawn.hsiao@...	2021-08-09 15:22
☐			DPPSK	●●●●●●●●●●	__	No	__	shawn.hsiao@...	2021-08-09 15:22
☐			DPPSK	●●●●●●●●●●	__	No	__	shawn.hsiao@...	2021-08-09 15:22

Page 1 of 4   Results per page: 10

The following table describes the labels in this screen.

Table 41   Site-wide > Configure > Cloud Authentication > DPPSK

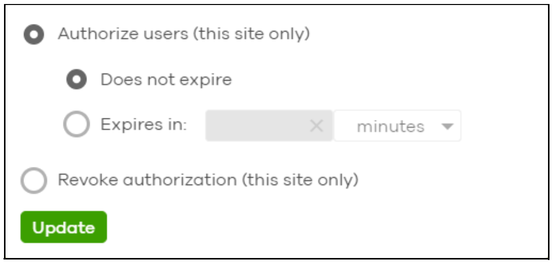
LABEL	DESCRIPTION
Authorization	Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (this site only) ● Does not expire ○ Expires in: minutes ▾ ○ Revoke authorization (this site only) Update
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.

Table 41 Site-wide > Configure > Cloud Authentication > DPPSK (continued)

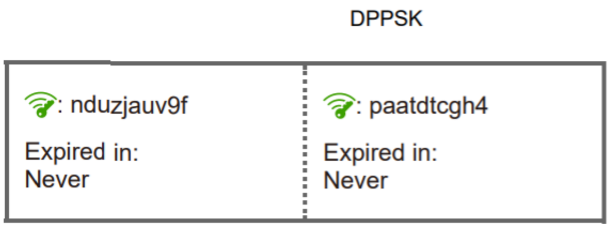
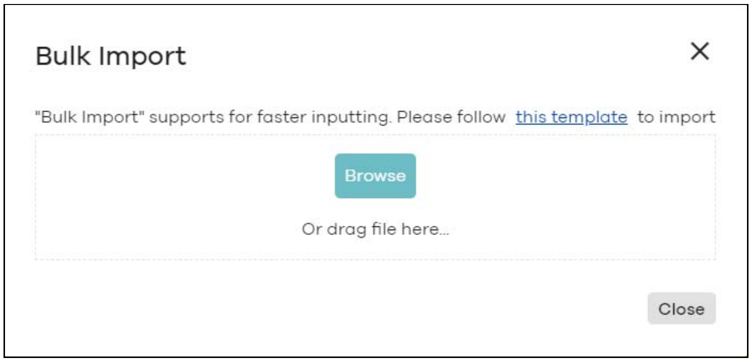
LABEL	DESCRIPTION
Print	Click this button to print the unique dynamic personal pre-shared key (DPPSK) and expiry time of each selected user account. The account details can be cut into cards, and then given to users in order to grant them WiFi network access.  DPPSK : nduzjauv9f Expired in: Never : paatdtcgh4 Expired in: Never
Search users	Enter a key word as the filter criteria to filter the list of user accounts.
N Users	This shows how many user accounts (N) match the filter criteria and how many user accounts of the selected type are created in total.
Import	Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.  Bulk Import "Bulk Import" supports for faster inputting. Please follow this template to import
Add	Click this button to create a single new account, or a batch of accounts. • Single DPPSK: See Section 12.4.7.7 on page 719. • Batch create DPPSK: See Section 12.4.7.8 on page 720.
Export	Click this button to save the account list as a CSV or XML file to your computer.
Email	This shows the email address of the user account.
Username	This shows the user name of the user account.
Account type	This shows the type of user account: USER, MAC, or DPPSK.
DPPSK	This shows the account's dynamic personal pre-shared key (DPPSK).
VLAN ID	This shows the VLAN assigned to the account.
Description	This shows the descriptive name of the user account.
Authorized	This shows whether the user has been authorized in this site or not.
Expire in	This shows the date and time that the account expires. This shows **--** if authentication is disabled for this account. This shows **Never** if the account never expires. This shows **Multiple value** if the account has different **Expire in** values across different sites.
Created by	This shows the email address of the administrator account that created the user.

Table 41 Site-wide > Configure > Cloud Authentication > DPPSK (continued)

LABEL	DESCRIPTION
Created at	This shows the date and time that the account was created.
▤	Click this icon to display a greater or lesser number of configuration fields.

4.9.4 Collaborative Detection & Response

Collaborative Detection & Response (CDR) allows you to detect wired and WiFi clients that are sending malicious traffic in your network and then block or quarantine traffic coming from them. In this way, malicious traffic is not spread throughout the network. Secure policies can block malicious traffic for specific traffic flows, but CDR can block malicious traffic from the sender. Malicious traffic is identified using a combination of Web Filtering, Anti-Malware and IPS (IDP) signatures.

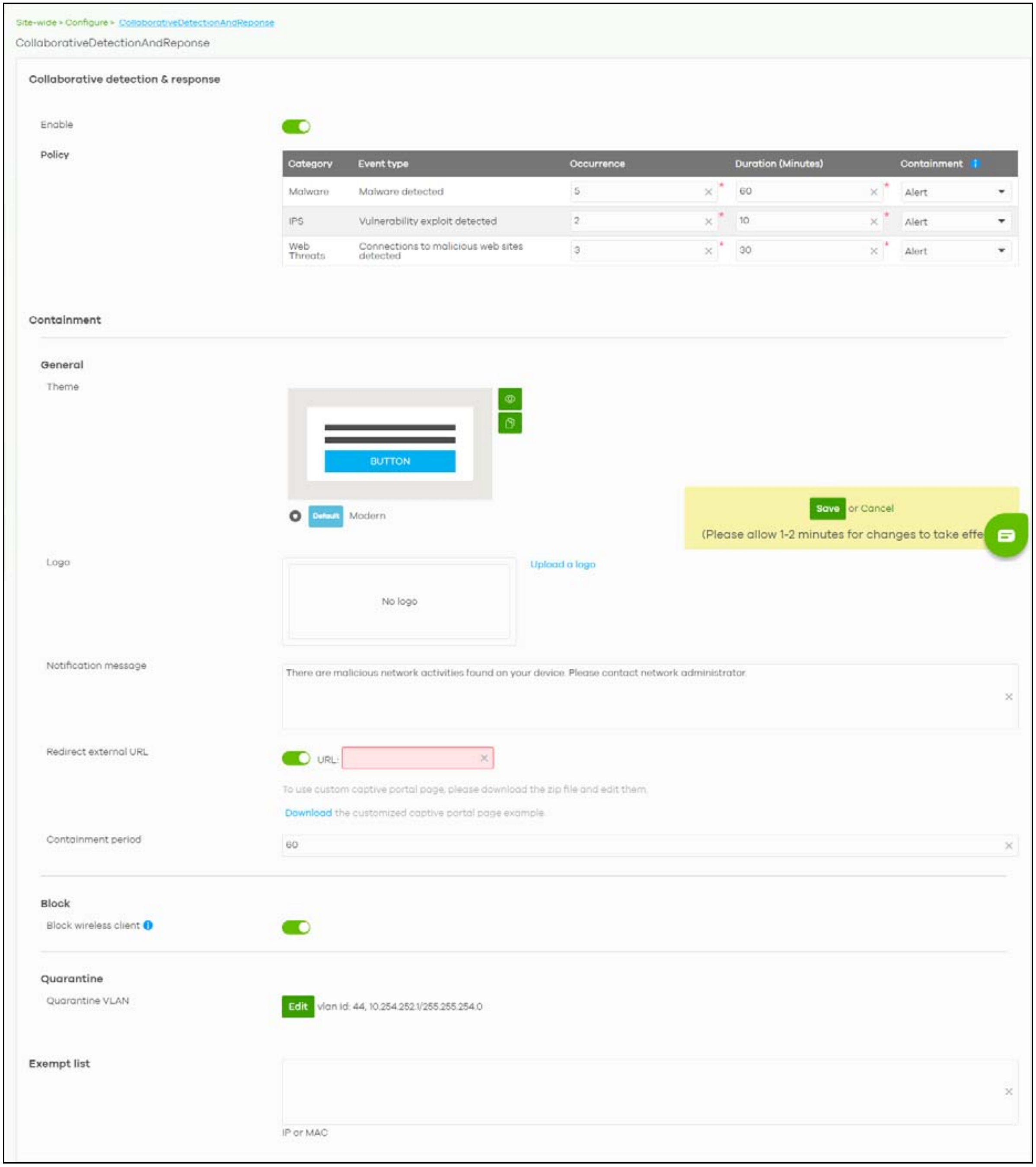
Note: To use the CDR feature, a Gold/UTM Security Pack license and a Nebula Pro Pack license is required.

The following table shows the CDR feature with/without a Gold/UTM Security Pack license.

Table 42 CDR Feature With/Without a Gold/UTM Security Pack License

CDR	WITHOUT GOLD/UTM SECURITY PACK	WITH GOLD/UTM SECURITY PACK	AFTER GOLD/UTM SECURITY PACK EXPIRES
With Nebula Pro Pack	CDR will not function. CDR settings will be grayed-out.	CDR full functionality.	CDR will disable its full functionality. • CDR fields in an “Enabled/ Disabled” state will show “Enabled/ Disabled” but grayed-out. • The **Policy** rule settings, **Quarantine VLAN**, and **Exempt list** will be kept in **Site-wide** > **Configure** > **Collaborative detection & response**. • Previously quarantined clients will be released.
With Nebula Base/Plus Pack	CDR will not function. CDR settings will be grayed-out.	User is notified that CDR is with partial functionality only. • CDR event detection is available • CDR triggered events are logged in the **Site-wide** > **Monitor** > **Site features logs** • **Containment** actions (**Alert**/**Block**/**Quarantine**) is not available • Previously blocked/ quarantined clients will be released in **Site-wide** > **Monitor** > **Containment list**.	CDR will disable its full functionality. • CDR fields in an “Enabled/ Disabled” state will show “Enabled/ Disabled” but grayed-out. • The **Policy** rule settings, **Quarantine VLAN**, and **Exempt list** will be kept in **Site-wide** > **Configure** > **Collaborative detection & response**. • Previously quarantined clients will be released.

Figure 70 Site-wide > Configure > Collaborative Detection & Response



Site-wide > Configure > CollaborativeDetectionAndReponse

CollaborativeDetectionAndReponse

Collaborative detection & response

Enable: on

Policy

Category	Event type	Occurrence	Duration (Minutes)	Containment
Malware	Malware detected	5	60	Alert
IPS	Vulnerability exploit detected	2	10	Alert
Web Threats	Connections to malicious web sites detected	3	30	Alert

Containment

General

Theme: ● Default ○ Modern

Save or Cancel

(Please allow 1-2 minutes for changes to take effe

Logo: No logo

Notification message: There are malicious network activities found on your device. Please contact network administrator.

Redirect external URL: on URL:

To use custom captive portal page, please download the zip file and edit them.

Download the customized captive portal page example.

Containment period: 60

Block

Block wireless client: on

Quarantine

Quarantine VLAN: vlan id: 44, 10.254.252.1/255.255.254.0

Exempt list

IP or MAC

The following table describes the labels in this screen.

Table 43 Site-wide > Configure > Collaborative Detection & Response

LABEL	DESCRIPTION
Collaborative detection & response	
Enable	Select this checkbox to activate Collaborative Detection & Response. Make sure you have active Web Filtering, Anti-Malware, IPS (Intrusion Prevention System), and CDR (Collaborative Detection & Response) licenses.
Policy	

Table 43   Site-wide > Configure > Collaborative Detection & Response (continued)

LABEL	DESCRIPTION
Category	Category refers to the signature type that identified the malicious traffic: **Malware** (Anti-Malware, Anti-Virus), **IDP** (IPS), and **Web Threat** (Content Filter and URL Threat Filtering).
Event Type	This displays some details on the category of malicious traffic detected.
Occurrence (1–100)	Enter the number of security events that need to occur within the defined **Duration** to trigger a CDR **Containment** action.
Duration (1–1440)	Enter the length of time in minutes the event should occur from a client the **Occurrence** number of times to trigger a CDR **Containment** action. For example, **Occurrence** is set to 10, and **Duration** is set to 100. If the NCC detects 10 or more occurrences of malicious traffic in less than 100 minutes, then **CDR Containment** is triggered.
Containment	Select the action to be taken when the number of security events exceed the threshold within the defined duration. **Alert**: Select this if you just want to issue a notification in NCC. **Block**: Select this if you want to block traffic from a suspect client at the NCC, or from a suspect WiFi client at the AP connected to the NCC. Traffic is still broadcast to other clients in the same subnet. A 'notification' web page is displayed when this action is triggered. **Quarantine**: Select this if you want to isolate traffic from a suspect client at the NCC in a quarantine VLAN. Traffic is not broadcast to other clients in the same subnet. A 'notification' web page is displayed to the client when this action is triggered.
Containment	Use this section to configure the selection containment action.
General	
Theme	Configure the CDR block page. • Click the **Preview** icon at the upper right corner of a theme image to display the block page in a new frame. • Click the **Copy** icon to create a new custom theme (block page).
Logo	This shows the logo image that you uploaded for the customized block page. Click **Choose File** and specify the location and file name of the logo graphic or click **Browse** to locate it. You can use the following image file formats: GIF, PNG, or JPG. File size must be less than 200 KB, and images larger than 244 x 190 will be resized.
Notification message	Enter the message that is displayed on the CDR block page. The client is redirected here when a **Block** or **Quarantine** action is triggered. For example, "Malicious traffic is coming from your device so traffic is temporarily stopped. Please contact the network administrator." **Redirect external URL**: Enter a URL in "http://domain" or "https://domain" format to an external notification page. The client is redirected here when a **Block** or **Quarantine** action is triggered. Make sure the external notification page is accessible from the NCC.
Redirect external URL	Enable this setting, and then enter a URL in "http://domain" or "https://domain" format to an external notification page. The client is redirected to this page when a **Block** or **Quarantine** action is triggered. You can download a sample block page by clicking **Download**. Note: The external notification page must be accessible from NCC.
Containment Period	Enter how long the client should be blocked or quarantined. This should be at least twice the DHCP server lease time in order to prevent false positives.
Block	Enter how long a suspect client should be blocked or quarantined. You can enter from 1 minute to 1 day (1,440 minutes). 0 means the suspect is blocked forever until released in **Site-wide** > **Monitor** > **Containment list**.
Block wireless client	Select this to have traffic from the suspect client blocked at the AP. Clear this to have traffic from the suspect client blocked at the NCC.

Table 43 Site-wide > Configure > Collaborative Detection & Response (continued)

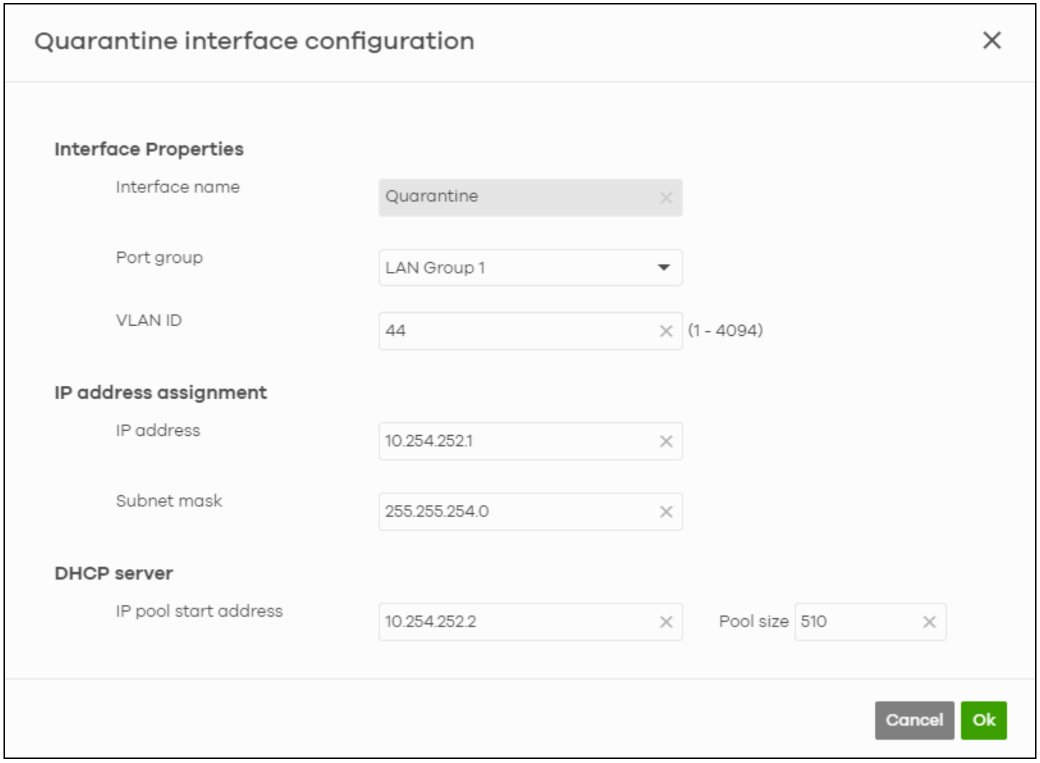
LABEL	DESCRIPTION
Quarantine	
Quarantine VLAN	Click **Set** to configure a VLAN in order to isolate traffic from suspect clients. Traffic from a suspect client is broadcast to all members in the VLAN.
Exempt list	Enter IPv4 and /or MAC addresses of client devices that are exempt from CDR checking.

4.9.5 Quarantine Interface Configuration

Click **Set** at **Site-wide** > **Configure** > **Collaborative detection & response** > **Containment** > **Quarantine** to configure the VLAN and interface used to isolate a client when a quarantine action is triggered. The following screen appears.

Note: Only IPv4 addresses can be used in quarantine VLANs.

Figure 71 Site-wide > Configure > Collaborative detection & response > Containment > Quarantine



Quarantine interface configuration

Interface Properties

Interface name: Quarantine

Port group: LAN Group 1

VLAN ID: 44 (1 - 4094)

IP address assignment

IP address: 10.254.252.1

Subnet mask: 255.255.254.0

DHCP server

IP pool start address: 10.254.252.2 Pool size: 510

Each field is explained in the following table.

Table 44 Site-wide > Configure > Collaborative detection & response > Containment > Quarantine

LABEL	DESCRIPTION
Interface Properties	
Interface Name	This field is read-only. The default name is “Quarantine”.
Port group	Select the name of the port group to which you want the interface to belong.
Base Port	Select the Ethernet interface on which the VLAN interface runs.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved)

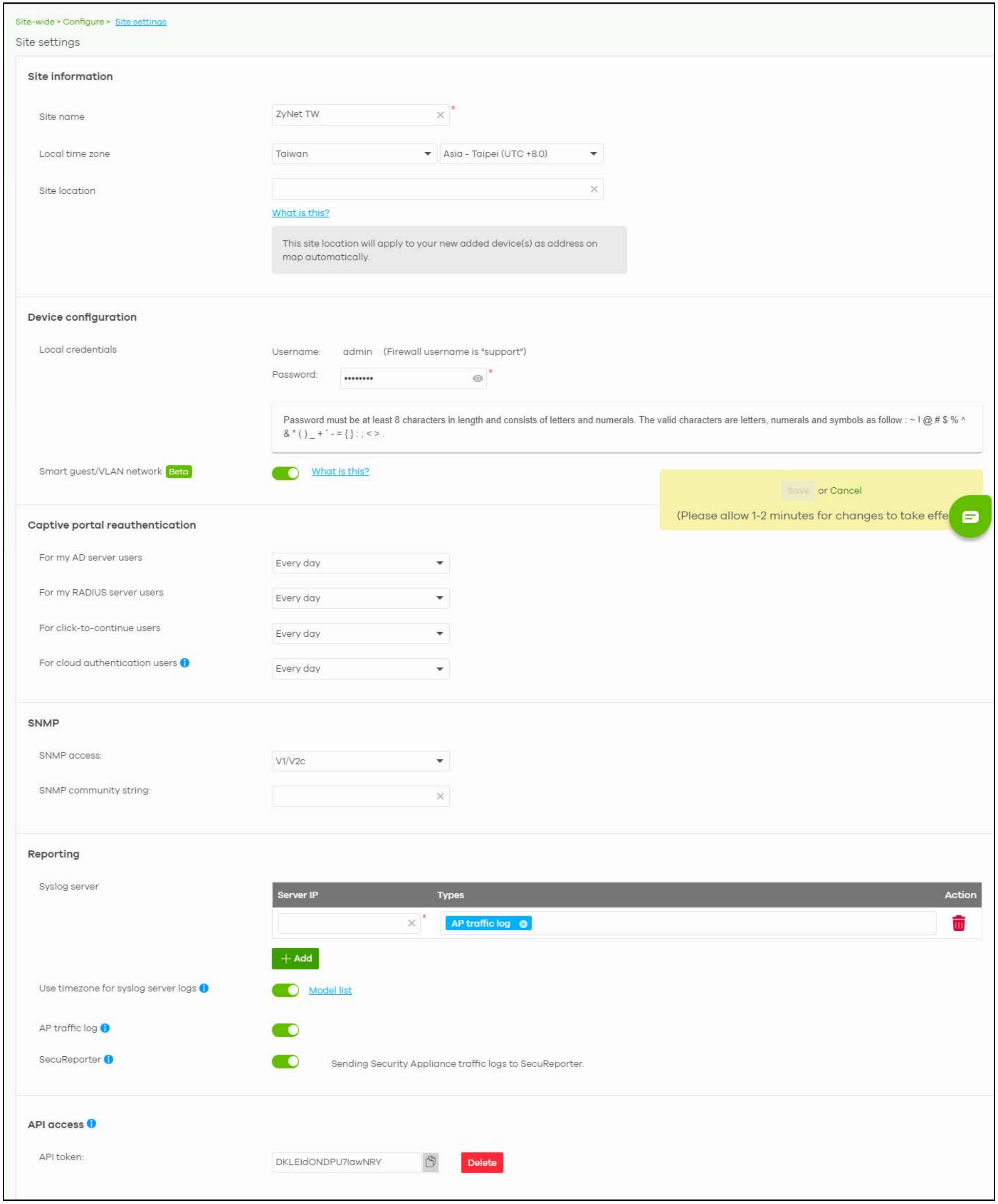
Table 44 Site-wide > Configure > Collaborative detection & response > Containment > Quarantine

LABEL	DESCRIPTION
IP address assignment	This is a 3-bit field within a 802.1Q VLAN tag that is used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest.
IP address	Enter the IP address for this interface.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
DHCP Server	
Get Automatically	Enter the IP address from which the Security Appliance begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add new** under **Static DHCP table**.
IP pool start address	Enter the IP address from which the Security Appliance begins allocating IP addresses for this VLAN.
Pool size	Enter the total number of IP addresses the DHCP server will hand out.
OK	Click **OK** to save your changes back to the NCC.
Cancel	Click **Cancel** to exit this screen without saving.

4.9.6 Site Settings

Use this screen to change the general settings for the site, such as the site name, Nebula Device login password, captive portal reauthentication, SNMP, AP traffic logs to a Syslog server, traffic logs to SecuReporter, and API access for DPPSK third-party integration. Click **Site-wide** > **Configure** > **Site settings** to access this screen.

Figure 72 Site-wide > Configure > Site settings



Site-wide > Configure > Site settings

Site settings

Site information

Site name	ZyNet TW *
Local time zone	Taiwan ▼ Asia - Taipei (UTC +8.0) ▼
Site location	What is this? This site location will apply to your new added device(s) as address on map automatically.

Device configuration

Local credentials	Username: admin (Firewall username is "support") Password: •••••••• * Password must be at least 8 characters in length and consists of letters and numerals. The valid characters are letters, numerals and symbols as follow : ~ ! @ # $ % ^ & * ( ) _ + ` - = { } : ; < > .
Smart guest/VLAN network Beta	What is this?

Save or Cancel

(Please allow 1-2 minutes for changes to take effe

Captive portal reauthentication

For my AD server users	Every day ▼
For my RADIUS server users	Every day ▼
For click-to-continue users	Every day ▼
For cloud authentication users	Every day ▼

SNMP

SNMP access:	V1/V2c ▼
SNMP community string:	

Reporting

Syslog server

Server IP	Types	Action
*	AP traffic log ⊗	🗑

+ Add

Use timezone for syslog server logs	Model list
AP traffic log	
SecuReporter	Sending Security Appliance traffic logs to SecuReporter.

API access

API token: DKLEidONDPU7lawNRY Delete

The following table describes the labels in this screen.

Table 45 Site-wide > Configure > Site settings

LABEL	DESCRIPTION
Site Information	
Site name	Enter a descriptive name for the site.
Local time zone	Choose the time zone of the site's location.
Site location	Enter the complete address or coordinates (physical location) of the Nebula Devices in the site. All newly added Nebula Devices will automatically use this as the default address and location on the Google map. Note: You can edit each Nebula Device's location on the Google map.
Device configuration	
Local credentials	The default password is generated automatically by the NCC when the site is created. You can specify a new password to access the status page of the Nebula Device's built-in web-based configurator. The settings here apply to all Nebula Devices in this site.
Smart guest/ VLAN network	Click **On** to enable this feature. This allows the NCC to check if the VLAN ID and guest network settings are consistent on the APs and Security Appliance in the same site to ensure guest network connectivity. The guest settings you configure for a gateway interface (in **Site-wide** > **Configure** > **Security gateway** > **Interface addressing**) will also apply to the WiFi networks (SSIDs) associated with the same VLAN ID (in **Site-wide** > **Configure** > **Access points** > **SSID settings**). For example, if you set a gateway interface in VLAN 100 as a guest interface, the SSID that belongs to VLAN 100 will also act as a guest network.
Captive portal reauthentication	
For my AD server users	Select how often the user (authenticated by an AD server) has to log in again.
For my RADIUS server users	Select how often the user (authenticated by a RADIUS server) has to log in again.
For click-to-continue users	Select how often the user (authenticated through the captive portal) has to log in again.
For cloud authentication users	Select how often the user (authenticated using the NCC user database) has to log in again.
SNMP	
SNMP access	Select **V1/V2c** to allow SNMP managers using SNMP to access the Nebula Devices in this site. Otherwise, select **Disable**.
SNMP community string	This field is available when you select **V1/V2c**. Enter the password for the incoming SNMP requests from the management station.
Reporting	
Syslog server	Click **Add** to create a new entry.
Server IP	Enter the IP address of the server.
Types	Select the type of logs the server is for. Note: Besides sending **Security appliance traffic log** to a Syslog server, you can also set the Security Appliance (through its Web Configurator) to save a copy of the logs to a connected USB storage device. **Security appliance traffic log** includes the traffic information (such as its source, destination or usage) of the Security Appliance clients. Note: The **Security appliance log** and **Security appliance traffic log** will not include Security Firewall(s) in Cloud Monitoring mode.

Table 45   Site-wide > Configure > Site settings (continued)

LABEL	DESCRIPTION
Action	Click the **Delete** icon to remove the entry.
Use timezone for syslog server logs	Click **On** to enable this feature. This allows the Syslog server logs to use the site's timezone. If disabled, the Syslog server logs will show GMT 0 time. GMT does not adjust automatically for Daylight Savings Time (DST). You must adjust for Daylight Savings directly in the Syslog server.
AP traffic log	Log traffic for access points in the site that have NAT mode enabled. You can also send the logs to a Syslog server, by selecting **AP traffic log** under **Syslog server** > **Types**. For details on configuring **NAT mode**, see Section 5.3.2 on page 320.
SecuReporter	Click **On** to enable this feature. This allows the NCC to send traffic logs to SecuReporter. Note: NCC will not include the traffic logs for Security Firewall(s) in Cloud Monitoring mode. Note: Disable this option if you have configured sending of traffic logs to an external syslog server.
API access	API access allows third-party software to integrate with the DPPSK feature in NCC. For more information, please contact Zyxel.
API token	Generate an API token for DPPSK third-party integration.
Copy	Click this button to copy the API key to the system's clipboard.
Delete	Click this button to delete the API key.

CHAPTER 5 Access Point

5.1 Overview

This chapter discusses the menus that you can use to monitor the Nebula-managed APs (Access Points) in your network and configure settings even before an AP is deployed and added to the site.

Nebula Device refers to Zyxel Hybrid APs (NAP / NWA / WAC / WAX Series) in this chapter. To view the list of Nebula Devices that can be managed through NCC, go to **Help** > **Support tools** > **Device function table**.

The following features in the **Access Point** menus apply to specific models only.

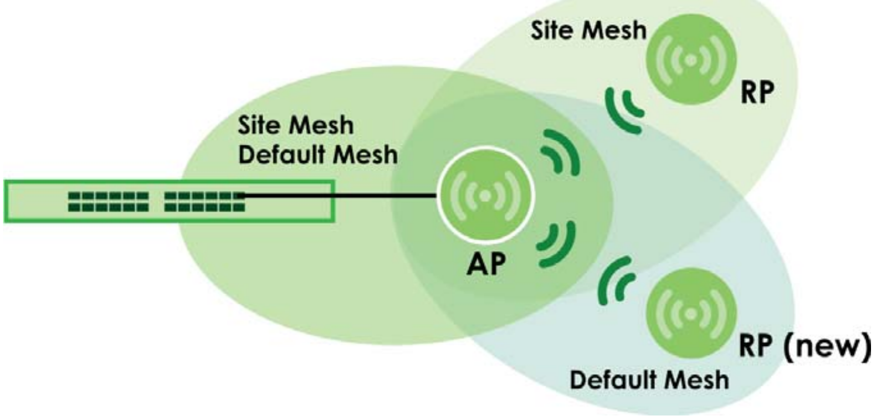
Table 46 Features/Fields Supported on Specific Nebula Devices Only

FEATURES/FIELDS	INCLUDED NEBULA DEVICES	LOCATION
Ethernet Secure Tunnel Setting in **Remote AP Setting**	WAC500H	Click a Nebula Device entry in the **Site-wide** > **Devices** > **Access points** screen to display individual Nebula Device statistics. See Section 4.3.1 on page 214 for more information.
Wired stations		
WPA3 in **Security options**	NWA110AX, WAX510D, WAX650S	Click **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**. See Section 5.3.2 on page 320 for more information.
Ethernet Traffic options Forwarding Mode	WAC500H	Click an entry in the **Port setting** table of the **Site-wide** > **Configure** > **Access points** > **AP & port settings** screen to access the **Edit** – **AP & port settings** screen. See Section 5.3.7.1 on page 347 for more information.

5.1.1 Nebula Smart Mesh

Nebula Smart Mesh, also called Smart Mesh or AP Smart Mesh, is a WiFi mesh solution for Nebula Devices. With Smart Mesh, you can have two or more Nebula Devices automatically create a mesh network within your home or office, ensuring there are no areas with a weak WiFi signal.

Figure 73 Nebula Smart Mesh



Smart Mesh assigns a role to each Nebula Device depending on its connection method.

- **Root AP** (**AP**): A Nebula Device (mesh controller) that is connected to the network by Ethernet and can reach the gateway device.
- **Repeater AP** (**RP**): A Nebula Device (mesh extender) that is connected to the network wirelessly, or that is connected to the network by Ethernet but cannot reach the gateway device.

The mesh extender rebroadcast the mesh controller's SSID, and then relay WiFi traffic back to the gateway.

To create a Smart Mesh network, add two or more Nebula Devices to the same Nebula-managed site and ensure that each Nebula Device has Smart Mesh enabled. Then connect one or more Nebula Devices to your network's gateway using an Ethernet cable, so that you have at least one mesh controller. Finally, place one or more non-wired Nebula Devices in areas where you want to extend WiFi coverage.

5.1.2 Smart Mesh Network Topology

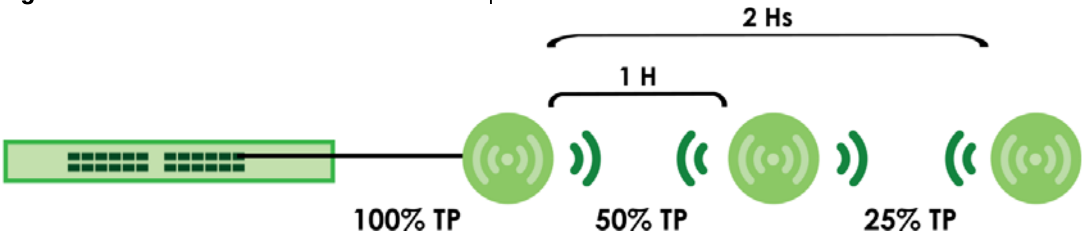
After you add a Nebula Device to an NCC site and then turn it on, the new Nebula Device automatically connects to a mesh network called the **default mesh**. The Nebula Device then tries to connect to a mesh controller and contact NCC. After the Nebula Device successfully contacts NCC and joins the site, the Nebula Device stops using the default mesh and instead connects to other Nebula Devices in the site using a dedicated network called the **site mesh**.

5.1.2.1 Smart Mesh Wireless Hops

Each mesh extender tries to connect to the site gateway through a mesh controller. If a mesh extender cannot connect directly to a mesh controller, then the mesh extender relays its WiFi traffic through another mesh extender. Each time traffic passes through a WiFi connection in the mesh network, it counts as one **hop**.

Nebula Smart Mesh supports an unlimited number of hops. However, each hop in a mesh network reduces network throughput by up to half. Therefore, we recommend only allowing a maximum of two hops within your Smart Mesh network.

Figure 74 Nebula Smart Mesh Wireless Hops

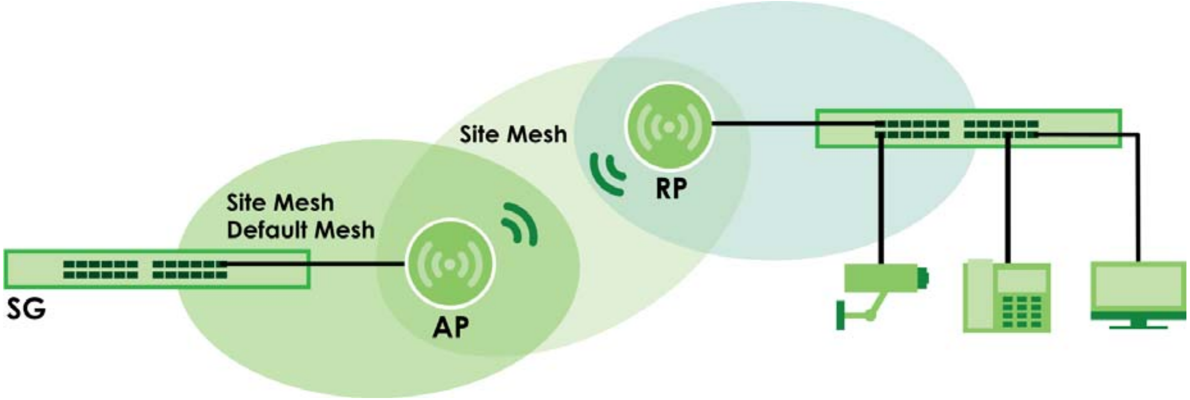


5.1.2.2 Wireless Bridge

Wireless bridge is a Smart Mesh feature that allows two Nebula Devices to automatically connect two network segments together over a WiFi connection. This is useful when you want to extend your wired network to a new area, but it is difficult to run cables to that area.

To use wireless bridge, enable **Wireless Bridge** on two Nebula Devices (**AP**, **RP**) in NCC. Then connect wired clients to one of the Nebula Device's LAN port. These wired clients form a new network segment and are able to reach the site gateway (**SG**) through the Nebula Device's WiFi connection.

Figure 75 Nebula Smart Mesh Wireless Bridge



5.2 Monitor

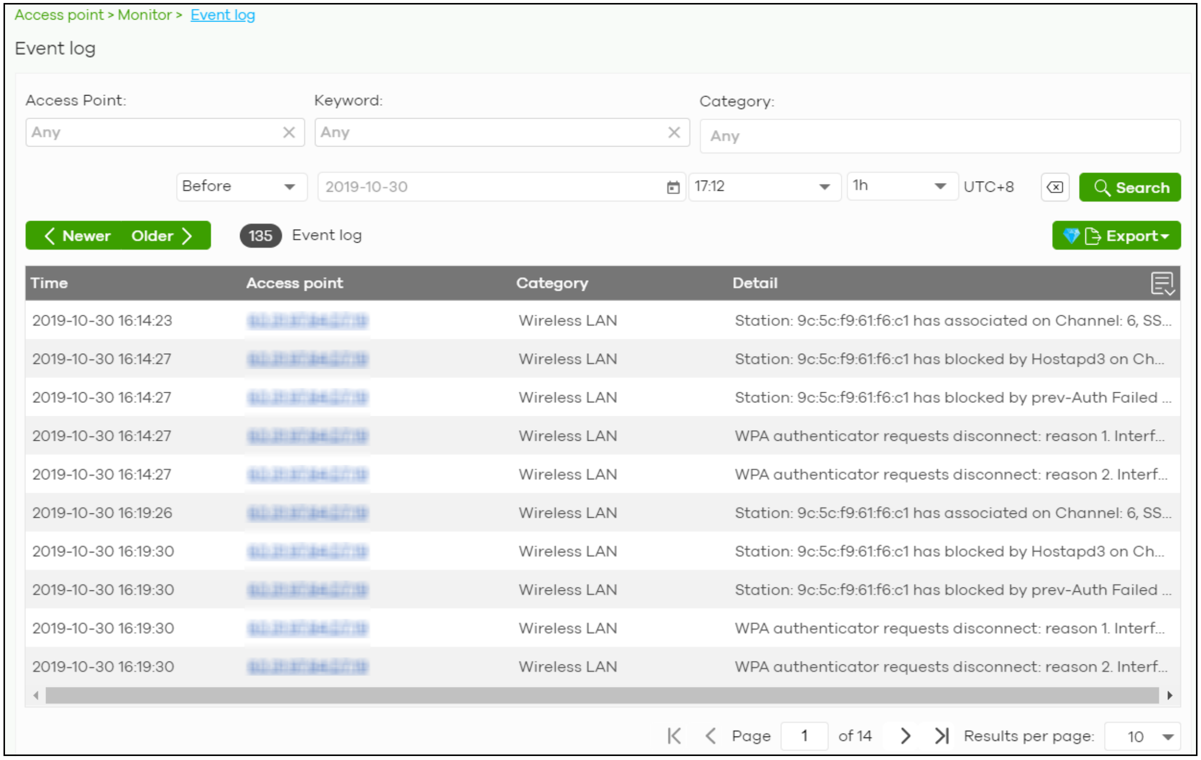
Use the **Monitor** menus to check Nebula Device event log messages and summary report for Nebula Devices in the selected site.

5.2.1 Event Log

Use this screen to view WiFi Nebula Device log messages. You can enter the Nebula Device name or a key word, select one or multiple event types, or specify a date/time or even a time range to display only the log messages related to it.

Click **Site-wide** > **Monitor** > **Access points** > **Event log** to access this screen.

Figure 76 Site-wide > Monitor > Access points > Event log



Access point > Monitor > Event log

Event log

Access Point: Any
Keyword: Any
Category: Any

Before | 2019-10-30 | 17:12 | 1h | UTC+8 | Search

Newer | Older | 135 Event log | Export

Time	Access point	Category	Detail
2019-10-30 16:14:23	[redacted]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has associated on Channel: 6, SS...
2019-10-30 16:14:27	[redacted]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by Hostapd3 on Ch...
2019-10-30 16:14:27	[redacted]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by prev-Auth Failed ...
2019-10-30 16:14:27	[redacted]	Wireless LAN	WPA authenticator requests disconnect: reason 1. Interf...
2019-10-30 16:14:27	[redacted]	Wireless LAN	WPA authenticator requests disconnect: reason 2. Interf...
2019-10-30 16:19:26	[redacted]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has associated on Channel: 6, SS...
2019-10-30 16:19:30	[redacted]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by Hostapd3 on Ch...
2019-10-30 16:19:30	[redacted]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by prev-Auth Failed ...
2019-10-30 16:19:30	[redacted]	Wireless LAN	WPA authenticator requests disconnect: reason 1. Interf...
2019-10-30 16:19:30	[redacted]	Wireless LAN	WPA authenticator requests disconnect: reason 2. Interf...

Page 1 of 14 | Results per page: 10

5.2.2 Vouchers

A voucher is a unique printable code that allows a user to authenticate with a WiFi network for a limited period of time. A user connects to the WiFi network's SSID and then enters the code in a captive portal. After a successful login, the expiry time of the voucher starts counting down.

Vouchers are useful in situations where you want to give individual users time-limited WiFi access. For example: A customer can purchase a voucher for 2 hours of Internet access in a hotel or coffee shop.

5.2.2.1 Using Vouchers

1 Go to **Site-wide** > **Configure** > **WiFi SSID**, and create a dedicated SSID for voucher-based WiFi access. For example, "Hotel_Guest_Network".
For details on configuring SSIDs, see Section 5.3.2 on page 320.

2 Go to **Site-wide** > **Configure** > **WiFi SSID**, select the SSID, and then under **Sign-in method** select **Voucher**.

3 Go to **Site-wide** > **Monitor** > **Access points** > **Vouchers** > **Settings** to configure how the vouchers will look when printed.
For details, see Section 5.2.2.4 on page 309.

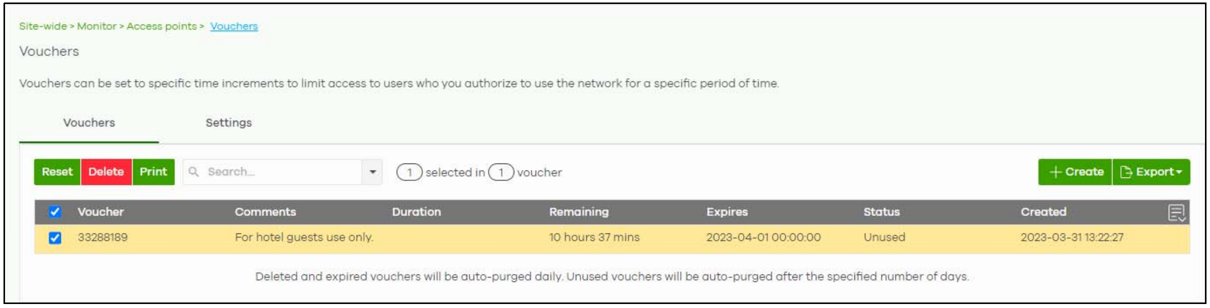
4 Go to **Site-wide** > **Monitor** > **Access points** > **Vouchers,** and then click **Create** to create one or more vouchers.

5.2.2.2 Vouchers Screen

This screen allows you to create and manage vouchers for WiFi network authentication.

Click **Site-wide** > **Monitor** > **Access points** > **Vouchers** to access this screen.

Figure 77 Site-wide > Monitor > Access points > Vouchers



Site-wide > Monitor > Access points > Vouchers

Vouchers

Vouchers can be set to specific time increments to limit access to users who you authorize to use the network for a specific period of time.

☑	Voucher	Comments	Duration	Remaining	Expires	Status	Created
☑	33288189	For hotel guests use only.		10 hours 37 mins	2023-04-01 00:00:00	Unused	2023-03-31 13:22:27

Deleted and expired vouchers will be auto-purged daily. Unused vouchers will be auto-purged after the specified number of days.

The following table describes the labels in this screen.

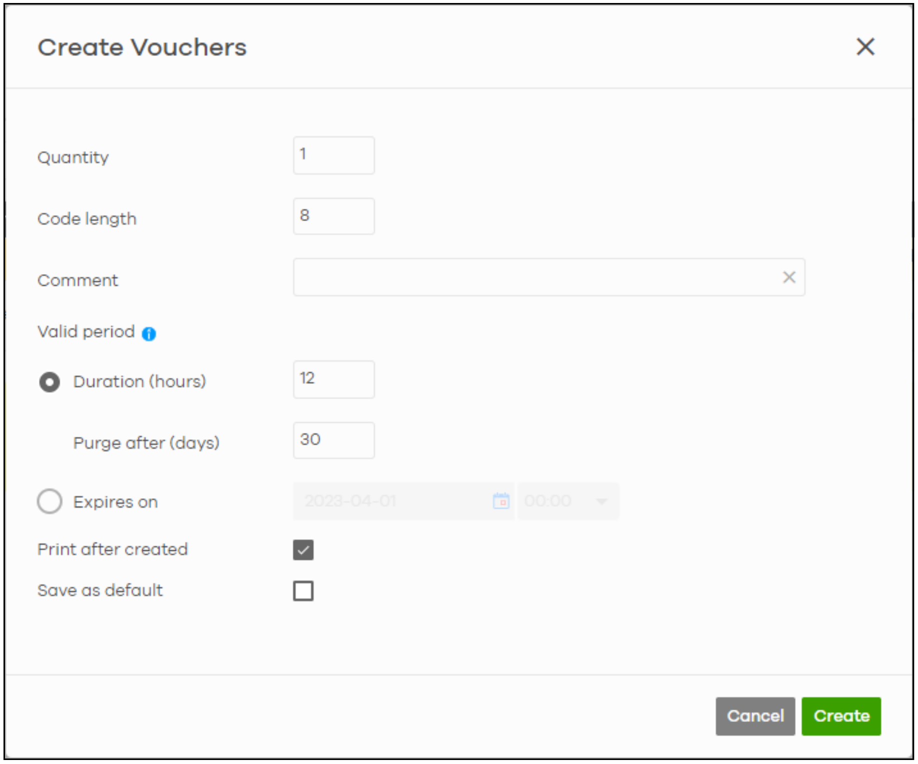
Table 47 Site-wide > Monitor > Vouchers

LABEL	DESCRIPTION
Reset	Select one or more vouchers and then click this button to reset the vouchers back to their original states. Each voucher's status is set to **Unused** and time remaining is reset to the time configured in **Duration**.
Delete	Select one or more vouchers and then click this button to delete the vouchers.
Print	Select one or more vouchers and then click this button to print the vouchers.
Search	Use this field to search for vouchers, by voucher code, duration, and/or status.
Create	Click this button to create one or more vouchers. For details, see Section 5.2.2.3 on page 307.
Export	Click this button to export the voucher table and all information in it to a CSV or XML file.
Voucher	This displays the voucher's unique authentication code.
Comments	This displays information about the voucher.
Duration	This displays how long the voucher is valid from when it is activated, in hours.
Remaining	This displays how much time is left before the voucher expires. NCC only starts counting this time after the voucher has been activated.
Expire in	This displays the date and time that the voucher will expire.
Status	This displays the current status of the voucher: **Unused**: The voucher has not yet been used for authentication. **Active**: A user has used the voucher for authentication. NCC has started counting down the duration. **Expire**: The voucher has reached the end of its duration period and can no longer be used. **Delete**: The voucher is unused and has reached the time set under **Purge after (days)**. Note: NCC automatically deletes vouchers with the status **Expire** or **Delete** after 24 hours. You can see a history of these automatic deletions in the NCC event log.
Created	This displays the date and time that the voucher was created.

5.2.2.3 Create Vouchers Screen

Use this screen to create one or more new vouchers.

Figure 78 Site-wide > Monitor > Access points > Vouchers > Create



Create Vouchers ×

Quantity: 1

Code length: 8

Comment:

Valid period

● Duration (hours): 12

Purge after (days): 30

○ Expires on: 2023-04-01 00:00

Print after created ☑

Save as default □

The following table describes the labels in this screen.

Table 48 Site-wide > Monitor > Vouchers > Create

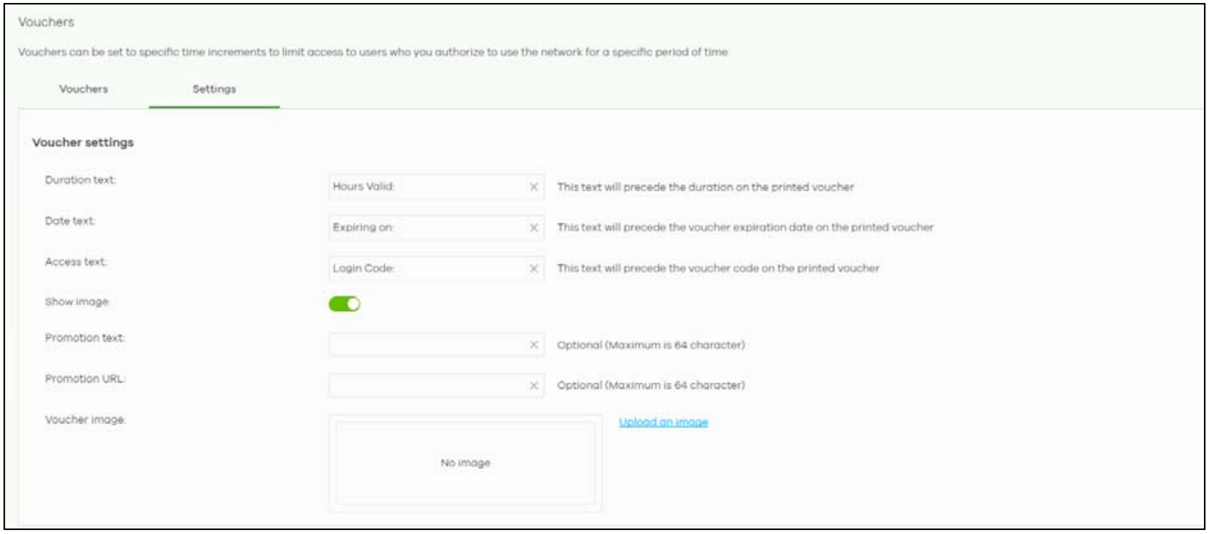
LABEL	DESCRIPTION
Quantity	Sets the number of vouchers you want to create. The valid range for this setting is 1 – 999.
Code length	Sets the length of the unique code on each voucher. The valid range for this setting is 6 – 10.
Comment	Enter information about the voucher that might be useful for other administrators.
Valid period	There are two ways to set your voucher's validity.
Duration (hours)	Sets how long the voucher is valid after it has been activated, in hours. The valid range for this setting is any whole number from 1 – 8760.
Purge after (days)	Sets how long a non-activated voucher is valid for, in days. The valid range for this setting is 1 – 180.
Expires on	Sets the date and time for the expiration of this voucher.
Print after created	Select this to print the vouchers immediately after clicking **Create**. Note: Before printing a voucher, select which SSID name to appear on the voucher when you have two or more SSIDs enabled on your site.
Save as default	Click this to make the settings on this page the default settings for new vouchers.

Note: Dynamic Personal Pre-Shared Keys (DPPSKs) also allow you to give individual users a printable password and time-limited WiFi access. For details, see Section 5.3.2 on page 320.

5.2.2.4 Voucher Settings Screen

Use this screen to change the voucher settings for the Nebula Device. Click **Site-wide** > **Monitor** > **Access points** > **Voucher** > **Settings** to access this screen.

Figure 79 Site-wide > Monitor > Access points > Voucher > Settings



Vouchers

Vouchers can be set to specific time increments to limit access to users who you authorize to use the network for a specific period of time

Vouchers | Settings

Voucher settings

Duration text:	Hours Valid:	This text will precede the duration on the printed voucher
Date text:	Expiring on:	This text will precede the voucher expiration date on the printed voucher
Access text:	Login Code:	This text will precede the voucher code on the printed voucher
Show image:	●	
Promotion text:		Optional (Maximum is 64 character)
Promotion URL:		Optional (Maximum is 64 character)
Voucher image:	No image	Upload an image

The following table describes the labels in this screen.

Table 49 Site-wide > Monitor > Access points > Voucher > Settings

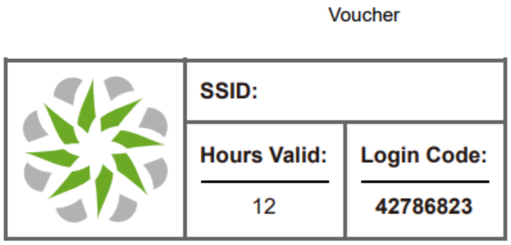
LABEL	DESCRIPTION
Voucher settings	Use these settings to configure how WiFi network authentication vouchers for this site look when printed.  Voucher SSID: Hours Valid: 12 Login Code: 42786823 For more information on vouchers, see Section 5.2.2 on page 306.
Duration text	Sets the text that precedes the duration on the voucher. The text must consist of 1 – 16 characters.
Date text	Sets the text that precedes the expiration date on the voucher. The text must consist of 1 – 16 characters.
Access text	Sets the text that precedes the voucher code on the voucher. The text must consist of 1 – 16 characters.
Show image	Sets whether to display an image at the top-left of the voucher. This image is optional.
Promotion text	Sets the promotional text on the voucher. This text is optional. The text must consist of 1 – 64 characters.
Promotion URL	Sets the promotional URL on the voucher. This URL is optional. The URL is displayed as a QR code on the voucher.

Table 49 Site-wide > Monitor > Access points > Voucher > Settings (continued)

LABEL	DESCRIPTION
Voucher image	This shows the uploaded image that will be displayed at the top-left of the voucher.
Upload an image	Click this button to upload an image from your local computer. The **Choose File** button appears. Click this button to locate the PNG (preferred for its transparency) / JPEG/GIF image file. The maximum image file size is 200 KB.
Replace this image	Click this button to change the uploaded image.
Remove this image	Click this button to delete the uploaded image.

5.2.3 Wireless Health

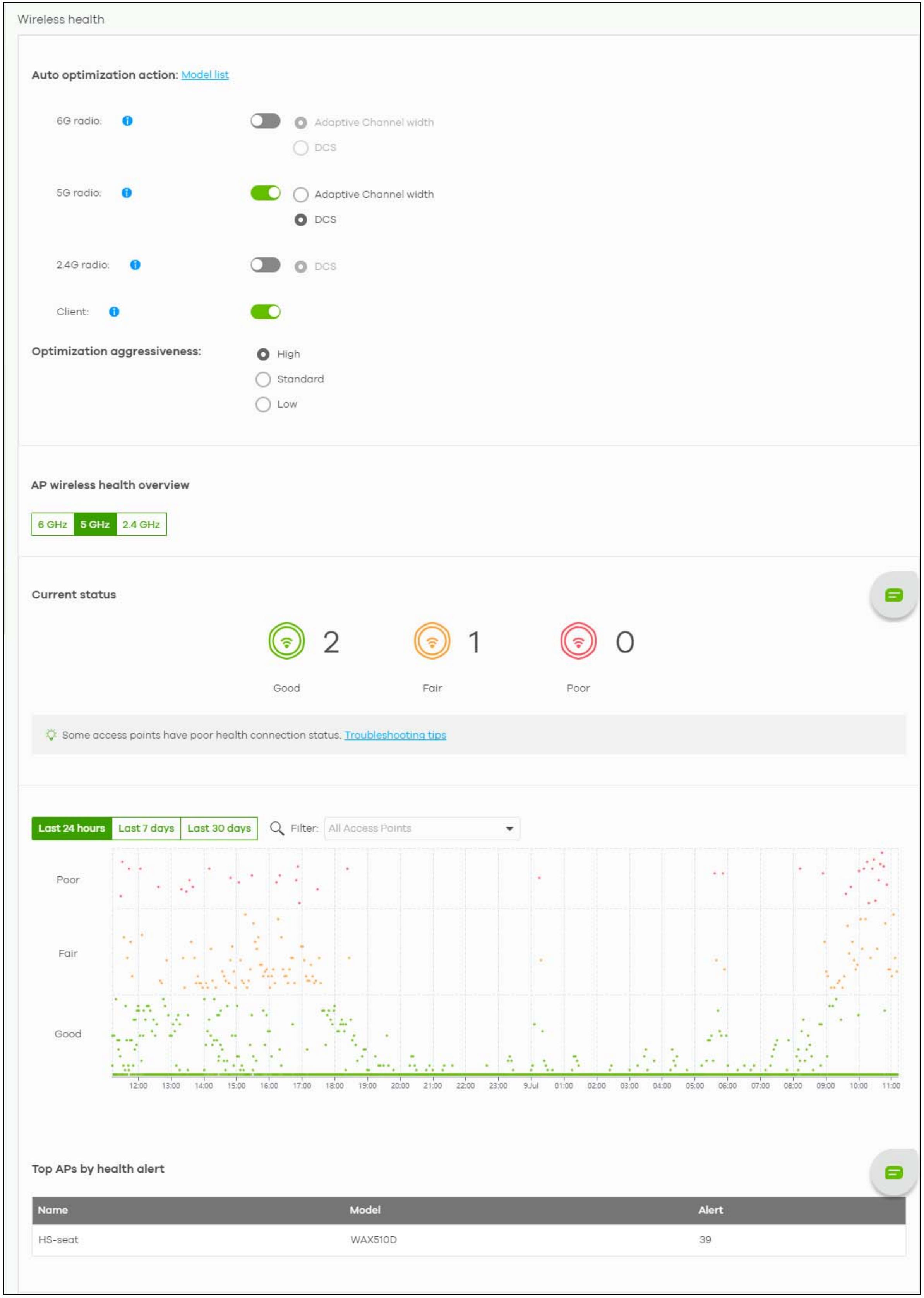
This screen lets you monitor the health of WiFi networks for your Nebula Devices and connected WiFi clients.

You can improve WiFi network performance by doing the following:

- Enable DCS (Dynamic Channel Selection) to select a radio channel with least interference
- Enable client steering to use a stronger WiFi signal
- Change channel bandwidth to reduce radio interference from other WiFi devices

Click **Site-wide** > **Monitor** > **Access points** > **Wireless health** to access this screen.

Figure 80 Site-wide > Monitor > Access points > Wireless health



Wireless health

Auto optimization action: Model list

6G radio: ○ ● Adaptive Channel width ○ DCS

5G radio: ● ○ Adaptive Channel width ● DCS

2.4G radio: ○ ● DCS

Client: ●

Optimization aggressiveness: ● High ○ Standard ○ Low

AP wireless health overview

6 GHz | 5 GHz | 2.4 GHz

Current status

2 Good

1 Fair

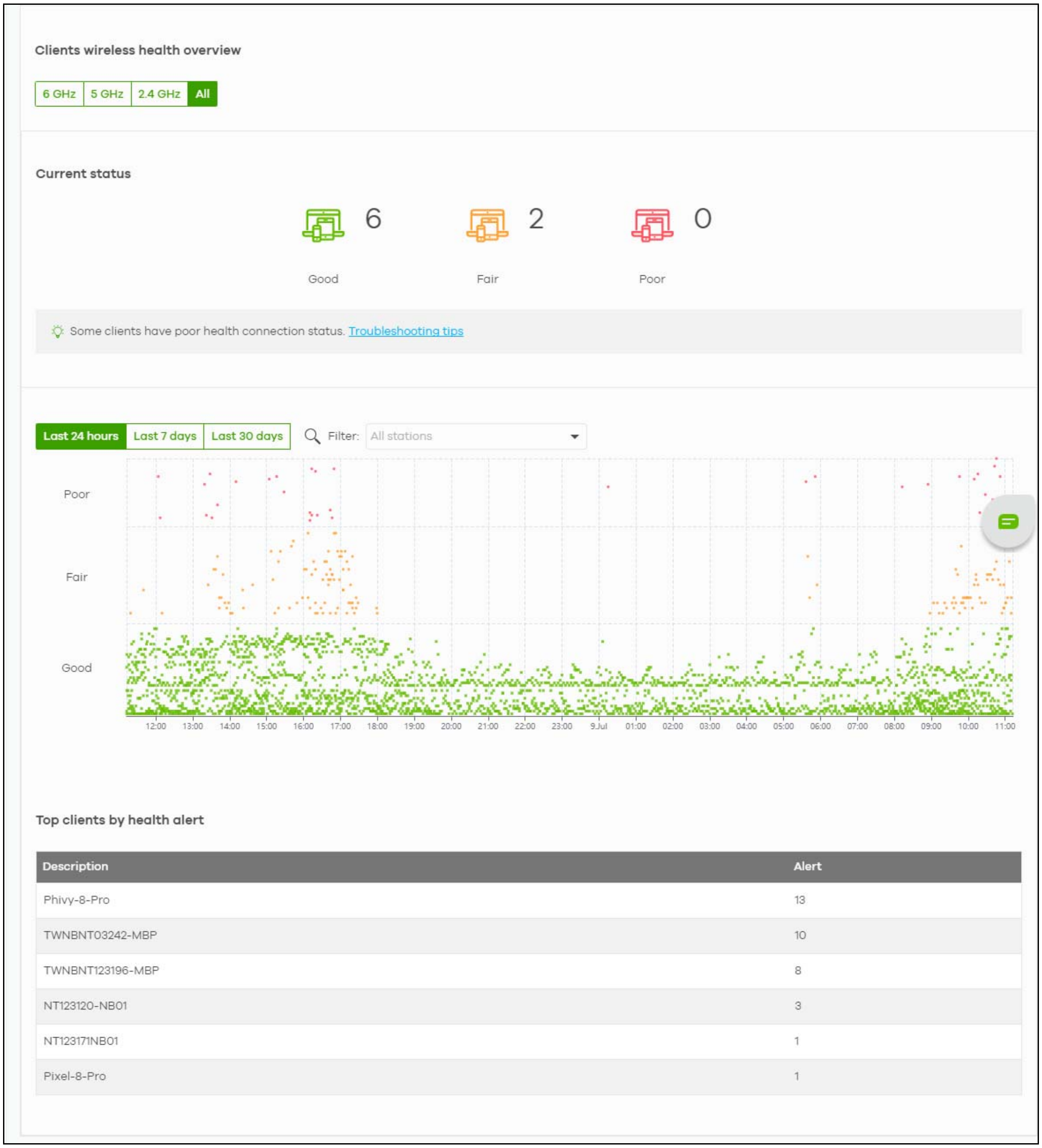
0 Poor

Some access points have poor health connection status. Troubleshooting tips

Last 24 hours | Last 7 days | Last 30 days — Filter: All Access Points

Top APs by health alert

Name	Model	Alert
HS-seat	WAX510D	39



Clients wireless health overview

Current status

6	2	0
Good	Fair	Poor

Some clients have poor health connection status. Troubleshooting tips

Top clients by health alert

Description	Alert
Phivy-8-Pro	13
TWNBNT03242-MBP	10
TWNBNT123196-MBP	8
NT123120-NB01	3
NT123171NB01	1
Pixel-8-Pro	1

The following table describes the labels in this screen.

Table 50 Site-wide > Monitor > Access points > Wireless health

LABEL	DESCRIPTION
Auto optimization action	
6G radio	Select **ON** to enable and specify how the Nebula Device improves the WiFi network performance. Otherwise, select **OFF** to disable it. • **Adaptive channel width** – select this option to have the Nebula Device change the channel bandwidth from 160 MHz to 80 MHz to reduce the radio interference with other WiFi devices. If adaptive channel width does not improve WiFi performance then the Nebula Device also performs Dynamic Channel Selection (DCS). • **DCS** (Dynamic Channel Selection) – select this option to have the Nebula Device scan and choose a radio channel that has least interference.
5G radio	Select **ON** to enable and specify how the Nebula Device improves the WiFi network performance. Otherwise, select **OFF** to disable it. • **Adaptive channel width** – select this option to have the Nebula Device change the channel bandwidth from 80 MHz to 20 MHz to reduce the radio interference with other WiFi devices. If adaptive channel width does not improve WiFi performance then the Nebula Device also performs Dynamic Channel Selection (DCS). • **DCS** (Dynamic Channel Selection) – select this option to have the Nebula Device scan and choose a radio channel that has least interference.
2.4G radio	Select **ON** to enable the Nebula Device to improve the WiFi network performance. Otherwise, select **OFF** to disable it. • **DCS** (Dynamic Channel Selection) – select this option to have the Nebula Device scan and choose a radio channel that has least interference.
Client	Select **ON** to have the Nebula Device try to steer the WiFi clients in poor health to a Nebula Device or SSID with a strong signal. Client steering to improve the signal strength is done every 30 minutes. Otherwise, select **OFF** to disable steering.
Optimization aggressiveness	The Nebula Device optimizes the WiFi network performance by doing the following:. • Change the channel bandwidth from 160 MHz to 80 MHz, or 80 MHz to 20 MHz to reduce radio interference from other wireless devices (Adaptive Channel Width). • Select a radio channel with least interference (DCS, Dynamic Channel Selection). • Direct clients to an AP with a stronger WiFi signal. There might be some disruption to the client's WiFi connections while the Nebula Device is optimizing the WiFi network. To minimize disruption, you can decide to optimize the WiFi network only when the WiFi network is below a certain level of busyness. **Low**, **Standard**, and **High** stand for different levels of busyness. The busyness level you select decides when the Nebula Device takes action to optimize the WiFi network. **Low**: Only perform WiFi network optimization action when the WiFi network traffic is below Low. **Standard**: Only perform WiFi network optimization action when the WiFi network traffic is **Low**. **High**: Only perform WiFi network optimization action when the WiFi network traffic is **Standard**, or **Low**.
AP wireless health overview	
Current status	This shows the number of supported Nebula Devices that are currently online, using the specified frequency band that are in **Good**, **Fair** or **Poor** wireless health threshold as detected by Nebula.
y-axis	The y-axis represents the state of wireless health.
x-axis	The x-axis shows the time period over which the Nebula Device health state is recorded.
Top APs by health alert	
Name	This shows the descriptive name of the Nebula Device.
Model	This shows the model number of the Nebula Device.

Table 50 Site-wide > Monitor > Access points > Wireless health (continued)

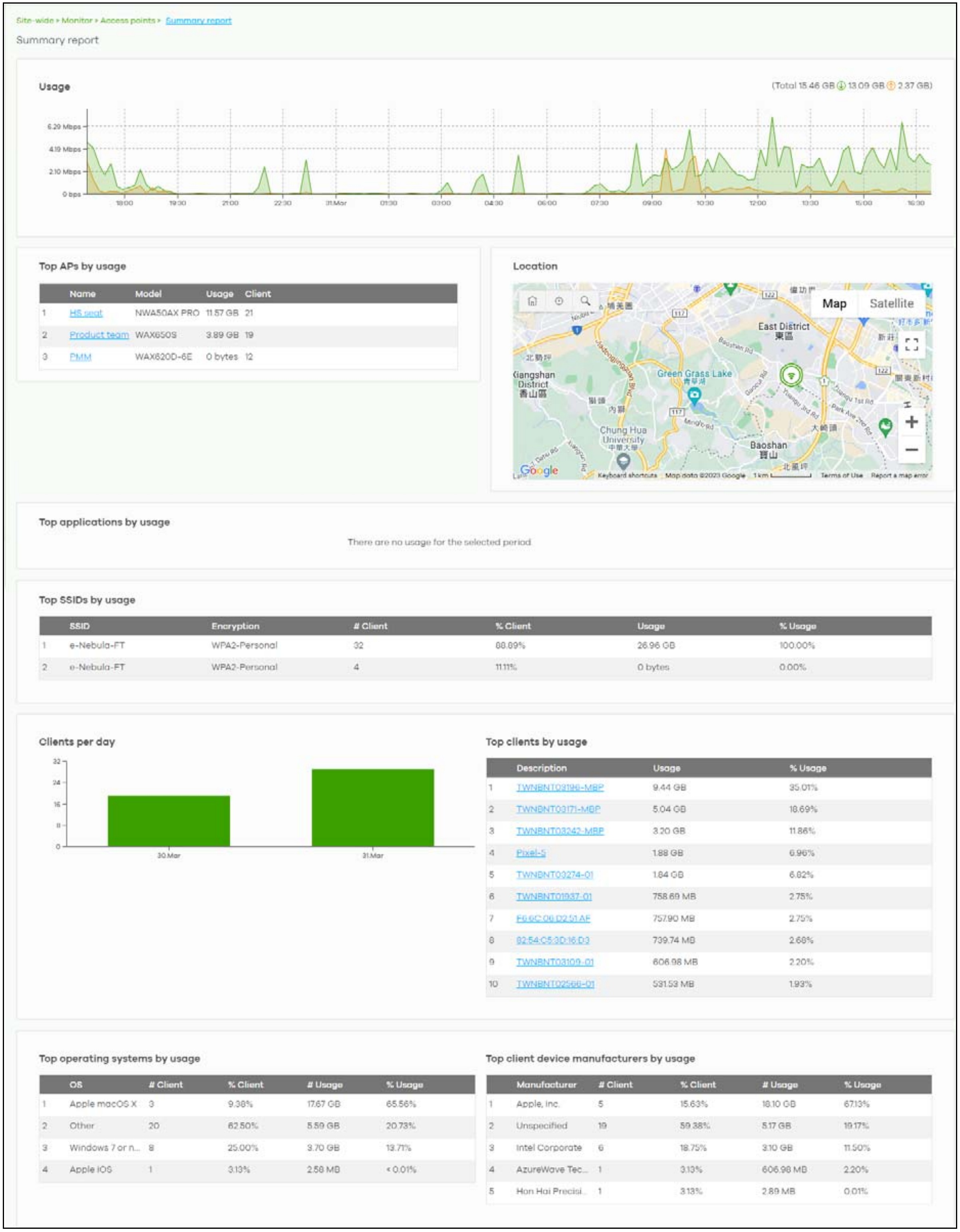
LABEL	DESCRIPTION
Alert	This shows how many times the Nebula Device is in a poor state of wireless health. The NCC generates a log when the Nebula Device is in poor wireless health. You can view the log messages in the **Site-wide** > **Monitor** > **Access points** > **Event log** screen.
Clients wireless health overview	
Current status	This shows the number of connected WiFi clients that are currently online, using the specified frequency band and in **Good**, **Fair** or **Poor** wireless health threshold as detected by Nebula.
Client health	Select to view the health of all WiFi clients which are connected to the supported Nebula Devices using the 6 GHz, 5 GHz or 2.4 GHz band. You can select to view the health report for the past day, week or month, as well as filter the WiFi station to view.
y-axis	The y-axis represents the state of wireless health.
x-axis	The x-axis shows the time period over which the client health state is recorded.
Top clients by health alert	
Description	This shows the descriptive name of the client.
Alert	This shows how many times the client is in a poor state of wireless health. The NCC generates a log when the client is in poor wireless health. You can view the log messages in the **Site-wide** > **Monitor** > **Access points** > **Event log** screen.

5.2.4 Summary Report

This screen displays network statistics for Nebula Devices of the selected site, such as bandwidth usage, top clients and/or top SSIDs.

Click **Site-wide** > **Monitor** > **Access points** > **Summary report** to access this screen.

Figure 81   Site-wide > Monitor > Access points > Summary report



Top APs by usage

	Name	Model	Usage	Client
1	HS seat	NWA50AX PRO	11.57 GB	21
2	Product team	WAX650S	3.89 GB	19
3	PMM	WAX620D-6E	0 bytes	12

Top applications by usage

There are no usage for the selected period

Top SSIDs by usage

	SSID	Encryption	# Client	% Client	Usage	% Usage
1	e-Nebula-FT	WPA2-Personal	32	88.89%	26.96 GB	100.00%
2	e-Nebula-FT	WPA2-Personal	4	11.11%	0 bytes	0.00%

Top clients by usage

	Description	Usage	% Usage
1	TWNBNT03196-MBP	9.44 GB	35.01%
2	TWNBNT03171-MBP	5.04 GB	18.69%
3	TWNBNT03242-MBP	3.20 GB	11.86%
4	Pixel-5	1.88 GB	6.96%
5	TWNBNT03274-01	1.84 GB	6.82%
6	TWNBNT01937-01	758.69 MB	2.75%
7	F6:6C:06:D2:51:AF	757.90 MB	2.75%
8	82:54:C5:3D:16:D3	739.74 MB	2.68%
9	TWNBNT03109-01	606.98 MB	2.20%
10	TWNBNT02566-01	531.53 MB	1.93%

Top operating systems by usage

	OS	# Client	% Client	# Usage	% Usage
1	Apple macOS X	3	9.38%	17.67 GB	65.56%
2	Other	20	62.50%	5.59 GB	20.73%
3	Windows 7 or n...	8	25.00%	3.70 GB	13.71%
4	Apple iOS	1	3.13%	2.58 MB	< 0.01%

Top client device manufacturers by usage

	Manufacturer	# Client	% Client	# Usage	% Usage
1	Apple, Inc.	5	15.63%	18.10 GB	67.13%
2	Unspecified	19	59.38%	5.17 GB	19.17%
3	Intel Corporate	6	18.75%	3.10 GB	11.50%
4	AzureWave Tec...	1	3.13%	606.98 MB	2.20%
5	Hon Hai Precisi...	1	3.13%	2.89 MB	0.01%

The following table describes the labels in this screen.

Table 51 Site-wide > Monitor > Access points > Summary report

LABEL	DESCRIPTION
Summary report	
Usage	
y-axis	The y-axis shows the transmission speed of data sent on this port in megabits per second (Mbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Top APs by usage	
#	This shows the ranking of the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Usage	This shows the amount of data transmitted or received by the Nebula Device.
Client	This shows how many clients are currently connecting to the Nebula Device.
Location This shows the location of the Nebula access points on the map.	
Top applications by usage	
#	This shows the ranking of the application.
Application	This shows the application name.
Category	This shows the category of the application, for example email, file sharing.
Usage	This shows the amount of data consumed by the application.
% Usage	This shows the percentage of usage for the application.
Top SSIDs by usage	
#	This shows the ranking of the SSID.
SSID	This shows the SSID network name.
Encryption	This shows the encryption method used by the SSID network.
# Client	This shows how many WiFi clients are connecting to this SSID.
% Client	This shows what percentage of associated WiFi clients are connecting to this SSID.
Usage	This shows the total amount of data transmitted or received by clients connecting to this SSID.
% Usage	This shows the percentage of usage for the clients connecting to this SSID.
Clients per day	
y-axis	The y-axis represents the number of clients.
x-axis	The x-axis represents the date.
Top clients by usage	
#	This shows the ranking of the client.
Description	This shows the descriptive name or MAC address of the client.
Usage	This shows the total amount of data transmitted and received by the client.
% Usage	This shows the percentage of usage for the client.
Top operating systems by usage	
#	This shows the ranking of the operating system.
OS	This shows the operating system of the client device.
# Client	This shows how many client devices use this operating system.

Table 51 Site-wide > Monitor > Access points > Summary report (continued)

LABEL	DESCRIPTION
% Client	This shows the percentage of top client devices which use this operating system.
# Usage	This shows the amount of data consumed by the client device on which this operating system is running.
% Usage	This shows the percentage of usage for top client devices which use this operating system.
Top client device manufacturers by usage	
#	This shows the ranking of the manufacturer.
Manufacturer	This shows the manufacturer name of the client device.
# Client	This shows how many client devices are made by the manufacturer.
% Client	This shows the percentage of top client devices which are made by the manufacturer.
# Usage	This shows the amount of data consumed by the client device.
% Usage	This shows the percentage of usage for the client device.

5.3 Configure

Use the **Configure** menus to set the WiFi security settings for Nebula Devices of the selected site.

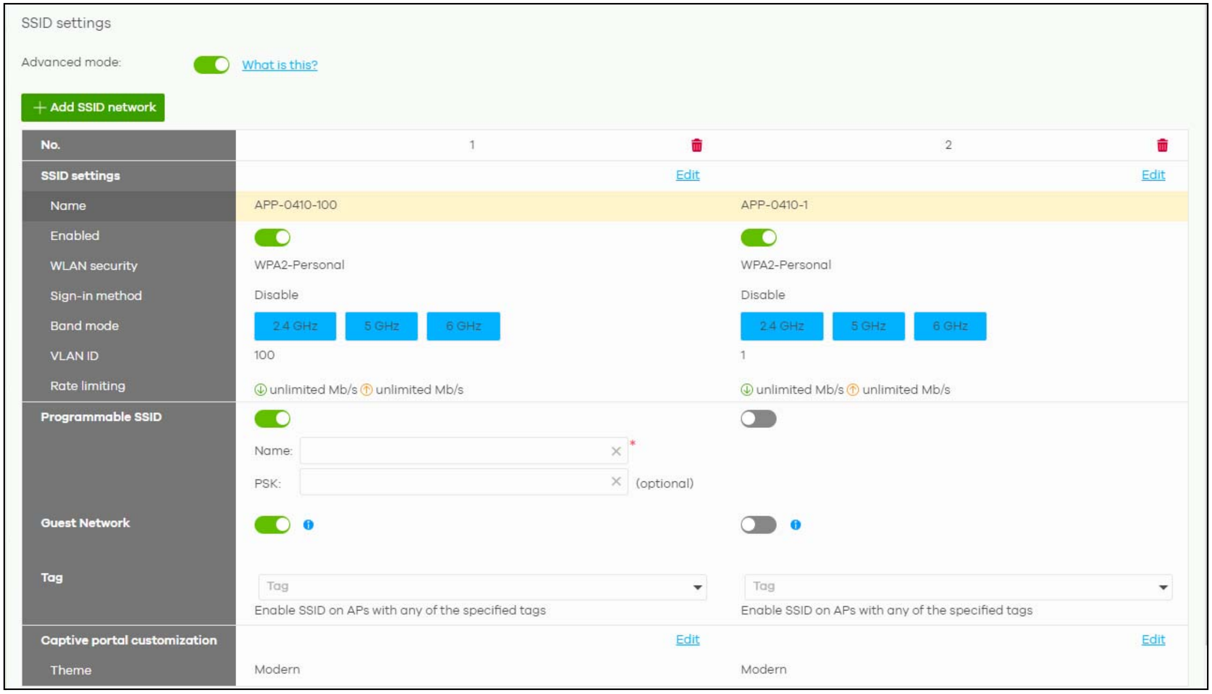
5.3.1 SSID Settings

This screen allows you to configure up to 24 different SSID profiles for your Nebula Devices. An SSID, or Service Set IDentifier, is basically the name of the WiFi network to which a WiFi client can connect. The SSID appears as readable text to any device capable of scanning for WiFi frequencies (such as the WiFi adapter in a laptop), and is displayed as the WiFi network name when a person makes a connection to it.

Note: The WiFi SSID settings on the NCC can currently support AP and SCR models only. At the time of writing, the Nebula mobile routers do not support this feature. If you are using a Nebula mobile router, configure the SSID settings through the mobile router's local Web Configurator.

Click **Site-wide** > **Configure** > **Access points** > **SSID settings** to access this screen.

Figure 82 Site-wide > Configure > Access points > SSID settings



SSID settings

Advanced mode: ● What is this?

+ Add SSID network

No.	1	2
SSID settings	Edit	Edit
Name	APP-0410-100	APP-0410-1
Enabled	●	●
WLAN security	WPA2-Personal	WPA2-Personal
Sign-in method	Disable	Disable
Band mode	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
VLAN ID	100	1
Rate limiting	unlimited Mb/s unlimited Mb/s	unlimited Mb/s unlimited Mb/s
Programmable SSID	● Name: * PSK: (optional)	○
Guest Network	●	○
Tag	Tag Enable SSID on APs with any of the specified tags	Tag Enable SSID on APs with any of the specified tags
Captive portal customization	Edit	Edit
Theme	Modern	Modern

The following table describes the labels in this screen.

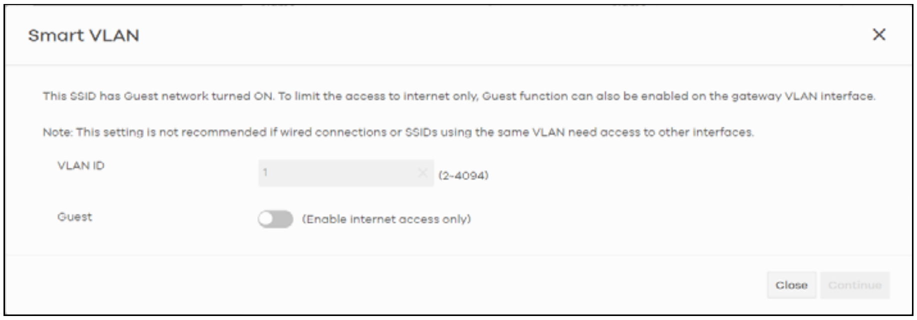
Table 52 Site-wide > Configure > Access points > SSID settings

LABEL	DESCRIPTION
Advanced mode	Select Off to disable **Advanced mode**. This allows you to create SSID profiles by only specifying an SSID name and optional password. NCC sets all other WiFi settings to default.
+ Add SSID network	Click this button to configure up to eight different SSID profiles for your Nebula Device. To configure more than eight SSID profiles (up to 24), enable **AP grouping** in **Site-wide** > **Configure** > **Access points** > **AP & port settings**. For details, see Section 5.3.7 on page 344. Note: Only four SSIDs are allowed on each SCR 50AXE. Note: Only eight SSIDs are allowed on each Nebula Device Access Points and USG LITE 60AX. Use the **Tag** field to assign up to eight AP groups per Nebula Device. A blank **Tag** field is counted as an AP group. Note: Disabling **AP grouping** in **Site-wide** > **Configure** > **Access points** > **AP & port settings** will hide **SSID9** to **SSID24**, but keep the settings.
No.	This shows the index number of this profile.
delete	Click this icon to remove the SSID profile.
SSID settings	
Edit	Click this button to go to the **SSID advanced settings** screen and configure WiFi security and advanced settings, such as band selection, enable assisted roaming and U-APSD (Unscheduled automatic power save delivery). See Table 53 on page 323 for more information on assisted roaming and U-APSD.
Name	This shows the SSID name for this profile. Click the text box and enter a new SSID if you want to change it.
Enabled	Click to turn on or off this profile.
WLAN security	This shows the encryption method used in this profile.

Table 52 Site-wide > Configure > Access points > SSID settings (continued)

LABEL	DESCRIPTION
Sign-in method	This shows the authentication method used in this profile or **Disable**.
Band mode	This shows whether the SSID use either 2.4 GHz band, 5 GHz band, or the 6 GHz band.
VLAN ID	This shows the ID number of the VLAN to which the SSID belongs.
Rate limiting	This shows the maximum incoming/outgoing transmission data rate (in Kbps) on a per-station basis.
Programmable SSID	Select On to have each Nebula Device that uses this SSID generate a unique SSID name and pre-shared key (PSK) based on the Nebula Device's model name, serial number, or MAC address. Use this method when you require more than 8 unique SSID names on your site. For example, a hotel can install a Nebula Device in each room and then have each Nebula Device broadcast a unique SSID based on the room number: FreeWiFi_Room1, FreeWiFi_Room2, FreeWiFi_Room3, and so on.
Name	**Name**: Enter a programmable SSID name in the format PREFIX+VALUE(X). This name overrides the original SSID name. • PREFIX: Optional prefix to add to the SSID, for example "FreeWiFi_". To use "$" in the SSID name, enter "$$" • VALUE: Specify a Nebula Device value to use to generate the SSID name. Use one of the following: $AP = Nebula Device device name. $MAC = Nebula Device MAC address. $SN = Nebula Device serial number. • X: Specify how many characters of the Nebula Device value to use in the SSID. A positive number means the first X characters, and a negative number means the last X characters. Example: *FreeWiFi_Room$AP(–3)* generates an SSID called "FreeWiFi_Room" + the last three characters of the access point device name.
PSK	**PSK**: Enter an optional programmable PSK in the format GENTYPE(Y). • GENTYPE: Specify how the Nebula Device will generate a random PSK. $GENMIX = The Nebula Device generates a mix of random letters and numbers. $GENNUM = The Nebula Device generates a mix of random numbers only. $AP = Nebula Device device name. $MAC = Nebula Device MAC address. $SN = Nebula Device serial number. Y = Specify the length of the PSD. The minimum length is 8. Example 1: $GENNUM(10) generates a unique 10-character PSK for this SSID, consisting only of numbers. Example 2: $MAC(-5)$SN(-5) uses the MAC address's last 5 characters and the serial number's last 5 characters (for example, 8E3AE02451). Example 3: ZYXEL-$GENMIX(4) appends the fixed characters 'ZYXEL' and generates a unique 4-character mix of random letters and numbers (for example, ZYXEL-3c4d). Note: You can specify a fixed PSK for this SSID at **Site-wide** > **Configure** > **Access points / Security router** > **SSID advanced settings**.

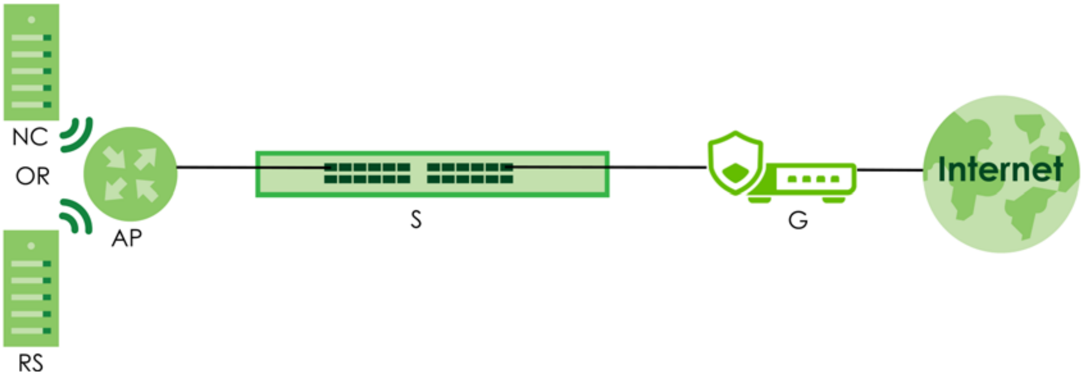
Table 52   Site-wide > Configure > Access points > SSID settings (continued)

LABEL	DESCRIPTION
Guest Network	Select On to set this WiFi network as a guest network. Layer 2 isolation and intra-BSS blocking are automatically enabled on the SSID. WiFi clients connecting to this SSID can access the Internet through the Nebula Device but cannot directly connect to the LAN or the WiFi clients in the same SSID or any other SSIDs. Note: In your VLAN-enabled network, if the SSID's gateway MAC address and the Nebula Device's gateway MAC address are different and belong to different VLANs, you need to manually add the SSID's gateway MAC address to the layer 2 isolation list. See Section 5.3.2 on page 320. Note: If you have a Nebula Security Appliance installed in the site but the gateway interface with the same VLAN ID is not configured as a guest interface, **Smart Guest/VLAN network tip, click here.** displays after you select **On**. Click **here** to open a screen where you can directly select to use the interface as a Guest interface.  Smart VLAN This SSID has Guest network turned ON. To limit the access to internet only, Guest function can also be enabled on the gateway VLAN interface. Note: This setting is not recommended if wired connections or SSIDs using the same VLAN need access to other interfaces. VLAN ID: 1 (2-4094) Guest: ○ (Enable internet access only)
Broadcasting APs	Select **All APs** or specify the AP to use this SSID profile. Note: This field only appears when you have a Security Router in your site.
Tag	Enter or select the tags you created for Nebula Devices in the **Site-wide** > **Devices** > **Access points** / **Security router** / **Mobile router** screen or **Site-wide** > **Devices** > **Access points** / **Security router** / **Mobile router: Details** screen. Only the Nebula Devices with the specified tag will broadcast this SSID. If you leave this field blank, all the Nebula Devices on the site will broadcast this SSID.
Note: At the time of writing, the following rules apply when the site includes both Access Point(s) and a Security Router: • Specify the Access Point(s) in Broadcasting APs and Tag to broadcast this SSID. • The Security Router must be specified in Broadcasting APs to broadcast this SSID.	
Captive portal customization	
Edit	Click this button to go to the **Captive portal** screen and configure the captive portal settings. See Section 5.3.3 on page 330.
Theme	If captive portal is enabled, this shows the name of the captive portal page used in this profile.

5.3.2 SSID Advanced Settings

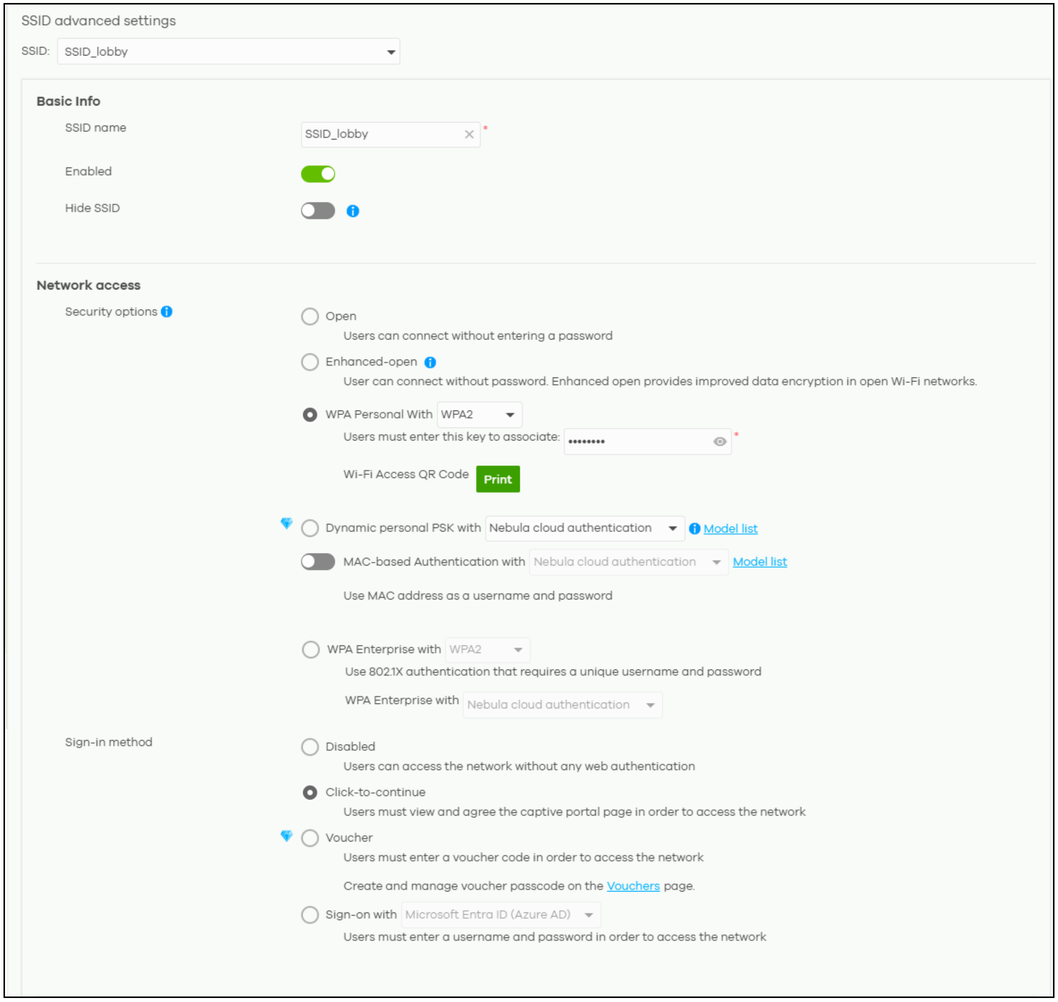
Use this screen to configure the WiFi security, L2 isolation, intra-BSS traffic blocking and walled garden settings for the SSID profiles.

As shown in the next figure, the Nebula (**AP**) can connect wirelessly to the Nebula Cloud server (**NC**) or RADIUS server (**RS**) for WPA2-Enterprise authentication.



Click **Site-wide** > **Configure** > **Access points** > **SSID advanced settings** to access this screen.

Figure 83 Site-wide > Configure > Access points > SSID advanced settings Part 1



SSID advanced settings

SSID: SSID_lobby ▾

Basic Info

SSID name: SSID_lobby ✕ *

Enabled: (on)

Hide SSID: (off) ⓘ

Network access

Security options ⓘ

○ Open
Users can connect without entering a password

○ Enhanced-open ⓘ
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.

● WPA Personal With WPA2 ▾
Users must enter this key to associate: •••••••• *
Wi-Fi Access QR Code **Print**

○ Dynamic personal PSK with Nebula cloud authentication ▾ ⓘ Model list

(off) MAC-based Authentication with Nebula cloud authentication ▾ Model list
Use MAC address as a username and password

○ WPA Enterprise with WPA2 ▾
Use 802.1X authentication that requires a unique username and password
WPA Enterprise with Nebula cloud authentication ▾

Sign-in method

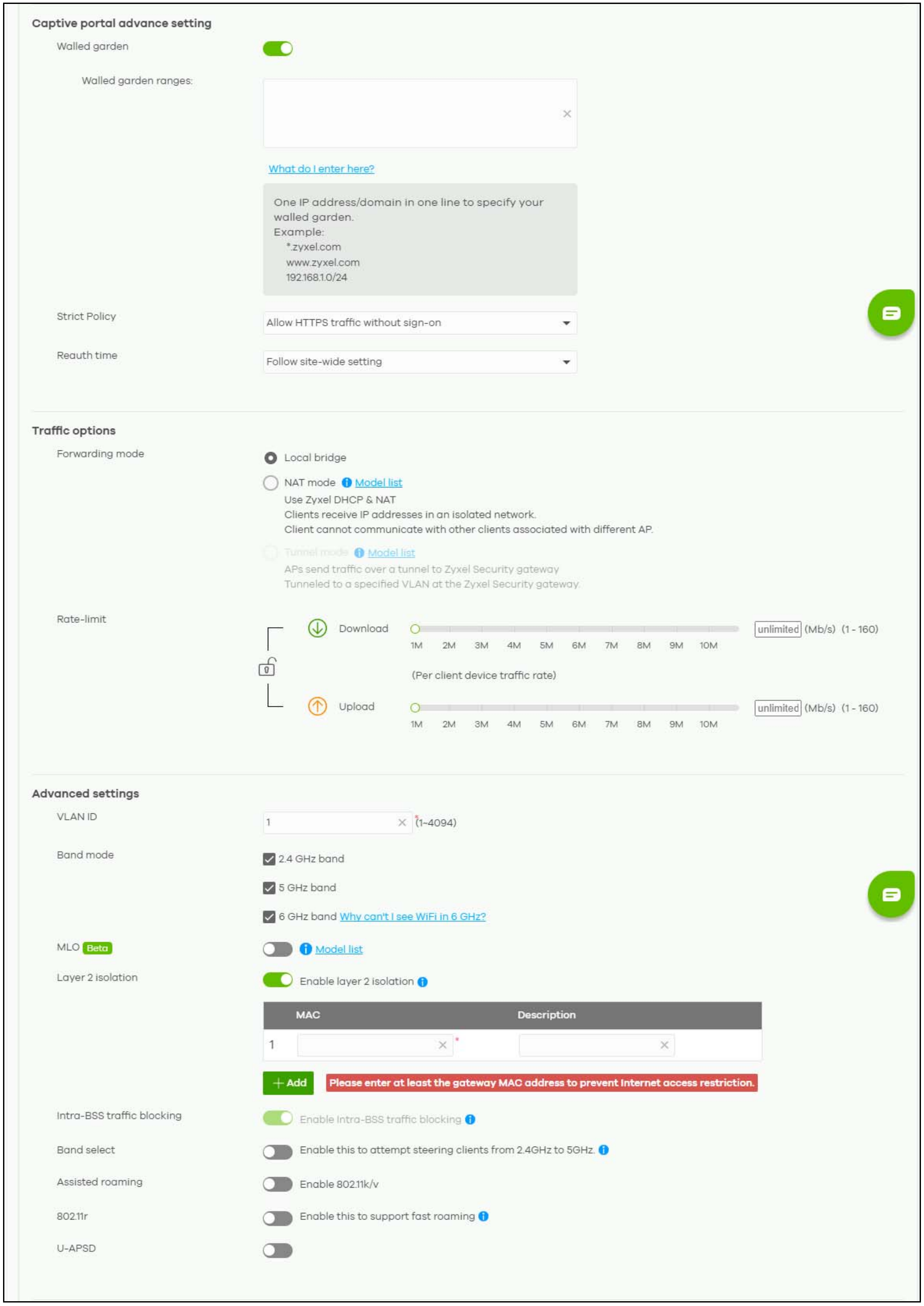
○ Disabled
Users can access the network without any web authentication

● Click-to-continue
Users must view and agree the captive portal page in order to access the network

○ Voucher
Users must enter a voucher code in order to access the network
Create and manage voucher passcode on the Vouchers page.

○ Sign-on with Microsoft Entra ID (Azure AD) ▾
Users must enter a username and password in order to access the network

Figure 84 Site-wide > Configure > Access points > SSID advanced settings Part 2



Captive portal advance setting

Walled garden: on

Walled garden ranges:

What do I enter here?

One IP address/domain in one line to specify your walled garden.
Example:
*.zyxel.com
www.zyxel.com
192.168.1.0/24

Strict Policy: Allow HTTPS traffic without sign-on

Reauth time: Follow site-wide setting

Traffic options

Forwarding mode:

● Local bridge

○ NAT mode Model list
Use Zyxel DHCP & NAT
Clients receive IP addresses in an isolated network.
Client cannot communicate with other clients associated with different AP.

○ Tunnel mode Model list
APs send traffic over a tunnel to Zyxel Security gateway
Tunneled to a specified VLAN at the Zyxel Security gateway.

Rate-limit:

Download unlimited (Mb/s) (1 - 160)

(Per client device traffic rate)

Upload unlimited (Mb/s) (1 - 160)

Advanced settings

VLAN ID: 1 (1~4094)

Band mode:

☑ 2.4 GHz band

☑ 5 GHz band

☑ 6 GHz band Why can't I see WiFi in 6 GHz?

MLO Beta: off Model list

Layer 2 isolation: on Enable layer 2 isolation

MAC	Description
1	

Please enter at least the gateway MAC address to prevent Internet access restriction.

Intra-BSS traffic blocking: on Enable Intra-BSS traffic blocking

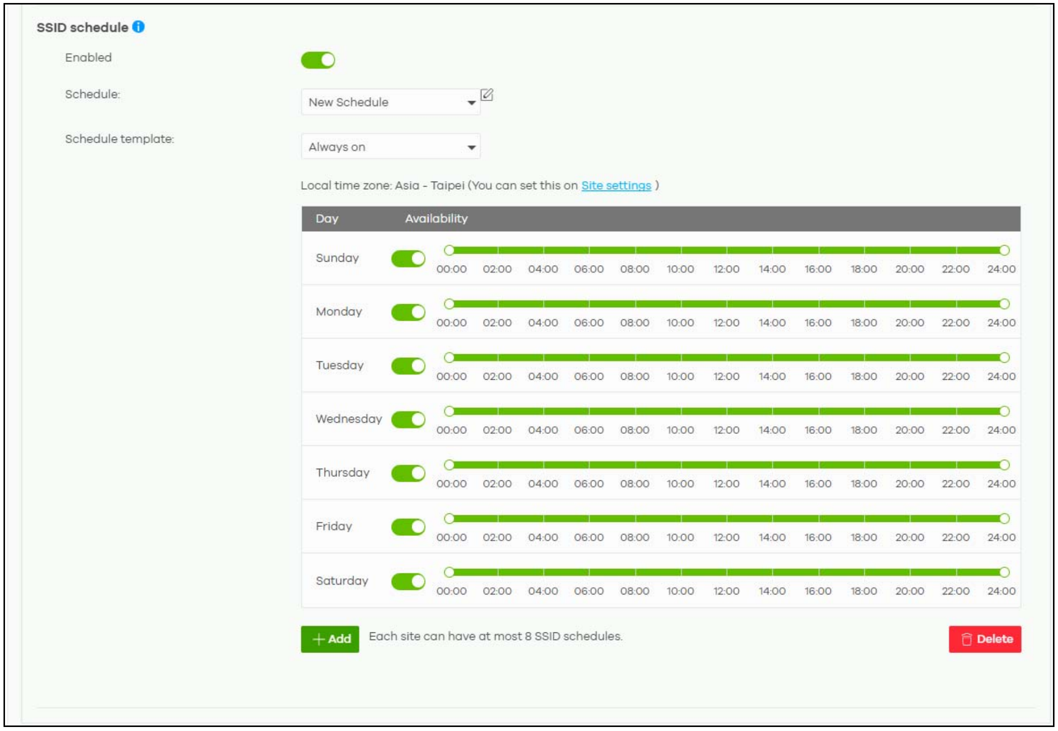
Band select: off Enable this to attempt steering clients from 2.4GHz to 5GHz.

Assisted roaming: off Enable 802.11k/v

802.11r: off Enable this to support fast roaming

U-APSD: off

Figure 85 Site-wide > Configure > Access points > SSID advanced settings Part 3



SSID schedule

Enabled

Schedule: New Schedule

Schedule template: Always on

Local time zone: Asia - Taipei (You can set this on Site settings)

Day	Availability
Sunday	00:00 – 24:00
Monday	00:00 – 24:00
Tuesday	00:00 – 24:00
Wednesday	00:00 – 24:00
Thursday	00:00 – 24:00
Friday	00:00 – 24:00
Saturday	00:00 – 24:00

Each site can have at most 8 SSID schedules.

The following table describes the labels in this screen.

Table 53 Site-wide > Configure > Access points > SSID advanced settings

LABEL	DESCRIPTION
SSID advanced settings	Select the SSID profile to which the settings you configure here is applied.
Basic information	
SSID name	This shows the SSID name as it appears to WiFi clients. Click the text box and enter a new SSID if you want to change it.
Enabled	Click this to enable the SSID to be discoverable by WiFi clients.
Hide SSID	Click this if you want to hide your SSID from WiFi clients. This tells any WiFi clients in the vicinity of the Nebula Device using this SSID profile not to display its SSID name as a potential connection. When an SSID is “hidden” and a WiFi client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your WiFi connection setup screens. Note: This field only appears when you have a Nebula Device AP and SCR 50AXE in your site.
Network access	Note: You cannot enable MAC authentication, 802.1X authentication and web authentication at the same time. Note: User accounts can be created and authenticated using the NCC user database. See Section on page 726.

Table 53   Site-wide > Configure > Access points > SSID advanced settings (continued)

LABEL	DESCRIPTION
Security options	Select **Open** to allow any client to associate this network without any data encryption or authentication. Select **Enhanced-open** to allow any client to associate this network without any password but with improved data encryption. Upon selecting **Enhanced-open** or **WPA Personal With WPA3**, **transition mode** generates two VAP so devices that do not support **Enhanced-Open**/**WPA Personal With WPA3** can connect using **Open**/**WPA Personal With WPA2** network. This is always **on** at the time of writing. Select **WPA Personal With (WPA1**/**WPA2**/**WPA3)** and enter a pre-shared key from 8 to 63 case-sensitive keyboard characters to enable WPA1/2/3-PSK data encryption. Upon selecting **WPA Personal With WPA3**, Nebula Devices that do not support it will revert to WPA2. • Turn on **802.11r** to enable IEEE 802.11r fast roaming on the access point. 802.11r fast roaming reduces the delay when the clients switch from one Nebula Device to another by allowing security keys to be stored on all Nebula Devices in a network. Information from the original association is passed to the new Nebula Device when the client roams. The client does not need to perform the whole 802.1x authentication process. Click **Print** to display the QR code that includes the password for quick access. You can save the QR code as PDF. To test, use a smartphone to scan the QR code. Click to join the network. The client device should connect to WiFi directly without asking the password. Select **Dynamic personal psk with** to have every user connect to the SSID using a unique pre-shared key (PSK) that is linked to their user account; together with **My RADIUS server** to use an external RADIUS server. Or select **Nebula cloud authentication** to use the NCC for MAC authentication. This allows you to revoke a user's WiFi network access by disabling their account. Enter an optional backup key in **Users can enter this backup key to associate** for clients who forget their DPPSK but still want to connect to the SSID. Note: DPPSK only supports **Click-to-continue** in the **Sign-in method**. Note: Only one SSID can be configured with DPPSK. After enabling this option, you must create one or more DPPSK users in the site or organization at **Site-wide** > **Configure** > **Cloud authentication** > **Account Type** > **DPPSK**. • For details on creating a site DPPSK user, see Section 4.9.3.3 on page 293. • For details on creating organization DPPSK users, see Section 12.4.7.3 on page 713. Turn on **MAC-based Authentication with** to authenticate WiFi clients by their MAC addresses together with **My RADIUS server** to use an external RADIUS server. Or select **Nebula cloud authentication** to use the NCC for MAC authentication. Select **WPA-Enterprise with** to enable 802.1X secure authentication. You can select **My RADIUS server** to use an external RADIUS server or select **Nebula cloud authentication** to use the NCC for 802.1X authentication. • Turn on **802.11r** to enable IEEE 802.11r fast roaming on the Nebula Device. 802.11r fast roaming reduces the delay when the clients switch from one Nebula Device to another by allowing security keys to be stored on all Nebula Devices in a network. Information from the original association is passed to the new Nebula Device when the client roams. The client does not need to perform the whole 802.1x authentication process. • Select **Two-Factor Authentication** to require that the user log in using both their password and a Google Authenticator code. To log in, users must have Two-Factor Authentication enabled on their account and have setup Google Authenticator on their mobile device. Select **Enable on RAP only** to only require Two-Factor Authentication when accessing the network through a remote access point (RAP).

Table 53 Site-wide > Configure > Access points > SSID advanced settings (continued)

LABEL	DESCRIPTION
Sign-in method	Select **Disabled** to turn off web authentication. Select **Click-to-continue** to block network traffic until a client agrees to the policy of user agreement. Note: After enabling **Click-to-continue**, the Nebula Device creates a user account with user name "clicktocontinue_X_Y", where X is the radio type (1 = 2.4 GHz, 2 = 5 GHz) and Y is the SSID number (1–8) of the SSID profile. The Nebula Device uses this account to authenticate clients who agree to the terms of the click-to-continue page. Select **Voucher** to require that a user logs in with a voucher code. For details on vouchers, see Section 5.2.2 on page 306. Note: Vouchers cannot be enabled if Dynamic Personal Pre-Shared Key (DPPSK) or WPA Enterprise are enabled. Select **Sign-on with** and: • select **Nebula cloud authentication** to block network traffic until a client authenticates with the NCC through the specifically designated web portal page. • select **My RADIUS server** to block network traffic until a client authenticates with an external RADIUS server through the specifically designated web portal page. Enable **MAC authentication fallback** when both RADIUS-based MAC authentication and web authentication are implemented. **Scenario 1**: When MAC authentication fails. A WiFi client tries to connect to the WiFi network using MAC authentication (RADIUS server). If MAC authentication fails, he will fall back to web authentication. The WiFi client needs to provide a user name and password for web authentication. **Scenario 2**: When MAC authentication is successful. A WiFi client tries to connect to the WiFi network and passes MAC authentication. Web authentication is then skipped. Note: When **MAC authentication fallback** is enabled, the WiFi client can avoid network disassociations due to MAC authentication failure. • select **Facebook** to block network traffic until a client authenticates with the NCC using Facebook Login. Facebook Login is a secure and quick way for users to log into your app or website using their existing Facebook accounts. If you get the App ID for your app at the Facebook developers site, you can enter your Facebook app ID to obtain more information about your users using Facebook Analytics, such as user activity, age, gender, and so on. Note: **Facebook Wi-Fi** authentication is no longer available (grayed-out). Meta Platforms, Inc. has stopped offering the Facebook Wi-Fi service. If you have been using **Facebook Wi-Fi** authentication, select another authentication method to continue your WiFi service. • select **Microsoft Entra ID (Azure AD)** to block network traffic until a client authenticates with the NCC using Microsoft's cloud-based identity and access management service. Then click **Download Metadata** / **Upload Metadata** file that contains the configuration details. The metadata file contains all the callback URLs (where to send the successful/ unsuccessful authentication responses to) as well as the certificates to use when communicating between the trusted Service Provider (SP) and Identity Provider (IdP). Note: Only one SSID can use Microsoft Entra ID authentication at a time. Since Microsoft Entra ID authentication is a Professional tier license feature, the SSID will be disabled when the organization's license has expired.

Table 53 Site-wide > Configure > Access points > SSID advanced settings (continued)

LABEL	DESCRIPTION
RADIUS server	This field is available only when you select to use the following: • **MAC-based Authentication with My RADIUS server** or **WPA2-Enterprise with My RADIUS server** in the **WLAN security** field, or • when you select **Sign-on with My RADIUS server** in the **Sign-in method** field. WPA2-Enterprise features the following: • Over-the-air encryption for wireless network security • Uses 128-bit encryption keys and dynamic session keys to guarantee the privacy of wireless networks as well as enterprise security. Click **Add** to specify the IP address/domain name, port number, and shared secret password of the RADIUS server to be used for authentication. Note: User must enter the **Account Format** and **Calling Station ID** when **MAC authentication fallback** field is enabled. Note: Nebula Devices with firmware version 5.50 or older will turn OFF this SSID when the **Host** field is configured with a domain name.
NAS Identifier	Enter the Network Access Server (**NAS**) **Identifier** on the Nebula Device to identify the Nebula Device to the RADIUS server, if required. This might be necessary if there are multiple Nebula Devices behind NAT using the same public WAN IP address for the RADIUS server.
RADIUS accounting	This field is available only when you select to use **WPA2-Enterprise with My RADIUS server** in the **WLAN security** field, or when you select **Sign-on with My RADIUS server** in the **Sign-in method** field. Select **RADIUS accounting enabled** to enable user accounting through an external RADIUS server. Select **RADIUS accounting disabled** to disable user accounting through an external RADIUS server.
RADIUS accounting servers	If you select **RADIUS accounting enabled**, click **Add** to specify the IP address, port number and shared secret password of the RADIUS server to be used for accounting.
Captive portal advance setting	
Walled garden	Select **On** to enable Walled garden.
Walled garden ranges	This field is not configurable if you set **Sign-in method** to **Disable**. With a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example. Select to turn on or off the walled garden feature. Specify walled garden web site links, which use a (wildcard) domain name or an IP address for web sites that all users are allowed to access without logging in.
Self-registration	This field is available only when you set **Sign-in method** to **Sign-on with Nebula Cloud authentication**. Select **Allow users to create accounts with auto authorized** or **Allow users to create accounts with manual authorized** to display a link in the captive portal login page. The link directs users to a page where they can create an account before they authenticate with the NCC. For **Allow users to create accounts with manual authorized**, users cannot log in with the account until the account is authorized and granted access. For **Allow users to create accounts with auto authorized**, users can just use the registered account to log in without administrator approval. Select **Don’t allow users to create accounts** to not display a link for account creation in the captive portal login page.

Table 53 Site-wide > Configure > Access points > SSID advanced settings (continued)

LABEL	DESCRIPTION
Simultaneous login limit	This field is available only when you set **Sign-in method** to **Sign-on with My RADIUS server** or **Sign-on with Nebula Cloud authentication**. Select **Unlimited** if you allow users to log in as many times as they want as long as they use different IP addresses. Select **1** to **10** if you do NOT allow users to have simultaneous logins.
Strict Policy	Select **Allow HTTPS traffic without sign-on** to let users use HTTPS to access a web site without authentication. Select **Block all access until sign-on** to block both HTTP and HTTPS traffic until users authenticate their connections. The portal page will not display automatically if users try to access a web site using HTTPS. They will see an error message in the web screen.
Reauth time	Select **Follow site-wide setting** or select a specific time the user can be logged in through the captive portal in one session before having to log in again.
NCAS disconnect behavior	This field is available only when: • you set **Sign-in method** to **Sign-on with Nebula Cloud authentication** • you enable **MAC-based Authentication with** and you select **Nebula cloud authentication** Select **Allowed** to allow any users to access the network without authentication when the NCAS (Nebula Cloud Authentication Server) is not reachable. Select **Limited** to allow only the currently connected users or the users in the white list to access the network.
Traffic options	
Forwarding mode	Select **Local bridge** if you only want to access the Internet. Network traffic from clients connected to the Nebula Device is sent directly to the network through the access point's local gateway. Select **NAT mode** to have the Nebula Device create a DHCP subnet with its own NAT for the SSID. This simplifies WiFi network management, as you do not need to configure a separate DHCP server. The following Nebula Device features do not work when **NAT mode** is enabled: • 802.11r • Layer2 isolation • Dynamic VLAN (cloud authentication, RADIUS server) Note: In NAT mode, clients cannot communicate with clients connected to a different Nebula Device. Select **Tunnel mode** to forward broadcast and multicast traffic using an existing VLAN interface in the Nebula Device (Security Firewall device). This is the interface you configured in **Site-wide** > **Configure** > **Security gateway** > **Interface addressing**. Note: Tunnel mode is available for Nebula Device (Security Firewall device) only. In Tunnel mode, make sure the ICMP protocol is enabled. See **Site-wide** > **Configure** > **Firewall**: **Policy routes/Traffic shaping** and **Site-wide** > **Configure** > **Firewall** > **Security policy**: **Action** for information. Select **Tunnel mode** for clients that want to access the network behind the Nebula Device. Select **Local bridge** for clients that want to access the Internet, but you do not want them to access the network behind the Nebula Device.

Table 53   Site-wide > Configure > Access points > SSID advanced settings (continued)

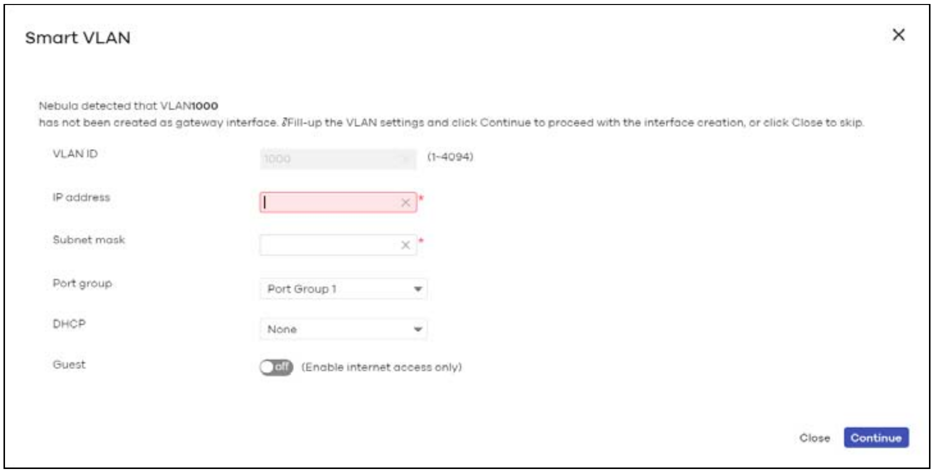
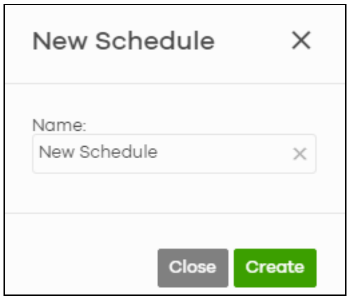
LABEL	DESCRIPTION
Rate-limit	Set the maximum data download and upload rates in Kbps, on a per-station basis. Click a lock icon to change the lock state. If the lock icon is locked, the limit you set applies to both download and upload traffic. If the lock is unlocked, you can set download and upload traffic to have different transmission speeds. Note: This feature is not available when you enable MLO.
Advanced settings	
VLAN ID	Enter the ID number of the VLAN to which the SSID belongs. Note: If you have a Nebula Security Appliance installed in the site but did not configure an identical VLAN interface on the gateway, **Smart Guest/VLAN network tip, click here**. displays. Click **here** to open a screen where you can create a gateway interface with the specified VLAN ID.  Smart VLAN Nebula detected that VLAN**1000** has not been created as gateway interface. ‍♂Fill-up the VLAN settings and click Continue to proceed with the interface creation, or click Close to skip. VLAN ID 1000 (1-4094) IP address * Subnet mask * Port group Port Group 1 DHCP None Guest off (Enable internet access only) Note: If you select **Tunnel mode** in **Forwarding mode**, the **Tunnel to gateway interface** field appears. Select **LAN1** as the default.
Band mode	Select to have the SSID use either **2.4GHz band**, **5GHz band**, or **6GHz band** only.

Table 53 Site-wide > Configure > Access points > SSID advanced settings (continued)

LABEL	DESCRIPTION
MLO	Select **MLO** to allow a WiFi7 client to connect to the WiFi7 Nebula Device using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. **MLO** makes WiFi7 ideal for streaming 4K / 8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Note: The following are not supported when MLO is selected. • WiFi aid (see **Site-wide** > **Clients** > **WiFi Aid** for more details on WiFi aid) • Band steering (see **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**: **Advanced settings** and **Site-wide** > **Configure** > **Security router** > **SSID advanced settings**: **Advanced settings** for more details on band steering) • WiFi fast roaming (see **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**: **Network access** and **Site-wide** > **Configure** > **Security router** > **SSID advanced settings**: **Network access** for more details on WiFi fast roaming) • Smart Mesh (see **Site-wide** > **Devices** > **Access points**: **Details** for more details on Smart Mesh) • Rate limit (see **Site-wide** > **Configure** > **Access points** > **SSID settings** for more details on rate limit) • RADIUS accounting (see **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**: **Network access** for more details on RADIUS accounting) • Traffic shaping (see **Site-wide** > **Configure** > **Access points** > **Traffic shaping** and **Site-wide** > **Configure** > **Security gateway** > **Traffic shaping** for more details) • Dynamic Personal Pre-Shared Key (DPPSK) (see **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**: **Advanced settings** for more details on DPPSK) • Connection Logs will not include the logs and data related to MLO clients (see **Site-wide** > **Monitor** > **Connection log** for more details on connection logs). • Layer 2 isolation (see **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**: **Advanced settings** for more details on layer 2 isolation) • Collaborative Detection & Response (CDR) (see **Site-wide** > **Configure** > **Collaborative Detection & Response** for more details on CDR)
Layer 2 isolation	This field is not configurable if you select NAT mode. Select to turn on or off layer-2 isolation. If a device's MAC addresses is NOT listed, it is blocked from communicating with other devices in an SSID on which layer-2 isolation is enabled. Click **Add** to enter the MAC address of each device that you want to allow to be accessed by other devices in the SSID on which layer-2 isolation is enabled.
Intra-BSS traffic blocking	Select **on** to prevent crossover traffic from within the same SSID. Select **off** to allow intra-BSS traffic.
Band select	Select to enable band steering. When enabled, the Nebula Device steers WiFi clients to the 5 GHz band. Note: This feature is not available when you enable MLO. Note: Band mode must be set to Concurrent operation (2.4 GHz and 5 GHz).
Assisted roaming	Select to turn on or off IEEE 802.11k/v assisted roaming on the Nebula Device. When the connected clients request 802.11k neighbor lists, the Nebula Device will respond with a list of neighbor Nebula Devices that can be candidates for roaming. When the 802.11v capable clients are using the 2.4 GHz band, the Nebula Device can send 802.11v messages to steer clients to the 5 GHz band.
802.11r	Select to turn on or off IEEE 802.11r fast roaming on the Nebula Device. 802.11r fast roaming reduces the delay when the clients switch from one Nebula Device to another, by allowing security keys to be stored on all Nebula Devices in a network. Information from the original association is passed to the new Nebula Device when the client roams. The client does not need to perform the whole 802.1x authentication process. Note: This feature is not available when you enable MLO.

Table 53 Site-wide > Configure > Access points > SSID advanced settings (continued)

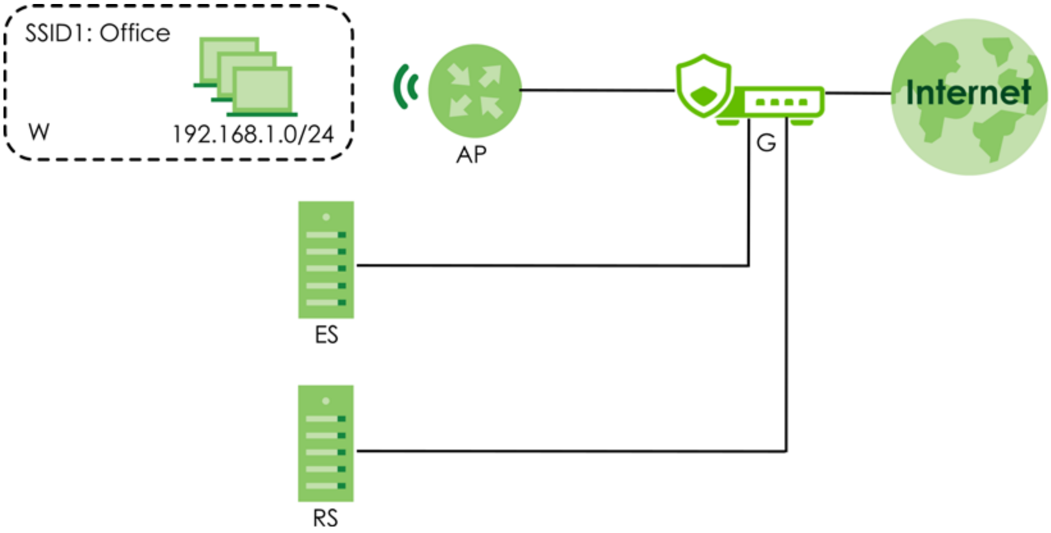
LABEL	DESCRIPTION
U-APSD	Select to turn on or off Automatic Power Save Delivery. This helps increase battery life for battery-powered WiFi clients connected to the Nebula Device.
SSID schedule	
Enabled	Click this switch to the right to enable and configure a schedule.
Schedule	Select a schedule to control when the SSID is enabled or disabled. You can click the edit icon to change the schedule name.
Schedule templates	Select a pre-defined schedule template or select **Custom schedule** and manually configure the day and time at which the SSID is enabled or disabled.
Day	This shows the day of the week.
Availability	Click this switch to the right to enable the SSID at the specified time on this day. Otherwise, click this switch to the left to disable the SSID on the day and at the specified time. Specify the hour and minute when the schedule begins and ends each day.
Add	Click this button to create a new schedule. A window pops up asking you to enter a descriptive name for the schedule for identification purposes.  New Schedule Name: New Schedule
Delete	Click this button to remove a schedule which is not used in any SSID profile.

5.3.3 Captive Portal Customization

Use this screen to configure captive portal settings for SSID profiles. A captive portal intercepts network traffic until the user authenticates his or her connection, usually through a specifically designated login web page.

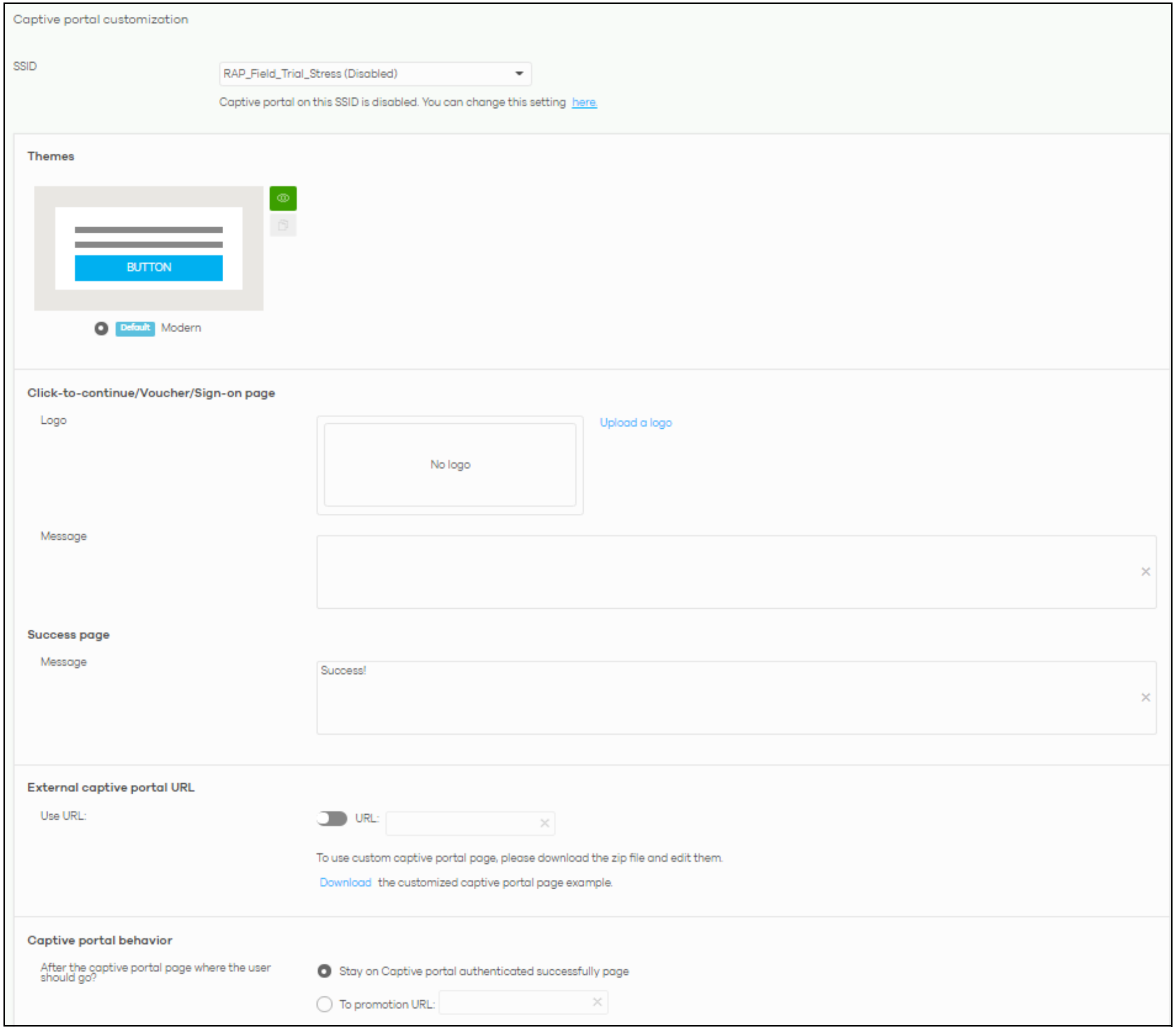
Note: The **Captive portal customization** options are not available when you select **Microsoft Entra ID (Azure AD)** authentication in **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**.

The following figure shows the WiFi clients (**W**) connecting to the (**AP**) through the SSID1: Office. The Security Gateway (**G**) connects to an external captive portal server (**ES**) or RADIUS Server (**RS**) for authentication.



Click **Site-wide** > **Configure** > **Access points** > **Captive portal customization** to access this screen.

Figure 86 Site-wide > Configure > Access points > Captive portal customization



Captive portal customization

SSID: RAP_Field_Trial_Stress (Disabled)

Captive portal on this SSID is disabled. You can change this setting here.

Themes

● Default Modern

Click-to-continue/Voucher/Sign-on page

Logo: No logo

Upload a logo

Message:

Success page

Message: Success!

External captive portal URL

Use URL: URL:

To use custom captive portal page, please download the zip file and edit them.

Download the customized captive portal page example.

Captive portal behavior

After the captive portal page where the user should go?

● Stay on Captive portal authenticated successfully page

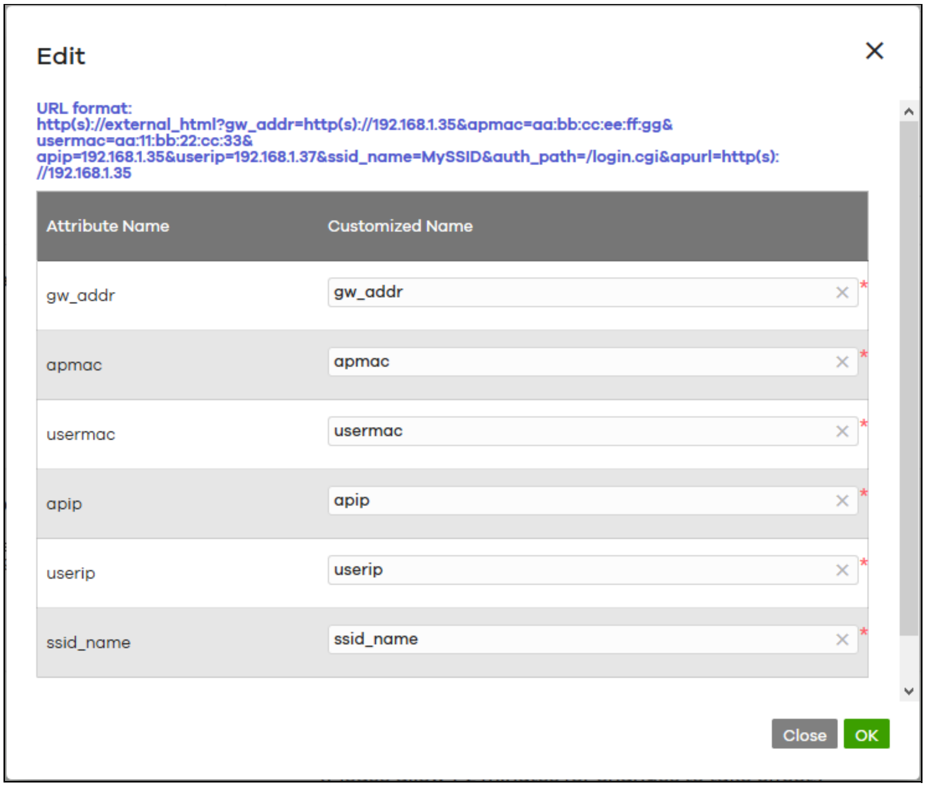
○ To promotion URL:

The following table describes the labels in this screen.

Table 54 Site-wide > Configure > Access points > Captive portal customization

LABEL	DESCRIPTION
SSID	Select the SSID profile to which the settings you configure here is applied.
Themes	This section is not configurable when **External captive portal URL** is set to **ON**. • Click the **Preview** icon at the upper right of a theme image to display the portal page in a new frame. • Click the **Copy** icon to create a new custom theme (login page). • Click the **Edit** icon of a custom theme to go to a screen where you can view and configure the details of the custom theme pages. See Section 5.3.3.1 on page 333. • Click the **Remove** icon to delete a custom theme page. Select the theme you want to use on the specified SSID.
Click-to-continue/Voucher/Sign-on page This section is not configurable when **External captive portal URL** is set to **ON**.	
Logo	This shows the logo image that you uploaded for the customized login page. Click **Upload a logo** and specify the location and file name of the logo graphic or click **Browse** to locate it. You can use the following image file formats: GIF, PNG, or JPG.
Message	Enter a note to display below the title. Use up to 1024 printable ASCII characters. Spaces are allowed.
Success page	
Message	Enter a note to display on the page that displays when a user logs in successfully. Use up to 1024 printable ASCII characters. Spaces are allowed.
External captive portal URL	

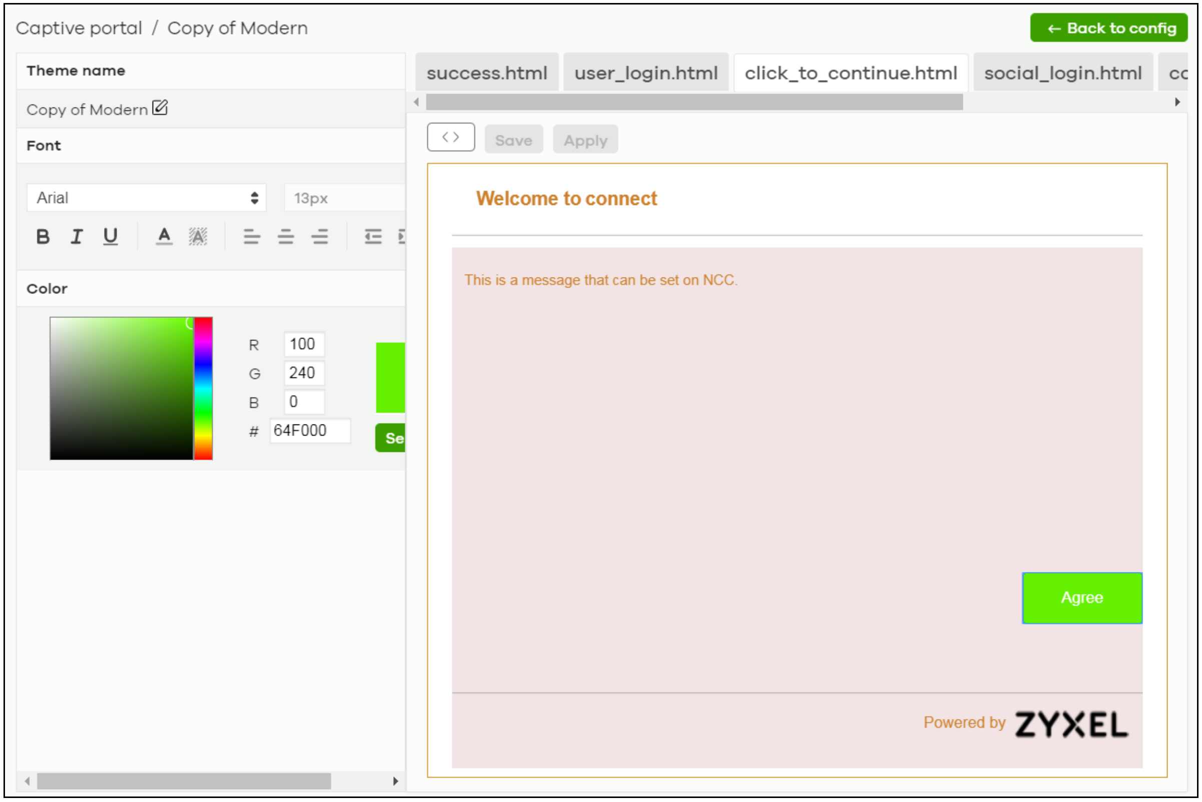
Table 54   Site-wide > Configure > Access points > Captive portal customization (continued)

LABEL	DESCRIPTION
Use URL	Select **On** to use a custom login page from an external web portal instead of the one built into the NCC. You can configure the look and feel of the web portal page. Specify the login page's URL; for example, http://IIS server IP Address/login.asp. The Internet Information Server (IIS) is the web server on which the web portal files are installed. Click Download to download a ZIP file containing example captive port files. Edit these files then upload them to a webserver which is accessible from NCC.  Edit URL format: http(s)://external_html?gw_addr=http(s)://192.168.1.35&apmac=aa:bb:cc:ee:ff:gg& usermac=aa:11:bb:22:cc:33& apip=192.168.1.35&userip=192.168.1.37&ssid_name=MySSID&auth_path=/login.cgi&apurl=http(s): //192.168.1.35 Attribute Name Customized Name gw_addr gw_addr apmac apmac usermac usermac apip apip userip userip ssid_name ssid_name Close OK
Captive portal behavior	
After the captive portal page where the user should go?	Select **To promotion URL** and specify the URL of the web site or page to which the user is redirected after a successful login. Otherwise, select **Stay on Captive portal authenticated successfully page**.

5.3.3.1 Custom Theme Edit

Use this screen to check what the custom portal pages look like. You can also view and modify the CSS values of the selected HTML file. Click a custom login page's **Edit** button in the **Site-wide** > **Configure** > **Access points** > **Captive portal** screen to access this screen.

Figure 87 Site-wide > Configure > Access points > Captive portal: Edit



Theme name: Copy of Modern

Font: Arial 13px

R 100
G 240
B 0
64F000

Welcome to connect

This is a message that can be set on NCC.

The following table describes the labels in this screen.

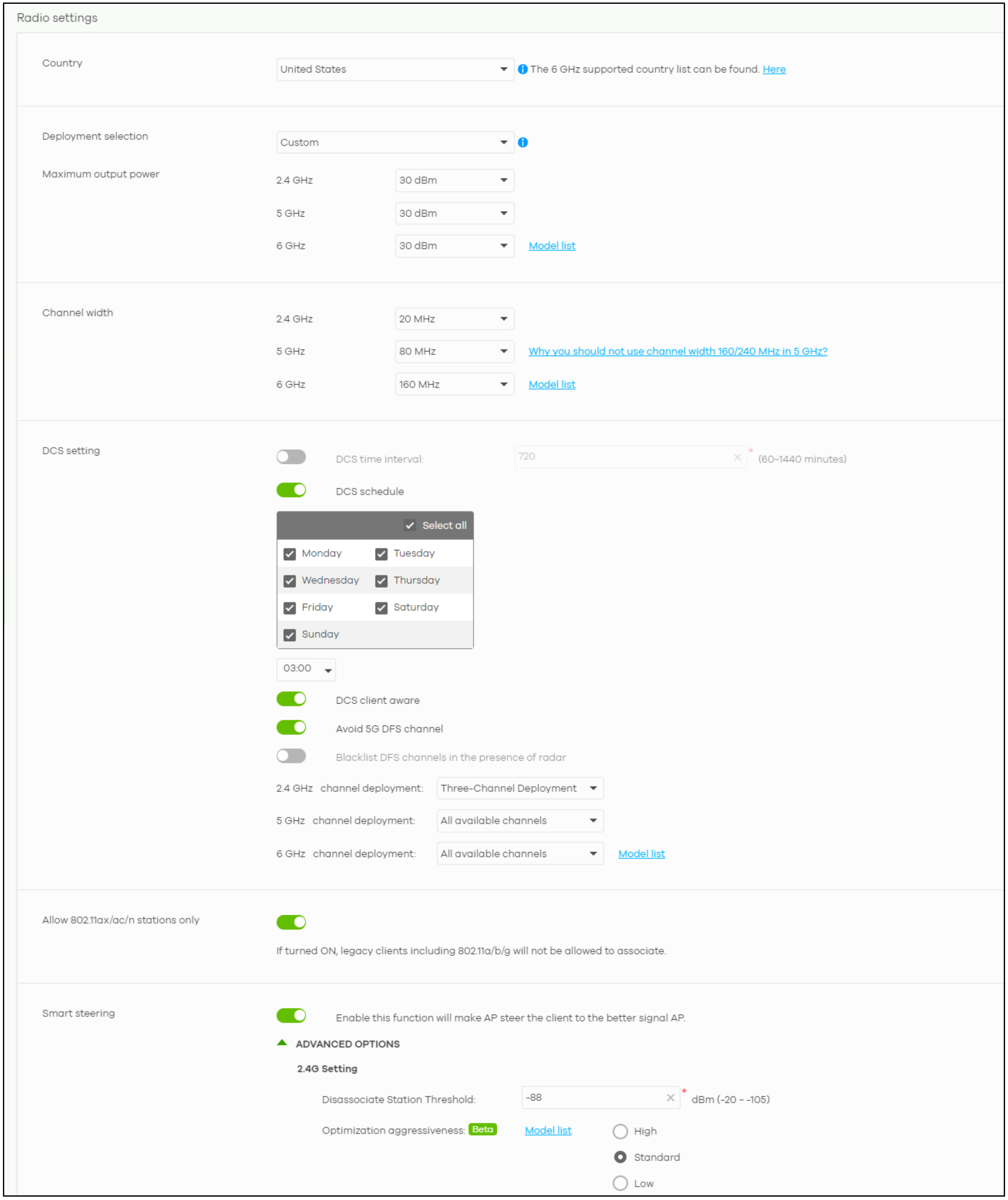
Table 55 Site-wide > Configure > Access points > Captive portal: Edit

LABEL	DESCRIPTION
Back to config	Click this button to return to the **Captive portal** screen.
Theme name	This shows the name of the theme. Click the edit icon the change it.
Font	Click the arrow to hide or display the configuration fields. To display this section and customize the font type and/or size, click on an item with text in the preview of the selected custom portal page (HTML file).
Color	Click the arrow to hide or display the configuration fields. Click an item in the preview of the selected custom portal page (HTML file) to customize its color, such as the color of the button, text, window's background, links, borders, and so on. Select a color that you want to use and click the **Select** button.
HTML/CSS	This shows the HTML file name of the portal page created for the selected custom theme. This also shows the name of the CSS files created for the selected custom theme. Click a HTML file to display the portal page. You can also change colors and modify the CSS values of the selected HTML file.
‹›	Click this button to view and modify the CSS values of the selected HTML file. It is recommended that you do NOT change the script code to ensure proper operation of the portal page.
👁	Click this button to preview the portal page (the selected HTML file).
Save	Click this button to save your settings for the selected HTML file to the NCC.
Apply	Click this button to save your settings for the selected HTML file to the NCC and apply them to the access points in the site.

5.3.4 Radio Settings

Use this screen to configure global radio settings for all Nebula Devices in the site. Click **Site-wide** > **Configure** > **Access points** > **Radio settings** to access this screen.

Figure 88 Site-wide > Configure > Access points > Radio settings



Radio settings

Country: United States — The 6 GHz supported country list can be found. Here

Deployment selection: Custom

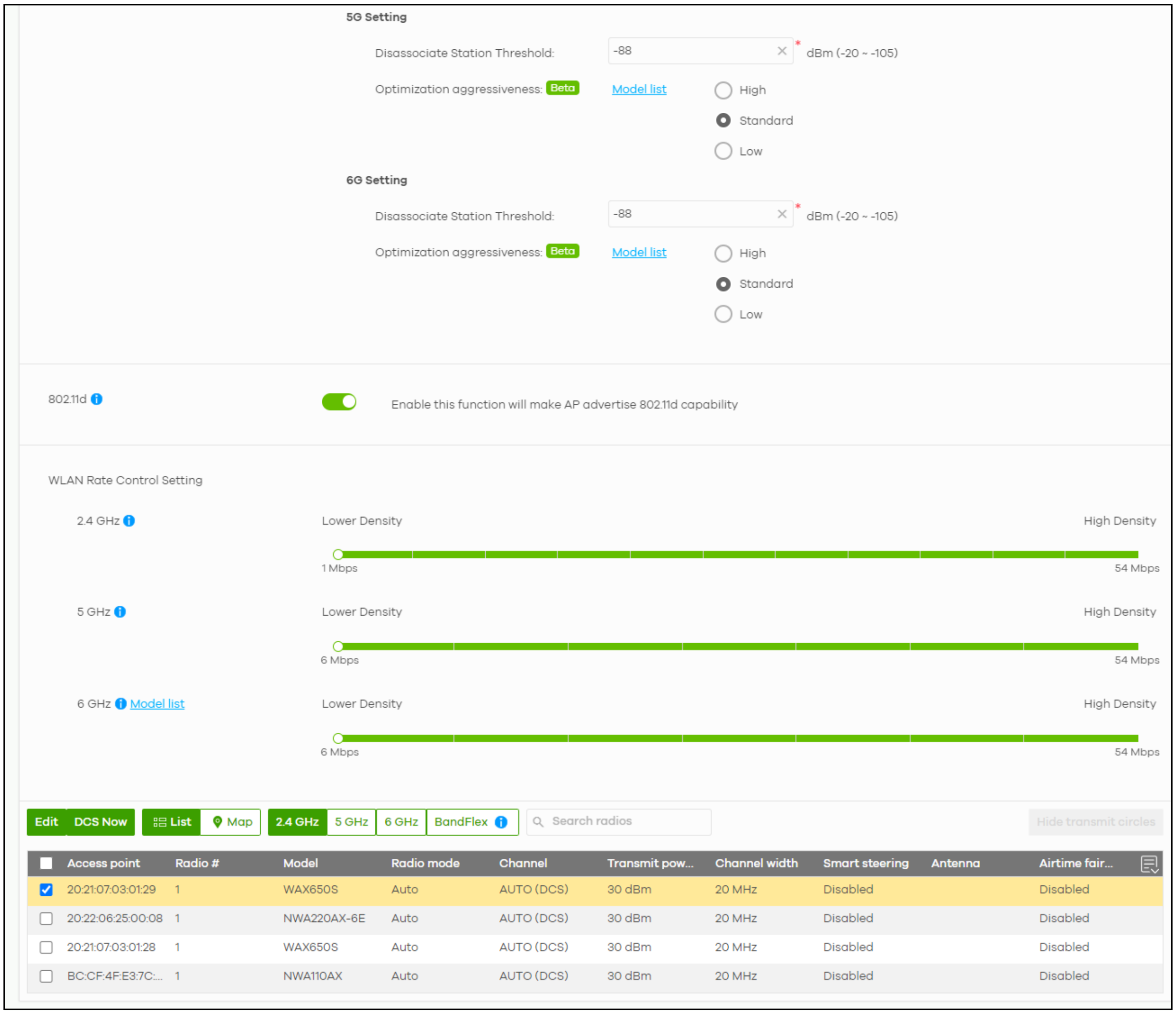
Maximum output power:
2.4 GHz: 30 dBm
5 GHz: 30 dBm
6 GHz: 30 dBm — Model list

Channel width:
2.4 GHz: 20 MHz
5 GHz: 80 MHz — Why you should not use channel width 160/240 MHz in 5 GHz?
6 GHz: 160 MHz — Model list

DCS setting:
DCS time interval: 720 * (60~1440 minutes)
DCS schedule
☑ Select all
☑ Monday ☑ Tuesday
☑ Wednesday ☑ Thursday
☑ Friday ☑ Saturday
☑ Sunday
03:00
DCS client aware
Avoid 5G DFS channel
Blacklist DFS channels in the presence of radar
2.4 GHz channel deployment: Three-Channel Deployment
5 GHz channel deployment: All available channels
6 GHz channel deployment: All available channels — Model list

Allow 802.11ax/ac/n stations only
If turned ON, legacy clients including 802.11a/b/g will not be allowed to associate.

Smart steering
Enable this function will make AP steer the client to the better signal AP.
ADVANCED OPTIONS
2.4G Setting
Disassociate Station Threshold: -88 * dBm (-20 ~ -105)
Optimization aggressiveness: Beta — Model list
○ High
● Standard
○ Low



5G Setting

Disassociate Station Threshold: -88 * dBm (-20 ~ -105)

Optimization aggressiveness: Beta Model list ○ High ● Standard ○ Low

6G Setting

Disassociate Station Threshold: -88 * dBm (-20 ~ -105)

Optimization aggressiveness: Beta Model list ○ High ● Standard ○ Low

802.11d — Enable this function will make AP advertise 802.11d capability

WLAN Rate Control Setting

2.4 GHz	Lower Density 1 Mbps	High Density 54 Mbps
5 GHz	Lower Density 6 Mbps	High Density 54 Mbps
6 GHz Model list	Lower Density 6 Mbps	High Density 54 Mbps

□	Access point	Radio #	Model	Radio mode	Channel	Transmit pow...	Channel width	Smart steering	Antenna	Airtime fair...
☑	20:21:07:03:01:29	1	WAX650S	Auto	AUTO (DCS)	30 dBm	20 MHz	Disabled		Disabled
□	20:22:06:25:00:08	1	NWA220AX-6E	Auto	AUTO (DCS)	30 dBm	20 MHz	Disabled		Disabled
□	20:21:07:03:01:28	1	WAX650S	Auto	AUTO (DCS)	30 dBm	20 MHz	Disabled		Disabled
□	BC:CF:4F:E3:7C:...	1	NWA110AX	Auto	AUTO (DCS)	30 dBm	20 MHz	Disabled		Disabled

The following table describes the labels in this screen.

Table 56 Site-wide > Configure > Access points > Radio settings

LABEL	DESCRIPTION
Country	Select the country where the Nebula Device is located or installed. The available channels vary depending on the country you selected. Be sure to select the correct or same country for both radios on a Nebula Device and all connected Nebula Devices in order to prevent roaming failure and interference with other systems.
Deployment selection	Select **High-density (More than 10 APs)** for the lowest output power for 10 or more Access Points. Select **Moderate-density (6-9 APs)** for moderate output power for 5 to 9 Access Points. Select **Low-density (2-5 APs)** for higher concentration of output power for less than 5 Access Points. Select **Single AP** for highest concentration of output power for a single Access Point.
Maximum output power	Selecting any of the options in the **Deployment selection** field will automatically set the maximum output power for 2.4 / 5 / 6 GHz. But you can change the setting (1 – 30 dBm).

Table 56 Site-wide > Configure > Access points > Radio settings (continued)

LABEL	DESCRIPTION
Channel width	Select the wireless channel bandwidth you want the access point to use. A standard 20 MHz channel offers transfer speeds of up to 144 Mbps (2.4 GHz) or 217 Mbps (5 GHz) whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps (2.4 GHz) or 450 Mbps (5 GHz). An IEEE 802.11ac-specific 80 MHz channel offers speeds of up to 1.3 Gbps. An IEEE 802.11be-specific 160 MHz channel offers speeds of up to 2.9 Gbps (6 GHz with 2 spatial streams) whereas a 320 MHz channel offers speeds of up to 5.8 Gbps (6 GHz with 2 spatial streams). 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. An 80 MHz channel consists of two adjacent 40 MHz channels. The WiFi clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. Note: It is suggested that you select **20 MHz** when there is more than one 2.4 GHz Nebula Device in the network. Note: It is not possible to set channel width to 160 MHz / 240 MHz on 5 GHz for the whole site. To configure a Nebula Device to use 160 MHz / 240 MHz on 5 GHz, select a supported Nebula Device in the table at the bottom of the screen, click **Edit**, and then select **160 MHz** under **Channel width**.
DCS setting	
DCS time interval	Select **ON** to set the DCS time interval (in minutes) to regulate how often the Nebula Device surveys the other Nebula Devices within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another Nebula Device, the Nebula Device will then dynamically select the next available clean channel or a channel with lower interference.
DCS schedule	Select **ON** to have the Nebula Device automatically find a less-used channel within its broadcast radius at a specific time on selected days of the week. You then need to select each day of the week and specify the time of the day (in 24-hour format) to have the Nebula Device use DCS to automatically scan and find a less-used channel.
DCS client aware	Select **ON** to have the Nebula Device wait until all connected clients have disconnected before switching channels.
Avoid 5G DFS channel	If your Nebula Devices are operating in an area known to have RADAR devices, the Nebula Device will choose non-DFS channels to provide a stable WiFi service.
Blacklist DFS channels in the presence of radar	Select **ON** to blacklist a channel if RADAR is detected. After being blacklisted, the Nebula Device will not use the channel again until the Nebula Device is rebooted. However, the Nebula Device can still use other DFS channels.
2.4 GHz channel deployment	Select **Three-Channel Deployment** to limit channel switching to channels 1, 6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels. Select **Four-Channel Deployment** to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1 – 11 then the Nebula Device uses channels 1, 4, 7, 11 in this configuration; otherwise, the Nebula Device uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum. Select **All available channels** to allow channel-hopping to have the Nebula Device automatically select the best channel. Select **Manual** to select the individual channels the Nebula Device switches between.

Table 56 Site-wide > Configure > Access points > Radio settings (continued)

LABEL	DESCRIPTION
5 GHz channel deployment	Select how you want to specify the channels the Nebula Device switches between for 5 GHz operation. Select **All available channels** to have the Nebula Device automatically select the best channel. Select **Manual** to select the individual channels the Nebula Device switches between. Note: The method is automatically set to **All available channels** when no channel is selected or any one of the previously selected channels is not supported.
6 GHz channel deployment	Select how you want to specify the channels the Nebula Device switches between for 6 GHz operation. Select **All available channels** to have the Nebula Device automatically select the best channel. Select **Manual** to select the individual channels the Nebula Device switches between. Note: The method is automatically set to **All available channels** when no channel is selected or any one of the previously selected channels is not supported.
Allow 802.11ax/ac/n stations only	Select **ON** to have the Nebula Device allow only IEEE 802.11n/ac/ax clients to connect, and reject IEEE 802.11a/b/g clients.
Smart Steering	Select **ON** to enable smart client steering on the Nebula Device. Client steering helps monitor WiFi clients and drop their connections to optimize the bandwidth when the clients are idle or have a low signal. When a WiFi client is dropped they have the opportunity to steer to an Nebula Device with a strong signal. Additionally, dual band WiFi clients can also steer from one band to another. Select **OFF** to disable this feature on the Nebula Device.
ADVANCED OPTIONS	Click this to display a greater or lesser number of configuration fields.
2.4G/5G/6G Setting	
Disassociate Station Threshold	Set a minimum kick-off signal strength. When a WiFi client's signal strength is lower than the specified threshold, the Nebula Device disconnects the WiFi client. –20 dBm is the strongest signal you can require and –105 dBm is the weakest.
Optimization aggressiveness	**High**, **Standard** and **Low** stand for different traffic rate threshold levels. The level you select here decides when the Nebula Device takes action to improve the access point's WiFi network performance. The Nebula Device will postpone the actions implemented on access points until your network is less busy if the threshold is exceeded. Select a suitable traffic rate threshold level for your network. **High**: Select this if you want the Nebula Device to postpone the action set when the access point network traffic is heavy. **Standard**: Select this if you want the Nebula Device to postpone the action set when the access point network traffic is medium. **Low**: Select this if you want the Nebula Device to postpone the action set when the access point network traffic is low.
802.11d	Click this to enable 802.11d on the access point. 802.11d is a WiFi network specification, for use in countries where 802.11 WiFi is restricted. Enabling 802.11d causes the Nebula Device to broadcast the country where it is located, which is determined by the Country setting. Note: Disable **802.11d** on older client devices with connection issues.
WLAN Rate Control Setting	

Table 56 Site-wide > Configure > Access points > Radio settings (continued)

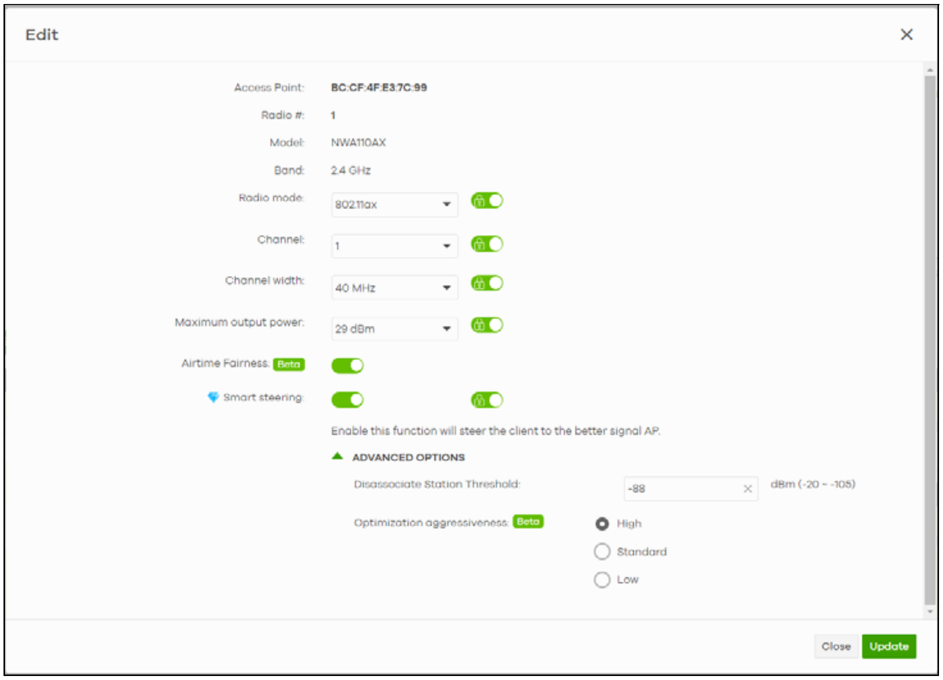
LABEL	DESCRIPTION
2.4 GHz / 5 GHz /6 GHz	Sets the minimum data rate that 2.4 GHz, 5 GHz, and 6 GHz WiFi clients can connect to the Nebula Device, in Mbps. Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the Nebula Device.
Edit	Click this button to modify the channel, output power, channel width, airtime fairness (the same setting will apply to both 2.4 GHz and 5 GHz), and smart steering settings for the selected Nebula Devices. On the Nebula Device that comes with internal antennas and also has an antenna switch, you can adjust coverage depending on the orientation of the antenna for the Nebula Device radios. Select **Wall** if you mount the Nebula Device to a wall. Select **Ceiling** if the Nebula Device is mounted on a ceiling. You can switch from **Wall** to **Ceiling** if there are still WiFi dead zones, and so on. If you select **Hardware Switch**, you use the physical antenna switch to adjust coverage and apply the same antenna orientation settings to both radios.  Edit Access Point: BC:CF:4F:E3:7C:99 Radio #: 1 Model: NWA110AX Band: 2.4 GHz Radio mode: 802.11ax Channel: 1 Channel width: 40 MHz Maximum output power: 29 dBm Airtime Fairness: Beta Smart steering: Enable this function will steer the client to the better signal AP. ADVANCED OPTIONS Disassociate Station Threshold: -88 dBm (-20 ~ -105) Optimization aggressiveness: Beta ● High ○ Standard ○ Low Close Update Note: On this screen, you can set channel width to 160 MHz for the 5/6 GHz channel, if the Nebula Device supports it.
DCS Now	Click this button to have the selected Nebula Devices immediately scan for and select a channel that has least interference.
List	Click this to display a list of all connected Nebula Devices.
Map	Click this to display the locations of all connected Nebula Devices on the Google map.
2.4 GHz	Click this to display the connected Nebula Devices using the 2.4 GHz frequency band.
5 GHz	Click this to display the connected Nebula Devices using the 5 GHz frequency band.
6 GHz	Click this to display the connected Nebula Devices using the 6 GHz frequency band.
BandFlex	Click this to display the connected Nebula Devices that supports BandFlex (5 GHz or 6 GHz frequency bands).
Hide transmit circles	Click this button to not show the transmission range on the Map.
Access point	This displays the descriptive name or MAC address of the connected Nebula Device.

Table 56 Site-wide > Configure > Access points > Radio settings (continued)

LABEL	DESCRIPTION
Radio #	This displays the number of the connected Nebula Device's radio.
Model	This displays the model name of the connected Nebula Device.
Radio mode	This displays the type of WiFi radio the Nebula Device is currently using, for example 802.11b/g/n.
Channel	This displays the channel ID currently being used by the connected Nebula Device's radio.
Transmit power	This displays the current transmitting power of the connected Nebula Device's radio. If the Nebula Device is offline, this shows the maximum output power you configured for the Nebula Device.
Channel width	This displays the wireless channel bandwidth the connected Nebula Device's radio is set to use.
Smart steering	This displays whether smart client steering is enabled or disabled on the connected Nebula Devices.
Antenna	This displays the antenna orientation settings for the Nebula Device that comes with internal antennas and also has an antenna switch.
Airtime fairness	This displays whether airtime fairness is enabled or disabled on the connected Nebula Device.
☑	Click this icon to display a greater or lesser number of configuration fields. For faster loading of data, select only the configuration fields listed that do NOT take a long time to fetch data.

The following table describes the pre-defined deployments and the related output power, channel width, DFS (Dynamic Frequency Selection) setting, rate control, and channel deployment.

Table 57 Radio Deployment Selection and Corresponding Parameters

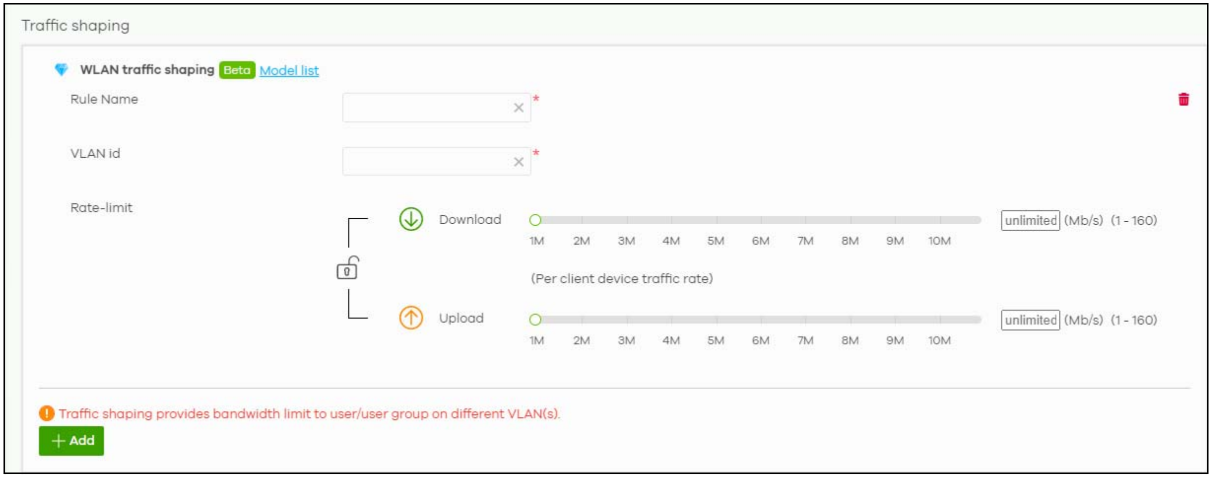
DEPLOYMENT		HIGH DENSITY	MODERATE DENSITY	LOW DENSITY	SINGLE AP
Number of APs		More than 10	6 – 9	2 – 5	1
Power (dBm)	2G	12	15	20	30 20 (EU)
	5G	15	18	30	30
	6G	18	21	30	30
Channel width (MHz)	5G	20	40	80	80
	6G	80	160	160	160
Avoid 5G DFS channel / Blacklist DFS channels in the presence of radar		Disabled / Enabled	Enabled / Disabled	Enabled / Disabled	Enabled / Disabled
Rate control (Mbps)	2.4G	11	1	1	1
	5G	12	6	6	6
2.4G channel deployment		All channels	Three-channel	Three-channel	Three-channel

5.3.5 Traffic Shaping

This feature is for dynamic VLAN application. The data limit set here applies to the VLAN on a per WiFi client basis. This has a higher priority than the data limit set in **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**, which is applied on a per station basis. Use this screen to configure maximum bandwidth on the Nebula Device.

Click **Site-wide** > **Configure** > **Access points** > **Traffic shaping** to access this screen.

Figure 89 Site-wide > Configure > Access point > Traffic shaping


Traffic shaping
WLAN traffic shaping
Beta
Model list
Rule Name
VLAN id
Rate-limit
Download
1M 2M 3M 4M 5M 6M 7M 8M 9M 10M
unlimited (Mb/s) (1 - 160)
(Per client device traffic rate)
Upload
1M 2M 3M 4M 5M 6M 7M 8M 9M 10M
unlimited (Mb/s) (1 - 160)
+ Add

Traffic shaping provides bandwidth limit to user/user group on different VLAN(s).

The following table describes the labels in this screen.

Table 58 Site-wide > Configure > Access points > Traffic shaping

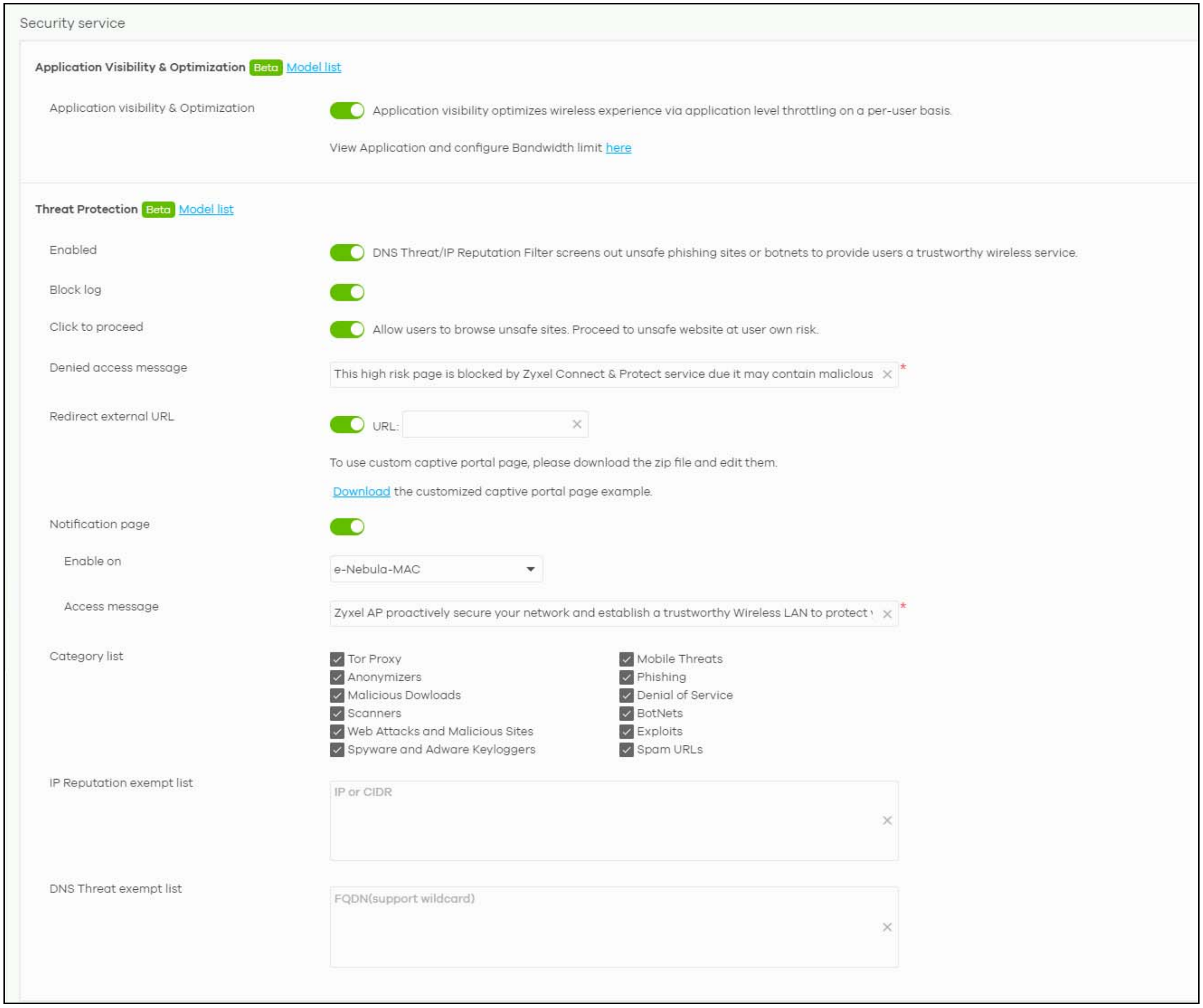
LABEL	DESCRIPTION
WLAN traffic shaping	
Rule Name	Enter the name of the traffic shaping rule. The name is used to refer to the traffic shaping rule. You may use 1 – 31 alphanumeric characters, underscores(_), or dashes (-). This value is case-sensitive.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.)
Rate-limit	Set the maximum data download and upload rate in Mb/s, on a per WiFi client basis. Allowed values are 1 – 160. Click the lock icon to change the lock state. If the lock icon is locked, the data limit you set applies to both download and upload traffic. If the lock is unlocked, you can set download and upload traffic to have different data limits.
Add	Click this button to create a new rule.

5.3.6 Security Service

Use this screen to enable or disable the features available in the security pack for your Nebula Device, such as application visibility and optimization and/or IP reputation filter.

Click **Site-wide** > **Configure** > **Access points** > **Security service** to access this screen.

Figure 90 Site-wide > Configure > Access points > Security service



Security service

Application Visibility & Optimization Beta Model list

Application visibility & Optimization — Application visibility optimizes wireless experience via application level throttling on a per-user basis.

View Application and configure Bandwidth limit here

Threat Protection Beta Model list

Enabled — DNS Threat/IP Reputation Filter screens out unsafe phishing sites or botnets to provide users a trustworthy wireless service.

Block log

Click to proceed — Allow users to browse unsafe sites. Proceed to unsafe website at user own risk.

Denied access message: This high risk page is blocked by Zyxel Connect & Protect service due it may contain malicious *

Redirect external URL — URL:

To use custom captive portal page, please download the zip file and edit them.

Download the customized captive portal page example.

Notification page

Enable on: e-Nebula-MAC

Access message: Zyxel AP proactively secure your network and establish a trustworthy Wireless LAN to protect *

Category list

- ☑ Tor Proxy
- ☑ Anonymizers
- ☑ Malicious Dowloads
- ☑ Scanners
- ☑ Web Attacks and Malicious Sites
- ☑ Spyware and Adware Keyloggers
- ☑ Mobile Threats
- ☑ Phishing
- ☑ Denial of Service
- ☑ BotNets
- ☑ Exploits
- ☑ Spam URLs

IP Reputation exempt list: IP or CIDR

DNS Threat exempt list: FQDN(support wildcard)

The following table describes the labels in this screen.

Table 59 Site-wide > Configure > Access points > Security service

LABEL	DESCRIPTION
Application Visibility & Optimization	
Application visibility & Optimization	Select this option to turn on application visibility and optimization. Application visibility and optimization does the following: • Detects the type of applications used by WiFi clients, • Throttles specific applications to save WiFi bandwidth. Application visibility provides a way for a Nebula Device to manage the use of various applications on its WiFi network. It can detect the type of applications used by WiFi clients and how much bandwidth they use. Application optimization limits the applications bandwidth usage by their categories. You can manage and view the applications and their categories in **Site-wide** > **Applications usage** > **Application view by Access Point**.
Threat Protection	

Table 59 Site-wide > Configure > Access points > Security service (continued)

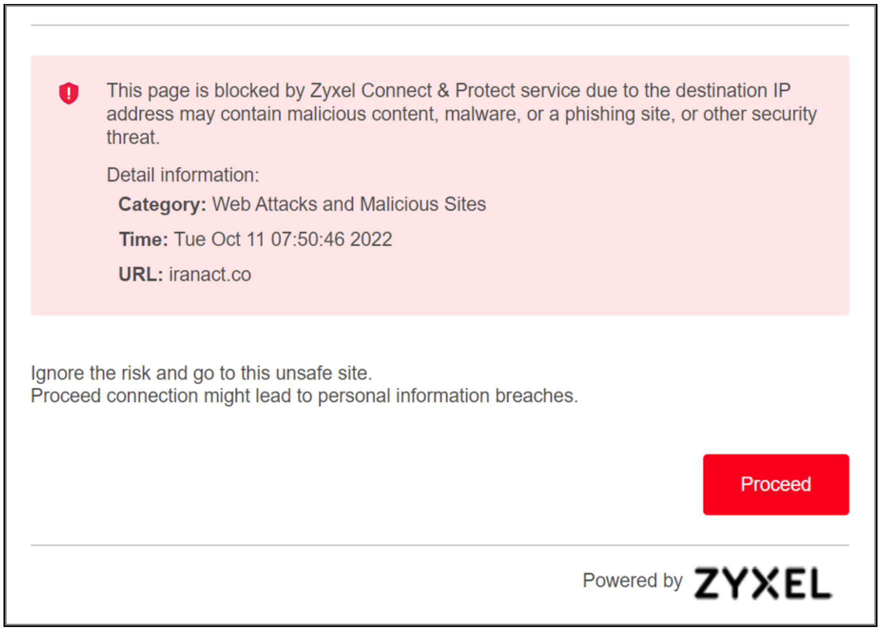
LABEL	DESCRIPTION
Enabled	Select this option to allow inspection of DNS queries made by clients on your network and turn on IP blocking on the Nebula Device. When you enable the DNS threat service, your Nebula Device inspects the DNS queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs). You can have the Nebula Device reply to the user with a fake DNS response (where the user will see a "Web Page Blocked!" page). When you enable the IP reputation service, your Nebula Device downloads signature files that identifies reputation of IPv4 addresses. You can have the Nebula Device forward, block, and/or log packets from IPv4 addresses based on these signatures and categories.
Block log	Select this option to create a log on the Nebula Device when the packet comes from an IPv4 address with bad reputation.
Click to proceed	Select this option to allow clients to browse unsafe websites. When enabled, the denied access message window includes the **Proceed** button. To continue, you must close and restart your web browser to visit the unsafe website.  This page is blocked by Zyxel Connect & Protect service due to the destination IP address may contain malicious content, malware, or a phishing site, or other security threat. Detail information: **Category:** Web Attacks and Malicious Sites **Time:** Tue Oct 11 07:50:46 2022 **URL:** iranact.co Ignore the risk and go to this unsafe site. Proceed connection might lead to personal information breaches. Proceed Powered by ZYXEL
Denied access message	Enter a message to be displayed when IP reputation filter blocks access to a web page. Use up to 127 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the Redirect external URL field. In this case if the IP reputation filter blocks access to a web page, the Nebula Device just opens the web page you specified without showing a denied access message.
Redirect external URL	Enter the URL of the web page to which you want to send users when their web access is blocked by IP reputation filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Notification page	Select this option to display the notification page.
Enable on	Select the SSID 1 – 8 that is allowed access to WiFi clients.
Access message	Enter a message to be displayed when access to a web page is allowed. Use up to 127 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator".

Table 59 Site-wide > Configure > Access points > Security service (continued)

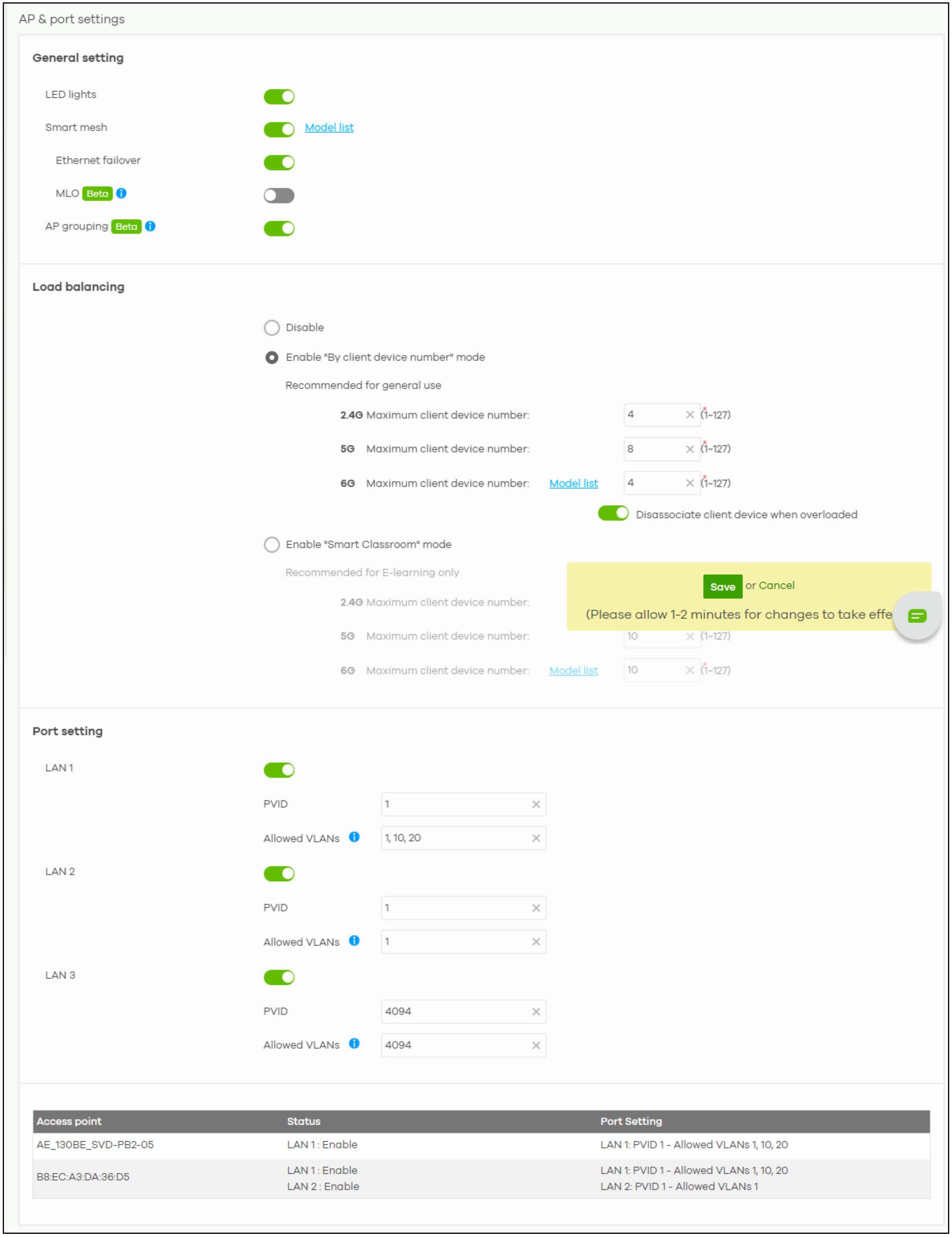
LABEL	DESCRIPTION
Category list	Select the categories of packets that come from the Internet and are known to pose a security threat to users or their computers.
IP Reputation exempt list	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Add the IPv4 addresses that the Nebula Device will allow the incoming and outgoing packets.
DNS Threat exempt list	Domain names that you want to allow access to, regardless of their reputation, can be allowed by adding them to this list. Add the Fully Qualified Domain Names (FQDNs) that the Nebula Device will allow the DNS query packets.

5.3.7 AP & Port Settings

Use this screen to configure general Nebula Device settings and network traffic load balancing between the Nebula Devices in the site. This screen also allows you to enable or disable a port on the managed Nebula Device and configure the port's VLAN settings. The port settings apply to all Nebula Devices that are assigned to the site and have one or more than one Ethernet LAN port (except the uplink port).

Click **Site-wide** > **Configure** > **Access points** > **AP & port settings** to access this screen.

Figure 91 Site-wide > Configure > Access points > AP & port settings



AP & port settings

General setting

LED lights: on

Smart mesh: on — Model list

Ethernet failover: on

MLO Beta: off

AP grouping Beta: on

Load balancing

○ Disable

● Enable "By client device number" mode

Recommended for general use

2.4G Maximum client device number: 4 (1~127)

5G Maximum client device number: 8 (1~127)

6G Maximum client device number: Model list 4 (1~127)

Disassociate client device when overloaded: on

○ Enable "Smart Classroom" mode

Recommended for E-learning only

2.4G Maximum client device number:

5G Maximum client device number: 10 (1~127)

6G Maximum client device number: Model list 10 (1~127)

Save or Cancel

(Please allow 1-2 minutes for changes to take effe

Port setting

LAN 1: on

PVID: 1

Allowed VLANs: 1, 10, 20

LAN 2: on

PVID: 1

Allowed VLANs: 1

LAN 3: on

PVID: 4094

Allowed VLANs: 4094

Access point	Status	Port Setting
AE_130BE_SVD-PB2-05	LAN 1 : Enable	LAN 1: PVID 1 - Allowed VLANs 1, 10, 20
B8:EC:A3:DA:36:D5	LAN 1 : Enable LAN 2 : Enable	LAN 1: PVID 1 - Allowed VLANs 1, 10, 20 LAN 2: PVID 1 - Allowed VLANs 1

The following table describes the labels in this screen.

Table 60 Site-wide > Configure > Access points > AP & port settings

LABEL	DESCRIPTION
General setting	
LED lights	Click to turn on or off the LEDs on the Nebula Devices.
Smart Mesh	Click to enable or disable the Nebula Smart Mesh feature on all Nebula Devices in the site. Click **Model list** to see whether your Nebula Device supports Nebula Smart Mesh. Note: Nebula Smart Mesh is a WiFi mesh solution for Nebula Devices. For details, see Section 5.1.1 on page 303. Note: You can override NCC settings and enable or disable Smart Mesh on individual Nebula Devices. For details, see Section 4.3.1.1 on page 218. Note: Disabling Nebula Device Smart Mesh automatically disables wireless bridge on all Nebula Devices in the site. For details on wireless bridge, see Section 4.3.1.1 on page 218.
Ethernet failover	When enabled, a wired Nebula Device in the site automatically changes its role from mesh controller to mesh extender if the Nebula Device is unable to reach the site's gateway. When disabled, a wired Nebula Device in the site automatically changes its role from mesh controller to mesh extender only if the Nebula Device's uplink Ethernet cable is unplugged. Note: For details on mesh controller and mesh extender, see Section 5.1.1 on page 303.
MLO	Select **MLO** (Multi-Link Operation) to allow a WiFi7 client to connect to the WiFi7 Nebula Device using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi7 ideal for streaming 4K / 8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games.
AP grouping	Select this option to enable the creation of up to 24 SSIDs per site in the **Site-wide** > **Configure** > **Access points** > **SSID settings** screen. Additionally, use tags to assign up to 8 SSIDs to each AP group.
Load balancing	
Disable	Select this option to disable load balancing on the Nebula Device.
Enable "By client device number" mode	Select this option to balance network traffic based on the number of specified client devices connected to the Nebula Device.
2.4G / 5G / 6G Maximum client device number	Enter the threshold number of client devices (1 to 127) at which the Nebula Device begins load balancing its connections.
Disassociate client device when overloaded	Select **ON** to disassociate WiFi clients connected to the Nebula Device when it becomes overloaded. Select **OFF** to disable this option, then the Nebula Device simply delays the connection until it can afford the bandwidth it requires, or it transfers the connection to another Nebula Device within its broadcast radius. The disassociation priority is determined automatically by the Nebula Device and is as follows: • **Idle Time** – Devices that have been idle the longest will be disassociated first. If none of the connected devices are idle, then the priority shifts to **Signal Strength**. • **Signal Strength** – Devices with the weakest signal strength will be disassociated first.

Table 60 Site-wide > Configure > Access points > AP & port settings (continued)

LABEL	DESCRIPTION
Enable "Smart Classroom" mode	Select this option to balance network traffic based on the number of specified client devices connected to the Nebula Device. The Nebula Device ignores association request and authentication request packets from any new client device when the maximum number of client devices is reached. The **Disassociate client device when overloaded** function is enabled by default and the disassociation priority is always Signal Strength when you select this option.
2.4G / 5G / 6G Maximum client device number	Enter the threshold number of client devices (1 to 127) at which the Nebula Device begins load balancing its connections.
Port setting	
LAN x	This is the name of the physical Ethernet port on the Nebula Device. This section lets you configure global port VLAN settings for all Nebula Devices in the site. To modify port settings for a specific Nebula Device, use its **Edit** button in the table below.
ON/OFF	Select **ON** to turn on the LAN port of the Nebula Device. Select **OFF** to disable the port.
PVID	Enter the port's PVID. A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
Allowed VLANs	Enter the VLAN ID numbers to which the port belongs. Only the network traffic from the allowed VLANs will be sent or received through this port. You can enter individual VLAN ID numbers separated by a comma or a range of VLANs by using a dash, such as 1,3,5–8.
Access point	This displays the descriptive name or MAC address of the connected Nebula Device. Only the Nebula Device that has an extra Ethernet LAN port will be listed, such as NAP203 or NAP303.
Status	This shows whether the Nebula Device's Ethernet LAN port is enabled or disabled.
Port Setting	This displays the port's VLAN settings for the managed Nebula Device.

5.3.7.1 Edit Port Settings

Click an entry in the **Port setting** table of the **Site-wide** > **Configure** > **Access points** > **AP & port settings** screen to access this screen.

Select **NAT mode** to have the Nebula Device create a DHCP subnet with its own NAT for the SSID. This simplifies WiFi network management, as you do not need to configure a separate DHCP server. Otherwise, select **Local bridge**.

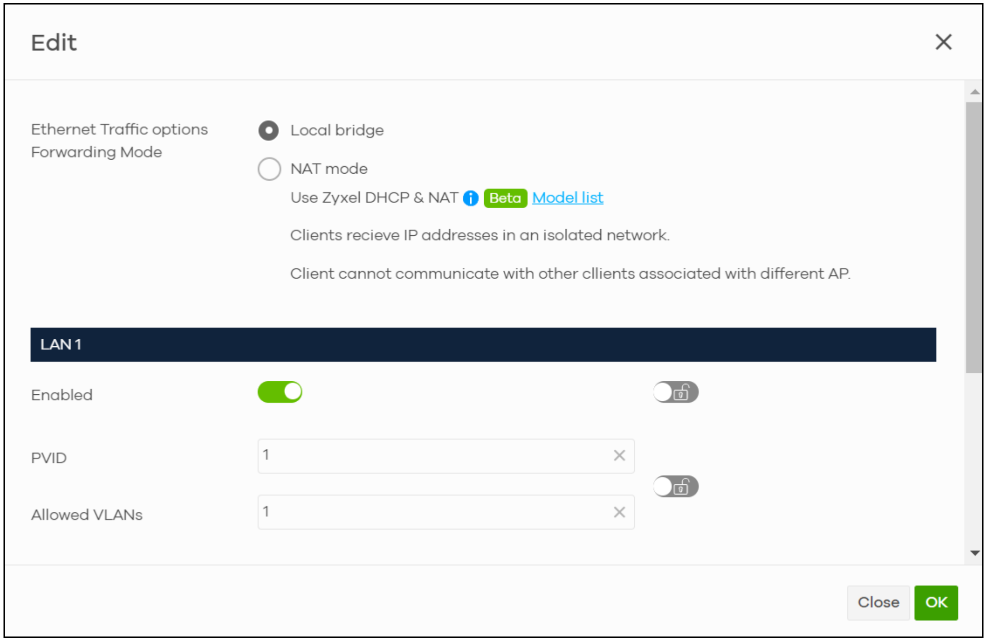
The following Nebula Device features do not work when NAT mode is enabled:

- 802.11r (see Table 53 on page 323 for more information on enabling 802.11r)
- Layer2 isolation
- Dynamic VLAN (cloud authentication, RADIUS server)

Note: In NAT mode, clients cannot communicate with clients connected to a different Nebula Device.
Only WAC500H supports **Ethernet Traffic options Forwarding Mode** at the time of writing.

By default, all Nebula Devices in the site use the global port settings. Use this screen to change the port settings on a per-device basis. You can turn on or off the port, modify its PVID or update the ID number of VLANs to which the port belongs.

Figure 92 Site-wide > Configure > Access points > AP & port settings: Edit



Edit

Ethernet Traffic options Forwarding Mode

● Local bridge

○ NAT mode

Use Zyxel DHCP & NAT Beta Model list

Clients recieve IP addresses in an isolated network.

Client cannot communicate with other cllients associated with different AP.

LAN 1

Enabled

PVID: 1

Allowed VLANs: 1

CHAPTER 6 Switch

6.1 Overview

This chapter discusses the menus that you can use to monitor the Nebula managed Switches in your network and configure settings even before a Nebula Device is deployed and added to the site.

Nebula Device refers to Zyxel Hybrid Switches (GS / XGS / XMG / XS Series) in this chapter. The Nebula Device can operate in either standalone or Nebula cloud management mode. When the Nebula Device is in standalone mode, it can be configured and managed by the Web Configurator. When the Nebula Device is in Nebula cloud management mode, it can be managed and provisioned by the NCC. To view the list of Nebula Devices that can be managed through NCC, go to **Help** > **Support tools** > **Device function table**.

6.2 Monitor

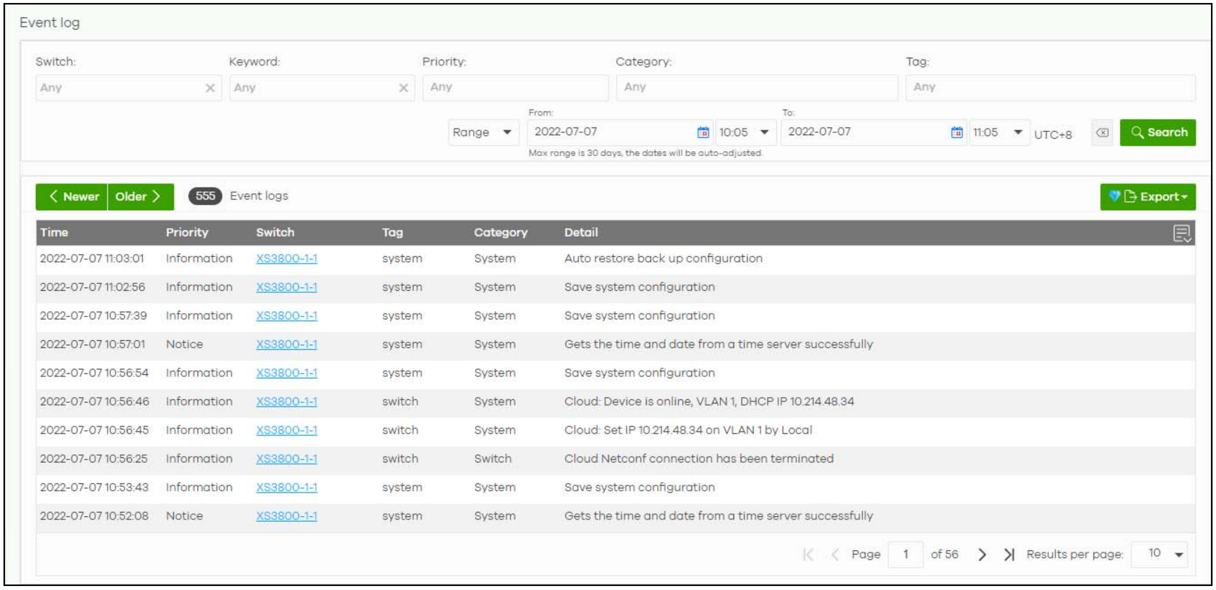
Use the **Monitor** menus to check the Nebula Device information, client information, event log messages and summary report for Nebula Devices in the selected site.

6.2.1 Event Log

Use this screen to view Nebula Device log messages. You can enter the Nebula Device name or a key word, select one or multiple event types, or specify a date/time or even a time range to display only the log messages related to it.

Click **Site-wide** > **Monitor** > **Switches** > **Event log** to access this screen.

Figure 93 Site-wide > Monitor > Switches > Event log



Event log

Switch: Any | Keyword: Any | Priority: Any | Category: Any | Tag: Any

Range | From: 2022-07-07 10:05 | To: 2022-07-07 11:05 | UTC+8 | Search

Max range is 30 days, the dates will be auto-adjusted.

< Newer | Older > | 555 Event logs | Export

Time	Priority	Switch	Tag	Category	Detail
2022-07-07 11:03:01	Information	XS3800-1-1	system	System	Auto restore back up configuration
2022-07-07 11:02:56	Information	XS3800-1-1	system	System	Save system configuration
2022-07-07 10:57:39	Information	XS3800-1-1	system	System	Save system configuration
2022-07-07 10:57:01	Notice	XS3800-1-1	system	System	Gets the time and date from a time server successfully
2022-07-07 10:56:54	Information	XS3800-1-1	system	System	Save system configuration
2022-07-07 10:56:46	Information	XS3800-1-1	switch	System	Cloud: Device is online, VLAN 1, DHCP IP 10.214.48.34
2022-07-07 10:56:45	Information	XS3800-1-1	switch	System	Cloud: Set IP 10.214.48.34 on VLAN 1 by Local
2022-07-07 10:56:25	Information	XS3800-1-1	switch	Switch	Cloud Netconf connection has been terminated
2022-07-07 10:53:43	Information	XS3800-1-1	system	System	Save system configuration
2022-07-07 10:52:08	Notice	XS3800-1-1	system	System	Gets the time and date from a time server successfully

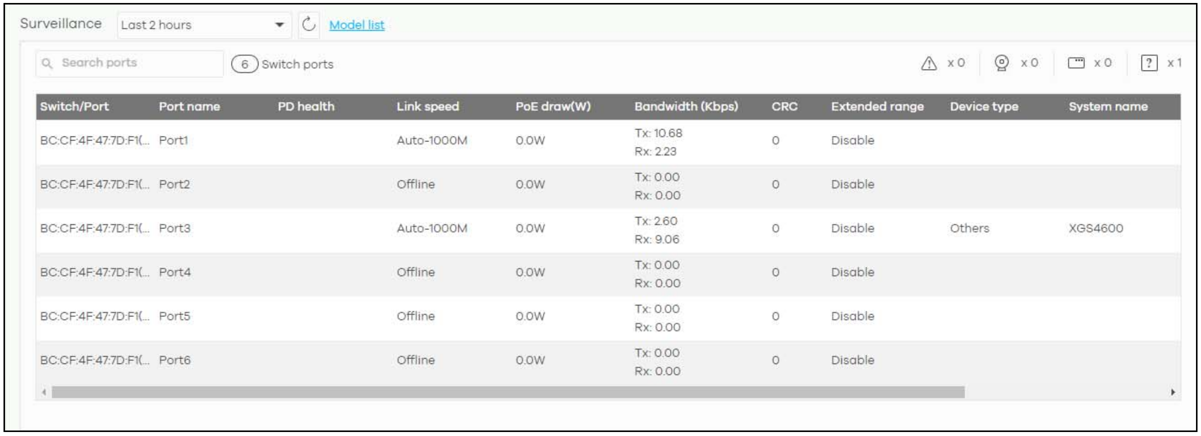
Page 1 of 56 | Results per page: 10

6.2.2 Surveillance

Use this screen to view information about Powered Devices (PDs) connected to ports on the Nebula Device.

Click **Site-wide** > **Monitor** > **Switches** > **Surveillance** to access this screen.

Figure 94 Site-wide > Monitor > Switches > Surveillance



Surveillance | Last 2 hours | Model list

Search ports | 6 Switch ports | ⚠ x 0 | x 0 | x 0 | ? x 1

Switch/Port	Port name	PD health	Link speed	PoE draw(W)	Bandwidth (Kbps)	CRC	Extended range	Device type	System name
BC:CF:4F:47:7D:F1(...	Port1		Auto-1000M	0.0W	Tx: 10.68 Rx: 2.23	0	Disable		
BC:CF:4F:47:7D:F1(...	Port2		Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable		
BC:CF:4F:47:7D:F1(...	Port3		Auto-1000M	0.0W	Tx: 2.60 Rx: 9.06	0	Disable	Others	XGS4600
BC:CF:4F:47:7D:F1(...	Port4		Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable		
BC:CF:4F:47:7D:F1(...	Port5		Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable		
BC:CF:4F:47:7D:F1(...	Port6		Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable		

The following table describes the labels in this screen.

Table 61 Site-wide > Monitor > Switches > Surveillance

LABEL	DESCRIPTION
Search ports	Enter a keyword to filter the list of ports or devices.
N switch ports	This shows the number of Nebula Device ports (N) in the list.
⚠	This shows the number of connected PDs that did not respond to an automatic PD alive check.
📷	This shows the number of ONVIF-compatible IP camera devices connected to Nebula Devices in the site.

Table 61 Site-wide > Monitor > Switches > Surveillance (continued)

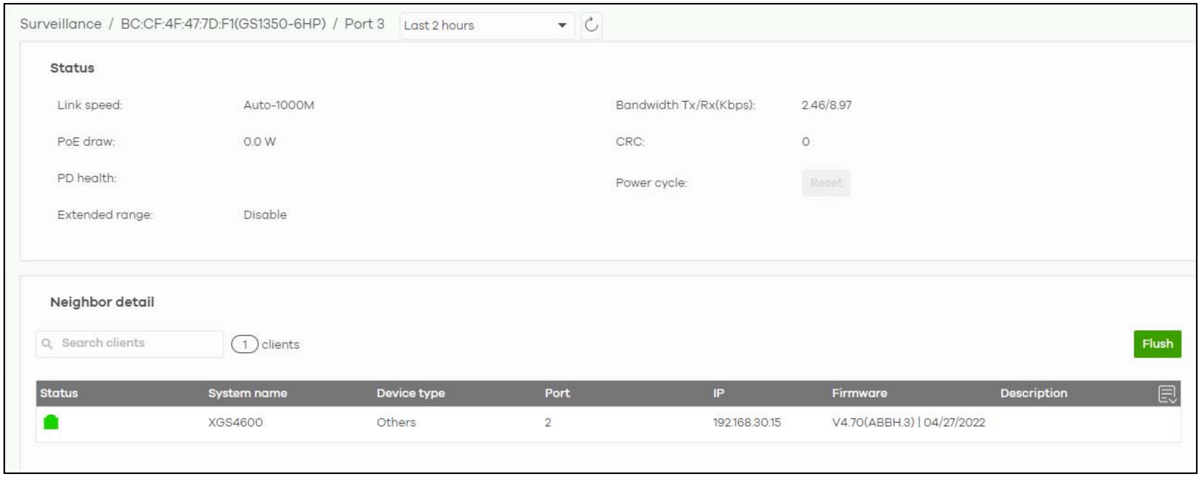
LABEL	DESCRIPTION
▭	This shows the number of ONVIF-compatible NVR devices connected to Nebula Devices in the site.
?	This shows the number of connected devices that did not respond to an ONVIF discovery query, or are of an unknown type.
Switch/Port	This shows the port number of the Nebula Device.
Port name	This shows the port description on the Nebula Device.
PD health	This shows the status of auto PD recovery on this port. • Red: The Nebula Device failed to get information from the PD connected to the port using LLDP, or the connected PD did not respond to the Nebula Device's ping requests. • Yellow: The Nebula Device is restarting the connected PD by turning the power off and turning it on again. • Green: The Nebula Device successfully discovered the connected PD using LLDP or ping. • **--**: Auto PD Recovery is not enabled on the Nebula Device and/or the port, or the switch is not supplying power to the connected PD. Note: For details on configuring auto PD recovery on a port, see Section 6.3.1 on page 362.
Link speed	This shows the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex or **H** for half). This field displays **Down** if the port is not connected to any device.
PoE draw(W)	This shows the total power that the connected PD draws from the port, in watts. This allows you to plan and use within the power budget of the Nebula Device.
Bandwidth (Kbps)	Tx shows the number of kilobytes per second transmitted on this port. Rx shows the number of kilobytes per second received on this port.
CRC	This shows the number of packets received with CRC (Cyclic Redundant Check) errors.
Extended range	This shows whether extended range is enabled on the port.
Device type	This shows the device type of the PD, as reported by ONVIF discovery.
System name	This shows the name of the connected PD, as reported by ONVIF or LLDP.
IP	This shows the IP address of the connected PD, as reported by ONVIF or LLDP.
Discovered devices	This shows how many devices are connected to the port. Click the number to go to the **Surveillance Port Details** screen.

6.2.3 Surveillance Port Details

Use this screen to view detailed information about a port on the **Surveillance** screen.

Go to **Site-wide** > **Monitor** > **Switches** > **Surveillance** and click on a value in the **Discovered Devices** column to access this screen.

Figure 95 Site-wide > Monitor > Switches > Surveillance > Port Details



Surveillance / BC:CF:4F:47:7D:F1(GS1350-6HP) / Port 3 Last 2 hours

Status

Link speed:	Auto-1000M	Bandwidth Tx/Rx(Kbps):	2.46/8.97
PoE draw:	0.0 W	CRC:	0
PD health:		Power cycle:	Reset
Extended range:	Disable		

Neighbor detail

Search clients 1 clients Flush

Status	System name	Device type	Port	IP	Firmware	Description
🟩	XGS4600	Others	2	192.168.30.15	V4.70(ABBH.3) | 04/27/2022	

The following table describes the labels in this screen.

Table 62 Site-wide > Monitor > Switches > Surveillance > Port Details

LABEL	DESCRIPTION
Status	
Link speed	This shows the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex or **H** for half). This field displays **Down** if the port is not connected to any device.
PoE draw	This shows the total power that the connected PD draws from the port, in watts. This allows you to plan and use within the power budget of the Nebula Device.
PD health	This shows the status of auto PD recovery on this port. • Red: The Nebula Device failed to get information from the PD connected to the port using LLDP, or the connected PD did not respond to the Nebula Device's ping requests. • Yellow: The Nebula Device is restarting the connected PD by turning the power off and turning it on again. • Green: The Nebula Device successfully discovered the connected PD using LLDP or ping. • **--**: Auto PD Recovery is not enabled on the Nebula Device and/or the port, or the Nebula Device is not supplying power to the connected PD. For details on configuring auto PD recovery on a port, see Section 6.3.1 on page 362.
Extended range	This shows whether extended range is enabled on the port.
Bandwidth Tx/Rx (%)	Tx shows the number of kilobytes per second transmitted on this port. Rx shows the number of kilobytes per second received on this port.
CRC	This shows the number of packets received with CRC (Cyclic Redundant Check) errors.
Power reset	Click **Power reset** to power off the PD connected to the port, by temporarily disabling then re-enabling PoE.
Neighbor detail	This section shows all clients connected to the port.
Search clients	Search for one or more clients in the list by keyword, status, system name, port, IP address, or firmware version.
clients	This shows the number of clients connected to this port.
Flush	Click this to remove all offline clients from the list.
Status	This shows whether the client is online (green) or offline (red), and whether the client is wired or wireless.
System name	This displays the system name of the Nebula Device.
Port	This displays the number of the Nebula Device port that is connected to the Nebula Device.

Table 62   Site-wide > Monitor > Switches > Surveillance > Port Details (continued)

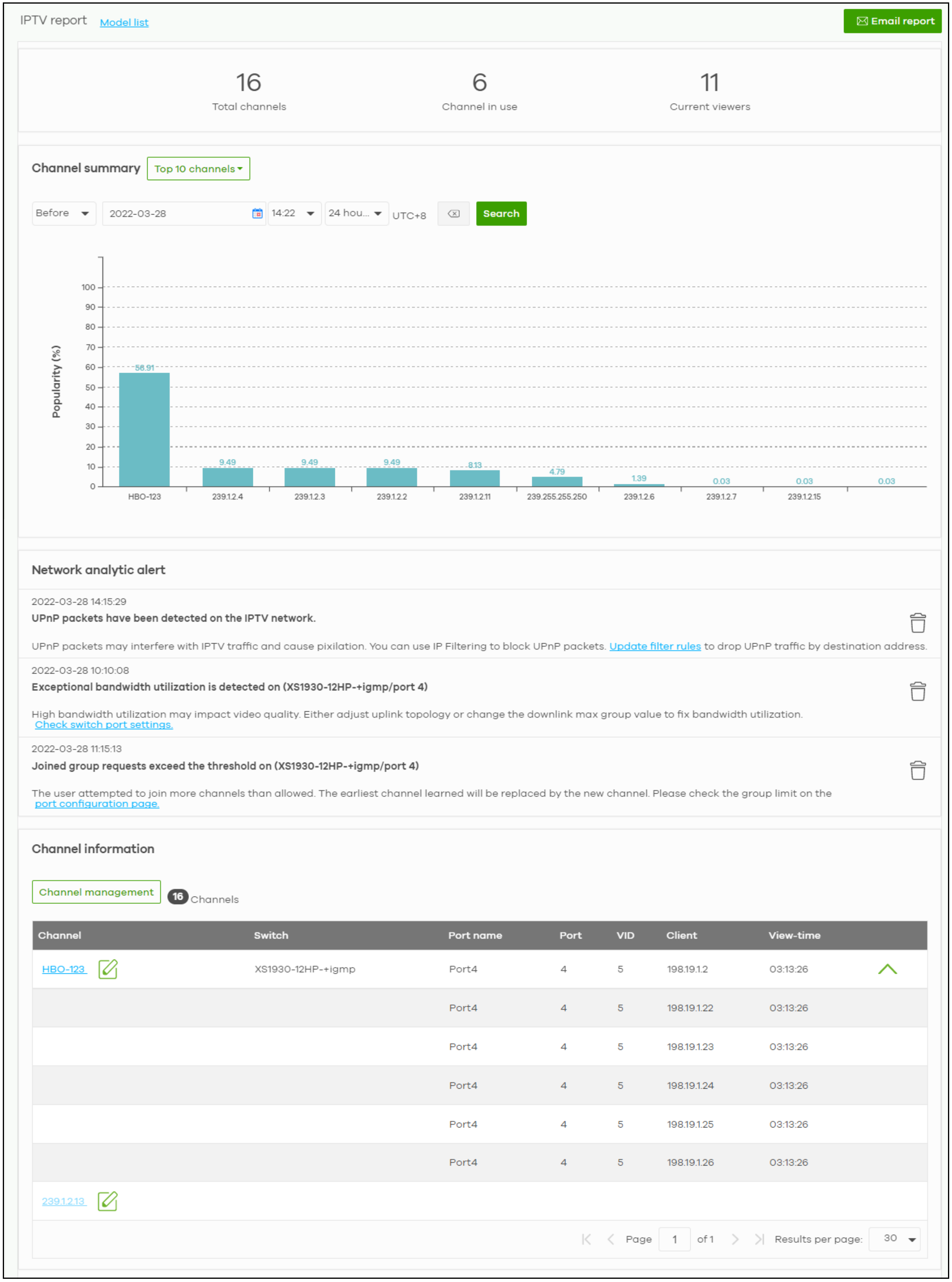
LABEL	DESCRIPTION
IP	This shows the IP address of the Nebula Device.
Firmware	This shows the firmware version currently installed on the Nebula Device.
Description	This shows the descriptive name of the Nebula Device.

6.2.4 IPTV Report

Use this screen to view available IPTV channels and client information.

Click **Site-wide** > **Monitor** > **Switches** > **IPTV report** to access this screen.

Figure 96 Site-wide > Monitor > Switches > IPTV Report



16 Total channels

6 Channel in use

11 Current viewers

Channel summary

2022-03-28

Network analytic alert

2022-03-28 14:15:29

UPnP packets have been detected on the IPTV network.

UPnP packets may interfere with IPTV traffic and cause pixilation. You can use IP Filtering to block UPnP packets. Update filter rules to drop UPnP traffic by destination address.

2022-03-28 10:10:08

Exceptional bandwidth utilization is detected on (XS1930-12HP-+igmp/port 4)

High bandwidth utilization may impact video quality. Either adjust uplink topology or change the downlink max group value to fix bandwidth utilization. Check switch port settings.

2022-03-28 11:15:13

Joined group requests exceed the threshold on (XS1930-12HP-+igmp/port 4)

The user attempted to join more channels than allowed. The earliest channel learned will be replaced by the new channel. Please check the group limit on the port configuration page.

Channel information

16 Channels

Channel	Switch	Port name	Port	VID	Client	View-time
HBO-123	XS1930-12HP-+igmp	Port4	4	5	198.19.1.2	03:13:26
		Port4	4	5	198.19.1.22	03:13:26
		Port4	4	5	198.19.1.23	03:13:26
		Port4	4	5	198.19.1.24	03:13:26
		Port4	4	5	198.19.1.25	03:13:26
		Port4	4	5	198.19.1.26	03:13:26
239.1.2.13						

The following table describes the labels in this screen.

Table 63 Site-wide > Monitor > Switches > IPTV Report

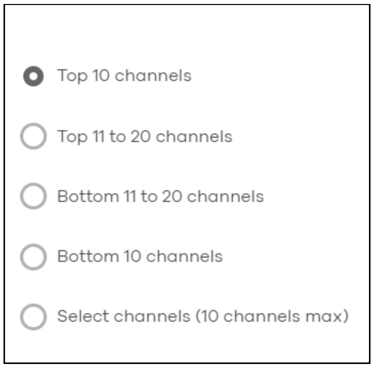
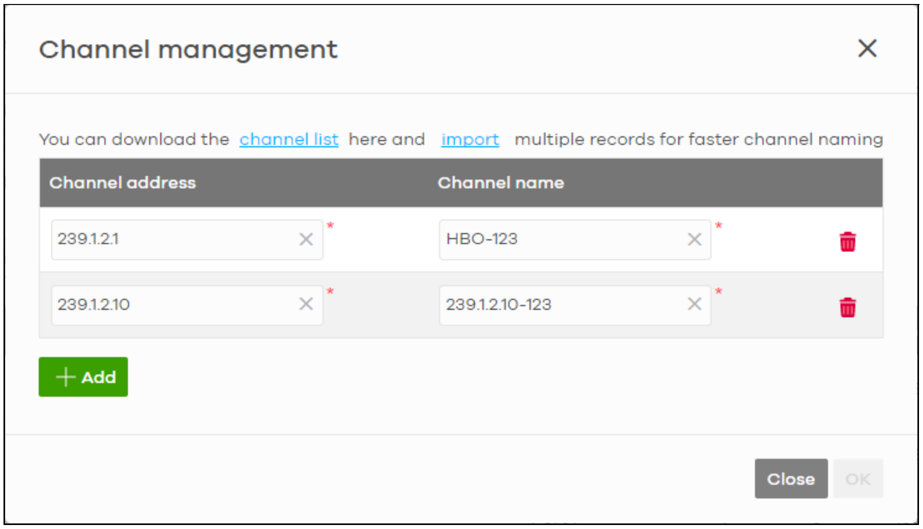
LABEL	DESCRIPTION
IPTV report	Click **Model list** to show the **Non-supported model list**. Click **See more** to go to the **Help** > **Support tools** > **Device function table** screen.
Email report	Click this button to send channel summary report by email, change the report logo and set email schedules.
Total channels	This shows the total number of IPTV channels that match the search criteria.
Channel in use	This shows the number of channels that are being watched by IPTV clients.
Current viewers	This shows the number of clients who are watching the IPTV channels.
Channel Summary	
	Select to view the channels according to the ranking. Alternatively, select **Select channels** to choose specific channels and click **Apply**.  ● Top 10 channels ○ Top 11 to 20 channels ○ Bottom 11 to 20 channels ○ Bottom 10 channels ○ Select channels (10 channels max)
Search	Specify a date/time and select to view the channels available in the past day, week or month before the specified date/time after you click **Search**. You can also select **Range** in the second field, set a time range and click **Search** to display only the channels available within the specified period of time.
y-axis	The y-axis represents the **Popularity (%)** of IPTV channels.
x-axis	The x-axis shows the name of the IPTV channel. It shows the channel's multicast group address by default.
Network Analytic Alert	This shows the alerts the NCC generates when an error or something abnormal is detected on the IPTV network. For example, the maximum number of the IGMP multicast groups (TV channels) a Nebula Device port can join is reached and new groups replace the earliest ones, UPnP packets are detected on the IPTV network and may interfere with IPTV traffic to cause TV pixelation, or high bandwidth usage on a certain Nebula Device port results in loss of video quality.
Channel Information	

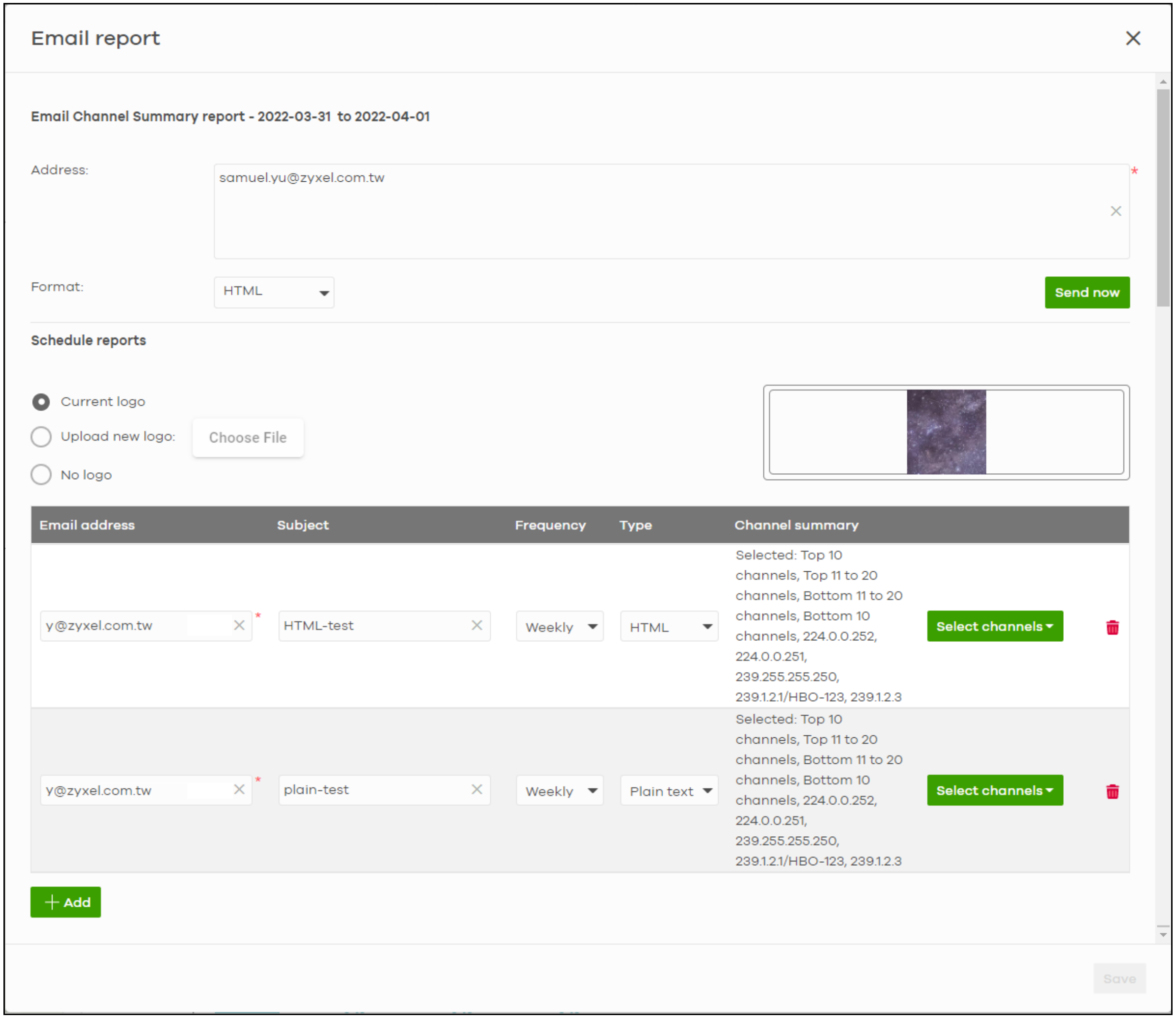
Table 63   Site-wide > Monitor > Switches > IPTV Report (continued)

LABEL	DESCRIPTION
Channel Management	Download the channel list and import multiple records for faster channel naming. Click **Add** to add new channels.  Channel management You can download the channel list here and import multiple records for faster channel naming Channel address: 239.1.2.1 — Channel name: HBO-123 Channel address: 239.1.2.10 — Channel name: 239.1.2.10-123
Channel	This shows the name of the channel. Click the edit icon to change the channel name. Click the channel name to display the channel's client statistics. See Section 6.2.4.2 on page 358.
Switch	This shows the name of the Nebula Device to which the client is connected.
Port Name	This shows the name of the Nebula Device port to which the client is connected.
Port	This shows the number of the Nebula Device port to which the client is connected.
VID	This shows the ID number of the VLAN to which the Nebula Device port belongs.
Client	This shows the IP address of the client who is watching the TV program on the channel.
View-time	This shows the amount of time the client has spent watching the IPTV channel.

6.2.4.1 Email Report

Use this screen to configure the email recipient's address, change the logo and set email schedules. To access this screen, click the **Email report** button in the **Site-wide** > **Monitor** > **Switches** > **IPTV Report** screen.

Figure 97 Site-wide > Monitor > Switches > IPTV Report: Email report



Email report

Email Channel Summary report - 2022-03-31 to 2022-04-01

Address: samuel.yu@zyxel.com.tw

Format: HTML

Schedule reports

● Current logo

○ Upload new logo:

○ No logo

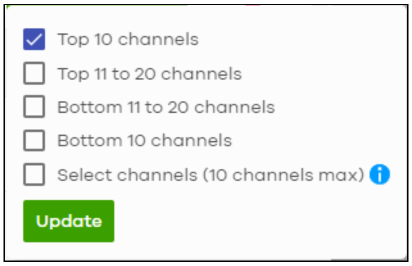
Email address	Subject	Frequency	Type	Channel summary
y@zyxel.com.tw	HTML-test	Weekly	HTML	Selected: Top 10 channels, Top 11 to 20 channels, Bottom 11 to 20 channels, Bottom 10 channels, 224.0.0.252, 224.0.0.251, 239.255.255.250, 239.1.2.1/HBO-123, 239.1.2.3
y@zyxel.com.tw	plain-test	Weekly	Plain text	Selected: Top 10 channels, Top 11 to 20 channels, Bottom 11 to 20 channels, Bottom 10 channels, 224.0.0.252, 224.0.0.251, 239.255.255.250, 239.1.2.1/HBO-123, 239.1.2.3

The following table describes the labels in this screen.

Table 64 Site-wide > Monitor > Switches > IPTV Report: Email report

LABEL	DESCRIPTION
Email Channel Summary report	This shows the range of the date/time you specified in the **Site-wide** > **Monitor** > **Switches** > **IPTV Report** screen.
Address	Enter the recipient's email address of the IPTV channel summary report.
Format	Select to send the IPTV channel summary report in **HTML** or **Plain text** format.
Send now	Click this button to send the IPTV channel summary report now.
Schedule reports	
logo	This shows the logo image that you uploaded for the customized IPTV channel summary report. Select **Current logo** to continue using the present logo. Select **Upload new logo** and click **Choose File** to locate the logo graphic. You can use the following image file formats: GIF, PNG, or JPG. File size must be less than 200 KB, and images larger than 244 x 190 will be resized. Select **No logo** if you do not want a logo to appear on the IPTV channel summary report.

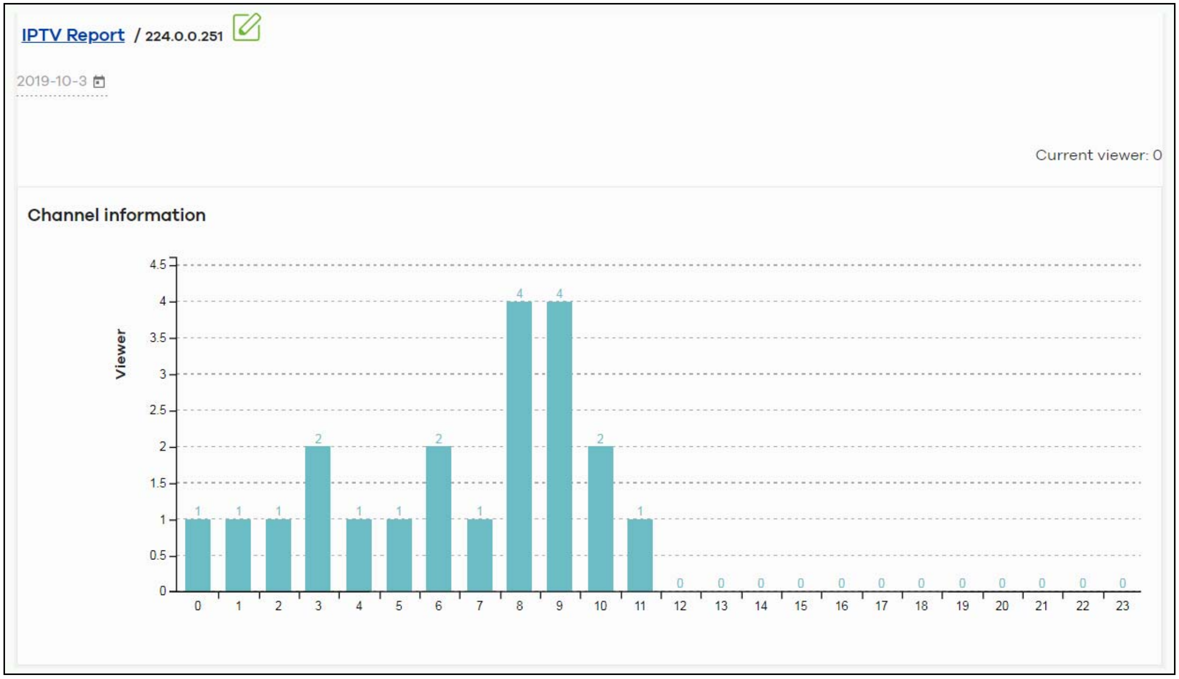
Table 64   Site-wide > Monitor > Switches > IPTV Report: Email report (continued)

LABEL	DESCRIPTION
+ Add	Click this button to add a scheduled IPTV channel summary report profile.
Email address	Enter the recipient's email address of the IPTV channel summary report.
Subject	Enter the subject of the IPTV channel summary report.
Frequency	Select to send the IPTV channel summary report **Monthly**, **Weekly**, or **Daily**.
Type	Select to send the IPTV channel summary report in **HTML** or **Plain text** format.
Channel summary	
	Select to view the channels report according to the ranking. Alternatively, select **Select channels** to choose specific channels and click **Update**.  ☑ Top 10 channels ☐ Top 11 to 20 channels ☐ Bottom 11 to 20 channels ☐ Bottom 10 channels ☐ Select channels (10 channels max) ⓘ Update
Remove	Click this to delete a scheduled profile.
Save	Click **Save** to save the new scheduled profile.

6.2.4.2 Channel Information

Use this screen to view the IPTV channel's client information and statistics. To access this screen, click a channel name from the **Channel Information** list in the **Site-wide** > **Monitor** > **Switches** > **IPTV Report** screen.

Figure 98   Site-wide > Monitor > Switches > IPTV Report: Channel Information



IPTV Report / 224.0.0.251

2019-10-3

Current viewer: 0

Channel information

The following table describes the labels in this screen.

Table 65 Switches > Monitor > Switches > IPTV Report: Channel Information

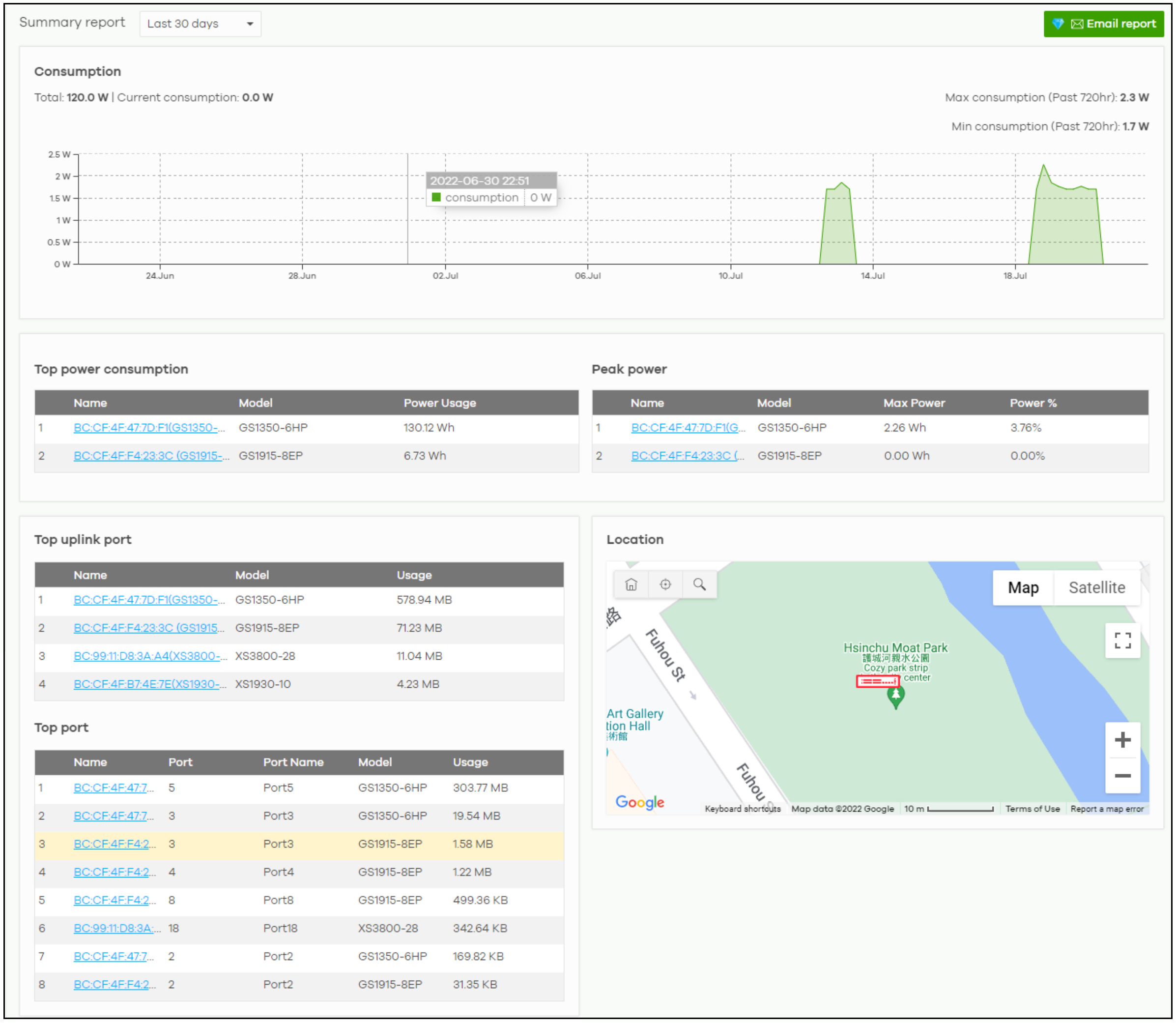
LABEL	DESCRIPTION
	Select a specific date to display only the clients who watch the IPTV channel on that day.
Current Viewer	This shows the number of clients who are currently watching the IPTV channel.
y-axis	The y-axis shows the number of clients watching the IPTV channel.
x-axis	The x-axis shows the hour of the day in 24-hour format.
Switch	This shows the name of the Nebula Device to which the client is connected.
Port Name	This shows the name of the Nebula Device port to which the client is connected.
Port	This shows the number of the Nebula Device port to which the client is connected.
VID	This shows the ID number of the VLAN to which the Nebula Device port belongs.
Client	This shows the IP address of the client who is watching the TV program on the channel.
View-time	This shows the amount of time the client has spent watching the IPTV channel.

6.2.5 Summary Report

This screen displays network statistics for Nebula Devices of the selected site, such as bandwidth usage, top ports and/or top Nebula Devices.

Click **Site-wide** > **Monitor** > **Switches** > **Summary Report** to access this screen.

Figure 99 Site-wide > Monitor > Switches > Summary Report



Consumption

Total: **120.0 W** | Current consumption: **0.0 W**

Max consumption (Past 720hr): **2.3 W**

Min consumption (Past 720hr): **1.7 W**

Top power consumption

	Name	Model	Power Usage
1	BC:CF:4F:47:7D:F1(GS1350-...	GS1350-6HP	130.12 Wh
2	BC:CF:4F:F4:23:3C (GS1915-...	GS1915-8EP	6.73 Wh

Peak power

	Name	Model	Max Power	Power %
1	BC:CF:4F:47:7D:F1(G...	GS1350-6HP	2.26 Wh	3.76%
2	BC:CF:4F:F4:23:3C (...	GS1915-8EP	0.00 Wh	0.00%

Top uplink port

	Name	Model	Usage
1	BC:CF:4F:47:7D:F1(GS1350-...	GS1350-6HP	578.94 MB
2	BC:CF:4F:F4:23:3C (GS1915...	GS1915-8EP	71.23 MB
3	BC:99:11:D8:3A:A4(XS3800-...	XS3800-28	11.04 MB
4	BC:CF:4F:B7:4E:7E(XS1930-...	XS1930-10	4.23 MB

Top port

	Name	Port	Port Name	Model	Usage
1	BC:CF:4F:47:7...	5	Port5	GS1350-6HP	303.77 MB
2	BC:CF:4F:47:7...	3	Port3	GS1350-6HP	19.54 MB
3	BC:CF:4F:F4:2...	3	Port3	GS1915-8EP	1.58 MB
4	BC:CF:4F:F4:2...	4	Port4	GS1915-8EP	1.22 MB
5	BC:CF:4F:F4:2...	8	Port8	GS1915-8EP	499.36 KB
6	BC:99:11:D8:3A:...	18	Port18	XS3800-28	342.64 KB
7	BC:CF:4F:47:7...	2	Port2	GS1350-6HP	169.82 KB
8	BC:CF:4F:F4:2...	2	Port2	GS1915-8EP	31.35 KB

Location

The following table describes the labels in this screen.

Table 66 Site-wide > Monitor > Switches > Summary Report

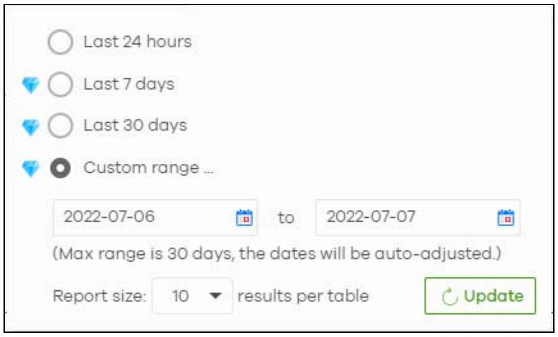
LABEL	DESCRIPTION
Switch – Summary report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ○ Last 7 days ○ Last 30 days ● Custom range ... 2022-07-06 to 2022-07-07 (Max range is 30 days, the dates will be auto-adjusted.) Report size: 10 results per table
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
Consumption	
Total	This shows the total power consumption of the Nebula Device ports.
Current Consumption	This shows the current power consumption of the Nebula Device ports.
Max Consumption	This shows the maximum power consumption of the Nebula Device ports.
Min Consumption	This shows the minimum power consumption of the Nebula Device ports.
y-axis	The y-axis shows how much power is used in Watts.
x-axis	The x-axis shows the time period over which the power consumption is recorded.
Top power consumption	
#	This shows the ranking of the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Power Usage	This shows the total amount of power consumed by the Nebula Device's connected PoE devices during the specified period of time.
Peak Power	
#	This shows the ranking of the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Max Power	This shows the maximum power consumption for the Nebula Device's connected PoE devices during the specified period of time.
Power %	This shows what percentage of the Nebula Device's total power budget has been consumed by connected PoE powered devices.
Top uplink port	
#	This shows the ranking of the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Usage	This shows the amount of data that has been transmitted through the Nebula Device's uplink port.
Top port	

Table 66 Site-wide > Monitor > Switches > Summary Report (continued)

LABEL	DESCRIPTION
#	This shows the ranking of the Nebula Device port.
Name	This shows the descriptive name of the Nebula Device.
Port	This shows the port number on the Nebula Device.
Model	This shows the model number of the Nebula Device.
Usage	This shows the amount of data that has been transmitted through the Nebula Device's port.
Location This shows the location of the Nebula Devices on the map.	

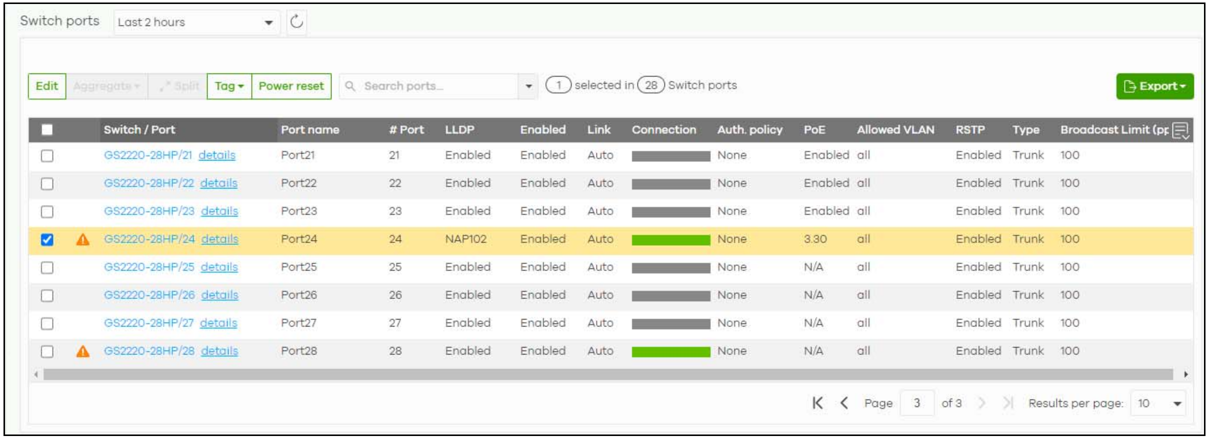
6.3 Configure

Use the **Configure** menus to configure port setting, IP filtering, RADIUS policies, PoE schedules, and other Nebula Device settings for Nebula Devices of the selected site.

6.3.1 Switch Ports

Use this screen to view port summary and configure Nebula Device settings for the ports. To access this screen, click **Site-wide** > **Configure** > **Switches** > **Switch ports** or click the **Configure ports** button in the **Site-wide** > **Devices** > **Switch: Switch Details** screen.

Figure 100 Site-wide > Configure > Switches > Switch ports



1 selected in 28 Switch ports

☐		Switch / Port	Port name	# Port	LLDP	Enabled	Link	Connection	Auth. policy	PoE	Allowed VLAN	RSTP	Type	Broadcast Limit (pp
☐		GS2220-28HP/21 details	Port21	21	Enabled	Enabled	Auto		None	Enabled	all	Enabled	Trunk	100
☐		GS2220-28HP/22 details	Port22	22	Enabled	Enabled	Auto		None	Enabled	all	Enabled	Trunk	100
☐		GS2220-28HP/23 details	Port23	23	Enabled	Enabled	Auto		None	Enabled	all	Enabled	Trunk	100
☑	⚠	GS2220-28HP/24 details	Port24	24	NAP102	Enabled	Auto	🟩	None	3.30	all	Enabled	Trunk	100
☐		GS2220-28HP/25 details	Port25	25	Enabled	Enabled	Auto		None	N/A	all	Enabled	Trunk	100
☐		GS2220-28HP/26 details	Port26	26	Enabled	Enabled	Auto		None	N/A	all	Enabled	Trunk	100
☐		GS2220-28HP/27 details	Port27	27	Enabled	Enabled	Auto		None	N/A	all	Enabled	Trunk	100
☐	⚠	GS2220-28HP/28 details	Port28	28	Enabled	Enabled	Auto	🟩	None	N/A	all	Enabled	Trunk	100

Page 3 of 3 Results per page: 10

The following table describes the labels in this screen.

Table 67 Site-wide > Configure > Switches > Switch ports

LABEL	DESCRIPTION
Switch ports	Select to view the detailed information and connection status of the Nebula Device port in the past two hours, day, week or month.
↻	Click this button to reload the data-related frames on this page.
Edit	Select the ports you want to configure and click this button to configure Nebula Device settings on the ports, such as link aggregation, PoE schedule, LLDP and STP.
Aggregate	Select more than one port and click this button to group the physical ports into one logical higher-capacity link.

Table 67 Site-wide > Configure > Switches > Switch ports (continued)

LABEL	DESCRIPTION
Split	Select a trunk group and click this button to delete the trunk group. The ports in this group then are not aggregated. A trunk group is one logical link containing multiple ports.
Tag	Click this button to create a new tag or delete an existing tag.
Power reset	Click this button to reboot the PD (powered device) connected to the PoE port. Follow the prompt and click **Confirm** to reboot the PD connected to this port. Note: This button is not available for an uplink port.
Search	Specify your desired filter criteria to filter the list of Nebula Device ports. You can filter the search by selecting one or more Nebula Devices. Under Ports, you can search for multiple ports separated by a comma, or a range separated by a hyphen. For example: 1,2,4–6.
Switch ports	This shows the number of ports on the Nebula Device.
Export	Click this button to save the Nebula Device port list as a CSV or XML file to your computer.
CRC alert icon	This prompt appears if CRC errors are detected in the port(s). Go to **Site-wide** > **Devices** > **Switches: Switch Details: Port Details** for the details. See Section 4.3.2.1 on page 229 for more information.
Switch / Port	This shows the Nebula Device name and port number. If the port is added to a trunk group, this also shows whether it is configured as a static member of the trunk group (**Static**) or configured to join the trunk group through LACP (**LACP**). If the port is connected to an uplink gateway, it shows **Uplink**. If the port is a stacking port, it shows the stacking name, slot ID and port number. Click **details** to display the port details screen. See Section 4.3.2.1 on page 229.
Port name	This shows the descriptive name of the port.
Port profiles	This shows the name of the port profile applied on this port.
#Port	This shows the port number.
LLDP	This shows whether Link Layer Discovery Protocol (LLDP) is supported on the port.
Received broadcast packets	This shows the number of good broadcast packets received.
Received bytes	This shows the number of bytes received on this port.
Received packets	This shows the number of received frames on this port.
Sent broadcast packets	This shows the number of good broadcast packets transmitted.
Sent bytes	This shows the number of bytes transmitted on this port.
Sent multicast packets	This shows the number of good multicast packets transmitted.
Received multicast packets	This shows the number of good multicast packets received.
Sent packets	This shows the number of transmitted frames on this port.
Total bytes	This shows the total number of bytes transmitted or received on this port.
Enabled	This shows whether the port is enabled or disabled.
Link	This shows the speed of the Ethernet connection on this port. **Auto** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support.

Table 67 Site-wide > Configure > Switches > Switch ports (continued)

LABEL	DESCRIPTION
Connection	This shows the connection status of the port. • Gray (#888888): The port is disconnected. • Orange (#FF8900): The port is connected and is transmitting data at 10 or 100 Mbps. • Green (#64BE00): The port is connected and is transmitting data at 1000 Mbps (1 Gbps). • Azure (#00B2FF): The port is connected and is transmitting data at 2.5 Gbps. • Violet (#8800FF): The port is connected and is transmitting data at 5 Gbps. • Blue (#004FEE): The port is connected and is transmitting data at 10000 Mbps (10 Gbps). When the port is in the STP blocking state, failed LACP negotiation state, or failed port authentication state, a blocked icon displays. Move the cursor over a time slot to see the actual date and time when a port is connected or disconnected.
Auth. policy	This shows the name of authentication policy applied to the port.
Allowed VLAN	This shows the VLANs from which the traffic comes is allowed to be transmitted or received on the port.
PoE	This shows whether PoE is enabled on the port.
RSTP	This shows whether RSTP is enabled on the port.
Status	If STP/RSTP is enabled, this field displays the STP state of the port. If STP/RSTP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **Disabled**.
Schedule	This shows the name of the PoE schedule applied to the port.
Type	This shows the port type (**Trunk** or **Access**).
PVID	This shows the port VLAN ID. It is a tag that adds to incoming untagged frames received on the port so that the frames are forwarded to the VLAN group that the tag defines.
Tag	This shows the user-specified tag that the Nebula Device adds to the outbound traffic on this port.
Storm Control	This shows whether traffic storm control is enabled or disabled on the port.
Broadcast Limit (pps)	This shows the maximum number of broadcast packets the Nebula Device accepts per second on this port.
Multicast Limit (pps)	This shows the maximum number of multicast packets the Nebula Device accepts per second on this port.
DLF Limit (pps)	This shows the maximum number of Destination Lookup Failure (DLF) packets the Nebula Device accepts per second on this port.
Loop Guard	This shows whether loop guard is enabled or disabled on the port.
Network Analytic Alert	An amber alert icon displays if the NCC generates alerts when an error or something abnormal is detected on the port for the IPTV network. Move the cursor over the alert icon to view the alert details.
IPSG protected	This shows whether IP source guard protection is enabled on this port.
Received CRC packets	This shows the number of CRC (Cyclic Redundancy Check) errors received on the port.
Number of IGMP Group	This shows the number of IGMP groups the port has joined.

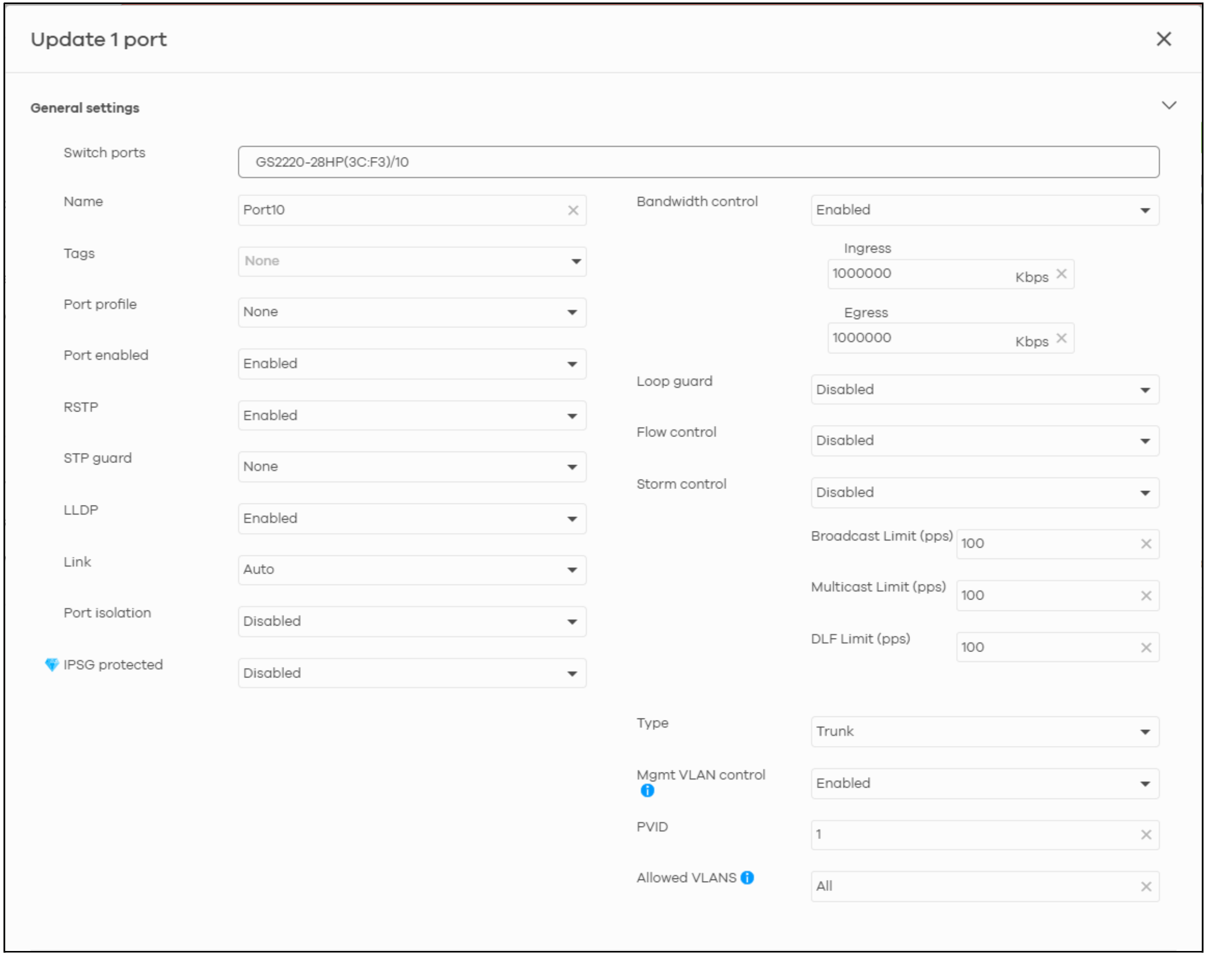
Table 67 Site-wide > Configure > Switches > Switch ports (continued)

LABEL	DESCRIPTION
Mgmt VLAN control	This shows if management control is enabled on this port. See Table 68 on page 366 for more information. Note: When the Nebula Device's Set IP address: Global VLAN configuration is enabled, it will use the site-wide management VLAN ID. When the Nebula Device's Set IP address: Global VLAN configuration is disabled, the Nebula Device's management VLAN will use its individual VLAN settings rather than the site-wide management VLAN ID.
Flow control	This shows if flow control is enabled on this port. See Table 68 on page 366 for more information.
☰	Click this icon to display a greater or lesser number of configuration fields.

6.3.1.1 Update ports

Click to select the port you want to configure in the **Site-wide** > **Configure** > **Switches** > **Switch ports** screen.

Figure 101 Site-wide > Configure > Switches > Switch ports: Edit



Update 1 port

General settings

Switch ports: GS2220-28HP(3C:F3)/10

Name: Port10

Tags: None

Port profile: None

Port enabled: Enabled

RSTP: Enabled

STP guard: None

LLDP: Enabled

Link: Auto

Port isolation: Disabled

IPSG protected: Disabled

Bandwidth control: Enabled

Ingress: 1000000 Kbps

Egress: 1000000 Kbps

Loop guard: Disabled

Flow control: Disabled

Storm control: Disabled

Broadcast Limit (pps): 100

Multicast Limit (pps): 100

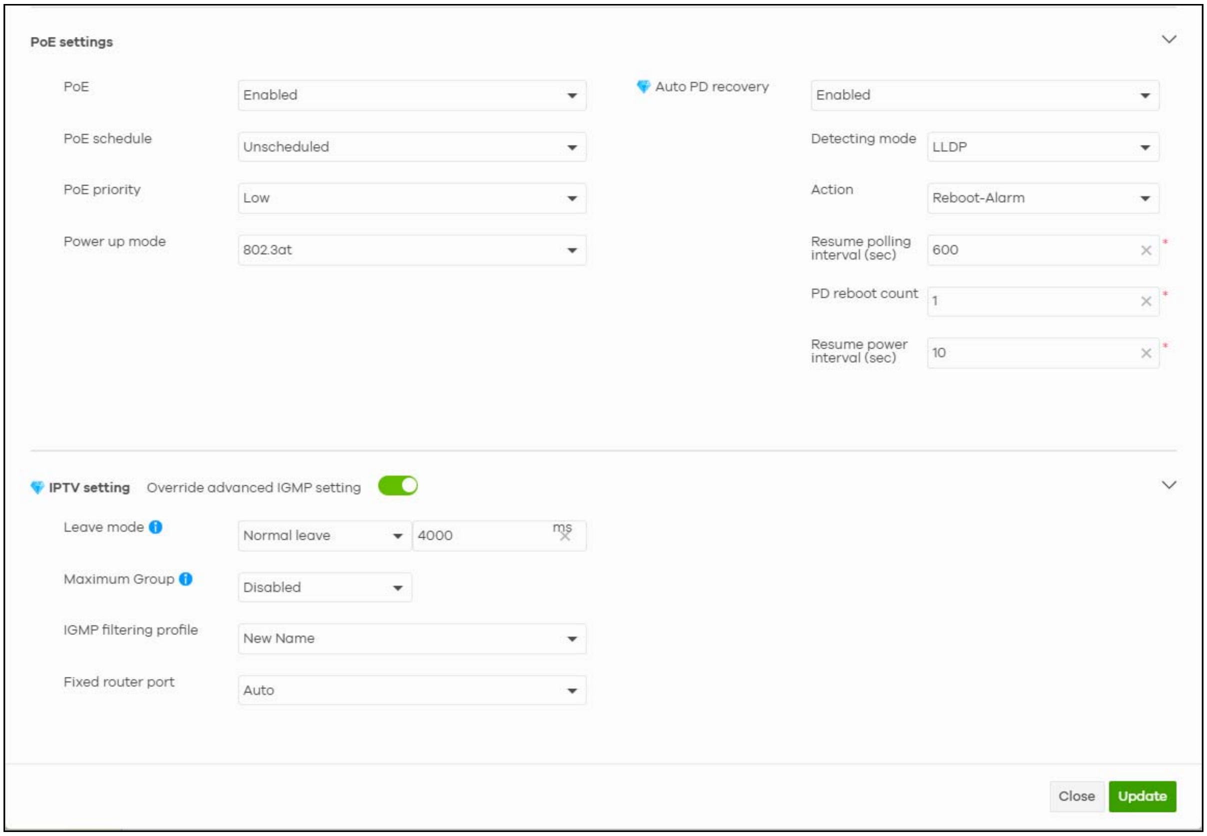
DLF Limit (pps): 100

Type: Trunk

Mgmt VLAN control: Enabled

PVID: 1

Allowed VLANS: All



PoE settings

PoE: Enabled

PoE schedule: Unscheduled

PoE priority: Low

Power up mode: 802.3at

Auto PD recovery: Enabled

Detecting mode: LLDP

Action: Reboot-Alarm

Resume polling interval (sec): 600

PD reboot count: 1

Resume power interval (sec): 10

IPTV setting   Override advanced IGMP setting

Leave mode: Normal leave   4000 ms

Maximum Group: Disabled

IGMP filtering profile: New Name

Fixed router port: Auto

The following table describes the labels in this screen.

Table 68   Site-wide > Configure > Switches > Switch ports: Edit

LABEL	DESCRIPTION
Switch ports	This shows the Nebula Device name and port number for the ports you are configuring in this screen.
Name	Enter a descriptive name for the ports.
Tags	Select or create a new tag for outgoing traffic on the ports.
Port profile	Select the port profile you created in **Site-wide** > **Configure** > **Switches** > **Port profiles** > **Create port profile** and make sure to enable this port profile to apply to this port. Note: You cannot create link aggregation on ports that have applied a port profile.
Port enabled	Select to enable or disable the ports. A port must be enabled for data transmission to occur.
RSTP	Select to enable or disable RSTP (Rapid Spanning Tree Protocol) on the ports. RSTP detects and breaks network loops and provides backup links between switches, bridges or routers. It ensures that only one path exists between any two stations on the network.
STP guard	This field is available only when RSTP is enabled on the ports. Select **Root guard** to prevent the Nebula Devices attached to the ports from becoming the root bridge. Select **BPDU guard** to have the Nebula Device shut down the ports if there is any BPDU received on the ports. Otherwise, select **None**.

Table 68 Site-wide > Configure > Switches > Switch ports: Edit (continued)

LABEL	DESCRIPTION
LLDP	Select to enable or disable LLDP (Link Layer Discovery Protocol) on the ports. LLDP allows the connected network device to advertise its identity and capabilities on the local network.
Link	Select the speed and the duplex mode of the Ethernet connection on the ports. Choices are **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex**, **100M/Full Duplex**, **1000M/Full Duplex**, **Auto**, **10M/AN**, and **100M/AN** (Gigabit connections only).
Extended range	Select to enable or disable extended range. Extended range allows the port to transmit power and data at a distance of 250 meters. Note: When enabled, the port's PoE **Power up mode** is locked to 802.3at, and the port's link speed is limited to 10M/Full Duplex.
Media type	You can insert either an SFP+ transceiver or an SFP+ Direct Attach Copper (DAC) cable into the 10 Gigabit interface of the Nebula Device. Select the media type (**SFP+** or **DAC 10G**) of the SFP+ module that is attached to the 10 Gigabit interface.
FEC	To minimize signal degradation of data at high transmission speeds (for example, 25 Gbps or 100 Gbps), set the same **FEC** (Forward Error Correction) type between the Nebula Device and the connected device. Select **Auto** to allow both connected ports to automatically set the FEC type according to the following rules: • For 10G transceivers, the FEC type on the port will automatically be **None**. • For 25G transceivers, the FEC type on the port will automatically be **CL108**. • For 100G transceivers, the FEC type on the port will automatically be **None** if the transceiver type is 100G LR4/ER4; all other types of transceiver will automatically be **CL91**. Select **CL74** when both connected ports support 25 Gbps speed and require low latency in data transmission. Select **CL91** when both connected ports support 25 Gbps and 100 Gbps speeds. Select **CL108** when both connected ports support 25 Gbps speed but low latency in data transmission is not required. Alternatively, select **None** when you do not need to set the FEC type. Note: Make sure to set the correct **Link** on this screen (see the previous field).
Port Isolation	Select to enable or disable port isolation on the ports. The ports with port isolation enabled cannot communicate with each other. They can communicate only with the CPU management port of the same Nebula Device and the Nebula Device's other ports on which the isolation feature is not enabled.
IPSG protected	Select to enable or disable IP source guard protection on the port. IP source guard checks incoming IPv4 packets on that port. A packet is allowed when it matches any entry in the IPSG binding table. If a user tries to send IPv4 packets to the Nebula Device that do not match an entry in the IPSG binding table, the Nebula Device will drop these packets. The Nebula Device forwards matching traffic normally.
Auth. policy	This field is available only when you select **Access** in the **Type** field. Select the authentication policy type and name of the pre-configured authentication policy that you want to apply to the ports. See Table 84 on page 407 for more information on authentication policy type. See Section 6.3.9 on page 405 for more information on configuring authentication policy. Select **Open** if you do NOT want to enable port authentication on the ports.

Table 68 Site-wide > Configure > Switches > Switch ports: Edit (continued)

LABEL	DESCRIPTION
Bandwidth Control	Select to enable or disable bandwidth control on the port. Bandwidth control means defining a maximum allowable bandwidth for incoming and/or outgoing traffic flows on a port.
Ingress	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on the ports.
Egress	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on the ports.
Loop guard	Select to enable or disable loop guard on the ports. Loop guard allows you to configure the Nebula Device to shut down a port if it detects that packets sent out on that port to the edge of your network loop back to the Nebula Device. While you can use STP (Spanning Tree Protocol) to prevent loops in the core of your network, STP cannot prevent loops that occur on the edge of your network. Note: The loop guard feature cannot be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.
Flow control	Select to enable or disable flow control on all ports. Enable flow control to allow the Nebula Device's port to send a pause signal to the connected device, and for the connected device to send a pause signal to the Nebula Device. The Nebula Device will temporarily stop sending signals after receiving a pause signal. Note: Make sure the connected device also supports flow control.
Storm control	Select to enable or disable broadcast storm control on the ports. Storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Nebula Device receives per second on the ports. When the maximum number of allowable packets is reached per second, the subsequent packets are discarded.
Broadcast Limit (pps)	Specifies the maximum number of broadcast packets the Nebula Device accepts per second on the ports.
Multicast Limit (pps)	Specifies the maximum number of multicast packets the Nebula Device accepts per second on the ports.
DLF Limit (pps)	Specifies the maximum number of DLF packets the Nebula Device accepts per second on the ports.
Type	Set the type of the port. Select **Access** to configure the port as an access port which can carry traffic for just one VLAN. Frames received on the port are tagged with the port VLAN ID. Select **Trunk** to configure the port as a trunk port which can carry traffic for multiple VLANs over a link. A trunk port is always connected to a Nebula Device or router.
Mgmt VLAN control	Select **Enabled** to configure the port as a management port. This allows the administrator to set the Nebula Device ports through which the device management VLAN traffic is allowed. The default value depends on your setting for the previous **Type** field. The default value is **Enabled** when the **Type** is **Trunk**. The default value is **Disabled** when the **Type** is **Access**. Note: Make sure to enable this for an uplink port to maintain connection with Nebula.

Table 68 Site-wide > Configure > Switches > Switch ports: Edit (continued)

LABEL	DESCRIPTION
VLAN type	This field is available only when you select **Access** in the **Type** field. **None**: This port is a regular access port and follows the device's access port rules. **Vendor ID based VLAN**: Apply the Vendor ID based VLAN settings from **Switch** > **Configure** > **Switch settings** to this port. **Voice VLAN**: Apply the Voice VLAN settings from **Site-wide** > **Configure** > **Switches** > **Switch settings** to this port. Note: For details on configuring Vendor ID based VLAN and Voice VLAN settings, see Section 6.3.11 on page 409.
PVID	A PVID (Port VLAN ID or native VLAN) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1and 4094 as the port VLAN ID.
Allowed VLANs	This field is available only when you select **Trunk** in the **Type** field. Specify the VLANs from which the traffic comes. You can then transmit or receive traffic on the ports. See Section 3.40 on page 183 for the steps in setting up dynamic VLAN with RADIUS. See Section 3.41 on page 185 for more information on monitoring dynamic VLANs using event logs.
PoE Settings	
PoE	Select **Enabled** to provide power to a PD connected to the ports.
PoE schedule	This field is available only when you enable PoE. Select a pre-defined schedule (created using the **Site-wide** > **Configure** > **Switches** > **PoE schedules** screen) to control when the Nebula Device enables PoE to provide power on the ports. Note: You must select **Unschedule** in the **PoE schedule** field before you can disable PoE on the ports. If you enable PoE and select **Unschedule**, PoE is always enabled on the ports. Note: The Nebula Device will follow the PoE schedule even when the Nebula Device is not connected to NCC. Click **Edit** to go to **Site-wide** > **Configure** > **Switches** > **PoE schedules** screen to create a new PoE schedule.
PoE priority	When the total power requested by the PDs exceeds the total PoE power budget on the Nebula Device, you can set the PD priority to allow the Nebula Device to provide power to ports with higher priority. Select **Low** to set the Nebula Device to assign the remaining power to the port after all critical and medium priority ports are served. Select **Medium** to set the Nebula Device to assign the remaining power to the port after all critical priority ports are served. Select **Critical** to give the highest PD priority on the port.

Table 68 Site-wide > Configure > Switches > Switch ports: Edit (continued)

LABEL	DESCRIPTION
Power up mode	Set how the Nebula Device provides power to a connected PD at power-up. **802.3at** – the Nebula Device supports the IEEE 802.3at High Power over Ethernet standard and can supply power of up to 30W per Ethernet port. IEEE 802.3at is also known as PoE+ or PoE Plus. An IEEE 802.3at compatible device is referred to as Type 2. Power Class 4 (High Power) can only be used by Type 2 devices. If the connected PD requires a Class 4 current when it is turned on, it will be powered up in this mode. **802.3af** – the Nebula Device follows the IEEE 802.3af Power over Ethernet standard to supply power to the connected PDs during power-up. **Legacy** – the Nebula Device can provide power to the connected PDs that require high inrush currents at power-up. Inrush current is the maximum, instantaneous input current drawn by the PD when first turned on. **Pre-802.3at** – the Nebula Device initially offers power on the port according to the IEEE 802.3af standard, and then switches to support the IEEE 802.3at standard within 75 milliseconds after a PD is connected to the port. Select this option if the Nebula Device is performing 2-event Layer-1 classification (PoE+ hardware classification) or the connected PD is NOT performing Layer 2 power classification using Link Layer Discovery Protocol (LLDP). **Force 802.3at** – the Nebula Device provides PD Wide Range Detection (WRD) with power of up to 33 W on the port without performing PoE classification. Select this if the connected PD does not comply with any PoE standard. **802.3bt** – the Nebula Device follows the IEEE 802.3bt standard to supply power of up to 60 W per Ethernet port to the connected PDs at power-up. **Pre-802.3bt** – the Nebula Device offers power on the port according to the IEEE 802.3bt standard. Select this if the connected PD was manufactured before the IEEE 802.3bt standard was implemented on September 2018, but requires power between 33 W and 60 W. IEEE 802.3bt is also known as PoE++ or PoE Plus Plus.
Auto PD recovery	Select to enable or disable automatic PD recovery on the port. Automatic PD recovery allows the Nebula Device to restart a Powered Device (PD) connected to the port by turning the device on and off again.
Detecting mode	Select **LLDP** to have the Nebula Device passively monitor current status of the connected Powered Device (PD) by reading LLDP packets from the PD on the port. Select **Ping** to have the Nebula Device ping the IP address of the connected Powered Device (PD) through the designated port to test whether the PD is reachable or not.
Action	Set the action to take when the connected Powered Device (PD) has stopped responding. Select **Reboot-Alarm** to have the Nebula Device send an SNMP trap and generate a log message, and then turn off the power of the connected PD and turn it back on again to restart the PD. Select **Alarm** to have the Nebula Device send an SNMP trap and generate a log message.
Neighbor IP	Set the IPv4 address of the Powered Device (PD) connected to this port. Note: If **Detecting Mode** is set to **Ping** and the PD supports LLDP, the connected PD's IPv4 address to which the Nebula Device sends ping requests is displayed automatically.
Polling interval (sec)	Specify the number of seconds the Nebula Device waits for a response before sending another ping request. For example, the Nebula Device will try to detect the PD status by performing ping requests every 20 seconds.
Polling count	Specify how many times the Nebula Device resends a ping request before considering the PD unreachable.

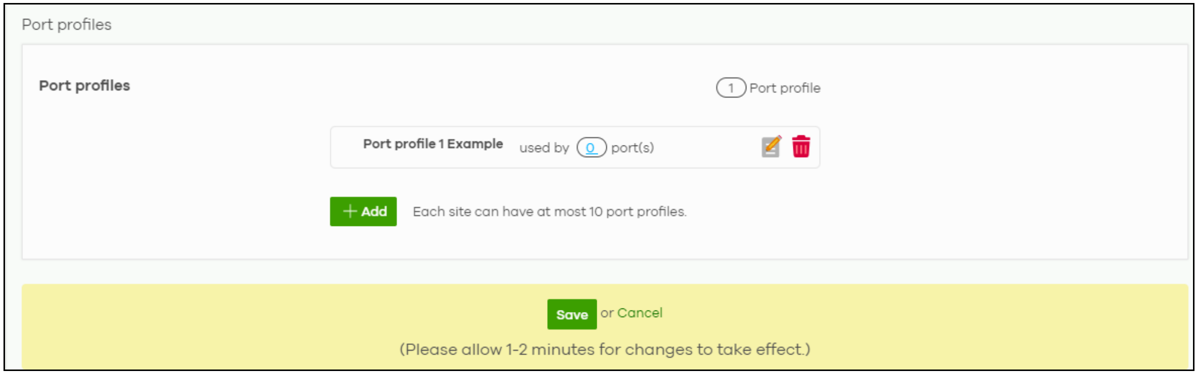
Table 68   Site-wide > Configure > Switches > Switch ports: Edit (continued)

LABEL	DESCRIPTION
Resume polling interval (sec)	Specify the number of seconds the Nebula Device waits before monitoring the PD status again after it restarts the PD on the port.
PD reboot count	Specify how many times the Nebula Device attempts to restart the PD on the port. The **PD Reboot Count** resets if any of the following conditions are true: • The Nebula Device successfully pings the PD. • You modify any **Auto PD Recovery** settings and apply them. • The Nebula Device restarts.
Resume power interval (sec)	Specify the number of seconds the Nebula Device waits before supplying power to the connected PD again after it restarts the PD on the port.
IPTV Setting	
Override advanced IGMP setting	Select ON to overwrite the port's advanced IGMP settings (configured in the **Site-wide** > **Configure** > **Switches** > **Advanced IGMP** screen) with the settings you configure in the fields below. Otherwise, select OFF.
Leave mode	Select **Immediate Leave** to remove this port from the multicast tree immediately when an IGMP leave message is received on this port. Select this option if there is only one host connected to this port. Select **Normal Leave** or **Fast Leave** and enter an IGMP normal/fast leave timeout value to have the Nebula Device wait for an IGMP report before the leave timeout when an IGMP leave message is received on this port. You need to specify how many milliseconds the Nebula Device waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host. In **Normal Leave** mode, when the Nebula Device receives an IGMP leave message from a host on a port, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The Nebula Device forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table. In **Fast Leave** mode, right after receiving an IGMP leave message from a host on a port, the Nebula Device itself sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process.
Maximum Group	Select **Enable** and enter the maximum number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report received on this port will replace the earliest group entry in the multicast forwarding table. Otherwise, select **Disable** to turn off multicast group limits.
IGMP filtering profile	An IGMP filtering profile specifies a range of multicast groups that clients connected to the Nebula Device are able to join. Select the name of the IGMP filtering profile to use for this port. Otherwise, select **No Select** to remove restrictions and allow the port to join any multicast group.
Fixed router port	Select **Auto** to have the Nebula Device use the port as an IGMP query port if the port receives IGMP query packets. The Nebula Device forwards IGMP join or leave packets to an IGMP query port. Select **Fixed** to have the Nebula Device always use the port as an IGMP query port. This helps prevent IGMP network topology changes when query packet losses occur in the network.
Close	Click this button to exit this screen without saving.
Update	Click this button to save your changes and close the screen.

6.3.2 Port Profiles

Use this screen to create profiles that can be applied to each port on the Nebula Device. A port profile can contain features such as RSTP (Rapid Spanning Tree Protocol), STP guard, port isolation, loop guard, storm control, and PoE (Power over Ethernet). To access this screen, click **Site-wide** > **Configure** > **Switches** > **Port profiles**.

Figure 102 Site-wide > Configure > Switches > Port profiles


Port profiles
Port profiles
1 Port profile
Port profile 1 Example
used by 0 port(s)
+ Add
Each site can have at most 10 port profiles.
Save
or Cancel
(Please allow 1-2 minutes for changes to take effect.)

The following table describes the labels in this screen.

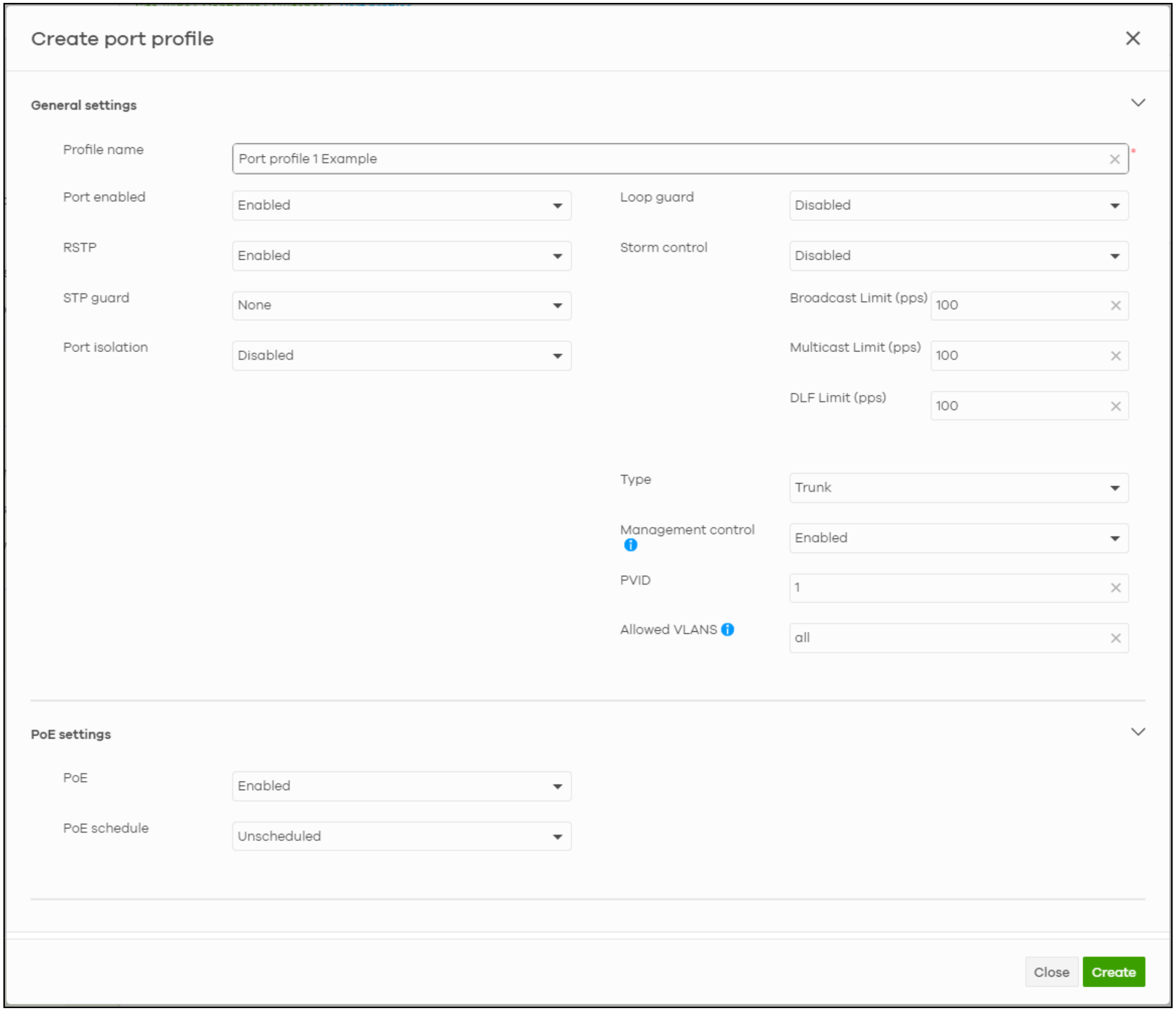
Table 69 Site-wide > Configure > Switches > Port profiles

LABEL	DESCRIPTION
Port profile	This shows the number of port profiles configured on this site.
used by port(s)	This shows the port profile name and the number of ports that are using this port profile. Click the number to go to the **Site-wide** > **Configure** > **Switches** > **Switch ports** screen.
edit	Click this icon to go to **Site-wide** > **Configure** > **Switches** > **Port profiles** > **Update port profile** to edit an existing port profile.
delete	Click this icon to remove the port profile. Note: You can remove a port profile only when the port profile is not applied to any port.
+ Add	Click this button to create a new port profile for Nebula Switches on the site. Note: Each site can only have a maximum of 10 port profiles.
Save	Click **Save** to save your changes and create the port profile.
Cancel	Click **Cancel** to exit this screen without saving.

6.3.2.1 Port Profile Configuration

Click the **Add** button or click the Edit button in the **Port profile** screen to open the **Site-wide** > **Configure** > **Switches** > **Port profiles** > **Create/Edit port profile** screen.

Figure 103 Site-wide > Configure > Switches > Port profiles > Create/Edit port profile



Create port profile

General settings

Profile name: Port profile 1 Example

Port enabled: Enabled

RSTP: Enabled

STP guard: None

Port isolation: Disabled

Loop guard: Disabled

Storm control: Disabled

Broadcast Limit (pps): 100

Multicast Limit (pps): 100

DLF Limit (pps): 100

Type: Trunk

Management control: Enabled

PVID: 1

Allowed VLANS: all

PoE settings

PoE: Enabled

PoE schedule: Unscheduled

The following table describes the labels in this screen.

Table 70 Site-wide > Configure > Switches > Port profiles > Create/Edit port profile

LABEL	DESCRIPTION
General settings	
Profile name	Enter a name for this profile for identification purposes. Use up to 127 characters (0 – 9 a – z). The casing does not matter.
Port enabled	Select to enable or disable the port. A port must be enabled for data transmission to occur.
RSTP	Select to enable RSTP (Rapid Spanning Tree Protocol) on this profile. RSTP detects and breaks network loops and provides backup links between switches, bridges, or routers. It ensures that only one path exists between any two stations on the network.
STP guard	This field is available only when **RSTP** is enabled on this profile. Select **Root guard** to prevent the Nebula Devices attached to the ports from becoming the root bridge. Select **BPDU guard** to have the Nebula Device shut down the ports if there is any BPDU received on the ports. Otherwise, select **None**.

Table 70 Site-wide > Configure > Switches > Port profiles > Create/Edit port profile (continued)

LABEL	DESCRIPTION
Port isolation	Select to enable port isolation on the ports. The ports with port isolation enabled cannot communicate with each other. They can communicate only with the CPU management port of the same Nebula Device and the ports on which the isolation feature is disabled.
Loop guard	Select to enable loop guard on the ports. Loop guard allows you to configure the Nebula Device to shut down a port if it detects that packets sent out on that port to the edge of your network loop back to the Nebula Device. While you can use STP (Spanning Tree Protocol) to prevent loops in the core of your network, STP cannot prevent loops that occur on the edge of your network. Note: You cannot enable the loop guard feature on the ports with Spanning Tree Protocol (RSTP, MRSTP, or MSTP) enabled.
Storm control	Select to enable broadcast storm control on the ports. Storm control limits the number of broadcast, multicast, and destination lookup failure (DLF) packets the Nebula Device receives per second on the ports. When the maximum number of allowable packets per second is reached, the subsequent packets are discarded.
Broadcast Limit (pps)	Specify the maximum number of broadcast packets per second the Nebula Device accepts on the ports.
Multicast Limit (pps)	Specify the maximum number of multicast packets per second the Nebula Device accepts on the ports.
DLF Limit (pps)	Specify the maximum number of DLF packets per second the Nebula Device accepts on the ports.
Type	Set the type of the port. Select **Access** to configure the port as an access port that can carry traffic for just one VLAN. Frames received on the port are tagged with the port VLAN ID. Select **Trunk** to configure the port as a trunk port to carry traffic for multiple VLANs over a link. A trunk port always connects to a Nebula Device or router.
Management control	Select **Enabled** to configure the port as a management port. The default is **Enabled**. This allows the administrator to set the Nebula Device ports to allow the device to manage VLAN traffic. Note: Make sure to enable this for an uplink port to maintain a connection with Nebula.
PVID	A PVID (Port VLAN ID or native VLAN) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1 and 4094 as the port VLAN ID.
Allowed VLANs	This field is available only when you select **Trunk** in the **Type** field. Specify the VLANs from which the traffic comes. You can then transmit or receive traffic on the ports. See Section 3.40 on page 183 for steps in setting up dynamic VLAN with RADIUS. See Section 3.41 on page 185 for more information on monitoring dynamic VLANs using event logs.
PoE settings	
PoE	Select **Enabled** to provide power to a PD connected to the ports.

Table 70 Site-wide > Configure > Switches > Port profiles > Create/Edit port profile (continued)

LABEL	DESCRIPTION
PoE schedule	This field is available only when you enable PoE. Select a pre-defined schedule (created using the **Site-wide** > **Configure** > **Switches** > **PoE schedules** screen) to control when the Nebula Device enables PoE to provide power on the ports. Note: You must select **Unscheduled** in the **PoE schedule** field before disabling PoE on the ports. If you enable PoE and select **Unscheduled**, then PoE is always enabled on the ports. Note: The Nebula Device will follow the PoE schedule even when the Nebula Device is disconnected from NCC. Click **Edit** to go to **Site-wide** > **Configure** > **Switches** > **PoE schedules** screen to create a new PoE schedule.
Close	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

6.3.3 Cloud Stacking Mode

In Cloud Stacking mode, you can stack Nebula Devices using the NCC. You can set the Nebula Device to Cloud Stacking mode and configure the stacking settings on the NCC.

In NCC, a Nebula Device in the stacking system is referred to as a slot. For example, slot 4 refers to the fourth Nebula Device in the stacking system.

Note: When you change modes, all Nebula Device configurations, including **Running Config**, **Config1**, **Config2** and **Custom Default** configuration, are erased. User accounts will be kept after mode changing if saved to a configuration file. The Nebula Device will automatically reboot with the Cloud Stacking mode or Cloud mode factory default settings correspondingly. You have to reconfigure everything again on each Nebula Device.

6.3.3.1 From Cloud Mode to Cloud Stacking Mode

Follow the steps below to stack Nebula Devices in Cloud mode:

1 Add the Nebula Devices to your site. See Section 3.2 on page 75 for more information.

Note: Each Nebula Device must have a successful connection to the Internet. The stacking ports of the Nebula Devices must not be connected to each other.

2 Use the **Create new stacking wizard** to add the Nebula Device to a stacking system on the NCC. See Section 6.3.4.1 on page 379 for more information. The Nebula Device will then go into Cloud Stacking mode.

Note: When you change from Cloud mode to Cloud Stacking mode, the Nebula Device keeps the IP address settings (DHCP-assigned or static IP address) you set in Cloud mode.

6.3.3.2 From Cloud Stacking Mode to Cloud Mode

Follow the steps below to change from Cloud Stacking mode to Cloud mode, that is remove stacking in Cloud Stacking mode:

1. Go to **Site-wide** > **Configure** > **Switches** > **Stacking management** to remove the Nebula Device from the stack system on the NCC. See Section 6.3.4.1 on page 379 for more information.
2. Reset the Nebula Device to its factory defaults. The Nebula Device will go to Standalone mode after you reset the Nebula Device, and you will lose all configurations done in NCC.
3. Make sure the Nebula Device can access the NCC and is registered on the NCC. The Nebula Device will then go into Cloud mode.

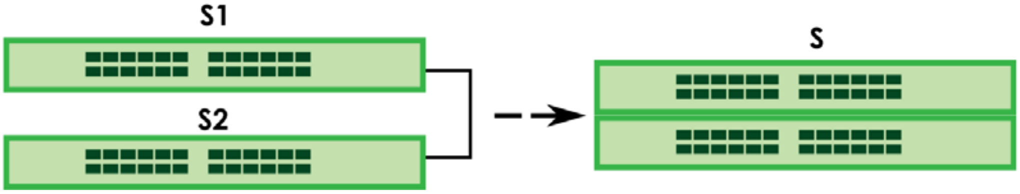
Important Notes

- Someone must be onsite to connect the stacking ports for each Nebula Device and then check the LED status. See the User's Guide for the stacking ports and LED status for each model. Follow the instructions on the wizard to connect the stacking ports on your Nebula Devices.
- The Nebula Device can only connect to other Nebula Devices of the same model and firmware version.
- NCC allows up to four Nebula Devices in a stack.
- NCC allows up to ten stacks per site.
- Each Nebula Device should have a valid Nebula Professional license.
- Each Nebula Device must belong to the same site in NCC.
- If the NCC detects any connection abnormality in your stack system, the NCC will pause the configuration process until all Nebula Devices in your stacking system are online and connected properly. You can check the stacking system status on the NCC. See Section 6.3.4.1 on page 379 for more information.
- You cannot switch from 2-Port Mode stacking to 4-Port Mode directly. You need to remove the stacking and re-create the stacking system. See Section 6.3.3.2 on page 376 for more information on removing stacking. See Section 6.3.4.2 on page 380 for more information on creating the stacking system.

6.3.4 Stacking Nebula Devices

Stacking is directly connecting Nebula Devices to form a larger system that behaves as a single Nebula Device or a virtual chassis with increased port density.

Figure 104 Switch Stacking Concept



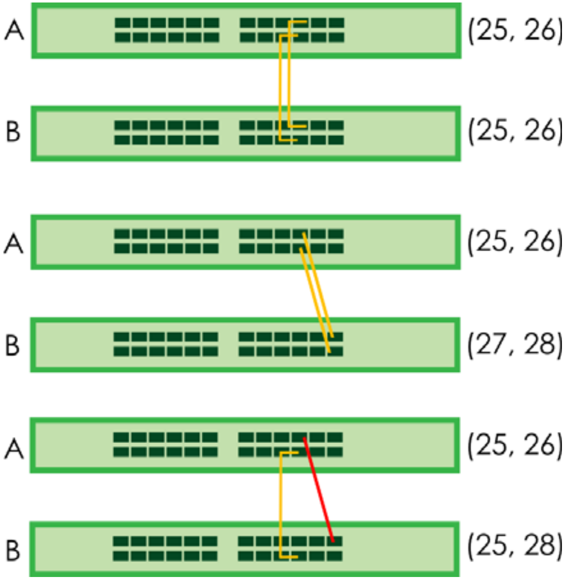
You can manage each Nebula Device in the stack from a master Nebula Device using the NCC.

Note: 'Nebula Device' refers to a Switch in the stacking system.

Each Nebula Device supports up to two stacking channels.

The Nebula Device ports of a stacking channel can only connect to the Nebula Device ports of one stacking channel on the neighboring Nebula Device. A stacking channel cannot simultaneously connect to two different stacking channels on the neighboring Nebula Device. For example, ports 25 and 26 (channel 1) on Nebula Device **A** can connect to ports 25 and 26 (channel 1) or ports 27 and 28 (channel 2) on Nebula Device **B**. You cannot connect port 26 (channel 1) on Nebula Device **A** to port 28 (channel 2) on Nebula Device **B** while connecting port 25 (channel 1) on Nebula Device **A** to port 25 (channel 1) on Nebula Device **B** at the same time.

Figure 105 Stacking Channel and Port Examples



4-Port and 2-Port Stacking Modes (XGS2220 Series)

In **4-port mode**, all four 10G stacking ports are used for stacking. Use this mode if you want to stack Nebula Devices with automatic link aggregation giving a stacking connection of 20 Gbps. The default algorithm type is src-dst-mac, and is not configurable.

In **2-port mode**, just the last two 10G stacking ports of the Nebula Device are used for stacking. Use this mode if you want to use the first two fiber ports for high-speed connections such as a fiber uplink connection and a connection to a 10G NAS. You may stack Nebula Devices without automatic link aggregation giving a stacking connection of 10 Gbps.

You must make the stacking connections as shown in the following tables.

Table 71 Stacking Channels in 2-Port Mode (XGS2220 Series)

	STACKING CHANNEL	STACKING PORT
XGS2220-30 / XGS2220-30HP / XGS2220-30F	1	29
	2	30
XGS2220-54 / XGS2220-54HP / XGS2220-54FP	1	53
	2	54

Table 72 Stacking Channels in 4-Port Mode (XGS2220 Series)

	STACKING CHANNEL	STACKING PORTS
XGS2220-30 / XGS2220-30HP / XGS2220-30F	1	27, 28
	2	29, 30
XGS2220-54 / XGS2220-54HP / XGS2220-54FP	1	51, 52
	2	53, 54

Table 73 Stacking Channels in 4-Port Mode (XS3800-28)

	STACKING CHANNEL	STACKING PORTS
XS3800-28	1	25, 26
	2	27, 28

Note: At the time of writing, XS3800-28 with firmware version ZyNOS 4.80(ABML.2) and later supports Cloud Stacking mode ('ABML' refers to the Nebula Device's model code). XGS2220 Series with firmware version ZyNOS 4.80 (patch 4) and later supports Cloud Stacking mode. See Section 6.3.3 on page 375 for more information on Cloud Stacking mode.

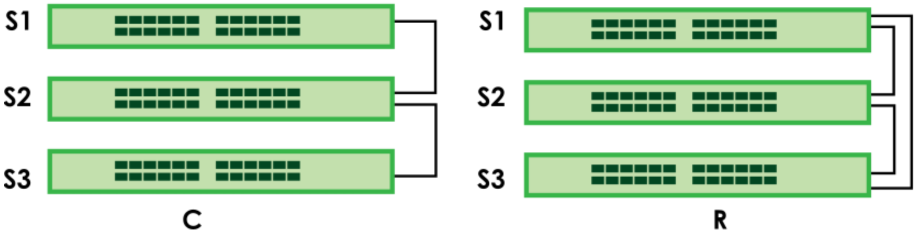
Chain Topology and Ring Topology

You can build a Nebula Device stack using a ring or chain topology.

In a chain (**C**) topology, each Nebula Device connects to the next Nebula Device with the last Nebula Device connected to the Nebula Device before it. If Nebula Device 3 fails, then only Nebula Devices 1 and 2 will still function.

In a ring (**R**) topology, each Nebula Device connects to the next Nebula Device with the last Nebula Device connected to the first. If Nebula Device 3 fails, then Nebula Devices 1, 2 and 4 will function as a chain topology.

Figure 106 Stacking Topology



Stacking will automatically choose a master Nebula Device. The Nebula Device with the longest up-time is selected. Uptime is measured in increments of 10 minutes. The Nebula Device with the higher number of increments is selected. If they have the same uptime, then the Nebula Device with the lowest MAC address will be the master.

This is the master election priority in a stack system:

1 Longest uptime

2 Lowest MAC address.

Note: Master election occurs when:

– a stacking port cable is disconnected

– a Nebula Device in the stack reboots

– you add a Nebula Device to the stack or

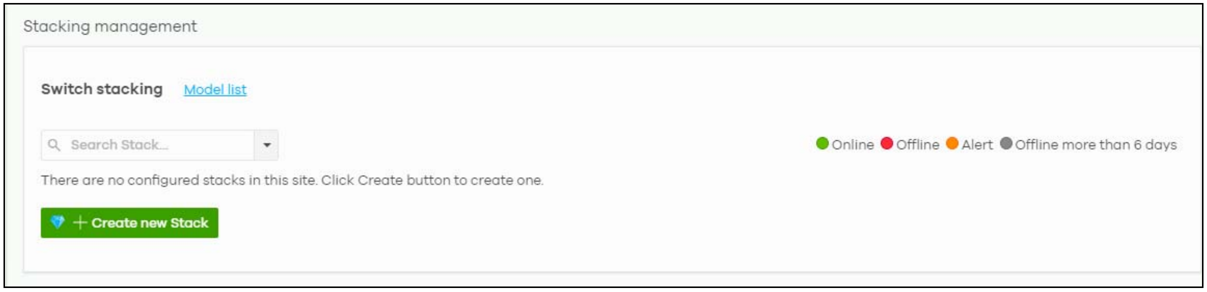
– a Nebula Device in the stack shuts down.

6.3.4.1 Stacking management

Use this screen to create a stack, configure the stack settings, and view the stack status of Nebula Devices on the NCC.

Click **Site-wide** > **Configure** > **Switches** > **Stacking management** to access this screen.

Figure 107 Site-wide > Configure > Switches > Stacking management



Stacking management

Switch stacking Model list

Search Stack...

● Online ● Offline ● Alert ● Offline more than 6 days

There are no configured stacks in this site. Click Create button to create one.

The following table describes the labels in this screen.

Table 74 Site-wide > Configure > Switches > Stacking management

LABEL	DESCRIPTION
Stack status/Name/ Members	Use this field to display the stacking system configured in NCC using criteria such as Stack status/Name/Members. Note: This field is blank if there is no stacking configured on the NCC.
Note: The following fields will appear after you create at least one stacking system.	

Table 74 Site-wide > Configure > Switches > Stacking management (continued)

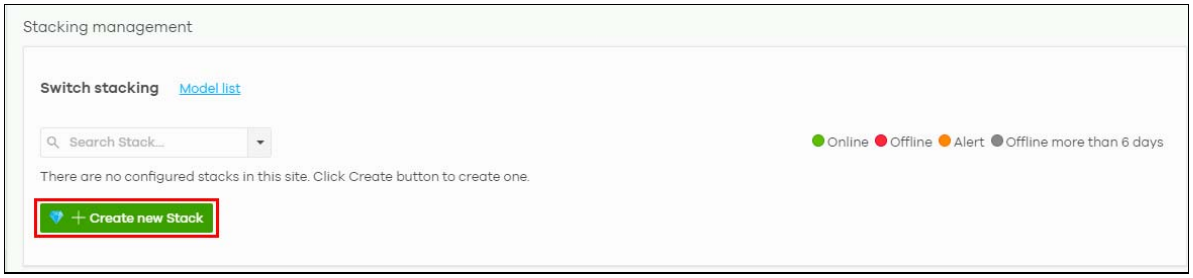
LABEL	DESCRIPTION
Status	This shows the status of the stacking system. • Green – all the Nebula Devices in the stacking system are online and the stack is configured correctly. • Green with lock icon – NCC has locked the stack system because it lacks provisioning. NCC needs to apply the site-wide port settings to all Nebula Devices in the stacking system (provisioning). To unlock, click the **Provision** button. See Section 6.3.4.2 on page 380 for more information. • Orange with lock icon – NCC has locked the stacking system because of one of the following reasons: One or more Nebula Devices are offline. Make sure all the stacking ports of the Nebula Devices are connected, the power is on, and one Nebula Device is connected to the Internet. You removed a Nebula Device from the stacking system in NCC but did not disconnect the onsite stacking cable. Disconnect the stacking cable. NCC has detected that the onsite Nebula Device's cable connection does not match the **Slot ID** configuration in NCC. • Red – the stacking system is offline. Make sure a Nebula Device has Internet connection. • Gray – the stacking system is offline for more than six days.
Name	This shows the NCC-assigned name of the stacking system. To change, click the **Name** to go to the **Slot management** screen. Click the **Name** on any Nebula Device to go to the **Site-wide** > **Devices** > **Switches** detail screen. See Section 4.3.2 on page 227 for more information.
Model	This shows the model type of the Nebula Device in the stacking system.
Configuration status	This shows **Up to date** when NCC has finished applying the site-wide settings to the stacking Nebula Device. Otherwise, it shows **Not up to date**.
Current version	This shows the ZyNOS firmware that is currently running on the Nebula Devices in the stacking system.
Slot	This shows the Nebula Device's name in the stacking system.
Stacking mode	This shows the number of stacking ports. **2-port** means the last 2 SFP+ slots are dedicated for Nebula Device stacking. **4-port** means the last 4 SFP+ slots are dedicated for Nebula Device stacking. Note: At the time of writing, only XGS2220 Series with firmware version ZyNOS 4.80 (patch 4) and later support **2-port / 4-port Stacking mode**.
Media type	This shows the media type (**SFP+** or **DAC**) of the SFP+ module that is attached to the 10 Gigabit interface.
Delete	Click this when you want to remove the stacking system on the NCC. The Nebula Devices will appear as individual devices in NCC. Reset the Nebula Devices to factory-default settings so that the Nebula Devices will not appear offline in NCC. Follow the steps in Section 6.3.3.2 on page 376 to change from Cloud Stacking mode to Cloud mode.
Create new Stack	Click this button to run the **Create a new Stacking wizard**. See the next section for more information.

6.3.4.2 Create a New Stacking System Wizard

The wizard helps you create a stacking system quickly.

Step1: Run the Wizard

Go to **Site-wide** > **Configure** > **Switches** > **Stacking management** and click **Create new Stack**.



Stacking management

Switch stacking Model list

Search Stack...

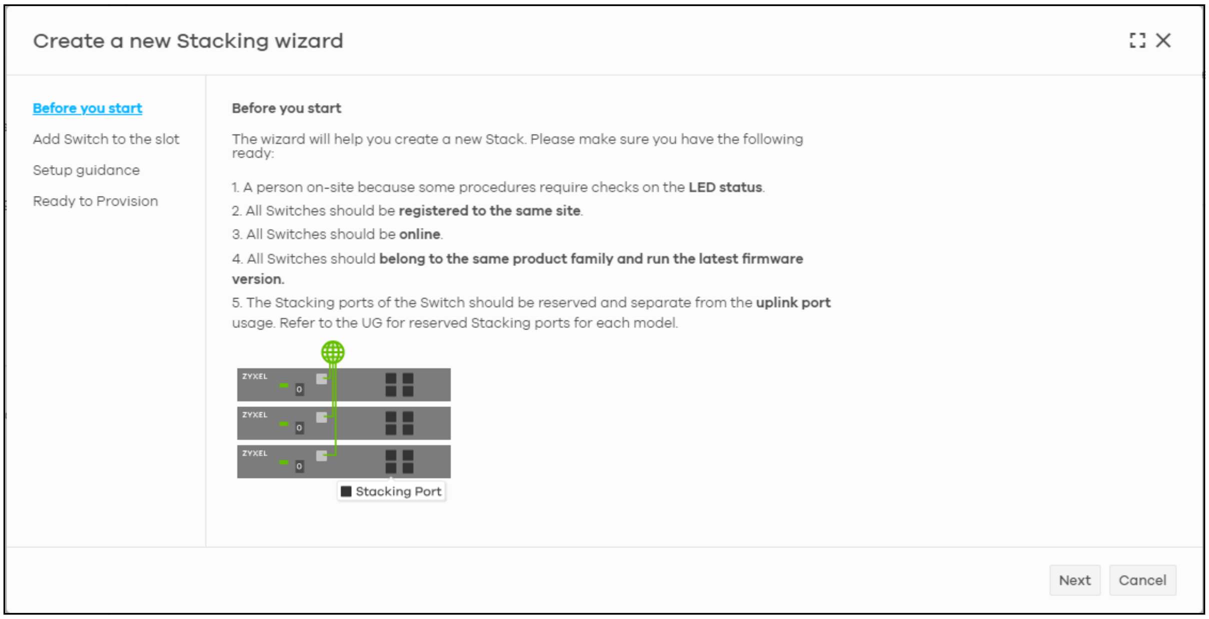
● Online ● Offline ● Alert ● Offline more than 6 days

There are no configured stacks in this site. Click Create button to create one.

Step2: Before you start

Make sure to do the steps listed on the screen. Then click **Next**.

Note: Someone must be onsite to connect the stacking ports for each Nebula Device and then check the LED status. Make sure that you do not make the stacking port connections yet.



Create a new Stacking wizard

Before you start

The wizard will help you create a new Stack. Please make sure you have the following ready:

1. A person on-site because some procedures require checks on the **LED status**.
2. All Switches should be **registered to the same site**.
3. All Switches should be **online**.
4. All Switches should **belong to the same product family and run the latest firmware version.**
5. The Stacking ports of the Switch should be reserved and separate from the **uplink port** usage. Refer to the UG for reserved Stacking ports for each model.

Step3: Add slot

1 Click **+Add** (**1**) and then select the first Nebula Device in the **Name** field (**2**) to add to the stacking system. Click **+Add** (**1**) and then select the second Nebula Device in the **Name** field (**2**) to add to the stacking system.

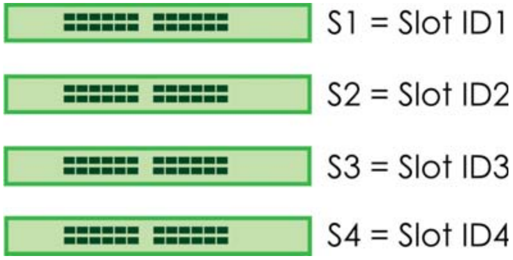
Note: The **Slot ID** is assigned based on the order the Nebula Device is added. The first Nebula Device (**S1**) added to the stacking system had **Slot ID 1**.

2 Select the media type (**SFP+** or **DAC**) (**3**) of the SFP+ module to attach to the stacking port.

3 Select the number of stacking ports (**2-ports** or **4-ports**) (**4**).

Note: At the time of writing, this field is only available for the XGS2220 Series. This field is not configurable for the XS3800-28, **4-ports** stacking mode.

Figure 108 Slot ID Sequence



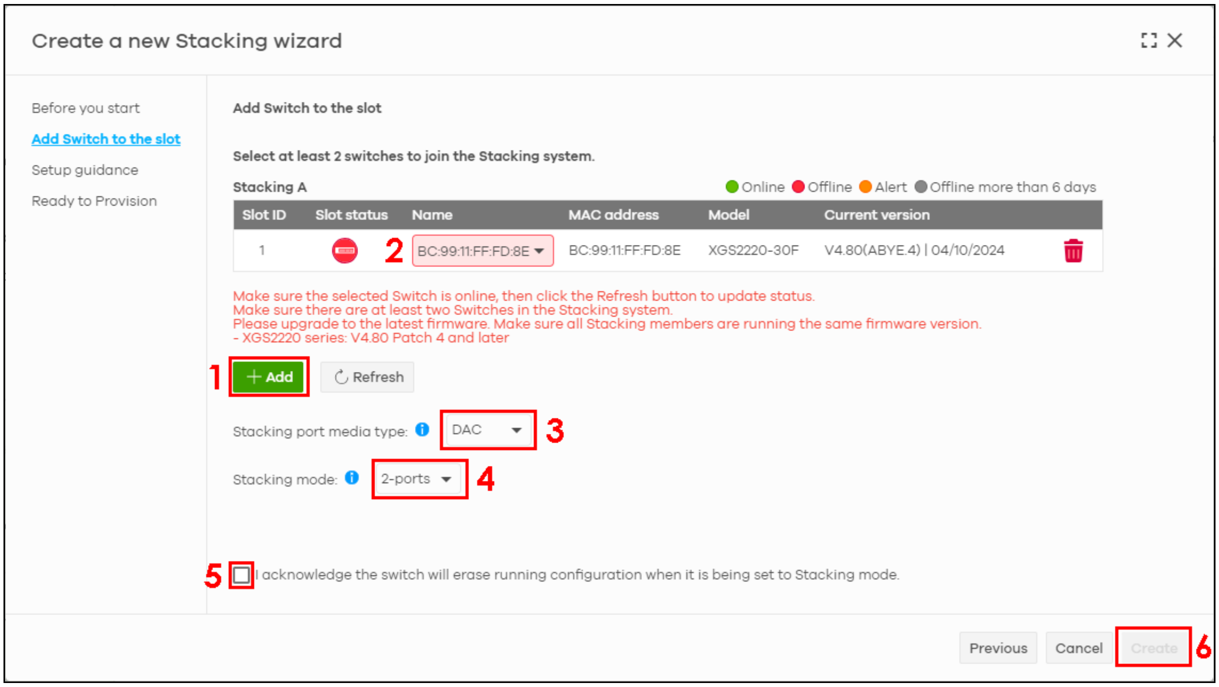
Note: Click **Refresh** to have NCC update the status of the Nebula Device(s), for example, from offline to online.

4 Click the **I acknowledge the Switch will erase running configuration when it is set to Stacking mode** checkbox (**5**). This means that you will lose all configurations made in NCC for each Nebula Device. You cannot back up the configurations in NCC first.

5 Then click **Create** (6). The Nebula Devices will automatically reboot to Cloud Stacking mode. NCC will assign the **Slot ID** to each Nebula Device.

Note: The **Create** button is enabled when:

- There are at least two online Nebula Devices in the stacking system
- The 'erase running configuration' confirmation box is selected.



Add Switch to the slot

Select at least 2 switches to join the Stacking system.

Stacking A

● Online ● Offline ● Alert ● Offline more than 6 days

Slot ID	Slot status	Name	MAC address	Model	Current version
1	●	BC:99:11:FF:FD:8E	BC:99:11:FF:FD:8E	XGS2220-30F	V4.80(ABYE.4) | 04/10/2024

Make sure the selected Switch is online, then click the Refresh button to update status.
Make sure there are at least two Switches in the Stacking system.
Please upgrade to the latest firmware. Make sure all Stacking members are running the same firmware version.
- XGS2220 series: V4.80 Patch 4 and later

Stacking port media type: DAC

Stacking mode: 2-ports

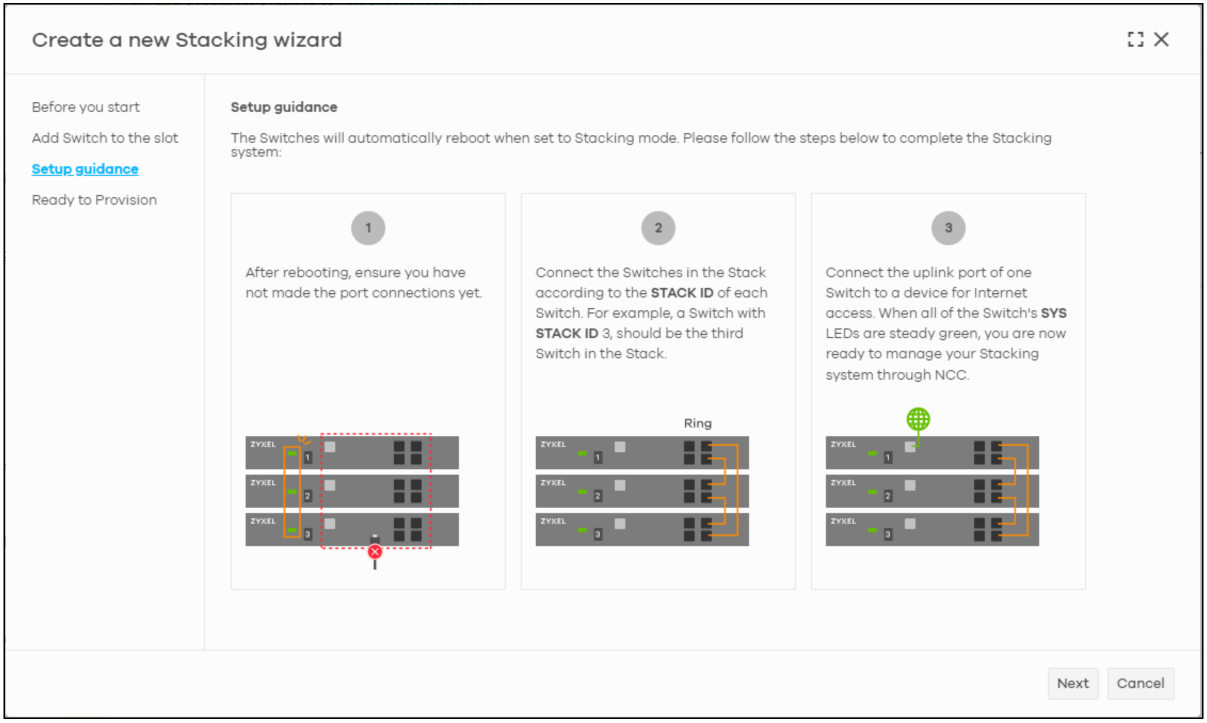
□ I acknowledge the switch will erase running configuration when it is being set to Stacking mode.

Step4: Setup guidance (onsite hardware connections)

1 Perform the hardware connections onsite. See Section 6.3.4.3 on page 385 for the steps.

2 Then click **Next**.

Figure 109 Setup Guidance (2-Port Mode)



Create a new Stacking wizard

Setup guidance

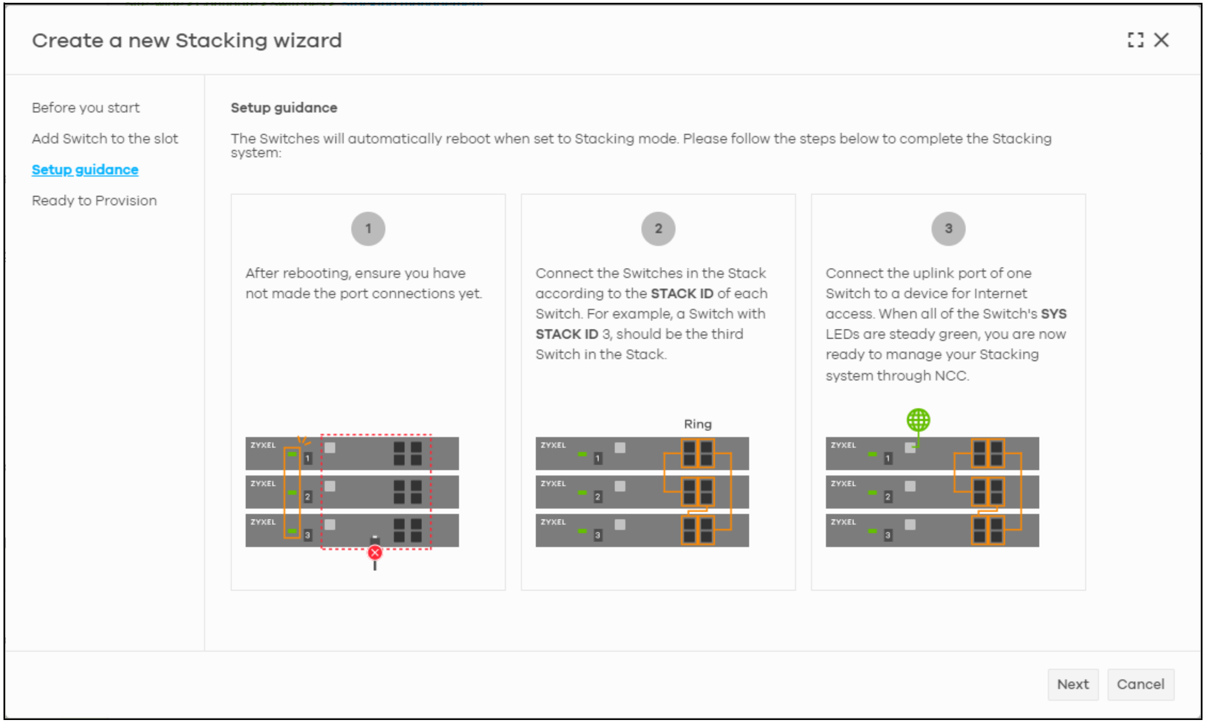
The Switches will automatically reboot when set to Stacking mode. Please follow the steps below to complete the Stacking system:

1 After rebooting, ensure you have not made the port connections yet.

2 Connect the Switches in the Stack according to the **STACK ID** of each Switch. For example, a Switch with **STACK ID** 3, should be the third Switch in the Stack.

3 Connect the uplink port of one Switch to a device for Internet access. When all of the Switch's **SYS** LEDs are steady green, you are now ready to manage your Stacking system through NCC.

Figure 110 Setup Guidance (4-Port Mode)



Create a new Stacking wizard

Setup guidance

The Switches will automatically reboot when set to Stacking mode. Please follow the steps below to complete the Stacking system:

1 After rebooting, ensure you have not made the port connections yet.

2 Connect the Switches in the Stack according to the **STACK ID** of each Switch. For example, a Switch with **STACK ID** 3, should be the third Switch in the Stack.

3 Connect the uplink port of one Switch to a device for Internet access. When all of the Switch's **SYS** LEDs are steady green, you are now ready to manage your Stacking system through NCC.

Step5: Ready to Provision

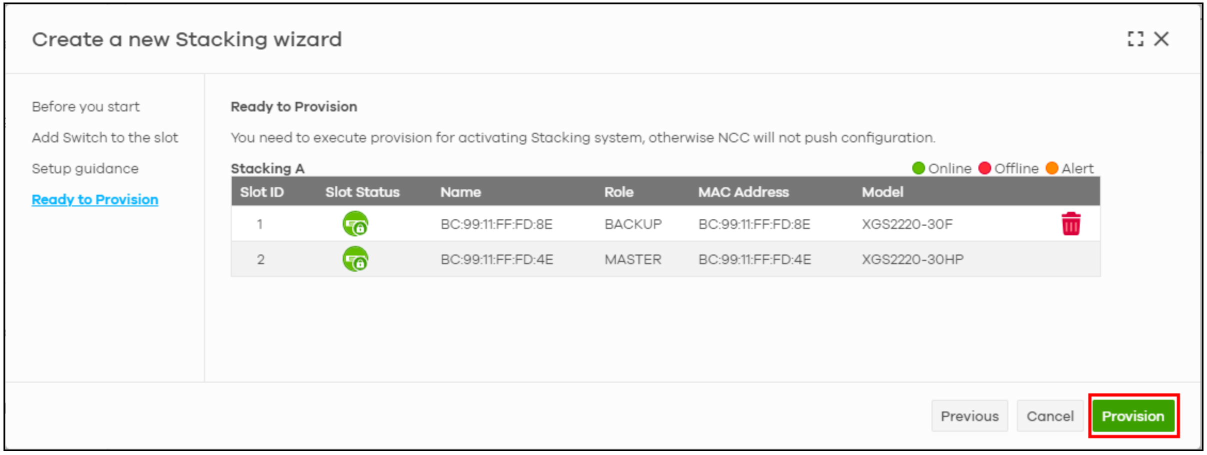
NCC must apply the site-wide port settings to all Nebula Devices in the stack. The **Slot Status** of the stacking Nebula Device appear green in the following screen when:

- All the Nebula Devices in the stacking system are online
- The Nebula Device connection order matches the **Slot ID** configuration in NCC.

Note: See Table 74 on page 379 for the **Slot Status** LED description.

Click **Provision** to apply the site-wide port settings and exit the wizard.

Figure 111 Ready to Provision



Create a new Stacking wizard

Before you start
Add Switch to the slot
Setup guidance
Ready to Provision

Ready to Provision

You need to execute provision for activating Stacking system, otherwise NCC will not push configuration.

Stacking A 🟢 Online 🔴 Offline 🟠 Alert

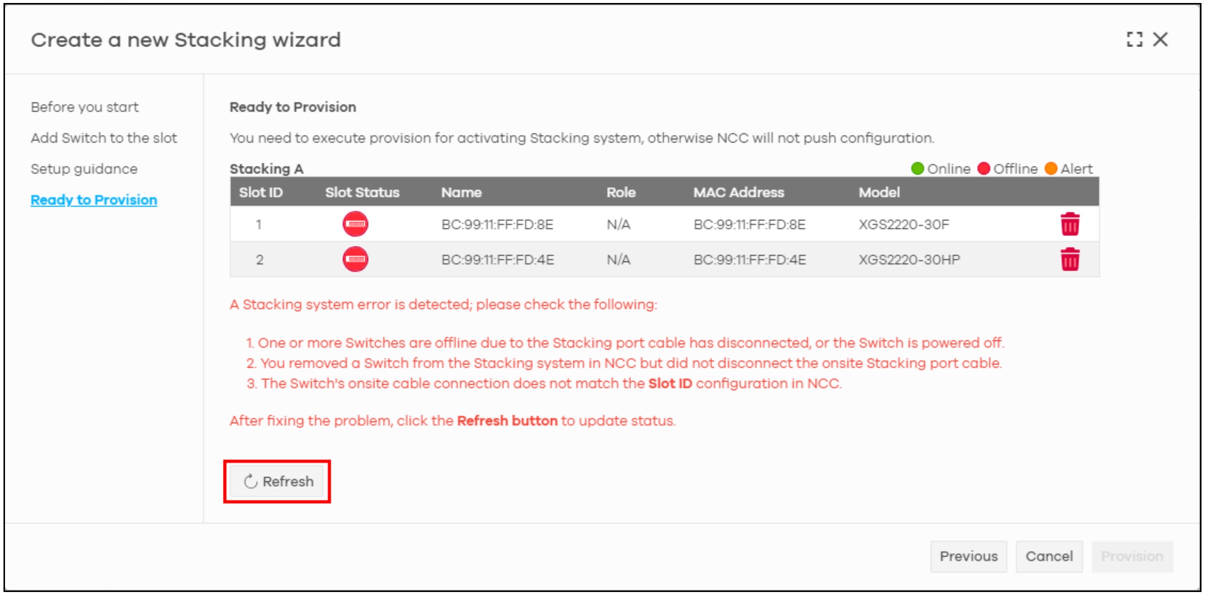
Slot ID	Slot Status	Name	Role	MAC Address	Model	
1	🟢	BC:99:11:FF:FD:8E	BACKUP	BC:99:11:FF:FD:8E	XGS2220-30F	🗑
2	🟢	BC:99:11:FF:FD:4E	MASTER	BC:99:11:FF:FD:4E	XGS2220-30HP	

The following screen appears when:

- One or more Nebula Devices in the stacking system are offline
- You remove a Nebula Device from the stacking system in NCC, but did not disconnect the onsite stacking port cable
- The Nebula Device's onsite cable connection does not match the **Slot ID** configuration in NCC.

After fixing the problem, click **Refresh** to have NCC update the stacking status. Click **Provision** when each stacking Nebula Device's **Slot Status** shows green with lock icon.

Figure 112 Not Ready to Provision



Create a new Stacking wizard

Before you start
Add Switch to the slot
Setup guidance
Ready to Provision

Ready to Provision

You need to execute provision for activating Stacking system, otherwise NCC will not push configuration.

Stacking A 🟢 Online 🔴 Offline 🟠 Alert

Slot ID	Slot Status	Name	Role	MAC Address	Model	
1	🔴	BC:99:11:FF:FD:8E	N/A	BC:99:11:FF:FD:8E	XGS2220-30F	🗑
2	🔴	BC:99:11:FF:FD:4E	N/A	BC:99:11:FF:FD:4E	XGS2220-30HP	🗑

A Stacking system error is detected; please check the following:

1. One or more Switches are offline due to the Stacking port cable has disconnected, or the Switch is powered off.
2. You removed a Switch from the Stacking system in NCC but did not disconnect the onsite Stacking port cable.
3. The Switch's onsite cable connection does not match the **Slot ID** configuration in NCC.

After fixing the problem, click the **Refresh button** to update status.

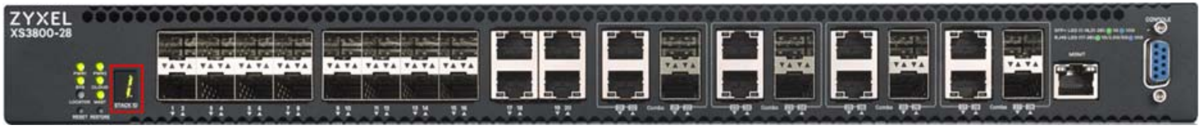
6.3.4.3 Hardware Connections (for Stacking)

Do the following steps onsite:

1 Remove all Ethernet cable connections from all ports on all the Nebula Devices that are going to be in the stacking system.

2 Check the **STACK ID** LED on each Nebula Device to find the Slot ID. Position the Nebula Devices accordingly.

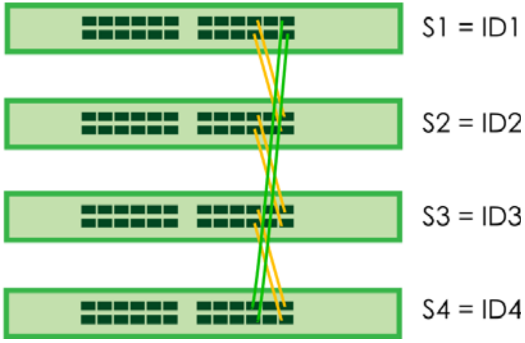
Figure 113 Nebula Device STACK ID LED



3 Connect the stacking cables to the stacking ports. See the example figure below.

- Ports 25 and 26 (channel 1) on Slot ID 1 (**S1**) connects to ports 27 and 28 (channel 2) on Slot ID 2 (**S2**).
- Ports 25 and 26 (channel 1) on Slot ID 2 (**S2**) connects to ports 27 and 28 (channel 2) on Slot ID 3 (**S3**).
- Ports 25 and 26 (channel 1) on Slot ID 3 (**S3**) connects to ports 27 and 28 (channel 2) on Slot ID 4 (**S4**).
- Ports 25 and 26 (channel 1) on Slot ID 4 (**S4**) connects to ports 27 and 28 (channel 2) on Slot ID 1 (**S1**).

Figure 114 Onsite Stacking Cable Connection: Ring Topology



4 Connect one Nebula Device’s uplink Ethernet port only to the Internet for the stacking system.

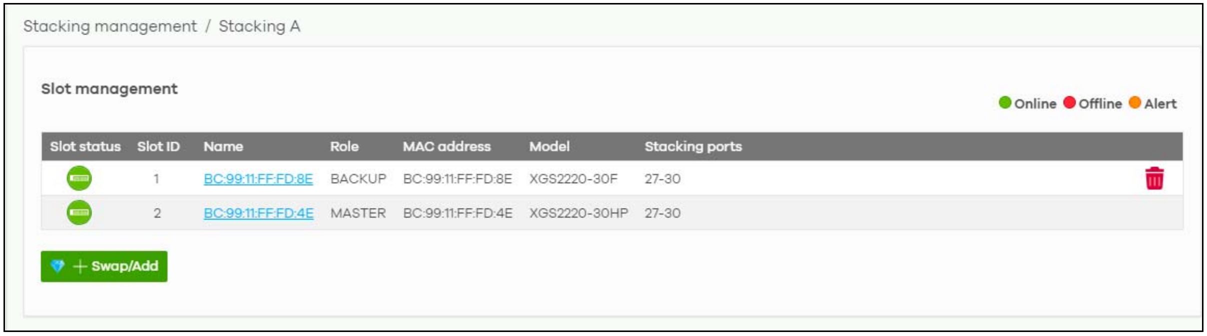
Note: A stacking port cannot be the uplink port.

5 Wait until all the Nebula Device’s **SYS** LED are steady green. You are now ready to manage your stacking system through NCC.

6.3.4.4 Slot Management

Use this screen to add, remove, or swap Nebula Devices in a stacking system. Click **Site-wide** > **Configure** > **Switches** > **Stacking management**, then click the name of the stacking system to access this screen.

Figure 115 Site-wide > Configure > Switches > Stacking management: Slot management



Stacking management / Stacking A

Slot management

● Online ● Offline ● Alert

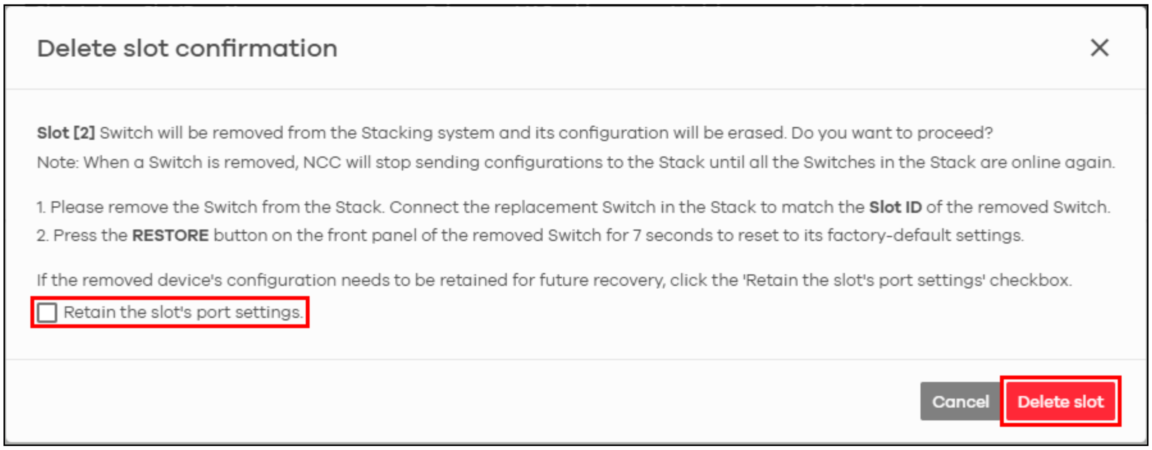
Slot status	Slot ID	Name	Role	MAC address	Model	Stacking ports	
●	1	BC:99:11:FF:FD:8E	BACKUP	BC:99:11:FF:FD:8E	XGS2220-30F	27-30	🗑
●	2	BC:99:11:FF:FD:4E	MASTER	BC:99:11:FF:FD:4E	XGS2220-30HP	27-30	

Remove a non-Master Nebula Device

To remove a Nebula Device except the master in a stacking system, do the following:

1 Select the Nebula Device you want to remove. Then click the delete icon on the right.

2 The following pop-up window appears. Select **Retain the slot's port setting** if you want to apply the setting to the new Nebula Device. Then, click **Delete slot**.



Delete slot confirmation

Slot [2] Switch will be removed from the Stacking system and its configuration will be erased. Do you want to proceed?

Note: When a Switch is removed, NCC will stop sending configurations to the Stack until all the Switches in the Stack are online again.

1. Please remove the Switch from the Stack. Connect the replacement Switch in the Stack to match the **Slot ID** of the removed Switch.
2. Press the **RESTORE** button on the front panel of the removed Switch for 7 seconds to reset to its factory-default settings.

If the removed device's configuration needs to be retained for future recovery, click the 'Retain the slot's port settings' checkbox.

□ Retain the slot's port settings.

Note: To apply the slot's port setting to another Nebula Device, make sure the Nebula Device is the same model and firmware version.

3 Disconnect the stacking cable on the Nebula Device onsite.

4 Press the **RESTORE** button on the front panel of the Nebula Device for more than 7 seconds to reset to the factory-default settings.

Remove a Master Nebula Device

To remove a master Nebula Device in a stacking system, do the following:

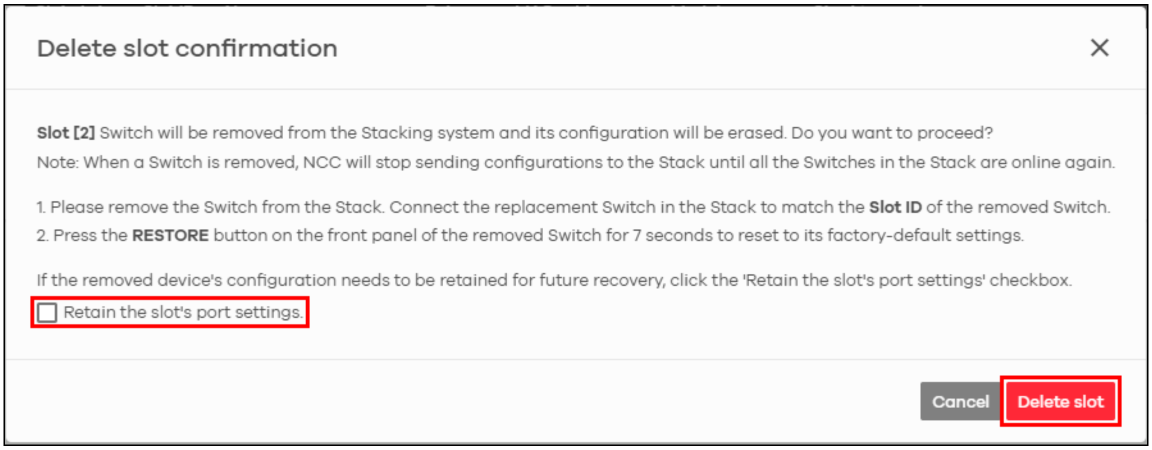
1 Disconnect the stacking cable to the master Nebula Device and reconnect. NCC will elect a new master Nebula Device for the stacking system. You can now remove the old master Nebula Device.

Note: To ensure continuity of the stacking system's management MAC address, the new master Nebula Device will inherit the old master Nebula Device's MAC address.

This is the MAC address that will display in the **Site-wide** > **Topology**, **Site-wide** > **Clients** > **Client list**, and **Site-wide** > **Devices** > **Switches**: **Switch Details** screens.

2 On the Nebula Device you want to remove, click the delete icon on the right.

3 The following pop-up window appears. Select **Retain the slot's port setting** if you want to apply the setting to the new Nebula Device. Then, click **Delete slot**.



Delete slot confirmation

Slot [2] Switch will be removed from the Stacking system and its configuration will be erased. Do you want to proceed?

Note: When a Switch is removed, NCC will stop sending configurations to the Stack until all the Switches in the Stack are online again.

1. Please remove the Switch from the Stack. Connect the replacement Switch in the Stack to match the **Slot ID** of the removed Switch.
2. Press the **RESTORE** button on the front panel of the removed Switch for 7 seconds to reset to its factory-default settings.

If the removed device's configuration needs to be retained for future recovery, click the 'Retain the slot's port settings' checkbox.

☐ Retain the slot's port settings.

Note: To apply the slot's port setting to another Nebula Device, make sure the Nebula Device is the same model and firmware version.

4 Disconnect the stacking cable on the Nebula Device onsite.

5 Press the **RESTORE** button on the front panel of the Nebula Device for more than 7 seconds to reset to the factory-default settings.

Add a Nebula Device

To add a Nebula Device to the stacking system, do the following:

1 Click **+ Swap/Add**, see Figure 115 on page 386.

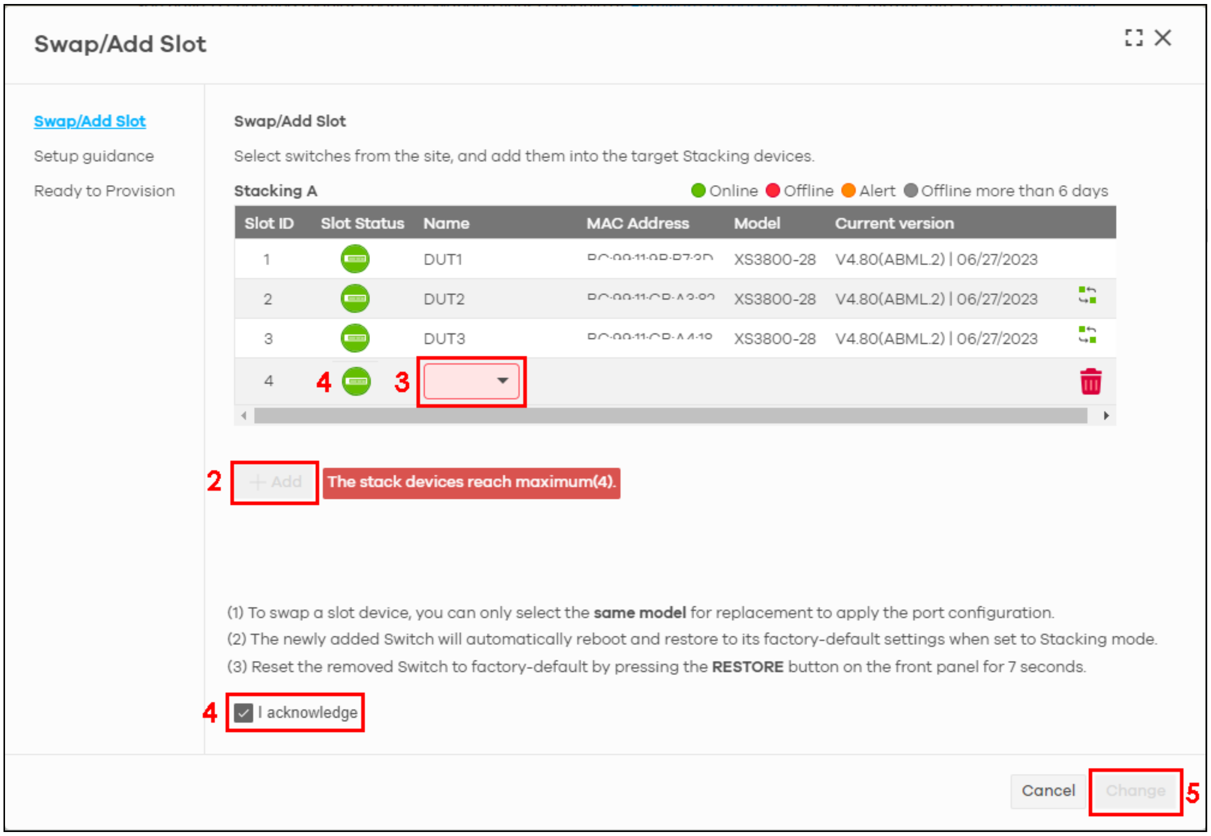
2 On the **Swap/Add Slot** screen, click **+ Add** to add another Nebula Device to the stacking system.

3 In the **Name** field, select the Nebula Device in your site to add to the stacking system.

4 When the **Slot Status** of the new Nebula Device is green, click **I acknowledge**.

Note: The **Slot Status** will show red when the Nebula Device is offline.

5 Click **Change**. The Nebula Device will automatically reboot to Cloud Stacking mode. NCC will assign the new **Slot ID** to the Nebula Device, see the **STACK ID** LED of the Nebula Device.



Swap/Add Slot

Swap/Add Slot

Select switches from the site, and add them into the target Stacking devices.

Stacking A

● Online ● Offline ● Alert ● Offline more than 6 days

Slot ID	Slot Status	Name	MAC Address	Model	Current version
1	●	DUT1	BC:99:11:9B:B7:3D	XS3800-28	V4.80(ABML.2) | 06/27/2023
2	●	DUT2	BC:99:11:CB:A3:92	XS3800-28	V4.80(ABML.2) | 06/27/2023
3	●	DUT3	BC:99:11:CB:A4:18	XS3800-28	V4.80(ABML.2) | 06/27/2023
4	●				

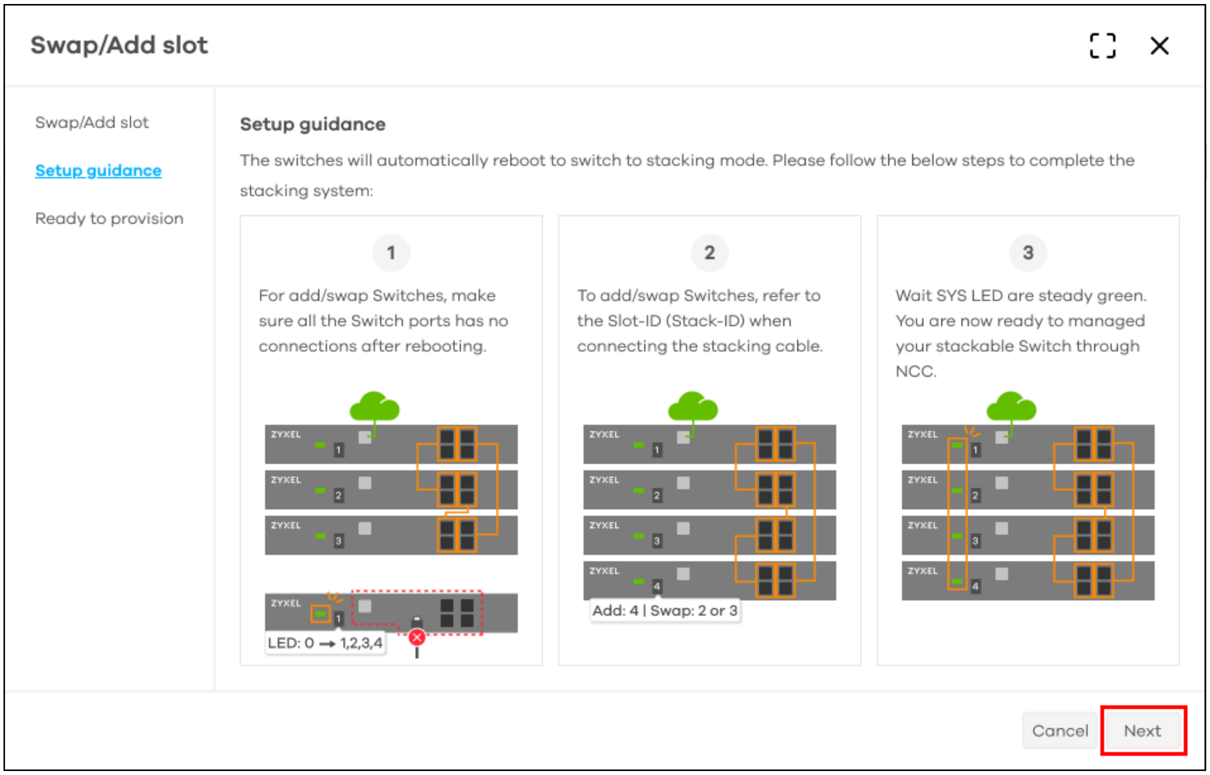
The stack devices reach maximum(4).

(1) To swap a slot device, you can only select the **same model** for replacement to apply the port configuration.
(2) The newly added Switch will automatically reboot and restore to its factory-default settings when set to Stacking mode.
(3) Reset the removed Switch to factory-default by pressing the **RESTORE** button on the front panel for 7 seconds.

☑ I acknowledge

6 Update the stacking cable connection onsite. See Section 6.3.4.3 on page 385 for the steps.

7 Then click **Next**.



Swap/Add slot

Swap/Add slot

Setup guidance

Ready to provision

Setup guidance

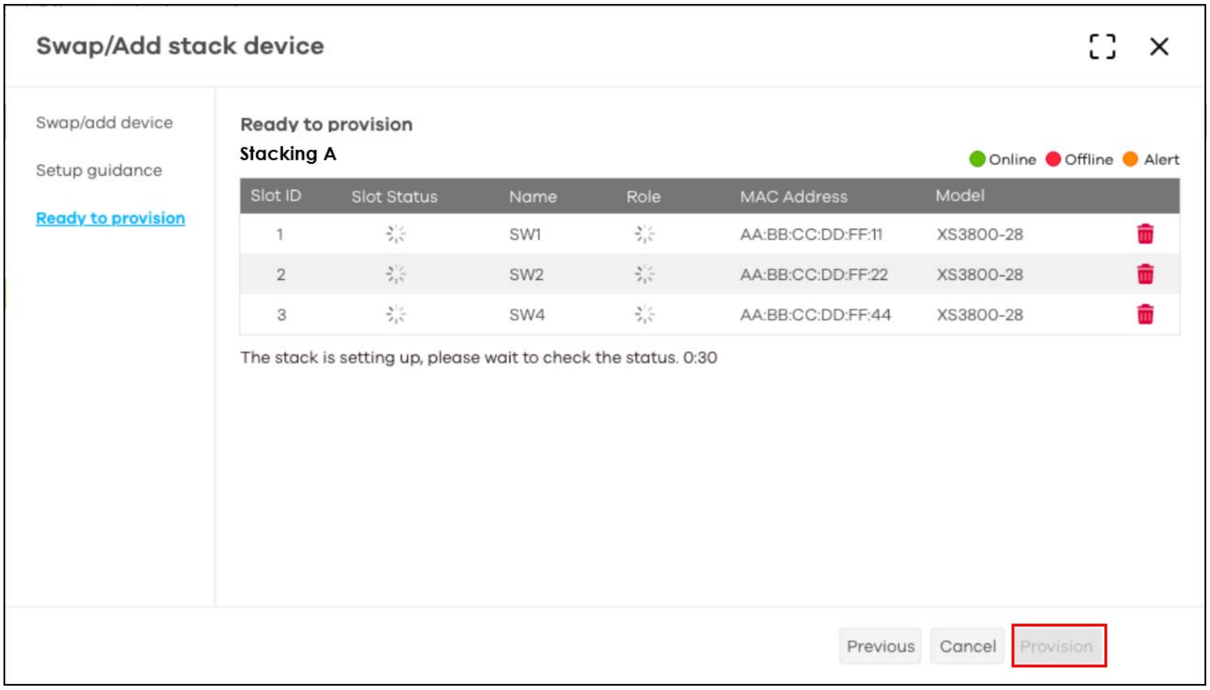
The switches will automatically reboot to switch to stacking mode. Please follow the below steps to complete the stacking system:

1 For add/swap Switches, make sure all the Switch ports has no connections after rebooting.

2 To add/swap Switches, refer to the Slot-ID (Stack-ID) when connecting the stacking cable.

3 Wait SYS LED are steady green. You are now ready to managed your stackable Switch through NCC.

8 Click **Provision** to apply the site-wide port settings to the new Nebula Device and exit the wizard.



Swap/Add stack device

Swap/add device

Setup guidance

Ready to provision

Ready to provision

Stacking A

● Online ● Offline ● Alert

Slot ID	Slot Status	Name	Role	MAC Address	Model	
1		SW1		AA:BB:CC:DD:FF:11	XS3800-28	🗑
2		SW2		AA:BB:CC:DD:FF:22	XS3800-28	🗑
3		SW4		AA:BB:CC:DD:FF:44	XS3800-28	🗑

The stack is setting up, please wait to check the status. 0:30

Note: If the new Nebula Device is the same model and firmware version, NCC will automatically restore the configurations to the new Nebula Device. Otherwise, the Nebula Device will restore to its factory-default settings to prevent mis-configurations in NCC. You need to reconfigure the port settings in NCC.

Note: The **Provision** button may be disabled (gray-out) when:

– One or more Nebula Devices in the stacking system are offline

– The Nebula Device's order of connection do not match the **Slot ID** configuration in NCC.

After fixing the problem, click **Reload** to update the stacking status. Then click **Provision** when all the stacking Nebula Device's **Slot Status** shows green with lock icon.

Swap a Nebula Device

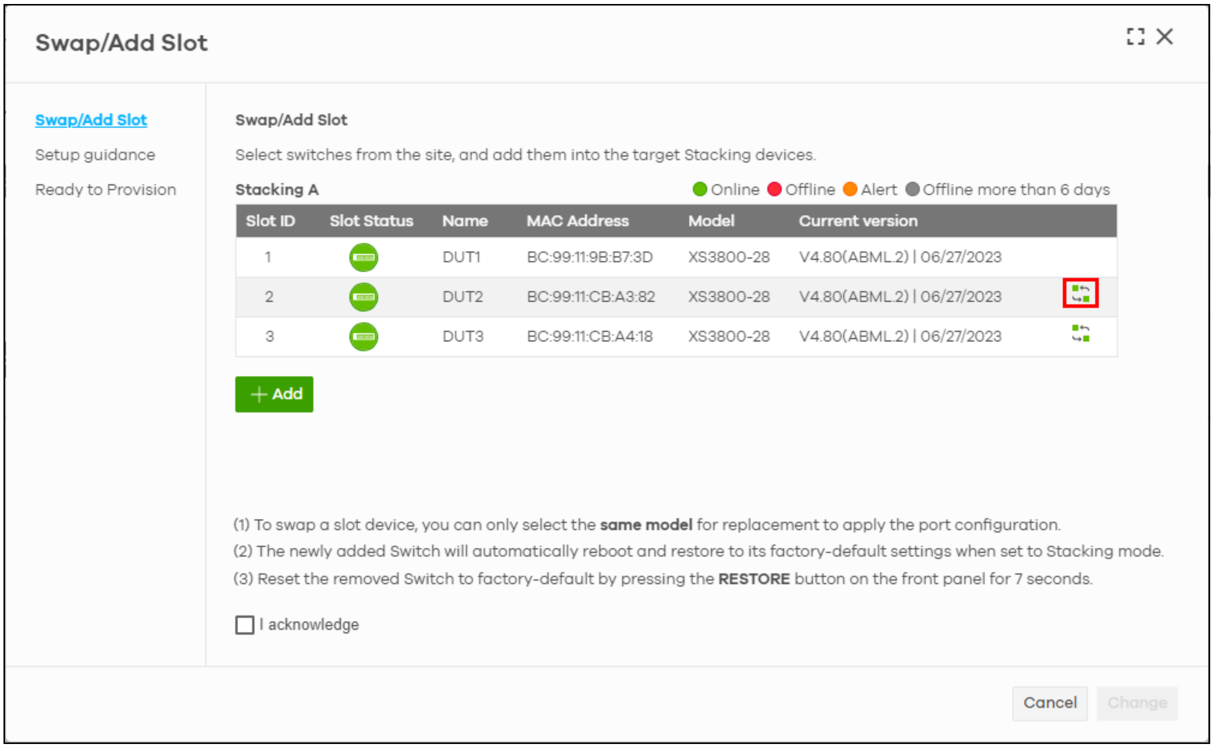
Note: To replace a faulty Nebula Device in a stacking system and keep the configurations, do NOT remove or swap the Nebula Device. See I need to replace a defective Nebula Device on my stacking system. I want to keep the NCC configurations. for more information.

Note: If the new Nebula Device is the same model and firmware version, NCC will automatically restore the configurations to the new Nebula Device. Use the swap icon to replace the Nebula Device, see step 2.
Otherwise, after replacing a new Nebula Device on a stacking system, the Nebula Device will restore to its factory-default settings to prevent mis-configurations in NCC. You need to reconfigure the port settings in NCC.

To swap a Nebula Device in the stacking system, do the following:

1 Click **+ Swap/Add**, see Figure 115 on page 386.

2 On the **Swap/Add Slot** screen, select the Nebula Device you want to swap and click the swap icon.



Swap/Add Slot

Swap/Add Slot

Select switches from the site, and add them into the target Stacking devices.

Stacking A

● Online ● Offline ● Alert ● Offline more than 6 days

Slot ID	Slot Status	Name	MAC Address	Model	Current version	
1	●	DUT1	BC:99:11:9B:B7:3D	XS3800-28	V4.80(ABML.2) | 06/27/2023	
2	●	DUT2	BC:99:11:CB:A3:82	XS3800-28	V4.80(ABML.2) | 06/27/2023	⇄
3	●	DUT3	BC:99:11:CB:A4:18	XS3800-28	V4.80(ABML.2) | 06/27/2023	⇄

(1) To swap a slot device, you can only select the **same model** for replacement to apply the port configuration.
(2) The newly added Switch will automatically reboot and restore to its factory-default settings when set to Stacking mode.
(3) Reset the removed Switch to factory-default by pressing the **RESTORE** button on the front panel for 7 seconds.

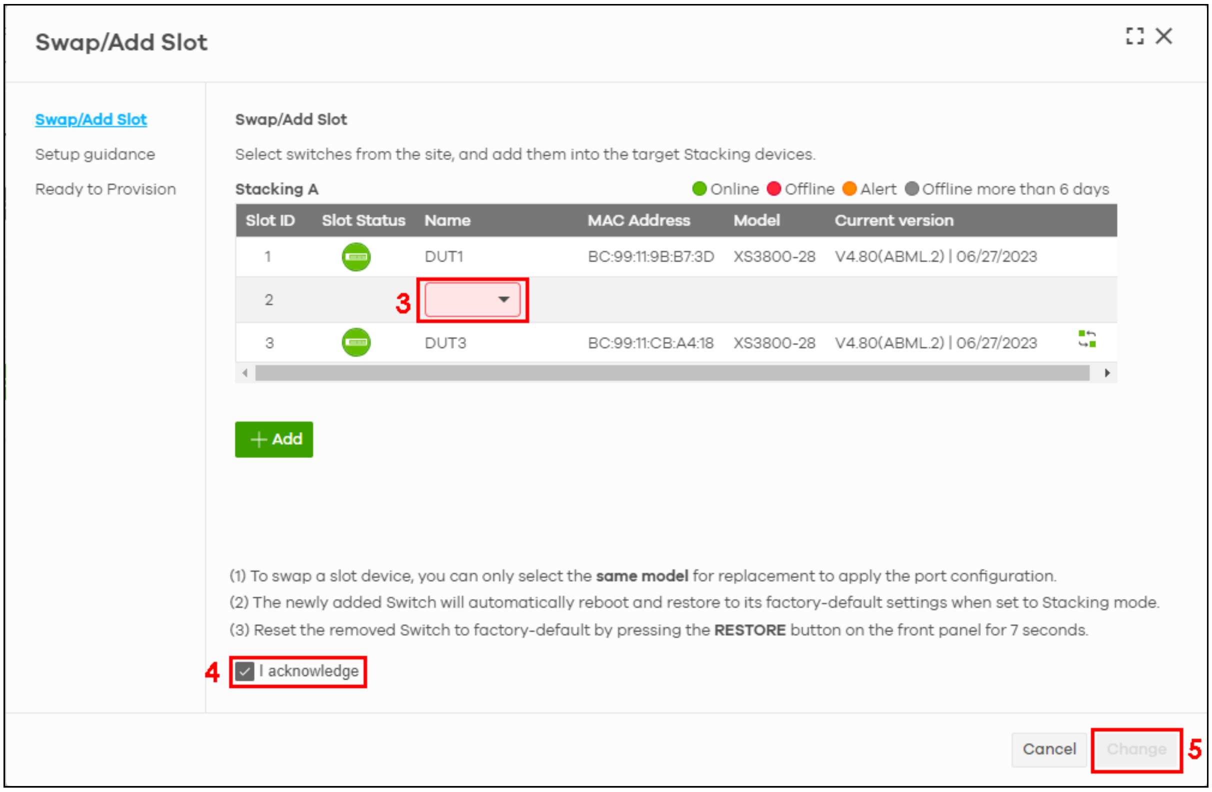
☐ I acknowledge

3 In the **Name** field, select the Nebula Device in your site to swap in the stacking system.

4 When the **Slot Status** of the new Nebula Device is green, click **I acknowledge**.

5 Click **Change**. The new Nebula Device will automatically reboot to Cloud Stacking mode. NCC will assign the previous **Slot ID** to the new Nebula Device, see the **STACK ID** LED on the front panel.

Note: The new Nebula Device will inherit the configuration of the old Nebula Device when both models are the same. For example, replace XGS2220-30F with another XGS2220-30F.



Swap/Add Slot

Swap/Add Slot

Setup guidance

Ready to Provision

Swap/Add Slot

Select switches from the site, and add them into the target Stacking devices.

Stacking A ● Online ● Offline ● Alert ● Offline more than 6 days

Slot ID	Slot Status	Name	MAC Address	Model	Current version
1	●	DUT1	BC:99:11:9B:B7:3D	XS3800-28	V4.80(ABML.2) | 06/27/2023
2		▾			
3	●	DUT3	BC:99:11:CB:A4:18	XS3800-28	V4.80(ABML.2) | 06/27/2023

+ Add

(1) To swap a slot device, you can only select the **same model** for replacement to apply the port configuration.

(2) The newly added Switch will automatically reboot and restore to its factory-default settings when set to Stacking mode.

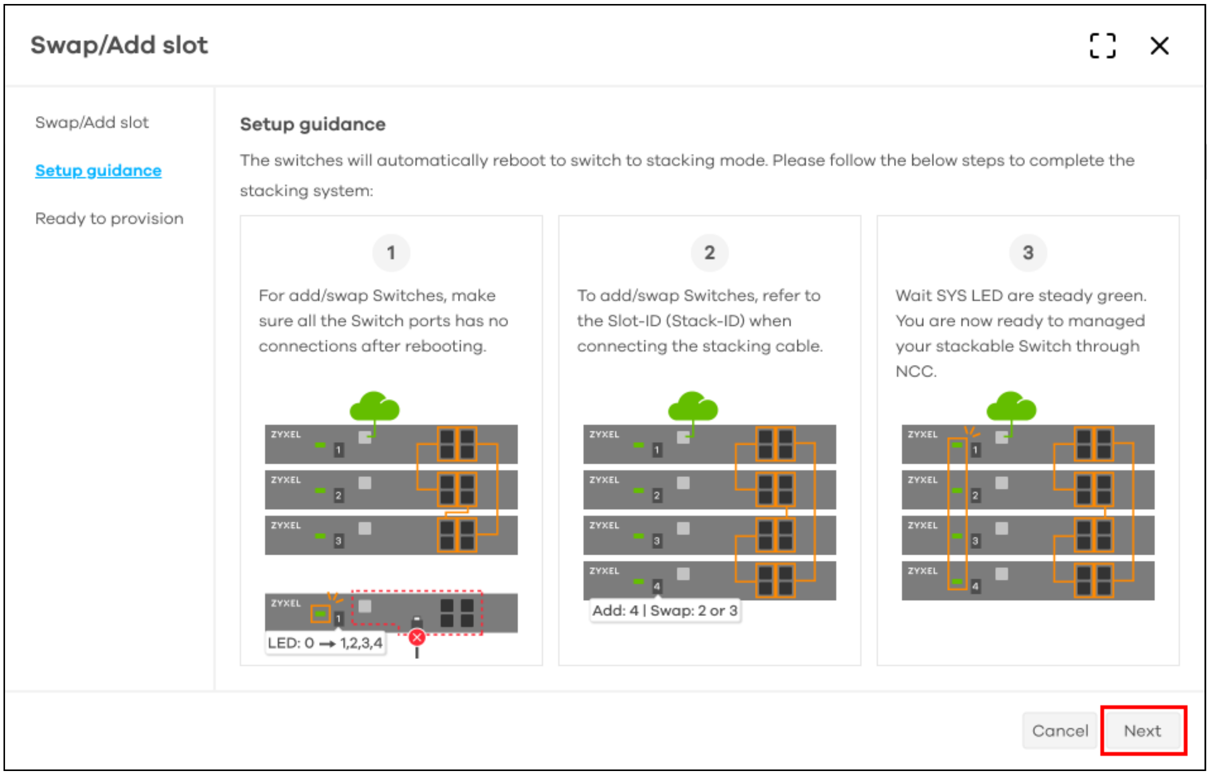
(3) Reset the removed Switch to factory-default by pressing the **RESTORE** button on the front panel for 7 seconds.

☑ I acknowledge

Cancel Change

6 Update the stacking cable connection onsite. See Section 6.3.4.3 on page 385 for the steps.

7 Then click **Next**.



Swap/Add slot

Swap/Add slot

Setup guidance

Ready to provision

Setup guidance

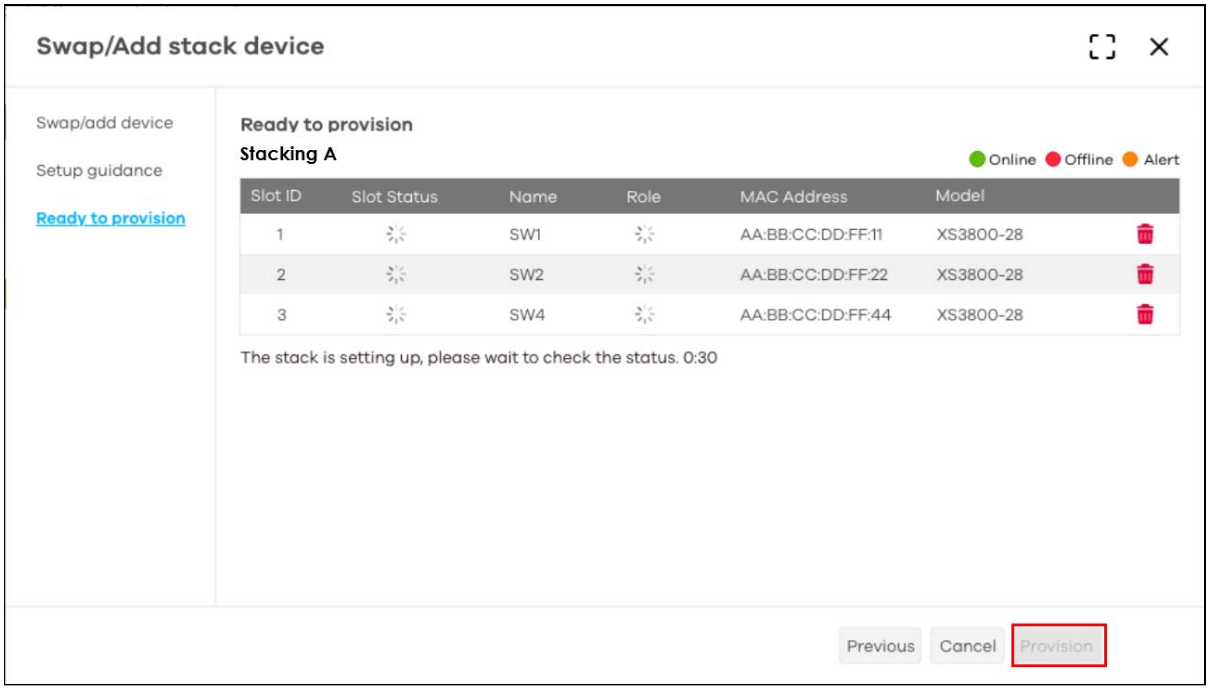
The switches will automatically reboot to switch to stacking mode. Please follow the below steps to complete the stacking system:

1 For add/swap Switches, make sure all the Switch ports has no connections after rebooting.

2 To add/swap Switches, refer to the Slot-ID (Stack-ID) when connecting the stacking cable.

3 Wait SYS LED are steady green. You are now ready to managed your stackable Switch through NCC.

8 Click **Provision** to apply the site-wide port settings to the new Nebula Device and exit the wizard.



Swap/Add stack device

Swap/add device

Setup guidance

Ready to provision

Ready to provision

Stacking A

● Online ● Offline ● Alert

Slot ID	Slot Status	Name	Role	MAC Address	Model	
1		SW1		AA:BB:CC:DD:FF:11	XS3800-28	
2		SW2		AA:BB:CC:DD:FF:22	XS3800-28	
3		SW4		AA:BB:CC:DD:FF:44	XS3800-28	

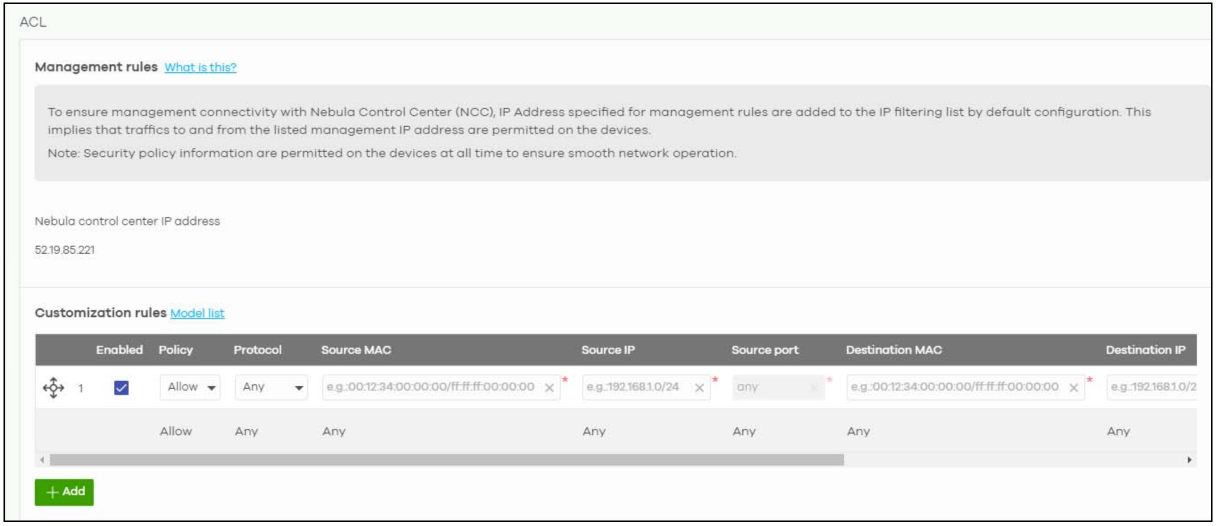
The stack is setting up, please wait to check the status. 0:30

6.3.5 ACL

ACL lets you allow or block traffic going through the Nebula Devices according to the rule settings. Use this screen to configure ACL rules on the Nebula Devices.

Click **Site-wide** > **Configure** > **Switches** > **ACL** to access this screen.

Figure 116 Site-wide > Configure > Switches > ACL



ACL

Management rules What is this?

To ensure management connectivity with Nebula Control Center (NCC), IP Address specified for management rules are added to the IP filtering list by default configuration. This implies that traffics to and from the listed management IP address are permitted on the devices.

Note: Security policy information are permitted on the devices at all time to ensure smooth network operation.

Nebula control center IP address

52.19.85.221

Customization rules Model list

	Enabled	Policy	Protocol	Source MAC	Source IP	Source port	Destination MAC	Destination IP
✥ 1	☑	Allow	Any	e.g.:00:12:34:00:00:00/ff:ff:ff:00:00:00	e.g.:192.168.1.0/24	any	e.g.:00:12:34:00:00:00/ff:ff:ff:00:00:00	e.g.:192.168.1.0/2
		Allow	Any	Any	Any	Any	Any	Any

+ Add

The following table describes the labels in this screen.

Table 75 Site-wide > Configure > Switches > ACL

LABEL	DESCRIPTION
Management rules	The NCC automatically creates rules to allow traffic from/to the Nebula Control Center IP addresses in the list.
Customization rules	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Policy	Select to allow or deny traffic that matches the filtering criteria in the rule.
Protocol	Select the type of IP protocol used to transport the traffic to which the rule is applied.
Source MAC	Enter the source MAC address of the packets that you want to filter.
Source IP	Enter the source IP address of the packets that you want to filter.
Source port	Enter the source port numbers that defines the traffic type.
Destination MAC	Enter the destination MAC address of the packets that you want to filter.
Destination IP	Enter the destination IP address of the packets that you want to filter.
Destination port	Enter the destination port numbers that defines the traffic type.
VLAN	Enter the ID number of the VLAN group to which the matched traffic belongs.
Description	Enter a descriptive name for the rule.
Delete	Click the delete icon to remove the rule.
Add	Click this button to create a new rule.

6.3.6 IP & Routing

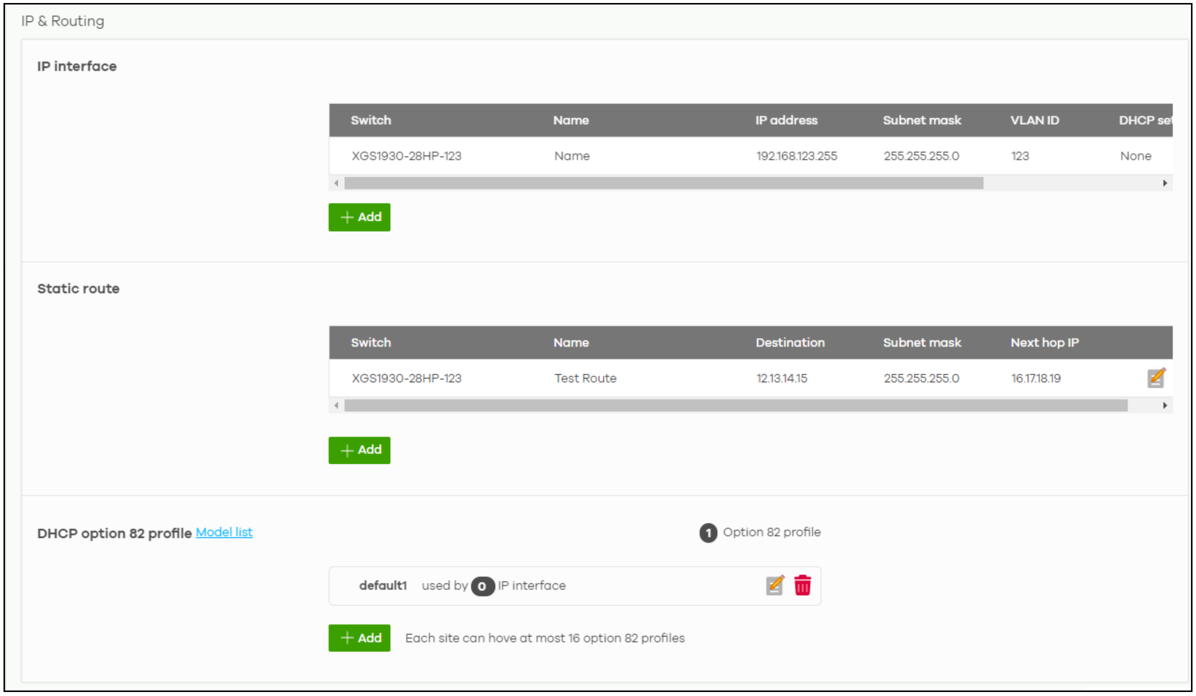
This screen enables you to create IP interfaces, static routes, and DHCP option 82 profiles on Nebula Devices in the site. This allows you to do the following:

- Create IP interfaces on a L2 Nebula Device for management or monitoring services, such as IGMP querier, auto PD recovery, ping, and ONVIF discovery.

- Create multiple IP interface on a L3 Nebula Device to route across VLANs.
- Create an IP interface and static route to specify the next hop to a specific destination subnet.
- Add Nebula Device (relay agent) information when forwarding client-originated DHCP packets to a DHCP server. This feature provides additional security when DHCP allocates network IPv4 addresses. This prevents DHCP client requests from untrusted sources.

Click **Site-wide** > **Configure** > **Switches** > **IP & Routing** to access this screen.

Figure 117 Site-wide > Configure > Switches > IP & Routing



IP & Routing

IP interface

Switch	Name	IP address	Subnet mask	VLAN ID	DHCP se
XGS1930-28HP-123	Name	192.168.123.255	255.255.255.0	123	None

+ Add

Static route

Switch	Name	Destination	Subnet mask	Next hop IP	
XGS1930-28HP-123	Test Route	12.13.14.15	255.255.255.0	16.17.18.19	✎

+ Add

DHCP option 82 profile Model list

1 Option 82 profile

default1 used by 0 IP interface

+ Add Each site can hove at most 16 option 82 profiles

The following table describes the labels in this screen.

Table 76 Site-wide > Configure > Switches > IP & Routing

LABEL	DESCRIPTION
IP interface	
Switch	This shows the name of the Nebula Device.
Name	This shows the name of the interface (network) on the Nebula Device.
IP address	This shows the IP address of the interface (network).
Subnet mask	This shows the subnet mask of the interface (network).
VLAN ID	This shows the ID number of the VLAN with which the interface (network) is associated.
DHCP setting	This shows the type of DHCP service the Nebula Device provides to the network in the site. This shows **None** when the Nebula Device does not provide any DHCP services. This shows **DHCP relay** when the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network in the site.
Relay profile	This shows the name of the DHCP option 82 profile that is bound to the IP interface. See Section 6.3.6.3 on page 398 on adding and enabling a DHCP option 82 profile on the IP interface. Otherwise, this shows **None**.
✎	Click this icon to modify the interface.

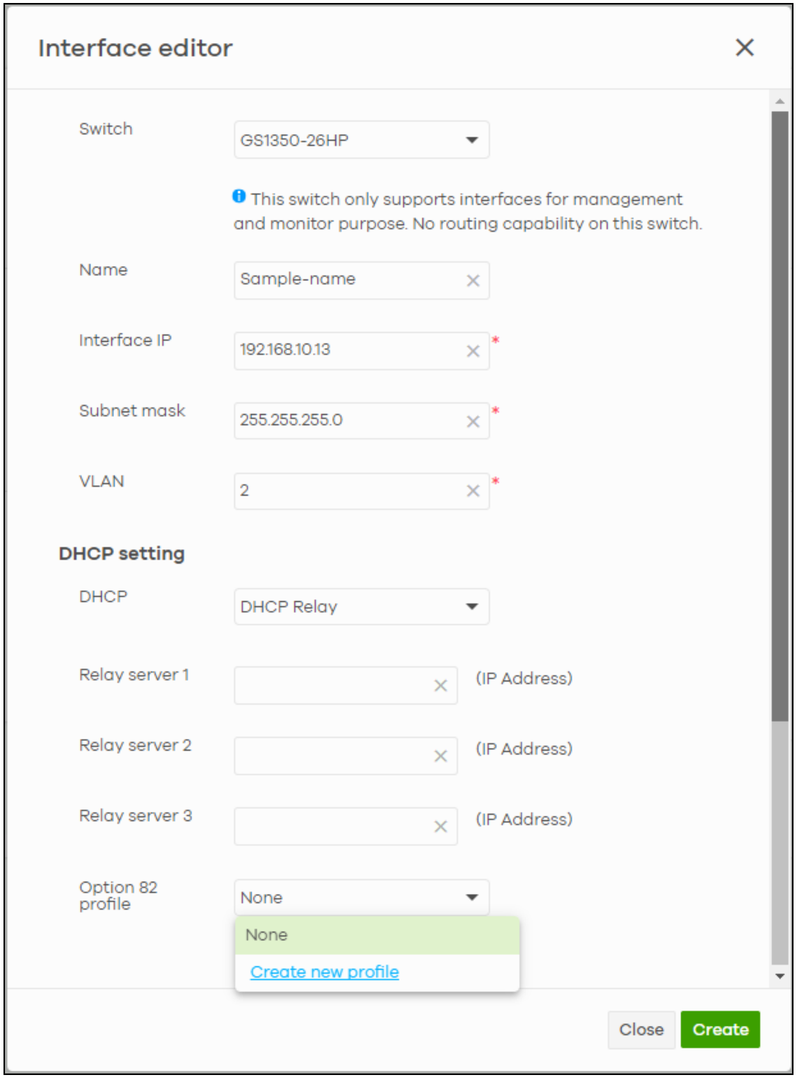
Table 76 Site-wide > Configure > Switches > IP & Routing (continued)

LABEL	DESCRIPTION
🗑	Click this icon to delete the interface.
+ Add	Click this button to create a new interface on a Nebula Device in the site.
Static route	
Switch	This shows the name of the Nebula Device.
Name	This shows the name of the static route.
Destination	This shows the destination IP address.
Subnet mask	This shows the IP subnet mask.
Next hop IP	This shows the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or Nebula Device on the same segment as your Security Appliance's interfaces. It helps forward packets to their destinations.
✎	Click this icon to modify the static route.
🗑	Click this icon to delete the static route.
+ Add	Click this button to create a new static route on a Nebula Device in the site.
DHCP option 82 profile	A DHCP option 82 profile allows the Nebula Device to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID. This shows the DHCP option 82 profile that is created on NCC.
✎	Click the edit icon to change the DHCP option 82 profile settings.
🗑	Click the remove icon to delete the DHCP option 82 profile. Note: Make sure the option 82 profile is not in use before deleting it. See Section 6.3.6.3 on page 398 for more information.
+ Add	Click this button to create a new DHCP option 82 profile on a Nebula Device in the site.

6.3.6.1 Add IP Interface

Click the **+ Add** button on the **Site-wide** > **Configure** > **Switches** > **IP & Routing** > **IP Interface** screen to access this screen.

Figure 118 Site-wide > Configure > Switches > IP & Routing > IP Interface > Add



Interface editor

Switch: GS1350-26HP

This switch only supports interfaces for management and monitor purpose. No routing capability on this switch.

Name: Sample-name

Interface IP: 192.168.10.13 *

Subnet mask: 255.255.255.0 *

VLAN: 2 *

DHCP setting

DHCP: DHCP Relay

Relay server 1: (IP Address)

Relay server 2: (IP Address)

Relay server 3: (IP Address)

Option 82 profile: None

The following table describes the labels in this screen.

Table 77 Site-wide > Configure > Switches > IP & Routing > IP Interface > Add

LABEL	DESCRIPTION
Switch	Select a Nebula Device in the site on which to create the interface.
Name	Enter a name of the interface (network) on the Nebula Device.
Interface IP	Enter the IP address of the interface (network). Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
Subnet mask	Enter the subnet mask of the interface (network).
VLAN	Enter the ID number of the VLAN with which the interface (network) is associated.
DHCP setting	
DHCP	Select **DHCP Relay** if you want the Nebula Device to route DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network in the site. Otherwise, select **None**.

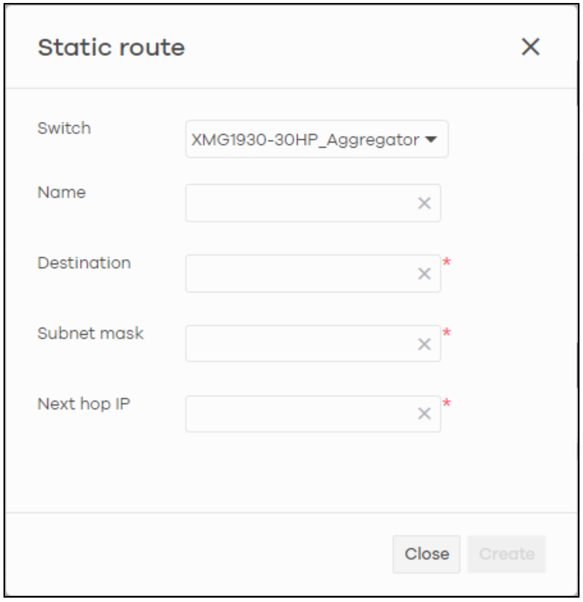
Table 77 Site-wide > Configure > Switches > IP & Routing > IP Interface > Add

LABEL	DESCRIPTION
Relay server 1	Enter the IPv4 address of a DHCP server for the network in the site.
Relay server 2 / 3	These fields are optional. Enter the IP address of another DHCP server for the network in the site.
Option 82 profile	Select an existing option 82 profile. Alternatively, click **Create new profile** to go to the **Option 82 profile** screen to add information such as port, VLAN ID, hostname, and MAC address (in hexadecimal format) to DHCP messages. This allows the DHCP server to assign the appropriate IP address according to the port, VLAN ID, hostname, and MAC address. Go to Section 6.3.6.3 on page 398 for more information. Otherwise, select **None**.
Close	Click **Close** to exit this screen without saving.
Create	Click **Create** to save your changes and create the interface.

6.3.6.2 Add Static Route

Click the **+ Add** button on the **Site-wide** > **Configure** > **Switches** > **IP & Routing** > **Static Route** screen to access this screen.

Figure 119 Site-wide > Configure > Switches > IP & Routing > Static Route > Add



Static route

Switch: XMG1930-30HP_Aggregator

Name

Destination *

Subnet mask *

Next hop IP *

The following table describes the labels in this screen.

Table 78 Site-wide > Configure > Switches > IP & Routing > Static Route > Add

LABEL	DESCRIPTION
Switch	Select a Nebula Device in the site on which to create the interface.
Name	Enter a descriptive name for this route.
Destination	Specifies the IP network address of the final destination.
Subnet mask	Enter the IP subnet mask.
Next hop IP	Enter the IP address of the next-hop gateway.

Table 78 Site-wide > Configure > Switches > IP & Routing > Static Route > Add

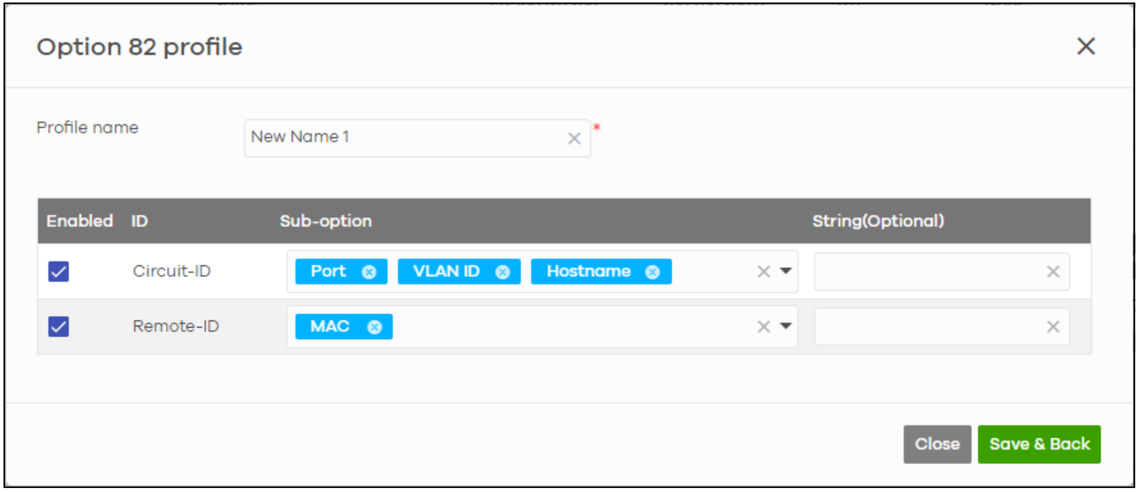
LABEL	DESCRIPTION
Close	Click **Close** to exit this screen without saving.
Create	Click **Create** to save your changes and create the static route.

6.3.6.3 Add Option 82 Profile

Use this screen to add information such as port, VLAN ID, hostname, and MAC address (in hexadecimal format) to DHCP messages. DHCP servers then create policies that match these new identifiers for DHCP assignment. Click the **+ Add** button on the **Site-wide** > **Configure** > **Switches** > **IP & Routing** > **DHCP option 82 profile** screen to access this screen.

Note: Each site can have up to 16 option 82 profiles only.

Figure 120 Site-wide > Configure > Switches > IP & Routing > DHCP option 82 profile > Add



Option 82 profile

Profile name: New Name 1 *

Enabled	ID	Sub-option	String(Optional)
☑	Circuit-ID	Port, VLAN ID, Hostname	
☑	Remote-ID	MAC	

The following table describes the labels in this screen.

Table 79 Site-wide > Configure > Switches > IP & Routing > DHCP option 82 profile > Add

LABEL	DESCRIPTION
Profile name	Enter a descriptive name for this profile, up to 64 keyboard characters.
Circuit-ID	Use this section to configure the Circuit ID sub-option to include information such as port, VLAN ID, and hostname (in hexadecimal format) that is specific to the DHCP relay agent (the Nebula Device). For example: '0014000a475331333530string'. Where: • '0014' is the port information, '00' is the slot ID and '14' is the port number • '000a' is the VLAN ID • '475331333530' is the hostname • 'string' is the optional string. See String (Optional) for more information.
Enabled	Select this checkbox to have the Nebula Device add the Circuit ID sub-option to client DHCP requests that it relays to a DHCP server.
ID	This identifies the row for **Circuit-ID** sub-option.

Table 79   Site-wide > Configure > Switches > IP & Routing > DHCP option 82 profile > Add

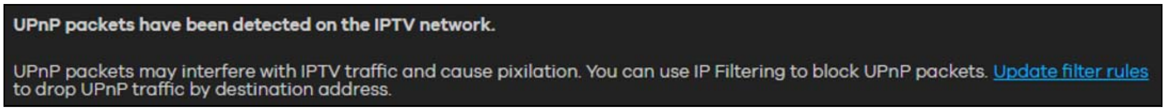
LABEL	DESCRIPTION
Sub-option	Select the **Port** option to have the Nebula Device add the port information that the DHCP client connects to. This allows the DHCP server to assign IPv4 addresses to the Nebula Device with the corresponding port information. Select the **VLAN ID** option to have the Nebula Device add the VLAN ID information to which the port belongs. This allows the DHCP server to assign IPv4 addresses to the Nebula Device with the corresponding VLAN ID. Select the **Hostname** option to add the system name information to the client DHCP requests that it relays to a DHCP server. This allows the DHCP server to assign IPv4 addresses to the Nebula Device with the corresponding hostname. Otherwise, leave this field blank.
String (Optional)	Enter an optional string of up to 64 printable ASCII characters that the Nebula Device adds into the client DHCP requests, except the characters inside the square brackets [?], [|], ['], ["] or [,].
Remote-ID	Use this section to configure the Remote ID sub-option to include information such as the MAC address (in hexadecimal format) that is specific to the DHCP relay agent (the Nebula Device). For example: ‘bccf4f000001custom’. Where: • ‘bccf4f000001’ is the MAC address • ‘custom’ is the optional string. See String (Optional) for more information.
Enabled	Select this checkbox to have the Nebula Device append the Remote ID sub-option to the option 82 field of DHCP requests.
ID	This identifies the row for **Remote-ID** sub-option.
Sub-option	Select the **MAC** option to have the Nebula Device add its MAC address information to the client DHCP requests that it relays to a DHCP server. Otherwise, leave this field blank.
String (Optional)	Enter an optional string of up to 64 printable ASCII characters that the Nebula Device adds into the client DHCP requests, except the characters inside the square brackets [?], [|], ['], ["] or [,].
Close	Click **Close** to exit this screen without saving.
Save & Back	Click **Save & Back** to save your changes and close this screen.

6.3.7 ONVIF Discovery

IP-based security products use a specific protocol for communication. One of the most common protocols is ONVIF (Open Network Video Interface Forum). ONVIF is a standard interface for interoperability of IP-based security products. When ONVIF is enabled and configured on a Nebula Device, the Nebula Device can obtain information from connected ONVIF-compatible devices, such as a device’s system name and IP address.

In NCC, you can configure ONVIF-compatible Nebula Devices (for example, GS1350) in a site to discover ONVIF-compatible devices in one designated VLAN.

Note: ONVIF and UPnP are similar protocols and may conflict with each other. If NCC detects UPnP packets on the same network as ONVIF, then it will prompt you to automatically create an ACL rule that blocks UPnP traffic (UDP, port 1900).



UPnP packets have been detected on the IPTV network.

UPnP packets may interfere with IPTV traffic and cause pixilation. You can use IP Filtering to block UPnP packets. Update filter rules to drop UPnP traffic by destination address.

6.3.7.1 Configuring ONVIF Discovery

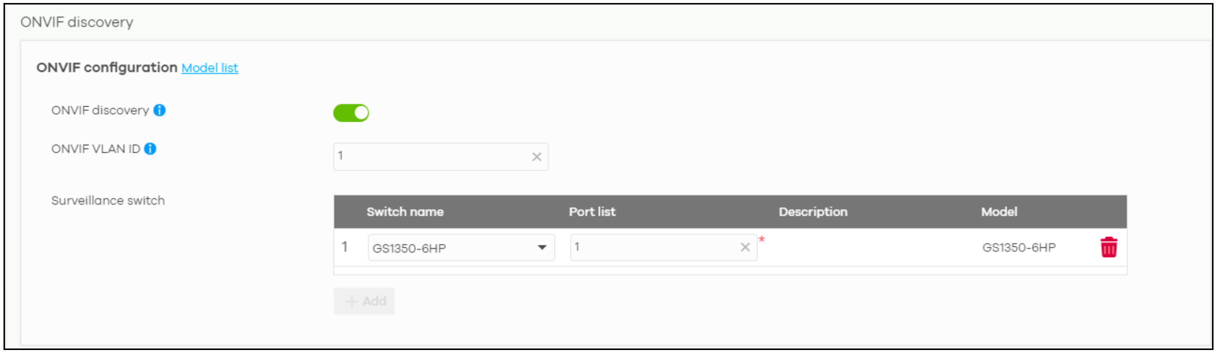
Follow these steps to configure ONVIF discovery within a site.

1. Decide on the VLAN ID you want to use for ONVIF discovery within the site. This VLAN is the ONVIF discovery VLAN.
2. Go to **Site-wide** > **Configure** > **Switches** > **IP & Routing**. For each Nebula Device that you want to enable ONVIF discovery on, add an IP interface for the Nebula Device on the ONVIF discovery VLAN.
3. Go to **Site-wide** > **Configure** > **Switches** > **ONVIF discovery.** Enable **ONVIF discovery**, and then set **ONVIF VLAN ID** to the ID of your ONVIF discovery VLAN.
4. For each Nebula Device that you want to enable ONVIF discovery on, click **+ Add**. Select the Nebula Device, and then enter the ports that you want to listen for ONVIF devices.

6.3.7.2 ONVIF Discovery Screen

Click **Site-wide** > **Configure** > **Switches** > **ONVIF discovery** to access this screen.

Figure 121 Site-wide > Configure > Switches > ONVIF discovery



ONVIF discovery

ONVIF configuration Model list

ONVIF discovery: on

ONVIF VLAN ID: 1

Surveillance switch

	Switch name	Port list	Description	Model	
1	GS1350-6HP	1		GS1350-6HP	🗑

+ Add

The following table describes the labels in this screen.

Table 80 Site-wide > Configure > Switches > ONVIF discovery

LABEL	DESCRIPTION
Model list	Click this to view a list of Zyxel Nebula Device models that support ONVIF discovery.
ONVIF discovery	Enable this to allow ONVIF-compatible Nebula Devices in the site to send ONVIF packets to discover or scan for ONVIF-compatible IP-based security devices.
ONVIF VLAN ID	Enter the ID number of the VLAN to run ONVIF. You can enter multiple VLAN IDs separated by a comma (,). For example, enter "1,2" for VLAN IDs 1 and 2.
Switch name	Select the Nebula Device that you want to enable ONVIF discovery on.
Port list	Enter the port numbers to allow discovery of ONVIF-compatible devices. You can enter multiple ports separated by comma (,) or hyphen (-) without spaces. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Description	Enter a descriptive name for this Nebula Device.
Model	This shows the Nebula Device model.
🗑	Click this icon to delete the ONVIF configuration for the Nebula Device.
+ Add	Click this to configure ONVIF discovery on another Nebula Device in the site.

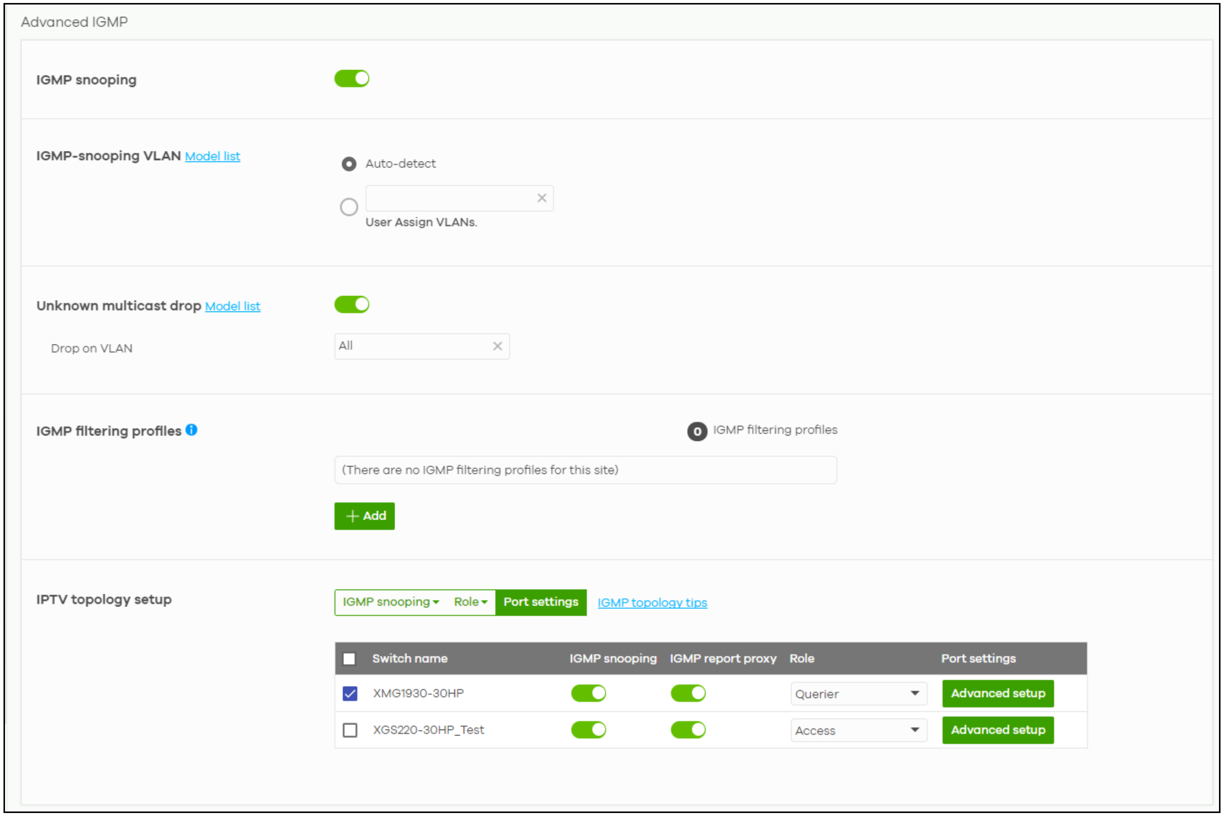
6.3.8 Advanced IGMP

A Nebula Device can passively snoop on IGMP packets transferred between IP multicast routers/Nebula Devices and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multi-casting accordingly. IGMP snooping allows the Nebula Device to learn multicast groups without you having to manually configure them.

The Nebula Device forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Nebula Device.

Use this screen to enable IGMP snooping on the Nebula Devices in the site, create IGMP filtering profiles and configure advanced IGMP snooping settings that apply to all ports on the Nebula Device for your IPTV network. Click **Site-wide** > **Configure** > **Switches** > **Advanced IGMP** to access this screen. You can make adjustments on a per-port basis using the **Site-wide** > **Configure** > **Switches** > **Switch ports** screen.

Figure 122 Site-wide > Configure > Switches > Advanced IGMP



Advanced IGMP

IGMP snooping

IGMP-snooping VLAN Model list

● Auto-detect

○ User Assign VLANs.

Unknown multicast drop Model list

Drop on VLAN: All

IGMP filtering profiles

0 IGMP filtering profiles

(There are no IGMP filtering profiles for this site)

IPTV topology setup

☐	Switch name	IGMP snooping	IGMP report proxy	Role	Port settings
☑	XMG1930-30HP	●	●	Querier	Advanced setup
☐	XGS220-30HP_Test	●	●	Access	Advanced setup

The following table describes the labels in this screen.

Table 81 Site-wide > Configure > Switches > Advanced IGMP

LABEL	DESCRIPTION
IGMP snooping	Select **ON** to enable and configure IGMP snooping settings on all Nebula Devices in the site. Select **OFF** to disable it.
IGMP-snooping VLAN	Select **Auto-detect** to have the Nebula Device learn multicast group membership information of any VLANs automatically. Select **User Assigned VLANs** and enter the VLAN IDs to have the Nebula Device only learn multicast group membership information of the VLANs that you specify. Click **Model List** to view a list of Zyxel Nebula Device models that do not support this feature. Note: The Nebula Device can perform IGMP snooping on up to 16 VLANs.
Unknown multicast drop	Specify the action to perform when the Nebula Device receives an unknown multicast frame. Select **ON** to discard the frames. Select **OFF** to send the frames to all ports. Click **Model List** to view a list of Zyxel Nebula Device models that do and do not support this feature.
Drop on VLAN	This allows you to define the VLANs in which unknown multicast packets can be dropped. Note: The Nebula Device can drop unknown multicast packets on up to 8 VLANs.
IGMP filtering profiles	An IGMP filtering profile specifies a range of multicast groups that clients connected to the Nebula Device are able to join. You can set the Nebula Device to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating a port to the profile.
✎	Click the edit icon to change the profile settings. See Section 6.3.8.1 on page 403.
🗑	Click the remove icon to delete the profile.
+Add	Click this button to create a new profile. See Section 6.3.8.1 on page 403.
IPTV topology setup The following three buttons are available only when there are multiple Nebula Devices in the site and your administrator account has full access to this screen.	
IGMP snooping	Select the Nebula Devices you want to configure and click this button to turn on or off IGMP snooping on the selected Nebula Devices.
Role	Select the Nebula Devices you want to configure and click this button to change the IGMP role of the selected Nebula Devices.
Port settings	Select the Nebula Devices you want to configure and click this button to open the **Port settings** screen, where you can change IGMP leave mode and IGMP filtering profile for the ports on the selected Nebula Devices. See Section 6.3.8.2 on page 404.
IGMP topology tips	Click this to view information about configuring your network and device roles to optimize IPTV performance.
The following list shows you the IGMP settings for each Nebula Device in the site.	
Switch Name	This shows the name of the Nebula Device in the site.
IGMP snooping	Click this to enable IGMP snooping on the Nebula Device. See Section 6.3.8 on page 401 for more information on IGMP snooping.

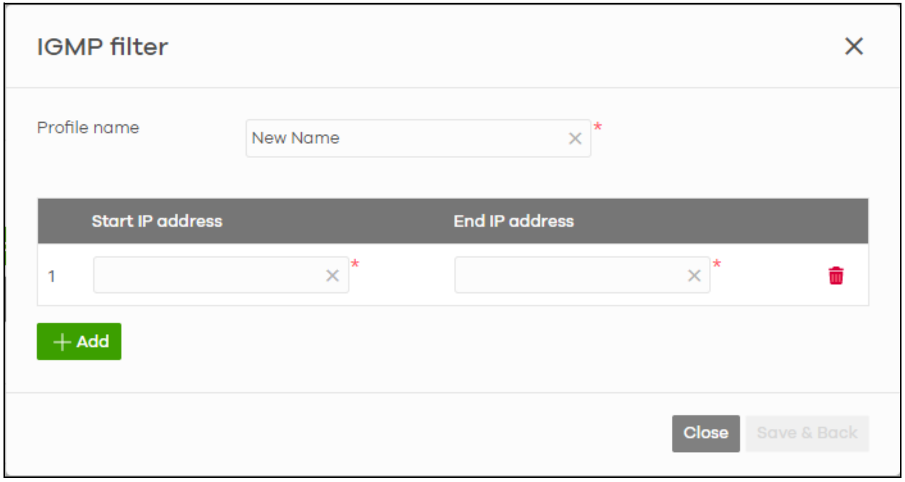
Table 81 Site-wide > Configure > Switches > Advanced IGMP (continued)

LABEL	DESCRIPTION
IGMP report proxy	Click this to enable IGMP report proxy on the Nebula Device. An IGMP report is generated when monitoring multicast address or membership query. It is highly recommended to disable this in the following conditions: • When the Nebula Device is deployed in a Networked AV environment. A Networked AV environment is specifically designed to simplify configuration and management of the Nebula Device for AVoIP (Audio-Video over Internet Protocol) application. • When the Nebula Device is connected to CPEs (customer premise equipment) that require a specific IPTV source. Some CPEs validate IPTVs based on the source IP and MAC address of their IGMP join request. IGMP report proxy trims down the amount of IGMP join packets and sends its own IGMP join request.
Role	This shows whether the Nebula Device is acting as an IGMP snooping querier, aggregation Nebula Device or access Nebula Device in the IPTV network.
Port settings	Click **Advanced setup** to open the **Port settings** screen, where you can change IGMP leave mode and IGMP filtering profile for the ports on the Nebula Device. See Section 6.3.8.2 on page 404.
The following fields display when the IGMP role of a Nebula Device is set to **Querier**.	
VLAN	Enter the ID number of the VLAN on which the Nebula Device learns the multicast group membership.
Querier IP Interface	Enter the IP address of the Nebula Device interface in IGMP querier mode. The Nebula Device acts as an IGMP querier in that network/VLAN to periodically send out IGMP query packets with the interface IP address and update its multicast forwarding table.
Mask	Enter the subnet mask of the Nebula Device interface in IGMP querier mode.
🗑	Click the remove icon to delete the rule.
Add	Click this button to create a new rule.

6.3.8.1 Add/Edit IGMP Filtering Profiles

Use this screen to create a new IGMP filtering profile or edit an existing profile. To access this screen, click the **Add** button or a profile's **Edit** button in the **IGMP filtering profiles** section of the **Site-wide** > **Configure** > **Switches** > **Advanced IGMP** screen.

Figure 123 Site-wide > Configure > Switches > Advanced IGMP: Add IGMP Filtering Profile



IGMP filter

Profile name: New Name

The following table describes the labels in this screen.

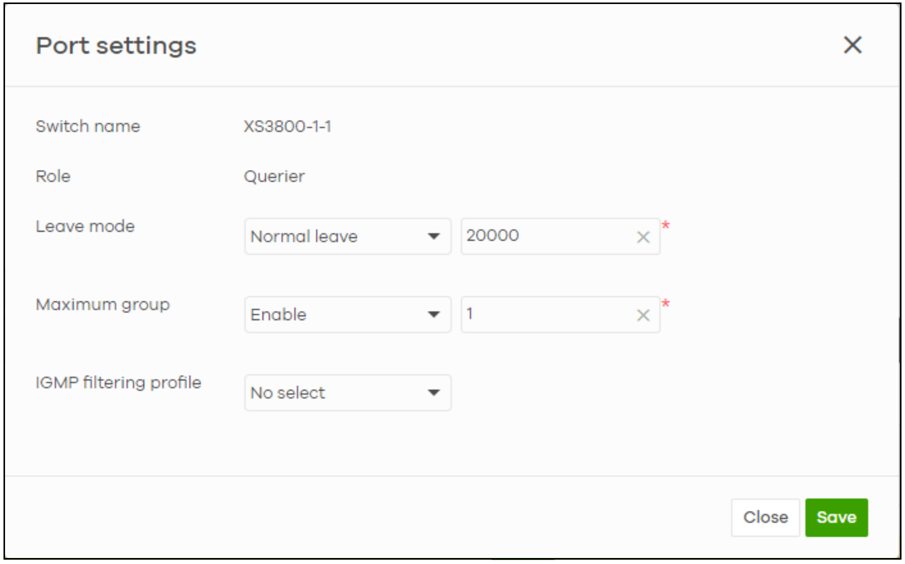
Table 82 Site-wide > Configure > Switches > Advanced IGMP: Add/Edit IGMP Filtering Profile

LABEL	DESCRIPTION
Profile name	Enter a descriptive name for this profile for identification purposes.
	This shows the index number of the rule.
Start IP address	Enter the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End IP address	Enter the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start IP Address** and **End IP Address** fields.
🗑	Click the remove icon to delete the rule.
+Add	Click this button to create a new rule in this profile.
Close	Click this button to exit this screen without saving.
Save & Back	Click this button to save your changes and close the screen.

6.3.8.2 IGMP Port Settings

Use this screen to modify the IGMP snooping settings, such as IGMP leave mode and filtering profile for all ports on the Nebula Device. To access this screen, select one or more Nebula Devices and click the **Port settings** button or click a Nebula Device's **Advanced setup** button in the **IPTV topology setup** section of the **Site-wide** > **Configure** > **Switches** > **Advanced IGMP** screen.

Figure 124 Site-wide > Configure > Switches > Advanced IGMP: Port settings



Port settings

Switch name	XS3800-1-1	
Role	Querier	
Leave mode	Normal leave	20000 *
Maximum group	Enable	1 *
IGMP filtering profile	No select	

The following table describes the labels in this screen.

Table 83 Site-wide > Configure > Switches > Advanced IGMP: Port settings

LABEL	DESCRIPTION
Switch name	This shows the name of the Nebula Devices that you select to configure.
Role	This shows whether the Nebula Devices you selected is an IGMP snooping querier, aggregation Nebula Device or access Nebula Device in the IPTV network.

Table 83 Site-wide > Configure > Switches > Advanced IGMP: Port settings (continued)

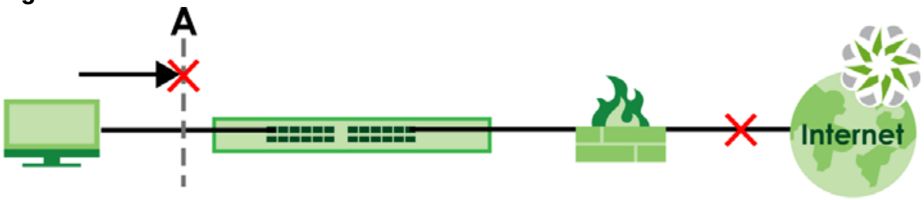
LABEL	DESCRIPTION
Leave mode	Select **Immediate Leave** to set the Nebula Device to remove this port from the multicast tree immediately when an IGMP leave message is received on this port. Select this option if there is only one host connected to this port. Select **Normal Leave** or **Fast Leave** and enter an IGMP normal/fast leave timeout value to have the Nebula Device wait for an IGMP report before the leave timeout when an IGMP leave message is received on this port. You need to specify how many milliseconds the Nebula Device waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host. In **Normal Leave** mode, when the Nebula Device receives an IGMP leave message from a host on a port, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The Nebula Device forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table. In **Fast Leave** mode, right after receiving an IGMP leave message from a host on a port, the Nebula Device itself sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process.
Maximum group	Select **Enable** and enter the maximum number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report received on this port will replace the earliest group entry in the multicast forwarding table. Otherwise, select **Disable** to turn off multicast group limits.
IGMP filtering profile	An IGMP filtering profile specifies a range of multicast groups that clients connected to the Nebula Device are able to join. Select the name of the IGMP filtering profile to use for this port. Otherwise, select **No Select** to remove restrictions and allow the port to join any multicast group.
Reset	Click this button to return the screen to its last-saved settings.
Close	Click this button to exit this screen without saving.
Save	Click this button to save your changes and close the screen.

6.3.9 Authentication

Use this screen to configure authentication servers and policies to validate access to ports on the Nebula Device using the Nebula cloud authentication server or an external RADIUS server.

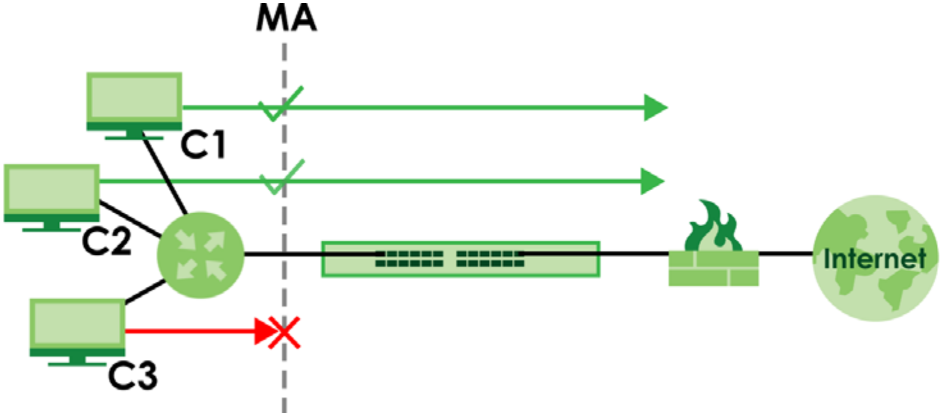
Note: Network traffic from clients will be denied when the Nebula cloud authentication (**A**) server (NCAS) cannot be reached.

Figure 125 NCAS Disconnect Behavior



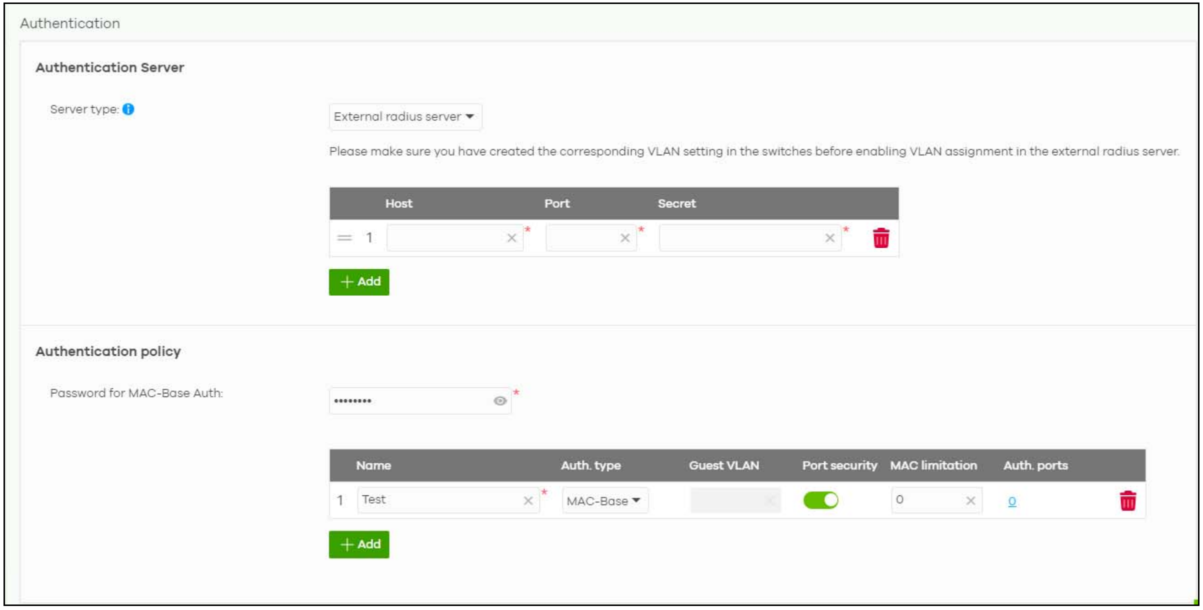
The following figure shows an example Nebula Device with ports enabled for MAC authentication. Clients 1 and 2 (C1, C2) passes MAC authentication (authorized). Client 3 (C3) fails MAC authentication (not authorized).

Figure 126 MAC Authentication Application



Click **Site-wide** > **Configure** > **Switches** > **Authentication** to access this screen.

Figure 127 Site-wide > Configure > Switches > Authentication



Authentication

Authentication Server

Server type: External radius server

Please make sure you have created the corresponding VLAN setting in the switches before enabling VLAN assignment in the external radius server.

	Host	Port	Secret
1			

+ Add

Authentication policy

Password for MAC-Base Auth: ••••••••

	Name	Auth. type	Guest VLAN	Port security	MAC limitation	Auth. ports
1	Test	MAC-Base		●	0	0

+ Add

The following table describes the labels in this screen.

Table 84   Site-wide > Configure > Switches > Authentication

LABEL	DESCRIPTION
Authentication Server	
Server type	Select **External radius server** to have both IEEE 802.1x (WPA-Enterprise) authentication and MAC-based authentication. The Nebula Device sends a request message to a RADIUS server in order to authenticate clients. The administrator must enter the IP address of the RADIUS server. The default port is 1812. Note: Make sure to configure VLAN for the Nebula Device before enabling VLAN assignment in the external RADIUS server. Select **Nebula cloud authentication** to have MAC-based authentication only. The Nebula Device sends HTTPS message to NCAS (Nebula Cloud Authentication Server) to authenticate clients. The default port is 443. See Section 3.39 on page 182 for the steps in setting up MAC authentication with NCAS. Blocked clients do not appear in the Nebula Device MAC address table. The Nebula Device re-authenticates blocked clients when: • 5 minutes after blocked client failed authentication • Blocked client disconnects and reconnects to the Nebula Device port. Note: The **Blocked** client in the **Site-wide** > **Clients** > **Client list** screen has a higher priority than MAC-based authentication. All network traffic from clients will be denied when the NCAS cannot be reached.
The following fields appear when you select **External radius server** as the **Server type**.	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Host	Enter the IP address of the external RADIUS server.
Port	Enter the port of the RADIUS server for authentication (default 1812).
Secret	Enter a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Nebula Device.
🗑	Click the remove icon to delete the entry.
Add	Click this button to create a new RADIUS server entry.
Authentication policy	You apply the policy to a port in **Site-wide** > **Configure** > **Switches** > **Switch ports**: **Edit** (a selected port).
Password for MAC-Base Auth	Enter the password the Nebula Device sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters.
Name	Enter a descriptive name for the policy.
Auth. type	Select **MAC-Base** if you want to validate access to the ports based on the MAC address and password of the client. Select **802.1X** if you want to validate access to the ports based on the user name and password provided by the client. Note: 802.1X is not supported when you select **Nebula cloud authentication** in **Server type**.
Guest VLAN	A guest VLAN is a pre-configured VLAN on the Nebula Device that allows non-authenticated users to access limited network resources through the Nebula Device. Enter the number that identifies the guest VLAN.
Port security	Click **On** to enable port security on the ports. Otherwise, select **Off** to disable port security on the ports.

Table 84 Site-wide > Configure > Switches > Authentication (continued)

LABEL	DESCRIPTION
MAC limitation	This field is configurable only when you enable port security. Specify the maximum number of MAC addresses learned on a port. For example, if you set the **MAC limitation** to 5, then only five clients can be learned on a specific port on any time.
Auth. ports	This shows the number of the Nebula Device ports to which this policy is applied.
🗑	Click the remove icon to delete the profile.
Add	Click this button to create a new policy.

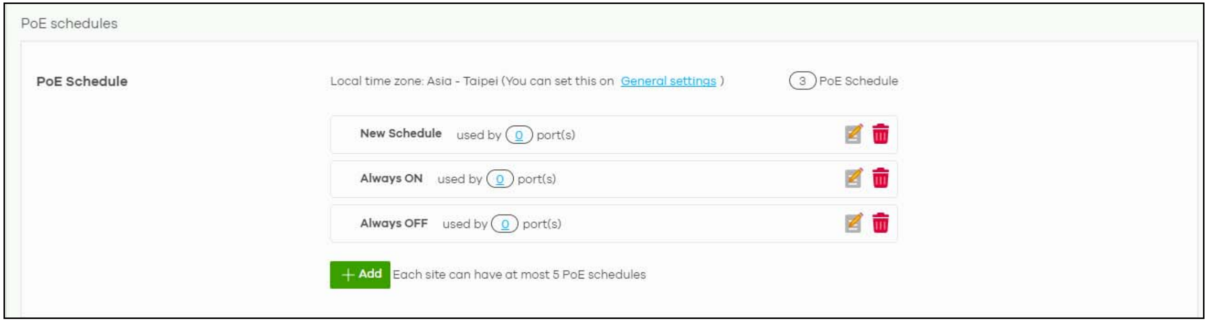
6.3.10 PoE Schedules

Use this screen to view and configure Power over Ethernet (PoE) schedules which can be applied to the ports. PoE is enabled at the specified time/date. Click **Site-wide** > **Configure** > **Switches** > **PoE schedules** to access this screen.

Note: The NCC will not generate an alert when PoE is disabled and the connected APs go offline because of the pre-defined PoE schedules.

The table shows the name of the existing schedules and the number of ports to which a schedule is applied. Click a schedule's edit icon to modify the schedule settings or click the **Add** button to create a new schedule. See Section 6.3.10.1 on page 408.

Figure 128 Site-wide > Configure > Switches > PoE schedules



PoE schedules

PoE Schedule

Local time zone: Asia - Taipei (You can set this on General settings)

3 PoE Schedule

New Schedule used by 0 port(s)

Always ON used by 0 port(s)

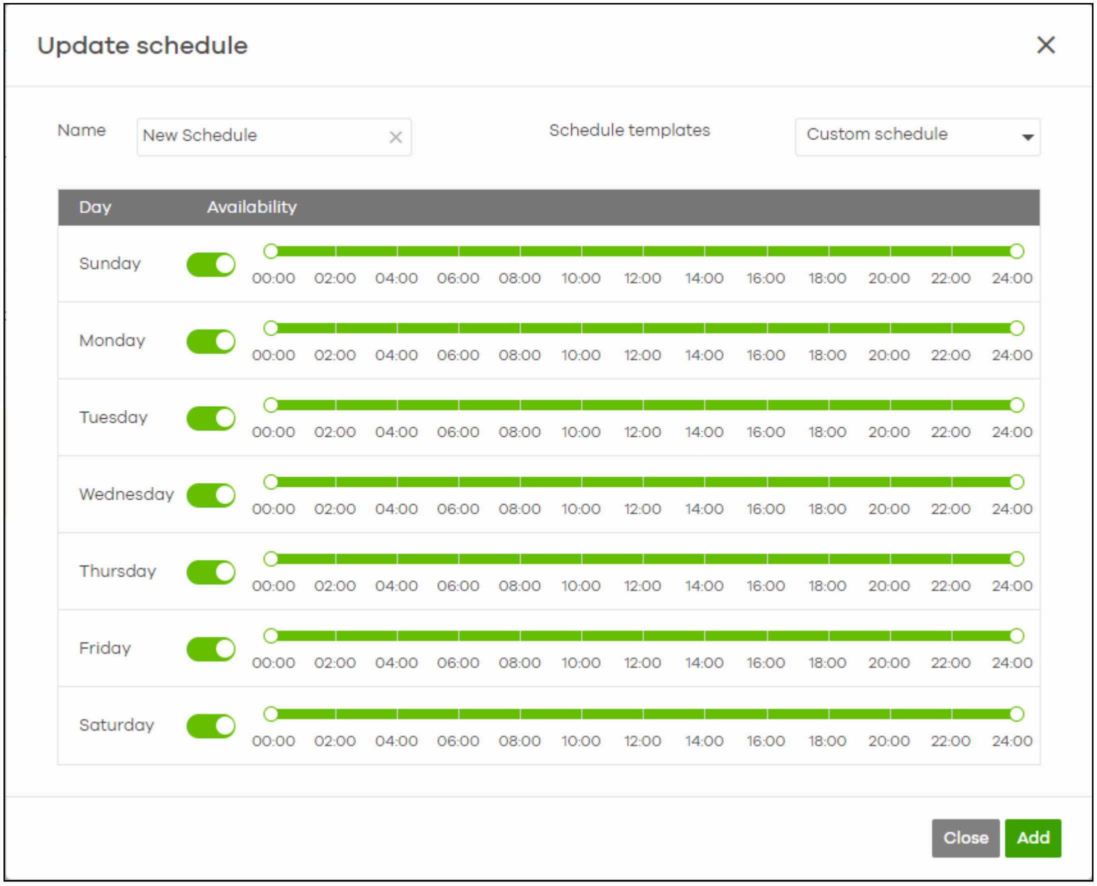
Always OFF used by 0 port(s)

Each site can have at most 5 PoE schedules

6.3.10.1 Create new schedule

Click the **Add** button in the **Site-wide** > **Configure** > **Switches** > **PoE schedules** screen to access this screen.

Figure 129 Site-wide > Configure > Switches > PoE schedule: Add



Update schedule

Name: New Schedule

Schedule templates: Custom schedule

Day	Availability
Sunday	On, 00:00 – 24:00
Monday	On, 00:00 – 24:00
Tuesday	On, 00:00 – 24:00
Wednesday	On, 00:00 – 24:00
Thursday	On, 00:00 – 24:00
Friday	On, 00:00 – 24:00
Saturday	On, 00:00 – 24:00

The following table describes the labels in this screen.

Table 85 Site-wide > Configure > Switches > PoE schedules: Add

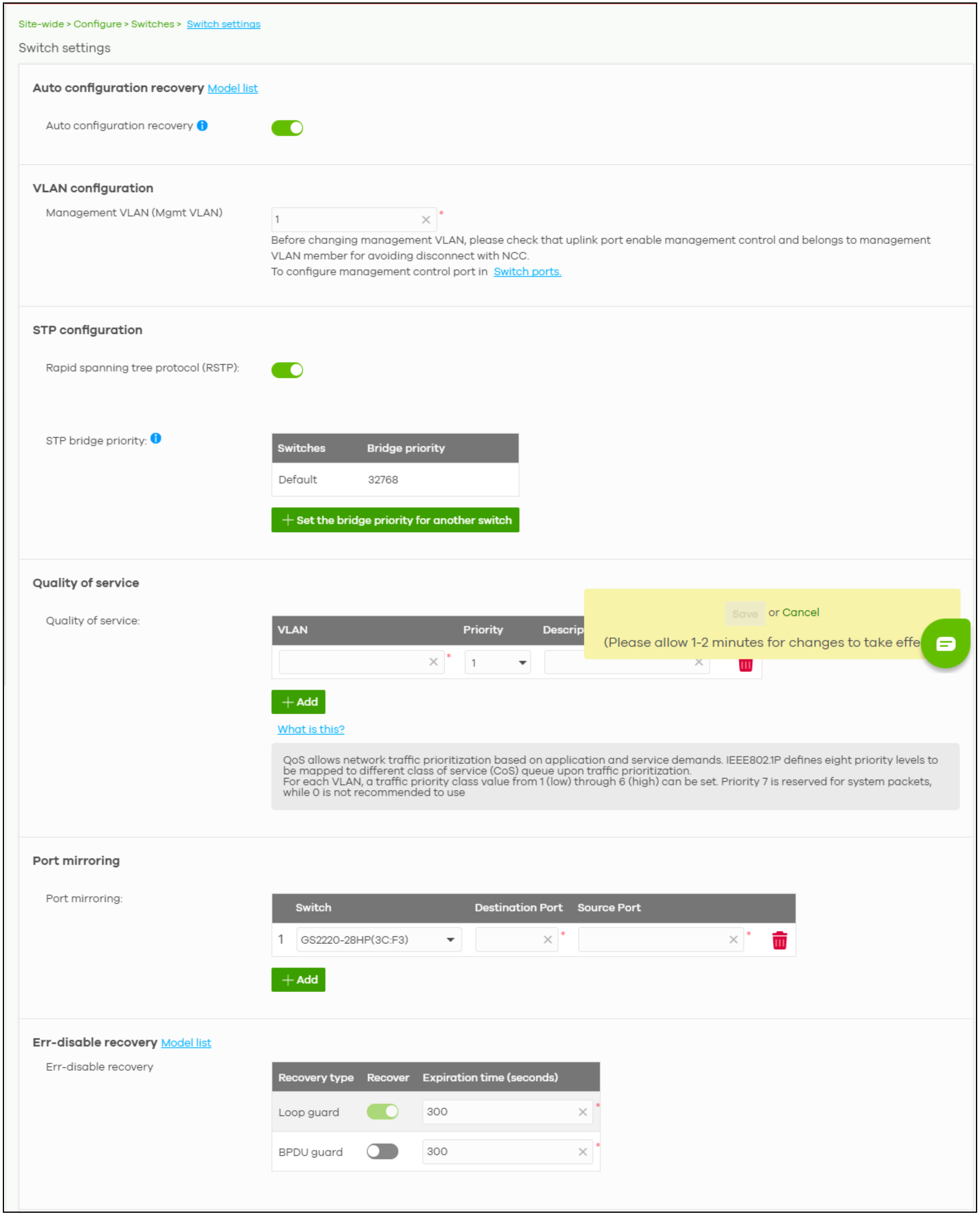
LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identification purposes.
Schedule templates	Select a pre-defined schedule template or select **Custom schedule** and manually configure the day and time at which PoE is enabled.
Day	This shows the day of the week.
Availability	Click **On** to enable PoE at the specified time on this day. Otherwise, select **Off** to turn PoE off on the day and at the specified time. Specify the hour and minute when the schedule begins and ends each day.
Close	Click this button to exit this screen without saving.
Add	Click this button to save your changes and close the screen.

6.3.11 Switch Settings

Use this screen to configure global Nebula Device settings, such as (R)STP, QoS, port mirroring, voice VLAN, DHCP server guard, and IP source guard.

Click **Site-wide** > **Configure** > **Switches** > **Switch settings** to access this screen.

Figure 130 Site-wide > Configure > Switches > Switch settings



Switch settings

Auto configuration recovery Model list

Auto configuration recovery: ●

VLAN configuration

Management VLAN (Mgmt VLAN): 1 *

Before changing management VLAN, please check that uplink port enable management control and belongs to management VLAN member for avoiding disconnect with NCC.
To configure management control port in Switch ports.

STP configuration

Rapid spanning tree protocol (RSTP): ●

STP bridge priority:

Switches	Bridge priority
Default	32768

Quality of service

Quality of service:

VLAN	Priority	Descrip
*	1	

(Please allow 1-2 minutes for changes to take effe

QoS allows network traffic prioritization based on application and service demands. IEEE802.1P defines eight priority levels to be mapped to different class of service (CoS) queue upon traffic prioritization.
For each VLAN, a traffic priority class value from 1 (low) through 6 (high) can be set. Priority 7 is reserved for system packets, while 0 is not recommended to use

Port mirroring

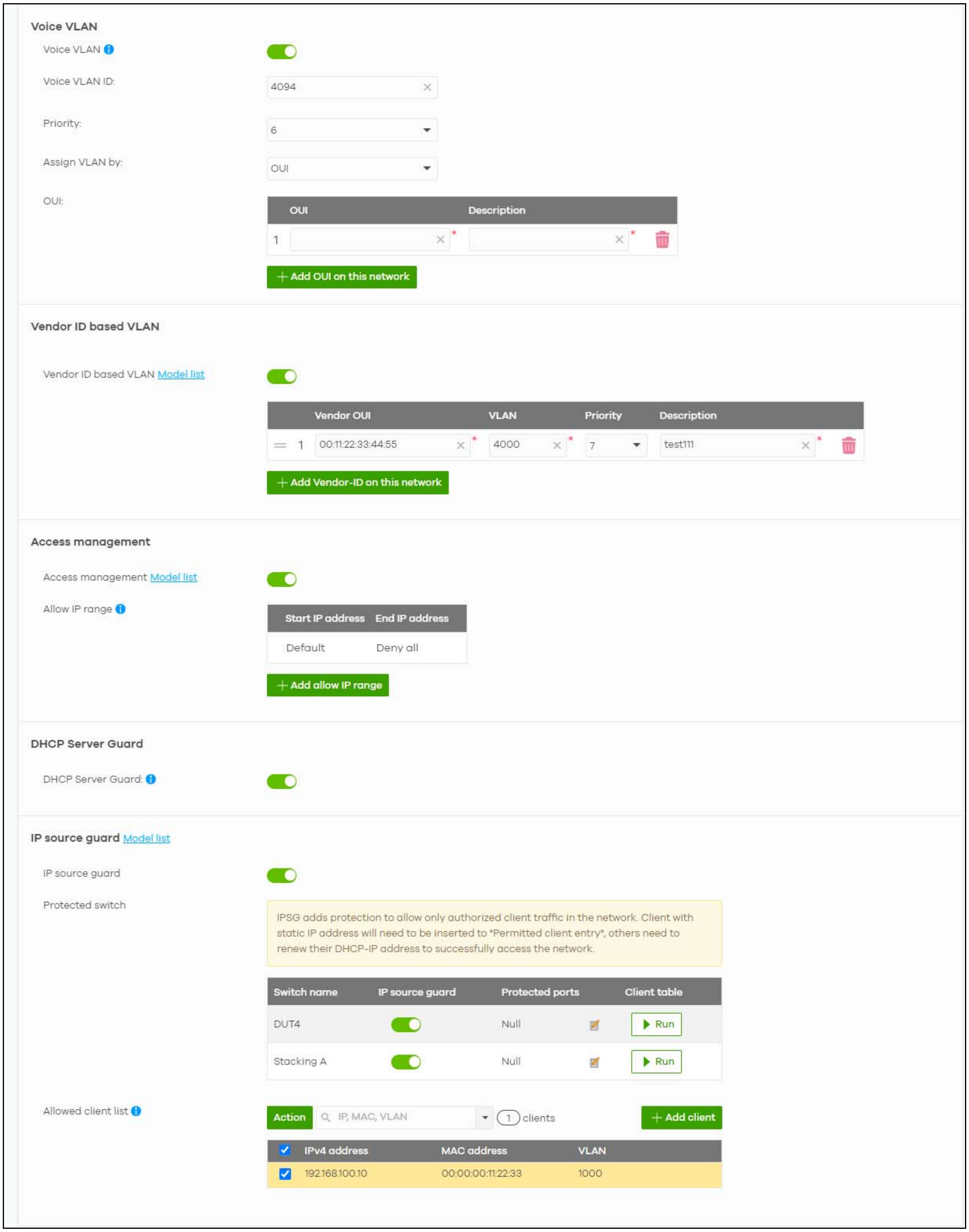
Port mirroring:

	Switch	Destination Port	Source Port
1	GS2220-28HP(3C:F3)	*	*

Err-disable recovery Model list

Err-disable recovery

Recovery type	Recover	Expiration time (seconds)
Loop guard	●	300 *
BPDU guard	○	300 *



Voice VLAN

Voice VLAN: ON

Voice VLAN ID: 4094

Priority: 6

Assign VLAN by: OUI

OUI:

	OUI	Description
1		

+ Add OUI on this network

Vendor ID based VLAN

Vendor ID based VLAN Model list: ON

	Vendor OUI	VLAN	Priority	Description
1	00:11:22:33:44:55	4000	7	test111

+ Add Vendor-ID on this network

Access management

Access management Model list: ON

Allow IP range

Start IP address	End IP address
Default	Deny all

+ Add allow IP range

DHCP Server Guard

DHCP Server Guard: ON

IP source guard Model list

IP source guard: ON

Protected switch

IPSG adds protection to allow only authorized client traffic in the network. Client with static IP address will need to be inserted to "Permitted client entry", others need to renew their DHCP-IP address to successfully access the network.

Switch name	IP source guard	Protected ports	Client table
DUT4	ON	Null	▶ Run
Stacking A	ON	Null	▶ Run

Allowed client list

Action | IP, MAC, VLAN | 1 clients | + Add client

☑	IPv4 address	MAC address	VLAN
☑	192.168.100.10	00:00:00:11:22:33	1000

The following table describes the labels in this screen.

Table 86 Site-wide > Configure > Switches > Switch settings

LABEL	DESCRIPTION
Auto configuration recovery	
Auto configuration recovery	When **On**, connectivity check to NCC is done 5 minutes after any configuration change. If an NCC connection problem is detected, the Nebula Device will return to its last saved custom default configuration. The Nebula Device will be locked by NCC and the banner **N Switches are currently protected by Auto Configuration Recovery** will be displayed. Otherwise, the latest configuration will be saved as the new custom default configuration. Note: If the NCC connectivity error occur 5 minutes after a configuration change, the Nebula Device will not return to its last saved configuration. Note: When **Auto configuration recovery** is turned **Off**, a pop-up message appears informing you that the locked Nebula Device(s) will be unlocked. Click **Confirm** if you wish to continue.
VLAN configuration	
Management VLAN (Mgmt VLAN)	Enter the VLAN identification number associated with the Nebula Device IP address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the Nebula Device make sure the port that you are connected to is a member of Management VLAN. Before changing the management VLAN for an uplink port, check the following to avoid disconnection with NCC: • **Management Control** is enabled in **Site-wide** > **Configure** > **Switches** > **Switch ports** • The uplink port belongs to the management VLAN in **Site-wide** > **Configure** > **Switches** > **Switch ports**: **PVID**.
STP configuration	
Rapid spanning tree protocol (RSTP)	Select **On** to enable RSTP on the Nebula Device. Otherwise, select **Off**.
STP bridge priority	Bridge priority is used in determining the root Nebula Device, root port and designated port. The Nebula Device with the highest priority (lowest numeric value) becomes the STP root Nebula Device. If all Nebula Devices have the same priority, the Nebula Device with the lowest MAC address will then become the root Nebula Device. The lower the numeric value you assign, the higher the priority for this bridge. Click **Set the bridge priority for another switch** to create a new entry. Select the Nebula Devices for which you want to configure the bridge priority, and select a value from the drop-down list box.
Quality of service	
Quality of service	Enter a VLAN ID and select the priority level that the Nebula Device assigns to frames belonging to this VLAN. Enter a descriptive name for the QoS (Quality of Service). Click **Add** to create a new entry.
Port mirroring	

Table 86 Site-wide > Configure > Switches > Switch settings (continued)

LABEL	DESCRIPTION
Port mirroring	Click **Add** to create a new entry. Select the Nebula Device/stacking system for which you want to configure port mirroring, specify the destination port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original ports, and also enter the source port on which you mirror the traffic. If the port is on a stacking Nebula Device, enter the slot ID/port number to specify the destination and source ports. For example, to specify slot ID 2 port 20 in a stacking system, enter '2/20'.
Err-disable recovery	
Err-disable recovery	Enter the number of seconds (from 30 to 86400) to wait to activate a port or allow specific packets on a port, after the loop guard / BPDU guard error was gone. The loop guard feature shuts down a port if it detects that packets sent out on that port loop back to the Nebula Device. The BPDU guard feature allows you to prevent any new STP-aware (Spanning Tree Protocol) switch from connecting to an existing network and causing STP topology changes in the network. If there is any BPDU detected on the ports on which BPDU guard is enabled, the Nebula Device disables the ports automatically. • **Loop guard** recovery is always enabled. • Click the switch to enable **BPDU guard** recovery. Default setting is disabled. • The range of **Expiration time (seconds)** for both **Loop guard** recovery and **BPDU guard** recovery is 30 to 86400.
Voice VLAN	
Voice VLAN	Select **On** to enable the Voice VLAN feature on the Nebula Device. Otherwise, select **Off**. It groups the voice traffic with defined priority into an assigned VLAN which enables the separation of voice and data traffic coming into the Nebula Device port.
Voice VLAN ID	Enter a VLAN ID number.
Priority	Select the priority level of the Voice VLAN from 1 to 6.
Assign VLAN by	Select how the Nebula Device assigns ports connected to VoIP devices to the Voice VLAN. **OUI** (Organizationally Unique Identifier): The Nebula Device assigns a port connected to a VoIP device to the Voice VLAN if the connected device's OUI matches any OUI in the list. **LLDP-MED**: The Nebula Device assigns a port connected to a VoIP device to the voice VLAN if the connected device is identified as a VoIP device using the LLDP-MED protocol. Note: The connected device must support LLDP-MED and have LLDP-MED enabled.
OUI	This field appears when you select **OUI** in the **Assign VLAN by** field. Click **Add OUI on this network** to add an OUI and a description for the OUI. An Organizationally Unique Identifier identifies a manufacturer. Typically, a device's OUI is the first three octets of the device's MAC address. For example, if you have an IP phone from Company A with MAC address 00:0a:95:9d:68:16, you can enter OUI *00:0a:95* to match all devices from Company A.
DSCP	This field appears when you select **LLDP-MED** in the **Assign VLAN by** field. Enter the Differentiated Services Code Point (DSCP) value for traffic on the voice VLAN. The value is defined from 0 through 63, and 0 is the default.
Vendor ID based VLAN	

Table 86   Site-wide > Configure > Switches > Switch settings (continued)

LABEL	DESCRIPTION
Vendor ID based VLAN	Select **On** to enable the Vendor ID based VLAN feature on the Nebula Device. Otherwise, select **Off**. Click the **Add Vendor-ID on this network** button to define the vendor MAC address OUI, assign to which VLAN, and set the priority. Enter a descriptive name for the Vendor ID based VLAN. Enter up to 64 characters for this field including special characters inside the square quotes [~!@#$%^&*()_+{}|:”<>–=[]\;’,/].
Access management	
Access management	Select **On** to enable the access management feature on the Nebula Device. Otherwise, select **Off**.
Allow IP range	Click the **Add allow IP range** button to set the connected devices’ starting and ending IP addresses that will be allowed to access the Nebula Devices through telnet, SSH, HTTP, HTTPS, and FTP.
DHCP Server Guard	
DHCP Server Guard	Select **On** to enable the DHCP server guard feature on the Nebula Device in order to prevent illegal DHCP servers. Only the first DHCP server that assigned the Nebula Device IP address is allowed to assign IP addresses to devices in this management VLAN. Otherwise, select **Off** to disable it.
IP source guard	
IP source guard	Select **On** to enable IP source guard protection. IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. When the client does not exist in the binding table, the client is unauthorized and traffic will be blocked. To successfully access the network: • Client with static IP address will need to be added to the **Allowed client list** • Client with dynamic IP address will need to get their IP address from an authorized DHCP server.
Protected switch	This shows the Nebula Device/stacking system. • Select **On** to enable IP source guard protection on the Nebula Device/stacking system. Then click **Save**. • Click the edit icon to go to **Site-wide** > **Configure** > **Switches** > **Switch ports** to configure **Protected ports** (see Section 6.3.1 on page 362 for more information). • Click **Run** to display a pop-up window showing the current client table. • Select the DHCP-snooping or Block entries and click **Transfer** to add these to the allowed client list. Then click **Save**.
Allowed client list	This allows the administrator to define a set of clients. Click **Add client** to define the **IPv4 address**, **MAC address**, and **VLAN** of the static client. A previous entry will be overwritten when you enter a duplicate MAC address and VLAN ID. Click **Action** > **Edit** to modify the static client entry. Then click **Update**. The **MAC address** and **VLAN** ID will appear in red when you enter a duplicate entry. Click **Action** > **Delete** to remove the static client entry. Click **Save** to activate the settings. Note: Maximum of 128 static entries is allowed per site.

CHAPTER 7 Security Router

7.1 Overview

This chapter discusses the menus that you can use to monitor the Nebula-managed Security Routers in your network and configure settings even before a Security Router is deployed and added to the site.

A Nebula Security Router is a router firewall that can be managed by Nebula. It is referred to as a Nebula Device in this chapter.

7.2 Monitor

Use the **Monitor** menus to check the Nebula Device information, client information, event log messages and threat report for the Nebula Device in the selected site.

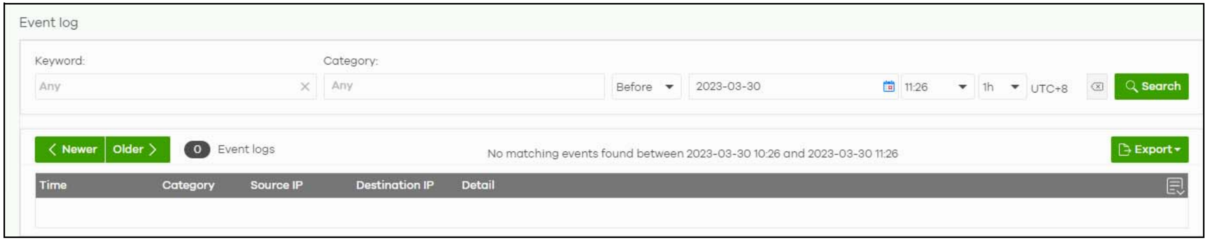
7.2.1 Event Log

Use this screen to view Nebula Device log messages. You can enter a key word, select one or multiple event types, or specify a date/time or a time range to display only the log messages that match these criteria.

Select **Range** to set a time range or select **Before** to choose a specific date/time and the number of hours/minutes to display only the log messages generated within a certain period of time (before the specified date/time). Then click **Search** to update the list of logs based on the search criteria. The maximum allowable time range is 30 days.

Click **Site-wide** > **Monitor** > **Security router** > **Event log** to access this screen.

Figure 131 Site-wide > Monitor > Security router > Event log



Event log

Keyword: Any

Category: Any

Before 2023-03-30 11:26 1h UTC+8

0 Event logs

No matching events found between 2023-03-30 10:26 and 2023-03-30 11:26

Time	Category	Source IP	Destination IP	Detail

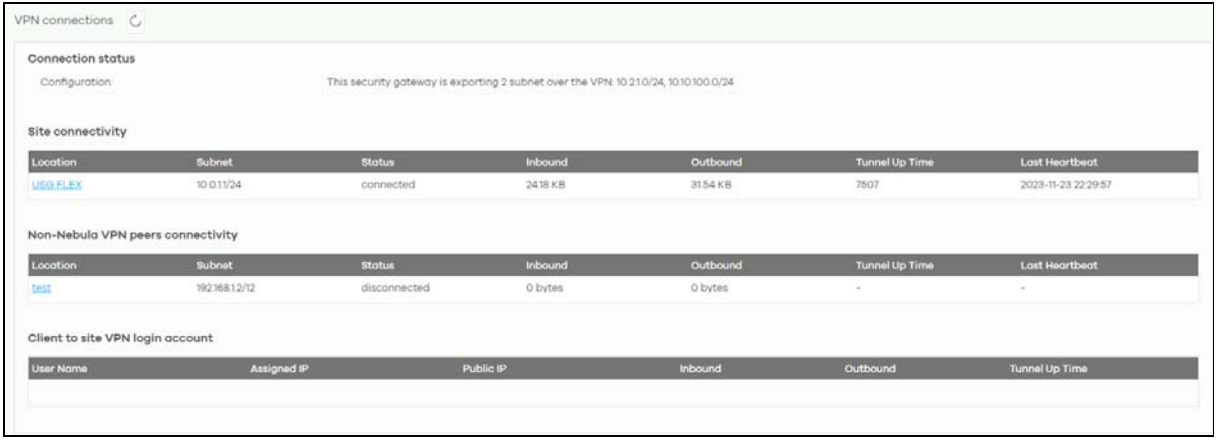
7.2.2 VPN Connections

Use this screen to view the status of site-to-site IPSec VPN connections.

Note: If the peer gateway is not a Nebula Device, go to the **Site-wide** > **Configure** > **Security router** > **Site-to-Site VPN** screen to view and configure a VPN rule. See Section 7.3.5 on page 442 for more information.

Click **Site-wide** > **Monitor** > **Security router** > **VPN connections** to access this screen.

Figure 132 Site-wide > Monitor > Security router > VPN connections



VPN connections

Connection status

Configuration: This security gateway is exporting 2 subnet over the VPN: 10.2.1.0/24, 10.10.100.0/24

Site connectivity

Location	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
USG FLEX	10.0.1.1/24	connected	24.18 KB	31.54 KB	7507	2023-11-23 22:29:57

Non-Nebula VPN peers connectivity

Location	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
test	192.168.1.2/12	disconnected	0 bytes	0 bytes	-	-

Client to site VPN login account

User Name	Assigned IP	Public IP	Inbound	Outbound	Tunnel Up Time

The following table describes the labels in this screen.

Table 87 Site-wide > Monitor > Security router > VPN connections

LABEL	DESCRIPTION
↻	Click this button to reload the data on this page.
Connection Status	
Configuration	This shows the number and address of the local networks behind the Nebula Device, on which the computers are allowed to use the VPN tunnel.
Site Connectivity	
Location	This shows the name of the site to which the Nebula peer gateway is assigned. Click the name to view the **VPN usage and connectivity** status screen.
Subnet	This shows the address of the local networks behind the Nebula peer gateway.
Status	This shows whether the VPN tunnel is connected or disconnected.
Last heartbeat	This shows the last date and time a heartbeat packet is sent to determine if the VPN tunnel is up or down.
Non-Nebula VPN peers connectivity	
Location	This shows the name of the site to which the Non-Nebula peer gateway (Zyxel or non-Zyxel IPSec VPN gateway and Cloud VPN (Azure VPN or AWS VPN)) is assigned. Click the name to go to the **Site-wide** > **Configure** > **Security router** > **Site-to-Site VPN** screen, where you can modify the VPN settings.
Subnet	This shows the address of the local networks behind the Non-Nebula peer gateway.
Status	This shows whether the VPN tunnel is connected or disconnected.
Inbound	This shows the amount of traffic that has gone through the VPN tunnel from the Non-Nebula peer gateway to the Nebula Device since the VPN tunnel was established.
Outbound	This shows the amount of traffic that has gone through the VPN tunnel from the Nebula Device to the Non-Nebula peer gateway since the VPN tunnel was established.
Tunnel up time	This shows how many seconds the VPN tunnel has been active.
Last heartbeat	This shows the last date and time a heartbeat packet was sent to determine if the VPN tunnel is up or down.

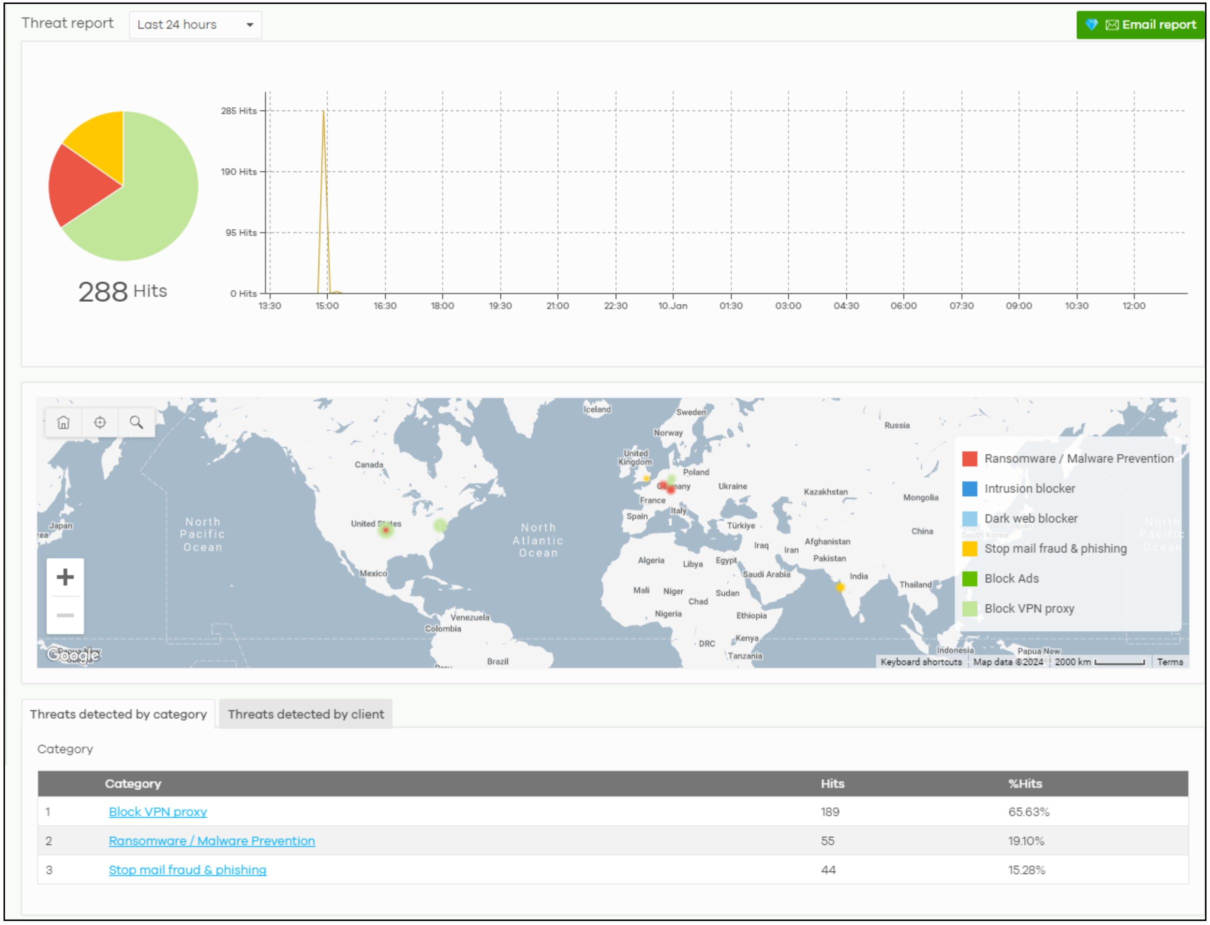
Table 87   Site-wide > Monitor > Security router > VPN connections (continued)

LABEL	DESCRIPTION
Client to site VPN login account See Section 7.3.6 on page 447 for information on configuring the VPN client settings on the Nebula Device. Note: The SCR 50AXE does not support the **Client to site VPN login account** feature.	
User Name	This shows the VPN client's login account name.
Assigned IP	This shows the IP address assigned by the Nebula Device to the VPN client device for use within the VPN tunnel.
Public IP	This shows the public IP address that the VPN client is using to connect to the site.
Inbound	This shows the amount of traffic that has gone through the VPN tunnel from the VPN client to the Nebula Device since the VPN tunnel was established.
Outbound	This shows the amount of traffic that has gone through the VPN tunnel from the Nebula Device to the VPN client since the VPN tunnel was established.
Tunnel up time	This shows how many seconds the VPN tunnel has been active.

7.2.3 Threat Report

Use this screen to view statistics for threat management categories. Click **Site-wide** > **Monitor** > **Security router** > **Threat report** to access this screen.

Figure 133   Site-wide > Monitor > Security router > Threat report



Threats detected by category | Threats detected by client

Category

	Category	Hits	%Hits
1	Block VPN proxy	189	65.63%
2	Ransomware / Malware Prevention	55	19.10%
3	Stop mail fraud & phishing	44	15.28%

The following table describes the labels in this screen.

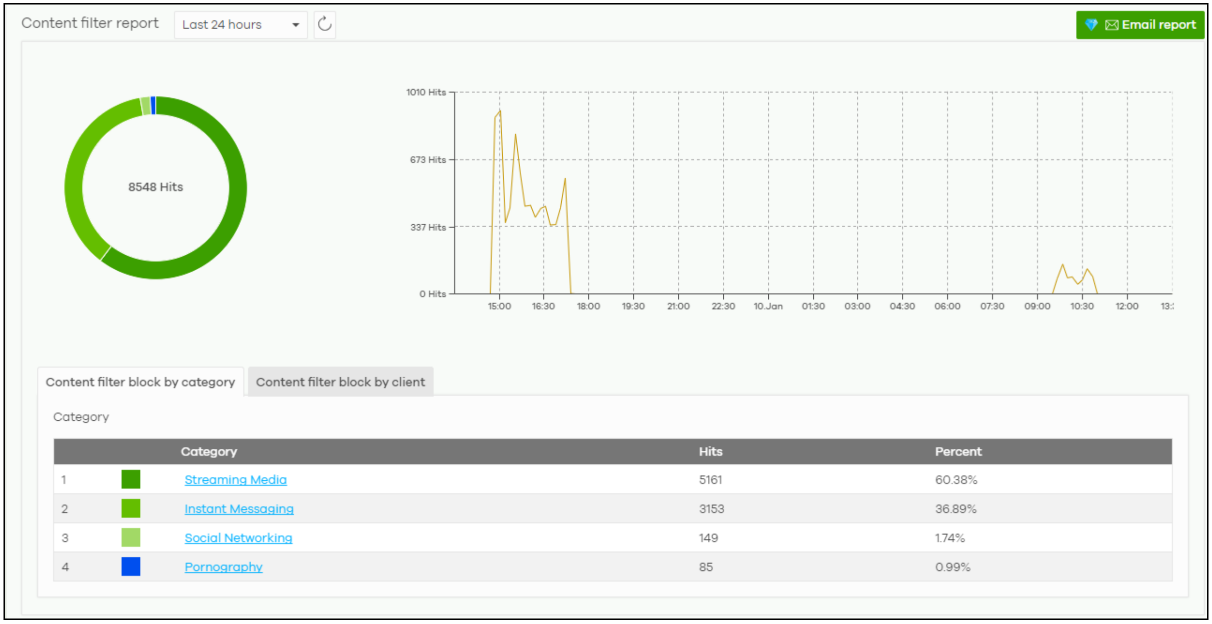
Table 88 Site-wide > Monitor > Security router > Threat report

LABEL	DESCRIPTION
Threat report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time the report will span. You can also select the number of results you want to view in a table. Then, click **Update**.
Email report	Click this button to send threat reports by email, change the logo and set email schedules.
Location	This shows the location on the map where the blocked threats occurred by category.
Threat detected by category	
Category	This shows the name of the category to which the threat belongs.
Domain/IP	This shows the domain name or IP address where the threat was encountered. Click the **Domain/IP** to display the individual category statistics table.
Hits	This shows the amount of hits on a specific threat category.
% Hits	This shows the percentage of the hit counts for the threat encountered by a specific category.
Action	Click **+ Add to Exception** to the domain name or IP address that will bypass the threat management category check. Click **x Remove from Exception** to remove the previously added domain name or IP address that will bypass the threat management category check. Note: A maximum of 50 entries can be added to the exception list.
Threat detected by client	
Description	This shows the name of the client device who encountered a threat. Click the name to display the individual client statistics table.
IPv4 address	This shows the IPv4 address of the client device who encountered a threat.
MAC address	This shows the MAC address of the client device who encountered a threat.
Hits	This shows the number of threat hits of the client device.
% Hits	This shows the percentage of the hit counts encountered by a specific client device.
Action	Click **Block client** to prevent Internet connection to the wired and WiFi LAN client. Click **Unblock Client** to allow the previously blocked wired and WiFi LAN client to connect to the Internet. Note: A maximum of 50 entries can be added to the exception list.

7.2.4 Content Filter Report

Use this screen to view statistics for content filter categories. Click **Site-wide** > **Monitor** > **Security router** > **Content Filter report** to access this screen.

Figure 134 Site-wide > Monitor > Security router > Content Filter report



Category

		Category	Hits	Percent
1	🟩	Streaming Media	5161	60.38%
2	🟩	Instant Messaging	3153	36.89%
3	🟩	Social Networking	149	1.74%
4	🟦	Pornography	85	0.99%

The following table describes the labels in this screen.

Table 89 Site-wide > Monitor > Security router > Content Filter report

LABEL	DESCRIPTION
Content Filter report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time the report will span. You can also select the number of results you want to view in a table. Then, click **Update**.
Email report	Click this button to send content filter reports by email, change the logo, set email format and schedules. Then, click **Save**.
y-axis	The y-axis shows the number of hits on web pages that the Nebula Device's content filter service has blocked.
x-axis	The x-axis shows the time period over which the web page is checked.
Content Filter block by category	
Category	This shows the name of the category to which the web page belongs. Click the **Category** to display the individual category statistics table.
Hits	This shows the amount of hits on a specific content filter block category.
% Hits	This shows the percentage of the hit counts that the Nebula Device's content filter service has blocked by a specific category.
Content Filter block by client	
Description	This shows the name of the client device who's web page was blocked by the Nebula Device's content filter service. Click the name to display the individual client statistics table.
IPv4 address	This shows the IPv4 address of the client device who's web page was blocked by the Nebula Device's content filter service.
MAC address	This shows the MAC address of the client device who's web page was blocked by the Nebula Device's content filter service.
Hits	This shows the number of content filter service blocks of the client device.
% Hits	This shows the percentage of the hit counts encountered by a specific client device.

7.3 Configure

Use the **Configure** menus to configure interface addressing, firewall, site-to-site VPN, captive portal, traffic shaping, authentication server, IPTV, and other gateway settings for the Nebula Device of the selected site.

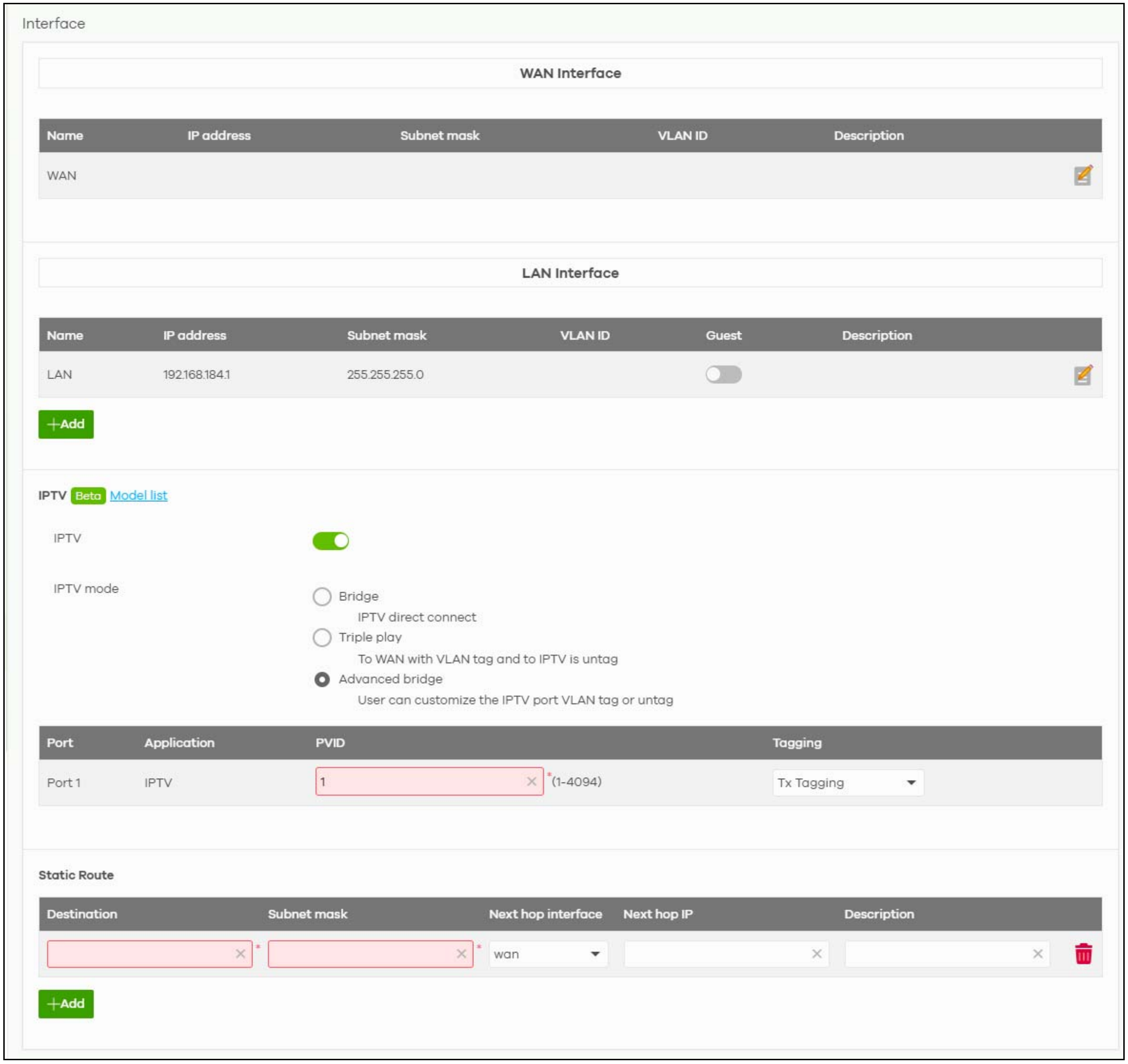
Note: Only one Security Router is allowed per site.

7.3.1 Interface

Use this screen to configure network interfaces on the Nebula Device. An interface consists of a VLAN ID and an IP address, plus other configuration settings.

To access this screen, click **Site-wide** > **Configure** > **Security router** > **Interface**.

Figure 135 Site-wide > Configure > Security router > Interface



Interface

WAN Interface

Name	IP address	Subnet mask	VLAN ID	Description
WAN				

LAN Interface

Name	IP address	Subnet mask	VLAN ID	Guest	Description
LAN	192168.184.1	255.255.255.0		○	

+Add

IPTV Beta Model list

IPTV ●

IPTV mode

○ Bridge
IPTV direct connect
○ Triple play
To WAN with VLAN tag and to IPTV is untag
● Advanced bridge
User can customize the IPTV port VLAN tag or untag

Port	Application	PVID	Tagging
Port 1	IPTV	1 *(1-4094)	Tx Tagging

Static Route

Destination	Subnet mask	Next hop interface	Next hop IP	Description
*	*	wan		

+Add

The following table describes the labels in this screen.

Table 90 Site-wide > Configure > Security router > Interface

LABEL	DESCRIPTION
Interface WAN Interface	
Name	This field is read-only.
IP address	This shows the IP address for this interface.
Subnet mask	This shows the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	This shows the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 2 – 4094. (0, 1 and 4095 are reserved.)
Description	This shows the description of this interface.
✎	Click the edit icon to modify this interface.
LAN Interface	
Name	This field is read-only if you are editing an existing LAN interface. Specify a name for the interface. The format of interface names is strict. Each name consists of 2 – 4 letters (interface type), followed by a number (x). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, VLAN interfaces are vlan0, vlan1, vlan2, and so on.
IP address	This is the IP address for this interface.
Subnet mask	This is the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	This shows the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 2 – 4094. (0, 1 and 4095 are reserved.)
Guest	Click the switch to the right to configure this interface as a Guest interface. Client devices connected to this Guest interface have Internet access but cannot access a non-guest interface. Alternatively, click the switch to the left to disable Internet access for client devices connected to this Guest interface. Note: You cannot turn on the guest interface when the subnet is used by the VPN.
Description	This shows the description of this interface.
✎	Click the edit icon to modify it.
Add	Click this button to create a new LAN interface.
IPTV	The following fields are available only when **IPTV** is enabled. Note: Nebula SCR 50AXE does not support IPTV.
IPTV	Click the switch to the right to turn on the IPTV (Internet Protocol Television) service. IPTV is a service that delivers video traffic over an Internet Protocol (IP) network connection.

Table 90 Site-wide > Configure > Security router > Interface (continued)

LABEL	DESCRIPTION
IPTV mode	Select **Bridge** mode when your IPTV service provider does not use a VLAN tag for the IPTV multicast traffic. Note: At the time or writing, Port 1 is the IPTV port. Select **Triple play** mode when your IPTV service provider uses a VLAN tag for the IPTV multicast traffic. The Nebula Device will tag outgoing traffic from port 1 with the IPTV service provider VLAN tag. Select **Advanced bridge** mode when a manageable Switch is connected to port 1 of the Nebula Device for IPTV traffic and Internet access. Make sure to assign a different VLAN ID for IPTV traffic.
Port 1	This field is available only when the **IPTV mode** is set to **Bridge**. Multicast traffic from the IPTV server on the Internet goes through the Nebula Device to port 1 only. This field is read-only.
VLAN ID	This field is available only when the **IPTV mode** is set to **Triple play**. Configure the IPTV VLAN ID, for example 4081. The Nebula Device will tag traffic from port 1 with the IPTV VLAN tag going to the Internet. Allowed values are 2 – 4094. (0, 1 and 4095 are reserved.) Note: The IPTV VLAN ID must not conflict with other VLAN IDs on the WAN or LAN interface.
Priority (802.1P)	This field is available only when the **IPTV mode** is set to **Triple play**. Enter the 802.1p number your IPTV service provider gave you to prioritize IPTV traffic. “0” is the lowest priority level and “7” is the highest. Note: At the time of writing, IPTV video traffic’s priority depends on the 802.1p number your IPTV service provider gave you.
Port	This field is available only when the **IPTV mode** is set to **Advanced bridge**. Multicast traffic from the IPTV server on the Internet goes through the Nebula Device to port 1 only. This field is read-only.
Application	This field is available only when the **IPTV mode** is set to **Advanced bridge**. Multicast traffic from the IPTV server on the Internet goes through the Nebula Device. This field is read-only.
PVID	This field is available only when the **IPTV mode** is set to **Advanced bridge**. Configure the IPTV VLAN ID, for example 4081. The Nebula Device will tag traffic from port 1 with the IPTV VLAN tag going to the Internet. Allowed values are 2 – 4094. (0, 1 and 4095 are reserved.) When the multicast traffic is through the WAN (Internet) then it is untagged. Note: The IPTV VLAN ID must not conflict with other VLAN IDs on the WAN or LAN interface.
Tagging	This field is available only when the **IPTV mode** is set to **Advanced bridge**. Select **Tx Tagging** for the connected manageable Switch to forward IPTV-tagged traffic to the subscribers. If you do not have a connected manageable Switch, select **Tx Untag** or select **Bridge** mode in **IPTV mode**.
Static Route	
Destination	Enter the destination IP address.

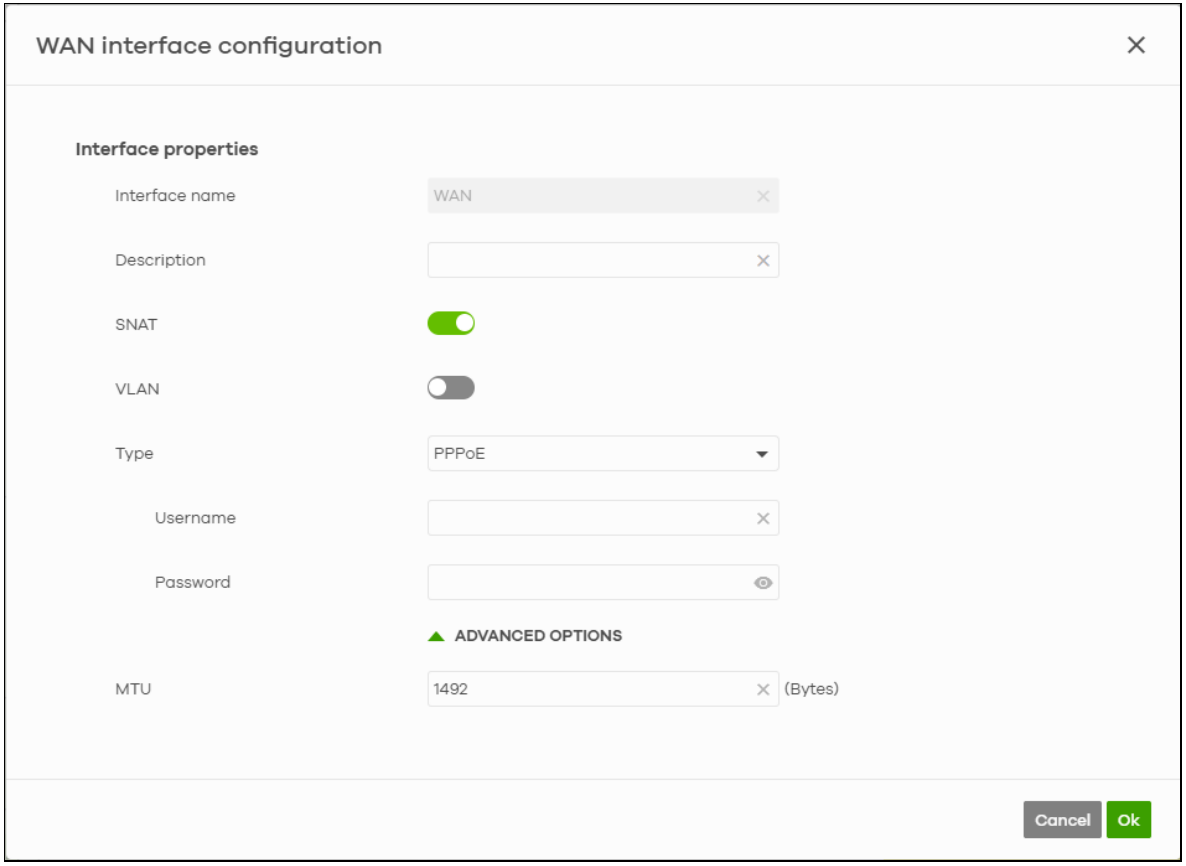
Table 90 Site-wide > Configure > Security router > Interface (continued)

LABEL	DESCRIPTION
Subnet mask	Enter an IP subnet mask. The route applies to all IP addresses in the subnet.
Next hop interface	Select the interface you want to send all traffic to.
Next hop IP	Enter the IP address of the next-hop gateway.
Description	This is the descriptive name of the static route, maximum up to 255 alphanumeric characters.
✎	Click this icon to modify a static route.
🗑	Click this icon to remove a static route.
Add	Click this button to create a new static route, maximum up to 20.

7.3.1.1 WAN Interface Configuration

Click the **Edit** button in the **WAN Interface** section to open the **Security router** > **Configure** > **Interface** > **WAN interface configuration** screen.

Figure 136 Site-wide > Configure > Security router > Interface > WAN interface configuration



WAN interface configuration

Interface properties

Interface name: WAN

Description:

SNAT: on

VLAN: off

Type: PPPoE

Username:

Password:

ADVANCED OPTIONS

MTU: 1492 (Bytes)

The following table describes the labels in this screen.

Table 91 Site-wide > Configure > Security router > Interface > WAN interface configuration

LABEL	DESCRIPTION
Interface properties	
Interface name	This field is read-only.

Table 91 Site-wide > Configure > Security router > Interface > WAN interface configuration (continued)

LABEL	DESCRIPTION
Description	Enter a description of the WAN interface here. You can use alphanumeric and ()+/ :=?!*#@$_%– characters, and it can be up to 512 characters long.
SNAT	Select this to enable SNAT. When enabled, the Nebula Device rewrites the source address of packets being sent from this interface to the interface's IP address.
VLAN	Select On to enable the VLAN feature on the WAN interface. Otherwise, select Off.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 2 – 4094. (0, 1 and 4095 are reserved.)
Type	Select the type of interface to create. **DHCP**: The interface will automatically get an IP address and other network settings from a DHCP server. **Static**: You must manually configure an IP address and other network settings for the interface. **PPPoE**: The interface will authenticate with an Internet Service Provider, and then automatically get an IP address from the ISP's DHCP server. You can use this type of interface to connect to a DSL modem. **PPPoE with static IP**: Assign a static IP address to the WAN interface and your WAN interface is getting an Internet connection from a PPPoE server.
IP address assignment	These fields are displayed if you select **Static**.
IP address	Enter the static IP address of this interface.
Subnet mask	Enter the subnet mask for this interface's IP address.
Default gateway	Enter the IP address of the Nebula Device through which this interface sends traffic.
First DNS server	Enter a DNS server's IP address. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Nebula Device uses the first and second DNS servers, in that order to resolve domain names for VPN, DDNS and the time server. Leave the field blank if you do not want to configure DNS servers.
Second DNS server	Enter the IP address of another DNS server. This field is optional.
These fields are displayed if you selected **PPPoE** or **PPPoE with static IP**.	
Username	Enter the user name provided by your ISP. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed.
Password	Enter the password provided by your ISP. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
IP address assignment	
IP address	Enter the static IP address of this interface.
DNS server	Enter a DNS server's IP address. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Nebula Device uses the first and second DNS servers, in that order to resolve domain names for VPN, DDNS and the time server. Leave the field blank if you do not want to configure DNS servers.
ADVANCED OPTIONS	
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Nebula Device divides it into smaller fragments. Allowed values are 1280 – 1500 for static IP/DHCP; 1280 – 1492 for PPPoE/PPPoE with static IP.

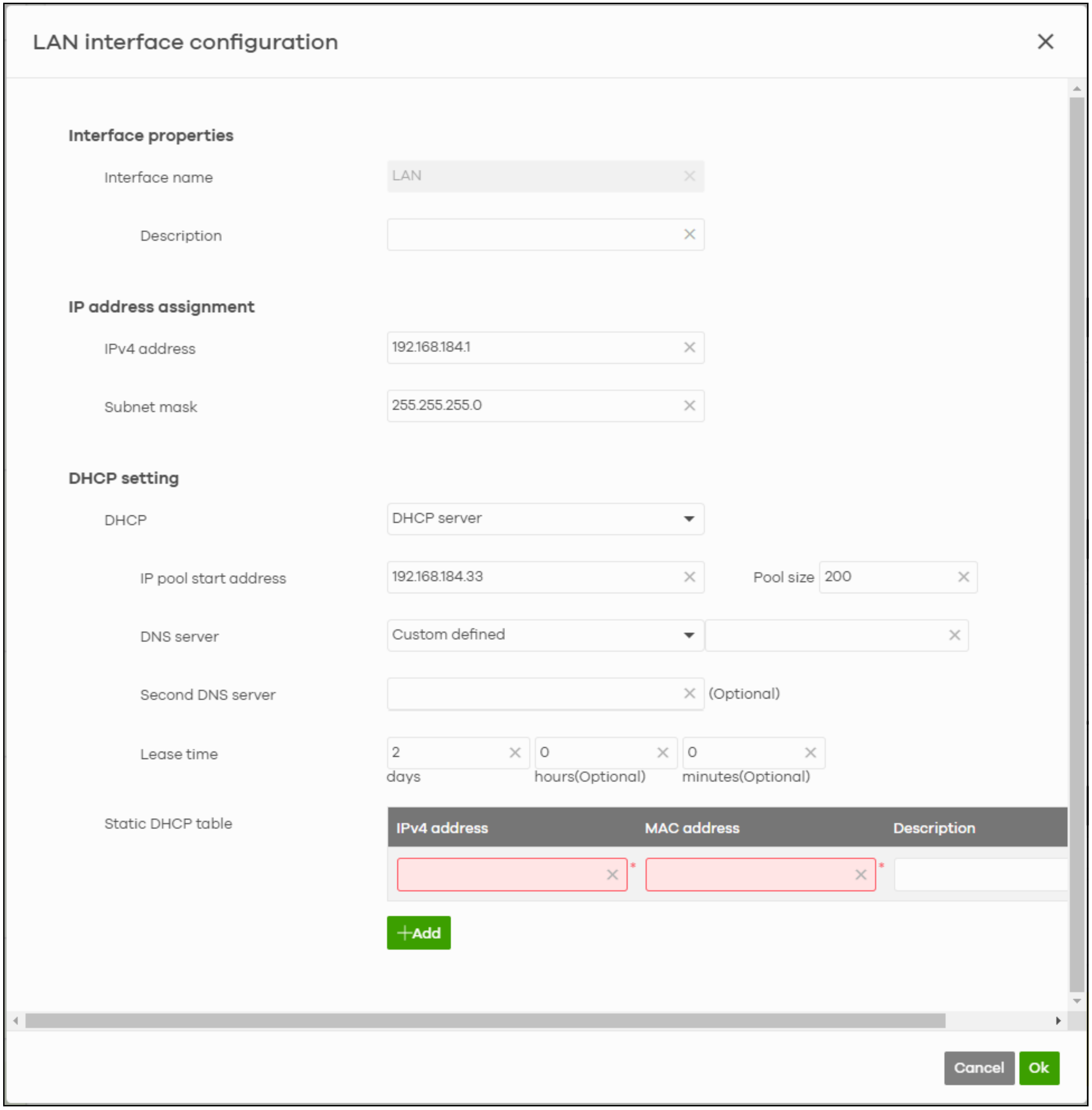
Table 91 Site-wide > Configure > Security router > Interface > WAN interface configuration (continued)

LABEL	DESCRIPTION
DHCP option 60	This field is available only when the **Type** is set to **DHCP**. DHCP option 60 is used by the Nebula Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Nebula Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Enter a string using up to 63 of these characters [a–z A–Z 0–9 !\"#$%&\'()*+,-./ :;<=>?@\[\\\]^_`{}] to identify this Nebula Device to the DHCP server. For example, Zyxel-TW.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

7.3.1.2 LAN Interface Configuration

Click the **Add** button or click the **Edit** button in the **LAN interface** section to open the **Site-wide** > **Configure** > **Security router** > **Interface** > **LAN interface configuration** screen.

Figure 137 Site-wide > Configure > Security router > Interface > LAN interface configuration



LAN interface configuration

Interface properties

Interface name	LAN
Description	

IP address assignment

IPv4 address	192.168.184.1
Subnet mask	255.255.255.0

DHCP setting

DHCP	DHCP server
IP pool start address	192.168.184.33 Pool size 200
DNS server	Custom defined
Second DNS server	(Optional)
Lease time	2 days, 0 hours(Optional), 0 minutes(Optional)

Static DHCP table

IPv4 address	MAC address	Description
*	*	

The following table describes the labels in this screen.

Table 92   Site-wide > Configure > Security router > Interface > LAN interface configuration

LABEL	DESCRIPTION
Interface properties	
Interface name	Specify a name for the LAN interface. Enter up to 15 alphanumeric characters. Note: The following reserved interface names in lowercase are not allowed. For example, 'vlan' or 'vlanxx' are not allowed, but 'VLAN or 'VLANxx' are allowed. • ethernet • ppp • vlan • bridge • virtual • wlan • cellular • aux • tunnel • status • summary • all
Description	Enter a description of the LAN interface here. You can use alphanumeric and ()+/:=?!*#@$_%– characters, and it can be up to 512 characters long.
IP address assignment	
IPv4 address	Enter the IPv4 address for this interface.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
DHCP setting DHCP	Select what type of DHCP service the Nebula Device provides to the network. Choices are: **None** – the Nebula Device does not provide any DHCP services. There is already a DHCP server on the network. **DHCP relay** – the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network. **DHCP server** – the Nebula Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Nebula Device is the DHCP server for the network.
This field appear if the Nebula Device is a DHCP Relay.	
DHCP server	Enter the IP address of a DHCP server for the network.
These fields appear if the Nebula Device is a DHCP Server.	
IP pool start address	Enter the IP address from which the Nebula Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the **Static DHCP table**. If this field is blank, the **Pool size** must also be blank. In this case, the Nebula Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.

Table 92 Site-wide > Configure > Security router > Interface > LAN interface configuration (continued)

LABEL	DESCRIPTION
DNS server	Specify the IP addresses of up to two DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom defined** – enter a static IP address. **From ISP** – select the DNS server that another interface received from its DHCP server. **This Router** – the DHCP clients use the IP address of this interface and the Nebula Device works as a DNS relay.
Second DNS server	Enter the IP address of another DNS server. This field is optional. Note: This field appears only when you select **Custom Defined** in **DNS Server**.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. **days, hours, and minutes (Optional)** – enter how long IP addresses are valid. Note: The minimum **Lease time** is 1 day and the maximum is 360 days.
Static DHCP table	Configure a list of static IP addresses the Nebula Device assigns to computers connected to the interface. Otherwise, the Nebula Device assigns an IP address dynamically using the interface's **IP pool start address** and **Pool size**.
IPv4 address	Enter the IPv4 address to assign to a device with this entry's MAC address.
MAC address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%– characters, and it can be up to 60 characters long.
🗑	Select an entry in this table and click this to delete it. This will also remove the client information on the **Site-wide** > **Clients** > **Client list**.
+Add	Click this to create an entry in the **Static DHCP table**. This will also add the client reserve IP policy on the **Site-wide** > **Clients** > **Client list**.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

7.3.1.3 IPTV Scenarios

The Nebula Device forwards IPTV multicast traffic to IPTV subscribers connected to port 1. The following are the supported IPTV scenarios:

- Your IPTV service provider does not use a VLAN tag for the IPTV multicast traffic.
- Your IPTV service provider uses a VLAN tag for the IPTV multicast traffic.
- Your IPTV service provider uses a VLAN tag for the IPTV multicast traffic and you have a VLAN-aware Switch in your network connected to port 1 of the Nebula Device.
- The Set Top Box tags IPTV traffic with a VLAN tag for IPTV multicast traffic. You also have a VLAN-aware Switch connected to port 1 of the Nebula Device.

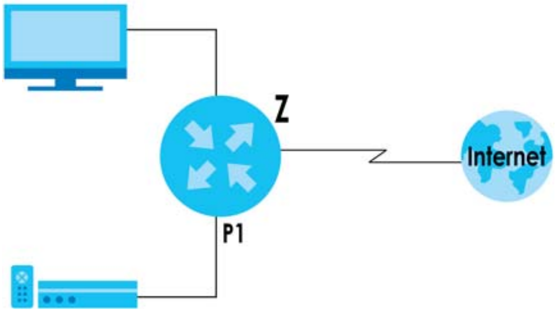
Note: Connect the IPTV subscribers to port 1 of the Nebula Device only.

7.3.1.4 IPTV Scenario Configurations

IPTV Bridge (IPTV Direct)

In this scenario, your IPTV service provider does not use a VLAN tag for the IPTV multicast traffic. Connect the IPTV subscriber to port 1 (**P1**) of the Nebula Device (**Z**). IPTV multicast traffic from the IPTV server on the Internet goes through the Nebula Device (**Z**) to this port (**P1**) only.

Figure 138 IPTV Bridge Application



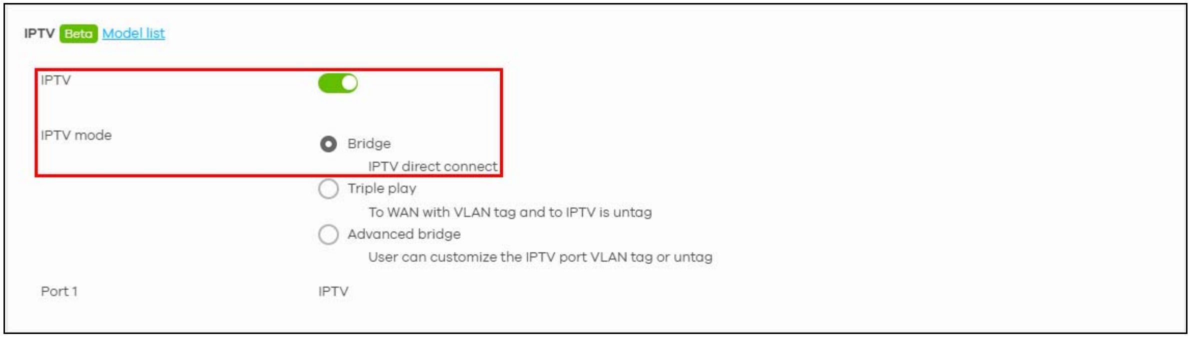
On NCC, do the following:

1 Go to **Site-wide** > **Configure** > **Security router** > **Interface**.

2 Click the **IPTV** switch to the right.

3 Select **Bridge** in **IPTV mode**.

Figure 139 Site-wide > Configure > Security router > Interface: Bridge Mode



IPTV Beta Model list

IPTV: on

IPTV mode:
- ● Bridge
  IPTV direct connect
- ○ Triple play
  To WAN with VLAN tag and to IPTV is untag
- ○ Advanced bridge
  User can customize the IPTV port VLAN tag or untag

Port 1: IPTV

IPTV Triple Play (IPTV with VLAN Tag)

In this scenario, your IPTV service provider uses a VLAN tag for the IPTV multicast traffic. The Nebula Device will tag outgoing traffic from port 1 (**P1**) with the IPTV service provider VLAN tag that you configured in NCC.

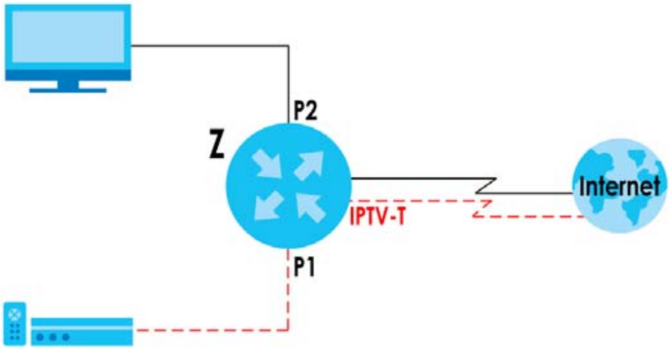
Configure an IPTV VLAN ID, for example **4081**, on the Nebula Device (**Z**), so that the Nebula Device (**Z**) will tag traffic from port 1 (**P1**) with the IPTV VLAN tag going to the Internet.

In the following figure, **IPTV-T** is the IPTV service provider VLAN tag.

Note: The IPTV VLAN ID must not conflict with other VLAN IDs on the WAN or LAN interface.

If your IPTV service provider gave you an 801.1p number to prioritize IPTV traffic, you may also configure it in the Nebula Device (**Z**).

Figure 140 IPTV Triple Play Application



On NCC, do the following:

1 Go to **Site-wide** > **Configure** > **Security router** > **Interface**.

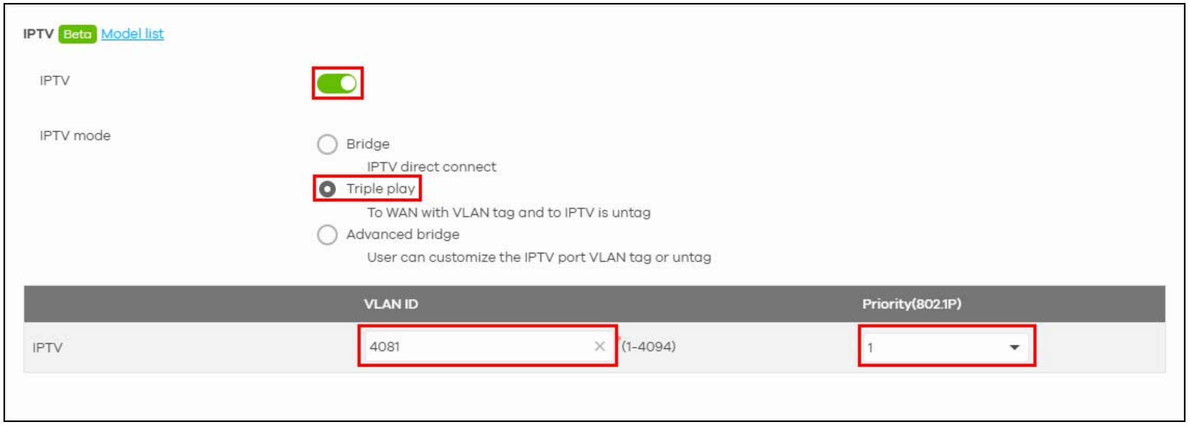
2 Click the **IPTV** switch to the right.

3 Select **Triple Play** in **IPTV mode**.

4 Enter **4081** in **VLAN ID**.

5 Select **1** in **Priority**.

Figure 141 Site-wide > Configure > Security router > Interface: Triple Play Mode



IPTV Beta Model list

IPTV ● (on)

IPTV mode
○ Bridge
IPTV direct connect
● Triple play
To WAN with VLAN tag and to IPTV is untag
○ Advanced bridge
User can customize the IPTV port VLAN tag or untag

	VLAN ID		Priority(802.1P)
IPTV	4081	(1-4094)	1

IPTV Advanced VLAN 1

In this scenario, your IPTV service provider uses a VLAN tag for the IPTV multicast traffic and you have a VLAN-aware Switch (**S**) in your network connected to port 1 (**P1**) of the Nebula Device. For this example scenario, connect the IPTV subscribers to a VLAN-aware Switch (**S**) that is connected to port 1 (**P1**) of the Nebula Device (**Z**).

Then make the following configurations:

- Configure the VLAN-aware Switch (**S**) to tag egress (outgoing) traffic going to port 1 (**P1**) on the Nebula Device (**Z**) with the IPTV service provider VLAN tag.

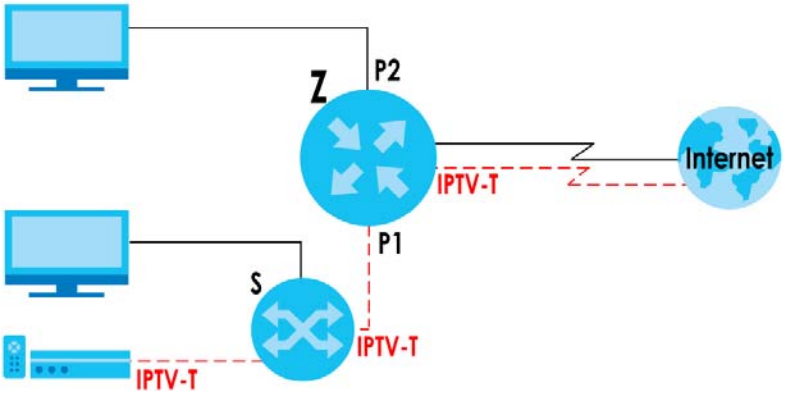
- Configure the Nebula Device (**Z**) to allow TX Tagging for incoming tagged traffic coming from the Switch and going to the Internet.

In the following figure, **IPTV-T** is the IPTV service provider VLAN tag.

Note: The IPTV VLAN ID must not conflict with other VLAN IDs on the WAN or LAN interface.

If your IPTV service provider gave you an 801.1p number to prioritize IPTV traffic, you may also configure it in the Nebula Device (**Z**).

Figure 142 IPTV Advanced VLAN 1 Application



On NCC, do the following:

1 Go to **Site-wide** > **Configure** > **Security router** > **Interface**.

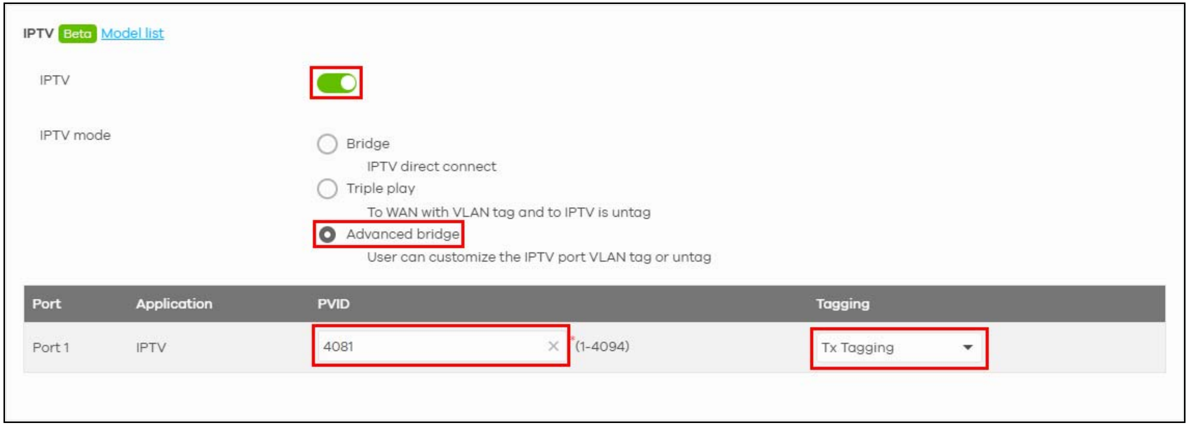
2 Click the **IPTV** switch to the right.

3 Select **Advanced bridge** in **IPTV mode**.

4 Enter **4081** in **PVID**.

5 Select **TX Tagging** in **Tagging**.

Figure 143 Site-wide > Configure > Security router > Interface: Advanced VLAN 1



IPTV Beta Model list

IPTV: on

IPTV mode:
○ Bridge
IPTV direct connect
○ Triple play
To WAN with VLAN tag and to IPTV is untag
● Advanced bridge
User can customize the IPTV port VLAN tag or untag

Port	Application	PVID	Tagging
Port 1	IPTV	4081 (1-4094)	Tx Tagging

IPTV Advanced VLAN 2

In this scenario, the Set Top Box (**STB**) tags IPTV traffic with a VLAN tag for IPTV multicast traffic. You also have a VLAN-aware Switch (**S**) connected to port 1 (**P1**) of the Nebula Device (**Z**). For this example scenario, connect the IPTV subscribers to a VLAN-aware Switch (**S**) that is connected to port 1 (**P1**) of the Nebula Device (**Z**).

Then make the following configurations:

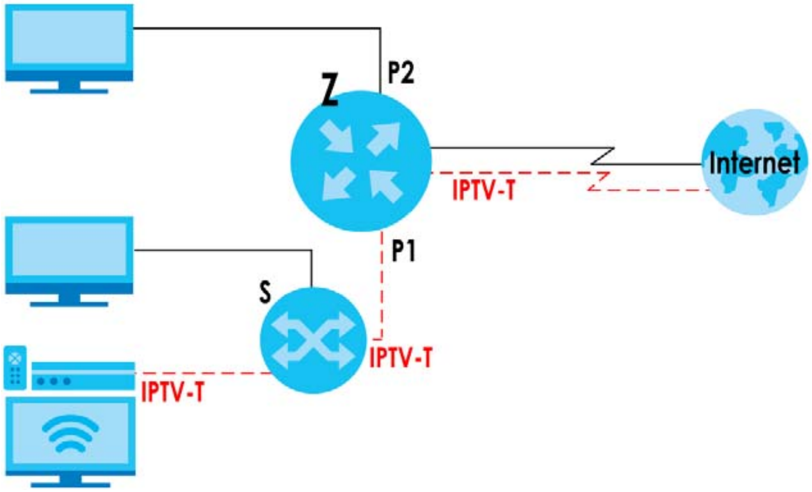
- Configure the VLAN-aware Switch (**S**) to forward IPTV-tagged traffic coming from the STB subscribers and going to the Switch (**S**).
- Configure the Nebula Device (**Z**) to also allow TX Tagging for tagged traffic coming from the Switch and going to the Internet.

In the following figure, **IPTV-T** is the IPTV service provider VLAN tag.

Note: The IPTV VLAN ID must not conflict with other VLAN IDs on the WAN or LAN interface.

If your IPTV service provider gave you an 801.1p number to prioritize IPTV traffic, you may also configure it in the Nebula Device (**Z**).

Figure 144 IPTV Advanced VLAN 2 Application



On NCC, do the following:

1 Go to **Site-wide** > **Configure** > **Security router** > **Interface**.

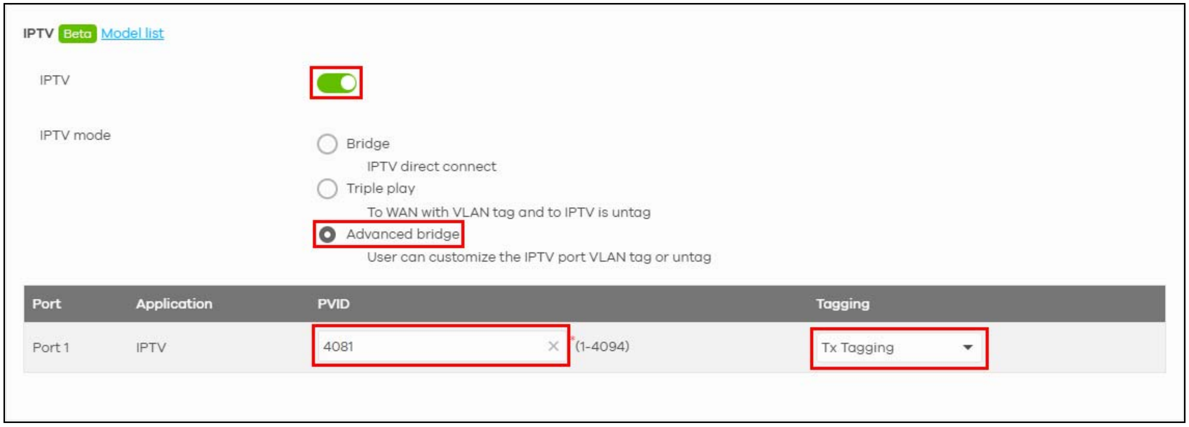
2 Click the **IPTV** switch to the right.

3 Select **Advanced bridge** in **IPTV mode**.

4 Enter **4081** in **PVID**.

5 Select **TX Tagging** in **Tagging**.

Figure 145 Site-wide > Configure > Security router > Interface: Advanced VLAN 2


IPTV Beta Model list

IPTV: ON

IPTV mode:
- ○ Bridge
  IPTV direct connect
- ○ Triple play
  To WAN with VLAN tag and to IPTV is untag
- ● Advanced bridge
  User can customize the IPTV port VLAN tag or untag

Port	Application	PVID	Tagging
Port 1	IPTV	4081 (1-4094)	Tx Tagging

7.3.2 Threat Management

Use this screen to enable the threat management categories such as:

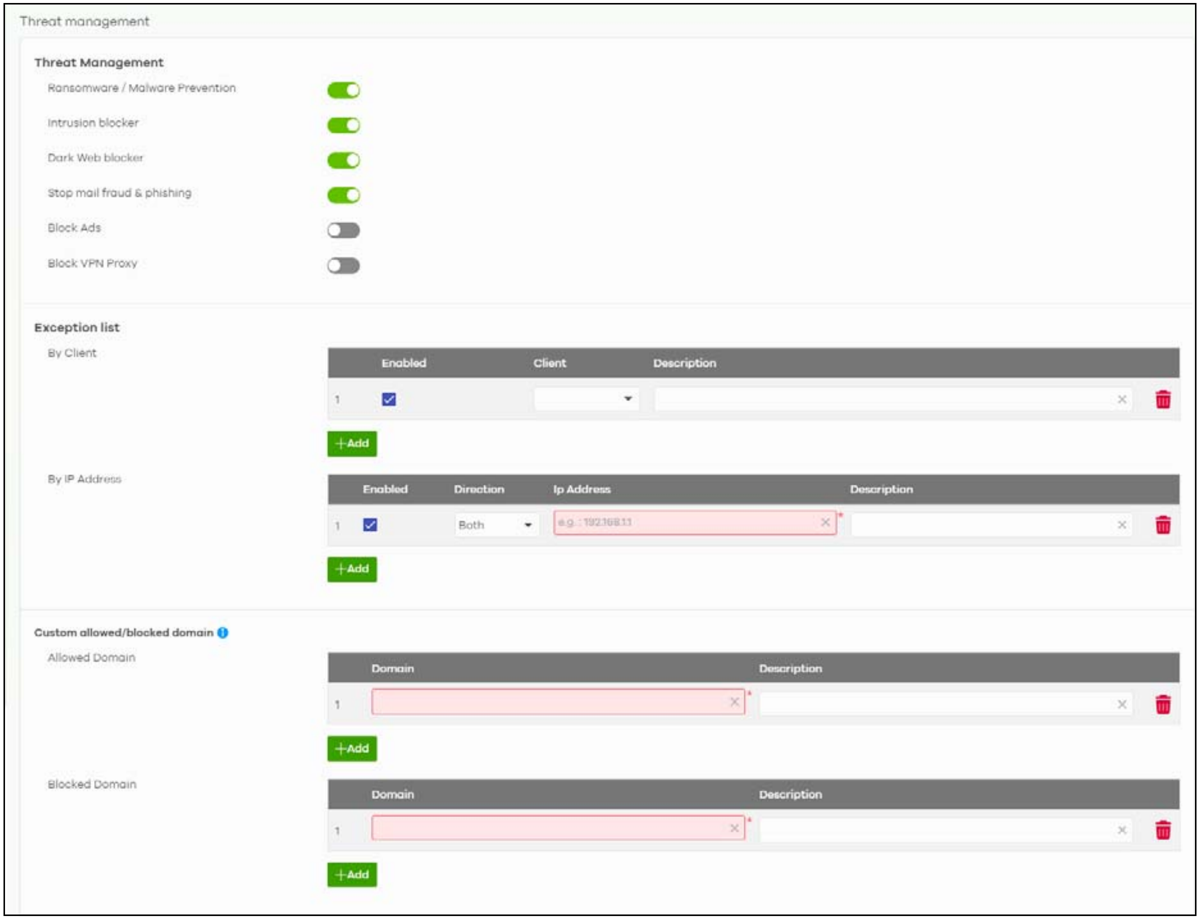
- Ransomware and malware prevention that protects LAN clients from accessing or downloading harmful web contents.
- Intrusion blocker that prevents personal data theft in your network.
- Dark Web blocker that prevents unauthorized access from TOR proxies to the LAN clients.
- Stop mail fraud and phishing that blocks access by your LAN clients to phishing websites and SPAM URLs.
- Ads blocker that prevents access to websites containing annoying advertisements with links to harmful programs.
- VPN proxy blocker that prevents LAN clients connected to the Nebula Device from sending personal data to a cybercriminal's VPN gateway.

You can also configure the following:

- Up to 50 exception list, using the Nebula Device connected client device's name or IP address
- Up to 50 allowed domain name list
- Up to 50 blocked domain name list.

Click **Site-wide** > **Configure** > **Security router** > **Threat management** to access this screen.

Figure 146 Site-wide > Configure > Security router > Threat management



Threat management

Threat Management

- Ransomware / Malware Prevention: ON
- Intrusion blocker: ON
- Dark Web blocker: ON
- Stop mail fraud & phishing: ON
- Block Ads: OFF
- Block VPN Proxy: OFF

Exception list

By Client

	Enabled	Client	Description
1	☑		

+Add

By IP Address

	Enabled	Direction	Ip Address	Description
1	☑	Both	e.g.: 192.168.1.1	

+Add

Custom allowed/blocked domain

Allowed Domain

	Domain	Description
1		

+Add

Blocked Domain

	Domain	Description
1		

+Add

The following table describes the labels in this screen.

Table 93 Site-wide > Configure > Security router > Threat management

LABEL	DESCRIPTION
Threat management	
Ransomware / Malware	Ransomware and malware prevention protects the LAN clients connected to the Nebula Device from accessing or downloading harmful web content. These contents may contain files that could harm your operating system and personal files. Click the switch to enable ransomware/malware protection on the Nebula Device.
Intrusion blocker	Intrusion blocker prevents cybercriminals from harming, spying, or stealing personal data in your network. Click the switch to enable intrusion blocker protection on the Nebula Device.
Dark Web blocker	The Dark Web is an anonymous network accessed by browsers such as TOR. The purpose of the Dark Web is to enable anonymous access to content and prevent the identification of both the request and destination. The dark web blocker prevents unauthorized access from TOR proxies to the LAN clients connected to the Nebula Device. Click the switch to enable dark web blocker protection on the browsers of LAN clients connected to the Nebula Device.
Stop mail fraud & phishing	Mail fraud and phishing sites protection blocks access by your LAN clients to phishing websites and spam URLs. Click the switch to enable mail fraud and phishing protection on the browsers of LAN clients connected to the Nebula Device.

Table 93 Site-wide > Configure > Security router > Threat management (continued)

LABEL	DESCRIPTION
Block Ads	Ad blocking or ad filtering prevents exposure to websites containing advertisements with links to harmful programs. Click the switch to enable ads blocker protection on the browsers of LAN clients connected to the Nebula Device.
Block VPN Proxy	VPN proxy blocker prevents the LAN clients connected to the Nebula Device from sending personal data to a cybercriminal's VPN gateway. Click the switch to enable VPN proxy blocker protection on the browsers of LAN clients connected to the Nebula Device.
Exception list	Both wired and WiFi LAN clients connected to the Nebula Device in this list will bypass the threat management category check. Note: A maximum of 50 entries can be added to the exception list.
By Client	**Enabled** – Select this option to turn on this client exception profile. This allows both wired and WiFi LAN clients connected to the Nebula Device to bypass the threat management category check. Select the **Client** from the drop-down list. See Section 4.5.0.1 on page 261 and Section 4.5.0.2 on page 264 for more information on WiFi and wired clients. Enter a **Description** of the allowed client. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 512 characters long.
🗑	Click this icon to remove the client exception profile.
Add	Click this to create a client exception profile.
By IP Address	**Enabled** – Select this option to turn on this IPv4 address exception profile. This allows the client with this IPv4 address to bypass the threat management category check. **Direction** – Select **Both** to allow incoming/outgoing packets to/from the Nebula Device that match this IPv4 address. Select **Source** to allow incoming packets to the Nebula Device that match this IPv4 address. Select **Destination** to allow outgoing packets from the Nebula Device that match this IPv4 address. Add the **IP Address** that the Nebula Device will allow incoming and/or outgoing packets. Enter a description of the allowed IPv4 address. The description can be up to 512 characters long.
🗑	Click this icon to remove the IPv4 address exception profile.
Add	Click this icon to create an IPv4 address exception profile.
Custom allowed/ blocked domain	Create a list of host names to allow access to, or block access to, regardless of their content rating. Note: A maximum of 50 entries can be added to the **Allowed Domain** and **Blocked Domain** lists.

Table 93 Site-wide > Configure > Security router > Threat management (continued)

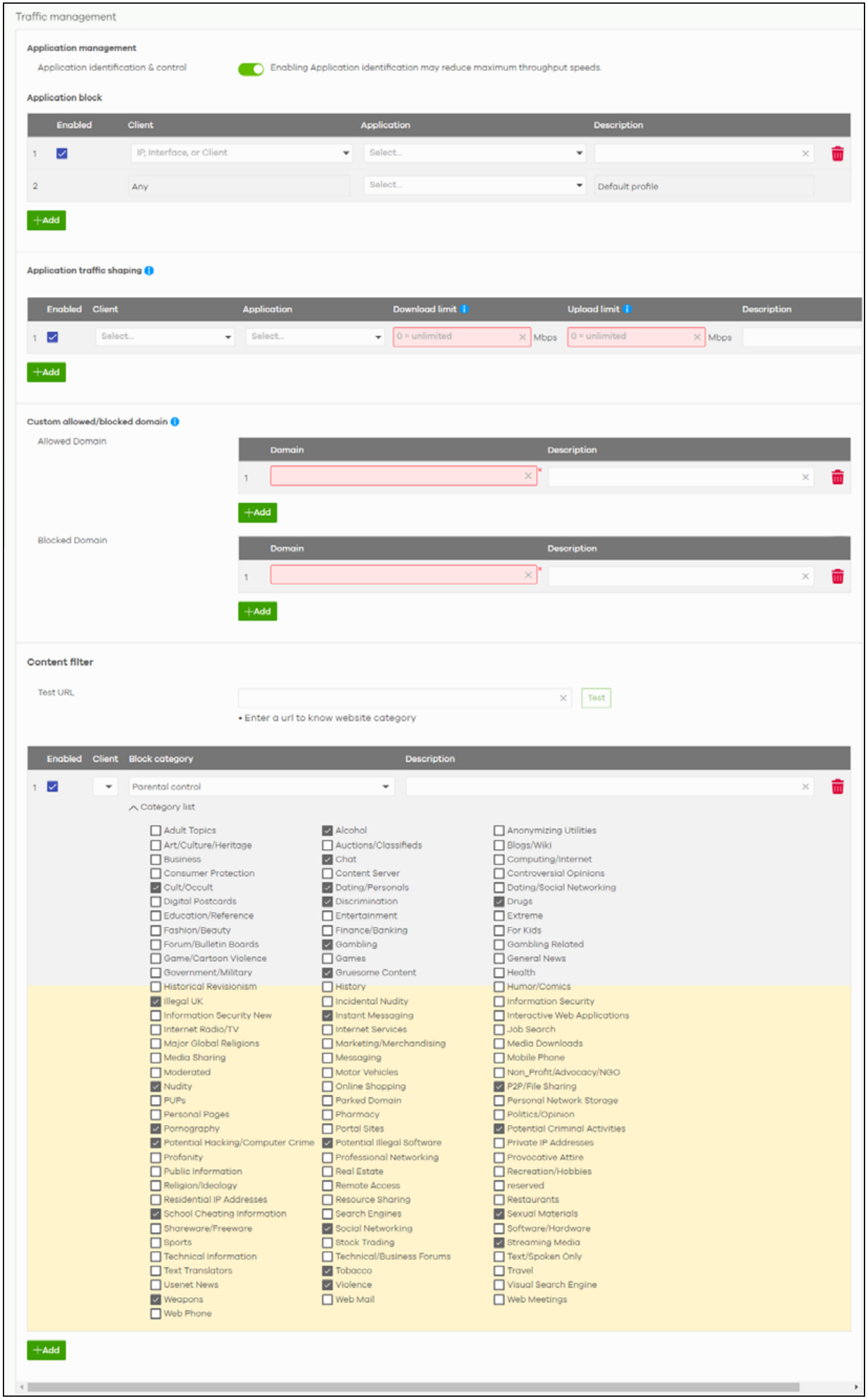
LABEL	DESCRIPTION
Allowed Domain	If you want to access any site, regardless of their content rating, add them to this list. **Domain** – Enter the host name, such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter. Enter a **Description** of the allowed domain. You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long. Click **Add** to create a domain name profile.
Blocked Domain	If you want to block specific sites, regardless of their content rating, add them to this list. **Domain** – Enter the host name, such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Enter a **Description** of the blocked domain. You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long. Click **Add** to create a domain name profile.

7.3.3 Traffic Management

Application management allows you to manage the use of various applications on the network. Content Filter allows you to control access to specific web sites or web content.

Click **Site-wide** > **Configure** > **Security router** > **Traffic management** to access this screen. Use this screen to control application usage and configure content filter.

Figure 147 Site-wide > Configure > Security router > Traffic management



Traffic management

Application management

Application identification & control — Enabling Application identification may reduce maximum throughput speeds.

Application block

	Enabled	Client	Application	Description
1	☑	IP, Interface, or Client	Select...	
2		Any	Select...	Default profile

+Add

Application traffic shaping

	Enabled	Client	Application	Download limit	Upload limit	Description
1	☑	Select...	Select...	0 = unlimited Mbps	0 = unlimited Mbps	

+Add

Custom allowed/blocked domain

Allowed Domain

	Domain	Description
1		

+Add

Blocked Domain

	Domain	Description
1		

+Add

Content filter

Test URL — Test

• Enter a url to know website category

	Enabled	Client	Block category	Description
1	☑		Parental control	

Category list

- □ Adult Topics
- □ Art/Culture/Heritage
- □ Business
- □ Consumer Protection
- ☑ Cult/Occult
- □ Digital Postcards
- □ Education/Reference
- □ Fashion/Beauty
- □ Forum/Bulletin Boards
- □ Game/Cartoon Violence
- □ Government/Military
- □ Historical Revisionism
- ☑ Illegal UK
- □ Information Security New
- □ Internet Radio/TV
- □ Major Global Religions
- □ Media Sharing
- □ Moderated
- ☑ Nudity
- □ PUPs
- □ Personal Pages
- ☑ Pornography
- ☑ Potential Hacking/Computer Crime
- □ Profanity
- □ Public Information
- □ Religion/Ideology
- □ Residential IP Addresses
- ☑ School Cheating Information
- □ Shareware/Freeware
- □ Sports
- □ Technical Information
- □ Text Translators
- □ Usenet News
- ☑ Weapons
- □ Web Phone
- ☑ Alcohol
- □ Auctions/Classifieds
- ☑ Chat
- □ Content Server
- ☑ Dating/Personals
- ☑ Discrimination
- □ Entertainment
- □ Finance/Banking
- ☑ Gambling
- □ Games
- ☑ Gruesome Content
- □ History
- □ Incidental Nudity
- ☑ Instant Messaging
- □ Internet Services
- □ Marketing/Merchandising
- □ Messaging
- □ Motor Vehicles
- □ Online Shopping
- □ Parked Domain
- □ Pharmacy
- □ Portal Sites
- ☑ Potential Illegal Software
- □ Professional Networking
- □ Real Estate
- □ Remote Access
- □ Resource Sharing
- □ Search Engines
- ☑ Social Networking
- □ Stock Trading
- □ Technical/Business Forums
- ☑ Tobacco
- ☑ Violence
- □ Web Mail
- □ Anonymizing Utilities
- □ Blogs/Wiki
- □ Computing/Internet
- □ Controversial Opinions
- □ Dating/Social Networking
- ☑ Drugs
- □ Extreme
- □ For Kids
- □ Gambling Related
- □ General News
- □ Health
- □ Humor/Comics
- □ Information Security
- □ Interactive Web Applications
- □ Job Search
- □ Media Downloads
- □ Mobile Phone
- □ Non_Profit/Advocacy/NGO
- ☑ P2P/File Sharing
- □ Personal Network Storage
- □ Politics/Opinion
- ☑ Potential Criminal Activities
- □ Private IP Addresses
- □ Provocative Attire
- □ Recreation/Hobbies
- □ reserved
- □ Restaurants
- ☑ Sexual Materials
- □ Software/Hardware
- ☑ Streaming Media
- □ Text/Spoken Only
- □ Travel
- □ Visual Search Engine
- □ Web Meetings

+Add

The following table describes the labels in this screen.

Table 94 Site-wide > Configure > Security router > Traffic management

LABEL	DESCRIPTION
Application management	
Application identification & control	Click this to enable the Nebula Device to control usage of applications for a client or all clients. When disabled: • the **Security router network applications** widget in the **Site-wide > Dashboard** screen will show **Application monitor disabled** • the **Site-wide > Applications usage** screen will show **Application identification is turned off**.
Application block	
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Client	Select the client, or enter a single IP address (LAN interface) or IPv4 CIDR (for example, 192.168.1.1/24) to which this rule applies. Then press **Enter** or click **+ Add new**. Or, select **Any** to apply the rule to all clients. Note: Entering a single IP address or IPv4 CIDR is not allowed for SCR 50AXE.
Application	Select **All** or select an application to apply the rule.
Description	Enter a description for this profile. The description can be up to 512 characters long.
🗑	Click this icon to remove the entry.
Add	Click this button to create up to five application management profiles.
Application traffic shaping	
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule. If there is a lock icon, go to the **Site-wide** > **Applications usage** screen to change the maximum downstream/upstream bandwidth. See Section 4.6 on page 269 for more information.
Client	Select the client, or enter a single IP address (LAN interface) or IPv4 CIDR (for example, 192.168.1.1/24) to which this rule applies. Then press **Enter.** Or, select **Any** to apply the rule to all clients.
Application	Select **All** or select an application to apply the rule.
Download limit	Set the maximum downstream bandwidth (1 to 1000 Mbps) for all client traffic that matches the policy will be shared.
Upload limit	Set the maximum upstream bandwidth (1 to 1000 Mbps) for all client traffic that matches the policy will be shared.
Description	Enter a description for this profile. The description can be up to 512 characters long.
🗑	Click this icon to remove the entry.
Add	Click this button to create up to 10 application traffic shaping rules.
Custom allowed/blocked domain	

Table 94 Site-wide > Configure > Security router > Traffic management (continued)

LABEL	DESCRIPTION
Allowed Domain	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. **Domain** – Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter. Enter a **Description** of the allowed domain. The description can be up to 60 characters long. Click 🗑 to remove the entry. Click **Add** to create a domain name profile.
Blocked Domain	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. **Domain** – Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Enter a **Description** of the blocked domain. The description can be up to 60 characters long. Click 🗑 to remove the entry. Click **Add** to create a domain name profile.
Content filter	
Test URL	You can check which category a web page belongs to. Enter a web site URL in the text box. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. Content Filter can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. URL to test displays both results in the test.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Client	Select **All** or select a client to apply the rule.
Block category	Select the block category. Choices are **Parental control**, **Productivity** and **Custom**.
Description	Enter a description for this profile. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 512 characters long.
Category list	Click to display or hide the category list. These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
🗑	Click this icon to remove the entry.
Add	Click this button to create up to five application categories and set actions for specific applications within the category.

7.3.4 Firewall

By default, a LAN user can initiate a session from within the LAN and the Nebula Device allows the response. However, the Nebula Device blocks incoming traffic initiated from the WAN and destined for the LAN. Use this screen to configure firewall rules for outbound traffic.

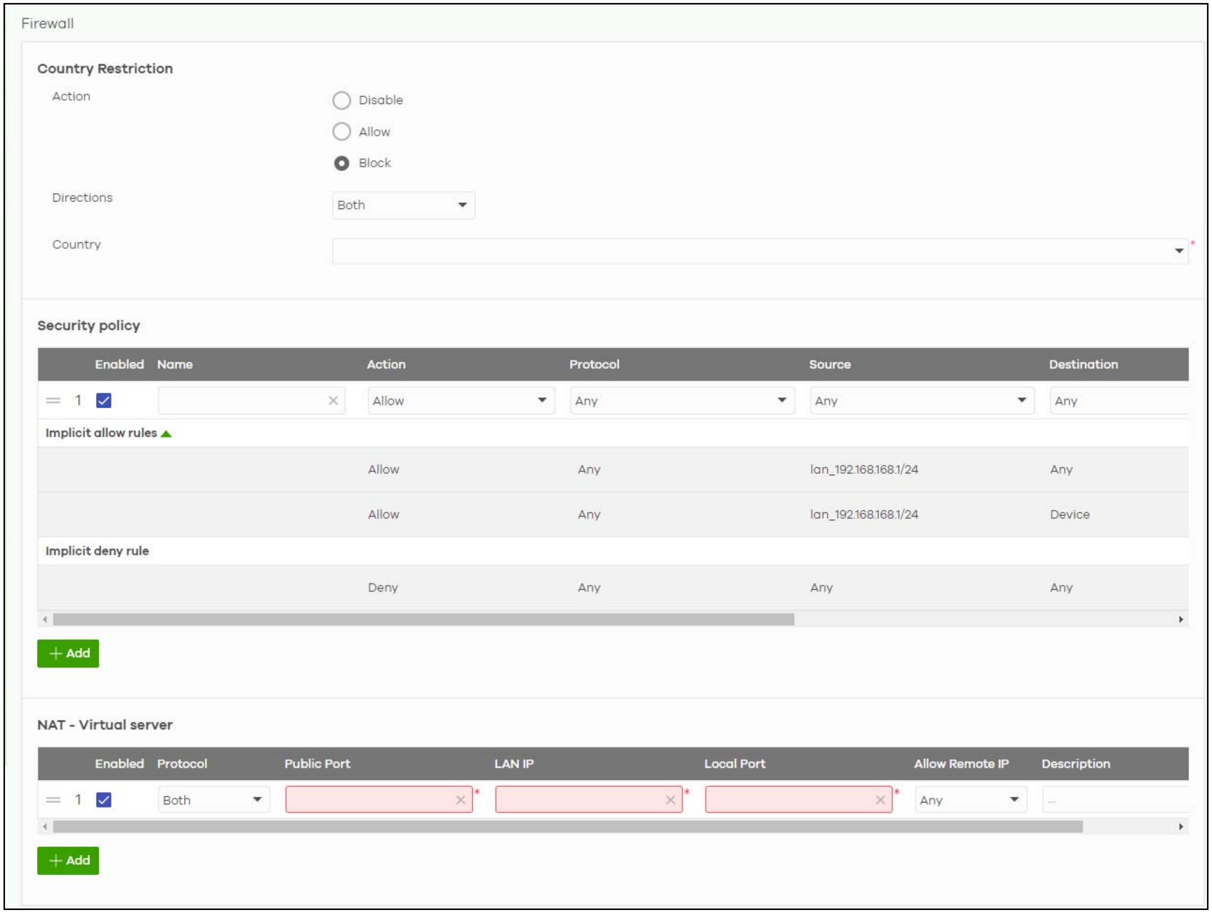
In addition, this screen allows you to create new NAT rules and edit/delete existing NAT rules.

Note: When adding a NAT rule, based on the NAT setting NCC will automatically add the incoming security policy (firewall) rule.

Click **Site-wide** > **Configure** > **Security router** > **Firewall** to access this screen.

Note: The Nebula Device has the following hidden default firewall rules: LAN to WAN is allowed, WAN to LAN is blocked.

Figure 148 Site-wide > Configure > Security router > Firewall



Firewall

Country Restriction

Action: ○ Disable ○ Allow ● Block

Directions: Both

Country:

Security policy

	Enabled	Name	Action	Protocol	Source	Destination
1	☑		Allow	Any	Any	Any
Implicit allow rules						
			Allow	Any	lan_192.168.168.1/24	Any
			Allow	Any	lan_192.168.168.1/24	Device
Implicit deny rule						
			Deny	Any	Any	Any

NAT - Virtual server

	Enabled	Protocol	Public Port	LAN IP	Local Port	Allow Remote IP	Description
1	☑	Both				Any	

The following table describes the labels in this screen.

Table 95 Site-wide > Configure > Security router > Firewall

LABEL	DESCRIPTION
Country Restriction	
Action	Choose one of the following actions: • **Disable**: Select this to hide the **Country Restriction** settings. • **Allow**: Select this to allow packets from the selected countries IP address in the **Country** field. Dropping of packets from countries not in the **Allow** list will occur. • **Block**: Select this to drop packets from the selected countries IP address in the **Country** field.
Directions	Select **Both** to allow incoming/outgoing packets to apply the firewall rules. Select **Incoming** to apply the firewall rules on incoming packets. Select **Outgoing** to apply the firewall rules on outgoing packets.
Country	Select up to 10 countries or regions to apply the firewall rules configured in this screen.
Security policy	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Name	Enter the name of the security policy.
Action	Select what the Nebula Device is to do with packets that match this rule. Select **Deny** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Allow** to permit the passage of the packets.
Protocol	Select the IP protocol to which this rule applies. Choices are: **ICMP**, **TCP**, **UDP**, **TCP and UDP** and **Any**.
Source	Specify the source IP addresses (LAN interface / country) to which this rule applies. You can add a CIDR, or enter a new IP address by clicking **Customize IP**. Enter **Any** to apply the rule to all IP addresses.
Destination	Specify the destination IP addresses (LAN interface / country) or subnet to which this rule applies. You can add a CIDR, or enter a new IP address by clicking **Customize IP**. Enter **Any** to apply the rule to all IP addresses.
Dst Port	Specify the destination ports to which this rule applies. By default, **Any** applies the rule to all ports.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the rule.
🗑	Click this icon to remove the rule.
Implicit allow rules	This shows the system generated **Allow** rules. • LAN interface / remote access VPN to **Any** • LAN interface / remote access VPN to Nebula Device
Implicit deny rule	This shows the system generated **Deny** rule. • **Any** to **Any**
Add	Click this button to create a new rule.
NAT – Virtual server	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Protocol	Select the IP protocol to which this rule applies. Choices are: **TCP**, **UDP**, and **Both**. Note: Select **Both** if you are unsure.
Public Port	Enter the translated destination port or range of translated destination ports if this NAT rule forwards the packet. The remote user will try to connect to this port.

Table 95   Site-wide > Configure > Security router > Firewall (continued)

LABEL	DESCRIPTION
LAN IP	Specify to which translated destination IP address this NAT rule forwards packets. This is the IP address of the internal server.
Local Port	Enter the original destination port or range of destination ports this NAT rule supports. The internal server should respond to this port.
Allow Remote IPs	Specify the remote IP addresses that are allowed to access the public IP address. You may restrict the remote users to connect from certain public IP addresses only. Select **Any** to allow all IP addresses.
Description	Enter the descriptive name of the policy of up to 255 printable ASCII characters.
🗑	Click this icon to remove the profile.
Add	Click this button to create a new schedule profile.

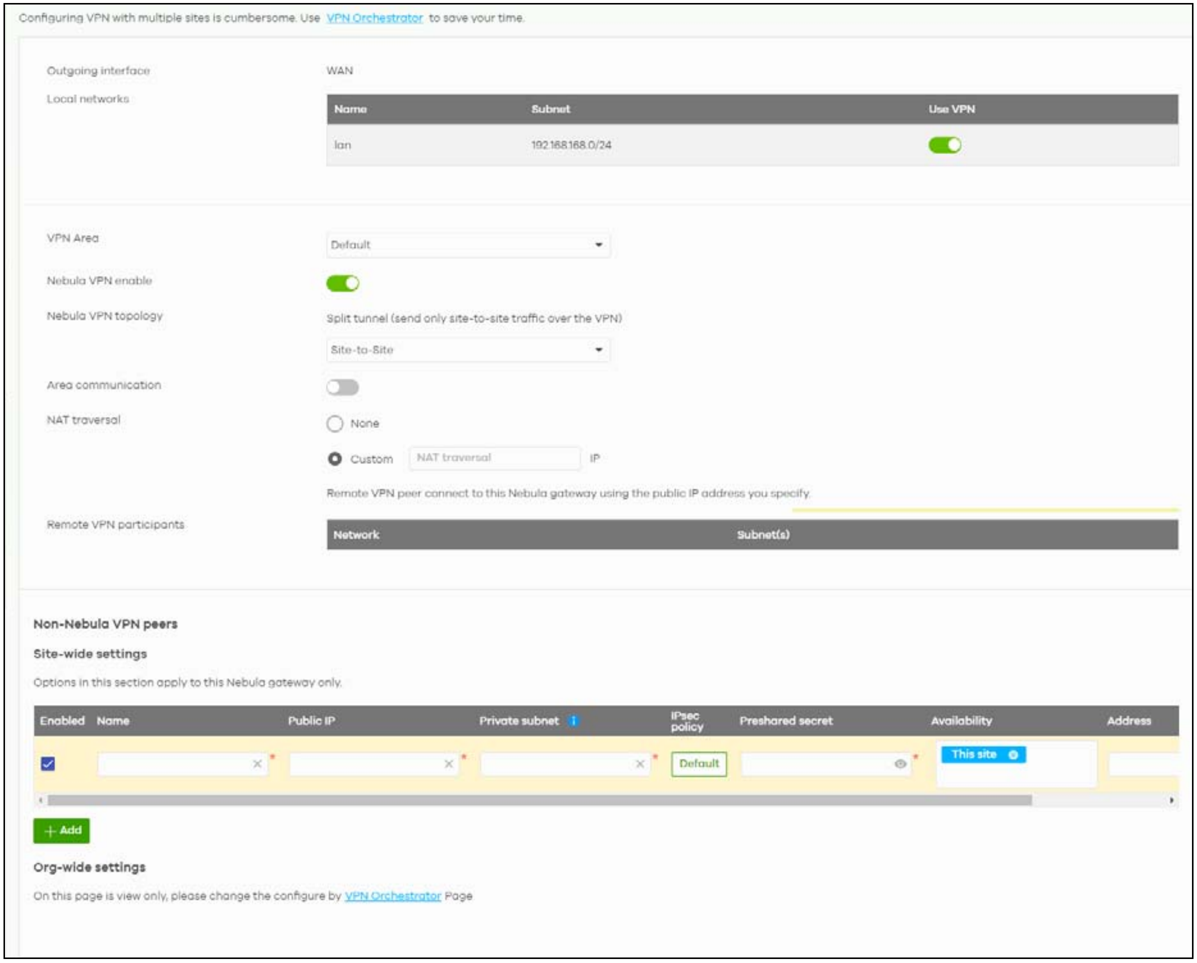
7.3.5 Site-to-Site VPN

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. Use this screen to configure VPN rules.

Note: Site-to-site VPN does not support both VPN sites behind NAT mode.

Click **Site-wide** > **Configure** > **Security router** > **Site-to-Site VPN** to access this screen.

Figure 149   Site-wide > Configure > Security router > Site-to-Site VPN



Configuring VPN with multiple sites is cumbersome. Use VPN Orchestrator to save your time.

Outgoing interface: WAN

Local networks

Name	Subnet	Use VPN
lan	192.168.168.0/24	ON

VPN Area: Default

Nebula VPN enable: ON

Nebula VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

Site-to-Site

Area communication: OFF

NAT traversal: ○ None

● Custom NAT traversal IP

Remote VPN peer connect to this Nebula gateway using the public IP address you specify.

Remote VPN participants

Network	Subnet(s)

Non-Nebula VPN peers

Site-wide settings

Options in this section apply to this Nebula gateway only.

Enabled	Name	Public IP	Private subnet	IPsec policy	Preshared secret	Availability	Address
☑				Default		This site	

+ Add

Org-wide settings

On this page is view only, please change the configure by VPN Orchestrator Page

The following table describes the labels in this screen.

Table 96   Site-wide > Configure > Security router > Site-to-Site VPN

LABEL	DESCRIPTION
Outgoing Interface	This displays **WAN** as the interface to which the VPN connection is going.
Local network	This shows the local network behind the Nebula Device.
Name	This shows the network name.
Subnet	This shows the IP address and subnet mask of the computer on the network.
Use VPN	Select ON to allow the computers on the network to use the VPN tunnel. Otherwise, select OFF. Note: Non-Nebula VPN peers use the first interface with a local policy. For example, when both 'lan1' and 'lan2' are enabled, the first interface in the list 'lan1' will be used regardless of the order they are created.
VPN Area	Select the VPN area of the site. For details, see Section 12.4.4.2 on page 691.
Nebula VPN enable	Click this to enable or disable site-to-site VPN on the site's Nebula Device. If you disable this setting, the site will leave the VPN area.

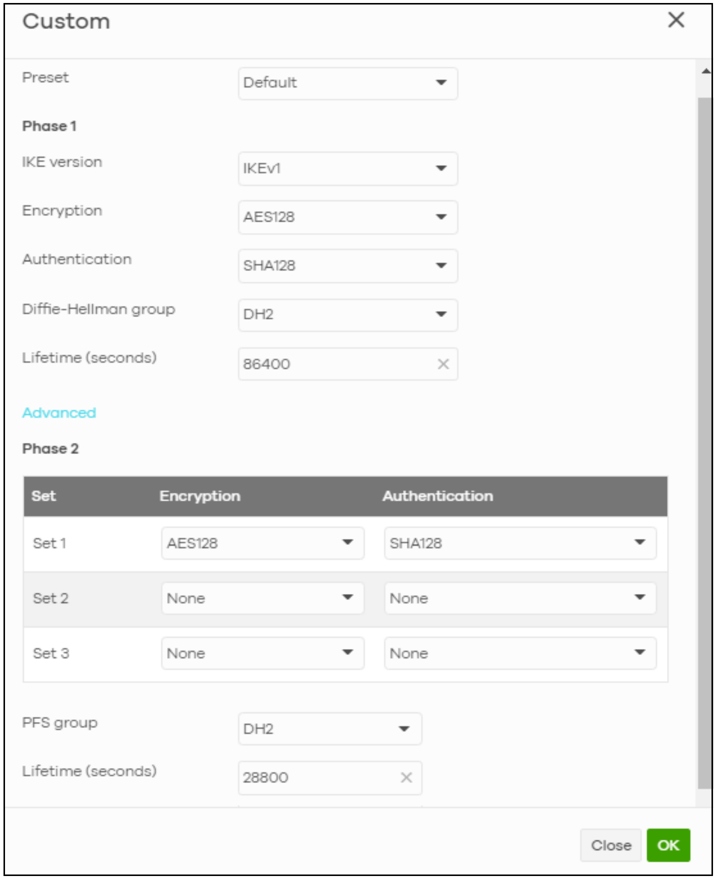
Table 96 Site-wide > Configure > Security router > Site-to-Site VPN (continued)

LABEL	DESCRIPTION
Nebula VPN Topology	Click this to select a topology for the VPN area. For details on topologies, see Section 12.4.4.1 on page 691. Select disable to disable VPN connections for all sites in the VPN area.
Area communication	Enable this to allow the site to communicate with sites in different VPN areas within the organization.
NAT traversal	If the Nebula Device is behind a NAT router, select **Custom** to enter the public IP address or **Auto** or the domain name that is configured and mapped to the Nebula Device on the NAT router. In the **NAT traversal** pop-up, select **WAN** and **Auto** to allow NCC to detect automatically the public IP of your Nebula Device. Note: To allow a site-to-site VPN connection, the NAT router must have the following ports open: UDP 500, 4500.
Remote VPN participants	This shows all sites within the VPN area.
Non-Nebula VPN peers	Configure this section to add a non-Nebula gateway to the VPN area.
+ Add	Click this button to add a non-Nebula gateway to the VPN area.
Enabled	Select the checkbox to enable VPN connections to the non-Nebula gateway.
Name	Enter the name of the non-Nebula gateway/VPN.
Public IP	Enter the public IPv4 address or FQDN of the non-Nebula gateway.
Private subnet	Enter the IP subnet that will be used for VPN connections. This is the other side's LAN subnet, which you want to reach from your side. The IP range must be reachable from other devices in the VPN area. Note: Use a subnet, for example 192.168.10.0/24. Do not use a gateway address, for example 192.168.10.1/24.
IPSec policy	Click to select a pre-defined policy or have a custom one. See Section 7.3.5.1 on page 444 for detailed information.
Preshared secret	Enter a pre-shared key (password). The Nebula Device and peer gateway use the key to identify each other when they negotiate the IKE SA.
Availability	Select which sites the non-Nebula gateway can connect to in the VPN area. Select **All sites** to allow the non-Nebula gateway to connect to any site in the VPN area. Select **This site** and the non-Nebula gateway can only connect to the Nebula Device in this site.
Address	Enter the address (physical location) of the device.
🗑	Click this icon to remove the non-Nebula gateway.
Add	Click this button to create a new non-Nebula gateway.

7.3.5.1 IPsec Policy

Click the **Default** button in the **Non-Nebula VPN peers** section of the **Site-wide** > **Configure** > **Security router** > **Site-to-Site VPN** screen to access this screen.

Figure 150 Site-wide > Configure > Security router > Site-to-Site VPN: IPsec Policy



Custom

Preset	Default
Phase 1	
IKE version	IKEv1
Encryption	AES128
Authentication	SHA128
Diffie-Hellman group	DH2
Lifetime (seconds)	86400

Advanced

Phase 2

Set	Encryption	Authentication
Set 1	AES128	SHA128
Set 2	None	None
Set 3	None	None

PFS group	DH2
Lifetime (seconds)	28800

The following table describes the labels in this screen.

Table 97 Site-wide > Configure > Security router > Site-to-Site VPN: IPsec Policy

LABEL	DESCRIPTION
Preset	Select a pre-defined IPSec policy, or select **Custom** to configure the policy settings yourself.
Phase1	IPSec VPN consists of two phases: Phase 1 (Authentication) and Phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).
IKE version	Select **IKEv1** or **IKEv2**. **IKEv1** and **IKEv2** applies to IPv4 traffic only. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** – a 56-bit key with the DES encryption algorithm **3DES** – a 168-bit key with the DES encryption algorithm **AES128** – a 128-bit key with the AES encryption algorithm **AES192** – a 192-bit key with the AES encryption algorithm **AES256** – a 256-bit key with the AES encryption algorithm The Nebula Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.

Table 97 Site-wide > Configure > Security router > Site-to-Site VPN: IPsec Policy (continued)

LABEL	DESCRIPTION
Authentication	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA128**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than MD5, but it is also slower. The remote IPSec router must use the same authentication algorithm.
Diffie-Hellman group	Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are: **DH1** – use a 768-bit random number Modular Exponential (MODP) DH group **DH2** – use a 1024-bit random number MODP **DH5** – use a 1536-bit random number MODP **DH14** – use a 2048-bit random number MODP **DH19** – use a 256-bit random number elliptic curve group **DH20** – use a 384-bit random number elliptic curve group **DH21** – use a 521-bit random number elliptic curve group **DH28** – use a 256-bit random number elliptic curve group **DH29** – use a 384-bit random number elliptic curve group **DH30** – use a 512-bit random number elliptic curve group Both routers must use the same DH key group.
Lifetime (seconds)	Enter the maximum number of seconds the IKE SA can last. When this time has passed, the Nebula Device and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Advanced	Click this to display a greater or lesser number of configuration fields.
Mode	Set the negotiation mode. **Main** encrypts the Nebula Device’s and remote IPSec router’s identities but takes more time to establish the IKE SA. **Aggressive** is faster but does not encrypt the identities.
Local ID	Enter an identifier used to identify the Nebula Device during authentication. This can be an IP address or hostname.
Peer ID	Enter an identifier used to identify the remote IPSec router during authentication. This can be an IP address or hostname.
Phase2	Phase 2 uses the SA that was established in phase 1 to negotiate SAs for IPSec.

Table 97 Site-wide > Configure > Security router > Site-to-Site VPN: IPsec Policy (continued)

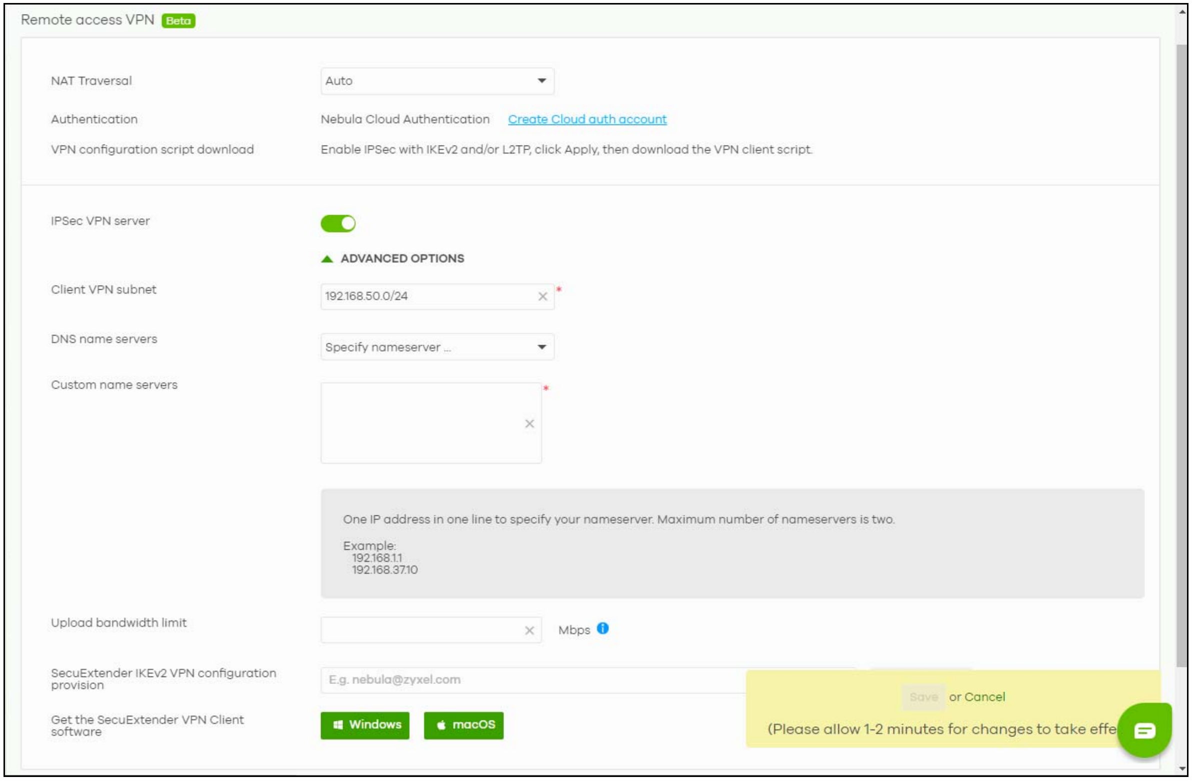
LABEL	DESCRIPTION
Encryption	Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **(None)** – no encryption key or algorithm **DES** – a 56-bit key with the DES encryption algorithm **3DES** – a 168-bit key with the DES encryption algorithm **AES128** – a 128-bit key with the AES encryption algorithm **AES192** – a 192-bit key with the AES encryption algorithm **AES256** – a 256-bit key with the AES encryption algorithm The Nebula Device and the remote IPSec router must both have at least one proposal that uses the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.
PFS group	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **None** – disable PFS **DH1** – use a 768-bit random number Modular Exponential (MODP) DH group **DH2** – use a 1024-bit random number MODP **DH5** – use a 1536-bit random number MODP **DH14** – use a 2048-bit random number MODP **DH19** – use a 256-bit random number elliptic curve group **DH20** – use a 384-bit random number elliptic curve group **DH21** – use a 521-bit random number elliptic curve group **DH28** – use a 256-bit random number elliptic curve group **DH29** – use a 384-bit random number elliptic curve group **DH30** – use a 512-bit random number elliptic curve group PFS changes the root key that is used to generate encryption keys for each IPSec SA. Both routers must use the same DH key group. PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.
Lifetime (seconds)	Enter the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The Nebula Device automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

7.3.6 Remote Access VPN

Use this screen to configure the VPN client settings on the Nebula Device. This allows incoming VPN clients to connect to the Nebula Device in order to access the site's network. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.

Click **Site-wide** > **Configure** > **Security router** > **Remote access VPN** to access this screen.

Figure 151 Site-wide > Configure > Security router > Remote access VPN



Remote access VPN

NAT Traversal	Auto
Authentication	Nebula Cloud Authentication Create Cloud auth account
VPN configuration script download	Enable IPSec with IKEv2 and/or L2TP, click Apply, then download the VPN client script.
IPSec VPN server	●
	▲ ADVANCED OPTIONS
Client VPN subnet	192.168.50.0/24 *
DNS name servers	Specify nameserver ...
Custom name servers	*
	One IP address in one line to specify your nameserver. Maximum number of nameservers is two. Example: 192.168.1.1 192.168.37.10
Upload bandwidth limit	Mbps
SecuExtender IKEv2 VPN configuration provision	E.g. nebula@zyxel.com
Get the SecuExtender VPN Client software	Windows macOS

The following table describes the labels in this screen.

Table 98 Site-wide > Configure > Security router > Remote access VPN

LABEL	DESCRIPTION
NAT Traversal	If the Nebula Device is behind a NAT router, select **+ Customize IP** to enter the public IP address that is configured and mapped to the Nebula Device on the NAT router. Select **None** to map to the WAN IP of the Nebula Device. NCC automatically updates the DNS server when the WAN IP changes. Or, select **Auto** to allow NCC to detect automatically the public IP of your Nebula Device. NCC automatically selects another WAN interface when the selected WAN interface is down. NCC automatically updates the DNS server when the public IP changes.
Authentication	Select how the Nebula Device authenticates a remote user before allowing access to the VPN tunnel. Click **Create a cloud auth account** to create a Nebula Cloud Authentication Server user account. This will automatically add the site where you create remote access VPN setup to the **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **User** screen and bypass two-factor authentication.
VPN configuration script download	Click the **Windows**, **iOS/macOS** or **Android (strongSwan)** icon to download a ZIP file containing the VPN remote access configuration script. After unzipping, save the certificate (.crt) and script (.bat) files to the same folder in your computer. This field is available only when the Nebula Device is online. Note: For **iOS/macOS**, the default authentication type is **Certificate**. To enter the user name and password, change the user authentication type to **Username**.
IPSec VPN server	Select this to enable the IPsec VPN server.
Client VPN subnet	Specify the IP addresses that the Nebula Device uses to assign to the VPN clients. The default subnet is **192.168.50.0/24**.

Table 98 Site-wide > Configure > Security router > Remote access VPN (continued)

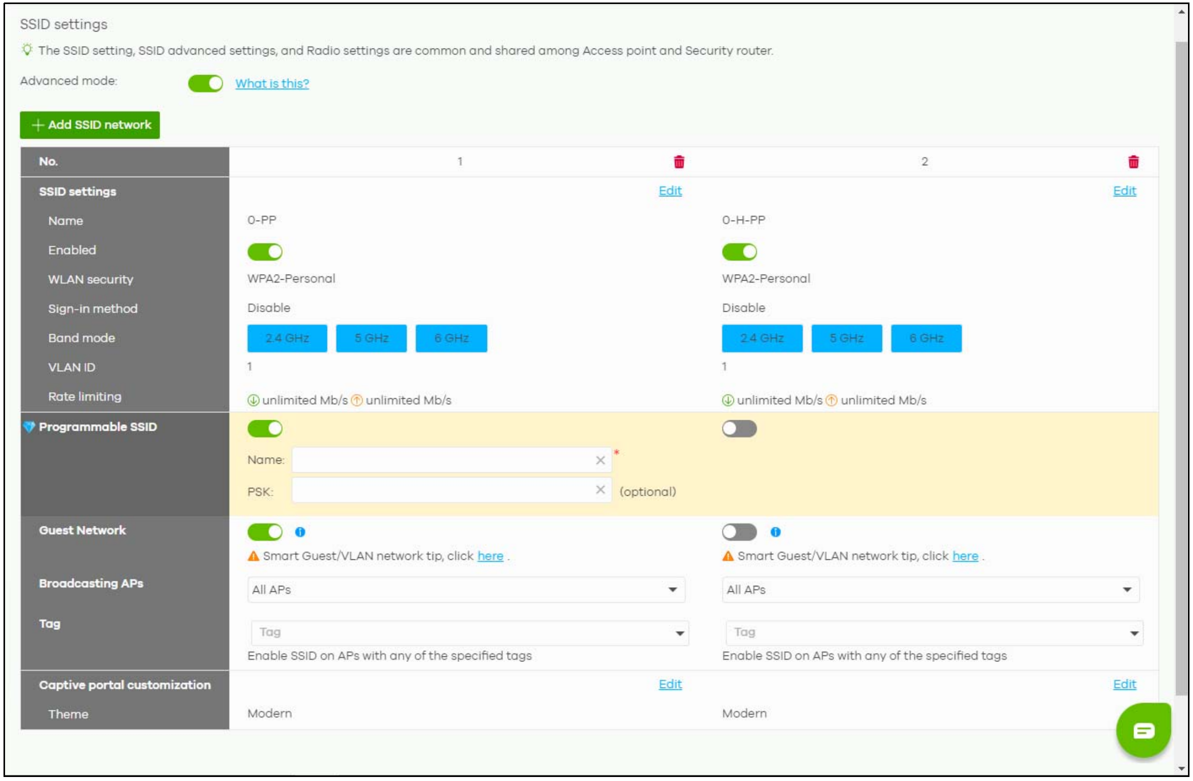
LABEL	DESCRIPTION
DNS name servers	Specify the DNS servers to assign to the remote users. Or select **Specify nameserver** to enter a static IP address.
Custom name servers	If you select **Specify nameserver** in the **DNS name servers** field, manually enter the DNS server IP addresses.
Upload Bandwidth Limit	Enter the maximum traffic load between VPN clients, 1 – 100 Mbps.
SecuExtender IKEv2 VPN configuration provision	Enter the email address to send new IKEv2 Remote Access VPN configuration file to VPN client. Then click **Send Email**. The VPN client needs to replace the IPSec VPN client configuration by importing the configuration file.
Get the SecuExtender VPN Client software	Click the **Windows** or **macOS** icon to download the SecuExtender VPN client software.

7.3.7 SSID Settings

This screen allows you to configure up to 8 different SSID profiles for your Nebula Devices. An SSID, or Service Set IDentifier, is basically the name of the WiFi network to which a WiFi client can connect. The SSID appears as readable text to any device capable of scanning for WiFi frequencies (such as the WiFi adapter in a laptop), and is displayed as the WiFi network name when a person makes a connection to it.

Click **Site-wide** > **Configure** > **Security router** > **SSID settings** to access this screen.

Figure 152 Site-wide > Configure > Security router > SSID settings



SSID settings

The SSID setting, SSID advanced settings, and Radio settings are common and shared among Access point and Security router.

Advanced mode: What is this?

No.	1	2
SSID settings	Edit	Edit
Name	0-PP	0-H-PP
Enabled	●	●
WLAN security	WPA2-Personal	WPA2-Personal
Sign-in method	Disable	Disable
Band mode	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
VLAN ID	1	1
Rate limiting	unlimited Mb/s unlimited Mb/s	unlimited Mb/s unlimited Mb/s
Programmable SSID	● Name: * PSK: (optional)	○
Guest Network	● Smart Guest/VLAN network tip, click here .	○ Smart Guest/VLAN network tip, click here .
Broadcasting APs	All APs	All APs
Tag	Tag Enable SSID on APs with any of the specified tags	Tag Enable SSID on APs with any of the specified tags
Captive portal customization	Edit	Edit
Theme	Modern	Modern

The following table describes the labels in this screen.

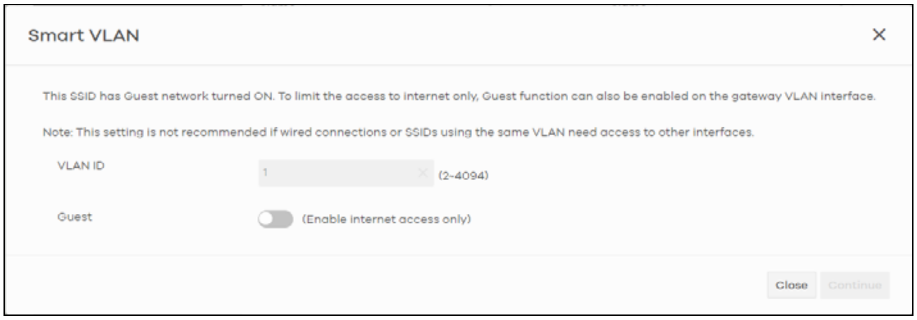
Table 99 Site-wide > Configure > Security router > SSID settings

LABEL	DESCRIPTION
Advanced mode	Select Off to disable **Advanced mode**. This allows you to create SSID profiles by only specifying an SSID name and optional password. NCC sets all other WiFi settings to default.
+ Add SSID network	Click this button to configure up to 8 different SSID profiles for your Nebula Device. To configure more than 8 SSID profiles (up to 24), enable **AP grouping** in **Site-wide** > **Configure** > **Access points** > **AP & port settings**. For details, see Section 5.3.7 on page 344. Note: Only 4 SSIDs are allowed on each SCR 50AXE. Note: Only 8 SSIDs are allowed on each Nebula Device Access Points and USG LITE 60AX. Use the **Tag** and/or **Broadcasting APs** fields to assign up to 8 AP groups per Nebula Device. A blank **Tag** / **Broadcasting APs** field is counted as an AP group. Note: Disabling **AP grouping** in **Site-wide** > **Configure** > **Access points** > **AP & port settings** will hide **SSID9** to **SSID24**, but keep the settings.
No.	This shows the index number of this profile.
delete	Click this icon to remove the SSID profile.
SSID settings	
Edit	Click this button to go to the **SSID advanced settings** screen and configure WiFi security and advanced settings, such as band selection, enable assisted roaming and U-APSD (Unscheduled automatic power save delivery). See Table 53 on page 323 for more information on assisted roaming and U-APSD.
Name	This shows the SSID name for this profile. Click the text box and enter a new SSID if you want to change it.
Enabled	Click to turn on or off this profile.
WLAN security	This shows the encryption method used in this profile.
Sign-in method	This shows the authentication method used in this profile or **Disable**.
Band mode	This shows whether the SSID use either 2.4 GHz band, 5 GHz band, or the 6 GHz band.
VLAN ID	This shows the ID number of the VLAN to which the SSID belongs.
Rate limiting	This shows the maximum incoming/outgoing transmission data rate (in Kbps) on a per-station basis.
Programmable SSID	Select On to have each Nebula Device that uses this SSID generate a unique SSID name and pre-shared key (PSK) based on the Nebula Device's model name, serial number, or MAC address. For example, a hotel can install a Nebula Device in each room and then have each Nebula Device broadcast a unique SSID based on the room number: FreeWiFi_Room1, FreeWiFi_Room2, FreeWiFi_Room3, and so on.

Table 99 Site-wide > Configure > Security router > SSID settings (continued)

LABEL	DESCRIPTION
Name	**Name**: Enter a programmable SSID name in the format PREFIX+VALUE(X). This name overrides the original SSID name. • PREFIX: Optional prefix to add to the SSID, for example "FreeWiFi_". To use "$" in the SSID name, enter "$$" • VALUE: Specify a Nebula Device value to use to generate the SSID name. Use one of the following: $AP = Nebula Device device name. $MAC = Nebula Device MAC address. $SN = Nebula Device serial number. • X: Specify how many characters of the Nebula Device value to use in the SSID. A positive number means the first X characters, and a negative number means the last X characters. Example: *FreeWiFi_Room$AP(–3)* generates an SSID called "FreeWiFi_Room" + the last three characters of the access point device name.
PSK	**PSK**: Enter an optional programmable PSK in the format GENTYPE(Y). • GENTYPE: Specify how the Nebula Device will generate a random PSK. $GENMIX = The Nebula Device generates a mix of random letters and numbers. $GENNUM = The Nebula Device generates a mix of random numbers only. $AP = Nebula Device device name. $MAC = Nebula Device MAC address. $SN = Nebula Device serial number. Y = Specify the length of the PSD. The minimum length is 8. Example 1: $GENNUM(10) generates a unique 10-character PSK for this SSID, consisting only of numbers. Example 2: $MAC(-5)$SN(-5) uses the MAC address's last 5 characters and the serial number's last 5 characters (for example, 8E3AE02451). Example 3: ZYXEL-$GENMIX(4) appends the fixed characters 'ZYXEL' and generates a unique 4-character mix of random letters and numbers (for example, ZYXEL-3c4d). Note: You can specify a fixed PSK for this SSID at **Site-wide** > **Configure** > **Access points / Security router** > **SSID advanced settings**.

Table 99 Site-wide > Configure > Security router > SSID settings (continued)

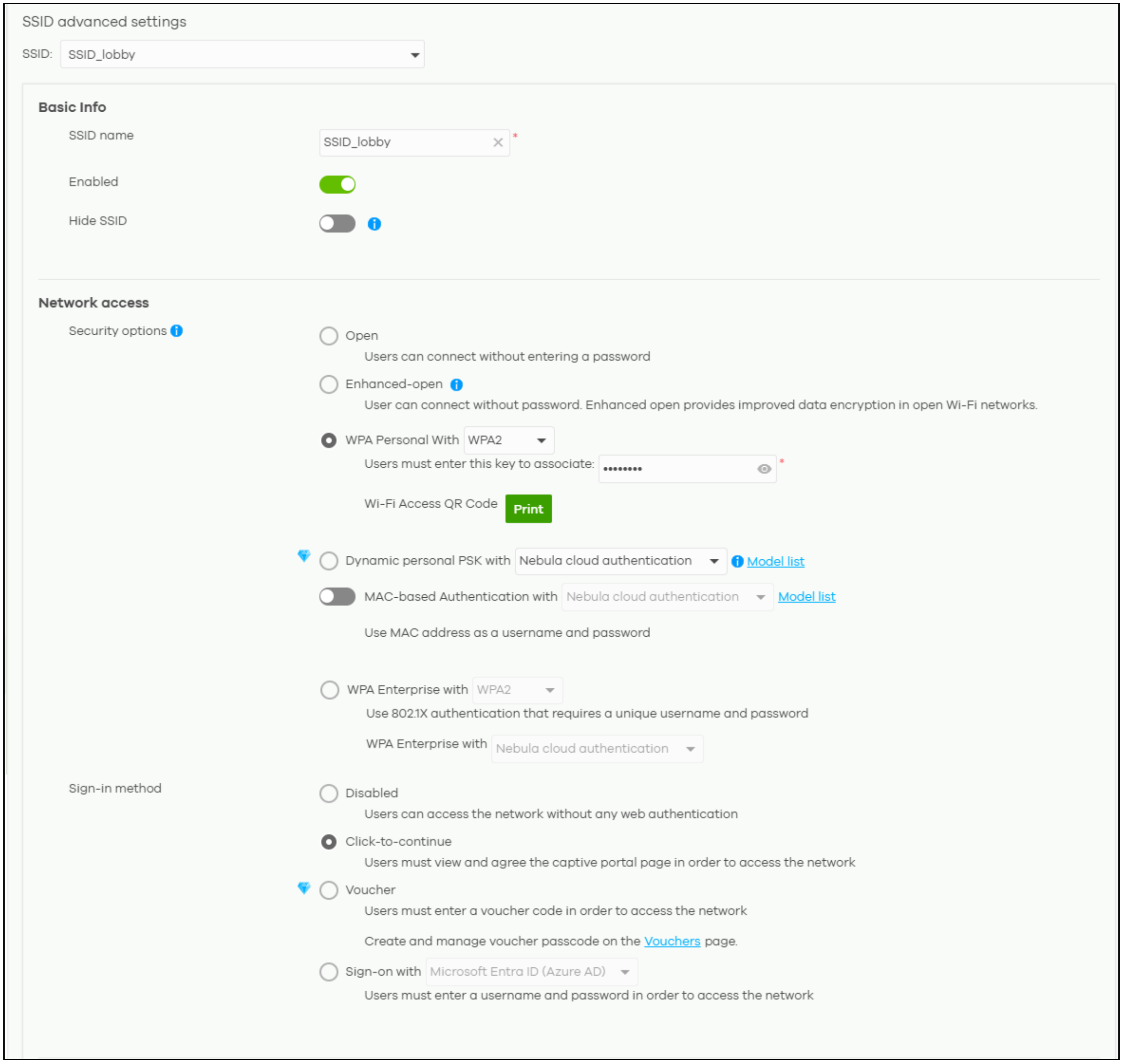
LABEL	DESCRIPTION
Guest Network	Select On to set this WiFi network as a guest network. Layer 2 isolation and intra-BSS blocking are automatically enabled on the SSID. WiFi clients connecting to this SSID can access the Internet through the Nebula Device but cannot directly connect to the LAN or the WiFi clients in the same SSID or any other SSIDs. Note: In your VLAN-enabled network, if the SSID's gateway MAC address and the Nebula Device's gateway MAC address are different and belong to different VLANs, you need to manually add the SSID's gateway MAC address to the layer 2 isolation list. See Section 5.3.2 on page 320. Note: If you have a Nebula Security Gateway installed in the site but the gateway interface with the same VLAN ID is not configured as a guest interface, **Smart Guest/VLAN network tip, click here.** displays after you select **On**. Click **here** to open a screen where you can directly select to use the interface as a Guest interface.  Smart VLAN This SSID has Guest network turned ON. To limit the access to internet only, Guest function can also be enabled on the gateway VLAN interface. Note: This setting is not recommended if wired connections or SSIDs using the same VLAN need access to other interfaces. VLAN ID: 1 (2-4094) Guest: ○ (Enable internet access only)
Broadcasting APs	Select **All APs** or specify the AP to use this SSID profile. Note: This field only appears when you have a Security Router in your site.
Tag	Enter or select the tags you created for Nebula Devices in the **Site-wide** > **Devices** > **Access points** screen or **Site-wide** > **Devices** > **Access points: Details** screen. Only the Nebula Devices with the specified tag will broadcast this SSID. If you leave this field blank, all the Nebula Devices on the site will broadcast this SSID.
Captive portal customization	
Edit	Click this button to go to the **Captive portal** screen and configure the captive portal settings. See Section 5.3.3 on page 330.
Theme	If captive portal is enabled, this shows the name of the captive portal page used in this profile.

7.3.8 SSID Advanced Settings

Use this screen to configure WiFi security, band selection, assisted roaming and U-APSD (Unscheduled automatic power save delivery) settings for the SSID profiles.

Click **Site-wide** > **Configure** > **Security router** > **SSID advanced settings** to access this screen.

Figure 153 Site-wide > Configure > Security router > SSID advanced settings Part 1



SSID advanced settings

SSID: SSID_lobby

Basic Info

SSID name: SSID_lobby *

Enabled: on

Hide SSID: off

Network access

Security options

○ Open
Users can connect without entering a password

○ Enhanced-open
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.

● WPA Personal With WPA2
Users must enter this key to associate: •••••••• *
Wi-Fi Access QR Code Print

○ Dynamic personal PSK with Nebula cloud authentication Model list
MAC-based Authentication with Nebula cloud authentication Model list
Use MAC address as a username and password

○ WPA Enterprise with WPA2
Use 802.1X authentication that requires a unique username and password
WPA Enterprise with Nebula cloud authentication

Sign-in method

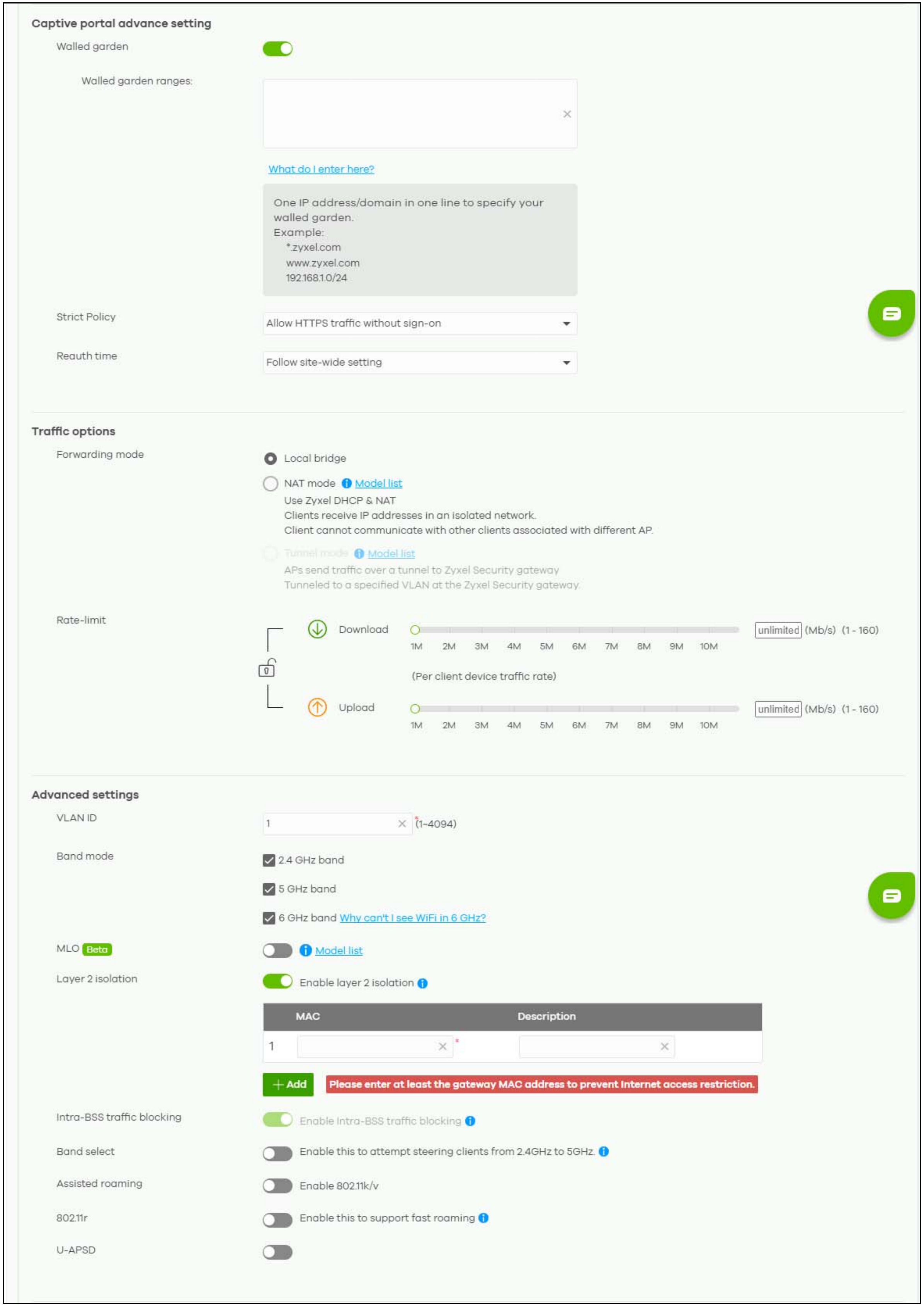
○ Disabled
Users can access the network without any web authentication

● Click-to-continue
Users must view and agree the captive portal page in order to access the network

○ Voucher
Users must enter a voucher code in order to access the network
Create and manage voucher passcode on the Vouchers page.

○ Sign-on with Microsoft Entra ID (Azure AD)
Users must enter a username and password in order to access the network

Figure 154 Site-wide > Configure > Security router > SSID advanced settings Part 2



Captive portal advance setting

Walled garden

Walled garden ranges:

What do I enter here?

One IP address/domain in one line to specify your walled garden.
Example:
*.zyxel.com
www.zyxel.com
192.168.1.0/24

Strict Policy: Allow HTTPS traffic without sign-on

Reauth time: Follow site-wide setting

Traffic options

Forwarding mode

● Local bridge

○ NAT mode Model list
Use Zyxel DHCP & NAT
Clients receive IP addresses in an isolated network.
Client cannot communicate with other clients associated with different AP.

○ Tunnel mode Model list
APs send traffic over a tunnel to Zyxel Security gateway
Tunneled to a specified VLAN at the Zyxel Security gateway

Rate-limit

Download 1M 2M 3M 4M 5M 6M 7M 8M 9M 10M unlimited (Mb/s) (1 - 160)

(Per client device traffic rate)

Upload 1M 2M 3M 4M 5M 6M 7M 8M 9M 10M unlimited (Mb/s) (1 - 160)

Advanced settings

VLAN ID: 1 (1~4094)

Band mode

☑ 2.4 GHz band

☑ 5 GHz band

☑ 6 GHz band Why can't I see WiFi in 6 GHz?

MLO Beta: Model list

Layer 2 isolation: Enable layer 2 isolation

MAC	Description
1	

+ Add

Please enter at least the gateway MAC address to prevent Internet access restriction.

Intra-BSS traffic blocking: Enable Intra-BSS traffic blocking

Band select: Enable this to attempt steering clients from 2.4GHz to 5GHz.

Assisted roaming: Enable 802.11k/v

802.11r: Enable this to support fast roaming

U-APSD

The following table describes the labels in this screen.

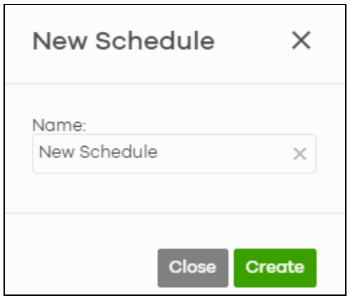
Table 100 Site-wide > Configure > Security router > SSID advanced settings

LABEL	DESCRIPTION
SSID advanced settings	Select the SSID profile to which the settings you configure here is applied.
Basic information	
SSID name	This shows the SSID name as it appears to WiFi clients. Click the text box and enter a new SSID if you want to change it.
Enabled	Click this to enable the SSID to be discoverable by WiFi clients.
Hide SSID	Click this if you want to hide your SSID from WiFi clients. This tells any WiFi clients in the vicinity of the Nebula Device using this SSID profile not to display its SSID name as a potential connection. When an SSID is "hidden" and a WiFi client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your WiFi connection setup screens. Note: This field will not appear when you have an SCR 50AXE but no Nebula Device AP(s) in your site.
Network access	Note: You cannot enable MAC authentication, 802.1X authentication and web authentication at the same time. Note: User accounts can be created and authenticated using the NCC user database. See Section on page 726.

Table 100 Site-wide > Configure > Security router > SSID advanced settings (continued)

LABEL	DESCRIPTION
Security options	Select **Open** to allow any client to associate this network without any data encryption or authentication. Select **Enhanced-open** to allow any client to associate this network without any password but with improved data encryption. Upon selecting **Enhanced-open** or **WPA Personal With WPA3**, **transition mode** generates two VAP so devices that do not support **Enhanced-Open**/**WPA Personal With WPA3** can connect using **Open**/**WPA Personal With WPA2** network. This is always **on** at the time of writing. Select **WPA Personal With (WPA2/WPA3)** and enter a pre-shared key from 8 to 63 case-sensitive keyboard characters to enable WPA2/3-PSK data encryption. Upon selecting **WPA Personal With WPA3**, Nebula Devices that do not support it will revert to WPA2. • Turn on **802.11r** to enable IEEE 802.11r fast roaming on the access point. 802.11r fast roaming reduces the delay when the clients switch from one Nebula Device to another by allowing security keys to be stored on all Nebula Devices in a network. Information from the original association is passed to the new Nebula Device when the client roams. The client does not need to perform the whole 802.1x authentication process. Click **Print** to display the QR code that includes the password for quick access. You can save the QR code as PDF. To test, use a smartphone to scan the QR code. Click to join the network. The client device should connect to WiFi directly without asking the password. Select **Dynamic personal psk** to have every user connect to the SSID using a unique pre-shared key (PSK) that is linked to their user account. This allows you to revoke a user's WiFi network access by disabling their account. After enabling this option, you must create one or more DPPSK users in the site or organization at **Site-wide** > **Configure** > **Cloud authentication** > **Account Type** > **DPPSK**. • For details on creating a site DPPSK user, see Section 4.9.3.3 on page 293. • For details on creating organization DPPSK users, see Section 12.4.7.3 on page 713. Turn on **MAC-based Authentication with** to authenticate WiFi clients by their MAC addresses together with **My RADIUS server** to use an external RADIUS server. Or select **Nebula cloud authentication** to use the NCC for MAC authentication. Select **WPA-Enterprise with** to enable 802.1X secure authentication. You can select **My RADIUS server** to use an external RADIUS server or select **Nebula cloud authentication** to use the NCC for 802.1X authentication. • Turn on **802.11r** to enable IEEE 802.11r fast roaming on the Nebula Device. 802.11r fast roaming reduces the delay when the clients switch from one Nebula Device to another by allowing security keys to be stored on all Nebula Devices in a network. Information from the original association is passed to the new Nebula Device when the client roams. The client does not need to perform the whole 802.1x authentication process. • Select **Two-Factor Authentication** to require that the user log in using both their password and a Google Authenticator code. To log in, users must have Two-Factor Authentication enabled on their account and have setup Google Authenticator on their mobile device. Select **Enable on RAP only** to only require Two-Factor Authentication when accessing the network through a remote access point (RAP).
Rate-limit	Set the maximum data download and upload rates in Kbps, on a per-station basis. Click a lock icon to change the lock state. If the lock icon is locked, the limit you set applies to both download and upload traffic. If the lock is unlocked, you can set download and upload traffic to have different transmission speeds.
Advanced settings	
VLAN ID	This shows the ID number of the VLAN to which the SSID belongs.
Band mode	Select to have the SSID use either **2.4 GHz band**, **5 GHz band**, or **6 GHz band** only.

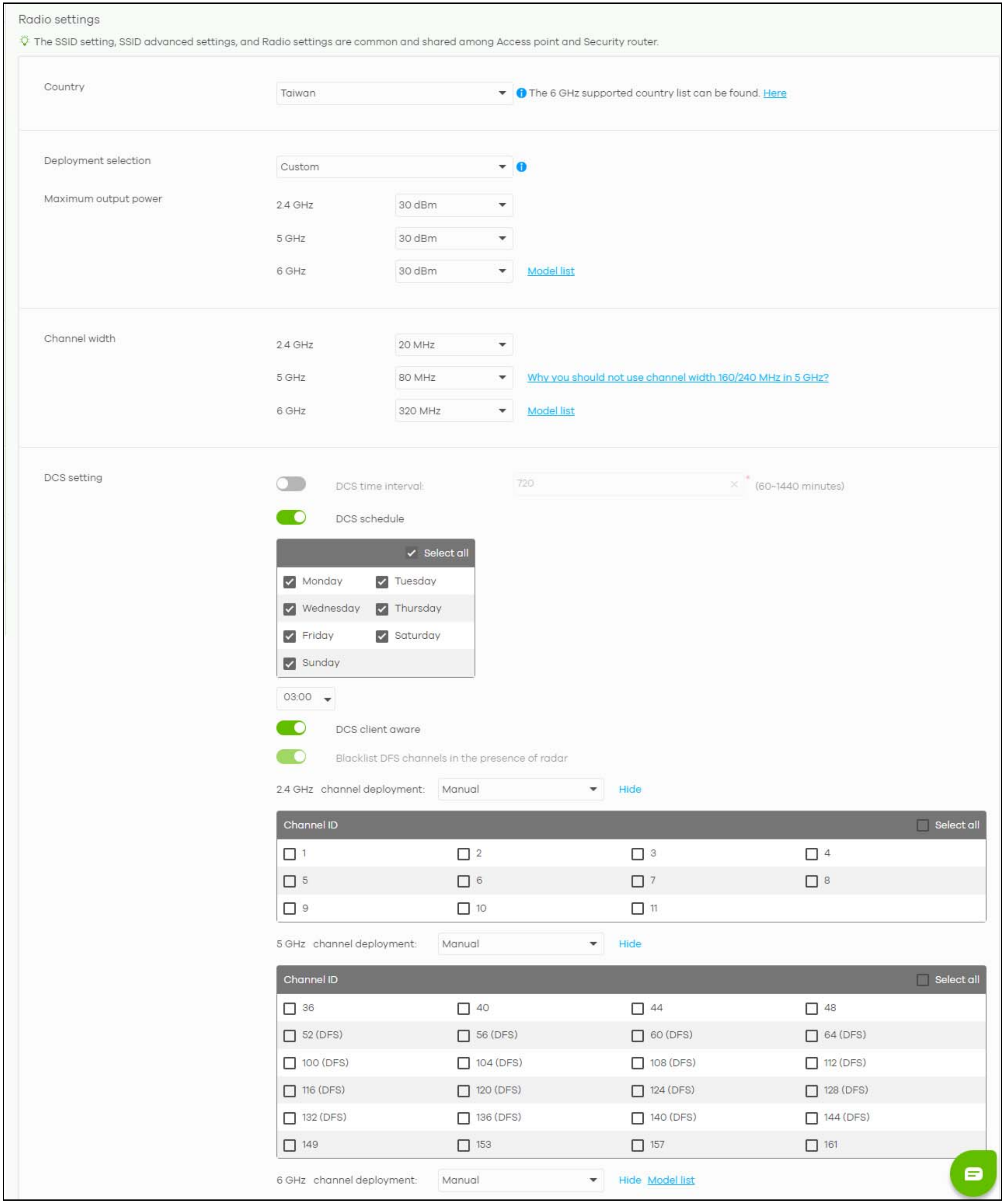
Table 100 Site-wide > Configure > Security router > SSID advanced settings (continued)

LABEL	DESCRIPTION
Layer 2 isolation	This field is not configurable if you select NAT mode. Select to turn on or off layer-2 isolation. If a device's MAC addresses is NOT listed, it is blocked from communicating with other devices in an SSID on which layer-2 isolation is enabled. Click **Add** to enter the MAC address of each device that you want to allow to be accessed by other devices in the SSID on which layer-2 isolation is enabled.
Intra-BSS traffic blocking	Click this switch to the left to prevent crossover traffic from within the same SSID. Click this switch to the right to allow intra-BSS traffic.
Band select	Select to enable band steering. When enabled, the Nebula Device steers WiFi clients to the 5 GHz band.
Assisted roaming	Select to turn on or off IEEE 802.11k/v assisted roaming on the Nebula Device. When the connected clients request 802.11k neighbor lists, the Nebula Device will response with a list of neighbor Nebula Devices that can be candidates for roaming. When the 802.11v capable clients are using the 2.4 GHz band, the Nebula Device can send 802.11v messages to steer clients to the 5 GHz band.
802.11r	Select to turn on or off IEEE 802.11r fast roaming on the Nebula Device. 802.11r fast roaming reduces the delay when the clients switch from one Nebula Device to another, by allowing security keys to be stored on all Nebula Devices in a network. Information from the original association is passed to the new Nebula Device when the client roams. The client does not need to perform the whole 802.1x authentication process.
U-APSD	Select to turn on or off Automatic Power Save Delivery. This helps increase battery life for battery-powered WiFi clients connected to the Nebula Device.
SSID schedule	
Enabled	Click this switch to the right to enable and configure a schedule.
Schedule	Select a schedule to control when the SSID is enabled or disabled. You can click the edit icon to change the schedule name.
Schedule templates	Select a pre-defined schedule template or select **Custom schedule** and manually configure the day and time at which the SSID is enabled or disabled.
Day	This shows the day of the week.
Availability	Click this switch to the right to enable the SSID at the specified time on this day. Otherwise, click this switch to the left to disable the SSID on the day and at the specified time. Specify the hour and minute when the schedule begins and ends each day.
Add	Click this button to create a new schedule. A window pops up asking you to enter a descriptive name for the schedule for identification purposes.  New Schedule Name: New Schedule
Delete	Click this button to remove a schedule which is not used in any SSID profile.

7.3.9 Radio Settings

Use this screen to configure global radio settings for the Nebula Device in the site. Click **Site-wide** > **Configure** > **Security router** > **Radio settings** to access this screen.

Figure 155 Site-wide > Configure > Security router > Radio settings Part 1



Radio settings

The SSID setting, SSID advanced settings, and Radio settings are common and shared among Access point and Security router.

Country: Taiwan — The 6 GHz supported country list can be found. Here

Deployment selection: Custom

Maximum output power
- 2.4 GHz: 30 dBm
- 5 GHz: 30 dBm
- 6 GHz: 30 dBm — Model list

Channel width
- 2.4 GHz: 20 MHz
- 5 GHz: 80 MHz — Why you should not use channel width 160/240 MHz in 5 GHz?
- 6 GHz: 320 MHz — Model list

DCS setting
- DCS time interval: 720 * (60~1440 minutes)
- DCS schedule

	☑ Select all
☑ Monday	☑ Tuesday
☑ Wednesday	☑ Thursday
☑ Friday	☑ Saturday
☑ Sunday	

03:00

- DCS client aware
- Blacklist DFS channels in the presence of radar

2.4 GHz channel deployment: Manual — Hide

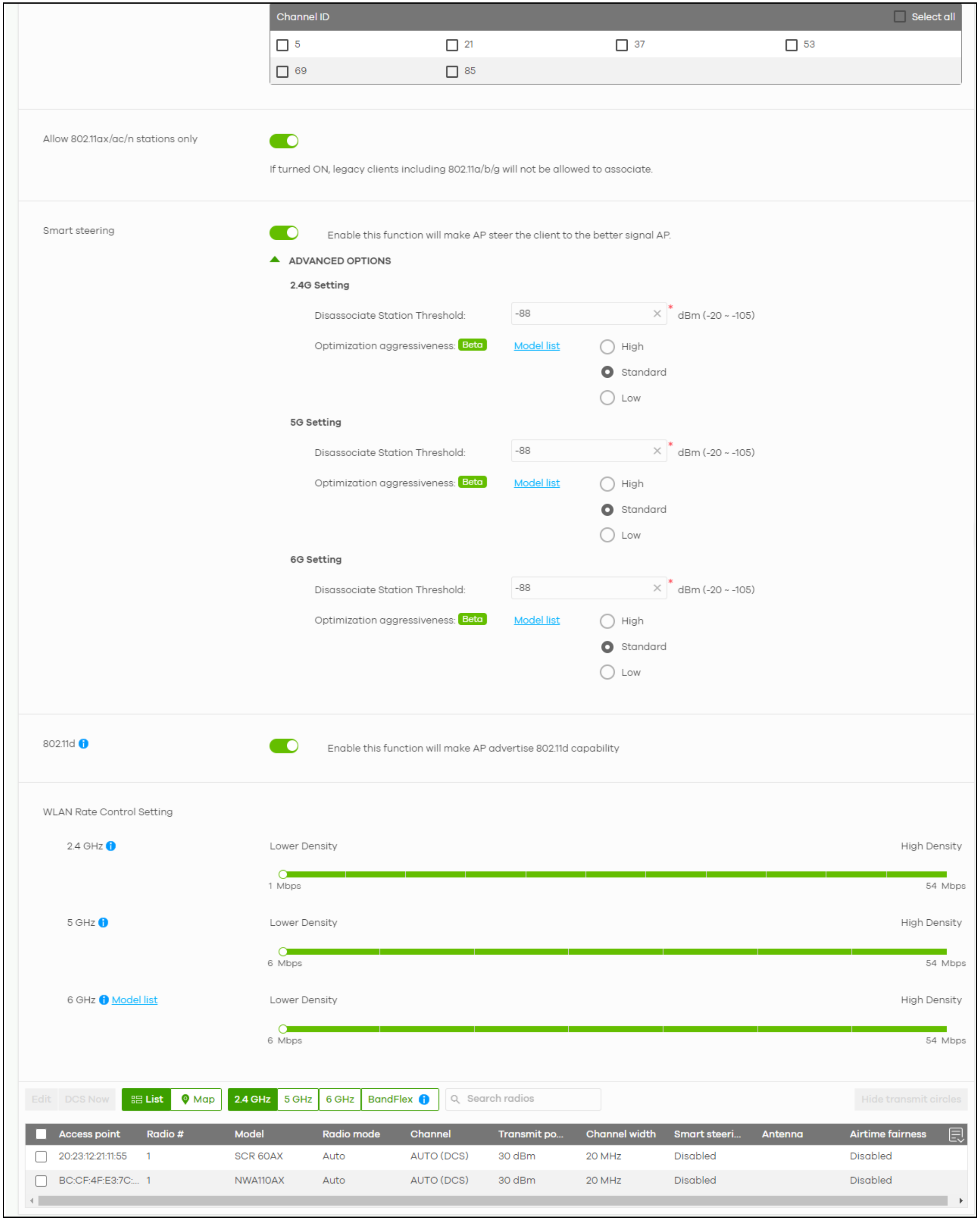
Channel ID			□ Select all
□ 1	□ 2	□ 3	□ 4
□ 5	□ 6	□ 7	□ 8
□ 9	□ 10	□ 11	

5 GHz channel deployment: Manual — Hide

Channel ID			□ Select all
□ 36	□ 40	□ 44	□ 48
□ 52 (DFS)	□ 56 (DFS)	□ 60 (DFS)	□ 64 (DFS)
□ 100 (DFS)	□ 104 (DFS)	□ 108 (DFS)	□ 112 (DFS)
□ 116 (DFS)	□ 120 (DFS)	□ 124 (DFS)	□ 128 (DFS)
□ 132 (DFS)	□ 136 (DFS)	□ 140 (DFS)	□ 144 (DFS)
□ 149	□ 153	□ 157	□ 161

6 GHz channel deployment: Manual — Hide Model list

Figure 156 Site-wide > Configure > Security router > Radio settings Part 2



Channel ID			□ Select all
□ 5	□ 21	□ 37	□ 53
□ 69	□ 85		

Allow 802.11ax/ac/n stations only: ON

If turned ON, legacy clients including 802.11a/b/g will not be allowed to associate.

Smart steering: ON — Enable this function will make AP steer the client to the better signal AP.

ADVANCED OPTIONS

2.4G Setting

Disassociate Station Threshold: -88 dBm (-20 ~ -105)

Optimization aggressiveness: Beta Model list ○ High ● Standard ○ Low

5G Setting

Disassociate Station Threshold: -88 dBm (-20 ~ -105)

Optimization aggressiveness: Beta Model list ○ High ● Standard ○ Low

6G Setting

Disassociate Station Threshold: -88 dBm (-20 ~ -105)

Optimization aggressiveness: Beta Model list ○ High ● Standard ○ Low

802.11d: ON — Enable this function will make AP advertise 802.11d capability

WLAN Rate Control Setting

2.4 GHz: Lower Density 1 Mbps — High Density 54 Mbps

5 GHz: Lower Density 6 Mbps — High Density 54 Mbps

6 GHz Model list: Lower Density 6 Mbps — High Density 54 Mbps

□	Access point	Radio #	Model	Radio mode	Channel	Transmit po...	Channel width	Smart steeri...	Antenna	Airtime fairness
□	20:23:12:21:11:55	1	SCR 60AX	Auto	AUTO (DCS)	30 dBm	20 MHz	Disabled		Disabled
□	BC:CF:4F:E3:7C:...	1	NWA110AX	Auto	AUTO (DCS)	30 dBm	20 MHz	Disabled		Disabled

The following table describes the labels in this screen.

Table 101 Site-wide > Configure > Security router > Radio settings

LABEL	DESCRIPTION
Country	Select the country where the Nebula Device is located or installed. The available channels vary depending on the country you selected. Be sure to select the correct or same country for both radios on a Nebula Device and all connected Nebula Devices in order to prevent roaming failure and interference with other systems.
Deployment selection	Select **High-density (More than 10 APs)** for the lowest output power for 10 or more Access Points. Select **Moderate-density (6-9 APs)** for moderate output power for 5 to 9 Access Points. Select **Low-density (2-5 APs)** for higher concentration of output power for less than 5 Access Points. Select **Single AP** for highest concentration of output power for a single Access Point.
Maximum output power	Selecting any of the options in the **Deployment selection** field will automatically set the maximum output power for 2.4 / 5 / 6 GHz. But you can change the setting (1 – 30 dBm).
Channel width	Select the wireless channel bandwidth you want the Nebula Device to use. A standard 20 MHz channel offers transfer speeds of up to 144 Mbps (2.4 GHz) or 217 Mbps (5 GHz) whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps (2.4 GHz) or 450 Mbps (5 GHz). An IEEE 802.11ac-specific 80 MHz channel offers speeds of up to 1.3 Gbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. An 80 MHz channel consists of two adjacent 40 MHz channels. The WiFi clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. Note: It is suggested that you select **20 MHz** when there is more than one 2.4 GHz Nebula Device in the network.
DCS setting	
DCS time interval	Select **ON** to set the DCS time interval (in minutes) to regulate how often the Nebula Device surveys the other Nebula Devices within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another Nebula Device, the Nebula Device will then dynamically select the next available clean channel or a channel with lower interference.
DCS schedule	Select **ON** to have the Nebula Device automatically find a less-used channel within its broadcast radius at a specific time on selected days of the week. You then need to select each day of the week and specify the time of the day (in 24-hour format) to have the Nebula Device use DCS to automatically scan and find a less-used channel.
DCS client aware	Select **ON** to have the Nebula Device wait until all connected clients have disconnected before switching channels.
Avoid 5G DFS channel	If your Nebula Devices are operating in an area known to have RADAR devices, the Nebula Device will choose non-DFS channels to provide a stable WiFi service.
Blacklist DFS channels in the presence of radar	Select **ON** to blacklist a channel if RADAR is detected. After being blacklisted, the Nebula Device will not use the channel again until the Nebula Device is rebooted. However, the Nebula Device can still use other DFS channels.
2.4 GHz channel deployment	Select **All available channels** to allow channel-hopping to have the Nebula Device automatically select the best channel. Select **Manual** to select the individual channels the Nebula Device switches between.

Table 101 Site-wide > Configure > Security router > Radio settings (continued)

LABEL	DESCRIPTION
5 GHz channel deployment	Select how you want to specify the channels the Nebula Device switches between for 5 GHz operation. Select **All available channels** to have the Nebula Device automatically select the best channel. Select **Manual** to select the individual channels the Nebula Device switches between. Note: The method is automatically set to **All available channels** when no channel is selected or any one of the previously selected channels is not supported.
6 GHz channel deployment	Select how you want to specify the channels the Nebula Device switches between for 6 GHz operation. Select **All available channels** to have the Nebula Device automatically select the best channel. Select **Manual** to select the individual channels the Nebula Device switches between. Note: The method is automatically set to **All available channels** when no channel is selected or any one of the previously selected channels is not supported.
Allow 802.11ax/ac/n stations only	Select **ON** to have the Nebula Device allow only IEEE 802.11n/ac/ax clients to connect, and reject IEEE 802.11a/b/g clients.
Smart Steering	Select **ON** to enable smart client steering on the Nebula Device. Client steering helps monitor WiFi clients and drop their connections to optimize the bandwidth when the clients are idle or have a low signal. When a WiFi client is dropped they have the opportunity to steer to a Nebula Device with a strong signal. Additionally, dual band WiFi clients can also steer from one band to another. Select **OFF** to disable this feature on the Nebula Device.
ADVANCED OPTIONS	Click this to display a greater or lesser number of configuration fields.
2.4G/5G/6G Setting	
Disassociate Station Threshold	Set a minimum kick-off signal strength. When a WiFi client's signal strength is lower than the specified threshold, the Nebula Device disconnects the WiFi client. –20 dBm is the strongest signal you can require and –105 dBm is the weakest.
Optimization aggressiveness	**High**, **Standard** and **Low** stand for different traffic rate threshold levels. The level you select here decides when the Nebula Device takes action to improve the Access Point's WiFi network performance. The Nebula Device will postpone the actions implemented on Access Points until your network is less busy if the threshold is exceeded. Select a suitable traffic rate threshold level for your network. **High**: Select this if you want the Nebula Device to postpone the action set when the Access Point network traffic is heavy. **Standard**: Select this if you want the Nebula Device to postpone the action set when the Access Point network traffic is medium. **Low**: Select this if you want the Nebula Device to postpone the action set when the Access Point network traffic is low.
802.11d	Click this to enable 802.11d on the Access Point. 802.11d is a WiFi network specification, for use in countries where 802.11 WiFi is restricted. Enabling 802.11d causes the Nebula Device to broadcast the country where it is located, which is determined by the Country setting.
WLAN Rate Control Setting	

Table 101   Site-wide > Configure > Security router > Radio settings (continued)

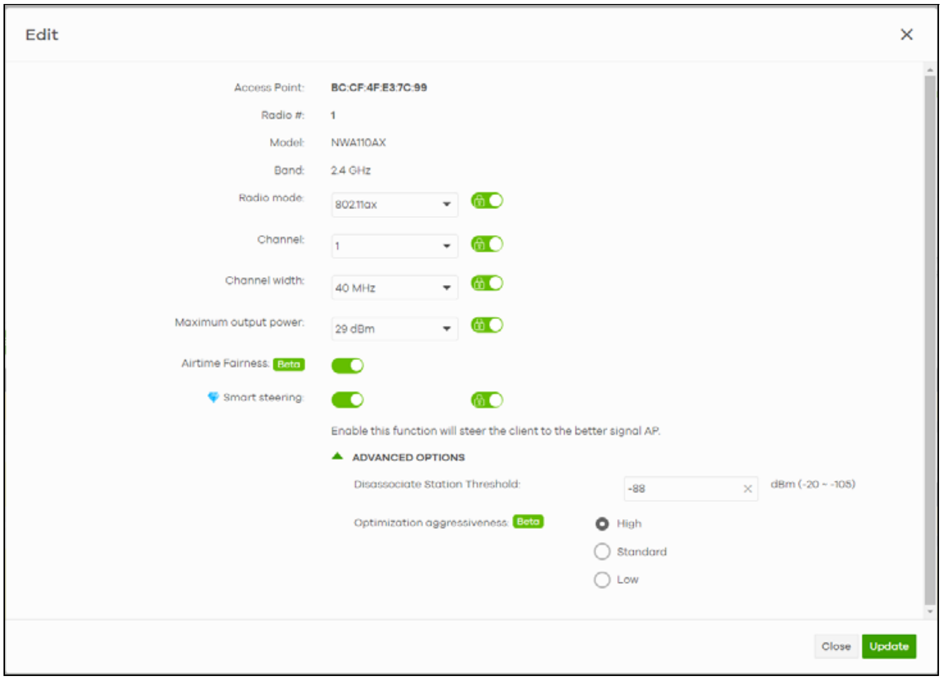
LABEL	DESCRIPTION
2.4 GHz / 5 GHz / 6 GHz	Sets the minimum data rate that 2.4 GHz, 5 GHz, and 6 GHz WiFi clients can connect to the Nebula Device, in Mbps. Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the Nebula Device.
Edit	Click this button to modify the channel, output power, channel width, airtime fairness (the same setting will apply to both 2.4 GHz and 5 GHz), and smart steering settings for the selected Nebula Devices. On the Nebula Device that comes with internal antennas and also has an antenna switch, you can adjust coverage depending on the orientation of the antenna for the Nebula Device radios. Select **Wall** if you mount the Nebula Device to a wall. Select **Ceiling** if the Nebula Device is mounted on a ceiling. You can switch from **Wall** to **Ceiling** if there are still WiFi dead zones, and so on. If you select **Hardware Switch**, you use the physical antenna switch to adjust coverage and apply the same antenna orientation settings to both radios.  Edit Access Point: BC:CF:4F:E3:7C:99 Radio #: 1 Model: NWA110AX Band: 2.4 GHz Radio mode: 802.11ax Channel: 1 Channel width: 40 MHz Maximum output power: 29 dBm Airtime Fairness: Beta Smart steering: Enable this function will steer the client to the better signal AP. ADVANCED OPTIONS Disassociate Station Threshold: -88 dBm (-20 ~ -105) Optimization aggressiveness: Beta ● High ○ Standard ○ Low Close Update Note: On this screen, you can set channel width to 160 MHz for the 5/6 GHz channel or 320 MHz for the 6 GHz channel, if the Nebula Device supports it.
DCS Now	Click this button to have the selected Nebula Devices immediately scan for and select a channel that has least interference.
List	Click this to display a list of all connected Nebula Devices.
Map	Click this to display the locations of all connected Nebula Devices on the Google map.
2.4 GHz	Click this to display the connected Nebula Devices using the 2.4 GHz frequency band.
5 GHz	Click this to display the connected Nebula Devices using the 5 GHz frequency band.
6 GHz	Click this to display the connected Nebula Devices using the 6 GHz frequency band.
BandFlex	Click this to display the connected Nebula Devices that supports BandFlex (5 GHz or 6 GHz frequency bands).
Hide transmit circles	Click this button to not show the transmission range on the Map.
Access point	This displays the descriptive name or MAC address of the connected Nebula Device.

Table 101 Site-wide > Configure > Security router > Radio settings (continued)

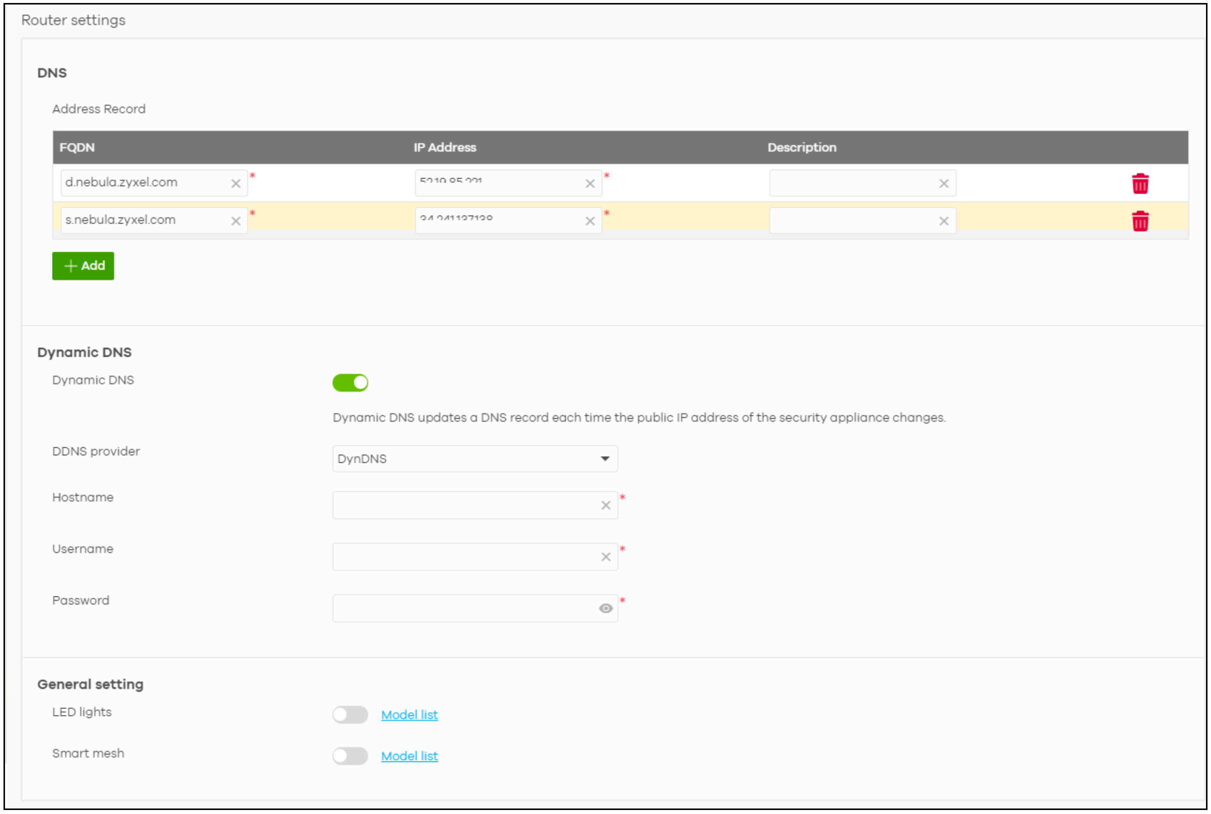
LABEL	DESCRIPTION
Radio #	This displays the number of the connected Nebula Device's radio.
Model	This displays the model name of the connected Nebula Device.
Radio mode	This displays the type of WiFi radio the Nebula Device is currently using, for example 802.11b/g/n.
Channel	This displays the channel ID currently being used by the connected Nebula Device's radio.
Transmit power	This displays the current transmitting power of the connected Nebula Device's radio. If the Nebula Device is offline, this shows the maximum output power you configured for the Nebula Device.
Channel width	This displays the wireless channel bandwidth the connected Nebula Device's radio is set to use.
Smart steering	This displays whether smart client steering is enabled or disabled on the connected Nebula Devices.
Antenna	This displays the antenna orientation settings for the Nebula Device that comes with internal antennas and also has an antenna switch.
Airtime fairness	This displays whether airtime fairness is enabled or disabled on the connected Nebula Device.
☰	Click this icon to display a greater or lesser number of configuration fields. For faster loading of data, select only the configuration fields listed that do NOT take a long time to fetch data.

7.3.10 Router Settings

Use this screen to configure DNS settings.

Click **Site-wide** > **Configure** > **Security router** > **Router settings** to access this screen.

Figure 157 Site-wide > Configure > Security router > Router settings



Router settings

DNS

Address Record

FQDN	IP Address	Description	
d.nebula.zyxel.com *	5219.85.221 *		🗑
s.nebula.zyxel.com *	34.241137138 *		🗑

+ Add

Dynamic DNS

Dynamic DNS: ●

Dynamic DNS updates a DNS record each time the public IP address of the security appliance changes.

DDNS provider: DynDNS

Hostname: *

Username: *

Password: *

General setting

LED lights: ○ Model list

Smart mesh: ○ Model list

The following table describes the labels in this screen.

Table 102 Site-wide > Configure > Security router > Router settings

LABEL	DESCRIPTION
DNS	
Address Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.
FQDN	Enter a host’s fully qualified domain name. Use up to 247 characters, a-ZA-Z0-9.–. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the host’s IP address.
Description	Enter the descriptive name of the DNS record of up to 255 printable ASCII characters.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry, maximum up to 20.
Dynamic DNS	
Dynamic DNS	Click On to use dynamic DNS. Otherwise, select Off to disable it.
DDNS provider	Select your Dynamic DNS service provider from the drop-down list box. If you select **User customize**, create your own DDNS service.
Hostname	Enter the domain name you registered.
Username	Enter the user name (email format) used when you registered your domain name. Up to 253 characters, A-Za-z0-9@.–_.

Table 102   Site-wide > Configure > Security router > Router settings (continued)

LABEL	DESCRIPTION
Password	Enter the password provided by the DDNS provider. Up to 53 characters, 0-9a-zA-Z~!@#$%^&*()_-+={[}] | \:;"'<,>.?/
Connection type	Select **Http** (Hypertext Transfer Protocol) to use the standard protocol for sending data between a browser and a website. HTTP transmits data in plain text, which means that third parties can intercept and read the information. Select **Https** (Hypertext Transfer Protocol Secure) to use HTTP with encryption and verification. This prevents third parties from eavesdropping on communications to and from the server.
URL	Enter the URL that can be used to access the server that will host the DDNS service.
General setting	
LED lights	Click to turn on or off the LEDs on the Nebula Devices. Click **Model list** to see the supported Security router.
Smart mesh	Click to enable or disable the Nebula Smart Mesh feature on all Nebula Devices in the site. Click **Model list** to see whether your Nebula Device supports Nebula Smart Mesh. Note: Nebula Smart Mesh is a WiFi mesh solution for Nebula Devices. For details, see Section 5.1.1 on page 303. Note: You can override NCC settings and enable or disable Smart Mesh on individual Nebula Devices. For details, see Section 4.3.1.1 on page 218. Note: Disabling Nebula Device Smart Mesh automatically disables wireless bridge on all Nebula Devices in the site. For details on wireless bridge, see Section 4.3.1.1 on page 218. Note: At the time of writing, the Security Router may only act as the root AP. Note: At the time of writing, the Security Router does not support wireless bridge.

CHAPTER 8 Firewall

8.1 Overview

This chapter describes the menus used to monitor and configure the Hybrid Security Firewall devices that acts as a security gateway in the current organization.

Nebula Device (also called Security Firewall device) refers to ZyWALL ATP / USG FLEX / USG20(W)-VPN Series devices in this chapter. The **Firewall** menus are shown for Security Firewall devices only.

8.2 Monitor

Use the **Monitor** menus to check the Nebula Device information, client information, event log messages and summary report for the Nebula Device in the selected site.

8.2.1 Clients

This menu item redirects to **Site-wide** > **Monitor** > **Clients**, with type set to **Security firewall clients**. For details, see Section 4.5 on page 258.

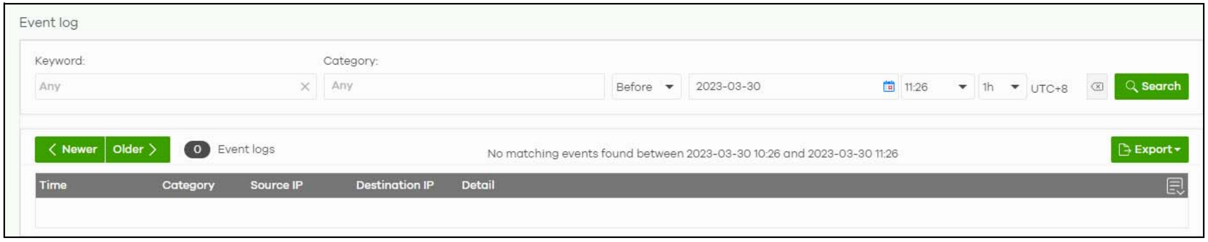
8.2.2 Event Log

Use this screen to view Nebula Device log messages. You can enter a key word, select one or multiple event types, or specify a date/time or a time range to display only the log messages that match these criteria.

Select **Range** to set a time range or select **Before** to choose a specific date/time and the number of hours/minutes to display only the log messages generated within a certain period of time (before the specified date/time). Then click **Search** to update the list of logs based on the search criteria. The maximum allowable time range is 30 days.

Click **Site-wide** > **Monitor** > **Firewall** > **Event log** to access this screen.

Figure 158 Site-wide > Monitor > Firewall > Event log



Event log

Keyword: Any

Category: Any

Before 2023-03-30 11:26 1h UTC+8

0 Event logs

No matching events found between 2023-03-30 10:26 and 2023-03-30 11:26

Time	Category	Source IP	Destination IP	Detail

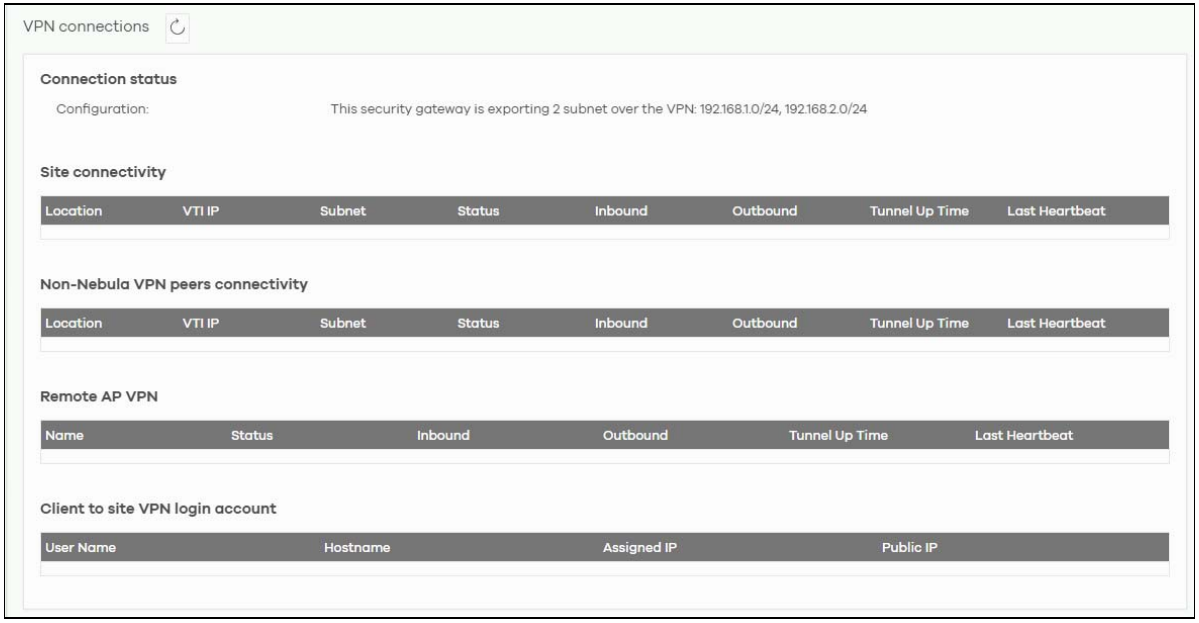
8.2.3 VPN Connections

Use this screen to view the status of site-to-site IPSec VPN connections and L2TP VPN connections.

Note: If the peer gateway is not a Nebula Device, go to the **Firewall** > **Configure** > **Site-to-Site VPN** screen to view and configure a VPN rule. See Section 8.3.6 on page 505 for more information.

Click **Site-wide** > **Monitor** > **Firewall** > **VPN connections** to access this screen.

Figure 159 Site-wide > Monitor > Firewall > VPN connections



VPN connections ↻

Connection status

Configuration: This security gateway is exporting 2 subnet over the VPN: 192.168.1.0/24, 192.168.2.0/24

Site connectivity

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat

Non-Nebula VPN peers connectivity

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat

Remote AP VPN

Name	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat

Client to site VPN login account

User Name	Hostname	Assigned IP	Public IP

The following table describes the labels in this screen.

Table 103 Site-wide > Monitor > Firewall > VPN connections

LABEL	DESCRIPTION
↻	Click this button to reload the data on this page.
Connection Status	
Configuration	This shows the number and address of the local networks behind the Nebula Device, on which the computers are allowed to use the VPN tunnel.
Site Connectivity	
Location	This shows the name of the site to which the Nebula peer gateway is assigned. Click the name to view the **VPN usage and connectivity** status screen.
VTI IP	This shows the IP address for this connection. IPSec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.
Subnet	This shows the address of the local networks behind the Nebula peer gateway.
Status	This shows whether the VPN tunnel is connected or disconnected.
Inbound	This shows the amount of traffic that has gone through the VPN tunnel from the Non-Nebula peer gateway to the Nebula Device since the VPN tunnel was established.
Outbound	This shows the amount of traffic that has gone through the VPN tunnel from the Nebula Device to the Non-Nebula peer gateway since the VPN tunnel was established.
Tunnel up time	This shows how many seconds the VPN tunnel has been active.

Table 103 Site-wide > Monitor > Firewall > VPN connections (continued)

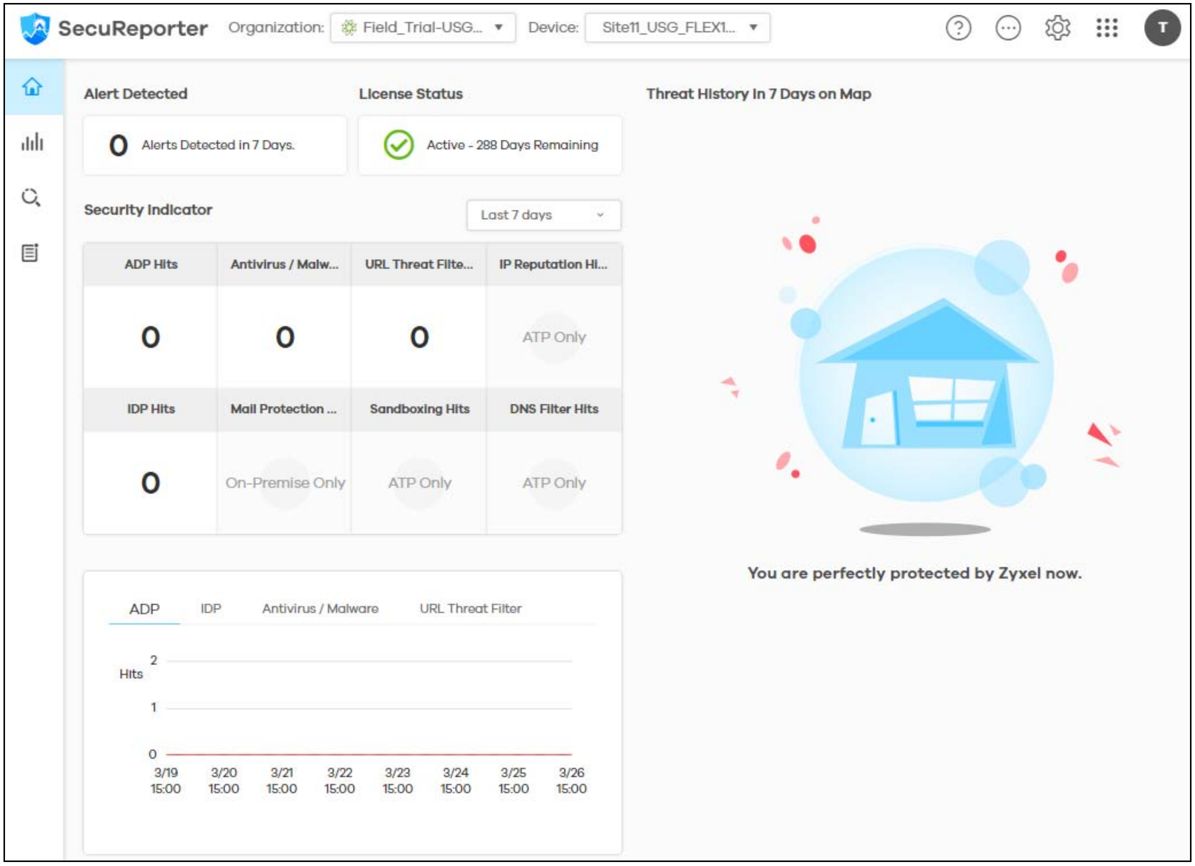
LABEL	DESCRIPTION
Last heartbeat	This shows the last date and time a heartbeat packet is sent to determine if the VPN tunnel is up or down.
Non-Nebula VPN peers connectivity	
Location	This shows the name of the site to which the Non-Nebula peer gateway (Zyxel or non-Zyxel IPSec VPN gateway and Cloud VPN (Azure VPN or AWS VPN)) is assigned. Click the name to go to the **Site-wide** > **Configure** > **Firewall** > **Site-to-Site VPN** screen, where you can modify the VPN settings.
VTI IP	This shows the IP address for this connection. IPSec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.
Subnet	This shows the address of the local networks behind the Non-Nebula peer gateway.
Status	This shows whether the VPN tunnel is connected or disconnected.
Inbound	This shows the amount of traffic that has gone through the VPN tunnel from the Non-Nebula peer gateway to the Nebula Device since the VPN tunnel was established.
Outbound	This shows the amount of traffic that has gone through the VPN tunnel from the Nebula Device to the Non-Nebula peer gateway since the VPN tunnel was established.
Tunnel up time	This shows how many seconds the VPN tunnel has been active.
Last heartbeat	This shows the last date and time a heartbeat packet was sent to determine if the VPN tunnel is up or down.
Remote AP VPN	
Name	This shows the name of the remote access point (AP).
Status	This shows whether the VPN tunnel is connected or disconnected.
Inbound	This shows the amount of traffic that has gone through the VPN tunnel from the remote AP to the Nebula Device since the VPN tunnel was established.
Outbound	This shows the amount of traffic that has gone through the VPN tunnel from the Nebula Device to the remote AP since the VPN tunnel was established.
Tunnel up time	This shows how many seconds the VPN tunnel has been active.
Last heartbeat	This shows the last date and time a heartbeat packet is sent to determine if the VPN tunnel is up or down.
Client to site VPN login account	
User Name	This shows the remote user's login account name.
Hostname	This shows the name of the computer that has this L2TP VPN connection with the Nebula Device.
Tunnel up time	This shows how many seconds the VPN tunnel has been active.
Assigned IP	This shows the IP address that the Nebula Device assigned for the remote user's computer to use within the L2TP VPN tunnel.
Public IP	This shows the public IP address that the remote user is using to connect to the Internet.

8.2.4 SecuReporter

Click **Site-wide** > **Monitor** > **Firewall** > **SecuReporter** to open SecuReporter for the current organization and site. SecuReporter allows you to view statistics for the following Nebula Security Services (NSS): Content filter, Intrusion Detection and Prevention (IDP), application patrol, anti-virus, anti-malware, URL threat filter.

Note: For more details, see the SecuReporter User's Guide.

Figure 160 Site-wide > Monitor > Firewall > SecuReporter



Alert Detected

0 Alerts Detected in 7 Days.

License Status

Active - 288 Days Remaining

Threat History In 7 Days on Map

Security Indicator

Last 7 days

ADP Hits	Antivirus / Malw...	URL Threat Filte...	IP Reputation Hi...
0	0	0	ATP Only
IDP Hits	**Mail Protection ...**	**Sandboxing Hits**	**DNS Filter Hits**
0	On-Premise Only	ATP Only	ATP Only

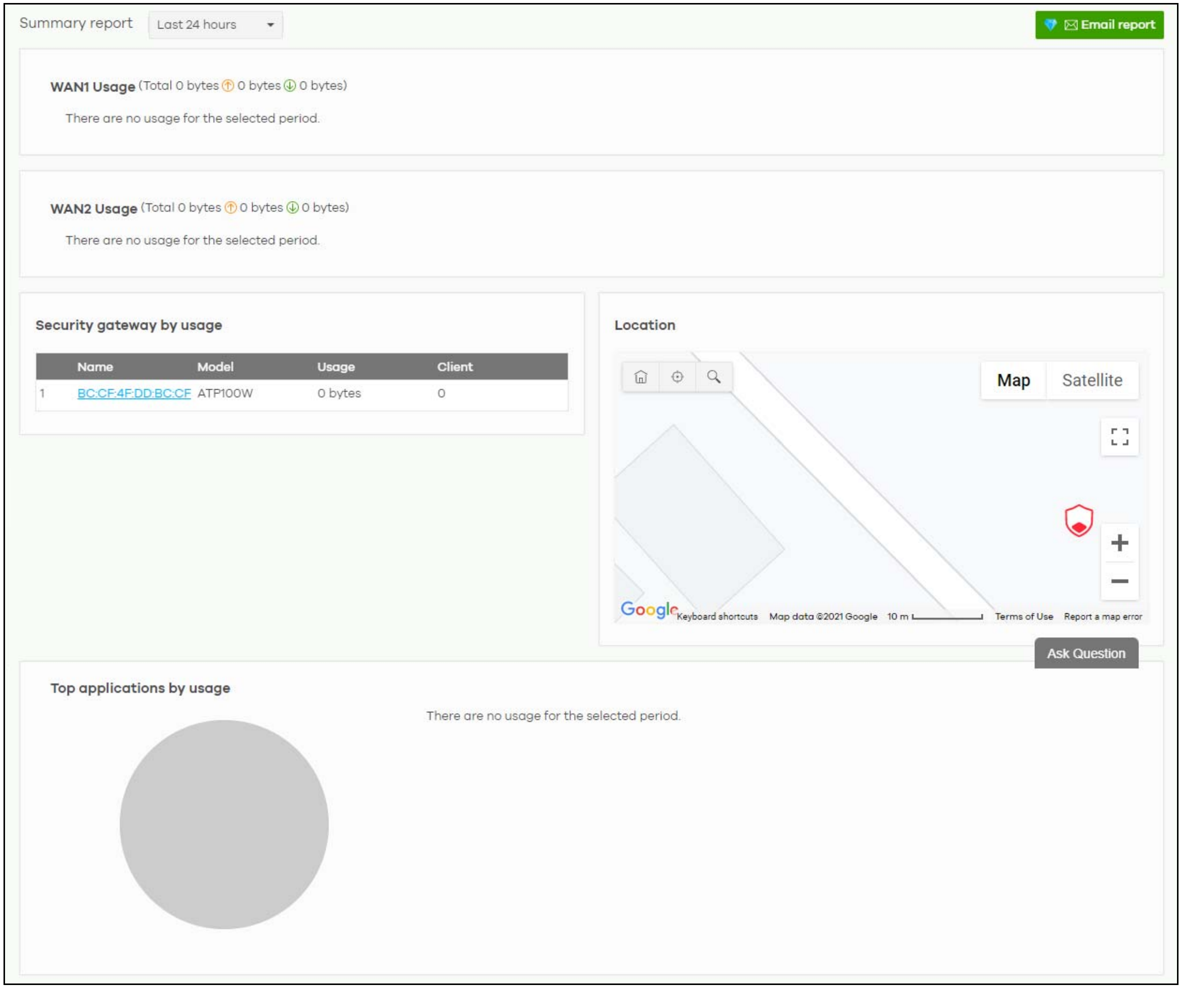
You are perfectly protected by Zyxel now.

8.2.5 Summary Report

This screen displays network statistics for the Nebula Device of the selected site, such as WAN usage, top applications and/or top clients.

Click **Site-wide** > **Monitor** > **Firewall** > **Summary report** to access this screen.

Figure 161 Site wide > Monitor > Firewall > Summary report



Summary report Last 24 hours

Email report

WAN1 Usage (Total 0 bytes ⇧ 0 bytes ⇩ 0 bytes)

There are no usage for the selected period.

WAN2 Usage (Total 0 bytes ⇧ 0 bytes ⇩ 0 bytes)

There are no usage for the selected period.

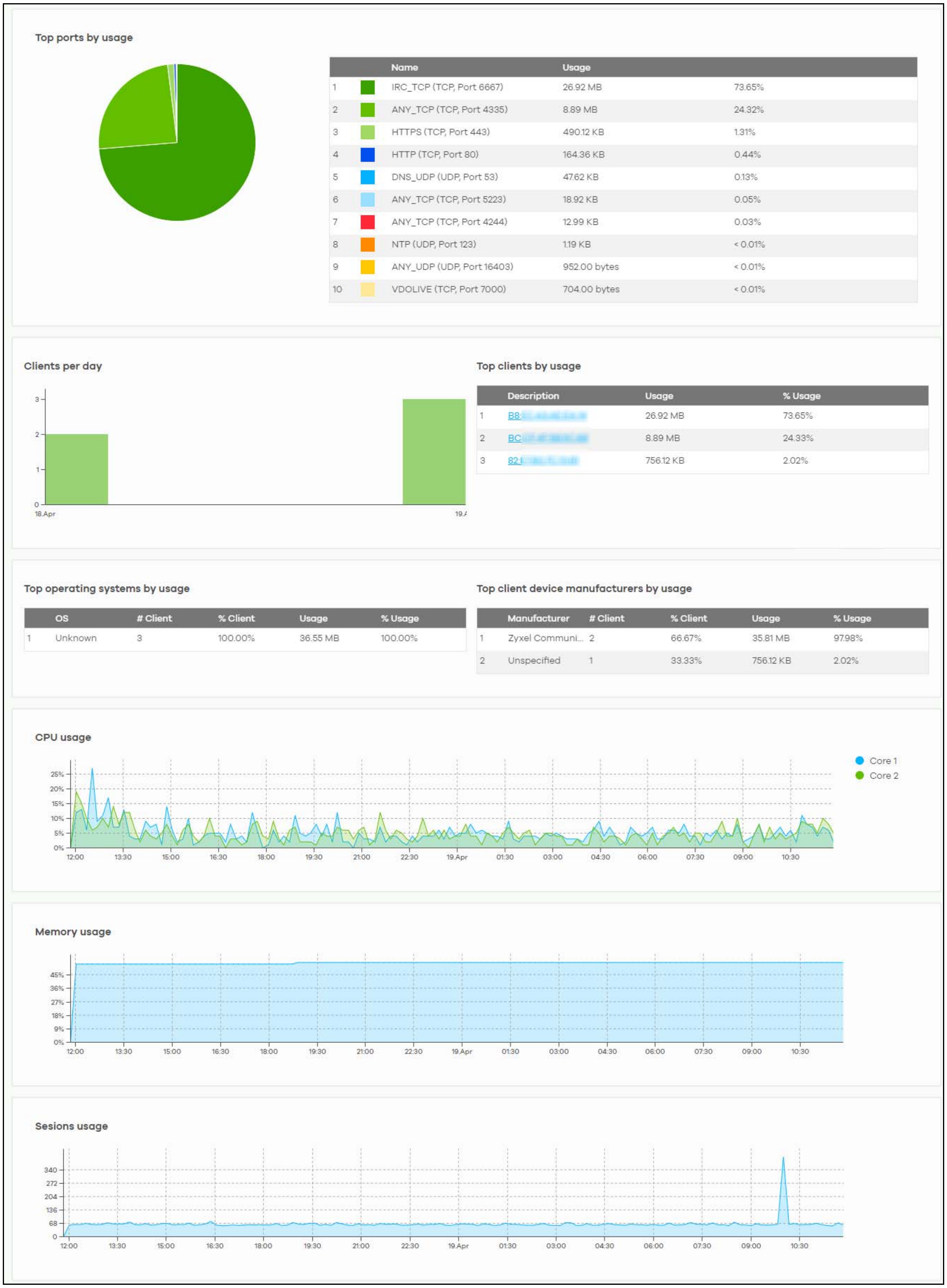
Security gateway by usage

	Name	Model	Usage	Client
1	BC:CF:4F:DD:BC:CF	ATP100W	0 bytes	0

Location

Top applications by usage

There are no usage for the selected period.



Top ports by usage

		Name	Usage	
1	🟩	IRC_TCP (TCP, Port 6667)	26.92 MB	73.65%
2	🟩	ANY_TCP (TCP, Port 4335)	8.89 MB	24.32%
3	🟩	HTTPS (TCP, Port 443)	490.12 KB	1.31%
4	🟦	HTTP (TCP, Port 80)	164.36 KB	0.44%
5	🟦	DNS_UDP (UDP, Port 53)	47.62 KB	0.13%
6	🟦	ANY_TCP (TCP, Port 5223)	18.92 KB	0.05%
7	🟥	ANY_TCP (TCP, Port 4244)	12.99 KB	0.03%
8	🟧	NTP (UDP, Port 123)	1.19 KB	< 0.01%
9	🟨	ANY_UDP (UDP, Port 16403)	952.00 bytes	< 0.01%
10	🟨	VDOLIVE (TCP, Port 7000)	704.00 bytes	< 0.01%

Clients per day

Top clients by usage

	Description	Usage	% Usage
1	B8:[redacted]	26.92 MB	73.65%
2	BC[redacted]	8.89 MB	24.33%
3	82:[redacted]	756.12 KB	2.02%

Top operating systems by usage

	OS	# Client	% Client	Usage	% Usage
1	Unknown	3	100.00%	36.55 MB	100.00%

Top client device manufacturers by usage

	Manufacturer	# Client	% Client	Usage	% Usage
1	Zyxel Communi...	2	66.67%	35.81 MB	97.98%
2	Unspecified	1	33.33%	756.12 KB	2.02%

CPU usage

Memory usage

Sesions usage

The following table describes the labels in this screen.

Table 104 Site-wide > Monitor > Firewall > Summary report

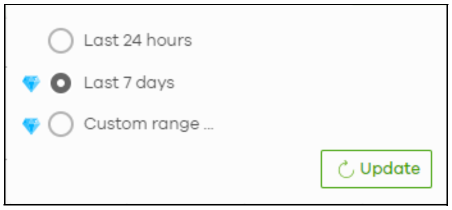
LABEL	DESCRIPTION
Security gateway – Summary report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ● Last 7 days ○ Custom range ... Update
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
WAN usage	
y-axis	The y-axis shows the transmission speed of data sent or received through the WAN connection in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
VPN usage	
y-axis	The y-axis shows the transmission speed of data sent or received through the VPN tunnel in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Nebula VPN usage	
y-axis	The y-axis shows the transmission speed of data sent or received through the VPN tunnels, in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Non-Nebula VPN usage	
y-axis	The y-axis shows the transmission speed of data sent or received through VPN tunnels, in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Remote AP VPN usage	
y-axis	The y-axis shows the transmission speed of data sent or received through the VPN tunnel between the Nebula Device and remote APs, in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Security gateway by usage	
	This shows the index number of the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Usage	This shows the amount of data that has been transmitted through the Nebula Device's WAN port.
Client	This shows the number of clients currently connected to the Nebula Device.
Location This shows the location of the Nebula Devices on the map.	
Top applications by usage	
	This shows the index number of the application.
Application	This shows the application name.

Table 104 Site-wide > Monitor > Firewall > Summary report (continued)

LABEL	DESCRIPTION
Category	This shows the name of the category to which the application belongs.
Usage	This shows the amount of data consumed by the application.
% Usage	This shows the percentage of usage for the application.
Top ports by usage	
	This shows the top ten applications/services and the ports that identify a service.
Name	This shows the service name and the associated port numbers.
Usage	This shows the amount of data consumed by the service.
% Usage	This shows the percentage of usage for the service.
Clients per day	
y-axis	The y-axis represents the number of clients.
x-axis	The x-axis represents the date.
Top clients by usage	
	This shows the index number of the client.
Description	This shows the descriptive name or MAC address of the client.
Usage	This shows the total amount of data transmitted and received by the client.
% Usage	This shows the percentage of usage for the client.
Top operating systems by usage	
	This shows the index number of the operating system.
OS	This shows the operating system of the client device.
# Client	This shows how many client devices use this operating system.
% Client	This shows the percentage of top client devices which use this operating system.
% Usage	This shows the percentage of usage for top client devices which use this operating system.
Top client device manufacturers by usage	
	This shows the index number of the client device.
Manufacturer	This shows the manufacturer name of the client device.
Client	This shows how many client devices are made by the manufacturer.
% Client	This shows the percentage of top client devices which are made by the manufacturer.
Usage	This shows the total amount of data transmitted and received by the client device.
% Usage	This shows the percentage of usage for the client device.
CPU usage	
y-axis	The y-axis shows what percentage of the Nebula Device's processing capability is currently being used.
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Memory usage	
y-axis	The y-axis shows what percentage of the Nebula Device's RAM is currently being used.
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Sessions usage	
y-axis	The y-axis shows how many sessions, both established and non-established, that were create from, to, or within the Nebula Device, or passed through the Nebula Device.
x-axis	The x-axis shows the time period over which the traffic flow occurred.

8.3 Configure

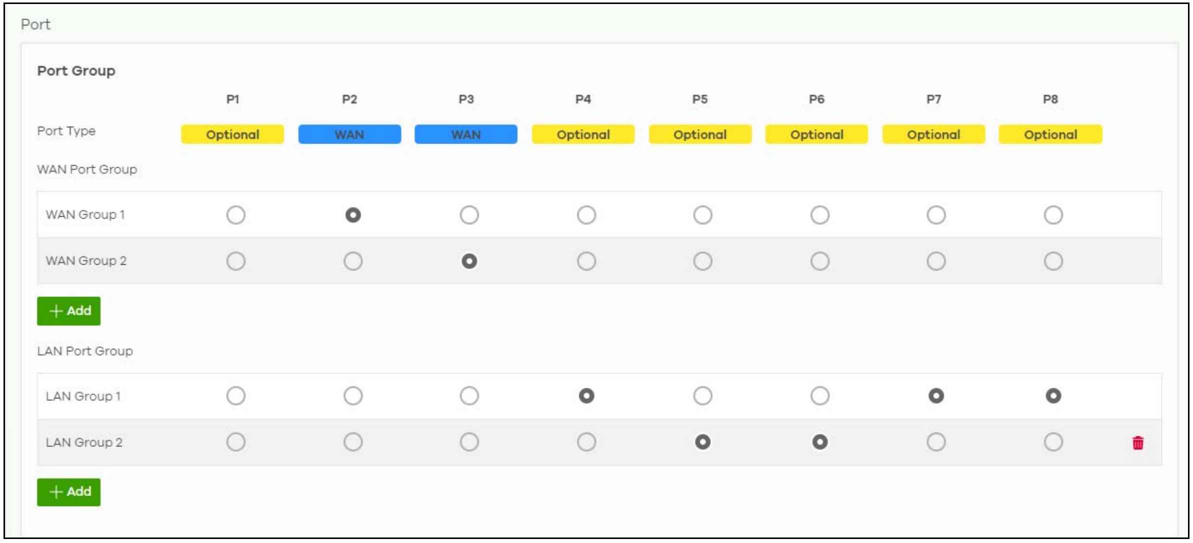
Use the **Configure** menus to configure interface addressing, firewall, site-to-site VPN, captive portal, traffic shaping, authentication server and other gateway settings for the Nebula Device of the selected site.

Note: Only one Security Appliance is allowed per site.

8.3.1 Port

Use this screen to configure port groups on the Nebula Device. To access this screen, click **Firewall** > **Configure** > **Port**.

Figure 162 Site-wide > Configure > Firewall > Port



Port

Port Group

	P1	P2	P3	P4	P5	P6	P7	P8	
Port Type	Optional	WAN	WAN	Optional	Optional	Optional	Optional	Optional	
WAN Port Group									
WAN Group 1	○	●	○	○	○	○	○	○	
WAN Group 2	○	○	●	○	○	○	○	○	
LAN Port Group									
LAN Group 1	○	○	○	●	○	○	●	●	
LAN Group 2	○	○	○	○	●	●	○	○	🗑

The following table describes the labels in this screen.

Table 105 Site-wide > Configure > Firewall > Port

LABEL	DESCRIPTION
Port Group	Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level. The physical LAN Ethernet ports, for example P1, P2, P3, are shown at the top of the screen. The port groups are shown at the left of the screen. Use the radio buttons to select which ports are in each port group. For example, to add port **P3** to **LAN Group 1**, select P3's radio button in the LAN Group 1 row. Note: See Table 1 on page 14 for the list of Nebula Device that do NOT have a P1 port.
Port Type	This shows whether the port is a **WAN** port or a **LAN** port. **Optional** means the port can be assigned as either WAN or LAN, by adding it to a WAN or LAN group.
WAN Port Group	
WAN Group 1	This shows the name of the WAN port group. Note: Each WAN port group can only contain one port.
🗑	Click this icon to remove a WAN port group.

Table 105   Site-wide > Configure > Firewall > Port (continued)

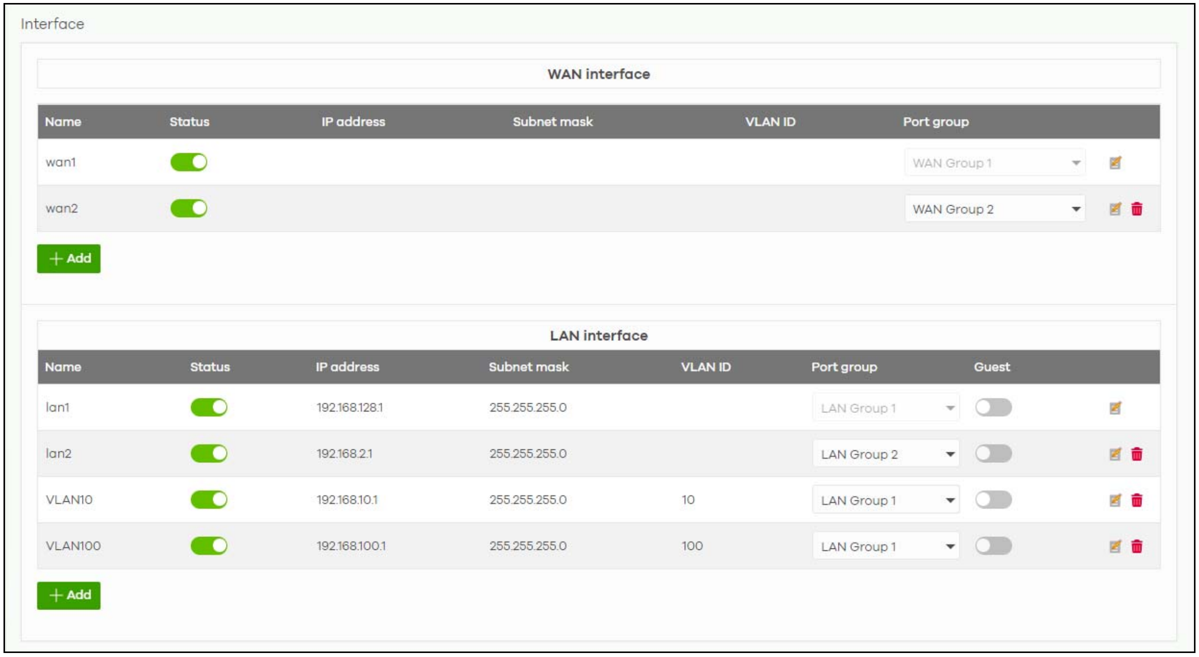
LABEL	DESCRIPTION
Add	Click this button to create a new WAN port group.
LAN Port Group	
LAN Group 1	This shows the name of the LAN port group.
🗑	Click this icon to remove a LAN port group.
Add	Click this button to create a new LAN port group.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

8.3.2 Interface

Use this screen to configure network interfaces on the Nebula Device. An interface consists of a port group, a VLAN ID, and an IP address, plus other configuration settings.

To access this screen, click **Site-wide** > **Configure** > **Firewall** > **Interface**.

Figure 163   Site-wide > Configure > Firewall > Interface



Interface

WAN interface

Name	Status	IP address	Subnet mask	VLAN ID	Port group
wan1	●				WAN Group 1
wan2	●				WAN Group 2

+ Add

LAN interface

Name	Status	IP address	Subnet mask	VLAN ID	Port group	Guest
lan1	●	192.168.128.1	255.255.255.0		LAN Group 1	○
lan2	●	192.168.2.1	255.255.255.0		LAN Group 2	○
VLAN10	●	192.168.10.1	255.255.255.0	10	LAN Group 1	○
VLAN100	●	192.168.100.1	255.255.255.0	100	LAN Group 1	○

+ Add

The following table describes the labels in this screen.

Table 106   Site-wide > Configure > Firewall > Interface

LABEL	DESCRIPTION
WAN Interface	
Name	This field is read-only if you are editing an existing WAN interface. Specify a name for the interface. The format of interface names is strict. Each name consists of 2 – 4 letters (interface type), followed by a number (x). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, VLAN interfaces are vlan0, vlan1, vlan2, and so on.

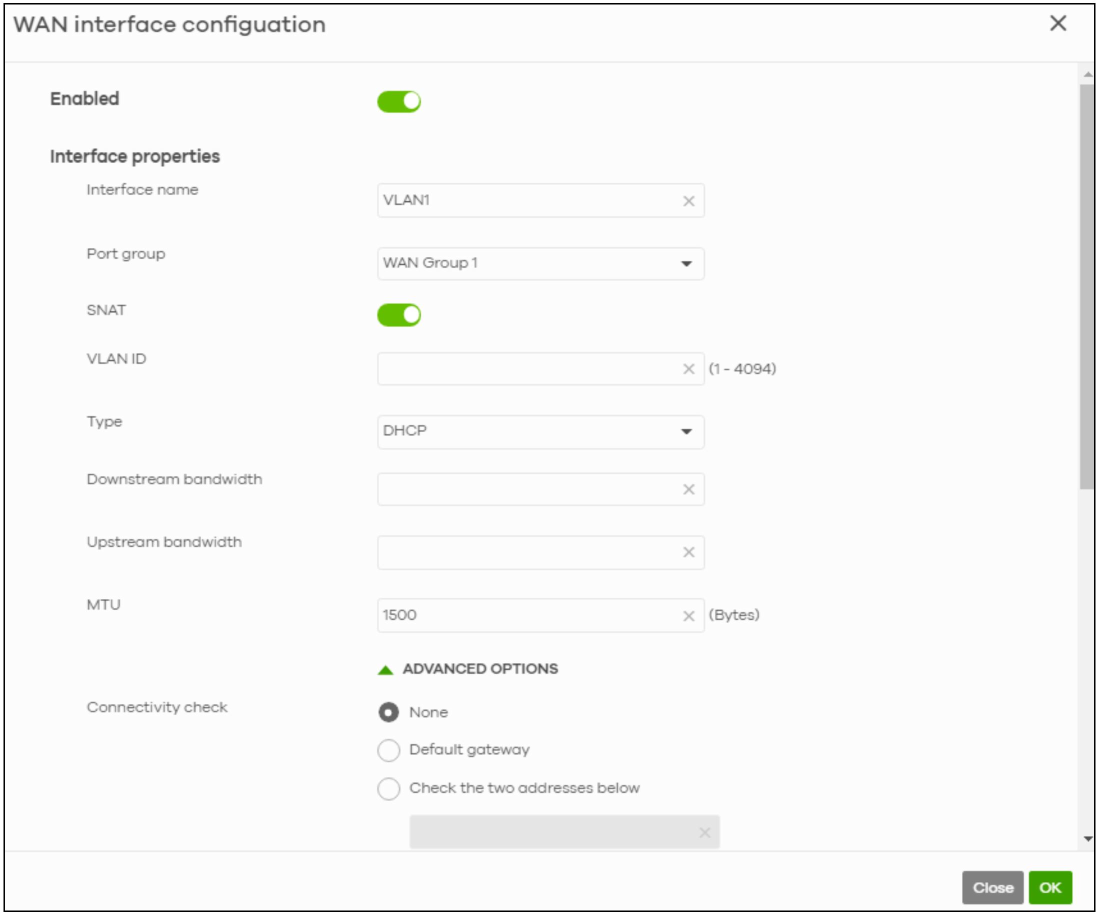
Table 106   Site-wide > Configure > Firewall > Interface (continued)

LABEL	DESCRIPTION
Status	Select this to activate the selected WAN interface.
IP address	This shows the IP address for this interface.
Subnet mask	This shows the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	This shows the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.) Note: NCC will show an error message when the VLAN ID in the interface is configured to be the same as the WAN port's VLAN ID.
Port group	Select the name of the port group to which you want the interface (network) to belong.
✎	Click the edit icon to modify the interface.
🗑	Click the remove icon to delete the interface.
Add	Click this button to create a virtual WAN interface, which associates a VLAN with a WAN port group.
LAN Interface	
Name	This field is read-only if you are editing an existing LAN interface. Specify a name for the interface. The format of interface names is strict. Each name consists of 2 – 4 letters (interface type), followed by a number (x). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, VLAN interfaces are vlan0, vlan1, vlan2, and so on.
Status	Select this to activate the LAN interface.
IP address	This is the IP address for this interface.
Subnet mask	This is the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	This is the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.) Note: NCC will show an error message when the VLAN ID in the Security Firewall interface is configured to be the same as the WAN port's VLAN ID.
Port group	Select the name of the port group to which you want the interface (network) to belong.
Guest	Click the switch to the right to configure this interface as a Guest interface. Client devices connected to this Guest interface have Internet access but cannot access a non-guest interface. Alternatively, click the switch to the left to disable Internet access for client devices connected to this Guest interface.
✎	Click the edit icon to modify it.
🗑	Click the remove icon to delete it.
Add	Click this button to create a virtual LAN interface, which associates a VLAN with a LAN port group.

8.3.2.1 WAN Interface Configuration

Click the **Add** button or click the **Edit** button in the **WAN Interface** section to open the **Site-wide** > **Configure** > **Firewall** > **Interface** > **WAN interface configuration** screen.

Figure 164 Site-wide > Configure > Firewall > Interface > WAN interface configuration



WAN interface configuation

Enabled

Interface properties

Interface name: VLAN1

Port group: WAN Group 1

SNAT

VLAN ID: (1 - 4094)

Type: DHCP

Downstream bandwidth

Upstream bandwidth

MTU: 1500 (Bytes)

ADVANCED OPTIONS

Connectivity check: ● None ○ Default gateway ○ Check the two addresses below

The following table describes the labels in this screen.

Table 107 Site-wide > Configure > Firewall > Interface > WAN interface configuration

LABEL	DESCRIPTION
Enable	Select this to enable the WAN interface.
Interface properties	
Interface name	Specify a name for the WAN interface.
Port group	Select the name of the port group to which you want the interface (network) to belong.
SNAT	Select this to enable SNAT. When enabled, the Nebula Device rewrites the source address of packets being sent from this interface to the interface's IP address.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.)

Table 107 Site-wide > Configure > Firewall > Interface > WAN interface configuration (continued)

LABEL	DESCRIPTION
Type	Select the type of interface to create. **DHCP**: The interface will automatically get an IP address and other network settings from a DHCP server. **Static**: You must manually configure an IP address and other network settings for the interface. **PPPoE**: The interface will authenticate with an Internet Service Provider, and then automatically get an IP address from the ISP's DHCP server. You can use this type of interface to connect to a DSL modem. **PPPoE with static IP**: Assign a static IP address to the WAN interface and your WAN interface is getting an Internet connection from a PPPoE server.
IP address assignment	These fields are displayed if you select **Static**.
IP address	Enter the static IP address of this interface. Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
Subnet mask	Enter the subnet mask for this interface's IP address.
Default gateway	Enter the IP address of the Nebula Device through which this interface sends traffic.
First DNS server	Enter a DNS server's IP address. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Nebula Device uses the first and second DNS servers, in that order to resolve domain names for VPN, DDNS and the time server. Leave the field blank if you do not want to configure DNS servers.
Second DNS server	Enter the IP address of another DNS server. This field is optional.
These fields are displayed if you selected **PPPoE** or **PPPoE with static IP**.	
Authentication Type	Select an authentication protocol for outgoing connection requests. Options are: • **Chap/PAP** – The Nebula Device accepts either CHAP or PAP when requested by the remote node. • **Chap** – The Nebula Device accepts CHAP only. • **PAP** – The Nebula Device accepts PAP only. • **MSCHAP** – The Nebula Device accepts MSCHAP only. • **MSCHAP-V2** – The Nebula Device accepts MSCHAP-V2 only.
Username	Enter the user name provided by your ISP. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed.
Password	Enter the password provided by your ISP. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
Retype password	Enter the password again to confirm it.
Downstream bandwidth	Enter the downstream bandwidth of the WAN connection. This value is used for WAN load balancing by algorithms such as weighed round robin.
Upstream bandwidth	Enter the upstream bandwidth of the WAN connection. This value is used for WAN load balancing by algorithms such as weighed round robin.
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Nebula Device divides it into smaller fragments. Allowed values are 576 – 1500.
ADVANCED OPTIONS	

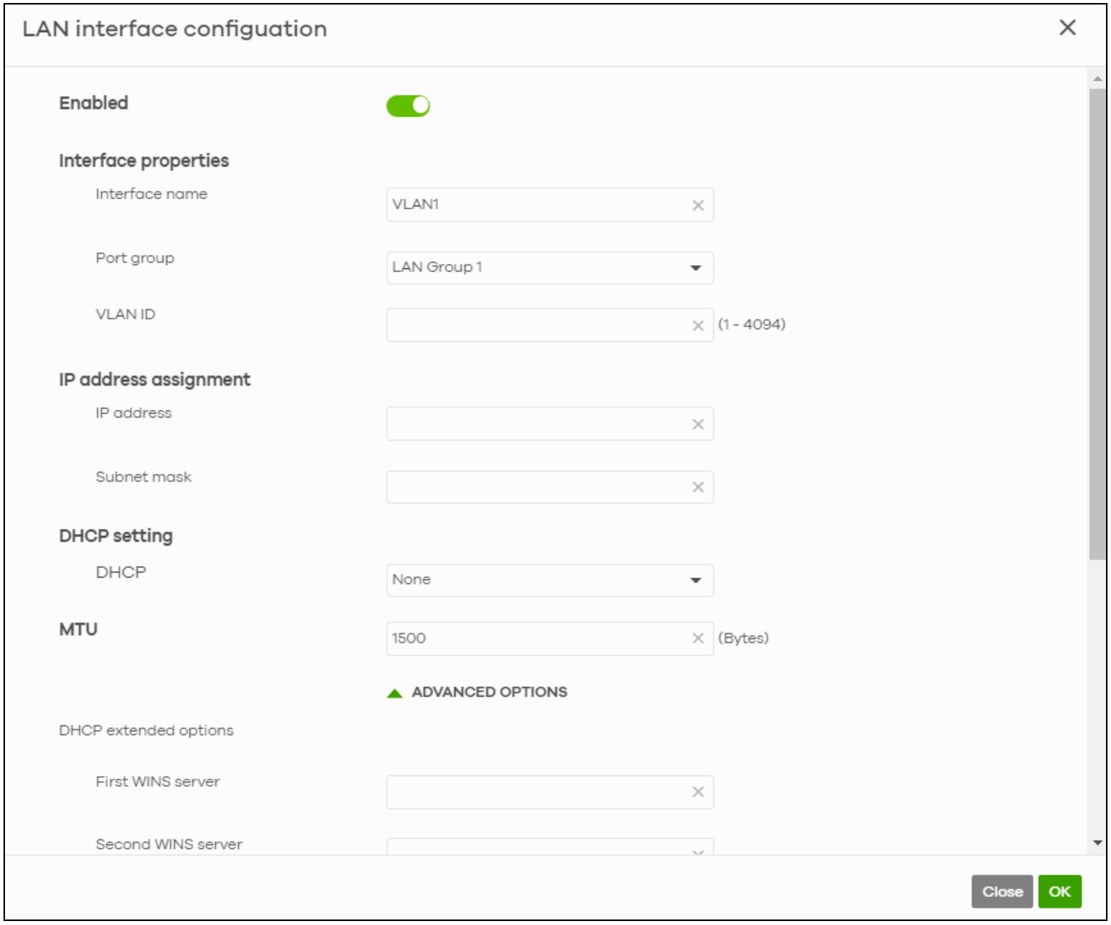
Table 107 Site-wide > Configure > Firewall > Interface > WAN interface configuration (continued)

LABEL	DESCRIPTION
Connectivity check	The interface can periodically check whether it can connect to its default gateway (**Default gateway**), or to two user-specified servers (**Check the two addresses below**). If the check fails, the interface's status changes to **Down**. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Nebula Device stops routing to the gateway.
Probe Succeeds When	This field applies when you select **Check the two addresses** and specify two domain names or IP addresses for the connectivity check. Select **any one** if you want the check to pass if at least one of the domain names or IP addresses responds. Select **all** if you want the check to pass only if both domain names or IP addresses respond.
Proxy ARP	Proxy ARP (RFC 1027) allows the Nebula Device to answer external interface ARP requests on behalf of a device on its internal interface. Click **Add new** to add the IP address or IP range of devices that the interface will answer proxy ARP requests for.
IP Address	Enter a single IPv4 address, an IPv4 CIDR (for example, 192.168.1.1/24) or an IPv4 Range (for example, 192.168.1.2–192.168.1.100). The Nebula Device answers external ARP requests if they match one of these target IP addresses. For example, if the IPv4 address is 192.168.1.5, then the Nebula Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address.
🗑	Click the remove icon to delete the proxy ARP IP address.
MAC address Setting	Have the interface use either the factory-assigned default MAC address, or a manually specified MAC address.
DHCP client mode	Choices are **Auto**, **Unicast** and **Broadcast**.
DHCP option 60	DHCP Option 60 is used by the Security Firewall for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Nebula Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Enter a string using up to 63 of these characters [a–z A–Z 0–9 !\"#$%&\'()*+,-./ :;<=>?@\[\\\]^_`{}] to identify this Nebula Device to the DHCP server. For example, Zyxel-TW.
IGMP proxy	Select this to allow the Nebula Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable IGMP Downstream on the interface which connects to the multicast hosts.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

8.3.2.2 LAN Interface Configuration

Click the **Add** button or click the **Edit** button in the **LAN interface** section to open the **Site-wide** > **Configure** > **Firewall** > **Interface** > **LAN interface configuration** screen.

Figure 165 Site-wide > Configure > Firewall > Interface > LAN interface configuration



LAN interface configuation

Enabled

Interface properties

Interface name: VLAN1

Port group: LAN Group 1

VLAN ID: (1 - 4094)

IP address assignment

IP address:

Subnet mask:

DHCP setting

DHCP: None

MTU: 1500 (Bytes)

DHCP extended options

First WINS server:

Second WINS server:

The following table describes the labels in this screen.

Table 108 Site-wide > Configure > Firewall > Interface > LAN interface configuration

LABEL	DESCRIPTION
Enable	Select this to enable the LAN interface.
Interface properties	
Interface name	Specify a name for the LAN interface.
Port group	Select the name of the port group to which you want the interface (network) to belong.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.)
IP address assignment	
IP address	Enter the IP address for this interface. Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.

Table 108 Site-wide > Configure > Firewall > Interface > LAN interface configuration (continued)

LABEL	DESCRIPTION
DHCP setting	Select what type of DHCP service the Nebula Device provides to the network. Choices are: **None** – the Nebula Device does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** – the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network. **DHCP Server** – the Nebula Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Nebula Device is the DHCP server for the network.
These fields appear if the Nebula Device is a DHCP Relay.	
DHCP server 1	Enter the IP address of a DHCP server for the network.
DHCP server 2	This field is optional. Enter the IP address of another DHCP server for the network.
These fields appear if the Nebula Device is a DHCP Server.	
IP pool start address	Enter the IP address from which the Nebula Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the **Static DHCP Table**. If this field is blank, the Pool Size must also be blank. In this case, the Nebula Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server, Second DNS Server, Third DNS Server	Specify the IP addresses of up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** – enter a static IP address. **From ISP** – select the DNS server that another interface received from its DHCP server. **This Gateway** – the DHCP clients use the IP address of this interface and the Nebula Device works as a DNS relay.
Lease Time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** – select this if IP addresses never expire. **days, hours, and minutes (Optional)** – select this to enter how long IP addresses are valid.
Static DHCP table	Configure a list of static IP addresses the Nebula Device assigns to computers connected to the interface. Otherwise, the Nebula Device assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size.
IP address	Enter the IP address to assign to a device with this entry's MAC address. Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%– characters, and it can be up to 60 characters long.
🗑	Select an entry in this table and click this to delete it. This will also remove the client information on the **Site-wide** > **Clients** > **Client list** screen.
Add New	Click this to create an entry in the Static DHCP table. This will also add the client reserve IP policy on the **Site-wide** > **Clients** > **Client list**.

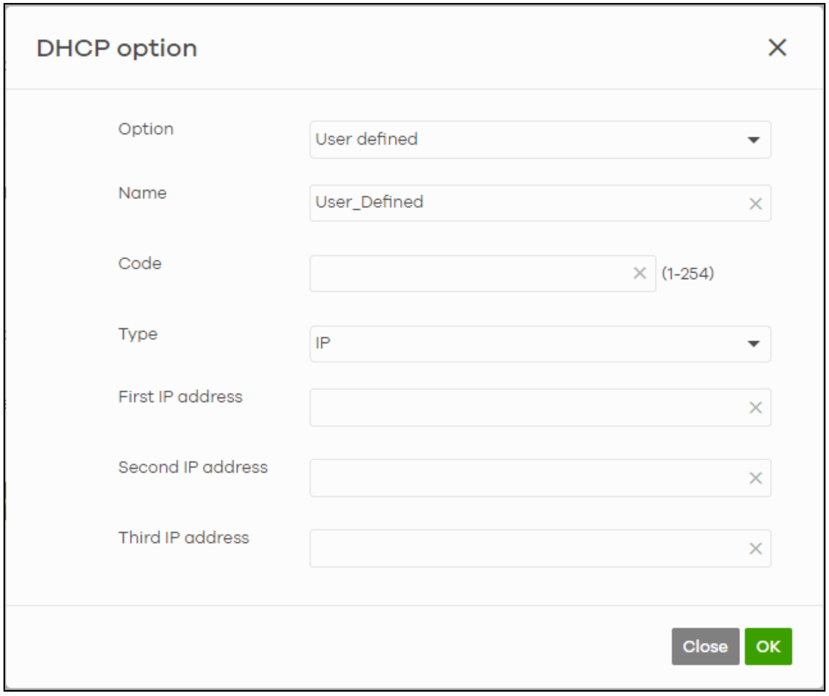
Table 108 Site-wide > Configure > Firewall > Interface > LAN interface configuration (continued)

LABEL	DESCRIPTION
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Nebula Device divides it into smaller fragments. Allowed values are 576 – 1500. Usually, this value is 1500.
ADVANCED OPTIONS	
DHCP extended options	This table is available if you select **ADVANCED OPTIONS**. Configure this table if you want to send more information to DHCP clients through DHCP packets. Click **Add new** to create an entry in this table. See Section 7.3.2.3 on page 189 for detailed information.
First WINS server Second WINS server	Enter the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
PXE server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system through a PXE-capable Network Interface Card (NIC). PXE is available for computers on internal interfaces to allow them to boot up using boot software on a PXE server. The Nebula Device acts as an intermediary between the PXE server and the computers that need boot software. The PXE server must have a public IPv4 address. You must enable DHCP server on the Nebula Device so that it can receive information from the PXE server.
PXE Boot loader file	A boot loader is a computer program that loads the operating system for the computer. Enter the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is entered, then the client computers cannot boot.
Default gateway	If you set this interface to DHCP server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway.
IGMP proxy	Select this to allow the Nebula Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable IGMP Downstream on the interface which connects to the multicast hosts.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

8.3.2.3 DHCP Option

Click the **Add new** button in the **DHCP extended options** section to open the **Site-wide** > **Configure** > **Firewall** > **Interface** > **LAN interface configuration: DHCP option** screen.

Figure 166 Site-wide > Configure > Firewall > Interface: LAN interface configuration: DHCP option



DHCP option

Option: User defined

Name: User_Defined

Code: (1-254)

Type: IP

First IP address

Second IP address

Third IP address

The following table describes the labels in this screen.

Table 109 Site-wide > Configure > Firewall > Interface: LAN interface configuration: DHCP option

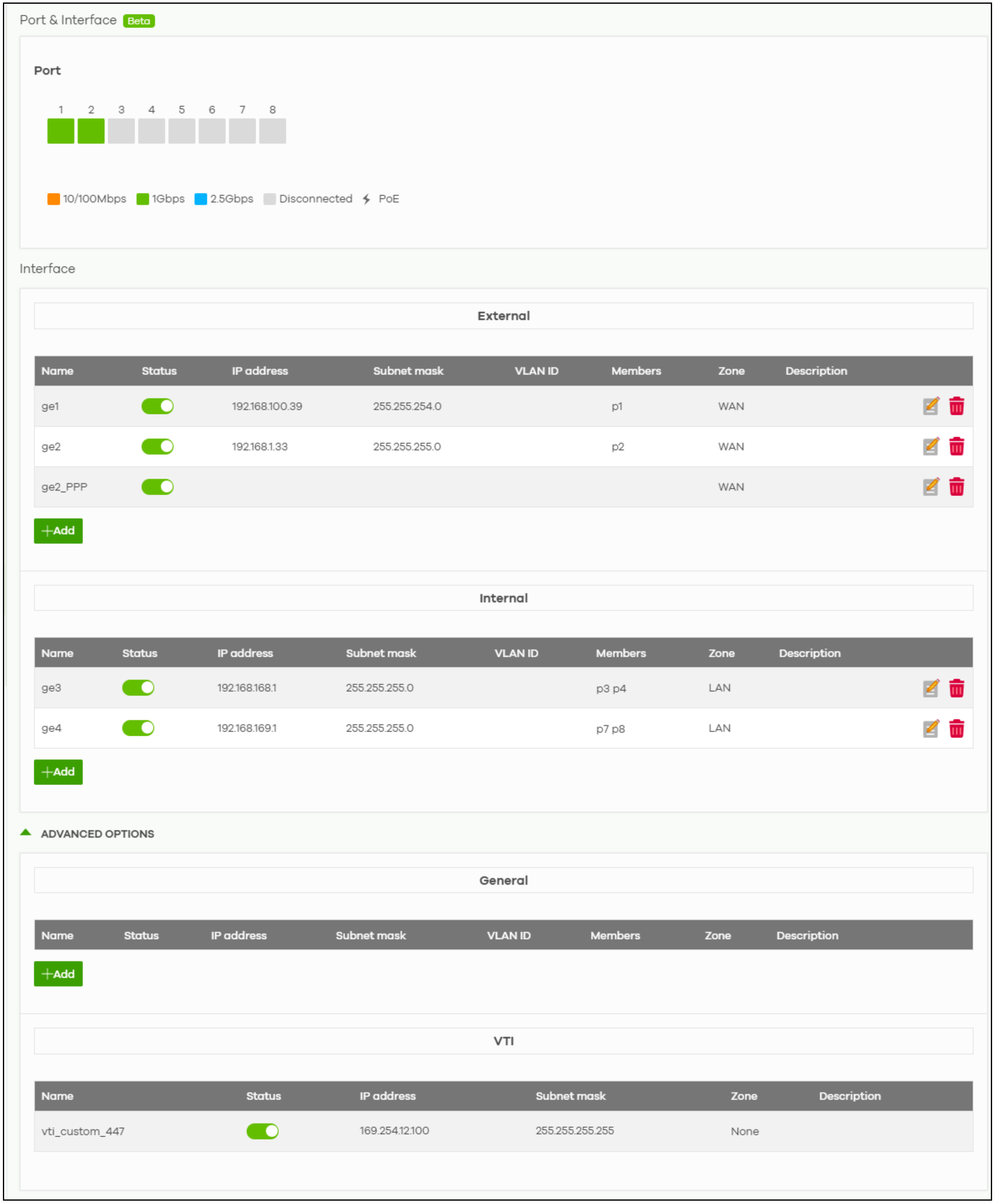
LABEL	DESCRIPTION
Option	Select which DHCP option that you want to add in the DHCP packets sent through the interface.
Name	This field displays the name of the selected DHCP option. If you selected **User defined** in the **Option** field, enter a descriptive name to identify the DHCP option.
Code	This field displays the code number of the selected DHCP option. If you selected **User defined** in the **Option** field, enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. If you selected **User defined** in the **Option** field, select an appropriate type for the value that you will enter in the next field. Misconfiguration could result in interface lockout.
Value	Enter the value for the selected DHCP option. For example, if you selected **TFTP Server Name (66)** and the type is **TEXT**, enter the DNS domain name of a TFTP server here. This field is mandatory.
First/Second/Third IP address	If you selected **User defined** / **Time/NTP/SIP/TFTP server** / **CAPWAP AC** in the **Option** field, enter up to three IP addresses.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

8.3.3 Port and Interface

Use this screen to configure port groups and network interfaces on the Nebula Device. An interface consists of a port group, a VLAN ID, and an IP address, plus other configuration settings. To access this screen, click **Firewall** > **Configure** > **Port and Interface**.

Note: The **Port and Interface** feature is for Security Firewall USG FLEX H Series only.

Figure 167 Site-wide > Configure > Firewall > Port and Interface



Port & Interface Beta

Port

1	2	3	4	5	6	7	8
🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜

🟧 10/100Mbps 🟩 1Gbps 🟦 2.5Gbps ⬜ Disconnected ⚡ PoE

Interface

External

Name	Status	IP address	Subnet mask	VLAN ID	Members	Zone	Description	
ge1	●	192.168.100.39	255.255.254.0		p1	WAN		✎ 🗑
ge2	●	192.168.1.33	255.255.255.0		p2	WAN		✎ 🗑
ge2_PPP	●					WAN		✎ 🗑

+Add

Internal

Name	Status	IP address	Subnet mask	VLAN ID	Members	Zone	Description	
ge3	●	192.168.168.1	255.255.255.0		p3 p4	LAN		✎ 🗑
ge4	●	192.168.169.1	255.255.255.0		p7 p8	LAN		✎ 🗑

+Add

▲ ADVANCED OPTIONS

General

Name	Status	IP address	Subnet mask	VLAN ID	Members	Zone	Description

+Add

VTI

Name	Status	IP address	Subnet mask	Zone	Description
vti_custom_447	●	169.254.12.100	255.255.255.255	None	

The following table describes the labels in this screen.

Table 110 Site-wide > Configure > Firewall > Port and Interface

LABEL	DESCRIPTION
Port	Move the pointer over a port to view the Nebula Device's port details, such as **Name**, **Status** and **Speed**. If the port is supplying power to a node using Power over Ethernet (PoE), you can click **Power reset** to perform a power cycle on the port. This action temporarily disables PoE and then re-enables it, in order to reboot connected PoE devices.
Interface External	
Name	This field displays the name of the interface.
Status	Click the switch to the right to enable this interface.
IP address	This field displays the IP address for this interface. If this field is empty, the interface does not have an IP address yet or is configured as 'Unassigned'.
Subnet mask	This field displays the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	This field displays the VLAN ID which is a 12-bit number that uniquely identifies each VLAN.
Members	This field displays the port(s) the interface is using.
Zone	This field displays the zone to which this interface belongs. An interface can only be in one zone.
Description	This field displays the description of the interface.
✎	Select an entry and click Edit to open a screen where you can modify the entry's settings.
🗑	To remove a virtual interface, select it and click Remove. The Nebula Device confirms you want to remove it before doing so. Note: You can remove an interface that belongs to one **Zone** only. For example, interface ge4 only belongs to the LAN **Zone**. After selecting this interface and clicking the Remove icon, the interface ge4 will be removed from the interface table. After clicking **OK**, the LAN **Zone** will also remove the interface ge4. To avoid losing connection between the Nebula Device and NCC, there must be at least one External interface. NCC will not allow you to remove the last External interface.
Add	Click this to add a new entry.
Internal	
Name	This field displays the name of the interface.
Status	Click the switch to the right to enable this interface.
IP address	This field displays the IP address for this interface. If this field is empty, the interface does not have an IP address yet or is configured as 'Unassigned'.
Subnet mask	This field displays the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	This field displays the VLAN ID which is a 12-bit number that uniquely identifies each VLAN.
Members	This field displays the port(s) the interface is using.
Zone	This field displays the zone to which this interface belongs. An interface can only be in one zone.
Description	This field displays the description of the interface.
✎	Select an entry and click Edit to open a screen where you can modify the entry's settings.
🗑	To remove a virtual interface, select it and click Remove. The Nebula Device confirms you want to remove it before doing so.
Add	Click this to add a new entry.

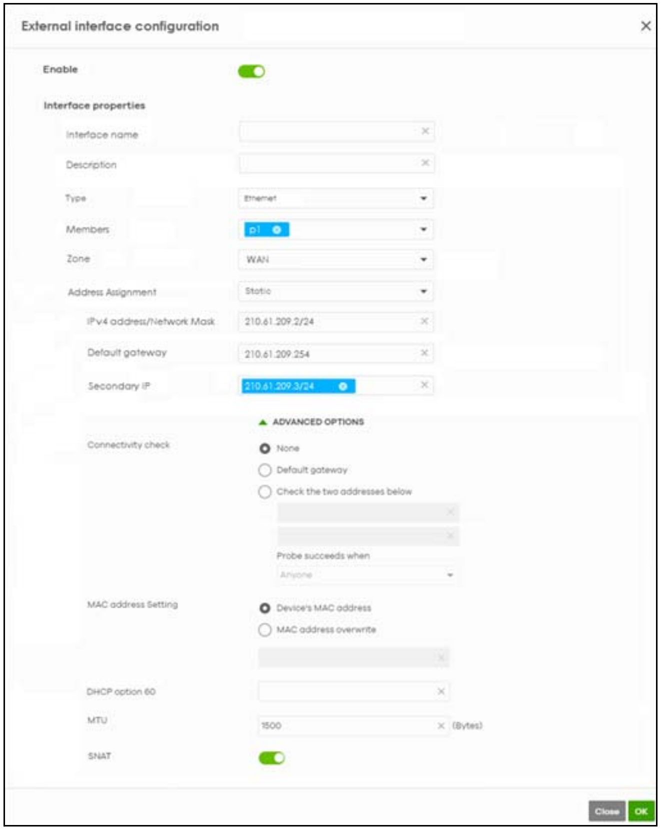
Table 110 Site-wide > Configure > Firewall > Port and Interface (continued)

LABEL	DESCRIPTION
ADVANCED OPTIONS	Click this to display a greater or lesser number of configuration fields.
General	
Name	This field displays the name of the interface.
Status	Click the switch to the right to enable this interface.
IP address	This field displays the IP address for this interface. If this field is empty, the interface does not have an IP address yet or is configured as 'Unassigned'.
Subnet mask	This field displays the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	This field displays the VLAN ID which is a 12-bit number that uniquely identifies each VLAN.
Members	This field displays the port(s) the interface is using.
Zone	This field displays the zone to which this interface belongs. An interface can only be in one zone.
Description	This field displays the description of the interface.
✎	Select an entry and click Edit to open a screen where you can modify the entry's settings.
🗑	To remove a virtual interface, select it and click Remove. The Nebula Device confirms you want to remove it before doing so.
Add	Click this to add a new entry.
VTI	
Name	This field displays the name of the interface.
Status	Click the switch to the right to enable this interface.
IP address	This field displays the IP address for this interface. If this field is empty, the interface does not have an IP address yet or is configured as 'Unassigned'.
Subnet mask	This field displays the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Zone	This field displays the zone to which this interface belongs. An interface can only be in one zone.
Description	This field displays the description of the interface.

8.3.3.1 External Interface Configuration

Click the **Add** button or click the **Edit** button in the **External Interface** section to open the **Site-wide** > **Configure** > **Firewall** > **Port and Interface** > **External interface configuration** screen.

Figure 168 Site-wide > Configure > Firewall > Port and Interface > External interface configuration



External interface configuration

Enable: on

Interface properties

Interface name:

Description:

Type: Ethernet

Members: p1

Zone: WAN

Address Assignment: Static

IPv4 address/Network Mask: 210.61.209.2/24

Default gateway: 210.61.209.254

Secondary IP: 210.61.209.3/24

ADVANCED OPTIONS

Connectivity check: ● None ○ Default gateway ○ Check the two addresses below

Probe succeeds when: Anyone

MAC address Setting: ● Device's MAC address ○ MAC address overwrite

DHCP option 60:

MTU: 1500 (Bytes)

SNAT: on

The following table describes the labels in this screen.

Table 111 Site-wide > Configure > Firewall > Port and Interface > External interface configuration

LABEL	DESCRIPTION
Enable	Click this switch to the right to enable the interface.
Interface properties	
Interface name	Enter a name for the interface. You may use 2 to 30 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a descriptive name for the interface.
Type	Select the type of interface to create. **DHCP**: The interface will automatically get an IP address and other network settings from a DHCP server. **Static**: You must manually configure an IP address and other network settings for the interface. **PPPoE**: The interface will authenticate with an Internet Service Provider, and then automatically get an IP address from the ISP's DHCP server. You can use this type of interface to connect to a DSL modem. **PPPoE with static IP**: Assign a static IP address to the WAN interface and your WAN interface is getting an Internet connection from a PPPoE server.
Members	Select the name of the port group to which you want the interface (network) to belong.
Zone	Select the zone to which this interface belongs. An interface can only be in one zone.

Table 111 Site-wide > Configure > Firewall > Port and Interface > External interface configuration

LABEL	DESCRIPTION
IP address assignment	These fields are displayed if you select **Static**.
IPv4 address/Network Mask	Enter the static IP address of this interface and the subnet mask for this interface's IP address. Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
Default gateway	Enter the IP address of the Nebula Device through which this interface sends traffic.
Secondary IP	Enter another IP address of the Nebula Device through which this interface sends traffic. This field is optional.
These fields are displayed if you selected **PPPoE** or **PPPoE with static IP**.	
Authentication Type	Select an authentication protocol for outgoing connection requests. Options are: • **Chap/PAP** – The Nebula Device accepts either CHAP or PAP when requested by the remote node. • **Chap** – The Nebula Device accepts CHAP only. • **PAP** – The Nebula Device accepts PAP only. • **MSCHAP** – The Nebula Device accepts MSCHAP only. • **MSCHAP-V2** – The Nebula Device accepts MSCHAP-V2 only.
Username	Enter the user name provided by your ISP. You can use 2 up to 64 alphanumeric characters and the underscore. '0-9a-zA-Z~`@#$%^&*()_+-={}[] | :";'<>,.?/' are allowed.
Password	Enter the password provided by your ISP. You can use 1 up to 63 alphanumeric characters and the underscore. 0-9a-zA-Z~`@#$%^&*()_+-={}[] | \:';'<>,./ are allowed. '?' is not allowed.
Retype password	Enter the password again to confirm it.
Service name	Enter the service name from your service provider. PPPoE uses a service name to identify and reach the PPPoE server. You can use up to 30 single-byte characters, including 0-9a-zA-Z._-
Compression	Select On to turn on stac compression. Select Off to turn off stac compression. Stac compression is data compression technique capable of compressing data by a factor of about four.
User Idle Timeout	Enter the idle timeout in seconds that elapses before the router automatically disconnects from the PPPoE server.
WAN IP	Enter the IP address of the WAN interface through which this connection will send traffic.
Gateway IP	Enter the IP address of the router through which this WAN connection will send traffic.
IP address	Enter the IP address for this interface.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers on the network.
ADVANCED OPTIONS	
Connectivity check	The interface can periodically check whether it can connect to its default gateway (**Default gateway**), or to two user-specified servers (**Check the two addresses below**). If the check fails, the interface's status changes to **Down**. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Nebula Device stops routing to the gateway.

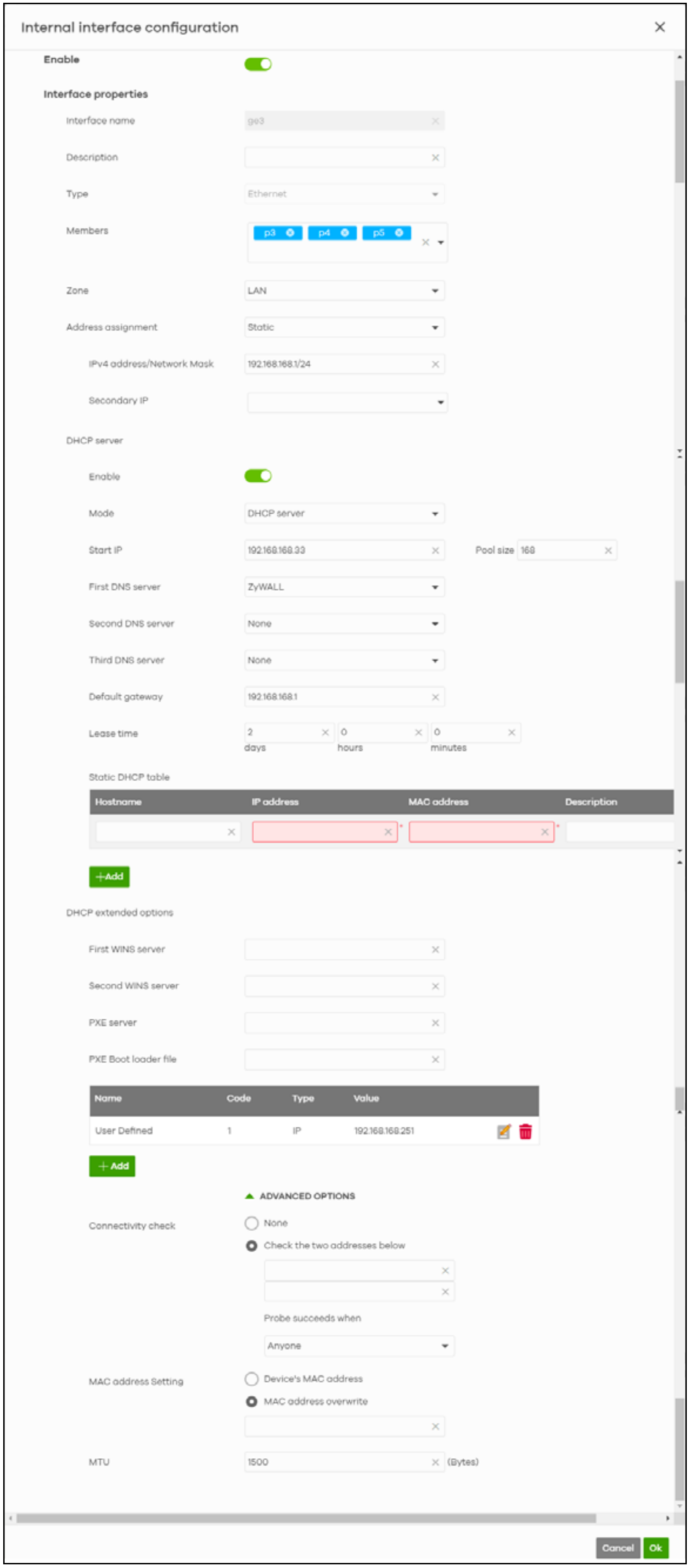
Table 111 Site-wide > Configure > Firewall > Port and Interface > External interface configuration

LABEL	DESCRIPTION
Probe succeeds when	This field applies when you select **Check the two addresses** and specify two domain names or IP addresses for the connectivity check. Select **any one** if you want the check to pass if at least one of the domain names or IP addresses responds. Select **all** if you want the check to pass only if both domain names or IP addresses respond.
MAC address Setting	Have the interface use either the factory-assigned default MAC address, or a manually specified MAC address.
DHCP option 60	DHCP Option 60 is used by the Security Firewall for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Nebula Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Enter a string using up to 63 of these characters [a–z A–Z 0–9 !\"#$%&\'()*+,-./ :;<=>?@\[\\\]^_`{}] to identify this Nebula Device to the DHCP server. For example, Zyxel-TW.
MTU	Enter the number (Bytes) to allow the Nebula Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
SNAT	Click this switch to the right to enable SNAT. When enabled, the Nebula Device rewrites the source address of packets being sent from this interface to the interface's IP address.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

8.3.3.2 Internal Interface Configuration

Click the **Add** button or click the **Edit** button in the **Internal interface** section to open the **Site-wide** > **Configure** > **Firewall** > **Port and Interface** > **Internal interface configuration** screen.

Figure 169 Site-wide > Configure > Firewall > Port and Interface > Internal interface configuration



Internal interface configuration

Enable	● On
Interface properties	
Interface name	ge3
Description	
Type	Ethernet
Members	p3, p4, p5
Zone	LAN
Address assignment	Static
IPv4 address/Network Mask	192.168.168.1/24
Secondary IP	
DHCP server	
Enable	● On
Mode	DHCP server
Start IP	192.168.168.33
Pool size	168
First DNS server	ZyWALL
Second DNS server	None
Third DNS server	None
Default gateway	192.168.168.1
Lease time	2 days 0 hours 0 minutes

Static DHCP table

Hostname	IP address	MAC address	Description

DHCP extended options

First WINS server	
Second WINS server	
PXE server	
PXE Boot loader file	

Name	Code	Type	Value
User Defined	1	IP	192.168.168.251

▲ ADVANCED OPTIONS

Connectivity check
○ None
● Check the two addresses below
Probe succeeds when: Anyone

MAC address Setting
○ Device's MAC address
● MAC address overwrite

MTU: 1500 (Bytes)

The following table describes the labels in this screen.

Table 112 Site-wide > Configure > Firewall > Port and Interface > Internal interface configuration

LABEL	DESCRIPTION
Enable	Select this to enable the interface.
Interface properties	
Interface name	Specify a name for the interface. You may use 2 to 30 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a descriptive name for the interface.
Type	Select the type of interface to create. **DHCP**: The interface will automatically get an IP address and other network settings from a DHCP server. **Static**: You must manually configure an IP address and other network settings for the interface. **PPPoE**: The interface will authenticate with an Internet Service Provider, and then automatically get an IP address from the ISP's DHCP server. You can use this type of interface to connect to a DSL modem. **PPPoE with static IP**: Assign a static IP address to the WAN interface and your WAN interface is getting an Internet connection from a PPPoE server.
Members	Select the name of the port group to which you want the interface (network) to belong.
Zone	Select the zone to which this interface belongs. An interface can only be in one zone.
Address assignment	These fields are displayed if you select **Static**.
IPv4 address/Network mask	Enter the IP address and the subnet mask for this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network. Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
Secondary IP	Enter another IP address for this interface. This field is optional.
These fields appear if the Nebula Device is a DHCP Relay.	
DHCP server 1	Enter the IP address of a DHCP server for the network.
DHCP server 2	This field is optional. Enter the IP address of another DHCP server for the network.
These fields appear if the Nebula Device is a DHCP Server.	
Enable	Click this switch to the right to enable the DHCP server.
Mode	Select what type of DHCP service the Nebula Device provides to the network. Choices are: **None** – the Nebula Device does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** – the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network. **DHCP Server** – the Nebula Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Nebula Device is the DHCP server for the network.

Table 112 Site-wide > Configure > Firewall > Port and Interface > Internal interface configuration

LABEL	DESCRIPTION
Start IP	Enter the IP address from which the Nebula Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the **Static DHCP Table**. If this field is blank, the Pool Size must also be blank. In this case, the Nebula Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server, Second DNS Server, Third DNS Server	Specify the IP addresses of up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** – enter a static IP address. **From ISP** – select the DNS server that another interface received from its DHCP server. **This Gateway** – the DHCP clients use the IP address of this interface and the Nebula Device works as a DNS relay.
Default gateway	If you set this interface to DHCP server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway.
Lease Time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. **days, hours,** and **minutes** – enter how long IP addresses are valid.
Static DHCP table	Configure a list of static IP addresses the Nebula Device assigns to computers connected to the interface. Otherwise, the Nebula Device assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size.
Hostname	By default, the Nebula Device's hostname is the MAC address. Enter a name to identify the Nebula Device. You can use up to 64 alphanumeric characters including period (.) and hyphen (-). Spaces are not allowed. Note: The period (.) and hyphen (-) cannot be the first character, last character, or appear consecutively on the Name. For example, -wax650, wax650-, wax650..wax650, wax650.-wax650.
IP address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address. Note: No IP address is required for an internal interface.
MAC address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry.
🗑	Select an entry in this table and click this to delete it. This will also remove the client information on the **Site-wide** > **Clients** > **Client list** screen.
Add	Click this to create an entry in the Static DHCP table. This will also add the client reserve IP policy on the **Site-wide** > **Clients** > **Client list**.
DHCP extended options	Configure this if you want to send more information to DHCP clients through DHCP packets.
First WINS server Second WINS server	Enter the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.

Table 112 Site-wide > Configure > Firewall > Port and Interface > Internal interface configuration

LABEL	DESCRIPTION
PXE server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system through a PXE-capable Network Interface Card (NIC). PXE is available for computers on internal interfaces to allow them to boot up using boot software on a PXE server. The Nebula Device acts as an intermediary between the PXE server and the computers that need boot software. The PXE server must have a public IPv4 address. You must enable DHCP server on the Nebula Device so that it can receive information from the PXE server.
PXE Boot loader file	A boot loader is a computer program that loads the operating system for the computer. Enter the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is entered, then the client computers cannot boot.
Name	This field displays the name of the selected DHCP option. Enter a descriptive name to identify the DHCP option. You may use 2 to 30 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Code	This field displays the code number of the selected DHCP option. Enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. Select an appropriate type for the value that you will enter in the next field. Misconfiguration could result in interface lockout.
Value	Enter the value for the selected DHCP option. For example, if you selected TFTP Server Name (66) and the type is TEXT, enter the DNS domain name of a TFTP server here. This field is mandatory.
✎	Select an entry and click Edit to open a screen where you can modify the entry's settings.
🗑	Select an entry in this table and click this to delete it.
Add	Click this to create an entry in this table.
ADVANCED OPTIONS	
Connectivity check	Select **Check the two addresses below** to specify one or two domain names or IP addresses for the connectivity check. You can type an IPv4 address in one field and a domain name in the other. For example, type "192.168.1.2" in the top field and "www.zyxel.com" in the bottom field. Select **Probe succeeds when** to specify two domain names or IP addresses for the connectivity check. Select **Anyone** if you want the check to pass if at least one of the domain names or IP addresses responds. Select **All** if you want the check to pass only if both domain names or IP addresses respond. Otherwise, select **None**.
MAC address setting	Select **Device's MAC address** to have the interface use the factory-assigned default MAC address. By default, the Nebula Device uses the factory-assigned MAC address to identify itself. Select **MAC address overwrite** to have the interface use a different MAC address. Enter a MAC address in the format 'xx:xx:xx:xx:xx:xx' or 'xx-xx-xx-xx-xx-xx'. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Nebula Device divides it into smaller fragments. Allowed values are 576 – 1500. Usually, this value is 1500.

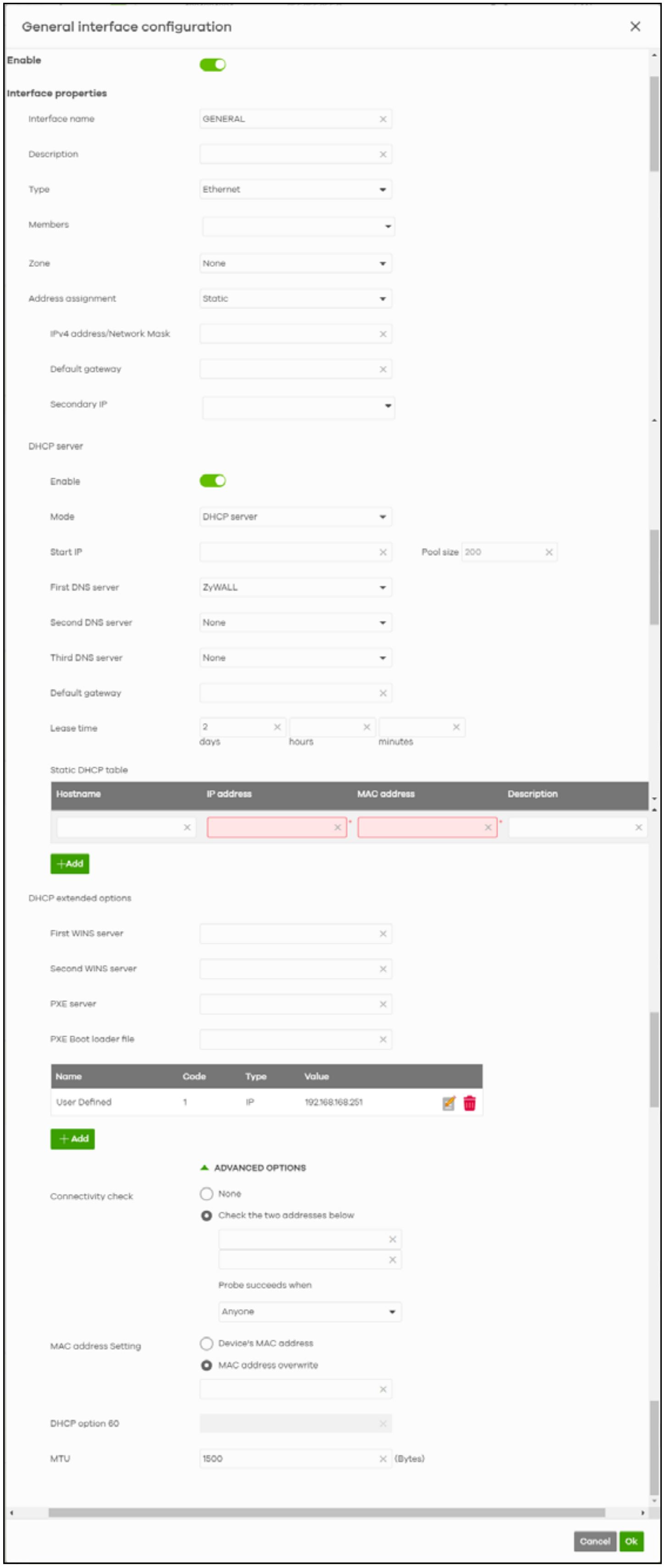
Table 112   Site-wide > Configure > Firewall > Port and Interface > Internal interface configuration

LABEL	DESCRIPTION
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

8.3.3.3 General Interface Configuration

Click the **Add** button or click the **Edit** button in the **General interface** section to open the **Site-wide** > **Configure** > **Firewall** > **Port and Interface** > **General interface configuration** screen.

Figure 170 Site-wide > Configure > Firewall > Port and Interface > General interface configuration



General interface configuration

Enable: On

Interface properties

Interface name	GENERAL
Description	
Type	Ethernet
Members	
Zone	None
Address assignment	Static
IPv4 address/Network Mask	
Default gateway	
Secondary IP	

DHCP server

Enable	On
Mode	DHCP server
Start IP	Pool size 200
First DNS server	ZyWALL
Second DNS server	None
Third DNS server	None
Default gateway	
Lease time	2 days, hours, minutes

Static DHCP table

Hostname	IP address	MAC address	Description

DHCP extended options

First WINS server	
Second WINS server	
PXE server	
PXE Boot loader file	

Name	Code	Type	Value
User Defined	1	IP	192.168.168.251

ADVANCED OPTIONS

Connectivity check: ○ None ● Check the two addresses below

Probe succeeds when: Anyone

MAC address Setting: ○ Device's MAC address ● MAC address overwrite

DHCP option 60:

MTU: 1500 (Bytes)

The following table describes the labels in this screen.

Table 113 Site-wide > Configure > Firewall > Port and Interface > General interface configuration

LABEL	DESCRIPTION
Enable	Select this to enable the interface.
Interface properties	
Interface name	Specify a name for the interface. You may use 2 to 30 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a descriptive name for the interface.
Type	Select the type of interface to create. **DHCP**: The interface will automatically get an IP address and other network settings from a DHCP server. **Static**: You must manually configure an IP address and other network settings for the interface. **PPPoE**: The interface will authenticate with an Internet Service Provider, and then automatically get an IP address from the ISP's DHCP server. You can use this type of interface to connect to a DSL modem. **PPPoE with static IP**: Assign a static IP address to the WAN interface and your WAN interface is getting an Internet connection from a PPPoE server.
Members	Select the name of the port group to which you want the interface (network) to belong.
Zone	Select the zone to which this interface belongs. An interface can only be in one zone.
Address assignment	These fields are displayed if you select **Static**.
IPv4 address/Network mask	Enter the IP address and the subnet mask for this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network. Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
Default gateway	If you set this interface to DHCP server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway.
Secondary IP	Enter another IP address for this interface. This field is optional.
These fields appear if the Nebula Device is a DHCP Relay.	
DHCP server 1	Enter the IP address of a DHCP server for the network.
DHCP server 2	This field is optional. Enter the IP address of another DHCP server for the network.
These fields appear if the Nebula Device is a DHCP Server.	
Enable	Click this switch to the right to enable the DHCP server.
Mode	Select what type of DHCP service the Nebula Device provides to the network. Choices are: **None** – the Nebula Device does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** – the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network. **DHCP Server** – the Nebula Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Nebula Device is the DHCP server for the network.

Table 113   Site-wide > Configure > Firewall > Port and Interface > General interface configuration

LABEL	DESCRIPTION
Start IP	Enter the IP address from which the Nebula Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the **Static DHCP Table**. If this field is blank, the **Pool Size** must also be blank. In this case, the Nebula Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server, Second DNS Server, Third DNS Server	Specify the IP addresses of up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** – enter a static IP address. **From ISP** – select the DNS server that another interface received from its DHCP server. **This Gateway** – the DHCP clients use the IP address of this interface and the Nebula Device works as a DNS relay.
Default gateway	If you set this interface to DHCP server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway.
Lease Time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. **days, hours,** and **minutes** – enter how long IP addresses are valid.
Static DHCP table	Configure a list of static IP addresses the Nebula Device assigns to computers connected to the interface. Otherwise, the Nebula Device assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size.
Hostname	By default, the Nebula Device's hostname is the MAC address. Enter a name to identify the Nebula Device. You can use up to 64 alphanumeric characters including period (.) and hyphen (-). Spaces are not allowed. Note: The period (.) and hyphen (-) cannot be the first character, last character, or appear consecutively on the Name. For example, -wax650, wax650-, wax650..wax650, wax650.-wax650.
IP address	Enter the IP address to assign to a device with this entry's MAC address. Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
MAC address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry.
🗑	Select an entry in this table and click this to delete it. This will also remove the client information on the **Site-wide** > **Clients** > **Client list** screen.
Add	Click this to create an entry in the Static DHCP table. This will also add the client reserve IP policy on the **Site-wide** > **Clients** > **Client list**.
DHCP extended options	Configure this if you want to send more information to DHCP clients through DHCP packets.
First WINS server Second WINS server	Enter the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.

Table 113 Site-wide > Configure > Firewall > Port and Interface > General interface configuration

LABEL	DESCRIPTION
PXE server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system through a PXE-capable Network Interface Card (NIC). PXE is available for computers on internal interfaces to allow them to boot up using boot software on a PXE server. The Nebula Device acts as an intermediary between the PXE server and the computers that need boot software. The PXE server must have a public IPv4 address. You must enable DHCP server on the Nebula Device so that it can receive information from the PXE server.
PXE Boot loader file	A boot loader is a computer program that loads the operating system for the computer. Enter the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is entered, then the client computers cannot boot.
Name	This field displays the name of the selected DHCP option. Enter a descriptive name to identify the DHCP option. You may use 2 to 30 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Code	This field displays the code number of the selected DHCP option. Enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. Select an appropriate type for the value that you will enter in the next field. Misconfiguration could result in interface lockout.
Value	Enter the value for the selected DHCP option. For example, if you selected TFTP Server Name (66) and the type is TEXT, enter the DNS domain name of a TFTP server here. This field is mandatory.
✎	Select an entry and click Edit to open a screen where you can modify the entry's settings.
🗑	Select an entry in this table and click this to delete it.
Add	Click this to create an entry in this table.
ADVANCED OPTIONS	
Connectivity check	Select **Check the two addresses below** to specify one or two domain names or IP addresses for the connectivity check. You can type an IPv4 address in one field and a domain name in the other. For example, type "192.168.1.2" in the top field and "www.zyxel.com" in the bottom field. Select **Probe succeeds when** to specify two domain names or IP addresses for the connectivity check. Select **Anyone** if you want the check to pass if at least one of the domain names or IP addresses responds. Select **All** if you want the check to pass only if both domain names or IP addresses respond. Otherwise, select **None**.
MAC address setting	Select **Device's MAC address** to have the interface use the factory-assigned default MAC address. By default, the Nebula Device uses the factory-assigned MAC address to identify itself. Select **MAC address overwrite** to have the interface use a different MAC address. Enter a MAC address in the format 'xx:xx:xx:xx:xx:xx' or 'xx-xx-xx-xx-xx-xx'. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.

Table 113 Site-wide > Configure > Firewall > Port and Interface > General interface configuration

LABEL	DESCRIPTION
DHCP option 60	DHCP Option 60 is used by the Nebula Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Nebula Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Type a string using up to 63 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./ :;<=>?@\[\\\]^_`{}] to identify this Nebula Device to the DHCP server. For example, Zyxel-TW.
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Nebula Device divides it into smaller fragments. Allowed values are 576 – 1500. Usually, this value is 1500.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

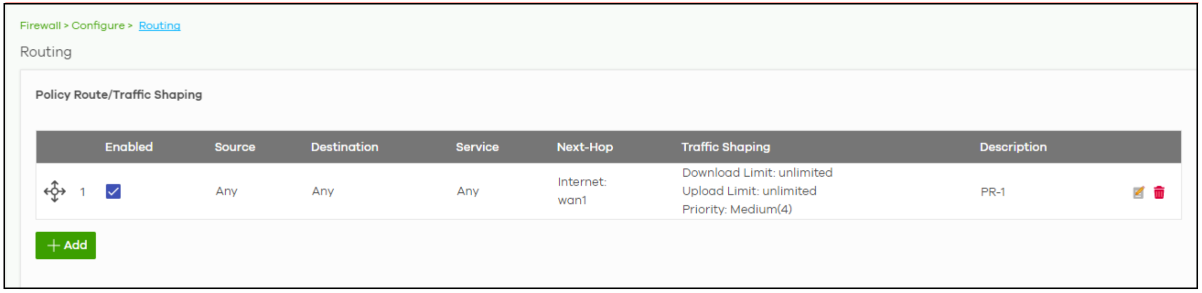
8.3.4 Routing

Use policy routes and static routes to override the Nebula Device's default routing behavior in order to send packets through the appropriate next-hop gateway, interface or VPN tunnel.

A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. Use this screen to configure policy routes.

Click **Site-wide** > **Configure** > **Firewall** > **Routing: Policy Route/Traffic Shaping** to access this screen.

Figure 171 Site-wide > Configure > Firewall > Routing: Policy Route/Traffic Shaping



Firewall > Configure > Routing

Routing

Policy Route/Traffic Shaping

	Enabled	Source	Destination	Service	Next-Hop	Traffic Shaping	Description
✥ 1	☑	Any	Any	Any	Internet: wan1	Download Limit: unlimited Upload Limit: unlimited Priority: Medium(4)	PR-1

The following table describes the labels in this screen.

Table 114 Site-wide > Configure > Firewall > Routing: Policy Route/Traffic Shaping

LABEL	DESCRIPTION
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Source	This shows the source IP addresses to which this rule applies. This could be an IP, CIDR, FQDN, or GEO IP (country) object.
Destination	This shows the destination IP addresses to which this rule applies. This could be an IP, CIDR, FQDN, or GEO IP (country) object.
Service	This is the name of the service object (port) or application. **Any** means all services. Select **Protocol** to specify a protocol by protocol ID number, as defined in the IPv4 header. For example, 1 = ICMP, 2 = IGMP.

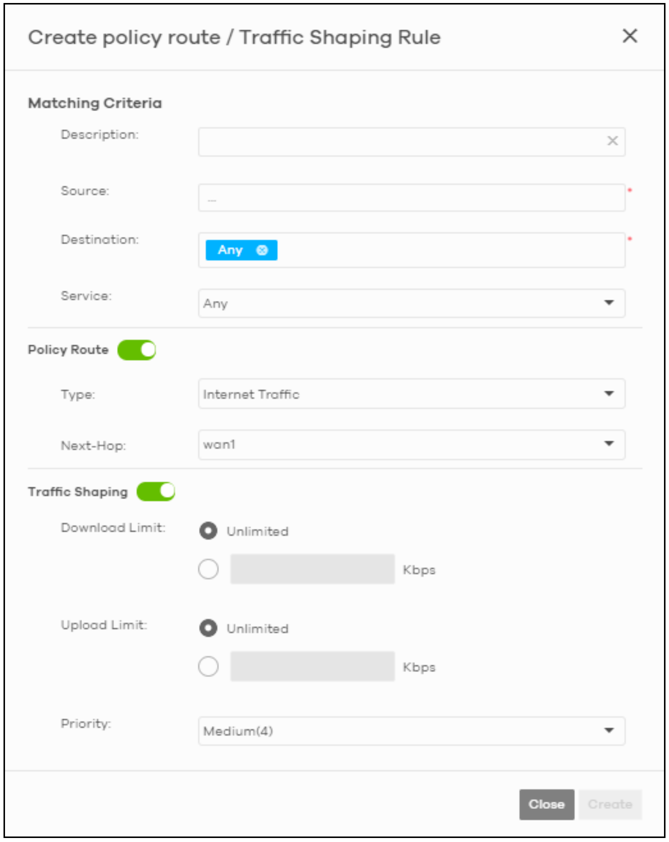
Table 114 Site-wide > Configure > Firewall > Routing: Policy Route/Traffic Shaping (continued)

LABEL	DESCRIPTION
Next Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, or outgoing interface.
Traffic Shaping	This displays the maximum downstream and upstream bandwidth for traffic from an individual source IP address and the priority level.
Description	This is the descriptive name of the policy.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this button to create a new policy route. See Section 8.3.8.1 on page 520 for more information.

8.3.4.1 Add/Edit Policy Route / Traffic Shaping Rule

Click the **Add** button or an edit icon in the **Site-wide** > **Configure** > **Firewall** > **Routing: Policy Route**/**Traffic Shaping: Add**/**Edit** screen to access this screen.

Figure 172 Site-wide > Configure > Firewall > Routing: Policy Route/Traffic Shaping: Add/Edit



Create policy route / Traffic Shaping Rule

Matching Criteria

Description:

Source:

Destination: Any

Service: Any

Policy Route

Type: Internet Traffic

Next-Hop: wan1

Traffic Shaping

Download Limit: ● Unlimited ○ Kbps

Upload Limit: ● Unlimited ○ Kbps

Priority: Medium(4)

The following table describes the labels in this screen.

Table 115 Site-wide > Configure > Firewall > Routing: Policy Route/Traffic Shaping: Add/Edit

LABEL	DESCRIPTION
Matching Criteria	
Description	Enter a descriptive name for the rule.

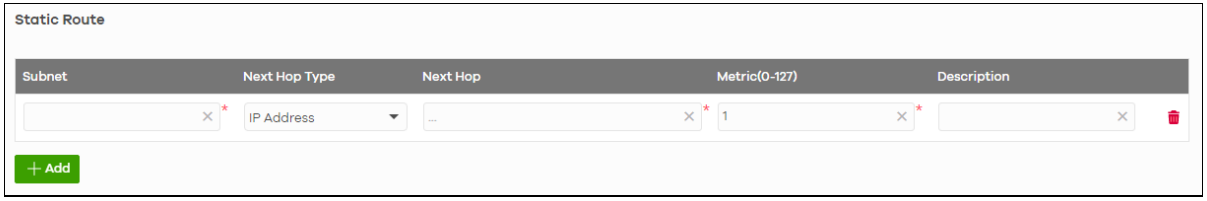
Table 115 Site-wide > Configure > Firewall > Routing: Policy Route/Traffic Shaping: Add/Edit (continued)

LABEL	DESCRIPTION
Source	Specify the source IP addresses (LAN interface / country) to which this rule applies. You can add multiple IP, CIDR, GEO IP (country) objects or a single FQDN object by pressing 'Enter', or enter a new IP address by clicking **Add**. Select **Any** to apply the rule to all IP addresses. Note: IP/CIDR, FQND, and GEO IP objects cannot be used at the same time. Multiple FQDNs are not supported. The IP FQDN does NOT support wildcards.
Destination	Specify the destination IP addresses (LAN interface / country) or subnet to which this rule applies. You can add multiple IP, CIDR, GEO IP (country) objects or a single FQDN object by pressing 'Enter', or enter a new IP address by clicking **Add**. Select **Any** to apply the rule to all IP addresses. Note: IP/CIDR, FQND, and GEO IP objects cannot be used at the same time. Multiple FQDNs are not supported.
Service	Select a protocol to apply the policy route to. **TCP**, **UDP**, **TCP & UDP**, **ICMP** – Match packets from the specified network protocol, going to the optional destination port. **Protocol** – Match packets for the specified custom protocol. Enter the **Protocol ID**, 1 – 143 (1 for **ICMP**, 6 for **TCP**, 17 for **UDP**; the **Service** will automatically select **ICMP** / **TCP** / **UDP** respectively). **Application** – Match packets from the application. Otherwise, select **Any**.
Policy Route	Select this to enable policy route.
Type	Select **Internet Traffic** to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface). Select **Intranet Traffic** to route the matched packets to the next-hop router or Switch you specified in the **Next-Hop** field. Select **VPN Traffic** to route the matched packets through the VPN tunnel you specified in the **Next-Hop** field.
Next-Hop	If you select **Internet Traffic** in the **Type** field, select the WAN interface to route the matched packets through the specified outgoing interface to a gateway connected to the interface. If you select **Intranet Traffic** in the **Type** field, enter the IP address of the next-hop router or Switch. If you select **VPN Traffic** in the **Type** field, select the remote VPN gateway's site name. • Only the VPN gateway sites belonging to the same **VPN Area** that you set in **Organization-wide** > **Organization-wide manage** > **VPN orchestrator** will be available. See Section 12.4.4.3 on page 692 for more information). • Setting a Policy Route to force traffic over a VPN tunnel between a Security Firewall and Nebula Security Gateway (NSG) is not supported. Both front/back end Nebula Devices must be the same type.
Traffic Shaping	Select this to restrict maximum downstream and upstream bandwidth for traffic in the policy route.
Download Limit	Set the maximum downstream bandwidth for traffic that matches the policy.
Upload limit	Set the maximum upstream bandwidth for traffic that matches the policy.
Priority	Enter a number between 1 and 6 to set the priority for traffic that matches this policy. The lower the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority.
Close	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

8.3.4.2 Static Route

Click the **Add** button in the **Static Route** section of the **Site-wide** > **Configure** > **Firewall** > **Routing: Static Route** screen to open the following screen.

Figure 173 Site-wide > Configure > Firewall > Routing: Static Route



The following table describes the labels in this screen.

Table 116 Site-wide > Configure > Firewall > Routing: Static Route

LABEL	DESCRIPTION
Subnet	Enter an IP subnet mask. The route applies to all IP addresses in the subnet.
Next Hop Type	Select **IP Address** or **Interface** to specify if you want to send all traffic to the gateway or interface.
Next Hop	Enter the IP address of the next-hop gateway.
Metric (0–127)	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be 0 – 127. In practice, 2 or 3 is usually a good number.
Description	This is the descriptive name of the static route.
🗑	Click this icon to remove a static route.
Add	Click this button to create a new static route.

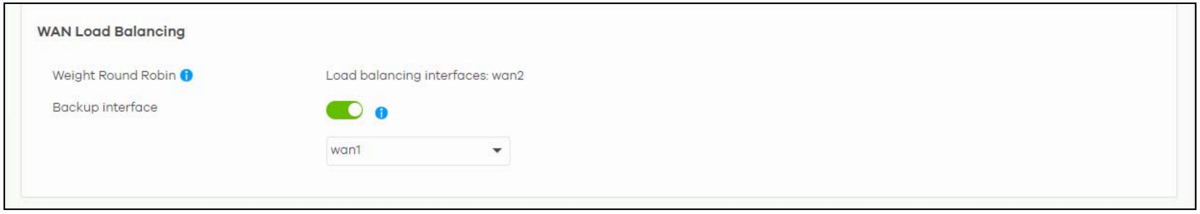
8.3.4.3 WAN Load Balancing

Go to **Site-wide** > **Configure** > **Firewall** > **Routing: WAN Load Balancing** to configure WAN load balancing.

By default, the Nebula Device adds all WAN interfaces to a load balancing group, and balances the traffic load between interfaces based on their respective weights (upload bandwidth). An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.

For example, if the weight ratio of WAN 1 and WAN 2 interfaces is 2:1, the Nebula Device chooses WAN 1 for two sessions’ traffic and WAN 2 for one session’s traffic in each round of three new sessions.

Figure 174 Site-wide > Configure > Firewall > Routing: WAN Load Balancing



The following table describes the labels in this section.

Table 117   Site-wide > Configure > Firewall > Routing: WAN Load Balancing

LABEL	DESCRIPTION
Weight Round Robin	Displays the WAN interfaces that are in the WAN load balancing group.
Backup interface	Select this to assign one WAN interface as the backup interface. The backup interface is removed from the WAN load balancing group, and handles all traffic if all load balancing interfaces are down.

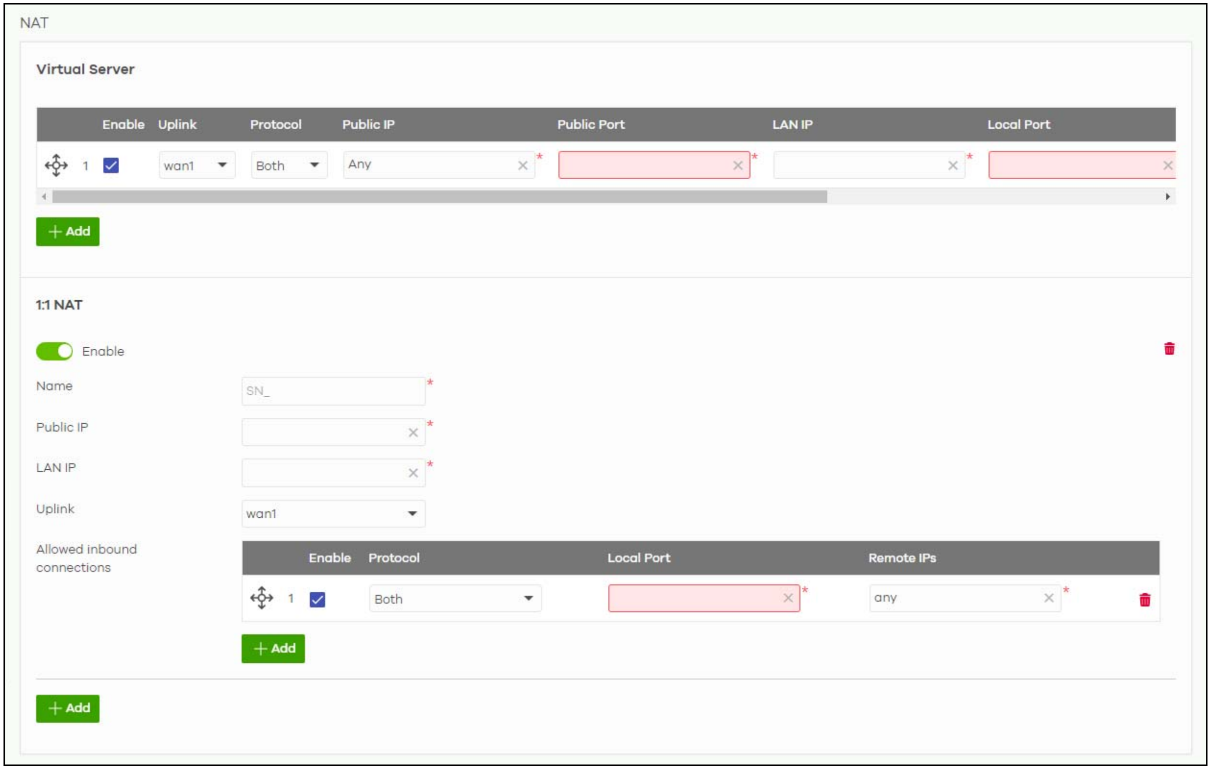
8.3.5 NAT

The NAT summary screen provides a summary of all NAT rules and their configuration. In addition, this screen allows you to create new NAT rules and edit and delete existing NAT rules.

Note: When adding/modifying/removing a NAT rule, based on the NAT setting NCC will automatically add/modify/remove the incoming security policy (firewall) rule in the **Implicit allow rules** list in the **Site-wide** > **Configure** > **Firewall** > **Security policy**.

To access this screen, click **Site-wide** > **Configure** > **Firewall** > **NAT**. The following screen appears, providing a summary of the existing NAT rules.

Figure 175   Site-wide > Configure > Firewall > NAT



NAT

Virtual Server

	Enable	Uplink	Protocol	Public IP	Public Port	LAN IP	Local Port
1	☑	wan1	Both	Any			

1:1 NAT

Enable

Name: SN_

Public IP:

LAN IP:

Uplink: wan1

Allowed inbound connections

	Enable	Protocol	Local Port	Remote IPs
1	☑	Both		any

The following table describes the labels in this screen.

Table 118 Site-wide > Configure > Firewall > NAT

LABEL	DESCRIPTION
Virtual Server	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enable	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Uplink	Select the interface of the Nebula Device on which packets for the NAT rule must be received.
Protocol	Select the IP protocol to which this rule applies. Choices are: **TCP**, **UDP**, and **Both**.
Public IP	Enter the destination IP address of the packets received by the interface specified in this NAT rule. Note: To enable NAT loop-back, enter a specific IP address instead of **Any** in this field. NAT loop-back allows communications between two hosts on the LAN behind the Nebula Device through an external IP address,
Public Port	Enter the translated destination port or range of translated destination ports if this NAT rule forwards the packet.
LAN IP	Specify to which translated destination IP address this NAT rule forwards packets.
Local Port	Enter the original destination port or range of destination ports this NAT rule supports.
Allow Remote IPs	Specify the remote IP addresses that are allowed to access the public IP address. You can add multiple IP, specify a range of IP addresses (CIDR), or GEO IP (country) objects. Select **Any** to allow all IP addresses. Note: IP/CIDR, and GEO IP objects cannot be used at the same time.
Description	This is the descriptive name of the policy.
🗑	Click the remove icon to delete it.
Add	Click this to create a new entry.
1:1 NAT	
Enable	Select this to turn on the rule. Otherwise, turn off the rule.
Name	Enter the name of the NAT rule. The name is used to refer to the NAT rule. You may use 1 – 31 alphanumeric characters, underscores(_), or dashes (-). This value is case-sensitive.
Public IP	Enter the destination IP address of the packets received by the interface specified in this NAT rule.
LAN IP	Specify to which translated destination IP address this NAT rule forwards packets.
Uplink	Select the interface of the Security Firewall on which packets for the NAT rule must be received.
Allowed Inbound connections	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enable	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Protocol	Select the IP protocol to which this rule applies. Choices are: **TCP**, **UDP**, and **Both**.
Local Port	Enter the original destination port or range of destination ports this NAT rule supports.
Remote IPs	Specify the remote IP addresses that are allowed to access the public IP address. You can add multiple IP, specify a range of IP addresses (CIDR), or GEO IP (country) objects. Select **Any** to allow all IP addresses. Note: IP/CIDR, and GEO IP objects cannot be used at the same time.

Table 118 Site-wide > Configure > Firewall > NAT (continued)

LABEL	DESCRIPTION
🗑	Click the remove icon to delete it.
Add	Click this to create a new entry.

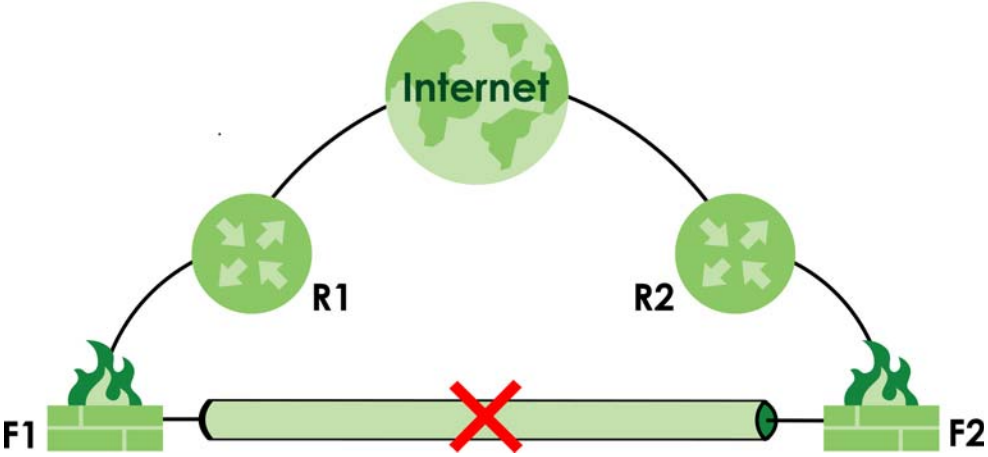
8.3.6 Site-to-Site VPN

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. Use this screen to configure a VPN rule.

Note: Site-to-site VPN does not support both VPN sites behind NAT mode.

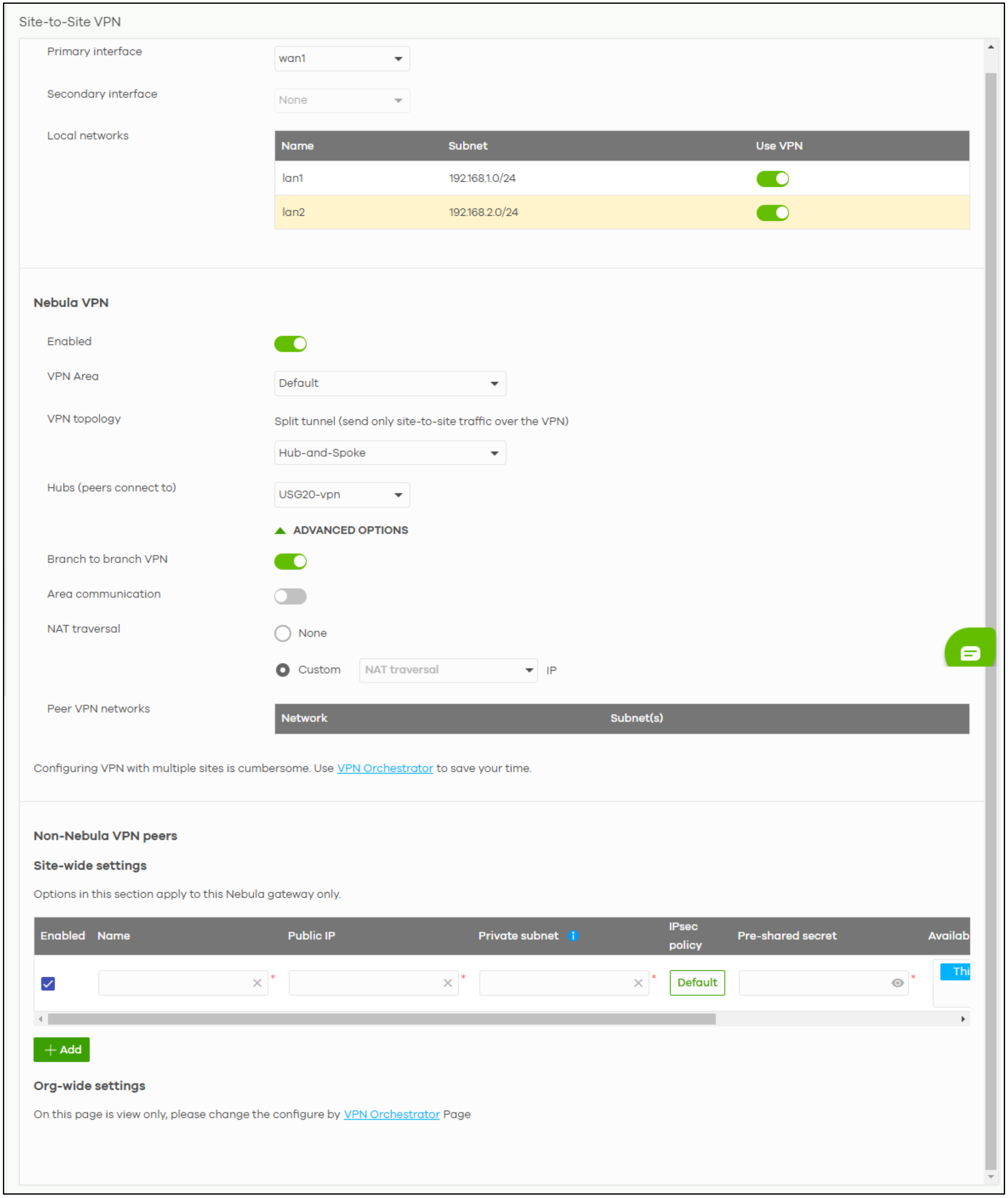
The following figure shows two routers (**R1**, **R2**) with NAT mode enabled. Site-to-site VPN between the two Firewall devices (**F1**, **F2**) is not allowed.

Figure 176 Two VPN Sites Behind NAT Example



Click **Site-wide** > **Configure** > **Firewall** > **Site-to-Site VPN** to access this screen.

Figure 177 Site-wide > Configure > Firewall > Site-to-Site VPN



Site-to-Site VPN

Primary interface: wan1

Secondary interface: None

Local networks

Name	Subnet	Use VPN
lan1	192.168.1.0/24	●
lan2	192.168.2.0/24	●

Nebula VPN

Enabled: ●

VPN Area: Default

VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

Hub-and-Spoke

Hubs (peers connect to): USG20-vpn

ADVANCED OPTIONS

Branch to branch VPN: ●

Area communication: ○

NAT traversal: ○ None

● Custom NAT traversal IP

Peer VPN networks

Network	Subnet(s)

Configuring VPN with multiple sites is cumbersome. Use VPN Orchestrator to save your time.

Non-Nebula VPN peers

Site-wide settings

Options in this section apply to this Nebula gateway only.

Enabled	Name	Public IP	Private subnet	IPsec policy	Pre-shared secret	Availab
☑				Default		Thi

Org-wide settings

On this page is view only, please change the configure by VPN Orchestrator Page

The following table describes the labels in this screen.

Table 119 Site-wide > Configure > Firewall > Site-to-Site VPN

LABEL	DESCRIPTION
Primary interface	Specify the primary WAN interface through which the Nebula Device forwards VPN traffic.
Secondary interface	Specify the secondary WAN interface through which the Nebula Device forwards VPN traffic (if any). This is the backup interface for VPN failover use.

Table 119 Site-wide > Configure > Firewall > Site-to-Site VPN (continued)

LABEL	DESCRIPTION
Local networks	This shows the local networks behind the Nebula Device. Note: Non-Nebula VPN peers use the first interface with a local policy. For example, both lan1 and lan2 are enabled. The first interface in the list 'lan1' will be used. Regardless of the order they are created.
Name	This shows the network name.
Subnet	This shows the IP address and subnet mask of the computer on the network.
Use VPN	Select **ON** to allow the computers on the network to use the VPN tunnel. Otherwise, select **OFF**.
Nebula VPN Enabled	Click this to enable or disable site-to-site VPN on the site's Nebula Device. If you disable this setting, the site will leave the VPN area.
VPN Area	Select the VPN area of the site. For details, see Section 12.4.4.2 on page 691.
VPN Topology	Click this to select a topology for the VPN area. For details on topologies, see Section 12.4.4.1 on page 691. Select disable to disable VPN connections for all sites in the VPN area.
Hubs (peers to connect to)	This field displays the hub sites that the current site is connected to, when **Topology** is set to **Hub-and-Spoke**. You can configure hub sites at **Organization-wide** > **Organization-wide manage** > **VPN orchestrator**.
Branch to branch VPN	Enable this to allow spoke sites to communicate with each other in the VPN area. When disabled, spoke sites can only communicate with hub sites.
Area communication	Enable this to allow the site to communicate with sites in different VPN areas within the organization.
NAT traversal	If the Nebula Device is behind a NAT router, select **Custom** to enter the public IP address or the domain name that is configured and mapped to the Nebula Device on the NAT router. Note: To allow a site-to-site VPN connection, the NAT router must have the following ports open: UDP 500, 4500.
Peer VPN networks	This shows all sites within the VPN area.
Non-Nebula VPN peers Site-wide settings	Configure this section to add a non-Nebula gateway to the VPN area.
+ Add	Click this button to add a non-Nebula gateway to the VPN area.
Enabled	Select the checkbox to enable VPN connections to the non-Nebula gateway.
Name	Enter the name of the non-Nebula gateway.
Public IP	Enter the public IPv4 address or FQDN of the non-Nebula gateway.
Private subnet	Enter the IP subnet that will be used for VPN connections. The IP range must be reachable from other devices in the VPN area.
IPSec policy	Click to select a pre-defined policy or have a custom one. See Section on page 551 for detailed information.
Pre-shared secret	Enter a pre-shared key (password). The Nebula Device and peer gateway use the key to identify each other when they negotiate the IKE SA.

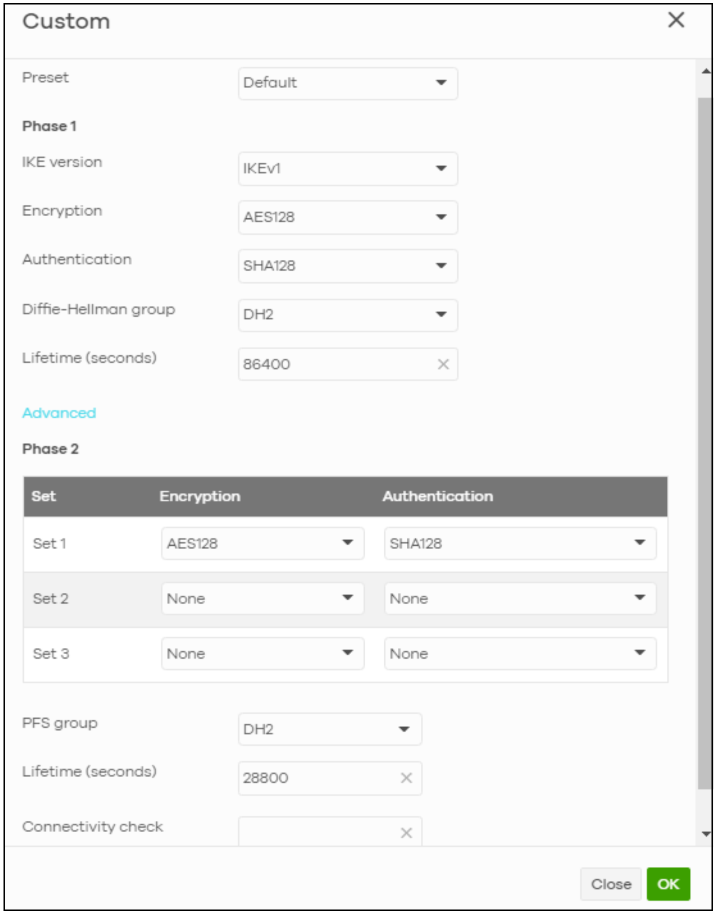
Table 119 Site-wide > Configure > Firewall > Site-to-Site VPN (continued)

LABEL	DESCRIPTION
Availability	Select which sites the non-Nebula gateway can connect to in the VPN area. Select **All sites** to allow the non-Nebula gateway to connect to any site in the VPN area. Select **This site** and the non-Nebula gateway can only connect to the Nebula Device in this site.
Address (physical location)	Enter the address (physical location) of the remote device. You can find this on the **VPN Topology** section on this screen.
🗑	Click the remove icon to delete a non-Nebula gateway from the VPN area.

8.3.6.1 IPsec Policy

Click the **Default** button in the **Non-Nebula VPN peers** section of the **Site-wide** > **Configure** > **Firewall** > **Site-to-Site VPN** screen to access this screen.

Figure 178 Site-wide > Configure > Firewall > Site-to-Site VPN: IPsec Policy



Custom

Preset: Default

Phase 1

IKE version: IKEv1

Encryption: AES128

Authentication: SHA128

Diffie-Hellman group: DH2

Lifetime (seconds): 86400

Advanced

Phase 2

Set	Encryption	Authentication
Set 1	AES128	SHA128
Set 2	None	None
Set 3	None	None

PFS group: DH2

Lifetime (seconds): 28800

Connectivity check:

The following table describes the labels in this screen.

Table 120 Site-wide > Configure > Firewall > Site-to-Site VPN: IPsec Policy

LABEL	DESCRIPTION
Preset	Select a pre-defined IPSec policy, or select **Custom** to configure the policy settings yourself.
Phase1	IPSec VPN consists of two phases: Phase 1 (Authentication) and Phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).
IKE version	Select **IKEv1** or **IKEv2**. **IKEv1** and **IKEv2** applies to IPv4 traffic only. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** – a 56-bit key with the DES encryption algorithm **3DES** – a 168-bit key with the DES encryption algorithm **AES128** – a 128-bit key with the AES encryption algorithm **AES192** – a 192-bit key with the AES encryption algorithm **AES256** – a 256-bit key with the AES encryption algorithm The Nebula Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA128**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than MD5, but it is also slower. The remote IPSec router must use the same authentication algorithm.
Diffie-Hellman group	Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are: **DH1** – use a 768-bit random number Modular Exponential (MODP) DH group **DH2** – use a 1024-bit random number MODP **DH5** – use a 1536-bit random number MODP **DH14** – use a 2048-bit random number MODP **DH19** – use a 256-bit random number elliptic curve group **DH20** – use a 384-bit random number elliptic curve group **DH21** – use a 521-bit random number elliptic curve group The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Lifetime (seconds)	Enter the maximum number of seconds the IKE SA can last. When this time has passed, the Nebula Device and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Advanced	Click this to display a greater or lesser number of configuration fields.
Mode	Set the negotiation mode. **Main** encrypts the Nebula Device's and remote IPSec router's identities but takes more time to establish the IKE SA. **Aggressive** is faster but does not encrypt the identities.

Table 120 Site-wide > Configure > Firewall > Site-to-Site VPN: IPsec Policy (continued)

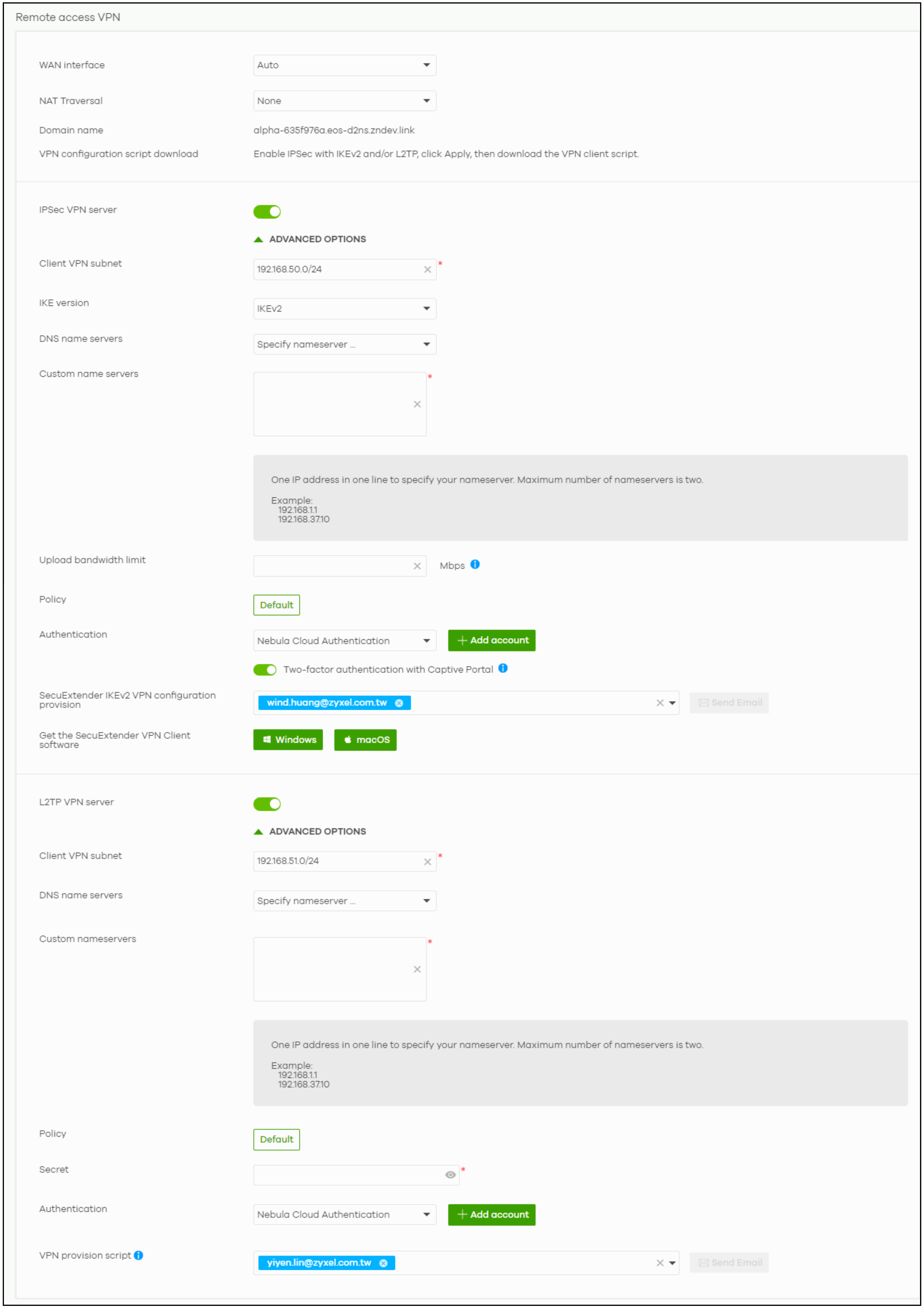
LABEL	DESCRIPTION
Local ID	Enter an identifier used to identify the Nebula Device during authentication. This can be an IP address or hostname.
Peer ID	Enter an identifier used to identify the remote IPSec router during authentication. This can be an IP address or hostname.
Phase2	Phase 2 uses the SA that was established in phase 1 to negotiate SAs for IPSec.
Encryption	Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **(None)** – no encryption key or algorithm **DES** – a 56-bit key with the DES encryption algorithm **3DES** – a 168-bit key with the DES encryption algorithm **AES128** – a 128-bit key with the AES encryption algorithm **AES192** – a 192-bit key with the AES encryption algorithm **AES256** – a 256-bit key with the AES encryption algorithm The Nebula Device and the remote IPSec router must both have at least one proposal that uses the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.
PFS group	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **None** – disable PFS **DH1** – enable PFS and use a 768-bit random number **DH2** – enable PFS and use a 1024-bit random number **DH5** – enable PFS and use a 1536-bit random number **DH14** – enable PFS and use a 2048-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.
Lifetime (seconds)	Enter the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The Nebula Device automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Connectivity check	Enter an IP address that the Nebula Device can ping, to check whether the non-Nebula VPN peer gateway is available. Note: By default, NCC will use the private subnet IP address to do connectivity check.
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

8.3.7 Remote Access VPN

Use this screen to configure the VPN client settings on the Nebula Device. This allows incoming VPN clients to connect to the Nebula Device in order to access the site's network. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.

Click **Site-wide** > **Configure** > **Firewall** > **Remote access VPN** to access this screen.

Figure 179 Site-wide > Configure > Firewall > Remote access VPN



Remote access VPN

WAN interface	Auto
NAT Traversal	None
Domain name	alpha-635f976a.eos-d2ns.zndev.link
VPN configuration script download	Enable IPSec with IKEv2 and/or L2TP, click Apply, then download the VPN client script.
IPSec VPN server	●
	▲ ADVANCED OPTIONS
Client VPN subnet	192.168.50.0/24 *
IKE version	IKEv2
DNS name servers	Specify nameserver ...
Custom name servers	*
	One IP address in one line to specify your nameserver. Maximum number of nameservers is two. Example: 192.168.1.1 192.168.37.10
Upload bandwidth limit	Mbps
Policy	Default
Authentication	Nebula Cloud Authentication + Add account
	● Two-factor authentication with Captive Portal
SecuExtender IKEv2 VPN configuration provision	wind.huang@zyxel.com.tw Send Email
Get the SecuExtender VPN Client software	Windows macOS
L2TP VPN server	●
	▲ ADVANCED OPTIONS
Client VPN subnet	192.168.51.0/24 *
DNS name servers	Specify nameserver ...
Custom nameservers	*
	One IP address in one line to specify your nameserver. Maximum number of nameservers is two. Example: 192.168.1.1 192.168.37.10
Policy	Default
Secret	*
Authentication	Nebula Cloud Authentication + Add account
VPN provision script	yiyen.lin@zyxel.com.tw Send Email

The following table describes the labels in this screen.

Table 121 Site-wide > Configure > Firewall > Remote access VPN

LABEL	DESCRIPTION
WAN interface	Select the WAN interface which VPN users connect to.
NAT Traversal	If the Nebula Device is behind a NAT router, select **+ Customize IP** to enter the public IP address that is configured and mapped to the Nebula Device on the NAT router. Select **None** to map to the WAN IP of the Nebula Device. NCC automatically updates the DNS server when the WAN IP changes. Or, select **Auto** to allow NCC to detect automatically the public IP of your Nebula Device. NCC automatically selects another WAN interface when the selected WAN interface is down. NCC automatically updates the DNS server when the public IP changes.
Domain name	This displays the domain name that maps to a WAN interface IP address. Note: The mapping priority is WAN1, WAN2. This field is available only when you select **AUTO** in the **WAN interface** field.
VPN configuration script download	Click the **Windows**, **iOS/macOS** or **Android (strongSwan)** icon to download a ZIP file containing the VPN remote access configuration script. After unzipping, save the certificate (.crt) and script (.bat) files to the same folder in your computer. This field is available only when you enable **IPSec VPN server** with **IKEv2** in IKE version field or **L2TP VPN server** and the Nebula Device is online. The **Android (strongSwan)** option is available only for **IPSec VPN server** with **IKEv2** in IKE version field. Note: For **iOS/macOS**, the default authentication type is **Certificate**. To enter the user name and password, change the user authentication type to **Username**.
IPSec VPN server	Select this to enable the IPsec VPN server.
Client VPN subnet	Specify the IP addresses that the Nebula Device uses to assign to the VPN clients. The default subnet is **192.168.50.0/24**.
IKE version	Select **IKEv1** or **IKEv2**. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely.
DNS name servers	Specify the DNS servers to assign to the remote users. Or select **Specify nameserver** to enter a static IP address.
Custom name servers	If you select **Specify nameserver** in the **DNS name servers** field, manually enter the DNS server IP addresses.
Upload Bandwidth Limit	This field is available only if you select **IKEv2** in **IKE version**. Enter the maximum traffic load between VPN clients, 1 – 100 Mbps.
Policy	Configure custom VPN tunnel settings. For details, see Section 8.3.7.1 on page 514.
Authentication	Select how the Nebula Device authenticates a remote user before allowing access to the VPN tunnel. Click **Create a cloud auth account** to create a Nebula Cloud Authentication Server user account. This will automatically add the site where you create remote access VPN setup to the **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **User** screen and bypass two-factor authentication.
Two-factor authentication with Captive Portal	Select this to require two-factor authentication for a user to access the Nebula Device through VPN. Note: Two-factor authentication is only supported with Zyxel SecuExtender IPSec client.

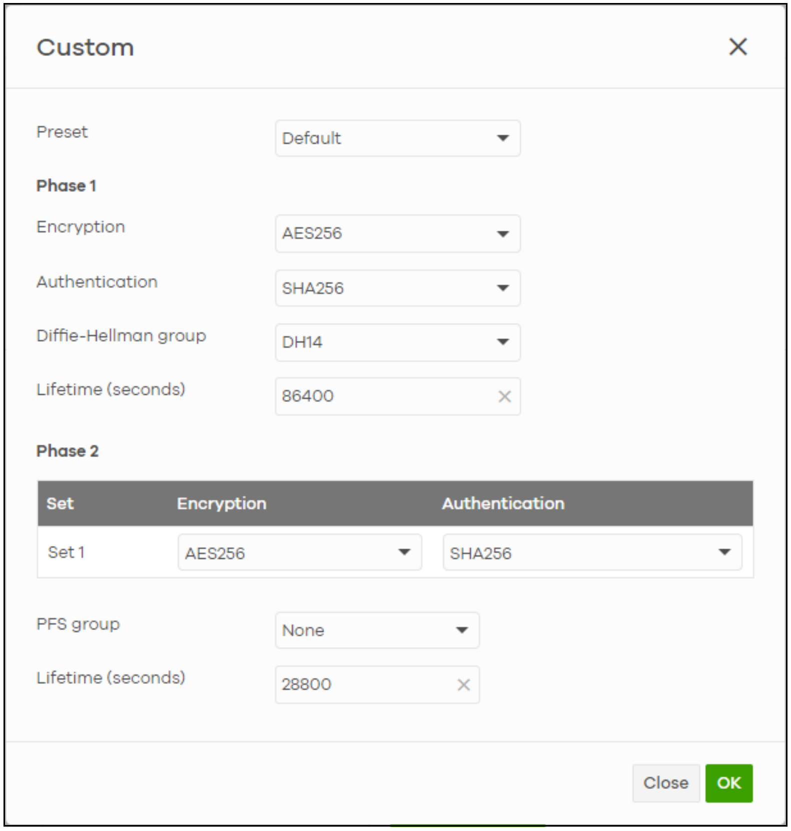
Table 121 Site-wide > Configure > Firewall > Remote access VPN (continued)

LABEL	DESCRIPTION
SecuExtender IKEv2 VPN configuration provision	Enter the email address to send new IKEv2 Remote Access VPN configuration file to VPN client. Then click **Send Email**. The VPN client needs to replace the IPSec VPN client configuration by importing the configuration file.
Get the SecuExtender VPN Client software	Click the **Windows** or **macOS** icon to download the SecuExtender VPN client software.
VPN configuration script download	Click the **Windows**, **iOS/macOS** or **Android (strongSwan)** icon to download a ZIP file containing the VPN remote access configuration script. After unzipping, save the certificate (.crt) and script (.bat) files to the same folder in your computer. This field is available only when you enable **IPSec VPN server** with **IKEv2** in IKE version field or **L2TP VPN server** and the Nebula Device is online. The **Android (strongSwan)** option is available only for **IPSec VPN server** with **IKEv2** in IKE version field. Note: For **iOS/macOS**, the default authentication type is **Certificate**. To enter the user name and password, change the user authentication type to **Username**.
L2TP VPN server	Select this to enable the L2TP over IPSec VPN server.
Client VPN subnet	Specify the IP addresses that the Nebula Device uses to assign to the VPN clients. The default L2TP VPN subnet is 192.168.51.0/24. This is the same for all the sites in your organization.
DNS name servers	Specify the DNS servers to assign to the remote users. Or select **Specify nameserver** to enter a static IP address.
Custom nameservers	If you select **Specify nameserver** in the **DNS name servers** field, manually enter the DNS server IP addresses.
Policy	Configure custom VPN tunnel settings. For details, see Section 8.3.7.1 on page 514.
Secret	This field is available only if you select **IKEv1** in **IKE version**. Enter the pre-shared key (password) which is used to set up the VPN tunnel. The password should be 8 – 32 characters.
Authentication	Select how the Nebula Device authenticates a remote user before allowing access to the VPN tunnel. Click **+Add account** to create a Nebula Cloud Authentication Server user account. This will automatically add the site where you create remote access VPN setup to the **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **User** screen and bypass two-factor authentication.
VPN provision script	Send an email to help automatically configure VPN settings on client devices so that the devices can remotely access this Nebula Device. The email contains two scripts; one for mac OS and iOS devices, and one for Windows 8 and Windows 10 devices. You can send the email to one or more email addresses. • If **Authentication** is set to **Nebula Cloud Authentication**, the default email address list contains all authorized VPN user email addresses and your email address. • If **Authentication** is set to **AD and RADIUS Authentication**, the default email address list contains your user email address. This field is available only when you select **L2TP over IPSec client** in the **Client VPN server** field.

8.3.7.1 Remote Access VPN > Custom VPN Policy

Click **Default** in **Site-wide** > **Configure** > **Firewall** > **Remote access VPN** > **Policy** to open the following screen.

Figure 180 Site-wide > Configure > Firewall > Remote access VPN: Default



Custom

Preset: Default

Phase 1

Encryption: AES256

Authentication: SHA256

Diffie-Hellman group: DH14

Lifetime (seconds): 86400

Phase 2

Set	Encryption	Authentication
Set 1	AES256	SHA256

PFS group: None

Lifetime (seconds): 28800

The following table describes the labels in this screen.

Table 122 Site-wide > Configure > Firewall > Remote access VPN: Default

LABEL	DESCRIPTION
Custom	
Preset	Select a pre-defined IPSec policy, or select **Custom** to configure the policy settings yourself.
Phase 1	
Encryption	Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **(None)** – no encryption key or algorithm **DES** – a 56-bit key with the DES encryption algorithm **3DES** – a 168-bit key with the DES encryption algorithm **AES128** – a 128-bit key with the AES encryption algorithm **AES192** – a 192-bit key with the AES encryption algorithm **AES256** – a 256-bit key with the AES encryption algorithm The Nebula Device and the remote IPSec router must both have at least one proposal that use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.

Table 122 Site-wide > Configure > Firewall > Remote access VPN: Default (continued)

LABEL	DESCRIPTION
Authentication	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA128**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than MD5, but it is also slower. The remote IPSec router must use the same authentication algorithm.
Diffie-Hellman group	Select the Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are: **DH1** – use a 768-bit random number Modular Exponential (MODP) DH group **DH2** – use a 1024-bit random number MODP **DH5** – use a 1536-bit random number MODP **DH14** – use a 2048-bit random number MODP **DH19** – use a 256-bit random number elliptic curve group **DH20** – use a 384-bit random number elliptic curve group **DH21** – use a 521-bit random number elliptic curve group The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Lifetime (seconds)	Enter the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The Nebula Device automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Phase 2	
Set	This shows the index number of the IPSec policy.
Encryption	Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **(None)** – no encryption key or algorithm **DES** – a 56-bit key with the DES encryption algorithm **3DES** – a 168-bit key with the DES encryption algorithm **AES128** – a 128-bit key with the AES encryption algorithm **AES192** – a 192-bit key with the AES encryption algorithm **AES256** – a 256-bit key with the AES encryption algorithm The Nebula Device and the remote IPSec router must both have at least one proposal that use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **None**, **SHA128**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than MD5, but it is also slower. The remote IPSec router must use the same authentication algorithm.

Table 122 Site-wide > Configure > Firewall > Remote access VPN: Default (continued)

LABEL	DESCRIPTION
PFS group	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **None** – disable PFS **DH1** – enable PFS and use a 768-bit random number **DH2** – enable PFS and use a 1024-bit random number **DH5** – enable PFS and use a 1536-bit random number **DH14** – enable PFS and use a 2048 bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.
Lifetime (seconds)	Enter the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The Security Firewall automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

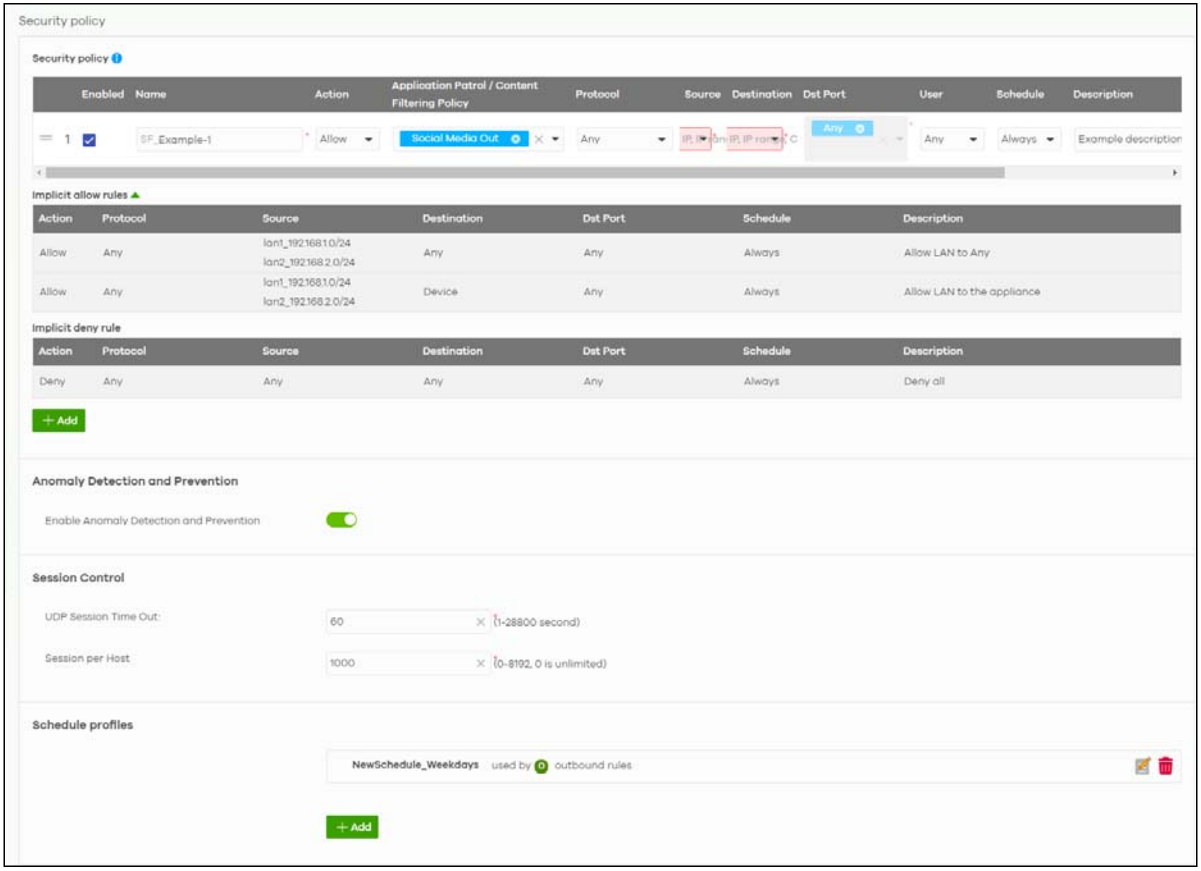
8.3.8 Security Policy

By default, a LAN user can initiate a session from within the LAN and the Nebula Device allows the response. However, the Nebula Device blocks incoming traffic initiated from the WAN and destined for the LAN. Use this screen to configure firewall rules for outbound traffic, application patrol and content filter, schedule profiles and port forwarding rules for inbound traffic.

Click **Site-wide** > **Configure** > **Firewall** > **Security policy** to access this screen.

Note: The Nebula Device has the following hidden default firewall rules: LAN to WAN is allowed, WAN to LAN is blocked.

Figure 181 Site-wide > Configure > Firewall > Security policy



Security policy

Security policy

	Enabled	Name	Action	Application Patrol / Content Filtering Policy	Protocol	Source	Destination	Dst Port	User	Schedule	Description
1	☑	SF_Example-1	Allow	Social Media Out	Any	IP, IP	IP, IP ran	Any	Any	Always	Example description

Implicit allow rules

Action	Protocol	Source	Destination	Dst Port	Schedule	Description
Allow	Any	lan1_192.168.1.0/24 lan2_192.168.2.0/24	Any	Any	Always	Allow LAN to Any
Allow	Any	lan1_192.168.1.0/24 lan2_192.168.2.0/24	Device	Any	Always	Allow LAN to the appliance

Implicit deny rule

Action	Protocol	Source	Destination	Dst Port	Schedule	Description
Deny	Any	Any	Any	Any	Always	Deny all

+ Add

Anomaly Detection and Prevention

Enable Anomaly Detection and Prevention ●

Session Control

UDP Session Time Out: 60 (1-28800 second)

Session per Host: 1000 (0-8192, 0 is unlimited)

Schedule profiles

NewSchedule_Weekdays used by 0 outbound rules

+ Add

The following table describes the labels in this screen.

Table 123 Site-wide > Configure > Firewall > Security policy

LABEL	DESCRIPTION
Security policy	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Name	Enter the name of the security policy.
Action	Select what the Nebula Device is to do with packets that match this rule. Select **Deny** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Allow** to permit the passage of the packets.
Application Patrol / Content Filtering Policy	Click the "**+**" to add an Application Patrol or Content Filter profile. The firewall takes the action set in the profile when traffic matches the profile's policy. Application Patrol manages the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers). See Section 8.3.8.1 on page 520 for how to create an Application Patrol profile. Content Filter controls access to specific web sites or web content. See Section 8.3.8.2 on page 521 for how to create a Content Filter profile.

Table 123 Site-wide > Configure > Firewall > Security policy (continued)

LABEL	DESCRIPTION
Protocol	Select the IP protocol to which this rule applies. Choices are: **ICMP**, **TCP**, **UDP**, **TCP and UDP** and **Any**.
Source	Specify the source IP addresses (LAN interface / country) to which this rule applies. You can add multiple IP, CIDR, FQDN, GEO IP (country) objects, or a single FQDN object by pressing 'Enter', or enter a new IP address by clicking **Add**. Enter **any** to apply the rule to all IP addresses. Note: IP/CIDR, FQDN, and GEO IP objects cannot be used at the same time. Multiple FQDNs are not supported. The IP FQDN does NOT support wildcards.
Destination	Specify the destination IP addresses (LAN interface / country) or subnet to which this rule applies. You can add multiple IP, CIDR, GEO IP (country) objects or a single FQDN object by pressing 'Enter', or enter a new IP address by clicking **Add**. Enter **any** to apply the rule to all IP addresses. Note: IP/CIDR, FQDN, and GEO IP objects cannot be used at the same time. Multiple FQDNs are not supported.
Dst Port	Specify the destination ports to which this rule applies. You can specify multiple ports by pressing 'Enter', or enter a new port by clicking **Add**. Enter **any** to apply the rule to all ports.
User	Select the **External User Group** name configured in **Site-wide** > **Configure** > **Firewall** > **Firewall settings**.
Schedule	Select the name of the schedule profile that the rule uses. **Always** means the rule is active at all times if enabled.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the rule.
Log	Select whether to have the Nebula Device generate a log (**ON**) or not (**OFF**) when traffic matches the profile's policy. Note: By default, **Log** is **ON** when the **Action** field is **Deny**. **Log** is **OFF** when the **Action** field is **Allow**.
🗑	Click this icon to remove the rule.
Implicit allow rules	This shows the system generated **Allow** rules. • 1:1 NAT • NAT virtual server • LAN interface / remote access VPN to **Any** • Guest interface to WAN interface • LAN interface / remote access VPN to Nebula Device • Guest interface to Nebula Device TCP (TCP:443, 80, 53) • Guest interface to Nebula Device UDP (UDP:53)
Implicit deny rule	This shows the system generated **Deny** rule. • **Any** to **Any**
Add	Click this button to create a new rule.
Anomaly Detection and Prevention	
Enable Anomaly Detection and Prevention	Select this to enable traffic anomaly and protocol anomaly detection and prevention.
Session Control	
UDP Session Time Out	Set how many seconds the Nebula Device will allow a UDP session to remain idle (without UDP traffic) before closing it.

Table 123 Site-wide > Configure > Firewall > Security policy (continued)

LABEL	DESCRIPTION
Session per Host	Use this field to set a common limit to the number of concurrent NAT/Security Policy sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Schedule profiles	
Schedule name	This shows the name of the schedule profile and the number of the outbound rules that are using this schedule profile.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this button to create a new schedule profile. See Section 8.3.8.3 on page 524 for more information.

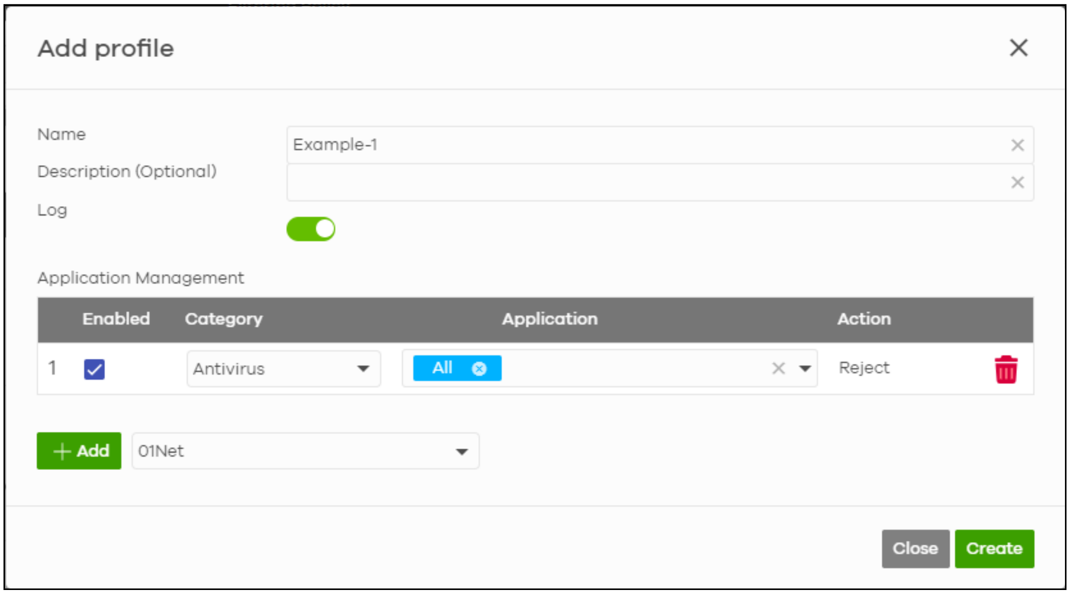
8.3.8.1 Add an Application Patrol Profile

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers).

An application patrol profile is a group of categories of application patrol signatures. For each profile, you can specify the default action the Nebula Device takes once a packet matches a signature (forward, drop, or reject a service's connections and/or create a log alert).

Click "**+**" in the **Application Patrol/Content Filtering Policy** field of the **Site-wide** > **Configure** > **Firewall** > **Security policy** screen to access this screen. Use the application patrol profile screens to customize action and log settings for a group of application patrol signatures.

Figure 182 Site-wide > Configure > Firewall > Security policy > Application patrol: Add an Application Profile



Add profile

Name: Example-1

Description (Optional):

Log: ●

Application Management

	Enabled	Category	Application	Action
1	☑	Antivirus	All	Reject

The following table describes the labels in this screen.

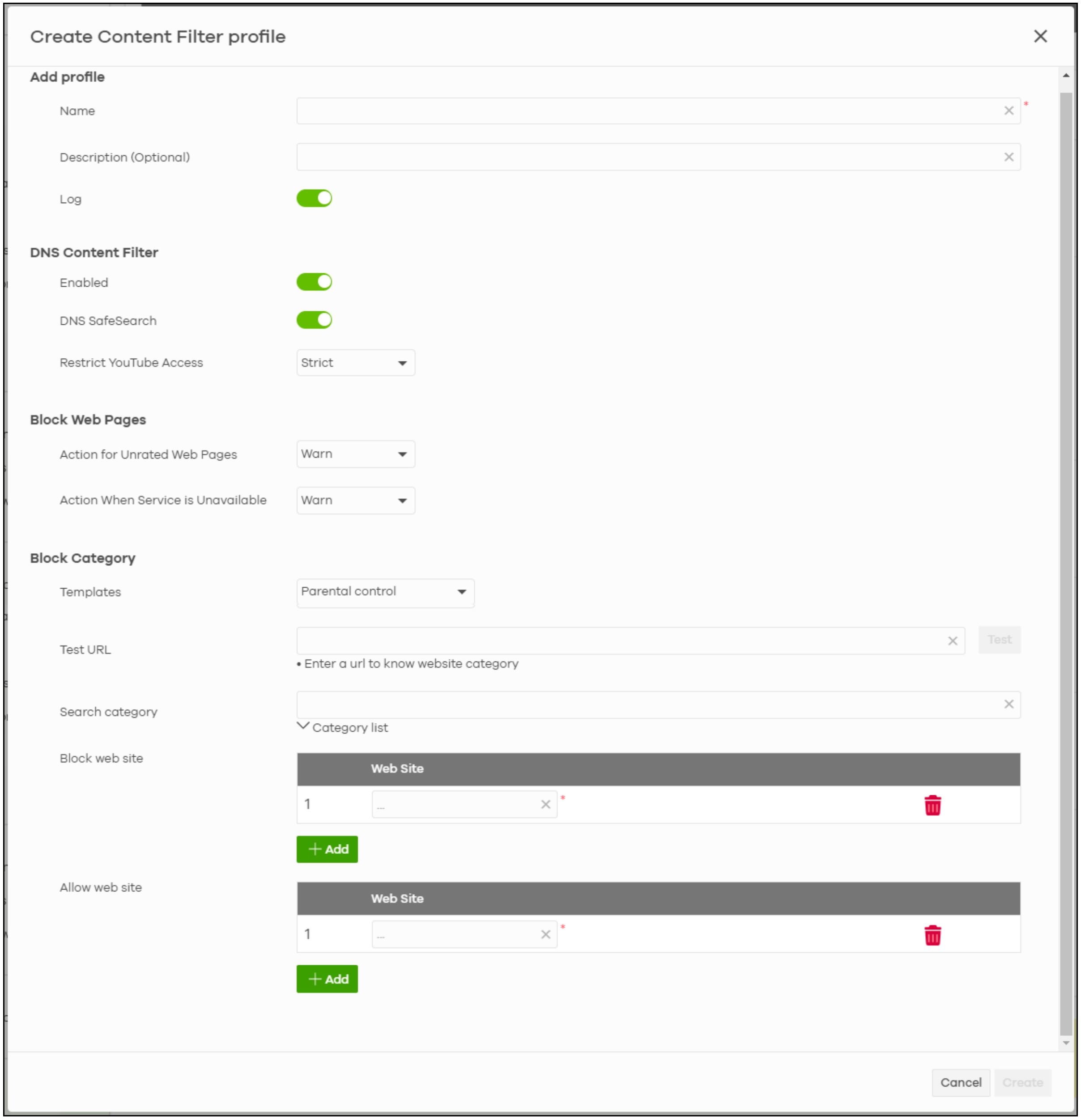
Table 124 Site-wide > Configure > Firewall > Security policy > Application patrol: Add an Application Profile

LABEL	DESCRIPTION
Name	Enter a name for this profile for identification purposes [a-zA-Z0-9_-], up to 30 characters.
Description (Optional)	Enter a description for this profile.
Log	Select whether to have the Nebula Device generate a log (**ON**) or not (**OFF**) by default when traffic matches an application signature in this category.
Application Management	
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Category	Select an application category.
Application	Select **All** or select an application within the category to apply the policy.
Action	Select the default action for the applications selected in this category. **Reject** – the Nebula Device drops packets that matches these application signatures and sends notification to clients. **Drop** – the Nebula Device silently drops packets that matches these application signatures without sending notification to clients. **Forward** – the Nebula Device routes packets that matches these application signatures.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new application category and set actions for specific applications within the category.
	Enter a name to search for relevant applications and click **Add** to create an entry.
Close	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

8.3.8.2 Add a Content Filter Profile

Click "**+**" in the **Application Patrol**/**Content Filtering Policy** section of the **Site-wide** > **Configure** > **Firewall** > **Security policy** screen to access this screen.

Figure 183 Site-wide > Configure > Firewall > Security policy > Content filtering: Create content filter profile



Create Content Filter profile

Add profile

Name

Description (Optional)

Log: On

DNS Content Filter

Enabled: On

DNS SafeSearch: On

Restrict YouTube Access: Strict

Block Web Pages

Action for Unrated Web Pages: Warn

Action When Service is Unavailable: Warn

Block Category

Templates: Parental control

Test URL

- Enter a url to know website category

Search category

Category list

Block web site

	Web Site
1	...

Allow web site

	Web Site
1	...

The following table describes the labels in this screen.

Table 125 Site-wide > Configure > Firewall > Security policy > Content filtering: Create Content Filter profile

LABEL	DESCRIPTION
Add profile	
Name	Enter a name for this profile for identification purposes. Use up to 127 characters (0 – 9 a – z). The casing does not matter.
Description (Optional)	Enter a description for this profile.

Table 125 Site-wide > Configure > Firewall > Security policy > Content filtering: Create Content Filter profile (continued)

LABEL	DESCRIPTION
Log	Select whether to have the Nebula Device generate a log (**ON**) or not (**OFF**) by default when traffic matches an application signature in this category.
DNS Content Filter	
Enabled	Select whether to enable DNS content filter, in addition to web content filtering. The DNS Content Filter allows the Nebula Device to block access to specific websites by inspecting DNS queries made by users on your network. Content Filter checks all DNS queries including DNS queries to remote DNS servers.
DNS SafeSearch	Select On to enable content filter on the YouTube search engine.
Restrict YouTube Access	Select **Strict**/**Moderate** to avoid explicit and inappropriate results. Note: Make sure to select a search category from the **Block Category** list. Otherwise, NCC automatically disables content filter and safe search. Note: To allow YouTube safe search, make sure **Streaming Media** is not selected in the **Block Category** list.
Block Web Pages	
Action for Unrated Web Pages	Select **Pass** to allow users to access web pages that the external web filtering service has not categorized. Select **Block** to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. Select **Warn** to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.
Action When Service is Unavailable	Select **Pass** to allow users to access any requested web page if the external content filter database is unavailable. Select **Block** to block access to any requested web page if the external content filter database is unavailable. Select **Warn** to display a warning message before allowing users to access any requested web page if the external content filter database is unavailable. The following are possible causes for the external content filter server not being available: • There is no response from the external content filter server within the time period specified in the Content Filter Server Unavailable Timeout field. • The Nebula Device is not able to resolve the domain name of the external content filter database. • There is an error response from the external content filter database. This can be caused by an expired content filter registration (External content filter's license key is invalid").
Block Category	
Templates	Select the block category. Choices are **Parental control**, **Productivity** and **Custom**.
Test URL	You can check which category a web page belongs to. Enter a web site URL in the text box, then click **Test**. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. Content Filter can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. URL to test displays both results in the test.

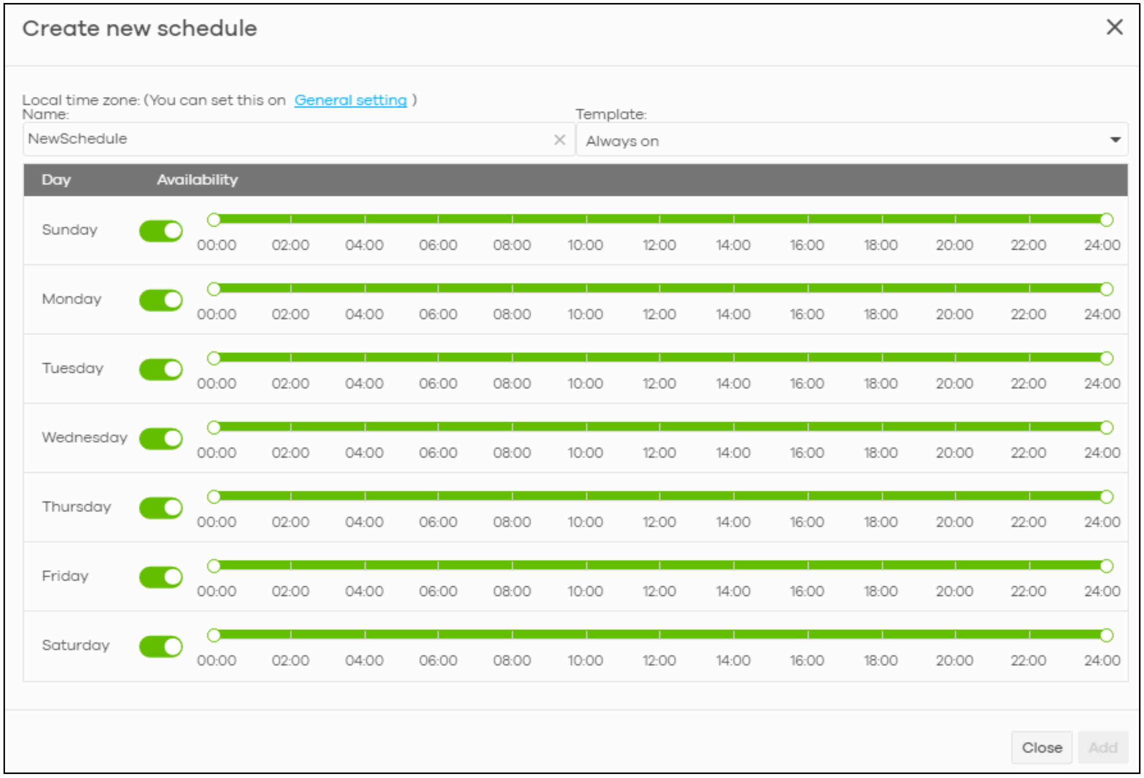
Table 125 Site-wide > Configure > Firewall > Security policy > Content filtering: Create Content Filter profile (continued)

LABEL	DESCRIPTION
Search category	Click to display or hide the category list. These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
Block web site	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0 – 9 a – z). The casing does not matter.
Add	Click this button to create a new application category and set actions for specific applications within the category.
🗑	Click this icon to remove the entry.
Allow web site	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0 – 9 a – z). The casing does not matter.
Add	Click this button to create a new application category and set actions for specific applications within the category.
🗑	Click this icon to remove the entry.
Cancel	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

8.3.8.3 Create a New Schedule

Click the **Add** button in the **Schedule Profiles** section of the **Site-wide** > **Configure** > **Firewall** > **Security policy** > **Schedule profiles** screen to access this screen.

Figure 184 Site-wide > Configure > Firewall > Security policy > Schedule profiles: Create new schedule



Create new schedule

Local time zone: (You can set this on General setting)

Name: NewSchedule

Template: Always on

Day	Availability
Sunday	On, 00:00 – 24:00
Monday	On, 00:00 – 24:00
Tuesday	On, 00:00 – 24:00
Wednesday	On, 00:00 – 24:00
Thursday	On, 00:00 – 24:00
Friday	On, 00:00 – 24:00
Saturday	On, 00:00 – 24:00

The following table describes the labels in this screen.

Table 126 Site-wide > Configure > Firewall > Security policy > Schedule profiles: Create new schedule

LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identification purposes.
Templates	Select a pre-defined schedule template or select **Custom schedule** and manually configure the day and time at which the associated firewall outbound rule is enabled.
Day	This shows the day of the week.
Availability	Click **On** to enable the associated rule at the specified time on this day. Otherwise, select **Off** to turn the associated rule off at the specified time on this day. Specify the hour and minute when the schedule begins and ends each day.
Close	Click this button to exit this screen without saving.
Add	Click this button to save your changes and close the screen.

8.3.9 Security Service

Use this screen to enable or disable the features available in the security pack for your Nebula Device, such as content filter, Intrusion Detection and Prevention (IDP) and/or anti-virus. As to application patrol, go to the **Firewall** screen to configure it since you need to have a firewall rule for outbound traffic.

Content filter allows you to block access to specific web sites. It can also block access to specific categories of web site content. IDP can detect malicious or suspicious packets used in network-based intrusions and respond instantaneously. Anti-virus helps protect your connected network from virus/spyware infection.

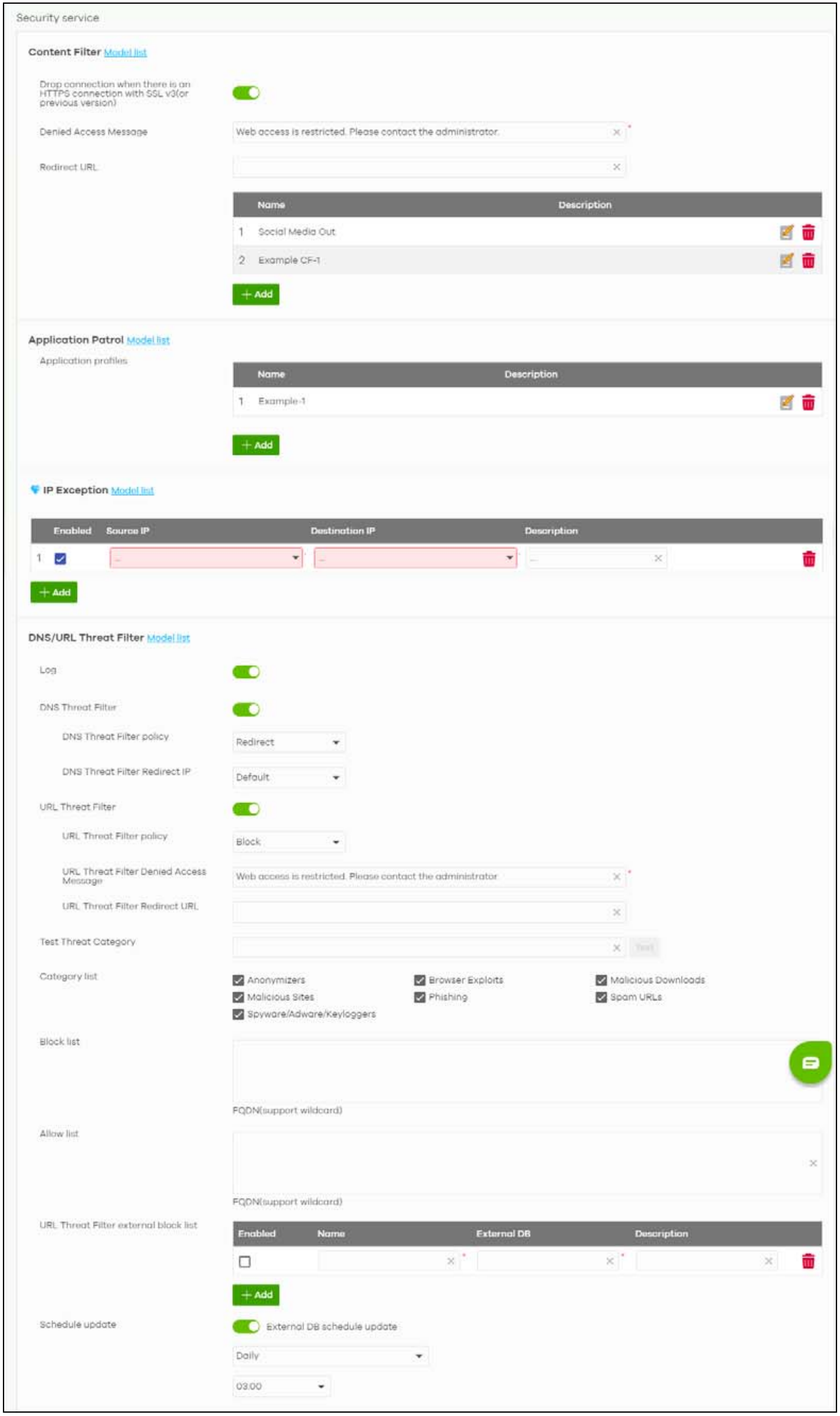
Note: Packet inspection signatures examine packet content for malicious data. Packet inspection applies to OSI (Open System Interconnection) layer-4 to layer-7 contents. You need to subscribe for IDP service in order to be able to download new signatures.

Note: If Security Profile Sync (SPS) is enabled, you cannot configure security settings on this screen. For details, see Section 12.4.5 on page 695.

8.3.9.1 For Security Firewall (USG FLEX / ATP Series)

This section describes the Security Service feature for USG FLEX / ATP Series. Click **Site-wide** > **Configure** > **Firewall** > **Security service** to access this screen.

Figure 185 Site-wide > Configure > Firewall > Security service



Security service

Content Filter Model list

Drop connection when there is an HTTPS connection with SSL v3(or previous version): On

Denied Access Message: Web access is restricted. Please contact the administrator.

Redirect URL:

	Name	Description
1	Social Media Out	
2	Example CF-1	

+ Add

Application Patrol Model list

Application profiles

	Name	Description
1	Example-1	

+ Add

IP Exception Model list

	Enabled	Source IP	Destination IP	Description
1	☑	-	-	-

+ Add

DNS/URL Threat Filter Model list

Log: On

DNS Threat Filter: On

DNS Threat Filter policy: Redirect

DNS Threat Filter Redirect IP: Default

URL Threat Filter: On

URL Threat Filter policy: Block

URL Threat Filter Denied Access Message: Web access is restricted. Please contact the administrator

URL Threat Filter Redirect URL:

Test Threat Category: Test

Category list:

☑ Anonymizers ☑ Browser Exploits ☑ Malicious Downloads
☑ Malicious Sites ☑ Phishing ☑ Spam URLs
☑ Spyware/Adware/Keyloggers

Block list:

FQDN(support wildcard)

Allow list:

FQDN(support wildcard)

URL Threat Filter external block list

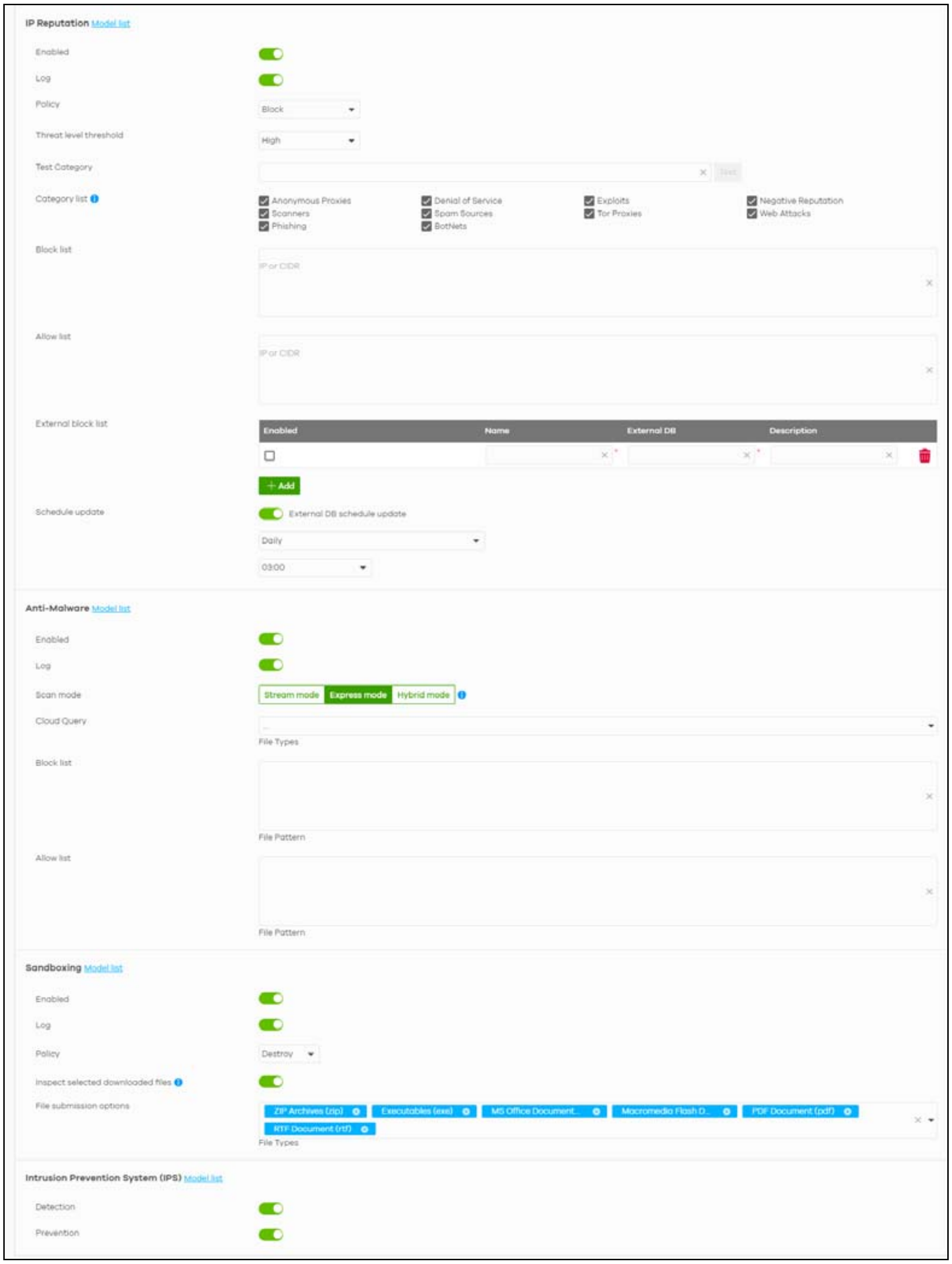
Enabled	Name	External DB	Description
☐			

+ Add

Schedule update: On External DB schedule update

Daily

03:00



IP Reputation Model list

Enabled: On

Log: On

Policy: Block

Threat level threshold: High

Test Category

Category list

☑ Anonymous Proxies
☑ Scanners
☑ Phishing
☑ Denial of Service
☑ Spam Sources
☑ BotNets
☑ Exploits
☑ Tor Proxies
☑ Negative Reputation
☑ Web Attacks

Block list: IP or CIDR

Allow list: IP or CIDR

External block list

Enabled	Name	External DB	Description
□			

+ Add

Schedule update: On External DB schedule update

Daily

03:00

Anti-Malware Model list

Enabled: On

Log: On

Scan mode: Stream mode / Express mode / Hybrid mode (Express mode selected)

Cloud Query: File Types

Block list: File Pattern

Allow list: File Pattern

Sandboxing Model list

Enabled: On

Log: On

Policy: Destroy

Inspect selected downloaded files: On

File submission options: ZIP Archives (zip), Executables (exe), MS Office Document..., Macromedia Flash D..., PDF Document (pdf), RTF Document (rtf)

File Types

Intrusion Prevention System (IPS) Model list

Detection: On

Prevention: On

The following table describes the labels in this screen.

Table 127 Site-wide > Configure > Firewall > Security service

LABEL	DESCRIPTION
Content Filter	
Drop connection when there is an HTTPS connection with SSL V3 (or previous version)	Select **On** to have the Nebula Device block HTTPS web pages using SSL V3 or a previous version.

Table 127 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0–9 a–z A–Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the **Redirect URL** field. In this case if the content filter blocks access to a web page, the Nebula Device just opens the web page you specified without showing a denied access message.
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0–9 a–z A–Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Name	This shows the name of this content filter profile.
Description	This shows the description for this profile.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this to create a content filter profile. See Section 8.3.8.2 on page 521 for more information.
Application Patrol Application profiles	
Name	This shows the name of this Application Patrol profile.
Description	This shows the description for this profile.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this to create an Application Patrol profile. See Section on page 553 for more information.
IP Exception	
Enabled	Select the checkbox to enable IP Exception. IP addresses listed here are not checked by security services.
Source IP	This field displays the source IP address of incoming traffic. It displays any if there is no restriction on the source IP address.
Destination IP	This field displays the destination IP address of incoming traffic. It displays any if there is no restriction on the destination IP address.
Description	Enter a description for this profile.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
DNS/URL Threat Filter	DNS filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs). If a user attempts to connect to a suspect site, where the DNS query packet contains an FQDN with a bad reputation, then a DNS query is sent from the user's computer and detected by the DNS Filter. The Nebula Device DNS filter will either drop the DNS query or reply to the user with a fake DNS response using the default dnsft.cloud.zyxel.com IP address (where the user will see a "Web Page Blocked!" page) or a custom IP address. When you enable the URL Threat filtering service, your Nebula Device downloads signature files that contain known URL Threat domain names and IP addresses. The Nebula Device will also access an external database, Cloud Query, that has millions of web sites categorized based on content. You can have the Nebula Device allow, block, warn and/or log access to web sites or hosts based on these signatures and categories.

Table 127 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed above.
DNS Threat Filter	Select **On** to turn on the rule. Otherwise, select **Off** to turn off the rule.
DNS Threat Filter Policy	Select **Pass** to have the Nebula Device allow the DNS query packet and not reply with a DNS reply packet containing a default or custom-defined IP address. Select **Redirect** to have the Nebula Device reply with a DNS reply packet containing a default or custom-defined IP address.
DNS Threat Filter Redirect IP	Enter the IP address to have the Nebula Device reply with a DNS reply packet containing a default or custom-defined IP address when a DNS query packet contains an FQDN with a bad reputation. The default IP is the dnsft.cloud.zyxel.com IP address. If you select a custom-defined IP, then enter a valid IPv4 address in the text box.
URL Threat Filter	Select **On** to turn on the rule. Otherwise, select **Off** to turn off the rule.
URL Threat Filter Policy	Select **Pass** to allow users to access web pages that the external web filtering service has not categorized. Select **Block** to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filter blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. Select **Warn** to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.
URL Threat Filter Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0–9 a–z A–Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the **Redirect URL** field. In this case if the content filter blocks access to a web page, the Nebula Device just opens the web page you specified without showing a denied access message.
URL Threat Filter Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0–9 a–z A–Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Test Threat Category	Enter a URL using http://domain or https://domain and click the **Test** button to check if the domain belongs to a URL threat category.
Category List	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
Block list	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.

Table 127 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Allow list	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
URL Threat Filter external block list	The Nebula Device uses black list entries stored in a file on a web server that supports HTTP or HTTPS. The Nebula Device blocks incoming and outgoing packets from the black list entries in this file.
Enabled	Select this to have the Nebula Device block the incoming packets that come from the listed addresses in the block list file on the server.
Name	Enter an identifying name for the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
External DB	Enter the exact file name, path and IP address of the server containing the block list file. The file type must be 'txt'. For example, http://172.16.107.20/blacklist-files/myip-ebl.txt The server must be reachable from the Nebula Device.
Description	Enter a description of the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Schedule update	The signatures for DNS Filter and URL Threat Filter are the same. These signatures are continually updated as new malware evolves. New signatures can be downloaded to the Nebula Device periodically if you have subscribed for the URL Threat filter signatures service. You need to create an account at myZyxel, register your Nebula Device and then subscribe for URL Threat filter service in order to be able to download new signatures from myZyxel. Select **Daily** to set the time of the day, or **Weekly** to set the day of the week and the time of the day. Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.
IP Reputation	
Enabled	Select this option to turn on IP blocking on the Nebula Device.
Log	Select this option to create a log on the Nebula Device when the packet comes from an IPv4 address with bad reputation.
Policy	Select **Pass** to have the Nebula Device allow the packet to go through. Select **Block** to have the Nebula Device deny the packets and send a TCP RST to both the sender and receiver when a packet comes from an IPv4 address with bad reputation.

Table 127   Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Threat level threshold	Select the threshold threat level to which the Nebula Device will take action (**High**, **Medium and above**, **Low and above**). The threat level is determined by the IP reputation engine. It grades IPv4 addresses. • **High**: an IPv4 address that scores 0 to 20 points. • **Medium and above**: an IPv4 address that scores 0 to 60 points. • **Low and above**: an IPv4 address that scores 0 to 80 points. For example, a score of "10" will cause the Nebula Device to take action whether you set the **Threat level threshold** at **High**, **Medium and above**, or **Low and above**. But a score of "61" will not cause the Nebula Device to take any action if you set the **Threat level threshold** at **Medium and above**.
Test Category	Enter an IPv4 address of a website, and click the **Test** button to check if the website associates with suspicious activities that could pose a security threat to users or their computers.
Category list	Select the categories of packets that come from the Internet and are known to pose a security threat to users or their computers.
Block list	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Add the IPv4 addresses that the Nebula Device will block the incoming packets.
Allow list	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Add the IPv4 addresses that the Nebula Device will allow the incoming packets.
External block list	
Enabled	Select this checkbox to have the Nebula Device block the incoming packets that come from the listed addresses in the block list file on the server.
Name	Enter the identifying name for the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
External DB	Enter the file name, path and IP address of the server containing the block list file. For example, http://172.16.107.20/blacklist-files/myip-ebl.txt
Description	Enter a description of the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Schedule update	New IP reputation signatures can be downloaded to the Nebula Device periodically if you have subscribed for the IP reputation signatures service.You need to create an account at Zyxel, register your Nebula Device and then subscribe for IP reputation service in order to be able to download new signatures from Zyxel. Select **Daily** to set the time of the day, or **Weekly** to set the day of the week and the time of the day. Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.
Anti-Malware	
Enabled	Select **On** to turn on the rule. Otherwise, select **Off** to turn off the rule.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed above.
Scan Mode	

Table 127 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Express Mode	In this mode you can define which types of files are scanned using the File Type For Scan fields. The Nebula Device then scans files by sending each file's hash value to a cloud database using cloud query. This is the fastest scan mode.
Stream Mode	In this mode the Nebula Device scans all files for viruses using its anti-malware signatures to detect known virus pattens. This is the deepest scan mode.
Hybrid Mode (for ATP devices only)	In this mode you can define which types of files are scanned using the File Type For Scan fields. The Nebula Device then scans files by sending each file's hash value to a cloud database using cloud query. It also scans files using anti-malware signatures, and Threat Intelligence Machine Learning. This mode combines Express Mode and Stream Mode to offer a balance of speed and security.
File decompression (ZIP and RAR)	Select this checkbox to have the Nebula Device scan a compressed file (the file does not need to have a "zip" or "rar" file extension). The Nebula Device first decompresses the file and then scans the contents for malware. Note: The Nebula Device decompresses a compressed file once. The Nebula Device does NOT decompress any files within a compressed file.
Destroy compressed files that could not be decompressed	When you select this checkbox, the Nebula Device deletes compressed files that use password encryption. Select this checkbox to have the Nebula Device delete any compressed files that it cannot decompress. The Nebula Device cannot decompress password protected files or a file within another compressed file. There are also limits to the number of compressed files that the Nebula Device can concurrently decompress. Note: The Nebula Device's firmware package cannot go through the Nebula Device with this checkbox enabled. The Nebula Device classifies the firmware package as a file that cannot be decompressed and then deletes it. Clear this checkbox when you download a firmware package from the Zyxel website. It is okay to upload a firmware package to the Nebula Device with the checkbox selected.
Cloud Query	Select the Cloud Query supported file types for the Nebula Device to scan for viruses.
Block list	This field displays the file or encryption pattern of the entry. Enter an MD5 hash or file pattern that would cause the Nebula Device to log and modify this file. File patterns: •Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. •A question mark (?) lets a single character in the file name vary. For example, use "a?.zip" (without the quotation marks) to specify aa.zip, ab.zip and so on. •Wildcards (*) let multiple files match the pattern. For example, use "*a.zip" (without the quotation marks) to specify any file that ends with "a.zip". A file named "testa.zip would match. There could be any number (of any type) of characters in front of the "a.zip" at the end and the file name would still match. A file named "test.zipa" for example would not match. •A * in the middle of a pattern has the Nebula Device check the beginning and end of the file name and ignore the middle. For example, with "abc*.zip", any file starting with "abc" and ending in ".zip" matches, no matter how many characters are in between. •The whole file name has to match if you do not use a question mark or asterisk. •If you do not use a wildcard, the Security Firewall checks up to the first 80 characters of a file name.

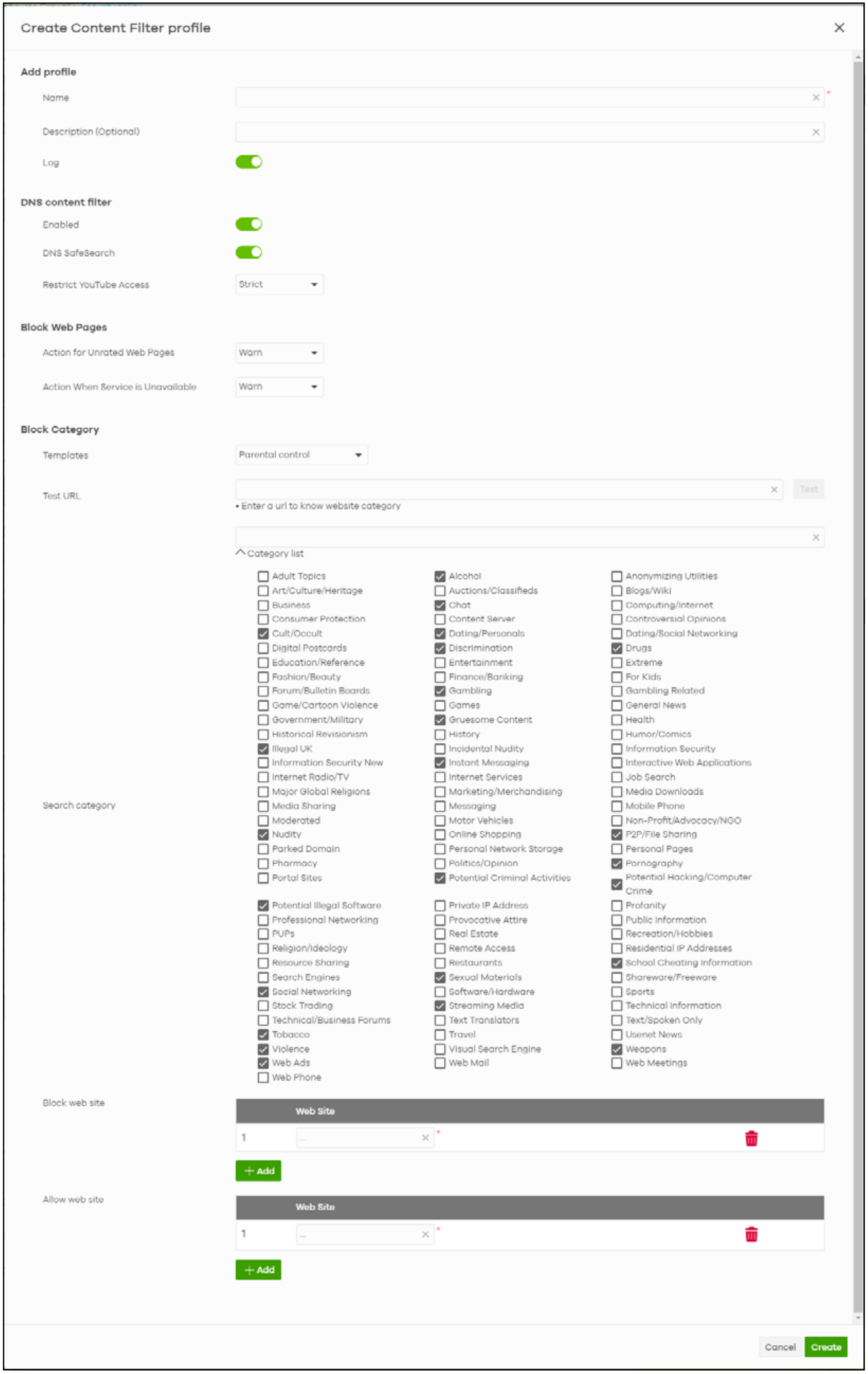
Table 127 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Allow list	Enter the file or encryption pattern for this entry. Enter an MD5 hash or file pattern to identify the names of files that the Nebula Device should not scan for viruses. File patterns: •Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. •A question mark (?) lets a single character in the file name vary. For example, use "a?.zip" (without the quotation marks) to specify aa.zip, ab.zip and so on. •Wildcards (*) let multiple files match the pattern. For example, use "*a.zip" (without the quotation marks) to specify any file that ends with "a.zip". A file named "testa.zip would match. There could be any number (of any type) of characters in front of the "a.zip" at the end and the file name would still match. A file named "test.zipa" for example would not match. •A * in the middle of a pattern has the Nebula Device check the beginning and end of the file name and ignore the middle. For example, with "abc*.zip", any file starting with "abc" and ending in ".zip" matches, no matter how many characters are in between. •The whole file name has to match if you do not use a question mark or asterisk. •If you do not use a wildcard, the Nebula Device checks up to the first 80 characters of a file name.
Sandboxing	Sandboxing provides a safe environment to separate running programs from your network and host devices. Unknown or untrusted programs/codes are uploaded to the Defend Center and executed within an isolated virtual machine (VM) to monitor and analyze the zero-day malware and advanced persistent threats (APTs) that may evade the Nebula Device's detection, such as anti-malware. Results of cloud sandboxing are sent from the server to the Nebula Device.
Enabled	Select this option to turn on sandboxing on the Nebula Device
Log	Enable this option to allow the Security Firewall to create a log when a suspicious file is detected.
Policy	Specify whether the Nebula Device deletes (**Destroy**) or forwards (**Allow**) malicious files. Malicious files are files given a high score for malware characteristics by the Defend Center.
Inspect selected downloaded files	Select this option to have the Nebula Device hold the downloaded file for up to 2 seconds if the downloaded file has never been inspected before. The Nebula Device will wait for the Defend Center's result and forward the file in 2 seconds. Sandbox detection may take longer than 2 seconds, so infected files could still possibly be forwarded to the user. Note: The Nebula Device only checks the file types you selected for sandbox inspection. The scan result will be removed from the Nebula Device cache after the Nebula Device restarts.
File submission options	Specify the type of files to be sent for sandbox inspection.
Intrusion Prevention System (IPS)	
Detection	Select **On** to enable Detection.
Prevention	Select **On** to enable Prevention.

Create a Content Filter Profile

Click the **Add** button in the **Content Filter** section of the **Site-wide** > **Configure** > **Firewall** > **Security service** screen to access this screen.

Figure 186 Site-wide > Configure > Firewall > Security service > Content Filter: Add/Edit



Create Content Filter profile ✕

Add profile

Name ✕ *

Description (Optional) ✕

Log

DNS content filter

Enabled

DNS SafeSearch

Restrict YouTube Access: Strict

Block Web Pages

Action for Unrated Web Pages: Warn

Action When Service is Unavailable: Warn

Block Category

Templates: Parental control

Test URL ✕ Test

• Enter a url to know website category

Search category

Category list

- ☐ Adult Topics
- ☐ Art/Culture/Heritage
- ☐ Business
- ☐ Consumer Protection
- ☑ Cult/Occult
- ☐ Digital Postcards
- ☐ Education/Reference
- ☐ Fashion/Beauty
- ☐ Forum/Bulletin Boards
- ☐ Game/Cartoon Violence
- ☐ Government/Military
- ☐ Historical Revisionism
- ☑ Illegal UK
- ☐ Information Security New
- ☐ Internet Radio/TV
- ☐ Major Global Religions
- ☐ Media Sharing
- ☐ Moderated
- ☑ Nudity
- ☐ Parked Domain
- ☐ Pharmacy
- ☐ Portal Sites
- ☑ Potential Illegal Software
- ☐ Professional Networking
- ☐ PUPs
- ☐ Religion/Ideology
- ☐ Resource Sharing
- ☐ Search Engines
- ☑ Social Networking
- ☐ Stock Trading
- ☐ Technical/Business Forums
- ☑ Tobacco
- ☑ Violence
- ☑ Web Ads
- ☐ Web Phone
- ☑ Alcohol
- ☐ Auctions/Classifieds
- ☑ Chat
- ☐ Content Server
- ☑ Dating/Personals
- ☑ Discrimination
- ☐ Entertainment
- ☐ Finance/Banking
- ☑ Gambling
- ☐ Games
- ☑ Gruesome Content
- ☐ History
- ☐ Incidental Nudity
- ☑ Instant Messaging
- ☐ Internet Services
- ☐ Marketing/Merchandising
- ☐ Messaging
- ☐ Motor Vehicles
- ☐ Online Shopping
- ☐ Personal Network Storage
- ☐ Politics/Opinion
- ☑ Potential Criminal Activities
- ☐ Private IP Address
- ☐ Provocative Attire
- ☐ Real Estate
- ☐ Remote Access
- ☐ Restaurants
- ☑ Sexual Materials
- ☐ Software/Hardware
- ☑ Streaming Media
- ☐ Text Translators
- ☐ Travel
- ☐ Visual Search Engine
- ☐ Web Mail
- ☐ Anonymizing Utilities
- ☐ Blogs/Wiki
- ☐ Computing/Internet
- ☐ Controversial Opinions
- ☐ Dating/Social Networking
- ☑ Drugs
- ☐ Extreme
- ☐ For Kids
- ☐ Gambling Related
- ☐ General News
- ☐ Health
- ☐ Humor/Comics
- ☐ Information Security
- ☐ Interactive Web Applications
- ☐ Job Search
- ☐ Media Downloads
- ☐ Mobile Phone
- ☐ Non-Profit/Advocacy/NGO
- ☑ P2P/File Sharing
- ☐ Personal Pages
- ☑ Pornography
- ☑ Potential Hacking/Computer Crime
- ☐ Profanity
- ☐ Public Information
- ☐ Recreation/Hobbies
- ☐ Residential IP Addresses
- ☑ School Cheating Information
- ☐ Shareware/Freeware
- ☐ Sports
- ☐ Technical Information
- ☐ Text/Spoken Only
- ☐ Usenet News
- ☑ Weapons
- ☐ Web Meetings

Block web site

	Web Site
1	... ✕ *

+ Add

Allow web site

	Web Site
1	... ✕ *

+ Add

Cancel Create

The following table describes the labels in this screen.

Table 128 Site-wide > Configure > Firewall > Security service > Content Filter: Add/Edit

LABEL	DESCRIPTION
Add profile	
Name	Enter a name for this profile for identification purposes. Use up to 127 characters (0 – 9 a – z). The casing does not matter.
Description (Optional)	Enter a description for this profile.
Log	Select whether to have the Nebula Device generate a log (**ON**) or not (**OFF**) by default when traffic matches an application signature in this category.
DNS content filter	Select this option to turn on DNS filtering on the Nebula Device. DNS filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs). The Nebula Device DNS content filter will either drop the DNS query or reply to the user with a fake DNS response.
DNS SafeSearch	Select whether to enable content filter on the YouTube search engine. This allows you to avoid explicit and inappropriate results by selecting **Strict**/**Moderate** in the **Restrict YouTube Access**.
Block Web Pages	
Action for Unrated Web Pages	Select **Pass** to allow users to access web pages that the external web filtering service has not categorized. Select **Block** to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filter blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. Select **Warn** to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.
Action when service is unavailable	Select **Pass** to allow users to access any requested web page if the external content filter database is unavailable. Select **Block** to block access to any requested web page if the external content filter database is unavailable. Select **Warn** to display a warning message before allowing users to access any requested web page if the external content filter database is unavailable. The following are possible causes for the external content filter server not being available: •There is no response from the external content filter server within the time period specified in the Content Filter Server Unavailable Timeout field. •The Nebula Device is not able to resolve the domain name of the external content filter database. •There is an error response from the external content filter database. This can be caused by an expired content filter registration (External content filter's license key is invalid").
Block Category The Nebula Device prevents users from accessing web pages that match the categories that you select below. When external database content filter blocks access to a web page, it displays the denied access message that you configured in the **Denied access message** field along with the category of the blocked web page.	

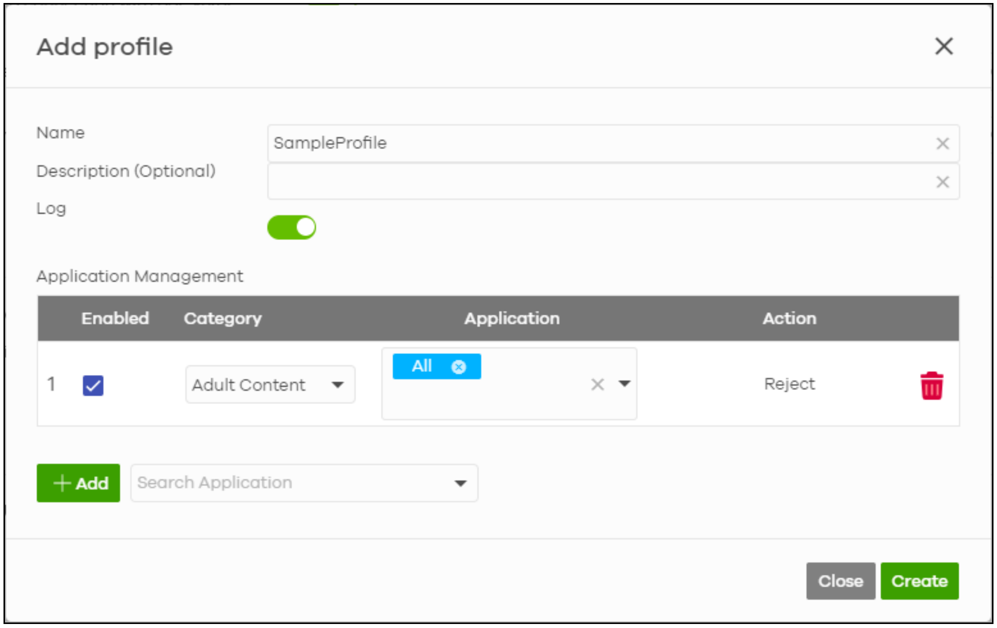
Table 128   Site-wide > Configure > Firewall > Security service > Content Filter: Add/Edit (continued)

LABEL	DESCRIPTION
Templates	Web pages are classified into a category based on their content. You can choose a pre-defined template that has already selected certain categories. Alternatively, choose **Custom** and manually select categories in this section to control access to specific types of Internet content.
Test URL	You can check which category a web page belongs to. Enter a web site URL in the text box, then click **Test**. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. Content Filter can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. **Test URL** displays both results in the test.
Search Category	Specify your desired filter criteria to filter the list of categories.
Category List	Click to display or hide the category list. These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
Block web site	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
Add	Click this button to add a new entry.
Allow web site	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
Add	Click this button to add a new entry.
🗑	Click this icon to remove the entry.
Cancel	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

Add Application Patrol Profile

Click the **Add** button in the **Application Patrol** section of the **Site-wide** > **Configure** > **Firewall** > **Security service** screen to access this screen.

Figure 187 Site-wide > Configure > Firewall > Security service > Application Patrol: Add/Edit



Add profile

Name: SampleProfile

Description (Optional):

Log: ●

Application Management

	Enabled	Category	Application	Action	
1	☑	Adult Content	All	Reject	🗑

The following table describes the labels in this screen.

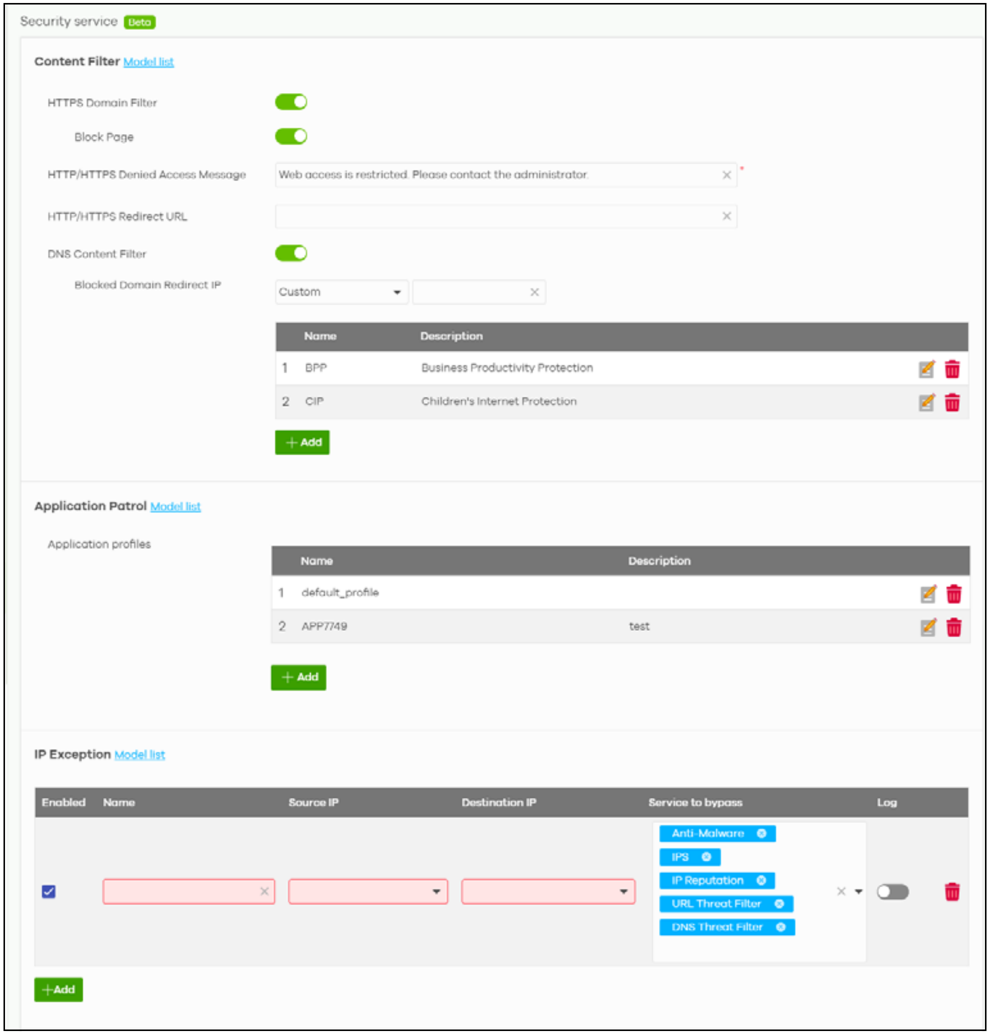
Table 129 Site-wide > Configure > Firewall > Security service > Application Patrol: Add/Edit

LABEL	DESCRIPTION
Add profile	
Name	Enter the name of the application patrol profile rule; use of up to 32 upper/ lowercase letters. Space not allowed.
Description (Optional)	Enter an optional description of the application patrol profile rule; use up to 255 keyboard characters.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed above.
Application Management	
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Category	Select an application category.
Application	Select **All** or select an application within the category to apply the policy.
Action	Displays the default action for the applications selected in this category. **Reject** – the Nebula Device drops packets that matches these application signatures and sends notification to clients.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new application category and set actions for specific applications within the category.
Search Application	Enter a name to search for relevant applications and click **Add** to create an entry.
Close	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

8.3.9.2 For Security Firewall (USG FLEX H Series)

This section describes the Security Service feature for USG FLEX H Series only. Click **Site-wide** > **Configure** > **Firewall** > **Security service** to access this screen.

Figure 188 Site-wide > Configure > Firewall > Security service



Security service

Content Filter Model list

HTTPS Domain Filter

Block Page

HTTP/HTTPS Denied Access Message: Web access is restricted. Please contact the administrator.

HTTP/HTTPS Redirect URL:

DNS Content Filter

Blocked Domain Redirect IP: Custom

	Name	Description
1	BPP	Business Productivity Protection
2	CIP	Children's Internet Protection

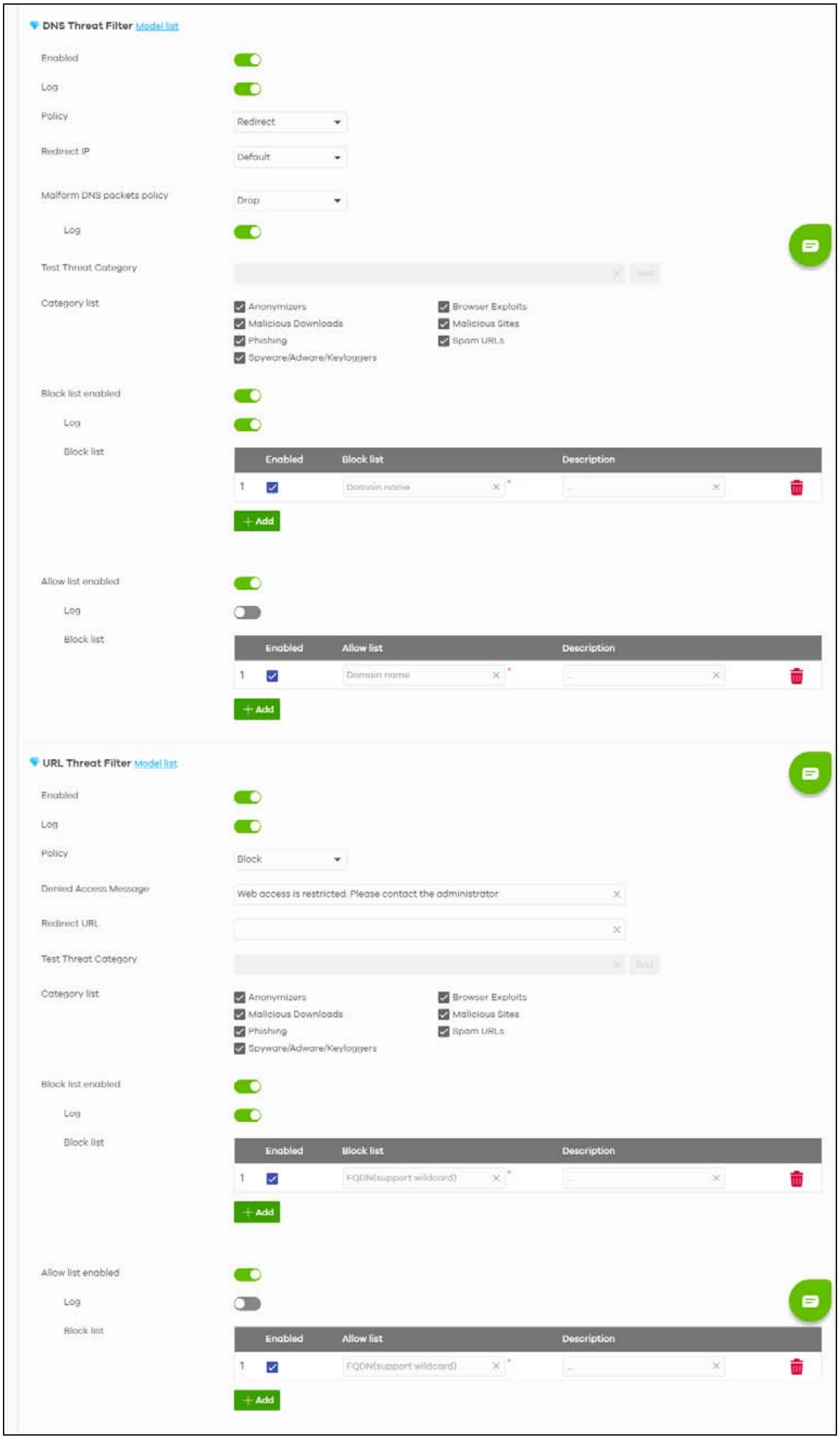
Application Patrol Model list

Application profiles

	Name	Description
1	default_profile	
2	APP7749	test

IP Exception Model list

Enabled	Name	Source IP	Destination IP	Service to bypass	Log
☑				Anti-Malware IPS IP Reputation URL Threat Filter DNS Threat Filter	



DNS Threat Filter Model list

Enabled: ●

Log: ●

Policy: Redirect ▾

Redirect IP: Default ▾

Malform DNS packets policy: Drop ▾

Log: ●

Test Threat Category: × Test

Category list:

☑ Anonymizers ☑ Browser Exploits
☑ Malicious Downloads ☑ Malicious Sites
☑ Phishing ☑ Spam URLs
☑ Spyware/Adware/Keyloggers

Block list enabled: ●

Log: ●

Block list

	Enabled	Block list	Description	
1	☑	Domain name × *	... ×	🗑

+ Add

Allow list enabled: ●

Log: ○

Block list

	Enabled	Allow list	Description	
1	☑	Domain name × *	... ×	🗑

+ Add

URL Threat Filter Model list

Enabled: ●

Log: ●

Policy: Block ▾

Denied Access Message: Web access is restricted. Please contact the administrator ×

Redirect URL: ×

Test Threat Category: × Test

Category list:

☑ Anonymizers ☑ Browser Exploits
☑ Malicious Downloads ☑ Malicious Sites
☑ Phishing ☑ Spam URLs
☑ Spyware/Adware/Keyloggers

Block list enabled: ●

Log: ●

Block list

	Enabled	Block list	Description	
1	☑	FQDN(support wildcard) × *	... ×	🗑

+ Add

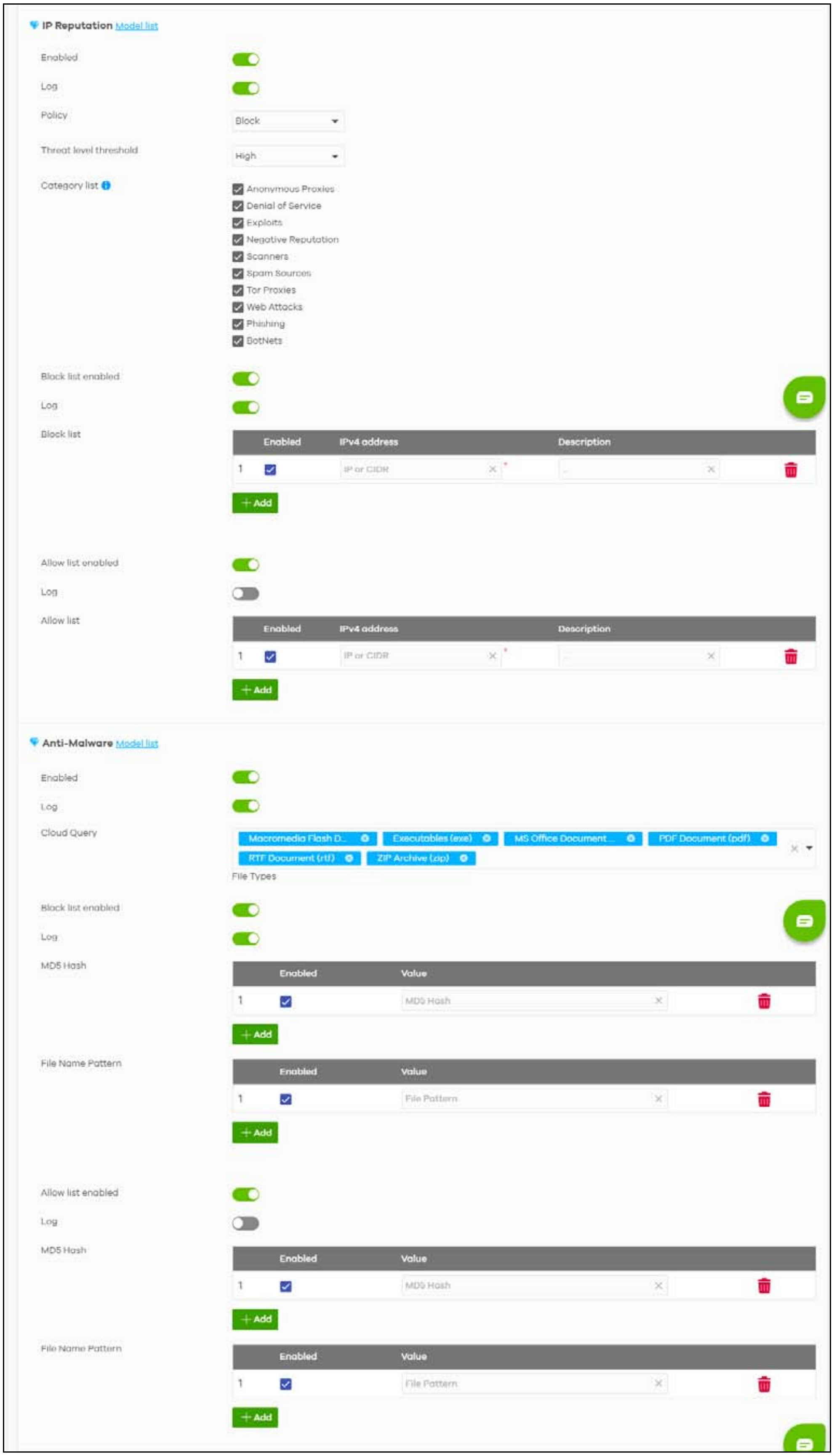
Allow list enabled: ●

Log: ○

Block list

	Enabled	Allow list	Description	
1	☑	FQDN(support wildcard) × *	... ×	🗑

+ Add



IP Reputation Model list

Enabled ●

Log ●

Policy: Block

Threat level threshold: High

Category list

- ☑ Anonymous Proxies
- ☑ Denial of Service
- ☑ Exploits
- ☑ Negative Reputation
- ☑ Scanners
- ☑ Spam Sources
- ☑ Tor Proxies
- ☑ Web Attacks
- ☑ Phishing
- ☑ BotNets

Block list enabled ●

Log ●

Block list

	Enabled	IPv4 address	Description	
1	☑	IP or CIDR		

+ Add

Allow list enabled ●

Log ○

Allow list

	Enabled	IPv4 address	Description	
1	☑	IP or CIDR		

+ Add

Anti-Malware Model list

Enabled ●

Log ●

Cloud Query: Macromedia Flash D... · Executables (exe) · MS Office Document... · PDF Document (pdf) · RTF Document (rtf) · ZIP Archive (zip)

File Types

Block list enabled ●

Log ●

MD5 Hash

	Enabled	Value	
1	☑	MD5 Hash	

+ Add

File Name Pattern

	Enabled	Value	
1	☑	File Pattern	

+ Add

Allow list enabled ●

Log ○

MD5 Hash

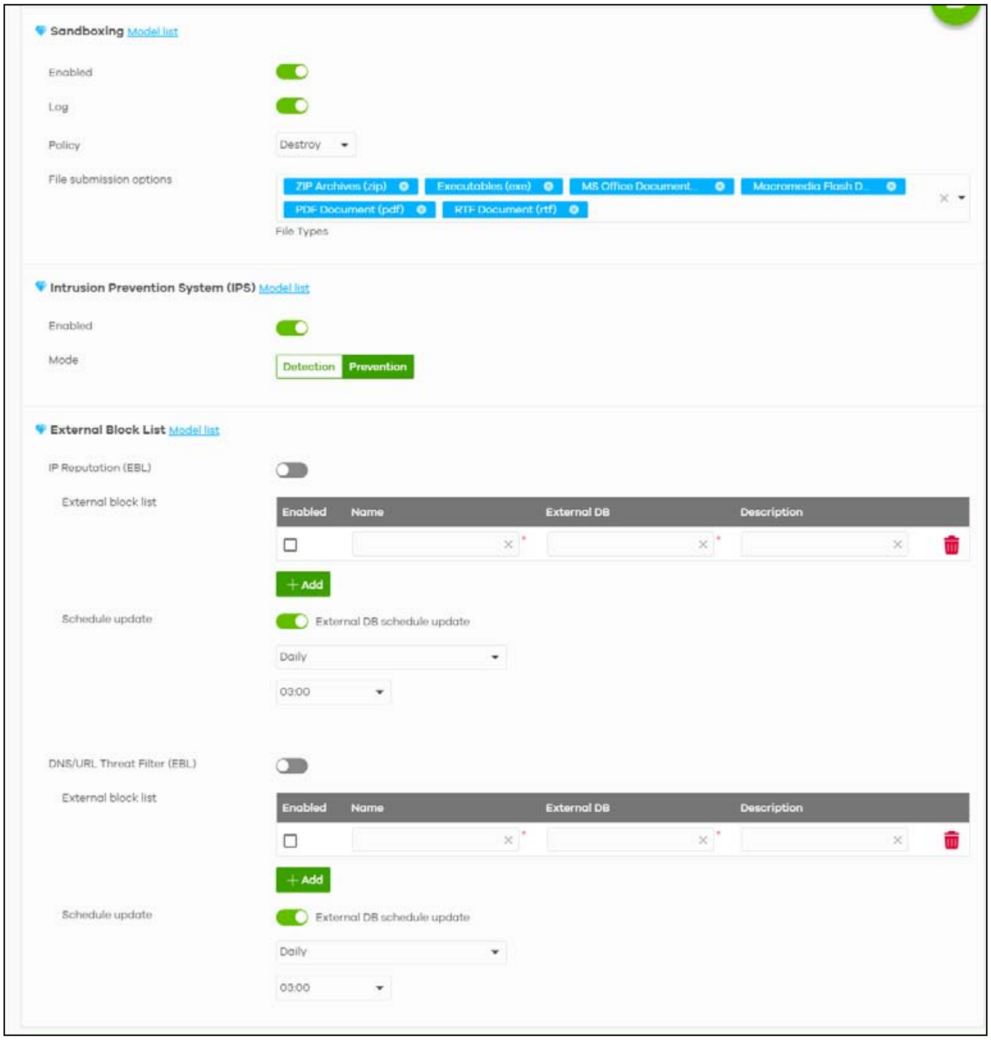
	Enabled	Value	
1	☑	MD5 Hash	

+ Add

File Name Pattern

	Enabled	Value	
1	☑	File Pattern	

+ Add



Sandboxing Model list

Enabled: On

Log: On

Policy: Destroy

File submission options: ZIP Archives (zip), Executables (exe), MS Office Document..., Macromedia Flash D..., PDF Document (pdf), RTF Document (rtf)

File Types

Intrusion Prevention System (IPS) Model list

Enabled: On

Mode: Detection [✓ Prevention]

External Block List Model list

IP Reputation (EBL): Off

External block list

Enabled	Name	External DB	Description
□			

+ Add

Schedule update: External DB schedule update (On)

Daily

03:00

DNS/URL Threat Filter (EBL): Off

External block list

Enabled	Name	External DB	Description
□			

+ Add

Schedule update: External DB schedule update (On)

Daily

03:00

The following table describes the labels in this screen.

Table 130   Site-wide > Configure > Firewall > Security service

LABEL	DESCRIPTION
Content Filter	
HTTPS Domain Filter	Select On to have the Nebula Device filter HTTPS domains by querying a category by domain name (www.google.com).
Block Page	Select On to have the Nebula Device block HTTPS web pages using SSL V3 or a previous version.
HTTP/HTTPS Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0–9 a–z A–Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the **HTTP/HTTPS Redirect URL** field. In this case if the content filter blocks access to a web page, the Nebula Device just opens the web page you specified without showing a denied access message.
HTTP/HTTPS Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0–9 a–z A–Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.

Table 130 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
DNS Content Filter	Select On to have the Nebula Device inspect DNS queries made by users on your network.
Blocked Domain Redirect IP	This is the URL of the web page to which you want to send users when their web access is blocked by DNS content filtering. The web page you specify here opens in a new frame below the denied access message. Select default to send users to the default web page when their web access is blocked by DNS content filter. Select custom-defined to send users to the web page you set when their web access is blocked by DNS content filter. Use "http://" followed by up to 255 characters (0-9 a-z A-Z;/ ?:@&=+$\.-_!~*'()%) in quotes. For example, http://192.168.2.17/blocked access.
Name	This shows the name of this content filter profile.
Description	This shows the description for this profile.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this to create a content filter profile. See Section 8.3.8.2 on page 521 for more information.
Application Patrol Application profiles	
Name	This shows the name of this Application Patrol profile.
Description	This shows the description for this profile.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this to create an Application Patrol profile. See Section on page 553 for more information.
IP Exception	
Enabled	Select the checkbox to enable IP Exception. IP addresses listed here are not checked by security services.
Name	This shows the name of this IP Exception profile.
Source IP	This field displays the source IP address of incoming traffic. It displays any if there is no restriction on the source IP address.
Destination IP	This field displays the destination IP address of incoming traffic. It displays any if there is no restriction on the destination IP address.
Service to bypass	This field displays which services will not inspect matched packets.
Log	Select On to allow the Nebula Device to generate a log when the incoming traffic is in the exception list.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.

Table 130 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
DNS Threat Filter	DNS filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs). If a user attempts to connect to a suspect site, where the DNS query packet contains an FQDN with a bad reputation, then a DNS query is sent from the user's computer and detected by the DNS Filter. The Nebula Device DNS filter will either drop the DNS query or reply to the user with a fake DNS response using the default dnsft.cloud.zyxel.com IP address (where the user will see a "Web Page Blocked!" page) or a custom IP address. When you enable the URL Threat filtering service, your Nebula Device downloads signature files that contain known URL Threat domain names and IP addresses. The Nebula Device will also access an external database, Cloud Query, that has millions of web sites categorized based on content. You can have the Nebula Device allow, block, warn and/or log access to web sites or hosts based on these signatures and categories.
Enabled	Select On to turn on the rule. Otherwise, select Off to turn off the rule.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
Policy	Select **Pass** to have the Nebula Device allow the DNS query packet and not reply with a DNS reply packet containing a default or custom-defined IP address. Select **Redirect** to have the Nebula Device reply with a DNS reply packet containing a default or custom-defined IP address.
Redirect IP	Enter the IP address to have the Nebula Device reply with a DNS reply packet containing a default or custom-defined IP address when a DNS query packet contains an FQDN with a bad reputation. The default IP is the dnsft.cloud.zyxel.com IP address. If you select a custom-defined IP, then enter a valid IPv4 address in the text box.
Malform DNS packets policy	Set what action the Nebula Device takes when there is an abnormal DNS query packet. A DNS packet is defined as malformed when: • The number of entries in the question count field in the DNS header is 0 • An error occurs when parsing the domain name in the question field • The length of the domain name exceeds 255 characters. **pass**: Select this action to have the Nebula Device allow the DNS query packet through the Nebula Device. **drop**: Select this action to have the Nebula Device discard the abnormal DNS query packet.
Log	Select whether to have the Nebula Device generate a log when there is an abnormal DNS query packet.
Test Threat Category	Enter a URL using http://domain or https://domain and click the **Test** button to check if the domain belongs to a URL threat category.
Category List	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
Block list enabled	Select On to have the Nebula Device block the incoming packets that come from the listed addresses in the block list.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
Block list Enabled	Select On to turn on an entry.

Table 130 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Block list	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
Description	Enter a description of the block entry. You can use 1 to 512 single-byte characters.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Allow list enabled	Select On to have the Nebula Device allow the incoming packets that come from the listed addresses in the allow list.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
Allow list Enabled	Select On to turn on an entry.
Allow list	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
Description	Enter a description of the allow entry. You can use 1 to 512 single-byte characters.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
URL Threat Filter Enabled	Select On to turn on the rule. Otherwise, select Off to turn off the rule.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
Policy	Select **Pass** to allow users to access web pages that the external web filtering service has not categorized. Select **Block** to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filter blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page.
Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0–9 a–z A–Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the **Redirect URL** field. In this case if the content filter blocks access to a web page, the Nebula Device just opens the web page you specified without showing a denied access message.

Table 130 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use “http://” or “https://” followed by up to 262 characters (0–9 a–z A–Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Test Threat Category	Enter a URL using http://domain or https://domain and click the **Test** button to check if the domain belongs to a URL threat category.
Category List	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
Block list enabled	Select On to have the Nebula Device block the incoming packets that come from the listed addresses in the block list.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
Block list Enabled	Select On to turn on an entry.
Block list	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All sub-domains are also blocked. For example, entering “bad-site.com” also blocks “www.badsite.com”, “partner.bad-site.com”, “press.bad-site.com”, and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
Description	Enter a description of the block entry. You can use 1 to 512 single-byte characters.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Allow list enabled	Select On to have the Nebula Device allow the incoming packets that come from the listed addresses in the allow list.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
Allow list Enabled	Select On to turn on an entry.
Allow list	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All sub-domains are allowed. For example, entering “zyxel.com” also allows “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
IP Reputation	
Enabled	Select this option to turn on IP blocking on the Nebula Device.
Log	Select this option to create a log on the Nebula Device when the packet comes from an IPv4 address with bad reputation.
Policy	Select **Pass** to have the Nebula Device allow the packet to go through. Select **Block** to have the Nebula Device deny the packets and send a TCP RST to both the sender and receiver when a packet comes from an IPv4 address with bad reputation.

Table 130 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Threat level threshold	Select the threshold threat level to which the Nebula Device will take action (**High**, **Medium and above**, **Low and above**). The threat level is determined by the IP reputation engine. It grades IPv4 addresses. • **High**: an IPv4 address that scores 0 to 20 points. • **Medium and above**: an IPv4 address that scores 0 to 60 points. • **Low and above**: an IPv4 address that scores 0 to 80 points. For example, a score of "10" will cause the Nebula Device to take action whether you set the **Threat level threshold** at **High**, **Medium and above**, or **Low and above**. But a score of "61" will not cause the Nebula Device to take any action if you set the **Threat level threshold** at **Medium and above**.
Category list	Select the categories of packets that come from the Internet and are known to pose a security threat to users or their computers.
Block list enabled	Select On to have the Nebula Device block the incoming packets that come from the listed addresses in the block list.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
Block list Enabled	Select On to turn on an entry.
IPv4 address	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Add the IPv4 addresses that the Nebula Device will block the incoming packets.
Description	Enter a description of the block entry. You can use 1 to 512 single-byte characters.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Allow list enabled	Select On to have the Nebula Device allow the incoming packets that come from the listed addresses in the allow list.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
Allow list Enabled	Select On to turn on an entry.
IPv4 address	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Add the IPv4 addresses that the Nebula Device will allow the incoming packets.
Description	Enter a description of the allow entry. You can use 1 to 512 single-byte characters.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Anti-Malware	
Enabled	Select **On** to turn on the rule. Otherwise, select **Off** to turn off the rule.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
Cloud Query	Select the Cloud Query supported file types for the Nebula Device to scan for viruses.
Block list enabled	Select On to have the Nebula Device block the incoming packets that come from the listed addresses in the block list.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.

Table 130   Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
MD5 Hash Enabled	Select On to turn on an entry.
Value	This field displays the encryption pattern of the entry. Enter an MD5 hash ([a-zA-Z0-9]* up to 32 characters maximum) that would cause the Nebula Device to log and modify this file.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
File Name Pattern Enabled	Select On to turn on an entry.
Value	This field displays the file pattern of the entry. Enter a file pattern ([a-zA-Z0-9.?*_-] up to 80 characters maximum) that would cause the Nebula Device to log and modify this file. File patterns: •Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. •A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on. •Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match. •A * in the middle of a pattern has the Nebula Device check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between. •The whole file name has to match if you do not use a question mark or asterisk. •If you do not use a wildcard, the Security Firewall checks up to the first 80 characters of a file name.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Allow list enabled	Select On to have the Nebula Device allow the incoming packets that come from the listed addresses in the allow list.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed.
MD5 Hash Enabled	Select On to turn on an entry.
Value	Enter the encryption pattern for this entry. Enter an MD5 hash ([a-zA-Z0-9]* up to 32 characters maximum) to identify the names of files that the Nebula Device should not scan for viruses.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
File Name Pattern Enabled	Select On to turn on an entry.

Table 130   Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Value	Enter the file pattern for this entry. Enter a file pattern ([a-zA-Z0-9.?*_-] up to 80 characters maximum) to identify the names of files that the Nebula Device should not scan for viruses. File patterns: •Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. •A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on. •Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match. •A * in the middle of a pattern has the Nebula Device check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between. •The whole file name has to match if you do not use a question mark or asterisk. •If you do not use a wildcard, the Nebula Device checks up to the first 80 characters of a file name.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Sandboxing	Sandboxing provides a safe environment to separate running programs from your network and host devices. Unknown or untrusted programs/codes are uploaded to the Defend Center and executed within an isolated virtual machine (VM) to monitor and analyze the zero-day malware and advanced persistent threats (APTs) that may evade the Nebula Device’s detection, such as anti-malware. Results of cloud sandboxing are sent from the server to the Nebula Device.
Enabled	Select this option to turn on sandboxing on the Nebula Device
Log	Enable this option to allow the Security Firewall to create a log when a suspicious file is detected.
Policy	Specify whether the Nebula Device deletes (**Destroy**) or forwards (**Allow**) malicious files. Malicious files are files given a high score for malware characteristics by the Defend Center.
File submission options	Specify the type of files to be sent for sandbox inspection.
Intrusion Prevention System (IPS)	
Enabled	Select **On** to enable Detection or Prevention.
Mode	Select **Prevention** to have the Nebula Device perform a user-specified action when a stream of data matches a malicious signature. Select **Detection** to have the Nebula Device only create a log message when a stream of data matches a malicious signature.
External block list	
IP Reputation (EBL)	Select this to have the Nebula Device block packets that come from the listed addresses in the block list file on the server.
External block list	The Nebula Device uses black list entries stored in a file on a web server that supports HTTP or HTTPS. The Nebula Device blocks incoming and outgoing packets from the black list entries in this file.
Enabled	Select this to have the Nebula Device block the incoming packets that come from the listed addresses in the block list file on the server.

Table 130   Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Name	Enter an identifying name for the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
External DB	Enter the exact file name, path and IP address of the server containing the block list file. The file type must be 'txt'. For example, http://172.16.107.20/blacklist-files/myip-ebl.txt The server must be reachable from the Nebula Device.
Description	Enter a description of the block list file. You can use 1 to 512 single-byte characters.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry, up to 4 maximum.
Schedule update	The signatures for IP Reputation are continually updated as new malware evolves. New signatures can be downloaded to the Nebula Device periodically if you have subscribed for the IP Reputation signatures service. You need to create an account at myZyxel, register your Nebula Device and then subscribe for IP Reputation filter service in order to be able to download new signatures from myZyxel. Enable **External DB schedule update** to have the Nebula Device automatically check for new signatures regularly at the time and day specified. Select **Daily** to set the time of the day, or **Weekly** to set the day of the week and the time of the day. Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.
DNS/URL Threat Filter (EBL)	Select this to have the Nebula Device block packets that come from the listed addresses in the block list file on the server.
External block list	The Nebula Device uses black list entries stored in a file on a web server that supports HTTP or HTTPS. The Nebula Device blocks incoming and outgoing packets from the black list entries in this file.
Enabled	Select this to have the Nebula Device block the incoming packets that come from the listed addresses in the block list file on the server.
Name	Enter an identifying name for the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
External DB	Enter the exact file name, path and IP address of the server containing the block list file. The file type must be 'txt'. For example, http://172.16.107.20/blacklist-files/myip-ebl.txt The server must be reachable from the Nebula Device.
Description	Enter a description of the block list file. You can use 1 to 512 single-byte characters.
🗑	Click this icon to remove the entry.

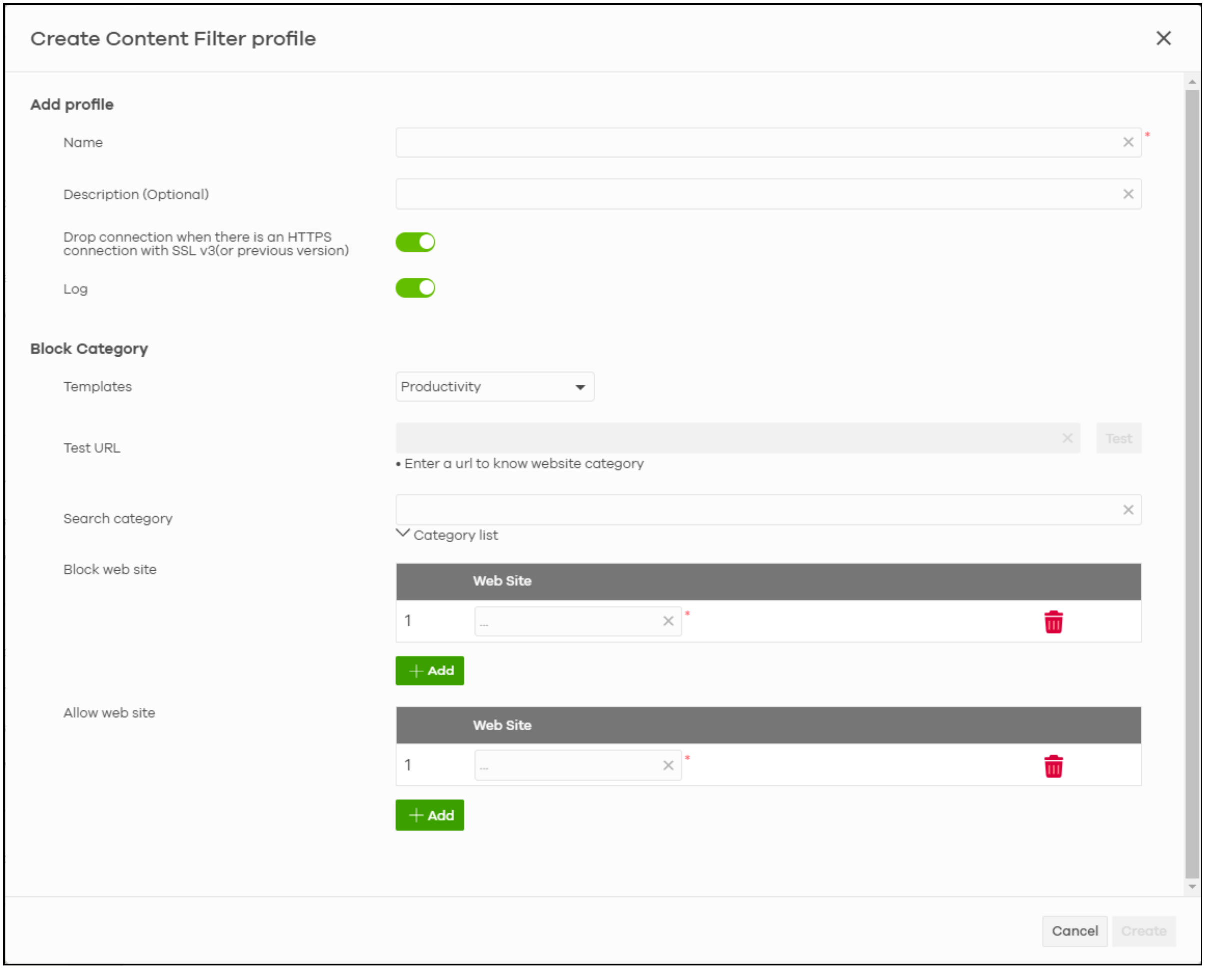
Table 130 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
Schedule update	The signatures for DNS Filter and URL Threat Filter are the same. These signatures are continually updated as new malware evolves. New signatures can be downloaded to the Nebula Device periodically if you have subscribed for the URL Threat filter signatures service. You need to create an account at myZyxel, register your Nebula Device and then subscribe for URL Threat filter service in order to be able to download new signatures from myZyxel. Enable **External DB schedule update** to have the Nebula Device automatically check for new signatures regularly at the time and day specified. Select **Daily** to set the time of the day, or **Weekly** to set the day of the week and the time of the day. Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.

Create a Content Filter Profile

Click the **Add** button in the **Content Filter** section of the **Site-wide** > **Configure** > **Firewall** > **Security service** screen to access this screen.

Figure 189 Site-wide > Configure > Firewall > Security service > Content Filter: Add/Edit



Create Content Filter profile

Add profile

Name

Description (Optional)

Drop connection when there is an HTTPS connection with SSL v3(or previous version)

Log

Block Category

Templates: Productivity

Test URL

• Enter a url to know website category

Search category

Category list

Block web site

	Web Site
1	...

Allow web site

	Web Site
1	...

The following table describes the labels in this screen.

Table 131 Site-wide > Configure > Firewall > Security service > Content Filter: Add/Edit

LABEL	DESCRIPTION
Add profile	
Name	Enter a name for this profile for identification purposes. Use up to 127 characters (0 – 9 a – z). The casing does not matter.
Description (Optional)	Enter a description for this profile.
Drop connection when there is an HTTPS connection with SSL V3 (or previous version)	Select On to have the Nebula Device block HTTPS web pages using SSL V3 or a previous version.
Log	Select whether to have the Nebula Device generate a log (On) or not (Off) by default when traffic matches an application signature in this category.
Block Category The Nebula Device prevents users from accessing web pages that match the categories that you select below. When external database content filter blocks access to a web page, it displays the denied access message that you configured in the **Denied access message** field along with the category of the blocked web page.	

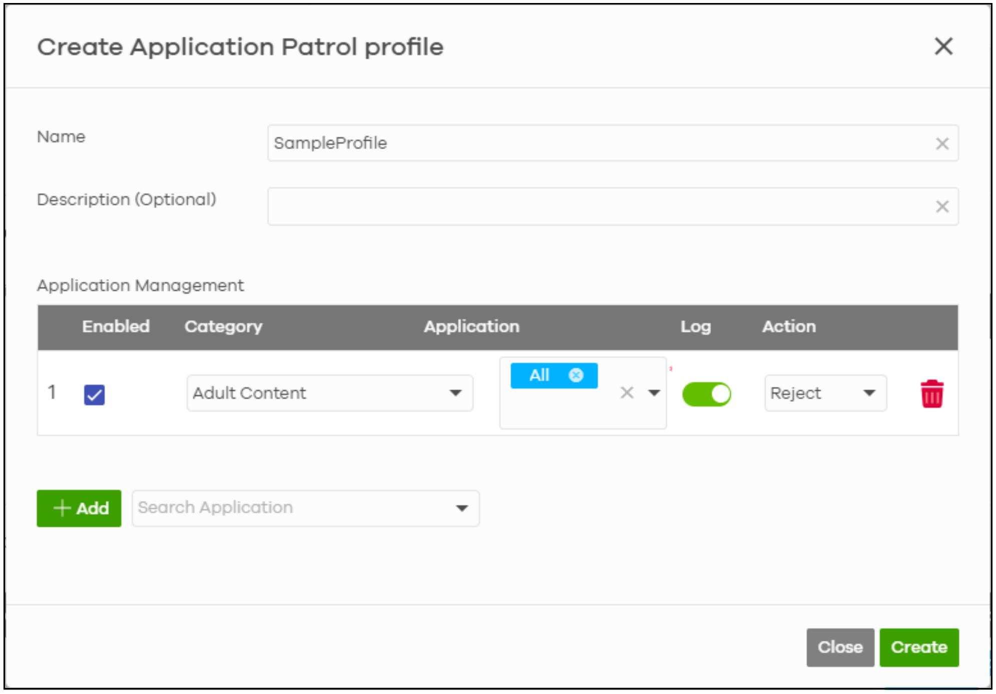
Table 131 Site-wide > Configure > Firewall > Security service > Content Filter: Add/Edit (continued)

LABEL	DESCRIPTION
Templates	Web pages are classified into a category based on their content. You can choose a pre-defined template that has already selected certain categories. Alternatively, choose **Custom** and manually select categories in this section to control access to specific types of Internet content.
Test URL	You can check which category a web page belongs to. Enter a web site URL in the text box, then click **Test**. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. Content Filter can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. **Test URL** displays both results in the test.
Search Category	Specify your desired filter criteria to filter the list of categories.
Category List	Click to display or hide the category list. These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
Block web site	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
Add	Click this button to add a new entry.
🗑	Click this icon to remove the entry.
Allow web site	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
Add	Click this button to add a new entry.
🗑	Click this icon to remove the entry.
Cancel	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

Add Application Patrol Profile

Click the **Add** button in the **Application Patrol** section of the **Site-wide** > **Configure** > **Firewall** > **Security service** screen to access this screen.

Figure 190 Site-wide > Configure > Firewall > Security service > Application Patrol: Add/Edit



Create Application Patrol profile

Name: SampleProfile

Description (Optional):

Application Management

	Enabled	Category	Application	Log	Action	
1	☑	Adult Content	All	●	Reject	🗑

The following table describes the labels in this screen.

Table 132 Site-wide > Configure > Firewall > Security service > Application Patrol: Add/Edit

LABEL	DESCRIPTION
Create Application Patrol profile	
Name	Enter the name of the application patrol profile rule; use of up to 32 upper/ lowercase letters. Space not allowed.
Description (Optional)	Enter an optional description of the application patrol profile rule; use up to 255 keyboard characters.
Application Management	
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Category	Select an application category.
Application	Select **All** or select an application within the category to apply the policy.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed above.
Action	Displays the default action for the applications selected in this category. **Forward** – the Nebula Device routes packets that matches these signatures. **Drop** – the Nebula Device silently drops packets that matches these signatures without sending a notification to both the sender and receiver. **Reject** – the Nebula Device drops packets that matches these application signatures and sends notification to clients.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new application category and set actions for specific applications within the category.
Search Application	Enter a name to search for relevant applications and click **Add** to create an entry.

Table 132 Site-wide > Configure > Firewall > Security service > Application Patrol: Add/Edit

LABEL	DESCRIPTION
Close	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

8.3.10 Object

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups. The sequence of members in the address group is not important.

Address objects and address groups are used in policy routes, security policies, application patrol, content filter, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filter.

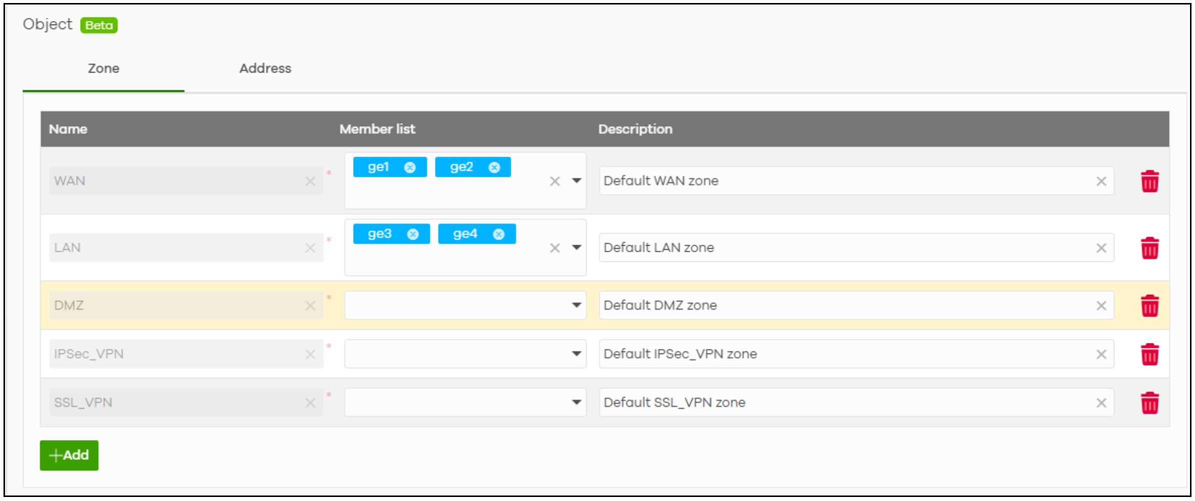
8.3.10.1 Zone Overview

Set up zones to configure network security and network policies in the Nebula Device. A zone is a group of interfaces and/or VPN tunnels. The Nebula Device uses zones instead of interfaces in many security and policy settings, such as Secure Policies rules, Security Service, and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

The **Zone** screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. Click **Site-wide** > **Configure** > **Firewall** > **Object** > **Zone** to access this screen.

Figure 191 Site-wide > Configure > Firewall > Object > Zone



Name	Member list	Description
WAN	ge1 ge2	Default WAN zone
LAN	ge3 ge4	Default LAN zone
DMZ		Default DMZ zone
IPSec_VPN		Default IPSec_VPN zone
SSL_VPN		Default SSL_VPN zone

The following table describes the labels in this screen.

Table 133 Site-wide > Configure > Firewall > Object > Zone

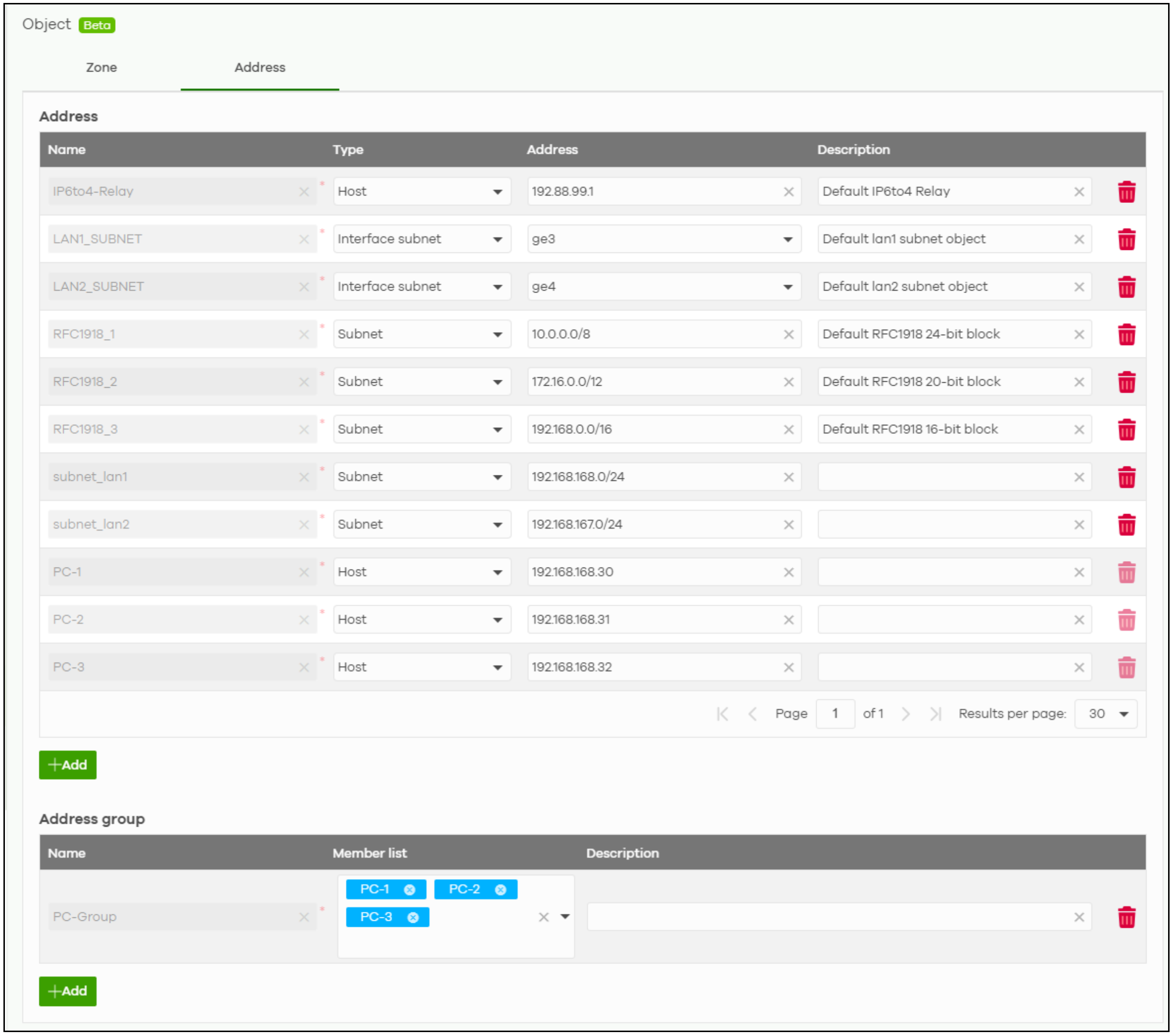
LABEL	DESCRIPTION
Name	This field displays the name of the zone. For a system default zone, the name is read only. For a user-configured zone, enter the name used to refer to the zone. You may use 2 to 30 single-byte characters, including 0-9a-zA-Z_.-, but the first character cannot be a number. This value is case-sensitive.
Member list	This field displays the names of the interfaces that belong to each zone. Select the interfaces and VPN tunnels that you want to add to the zone you are editing.
Description	This field displays the description of the zone. Enter the description associated with the zone, if any. You can use 1 to 512 single-byte characters.
Add	Click this to create a new, user-configured zone.
🗑	To remove a zone, select it and click Remove. The Nebula Device confirms you want to remove it before doing so.

8.3.10.2 IPv4 Address Overview

The **Address** screen is used to create, maintain, and remove addresses.

The **Address** screen provides a summary of all addresses and address groups in the Nebula Device. To access this screen, click **Site-wide** > **Configure** > **Firewall** > **Object** > **Address**.

Figure 192 Site-wide > Configure > Firewall > Object > Address



Address

Name	Type	Address	Description
IP6to4-Relay	Host	192.88.99.1	Default IP6to4 Relay
LAN1_SUBNET	Interface subnet	ge3	Default lan1 subnet object
LAN2_SUBNET	Interface subnet	ge4	Default lan2 subnet object
RFC1918_1	Subnet	10.0.0.0/8	Default RFC1918 24-bit block
RFC1918_2	Subnet	172.16.0.0/12	Default RFC1918 20-bit block
RFC1918_3	Subnet	192.168.0.0/16	Default RFC1918 16-bit block
subnet_lan1	Subnet	192.168.168.0/24	
subnet_lan2	Subnet	192.168.167.0/24	
PC-1	Host	192.168.168.30	
PC-2	Host	192.168.168.31	
PC-3	Host	192.168.168.32	

Address group

Name	Member list	Description
PC-Group	PC-1 PC-2 PC-3	

The following table describes the labels in this screen.

Table 134 Site-wide > Configure > Firewall > Object > Address

LABEL	DESCRIPTION
Address	
Name	This field displays the configured name of each address object. Enter a name used to refer to the address. You may use 2 to 30 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. Note: This is a required field and is not editable anymore after clicking **Apply**.

Table 134 Site-wide > Configure > Firewall > Object > Address (continued)

LABEL	DESCRIPTION
Type	This field displays the type of each address object. "INTERFACE" means the object uses the settings of one of the Nebula Device's interfaces. Select the type of address you want to create. • **Host** – the object uses an IPv4 address to define a host address. • **Range** – the object uses a range IPv4 address defined by a **Starting IP address** and an **Ending IP address**. • **Subnet** – the object uses a network address defined by a **Network** IPv4 address and **Netmask** subnet mask. • **Interface IP** – the object uses the IPv4 address of one of the Nebula Device's interfaces. • **Interface subnet** – the object uses the subnet mask of one of the Nebula Device's interfaces. • **Interface gateway** – the object uses the gateway IPv4 address of one of the Nebula Device's interfaces. • **Geography** – the object uses the IPv4 addresses of a country to represent a country. • **FQDN** – the object uses the Fully Qualified Domain Name (FQDN) to represent a website. An FQDN consists of a host and domain name. For example, 'www.zyxel.com.tw' is a fully qualified domain name, where 'www' is the host, 'zyxel' is the third-level domain, 'com' is the second-level domain, and "tw" is the top level domain. Note: The Nebula Device automatically updates address objects that are based on an interface's IPv4 address, subnet, or gateway if the interface's IPv4 address settings change. For example, if you change 1's IPv4 address, the Nebula Device automatically updates the corresponding interface-based, LAN subnet address object.
Address	This field displays the IPv4 addresses represented by each address object. If the object's settings are based on one of the Nebula Device's interfaces, the name of the interface displays first followed by the object's current address settings. Note: This field cannot be blank. Enter the IPv4 address that this address object represents.
Description	This field displays the description of the address. Enter the description associated with the address, if any. You can use 1 to 512 single-byte characters.
Add	Click this to create a new address.
🗑	To remove a user-configured address, select it and click Remove. The Nebula Device confirms you want to remove it before doing so.
Address group	
Name	This field displays the name of each address group. Enter a name used to refer to the address group. You may use 2 to 30 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. Note: This is a required field and is not editable anymore after clicking **Apply**.
Member list	This field displays the names of the address and address group objects that have been added to the address group. The order of members is not important. Select items from this list that you want to be members. Note: This field is optional. Only objects of the same address type can be added to an address group.

Table 134 Site-wide > Configure > Firewall > Object > Address (continued)

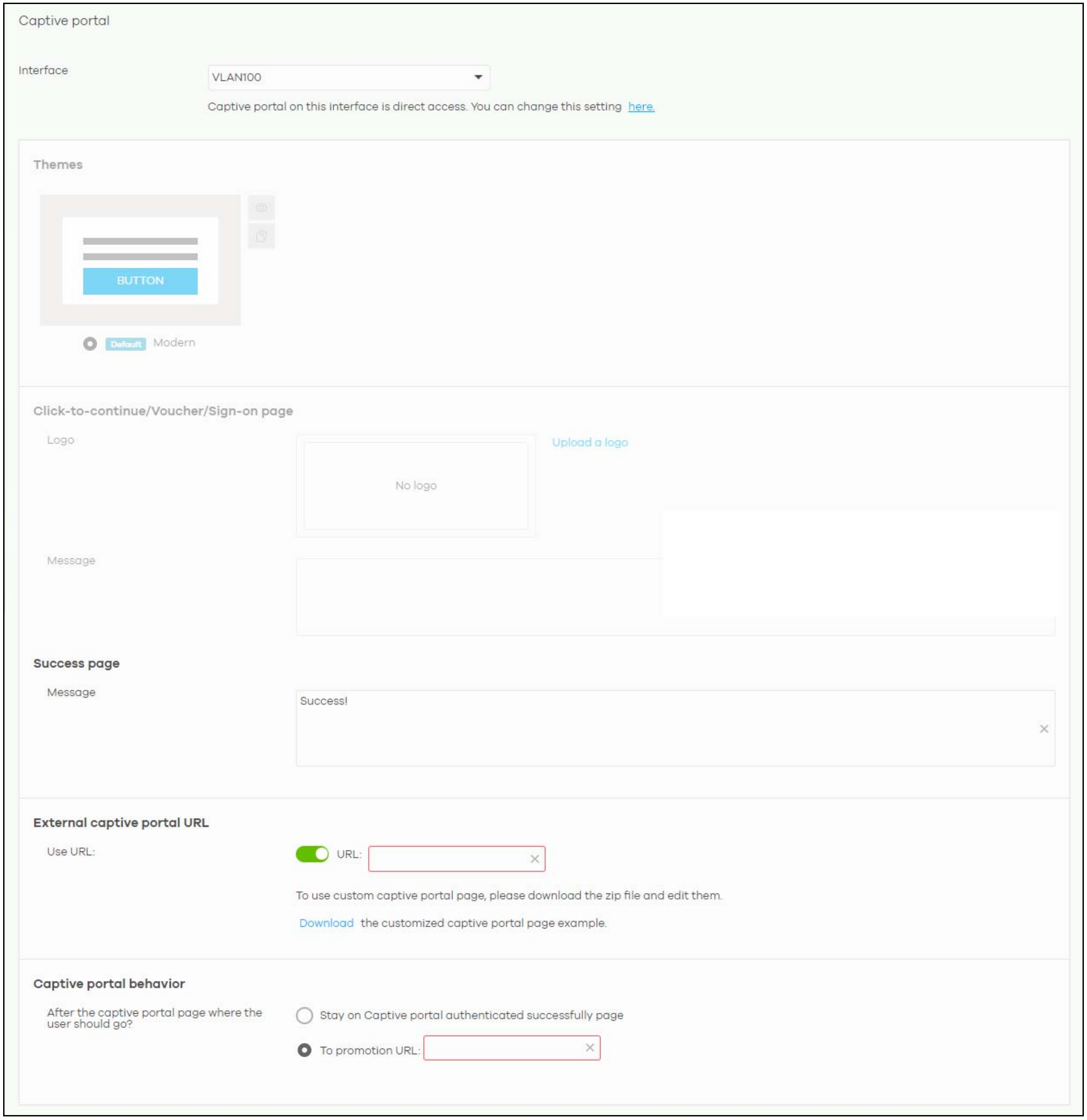
LABEL	DESCRIPTION
Description	This field displays the description of each address group, if any. Enter the description associated with the address group, if any. You can use 1 to 512 single-byte characters.
Add	Click this to add a new entry.
🗑	To remove an entry, select it and click Remove. The Nebula Device confirms you want to remove it before doing so.

8.3.11 Captive Portal

Use this screen to configure captive portal settings for each interface. A captive portal can intercept network traffic until the user authenticates his or her connection, usually through a specifically designated login web page.

Click **Site-wide** > **Configure** > **Firewall** > **Captive portal** to access this screen.

Figure 193 Site-wide > Configure > Firewall > Captive portal



Captive portal

Interface: VLAN100

Captive portal on this interface is direct access. You can change this setting here.

Themes

BUTTON

○ Default Modern

Click-to-continue/Voucher/Sign-on page

Logo: No logo — Upload a logo

Message

Success page

Message: Success!

External captive portal URL

Use URL: URL:

To use custom captive portal page, please download the zip file and edit them.

Download the customized captive portal page example.

Captive portal behavior

After the captive portal page where the user should go?

○ Stay on Captive portal authenticated successfully page

● To promotion URL:

The following table describes the labels in this screen.

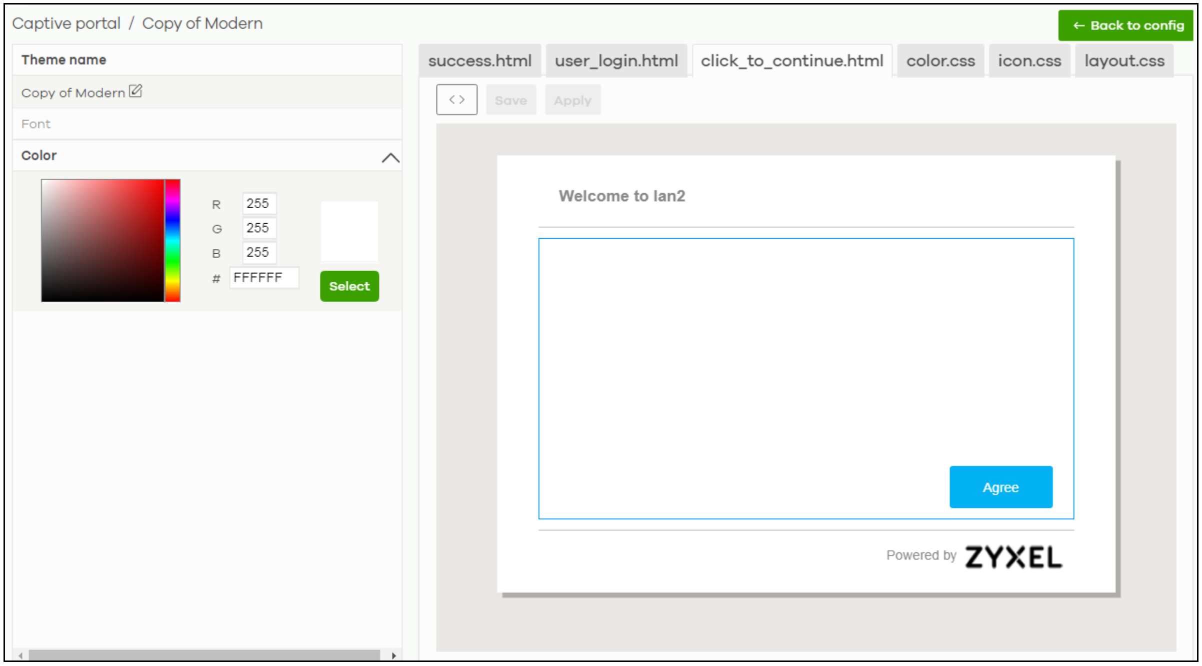
Table 135 Site-wide > Configure > Firewall > Captive portal

LABEL	DESCRIPTION
Interface	Select the Nebula Device's interface (network) to which the settings you configure here is applied.
Themes	This section is not configurable when **External captive portal URL** is set to **ON**. • Click the **Preview** icon at the upper right of a theme image to display the portal page in a new frame. • Click the **Copy** icon to create a new custom theme (portal page). • Click the **Edit** icon of a custom theme to go to a screen, where you can view and configure the details of the custom portal pages. See Section 8.3.10.1 on page 555. • Click the **Remove** icon to delete a custom theme. Select the theme you want to use on the specified interface.
Click-to-continue/Sign-on page This section is not configurable when **External captive portal URL** is set to **ON**.	
Logo	This shows the logo image that you uploaded for the customized login page. Click **Upload a logo** and specify the location and file name of the logo graphic or click **Browse** to locate it. You can use the following image file formats: GIF, PNG, or JPG.
Message	Enter a note to display below the title. Use up to 1024 printable ASCII characters. Spaces are allowed.
Success page	
Message	Enter a note to display on the page that displays when a user logs in successfully. Use up to 1024 printable ASCII characters. Spaces are allowed.
External captive portal URL	
Use URL	Select **On** to use a custom login page from an external web portal instead of the one built into the NCC. You can configure the look and feel of the web portal page. Specify the login page's URL; for example, http://IIS server IP Address/login.asp. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Captive portal behavior	
After the captive portal page where the user should go?	Select **To promotion URL** and specify the URL of the web site/page to which the user is redirected after a successful login. Otherwise, select **Stay on Captive portal authenticated successfully page**.

8.3.11.1 Custom Theme Edit

Use this screen to check what the custom portal pages look like. You can also view and modify the CSS values of the selected HTML file. Click a custom login page's **Edit** button in the **Site-wide** > **Configure** > **Firewall** > **Captive portal** screen to access this screen.

Figure 194 Site-wide > Configure > Firewall > Captive portal: Edit



R 255
G 255
B 255
FFFFFF

The following table describes the labels in this screen.

Table 136 Site-wide > Configure > Firewall > Captive portal: Edit

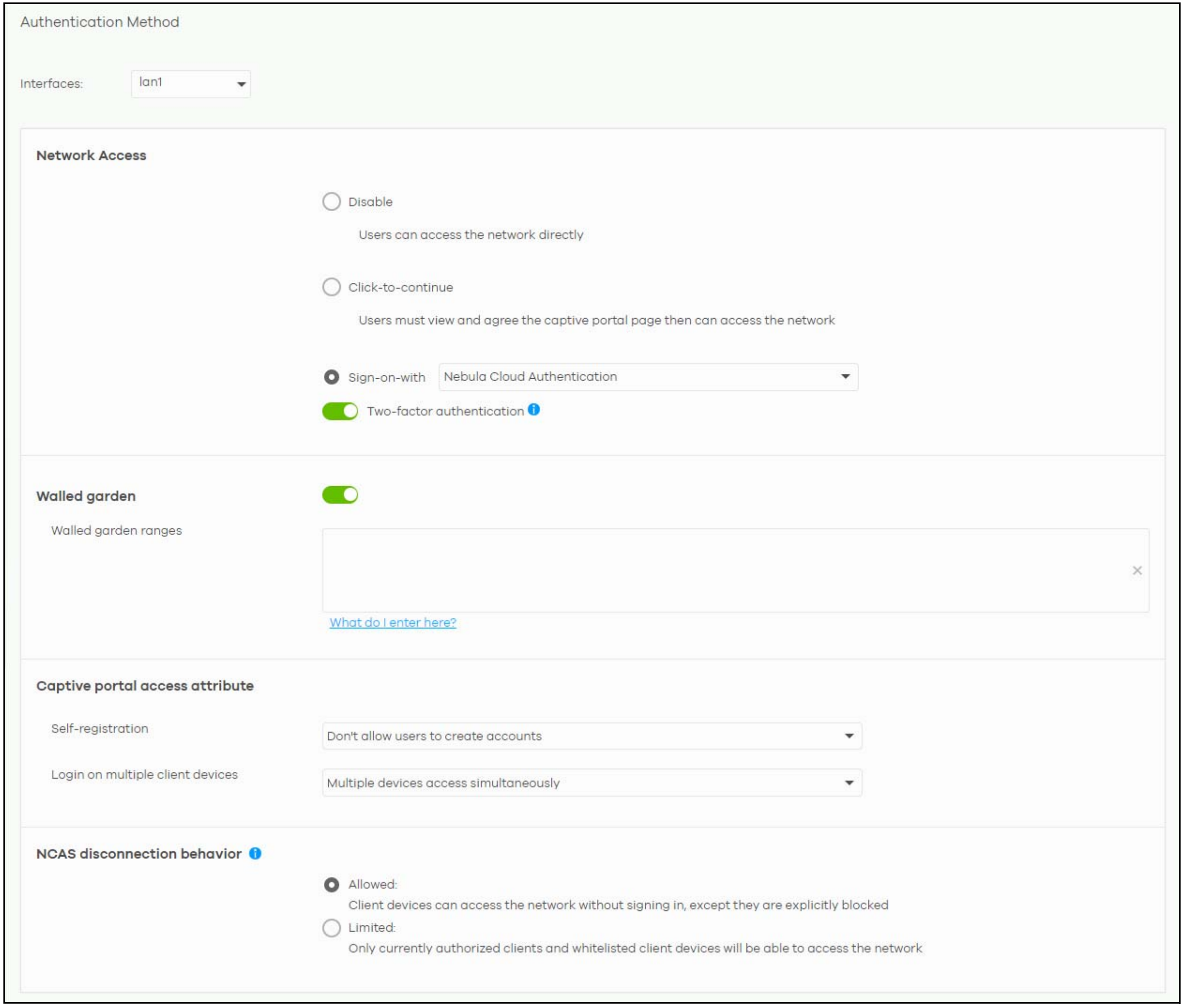
LABEL	DESCRIPTION
Back to config	Click this button to return to the **Captive portal** screen.
Theme name	This shows the name of the theme. Click the edit icon to change it.
Font	Click the arrow to hide or display the configuration fields. To display this section and customize the font type and/or size, click an item with text in the preview of the selected custom portal page (HTML file).
Color	Click the arrow to hide or display the configuration fields. Click an item in the preview of the selected custom portal page (HTML file) to display this section and customize its color, such as the color of the button, text, window's background, links, borders, and so on. Select a color that you want to use and click the **Select** button.
HTML/CSS	This shows the HTML file name of the portal page created for the selected custom theme. This also shows the name of the CSS files created for the selected custom theme. Click an HTML file to display the portal page. You can also change colors and modify the CSS values of the selected HTML file.
< >	Click this button to view and modify the CSS values of the selected HTML file. It is recommended that you do NOT change the script code to ensure proper operation of the portal page.
◎	Click this button to preview the portal page (the selected HTML file).
Save	Click this button to save your settings for the selected HTML file to the NCC.
Apply	Click this button to save your settings for the selected HTML file to the NCC and apply them to the Nebula Device in the site.

8.3.12 Authentication Method

Use this screen to enable or disable web authentication on an interface.

Click **Site-wide** > **Configure** > **Firewall** > **Authentication method** to access this screen.

Figure 195 Site-wide > Configure > Firewall > Authentication method



Authentication Method

Interfaces: lan1

Network Access

○ Disable

Users can access the network directly

○ Click-to-continue

Users must view and agree the captive portal page then can access the network

● Sign-on-with Nebula Cloud Authentication

Two-factor authentication: on

Walled garden: on

Walled garden ranges

What do I enter here?

Captive portal access attribute

Self-registration: Don't allow users to create accounts

Login on multiple client devices: Multiple devices access simultaneously

NCAS disconnection behavior

● Allowed:
Client devices can access the network without signing in, except they are explicitly blocked

○ Limited:
Only currently authorized clients and whitelisted client devices will be able to access the network

The following table describes the labels in this screen.

Table 137 Site-wide > Configure > Firewall > Authentication method

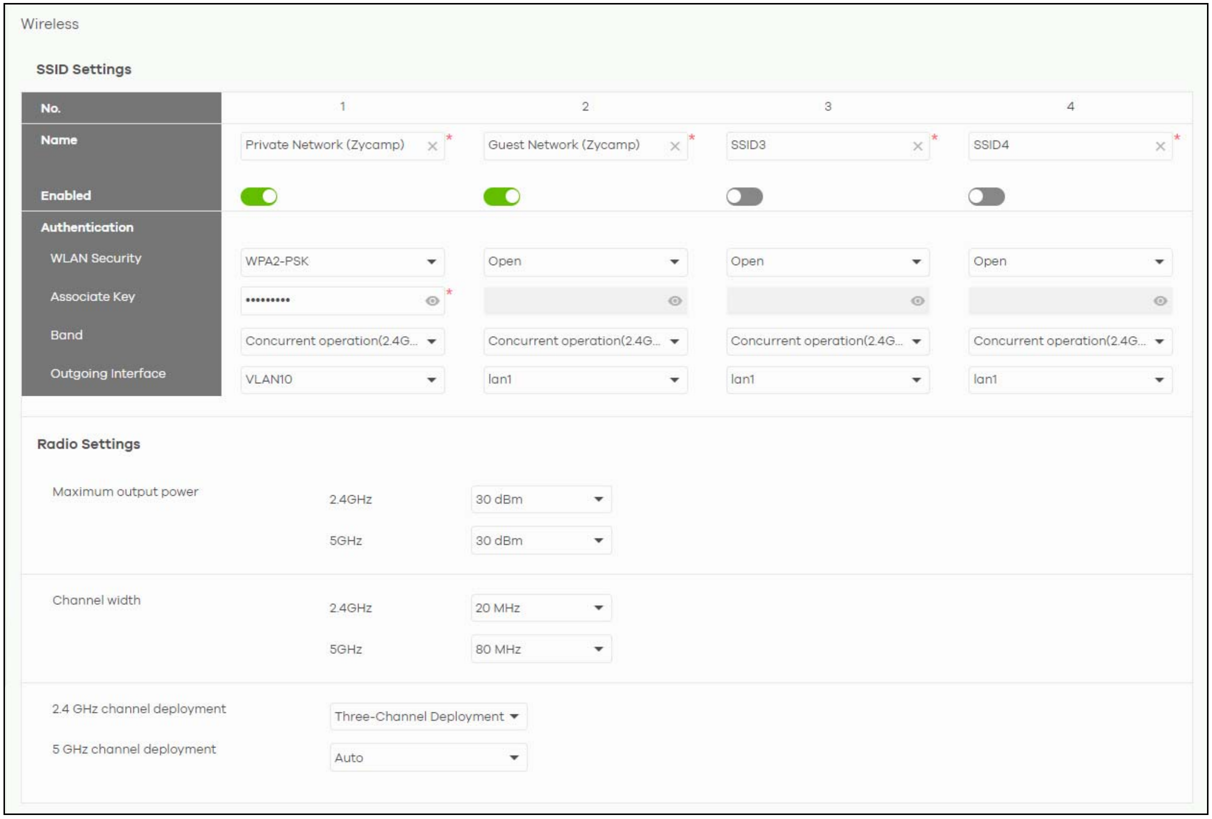
LABEL	DESCRIPTION
Interfaces	Select the Nebula Device's interface (network) to which the settings you configure here is applied.
Network Access	Select **Disable** to turn off web authentication. Select **Click-to-continue** to block network traffic until a client agrees to the policy of user agreement. Select **Sign-on with** to block network traffic until a client authenticates with an external RADIUS or AD server through the specifically designated web portal page. Select **Nebula Cloud Authentication** or an authentication server that you have configured in the **Site-wide** > **Configure** > **Firewall** > **Firewall settings** screen (see Section 8.3.14 on page 566). Select Two-Factor Authentication to require that the user log in using both their password and a Google Authenticator code. To log in, users must have Two-Factor Authentication enabled on their account and have setup Google Authenticator on their mobile device.
Walled garden	This field is not configurable if you set **Network Access** to **Disable**. Select to turn on or off the walled garden feature. With a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example.
Walled garden ranges	Specify walled garden web site links, which use a domain name or an IP address for web sites that all users are allowed to access without logging in.
Captive portal access attribute	
Self-registration	This field is available only when you select **Sign-on with Nebula Cloud authentication** in the **Network Access** field. Select **Allow users to create accounts with auto authorized** or **Allow users to create accounts with manual authorized** to display a link in the captive portal login page. The link directs users to a page where they can create an account before they authenticate with the NCC. For **Allow users to create accounts with manual authorized**, users cannot log in with the account until the account is authorized and granted access. For **Allow users to create accounts with auto authorized**, users can just use the registered account to log in without administrator approval. Select **Don't allow users to create accounts** to not display a link for account creation in the captive portal login page.
Login on multiple client devices	This field is available only when you select **Sign-on with** in the **Network Access** field. Select **Multiple devices access simultaneously** if you allow users to log in as many times as they want as long as they use different IP addresses. Select **One device at a time** if you do not allow users to have simultaneous logins.
NCAS disconnection behavior	This field is available only when you select **Sign-on with Nebula Cloud Authentication** in the **Network Access** field. Select **Allowed** to allow any users to access the network without authentication when the NCAS (Nebula Cloud Authentication Server) is not reachable. Select **Limited** to allow only the currently connected users or the users in the white list to access the network.

8.3.13 Wireless

This screen allows you to configure different SSID profiles for your Nebula Device. An SSID, or Service Set IDentifier, is the name of the WiFi network to which a WiFi client can connect. The SSID appears as readable text to any device capable of scanning for WiFi frequencies (such as the WiFi adapter in a laptop), and is displayed as the WiFi network name when a person makes a connection to it.

Click **Site-wide** > **Configure** > **Firewall** > **Wireless** to access this screen.

Figure 196 Site-wide > Configure > Firewall > Wireless



Wireless

SSID Settings

No.	1	2	3	4
Name	Private Network (Zycamp)	Guest Network (Zycamp)	SSID3	SSID4
Enabled	●	●	○	○
Authentication				
WLAN Security	WPA2-PSK	Open	Open	Open
Associate Key	•••••••••			
Band	Concurrent operation(2.4G...	Concurrent operation(2.4G...	Concurrent operation(2.4G...	Concurrent operation(2.4G...
Outgoing Interface	VLAN10	lan1	lan1	lan1

Radio Settings

Maximum output power
2.4GHz 30 dBm
5GHz 30 dBm

Channel width
2.4GHz 20 MHz
5GHz 80 MHz

2.4 GHz channel deployment: Three-Channel Deployment
5 GHz channel deployment: Auto

The following table describes the labels in this screen.

Table 138 Site-wide > Configure > Firewall > Wireless

LABEL	DESCRIPTION
SSID Settings	
No.	This shows the SSID number.
Name	This shows the SSID name as it appears to WiFi clients.
Enabled	Click this to enable the SSID to be discoverable by WiFi clients.
Authentication	
WLAN Security	Select **Open** to allow any WiFi client to associate with this network without any data encryption nor authentication. Select **WPA2-PSK** to enable WPA2-PSK data encryption.
Associate Key	Enter a pre-shared key from 8 to 64 case-sensitive keyboard characters to enable WPA2-PSK data encryption.
Band	Select to have the SSID use either **2.4 GHz band only** or the **5 GHz band only**. If you select **Concurrent operation (2.4 GHz and 5 GHz)**, the SSID uses both frequency bands.
Outgoing Interface	Select the interface for outgoing traffic from the Nebula Device to the Internet.

Table 138 Site-wide > Configure > Firewall > Wireless (continued)

LABEL	DESCRIPTION
Radio Settings	
Maximum output power	Enter the maximum output power of the radio (in dBm).
Channel width	Select the WiFi channel bandwidth you want the Nebula Device to use. A standard 20 MHz channel offers transfer speeds of up to 144 Mbps (2.4 GHz) or 217 Mbps (5 GHz) whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps (2.4 GHz) or 450 Mbps (5 GHz). An IEEE 802.11ac-specific 80 MHz channel offers speeds of up to 1.3 Gbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. An 80 MHz channel consists of two adjacent 40 MHz channels. The WiFi clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. Note: It is suggested that you select 20 MHz when there is more than one 2.4 GHz Nebula Device in the network.
2.4 GHz channel deployment	Select **Three-Channel Deployment** to limit channel switching to channels 1, 6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three “safe” channels. Select **Four-Channel Deployment** to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1 – 11 then the Nebula Device uses channels 1, 4, 7, 11 in this configuration; otherwise, the Nebula Device uses channels 1, 5, 9, 13 in this configuration. **Four-Channel Deployment** expands your pool of possible channels while keeping the channel interference to a minimum. Select **Manual** to choose the allowable channels 1 – 11.
5 GHz channel deployment	Select how you want to specify the channels the Nebula Device switches between for 5 GHz operation. Select **Auto** to have the Nebula Device automatically select the best channel. Select **Manual** to choose from the allowable channels.

8.3.14 Firewall Settings

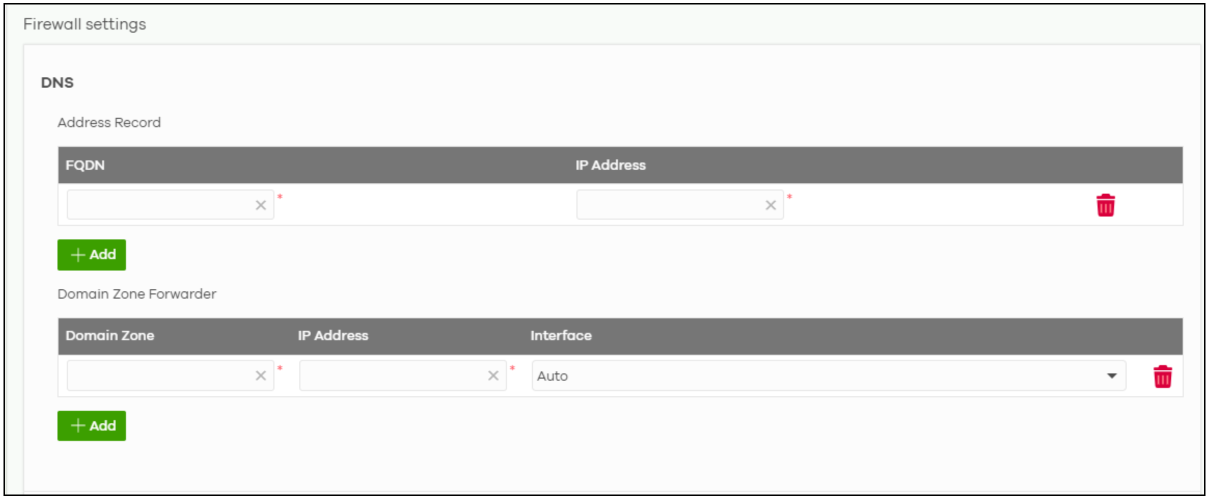
Use this screen to configure DNS settings and external AD (Active Directory), RADIUS, or LDAP server that the Nebula Device can use for authenticating users.

AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.

This screen also lets you configure the addresses of walled garden web sites that users can access without logging into the Nebula Device. The settings in this screen apply to all networks (interfaces) on the Nebula Device. If you want to configure walled garden web site links for a specific interface, use the **Authentication method** screen.

Click **Site-wide** > **Configure** > **Firewall** > **Firewall settings** to access this screen.

Figure 197 Site-wide > Configure > Firewall > Firewall settings: DNS



Firewall settings

DNS

Address Record

FQDN	IP Address	
× *	× *	🗑

+ Add

Domain Zone Forwarder

Domain Zone	IP Address	Interface	
× *	× *	Auto	🗑

+ Add

The following table describes the labels in this screen.

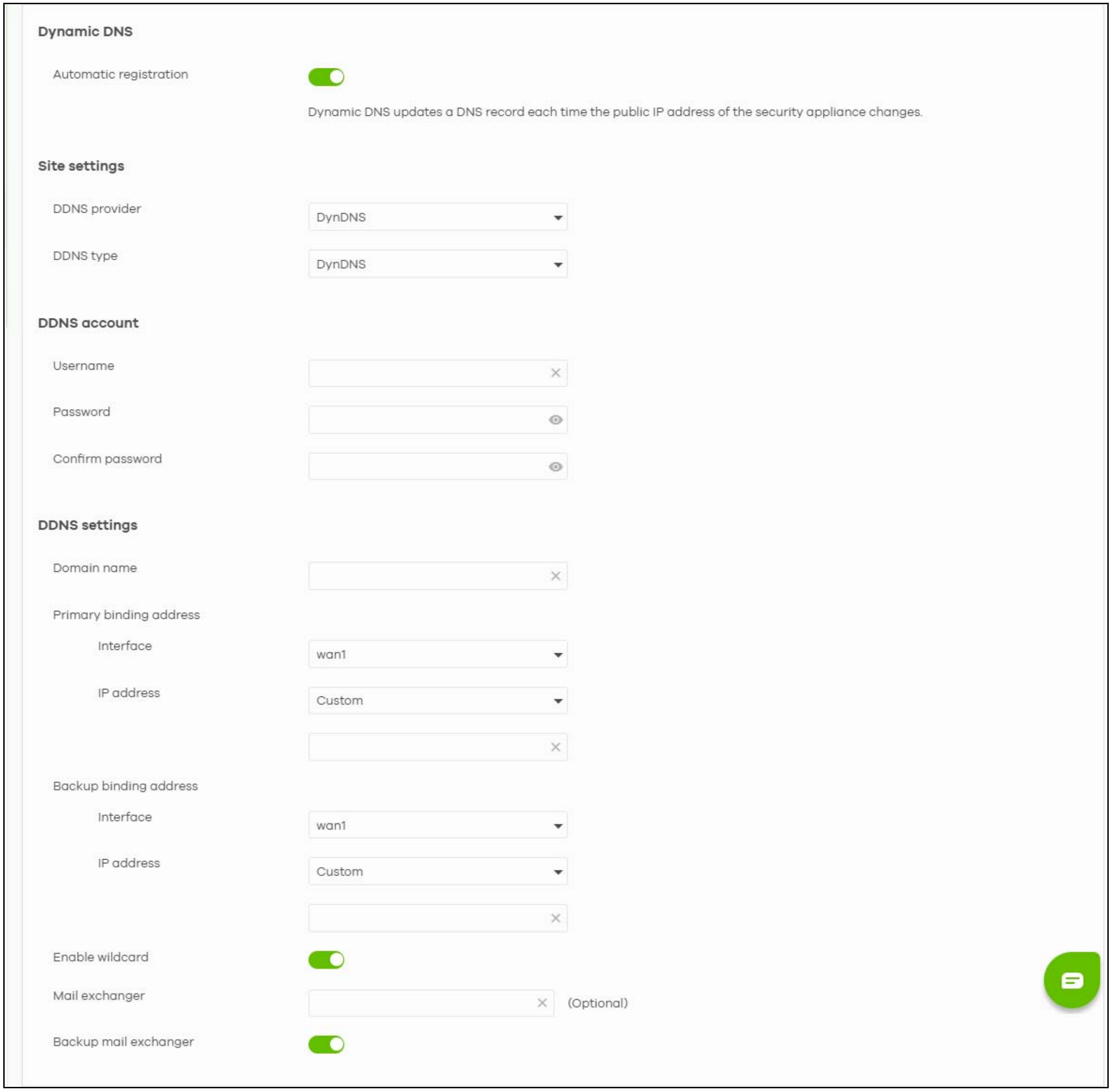
Table 139 Site-wide > Configure > Firewall > Firewall settings: DNS

LABEL	DESCRIPTION
DNS	
Address Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IPv4 address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.
FQDN	This field is only available if the Address Type is FQDN, in which case this field cannot be blank. Enter the FQDN of the website that this address object represents. You can enter a wildcard in the first position. For example, ‘*.zyxel.com’.
IP Address	Enter the host’s IPv4 address.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Domain Zone Forwarder	This specifies a DNS server’s IP address. The Nebula Device can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the Nebula Device needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
Domain Zone	A domain is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. Whenever the Nebula Device receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address.
IP Address	Enter the DNS server's IP address.
Interface	Select the interface through which the Nebula Device sends DNS queries to the specified DNS server.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.

8.3.14.1 Dynamic DNS

Enable **Dynamic DNS** to open the **Site-wide** > **Configure** > **Firewall** > **Firewall settings: Dynamic DNS** screen.

Figure 198 Site-wide > Configure > Firewall > Firewall settings: Dynamic DNS



Dynamic DNS

Automatic registration: on

Dynamic DNS updates a DNS record each time the public IP address of the security appliance changes.

Site settings

DDNS provider: DynDNS

DDNS type: DynDNS

DDNS account

Username

Password

Confirm password

DDNS settings

Domain name

Primary binding address

Interface: wan1

IP address: Custom

Backup binding address

Interface: wan1

IP address: Custom

Enable wildcard: on

Mail exchanger (Optional)

Backup mail exchanger: on

The following table describes the labels in this screen.

Table 140 Site-wide > Configure > Firewall > Firewall settings: Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	
Automatic registration	Click On to use dynamic DNS. Otherwise, select Off to disable it.
Site settings	
DDNS provider	Select your Dynamic DNS service provider from the drop-down list box. If you select **User customize**, create your own DDNS service.
DDNS type	Select the type of DDNS service you are using. This will depend on your choice of the **DDNS provider**.
DDNS account	

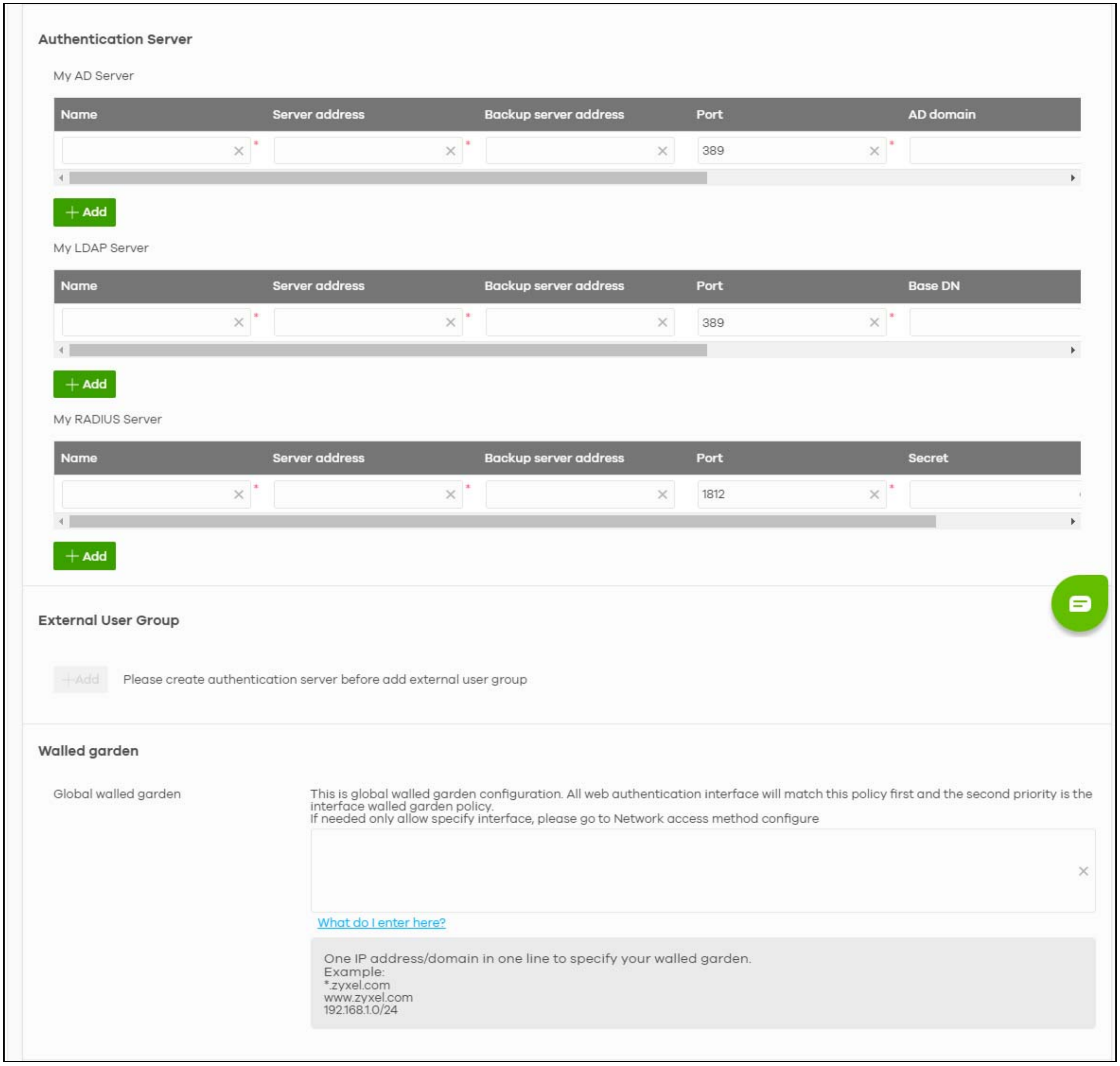
Table 140 Site-wide > Configure > Firewall > Firewall settings: Dynamic DNS (continued)

LABEL	DESCRIPTION
Username	Enter the user name used when you registered your domain name, up to 31 characters [a-zA-Z0-9_-][:a-zA-Z0-9@\._–].
Password	Enter the password provided by the DDNS provider, up to 63 characters [0-9a-zA-Z`~!@#$%^&*()_\\-+={}|;:<>,./\'"]|[\\\\].
Confirm password	Enter the password again to confirm it.
DDNS settings	
Domain name	Enter the domain name you registered.
Primary binding address	Use these fields to set how the Nebula Device determines the IP address that is mapped to your domain name in the DDNS server. The Nebula Device uses the **Backup binding address** if the interface specified by these settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name.
IP address	Select **Auto** if the interface has a dynamic IP address. The DDNS server checks the source IP address of the packets from the Nebula Device for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the Nebula Device and the DDNS server. Note: The Nebula Device may not determine the proper IP address if there is an HTTP proxy server between the Nebula Device and the DDNS server. Select **Custom** if you have a static IP address. Enter the IP address to use it for the domain name. Select **Interface** to have the Nebula Device use the IP address of the specified interface.
Backup binding address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the **Primary binding address** settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name.
IP address	Select **Auto** if the interface has a dynamic IP address. The DDNS server checks the source IP address of the packets from the Nebula Device for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the Nebula Device and the DDNS server. Note: Note: The Nebula Device may not determine the proper IP address if there is an HTTP proxy server between the gateway and the DDNS server. Select **Custom** if you have a static IP address. Enter the IP address to use it for the domain name. Select **Interface** to have the Security Firewall use the IP address of the specified interface.
Enable wildcard	This option is only available with a DynDNS account. Enable the wildcard feature to alias sub-domains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Table 140 Site-wide > Configure > Firewall > Firewall settings: Dynamic DNS (continued)

LABEL	DESCRIPTION
Mail exchanger	This option is only available with a DynDNS account. DynDNS can route email for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes email for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger. If you are using this service, type the host record of your mail server here. Otherwise, leave the field blank.
Backup mail exchanger	This option is only available with a DynDNS account. Select this checkbox if you are using DynDNS's backup service for email. With this service, DynDNS holds onto your email if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. See www.dyndns.org for more information about this service.

Figure 199 Site-wide > Configure > Firewall > Firewall settings (Authentication Server / External User Group / Walled garden)



Authentication Server

My AD Server

Name	Server address	Backup server address	Port	AD domain
			389	

+ Add

My LDAP Server

Name	Server address	Backup server address	Port	Base DN
			389	

+ Add

My RADIUS Server

Name	Server address	Backup server address	Port	Secret
			1812	

+ Add

External User Group

+ Add Please create authentication server before add external user group

Walled garden

Global walled garden

This is global walled garden configuration. All web authentication interface will match this policy first and the second priority is the interface walled garden policy.
If needed only allow specify interface, please go to Network access method configure

What do I enter here?

One IP address/domain in one line to specify your walled garden.
Example:
*.zyxel.com
www.zyxel.com
192.168.1.0/24

The following table describes the labels in this screen.

Table 141 Site-wide > Configure > Firewall > Firewall settings (Authentication Server / External User / Walled garden)

LABEL	DESCRIPTION
Authentication Server My AD Server	
Name	Enter a descriptive name for the server.
Server address	Enter the address of the AD server.
Backup server address	If the AD server has a backup server, enter its address here.
Port	Specify the port number on the AD server to which the Nebula Device sends authentication requests. Enter a number between 1 and 65535.
AD domain	Specify the Active Directory forest root domain name.
Domain admin	Enter the name of the user that is located in the container for Active Directory Users, who is a member of the Domain Admin group.
Password	Enter the password of the Domain Admin user account.
Advanced	Click to open a screen where you can select to use **Default** or **Custom** advanced settings. See Section 8.3.14.3 on page 574.
🗑	Click this icon to remove the server.
Add	Click this button to create a new server.
My LDAP Server	
Name	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server address	Enter the address of the LDAP server.
Backup server address	If the LDAP server has a backup server, enter its address here.
Port	Specify the port number on the LDAP server to which the Nebula Device sends authentication requests. Enter a number between 1 and 65535.
Base DN	Specify the directory (up to 127 alphanumerical characters). For example, o=Zyxel, c=US.
Bind DN	Specify the bind DN for logging into the AD or LDAP server. Enter up to 127 alphanumerical characters. For example, cn=zywallAdmin specifies zywallAdmin as the user name.
Password	If required, enter the password (up to 15 alphanumerical characters) required to bind or log in to the LDAP server.
Advanced	Click to open a screen where you can select to use **Default** or **Custom** advanced settings. See Section 8.3.14.3 on page 574.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new server.
My RADIUS Server	
Name	Enter a descriptive name for the server.
Server address	Enter the address of the RADIUS server.
Backup server address	If the RADIUS server has a backup server, enter its address here.
Port	Specify the port number on the RADIUS server to which the Nebula Device sends authentication requests. Enter a number between 1 and 65535.

Table 141 Site-wide > Configure > Firewall > Firewall settings (Authentication Server / External User / Walled garden) (continued)

LABEL	DESCRIPTION
Secret	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the Nebula Device. The key is not sent over the network. This key must be the same on the external authentication server and the Security Firewall.
Advanced	Click to open a screen where you can select to use **Default** or **Custom** advanced settings. See Section 8.3.14.3 on page 574.
🗑	Click this icon to remove the server.
Add	Click this button to create a new server.
External User Group	
Group Name	Enter a descriptive name for the group, up to 31 characters [0–9][a–z][A–Z][@.-_] but the first character must be an alphabet.
Authentication Server	Select the **Name** of the **Authentication Server** you added in **My AD Server**, **My LDAP Server**, or **My RADIUS Server**.
Group ID	Enter the name of the attribute that the Nebula Device checks to determine to which group an external user belongs. The value for this attribute is called a group identifier; it determines to which group an external user belongs.
Add	Click this button to create a new group. The maximum number of external user groups is 20.
Walled garden	
Global walled garden	With a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example. Specify walled garden web site links, which use a domain name or an IP address for web sites that all users are allowed to access without logging in.

8.3.14.2 SIP ALG

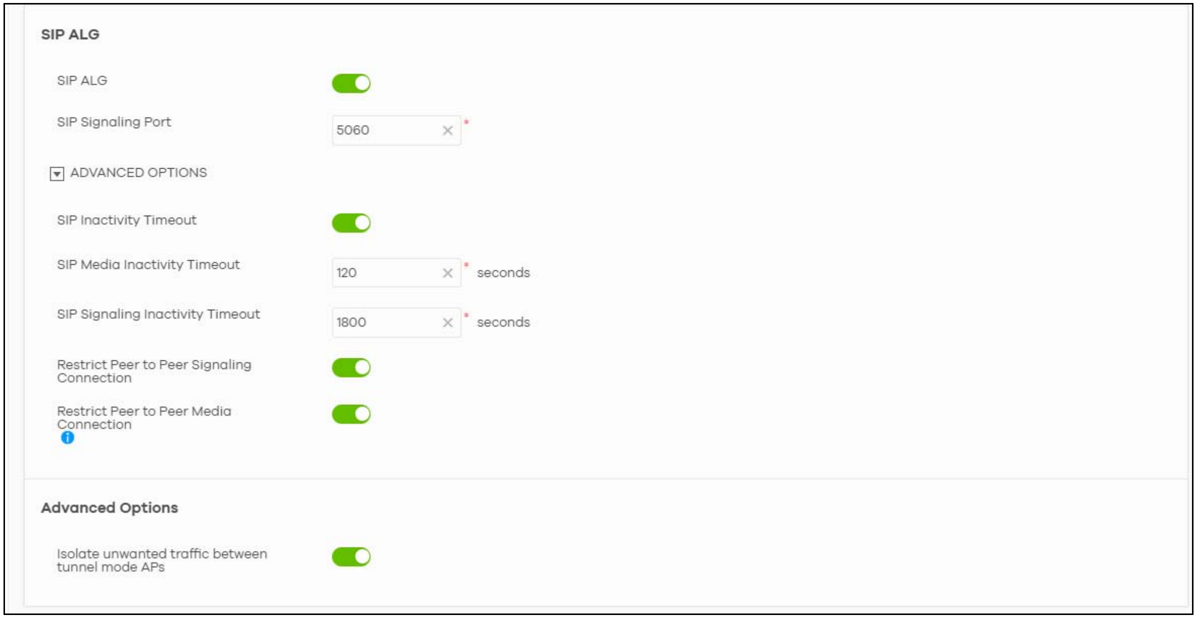
Application Layer Gateway (ALG) allows the following applications to operate properly through the NCC’s NAT.

SIP (Session Initiation Protocol) is an application-layer protocol that can be used to create voice and multimedia sessions over Internet.

Go to **SIP ALG** in the **Site-wide** > **Configure** > **Firewall** > **Firewall settings** screen to access this screen. Use this screen to turn the ALG off or on, configure the port numbers to which they apply, and configure SIP ALG time outs.

Note: If the NCC provides an ALG for a service, you must enable the ALG in order to use the application patrol on that service’s traffic.

Figure 200 Site-wide > Configure > Firewall > Firewall settings: SIP ALG / Advanced Options



SIP ALG

SIP ALG: On

SIP Signaling Port: 5060

ADVANCED OPTIONS

SIP Inactivity Timeout: On

SIP Media Inactivity Timeout: 120 seconds

SIP Signaling Inactivity Timeout: 1800 seconds

Restrict Peer to Peer Signaling Connection: On

Restrict Peer to Peer Media Connection: On

Advanced Options

Isolate unwanted traffic between tunnel mode APs: On

The following table describes the labels in this screen.

Table 142 Site-wide > Configure > Firewall > Firewall settings: SIP ALG / Advanced Options

LABEL	DESCRIPTION
SIP ALG	Turn on SIP ALG to detect SIP traffic and help build SIP sessions through the Nebula Device's NAT. Enabling the SIP ALG also allows you to use the application patrol to detect SIP traffic and manage SIP traffic bandwidth.
SIP Signaling Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here. Use the **Add** icon to add fields if you are also using SIP on additional UDP port numbers (1025 – 65535).
ADVANCED OPTIONS	Click the arrow to show the fields for setting the SIP inactivity timeout and restrict peer-to-peer connection.
SIP Inactivity Timeout	Select this to have the Nebula Device apply SIP media and signaling inactivity time out limits. These timeouts will take priority over the SIP session time out "Expires" value in a SIP registration response packet.
SIP Media Inactivity Timeout	Use this field to set how many seconds (1 – 86400) the Nebula Device will allow a SIP session to remain idle (without voice traffic) before dropping it. If no voice packets go through SIP ALG before the timeout period expires, the Nebula Device deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.
SIP Signaling Inactivity Timeout	Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the Nebula Device. If the SIP client does not have this mechanism and makes no calls during the Nebula Device SIP timeout, the Nebula Device deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1 – 86400).
Restrict Peer to Peer Signaling Connection	A signaling connection is used to set up the SIP connection. Enable this if you want signaling connections to only arrive from the IP addresses you have already registered with. Signaling connections from other IP addresses will be dropped.
Restrict Peer to Peer Media Connection	A media connection is the audio transfer in a SIP connection. Enable this if you want media connections to only arrive from the IP addresses you registered with. Media connections from other IP addresses will be dropped.

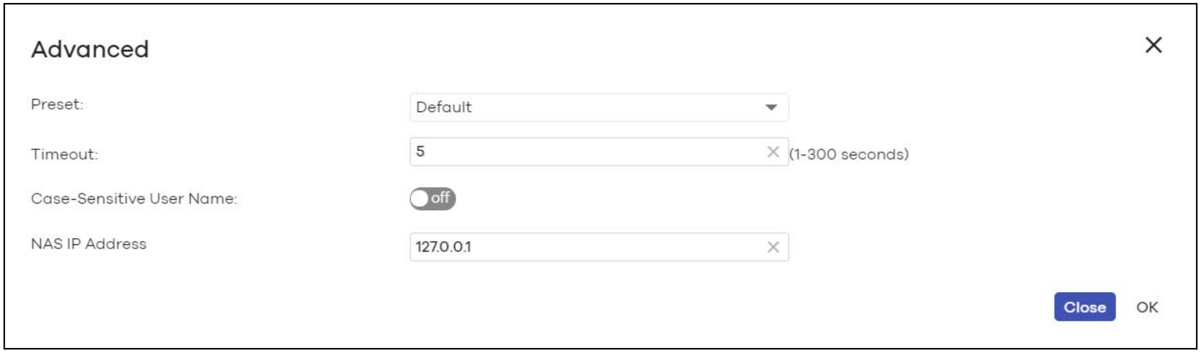
Table 142 Site-wide > Configure > Firewall > Firewall settings: SIP ALG / Advanced Options (continued)

LABEL	DESCRIPTION
Advanced Options	
Isolate unwanted traffic between tunnel mode APs	Select On to block broadcast and multicast traffic coming from Remote APs (RAPs).

8.3.14.3 Advanced Settings

Click the **Advanced** column in the **Site-wide** > **Configure** > **Firewall** > **Firewall settings** screen to access this screen.

Figure 201 Site-wide > Configure > Firewall > Firewall settings: Advanced



Advanced

Preset: Default

Timeout: 5 (1-300 seconds)

Case-Sensitive User Name: off

NAS IP Address 127.0.0.1

The following table describes the labels in this screen.

Table 143 Site-wide > Configure > Firewall > Firewall settings: Advanced

LABEL	DESCRIPTION
Preset	Select **Default** to use the pre-defined settings, or select **Custom** to configure your own settings.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the Nebula Device disconnects from the server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the servers or the AD or server is down.
Case-Sensitive User Name	Click **ON** if the server checks the case of the user name. Otherwise, click **OFF** to not configure your user name as case-sensitive.
Group Membership Attribute	Enter the name of the attribute that the gateway checks to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named “memberOf” with values like “sales”, “RD”, and “management”. Then you could also create a ext-group-user user object for each group. One with “sales” as the group identifier, another for “RD” and a third for “management”.
LDAP-only Fields	
Login Name Attribute	Enter the type of identifier the users are to use to log in. For example “name” or “email address”.
RADIUS-only Fields	
NAS IP Address	Enter the IP address of the NAS (Network Access Server).
NAS Identifier	Enter the Network Access Server (**NAS**) **Identifier** on the Nebula Device to identify the Nebula Device to the RADIUS server, if required. This might be necessary if there are multiple Nebula Devices behind NAT using the same public WAN IP address for the RADIUS server.

Table 143   Site-wide > Configure > Firewall > Firewall settings: Advanced (continued)

LABEL	DESCRIPTION
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

CHAPTER 9
Security Gateway

9.1 Overview

This chapter discusses the menus that you can use to monitor the Nebula managed Security Gateways in your network and configure settings even before a gateway is deployed and added to the site.

Nebula Device refers to Nebula NSG devices in this chapter. The **Security gateway** menus are shown for Nebula NSG devices only.

9.2 Monitor

Use the **Monitor** menus to check the Nebula Device information, client information, event log messages and summary report for the Nebula Device in the selected site.

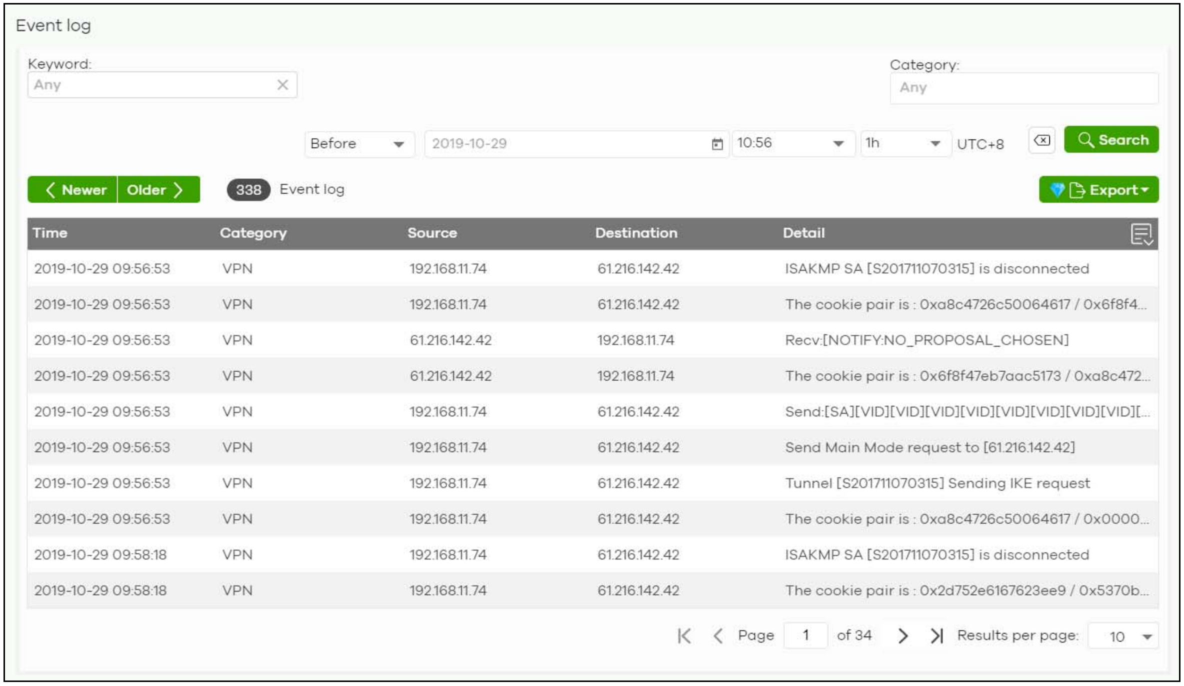
9.2.1 Event Log

Use this screen to view Nebula Device log messages. You can enter a key word, select one or multiple event types, or specify a date/time or a time range to display only the log messages that match these criteria.

Select **Range** to set a time range or select **Before** to choose a specific date/time and the number of hours/minutes to display only the log messages generated within a certain period of time (before the specified date/time). Then click **Search** to update the list of logs based on the search criteria. The maximum allowable time range is 30 days.

Click **Site-wide** > **Monitor** > **Security gateway** > **Event log** to access this screen.

Figure 202 Site-wide > Monitor > Security gateway > Event log



Event log

Keyword: Any

Category: Any

Before | 2019-10-29 | 10:56 | 1h | UTC+8

338 Event log

Time	Category	Source	Destination	Detail
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	ISAKMP SA [S201711070315] is disconnected
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	The cookie pair is : 0xa8c4726c50064617 / 0x6f8f4...
2019-10-29 09:56:53	VPN	61.216.142.42	192.168.11.74	Recv:[NOTIFY:NO_PROPOSAL_CHOSEN]
2019-10-29 09:56:53	VPN	61.216.142.42	192.168.11.74	The cookie pair is : 0x6f8f47eb7aac5173 / 0xa8c472...
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	Send:[SA][VID][VID][VID][VID][VID][VID][VID][VID][...
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	Send Main Mode request to [61.216.142.42]
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	Tunnel [S201711070315] Sending IKE request
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	The cookie pair is : 0xa8c4726c50064617 / 0x0000...
2019-10-29 09:58:18	VPN	192.168.11.74	61.216.142.42	ISAKMP SA [S201711070315] is disconnected
2019-10-29 09:58:18	VPN	192.168.11.74	61.216.142.42	The cookie pair is : 0x2d752e6167623ee9 / 0x5370b...

Page 1 of 34 Results per page: 10

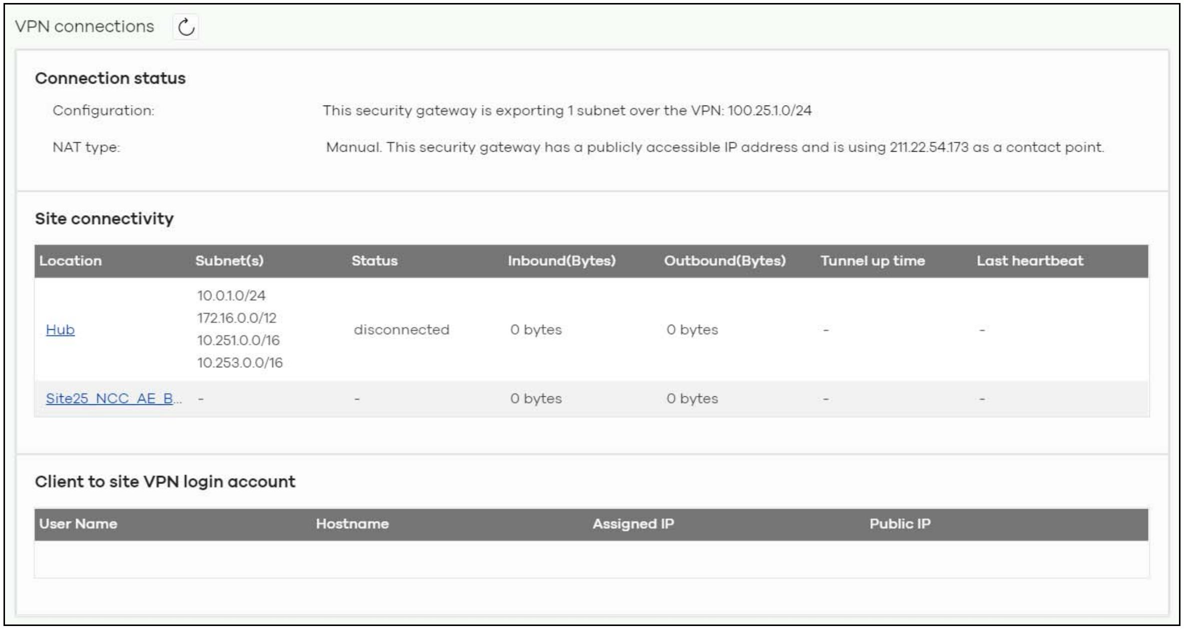
9.2.2 VPN Connections

Use this screen to view the status of site-to-site IPSec VPN connections and L2TP VPN connections.

Note: If the peer gateway is not a Nebula Device, go to the **Site-wide** > **Configure** > **Security gateway** > **Site-to-Site VPN** screen to view and configure a VPN rule. See Section 9.3.6 on page 610 for more information.

Click **Site-wide** > **Monitor** > **Security gateway** > **VPN Connections** to access this screen.

Figure 203 Site-wide > Monitor > Security gateway > VPN Connections



VPN connections ↻

Connection status

Configuration: This security gateway is exporting 1 subnet over the VPN: 100.25.1.0/24

NAT type: Manual. This security gateway has a publicly accessible IP address and is using 211.22.54.173 as a contact point.

Site connectivity

Location	Subnet(s)	Status	Inbound(Bytes)	Outbound(Bytes)	Tunnel up time	Last heartbeat
Hub	10.0.1.0/24 172.16.0.0/12 10.251.0.0/16 10.253.0.0/16	disconnected	0 bytes	0 bytes	-	-
Site25_NCC_AE_B...	-	-	0 bytes	0 bytes	-	-

Client to site VPN login account

User Name	Hostname	Assigned IP	Public IP

The following table describes the labels in this screen.

Table 144 Site-wide > Monitor > Security gateway > VPN Connections

LABEL	DESCRIPTION
↻	Click this button to reload the data-related frames on this page.
Connection Status	
Configuration	This shows the number and address of the local networks behind the Nebula Device, on which the computers are allowed to use the VPN tunnel.
NAT Type	This shows the public IP address or the domain name that is configured and mapped to the Nebula Device on the NAT router.
Site Connectivity	
Location	This shows the name of the site to which the peer gateway is assigned. Click the name to go to the **Site-wide** > **Configure** > **Security gateway** > **Site-to-Site VPN** screen, where you can modify the VPN settings.
Subnet(s)	This shows the address of the local networks behind the Nebula Device.
Status	This shows whether the VPN tunnel is connected or disconnected.
Inbound (Bytes)	This shows the amount of traffic that has gone through the VPN tunnel from the remote IPSec router to the Nebula Device since the VPN tunnel was established.
Outbound (Bytes)	This shows the amount of traffic that has gone through the VPN tunnel from the Nebula Device to the remote IPSec router since the VPN tunnel was established.
Tunnel up time	This shows how many seconds the VPN tunnel has been active.
Last heartbeat	This shows the last date and time a heartbeat packet is sent to determine if the VPN tunnel is up or down.
Client to site VPN login account	
User Name	This shows the remote user's login account name.
Hostname	This shows the name of the computer that has this L2TP VPN connection with the Nebula Device.

Table 144 Site-wide > Monitor > Security gateway > VPN Connections (continued)

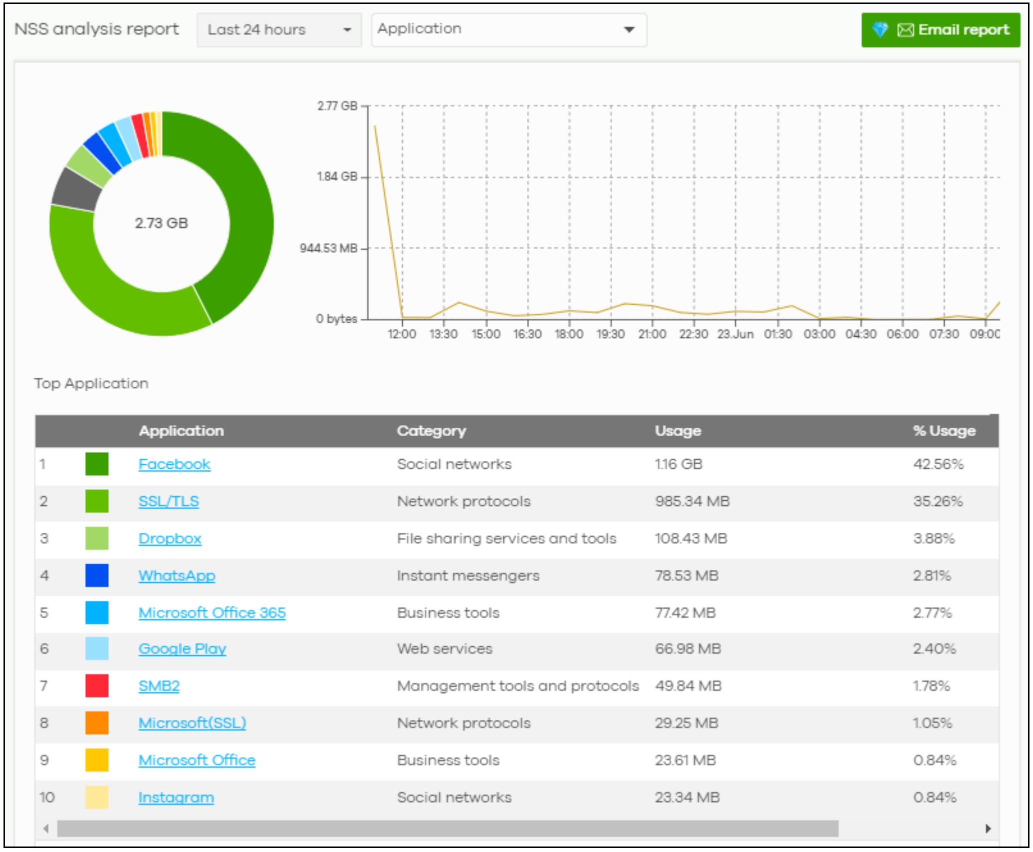
LABEL	DESCRIPTION
Assigned IP	This shows the IP address that the Nebula Device assigned for the remote user's computer to use within the L2TP VPN tunnel.
Public IP	This shows the public IP address that the remote user is using to connect to the Internet.

9.2.3 NSS Analysis Report

Use this screen to view the statistics report for NSS (Nebula Security Service), such as content filter, Intrusion Detection and Prevention (IDP), application patrol, and anti-virus. The screen varies depending on the service type (**Application**, **Content Filtering**, or **Anti-Virus**) you select.

Click **Site-wide** > **Monitor** > **Security gateway** > **NSS analysis report** to access this screen.

Figure 204 Site-wide > Monitor > Security gateway > NSS Analysis Report



NSS analysis report — Last 24 hours — Application — Email report

Top Application

		Application	Category	Usage	% Usage
1	🟩	Facebook	Social networks	1.16 GB	42.56%
2	🟩	SSL/TLS	Network protocols	985.34 MB	35.26%
3	🟩	Dropbox	File sharing services and tools	108.43 MB	3.88%
4	🟦	WhatsApp	Instant messengers	78.53 MB	2.81%
5	🟦	Microsoft Office 365	Business tools	77.42 MB	2.77%
6	🟦	Google Play	Web services	66.98 MB	2.40%
7	🟥	SMB2	Management tools and protocols	49.84 MB	1.78%
8	🟧	Microsoft(SSL)	Network protocols	29.25 MB	1.05%
9	🟨	Microsoft Office	Business tools	23.61 MB	0.84%
10	🟨	Instagram	Social networks	23.34 MB	0.84%

The following table describes the labels in this screen.

Table 145   Site-wide > Monitor > Security gateway > NSS Analysis Report

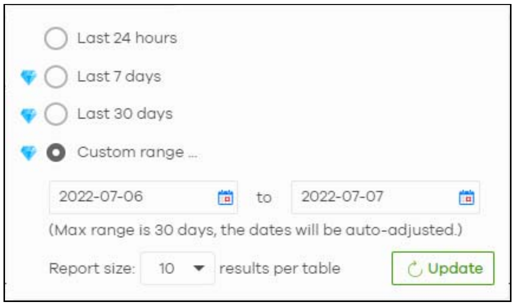
LABEL	DESCRIPTION
Security Appliance – NSS Analysis	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ○ Last 7 days ○ Last 30 days ● Custom range ... 2022-07-06 to 2022-07-07 (Max range is 30 days, the dates will be auto-adjusted.) Report size: 10 results per table
	Select the type of service for which you want to view the statistics report.
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
Application The following fields displays when you select to view the application statistics. Click an application name to view information about the clients who use that application. Click **Top Application** under the chart to switch back to the previous screen.	
y-axis	The y-axis shows the amount of the application's traffic which has been transmitted or received.
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Application	This shows the name of the application. Click an application name to view the IPv4 addresses of the clients who used the application.
Description	This shows the name of the client who used the application. This field is available when you click the application name. Click the name to display the individual client statistics. See Section 9.2.1 on page 576.
IPv4 Address	This shows the IPv4 address of the client who used the application. This field is available when you click the application name.
MAC Address	This shows the MAC address of the client who used the application. This field is available when you click the application name.
Category	This shows the name of the category to which the application belongs.
Usage	This shows the total amount of data consumed by the application used by all or a specific IPv4 address.
% Usage	This shows the percentage of usage for the application used by all or a specific IPv4 address.
Content Filtering The following fields display when you select to view the content filter statistics. Click a website URL to view information about the clients who tried to access that web page. Click **Content Filtering** under the chart to switch back to the previous screen.	
y-axis	The y-axis shows the number of hits on web pages that the Nebula Device's content filter service has blocked.
x-axis	The x-axis shows the time period over which the web page is checked.
Website	This shows the URL of the web page to which the Nebula Device blocked access. Click a website URL to view the IPv4 addresses of the clients who tried to access the web page.

Table 145 Site-wide > Monitor > Security gateway > NSS Analysis Report (continued)

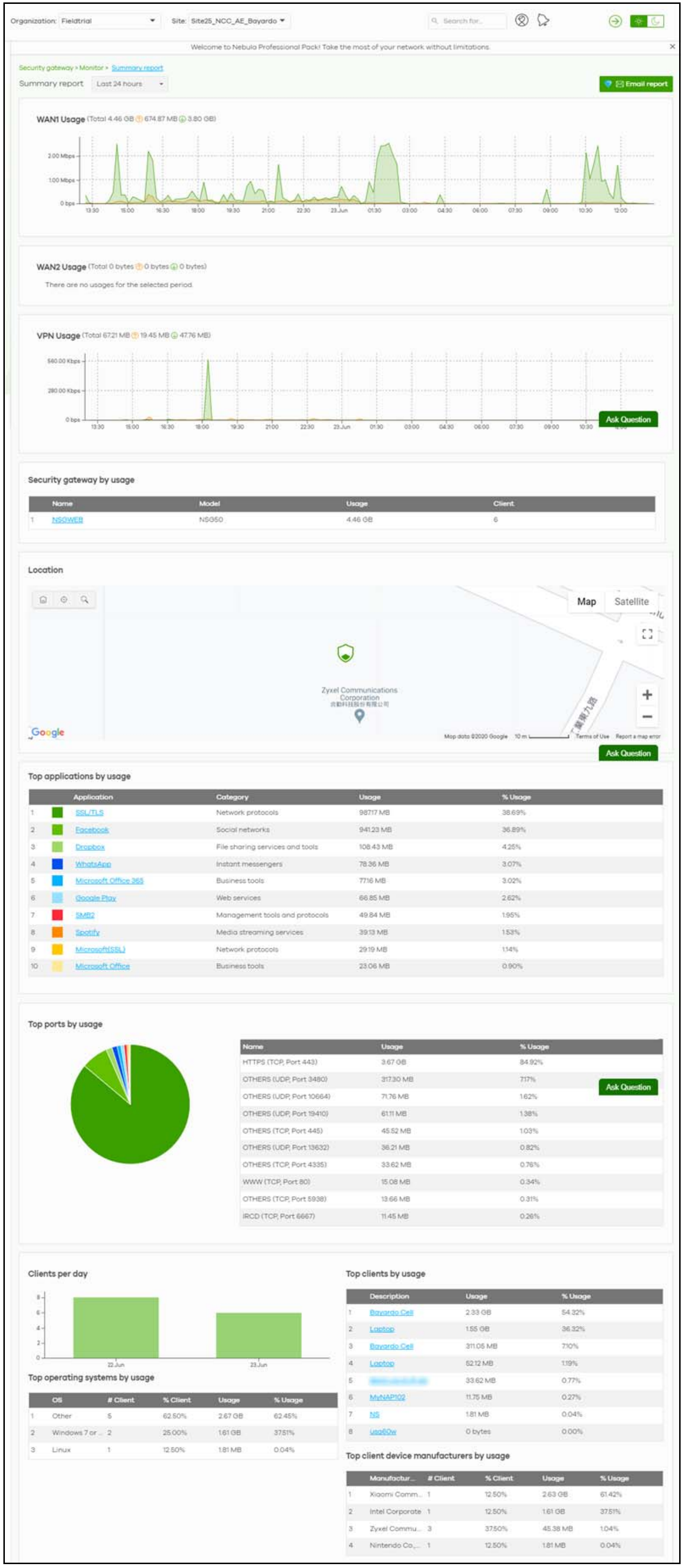
LABEL	DESCRIPTION
Description	This shows the name of the client who tried to access the web page. This field is available when you click the website URL. Click the name to display the individual client statistics. See Section 9.2.1 on page 576.
IPv4 Address	This shows the IPv4 address of the client who tried to access the web page. This field is available when you click the website URL.
MAC Address	This shows the MAC address of the client who tried to access the web page. This field is available when you click the website URL.
Category	This shows the name of the category to which the web page belongs.
Hits	This shows the number of hits on the web page visited by all or a specific IPv4 address.
% Hits	This shows the percentage of the hit counts for the web page visited by all or a specific IPv4 address.
Anti-Virus The following fields are displayed when you select **Anti-Virus**. Click a virus name to view information about the clients who sent the virus. Click the number in the center of the donut chart or **Anti-Virus** under the chart to switch back to the previous screen.	
y-axis	The y-axis shows the total number of viruses that the gateway has detected.
x-axis	The x-axis shows the time period over which the virus is detected.
Virus Name	This shows the name of the virus that the Nebula Device has detected and blocked. Click a virus name to view the IPv4 addresses of the clients who sent the virus.
Description	This shows the name of the client who sent the virus. This field is available when you click the virus name. Click the name to display the individual client statistics. See Section 9.2.1 on page 576.
IPv4 Address	This shows the IPv4 address of the virus sender. This field is available when you click the virus name.
MAC Address	This shows the MAC address of the virus sender. This field is available when you click the virus name.
Hits	This shows how many times the gateway has detected the virus sent by all or a specific IPv4 address.
% Hits	This shows the percentage of the hit counts for the virus sent by all or a specific IPv4 address.
Intrusion Detection / Prevention The following fields are displayed when you select **Intrusion Detection / Prevention**. The donut chart shows the number of potential network attacks detected by the Intrusion Detection and Prevention (IDP) service, if any. The number in the center of the donut chart indicates the number of network attacks blocked by the IDP service.	
Signature Name	The name of the IDP signature that triggered the hit. The signature name identifies the type of intrusion pattern
Hits	This shows the total number of network attacks blocked by the IDP service.
% Hits	This shows the number of network attacks blocked as a percentage of the total number of network requests scanned by the IDP service.

9.2.4 Summary Report

This screen displays network statistics for the Nebula Device of the selected site, such as WAN usage, top applications and/or top clients.

Click **Site-wide** > **Monitor** > **Security gateway** > **Summary report** to access this screen.

Figure 205 Site-wide > Monitor > Security gateway > Summary report



WAN1 Usage (Total 4.46 GB 674.87 MB 3.80 GB)

WAN2 Usage (Total 0 bytes 0 bytes 0 bytes)

There are no usages for the selected period.

VPN Usage (Total 67.21 MB 19.45 MB 47.76 MB)

Security gateway by usage

	Name	Model	Usage	Client
1	NSGWEB	NSG50	4.46 GB	6

Location

Top applications by usage

		Application	Category	Usage	% Usage
1	🟩	SSL/TLS	Network protocols	987.17 MB	38.69%
2	🟩	Facebook	Social networks	941.23 MB	36.89%
3	🟩	Dropbox	File sharing services and tools	108.43 MB	4.25%
4	🟦	WhatsApp	Instant messengers	78.36 MB	3.07%
5	🟦	Microsoft Office 365	Business tools	77.16 MB	3.02%
6	🟦	Google Play	Web services	66.85 MB	2.62%
7	🟥	SMB2	Management tools and protocols	49.84 MB	1.95%
8	🟧	Spotify	Media streaming services	39.13 MB	1.53%
9	🟨	Microsoft(SSL)	Network protocols	29.19 MB	1.14%
10	🟨	Microsoft Office	Business tools	23.06 MB	0.90%

Top ports by usage

Name	Usage	% Usage
HTTPS (TCP, Port 443)	3.67 GB	84.92%
OTHERS (UDP, Port 3480)	317.30 MB	7.17%
OTHERS (UDP, Port 10664)	71.76 MB	1.62%
OTHERS (UDP, Port 19410)	61.11 MB	1.38%
OTHERS (TCP, Port 445)	45.52 MB	1.03%
OTHERS (UDP, Port 13632)	36.21 MB	0.82%
OTHERS (TCP, Port 4335)	33.62 MB	0.76%
WWW (TCP, Port 80)	15.08 MB	0.34%
OTHERS (TCP, Port 5938)	13.66 MB	0.31%
IRCD (TCP, Port 6667)	11.45 MB	0.26%

Clients per day

Top operating systems by usage

	OS	# Client	% Client	Usage	% Usage
1	Other	5	62.50%	2.67 GB	62.45%
2	Windows 7 or ...	2	25.00%	1.61 GB	37.51%
3	Linux	1	12.50%	1.81 MB	0.04%

Top clients by usage

	Description	Usage	% Usage
1	Bayardo Cell	2.33 GB	54.32%
2	Laptop	1.55 GB	36.32%
3	Bayardo Cell	311.05 MB	7.10%
4	Laptop	52.12 MB	1.19%
5	[redacted]	33.62 MB	0.77%
6	MyNAP102	11.75 MB	0.27%
7	NS	1.81 MB	0.04%
8	usg60w	0 bytes	0.00%

Top client device manufacturers by usage

	Manufactur...	# Client	% Client	Usage	% Usage
1	Xiaomi Comm...	1	12.50%	2.63 GB	61.42%
2	Intel Corporate	1	12.50%	1.61 GB	37.51%
3	Zyxel Commu...	3	37.50%	45.38 MB	1.04%
4	Nintendo Co.,...	1	12.50%	1.81 MB	0.04%

The following table describes the labels in this screen.

Table 146 Site-wide > Monitor > Security gateway > Summary report

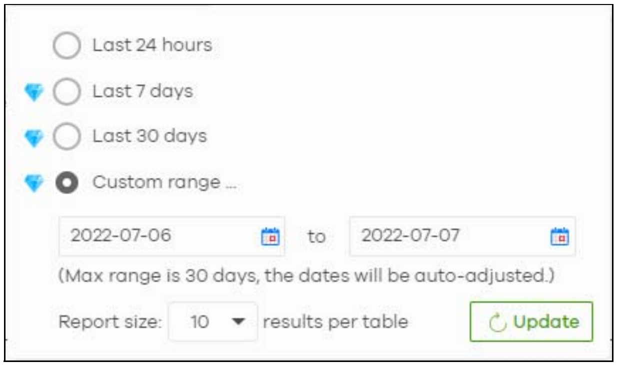
LABEL	DESCRIPTION
Security gateway – Summary report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ○ Last 7 days ○ Last 30 days ● Custom range ... 2022-07-06 to 2022-07-07 (Max range is 30 days, the dates will be auto-adjusted.) Report size: 10 results per table Update
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
WAN1/WAN2 usage	
y-axis	The y-axis shows the transmission speed of data sent or received through the WAN connection in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
VPN usage	
y-axis	The y-axis shows the transmission speed of data sent or received through the VPN tunnel in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Security gateway by usage	
	This shows the index number of the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Usage	This shows the amount of data that has been transmitted through the Nebula Device's WAN port.
Client	This shows the number of clients currently connected to the Nebula Device.
Location This shows the location of the Nebula Devices on the map.	
Top applications by usage	
	This shows the index number of the application.
Application	This shows the application name.
Category	This shows the name of the category to which the application belongs.
Usage	This shows the amount of data consumed by the application.
% Usage	This shows the percentage of usage for the application.
Top ports by usage	This shows the top ten applications/services and the ports that identify a service.
Name	This shows the service name and the associated port numbers.
Usage	This shows the amount of data consumed by the service.
% Usage	This shows the percentage of usage for the service.

Table 146 Site-wide > Monitor > Security gateway > Summary report (continued)

LABEL	DESCRIPTION
Clients per day	
y-axis	The y-axis represents the number of clients.
x-axis	The x-axis represents the date.
Top operating systems by usage	
	This shows the index number of the operating system.
OS	This shows the operating system of the client device.
# Client	This shows how many client devices use this operating system.
% Client	This shows the percentage of top client devices which use this operating system.
# Usage	This shows the amount of data consumed by the client device on which this operating system is running.
% Usage	This shows the percentage of usage for top client devices which use this operating system.
Top clients by usage	
	This shows the index number of the client.
Description	This shows the descriptive name or MAC address of the client.
Usage	This shows the total amount of data transmitted and received by the client.
% Usage	This shows the percentage of usage for the client.
Top client device manufacturers by usage	
	This shows the index number of the client device.
Manufacturer	This shows the manufacturer name of the client device.
Client	This shows how many client devices are made by the manufacturer.
% Client	This shows the percentage of top client devices which are made by the manufacturer.
Usage	This shows the total amount of data transmitted and received by the client device.
% Usage	This shows the percentage of usage for the client device.

9.3 Configure

Use the **Configure** menus to configure interface addressing, firewall, site-to-site VPN, captive portal, traffic shaping, authentication server and other Nebula Device settings for the Nebula Device of the selected site.

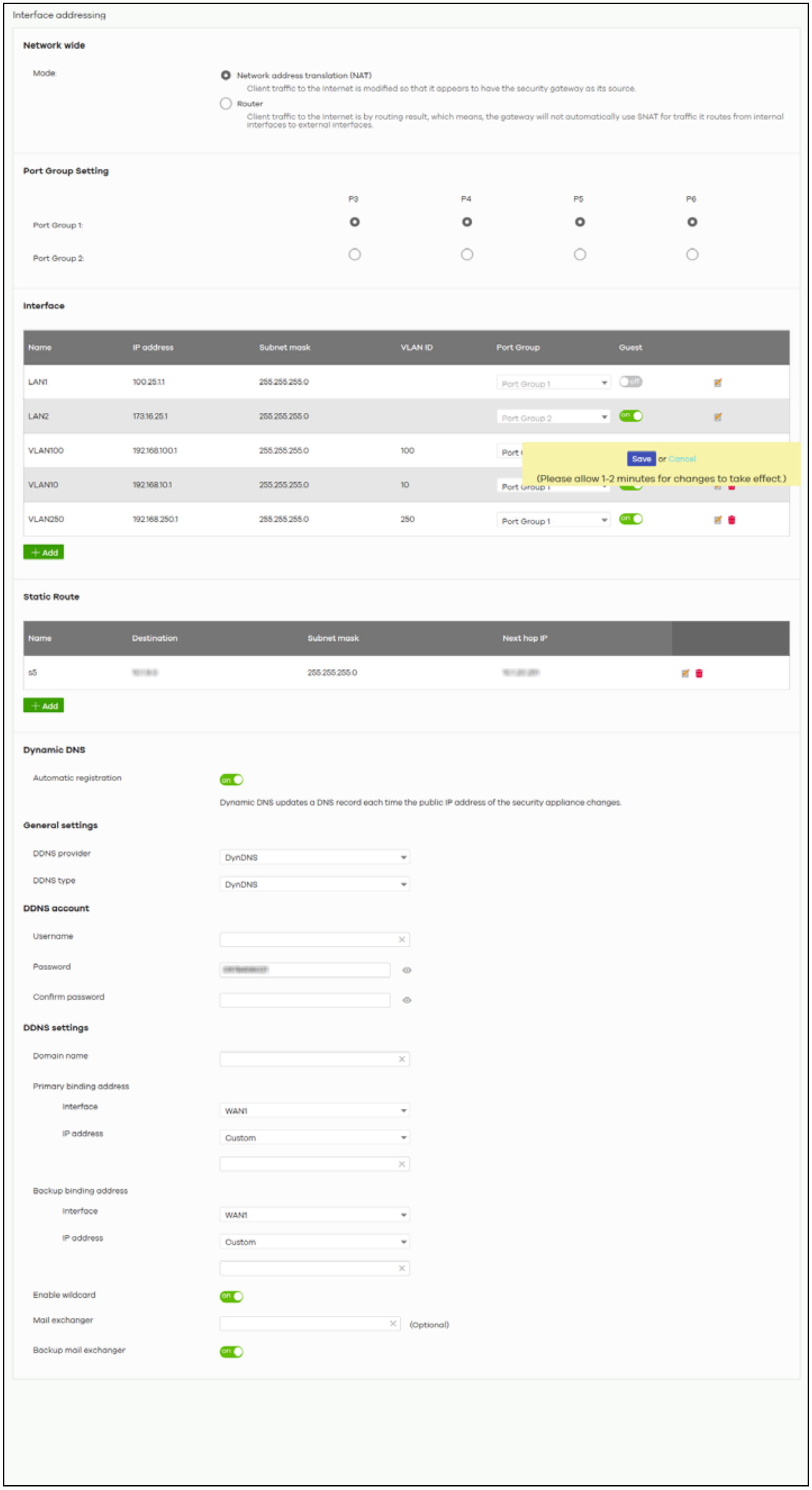
Note: Only one Security Appliance is allowed per site.

9.3.1 Interface Addressing

Use this screen to configure network mode, port grouping, interface address, static route and DDNS settings on the Nebula Device. To access this screen, click **Site-wide** > **Configure** > **Security gateway** > **Interface addressing**.

Note: If the gateway device of the site supports link aggregation, for example model NSG300, then the **Interface addressing** screen changes to allow you to configure link aggregation groups. For details, see Section 9.3.5 on page 607.

Figure 206 Site-wide > Configure > Security gateway > Interface addressing



Interface addressing

Network wide

Mode:

● Network address translation (NAT)
Client traffic to the Internet is modified so that it appears to have the security gateway as its source.

○ Router
Client traffic to the Internet is by routing result, which means, the gateway will not automatically use SNAT for traffic it routes from internal interfaces to external interfaces.

Port Group Setting

	P3	P4	P5	P6
Port Group 1:	●	●	●	●
Port Group 2:	○	○	○	○

Interface

Name	IP address	Subnet mask	VLAN ID	Port Group	Guest	
LAN1	100.25.1.1	255.255.255.0		Port Group 1	off	
LAN2	173.16.25.1	255.255.255.0		Port Group 2	on	
VLAN100	192.168.100.1	255.255.255.0	100	Port		
VLAN10	192.168.10.1	255.255.255.0	10	Port Group 1		
VLAN250	192.168.250.1	255.255.255.0	250	Port Group 1	on	

Save or Cancel
(Please allow 1-2 minutes for changes to take effect.)

+ Add

Static Route

Name	Destination	Subnet mask	Next hop IP	
s5	[redacted]	255.255.255.0	[redacted]	

+ Add

Dynamic DNS

Automatic registration: on

Dynamic DNS updates a DNS record each time the public IP address of the security appliance changes.

General settings

DDNS provider: DynDNS

DDNS type: DynDNS

DDNS account

Username:

Password: [redacted]

Confirm password:

DDNS settings

Domain name:

Primary binding address

Interface: WAN1

IP address: Custom

Backup binding address

Interface: WAN1

IP address: Custom

Enable wildcard: on

Mail exchanger: (Optional)

Backup mail exchanger: on

The following table describes the labels in this screen.

Table 147   Site-wide > Configure > Security gateway > Interface addressing

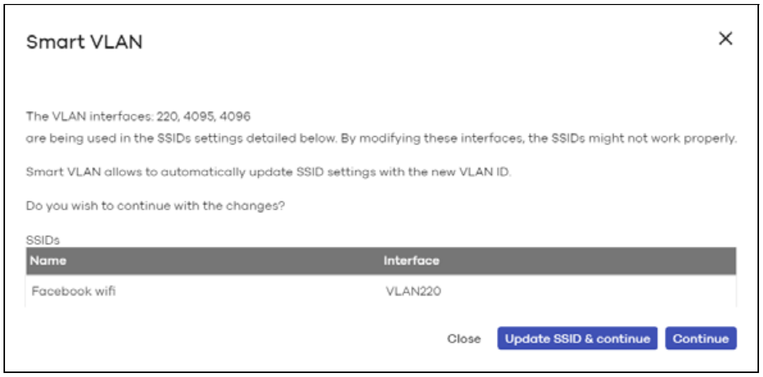
LABEL	DESCRIPTION
Network wide	
Mode	Select **Network address translation (NAT)** to have the Nebula Device automatically use SNAT for traffic it routes from internal interfaces to external interfaces. Select **Router** to have the Nebula Device forward packets according to the routing policies. The Nebula Device does not automatically convert a packet's source IP address.
Port Group Setting	Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level. The physical LAN Ethernet ports are shown at the top (P3, P4, and so on) and the port groups are shown at the left of the screen. Use the radio buttons to select which ports are in each port group. For example, select a port's **Port Group 1** radio button to use the port as part of the first port group. The port will use the first group's IP address. Note: You cannot select ports 1 and 2, as these ports are reserved for WAN usage.
Interface By default, LAN1 is created on top of port group 1 and LAN2 is on top of port group 2.	
Name	This shows the name of the interface (network) on the Nebula Device.
IP address	This shows the IP address of the interface (network).
Subnet mask	This shows the subnet mask of the interface (network).
VLAN ID	This shows the ID number of the VLAN with which the interface (network) is associated. If you have associated an SSID with the VLAN ID, the **Smart VLAN** screen displays after you change or delete the VLAN ID and click **Save**. You can exit the screen without saving, or apply your changes directly. If the **Smart guest/VLAN network** feature is enabled in the **Site-wide** > **Configure** > **Site settings** screen, you can select to apply the changes and update the SSID's VLAN setting as well.  Smart VLAN The VLAN interfaces: 220, 4095, 4096 are being used in the SSIDs settings detailed below. By modifying these interfaces, the SSIDs might not work properly. Smart VLAN allows to automatically update SSID settings with the new VLAN ID. Do you wish to continue with the changes? SSIDs Name: Facebook wifi — Interface: VLAN220
Port group	This shows the name of the port group to which the interface (network) belongs.

Table 147 Site-wide > Configure > Security gateway > Interface addressing (continued)

LABEL	DESCRIPTION
Guest	Click the switch to the right to configure this interface as a Guest interface. Client devices connected to this Guest interface have Internet access but cannot access a non-guest interface. Alternatively, click the switch to the left to disable Internet access for client devices connected to this Guest interface. Note: If the **Smart guest/VLAN network** feature is enabled in the **Site-wide** > **Configure** > **Site settings** screen, the guest settings you configure for an interface also apply to the WiFi networks (SSIDs) associated with the same VLAN ID. For example, if you set an interface in VLAN 100 as a guest interface, the SSID that belongs to VLAN 100 will also act as a guest network.
✎	Click this button to modify the network settings. See Section 9.3.1.1 on page 589 for detailed information.
🗑	Click this icon to remove a VLAN entry.
Add	Click this button to create a VLAN, which is then associated with one Ethernet interface (network). See Section 9.3.1.1 on page 589 for detailed information.
Static Route	
Name	This shows the name of the static route.
Destination	This shows the destination IP address.
Subnet mask	This shows the IP subnet mask.
Next hop IP	This shows the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your Nebula Device's interfaces. It helps forward packets to their destinations.
✎	Click this button to modify the static route settings. See Section 9.3.2.4 on page 598 for detailed information.
🗑	Click this icon to remove a static route.
Add	Click this button to create a new static route. See Section 9.3.2.4 on page 598 for detailed information.
Dynamic DNS	
Automatic registration	Click **On** to use dynamic DNS. Otherwise, select **Off** to disable it.
General Settings	
DDNS provider	Select your Dynamic DNS service provider from the drop-down list box. If you select **User custom**, create your own DDNS service.
DDNS type	Select the type of DDNS service you are using. Select **User custom** to create your own DDNS service and configure the **DYNDNS Server**, **URL**, and **Additional DDNS Options** fields below.
DDNS account	
Username	Enter the user name used when you registered your domain name.
Password	Enter the password provided by the DDNS provider.
Confirm password	Enter the password again to confirm it.
DDNS settings	
Domain name	Enter the domain name you registered.
Primary binding address	Use these fields to set how the Nebula Device determines the IP address that is mapped to your domain name in the DDNS server. The Nebula Device uses the **Backup binding address** if the interface specified by these settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name.

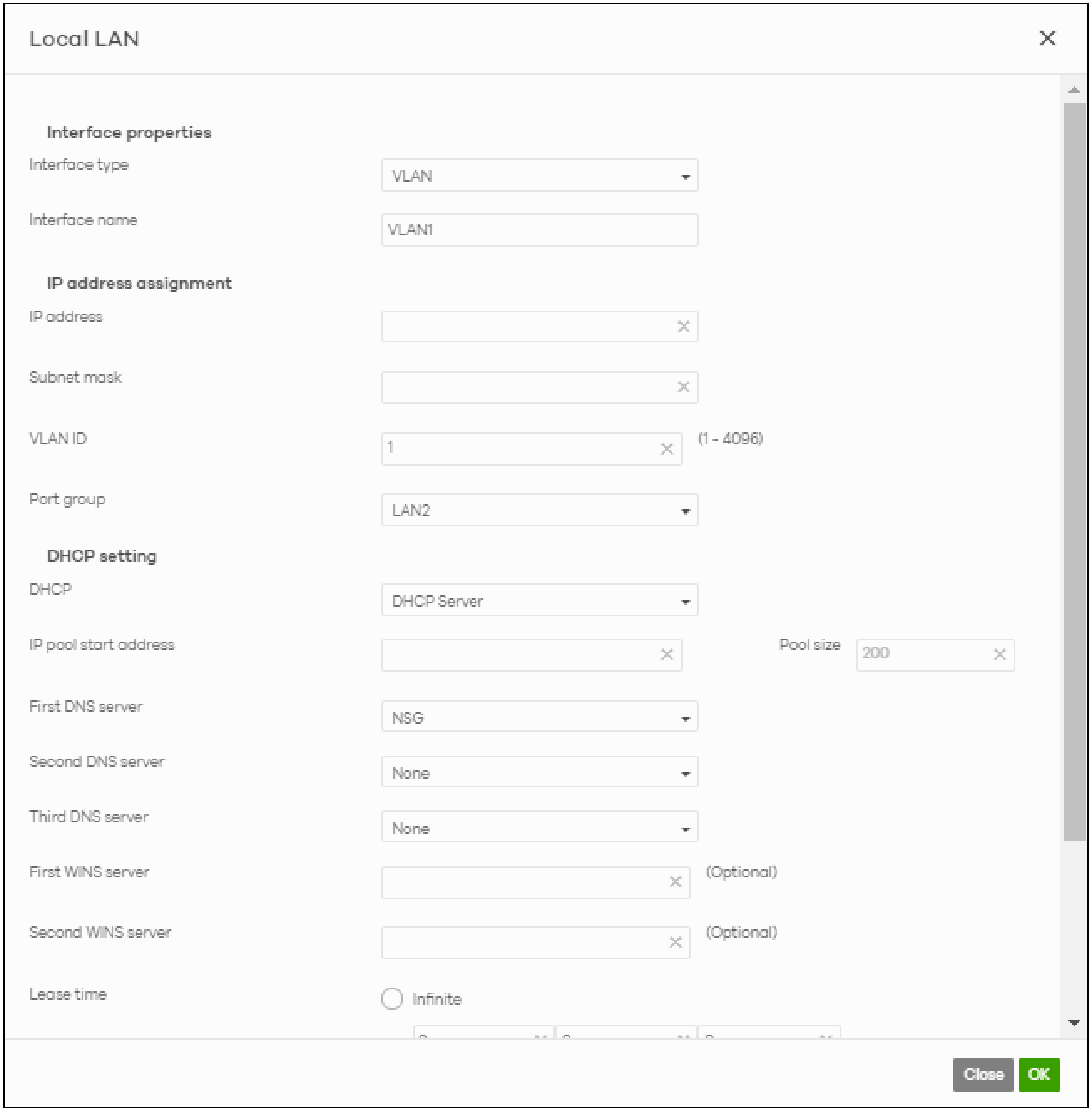
Table 147 Site-wide > Configure > Security gateway > Interface addressing (continued)

LABEL	DESCRIPTION
IP address	Select **Auto** if the interface has a dynamic IP address. The DDNS server checks the source IP address of the packets from the Nebula Device for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the Nebula Device and the DDNS server. Note: The Nebula Device may not determine the proper IP address if there is an HTTP proxy server between the Nebula Device and the DDNS server. Select **Custom** if you have a static IP address. Enter the IP address to use it for the domain name. Select **Interface** to have the Nebula Device use the IP address of the specified interface.
Backup binding address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the **Primary binding address** settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name.
IP address	Select **Auto** if the interface has a dynamic IP address. The DDNS server checks the source IP address of the packets from the Nebula Device for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the Nebula Device and the DDNS server. Note: The Nebula Device may not determine the proper IP address if there is an HTTP proxy server between the Nebula Device and the DDNS server. Select **Custom** if you have a static IP address. Enter the IP address to use it for the domain name. Select **Interface** to have the Nebula Device use the IP address of the specified interface.
Enable wildcard	This option is only available with a DynDNS account. Enable the wildcard feature to alias sub-domains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.
Mail exchanger	This option is only available with a DynDNS account. DynDNS can route email for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes email for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger. If you are using this service, type the host record of your mail server here. Otherwise, leave the field blank.
Backup mail exchanger	This option is only available with a DynDNS account. Select this checkbox if you are using DynDNS's backup service for email. With this service, DynDNS holds onto your email if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. See www.dyndns.org for more information about this service.
DYNDNS Server	This field displays when you select **User custom** from the **DDNS provider** field above. Enter the IP address of the server that will host the DDNS service.
URL	This field displays when you select **User custom** from the **DDNS provider** field above. Enter the URL that can be used to access the server that will host the DDNS service.
Additional DDNS Options	This field displays when you select **User custom** from the **DDNS provider** field above. These are the options supported at the time of writing: • dyndns_system to specify the DYNDNS Server type – for example, dyndns@dyndns.org • ip_server_name which should be the URL to get the server's public IP address – for example, http://myip.easylife.tw/

9.3.1.1 Local LAN (Add VLAN)

Click the **Add** button or click the **Edit** button in the **Interface** section of the **Site-wide** > **Configure** > **Security gateway** > **Interface addressing** screen.

Figure 207 Site-wide > Configure > Security gateway > Interface addressing: Local LAN (VLAN)



Local LAN

Interface properties

Interface type	VLAN	
Interface name	VLAN1	

IP address assignment

IP address		
Subnet mask		
VLAN ID	1	(1 - 4096)
Port group	LAN2	

DHCP setting

DHCP	DHCP Server		
IP pool start address		Pool size	200
First DNS server	NSG		
Second DNS server	None		
Third DNS server	None		
First WINS server		(Optional)	
Second WINS server		(Optional)	
Lease time	○ Infinite		

The following table describes the labels in this screen.

Table 148 Site-wide > Configure > Security gateway > Interface addressing: Local LAN (VLAN)

LABEL	DESCRIPTION
Interface properties	
Interface type	Select VLAN to add a virtual interface. Note: This field only appears if the Nebula Device supports Link Aggregation Groups (LAGs). If the Nebula Device does not support LAGs, then VLAN is the default interface type.
Interface name	This field is read-only if you are editing an existing interface. Specify a name for the interface. The format of interface names is strict. Each name consists of 2 – 4 letters (interface type), followed by a number (x). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, VLAN interfaces are vlan0, vlan1, vlan2, and so on.
IP address assignment	
IP address	Enter the IP address for this interface.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.) Note: NCC will show an error message when the VLAN ID in the NSG interface is configured to be the same as the WAN port's VLAN ID.
Port group	Select the name of the port group to which you want the interface (network) to belong.
DHCP setting	
DHCP	Select what type of DHCP service the Nebula Device provides to the network. Choices are: **None** – the Nebula Device does not provide any DHCP service. There is already a DHCP server on the network. **DHCP Relay** – the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network. **DHCP Server** – the Nebula Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Nebula Device is the DHCP server for the network.
These fields appear if the Nebula Device is a **DHCP Relay**.	
Relay server 1	Enter the IP address of a DHCP server for the network.
Relay server 2	This field is optional. Enter the IP address of another DHCP server for the network.
These fields appear if the Nebula Device is a **DHCP Server**.	
IP pool start address	Enter the IP address from which the Nebula Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add new** under **Static DHCP Table**.
Pool size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet mask**. For example, if the **Subnet mask** is 255.255.255.0 and **IP pool start address** is 10.10.10.10, the Nebula Device can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.

Table 148 Site-wide > Configure > Security gateway > Interface addressing: Local LAN (VLAN)

LABEL	DESCRIPTION
First DNS server Second DNS server Third DNS server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** – enter a static IP address. **From ISP** – select the DNS server that another interface received from its DHCP server. **NSG** – the DHCP clients use the IP address of this interface and the Nebula Device works as a DNS relay.
First WINS server Second WINS server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** – select this if IP addresses never expire. **days, hours, minutes** – select this to enter how long IP addresses are valid.
Extended options	This table is available if you selected **DHCP server**. Configure this table if you want to send more information to DHCP clients through DHCP packets. Click **Add new** to create an entry in this table. See Section 9.3.2.3 on page 596 for detailed information.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.
	Click the edit icon to modify it. Click the remove icon to delete it.
Static DHCP Table	Configure a list of static IP addresses the Nebula Device assigns to computers connected to the interface. Otherwise, the Nebula Device assigns an IP address dynamically using the interface's **IP pool start address** and **Pool size**. Click **Add new** to create an entry in this table.
IP address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

9.3.2 Link Aggregation Groups

A Link Aggregation Group (LAG) combines multiple Ethernet ports into a single logical interface, in order to increase network bandwidth and/or availability.

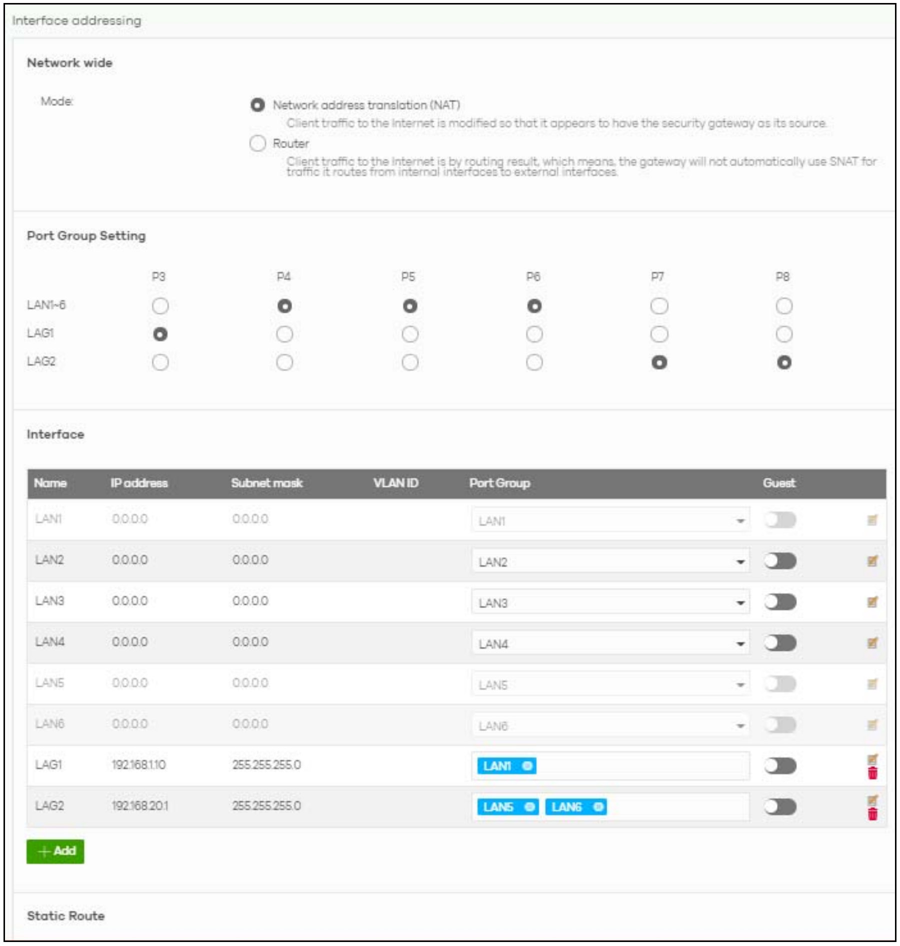
Ports in the group can all connect to a target simultaneously, combining their bandwidth. A LAG can also offer higher network availability; if any port in the group becomes disconnected, the LAG can continue sending data using another port.

9.3.2.1 Interface Addressing with Link Aggregation Groups

If the Nebula Device of the selected site supports Link Aggregation Groups (LAGs), for example NSG300, you can create a LAG by clicking **Add**.

After you create a LAG, the **Port Group Settings** and **Interface** sections of the **Interface addressing** screen change. The new screen layout allows you to view and configure which ports are in a LAG.

Figure 208 Site-wide > Configure > Security gateway > Interface addressing (LAG Interface Type)



Interface addressing

Network wide

Mode: ● Network address translation (NAT)
Client traffic to the Internet is modified so that it appears to have the security gateway as its source.
○ Router
Client traffic to the Internet is by routing result, which means, the gateway will not automatically use SNAT for traffic it routes from internal interfaces to external interfaces.

Port Group Setting

	P3	P4	P5	P6	P7	P8
LAN1~6	○	●	●	●	○	○
LAG1	●	○	○	○	○	○
LAG2	○	○	○	○	●	●

Interface

Name	IP address	Subnet mask	VLAN ID	Port Group	Guest
LAN1	0.0.0.0	0.0.0.0		LAN1	
LAN2	0.0.0.0	0.0.0.0		LAN2	
LAN3	0.0.0.0	0.0.0.0		LAN3	
LAN4	0.0.0.0	0.0.0.0		LAN4	
LAN5	0.0.0.0	0.0.0.0		LAN5	
LAN6	0.0.0.0	0.0.0.0		LAN6	
LAG1	192.168.1.10	255.255.255.0		LAN1	
LAG2	192.168.20.1	255.255.255.0		LAN5 LAN6	

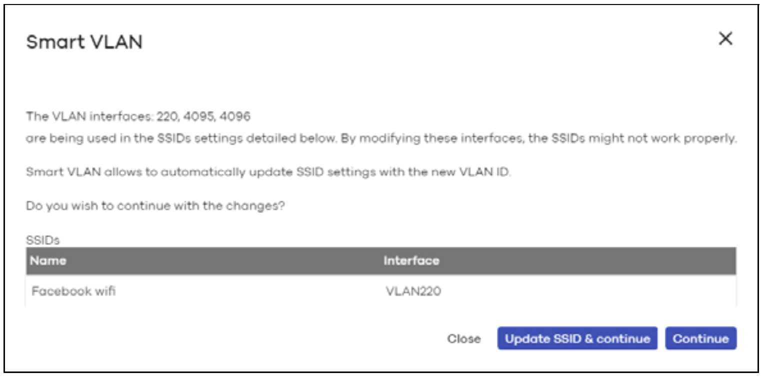
Static Route

The following table describes the labels in this screen.

Table 149 Site-wide > Configure > Security gateway > Interface addressing (LAG Interface Type)

LABEL	DESCRIPTION
Port Group Setting	Select which port group or Link Aggregation Group (LAG) an Ethernet port belongs to. When LAGs are enabled, NCC adds each available LAN Ethernet port (port 3 and higher) to a separate port group, named LAN1, LAN2, LAN3, and so on. These default port groups cannot be modified or renamed.
Interface	
Name	This shows the name of the interface (network) on the Nebula Device.
IP address	This shows the IP address of the interface (network).
Subnet mask	This shows the subnet mask of the interface (network).

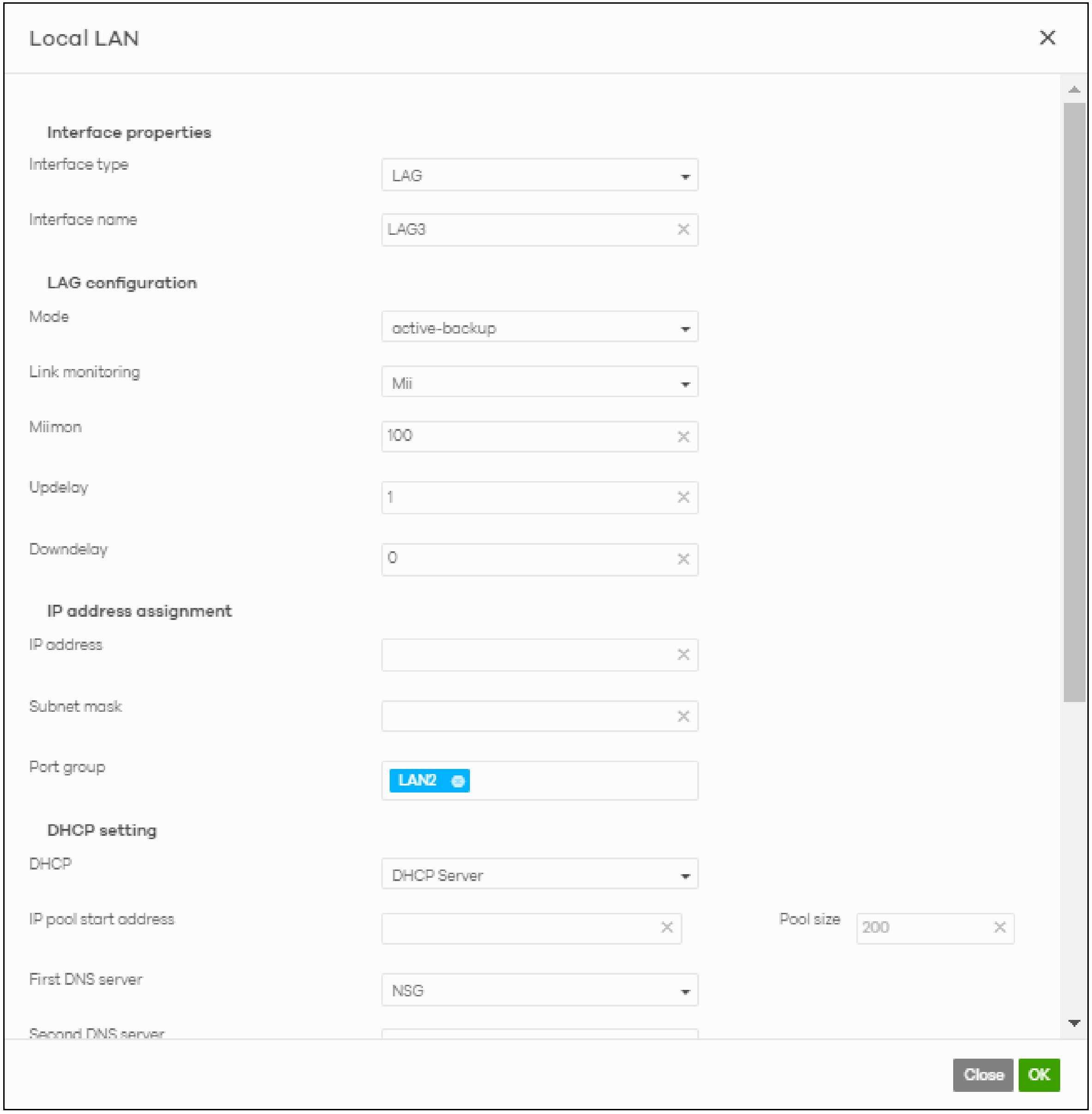
Table 149   Site-wide > Configure > Security gateway > Interface addressing (LAG Interface Type)

LABEL	DESCRIPTION
VLAN ID	This shows the ID number of the VLAN with which the interface (network) is associated. Note: If you have associated an SSID with the VLAN ID, the **Smart VLAN** screen displays after you change or delete the VLAN ID and click **Save**. You can exit the screen without saving, or apply your changes directly. If the **Smart guest/ VLAN network** feature is enabled in the **Site-wide** > **Configure** > **Site settings** screen, you can select to apply the changes and update the SSID's VLAN setting as well.  Smart VLAN The VLAN interfaces: 220, 4095, 4096 are being used in the SSIDs settings detailed below. By modifying these interfaces, the SSIDs might not work properly. Smart VLAN allows to automatically update SSID settings with the new VLAN ID. Do you wish to continue with the changes? SSIDs Name — Interface Facebook wifi — VLAN220
Port group	For an Ethernet port, this shows the name of the port group to which the port belongs. For a link aggregation group, this shows its member port groups.
Guest	Select **On** to configure the interface as a Guest interface. Devices connected to a Guest interface will have Internet access but cannot communicate with each other directly or access network sources behind the Nebula Device. Otherwise, select **Off** to not use the interface as a Guest interface. Note: If the **Smart guest/VLAN network** feature is enabled in the **Site-wide** > **Configure** > **Site settings** screen, the guest settings you configure for an interface also apply to the WiFi networks (SSIDs) associated with the same VLAN ID. For example, if you set an interface in VLAN 100 as a guest interface, the SSID that belongs to VLAN 100 will also act as a guest network.
✎	Click this button to modify the network settings. See Section 9.3.1.1 on page 589 for detailed information. If the interface is a member of a link aggregation group, you cannot edit the interface's network settings.
🗑	Click this icon to delete a VLAN entry or link aggregation group.
Add	Click this button to create a VLAN or link aggregation group. • For details on creating a VLAN, see Section 9.3.1.1 on page 589. • For details on creating a link aggregation group, see Section 9.3.2.2 on page 593.

9.3.2.2 Local LAN (LAG Interface Type)

Click the **Add** button or click the **Edit** button in the **Interface** section of the **Site-wide** > **Configure** > **Security gateway** > **Interface addressing** screen.

Figure 209 Site-wide > Configure > Security gateway > Interface addressing: Local LAN (LAG Interface Type)



Local LAN

Interface properties

Interface type: LAG

Interface name: LAG3

LAG configuration

Mode: active-backup

Link monitoring: Mii

Miimon: 100

Updelay: 1

Downdelay: 0

IP address assignment

IP address:

Subnet mask:

Port group: LAN2

DHCP setting

DHCP: DHCP Server

IP pool start address:

Pool size: 200

First DNS server: NSG

Second DNS server

The following table describes the labels in this screen.

Table 150 Site-wide > Configure > Security gateway > Interface addressing: Local LAN (LAG Interface Type)

LABEL	DESCRIPTION
Interface properties	
Interface type	Select LAG to add a link aggregation group. Note: This field only appears if the Nebula Device supports Link Aggregation Groups (LAGs). If the Nebula Device does not support LAGs, a VLAN is created by default.
Interface name	Specify a name for the interface. This must be "LAG" plus a number, for example "LAG1".

Table 150 Site-wide > Configure > Security gateway > Interface addressing: Local LAN (LAG Interface Type) (continued)

LABEL	DESCRIPTION
LAG Configuration	
Mode	Select a mode for this Link Aggregation Group (LAG) interface. Choices are as follows: • **active-backup**: Only one port in the LAG interface is active and another port becomes active only if the active port fails. • **802.3ad** (IEEE 802.3ad Dynamic link aggregation): Link Aggregation Control Protocol (LACP) negotiates automatic combining of ports and balances the traffic load across the LAG link by sending LACP packets to the directly connected device that also implements LACP. The ports must have the same speed and duplex settings. • **balance-alb** (adaptive load balancing): Traffic is distributed according to the current load on each port by ARP negotiation. Incoming traffic is received by the current port. If the receiving port fails, another port takes over the MAC address of the failed receiving port.
Link Monitoring	Select how each link is monitored. **mii** (Media Independent Interface) – The Nebula Device monitors the state of the local interface only. The Nebula Device cannot tell if the link can transmit or receive packets. **arp** – The Nebula Device monitors the link by sending ARP queries. The Nebula Device then uses the reply to know if the link is up and that traffic is flowing through the link.
Miimom	This field displays for **mii** Link Monitoring. Set the interval in milliseconds that the system polls the Media Independent Interface (MII) to get the link's status.
Updelay	This field displays for **mii** Link Monitoring. Set the waiting time in milliseconds to confirm that a member interface link is up.
Downdelay	This field displays for **mii** Link Monitoring. Set the waiting time in milliseconds to confirm that a member interface link is down.
IP address assignment	
IP address	Enter the IP address for this interface.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.) Note: NCC will show an error message when the VLAN ID in the NSG interface is configured to be the same as the WAN port's VLAN ID.
Port group	Select the name of the port group to which you want the interface (network) to belong.
DHCP setting	
DHCP	Select what type of DHCP service the Nebula Device provides to the network. Choices are: **None** – the Nebula Device does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** – the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network. **DHCP Server** – the Nebula Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Nebula Device is the DHCP server for the network.
These fields appear if the Nebula Device is a **DHCP Relay**.	
Relay server 1	Enter the IP address of a DHCP server for the network.
Relay server 2	This field is optional. Enter the IP address of another DHCP server for the network.
These fields appear if the Nebula Device is a **DHCP Server**.	

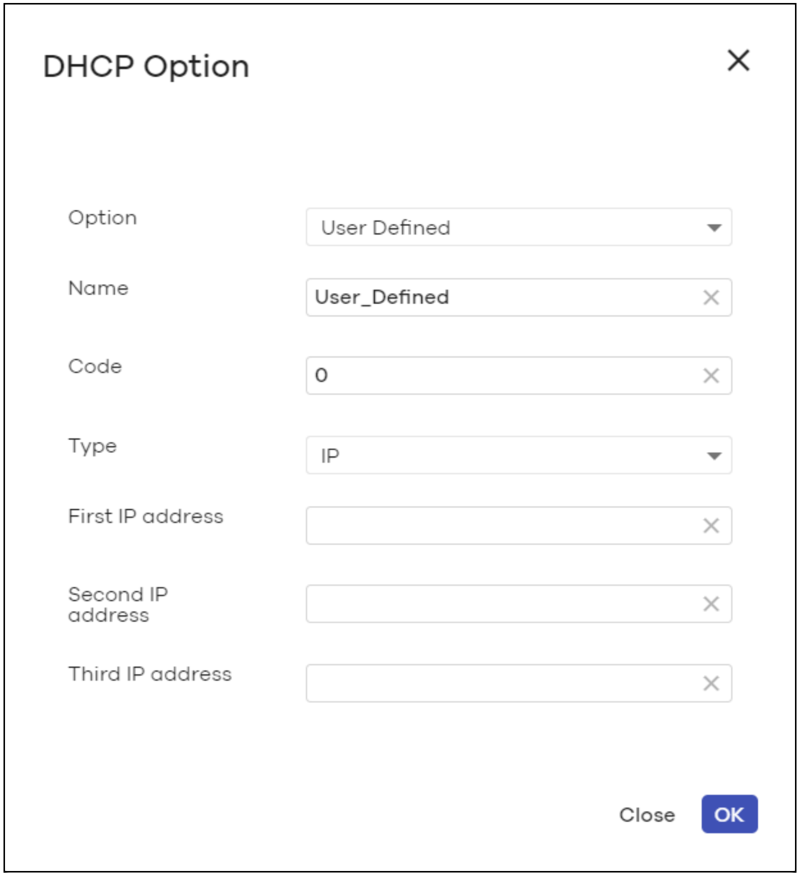
Table 150 Site-wide > Configure > Security gateway > Interface addressing: Local LAN (LAG Interface Type) (continued)

LABEL	DESCRIPTION
IP pool start address	Enter the IP address from which the Nebula Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add new** under **Static DHCP Table**.
Pool size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet mask**. For example, if the **Subnet mask** is 255.255.255.0 and **IP pool start address** is 10.10.10.10, the Nebula Device can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.
First DNS server Second DNS server Third DNS server	Specify the IP addresses of up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** – enter a static IP address. **From ISP** – select the DNS server that another interface received from its DHCP server. **NSG** – the DHCP clients use the IP address of this interface and the Nebula Device works as a DNS relay.
First WINS server Second WINS server	Enter the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** – select this if IP addresses never expire **days, hours, minutes** – select this to enter how long IP addresses are valid.
Extended options	This table is available if you selected **DHCP server**. Configure this table if you want to send more information to DHCP clients through DHCP packets. Click **Add new** to create an entry in this table. See Section 9.3.2.3 on page 596 for detailed information.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.
	Click the edit icon to modify it. Click the remove icon to delete it.
Static DHCP Table	Configure a list of static IP addresses the Nebula Device assigns to computers connected to the interface. Otherwise, the Nebula Device assigns an IP address dynamically using the interface's **IP pool start address** and **Pool size**. Click **Add new** to create an entry in this table.
IP address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

9.3.2.3 DHCP Option

Click the **Add new** button under **Extended options** in the **Site-wide** > **Configure** > **Security gateway** > **Interface addressing: Local LAN** screen.

Figure 210 Site-wide > Configure > Security gateway > Interface addressing: Local LAN: DHCP Option



DHCP Option

Option	User Defined
Name	User_Defined
Code	0
Type	IP
First IP address	
Second IP address	
Third IP address	

The following table describes the labels in this screen.

Table 151 Site-wide > Configure > Security gateway > Interface addressing: Local LAN: DHCP Option

LABEL	DESCRIPTION
Option	Select which DHCP option that you want to add in the DHCP packets sent through the interface.
Name	This field displays the name of the selected DHCP option. If you selected **User_Defined** in the **Option** field, enter a descriptive name to identify the DHCP option.
Code	This field displays the code number of the selected DHCP option. If you selected **User_Defined** in the **Option** field, enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. If you selected **User_Defined** in the **Option** field, select an appropriate type for the value that you will enter in the next field. Misconfiguration could result in interface lockout.
Value	Enter the value for the selected DHCP option. For example, if you selected **TFTP Server Name (66)** and the type is **TEXT**, enter the DNS domain name of a TFTP server here. This field is mandatory.
First IP address Second IP address Third IP address	If you selected **Time Server (4)**, **NTP Server (41)**, **SIP Server (120)**, **CAPWAP AC (138)**, or **TFTP Server (150)**, you have to enter at least one IP address of the corresponding servers in these fields. The servers should be listed in order of your preference.
First enterprise ID Second enterprise ID	If you selected **VIVC (124)** or **VIVS (125)**, you have to enter at least one vendor's 32-bit enterprise number in these fields. An enterprise number is a unique number that identifies a company.

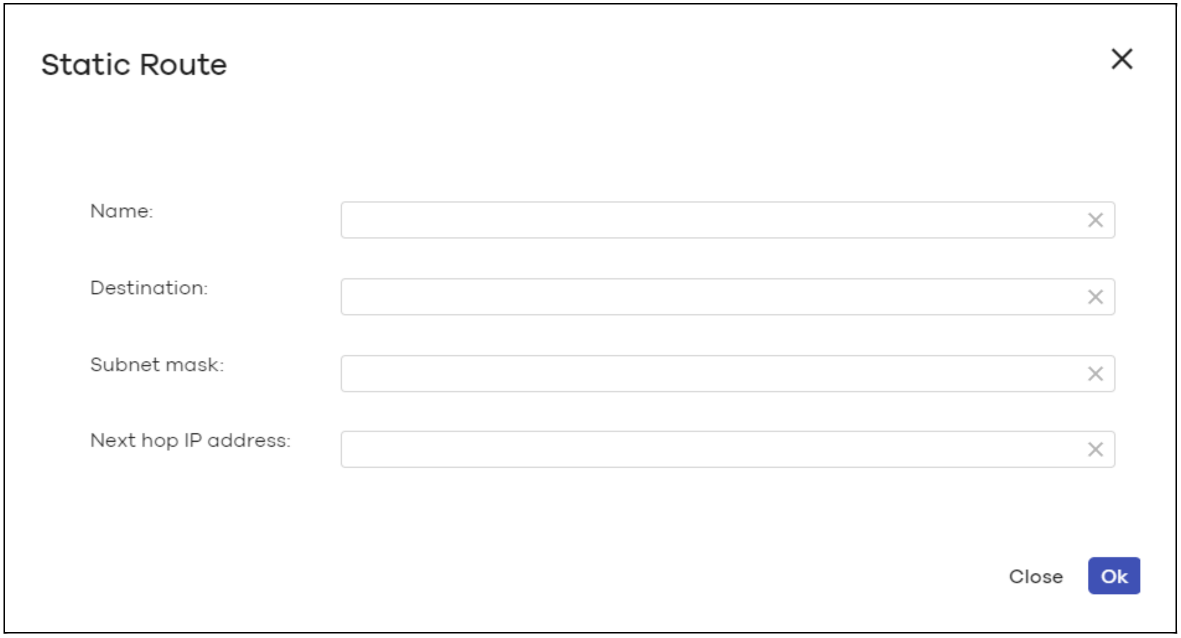
Table 151 Site-wide > Configure > Security gateway > Interface addressing: Local LAN: DHCP Option

LABEL	DESCRIPTION
First class Second class	If you selected **VIVC (124)**, enter the details of the hardware configuration of the host on which the client is running, or of industry consortium compliance.
First information Second information	If you selected **VIVS (125)**, enter additional information for the corresponding enterprise number in these fields.
First FQDN Second FQDN Third FQDN	If the **Type** is **FQDN**, you have to enter at least one domain name of the corresponding servers in these fields. The servers should be listed in order of your preference.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

9.3.2.4 Static Route

Click the **Add** button in the **Static Route** section of the **Site-wide** > **Configure** > **Security gateway** > **Interface addressing** screen.

Figure 211 Site-wide > Configure > Security gateway > Interface addressing: Static Route



The following table describes the labels in this screen.

Table 152 Site-wide > Configure > Security gateway > Interface addressing: Static Route

LABEL	DESCRIPTION
Name	Enter a descriptive name for this route.
Destination	Specifies the IP network address of the final destination. Routing is always based on network number.
Subnet mask	Enter the IP subnet mask.
Next hop IP address	Enter the IP address of the next-hop gateway.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

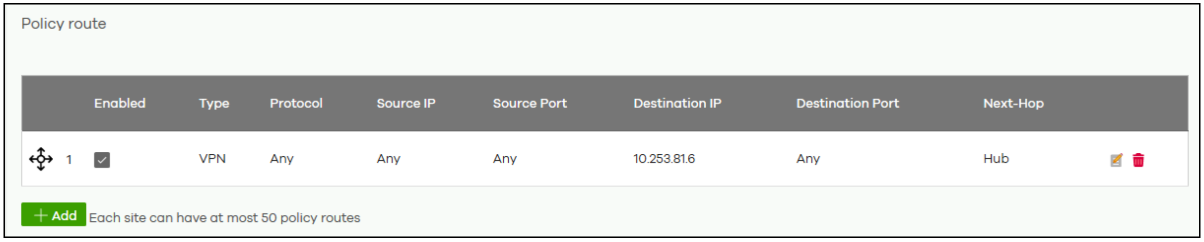
9.3.3 Policy Route

Use policy routes and static routes to override the Nebula Device's default routing behavior in order to send packets through the appropriate next-hop gateway, interface or VPN tunnel.

A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. Use this screen to configure policy routes.

Click **Site-wide** > **Configure** > **Security gateway** > **Policy route** to access this screen.

Figure 212 Site-wide > Configure > Security gateway > Policy route



Policy route

		Enabled	Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	Next-Hop	
✥	1	☑	VPN	Any	Any	Any	10.253.81.6	Any	Hub	✎ 🗑

+ Add Each site can have at most 50 policy routes

The following table describes the labels in this screen.

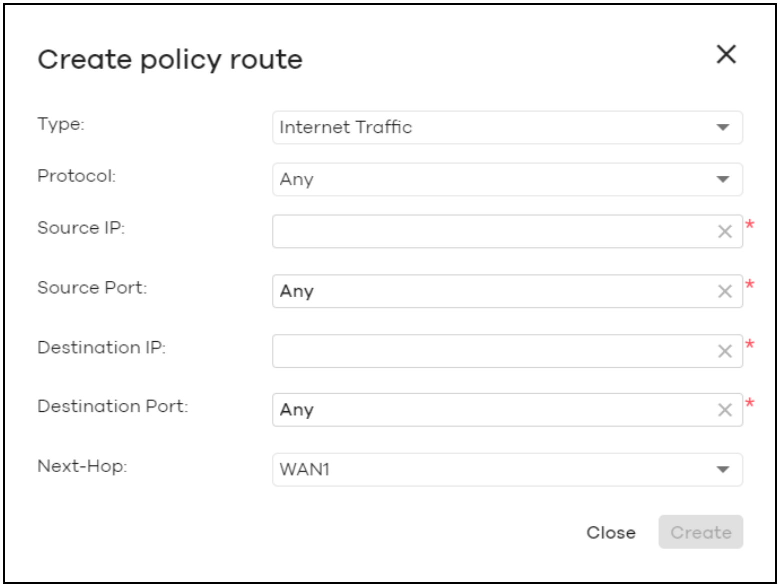
Table 153 Site-wide > Configure > Security gateway > Policy route

LABEL	DESCRIPTION
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Type	This shows whether the packets will be routed to a different gateway (**INTRANET**), VPN tunnel (**VPN**) or outgoing interface (**INTERNET**).
Protocol	This displays the IP protocol that defines the service used by the packets. **Any** means all services.
Source IP	This is the source IP addresses from which the packets are sent.
Source Port	This displays the port that the source IP addresses are using in this policy route rule. The gateway applies the policy route to the packets sent from the corresponding service port. **Any** means all service ports.
Destination IP	This is the destination IP addresses to which the packets are transmitted.
Destination Port	This displays the port that the destination IP addresses are using in this policy route rule. **Any** means all service ports.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel or outgoing interface.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this button to create a new policy route. See Section 9.3.4.1 on page 605 for more information.

9.3.3.1 Add/Edit policy route

Click the **Add** button or an edit icon in the **Site-wide** > **Configure** > **Security gateway** > **Policy route** screen to access this screen.

Figure 213 Site-wide > Configure > Security gateway > Policy route: Add/Edit



Create policy route

Type: Internet Traffic

Protocol: Any

Source IP:

Source Port: Any

Destination IP:

Destination Port: Any

Next-Hop: WAN1

The following table describes the labels in this screen.

Table 154 Site-wide > Configure > Security gateway > Policy Route: Add/Edit

LABEL	DESCRIPTION
Type	Select **Internet Traffic** to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface). Select **Intranet Traffic** to route the matched packets to the next-hop router or switch you specified in the **Next-Hop** field. Select **VPN Traffic** to route the matched packets through the VPN tunnel you specified in the **Next-Hop** field.
Protocol	Select **TCP** or **UDP** if you want to specify a protocol for the policy route. Otherwise, select **Any**.
Source IP	Enter a source IP address from which the packets are sent.
Source Port	Enter the port number (1 – 65535) from which the packets are sent. The Nebula Device applies the policy route to the packets sent from the corresponding service port. **Any** means all service ports.
Destination IP	Enter a destination IP address to which the packets go.
Destination Port	Enter the port number (1 – 65535) to which the packets go. The Nebula Device applies the policy route to the packets that go to the corresponding service port. **Any** means all service ports.
Next-Hop	If you select **Internet Traffic** in the **Type** field, select the WAN interface to route the matched packets through the specified outgoing interface to a Nebula Device connected to the interface. If you select **Intranet Traffic** in the **Type** field, enter the IP address of the next-hop router or switch. If you select **VPN Traffic** in the **Type** field, select the remote VPN gateway's site name.
Close	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

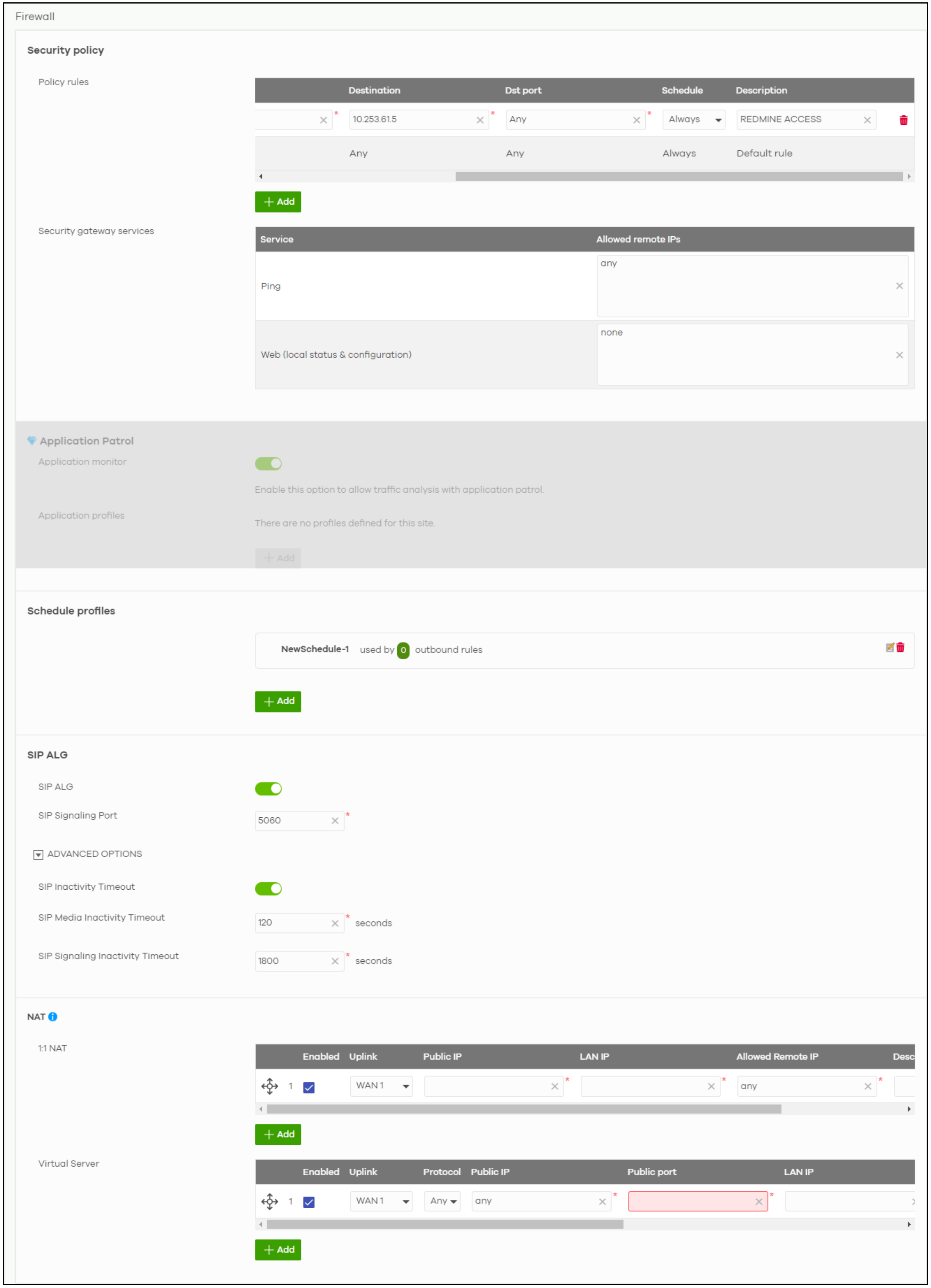
9.3.4 Firewall

By default, a LAN user can initiate a session from within the LAN and the Nebula Device allows the response. However, the Nebula Device blocks incoming traffic initiated from the WAN and destined for the LAN. Use this screen to configure firewall rules for outbound traffic, application patrol, schedule profiles and port forwarding rules for inbound traffic.

Click **Site-wide** > **Configure** > **Security gateway** > **Firewall** to access this screen.

Note: The Nebula Device has the following hidden default firewall rules: LAN to WAN is allowed, WAN to LAN is blocked.

Figure 214 Site-wide > Configure > Security gateway > Firewall



Firewall

Security policy

Policy rules

	Destination	Dst port	Schedule	Description	
× *	10.253.61.5 × *	Any × *	Always ▾	REDMINE ACCESS ×	🗑
	Any	Any	Always	Default rule	

+ Add

Security gateway services

Service	Allowed remote IPs
Ping	any ×
Web (local status & configuration)	none ×

Application Patrol

Application monitor

Enable this option to allow traffic analysis with application patrol.

Application profiles

There are no profiles defined for this site.

+ Add

Schedule profiles

NewSchedule-1 used by 0 outbound rules

+ Add

SIP ALG

SIP ALG

SIP Signaling Port 5060 × *

ADVANCED OPTIONS

SIP Inactivity Timeout

SIP Media Inactivity Timeout 120 × * seconds

SIP Signaling Inactivity Timeout 1800 × * seconds

NAT

1:1 NAT

	Enabled	Uplink	Public IP	LAN IP	Allowed Remote IP	Desc
✥ 1	☑	WAN 1 ▾	× *	× *	any × *	

+ Add

Virtual Server

	Enabled	Uplink	Protocol	Public IP	Public port	LAN IP
✥ 1	☑	WAN 1 ▾	Any ▾	any ×	× *	

+ Add

The following table describes the labels in this screen.

Table 155   Site-wide > Configure > Security gateway > Firewall

LABEL	DESCRIPTION
Security Policy	
Policy rules	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Policy	Select what the Nebula Device is to do with packets that match this rule. Select **Deny** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Allow** to permit the passage of the packets. Select a pre-defined application patrol profile to have the Nebula Device take the action set in the profile when traffic matches the application patrol signatures. See Section 9.3.4.1 on page 605 for how to create an application patrol profile.
Protocol	Select the IP protocol to which this rule applies. Choices are: **TCP**, **UDP**, and **Any**.
Source	Specify the source IP addresses to which this rule applies. You can specify multiple IP addresses or subnets in the field separated by a comma (","). Enter **any** to apply the rule to all IP addresses.
Destination	Specify the destination IP addresses or subnet to which this rule applies. You can specify multiple IP addresses or subnets in the field separated by a comma (","). Enter **any** to apply the rule to all IP addresses.
Dst Port	Specify the destination ports to which this rule applies. You can specify multiple ports separated by a comma (","). Enter **any** to apply the rule to all ports.
Schedule	Select the name of the schedule profile that the rule uses. **Always** means the rule is active at all times if enabled.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the rule.
🗑	Click this icon to remove the rule.
Add	Click this button to create a new rule.
Security gateway services	
Service	This shows the name of the service.
Allowed remote IPs	Specify the IP address or a range of IP addresses (CIDR) with which the computer is allowed to access the Nebula Device using the service. **Any** allows all IP addresses.
Application Patrol	
Application monitor	Click **On** to enable traffic analysis for all applications and display information about the top 10 applications in the **Site-wide** > **Dashboard: Traffic summary** screen. Otherwise, select **Off** to disable traffic analysis for applications.
Application profiles	
Name	This shows the name of the application patrol profile.
Description	This shows the description of the application patrol profile.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this button to create a new application patrol profile. See Section 9.3.4.1 on page 605 for more information.
Schedule profiles	
	This shows the name of the schedule profile and the number of the outbound rules that are using this schedule profile.

Table 155 Site-wide > Configure > Security gateway > Firewall (continued)

LABEL	DESCRIPTION
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this button to create a new schedule profile. See Section 9.3.4.2 on page 606 for more information.
SIP ALG	
SIP ALG	Session Initiation Protocol (SIP) is an application-layer protocol that can be used to create voice and multimedia sessions over the Internet. Application Layer Gateway (ALG) allows the following applications to operate properly through the Nebula Device's NAT. Turn **on** the SIP ALG to detect SIP traffic and help build SIP sessions through the Nebula Device's NAT. Enabling the SIP ALG also allows you to use the application patrol to detect SIP traffic and manage the SIP traffic's bandwidth.
SIP Signaling Port	If you are using a custom UDP port number (not **5060**) for SIP traffic, enter it here.
ADVANCED OPTIONS	
SIP Inactivity Timeout	Select this option to have the Nebula Device apply SIP media and signaling inactivity time out limits.
SIP Media Inactivity Timeout	Use this field to set how many **seconds** (**1** – **86400**) the Nebula Device will allow a SIP session to remain idle (without voice traffic) before dropping it. If no voice packets go through the SIP ALG before the timeout period expires, the Nebula Device deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.
SIP Signaling Inactivity Timeout	Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the Nebula Device. If the SIP client does not have this mechanism and makes no calls during the Nebula Device SIP timeout, the Nebula Device deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (**1** – **86400**).
NAT	
1:1 NAT A 1:1 NAT rule maps a public IP address to the private IP address of a LAN server to give WAN users access. If a private network server will initiate sessions to the outside clients, 1:1 NAT lets the Nebula Device translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server.	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Uplink	Select the interface of the Nebula Device on which packets for the NAT rule must be received.
Public IP	Enter the destination IP address of the packets received by the interface specified in this NAT rule. Note: To enable NAT loop-back, enter a specific IP address instead of **any** in this field. NAT loop-back allows communications between two hosts on the LAN behind the Nebula Device through an external IP address.
LAN IP	Specify to which translated destination IP address this NAT rule forwards packets.
Allowed Remote IP	Specify the remote IP address with which the computer is allowed to use the public IP address to access the private network server. You can specify a range of IP addresses. **any** allows all IP addresses.

Table 155 Site-wide > Configure > Security gateway > Firewall (continued)

LABEL	DESCRIPTION
Description	Enter a description for the rule.
🗑	Click this icon to remove the rule.
Add	Click this button to create a new 1:1 NAT mapping rule.
Virtual server	
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Uplink	Select the interface of the Nebula Device on which packets for the NAT rule must be received.
Protocol	Select the protocol (**TCP**, **UDP**, or **Any**) used by the service requesting the connection.
Public IP	Enter the destination IP address of the packets received by the interface specified in this NAT rule. Note: To enable NAT loop-back, enter a specific IP address instead of **any** in this field. NAT loop-back allows communications between two hosts on the LAN behind the Nebula Device through an external IP address.
Public port	Enter the translated destination port or range of translated destination ports if this NAT rule forwards the packet.
LAN IP	Specify to which translated destination IP address this NAT rule forwards packets.
Local port	Enter the original destination port or range of destination ports this NAT rule supports.
Allowed Remote IP	Specify the remote IP address with which the computer is allowed to use the public IP address to access the private network server. You can specify a range of IP addresses. **any** allows all IP addresses.
Description	Enter a description for the rule.
🗑	Click this icon to remove the rule.
Add	Click this button to create a new virtual server mapping rule.

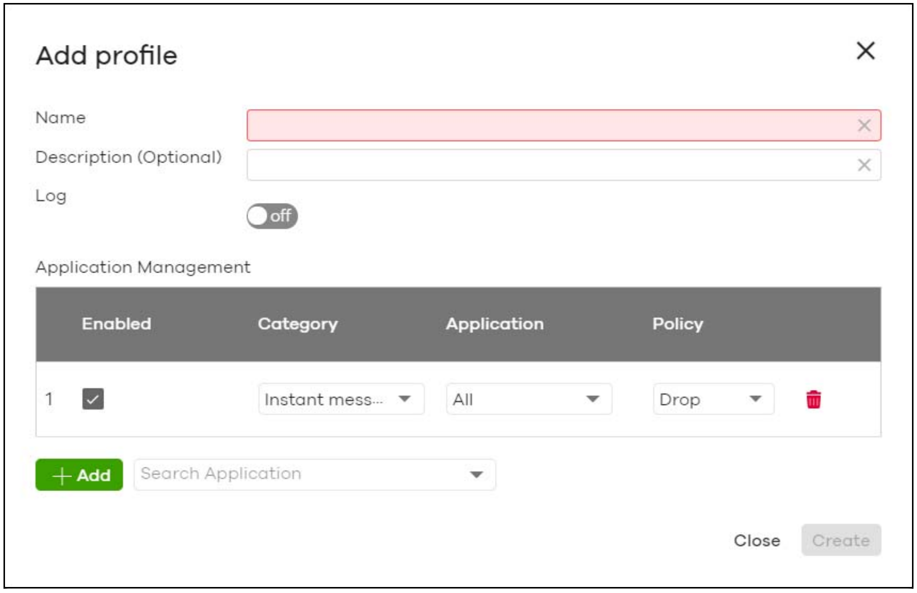
9.3.4.1 Add application patrol profile

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers).

An application patrol profile is a group of categories of application patrol signatures. For each profile, you can specify the default action the Nebula Device takes once a packet matches a signature (forward, drop, or reject a service's connections and/or create a log alert).

Click the **Add** button in the **Application patrol** section of the **Site-wide** > **Configure** > **Security gateway** > **Firewall** screen to access this screen. Use the application patrol profile screens to customize action and log settings for a group of application patrol signatures.

Figure 215 Site-wide > Configure > Security gateway > Firewall: Add an application profile



Add profile

Name

Description (Optional)

Log

off

Application Management

	Enabled	Category	Application	Policy	
1	☑	Instant mess...	All	Drop	🗑

The following table describes the labels in this screen.

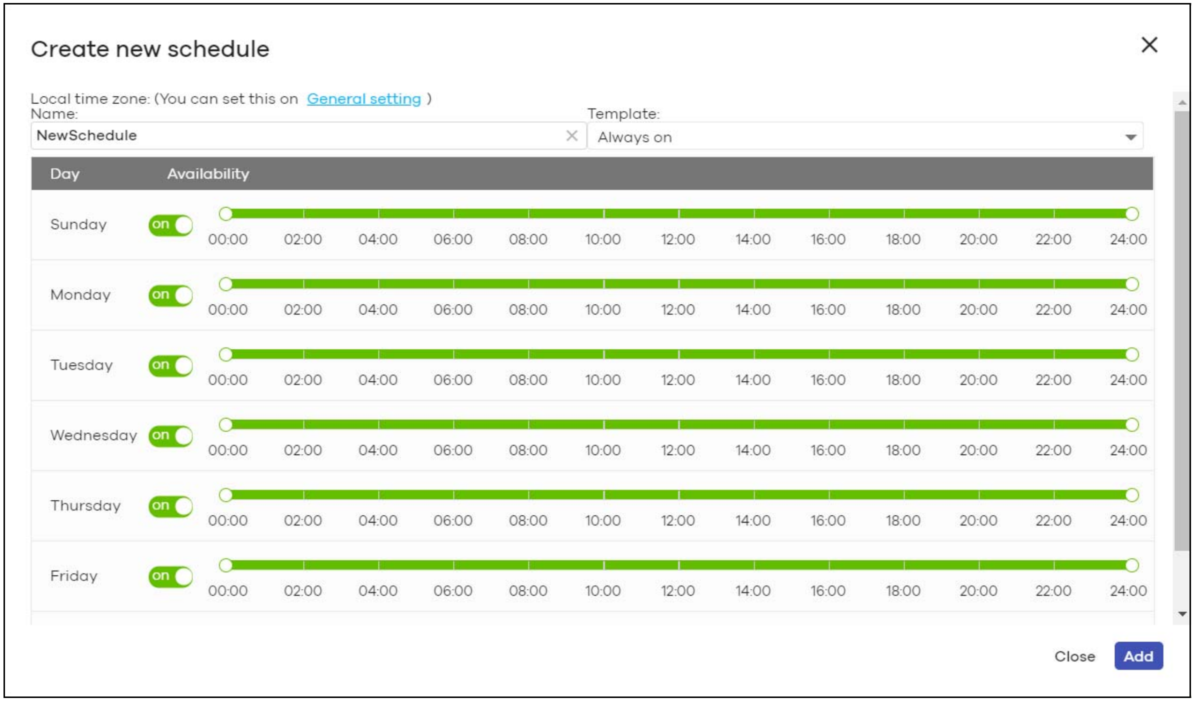
Table 156 Site-wide > Configure > Security gateway > Firewall: Add an application profile

LABEL	DESCRIPTION
Name	Enter a name for this profile for identification purposes.
Description	Enter a description for this profile.
Log	Select whether to have the Nebula Device generate a log (**ON**) or not (**OFF**) by default when traffic matches an application signature in this category.
Application management	
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Category	Select an application category.
Application	Select **All** or select an application within the category to apply the policy.
Policy	Select the default action for the applications selected in this category. **Forward** – the Nebula Device routes packets that matches these application signatures. **Drop** – the Nebula Device silently drops packets that matches these application signatures without notification. **Reject** – the Nebula Device drops packets that matches these application signatures and sends notification to clients.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new application category and set actions for specific applications within the category.
	Enter a name to search for relevant applications and click **Add** to create an entry.
Close	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

9.3.4.2 Create new schedule

Click the **Add** button in the **Schedule Profiles** section of the **Site-wide** > **Configure** > **Security gateway** > **Firewall** screen to access this screen.

Figure 216 Site-wide > Configure > Security gateway > Firewall: Add a schedule profile



Create new schedule

Local time zone: (You can set this on General setting)

Name: NewSchedule

Template: Always on

Day	Availability
Sunday	on
Monday	on
Tuesday	on
Wednesday	on
Thursday	on
Friday	on

The following table describes the labels in this screen.

Table 157 Site-wide > Configure > Security gateway > Firewall: Add a schedule profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identification purposes.
Templates	Select a pre-defined schedule template or select **Custom schedule** and manually configure the day and time at which the associated firewall outbound rule is enabled.
Day	This shows the day of the week.
Availability	Click **On** to enable the associated rule at the specified time on this day. Otherwise, select **Off** to turn the associated rule off at the specified time on this day. Specify the hour and minute when the schedule begins and ends each day.
Close	Click this button to exit this screen without saving.
Add	Click this button to save your changes and close the screen.

9.3.5 Security Service

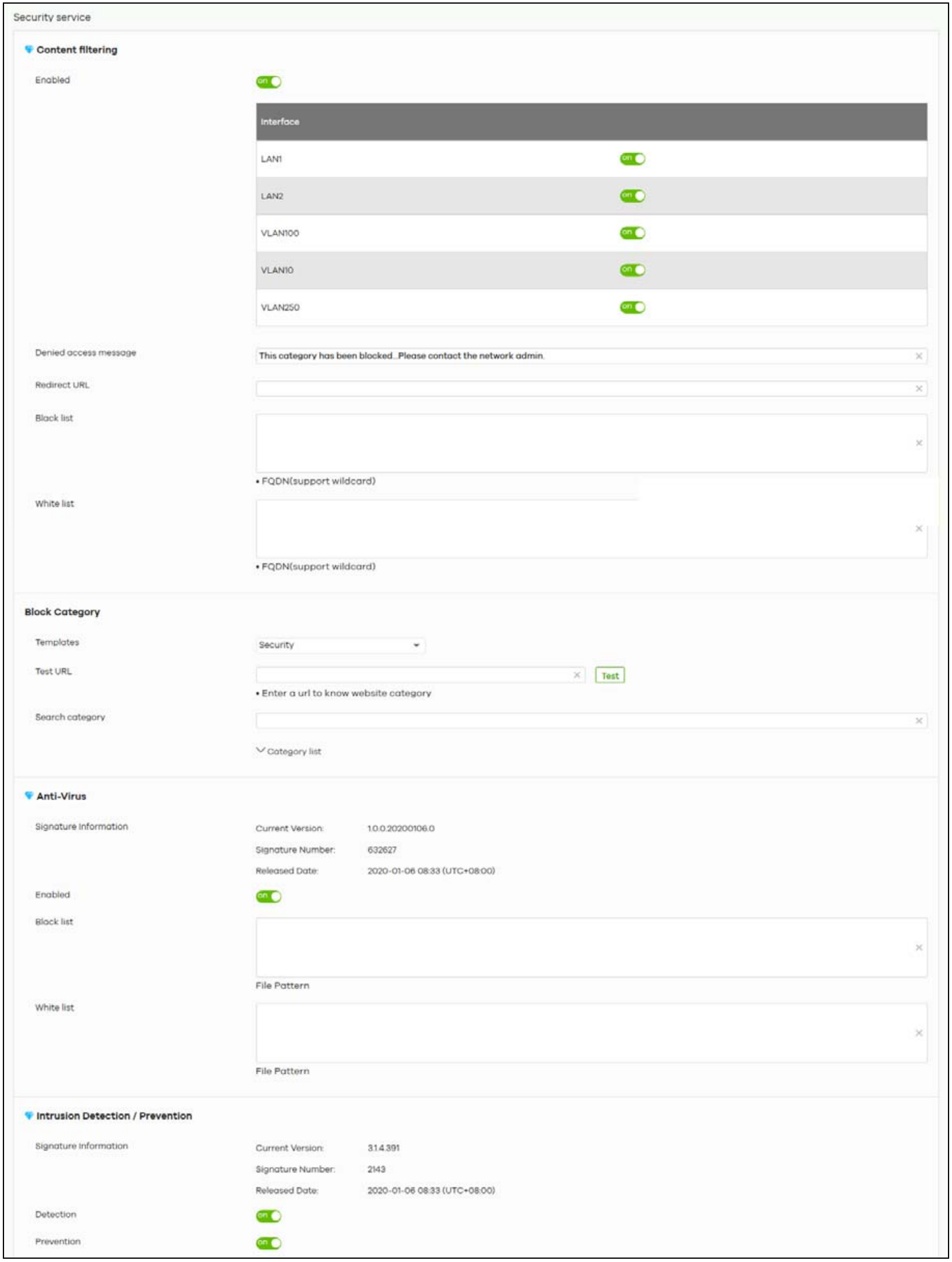
Use this screen to enable or disable the features available in the security pack for your Nebula Device, such as content filter, Intrusion Detection and Prevention (IDP) and/or anti-virus. As to application patrol, go to the **Firewall** screen to configure it since you need to have a firewall rule for outbound traffic.

Content filter allows you to block access to specific web sites. It can also block access to specific categories of web site content. IDP can detect malicious or suspicious packets used in network-based intrusions and respond instantaneously. Anti-virus helps protect your connected network from virus/spy-ware infection.

Click **Site-wide** > **Configure** > **Security gateway** > **Security service** to access this screen.

Note: Packet inspection signatures examine packet content for malicious data. Packet inspection applies to OSI (Open System Interconnection) layer-4 to layer-7 contents. You need to subscribe for IDP service in order to be able to download new signatures.

Figure 217 Site-wide > Configure > Security gateway > Security service



Security service

Content filtering

Enabled: on

Interface	
LAN1	on
LAN2	on
VLAN100	on
VLAN10	on
VLAN250	on

Denied access message: This category has been blocked. Please contact the network admin.

Redirect URL:

Black list:

• FQDN(support wildcard)

White list:

• FQDN(support wildcard)

Block Category

Templates: Security

Test URL: Test

• Enter a url to know website category

Search category:

Category list

Anti-Virus

Signature Information:

Current Version: 1.0.0.20200106.0

Signature Number: 632627

Released Date: 2020-01-06 08:33 (UTC+08:00)

Enabled: on

Black list:

File Pattern

White list:

File Pattern

Intrusion Detection / Prevention

Signature Information:

Current Version: 3.1.4.391

Signature Number: 2143

Released Date: 2020-01-06 08:33 (UTC+08:00)

Detection: on

Prevention: on

The following table describes the labels in this screen.

Table 158 Site-wide > Configure > Security gateway > Security service

LABEL	DESCRIPTION
Content Filtering	
Enabled	Click **ON** to enable the content filter feature on the Nebula Device. Otherwise, click **OFF** to disable it.
Interface	This shows the name of the interfaces created on the Nebula Device. Click **ON** to enable content filter on the interfaces.
Denied access message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the Nebula Device just opens the web page you specified without showing a denied access message.
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Black list	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0–9a–z–). The casing does not matter.
White list	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0–9a–z–). The casing does not matter.
Block Category The Nebula Device prevents users from accessing web pages that match the categories that you select below. When external database content filter blocks access to a web page, it displays the denied access message that you configured in the **Denied access message** field along with the category of the blocked web page.	
Templates	Web pages are classified into a category based on their content. You can choose a pre-defined template that has already selected certain categories. Alternatively, choose **Custom** and manually select categories in this section to control access to specific types of Internet content.
Test URL	You can check which category a web page belongs to. Enter a web site URL in the text box. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. Content Filter can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. **Test URL** displays both results in the test.

Table 158   Site-wide > Configure > Security gateway > Security service (continued)

LABEL	DESCRIPTION
Search Category	Specify your desired filter criteria to filter the list of categories.
Category List	Click to display or hide the category list. These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
Anti-Virus	
Signature Information	This shows the **Current Version** of the anti-virus definition, its **Signature Number** and the **Released Date**.
Enabled	Click **On** to enable anti-virus on the Nebula Device. Otherwise, select **Off** to disable it.
Black/White List	Use this to set up anti-virus black (blocked) and white (allowed) lists of virus file patterns.
File Pattern	For a black list entry, specify a pattern to identify the names of files that the Nebula Device should log and delete. For a white list entry, specify a pattern to identify the names of files that the Nebula Device should not scan for viruses. • Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. • A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on. • Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match. • An * in the middle of a pattern has the Nebula Device check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between. • The whole file name has to match if you do not use a question mark or asterisk. • If you do not use a wildcard, the Nebula Device checks up to the first 80 characters of a file name.
Intrusion Detection / Prevention System	
Signature Information	This shows the **Current Version** of the anti-intrusion definition, its **Signature Number** and the **Released Date**.
Detection	Click **On** to detect malicious or suspicious packets. Otherwise, select **Off** to disable it.
Prevention	Click **On** to identify and respond to intrusions. Otherwise, select **Off** to disable it.

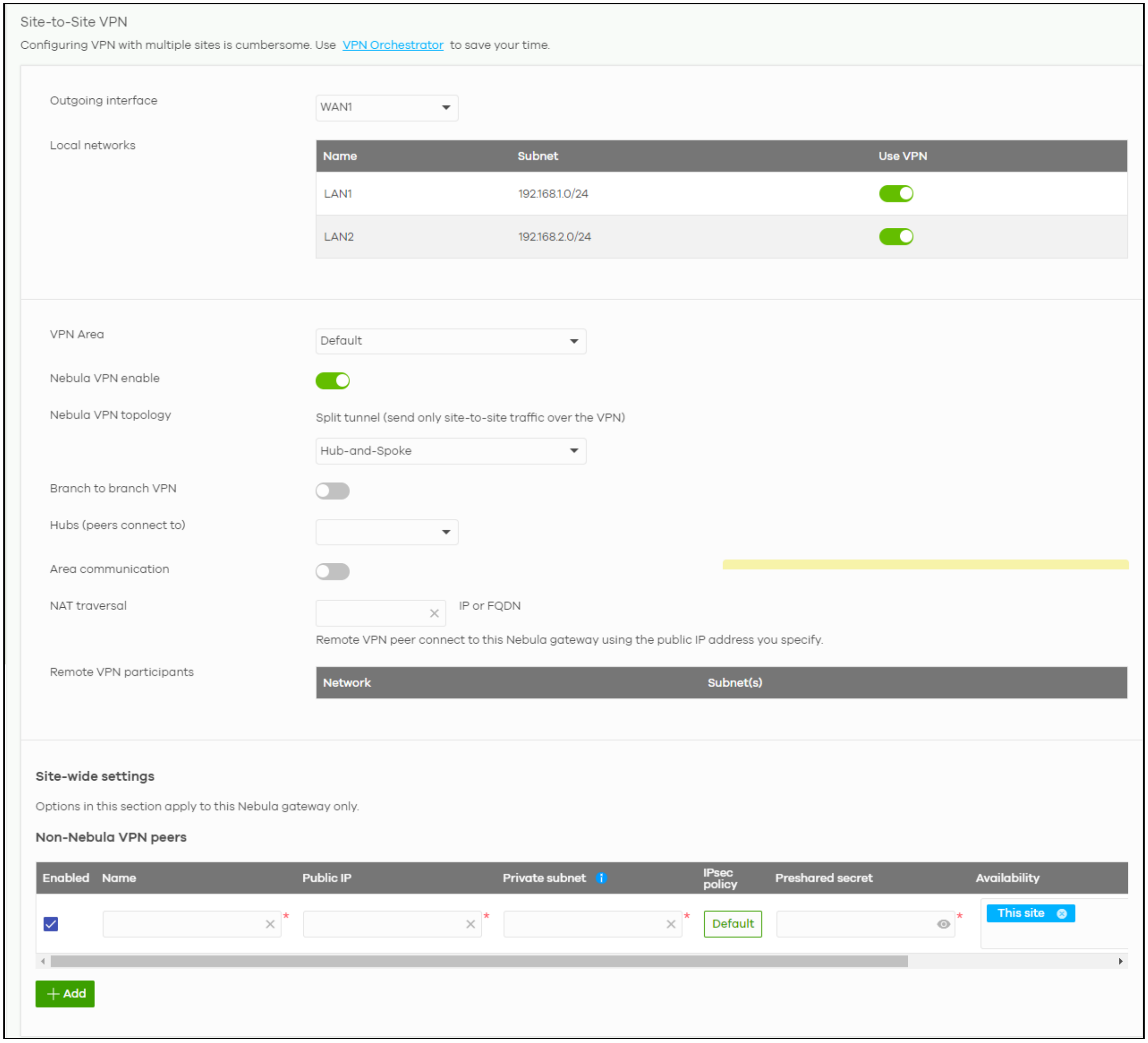
9.3.6 Site-to-Site VPN

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. Use this screen to configure a VPN rule.

Note: Site-to-site VPN do not support both sites behind NAT scenario.

Click **Site-wide** > **Configure** > **Security gateway** > **Site-to-Site VPN** to access this screen.

Figure 218 Site-wide > Configure > Security gateway > Site-to-Site VPN



Site-to-Site VPN

Configuring VPN with multiple sites is cumbersome. Use VPN Orchestrator to save your time.

Outgoing interface: WAN1

Local networks

Name	Subnet	Use VPN
LAN1	192.168.1.0/24	●
LAN2	192.168.2.0/24	●

VPN Area: Default

Nebula VPN enable: ●

Nebula VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

Hub-and-Spoke

Branch to branch VPN: ○

Hubs (peers connect to)

Area communication: ○

NAT traversal: IP or FQDN

Remote VPN peer connect to this Nebula gateway using the public IP address you specify.

Remote VPN participants

Network	Subnet(s)

Site-wide settings

Options in this section apply to this Nebula gateway only.

Non-Nebula VPN peers

Enabled	Name	Public IP	Private subnet	IPsec policy	Preshared secret	Availability
☑				Default		This site

The following table describes the labels in this screen.

Table 159 Site-wide > Configure > Security gateway > Site-to-Site VPN

LABEL	DESCRIPTION
Outgoing Interface	Select the WAN interface to which the VPN connection is going. Select **AUTO** to send VPN traffic through a different WAN interface when the primary WAN interface is down or disabled.
Preferred uplink	Specify the primary WAN interface through which the Nebula Device forwards VPN traffic when you set **Outgoing Interface** to **AUTO**.
Local networks	This shows the local networks behind the Nebula Device.
Name	This shows the network name.
Subnet	This shows the IP address and subnet mask of the computer on the network.
Use VPN	Click this to allow or disallow the computer connected to the LAN port to use VPN.
VPN Area	Select the VPN area of the site. For details, see Section 12.4.4.2 on page 691.

Table 159 Site-wide > Configure > Security gateway > Site-to-Site VPN (continued)

LABEL	DESCRIPTION
Nebula VPN enable	Click this to enable or disable site-to-site VPN on the site's Nebula Device. If you disable this setting, the site will leave the VPN area.
Nebula VPN Topology	This shows the VPN mode supported by the Nebula Device. Select a VPN topology. Select **Disable** to not set a VPN connection. In the **Site-to-Site** VPN topology, the remote IPSec device has a static IP address or a domain name. This Nebula Device can initiate the VPN tunnel. In the **Hub-and-Spoke** VPN topology, there is a VPN connection between each spoke router and the hub router, which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself. In the **Server-and-Client** VPN topology, incoming connections from IPSec VPN clients are allowed. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
Branch to branch VPN	Enable this to allow spoke sites to communicate with each other in the VPN area. When disabled, spoke sites can only communicate with hub sites.
Hubs (peers to connect to)	This field is available when you set **Topology** to **Hub-and-Spoke**. The field is configurable only when the Nebula Device of the selected site is the hub router. You can select another site's name to have the Nebula Device of that site act as the hub router in the **Hub-and-Spoke** VPN topology.
Area communication	Enable this to allow the site to communicate with sites in different VPN areas within the organization.
NAT traversal	If the Nebula Device is behind a NAT router, enter the public IP address or the domain name that is configured and mapped to the Nebula Device on the NAT router.
Server (client connect to)	This field is available when you set **Topology** to **Server-and-Client**. The field is configurable only when the Nebula Device of the selected site is the VPN server. You can select another site's name to have the Nebula Device of that site act as the VPN server.
Client-to-Client communication	Select **On** to allow VPN traffic to transmit between VPN clients by going through the server. The field is configurable only when the Nebula Device of the selected site is the VPN server.
Remote VPN participants	This shows the remote (peer) Nebula Device's network name and address.
Non-Nebula VPN peers	If the remote VPN gateway is not a Nebula Device, use this section to set up a VPN connection between it and the Nebula Device.
+ Add	Click this button to add a non-Nebula gateway to the VPN area.
Enabled	Select the checkbox to turn on the rule. Otherwise, clear the checkbox to turn off the rule.
Name	Enter the name of the peer gateway.
Public IP	Enter the public IP address of the peer gateway.
Private subnet	Enter the local network address or subnet behind the peer gateway.
IPSec policy	Click to select a pre-defined policy or have a custom one. See Section 9.3.6.1 on page 613 for detailed information.
Preshared secret	Enter a pre-shared key (password). The Nebula Device and peer gateway use the key to identify each other when they negotiate the IKE SA.

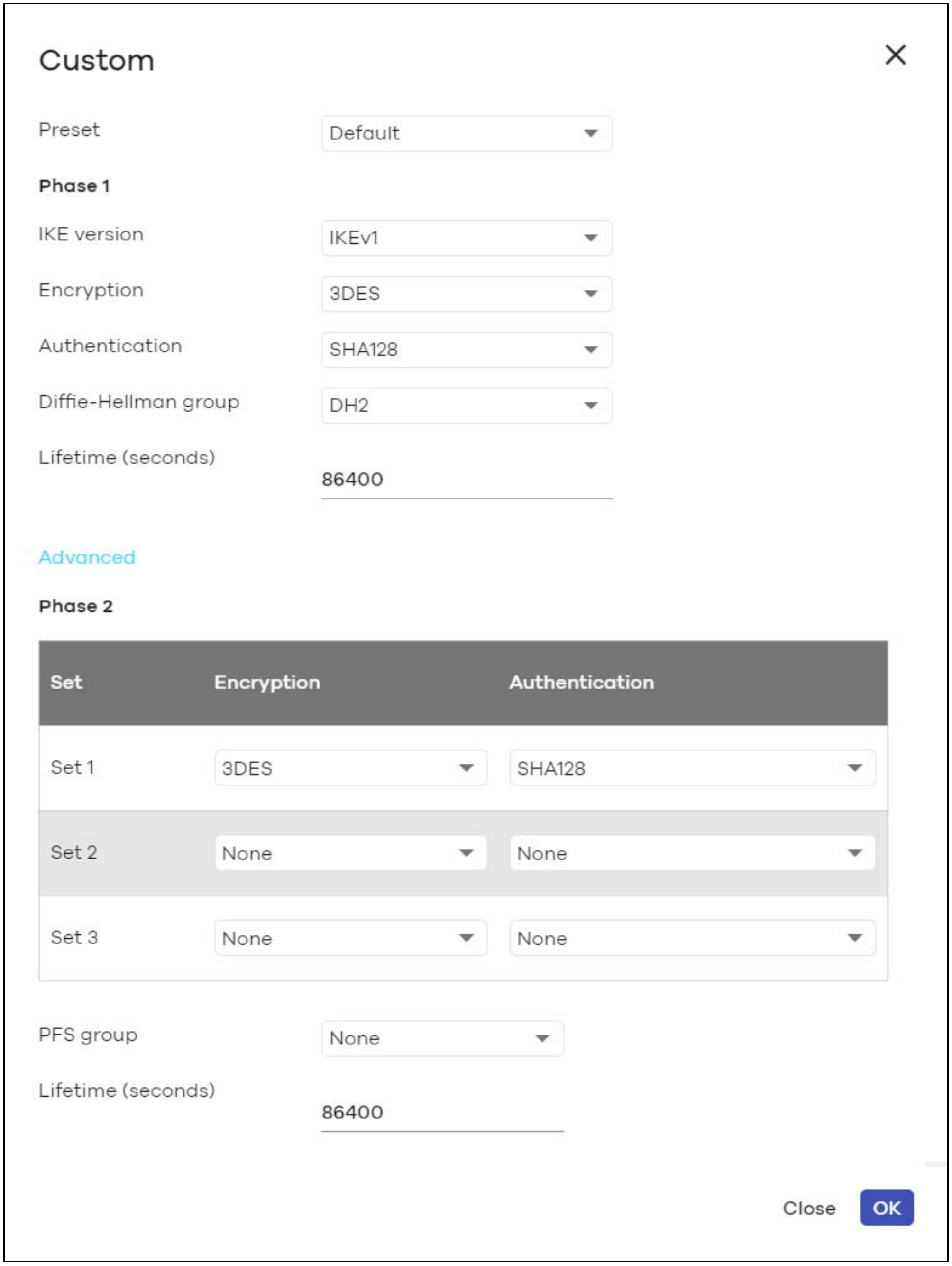
Table 159 Site-wide > Configure > Security gateway > Site-to-Site VPN (continued)

LABEL	DESCRIPTION
Availability	Select **All sites** to allow the peer gateway to connect to any Nebula Device in the organization through a VPN tunnel. Select **This site** and the peer gateway can only connect to the Nebula Device in this site through a VPN tunnel. You can also configure any specific sites in the organization,
Address	Enter the address (physical location) of the device.
Remove	Click the remove icon to delete the entry.
Add	Click this button to add a peer VPN gateway to the list.

9.3.6.1 Custom IPSec Policy

Click an existing **IPSec Policy** button in the **Non-Nebula VPN peers** section of the **Site-wide** > **Configure** > **Security gateway** > **Site-to-Site VPN** screen to access this screen.

Figure 219 Site-wide > Configure > Security gateway > Site-to-Site VPN: Custom IPSec Policy



Custom

Preset: Default

Phase 1

IKE version: IKEv1

Encryption: 3DES

Authentication: SHA128

Diffie-Hellman group: DH2

Lifetime (seconds): 86400

Advanced

Phase 2

Set	Encryption	Authentication
Set 1	3DES	SHA128
Set 2	None	None
Set 3	None	None

PFS group: None

Lifetime (seconds): 86400

The following table describes the labels in this screen.

Table 160 Site-wide > Configure > Security gateway > Site-to-Site VPN: Custom IPSec Policy

LABEL	DESCRIPTION
Preset	Select a pre-defined IPSec policy, or select **Custom** to configure the policy settings yourself.
Phase 1	IPSec VPN consists of two phases: Phase 1 (Authentication) and Phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

Table 160 Site-wide > Configure > Security gateway > Site-to-Site VPN: Custom IPSec Policy (continued)

LABEL	DESCRIPTION
IKE version	Select **IKEv1** or **IKEv2**. **IKEv1** applies to IPv4 traffic only. **IKEv2** applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** – a 56-bit key with the DES encryption algorithm **3DES** – a 168-bit key with the DES encryption algorithm **AES128** – a 128-bit key with the AES encryption algorithm **AES192** – a 192-bit key with the AES encryption algorithm **AES256** – a 256-bit key with the AES encryption algorithm The Nebula Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA128**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than MD5, but it is also slower. The remote IPSec router must use the same authentication algorithm.
Diffie-Hellman group	Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are: **DH1** – use a 768-bit random number Modular Exponential (MODP) DH group **DH2** – use a 1024-bit random number MODP **DH5** – use a 1536-bit random number MODP **DH14** – use a 2048-bit random number MODP The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Lifetime (seconds)	Type the maximum number of seconds the IKE SA can last. When this time has passed, the Nebula Device and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Advanced	Click this to display a greater or lesser number of configuration fields.
Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are: **Main** – this encrypts the Nebula Device's and remote IPSec router's identities but takes more time to establish the IKE SA **Aggressive** – this is faster but does not encrypt the identities The Nebula Device and the remote IPSec router must use the same negotiation mode.
Local ID	Enter the identity of the Nebula Device during authentication. **Any** indicates that the remote IPSec router does not check the identity of the Nebula Device.
Peer ID	Enter the identity of the remote IPSec router during authentication. **Any** indicates that the Nebula Device does not check the identity of the remote IPSec router.
Phase 2	Phase 2 uses the SA that was established in phase 1 to negotiate SAs for IPSec.

Table 160 Site-wide > Configure > Security gateway > Site-to-Site VPN: Custom IPSec Policy (continued)

LABEL	DESCRIPTION
Encryption	Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **(none)** – no encryption key or algorithm **DES** – a 56-bit key with the DES encryption algorithm **3DES** – a 168-bit key with the DES encryption algorithm **AES128** – a 128-bit key with the AES encryption algorithm **AES192** – a 192-bit key with the AES encryption algorithm **AES256** – a 256-bit key with the AES encryption algorithm The Nebula Device and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **None**, **MD5**, **SHA128**, **SHA256**, and **SHA512**. SHA is generally considered stronger than MD5, but it is also slower. The Nebula Device and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
PFS group	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **None** – disable PFS **DH1** – enable PFS and use a 768-bit random number **DH2** – enable PFS and use a 1024-bit random number **DH5** – enable PFS and use a 1536-bit random number **DH14** – enable PFS and use a 2048-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.
Lifetime (seconds)	Enter the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The Nebula Device automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
VPN tunnel interface (optional) IPSec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table. VTI allows static routes to send traffic over the VPN. The IPSec tunnel endpoint is associated with an actual (virtual) interface. Therefore many interface capabilities such as Policy Route, Static Route, Trunk, and BWM can be applied to the IPSec tunnel as soon as the tunnel is active. IPSec VTI simplifies network management and load balancing. Create a trunk using VPN tunnel interfaces for load balancing. This section is available when you select **IKEv2** in the **IKE Version** field.	
IP address	Enter the IP address of the VPN tunnel interface.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

9.3.7 Remote Access VPN

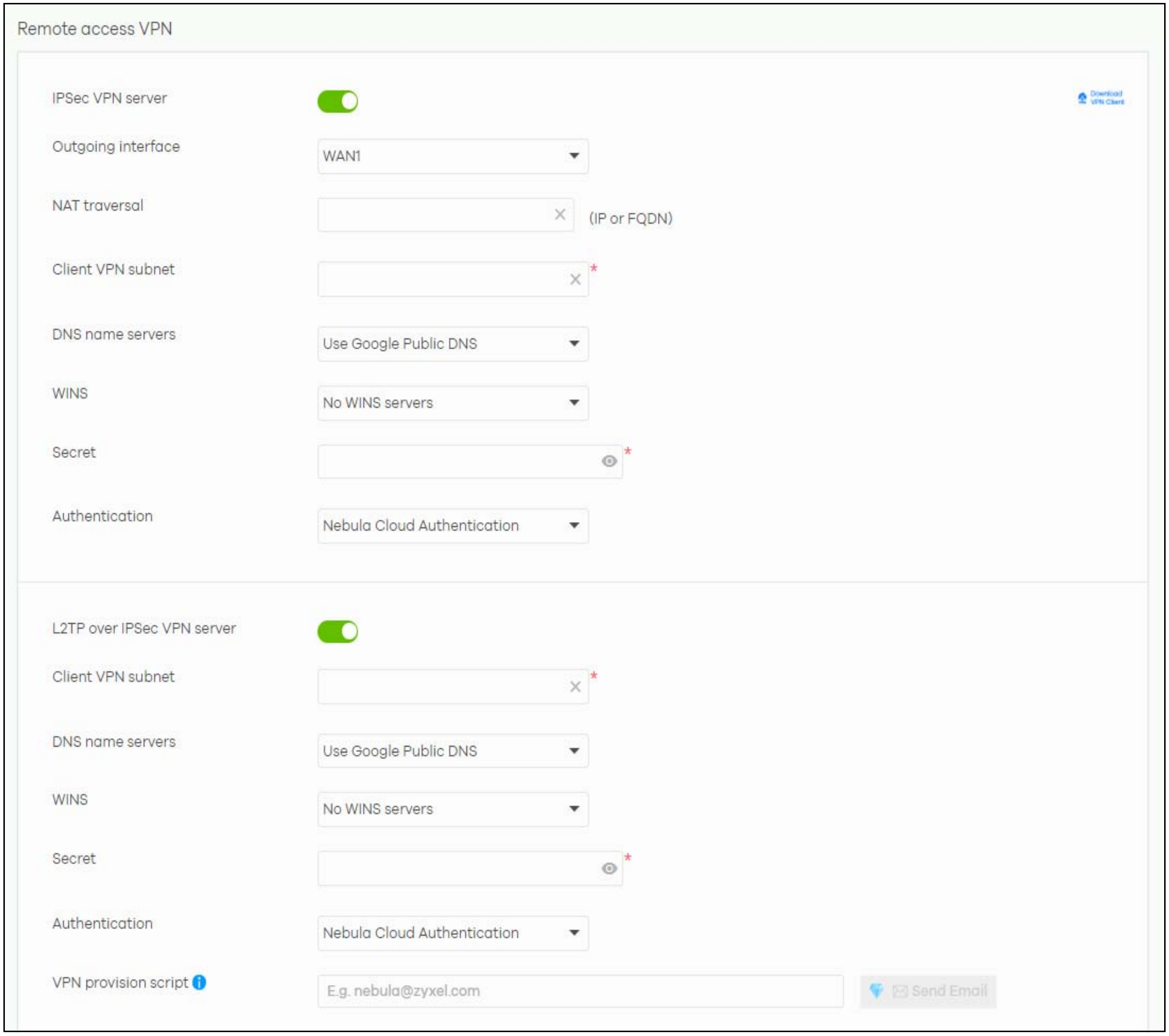
Use this screen to configure the VPN client settings.

Internet Protocol Security (IPSec) VPN connects IPSec routers or remote users using IPSec client software. This standards-based VPN offers flexible solutions for secure data communications across a public network. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first and then an L2TP tunnel is built inside it.

Click **Site-wide** > **Configure** > **Security gateway** > **Remote access VPN** to access this screen.

Figure 220 Site-wide > Configure > Security gateway > Remote access VPN



Remote access VPN

IPSec VPN server	●
Outgoing interface	WAN1
NAT traversal	(IP or FQDN)
Client VPN subnet	*
DNS name servers	Use Google Public DNS
WINS	No WINS servers
Secret	*
Authentication	Nebula Cloud Authentication
L2TP over IPSec VPN server	●
Client VPN subnet	*
DNS name servers	Use Google Public DNS
WINS	No WINS servers
Secret	*
Authentication	Nebula Cloud Authentication
VPN provision script	E.g. nebula@zyxel.com

The following table describes the labels in this screen.

Table 161 Site-wide > Configure > Security gateway > Remote access VPN

LABEL	DESCRIPTION
Download VPN Client	Click this icon to download VPN client software.
IPSec VPN server	Select to enable the **IPSec client** feature on the Nebula Device. Otherwise, select **Disable** to turn it off.
Outgoing interface	Select the WAN interface to which the IPSec VPN connection is going.
NAT traversal	Enter the IP address or domain name of the NAT router if the IPSec VPN tunnel must pass through NAT (there is a NAT router between the IPSec devices).
Client VPN subnet	Specify the IP addresses that the Nebula Device uses to assign to the IPSec VPN clients.
DNS name servers	Specify the IP addresses of DNS servers to assign to the remote users. Select **Use Google Public DNS** to use the DNS service offered by Google. Otherwise, select **Specify nameserver** to enter a static IP address.
Custom nameservers	If you select **Specify nameserver** in the **DNS name servers** field, manually enter the DNS server IP addresses.
WINS	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Select **No WINS Servers** to not send WINS server addresses to the users. Otherwise, select **Specify nameserver** to enter the IP addresses of WINS servers to assign to the remote users.
Custom nameservers	If you select **Specify nameserver** in the **WINS** field, manually enter the WINS server IP addresses.
Secret	Enter the pre-shared key (password) which is used to set up the **IPSec** VPN tunnel.
Authentication	Select how the Nebula Device authenticates a remote user before allowing access to the IPSec VPN tunnel.
L2TP over IPSec VPN server	Select to enable the L2TP over IPSec VPN feature on the Nebula Device. Otherwise, select **Disable** to turn it off.
Client VPN subnet	Specify the IP addresses that the Nebula Device uses to assign to the L2TP over IPSec VPN clients.
DNS name servers	Specify the IP addresses of DNS servers to assign to the remote users. Select **Use Google Public DNS** to use the DNS service offered by Google. Otherwise, select **Specify nameserver** to enter a static IP address.
Custom nameservers	If you select **Specify nameserver** in the **DNS name servers** field, manually enter the DNS server IP addresses.
WINS	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Select **No WINS Servers** to not send WINS server addresses to the users. Otherwise, select **Specify nameserver** to enter the IP addresses of WINS servers to assign to the remote users.
Custom nameservers	If you select **Specify nameserver** in the **WINS** field, manually enter the WINS server IP addresses.
Secret	Enter the pre-shared key (password) which is used to set up the L2TP over IPSec VPN tunnel.

Table 161 Site-wide > Configure > Security gateway > Remote access VPN (continued)

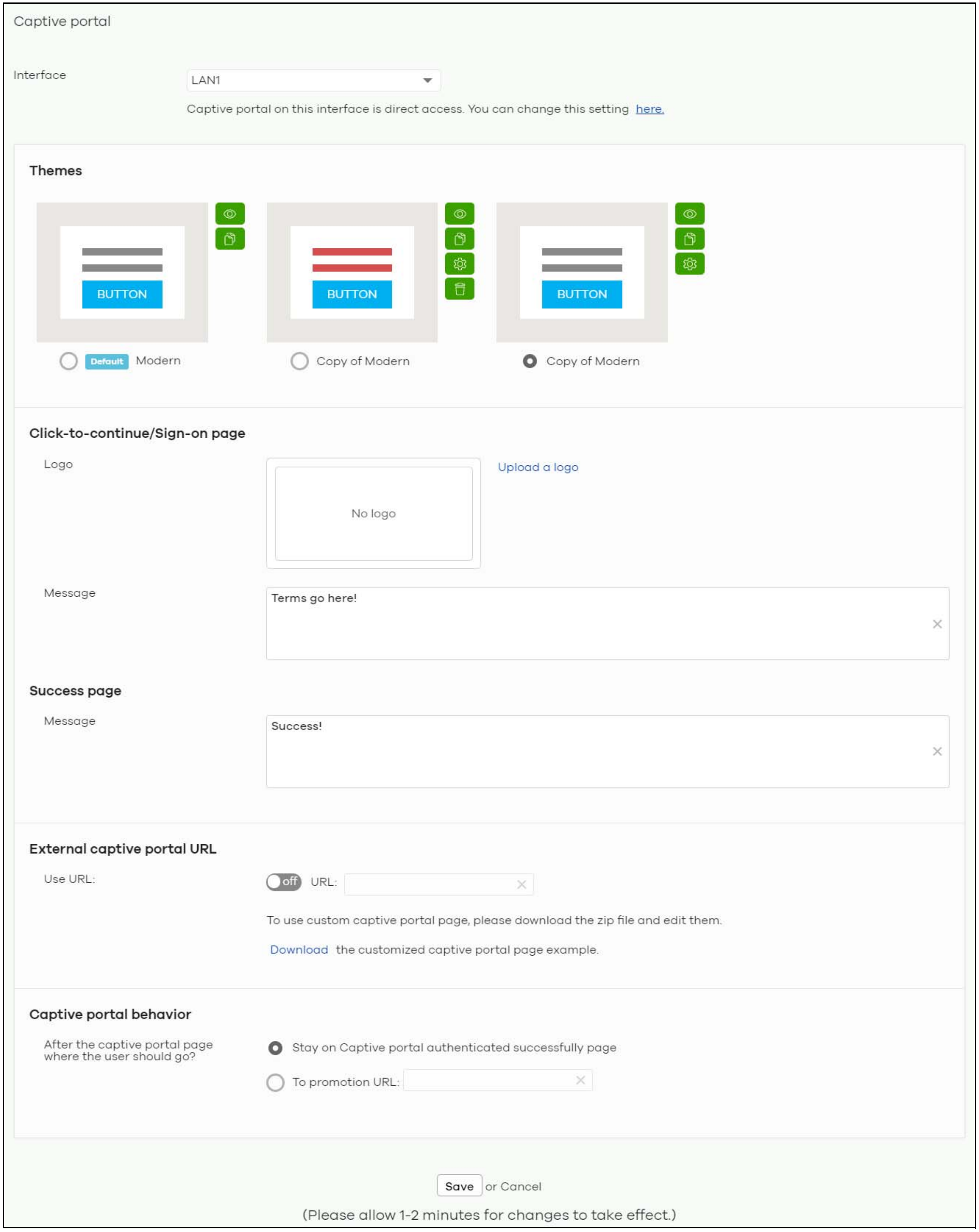
LABEL	DESCRIPTION
Authentication	Select how the Nebula Device authenticates a remote user before allowing access to the L2TP over IPSec VPN tunnel.
VPN provision script	Send an email to help automatically configure VPN settings on client devices so that the devices can remotely access this Nebula Device. The email contains two scripts; one for mac OS and iOS devices, and one for Windows 8 and Windows 10 devices. You can send the email to one or more email addresses. • If **Authentication** is set to **Nebula Cloud Authentication**, the default email address list contains all authorized VPN user email addresses and your email address. • If **Authentication** is set to **AD and RADIUS Authentication**, the default email address list contains your user email address.

9.3.8 Captive Portal

Use this screen to configure captive portal settings for each interface. A captive portal can intercept network traffic until the user authenticates his or her connection, usually through a specifically designated login web page.

Click **Site-wide** > **Configure** > **Security gateway** > **Captive portal** to access this screen.

Figure 221 Site-wide > Configure > Security gateway > Captive portal



Captive portal

Interface: LAN1

Captive portal on this interface is direct access. You can change this setting here.

Themes

○ Default Modern ○ Copy of Modern ● Copy of Modern

Click-to-continue/Sign-on page

Logo: No logo — Upload a logo

Message: Terms go here!

Success page

Message: Success!

External captive portal URL

Use URL: off URL:

To use custom captive portal page, please download the zip file and edit them.

Download the customized captive portal page example.

Captive portal behavior

After the captive portal page where the user should go?

● Stay on Captive portal authenticated successfully page

○ To promotion URL:

Save or Cancel

(Please allow 1-2 minutes for changes to take effect.)

The following table describes the labels in this screen.

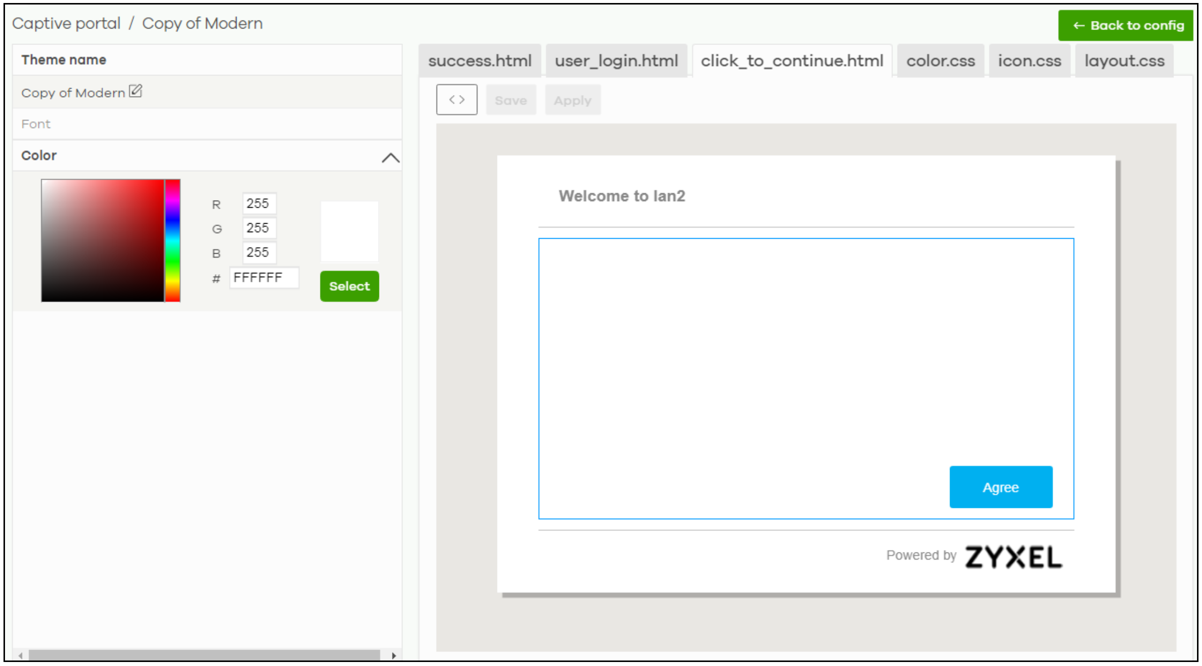
Table 162 Site-wide > Configure > Security gateway > Captive portal

LABEL	DESCRIPTION
Interface	Select the Nebula Device's interface (network) to which the settings you configure here is applied.
Themes	This section is not configurable when **External captive portal URL** is set to **ON**. • Click the **Preview** icon at the upper right of a theme image to display the portal page in a new frame. • Click the **Copy** icon to create a new custom theme (portal page). • Click the **Edit** icon of a custom theme to go to a screen, where you can view and configure the details of the custom portal pages. See Section 9.3.8.1 on page 621. • Click the **Remove** icon to delete a custom theme. Select the theme you want to use on the specified interface.
Click-to-continue/Sign-on page This section is not configurable when **External captive portal URL** is set to **ON**.	
Logo	This shows the logo image that you uploaded for the customized login page. Click **Upload a logo** and specify the location and file name of the logo graphic or click **Browse** to locate it. You can use the following image file formats: GIF, PNG, or JPG.
Message	Enter a note to display below the title. Use up to 1024 printable ASCII characters. Spaces are allowed.
Success page	
Message	Enter a note to display on the page that displays when a user logs in successfully. Use up to 1024 printable ASCII characters. Spaces are allowed.
External captive portal URL	
Use URL	Select **On** to use a custom login page from an external web portal instead of the one built into the NCC. You can configure the look and feel of the web portal page. Specify the login page's URL; for example, http://IIS server IP Address/login.asp. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Captive portal behavior	
After the captive portal page where the user should go?	Select **To promotion URL** and specify the URL of the web site/page to which the user is redirected after a successful login. Otherwise, select **Stay on Captive portal authenticated successfully page**.

9.3.8.1 Custom Theme Edit

Use this screen to check what the custom portal pages look like. You can also view and modify the CSS values of the selected HTML file. Click a custom login page's **Edit** button in the **Site-wide** > **Configure** > **Security gateway** > **Captive portal** screen to access this screen.

Figure 222 Site-wide > Configure > Security gateway > Captive portal: Edit



R 255
G 255
B 255
FFFFFF

The following table describes the labels in this screen.

Table 163 Site-wide > Configure > Security gateway > Captive portal: Edit

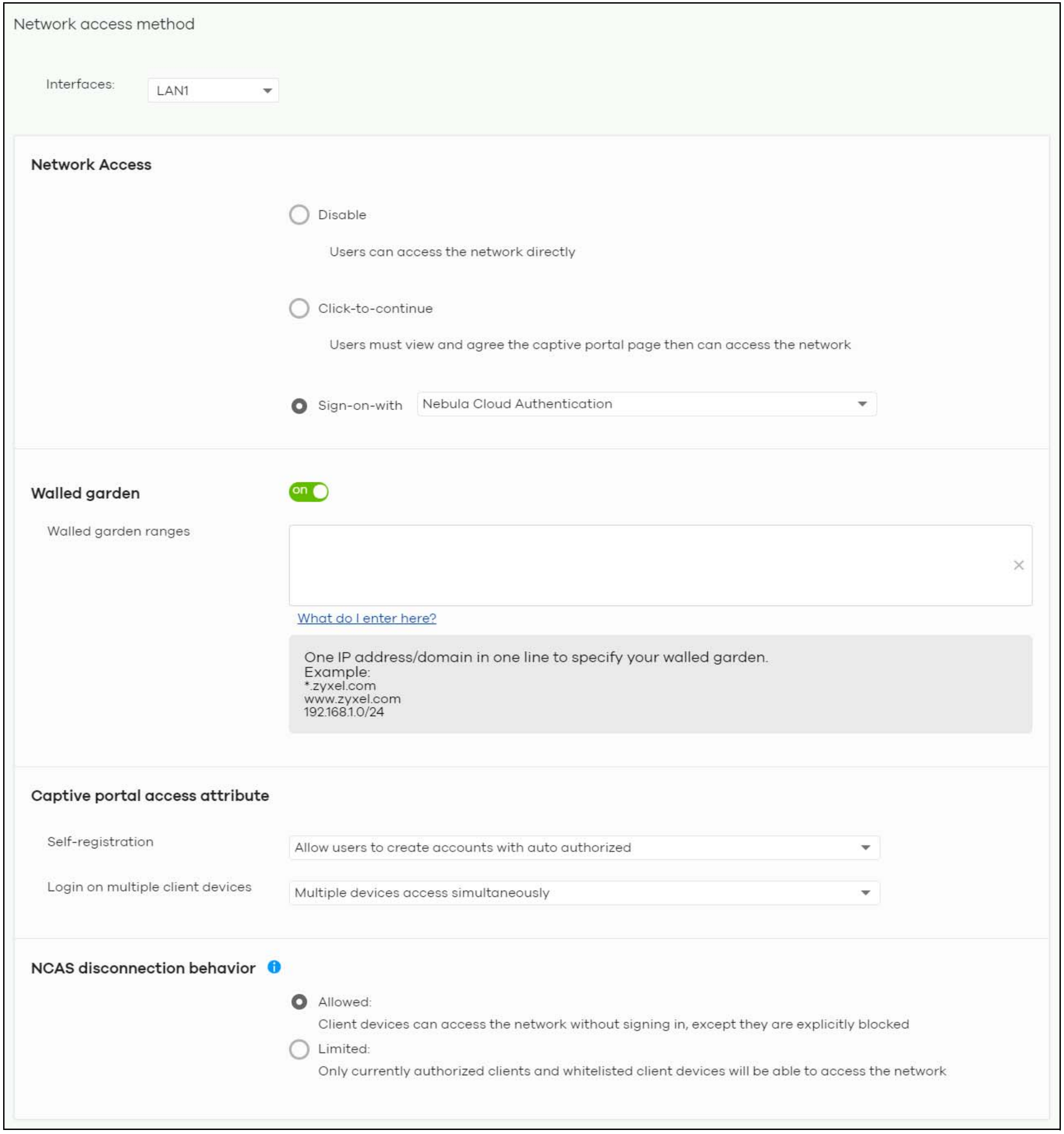
LABEL	DESCRIPTION
Back to config	Click this button to return to the **Captive portal** screen.
Theme name	This shows the name of the theme. Click the edit icon to change it.
Font	Click the arrow to hide or display the configuration fields. To display this section and customize the font type and/or size, click an item with text in the preview of the selected custom portal page (HTML file).
Color	Click the arrow to hide or display the configuration fields. Click an item in the preview of the selected custom portal page (HTML file) to display this section and customize its color, such as the color of the button, text, window's background, links, borders, and so on. Select a color that you want to use and click the **Select** button.
HTML/CSS	This shows the HTML file name of the portal page created for the selected custom theme. This also shows the name of the CSS files created for the selected custom theme. Click an HTML file to display the portal page. You can also change colors and modify the CSS values of the selected HTML file.
< >	Click this button to view and modify the CSS values of the selected HTML file. It is recommended that you do NOT change the script code to ensure proper operation of the portal page.
◎	Click this button to preview the portal page (the selected HTML file).
Save	Click this button to save your settings for the selected HTML file to the NCC.
Apply	Click this button to save your settings for the selected HTML file to the NCC and apply them to the Nebula Device in the site.

9.3.9 Network Access Method

Use this screen to enable or disable web authentication on an interface.

Click **Site-wide** > **Configure** > **Security gateway** > **Network access method** to access this screen.

Figure 223 Site-wide > Configure > Security gateway > Network access method



Network access method

Interfaces: LAN1

Network Access

○ Disable

Users can access the network directly

○ Click-to-continue

Users must view and agree the captive portal page then can access the network

● Sign-on-with Nebula Cloud Authentication

Walled garden on

Walled garden ranges

What do I enter here?

One IP address/domain in one line to specify your walled garden.
Example:
*.zyxel.com
www.zyxel.com
192.168.1.0/24

Captive portal access attribute

Self-registration: Allow users to create accounts with auto authorized

Login on multiple client devices: Multiple devices access simultaneously

NCAS disconnection behavior

● Allowed:
Client devices can access the network without signing in, except they are explicitly blocked

○ Limited:
Only currently authorized clients and whitelisted client devices will be able to access the network

The following table describes the labels in this screen.

Table 164 Site-wide > Configure > Security gateway > Network access method

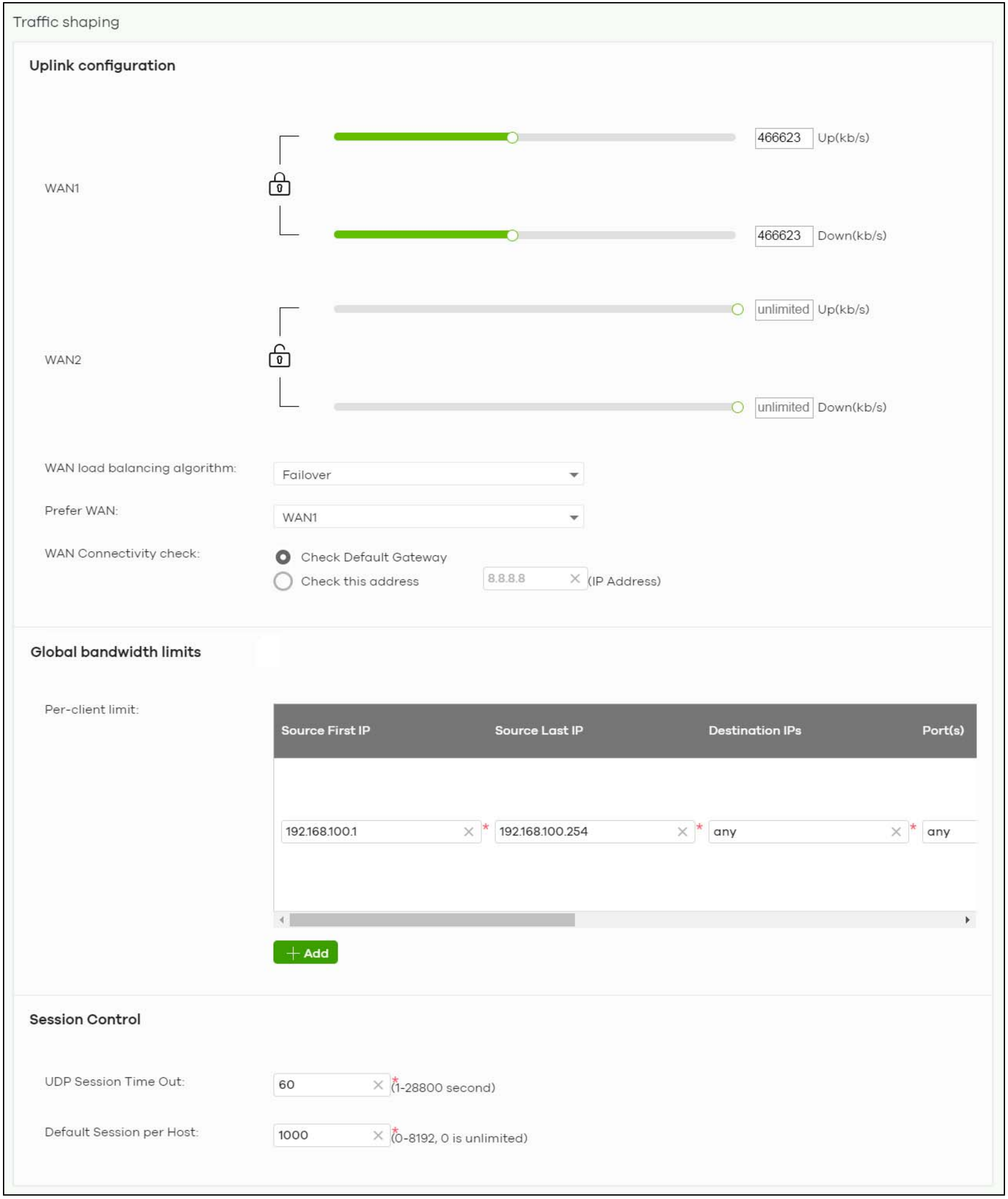
LABEL	DESCRIPTION
Interfaces	Select the Nebula Device's interface (network) to which the settings you configure here is applied.
Network Access	Select **Disable** to turn off web authentication. Select **Click-to-continue** to block network traffic until a client agrees to the policy of user agreement. Select **Sign-on with** to block network traffic until a client authenticates with an external RADIUS or AD server through the specifically designated web portal page. Select **Nebula Cloud Authentication** or an authentication server that you have configured in the **Site-wide** > **Configure** > **Security gateway** > **Gateway settings** screen (see Section 9.3.11 on page 627). Select Two-Factor Authentication to require that the user log in using both their password and a Google Authenticator code. To log in, users must have Two-Factor Authentication enabled on their account and have setup Google Authenticator on their mobile device.
Walled garden	This field is not configurable if you set **Network Access** to **Disable**. Select to turn on or off the walled garden feature. With a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example.
Walled garden ranges	Specify walled garden web site links, which use a domain name or an IP address for web sites that all users are allowed to access without logging in.
Captive portal access attribute	
Self-registration	This field is available only when you select **Sign-on with Nebula Cloud authentication** in the **Network Access** field. Select **Allow users to create accounts with auto authorized** or **Allow users to create accounts with manual authorized** to display a link in the captive portal login page. The link directs users to a page where they can create an account before they authenticate with the NCC. For **Allow users to create accounts with manual authorized**, users cannot log in with the account until the account is authorized and granted access. For **Allow users to create accounts with auto authorized**, users can just use the registered account to log in without administrator approval. Select **Don't allow users to create accounts** to not display a link for account creation in the captive portal login page.
Login on multiple client devices	This field is available only when you select **Sign-on with** in the **Network Access** field. Select **Multiple devices access simultaneously** if you allow users to log in as many times as they want as long as they use different IP addresses. Select **One device at a time** if you do NOT allow users to have simultaneous logins.
NCAS disconnection behavior	This field is available only when you select **Sign-on with Nebula Cloud Authentication** in the **Network Access** field. Select **Allowed** to allow any users to access the network without authentication when the NCAS (Nebula Cloud Authentication Server) is not reachable. Select **Limited** to allow only the currently connected users or the users in the white list to access the network.

9.3.10 Traffic Shaping

Use this screen to configure maximum bandwidth and load balancing on the Nebula Device.

Click **Site-wide** > **Configure** > **Security gateway** > **Traffic shaping** to access this screen.

Figure 224 Site-wide > Configure > Security gateway > Traffic shaping



Traffic shaping

Uplink configuration

WAN1: 466623 Up(kb/s), 466623 Down(kb/s)

WAN2: unlimited Up(kb/s), unlimited Down(kb/s)

WAN load balancing algorithm: Failover

Prefer WAN: WAN1

WAN Connectivity check:
● Check Default Gateway
○ Check this address 8.8.8.8 (IP Address)

Global bandwidth limits

Per-client limit:

Source First IP	Source Last IP	Destination IPs	Port(s)
192.168.100.1 *	192.168.100.254 *	any *	any

Session Control

UDP Session Time Out: 60 * (1-28800 second)

Default Session per Host: 1000 * (0-8192, 0 is unlimited)

The following table describes the labels in this screen.

Table 165 Site-wide > Configure > Security gateway > Traffic shaping

LABEL	DESCRIPTION
Uplink configuration	
WAN 1 WAN 2	Set the amount of upstream/downstream bandwidth for the WAN interface. Click a lock icon to change the lock state. If the lock icon for a WAN interface is locked, the bandwidth limit you set applies to both inbound and outbound traffic. If the lock is unlocked, you can set inbound and outbound traffic to have different transmission speeds.
WAN load balancing algorithm	Select a load balancing method to use from the drop-down list box. • Select **Least Load First** to send new session traffic through the least utilized WAN interface. • Select **Round Robin** to balance the traffic load between interfaces based on their respective weights (bandwidth). An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of WAN 1 and WAN 2 interfaces is 2:1, the Nebula Device chooses WAN 1 for two sessions' traffic and WAN 2 for one session's traffic in each round of three new sessions. • Select **Failover** to send traffic through a second WAN interface when the primary WAN interface is down or disabled.
Prefer WAN	Specify the primary WAN interface through which the Nebula Device forwards traffic. This field is available when you set **WAN load balancing algorithm** to **Failover**.
WAN Connectivity check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. The Nebula Device resumes routing to the gateway the first time the gateway passes the connectivity check. If the WAN connection is down (the check fails), the Nebula Device will switch (failover) to use a redundant WAN connection. • Select **Check Default Gateway** to use the default gateway for the connectivity check. • Select **Check this address** to specify a domain name or IP address for the connectivity check. Note: If you select **Check this address** but the IP address you specified cannot be reached through the primary WAN interface, the Nebula Device will switch to the other one even if the primary WAN connection is still up. Make sure your Nebula Device supports multiple WAN interfaces and both WAN connections are configured properly before you select **Check this address**. This field is available when you set **WAN load balancing algorithm** to **Failover**.
Global bandwidth limits	
Per-client limit	You can limit a client's outbound or inbound bandwidth.
Source First IP	Enter the first IP address in a range of source IP addresses for which the Nebula Device applies the rule.
Source Last IP	Enter the last IP address in a range of source IP addresses for which the Nebula Device applies the rule.
Destination IPs	Enter the destination IP addresses for which the Nebula Device applies the rule. Enter **any** if the rule is effective for every destination.
Port(s)	Enter the port numbers (1 – 65535) to which the packets go. The Nebula Device applies the rule to the packets that go to the corresponding service port. **any** means all service ports.
Protocol	Select **TCP** or **UDP** if you want to specify a protocol for the rule. Otherwise select **Any**. **Any** means the rule is applicable to all services.

Table 165 Site-wide > Configure > Security gateway > Traffic shaping (continued)

LABEL	DESCRIPTION
Down/Up	Set the maximum upstream/downstream bandwidth for traffic from an individual source IP address. Click a lock icon to change the lock state. If the lock icon is locked, the bandwidth limit you set applies to both inbound and outbound traffic. If the lock is unlocked, you can set inbound and outbound traffic to have different transmission speeds.
Priority	Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority.
🗑	Click this icon to remove the rule.
Add	Click this button to create a new rule.
Session Control	
UDP Session Time Out	Set how many seconds the Nebula Device will allow a UDP session to remain idle (without UDP traffic) before closing it.
Default Session per Host	Set a common limit to the number of concurrent NAT/Security Policy sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.

9.3.11 Gateway Settings

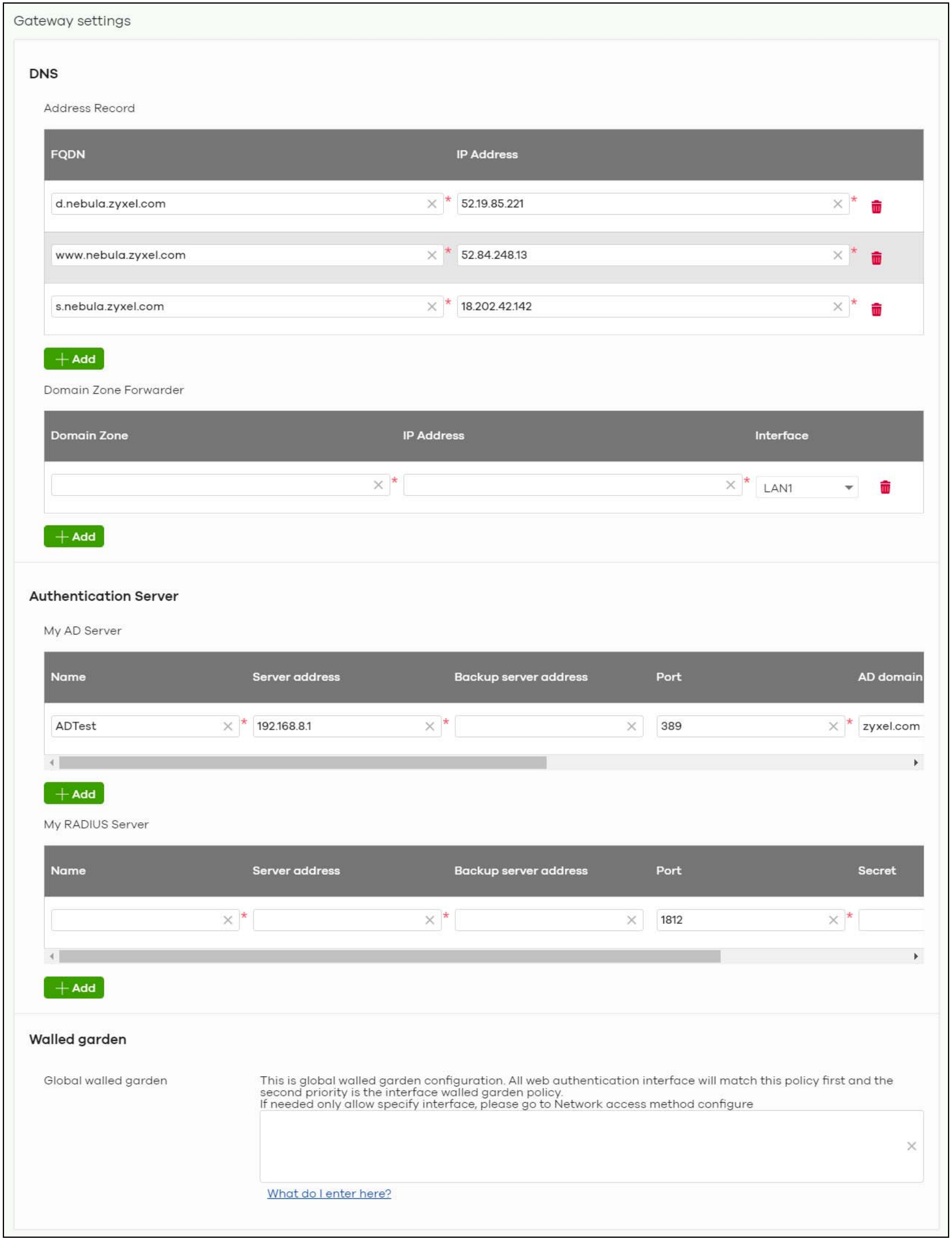
Use this screen to configure DNS settings and external AD (Active Directory) server or RADIUS server that the Nebula Device can use in authenticating users.

AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.

This screen also lets you configure the addresses of walled garden web sites that users can access without logging into the Nebula Device. The settings in this screen apply to all networks (interfaces) on the Nebula Device. If you want to configure walled garden web site links for a specific interface, use the **Network access method** screen.

Click **Site-wide** > **Configure** > **Security gateway** > **Gateway settings** to access this screen.

Figure 225 Site-wide > Configure > Security gateway > Gateway settings



Gateway settings

DNS

Address Record

FQDN	IP Address
d.nebula.zyxel.com	52.19.85.221
www.nebula.zyxel.com	52.84.248.13
s.nebula.zyxel.com	18.202.42.142

+ Add

Domain Zone Forwarder

Domain Zone	IP Address	Interface
		LAN1

+ Add

Authentication Server

My AD Server

Name	Server address	Backup server address	Port	AD domain
ADTest	192.168.8.1		389	zyxel.com

+ Add

My RADIUS Server

Name	Server address	Backup server address	Port	Secret
			1812	

+ Add

Walled garden

Global walled garden

This is global walled garden configuration. All web authentication interface will match this policy first and the second priority is the interface walled garden policy.
If needed only allow specify interface, please go to Network access method configure

What do I enter here?

The following table describes the labels in this screen.

Table 166   Site-wide > Configure > Security gateway > Gateway settings

LABEL	DESCRIPTION
DNS	
Address Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.
FQDN	Enter a host’s fully qualified domain name. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the host’s IP address.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Domain Zone Forwarder	This specifies a DNS server’s IP address. The Nebula Device can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the Nebula Device needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. Whenever the Nebula Device needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address.
IP Address	Enter the DNS server's IP address.
Interface	Select the interface through which the Nebula Device sends DNS queries to the specified DNS server.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Authentication Server My AD Server	
Name	Enter a descriptive name for the server.
Server address	Enter the address of the AD server.
Backup server address	If the AD server has a backup server, enter its address here.
Port	Specify the port number on the AD server to which the Nebula Device sends authentication requests. Enter a number between 1 and 65535.
AD domain	Specify the Active Directory forest root domain name.
Domain admin	Enter the name of the user that is located in the container for Active Directory Users, who is a member of the Domain Admin group.
Password	Enter the password of the Domain Admin user account.
Advanced	Click to open a screen where you can select to use **Default** or **Custom** advanced settings. See Section 9.3.11.1 on page 630.
🗑	Click this icon to remove the server.
Add	Click this button to create a new server.
My RADIUS server	
Name	Enter a descriptive name for the server.
Server address	Enter the address of the RADIUS server.
Backup server address	If the RADIUS server has a backup server, enter its address here.

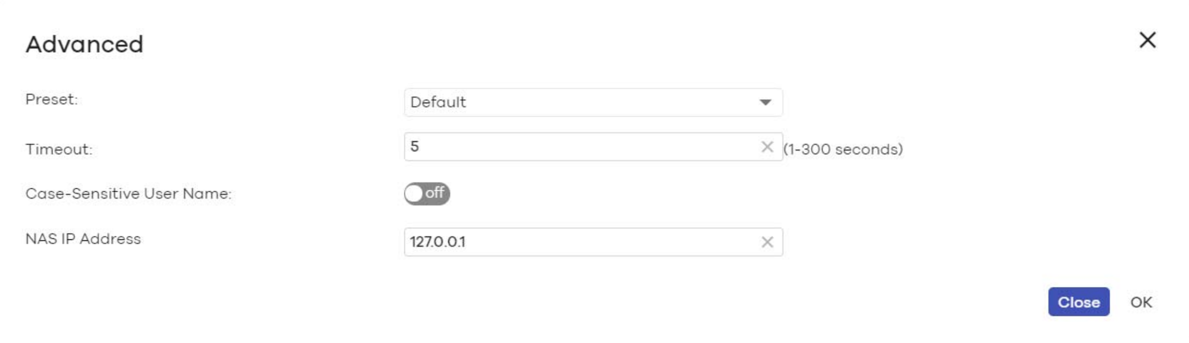
Table 166   Site-wide > Configure > Security gateway > Gateway settings (continued)

LABEL	DESCRIPTION
Port	Specify the port number on the RADIUS server to which the Nebula Device sends authentication requests. Enter a number between 1 and 65535.
Secret	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the Nebula Device. The key is not sent over the network. This key must be the same on the external authentication server and the Nebula Device.
Advanced	Click to open a screen where you can select to use **Default** or **Custom** advanced settings. See Section 9.3.11.1 on page 630.
🗑	Click this icon to remove the server.
Add	Click this button to create a new server.
Walled garden	
Global Walled garden	With a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example. Specify walled garden web site links, which use a domain name or an IP address for web sites that all users are allowed to access without logging in.

9.3.11.1 Advanced Settings

Click the **Advanced** column in the **Site-wide** > **Configure** > **Security gateway** > **Gateway settings** screen to access this screen.

Figure 226   Site-wide > Configure > Security gateway > Gateway settings: Advanced



Advanced

Preset: Default

Timeout: 5 (1-300 seconds)

Case-Sensitive User Name: off

NAS IP Address 127.0.0.1

The following table describes the labels in this screen.

Table 167   Site-wide > Configure > Security gateway > Gateway settings: Advanced

LABEL	DESCRIPTION
Preset	Select **Default** to use the pre-defined settings, or select **Custom** to configure your own settings.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the Nebula Device disconnects from the server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the servers or the AD or server is down.
Case-Sensitive User Name	Click **ON** if the server checks the case of the user name. Otherwise, click **OFF** to not configure your user name as case-sensitive.
NAS IP Address	This field is only for RADIUS. Enter the IP address of the NAS (Network Access Server).

Table 167   Site-wide > Configure > Security gateway > Gateway settings: Advanced (continued)

LABEL	DESCRIPTION
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

CHAPTER 10
Mobile Router

10.1 Overview

This chapter discusses the menus that you can use to monitor the Nebula-managed Mobile Routers in your network and configure settings even before a Mobile Router is deployed and added to the site.

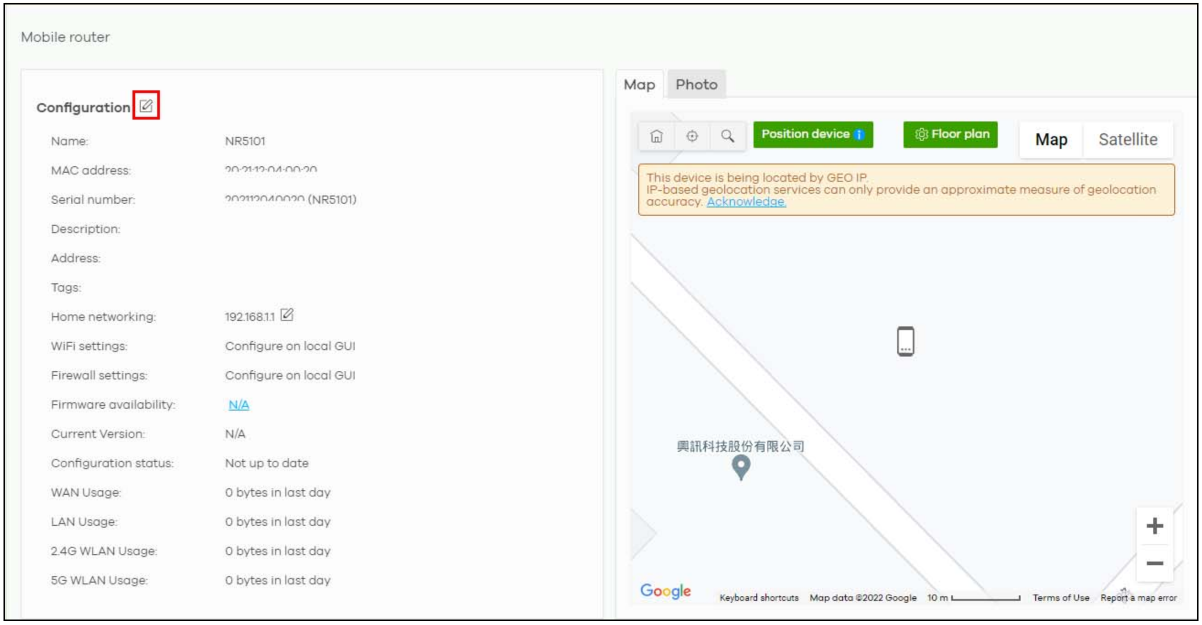
A Nebula Mobile Router is an LTE or NR cellular 5G indoor or outdoor router that can be managed by Nebula. It is referred to as a Nebula Device in this chapter.

10.2 Configuration

From the navigation panel, click **Site-wide** > **Devices** > **Mobile router** and the following screen appears. The **Configuration** screen allows you to view the information of your indoor or outdoor Nebula Device in a selected site. To edit the **Name**, **MAC address**, **Serial number**, **Description**, **Address**, and **Tags** of your Nebula Device, click the edit icon (✎) in the **Configuration** field.

Note: Only one Mobile Router is allowed per site.

Figure 227 Site-wide > Devices > Mobile router > Configuration (Indoor)



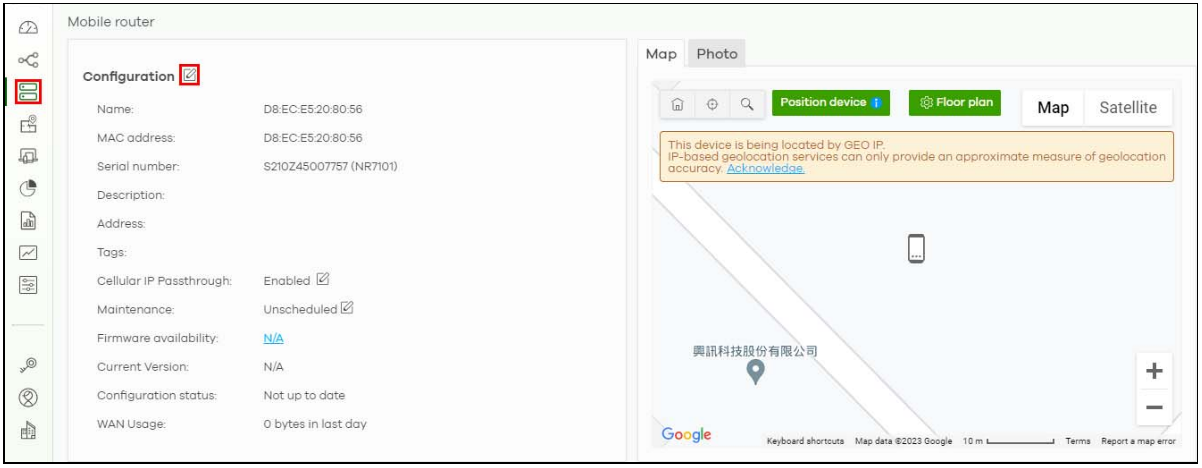
Mobile router

Configuration ✎

Name:	NR5101
MAC address:	20:21:12:04:00:20
Serial number:	202112040020 (NR5101)
Description:	
Address:	
Tags:	
Home networking:	192.168.1.1 ✎
WiFi settings:	Configure on local GUI
Firewall settings:	Configure on local GUI
Firmware availability:	N/A
Current Version:	N/A
Configuration status:	Not up to date
WAN Usage:	0 bytes in last day
LAN Usage:	0 bytes in last day
2.4G WLAN Usage:	0 bytes in last day
5G WLAN Usage:	0 bytes in last day

This device is being located by GEO IP.
IP-based geolocation services can only provide an approximate measure of geolocation accuracy. Acknowledge.

Figure 228 Site-wide > Devices > Mobile router > Configuration (Outdoor)



Mobile router

Configuration

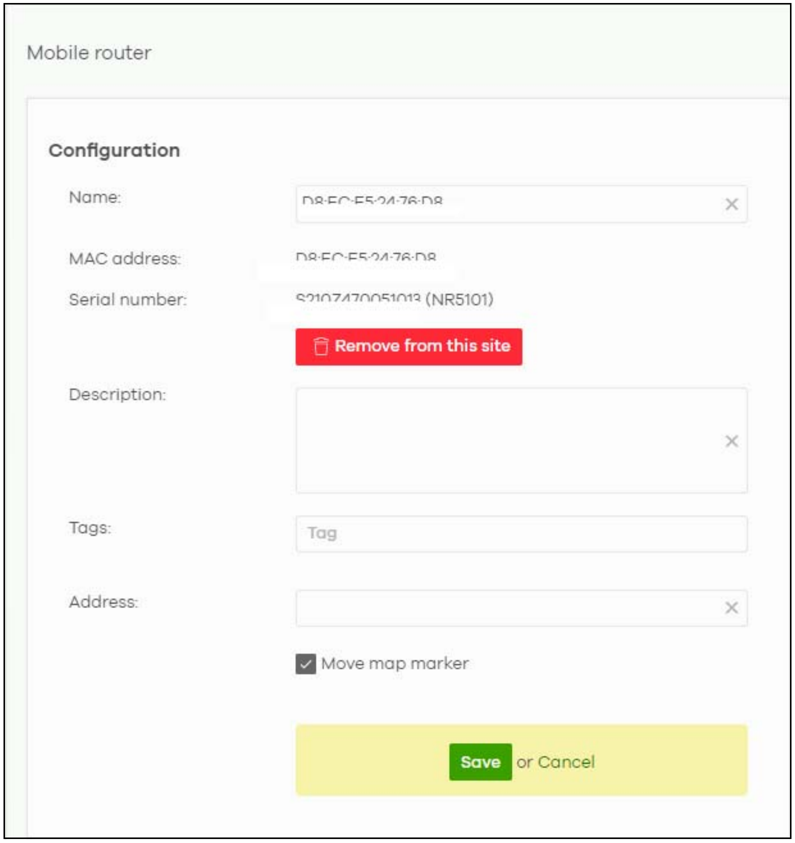
Name:	D8:EC:E5:20:80:56
MAC address:	D8:EC:E5:20:80:56
Serial number:	S210Z45007757 (NR7101)
Description:	
Address:	
Tags:	
Cellular IP Passthrough:	Enabled
Maintenance:	Unscheduled
Firmware availability:	N/A
Current Version:	N/A
Configuration status:	Not up to date
WAN Usage:	0 bytes in last day

This device is being located by GEO IP.
IP-based geolocation services can only provide an approximate measure of geolocation accuracy. Acknowledge.

10.2.1 Configuration: Edit

The following screen displays after you click the edit icon. Use the **Site-wide** > **Devices** > **Mobile router** > **Configuration**: **Edit** screen to configure your indoor and outdoor Nebula Device information. You can also move the Nebula Device to another site.

Figure 229 Site-wide > Devices > Mobile router > Configuration: Edit



Mobile router

Configuration

Name:	D8:EC:E5:24:76:D8
MAC address:	D8:EC:E5:24:76:D8
Serial number:	S2107470051013 (NR5101)
Description:	
Tags:	Tag
Address:	

☑ Move map marker

The following table describes the labels in this screen.

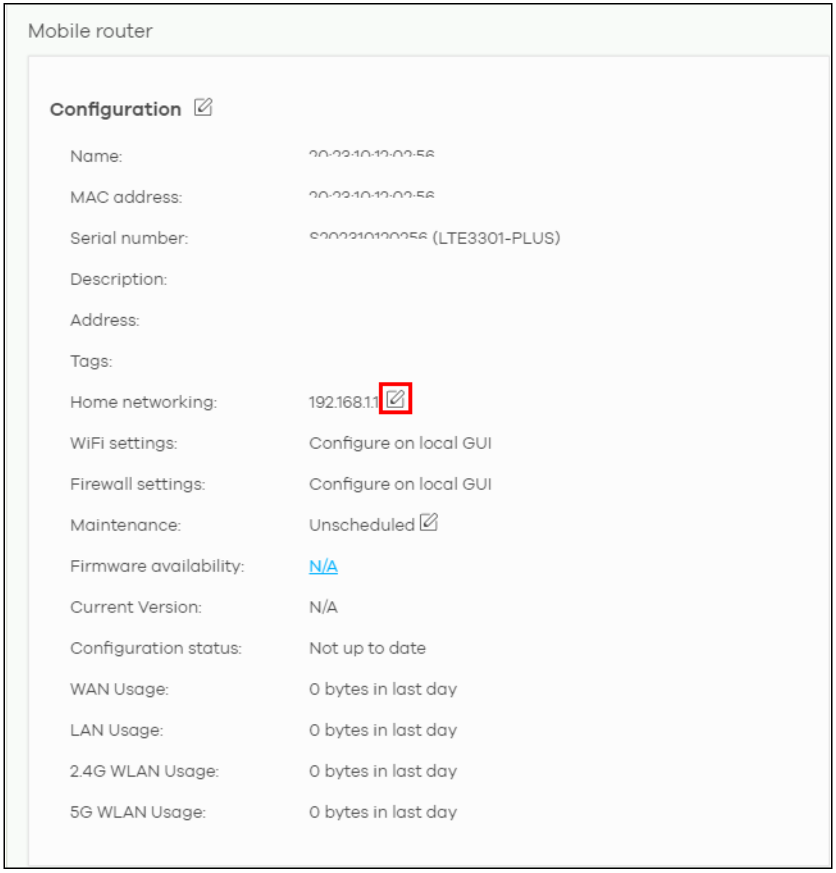
Table 168   Site-wide > Devices > Mobile router > Configuration: Edit

LABEL	DESCRIPTION
Configuration	
Name	Enter a descriptive name for the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
Serial number	This shows the serial number of the Nebula Device.
Description	Enter a user-specified description for the Nebula Device.
Tags	Enter a user-specified tag for the Nebula Device.
Address	Enter a user-specified address for the Nebula Device.
Save	Click **Save** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.2.2 Home Networking

To configure the **Home networking** setting, click the edit icon (✎) in the **Home networking** field.

Figure 230   Site-wide > Devices > Mobile router > Configuration: Home networking (Indoor)



Mobile router

Configuration ✎

Name: 20:23:10:12:02:56

MAC address: 20:23:10:12:02:56

Serial number: S202310120256 (LTE3301-PLUS)

Description:

Address:

Tags:

Home networking: 192.168.1.1 ✎

WiFi settings: Configure on local GUI

Firewall settings: Configure on local GUI

Maintenance: Unscheduled ✎

Firmware availability: N/A

Current Version: N/A

Configuration status: Not up to date

WAN Usage: 0 bytes in last day

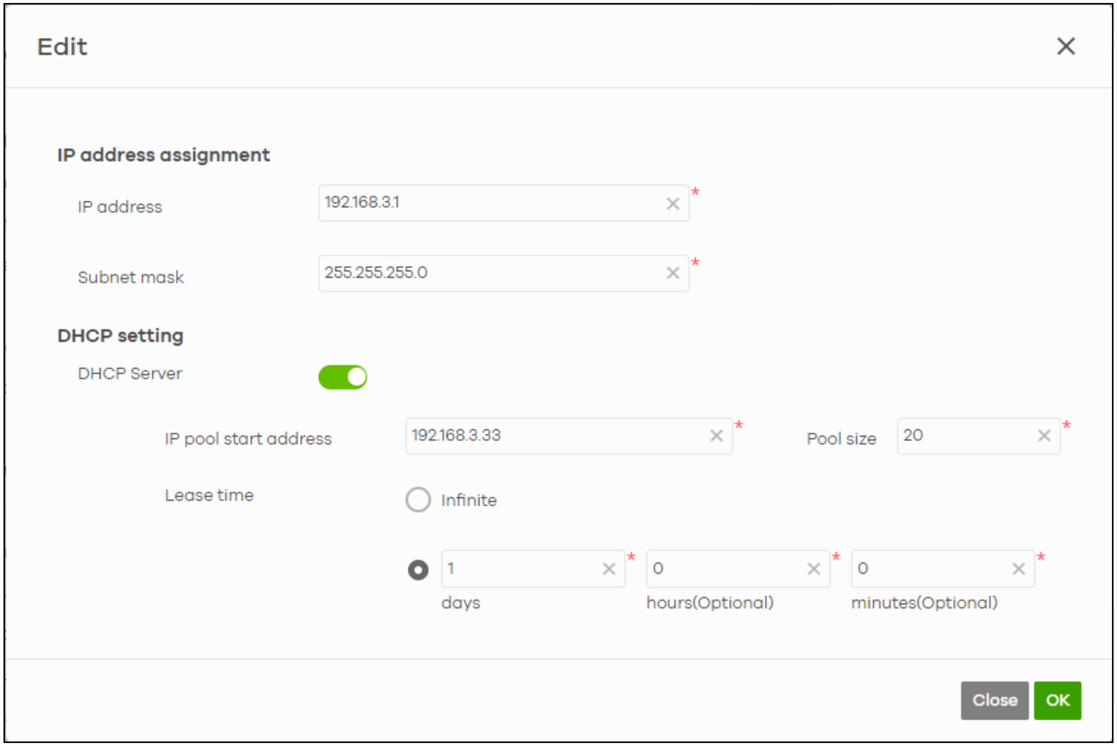
LAN Usage: 0 bytes in last day

2.4G WLAN Usage: 0 bytes in last day

5G WLAN Usage: 0 bytes in last day

The following **Site-wide** > **Devices** > **Mobile router** > **Configuration** > **Home networking**: **Edit** screen displays. Use this screen to configure the LAN IP address and DHCP server settings of your indoor Nebula Device.

Figure 231 Site-wide > Devices > Mobile router > Configuration > Home networking: Edit



Edit

IP address assignment

IP address: 192.168.3.1 *

Subnet mask: 255.255.255.0 *

DHCP setting

DHCP Server: on

IP pool start address: 192.168.3.33 *

Pool size: 20 *

Lease time: ○ Infinite

● 1 * days, 0 * hours(Optional), 0 * minutes(Optional)

The following table describes the labels in this screen.

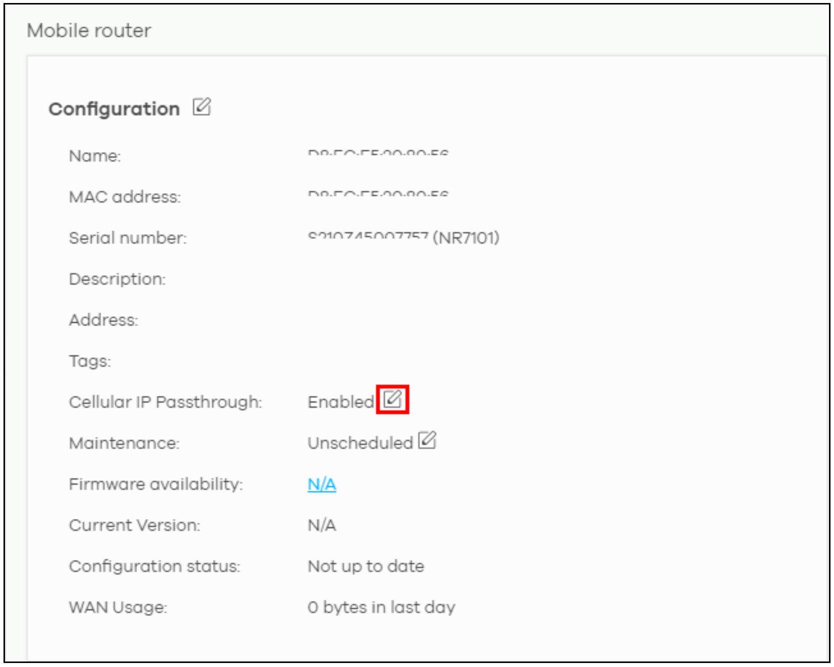
Table 169 Site-wide > Devices > Mobile router > Configuration > Home networking: Edit

LABEL	DESCRIPTION
IP address assignment	
IP address	Enter the IP address for this interface. Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
DHCP setting	
DHCP Server	Select this to disable or enable the DHCP server.
IP pool start address	Enter the IP address from which the Nebula Device begins allocating IP addresses.
Pool size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet mask**. For example, if the Subnet mask is 255.255.255.0 and IP pool start address is 10.10.10.10, the security gateway can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **Infinite** – select this if IP addresses never expire; **days**, **hours**, **minutes** – select this to enter how long IP addresses are valid.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

10.2.3 Cellular IP Passthrough

To configure the cellular IP passthrough setting, click the edit icon (✎) in the **Cellular IP Passthrough** field. IP passthrough allows a LAN computer on the local network of the Nebula Device to have access to web services using a public IPv4 address. When IP passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.

Figure 232 Site-wide > Devices > Mobile router > Configuration: Cellular IP Passthrough (Outdoor)



Mobile router

Configuration ✎

Name: [illegible]

MAC address: [illegible]

Serial number: S210745007757 (NR7101)

Description:

Address:

Tags:

Cellular IP Passthrough: Enabled ✎

Maintenance: Unscheduled ✎

Firmware availability: N/A

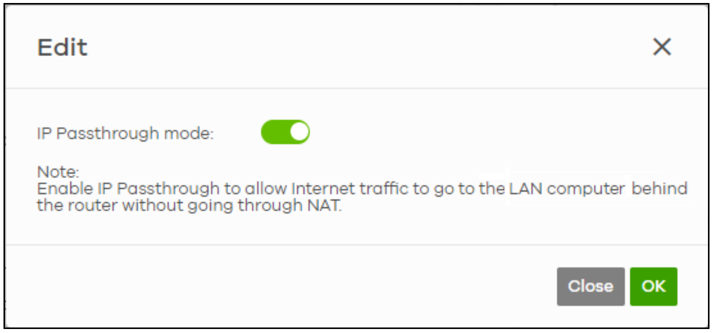
Current Version: N/A

Configuration status: Not up to date

WAN Usage: 0 bytes in last day

The following **Site-wide** > **Devices** > **Mobile router** > **Configuration** > **Cellular IP Passthrough**: **Edit** screen displays. Use this screen to disable or enable IP passthrough on your outdoor Nebula Device. Slide the switch to the right to enable IP passthrough.

Figure 233 Site-wide > Devices > Mobile router > Configuration > Cellular IP Passthrough: Edit



IP Passthrough mode: ●

Note:
Enable IP Passthrough to allow Internet traffic to go to the LAN computer behind the router without going through NAT.

The following table describes the labels in this screen.

Table 170 Site-wide > Devices > Mobile router > Configuration > Cellular IP Passthrough: Edit

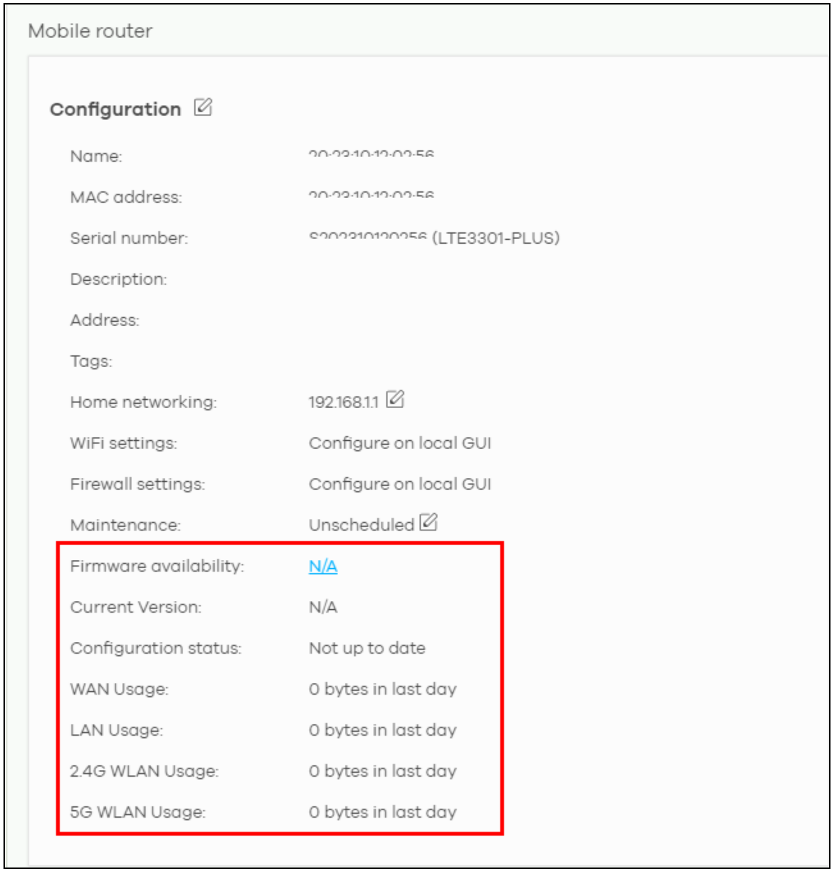
LABEL	DESCRIPTION
IP Passthrough mode	This displays if IP passthrough is enabled on the Nebula Device.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

10.2.4 Firmware Status

Go back to the **Site-wide** > **Devices** > **Mobile router** > **Configuration** screen to view the firmware version and WAN/LAN/WLAN usage of your indoor or outdoor Nebula Device.

Note: **LAN Usage**, **2.4G WLAN Usage** and **5G WLAN Usage** are only available for indoor Nebula Devices.

Figure 234 Site-wide > Devices > Mobile router > Configuration > Firmware status



Mobile router

Configuration

Name: 20:23:10:12:02:56

MAC address: 20:23:10:12:02:56

Serial number: S202310120256 (LTE3301-PLUS)

Description:

Address:

Tags:

Home networking: 192.168.1.1

WiFi settings: Configure on local GUI

Firewall settings: Configure on local GUI

Maintenance: Unscheduled

Firmware availability: N/A

Current Version: N/A

Configuration status: Not up to date

WAN Usage: 0 bytes in last day

LAN Usage: 0 bytes in last day

2.4G WLAN Usage: 0 bytes in last day

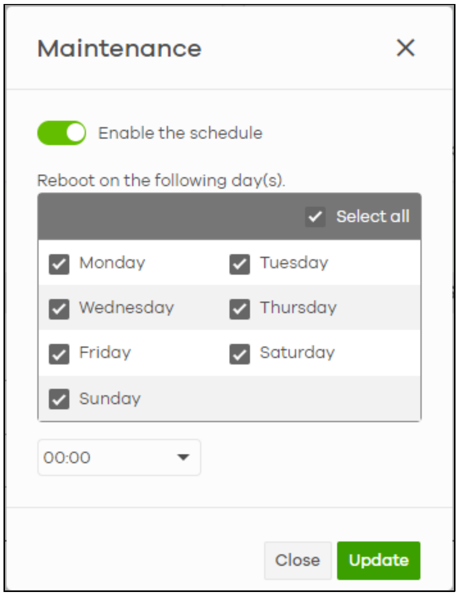
5G WLAN Usage: 0 bytes in last day

The following table describes the labels in this screen.

Table 171 Site-wide > Devices > Mobile router > Configuration > Firmware status

LABEL	DESCRIPTION
WiFi settings	Configure the Nebula Device's WiFi settings using its Web Configurator. Refer to the Nebula Device's User's Guide for more information. Note: This field is NOT configurable.
Firewall settings	Configure the Nebula Device's firewall settings using its Web Configurator. Refer to the Nebula Device's User's Guide for more information. Note: This field is NOT configurable.
Maintenance	This shows whether automatic reboot is scheduled on the Nebula Device.

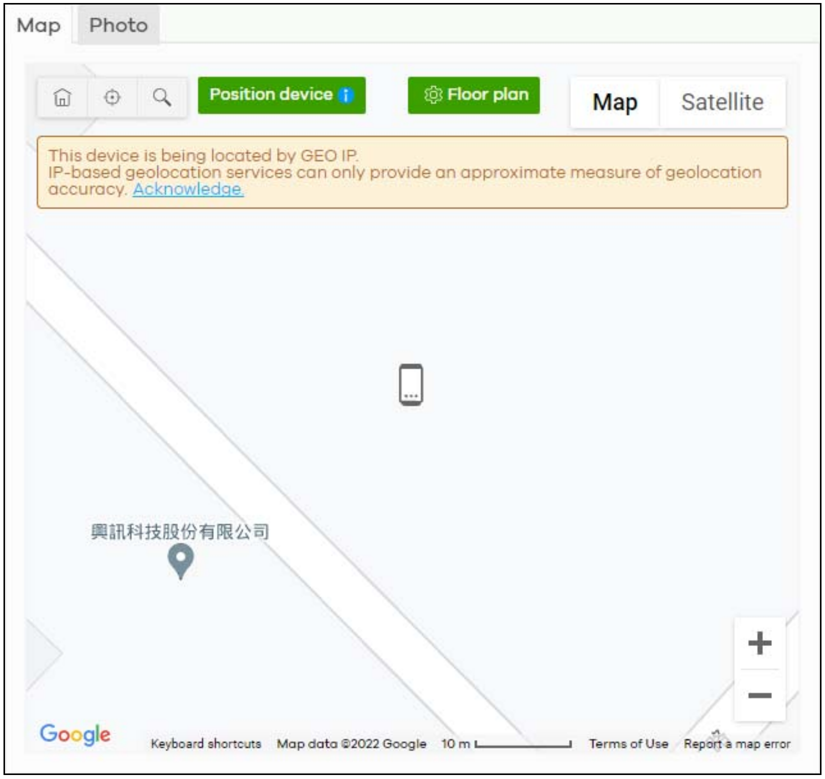
Table 171 Site-wide > Devices > Mobile router > Configuration > Firmware status (continued)

LABEL	DESCRIPTION
Edit	Click the **Enable the schedule** switch to the right to have the Nebula Device restart at a specific time on selected days of the week. By scheduling a reboot, you can have the Nebula Device refresh the network connections at a specified time, allowing automatic reconnection with WiFi clients in case of a connection failure. Select the day(s) of the week to have the automatic restart. Specify the time of the day (in 24-hour format) to have the Nebula Device automatically restart. For example, 23:00 is 11:00 PM.  Maintenance Enable the schedule Reboot on the following day(s). ☑ Select all ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday 00:00 Close Update
Firmware availability	The NCC automatically detects whether the firmware is up-to-date or not. Click the value in the **Firmware availability** field to go to the **Site-wide** > **Configure** > **Firmware management** screen and configure your Firmware management settings.
Current Version	This shows the firmware version currently installed on the Nebula Device.
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
WAN Usage	This shows the total amount of data consumed by the Nebula Device on the WAN (uplink/downlink) in the past 24 hours.
LAN Usage (indoor NCCs only)	This shows the total amount of data consumed by the Nebula Device on the LAN (upllink/downlink) in the past 24 hours.
2.4G WLAN Usage (indoor NCCs only)	This shows the total amount of data consumed by the Nebula Device on the 2.4G WiFi network (uplink/downlink) in the past 24 hours.
5G WLAN Usage (indoor NCCs only)	This shows the total amount of data consumed by the Nebula Device on the 5G WiFi network (uplink/downlink) in the past 24 hours.

10.3 Map/Photo

Click the **Map** tab. This shows the location of the Nebula Device on Google map. To upload a photo of the Nebula Device, select the **Photo** tab.

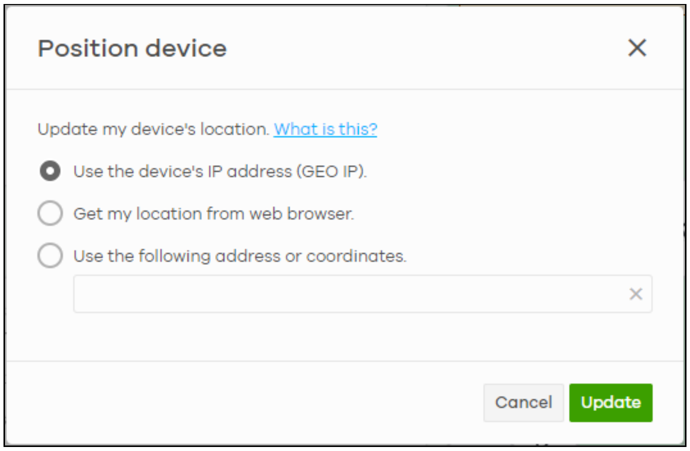
Figure 235 Site-wide > Devices > Mobile router > Map



This device is being located by GEO IP.
IP-based geolocation services can only provide an approximate measure of geolocation accuracy. Acknowledge.

The following table describes the labels in this screen.

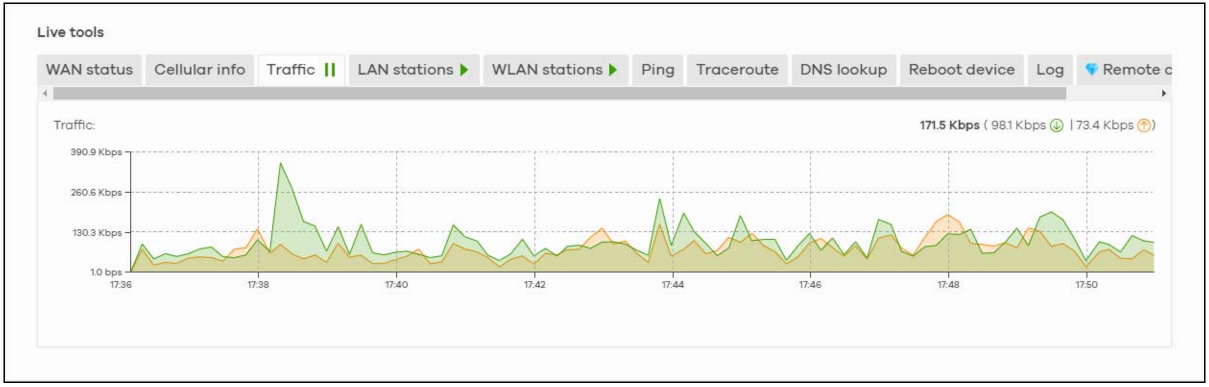
Table 172   Site-wide > Devices > Mobile router > Map/Photo

LABEL	DESCRIPTION
Map	This shows the location of the Nebula Device on Google Maps (**Map** view or **Satellite** imagery view) or on a floor plan. Click **Floor plan** to display a list of existing floor plans. Each floor plan has a drawing that shows the rooms scaled and viewed from above. Drag-and-drop your Nebula Device directly on the Google map or click **Position device** to update the Nebula Device's address (physical location).  Position device Update my device's location. What is this? ● Use the device's IP address (GEO IP). ○ Get my location from web browser. ○ Use the following address or coordinates. - Select **GEO IP** to use the public IP address of the Nebula Device. - Select **Get my location from web browser** to use the public IP address of the computer accessing the NCC portal. - Select **Use the following address or coordinates** to enter the complete address or coordinates of the Nebula Device. Note: Nebula Devices that are offline cannot use GEO IP.
Photo	This shows the photo of the Nebula Device. Click **Add** to upload up to five photos of your Nebula Device. Click the remove icon (🗑) to delete a photo.

10.4 Live Tools

Use live tools to view various interface information, system/security logs, perform diagnostics, reboot or establish a remote connection to the Nebula Device.

Figure 236   Site-wide > Devices > Mobile router > Live tools > Traffic (Example)



Live tools

Note: In the **Traffic**, **LAN stations**, and **WLAN stations** screens, click the pause icon (⏸) to stop getting data for the respective screens. Alternatively, click the play icon (▶) to continue.

The following table describes the labels in this screen.

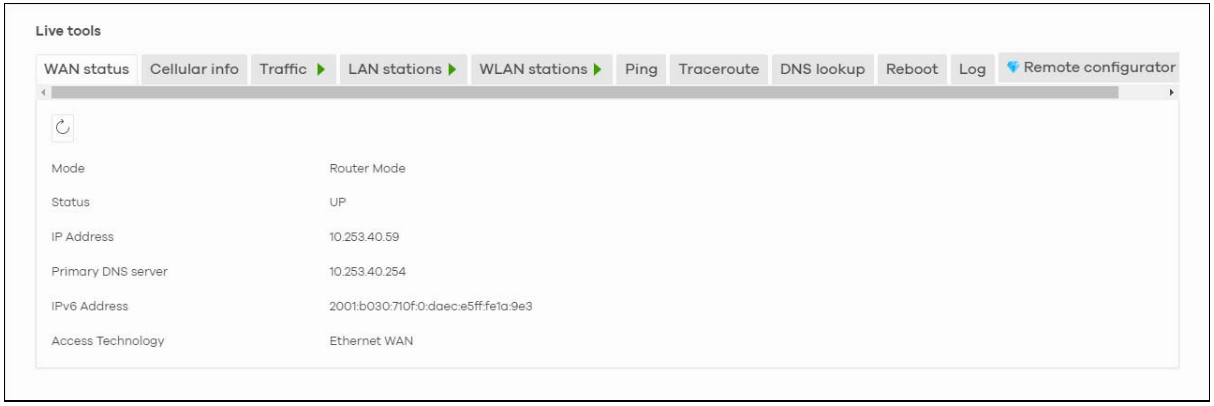
Table 173 Site-wide > Devices > Mobile router > Live tools

LABEL	DESCRIPTION
WAN status	This shows the connection status of the Ethernet WAN interface. See Section 10.4.1 on page 641 for more information.
Cellular info	This shows the connection status of the cellular WAN interface. See Section 10.4.2 on page 642 for more information.
Traffic	This shows the Nebula Device traffic statistics. The y-axis represents the transmission rate for uplink and downlink traffic. The x-axis represents the time period over which the traffic flow occurred.
LAN stations	This shows the Nebula Device's connected LAN clients' **MAC address** and **IPv4 Address**.
WLAN stations (indoor NCCs only)	This shows the Nebula Device's connected WiFi clients' **MAC address**, **SSID name**, **IPv4 address**, **Signal strength**, **Security**, **Channel**, **Tx rate**, **Rx rate**, **Tx/Rx**, and **Capability.** See Section 10.4.4 on page 649 for more information.
Ping	Enter the hostname or IP address of a computer that you want to perform ping from the Nebula Device in order to test a connection and click **Ping**. This can be used to determine if the Nebula Device and the computer are able to communicate with each other.
Traceroute	Enter the domain name or IP address of a computer that you want to perform traceroute from the Nebula Device and click **Run**. This determines the path a packet takes to the specified computer.
DNS lookup	Enter a host domain name and click **Run** to resolve the IP address for the specified domain name.
Reboot device	Click this button to restart the Nebula Device.
Log	Select this to display **System log** and **Security log** entries in the past 24 hours.
Remote configurator	Click **Establish** to use TCP (Transmission Control Protocol) port 443 to establish a remote connection to this Nebula Device. The Nebula Device will create a reverse SSH (Secure SHell) connection. After clicking **Ok**, NCC will provide a remote connection IPv4 address and service port number. For example, https://63.35.218.205:31479. Use this IPv4 address and port to connect to the Nebula Device to open the Web Configurator. The remote session will be available for 30 minutes. In case the connection cannot be established, confirm that the network allows **Port 443**. Note: Remote configuration is only available if the Nebula Device is running the latest firmware. Otherwise, **Device firmware is not up to date, please update it.** will appear when you click **Establish**.

10.4.1 WAN Status

Go to the **Site-wide** > **Devices** > **Mobile router** > **Live tools** > **WAN status** screen to view the Ethernet WAN status of the Nebula Device.

Figure 237 Site-wide > Devices > Mobile router > Live tools > WAN status



Mode Router Mode

Status UP

IP Address 10.253.40.59

Primary DNS server 10.253.40.254

IPv6 Address 2001:b030:710f:0:daec:e5ff:fe1a:9e3

Access Technology Ethernet WAN

The following table describes the labels in this screen.

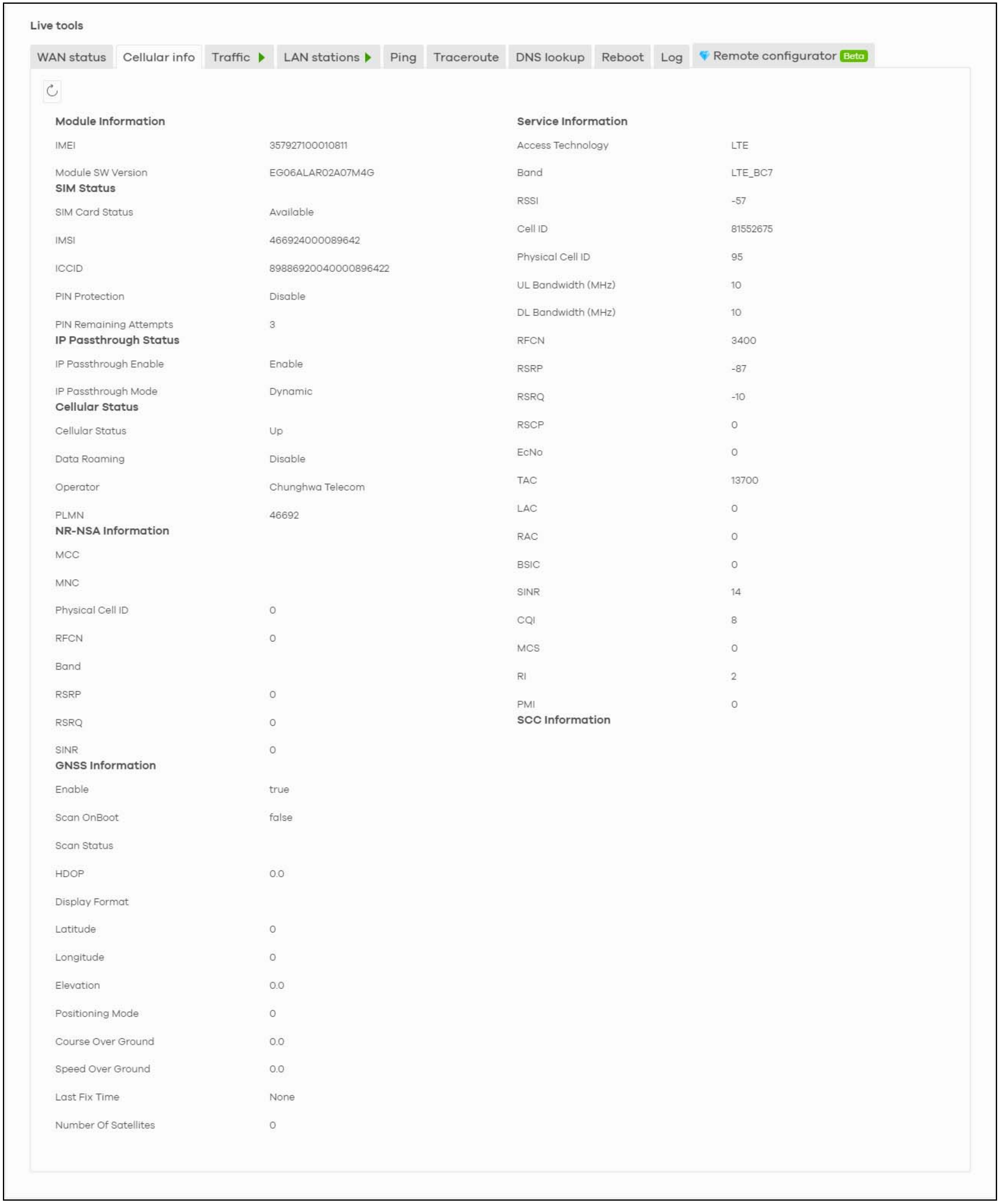
Table 174 Site-wide > Devices > Mobile router > Live tools > WAN status

LABEL	DESCRIPTION
↻	Click this button to reload the data-related frames on this page.
Mode	This displays which operating mode the Nebula Device is assigned to.
Status	This displays whether the Nebula Device is online/offline.
IP Address	This shows the LAN IPv4 address of the Nebula Device.
Primary DNS server	The shows the first DNS server address assigned by the ISP.
IPv6 Address	This shows the LAN IPv6 address of the Nebula Device.
Access Technology	This displays the type of the network (such as NR, LTE, Ethernet WAN) to which the Nebula Device is connecting.
Signal Strength	This show the signal strength of the Nebula Device.

10.4.2 Cellular Info

Go to the **Site-wide** > **Devices** > **Mobile router** > **Live tools** > **Cellular Info** screen to view the cellular WAN status of the Nebula Device.

Figure 238 Site-wide > Devices > Mobile router > Live tools > Cellular Info



Module Information

IMEI	357927100010811
Module SW Version	EG06ALAR02A07M4G

SIM Status

SIM Card Status	Available
IMSI	466924000089642
ICCID	89886920040000896422
PIN Protection	Disable
PIN Remaining Attempts	3

IP Passthrough Status

IP Passthrough Enable	Enable
IP Passthrough Mode	Dynamic

Cellular Status

Cellular Status	Up
Data Roaming	Disable
Operator	Chunghwa Telecom
PLMN	46692

NR-NSA Information

MCC	
MNC	
Physical Cell ID	0
RFCN	0
Band	
RSRP	0
RSRQ	0
SINR	0

GNSS Information

Enable	true
Scan OnBoot	false
Scan Status	
HDOP	0.0
Display Format	
Latitude	0
Longitude	0
Elevation	0.0
Positioning Mode	0
Course Over Ground	0.0
Speed Over Ground	0.0
Last Fix Time	None
Number Of Satellites	0

Service Information

Access Technology	LTE
Band	LTE_BC7
RSSI	-57
Cell ID	81552675
Physical Cell ID	95
UL Bandwidth (MHz)	10
DL Bandwidth (MHz)	10
RFCN	3400
RSRP	-87
RSRQ	-10
RSCP	0
EcNo	0
TAC	13700
LAC	0
RAC	0
BSIC	0
SINR	14
CQI	8
MCS	0
RI	2
PMI	0

SCC Information

The following table describes the labels in this screen.

Table 175 Site-wide > Devices > Mobile router > Live tools > Cellular Info

LABEL	DESCRIPTION
Module Information	
IMEI	This shows the International Mobile Equipment Identity of the Nebula Device.

Table 175 Site-wide > Devices > Mobile router > Live tools > Cellular Info (continued)

LABEL	DESCRIPTION
Module SW Version	This shows the software version of the cellular network module.
SIM Status	
SM Card Status	This displays the SIM card status: **None** – the Nebula Device does not detect that there is a SIM card inserted. **Available** – the SIM card could either have or does not have PIN code security. **Locked** – the SIM card has PIN code security, but you did not enter the PIN code yet. **Blocked** – you entered an incorrect PIN code too many times, so the SIM card has been locked. Call the ISP (Internet Service Provider) for a PUK (Pin Unlock Key) to unlock the SIM card. **Error** – the Nebula Device detected that the SIM card has errors.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the installed SIM card. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
ICCID	Integrated Circuit Card Identifier (ICCID). This is the serial number of the SIM card.
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. This field shows **Enable** if **PIN Protection** is enabled. Otherwise, this field shows **Disable**.
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
IP Passthrough Status	
IP Passthrough Enable	This displays if IP passthrough is enabled on the Nebula Device. IP passthrough allows a LAN computer on the local network of the Nebula Device to have access to web services using the public IP address. When IP passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.
IP Passthrough Mode	This displays the IP passthrough mode. This displays **Dynamic** and the Nebula Device will allow traffic to be forwarded to the first LAN computer requesting an IP address from the Nebula Device. This displays **Fixed** and the Nebula Device will allow traffic to be forwarded to a specific LAN computer on the local network of the Nebula Device.
Cellular Status	
Cellular Status	This displays the status of the cellular Internet connection.
Data Roaming	This displays if data roaming is enabled on the Nebula Device. 4G roaming is to use your NCC in an area which is not covered by your service provider. Enable roaming to ensure that your Nebula Device is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
Operator	This displays the name of the service provider.
PLMN	This displays the PLMN (Public Land Mobile Network) number.
NR-NSA Information	This displays the status of the cellular Internet connection.
MCC	This shows the Mobile Country Code (MCC). MCC is a unique code that identifies the country where a Public Land Mobile Network (PLMN) is at.
MNC	This shows the Mobile Network Code (MNC). MNC is a unique code that identifies a Public Land Mobile Network (PLMN) in a country. MCC and MNC combined together are used to identify a globally unique PLMN.
Physical Cell ID	This shows the Physical Cell ID (PCI), which are queries and replies between the Nebula Device and the mobile network it is connecting to. The normal range is 1 to 504.

Table 175 Site-wide > Devices > Mobile router > Live tools > Cellular Info (continued)

LABEL	DESCRIPTION
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Nebula Device is connecting. The value depends on the type of the mobile network (such as LTE, UMTS, GSM) to which the Nebula Device is connecting: • For UMTS (3G), it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101. • For LTE/5G, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. The value is '0' (zero) or 'N/A' if there is no network connection.
Band	This displays the current cellular band of your Nebula Device.
RSRP	This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Element (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth. The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214. The reporting range is specified in 3GPP-TS.36.133. An undetectable signal is indicated by the lower limit, example –140 dBm. This parameter is for LTE only. The normal range is –30 to –140. The value is –140 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSRQ	This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal. The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable signal is indicated by the lower limit, example –240. This parameter is for LTE only. The normal range is –30 to –240. The value is –240 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) of the SCC.
Service Information	If the cellular service provider supports carrier aggregation (CA), then this section displays statistics for the connection's primary component carrier (PCC).
Access Technology	This displays the type of the network (such as NR, LTE, Ethernet WAN) to which the Nebula Device is connecting.
Band	This displays the current cellular band of your Nebula Device.
RSSI	This displays the cellular signal strength between an associated cellular station and the Nebula Device for this SCC.
Cell ID	This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Nebula Device is connecting. The value depends on the Current Access Technology: • For GPRS, it is the Cell Identity as specified in 3GPP-TS.25.331. • For UMTS, it is the Cell Identity as defined in SIB3 3GPP-TS.25.331, 3GPP-TS.24.008. • For LTE/5G, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331. The value is '0' (zero) or 'N/A' if there is no network connection.
Physical Cell ID	This displays the Physical Cell ID (PCI) of the SCC.

Table 175 Site-wide > Devices > Mobile router > Live tools > Cellular Info (continued)

LABEL	DESCRIPTION
UL Bandwidth (MHz)	This shows the uplink cellular channel bandwidth from the Nebula Device to the base station. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
DL Bandwidth (MHz)	This shows the downlink cellular channel bandwidth from the base station to the Nebula Device. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Nebula Device is connecting. The value depends on the type of the mobile network (such as LTE, UMTS, GSM) to which the Nebula Device is connecting: • For UMTS (3G), it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101. • For LTE/5G, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. The value is ‘0’ (zero) or ‘N/A’ if there is no network connection.
RSRP	This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Element (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth. The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214. The reporting range is specified in 3GPP-TS.36.133. An undetectable signal is indicated by the lower limit, example –140 dBm. This parameter is for LTE only. The normal range is –30 to –140. The value is –140 if the Current Access Technology is not LTE. The value is ‘N/A’ if there is no network connection.
RSRQ	This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal. The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable signal is indicated by the lower limit, example –240. This parameter is for LTE only. The normal range is –30 to –240. The value is –240 if the Current Access Technology is not LTE. The value is ‘N/A’ if there is no network connection.
RSCP	This displays the Received Signal Code Power, which measures the power of channel used by the Nebula Device. The received signal level, in dBm, is of the CPICH channel (Ref. 3GPP TS 25.133). An undetectable signal is indicated by the lower limit, example –120 dBm. This parameter is for UMTS only. The normal range is –30 to –120. The value is –120 if the Current Access Technology is not UMTS. The value is ‘N/A’ if there is no network connection.
EcNo	This displays the ratio (in dB) of the received energy per chip and the interference level. The measured EcNo is in 0.1 dB and is received in the downlink pilot channel. An undetectable signal is indicated by the lower limit, example –240 dB. This parameter is for UMTS only. The normal range is –30 to –240. The value is –240 if the Current Access Technology is not UMTS or there is no network connection.

Table 175 Site-wide > Devices > Mobile router > Live tools > Cellular Info (continued)

LABEL	DESCRIPTION
TAC	This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber. The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101. This parameter is for LTE only. The value is '0' (zero) or 'N/A' if the Current Access Technology is not LTE or there is no network connection.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN. The LAC of the connected cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC) and LAC uniquely identifies the LAI (Location Area ID) [3GPP-TS.23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.
RAC	This displays the RAC (Routing Area Code), which is used in mobile network "packet domain service" (PS) to identify a routing area within a location area. In a mobile network, the Nebula Device uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and uses RAC to identify the location of data service like HSDPA or LTE. The RAC of the connected UTRAN cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC), LAC, and RAC uniquely identifies the RAI (Routing Area ID) [3GPPTS. 23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.
BSIC	The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station. This parameter is for GPRS only. The value is '0' (zero) if the Current Access Technology is not GPRS. The value is 'N/A' if there is no network connection.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
CQI	This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good or bad the communication channel quality is.
MCS	MCS stands for modulation coding scheme. The base station selects MCS based on current radio conditions. The higher the MCS the more bits can be transmitted per time unit.
RI	This displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
PMI	This displays the Precoding Matrix Indicator (PMI). PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer). PMI determines how cellular data are encoded for the antennas to improve downlink rate.
SCC Information	If the cellular service provider supports carrier aggregation (CA), then this section displays statistics for the connection's secondary component carriers (SCCs).
GNSS Information	Global Navigation Satellite System (GNSS) sends position and timing data from high orbit artificial satellites. It works with GPS navigational satellites to provide better receiver accuracy and reliability than just using GPS alone. This is necessary for 5G networks that require very accurate timing for time and frequency synchronization. With GNSS, your can easily locate the Nebula Device with accurate information.

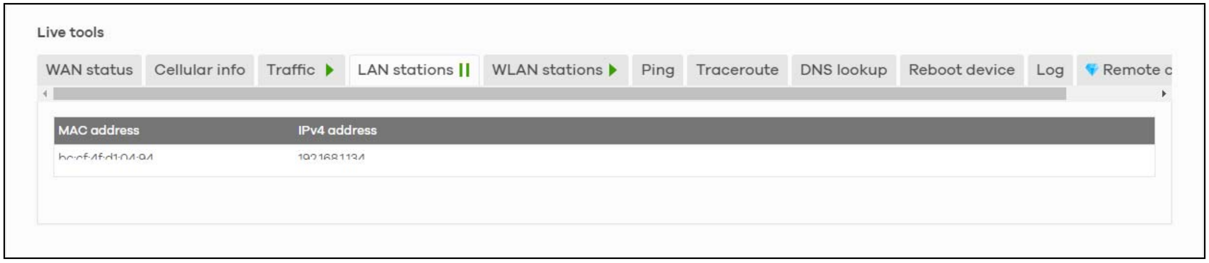
Table 175 Site-wide > Devices > Mobile router > Live tools > Cellular Info (continued)

LABEL	DESCRIPTION
Enable	This shows if GNSS is enabled. Note: This can only be configured by a qualified service technician.
Scan OnBoot	This shows Enable if Scan OnBoot is enabled, so that GNSS runs automatically after the Nebula Device is turned on. Note: This can only be configured by a qualified service technician.
Scan Status	This shows GNSS error codes for debugging by a qualified service technician.
HDOP	Horizontal Dilution of Precision (HDOP) shows how accurate data collected by the Nebula Device is according to the current satellite configuration. A smaller value of HDOP means a higher precision.
Display Format	This shows the latitude and longitude display modes. There are three modes: 0, 1, and 2. Below are examples for these modes shown in latitude/longitude. 0 – ddmm.mmmmN/S, dddmm.mmmmE/W 1 – ddmm.mmmmmm, N/S, dddmm.mmmmmm, E/W 2 – (–)dd.ddddd, (–)ddd.ddddd N/S/E/W: North/South/East/West "–" : Negative values refer to South latitude/West longitude respectively. Positive values refer to North latitude/East longitude respectively.
Latitude	This shows the latitude coordinate of the Nebula Device. These positioning values (latitude, longitude, and altitude) help you locate the Nebula Device accurately.
Longitude	This shows the longitude coordinate of the Nebula Device.
Elevation	This shows the altitude of the Nebula Device above sea level in meters.
Positioning Mode	This shows the GNSS positioning mode. 2D ("2") GNSS positioning mode displays latitude and longitude coordinates; 3D ("2") GNSS positioning mode displays latitude and longitude coordinates, and elevation.
Course Over Ground	This shows the course of the Nebula Device based on true North. Course Over Ground (COG) is different from the direction an object is headed, but the path derived from its actual motion (considered as Track), since the motion of an object is often with respect to other factors like wind and tides.
Speed Over Ground	This shows the Speed Over Ground (SOG) of the Nebula Device. SOG is the true object speed over the surface of the Earth.
Last Fix Time	This shows the last time in UTC format that the position of the Nebula Device was updated.
Number of Satellites	This shows the number of current active satellites. GNSS requires at least four satellites to determine the position of the Nebula Device.

10.4.3 LAN Stations

Go to the **Site-wide** > **Devices** > **Mobile router** > **Live tools** > **LAN stations** screen to view the LAN status of the Nebula Device. Click the pause icon (❚❚) to stop scanning for LAN stations. Alternatively, click the play icon (▶) to continue scanning.

Figure 239 Site-wide > Devices > Mobile router > Live tools > LAN stations



MAC address	IPv4 address
bc:cf:4f:d1:04:94	192.168.1.134

The following table describes the labels in this screen.

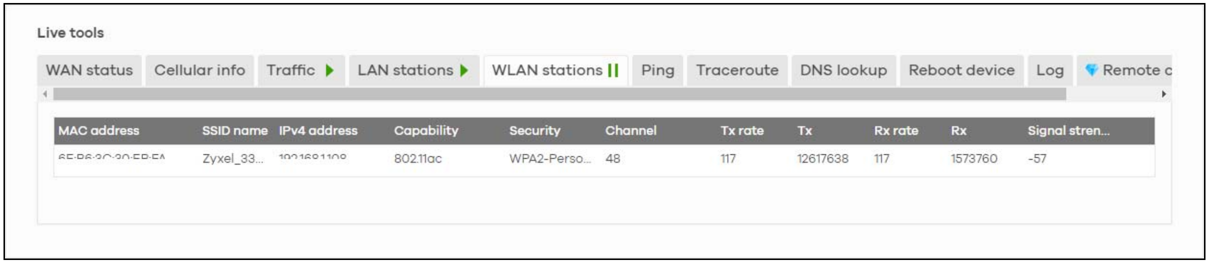
Table 176 Site-wide > Devices > Mobile router > Live tools > LAN stations

LABEL	DESCRIPTION
MAC address	This field displays the MAC address of the LAN station.
IPv4 address	This indicate the IPv4 address of the LAN station.

10.4.4 WLAN Stations

Go to the **Site-wide** > **Devices** > **Mobile router** > **Live tools** > **WLAN stations** screen to view the WiFi status of the Nebula Device. Click the pause icon (❚❚) to stop scanning for WiFi stations. Alternatively, click the play icon (▶) to continue scanning.

Figure 240 Site-wide > Devices > Mobile router > Live tools > WLAN stations



MAC address	SSID name	IPv4 address	Capability	Security	Channel	Tx rate	Tx	Rx rate	Rx	Signal stren...
6E:B6:3C:30:EB:EA	Zyxel_33...	192.168.1.108	802.11ac	WPA2-Perso...	48	117	12617638	117	1573760	-57

The following table describes the labels in this screen.

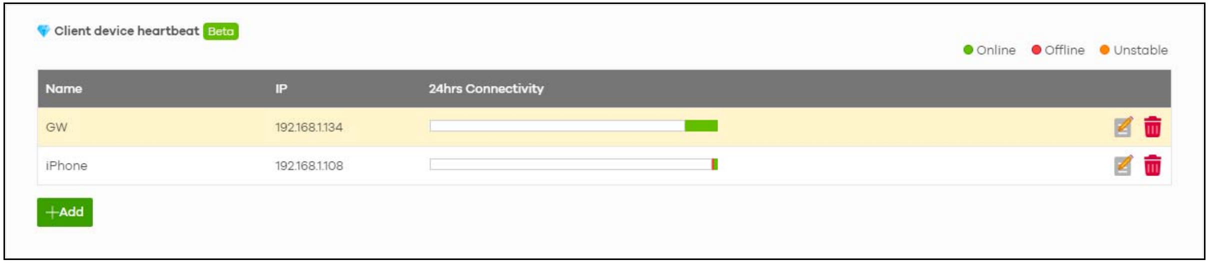
Table 177 Site-wide > Devices > Mobile router > Live tools > WLAN stations

LABEL	DESCRIPTION
MAC address	This field displays the MAC address of an associated WiFi station.
SSID name	This is the descriptive name used to identify the Nebula Device in a WiFi network.
IPv4 address	This indicate the IPv4 address of the gateway that helps forward this route's traffic.
Capability	This shows the WiFi standard supported by the client or the supported standards currently used by the client.
Security	This displays the type of security mode the WiFi interface is using in the WiFi network.
Channel	This is the channel number currently used by the WiFi interface.
Tx rate	This shows the maximum transmission rate of the client.
Tx	This shows the amount of data transmitted by the client since it last connected.
Rx rate	This shows the maximum reception rate of the client.
Rx	This shows the amount of data received by the client since it last connected.
Signal strength	This shows the RSSI (Received Signal Strength Indicator) of the client's WiFi connection.

10.5 Client Device Heartbeat

Use the **Site-wide** > **Devices** > **Mobile router** > **Client device heartbeat** screen to monitor the network status of LAN client devices connected to the Nebula Device (mobile router), such as NAS server, printer, or IP camera.

Figure 241 Site-wide > Devices > Mobile router > Client device heartbeat



Client device heartbeat Beta

● Online ● Offline ● Unstable

Name	IP	24hrs Connectivity
GW	192.168.1.134	
iPhone	192.168.1.108	

+Add

The following table describes the labels in this screen.

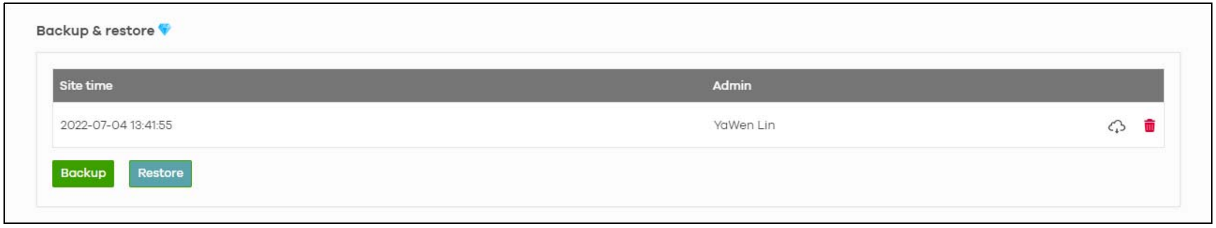
Table 178 Site-wide > Devices > Mobile router > Client device heartbeat

LABEL	DESCRIPTION
Client device heartbeat	
Name	This shows the name of the client device to monitor.
IP	This shows the local (LAN) IP address of the client device connected to the Nebula Device.
24hrs Connectivity	This shows the status over the past 24 hours between the Nebula Device and client device, beginning when the client device was added to the list. Hover the mouse over a colored bar to display the monitored time range. The Nebula Device monitors the link by sending 3 queries in intervals. The Nebula Device then uses the reply to know if the link is up and the transmission quality of the link. • Green (online): This shows green when the Nebula Device is able to get 3 replies to the 3 queries from the client device. • Orange (unstable): This shows orange when the Nebula Device is able to get 1 or 2 replies to the 3 queries from the client device. • Red (offline): This shows red when the Nebula Device got no reply from the monitored client device. • White (no connection between the Nebula Device and the client device). This shows white when: Before adding the client device to monitor to the list, or There is no link between the Nebula Device and NCC, and you reboot the client device, or The Nebula Device license has expired, or The client device was removed from the list and added back within 24 hours.
✎	Click the edit icon to change the name of the client device, then click **Save**.
🗑	Click the remove icon to remove the client device from monitoring, then click **Save**.
+Add	Click this button to add up to 5 client devices for monitoring. 1. Enter a descriptive name, 1 – 64 characters including 0–9 a–z A–Z `~!@#$%&*(_+-={} | [];"'./<> ?) in the **Name** field. 2. Enter the IPv4 address of the client device to monitor in the **IP** field. 3. Then click **Save**.

10.6 Backup & Restore

Use the **Site-wide** > **Devices** > **Mobile router** > **Backup & restore** screen to back up your configuration settings to the cloud or restore your current setting to the backup configuration.

Figure 242 Site-wide > Devices > Mobile router > Backup & restore



Backup & restore

Site time	Admin
2022-07-04 13:41:55	YaWen Lin

The following table describes the labels in this screen.

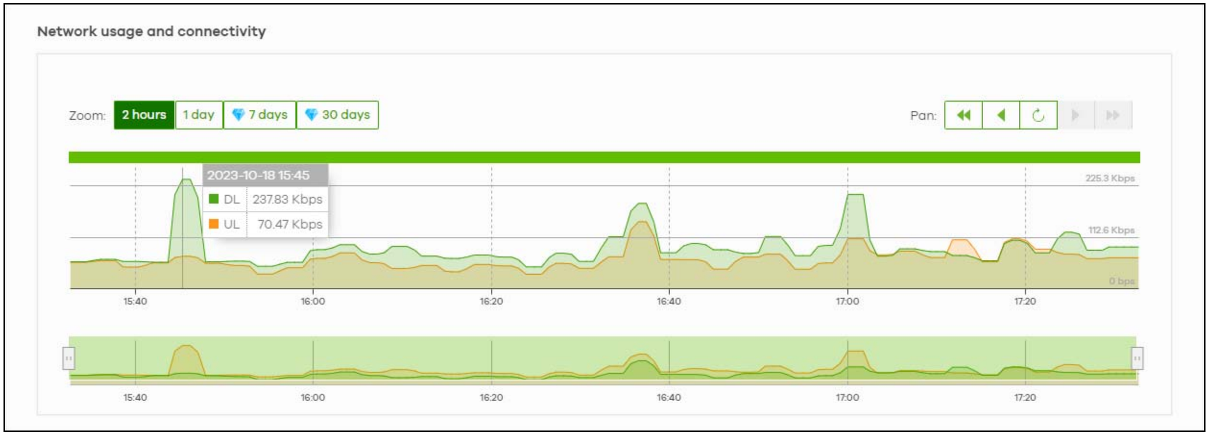
Table 179 Site-wide > Devices > Mobile router > Backup & restore

LABEL	DESCRIPTION
Backup & restore	
Site time	This shows the date and time of the site, to which the change was applied, when the log was recorded.
Admin	This shows the name of the administrator who made the back up.
Backup	Click this button to create a new backup of the current configuration of the Nebula Device to the NCC. Click the Download icon (☁) to download the configuration file to your computer or laptop. Click the Delete icon (🗑) to remove the configuration file on the Nebula Device.
Restore	Click this button to overwrite the settings of the Nebula Device with the selected configuration backup.

10.7 Network Usage and Connectivity

Go to the **Site-wide** > **Devices** > **Mobile router** > **Network usage and connectivity** screen and then move the cursor to see the transmission rate (uplink/downlink) of a specific time.

Figure 243 Site-wide > Devices > Mobile router > Network usage and connectivity



The following table describes the labels in this screen.

Table 180 Site-wide > Devices > Mobile router > Network usage and connectivity

LABEL	DESCRIPTION
Network usage and connectivity Move the cursor over the chart to see the transmission rate at a specific time.	
Zoom	Select a time period to view the statistics in the past 2 hours, day, week, or month.
Pan	Use this to move backward or forward by one day or a week.

CHAPTER 11 Accessory

11.1 Overview

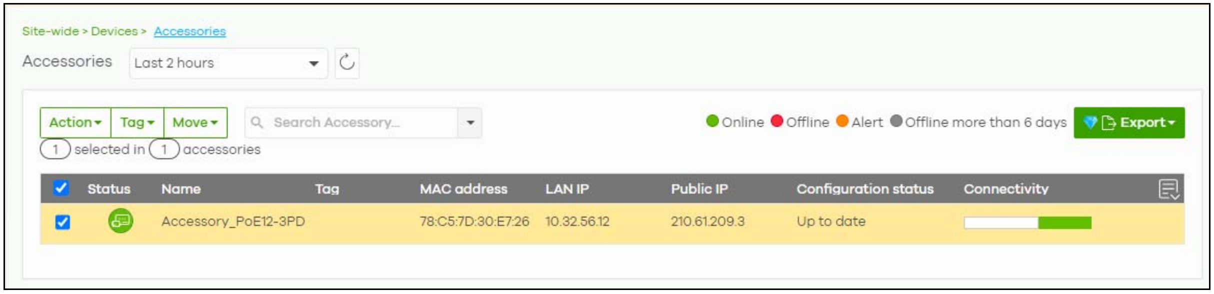
This chapter discusses the menus that you can use to monitor the Nebula-managed Accessories in your network and configure settings even before an Accesssory is deployed and added to the site.

An Accessory can be managed by Nebula. It is referred to as a Nebula Device in this chapter.

11.2 Configuration

From the navigation panel, click **Site-wide** > **Devices** > **Accessory** and the following screen appears.

Figure 244 Site-wide > Devices > Accessories


Site-wide > Devices > Accessories
Accessories
Last 2 hours
Action
Tag
Move
Search Accessory...
1 selected in 1 accessories
● Online ● Offline ● Alert ● Offline more than 6 days
Export

☑	Status	Name	Tag	MAC address	LAN IP	Public IP	Configuration status	Connectivity
☑	●	Accessory_PoE12-3PD		78:C5:7D:30:E7:26	10.32.56.12	210.61.209.3	Up to date	

The following table describes the labels in this screen.

Table 181 Site-wide > Devices > Accessories

LABEL	DESCRIPTION
Accessories	Select to view device information and connection status in the past 2 hours, day, week, month.
↻	Click this button to reload the data-related frames on this page.
Action	Perform an action on the selected Nebula Devices.
Reboot	Select this to restart the Nebula Device.
Tag	Select one or multiple Nebula Devices and click this button to create a new tag for the Nebula Devices or delete an existing tag.
Move	Select one or multiple Nebula Devices and click this button to move the Nebula Devices to another site or remove the Nebula Devices from the current site.
Search	Specify your desired filter criteria to filter the list of Nebula Devices.
Accessories	This shows the number of Nebula Devices connected to the site network.
Export	Click this button to save the accessories list as a CSV or XML file to your computer.
*	Click this to select all the rows in this table.

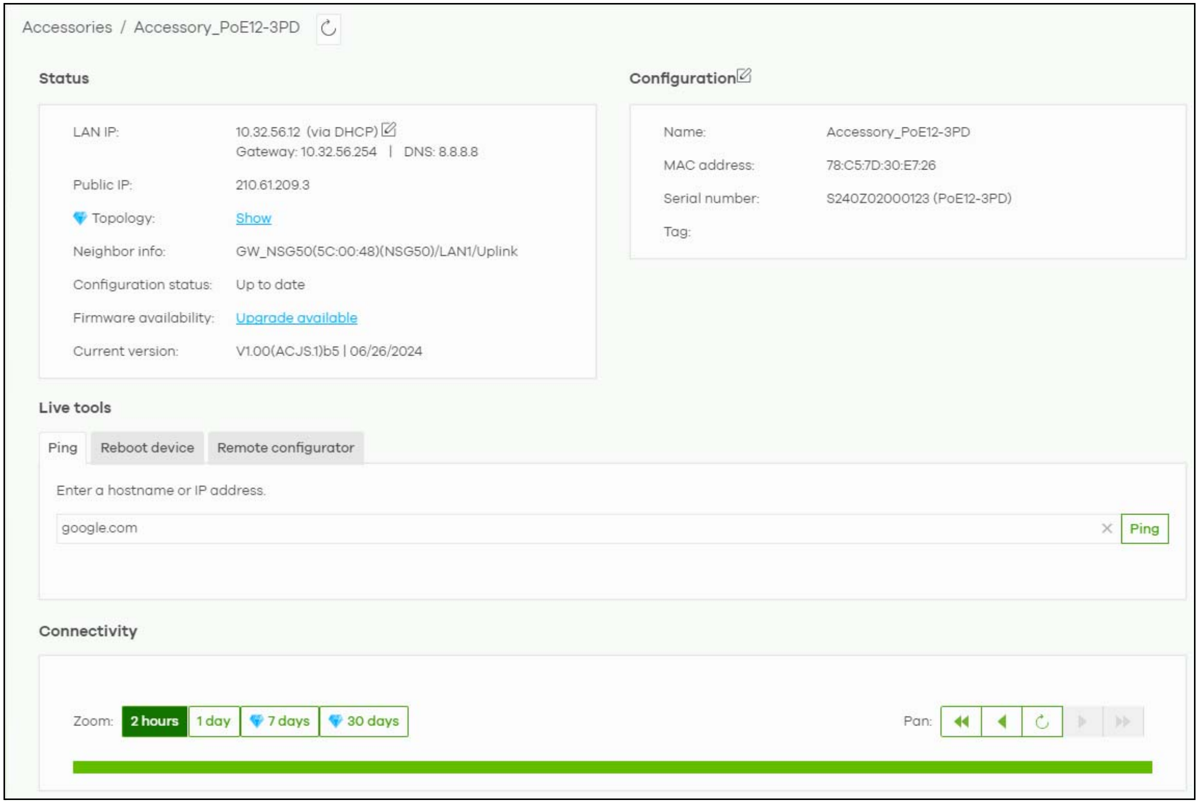
Table 181 Site-wide > Devices > Accessories (continued)

LABEL	DESCRIPTION
Status	This shows the status of the Nebula Device. • Green: The Nebula Device is online and has no alerts. • Amber: The Nebula Device has alerts. Hover the mouse over the icon to find the problem. • Red: The Nebula Device is offline. • Gray: The Nebula Device has been offline for 7 days or more. Click the Nebula Device on this page to go to the Nebula Device's details screen for more information.
Name	This shows the descriptive name of the Nebula Device.
Tag	This shows the user-specified tag for the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
LAN IP	This shows the local (LAN) IP address of the Nebula Device.
Public IP	This shows the global (WAN) IP address of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
Product information	This shows the production information of the Nebula Device.
Connectivity	This shows the accessory connection status. The red time slot indicates the connection to the NCC is down, and the green time slot indicates the connection is up. Move the cursor over a time slot to see the actual date and time when an Nebula Device is connected or disconnected.
Serial number	This shows the serial number of the Nebula Device.
Firmware status	This shows whether the firmware installed on the Nebula Device is up-to-date.
Firmware type	This shows **Stable** when the installed firmware may not have the latest features but has passed Zyxel internal and external testing. This shows **Latest** when the installed firmware is the most recent release with the latest features, improvements, and bug fixes. This shows **General Availability** when the installed firmware is a release before **Latest**, but is still undergoing Zyxel external testing. This shows **Dedicated** when the installed firmware is locked and Zyxel support is monitoring. Contact Zyxel customer support if you want to unlock the firmware in order to upgrade to a later one. This shows **Beta** when the installed firmware is a release version for testing the latest features and is still undergoing Zyxel internal and external testing. This shows **N/A** when the Nebula Device is offline and its firmware status is not available.
Firmware availability	This shows whether the firmware on the Nebula Device is **Up to date**, there is firmware update available for the Nebula Device (**Upgrade available**), or a specific version of firmware has been installed by Zyxel customer support (**Locked**).
Current version	This shows the firmware version currently installed on the Nebula Device.
IP type	This shows whether the IP address was assigned automatically (**DHCP**), or manually (**Static IP**).
☑	Click this icon to display a greater or lesser number of configuration fields. For faster loading of data, select only the configuration fields listed that do NOT take a long time to fetch data.

11.2.0.1 Accessories Details

Click a Nebula Device entry in the **Site-wide** > **Devices** > **Accessories** screen to display individual Nebula Device statistics.

Figure 245 Site-wide > Devices > Accessories: Details



Accessories / Accessory_PoE12-3PD

Status

LAN IP: 10.32.56.12 (via DHCP)
Gateway: 10.32.56.254 | DNS: 8.8.8.8
Public IP: 210.61.209.3
Topology: Show
Neighbor info: GW_NSG50(5C:00:48)(NSG50)/LAN1/Uplink
Configuration status: Up to date
Firmware availability: Upgrade available
Current version: V1.00(ACJS.1)b5 | 06/26/2024

Configuration

Name: Accessory_PoE12-3PD
MAC address: 78:C5:7D:30:E7:26
Serial number: S240Z02000123 (PoE12-3PD)
Tag:

Live tools

Enter a hostname or IP address.

google.com

Connectivity

The following table describes the labels in this screen.

Table 182 Site-wide > Devices > Accessories: Details

LABEL	DESCRIPTION
↻	Click this button to reload the data-related frames on this page.
Status	

Table 182 Site-wide > Devices > Accessories: Details (continued)

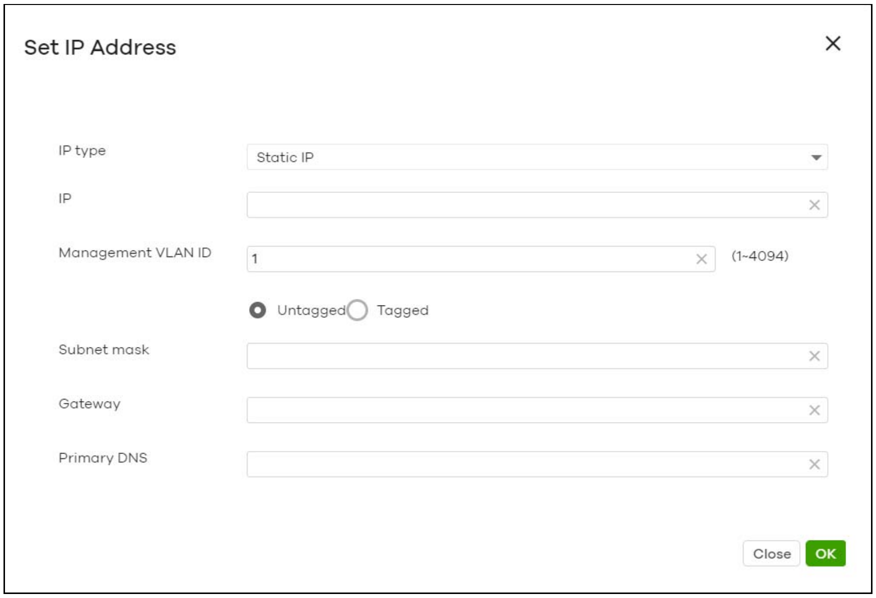
LABEL	DESCRIPTION
LAN IP	This shows the local (LAN) IP address of the Nebula Device. It also shows the IP addresses of the gateway and DNS server. Click the edit icon to open a screen where you can change the IP addresses, VLAN ID number and tagging setting.  Set IP Address IP type: Static IP IP: Management VLAN ID: 1 (1~4094) ● Untagged ○ Tagged Subnet mask: Gateway: Primary DNS: Close OK Note: To prevent an IP address conflict, NCC will prevent input of an IP address already used by another Nebula Device in the same site.
Public IP	This shows the global (WAN) IP address of the Nebula Device.
Topology	Click **Show** to go to the **Site-wide** > **Topology** screen. See Section 4.2 on page 208.
Neighbor info	This shows the LLDP information received on the up-link port.
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
Firmware availability	This shows whether the firmware on the Nebula Device is up-to-date or there is firmware update available for the Nebula Device.
Current version	This shows the firmware version currently installed on the Nebula Device.
Configuration Click the edit configuration icon to change the Nebula Device name and tags. You can also move the Nebula Device to another site or remove. By default, the Nebula Device's hostname is the MAC address. Enter a **Name** to identify the Nebula Device. You can use up to 64 alphanumeric characters including period (.) and hyphen (-). Spaces are not allowed. Note: The period (.) and hyphen (-) cannot be the first character, last character, or appear consecutively on the **Name**. For example, -wax650, wax650-, wax650..wax650, wax650.-wax650.	
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
Serial number	This shows the serial number of the Nebula Device.
Change site	Select the new site from the drop-down menu or click **Remove** to remove the Nebula Device from the site.
Tags	This shows the user-specified tag for the Nebula Device.
Live tools	

Table 182 Site-wide > Devices > Accessories: Details (continued)

LABEL	DESCRIPTION
Ping	Enter the domain name or IP address of a computer that you want to perform ping from the Nebula Device in order to test a connection and click **Ping**. This can be used to determine if the Nebula Device and the computer are able to communicate with each other.
Reboot device	Click the **Reboot** button to restart the Nebula Device. Note: All connected clients will be temporarily disconnected during reboot.
Remote configurator	This allows you to establish a remote connection to this Nebula Device by specifying the IP address and port number. Then click **Establish**. This feature is available to the organization owner, organization administrators with full privileges, and site administrators with full privileges.
Connectivity Move the cursor over the chart to see the transmission rate at a specific time.	
Zoom	Select to view the statistics in the past 2 hours, day, week, or month.
Pan	Click to move backward or forward by one day or week.

PART III

Manage by Organization Deployment

CHAPTER 12
Organization-wide

12.1 Overview

This chapter discusses the menus that you can use to monitor your organization and manage sites, Nebula Devices, accounts, licenses, and VPN members for the organization.

12.2 License & inventory

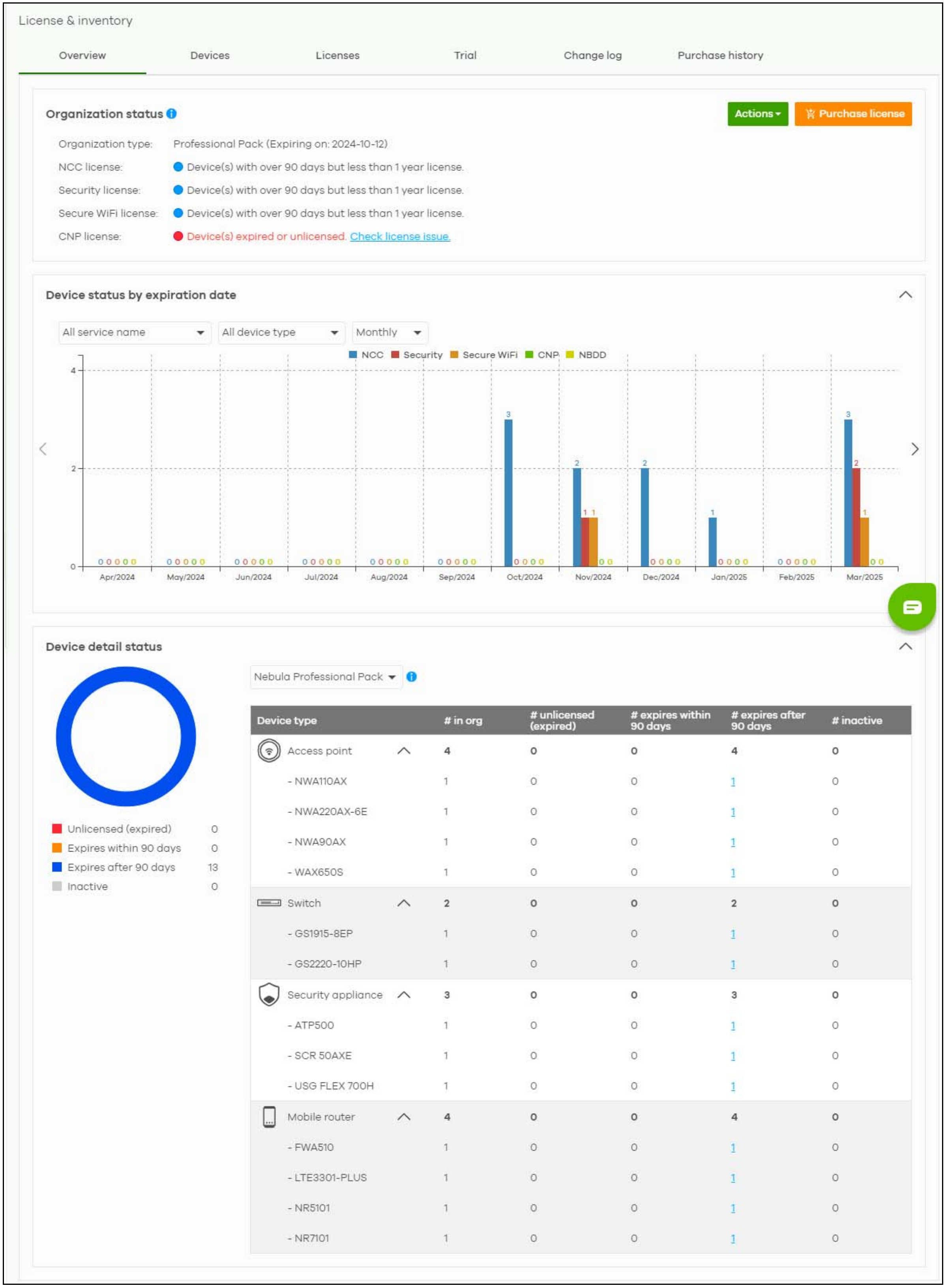
The following section describes license management screens in NCC.

Unused licenses can be transferred from a Nebula Device in an Organization to another Nebula Device in an Organization.

12.2.1 License & Inventory Overview Screen

Use these screens to view licenses and Nebula Devices in the organization. Click **Organization-wide** > **License & inventory** > **Overview** to access this screen.

Figure 246 Organization-wide > License & inventory > Overview



License & inventory

Organization status

Organization type:	Professional Pack (Expiring on: 2024-10-12)
NCC license:	● Device(s) with over 90 days but less than 1 year license.
Security license:	● Device(s) with over 90 days but less than 1 year license.
Secure WiFi license:	● Device(s) with over 90 days but less than 1 year license.
CNP license:	● Device(s) expired or unlicensed. Check license issue.

Device status by expiration date

All service name | All device type | Monthly

Device detail status

🟥 Unlicensed (expired)	0
🟧 Expires within 90 days	0
🟦 Expires after 90 days	13
⬜ Inactive	0

Nebula Professional Pack

Device type	# in org	# unlicensed (expired)	# expires within 90 days	# expires after 90 days	# inactive
Access point	4	0	0	4	0
- NWA110AX	1	0	0	1	0
- NWA220AX-6E	1	0	0	1	0
- NWA90AX	1	0	0	1	0
- WAX650S	1	0	0	1	0
Switch	2	0	0	2	0
- GS1915-8EP	1	0	0	1	0
- GS2220-10HP	1	0	0	1	0
Security appliance	3	0	0	3	0
- ATP500	1	0	0	1	0
- SCR 50AXE	1	0	0	1	0
- USG FLEX 700H	1	0	0	1	0
Mobile router	4	0	0	4	0
- FWA510	1	0	0	1	0
- LTE3301-PLUS	1	0	0	1	0
- NR5101	1	0	0	1	0
- NR7101	1	0	0	1	0

The following table describes the labels in this screen.

Table 183 Organization-wide > License & inventory > Overview

LABEL	DESCRIPTION
Organization Status	
Actions	Click this button to add licenses and/or Nebula Devices to the organization. Choose one of the following actions: • **Add more devices**: Add new Nebula Devices to the organization, by serial number and MAC address. For details, see Section 12.2.2 on page 662. • **Add more licenses**: Add new licenses to the organization, by license key. For details, see Section 12.2.4 on page 664. • **Install wizard**: Add Nebula Devices and licenses to the organization, assign the licenses to the Nebula Devices, and then upgrade the organization if required. For details, see Section 12.2.5 on page 664.
Purchase License	Click this button to go to a window that will ask if you wish to be redirected to the Zyxel Circle web site (if the NCC account has a Circle account). If you do not have a Circle account, you can do the following: 1. Select what license to purchase and set the target expiration date to keep the Pro/Plus tier features/services running. 2. You may export the list of required licenses to your computer. 3. After calculating the license to purchase, click the **Zyxel license marketplace** (**Check out**) button to complete your purchase. Purchased licenses are directly assigned to Nebula Device(s). **Unused** licenses assigned to your organization will not be counted as it is not yet assigned to a Nebula Device. This button is available only for the Full (Delegated) administrator privilege or Owner administrator account with a registered Nebula Device(s).
Upgrade Now	Click this button to upgrade the organization to Plus or Pro tier. The button is only available if you have a Plus or Pro license for every Nebula Device in the organization.
Downgrade Now	Click this button to downgrade the organization from Plus or Pro to Base tier, or from Pro to Plus tier. All active NCC licenses in the organization will stay active and continue to count down to their expiry time.
Organization type	This shows the licensing tier of the organization. Possible values are: **Base**, **Plus Pack**, **Professional Pack,** and **Trial**.
NCC license	This shows whether there are any Nebula Devices with near expiring licenses.
Security license	This shows whether the current site has an active NSS or UTM license.
Secure WiFi license	This shows whether the current site has an active Secure WiFi license. A Secure WiFi license unlocks the Remote AP feature. Remote AP allows users connected to an off-site (remote) AP to connect to on-site resources behind the Nebula Device through a secure IPSec VPN tunnel.
CNP/CNP+ license	This shows whether the current site has an active CNP (Connect & Protect) or CNP+ Connect & Protect Plus) license. A CNP license unlocks security services, such as threat protection using DNS and IP reputation filters. A CNP+ license unlocks security services, such as application visibility and threat protection using DNS and IP reputation filters.

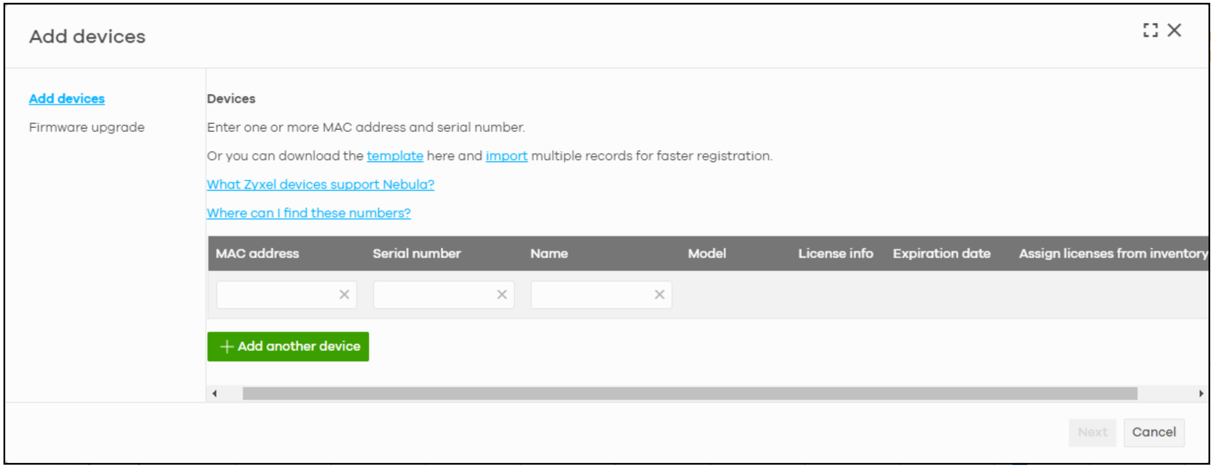
Table 183 Organization-wide > License & inventory > Overview (continued)

LABEL	DESCRIPTION
Device status by expiration date	Click this button to select the data to be shown in the graph. Choose one from each of the following criteria: • **All service name**, **Gold Security Pack**, **Nebula Professional Pack**, **Nebula Plus Pack**, **Nebula Security Pack**, **UTM Security Pack**, **Content Filter Pack**, **Elite Pack**, **Secure WiFi**, **Connect & Protect**, **Next Business Day Delivery Service**: select the category of licenses to display. • **All device type**, **Access point**, **Switch**, **Security appliance**, or **Mobile router**: select the category of Nebula Device to display. • **Monthly**, **Quarterly**, or **Yearly**: select the period of time to display.
Device detail status	
License type	Select the license type to filter your selection (**Nebula Professional Pack**, **Nebula Plus Pack**, **Gold Security Pack**, **Nebula Security Pack**, **UTM Security Pack**, **Content Filter Pack**, **Elite Pack**, **Secure WiFi**, **Connect & Protect**, **Access L3**, **Next Business Day Delivery Service**).
Device type	This shows the category of Nebula Device (**Access point**, **Switch**, **Security appliance**, **Mobile router**) and Nebula Device model.
# in org	This shows the total number of Nebula Devices of the specified category and model that are in the organization.
# unlicensed (expired)	This shows the total number of Nebula Devices of the specified category and model that have: • No NCC Pro or Plus license. • An expired NCC Pro or Plus license.
# expires within 90 days	This shows the total number of Nebula Devices of the specified category and model that have an NCC Pro or Plus license that will expire within 90 days.
# expires after 90 days	This shows the total number of Nebula Devices of the specified category and model that have an NCC Pro or Plus license that have more than 90 days before expiration.
# inactive	This shows the total number of Nebula Devices of the specified category and model that have an NCC Pro or Plus license that has not been activated.

12.2.2 Add Devices Screen

Use this screen to add Nebula Devices to an organization. Click **Organization-wide** > **License & inventory** > **Overview** > **Actions** > **Add more devices** to access this screen.

Figure 247 Organization-wide > License & inventory > Overview: Add devices: Add devices



Add devices

Add devices

Firmware upgrade

Devices

Enter one or more MAC address and serial number.

Or you can download the template here and import multiple records for faster registration.

What Zyxel devices support Nebula?

Where can I find these numbers?

MAC address	Serial number	Name	Model	License info	Expiration date	Assign licenses from inventory

The following table describes the labels in this screen.

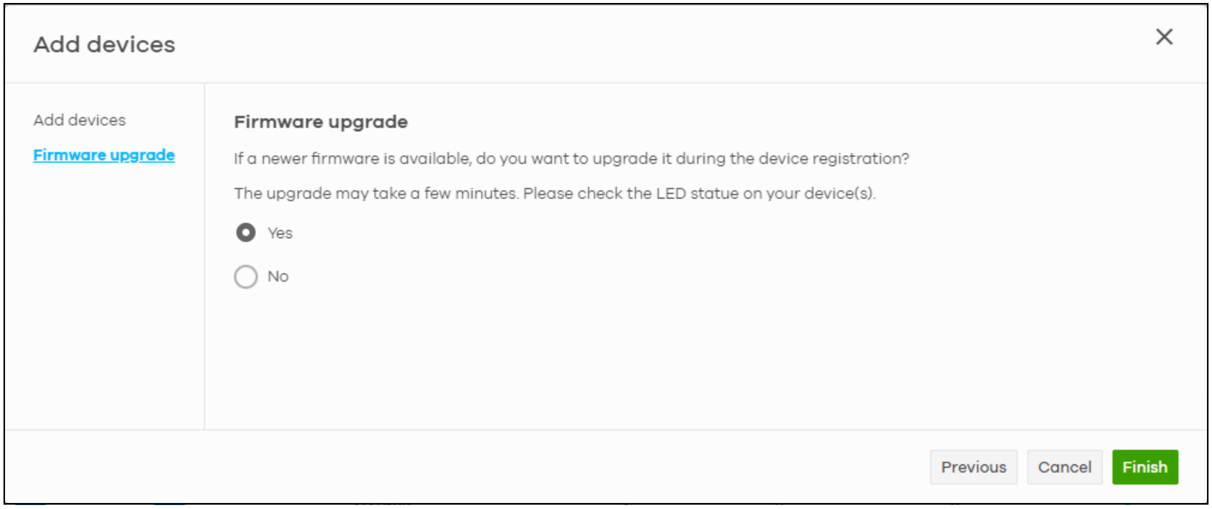
Table 184 Organization-wide > License & inventory > Overview: Add devices: Add devices

LABEL	DESCRIPTION
template	Click this to download an XLSX file that you can use as a template to import a large number of Nebula Devices at once. Follow the instructions and formatting in the template to add the Nebula Device's serial numbers and MAC addresses.
import	Click this to upload a completed template XLSX file and import all Nebula Devices in the file.
MAC address	Enter the MAC address of the new Nebula Device.
Serial number	Enter the serial number of the new Nebula Device.
Name	Enter a name for the new Nebula Device. It can consist of 1 – 64 characters.
Model	This shows the model number of the Nebula Device being added.
License info	This shows the type of NCC license activated on the Nebula Device, if there is one. Otherwise, it shows a '–' (dash).
Expiration date	This shows the expiration date of the NCC license activated on the Nebula Device, if there is one. Otherwise, it shows a '–' (dash).
Assign licenses from inventory	Click here to assign unassigned licenses already in the organization to the Nebula Device. Note: If the organization is a Pro or Plus tier, you must assign a Pro or Plus license to the Nebula Device within 15 days.
🗑	Click the remove icon to delete the entry.
Add another device	Click this to add another Nebula Device to the organization.
Acknowledge	Select this to confirm that your NCC account will be the owner of the new Nebula Devices.
Next	Click this to add the Nebula Devices to the organization.
Cancel	Click this to close the screen without saving.

12.2.3 Firmware Upgrade Screen

If a newer Nebula Device firmware is available, use this screen to upgrade it. Click **Organization-wide** > **License & inventory** > **Overview** > **Actions** > **Add more devices** > **Firmware upgrade** to access this screen.

Figure 248 Organization-wide > License & inventory > Overview: Add devices: Firmware upgrade



Firmware upgrade

If a newer firmware is available, do you want to upgrade it during the device registration?

The upgrade may take a few minutes. Please check the LED statue on your device(s).

● Yes

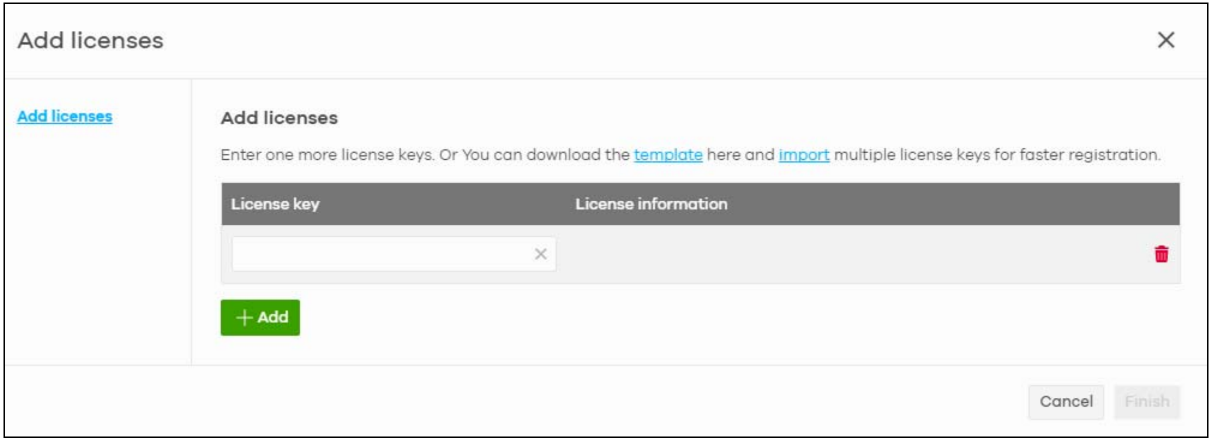
○ No

Note: If you choose not to upgrade the firmware, NCC will still perform an upgrade if the Nebula Device's firmware has security vulnerabilities, and/or lacks key performance improvements.

12.2.4 Add Licenses Screen

Use this screen to add licenses to an organization. Click **Organization-wide** > **License & inventory** > **Overview** > **Actions** > **Add more licenses** to access this screen.

Figure 249 Organization-wide > License & inventory > Overview: Add licenses



Enter one more license keys. Or You can download the template here and import multiple license keys for faster registration.

The following table describes the labels in this screen.

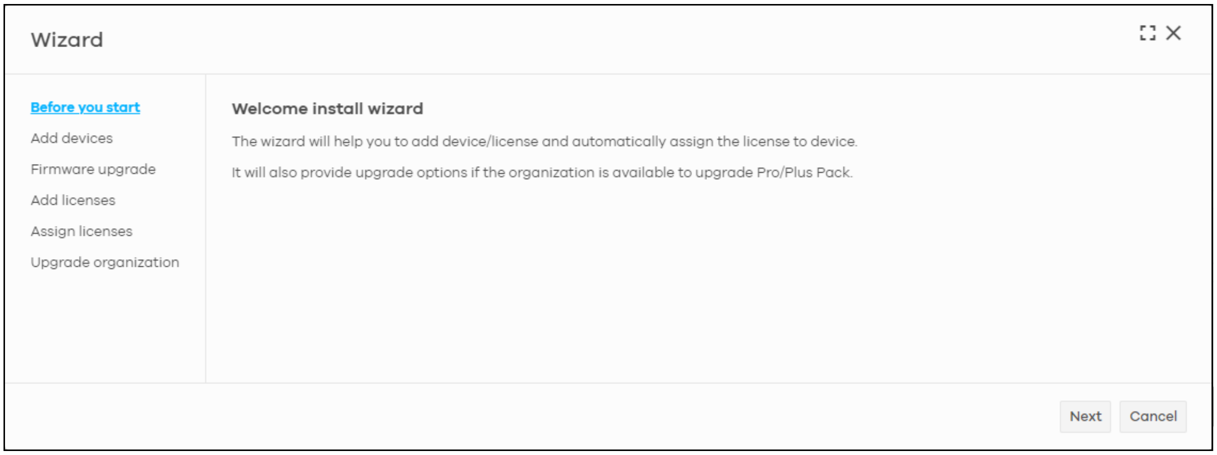
Table 185 Organization-wide > License & inventory > Overview: Add licenses

LABEL	DESCRIPTION
template	Click this to download an XLSX file that you can use as a template to import a large number of licenses at once. Follow the instructions and formatting in the template to add the license keys.
import	Click this to upload a completed template XLSX file and import all licenses in the file.
License key	Enter the license key of the new license.
License information	This shows the license type and validity period of the license being added.
🗑	Click the remove icon to delete the entry.
Add	Click this to add another license to the organization.
Finish	Click this to add the license to the organization.
Cancel	Click this to close the screen without saving.

12.2.5 Install Wizard

Use this wizard to add licenses and Nebula Devices to an organization, assign licenses to the new Nebula Devices, and then upgrade the organization if required. Follow the steps below to use the wizard.

1 Click **Organization-wide** > **License & inventory** > **Overview** > **Actions** > **Install wizard**. After the wizard window opens, click **Next**.



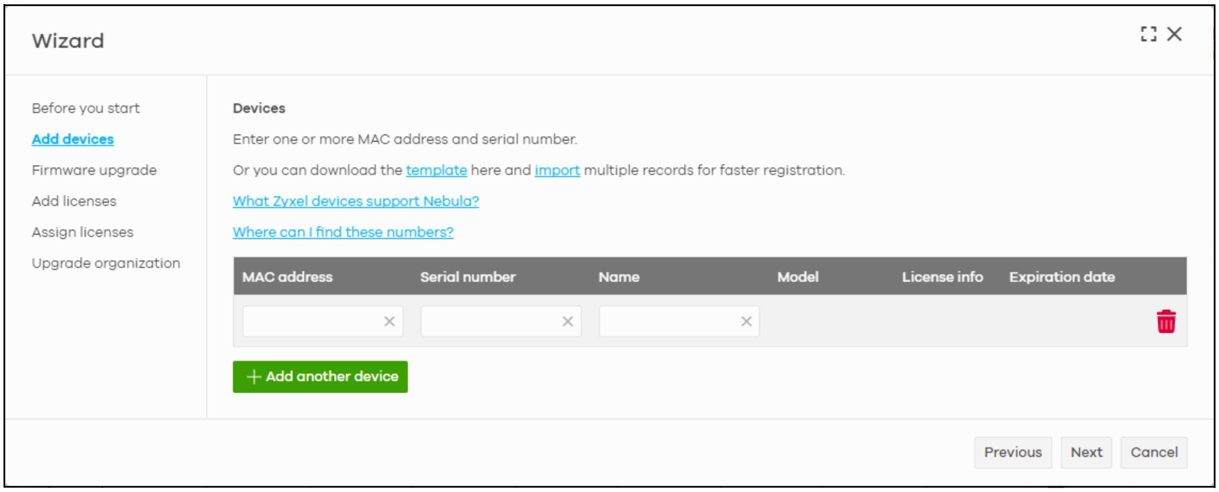
Wizard

Welcome install wizard

The wizard will help you to add device/license and automatically assign the license to device.

It will also provide upgrade options if the organization is available to upgrade Pro/Plus Pack.

2 Add the MAC address and serial number of one or more Nebula Devices, select **Acknowledge**, and then click **Next**. For more information on this page, see Section 12.2.2 on page 662.



Wizard

Devices

Enter one or more MAC address and serial number.

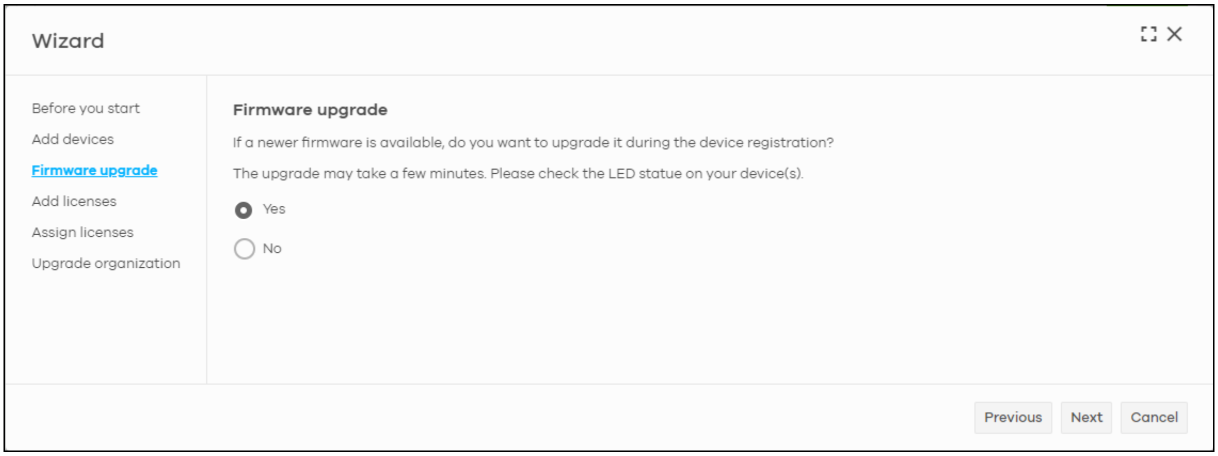
Or you can download the template here and import multiple records for faster registration.

What Zyxel devices support Nebula?

Where can I find these numbers?

MAC address	Serial number	Name	Model	License info	Expiration date

3 Click **Yes** (selected by default) to upgrade the Nebula Device firmware. If you select **No**, NCC will still perform an upgrade if the Nebula Device's firmware have security vulnerabilities, and/or lack key performance improvements. Click **Next** to continue.



Wizard

Firmware upgrade

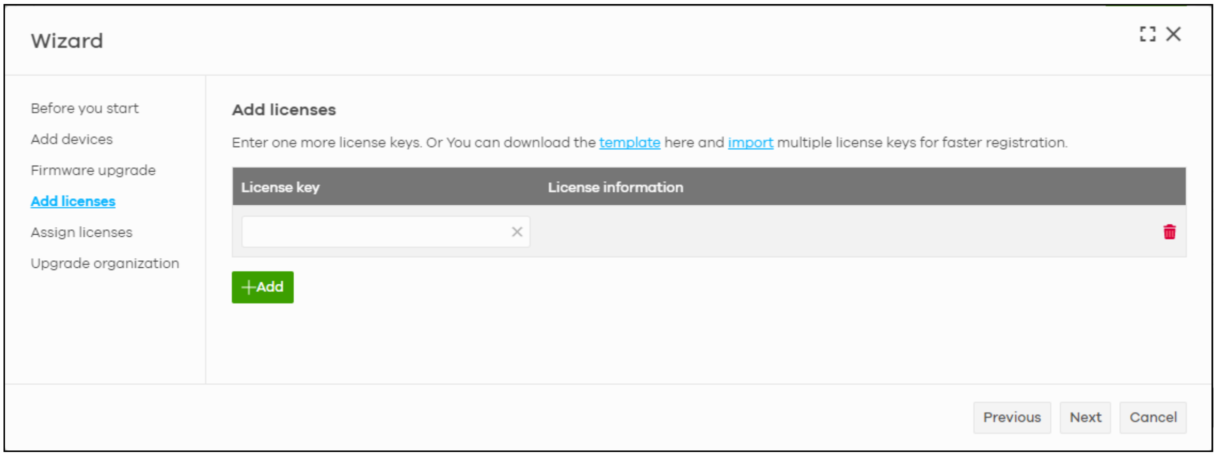
If a newer firmware is available, do you want to upgrade it during the device registration?

The upgrade may take a few minutes. Please check the LED statue on your device(s).

● Yes

○ No

4 Add the license keys of one or more licenses, and then click **Next**. For more information on this page, see Section 12.2.4 on page 664.



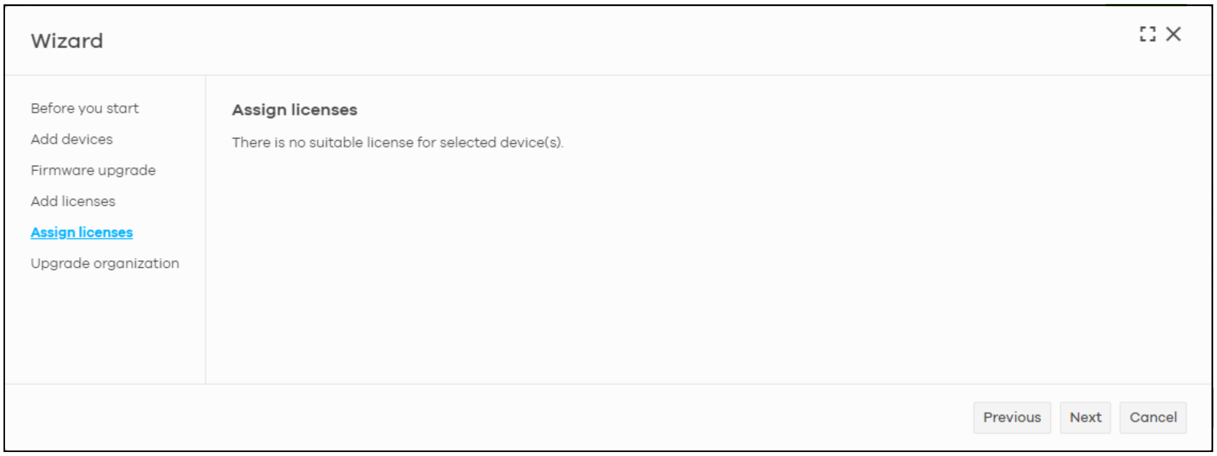
Wizard

Add licenses

Enter one more license keys. Or You can download the template here and import multiple license keys for faster registration.

License key	License information

5 NCC automatically tries to assign an unused license to each matching Nebula Device. Reassign unused licenses for each Nebula Device manually by clicking **Select # of license**. Then click **Next**.

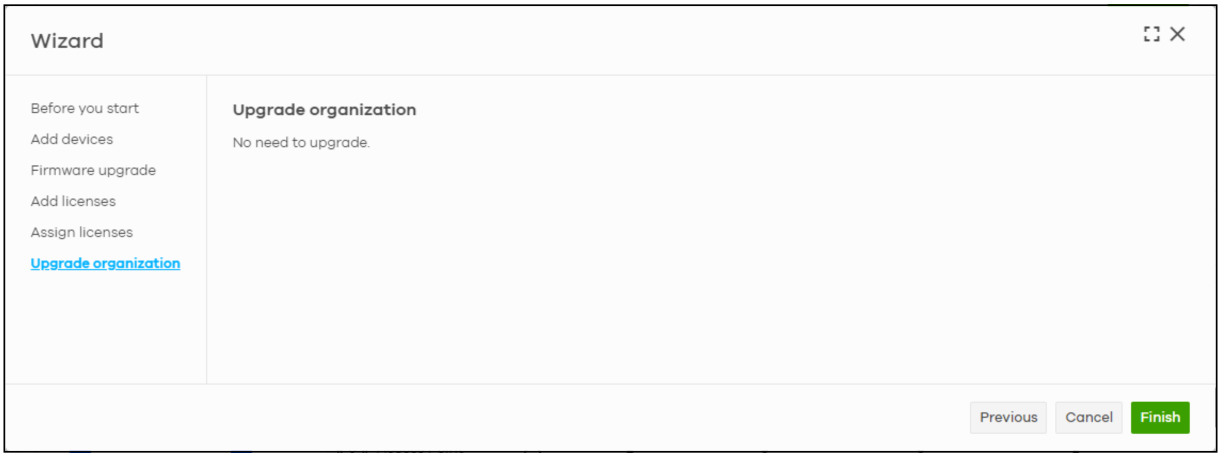


Wizard

Assign licenses

There is no suitable license for selected device(s).

6 If the organization is on the base tier and you have added sufficient licenses for all Nebula Devices, you are given the option to upgrade to the Pro or Plus tier. Select **Yes** or **No**, and then click **Finish**.



Wizard

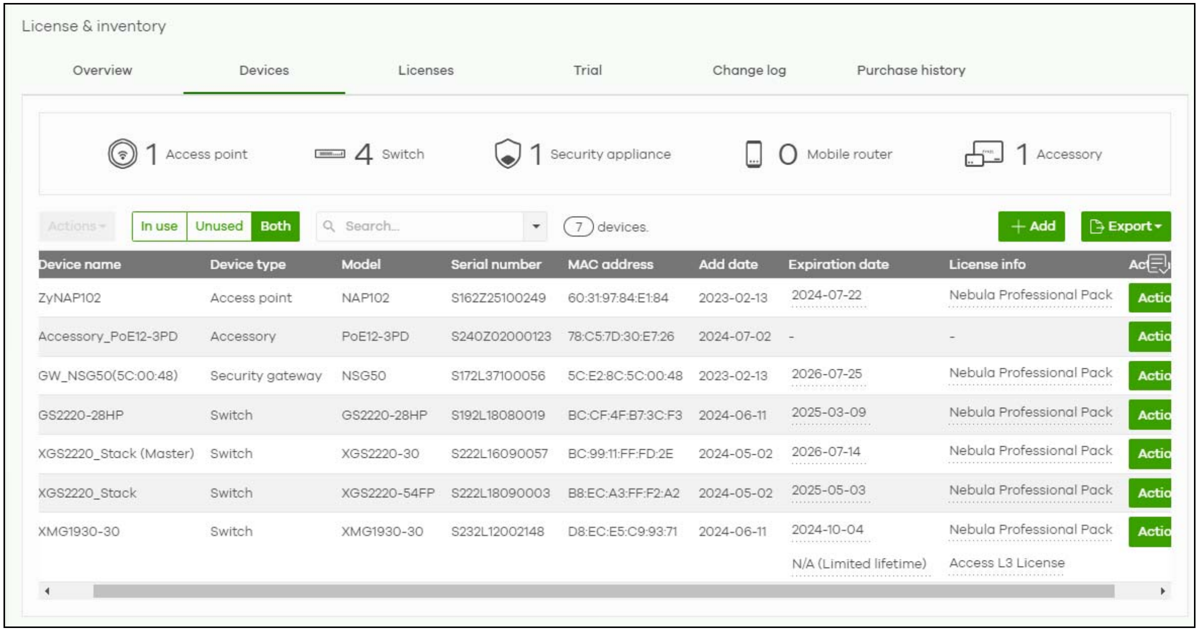
Upgrade organization

No need to upgrade.

12.2.6 License & Inventory Devices Screen

Use these screen to view and manage Nebula Devices in the organization. Click **Organization-wide** > **License & inventory** > **Devices** to access this screen.

Figure 250 Organization-wide > License & inventory > Devices



License & inventory

1 Access point · 4 Switch · 1 Security appliance · 0 Mobile router · 1 Accessory

7 devices.

Device name	Device type	Model	Serial number	MAC address	Add date	Expiration date	License info	Ac
ZyNAP102	Access point	NAP102	S162Z25100249	60:31:97:84:E1:84	2023-02-13	2024-07-22	Nebula Professional Pack	Actio
Accessory_PoE12-3PD	Accessory	PoE12-3PD	S240Z02000123	78:C5:7D:30:E7:26	2024-07-02	-	-	Actio
GW_NSG50(5C:00:48)	Security gateway	NSG50	S172L37100056	5C:E2:8C:5C:00:48	2023-02-13	2026-07-25	Nebula Professional Pack	Actio
GS2220-28HP	Switch	GS2220-28HP	S192L18080019	BC:CF:4F:B7:3C:F3	2024-06-11	2025-03-09	Nebula Professional Pack	Actio
XGS2220_Stack (Master)	Switch	XGS2220-30	S222L16090057	BC:99:11:FF:FD:2E	2024-05-02	2026-07-14	Nebula Professional Pack	Actio
XGS2220_Stack	Switch	XGS2220-54FP	S222L18090003	B8:EC:A3:FF:F2:A2	2024-05-02	2025-05-03	Nebula Professional Pack	Actio
XMG1930-30	Switch	XMG1930-30	S232L12002148	D8:EC:E5:C9:93:71	2024-06-11	2024-10-04 N/A (Limited lifetime)	Nebula Professional Pack Access L3 License	Actio

The following table describes the labels in this screen.

Table 186 Organization-wide > License & inventory > Devices

LABEL	DESCRIPTION
N Access Point	This shows the total number of access points (N) in the organization.
N Switch	This shows the total number of switches (N) in the organization.
N Security Appliance	This shows the total number of Security Gateway devices (N) in the organization.
N Mobile Router	This shows the total number of Mobile Router devices (N) in the organization.
N Accessory	This shows the total number of accessories (N) in the organization.

Table 186 Organization-wide > License & inventory > Devices (continued)

LABEL	DESCRIPTION
Actions	Select one or more Nebula Devices and then click this button to perform one of the following actions: **Change organization:** Moves the Nebula Device to an organization. The organizations must have the same owners. **Change site assignment**: Moves the selected Nebula Devices to a site, or remove them from their current site while leaving them in the organization. Note: When you change the site for a Security Firewall (see Table 1 on page 14 for information on the supported Security Firewall devices), select the deployment method for management by Nebula (see Step 8: Set up the Deployment Method on page 69 for more information), configure the WAN settings and choose the installation method. **Remove from organization**: Remove the Nebula Devices from NCC. You can manage the Nebula Devices in standalone mode, or re-add them to NCC later. **Assign license**: Assign licenses to the selected Nebula Devices. **Undo assign**: Unlink the inactive licenses from the associated Nebula Devices. After unlinking, the license will be categorized as unused in **Inventory**. An inactive license is a license that has been assigned to a Nebula Device but is not yet in use or queued. **Transfer license**: Moves the unused licenses linked to a Nebula Device to another Nebula Device. Nebula Devices can be in the same organization or in a different organization. The Nebula Devices must have the same owner. Bundled, Trial, and Promotion licenses cannot be transferred. **Purchase license**: Select what license to purchase and target expiration date to keep the Pro/Plus tier features/services running. You may export the list of required licenses to your computer. Then click the **Zyxel license marketplace** (**Check out**) button to complete your purchase. **Unused** licenses assigned to your organization will not count as it is not yet assigned to a Nebula Device. This button is available only for the Organization (Delegated) or Owner administrator account with a registered Nebula Device(s).
In use / Unused / Both	Select to display the Nebula Device currently in a site (**In use**), not current (**Unused**), or show all (**Both**).
Search	Enter a keyword or specify one or more filter criteria to filter the list of Nebula Devices and Security Firewall(s) in Cloud Monitoring mode.
+ Add	Add one or more new Nebula Devices to the organization, by entering the Nebula Device's MAC address and serial number. For details, see Section 12.2.2 on page 662.
Export	Click this button to save the Nebula Device list as a CSV or XML file to your computer.
	Select an entry's checkbox to select a specific Nebula Device. Otherwise, select the checkbox in the table heading row to select all Nebula Devices.
Device name	This shows the hostname of the Nebula Device.
Device type	This shows the category of Nebula Device (**Access Point**, **Switch**, **Security Router**, **Firewall**, **Gateway**, **Mobile Router**, **Accessory**) and Nebula Device model.
Site	This shows the site that the Nebula Device is currently in. If the Nebula Device is not in any site, the value is blank.
Model	This shows the Nebula Device's model.
Serial Number	This shows the Nebula Device's serial number.
MAC address	This shows the MAC address of the Nebula Device's first Ethernet port.
Device tag	This shows the tag created and added to the Nebula Device.

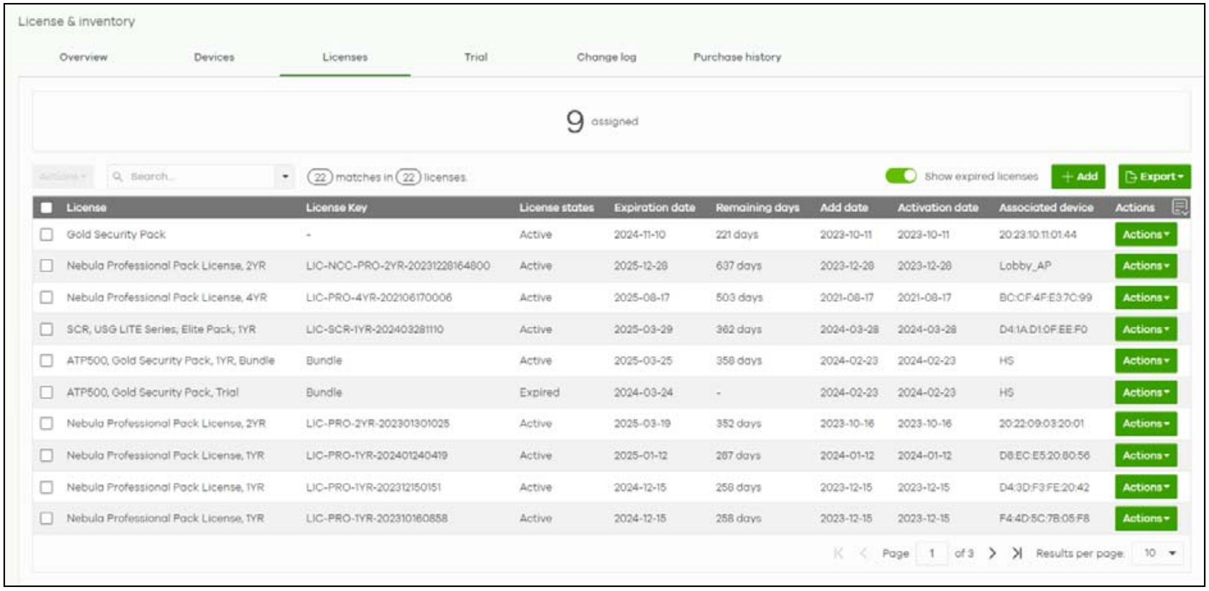
Table 186 Organization-wide > License & inventory > Devices (continued)

LABEL	DESCRIPTION
Add date	This shows the date on which the Nebula Device was added to NCC. If the Security Firewall has NOT yet connected to NCC (see Table 1 on page 14 for the list of Security Firewalls): • **Native mode**. Click this button and select **Nebula Native mode** in the **Deployment Method**. Follow the instructions to connect the Security Firewall to NCC. • **Waiting ZTP** will be shown if **Native mode** is not available. Click the **Waiting ZTP** button and select **Zero Touch Provisioning** in **Deployment Method** to configure the ZTP settings. Note: The **Deployment Method** screen will not show for Security Firewall(s) in Cloud Monitoring mode.
Unused / In use	This shows **Unused** if the Nebula Device is not assigned to a site, or **In use** if the Nebula Device is currently in a site.
Country	This shows the country in which the Nebula Device is located.
Expiration date	This shows the date on which the Nebula Device's NCC license will expire.
License info	This shows the type of NCC license assigned to the Nebula Device. Note: Move the pointer over this field to see information about all licenses associated with this Nebula Device.
Action	Select one or more Nebula Devices and then click this button to perform one of the following actions: **Change organization:** Moves the Nebula Device to an organization. The organizations must have the same owners. **Change site assignment**: Moves the selected Nebula Devices to a selected site, or removes them from their current site while leaving them in the organization. Note: When you change the site for a Security Firewall (see Table 1 on page 14 for information on the supported Security Firewall devices), select the deployment method for management by Nebula (see Step 8: Set up the Deployment Method on page 69 for more information), configure the WAN settings and choose the installation method. **Remove from organization**: Remove the Nebula Devices from NCC. You can manage the Nebula Devices in standalone mode, or re-add them to NCC later. **Assign license**: Assign unassigned licenses to the selected Nebula Devices. **Undo assign**: Unlink the inactive licenses from the associated Nebula Devices. After unlinking, the license will be categorized as unused in **Inventory**. An inactive license is a license that has been assigned to a Nebula Device but is not yet in use or queued. **Transfer license**: Moves unused licenses linked from one Nebula Device to another Nebula Device. The Nebula Devices can be in the same organization or in a different organization. The Nebula Devices must have the same owner. Bundled, Trial, and Promotion licenses cannot be transferred.

12.2.7 License & Inventory Licenses Screen

Use these screen to view and manage licenses in the organization. Click **Organization-wide** > **License & inventory** > **Licenses** to access this screen.

Figure 251 Organization-wide > License & inventory > Licenses



9 assigned

22 matches in 22 licenses.

License	License Key	License states	Expiration date	Remaining days	Add date	Activation date	Associated device	Actions
Gold Security Pack	-	Active	2024-11-10	221 days	2023-10-11	2023-10-11	20:23:10:11:01:44	Actions
Nebula Professional Pack License, 2YR	LIC-NCC-PRO-2YR-20231228164800	Active	2025-12-28	637 days	2023-12-28	2023-12-28	Lobby_AP	Actions
Nebula Professional Pack License, 4YR	LIC-PRO-4YR-202106170006	Active	2025-08-17	503 days	2021-08-17	2021-08-17	BC:CF:4F:E3:7C:99	Actions
SCR, USG LITE Series, Elite Pack, 1YR	LIC-SCR-1YR-20240328110	Active	2025-03-29	362 days	2024-03-28	2024-03-28	D4:1A:D1:0F:EE:F0	Actions
ATP500, Gold Security Pack, 1YR, Bundle	Bundle	Active	2025-03-25	358 days	2024-02-23	2024-02-23	HS	Actions
ATP500, Gold Security Pack, Trial	Bundle	Expired	2024-03-24	-	2024-02-23	2024-02-23	HS	Actions
Nebula Professional Pack License, 2YR	LIC-PRO-2YR-202301301025	Active	2025-03-19	352 days	2023-10-16	2023-10-16	20:22:09:03:20:01	Actions
Nebula Professional Pack License, 1YR	LIC-PRO-1YR-202401240419	Active	2025-01-12	287 days	2024-01-12	2024-01-12	D8:EC:E5:20:80:56	Actions
Nebula Professional Pack License, 1YR	LIC-PRO-1YR-202312150151	Active	2024-12-15	258 days	2023-12-15	2023-12-15	D4:3D:F3:FE:20:42	Actions
Nebula Professional Pack License, 1YR	LIC-PRO-1YR-202310160858	Active	2024-12-15	258 days	2023-12-15	2023-12-15	F4:4D:5C:7B:05:F8	Actions

The following table describes the labels in this screen.

Table 187 Organization-wide > License & inventory > Licenses

LABEL	DESCRIPTION
N assigned	This shows the total number of licenses (N) in the organization that are assigned to a Nebula Device and activated.
N unused (Pro Pack, 1MO/1YR/2YR/4YR/7YR) or N unused (Plus Pack, 1MO/1YR/2YR)	This shows the total number of Nebula Professional Pack or Nebula Plus Pack licenses (N) in the organization that are not assigned to a Nebula Device.
N unused (UTM Pack, 1MO/1YR/2YR)	This shows the total number of UTM Security Pack licenses (N) in the organization that are not assigned to a Nebula Device.
Actions	Select one or more Nebula Devices and then click this button to perform one of the following actions: **Change organization:** Moves the selected licenses to an organization. The organizations must have the same owners. **Assign License**: Assign the selected licenses to one or more Nebula Devices. Only the licenses applicable for the Nebula Device can be selected. **Undo assign**: Unlink the inactive licenses from the associated Nebula Devices. After unlinking, the license will be categorized as unused in **Inventory**. An inactive license is a license that has been assigned to a Nebula Device but is not yet in use or queued. **Transfer license**: Moves the unused licenses linked to a Nebula Device to another Nebula Device. The Nebula Devices can be in the same organization or in a different organization. The Nebula Devices must have the same owner. Bundled, Trial, and Promotion licenses cannot be transferred.
Search	Enter a keyword or specify one or more filter criteria to filter the list of licenses.
N licenses	This shows the total assigned and unassigned licenses in the organization.

Table 187 Organization-wide > License & inventory > Licenses (continued)

LABEL	DESCRIPTION
Show expired licenses	Click this to display licenses that are past their validity.
+ Add	Add one or more new licenses to the organization, by entering their license keys. For details, see Section 12.2.4 on page 664.
Export	Click this to save the license list as a CSV or XML file to your computer.
License Key	This shows the key of license, including bundled licenses.
Service	This shows the service that license is for, for example "Nebula Professional Pack".
License states	This shows the current status of the license: • **Activated**: The license is assigned to a specific Nebula Device and in use. • **Inactive**: The license is assigned to a specific Nebula Device but not activated. • **Expired**: The license is past its validity. • **Queued**: The license is assigned to a specific Nebula Device, and the license is waiting for the currently active license to expire. • **Unused**: The license is not assigned to a specific Nebula Device. • **Deferred**: Activation of the license is intentionally delayed on a specific Nebula Device.
Expiration date	This shows the date on which the license will expire. **Queued** means there are multiple licenses assigned to the Nebula Device, and the license is waiting for the currently active license to expire.
Remaining days	This shows how days remain until the license expires.
Add date	This shows the date on which the license was added to NCC. If the Security Firewall has NOT yet connected to NCC: • **Native mode**. Click this button and select **Nebula Native mode** in **Deployment Method**. Follow the instructions to connect the Security Firewall to NCC. • **Waiting ZTP** will be shown if **Native mode** is not available. Click the **Waiting ZTP** button and select **Zero Touch Provisioning** in **Deployment Method** to configure the ZTP settings. Note: The **Deployment Method** screen will not show for Security Firewall(s) in Cloud Monitoring mode.
Activation date	This shows the date on which the license was activated.
Associated device	This shows the name and model of the Nebula Device that the license is assigned to.
Associated site	This shows the name of the site that the license is being used in. Click the site to go to its dashboard.
Action	Click this button to perform the following actions: **Change organization:** Moves the selected licenses to an organization. The organizations must have the same owners. **Assign License**: Assign the selected licenses to one or more Nebula Devices. Only the licenses applicable for the Nebula Device can be selected. **Undo assign**: Unlink the inactive licenses from the associated Nebula Devices. After unlinking, the license will be categorized as unused in **Inventory**. An inactive license is a license that has been assigned to a Nebula Device but is not yet in use or queued. **Transfer license**: Moves the unused licenses linked to a Nebula Device to another Nebula Device. The Nebula Devices can be in the same organization or in a different organization. The Nebula Devices must have the same owner. Bundled, Trial, and Promotion licenses cannot be transferred.

12.2.8 License & Inventory Trial Screen

A free 30-day trial license is available for each Nebula organization you create. Trial licenses are available even if you have no Nebula Devices in the organization.

Note: Make sure services are usable by the Nebula Device before activating the trial license.

All trial licenses apply to all Nebula Devices in an organization. There is no limit to the number of organizations. You will lose access to related services or advanced NCC features when trial expires. You must then buy a standard license (not a trial) for each Nebula Device.

Activating a standard license during the trial period will add the remaining trial time to the standard license time. However, activating a Nebula Professional Pack license during the trial period will cancel the trial. NCC activates inactive licenses when the associated trial has expired.

If you activate the Nebula Professional Pack Trial, you can use advanced features in Nebula Devices in all organizations.

Moving a Nebula Device to another organization will cancel its trial license. However, a trial license is still available for the Nebula Device if you did not activate a trial or standard license of the same type in the new organization.

Note: Each trial license is not available if you previously activated a trial or standard license of the same type.

At the time of writing, trial licenses are associated with the following:

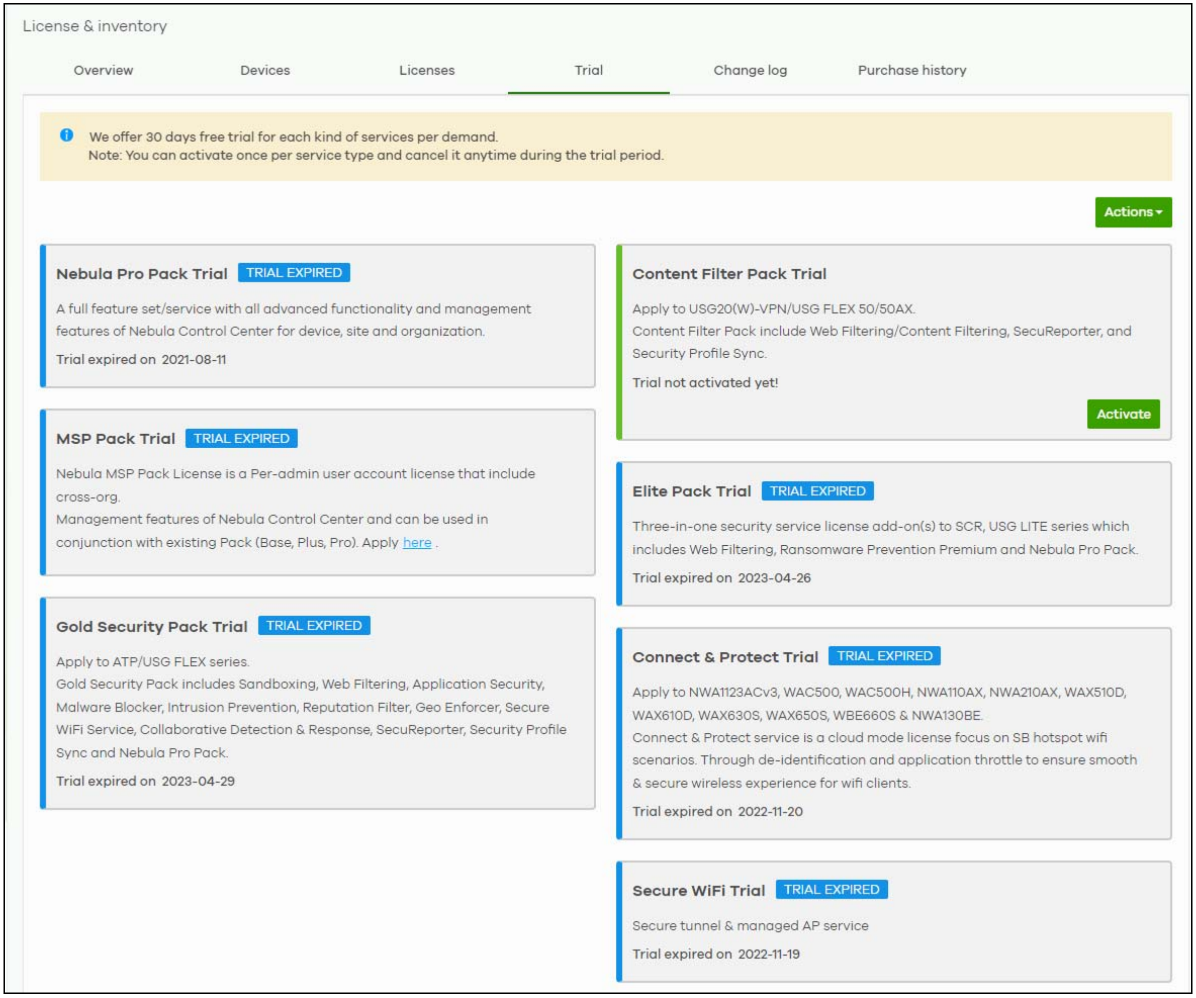
Table 188 Trial Licenses Summary

TRIAL LICENSE	ASSOCIATED FEATURES OR NEBULA DEVICES
Nebula Pro Pack Trial	This is for advanced features, except open API access, within the Nebula Device's organization. See Section 4.9.6 on page 299 for more information on open API access.
MSP Pack Trial	This is for new NCC accounts or NCC accounts that have not used MSP before. This allows you to manage multiple organizations.
Gold Security Pack Trial	This is for ATP devices and USG FLEX devices except USG20-VPN / USG20W-VPN / USG FLEX 50. Note: The Gold Security Pack Trial also includes use of advanced features except open API access from the Nebula Pro Pack Trial.
Content Filter Pack Trial	This is for USG FLEX 50 / USG20-VPN / USG20W-VPN devices.
Elite Pack Trial	This unlocks security services for SCR 50AXE / USG LITE 60AX.
Connect & Protect Trial	This allows you to manage small business WiFi hotspots using an NWA1123-ACv3, WAC500, WAC500H, NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, or WAX650S.
Secure WiFi Trial	This is for remote APs (access points) to securely connect a ZyWALL ATP / USG FLEX (except USG FLEX 50) in the office.

See Table 2 on page 17 for detailed information on the licenses available in NCC.

Use this screen to view the status and activate trial licenses for Nebula Devices within the organization. Click **Organization-wide** > **License & inventory** > **Trial** to access this screen.

Figure 252 Organization-wide > License & inventory > Trial


License & inventory

We offer 30 days free trial for each kind of services per demand.
Note: You can activate once per service type and cancel it anytime during the trial period.

Nebula Pro Pack Trial TRIAL EXPIRED

A full feature set/service with all advanced functionality and management features of Nebula Control Center for device, site and organization.

Trial expired on 2021-08-11

MSP Pack Trial TRIAL EXPIRED

Nebula MSP Pack License is a Per-admin user account license that include cross-org.
Management features of Nebula Control Center and can be used in conjunction with existing Pack (Base, Plus, Pro). Apply here .

Gold Security Pack Trial TRIAL EXPIRED

Apply to ATP/USG FLEX series.
Gold Security Pack includes Sandboxing, Web Filtering, Application Security, Malware Blocker, Intrusion Prevention, Reputation Filter, Geo Enforcer, Secure WiFi Service, Collaborative Detection & Response, SecuReporter, Security Profile Sync and Nebula Pro Pack.

Trial expired on 2023-04-29

Content Filter Pack Trial

Apply to USG20(W)-VPN/USG FLEX 50/50AX.
Content Filter Pack include Web Filtering/Content Filtering, SecuReporter, and Security Profile Sync.

Trial not activated yet!

Elite Pack Trial TRIAL EXPIRED

Three-in-one security service license add-on(s) to SCR, USG LITE series which includes Web Filtering, Ransomware Prevention Premium and Nebula Pro Pack.

Trial expired on 2023-04-26

Connect & Protect Trial TRIAL EXPIRED

Apply to NWA1123ACv3, WAC500, WAC500H, NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, WAX650S, WBE660S & NWA130BE.
Connect & Protect service is a cloud mode license focus on SB hotspot wifi scenarios. Through de-identification and application throttle to ensure smooth & secure wireless experience for wifi clients.

Trial expired on 2022-11-20

Secure WiFi Trial TRIAL EXPIRED

Secure tunnel & managed AP service

Trial expired on 2022-11-19

The following table describes the labels in this screen.

Table 189 Organization-wide > License & inventory > Trial

LABEL	DESCRIPTION
Actions	Click this to perform one of the following actions: • **Activate trial for all**: select this to start using all trial licenses available for your organization. Then click **Confirm** to continue. • **Deactivate trial for all**: select this to cancel all trial licenses currently in use in your organization. Then click **Confirm** to continue. Note: When you cancel any trial license, you cannot re-activate the unused portion of the trial license.
(Status)	The status displays next to the name of a trial license. If no status displays, it means you can activate the trial license. The trial license can be used on the Nebula Devices within the organization. Click **Activate** to start using the services of the trial license. Note: You can activate each type of 30-day trial license on each organization only once.

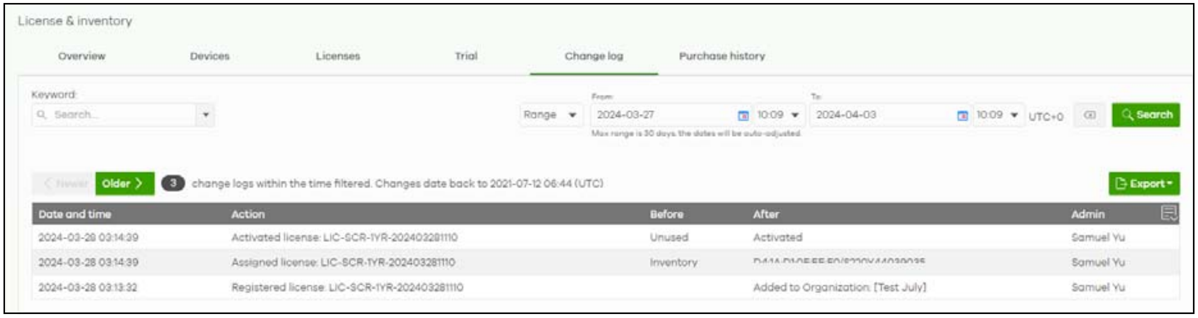
Table 189 Organization-wide > License & inventory > Trial (continued)

LABEL	DESCRIPTION
IN PROGRESS	The 30-day countdown for the trial license has begun. Click **Deactivate** if you want to cancel the trial license. Note: You can cancel the trial license anytime during the 30-day trial period, but you cannot re-activate it.
TRIAL EXPIRED	You have previously activated a trial or standard license and the license period has ended.
CANCELED	You have deactivated the trial license during the 30-day trial period.
Activate	Click this to start using the 30-day trial license. Then click **Confirm** to continue.
Deactivate	Click this to cancel the 30-day trial license anytime before it expires. Then click **Confirm** to continue.

12.2.9 License & Inventory Change Log Screen

Use this screen to view a record of Nebula Device and license actions within the organization. The log also shows the change in state of the organization, as a before and after, as a result of each action. Click **Organization-wide** > **License & inventory** > **Change log** to access this screen.

Figure 253 Organization-wide > License & inventory > Change log



3 change logs within the time filtered. Changes date back to 2021-07-12 06:44 (UTC)

Date and time	Action	Before	After	Admin
2024-03-28 03:14:39	Activated license: LIC-SCR-1YR-202403281110	Unused	Activated	Samuel Yu
2024-03-28 03:14:39	Assigned license: LIC-SCR-1YR-202403281110	Inventory	[illegible]	Samuel Yu
2024-03-28 03:13:32	Registered license: LIC-SCR-1YR-202403281110		Added to Organization: [Test July]	Samuel Yu

The following table describes the labels in this screen.

Table 190 Organization-wide > License & inventory > Change log

LABEL	DESCRIPTION
Keyword	Enter a keyword or specify one or more filter criteria to filter the list of log entries.
Range / Before	Select a filtering option, set a date, and then click **Search** to filter log entries by date. **Range**: Display log entries from the first specified date to the second specified date. **Before**: Display log entries from the beginning of the log to the selected date.
Search	Click this to update the list of logs based on the search criteria.
Reset filters ⌫	Click this to return the search criteria to the previously saved time setting.
Newer / Older	Click to view the list of log messages with the most recent or oldest message displayed first.
	This shows the total number of the log messages that match the search criteria. It also shows the date and time the very first log was created.
Export	Click this button to save the log list as a CSV or XML file to your computer.
Date and time	This shows the date and time in UTC+00:00 (or UTC+0) when the log was recorded. UTC is a standard time for use around the world (formerly known as Greenwich Mean Time or GMT). UTC is an international abbreviation that is neither French nor English. It means both "Temps Universel Coordonné" and "Coordinated Universal Time".

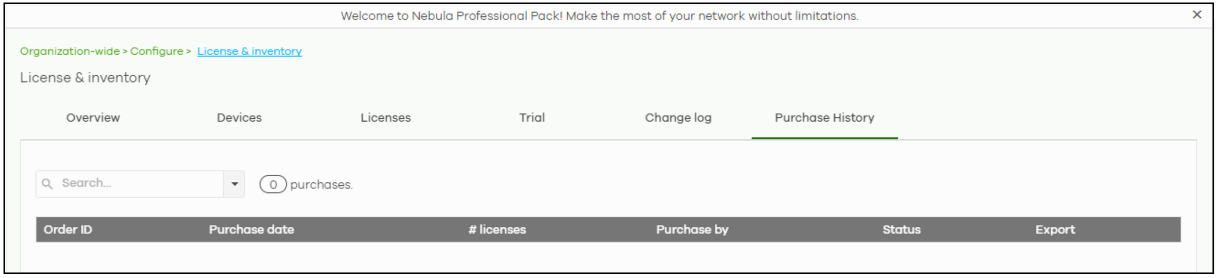
Table 190 Organization-wide > License & inventory > Change log (continued)

LABEL	DESCRIPTION
Action	This shows the action that triggered the log entry.
Before	This shows the old setting or state that was overwritten with the new value.
After	This shows the new setting or state.
Admin	This shows the name of the NCC administrator account that made the changes.
▤	Click this icon to display a greater or lesser number of configuration fields.

12.2.10 License & Inventory Purchase History Screen

Use this screen to view a record of Nebula Device license purchased within the organization. Click **Organization-wide** > **License & inventory** > **Purchase history** to access this screen.

Figure 254 Organization-wide > License & inventory > Purchase history



Welcome to Nebula Professional Pack! Make the most of your network without limitations.

The following table describes the labels in this screen.

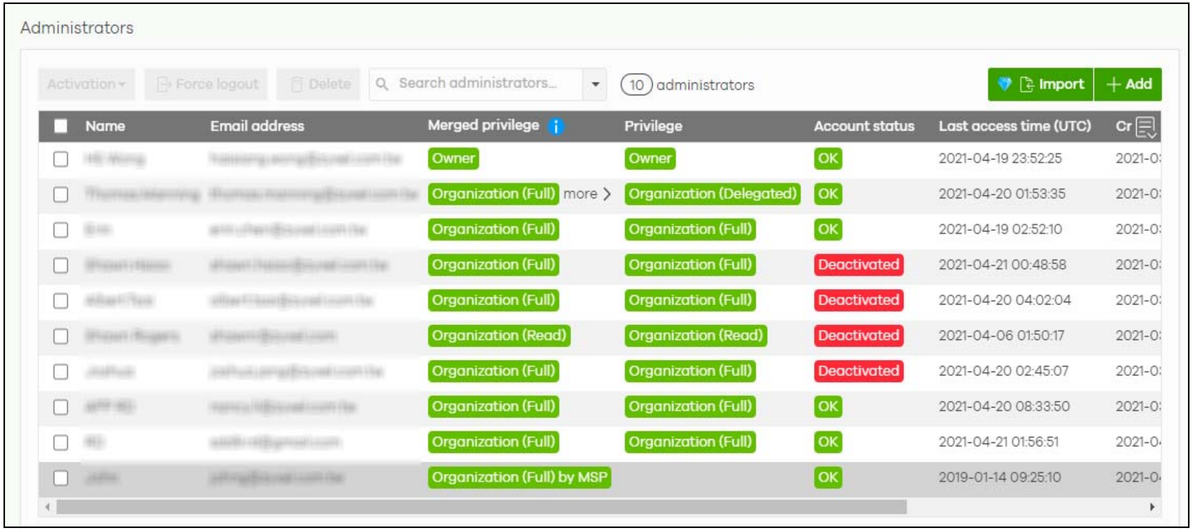
Table 191 Organization-wide > License & inventory > Purchase history

LABEL	DESCRIPTION
Keyword	Enter a keyword or specify one or more filter criteria to filter the list of purchased license entries.
Search	Click this to update the list of logs based on the search criteria.
N purchases	This displays the total purchased licenses in the organization.
Order ID	This displays a unique code that identifies the order. Clicking this link will take you to the **Marketplace** > **Order History** screen.
Purchase date	This displays the date that the order was created.
# licenses	This displays the number of licenses purchased for the specified license type.
Purchase by	This displays the email address of the NCC account that created the order.
Status	This displays the current status of the order. • **Done**: The order has been paid for and the license was successfully activated on the target Nebula Device. • **Processing**: The license activation on the target Nebula Device is still under process. • **Failed**: The license was not successfully activated on the target Nebula Device.
Export	Click this to download the order details as a CSV or XML file to your computer. This includes the **Order ID** and each license's assigned device information.

12.3 Administrators

Use this screen to view, manage and create administrator accounts for the specified organization. Click **Organization-wide** > **Administrators** to access this screen.

Figure 255 Organization-wide > Administrators



Administrators

□	Name	Email address	Merged privilege	Privilege	Account status	Last access time (UTC)	Cr
□	[redacted]	[redacted]	Owner	Owner	OK	2021-04-19 23:52:25	2021-0
□	[redacted]	[redacted]	Organization (Full) more >	Organization (Delegated)	OK	2021-04-20 01:53:35	2021-0
□	[redacted]	[redacted]	Organization (Full)	Organization (Full)	OK	2021-04-19 02:52:10	2021-0
□	[redacted]	[redacted]	Organization (Full)	Organization (Full)	Deactivated	2021-04-21 00:48:58	2021-0
□	[redacted]	[redacted]	Organization (Full)	Organization (Full)	Deactivated	2021-04-20 04:02:04	2021-0
□	[redacted]	[redacted]	Organization (Read)	Organization (Read)	Deactivated	2021-04-06 01:50:17	2021-0
□	[redacted]	[redacted]	Organization (Full)	Organization (Full)	Deactivated	2021-04-20 02:45:07	2021-0
□	[redacted]	[redacted]	Organization (Full)	Organization (Full)	OK	2021-04-20 08:33:50	2021-0
□	[redacted]	[redacted]	Organization (Full)	Organization (Full)	OK	2021-04-21 01:56:51	2021-0
□	[redacted]	[redacted]	Organization (Full) by MSP		OK	2019-01-14 09:25:10	2021-0

The following table describes the labels in this screen.

Table 192 Organization-wide > Administrators

LABEL	DESCRIPTION
Activation	Click this button to **Activate/Deactivate** the selected accounts. Then click **Update**.
Force logout	Click this button to force the selected accounts to log out of the NCC.
Delete	Click this button to remove the selected accounts.
Search	Specify your desired filter criteria to filter the list of administrator accounts.
administrators	This shows the number of administrator accounts in the list.

Table 192 Organization-wide > Administrators (continued)

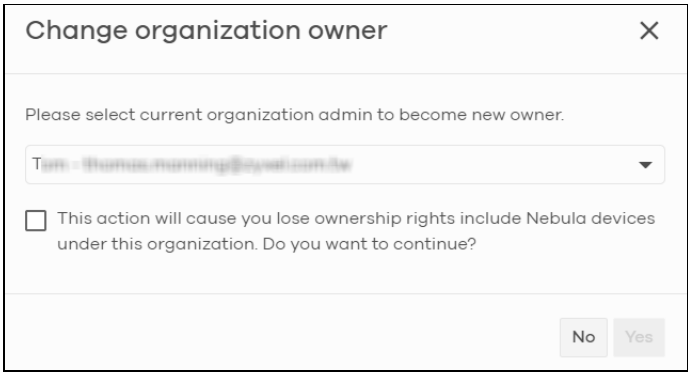
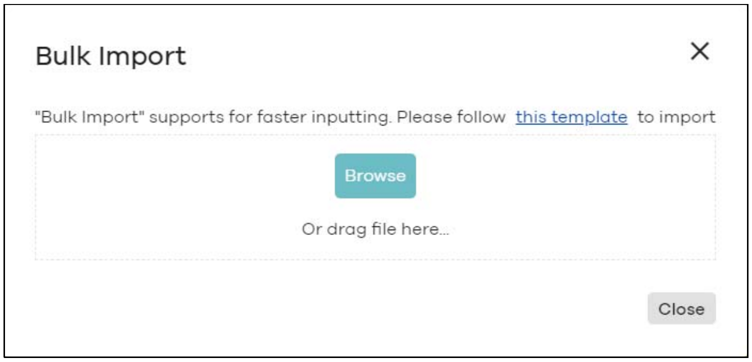
LABEL	DESCRIPTION
Change owner	This button is only available if you are the organization owner. Click this button to transfer ownership of the organization to another user account. The new owner account must be an organization full administrator. Change organization owner Please select current organization admin to become new owner. T[redacted] □ This action will cause you lose ownership rights include Nebula devices under this organization. Do you want to continue? After transferring ownership, NCC performs the following actions: • Changes your account from organization owner to organization full administrator. • Transfers all Nebula Devices and licenses in the organization to the new owner. • Sends the new owner an email, notifying them of the change.
Import	Click this button to create administrator accounts in bulk by importing a complete list of all new administrators in an Excel file. Bulk Import "Bulk Import" supports for faster inputting. Please follow this template to import
Add	Click this button to create a new administrator account. See Section 12.3.0.1 on page 678.
Name	This shows the name of the administrator account.
Email address	This shows the email address of the administrator account.
Merged privilege	This shows the final privilege the account has in the organization, when organization privileges configured on different screens are combined and prioritized. Organization privileges can be configured on the following screens; the highest privilege level takes priority: • **MSP cross-org manage** > **Admins & teams** > **Admins** • **MSP cross-org manage** > **Admins & teams** > **Teams** • **Group-wide manage** > **Administrators** • **Organization-wide** > **Administrators** For more information, see Section 14.3.1 on page 746.

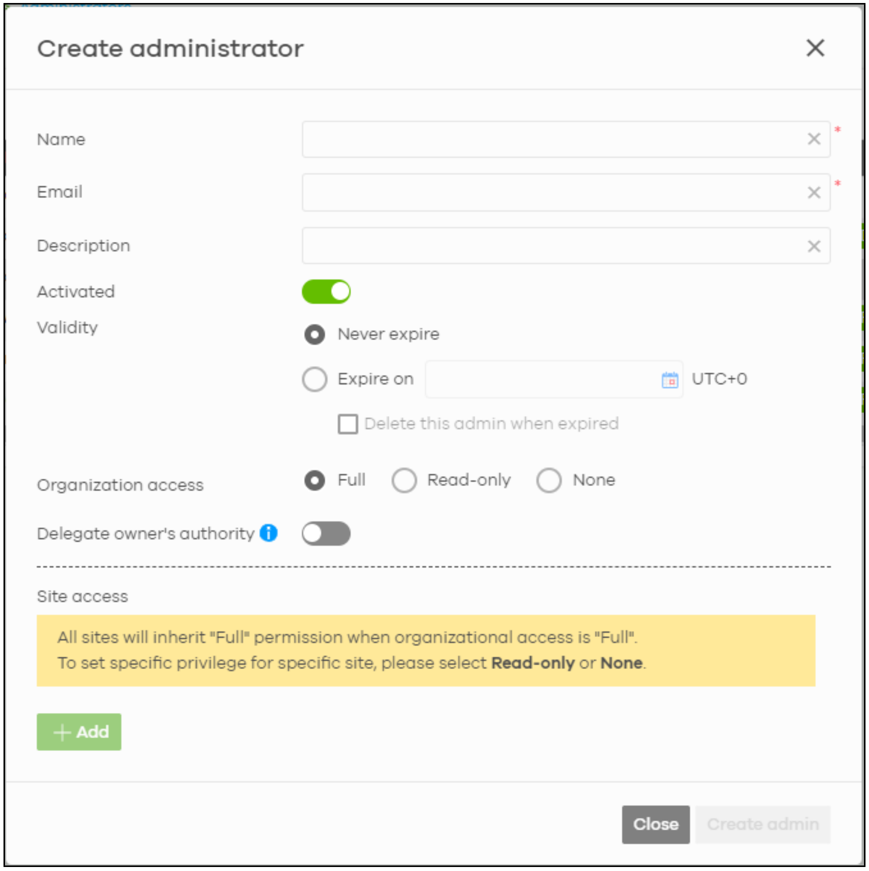
Table 192   Organization-wide > Administrators (continued)

LABEL	DESCRIPTION
Privilege	This shows whether the administrator account has read-only, monitor-only, guest ambassador, or read and write (full) access to the organization and sites. **Installer** indicates that the administrator account can register Nebula Devices at a site. **Owner** indicates that the administrator account is the creator of the organization, who has full access to that organization and cannot be deleted by other administrators. **Organization (Delegated)** means that the administrator account has delegated owner privileges. This type of account can perform all of the same actions as the organization owner, except for the following: • Delete organization • Transfer organization ownership • Assign delegate owner privileges to an administrator account.
Account status	This shows whether the administrator account has been validated (**OK**). It shows **Deactivated** if an administrator account has been created but cannot be used. This may happen since you can only have up to five active administrator account on Nebula (free). It shows **Unverified** if Nebula has no record of this administrator account. It shows **Expired** if the administrator account has passed the expiration time and cannot access the organization.
Last access time	This shows the last date and time traffic was sent from the administrator account.
Create date	This shows the date and time the administrator account was created.
Status change date	This shows the last date and time the administrator account status was changed.
☰	Click this icon to display a greater or lesser number of configuration fields.

12.3.0.1 Create/Update Administrator

In the **Organization-wide** > **Administrator** screen, click the **Add** button to create a new administrator account or double-click an existing account entry to modify the account settings.

Figure 256 Organization-wide > Administrator: Create/Update administrator



Create administrator

Name

Email

Description

Activated

Validity

● Never expire

○ Expire on UTC+0

□ Delete this admin when expired

Organization access ● Full ○ Read-only ○ None

Delegate owner's authority

Site access

All sites will inherit "Full" permission when organizational access is "Full".
To set specific privilege for specific site, please select **Read-only** or **None**.

The following table describes the labels in this screen.

Table 193 Organization-wide > Administrator: Create/Update administrator

LABEL	DESCRIPTION
Name	Enter a descriptive name for the administrator account.
Email	Enter the email address of the administrator account, which is used to log into NCC. This field is read-only if you are editing an existing account.
Description	Enter a description for this administrator. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Activated	Click the switch to the right to enable the account. Alternatively, click the switch to the left to disable the account.
Validity	Specify how long the account is valid. Choices are: **Never expire** – select this if the account never expire. **Expire on** – select this to specify the date the account can no longer access the organization. Select **Delete this admin when expired** to remove this account from the administrator list when the **Expire on** date has been reached. Otherwise, this account will remain on the administrator list with an inactivated status.

Table 193 Organization-wide > Administrator: Create/Update administrator (continued)

LABEL	DESCRIPTION
Organization access	Set the administrator account's access to the organization. When an administrator account has read and write (**Full**) access, the administrator can create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula Devices in the organization. Note: The administrator account you use to create an organization is the organization creator account that has full access to that organization. The organization creator account cannot be deleted by other organization administrators. If you select **Read-only**, the administrator account can be the organization administrator (that has no write access to the organization) and also be a site administrator. If you select **None**, the administrator account can only be a site administrator.
Delegate owner's authority	This setting is only available when **Organization access** is set to **Full**. Select this setting to grant delegate owner privileges to an organization full administrator account. An account with delegate owner privileges can perform all of the same actions as the organization owner, except for the following: • Delete organization • Transfer organization ownership • Assign delegate owner privileges to an administrator account.
YES, I want to do it.	The checkbox displays only when an administrator that has full access to the organization disables the **Activated** switch to disable his/her own account. Note: After you select the checkbox and click **Update admin**, you lose administrator privileges and cannot manage the organization again. If you have other organizations created on your account, you can click and select another organization to manage in the **MSP Portal** screen.
Site	This field is available only when you set the account's organization access to **Read-only** or **None**. Select the site to which you want to set the account's access.
Privilege	This field is available only when you set the account's organization access to **Read-only** or **None**. Set the administrator account's access to the site. You can select from **Read-only**, **Monitor-only**, **Guest Ambassador**, **Installer** and **Full** (read and write). An administrator account that has **Guest Ambassador** access can create, remove or manage guest accounts using the **Cloud authentication** screen (see Section on page 726). **Installer** access allows an administrator to register Nebula Devices at this site.
Add	Click this button to create a new entry in order to configure the account's access to another site.
Close	Click this button to exit this screen without saving.
Create admin/ Update admin	Click this button to save your changes and close the screen.

12.4 Organization-wide Manage

Use the **Organization-wide manage** menus to create new sites, register or unregister a Nebula Device, change organization general settings, and manage licenses, user accounts, administrator accounts or VPN members in the organization.

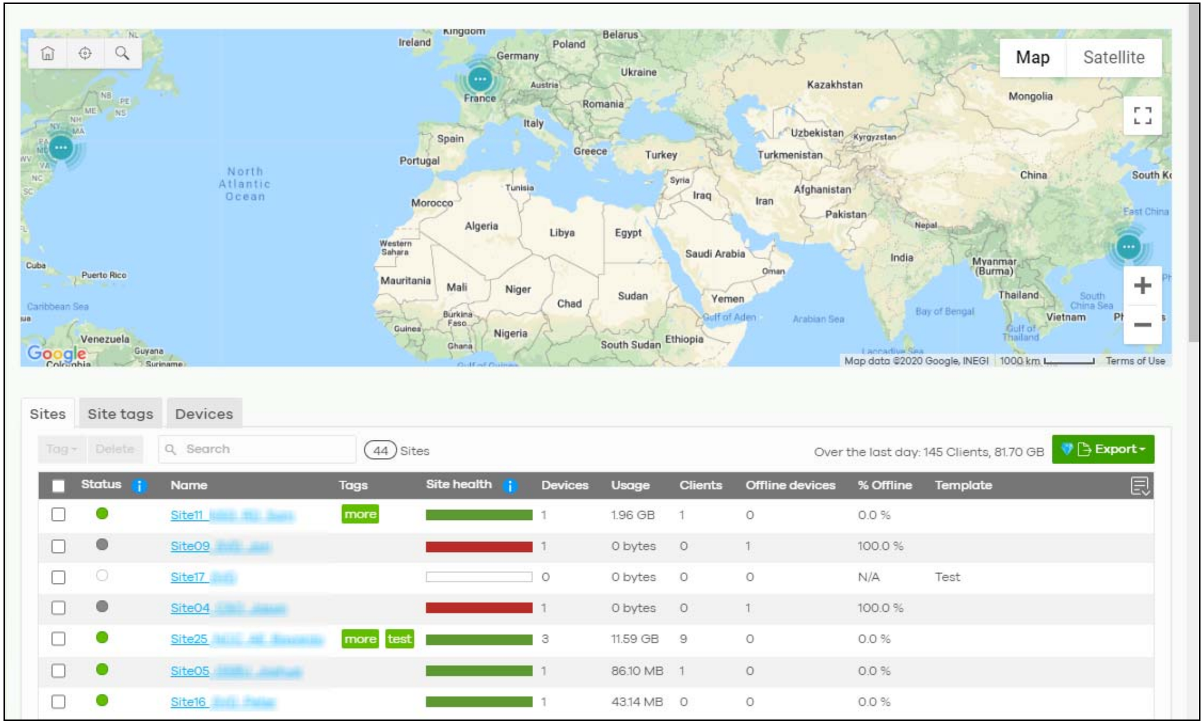
12.4.1 Organization Portal

This screen shows you the site locations on a Google map and the summary of sites, site tags and connected Nebula Devices for the selected organization.

Note: The Nebula Accessories will not display on Google map.

Click **Organization-wide** > **Organization-wide manage** > **Organization portal** to access this screen.

Figure 257 Organization-wide > Organization-wide manage > Organization portal



44 Sites

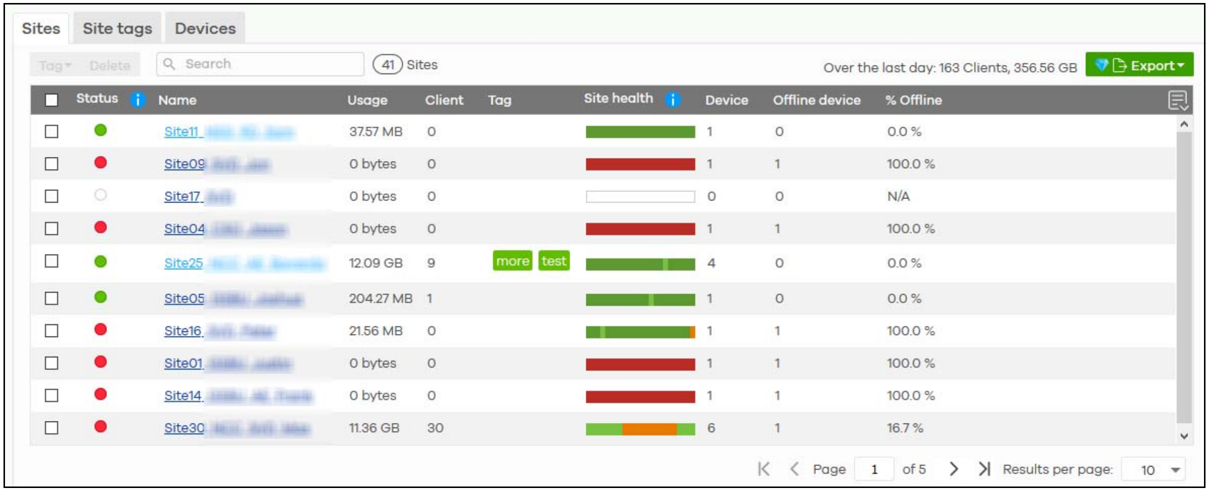
Over the last day: 145 Clients, 81.70 GB

☐	Status	Name	Tags	Site health	Devices	Usage	Clients	Offline devices	% Offline	Template
☐	●	Site11 [redacted]	more	🟩	1	1.96 GB	1	0	0.0 %	
☐	●	Site09 [redacted]		🟥	1	0 bytes	0	1	100.0 %	
☐	○	Site17 [redacted]		▭	0	0 bytes	0	0	N/A	Test
☐	●	Site04 [redacted]		🟥	1	0 bytes	0	1	100.0 %	
☐	●	Site25 [redacted]	more test	🟩	3	11.59 GB	9	0	0.0 %	
☐	●	Site05 [redacted]		🟩	1	86.10 MB	1	0	0.0 %	
☐	●	Site16 [redacted]		🟩	1	43.14 MB	0	0	0.0 %	

12.4.1.1 Sites

Click the **Sites** tab in the **Overview** screen to view detailed information of the sites which are associated with the selected organization.

Figure 258 Organization-wide > Organization-wide manage > Organization portal: Sites



41 Sites

Over the last day: 163 Clients, 356.56 GB

☐	Status	Name	Usage	Client	Tag	Site health	Device	Offline device	% Offline
☐	●	Site11 [redacted]	37.57 MB	0		🟩	1	0	0.0 %
☐	●	Site09 [redacted]	0 bytes	0		🟥	1	1	100.0 %
☐	○	Site17 [redacted]	0 bytes	0		□	0	0	N/A
☐	●	Site04 [redacted]	0 bytes	0		🟥	1	1	100.0 %
☐	●	Site25 [redacted]	12.09 GB	9	more test	🟩	4	0	0.0 %
☐	●	Site05 [redacted]	204.27 MB	1		🟩	1	0	0.0 %
☐	●	Site16 [redacted]	21.56 MB	0		🟩	1	1	100.0 %
☐	●	Site01 [redacted]	0 bytes	0		🟥	1	1	100.0 %
☐	●	Site14 [redacted]	0 bytes	0		🟥	1	1	100.0 %
☐	●	Site30 [redacted]	11.36 GB	30		🟩	6	1	16.7 %

Page 1 of 5 Results per page: 10

The following table describes the labels in this screen.

Table 194 Organization-wide > Organization-wide manage > Organization portal: Sites

LABEL	DESCRIPTION
Tag	Select one or multiple sites and click this button to create a new tag for the sites or delete an existing tag.
Delete	Select the sites and click this button to remove it.
Search	Enter a key word as the filter criteria to filter the list of sites.
Sites	This shows the number of sites in this organization.
Over the last day	This shows how many clients are associated with the sites in this organization and the total amount of data transmitted or received by the clients in the past day.
Export	Click this button to save the site list as a CSV or XML file to your computer.
Status	This shows the status of Nebula Devices in the site. • Green: All Nebula Devices are online and have no alerts. • Amber: Some Nebula Devices have alerts. • Red: Some Nebula Devices are offline. • Gray: All Nebula Devices have been offline for 7 days or more. • White: No Nebula Devices.
Name	This shows the descriptive name of the site.
Usage	This shows the amount of data consumed by the site. Note: This shows '–' for Nebula Accessories.
Clients	This shows the number of clients connected to Nebula Devices in the site. Note: This shows '–' for Nebula Accessories.
Tag	This shows the user-specified tag that is added to the site.
Site health	This shows the percentage of uptime in a given time interval to indicate the site's network availability. • Green: 95 – 100% network uptime • Dark green: 75 – 95% network uptime • Brown: 50 – 75% network uptime • Red: < 50% network uptime • Grey: No uptime data
Device	This shows the total number of Nebula Devices deployed in the site.

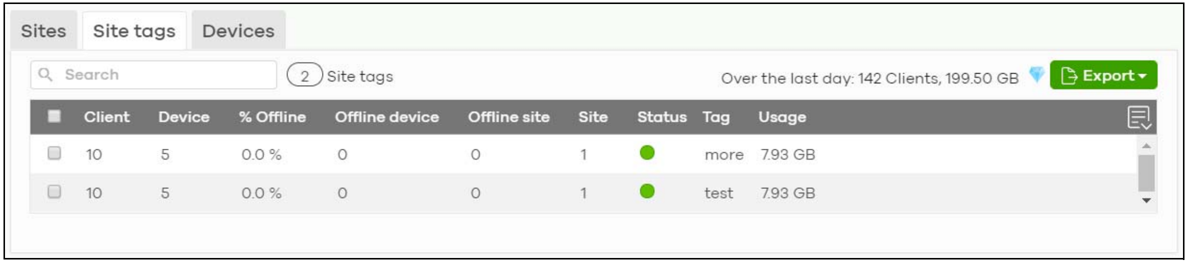
Table 194 Organization-wide > Organization-wide manage > Organization portal: Sites (continued)

LABEL	DESCRIPTION
Offline device	This shows the number of Nebula Devices which are added to the site but not accessible by the NCC now.
% Offline	This shows what percentage of the connected clients are currently offline.
▤	Click this icon to display a greater or lesser number of configuration fields.

12.4.1.2 Site tags

Click the **Site tags** tab in the **Overview** screen to view the tags created and added to the sites for monitoring or management purposes.

Figure 259 Organization-wide > Organization-wide manage > Organization portal: Site tags



Sites | Site tags | Devices

Search | 2 Site tags | Over the last day: 142 Clients, 199.50 GB | Export

☐	Client	Device	% Offline	Offline device	Offline site	Site	Status	Tag	Usage
☐	10	5	0.0 %	0	0	1	●	more	7.93 GB
☐	10	5	0.0 %	0	0	1	●	test	7.93 GB

The following table describes the labels in this screen.

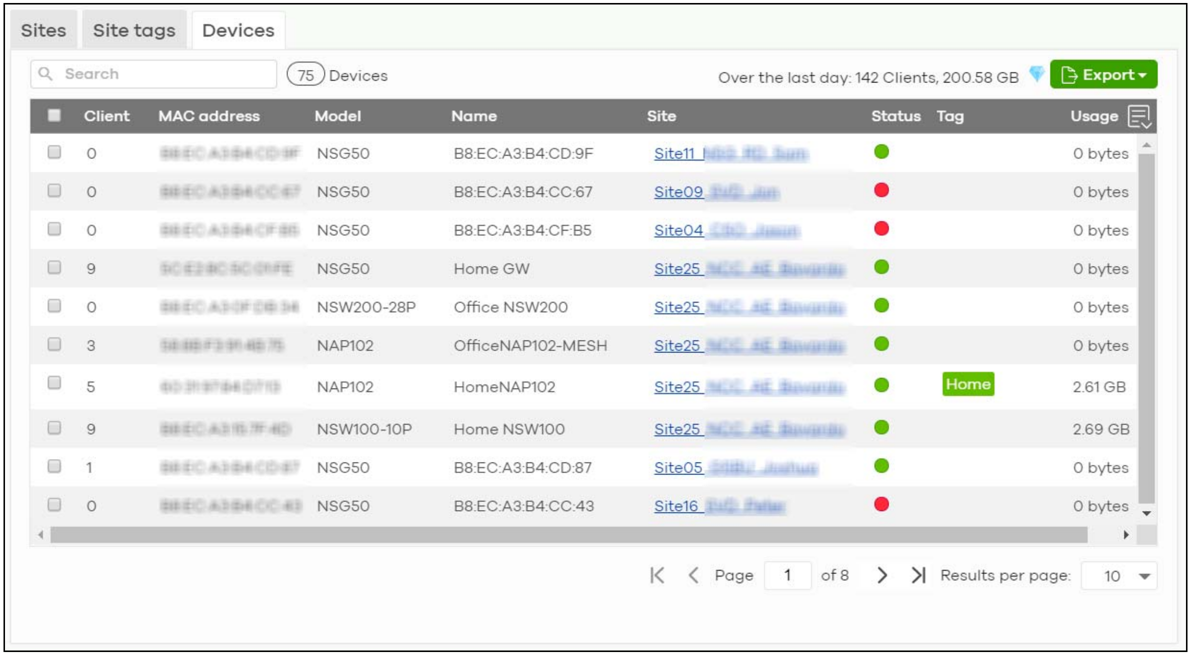
Table 195 Organization-wide > Organization-wide manage > Organization portal: Site tags

LABEL	DESCRIPTION
Search	Enter a key word as the filter criteria to filter the list of tags.
Site tags	This shows the number of site tags created and added to the sites in this organization.
Over the last day	This shows the number of clients associated with the sites in this organization and the total amount of data transmitted or received by the clients in the past day.
Export	Click this button to save the tag list as a CSV or XML file to your computer.
Status	This shows the status of Nebula Devices in sites with the specified tag. • Green: All Nebula Devices are online and have no alerts. • Amber: Some Nebula Devices have alerts. • Red: Some Nebula Devices are offline. • Gray: All Nebula Devices have been offline for 7 days or more. • White: No Nebula Devices.
Tag	This shows the name of the specified tag.
Site	This shows the total number of sites with the specified tag.
Offline device	This shows the number of offline Nebula Devices in all sites with the specified tag.
Clients	This shows the number of clients in sites with the specified tag. Note: This shows '–' for Nebula Accessories.
Usage	This shows the total amount of data consumed in all sites with the specified tag. Note: This shows '–' for Nebula Accessories.
Device	This shows the total number of Nebula Devices deployed to all sites with the specified tag.
Offline site	This shows the number of offline sites with the specified tag.
% Offline	This shows what percentage of all sites with the specified tag are currently offline.
▤	Click this icon to display a greater or lesser number of configuration fields.

12.4.1.3 Devices

Click the **Devices** tab in the **Organization portal** screen to view the detailed information about Nebula Devices which are connected to the sites in the selected organization.

Figure 260 Organization-wide > Organization-wide manage > Organization portal: Devices



75 Devices

Over the last day: 142 Clients, 200.58 GB

□	Client	MAC address	Model	Name	Site	Status	Tag	Usage
□	0	[redacted]	NSG50	B8:EC:A3:B4:CD:9F	Site11 [redacted]	🟢		0 bytes
□	0	[redacted]	NSG50	B8:EC:A3:B4:CC:67	Site09 [redacted]	🔴		0 bytes
□	0	[redacted]	NSG50	B8:EC:A3:B4:CF:B5	Site04 [redacted]	🔴		0 bytes
□	9	[redacted]	NSG50	Home GW	Site25 [redacted]	🟢		0 bytes
□	0	[redacted]	NSW200-28P	Office NSW200	Site25 [redacted]	🟢		0 bytes
□	3	[redacted]	NAP102	OfficeNAP102-MESH	Site25 [redacted]	🟢		0 bytes
□	5	[redacted]	NAP102	HomeNAP102	Site25 [redacted]	🟢	Home	2.61 GB
□	9	[redacted]	NSW100-10P	Home NSW100	Site25 [redacted]	🟢		2.69 GB
□	1	[redacted]	NSG50	B8:EC:A3:B4:CD:87	Site05 [redacted]	🟢		0 bytes
□	0	[redacted]	NSG50	B8:EC:A3:B4:CC:43	Site16 [redacted]	🔴		0 bytes

Page 1 of 8 Results per page: 10

The following table describes the labels in this screen.

Table 196 Organization-wide > Organization-wide manage > Organization portal: Devices

LABEL	DESCRIPTION
Search	Enter a key word as the filter criteria to filter the list of connected Nebula Devices.
Devices	This shows the number of Nebula Devices assigned to the sites in this organization.
Over the last day	This shows the number of clients associated with the sites in this organization and the total amount of data transmitted or received by the clients in the past day.
Export	Click this button to save the Nebula Device list as a CSV or XML file to your computer.
Status	This shows the status of the Nebula Device. • Green: The Nebula Device is online. • Amber: The Nebula Device recently had alerts. • Red: The Nebula Device was recently offline. • Gray: The Nebula Device has been offline for more than 6 days.
Model	This shows the model number of the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.
Site	This shows the name of the site to which the Nebula Device is connected.
MAC address	This shows the MAC address of the Nebula Device.
Tag	This shows the user-specified tag for the Nebula Device.
Clients	This shows the number of the clients which are currently connected to the Nebula Device. Note: This shows '–' for Accessories.

Table 196   Organization-wide > Organization-wide manage > Organization portal: Devices (continued)

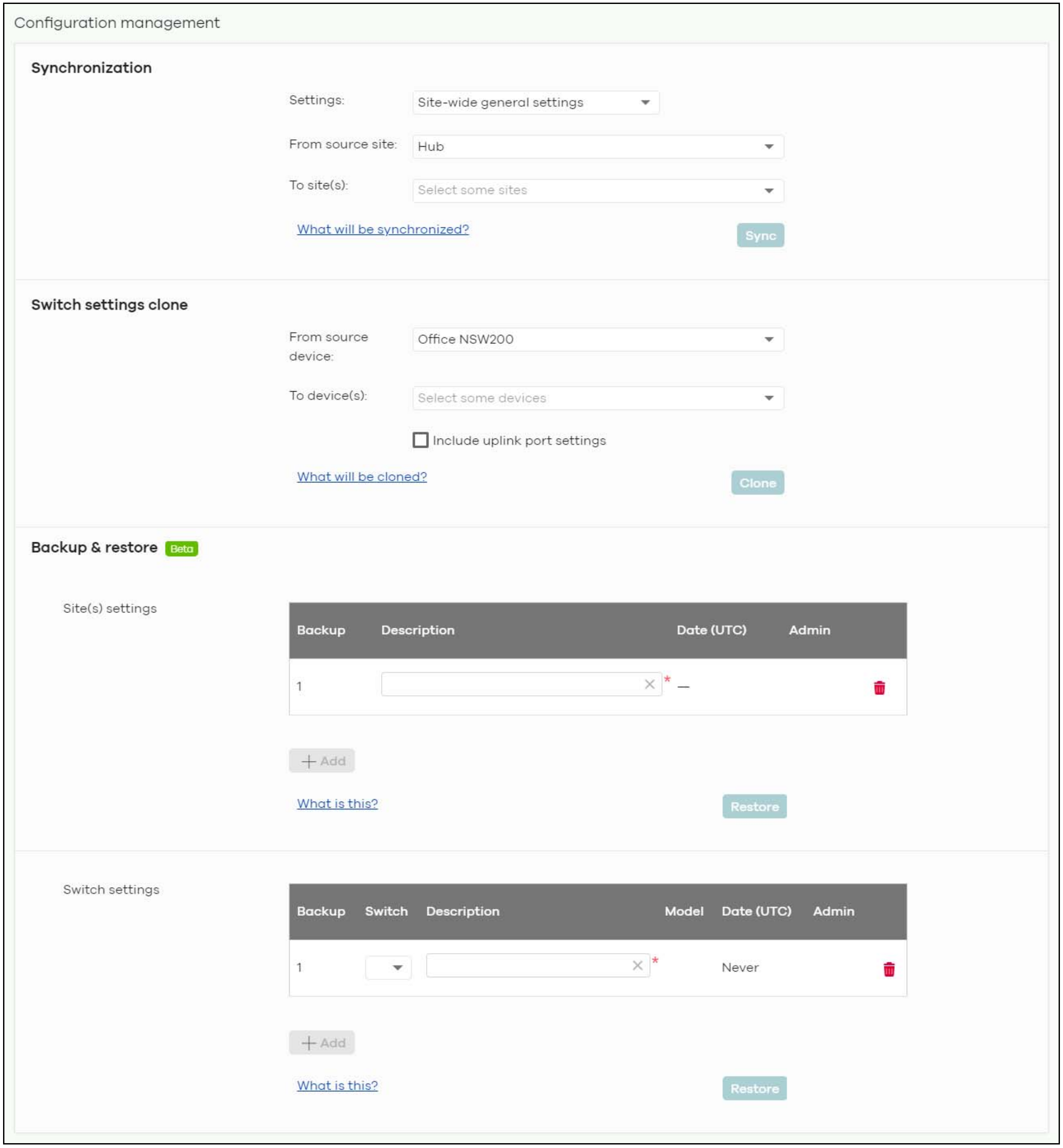
LABEL	DESCRIPTION
Usage	This shows the amount of data consumed by the Nebula Device. Note: This shows '–' for Accessories.
Serial number	This shows the serial number of the Nebula Device.
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
Connectivity	This shows the Nebula Device connection status. The red time slot indicates the connection to the NCC is down, and the green time slot indicates the connection is up. Move the cursor over a time slot to see the actual date and time when a Nebula Device is connected or disconnected.
Public IP	This shows the global (WAN) IP address of the Nebula Device.
🗒	Click this icon to display a greater or lesser number of configuration fields.

12.4.2 Configuration Management

Configuration synchronization allows you to easily copy configurations from one site or Nebula Device to another. Use this screen to synchronize the configuration between sites or switch ports. You can also back up the current configurations for sites or switches to the NCC and restore the configuration at a later date.

Click **Organization-wide** > **Organization-wide manage** > **Configuration management** to access this screen.

Figure 261 Organization-wide > Organization-wide manage > Configuration management



Configuration management

Synchronization

Settings: Site-wide general settings

From source site: Hub

To site(s): Select some sites

Switch settings clone

From source device: Office NSW200

To device(s): Select some devices

□ Include uplink port settings

Backup & restore Beta

Site(s) settings

Backup	Description	Date (UTC)	Admin
1	*	—	

Switch settings

Backup	Switch	Description	Model	Date (UTC)	Admin
1		*		Never	

The following table describes the labels in this screen.

Table 197 Organization-wide > Organization-wide manage > Configuration management

LABEL	DESCRIPTION
Synchronization	
Settings	Specify whether general site configuration or just SSID settings of a site will be propagated to other sites. Click **What will be synchronized?** to view detailed information.
From source site	Select the site from which you want to copy its site configuration to other sites.
To Site(s)	Select one or more sites to which you want to import the copied site configuration. You can also select the site tags created using the **Organization-wide** > **Organization-wide manage** > **Organization portal: Sites** screen.

Table 197 Organization-wide > Organization-wide manage > Configuration management (continued)

LABEL	DESCRIPTION
Sync	Click this button to start synchronizing configuration settings between the selected sites.
Switch settings clone	
From source device	Select the Nebula Switch from which you want to copy its Switch port settings to other Nebula Devices.
To device(s)	Select one or more Nebula Switches to which you want to import the copied Switch port settings. Note: Only Nebula Switches of the same model can synchronize. Both Switches should be registered to a site in the organization.
Clone	Click this button to start synchronizing Switch port settings between the selected Nebula Devices.
Backup & Restore Note: To back up or restore a previously saved configuration, your administrator account should have full access to the organization. Note: The Security Firewall(s) in Cloud Monitoring mode cannot use the back up or restore function.	
Site(s) settings	You can create up to three site configuration backups for the organization. The NCC automatically creates and saves one backup when you perform configuration restoration. The automatic backup cannot be deleted.
Backup	This shows the index number of the site configuration backup.
Description	This shows the descriptive name of the backup. Note: When you click **Add** to create a new backup, you need to enter a name for the backup in order to save it to the NCC.
Date (UTC)	This shows the date and time the backup was saved on the NCC server.
Admin	This shows the name of the administrator account who performed the backup.
Remove	Click the remove icon to delete the backup.
Add	Click this button to create a new configuration backup of all the sites in the organization.
Restore from backup	Select the backup you want to restore.
Restore to site(s)	Select one or more sites to which you want to restore the specified configuration backup.
Restore	Click this button to overwrite the settings of the sites with the selected configuration backup.
Switch settings	At the time of writing, only one backup is allowed per Nebula Device.
Backup	This shows the index number of the Switch configuration backup.
Switch	This shows the name of the Switch.
Description	This shows the descriptive name of the backup. Note: When you click **Add** to create a new backup, you need to enter a name for the backup in order to save it to the NCC.
Model	This shows the model number of the Switch.
Date (UTC)	This shows the date and time the backup was saved on the NCC server.
Admin	This shows the name of the administrator account who performed the backup.
Remove	Click the remove icon to delete the backup.
Add	Click this button to create a new configuration backup of a specific Switch. This button is selectable only when you have at least one Switch in the organization.

Table 197 Organization-wide > Organization-wide manage > Configuration management (continued)

LABEL	DESCRIPTION
Restore from backup	Select the backup you want to restore.
Restore to device(s)	Select one or more Nebula Switches to which you want to restore the specified configuration backup. Note: You can restore the backup to the same Switch or Switches of the same model and registered to a site in the organization.
Restore	Click this button to overwrite the settings of the Switches with the selected configuration backup.

12.4.3 Configuration Templates

A configuration template is a virtual site. The settings you configured in a template will apply to the real sites which are bound to the template. If you do not want to apply any new settings from the template to a site, just unbind that site. If you want to configure some specific settings directly in a site after the site is bound to a template, turn on the local override function (see Section 12.4.3.3 on page 690).

Use this screen to create and manage configuration templates. You can then bind or unbind a site from the template (see Section 12.4.3.1 on page 689).

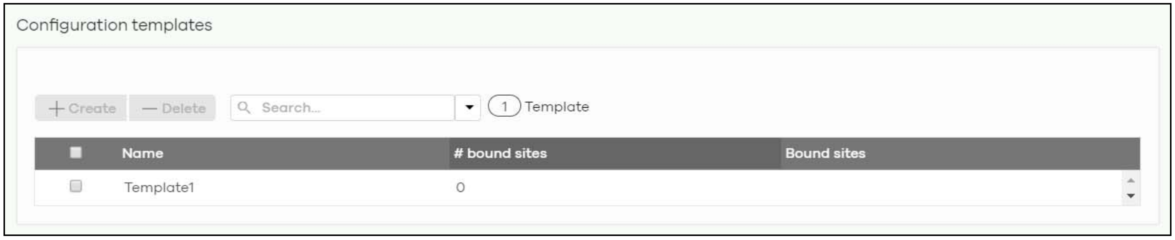
Note: A site can only be bound to one template. The same template can be used by multiple sites. The sites and the template should belong to the same organization for binding.

Note: If the NCC service is downgraded from Nebula Professional Pack to Nebula Base, all the sites will be unbound from the templates but retain the settings already applied from the template.

Note: The settings from the Configuration templates will not apply to Security Firewall(s) in Cloud Monitoring mode.

Click **Organization-wide** > **Organization-wide manage** > **Configuration templates** to access this screen.

Figure 262 Organization-wide > Organization-wide manage > Configuration templates

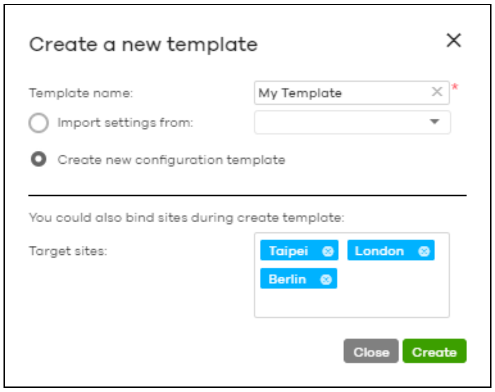
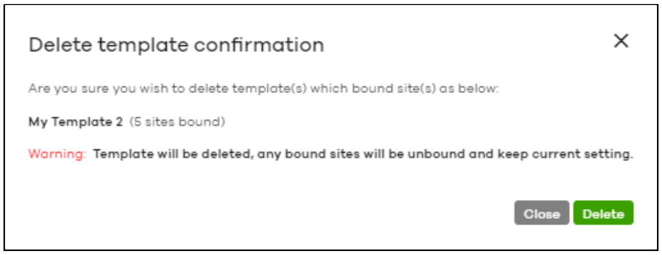


Configuration templates

□	Name	# bound sites	Bound sites
□	Template1	0	

The following table describes the labels in this screen.

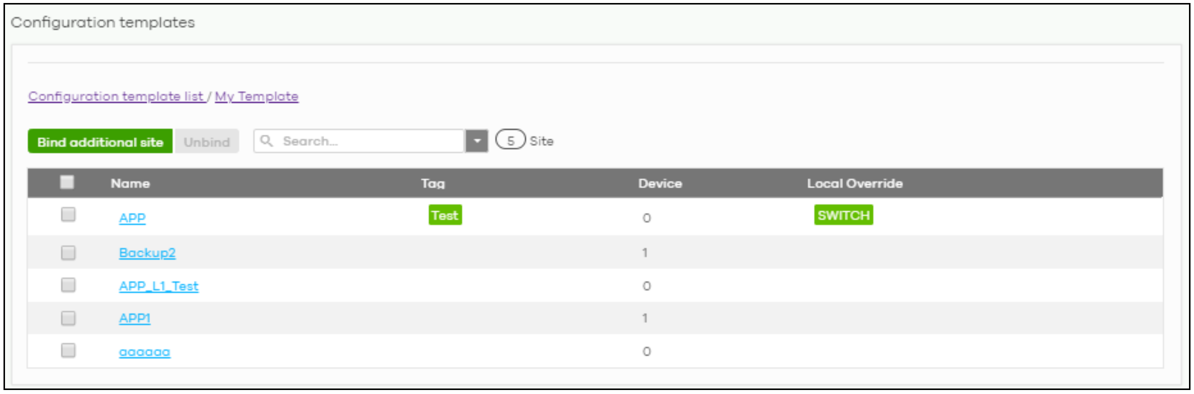
Table 198 Organization-wide > Organization-wide manage > Configuration templates

LABEL	DESCRIPTION
Create	Click this button to create a new configuration template. You can copy settings from an existing site or configuration template, or have a new template with default settings. It is optional to bind one or more sites to the template when you are creating a template.  Create a new template Template name: My Template * ○ Import settings from: ● Create new configuration template You could also bind sites during create template: Target sites: Taipei London Berlin
Delete	Click this button to remove the selected templates. A window pops up asking you to confirm that you want to delete the templates. If you remove a template that is being used by a site, the site will be unbound from the template automatically and retain the settings previously applied from the template.  Delete template confirmation Are you sure you wish to delete template(s) which bound site(s) as below: My Template 2 (5 sites bound) Warning: Template will be deleted, any bound sites will be unbound and keep current setting.
Search	Enter a key word as the filter criteria to filter the list of templates.
Templates	This shows how many templates match the filter criteria and how many templates are created in total.
Name	This shows the name of the template.
# Bound sites	This shows the number of the sites bound to the template.
Bound sites	This shows the name of the sites bound to the template.

12.4.3.1 Site Binding

Use this screen to bind or unbind a site from a template. Click an existing template from the list in the **Organization-wide** > **Organization-wide manage** > **Configuration templates** screen to access this screen. To go back to the previous screen, click the **Configuration templates list** link.

Figure 263 Organization-wide > Organization-wide manage > Configuration templates: Template



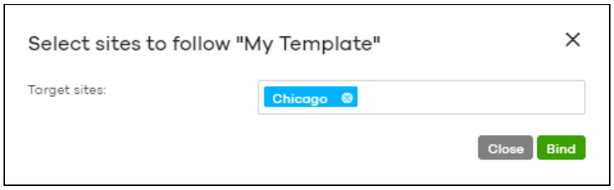
Configuration templates

Configuration template list / My Template

☐	Name	Tag	Device	Local Override
☐	APP	Test	0	SWITCH
☐	Backup2		1	
☐	APP_L1_Test		0	
☐	APP1		1	
☐	aaaaaa		0	

The following table describes the labels in this screen.

Table 199 Organization-wide > Organization-wide manage > Configuration templates: Template

LABEL	DESCRIPTION
Bind additional site	Click this button to bind more sites to the template. A window displays. Select the name of the sites in the **Target sites** field and click **Bind**.  Select sites to follow "My Template" Target sites: Chicago Close Bind
Unbind	Click this button to remove the selected sites from the template. The site which is unbound from the template still retains the settings applied from the template.
Search	Enter a key word as the filter criteria to filter the list of sites.
Sites	This shows how many sites match the filter criteria and how many sites are bound to the template in total.
Name	This shows the name of the site bound to the template.
Tag	This shows the tags added to the site.
Device	This shows the number of Nebula Devices which are assigned to the site.
Local override	This shows which settings in the template do not apply to the site.

12.4.3.2 Template settings

An administrator that has full access to the organization can modify the template configurations. To access a template's configuration screen, select the template name from the **Site** field in the NCC title bar. It also shows the number of sites that are bound to the template on each configuration screen.

Note: At the time of writing, you can use a template to configure site-wide, Switches, and access points settings.

12.4.3.3 Local Override

When a site is bound to a template, you can see the name of the template on the site's configuration screens (which are also available in a template and can be configured).

There is also an option to make the changes you made locally to a site persist. If you select the override checkbox of the site's configuration screen, all the configuration screens under the same menu tab

(**Site-Wide** or **Switches**) are configurable. Settings in these screens will not be affected and modified by the template. If the override checkbox is not selected, any changes of the same configuration screen in the template apply to the site.

12.4.3.4 Switch Port Profile and Configuration

Just as a configuration template is a virtual site, so is a profile to a Switch. The settings you configured in a profile will apply to the Switches which are bound to the profile. If you do not want to apply any new settings from the profile to a Switch, just unbind that Switch. If you want to configure some specific settings directly in a Switch (For example, a port's **Broadcast (pps)** value. See Section 6.3.1.1 on page 365 for details.) after the Switch is bound to a profile, turn on the local override function (see Section 12.4.3.3 on page 690).

12.4.4 VPN Orchestrator

VPN Orchestrator enables you to automatically create Virtual Private Network (VPN) connections between sites within an organization. This allows the Security Gateway of each site and the Nebula Devices behind it to communicate securely.

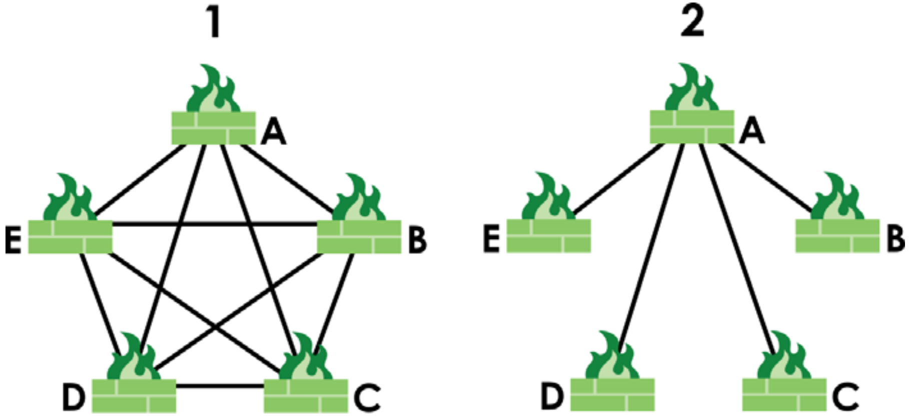
Note: You can manually create VPN connections between sites at **Site-wide** > **Configure** > **Security Gateway** > **Site-to-Site VPN** or **Site-wide** > **Configure** > **Firewall** > **Site-to-Site VPN**.

12.4.4.1 Topology Overview

There are two topologies you can use when creating a site-to-site VPN.

- **Fully Meshed**: In a fully-meshed VPN topology (**1** in the figure below), there is a VPN connection between every two sites in the organization. Sites can communicate directly with each other, but having permanent tunnels between every site takes up more resources.
- **Hub-and-spoke**: In a hub-and-spoke topology (**2** in the figure below), every site is either a hub or a spoke. There is a VPN connection between each spoke site (**B**, **C**, **D**, and **E**) and the hub site (**A**). Traffic from each spoke site must first go through the hub site. If the hub site fails, the site-to-site VPN network fails. To avoid this, you can assign more than one hub site.

Figure 264 VPN Topologies (Fully Meshed and Hub-and-Spoke)



12.4.4.2 VPN Areas

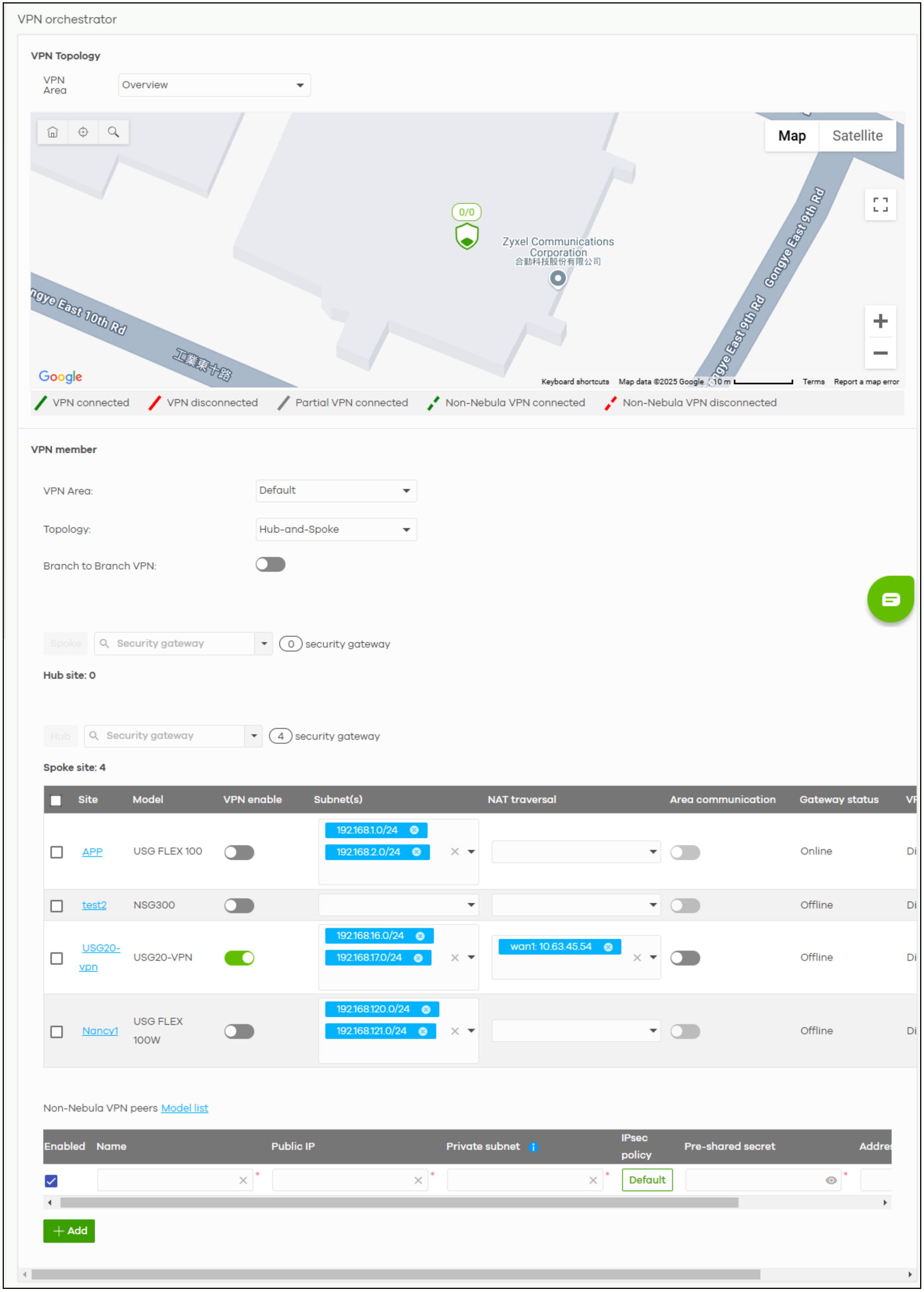
An organization can contain multiple VPN areas. Each VPN area is an independent VPN with its own sites, settings, and topology. Every organization has a default VPN area called Default, which cannot be deleted. Sites in different VPN areas within the same organization can communicate if you enable the **Area communication** setting.

12.4.4.3 VPN Orchestrator Screen

Use this screen to manage and create site-to-site VPNs within the current organization. Click **Organization-wide** > **Organization-wide manage** > **VPN orchestrator** to access this screen.

Note: The Security Firewall(s) in Cloud Monitoring mode will not show on the list and map.

Figure 265 Organization-wide > Organization-wide manage > VPN orchestrator



VPN orchestrator

VPN Topology

VPN Area: Overview

/ VPN connected / VPN disconnected / Partial VPN connected / Non-Nebula VPN connected / Non-Nebula VPN disconnected

VPN member

VPN Area: Default

Topology: Hub-and-Spoke

Branch to Branch VPN: ○

Spoke | Security gateway | (0) security gateway

Hub site: 0

Hub | Security gateway | (4) security gateway

Spoke site: 4

□	Site	Model	VPN enable	Subnet(s)	NAT traversal	Area communication	Gateway status	VI
□	APP	USG FLEX 100	○	192.168.1.0/24 192.168.2.0/24		○	Online	Di
□	test2	NSG300	○			○	Offline	Di
□	USG20-vpn	USG20-VPN	●	192.168.16.0/24 192.168.17.0/24	wan1: 10.63.45.54	○	Offline	Di
□	Nancy1	USG FLEX 100W	○	192.168.120.0/24 192.168.121.0/24		○	Offline	Di

Non-Nebula VPN peers Model list

Enabled	Name	Public IP	Private subnet	IPsec policy	Pre-shared secret	Addre
☑	*	*	*	Default	*	

+ Add

The following table describes the labels in this screen.

Table 200 Organization-wide > Organization-wide manage > VPN orchestrator

LABEL	DESCRIPTION
VPN Topology	
VPN Area	Select the name of a VPN area to view on the map. Select **Overview** to view all VPN areas in this organization on the map.
VPN Member	
VPN Area	Select the name of a VPN to configure. Select **+ Create VPN area** to create a new VPN within the organization.
🗑	Click the remove icon to delete the VPN area.
Topology	Click this to select a topology for the VPN area. For details on topologies, see Section 12.4.4.1 on page 691. Select **Disable** to disable VPN connections for all sites in the VPN area.
The following settings are shown when **Topology** is set to **Hub-and-Spoke**.	
Branch to Branch VPN	Enable this to allow spoke sites to communicate with each other in the VPN area. When disabled, spoke sites can only communicate with hub sites.
Spoke	Select one or more sites and then click this to assign the sites as spokes. The sites are added to the spoke list.
Hub	Select one or more sites and then click this to assign the sites as hubs. The sites are added to the hubs list.
Security Gateway	Enter the name of a site or Nebula Device to filter the list of sites.
Hub site	This shows the number of hub site. Note: Only one hub site is supported.
Spoke site: N	This shows the number of spoke sites (N) in the spoke list.
#	This shows the priority of the hub site. If the VPN area contains multiple hub sites, then the spoke sites always send traffic through the available hub with the highest priority. You can change the priority of a site by clicking the move icon (✥), and then dragging the site up or down in the list.
Site	This shows the name of the site in the VPN area. Click the name to go to the site's VPN configuration page (**Site-wide** > **Configure** > **Firewall** > **Site-to-Site VPN**).
Model	This shows the model of the site's Security Appliance device.
VPN enable	Click this to enable (join) or disable (leave) site-to-site VPN on the site's Security Appliance. If you disable this setting, the site will leave the VPN area.
Subnets	This shows the IP subnets of all LAN interfaces behind the site's Security Appliance.
NAT traversal	If the Security Appliance is behind a NAT router, enter the public IP address or the domain name that is configured and mapped to the Security Appliance on the NAT router.
Area communication	Enable this to allow the site to communicate with sites in different VPN areas within the organization. If **Topology** is set to **Site-to-Site**, then you must assign at least one site in each VPN area as the **Area Leader**. The area leaders create VPN tunnels between VPN areas.
Gateway status	This shows whether the site's Security Appliance is currently online.
VPN status	This shows whether the VPN is currently connected.
WAN status	This shows the IP address of the WAN interface and the public IP address of the site's Security Appliance.

Table 200 Organization-wide > Organization-wide manage > VPN orchestrator (continued)

LABEL	DESCRIPTION
Non-Nebula VPN peers	Configure this section to add a non-Nebula gateway, such as an on-premise ZyWALL series device or non-Zyxel gateway, to the VPN area.
+ Add	Click this button to add a non-Nebula gateway to the VPN area.
Enabled	Select the checkbox to enable VPN connections to the non-Nebula gateway.
Name	Enter the name of the non-Nebula gateway.
Public IP	Enter the public IP address of the non-Nebula gateway. The public IP address supports both FQDN (Fully Qualified Domain Name) and IP formats.
Private Subnet	Enter the IP subnet that will be used for VPN connections. The IP range must be reachable from other Nebula Devices in the VPN area.
IPSec policy	Click to select a pre-defined policy or have a custom one. See Section 9.3.6.1 on page 613 for detailed information.
Pre-shared secret	Enter a pre-shared key (password). The Nebula Security Appliance and peer gateway use the key to identify each other when they negotiate the IKE SA.
Address (physical location)	Enter the address (physical location) of the remote device. You can find this on the **VPN Topology** section on this screen.
🗑	Click the remove icon to delete the entry.

12.4.5 Security Profile Sync

Security profile sync allows you to share the same Security Firewall device security service settings with multiple sites in an organization. This replaces the Unified Threat Management (UTM) settings configured for each site at **Site-wide** > **Configure** > **Firewall** > **Security service**.

12.4.5.1 Configuring Security Profile Sync

Follow the steps below to enable security profile sync in an organization.

1 Go to **Organization-wide** > **Organization-wide manage** > **Security profile sync**. Select **Enabled**, and then under **Sync sites** add the sites that you want to share security settings.

Note: You can only add sites that have a Security Firewall device.

2 Configure security service settings for **Content Filter**, **Application Patrol**, **DNS/URL Threat Filter**, **IP Reputation**, **Anti-Malware**, **Sandboxing**, and **Intrusion Prevention System (IPS)**. Then click **Save**. All security settings are synced to the selected sites.

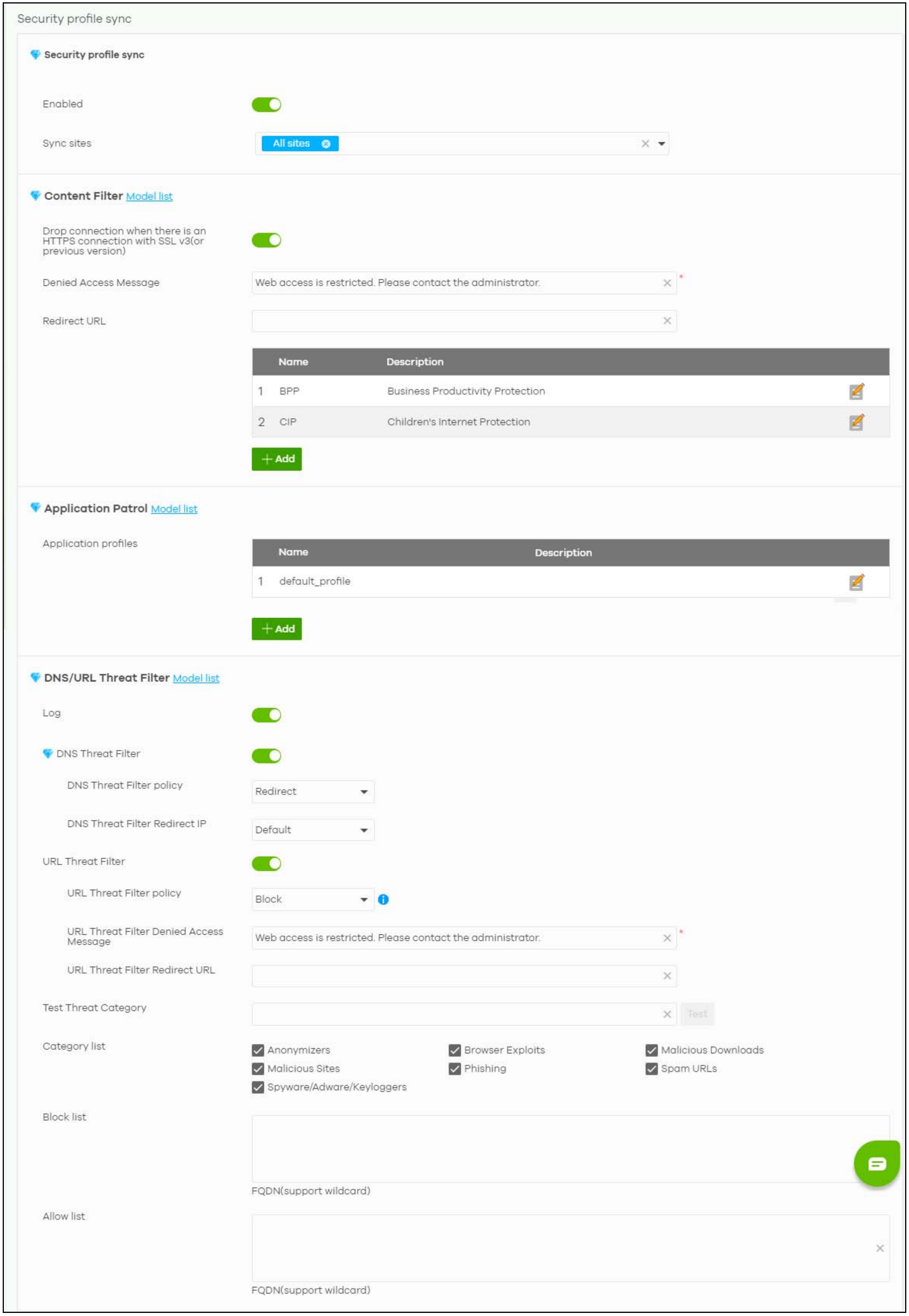
3 If you change the settings in the **Security profile sync** screen, the changes will be copied to all selected sites.

4 If you want to modify security settings for an individual site, go to **Site-wide** > **Configure** > **Firewall** > **Security service** and select **Override security profile sync**.

12.4.5.2 Security Profile Sync Screen

Use this screen to enable and configure security profile sync. Click **Organization-wide** > **Organization-wide manage** > **Security profile sync** to access this screen.

Figure 266 Organization-wide > Organization-wide manage > Security Profile Sync



Security profile sync

Security profile sync

Enabled

Sync sites: All sites

Content Filter Model list

Drop connection when there is an HTTPS connection with SSL v3(or previous version)

Denied Access Message: Web access is restricted. Please contact the administrator.

Redirect URL

	Name	Description
1	BPP	Business Productivity Protection
2	CIP	Children's Internet Protection

+ Add

Application Patrol Model list

Application profiles

	Name	Description
1	default_profile	

+ Add

DNS/URL Threat Filter Model list

Log

DNS Threat Filter

DNS Threat Filter policy: Redirect

DNS Threat Filter Redirect IP: Default

URL Threat Filter

URL Threat Filter policy: Block

URL Threat Filter Denied Access Message: Web access is restricted. Please contact the administrator.

URL Threat Filter Redirect URL

Test Threat Category Test

Category list

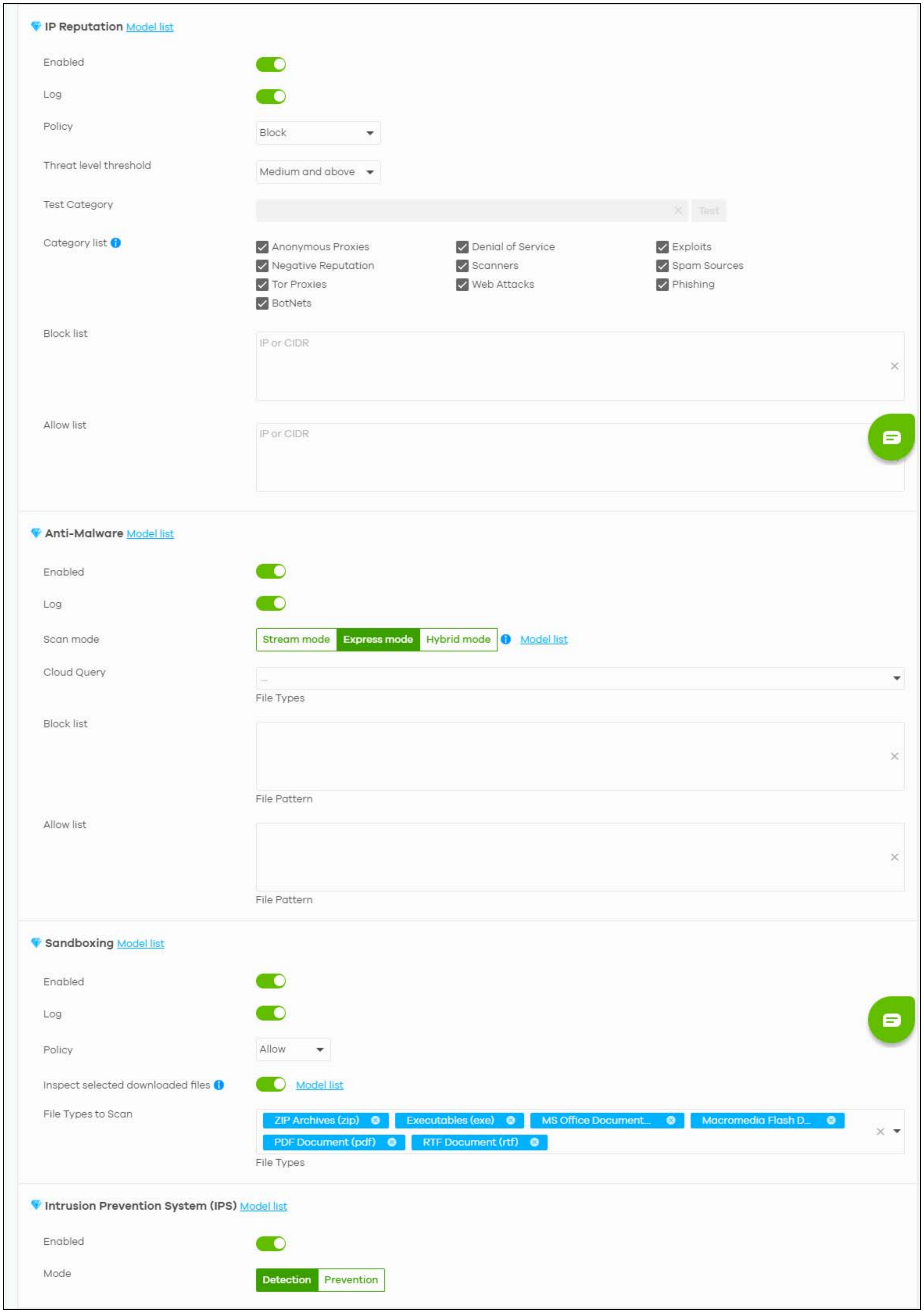
- ☑ Anonymizers
- ☑ Malicious Sites
- ☑ Spyware/Adware/Keyloggers
- ☑ Browser Exploits
- ☑ Phishing
- ☑ Malicious Downloads
- ☑ Spam URLs

Block list

FQDN(support wildcard)

Allow list

FQDN(support wildcard)



IP Reputation Model list

Enabled: on

Log: on

Policy: Block

Threat level threshold: Medium and above

Test Category: Test

Category list

☑ Anonymous Proxies ☑ Denial of Service ☑ Exploits
☑ Negative Reputation ☑ Scanners ☑ Spam Sources
☑ Tor Proxies ☑ Web Attacks ☑ Phishing
☑ BotNets

Block list: IP or CIDR

Allow list: IP or CIDR

Anti-Malware Model list

Enabled: on

Log: on

Scan mode: Stream mode | Express mode | Hybrid mode Model list

Cloud Query: --
File Types

Block list:
File Pattern

Allow list:
File Pattern

Sandboxing Model list

Enabled: on

Log: on

Policy: Allow

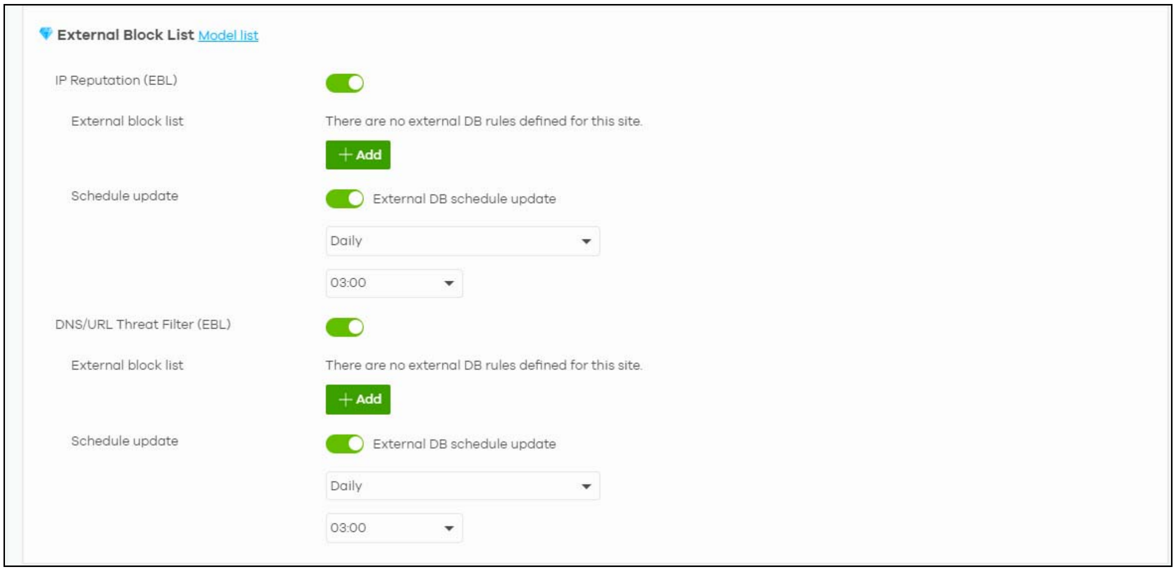
Inspect selected downloaded files: on Model list

File Types to Scan: ZIP Archives (zip), Executables (exe), MS Office Document..., Macromedia Flash D..., PDF Document (pdf), RTF Document (rtf)
File Types

Intrusion Prevention System (IPS) Model list

Enabled: on

Mode: Detection | Prevention



External Block List Model list

IP Reputation (EBL)

External block list: There are no external DB rules defined for this site.

Schedule update: External DB schedule update — Daily — 03:00

DNS/URL Threat Filter (EBL)

External block list: There are no external DB rules defined for this site.

Schedule update: External DB schedule update — Daily — 03:00

The following table describes the labels in this screen.

Table 201 Organization-wide > Organization-wide manage > Security profile sync

LABEL	DESCRIPTION
Security profile sync	
Enabled	Click this to enable or disable security profile sync for the organization.
Sync sites	Select one or more sites that you want to apply the following security settings configured on this screen: • Content Filter • Application Patrol • DNS/URL Threat Filter • IP Reputation • Anti-Malware • Sandboxing • Intrusion Prevention System (IPS) • External block list (for IP Reputation and DNS/URL Threat Filter) Alternatively, select **All sites** to apply the security settings to all sites in the organization. Note: You can only add sites that have a Security Firewall device.
Content Filter	
Drop connection when there is an HTTPS connection with SSL v3 (or previous version)	Select **On** to have the Nebula Security Firewall block HTTPS web pages using SSL V3 or a previous version.
Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0–9a–zA–Z;/?:@&=+$\.–_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the Nebula Security Firewall just opens the web page you specified without showing a denied access message.

Table 201 Organization-wide > Organization-wide manage > Security profile sync (continued)

LABEL	DESCRIPTION
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Enabled	Select the checkbox to enable the content filter profile.
Description	Enter a description for this profile.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this to create a content filter profile. See Section on page 551 for more information.
Application Patrol Application profiles	
Name	Enter a name for this profile for identification purposes.
Description	Enter a description for this profile.
✎	Click this icon to change the profile settings.
🗑	Click this icon to remove the profile.
Add	Click this icon to create an application patrol profile. See Section on page 553 for more information.
DNS/URL Threat Filter	
Log	Select whether to have the Nebula Device generate a log (log), log and alert (log alert) or not (no) when the policy is matched to the criteria listed above.
DNS Threat Filter	Select **On** to turn on the rule. Otherwise, select **Off** to turn off the rule.
DNS Threat Filter policy	Select **Pass** to have the Nebula Device allow the DNS query packet and not reply with a DNS reply packet containing a default or custom-defined IP address. Select **Redirect** to have the Nebula Device reply with a DNS reply packet containing a default or custom-defined IP address.
DNS Threat Filter Redirect IP	Enter the IP address to have the Nebula Device reply with a DNS reply packet containing a default or custom-defined IP address when a DNS query packet contains an FQDN with a bad reputation. The default IP is the dnsft.cloud.zyxel.com IP address. If you select a custom-defined IP, then enter a valid IPv4 address in the text box.
URL Threat Filter	Select **On** to turn on the rule. Otherwise, select **Off** to turn off the rule.
URL Threat Filter Policy	Select **Pass** to allow users to access web pages that the external web filtering service has not categorized. Select **Block** to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filter blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. Select **Warn** to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.
URL Threat Filter Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the Nebula Device just opens the web page you specified without showing a denied access message.

Table 201 Organization-wide > Organization-wide manage > Security profile sync (continued)

LABEL	DESCRIPTION
URL Threat Filter Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Test Threat Category	Enter a URL using http://domain or https://domain and click the **Test** button to check if the domain belongs to a URL threat category.
Category List	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
Block list	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
Allow list	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0–9 a–z). The casing does not matter.
IP Reputation	
Enabled	Select this option to turn on IP blocking on the Nebula Device.
Log	Select this option to create a log on the Nebula Device when the packet comes from an IPv4 address with bad reputation.
Policy	Select **Pass** to have the Nebula Device allow the packet to go through. Select **Block** to have the Nebula Device deny the packets and send a TCP RST to both the sender and receiver when a packet comes from an IPv4 address with bad reputation.
Threat level threshold	Select the threshold threat level to which the Nebula Device will take action (**High**, **Medium and above**, **Low and above**). The threat level is determined by the IP reputation engine. It grades IPv4 addresses. • **High**: an IPv4 address that scores 0 to 20 points. • **Medium and above**: an IPv4 address that scores 0 to 60 points. • **Low and above**: an IPv4 address that scores 0 to 80 points. For example, a score of "10" will cause the Nebula Device to take action whether you set the **Threat level threshold** at **High**, **Medium and above**, or **Low and above**. But a score of "61" will not cause the Nebula Device to take any action if you set the **Threat level threshold** at **Medium and above**.
Test Category	Enter an IPv4 address of a website, and click the **Test** button to check if the website associates with suspicious activities that could pose a security threat to users or their computers.
Category list	Select the categories of packets that come from the Internet and are known to pose a security threat to users or their computers.

Table 201 Organization-wide > Organization-wide manage > Security profile sync (continued)

LABEL	DESCRIPTION
Block list	Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list. Add the IPv4 addresses that the Nebula Device will block the incoming packets.
Allow list	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. Add the IPv4 addresses that the Nebula Device will allow the incoming packets.
Anti-Malware	
Enabled	Select **On** to turn on the rule. Otherwise, select **Off** to turn off the rule.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed above.
Scan mode	
Express mode	In this mode you can define which types of files are scanned using the File Type For Scan fields. The Nebula Device then scans files by sending each file's hash value to a cloud database using cloud query. This is the fastest scan mode.
Stream mode	In this mode the Nebula Device scans all files for viruses using its anti-malware signatures to detect known virus pattens. This is the deepest scan mode.
Hybrid mode	In this mode you can define which types of files are scanned using the File Type For Scan fields. The Nebula Device then scans files by sending each file's hash value to a cloud database using cloud query. It also scans files using anti-malware signatures, and Threat Intelligence Machine Learning. This mode combines **Express Mode** and **Stream Mode** to offer a balance of speed and security.
Cloud Query	Select the Cloud Query supported file types for the Nebula Device to scan for viruses.
Block list	This field displays the file or encryption pattern of the entry. Enter a file pattern that would cause the Nebula Device to log and modify this file. •Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. •A question mark (?) lets a single character in the file name vary. For example, use "a?.zip" (without the quotation marks) to specify aa.zip, ab.zip and so on. •Wildcards (*) let multiple files match the pattern. For example, use "*a.zip" (without the quotation marks) to specify any file that ends with "a.zip". A file named "testa.zip would match. There could be any number (of any type) of characters in front of the "a.zip" at the end and the file name would still match. A file named "test.zipa" for example would not match. •A * in the middle of a pattern has the Nebula Device check the beginning and end of the file name and ignore the middle. For example, with "abc*.zip", any file starting with "abc" and ending in ".zip" matches, no matter how many characters are in between. •The whole file name has to match if you do not use a question mark or asterisk. •If you do not use a wildcard, the Nebula Device checks up to the first 80 characters of a file name.

Table 201 Organization-wide > Organization-wide manage > Security profile sync (continued)

LABEL	DESCRIPTION
Allow list	Enter the file or encryption pattern for this entry. Specify a pattern to identify the names of files that the Nebula Device should not scan for viruses. •Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. •A question mark (?) lets a single character in the file name vary. For example, use "a?.zip" (without the quotation marks) to specify aa.zip, ab.zip and so on. •Wildcards (*) let multiple files match the pattern. For example, use "*a.zip" (without the quotation marks) to specify any file that ends with "a.zip". A file named "testa.zip would match. There could be any number (of any type) of characters in front of the "a.zip" at the end and the file name would still match. A file named "test.zipa" for example would not match. •A * in the middle of a pattern has the Nebula Device check the beginning and end of the file name and ignore the middle. For example, with "abc*.zip", any file starting with "abc" and ending in ".zip" matches, no matter how many characters are in between. •The whole file name has to match if you do not use a question mark or asterisk. •If you do not use a wildcard, the Nebula Device checks up to the first 80 characters of a file name.
Sandboxing	Sandboxing provides a safe environment to separate running programs from your network and host devices. Unknown or untrusted programs/codes are uploaded to the Defend Center and executed within an isolated virtual machine (VM) to monitor and analyze the zero-day malware and advanced persistent threats (APTs) that may evade the Nebula Device's detection, such as anti-malware. Results of cloud sandboxing are sent from the server to the Nebula Device.
Enabled	Select this option to turn on sandboxing on the Nebula Device
Log	Enable this option to allow the Security Firewall to create a log when a suspicious file is detected.
Policy	Specify whether the Nebula Device deletes (**Destroy**) or forwards (**Allow**) malicious files. Malicious files are files given a high score for malware characteristics by the Defend Center.
Inspect selected downloaded files	Select this option to have the Nebula Device hold the downloaded file for up to 2 seconds if the downloaded file has never been inspected before. The Nebula Device will wait for the Defend Center's result and forward the file in 2 seconds. Sandbox detection may take longer than 2 seconds, so infected files could still possibly be forwarded to the user. Note: The Nebula Device only checks the file types you selected for sandbox inspection. The scan result will be removed from the Nebula Device cache after the Nebula Device restarts.
File Types to Scan	Specify the type of files to be sent for sandbox inspection.
Intrusion Prevention System (IPS)	
Enabled	Select this to activate the IPS feature which detects and prevents malicious or suspicious packets and responds instantaneously.
Mode	Select **Detection** to have the Nebula Device only create a log message when a stream of data matches a malicious signature. Alternatively, select **Prevention** to have the Nebula Device perform a user-specified action when a stream of data matches a malicious signature.
External Block List	
IP Reputation (EBL)	Select this to have the Nebula Device block the incoming packets that come from the listed addresses in the block list file on the server.
External block list	
Enabled	Select this to turn on the rule.

Table 201 Organization-wide > Organization-wide manage > Security profile sync (continued)

LABEL	DESCRIPTION
Name	Enter an identifying name for the block list file. You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long.
External DB	Enter the exact file name, path and IP address of the server containing the block list file. The file type must be 'txt'. For example, http://172.16.107.20/blacklist-files/myip-ebl.txt The server must be reachable from the Nebula Device.
Description	Enter a description of the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new IP reputation external block list profile entry.
Schedule update	The signatures for DNS Filter and URL Threat Filter are the same. These signatures are continually updated as new malware evolves. New signatures can be downloaded to the Nebula Device periodically if you have subscribed for the URL Threat filter signatures service. You need to create an account at Zyxel, register your Nebula Device and then subscribe for URL Threat filter service in order to be able to download new signatures from Zyxel. Select **External DB schedule update** and **Daily** to set the time of the day, or **Weekly** to set the day of the week and the time of the day. Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.
DNS/URL Threat Filter (EBL)	Select this to have the Nebula Device automatically block packets that come from the listed addresses in the block list file on the server.
External block list	
Enabled	Select this to turn on the rule.
Name	Enter the identifying name for the block list file. You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long.
External DB	Enter the file name, path and IP address of the server containing the block list file. For example, http://172.16.107.20/blacklist-files/myip-ebl.txt
Description	Enter a description of the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new DNS/URL threat filter external block list entry.
Schedule update	New IP reputation signatures can be downloaded to the Nebula Device periodically if you have subscribed for the IP reputation signatures service.You need to create an account at Zyxel, register your Nebula Device and then subscribe for IP reputation service in order to be able to download new signatures from Zyxel. Select **External DB schedule update** and **Daily** to set the time of the day, or **Weekly** to set the day of the week and the time of the day. Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.

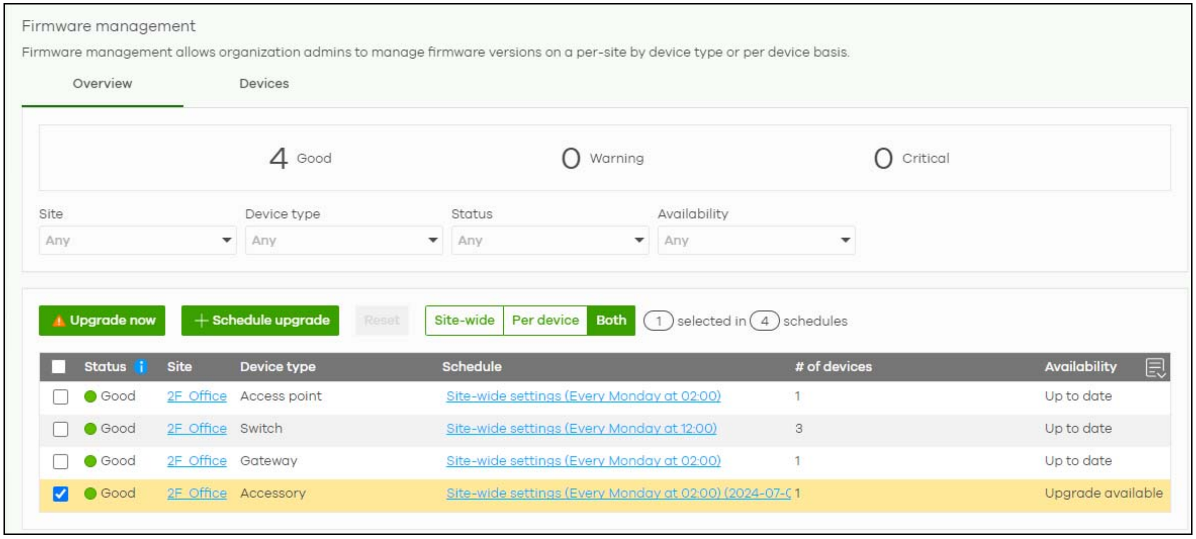
12.4.6 Firmware Management

Use this screen to upgrade Nebula Device firmware, or schedule a firmware upgrade for Nebula Devices within the sites in the organization. Click **Organization-wide** > **Organization-wide manage** > **Firmware management** to access this screen.

12.4.6.1 Firmware Management Overview Screen

Use this screen to view and/or schedule a firmware upgrade for Nebula Devices within each site in the organization. You can make different schedules for different sites in the organization. Click **Organization-wide** > **Organization-wide manage** > **Firmware management** > **Overview** to access this screen.

Figure 267 Organization-wide > Organization-wide manage > Firmware management > Overview



Firmware management

Firmware management allows organization admins to manage firmware versions on a per-site by device type or per device basis.

Site: Any
Device type: Any
Status: Any
Availability: Any

1 selected in 4 schedules

☐	Status	Site	Device type	Schedule	# of devices	Availability
☐	● Good	2F_Office	Access point	Site-wide settings (Every Monday at 02:00)	1	Up to date
☐	● Good	2F_Office	Switch	Site-wide settings (Every Monday at 12:00)	3	Up to date
☐	● Good	2F_Office	Gateway	Site-wide settings (Every Monday at 02:00)	1	Up to date
☑	● Good	2F_Office	Accessory	Site-wide settings (Every Monday at 02:00) (2024-07-(	1	Upgrade available

You can select Nebula Devices by device type and by site, but you cannot select individual Nebula Devices. For example, you can upgrade all Switches in Site A and all APs in Site B. To upgrade individual Nebula Devices, go to **Organization-wide** > **Organization-wide manage** > **Firmware management** > **Devices**.

Note: This is a Nebula Professional Pack feature. If your Nebula Professional Pack license expires, scheduled firmware upgrades will still run.

12.4.6.2 Firmware Upgrade Priority

NCC prioritizes the different Nebula Device firmware upgrade schedules as follows, from highest to lowest as follows:

1. Individual Nebula Device upgrade schedule (set at **MSP** > **MSP cross-org manage** > **Firmware upgrades** > **Schedule upgrades**).
2. Individual Nebula Device upgrade schedule (set at **Organization-wide** > **Organization-wide manage** > **Firmware management** > **Devices**).
3. Organization-wide or site-wide upgrade schedule. If both are set, the schedule that was most recently set takes priority.
4. NCC default per-device upgrade schedule and default site-wide upgrade schedule (14 days after new firmware is released).

12.4.6.3 Firmware Management Overview Screen

The following table describes the labels in this screen.

Table 202 Organization-wide > Organization-wide manage > Firmware management > Overview

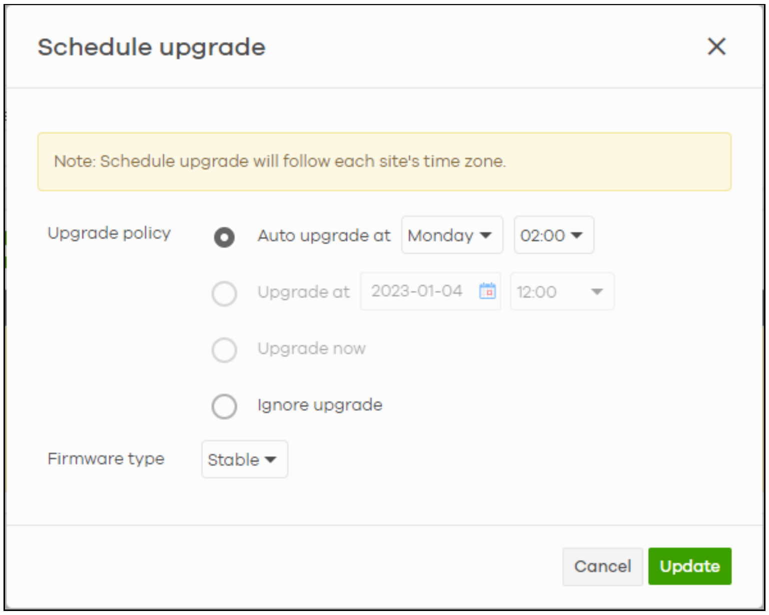
LABEL	DESCRIPTION
Site	You can set the filter to display specific Nebula Devices in a site in your organization. By default, all the sites are displayed (**Any**).
Device type	Select the type of Nebula Device. By default, all the Nebula Devices are displayed (**Any**).
Status	Select the Nebula Devices by their firmware status. By default, all Nebula Devices are displayed (**Any**). Select **Good** to display the Nebula Devices running a stable firmware and no immediate action is required. Select **Warning** to display the Nebula Devices with a newer firmware available and immediate action is recommended. The newer firmware may contain security enhancements, new features, and performance improvements. Select **Critical** to display the Nebula Devices with a newer firmware available and immediate action is required. The existing firmware may have security vulnerabilities and/or lack key performance improvements. Select **N/A** to display the Nebula Devices that are offline and its firmware status is not available.
Availability	Select to show the Nebula Devices with **Up to date** firmware, or with firmware update available for the Nebula Device (**Upgrade available**), or with a specific version of firmware has been installed by Zyxel customer support (**Locked**). By default, all available firmware is displayed (**Any**).
Upgrade Now	Click this to immediately upgrade the firmware on all selected sites. This button is selectable only when there is firmware update available for the Nebula Devices for the selected sites.
Schedule Upgrade	Click this to pop-up a window where you can set a specific date and time to upgrade the Nebula Devices firmware on the selected sites.  Schedule upgrade Note: Schedule upgrade will follow each site's time zone. Upgrade policy ● Auto upgrade at Monday 02:00 ○ Upgrade at 2023-01-04 12:00 ○ Upgrade now ○ Ignore upgrade Firmware type Stable Cancel Update Note: Nebula Devices are upgraded according to the time zone of the site they are in.

Table 202 Organization-wide > Organization-wide manage > Firmware management > Overview

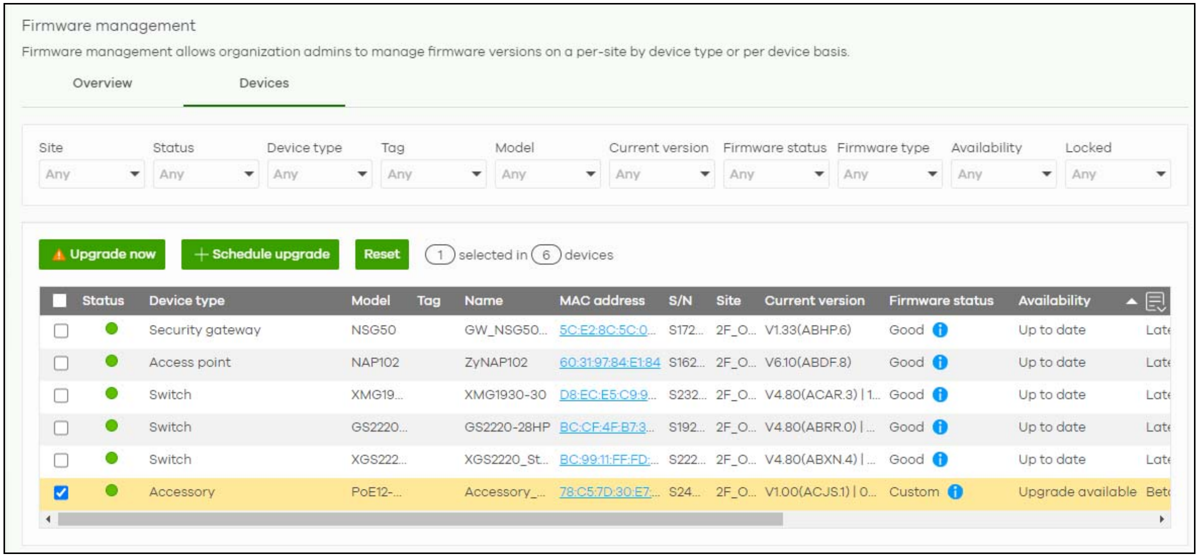
LABEL	DESCRIPTION
Reset	Select one or more **Site-wide** firmware upgrade **Schedule**s, and then click **Reset** to restore the default site-wide settings **(Every Monday at 02:00)**. Select one or more **Per device** firmware upgrade **Schedule**s, and then click **Reset** to allow the Nebula Devices to follow the site-wide firmware management settings.
Site-wide/Per device /Both	Select your desired filter criteria to filter the list of firmware upgrade schedules.
Note: Drag the following column headings to change the order. Click the column heading to change the sorting, ascending or descending order.	
Status	This shows the status of the Nebula Device's firmware. • Green: All Nebula Devices are running **Stable** or above firmware. • Amber: One or more Nebula Devices is not running the **Latest** firmware. • Red: One or more Nebula Devices is running firmware that may have security vulnerabilities and/or lack key performance improvements. • Gray: No schedule is set for upgrading the Nebula Device's firmware.
Site	This shows which site the Nebula Device is in. Click the site name to go to the site's Dashboard.
Device type	This shows the type of Nebula Device.
Schedule	This shows the day and time when a new firmware upgrade is scheduled to occur. **Site-wide settings** means the Nebula Device is following the site-wide firmware schedule. **Per device settings** means a firmware schedule is set for the Nebula Device and it will not follow the site-wide firmware schedule.
# of devices	This shows the number of Nebula Devices in the site for a particular **Schedule status**. Click this to change the schedule (see the **Schedule upgrade** field in Table 203 on page 707 for more information).
Availability	This shows whether the firmware on the Nebula Device is **Up to date**, there is firmware update available for the Nebula Device (**Upgrade available**), or a specific version of firmware has been installed by Zyxel customer support (**Locked**).
☑	Click this icon to show and hide columns in the table.

12.4.6.4 Firmware Management Devices Screen

Use this screen to make different firmware upgrade schedules for the Nebula Devices in the organization. Click **Organization-wide** > **Organization-wide manage** > **Firmware management** > **Devices** to access this screen.

Note: While installing a firmware update, the Nebula Device will continue to operate normally until it reboots. The reboot will take 3 to 5 minutes, so it is best to pick an upgrade time that has minimal impact on your network.

Figure 268 Organization-wide > Organization-wide manage > Firmware management > Devices



Firmware management

Firmware management allows organization admins to manage firmware versions on a per-site by device type or per device basis.

Site	Status	Device type	Tag	Model	Current version	Firmware status	Firmware type	Availability	Locked
Any	Any	Any	Any	Any	Any	Any	Any	Any	Any

1 selected in 6 devices

☐	Status	Device type	Model	Tag	Name	MAC address	S/N	Site	Current version	Firmware status	Availability	
☐	●	Security gateway	NSG50		GW_NSG50...	5C:E2:8C:5C:0...	S172...	2F_O...	V1.33(ABHP.6)	Good	Up to date	Late
☐	●	Access point	NAP102		ZyNAP102	60:31:97:84:E1:84	S162...	2F_O...	V6.10(ABDF.8)	Good	Up to date	Late
☐	●	Switch	XMG19...		XMG1930-30	D8:EC:E5:C9:9...	S232...	2F_O...	V4.80(ACAR.3) | 1...	Good	Up to date	Late
☐	●	Switch	GS2220...		GS2220-28HP	BC:CF:4F:B7:3...	S192...	2F_O...	V4.80(ABRR.0) | ...	Good	Up to date	Late
☐	●	Switch	XGS222...		XGS2220_St...	BC:99:11:FF:FD:...	S222...	2F_O...	V4.80(ABXN.4) | ...	Good	Up to date	Late
☑	●	Accessory	PoE12-...		Accessory_...	78:C5:7D:30:E7:...	S24...	2F_O...	V1.00(ACJS.1) | 0...	Custom	Upgrade available	Bet

The following table describes the labels in this screen.

Table 203 Organization-wide > Organization-wide manage > Firmware management > Devices

LABEL	DESCRIPTION
Site/Status/Device type/Tag/Model/ Current version/ Firmware status/ Firmware type/ Availability/Locked	Specify your desired filter criteria to filter the list of Nebula Devices.
Upgrade Now	Click this to immediately install the firmware on the selected Nebula Devices. This button is selectable only when there is firmware update available for the selected Nebula Devices.

Table 203   Organization-wide > Organization-wide manage > Firmware management > Devices

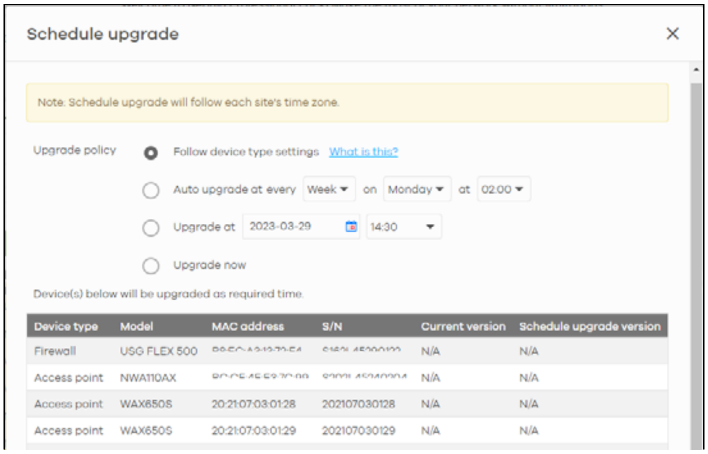
LABEL	DESCRIPTION
Schedule upgrade	Click this to pop up a window where you can create a new schedule for the selected Nebula Devices. You can select to upgrade firmware according to the organization-wide schedule configured for the Nebula Device type in the site, create a recurring schedule, edit the schedule with a specific date and time when firmware update is available for all the selected Nebula Devices, or immediately install the firmware. With a recurring schedule, the NCC will check and perform a firmware update when a new firmware release is available for any of the selected Nebula Devices. If the NCC service is downgraded from Nebula Professional Pack to Nebula Base, the Nebula Devices automatically changes to adhere to the organization-wide schedule.  Schedule upgrade Note: Schedule upgrade will follow each site's time zone. Upgrade policy ● Follow device type settings What is this? ○ Auto upgrade at every Week on Monday at 02:00 ○ Upgrade at 2023-03-29 14:30 ○ Upgrade now Device(s) below will be upgraded as required time. Device type / Model / MAC address / S/N / Current version / Schedule upgrade version Firewall / USG FLEX 500 / [illegible] / [illegible] / N/A / N/A Access point / NWA110AX / [illegible] / [illegible] / N/A / N/A Access point / WAX650S / 20:21:07:03:01:28 / 202107030128 / N/A / N/A Access point / WAX650S / 20:21:07:03:01:29 / 202107030129 / N/A / N/A
Reset	Select one or more Nebula Devices, and then click **Reset** to allow the Nebula Devices to follow the site-wide firmware management settings.
Status	This shows the status of the Nebula Device. • Green: The Nebula Device is online and has no alerts. • Amber: The Nebula Device has alerts. • Red: The Nebula Device is offline. • Gray: The Nebula Device has been offline for 7 days or more.
Device type	This shows the type of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Tag	This shows the tag created and added to the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
S/N	This shows the serial number of the Nebula Device.
Site	This shows the descriptive name of the site.
Current version	This shows the version number of the firmware the Nebula Device is currently running. It shows **N/A** when the Nebula Device goes offline and its firmware version is not available.

Table 203 Organization-wide > Organization-wide manage > Firmware management > Devices

LABEL	DESCRIPTION
Firmware status	The status shows **Good** if the Nebula Device is running a stable firmware and no immediate action is required. See the description of a stable firmware on the next field **Firmware type**. The status shows **Warning** if a newer firmware is available and immediate action is recommended. The newer firmware may contain security enhancements, new features, and performance improvements. The status shows **Critical** if a newer firmware is available and immediate action is required. The firmware may have security vulnerabilities and/or lack key performance improvements. The status shows **Custom** if the Nebula Device is running a firmware with specialized features that is not available to the general public. The status changes to **Upgrading...** after you click **Upgrade Now** to install the firmware immediately.
Firmware type	This shows **Stable** when the installed firmware may not have the latest features but has passed Zyxel internal and external testing. This shows **Latest** when the installed firmware is the most recent release with the latest features, improvements, and bug fixes. This shows **General Availability** when the installed firmware is a release before **Latest**, but is still undergoing Zyxel external testing. This shows **Dedicated** when the installed firmware is locked and Zyxel support is monitoring. Contact Zyxel customer support if you want to unlock the firmware in order to upgrade to a later one. This shows **Beta** when the installed firmware is a release version for testing the latest features and is still undergoing Zyxel internal and external testing. This shows **N/A** when the Nebula Device is offline and its firmware status is not available. Note: See Table 204 on page 710 for an example **Firmware type** version progression example scenario.
Availability	This shows whether the firmware on the Nebula Device is **Up to date**, or with a firmware update available for the Nebula Device (**Upgrade available**), or with a specific version of firmware has been installed by Zyxel customer support (**Locked**).
Upgrade scheduled	This shows the date and time when a new firmware upgrade is scheduled to occur. Otherwise, it shows **Follow upgrade time** and the Nebula Device sticks to the site-wide schedule or **No** when the firmware on the Nebula Device is up-to-date or the Nebula Device goes offline and its firmware status is not available. A lock icon displays if a specific schedule is created for the Nebula Device, which means the Nebula Device firmware will not be upgraded according to the schedule configured for all Nebula Devices in the site.
Last upgrade time	This shows the last date and time the firmware was upgraded on the Nebula Device.
Schedule upgrade version	This shows the version number of the firmware which is scheduled to be installed.
▤	Click this icon to display a greater or lesser number of configuration fields.

Firmware Type / Version Progression

The following table shows an example firmware version progression scenario.

Table 204 Firmware Type Version Progression Example

VERSION NUMBER TIMELINE	FIRMWARE TYPE	VERSION NUMBER TIMELINE	FIRMWARE TYPE
V6	Latest	V5	General Availability
V7	Latest	V6	General Availability

Note: Zyxel will select a previous version, (for example, V3) as a **Stable** release if no major issues have been reported by users.
There can only be one Latest and one Stable firmware.

12.4.7 Cloud Authentication

Use this screen to view and manage the user accounts which are authenticated using the NCC user database, rather than an external RADIUS server. Click **Organization-wide** > **Organization-wide manage** > **Cloud authentication** to access this screen.

Note: The changes you made in this screen apply to all sites in the organization. To change the cloud authentication settings for a specific site, go to **Site-wide** > **Configure** > **Cloud authentication** (see Section 4.9 on page 277).

Note: The settings in this screen will not apply to Security Firewall(s) in Cloud Monitoring mode.

12.4.7.1 User Account Types

NCC has the following types of user accounts. For details on using these accounts for WiFi and network authentication, see Section 5.3.2 on page 320.

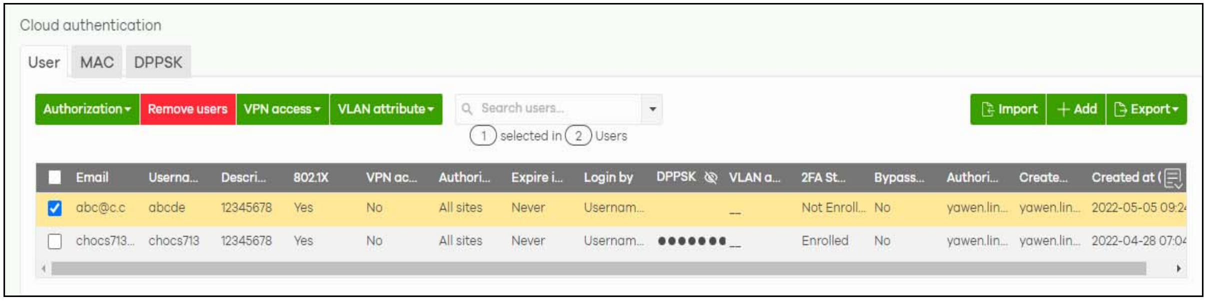
Table 205 Cloud Authentication: User Account Types

ACCOUNT TYPE	DESCRIPTION	AUTHENTICATION METHODS
User	The user account can gain access to the networks by authenticating using a pre-created user name and password, or their email address. This type of user account also supports DPPSK and two-factor authentication.	• WiFi authentication (WPA-Enterprise) • Network access through captive portal • VPN Access • WiFi authentication + network authentication through DPPSK
MAC	The Nebula Device account that can gain access to the networks by authenticating using its MAC address.	• MAC-based Nebula Device authentication (combined with DPPSK)
DPPSK	A user that can gain access to the network using a unique dynamic Personal Pre-Shared key that is linked to their user account.	• WiFi authentication + network authentication through DPPSK

12.4.7.2 Cloud Authentication User Screen

Use this screen to view and manage regular NCC network user accounts. Click **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **User** to access this screen.

Figure 269 Organization-wide > Organization-wide manage > Cloud authentication > User



Cloud authentication

User | MAC | DPPSK

Authorization ▾ | Remove users | VPN access ▾ | VLAN attribute ▾ | Search users... ▾ | Import | + Add | Export ▾

1 selected in 2 Users

☐	Email	Userna...	Descri...	802.1X	VPN ac...	Authori...	Expire i...	Login by	DPPSK	VLAN a...	2FA St...	Bypass...	Authori...	Create...	Created at (
☑	abc@c.c	abcde	12345678	Yes	No	All sites	Never	Usernam...		__	Not Enroll...	No	yawen.lin...	yawen.lin...	2022-05-05 09:2
☐	chocs713...	chocs713	12345678	Yes	No	All sites	Never	Usernam...	●●●●●●●	__	Enrolled	No	yawen.lin...	yawen.lin...	2022-04-28 07:0

The following table describes the labels in this screen.

Note: Some of the actions on this screen are only available if your administrator account has full access to the organization.

Table 206 Organization-wide > Organization-wide manage > Cloud authentication > User

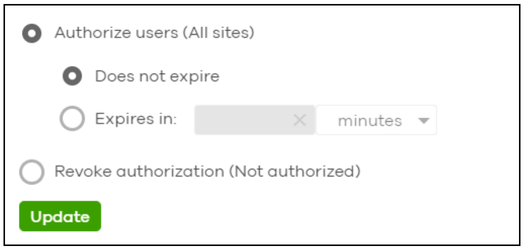
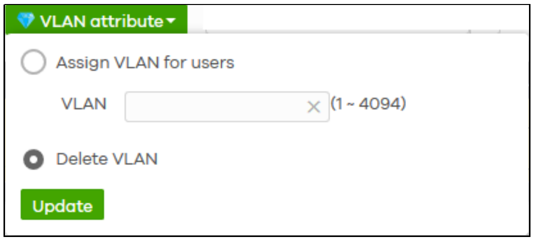
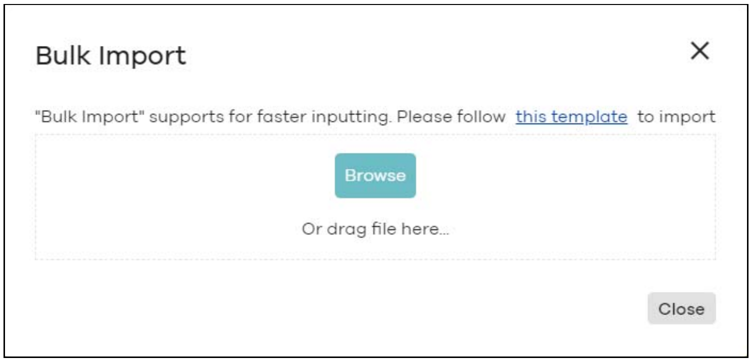
LABEL	DESCRIPTION
Authorization	Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (All sites) ● Does not expire ○ Expires in: ✕ minutes ▾ ○ Revoke authorization (Not authorized) Update
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
VPN access	Select one or more than one user account and click this button to configure whether the accounts can be used to connect to the organization's networks through VPN.
VLAN attribute	Select one or more than one user account and click this button to assign the users to a specific VLAN ID, or clear the VLAN ID. Then click **Update**.  VLAN attribute ▾ ○ Assign VLAN for users VLAN ✕ (1 ~ 4094) ● Delete VLAN Update
Print	Click this button to print information about each selected user account, such as their user name and password.
Search users	Enter a key word as the filter criteria to filter the list of user accounts.
N User	This shows how many user accounts (N) match the filter criteria and how many user accounts of the selected type are created in total.

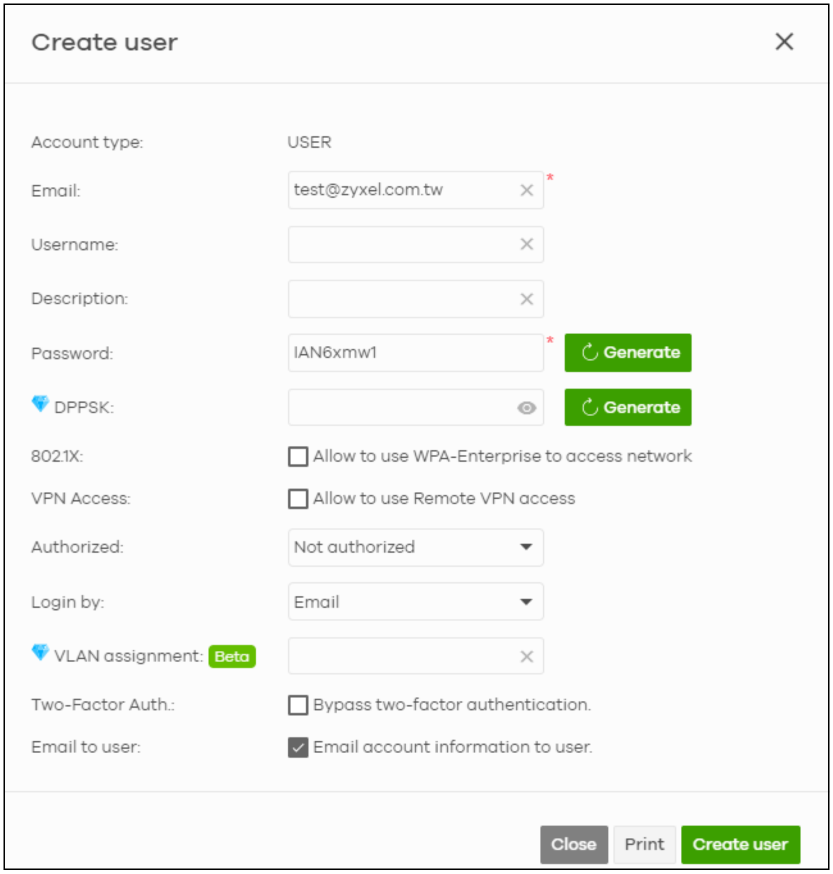
Table 206   Organization-wide > Organization-wide manage > Cloud authentication > User (continued)

LABEL	DESCRIPTION
Import	Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.  Bulk Import "Bulk Import" supports for faster inputting. Please follow this template to import
Add	Click this button to create a new user account. See Section 12.4.7.3 on page 713.
Export	Click this button to save the account list as a CSV or XML file to your computer.
Email	This shows the email address of the user account.
Username	This shows the user name of the user account.
Description	This shows the descriptive name of the user account.
802.1X	This shows whether 802.1X (WPA-Enterprise) authentication is enabled on the account.
VPN access	This shows whether the accounts can be used to connect to the organization's networks through VPN.
Authorized	This shows whether the user has been authorized or not (**No**). If the user is authorized, it shows **All sites** or the name of the site to which the user is allowed access.
Expire in (UTC)	This shows the date and time that the account expires. This shows **--** if authentication is disabled for this account. This shows **Never** if the account never expires. This shows **Multiple value** if the account has different **Expire in** values across different sites.
Login by	This shows whether the user needs to log in with the email address and/or user name.
DPPSK	This shows the account's dynamic personal pre-shared key (DPPSK), if one is set.
VLAN assignment	This field is available only when the account type is set to **User**. This shows the VLAN assigned to the user.
2FA Status	This shows whether the account has set up two-factor authentication yet.
Bypass 2FA	This shows whether the account is allowed to bypass two-factor authentication, if two-factor authentication is enabled on a captive portal or VPN gateway.
Authorized by	This shows the email address of the administrator account that authorized the user. If the account has been authorized by different admins across different sites, it shows **Multiple value**.
Created by	This shows the email address of the administrator account that created the user.
Created at	This shows the date and time that the account was created.
☰	Click this icon to display a greater or lesser number of configuration fields.

12.4.7.3 Create/Update User Account

In the **Site-wide** or **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **User** screen, click the **Add** button to create a new user account or double-click an existing account entry to modify the account settings.

Figure 270 Organization-wide > Organization-wide manage > Cloud authentication > User: Create/Update user



Create user

Account type:	USER
Email:	test@zyxel.com.tw *
Username:	
Description:	
Password:	IAN6xmw1 * Generate
DPPSK:	Generate
802.1X:	□ Allow to use WPA-Enterprise to access network
VPN Access:	□ Allow to use Remote VPN access
Authorized:	Not authorized
Login by:	Email
VLAN assignment: Beta	
Two-Factor Auth.:	□ Bypass two-factor authentication.
Email to user:	☑ Email account information to user.

The following table describes the labels in this screen.

Table 207 Organization-wide > Organization-wide manage > Cloud authentication > User: Create/Update user

LABEL	DESCRIPTION
Account type	This shows the type of the user account.
Email	Enter the email address of the user account, which is used to log into the networks.
Username	Enter a user name for this account. Note: This field is optional if **Login by** is set to **Email**.
Description	Enter a descriptive name for the account.
Password	Enter the password of this user account. It can consist of 4 – 31 alphanumeric characters. You can click **Generate** to have NCC create a password for the account automatically.

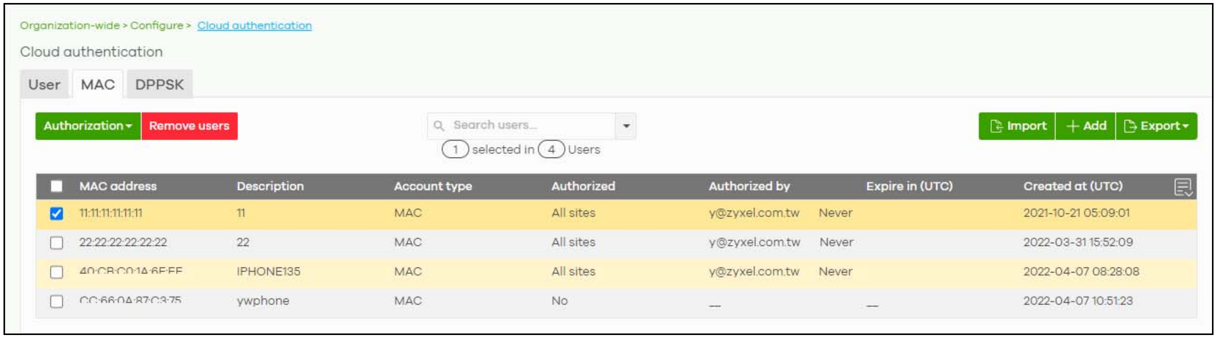
Table 207 Organization-wide > Organization-wide manage > Cloud authentication > User: Create/ Update user (continued)

LABEL	DESCRIPTION
DPPSK	Enter a dynamic personal pre-shared key (DPPSK) for this DPPSK user account, if you want to be able to authenticate using DPPSK in addition to a user name and password. It can consist of 8 – 31 alphanumeric characters. You can click **Generate** to have the NCC create a DPPSK for the account automatically.
802.1X	Select this to allow the account to be used for single sign-on (SSO) network and WiFi authentication using 802.1X (WPA-Enterprise).
VPN Access	Select this to allow the account to be used to connect to the organization's networks through VPN.
Authorized	Set whether you want to authorize the user of this account. You can select to authorize the user's access to **All Sites** or **Specified Sites** in the organization. If you select **Specified Sites**, a field displays allowing you to specify the sites to which the user access is authorized.
Expire in	This field is available only when the user is authorized. Click **Change** to specify the number of minutes/hours/days/weeks the user can be logged into the network in one session before the user of this account has to log in again. Note: If the account has been set with different **Expire in** values across different sites, it will show **Multiple value** and the **Change** link. Otherwise, select **Never** and the user of this account will never be logged out.
Login by	Select whether the user needs to log in with the email address and/or user name.
VLAN assignment	This allows you to assign a user to a specific VLAN based on the user credentials instead of using a RADIUS server.
Bypass two-factor authentication	This shows whether the account is allowed to bypass two-factor authentication, if two-factor authentication is enabled on a captive portal or VPN gateway.
Email account information to user	Select this to send a copy of the information on this screen to the account email address, after the account has been created.
Close	Click this button to exit this screen without saving.
Print	Click this button to print the account information.
Create user	Click this button to save your changes and close the screen.

12.4.7.4 Cloud Authentication MAC Screen

Use this screen to view and manage NCC Nebula Device user accounts, used for MAC-based authorization. Click **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **MAC** to access this screen.

Figure 271 Organization-wide > Organization-wide manage > Cloud authentication > MAC



Organization-wide > Configure > Cloud authentication

Cloud authentication

☐	MAC address	Description	Account type	Authorized	Authorized by	Expire in (UTC)	Created at (UTC)
☑	11:11:11:11:11:11	11	MAC	All sites	y@zyxel.com.tw	Never	2021-10-21 05:09:01
☐	22:22:22:22:22:22	22	MAC	All sites	y@zyxel.com.tw	Never	2022-03-31 15:52:09
☐	40:CB:C0:1A:6F:FF	IPHONE135	MAC	All sites	y@zyxel.com.tw	Never	2022-04-07 08:28:08
☐	CC:66:0A:87:C3:75	ywphone	MAC	No	—	—	2022-04-07 10:51:23

The following table describes the labels in this screen.

Note: Some of the actions on this screen are only available if your administrator account has full access to the organization.

Table 208 Organization-wide > Organization-wide manage > Cloud authentication > MAC

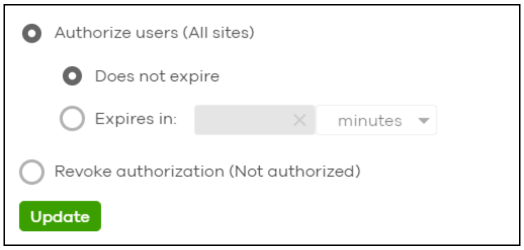
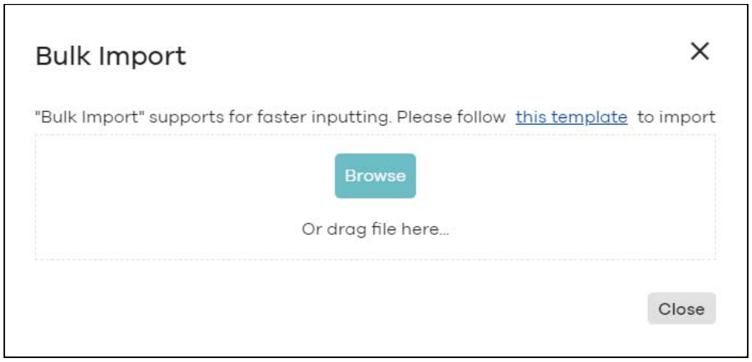
LABEL	DESCRIPTION
Authorization	Select one or more than one account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (All sites) ● Does not expire ○ Expires in: minutes ▾ ○ Revoke authorization (Not authorized) Update
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
Search users	Enter a key word as the filter criteria to filter the list of user accounts.
N User	This shows how many user accounts (N) match the filter criteria and how many user accounts of the selected type are created in total.
Import	Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.  Bulk Import ✕ "Bulk Import" supports for faster inputting. Please follow this template to import Browse Or drag file here... Close
Add	Click this button to create a new user account. See Section 12.4.7.5 on page 716.
Export	Click this button to save the account list as a CSV or XML file to your computer.
Email	This shows the email address of the user account.

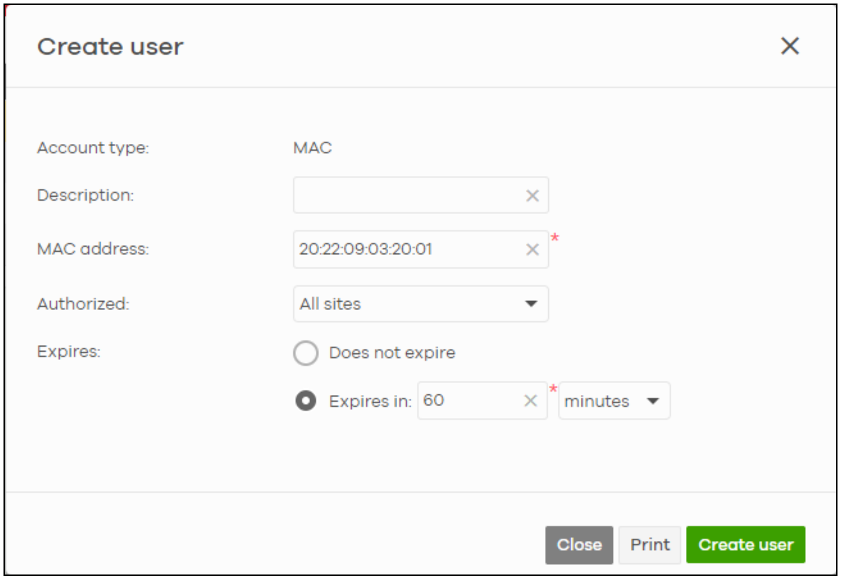
Table 208 Organization-wide > Organization-wide manage > Cloud authentication > MAC (continued)

LABEL	DESCRIPTION
MAC address	This shows the MAC address of the user account.
Description	This shows the descriptive name of the user account.
Account type	This shows the type of user account: USER, MAC, or DPPSK.
Authorized	This shows whether the user has been authorized or not (**No**). If the user is authorized, it shows **All sites** or the name of the site to which the user is allowed access.
Authorized by	This shows the email address of the administrator account that authorized the user. If the account has been authorized by different admins across different sites, it shows **Multiple value**.
Expire in (UTC)	This shows the date and time that the account expires. This shows **--** if authentication is disabled for this account. This shows **Never** if the account never expires. This shows **Multiple value** if the account has different **Expire in** values across different sites.
Created at	This shows the date and time that the account was created.
☰	Click this icon to display a greater or lesser number of configuration fields.

12.4.7.5 Create/Update MAC Account

In the **Site-wide** or **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **MAC** screen, click the **Add** button to create a new user account or double-click an existing account entry to modify the account settings.

Figure 272 Organization-wide > Organization-wide manage > Cloud authentication > MAC: Create/ Update user



Create user

Account type: MAC

Description:

MAC address: 20:22:09:03:20:01 *

Authorized: All sites

Expires:

○ Does not expire

● Expires in: 60 * minutes

The following table describes the labels in this screen.

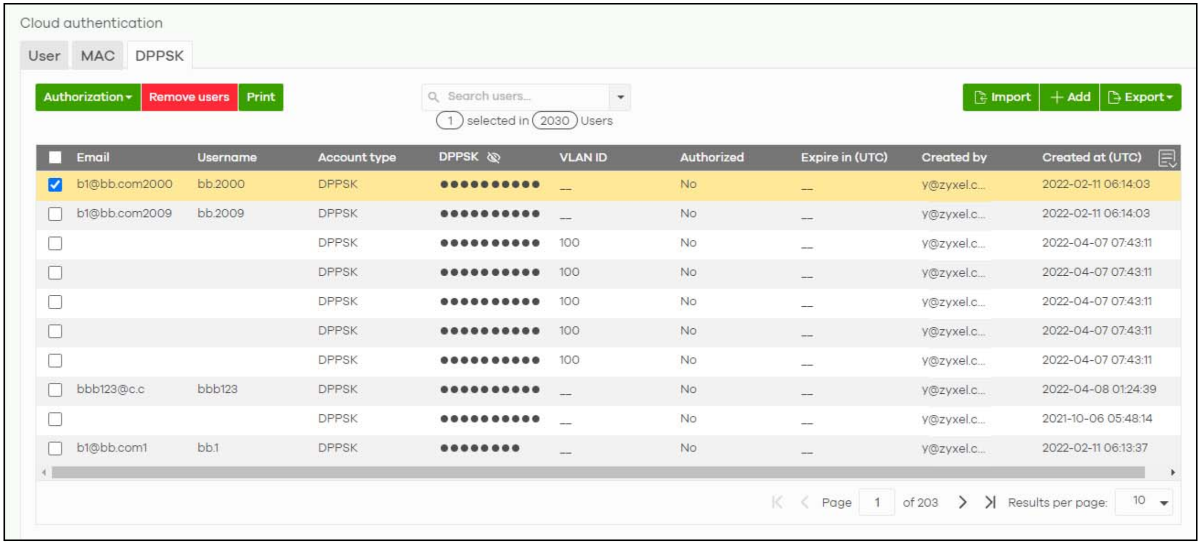
Table 209 Organization-wide > Organization-wide manage > Cloud authentication > MAC: Create/ Update user

LABEL	DESCRIPTION
Account type	This shows the type of the user account.
Description	Enter a descriptive name for the account.
MAC address	Enter a MAC address for this account.
Authorized	Set whether you want to allow the user of this account access to sites. Select **All Sites** or **Specified sites** to allow the user access to all or some sites in the organization. If you select **Specified sites**, a field displays allowing you to specify the sites to which the user access is authorized. Select **Not authorized** to prevent the user access to all the sites in the organization.
Expires	Specify the number of **minutes**/**hours**/**days**/**weeks** the user has access to site(s) in the organization.
Close	Click this button to exit this screen without saving.
Print	Click this button to print the account information.
Create user	Click this button to save your changes and close the screen.

12.4.7.6 Cloud Authentication DPPSK Screen

Use this screen to view and manage DPPSK network user accounts. Click **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **DPPSK** to access this screen.

Figure 273 Organization-wide > Organization-wide manage > Cloud authentication > DPPSK



1 selected in 2030 Users

☐	Email	Username	Account type	DPPSK	VLAN ID	Authorized	Expire in (UTC)	Created by	Created at (UTC)
☑	b1@bb.com2000	bb.2000	DPPSK	●●●●●●●●●●●	_	No	_	y@zyxel.c...	2022-02-11 06:14:03
☐	b1@bb.com2009	bb.2009	DPPSK	●●●●●●●●●●●	_	No	_	y@zyxel.c...	2022-02-11 06:14:03
☐			DPPSK	●●●●●●●●●●●	100	No	_	y@zyxel.c...	2022-04-07 07:43:11
☐			DPPSK	●●●●●●●●●●●	100	No	_	y@zyxel.c...	2022-04-07 07:43:11
☐			DPPSK	●●●●●●●●●●●	100	No	_	y@zyxel.c...	2022-04-07 07:43:11
☐			DPPSK	●●●●●●●●●●●	100	No	_	y@zyxel.c...	2022-04-07 07:43:11
☐			DPPSK	●●●●●●●●●●●	100	No	_	y@zyxel.c...	2022-04-07 07:43:11
☐	bbb123@c.c	bbb123	DPPSK	●●●●●●●●●●●	_	No	_	y@zyxel.c...	2022-04-08 01:24:39
☐			DPPSK	●●●●●●●●●●●	_	No	_	y@zyxel.c...	2021-10-06 05:48:14
☐	b1@bb.com1	bb.1	DPPSK	●●●●●●●●	_	No	_	y@zyxel.c...	2022-02-11 06:13:37

Page 1 of 203 Results per page: 10

The following table describes the labels in this screen.

Table 210   Organization-wide > Organization-wide manage > Cloud authentication > DPPSK

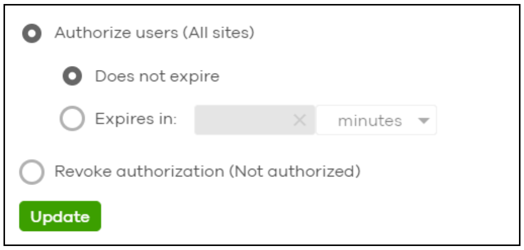
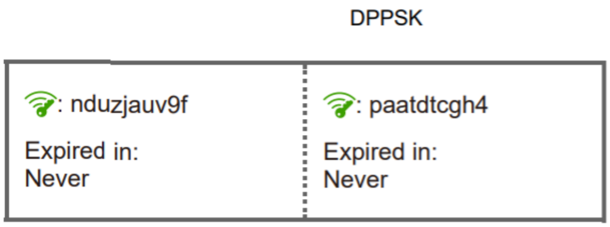
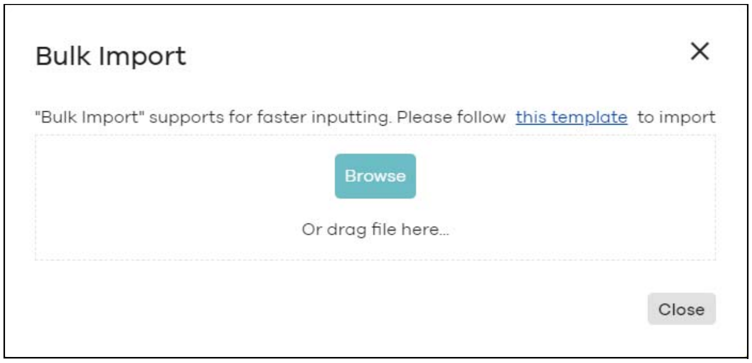
LABEL	DESCRIPTION
Authorization	Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (All sites) ● Does not expire ○ Expires in: minutes ○ Revoke authorization (Not authorized) Update
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
Print	Click this button to print the unique dynamic personal pre-shared key (DPPSK) and expiry time of each selected user account. The account details can be cut into cards, and then given to users in order to grant them WiFi network access.  DPPSK : nduzjauv9f Expired in: Never : paatdtcgh4 Expired in: Never
Search users	Enter a key word as the filter criteria to filter the list of user accounts.
N Users	This shows how many user accounts (N) match the filter criteria and how many user accounts of the selected type are created in total.
Import	Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.  Bulk Import "Bulk Import" supports for faster inputting. Please follow this template to import Browse Or drag file here... Close
Add	Click this button to create a single new account, or a batch of accounts. • Single DPPSK: See Section 12.4.7.7 on page 719. • Batch create DPPSK: See Section 12.4.7.8 on page 720.
Export	Click this button to save the account list as a CSV or XML file to your computer.
Email	This shows the email address of the user account.
Username	This shows the user name of the user account.

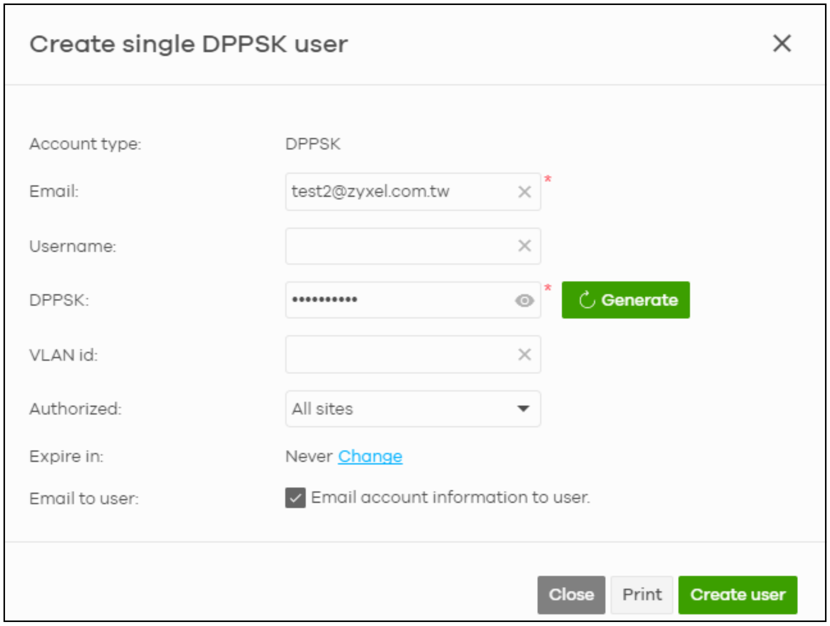
Table 210 Organization-wide > Organization-wide manage > Cloud authentication > DPPSK

LABEL	DESCRIPTION
Account type	This shows the type of user account: USER, MAC, or DPPSK.
DPPSK	This shows the account's dynamic personal pre-shared key (DPPSK).
VLAN ID	This shows the VLAN assigned to the account.
Description	This shows the descriptive name of the user account.
Authorized	This shows whether the user has been authorized or not (**No**). If the user is authorized, it shows **All sites** or the name of the site to which the user is allowed access.
Expire in (UTC)	This shows the date and time that the account expires. This shows **--** if authentication is disabled for this account. This shows **Never** if the account never expires. This shows **Multiple value** if the account has different **Expire in** values across different sites.
Created by	This shows the email address of the administrator account that created the user.
Created at	This shows the date and time that the account was created.
▤	Click this icon to display a greater or lesser number of configuration fields.

12.4.7.7 Add/Edit DPPSK Account

In the **Site-wide** or **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **DPPSK** screen, click **Add** > **Single DPPSK** to create a new user account or double-click an existing account entry to modify the account settings.

Figure 274 Organization-wide > Organization-wide manage > Cloud authentication > DPPSK: Create/ Update DPPSK user



Create single DPPSK user

Account type:	DPPSK
Email:	test2@zyxel.com.tw
Username:	
DPPSK:	••••••••••
VLAN id:	
Authorized:	All sites
Expire in:	Never Change
Email to user:	☑ Email account information to user.

The following table describes the labels in this screen.

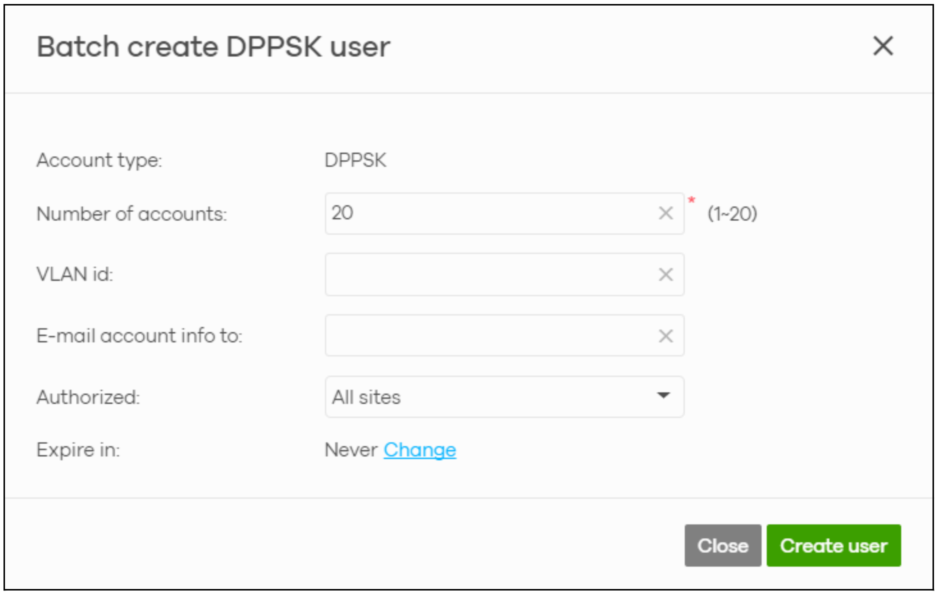
Table 211 Organization-wide > Organization-wide manage > Cloud authentication > DPPSK: Create/ Update DPPSK user

LABEL	DESCRIPTION
Account type	This shows the type of the user account.
Email	Enter the email address of the user account, which is used to log into the networks.
Username	Enter a user name for this account.
Description	Enter a descriptive name for the account.
DPPSK	Enter a dynamic personal pre-shared key (DPPSK) for this DPPSK user account. It can consist of 8 – 31 alphanumeric characters. You can click **Generate** to have the NCC create a DPPSK for the account automatically.
VLAN id	Enter the ID of a VLAN to assign a user to a specific VLAN.
Authorized	Set whether you want to authorize the user of this account. You can select to authorize the user's access to **All Sites** or **Specified Sites** in the organization. If you select **Specified Sites**, a field displays allowing you to specify the sites to which the user access is authorized.
Expire in	This field is available only when the user is authorized. Click **Change** to specify the number of minutes/hours/days/weeks the user can be logged into the network in one session before the user of this account has to log in again. Note: If the account has been set with different **Expire in** values across different sites, it will show **Multiple value** and the **Change** link. Otherwise, select **Never** and the user of this account will never be logged out.
Email account information to user	Select this to send a copy of the information on this screen to the account email address, after the account has been created.
Close	Click this button to exit this screen without saving.
Print	Click this button to print the account information.
Create user	Click this button to save your changes and close the screen.

12.4.7.8 Batch Create DPPSK Accounts

To have NCC create multiple DPPSK user accounts, each with a unique dynamic personal pre-shared key (DPPSK), go to the **Site-wide** or **Organization-wide** > **Organization-wide manage** > **Cloud authentication** > **DPPSK** screen, click **Add**, and then select **Batch Create DPPSK**.

Figure 275 Organization-wide > Organization-wide manage > Cloud authentication: Batch Create DPPSK



Batch create DPPSK user

Account type: DPPSK

Number of accounts: 20 * (1~20)

VLAN id:

E-mail account info to:

Authorized: All sites

Expire in: Never Change

The following table describes the labels in this screen.

Table 212 Organization-wide > Organization-wide manage > Cloud authentication: Batch Create DPPSK

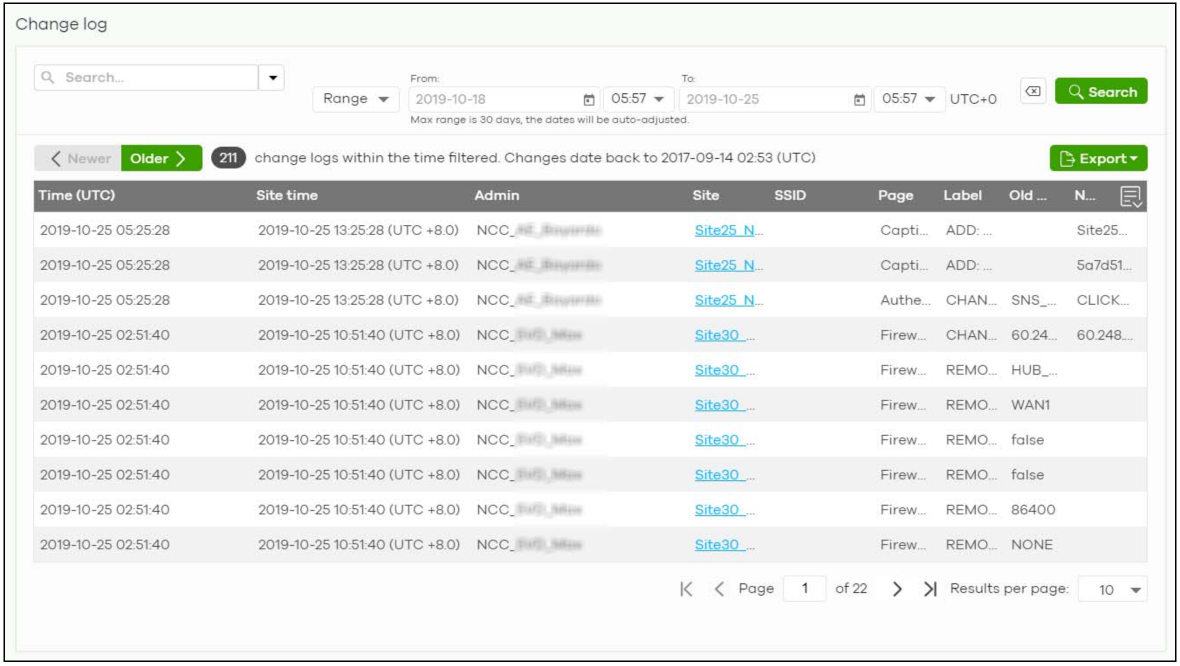
LABEL	DESCRIPTION
Number of accounts	Enter how many DPPSK user accounts you want to create.
VLAN id	Assign the users to a specific VLAN based on the user's dynamic personal pre-shared key (DPPSK).
E-mail account info to	Send a copy of each user account's dynamic personal pre-shared key (DPPSK) and expiry date to the specified email address. This information is in a printable format. The expiry date includes a time and date in UTC format.
Authorized	Set whether you want to authorize the user of this account. You can select to authorize the user's access to **All Sites** or **Specified Sites** in the organization. If you select **Specified Sites**, a field displays allowing you to specify the sites to which the user access is authorized.
Expire in	This field is available only when the user is authorized. Click **Change** to specify the number of minutes/hours/days/weeks the user can be logged into the network in one session before the user of this account has to log in again. Note: If the account has been set with different **Expire in** values across different sites, it will show **Multiple value** and the **Change** link. Otherwise, select **Never** and the user of this account will never be logged out.
Close	Click this button to exit this screen without saving.
Create user	Click this button to save your changes and close the screen.

12.4.8 Change Log

Use this screen to view logged messages for changes in the specified organization. Click **Organization-wide** > **Organization-wide manage** > **Change log** to access this screen.

When the log is full, it deletes older entries one by one to make room for new ones.

Figure 276 Organization-wide > Organization-wide manage > Change log



211 change logs within the time filtered. Changes date back to 2017-09-14 02:53 (UTC)

Time (UTC)	Site time	Admin	Site	SSID	Page	Label	Old ...	N...
2019-10-25 05:25:28	2019-10-25 13:25:28 (UTC +8.0)	NCC_[redacted]	Site25_N...		Capti...	ADD: ...		Site25...
2019-10-25 05:25:28	2019-10-25 13:25:28 (UTC +8.0)	NCC_[redacted]	Site25_N...		Capti...	ADD: ...		5a7d51...
2019-10-25 05:25:28	2019-10-25 13:25:28 (UTC +8.0)	NCC_[redacted]	Site25_N...		Authe...	CHAN...	SNS_...	CLICK...
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_[redacted]	Site30_...		Firew...	CHAN...	60.24...	60.248...
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_[redacted]	Site30_...		Firew...	REMO...	HUB_...	
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_[redacted]	Site30_...		Firew...	REMO...	WAN1	
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_[redacted]	Site30_...		Firew...	REMO...	false	
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_[redacted]	Site30_...		Firew...	REMO...	false	
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_[redacted]	Site30_...		Firew...	REMO...	86400	
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_[redacted]	Site30_...		Firew...	REMO...	NONE	

The following table describes the labels in this screen.

Table 213 Organization-wide > Organization-wide manage > Change log

LABEL	DESCRIPTION
Search	Click to enter one or more key words as the search criteria to filter the list of logs.
Range/Before	Select **Range** to set a time range or select **Before** to choose a specific date/time and the number of hours/minutes to display only the log messages generated within a certain period of time (before the specified date/time). The maximum allowable time range is 30 days.
Search	Click this to update the list of logs based on the search criteria.
Reset filters ⌫	Click this to return the search criteria to the previously saved time setting.
Newer/Older	Click to view a list of log messages with the most recent or oldest message displayed first.
	This shows the total number of the log messages that match the search criteria. It also shows the date and time the very first log was created.
Export	Click this button to save the log list as a CSV or XML file to your computer.
Time (UTC)	This shows the date and time in UTC+00:00 (or UTC+0) when the log was recorded. UTC is a standard time for use around the world (formerly known as Greenwich Mean Time or GMT). UTC is an international abbreviation that is neither French nor English. It means both "Temps Universel Coordonné" and "Coordinated Universal Time".
Site Time	This shows the date and time of the site, to which the change was applied, when the log was recorded.
Admin	This shows the name of the administrator who made the changes.
Site	This shows the name of the site to which the change was applied.

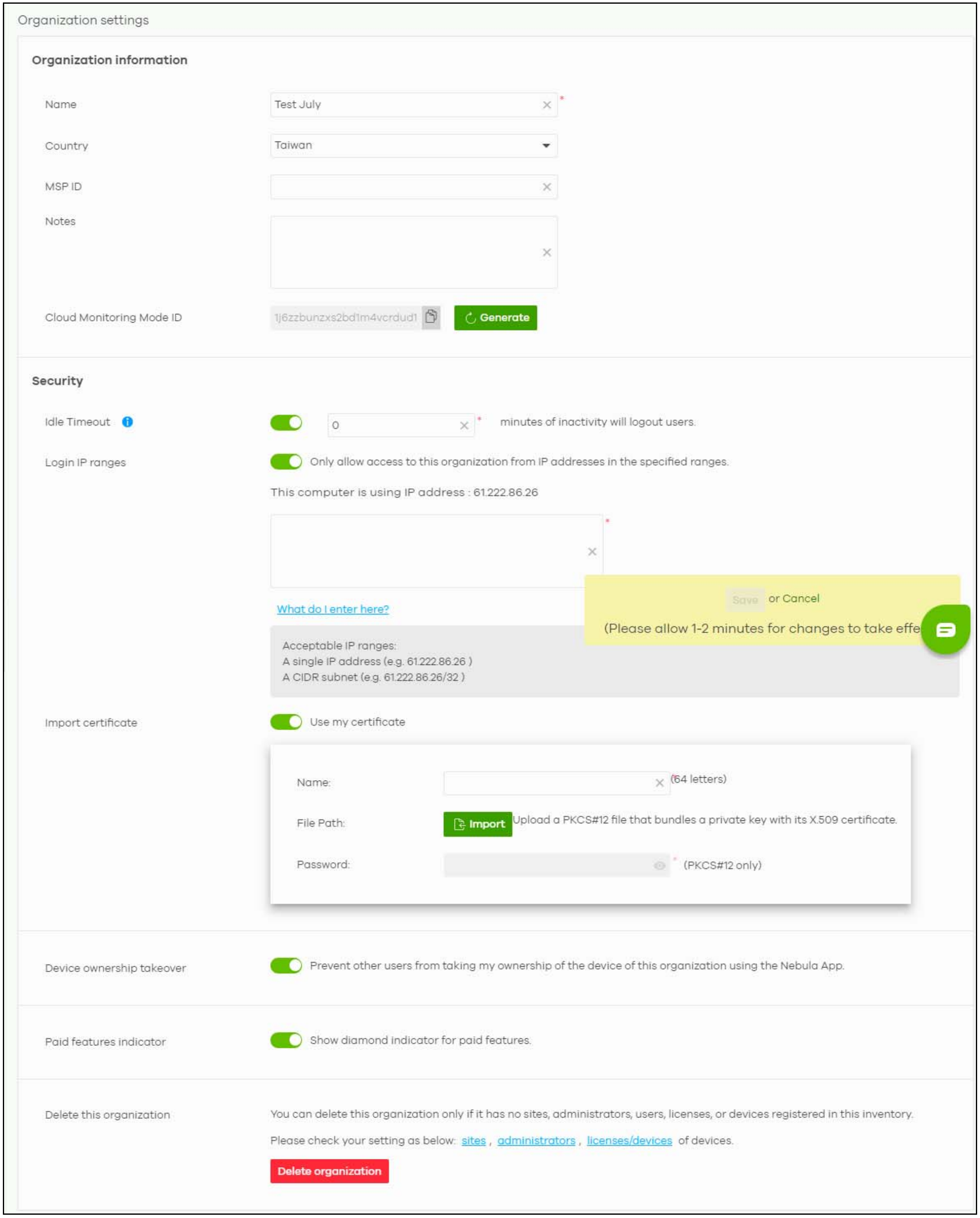
Table 213 Organization-wide > Organization-wide manage > Change log (continued)

LABEL	DESCRIPTION
SSID	This shows the SSID name to which the change was applied.
Page	This shows the name of the NCC menu in which the change was made.
Label	This shows the reason for the log.
Old value	This shows the old setting that was discarded and overwritten with the new attribute value.
New value	This shows the new setting that was adopted.
▤	Click this icon to display a greater or lesser number of configuration fields.

12.4.9 Organization Settings

Use this screen to change your general organization settings, such as the organization name and security. Click **Organization-wide** > **Organization-wide manage** > **Organization settings** to access this screen.

Figure 277 Organization-wide > Organization-wide manage > Organization settings



Organization settings

Organization information

Name: Test July *

Country: Taiwan

MSP ID:

Notes:

Cloud Monitoring Mode ID: 1j6zzbunzxs2bd1m4vcrdud1

Security

Idle Timeout: 0 * minutes of inactivity will logout users.

Login IP ranges: Only allow access to this organization from IP addresses in the specified ranges.

This computer is using IP address : 61.222.86.26

What do I enter here?

Acceptable IP ranges:
A single IP address (e.g. 61.222.86.26)
A CIDR subnet (e.g. 61.222.86.26/32)

(Please allow 1-2 minutes for changes to take effe

Import certificate: Use my certificate

Name: (64 letters)

File Path: Upload a PKCS#12 file that bundles a private key with its X.509 certificate.

Password: * (PKCS#12 only)

Device ownership takeover: Prevent other users from taking my ownership of the device of this organization using the Nebula App.

Paid features indicator: Show diamond indicator for paid features.

Delete this organization: You can delete this organization only if it has no sites, administrators, users, licenses, or devices registered in this inventory.

Please check your setting as below: sites , administrators , licenses/devices of devices.

The following table describes the labels in this screen.

Table 214 Organization-wide > Organization-wide manage > Organization settings

LABEL	DESCRIPTION
Organization information	
Name	Enter a descriptive name for the organization.
Country	Select the country where the organization is located. Note: This field is only for reference. It does not affect any other fields or features in NCC.
MSP ID	Enter the customer ID used by the administrator of the organization on another system. For example, CRM (Customer Relationship Management) and ERP (Enterprise Resource Planning) systems. Note: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 64 characters.
Notes	Enter the user-specified description of the MSP ID. Note: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 256 characters.
Cloud Monitoring Mode ID	To allow NCC to monitor your on premise Security Firewall, select **Cloud Monitoring Mode** on the Web Configurator of the Security Firewall. See the Security Firewall's User's Guide for more information. Click the copy icon to copy and paste the **Cloud Monitoring mode ID** into the **Configuration** > **Mgmt. & Analytics** > **Nebula** > **Cloud Monitoring Mode**.
Generate	The **Cloud Monitoring mode ID** is composed of 24 random alphanumeric characters. Click this button to have NCC create a new **Cloud Monitoring mode ID**.
Security	
Idle timeout	Select **ON** and enter the number of minutes each user can be logged in and idle before the NCC automatically logs out the user. Select **OFF** if you do not want the NCC to log out idle users.
Two-factor authentication	Select **ON** to enable two-factor authentication login for all administrators of this organization. Note: If this option is unavailable, you must enable **Two-factor authentication** in **Account** > **Manage account**, log out of NCC, and then log in again before you can enable organization-wide two-factor authentication in this screen. The following administrators will be forcibly log out and prevented from logging in after enabling this option: • administrators using Google/Apple Accounts to login, and • administrators who did not enable **Two-factor authentication** in the **Account** > **Manage account**. Note: Two-factor authentication is mandatory but unavailable for administrators using Google/Apple Accounts for login. Administrators using Google/Apple Account for login must contact customer support to change their login email address.
Login IP ranges	Select **ON** and specify the IP address range of the computers from which an administrator is allowed to log into the NCC. Select **OFF** to allow any IP address of the computer from which an administrator can log into the NCC.
Import certificate	

Table 214 Organization-wide > Organization-wide manage > Organization settings (continued)

LABEL	DESCRIPTION
Use my certificate	Select **ON** to import a certificate that can be used by connected Nebula Access Points in WPA2 authentication.
Name	Enter a name for the certificate (up to 64 letters).
File Path	Click to find the certificate file you want to upload.
Import	Click this button to save a new certificate to the NCC.
Password	Enter the certificate file's password.
Device ownership takeover	By default, your Nebula Device can transfer to another administrator's organization by using the Nebula Mobile app to scan the QR code. Click this switch to the right to prohibit Nebula Device transfer between administrators.
Paid features indicator	Select **ON** to show the diamond indicator for NCC features that require a license to unlock.
Delete this organization	Click the **Delete organization** button to remove the organization when it does not have any sites, Nebula Devices or users. Note: You will be redirected to the **Choose organization** page after this organization is deleted.

PART IV

Manage by Group Deployment

CHAPTER 13
Group-wide

13.1 Introduction

This chapter discusses the menus that you can use to monitor and manage your groups settings.

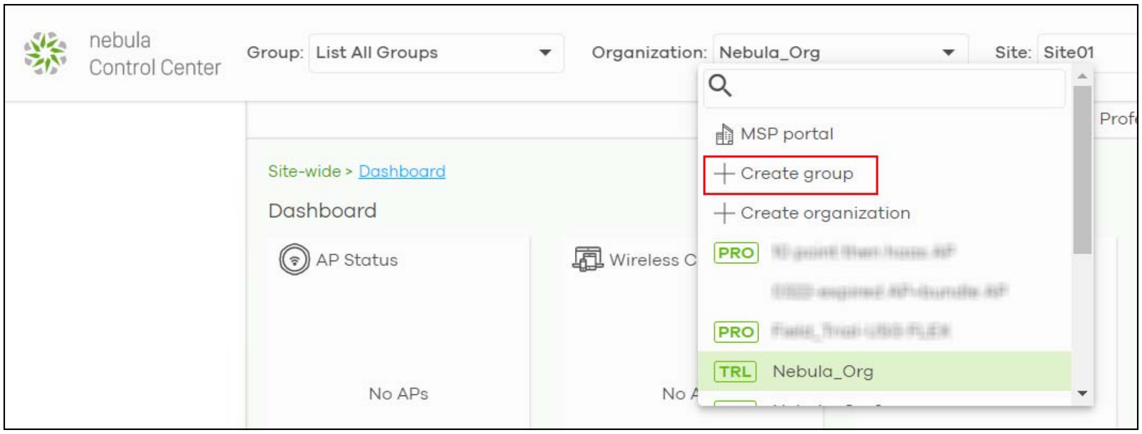
A group is a collection of two or more organizations. Groups allow you to view and manage multiple organizations, and create VPN links between groups in the organization.

13.1.1 Creating a Group

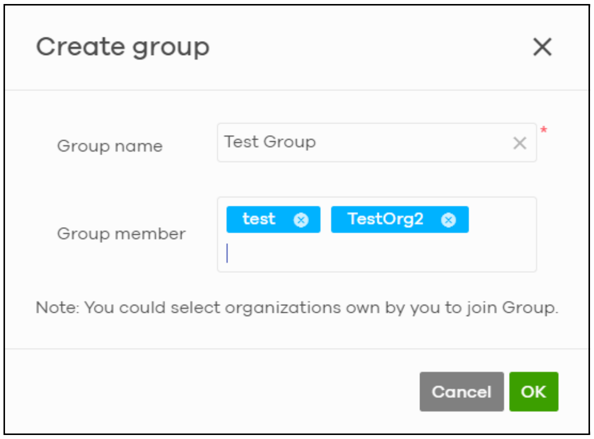
Follow the steps below to create a group.

1 Ensure that you are the owner of two or more Pro Pack organizations that are not currently in a group.

2 Click the **Organization** list, and then select **Create Group**.



3 In the **Create group** window, enter a group name and then select two or more organizations to add to the group. You must be the group owner, and each group must have a Pro Pack license. Then click **OK**.



Create group

Group name: Test Group

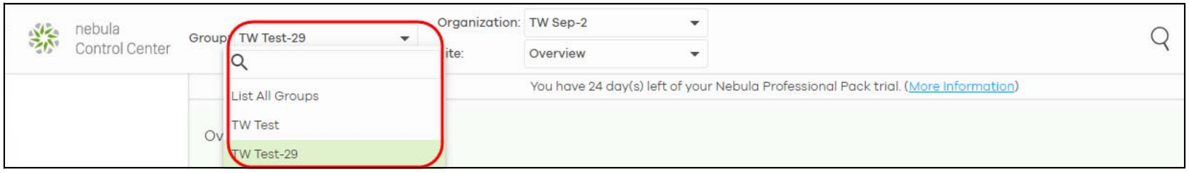
Group member: test, TestOrg2

Note: You could select organizations own by you to join Group.

13.1.2 Group-Wide Menu

The **Group-wide** menu and the **Group** list appear when you create at least one group. You can select a group to manage by selecting it in the **Group** list.

Figure 278 Group-wide > Group-wide manage > Overview: Group



Group: TW Test-29

Organization: TW Sep-2

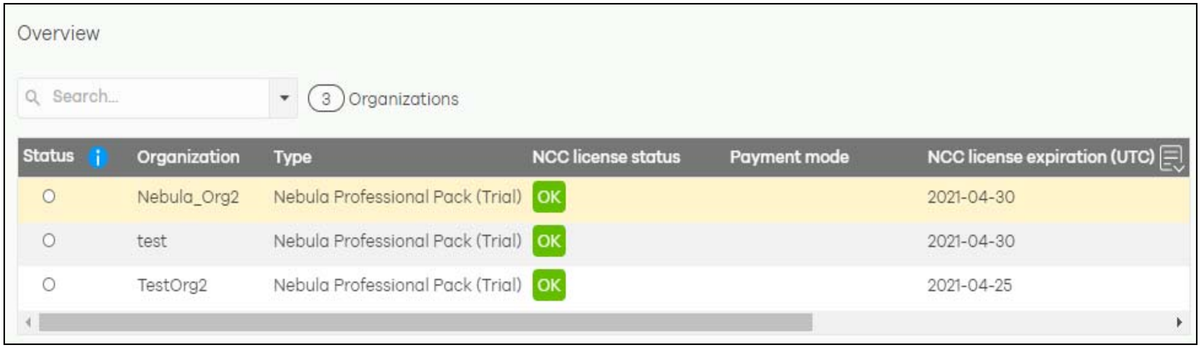
ite: Overview

You have 24 day(s) left of your Nebula Professional Pack trial. (More Information)

13.2 Group Portal

The overview screen allows you to view the status of organizations in a group. Click **Group-wide** > **Group-wide manage** > **Group portal** to access this screen.

Figure 279 Group-wide > Group-wide manage > Group portal



Overview

3 Organizations

Status	Organization	Type	NCC license status	Payment mode	NCC license expiration (UTC)
○	Nebula_Org2	Nebula Professional Pack (Trial)	OK		2021-04-30
○	test	Nebula Professional Pack (Trial)	OK		2021-04-30
○	TestOrg2	Nebula Professional Pack (Trial)	OK		2021-04-25

The following table describes the labels in this screen.

Table 215 Group-wide > Group-wide manage > Group portal

LABEL	DESCRIPTION
Search	Specify your desired filter criteria to filter the list of organizations.
matches in	This shows the number of organizations that match your filter criteria after you perform a search.
N Organizations	This shows the number of organizations (N) tin the group.
Status	This shows the status of Nebula Devices in the organization. • Green: All Nebula Devices are online and have no alerts. • Amber: One or more Nebula Devices have alerts. • Red: One or more Nebula Devices are offline. • Gray: All Nebula Devices have been offline for 7 days or more. • White: No Nebula Devices.
Organization	This shows the descriptive name of the organization.
Type	This shows the NCC license type of the organization.
NCC License Status	This shows whether the license is valid (**OK**), the license has expired and the organization downgraded from NCC Pro or Plus Pack to the base tier (**Expired**), or this is a free organization and an NCC license is not required (**N/A**).
Payment mode	This shows the payment method of the organization’s license if you arranged a special payment method with Zyxel. If you bought the license through the Zyxel web store or a third-party vendor, the value will be blank.
NCC License expiration (UTC)	This shows the date when the license will expire, or **N/A** when there are no Nebula Devices in the organization or if this is a free organization and an NCC license is not required.
Sites	This shows the number of sites belonging to this organization.
Devices	This shows the number of Nebula Devices in the organization that have one of the following status: • Green: The Nebula Device is online and has no alerts. • Amber: The Nebula Device has alerts. • Red: The Nebula Device has been offline for less than 7 days. • Gray: The Nebula Device has been offline for 7 days or more.
AP	This shows the number of Nebula Access Points in the organization.
SW	This shows the number of Nebula Switches in the organization.
SA	This shows the number of NSG and USG FLEX, ATP series, and USG20(W)-VPN Security Appliances connected to the sites in this organization.

13.3 Org-to-Org VPN

Org-to-Org VPN allows Nebula Devices in different organizations in a group to access each other’s services, such as a website, database, or ERP server, through VPN tunnels.

Note: The Security Firewall(s) in Cloud Monitoring mode will not show on the list.

13.3.1 Configure Org-to-Org VPN

Follow the steps below to configure Org-to-Org VPN in the group.

1 Configure Smart VPN for each organization you want included in the Org-to-Org VPN.

1a In the **Organization** list, select the organization.

1b Go to **Organization-wide** > **Organization-wide manage** > **VPN orchestrator**.

1c Configure a VPN area with hub-and-spoke topology, and then assign at least one site as a hub. If a site contains a server that you want to share between organizations, then ensure the server is in a hub site or that **Branch to Branch VPN** is enabled.

2 Go to **Group-wide** > **Group-wide manage** > **Org-to-Org VPN**, and then enable **Hub to Hub VPN**.

3 Click **+ Hub**. In the **Select Hubs** window, add at least one hub site from each organization to the **Within Org-to-Org** list.

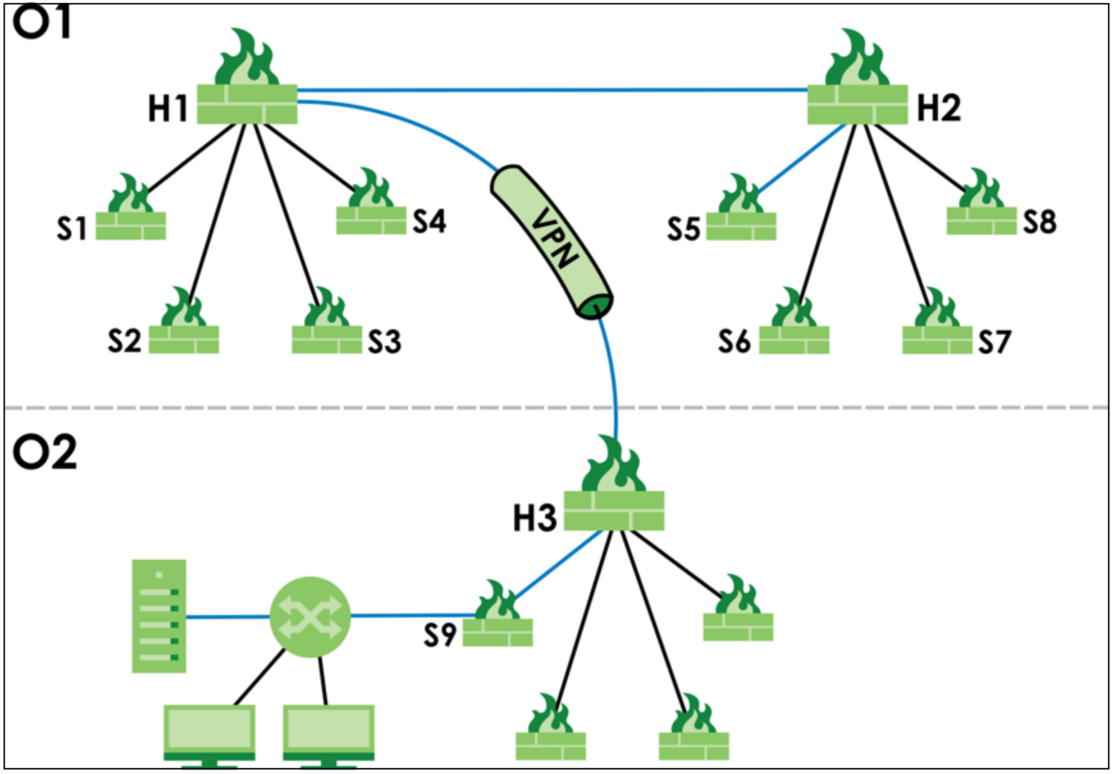
4 Click **+ Org-to-Org Service**, and add a server's fully qualified domain name (FQDN) and IP address.

5 Devices in the organizations included in the Org-to-Org VPN are now able to access the server by IP address or FQDN.

13.3.2 Org-to-Org VPN Example

Figure 280 shows organization **O1** with two VPN areas and hubs **H1** and **H2**. **Area communication** and **Branch to Branch VPN** are both enabled. It shows another organization **O2** with its own set of sites and a hub. **H1** and **H3** belong to the **Org-to-Org VPN.** The server behind **S9** is listed as an **org-to-org service**. If a Nebula Device behind **S5** wants to access the server behind **S9,** traffic will pass through its hub **H2** and then to **H1** and **H3**.

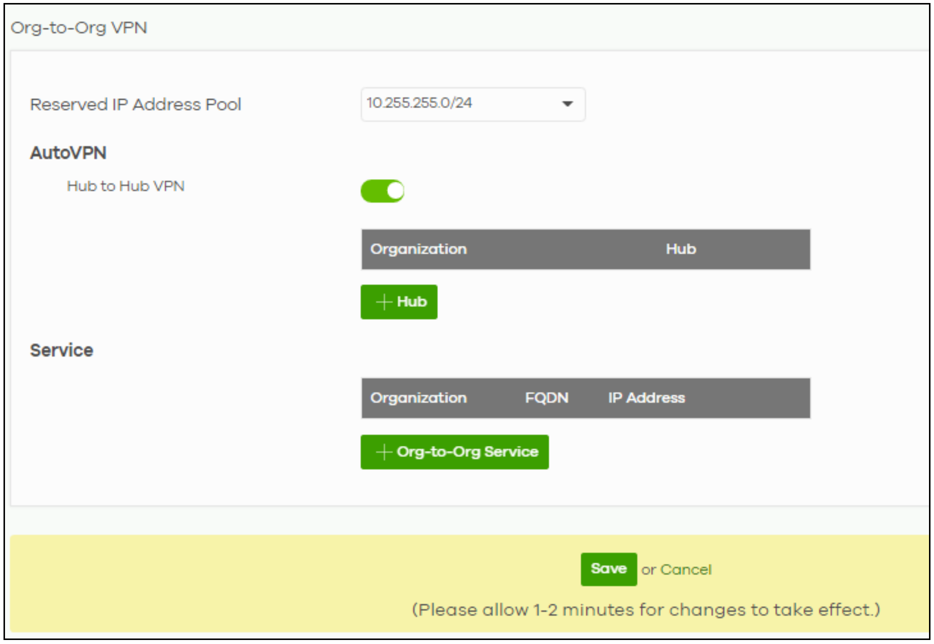
Figure 280 Org-to-Org VPN Example



13.3.3 Org-to-Org VPN Screen

Click **Group-wide** > **Group-wide manage** > **Org-to-Org VPN** to access this screen.

Figure 281 Group-wide > Group-wide manage > Org-to-Org VPN



Org-to-Org VPN

Reserved IP Address Pool: 10.255.255.0/24

(Please allow 1-2 minutes for changes to take effect.)

The following table describes the labels in this screen.

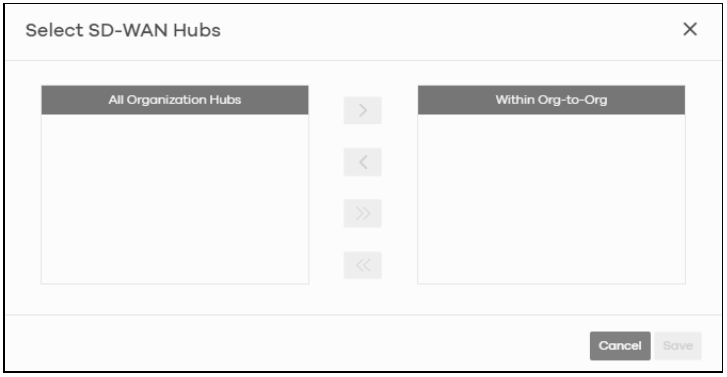
Table 216 Group-wide > Group-wide manage > Org-to-Org VPN

LABEL	DESCRIPTION
Reserved IP Address Pool	Specify the IP addresses that Nebula Devices use to create the VPN tunnels between the gateway devices in the org-to-org VPN network. You can select a set or custom range. This IP address range must not overlap with any IP address ranges already in use within any sites in the org-to-org VPN.
AutoVPN	
Hub to Hub VPN	Turn the switch to **On** to enable create VPN tunnels between the hubs in the list. This is required to enable Org-to-Org VPN. When this setting is disabled, Org-to-Org VPN will not work and can only be configured.
Organization	This column lists down the organization to which the hub site belongs.
Hub	This column lists down the names of the hub sites included in the **Org-to-Org VPN**.
+Hub	Click this to set up which hub site you want to add to the **Org-to-Org VPN**.
Service	
Organization	This displays the organization to which the network service belongs.
FQDN	This displays the Fully-Qualified Domain Name (FQDN) associated with the network service which Security Gateway devices and Nebula Devices behind them are given access.
IP Address	This displays the IP address of the network service which Security Gateway devices and Nebula Devices behind them are given access.
+Org-to-Org Service	Click this to add a service that can be accessed within the org-to-org VPN.
Save	Click this button to save your changes and close the screen.
Cancel	Click **Cancel** to exit this screen without saving.

13.3.4 Add Hub

Click the **+Hub** button on the **Group-wide** > **Group-wide manage** > **Org-to-Org VPN** screen to access the following screen. If **Hub to Hub VPN** is enabled, use this screen to select which hubs you want to include in the **Org-to-Org VPN**.

Figure 282 Group-wide > Group-wide manage > Org-to-Org VPN: SD-WAN Hubs



Hubs are listed in this screen and you may choose whether to include them in the org-to-org network or not by clicking the "<"and ">" buttons. The "<<" and ">>" buttons move all hubs at once. Details about this screen are described in the table below.

The following table describes the labels in this screen.

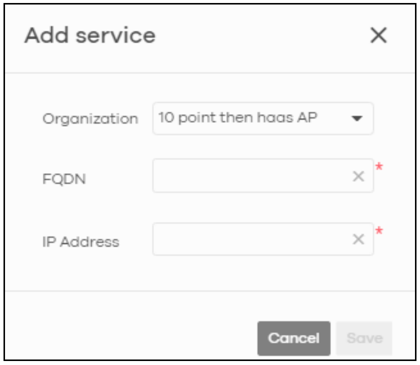
Table 217 Group-wide > Group-wide manage > Org-to-Org VPN: SD-WAN Hubs

LABEL	DESCRIPTION
All Organization Hubs	This box lists all hub sites in the group that are outside the org-to-org network. It shows the name of the hub followed by the Organization it belongs to in parentheses.
Within Org-to-Org	This box lists all hub sites inside the org-to-org network. It shows the name of the hub followed by the Organization it belongs to in parentheses.
Cancel	Click **Cancel** to exit this screen without saving.
Save	Click **Save** to add the hubs to the org-to-org network.

13.3.5 Service

Use this screen to add a service accessible through the org-to-org VPN. Note that you can choose to add only the FQDN or only the IP address. Click **+Org-to-Org Service** and then the following screen appears.

Figure 283 Group-wide > Group-wide manage > Org-to-Org VPN: Service



Organization: 10 point then haas AP

FQDN: *

IP Address: *

The following table describes the labels in this screen.

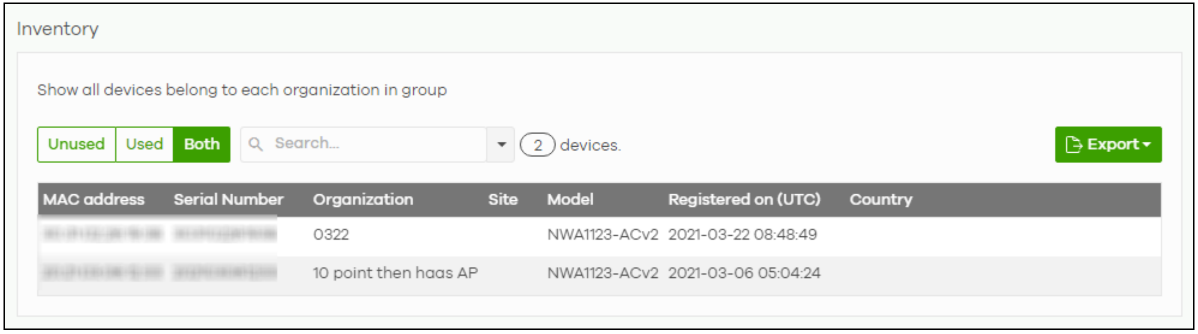
Table 218 Group-wide > Group-wide manage > Org-to-Org VPN: Service

LABEL	DESCRIPTION
Organization	Select the organization to which the service you want to add is linked to.
FQDN	Enter the Fully-Qualified Domain Name (FQDN) associated with the service. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the IP address of the service you want to add to the org-to-org VPN.
Save	Click **Save** to allow access to the service through the org-to-org VPN.
Cancel	Click **Cancel** to exit this screen without saving.

13.4 Inventory

Use this screen to view all Nebula Devices in the organizations of the selected group. Click **Group-wide** > **Group-wide manage** > **Inventory** to access this screen.

Figure 284 Group-wide > Group-wide manage > Inventory



Inventory

Show all devices belong to each organization in group

MAC address	Serial Number	Organization	Site	Model	Registered on (UTC)	Country
[redacted]	[redacted]	0322		NWA1123-ACv2	2021-03-22 08:48:49	
[redacted]	[redacted]	10 point then haas AP		NWA1123-ACv2	2021-03-06 05:04:24	

The following table describes the labels in this screen.

Table 219 Group-wide > Group-wide manage > Inventory

LABEL	DESCRIPTION
Unused	Click this button to show the Nebula Devices which are not assigned to a site yet.
Used	Click this button to show the Nebula Devices which are assigned to a site.
Both	Click this button to show all Nebula Devices which are registered for the organizations in the group.
Search	Enter a key word as the filter criteria to filter the list of connected Nebula Devices. Open the search box drop-down list to filter the search results by site, model, and country.
Devices	This shows the number of the Nebula Devices in the list.
Export	Click this button to save the Nebula Device list as a CSV or XML file to your computer.
MAC address	This shows the MAC address of the Nebula Device. Click on the MAC address to view the Nebula Device details page.
Serial number	This shows the serial number of the Nebula Device.

Table 219 Group-wide > Group-wide manage > Inventory (continued)

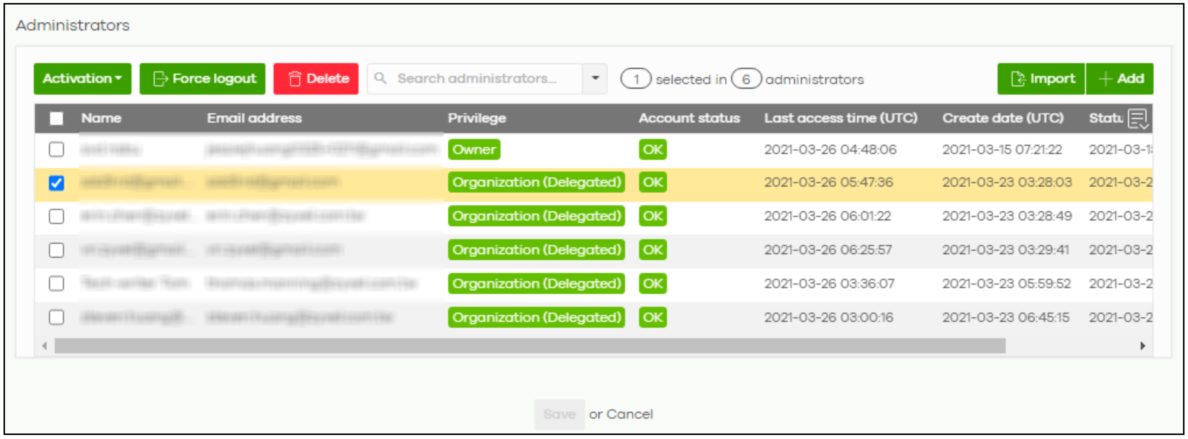
LABEL	DESCRIPTION
Organization	This shows the organization of the Nebula Device.
Site	This shows the name of the site to which the Nebula Device is connected.
Model	This shows the model number of the Nebula Device.
Registered on (UTC)	This shows the date and time that the Nebula Device was registered at the NCC.
Country	This shows the country where the Nebula Device is located.

13.5 Administrators

Group Administrator accounts can be added, modified, or deleted through this screen. A group administrator has administrator privileges in all organizations in the group. Group administrators are registered using their NCC account email address.

Click **Group-wide** > **Group-wide manage** > **Administrators** to access this screen.

Figure 285 Group-wide > Group-wide manage > Administrators



Administrators

1 selected in 6 administrators

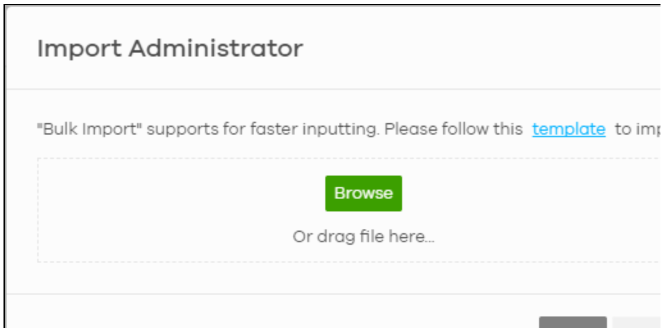
☐	Name	Email address	Privilege	Account status	Last access time (UTC)	Create date (UTC)	Statu
☐	[redacted]	[redacted]	Owner	OK	2021-03-26 04:48:06	2021-03-15 07:21:22	2021-03-1
☑	[redacted]	[redacted]	Organization (Delegated)	OK	2021-03-26 05:47:36	2021-03-23 03:28:03	2021-03-2
☐	[redacted]	[redacted]	Organization (Delegated)	OK	2021-03-26 06:01:22	2021-03-23 03:28:49	2021-03-2
☐	[redacted]	[redacted]	Organization (Delegated)	OK	2021-03-26 06:25:57	2021-03-23 03:29:41	2021-03-2
☐	[redacted]	[redacted]	Organization (Delegated)	OK	2021-03-26 03:36:07	2021-03-23 05:59:52	2021-03-2
☐	[redacted]	[redacted]	Organization (Delegated)	OK	2021-03-26 03:00:16	2021-03-23 06:45:15	2021-03-2

The following table describes the labels in this screen.

Table 220 Group-wide > Group-wide manage > Administrators

LABEL	DESCRIPTION
Activation	Click this button to **Activate/Deactivate** the selected accounts. Then, click **Update**.
Force logout	Click this button to force the selected accounts to log out of NCC.
Delete	Click this button to remove group administrator privileges for the selected accounts.
Search	Specify your desired filter criteria to filter the list of administrator accounts.
administrators	This shows the number of administrator accounts in the list.

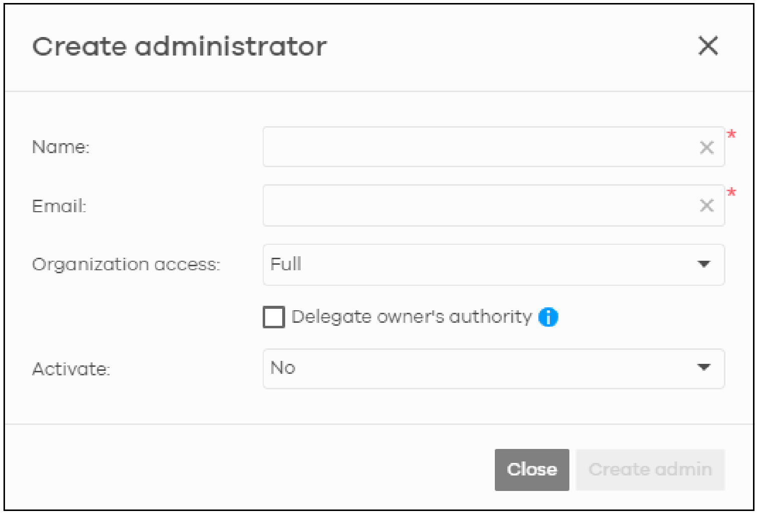
Table 220 Group-wide > Group-wide manage > Administrators (continued)

LABEL	DESCRIPTION
Import	Click this button to create administrator accounts in bulk by importing a complete list of all new administrators in an Excel file.  Import Administrator "Bulk Import" supports for faster inputting. Please follow this template to imp
Add	Click this button to create a new group administrator account. See Section 13.5.1 on page 736.
Name	This shows the name of the administrator account.
Email address	This shows the email address of the administrator account.
Privilege	This shows the privileges the administrator has within all organizations in the group. **Full**: the administrator can edit settings, create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula Devices in the organization. **Read-only:** the administrator account has no write access to the organization, but can be a site administrator. **Delegate owner's authority**: The administrator account has delegated owner privileges. This type of account can perform all of the same actions as the organization owner, except for the following: • Delete organization • Transfer organization ownership • Assign delegate owner privileges to an administrator account.
Account status	This shows whether the administrator account has been validated (**OK**). It shows **Deactivated** if an administrator account has been created but cannot be used. This may happen since you can only have up to five active administrator accounts in the NCC base tier.
Last access time	This shows the last date and time traffic was sent from the administrator account.
Create date	This shows the date and time the administrator account was created.
Status change date	This shows the last date and time the administrator account status was changed.
☰	Click this icon to display a greater or lesser number of configuration fields.

13.5.1 Create/Update Administrator

In the **Group-wide** > **Group-wide manage** > **Administrators** screen, click the **Add** button to add a new group administrator account or double-click an existing account entry to modify the account settings.

Figure 286 Group-wide > Group-wide manage > Administrators: Create/Update administrator



Create administrator

Name: *

Email: *

Organization access: Full

□ Delegate owner's authority

Activate: No

The following table describes the labels in this screen.

Table 221 Group-wide > Group-wide manage > Administrators: Create/Update administrator

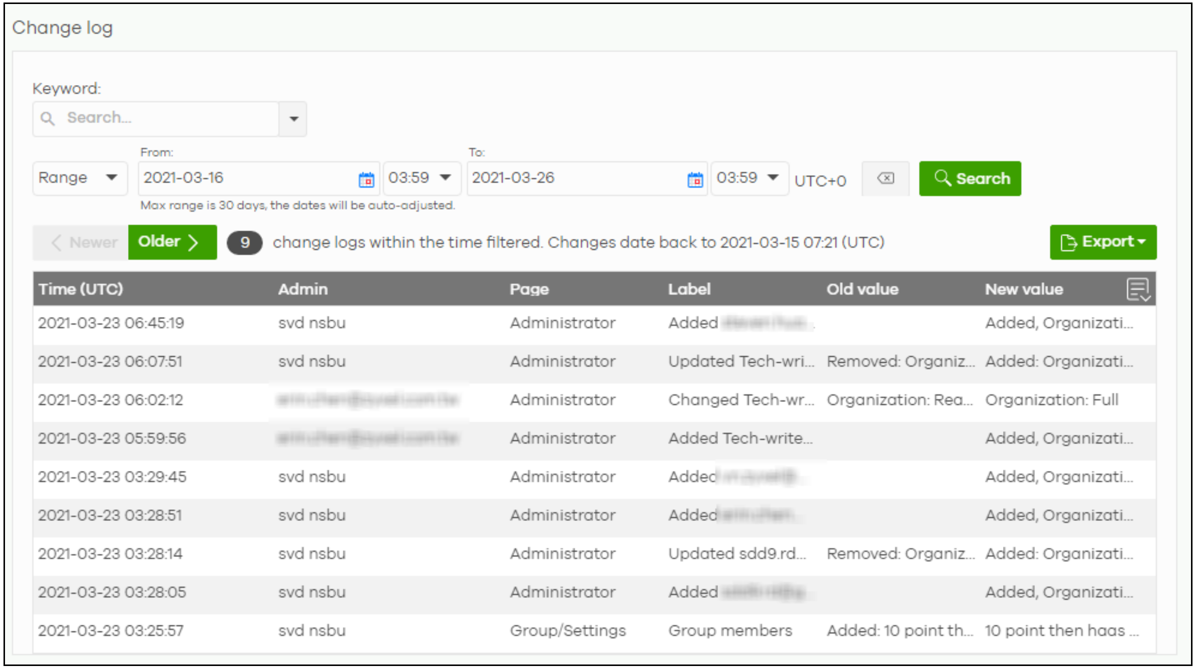
LABEL	DESCRIPTION
Name	Enter a descriptive name for the administrator account.
Email	Enter the email address of the administrator account, which is used to log into the NCC. This field is read-only if you are editing an existing account.
Organization access	This shows the privileges the administrator has within all organizations in the group. **Full**: the administrator can edit settings, create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula Devices in the organization. **Read-only:** the administrator account has no write access to the organization, but can be a site administrator.
Delegate owner's authority	This setting is only available when **Organization access** is set to **Full**. Select this setting to grant delegate owner privileges to an organization full administrator account. An account with delegate owner privileges can perform all of the same actions as the organization owner, except for the following: • Delete organization • Transfer organization ownership • Assign delegate owner privileges to an administrator account.
Activate	Select **Yes** to enable the account or **No** to temporarily disable the account.
Close	Click this button to exit this screen without saving.
Create admin/ Update admin	Click this button to save your changes and close the screen.

13.6 Change Log

Use this screen to view logged messages for changes in all organizations in the group. Click **Group-wide** > **Group-wide manage** > **Change log** to access this screen.

When the log is full, it deletes older entries one by one to make room for newer ones.

Figure 287 Group-wide > Group-wide manage > Change log



Change log

Keyword:

Range
From: 2021-03-16 03:59
To: 2021-03-26 03:59 UTC+0

Max range is 30 days, the dates will be auto-adjusted.

9 change logs within the time filtered. Changes date back to 2021-03-15 07:21 (UTC)

Time (UTC)	Admin	Page	Label	Old value	New value
2021-03-23 06:45:19	svd nsbu	Administrator	Added [redacted]		Added, Organizati...
2021-03-23 06:07:51	svd nsbu	Administrator	Updated Tech-wri...	Removed: Organiz...	Added: Organizati...
2021-03-23 06:02:12	[redacted]	Administrator	Changed Tech-wr...	Organization: Rea...	Organization: Full
2021-03-23 05:59:56	[redacted]	Administrator	Added Tech-write...		Added, Organizati...
2021-03-23 03:29:45	svd nsbu	Administrator	Added [redacted]		Added, Organizati...
2021-03-23 03:28:51	svd nsbu	Administrator	Added [redacted]		Added, Organizati...
2021-03-23 03:28:14	svd nsbu	Administrator	Updated sdd9.rd...	Removed: Organiz...	Added: Organizati...
2021-03-23 03:28:05	svd nsbu	Administrator	Added [redacted]		Added, Organizati...
2021-03-23 03:25:57	svd nsbu	Group/Settings	Group members	Added: 10 point th...	10 point then haas ...

The following table describes the labels in this screen.

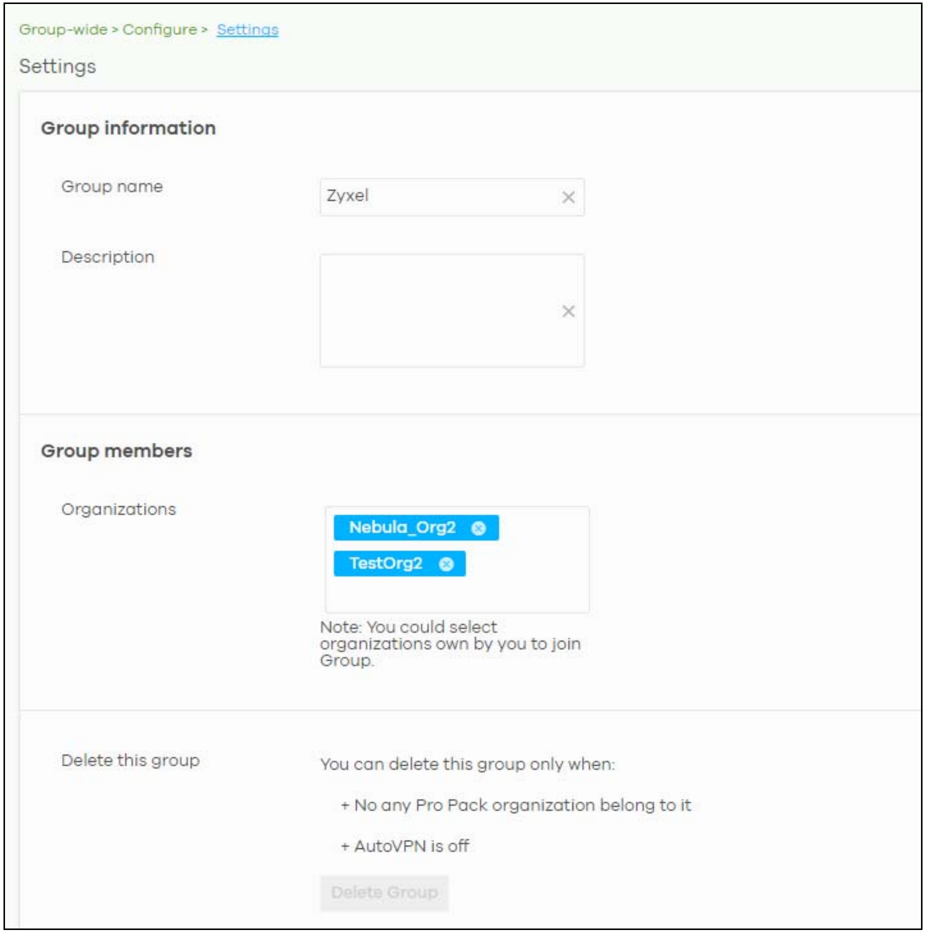
Table 222 Group-wide > Group-wide manage > Change log

LABEL	DESCRIPTION
Keyword	Enter a keyword or specify one or more filter criteria to filter the list of log entries.
Range/Before	Select a filtering option, set a date, and then click **Search** to filter log entries by date. **Range**: Display log entries from the first specified date to the second specified date. **Before**: Display log entries from the beginning of the log to the selected date.
Search	Click this to update the list of logs based on the search criteria.
Reset filters ⌫	Click this to return the search criteria to the previously saved time setting.
Newer/Older	Click to sort the log messages by most recent or oldest.
N change logs within the time filtered.	This shows the total number of the log messages that match the search criteria. It also shows the date and time the very first log was created.
Export	Click this button to download the log list as a CSV or XML file to your computer.
Time (UTC)	This shows the date and time in UTC+00:00 (or UTC+0) when the log was recorded. UTC is a standard time for use around the world (formerly known as Greenwich Mean Time or GMT). UTC is an international abbreviation that is neither French nor English. It means both "Temps Universel Coordonné" and "Coordinated Universal Time".
Admin	This shows the name of the NCC administrator account that made the changes.
Page	This shows the name of the NCC menu in which the change was made.
Label	This shows the action that triggered the log entry
Old value	This shows the old setting or state that was overwritten with the new value.
New value	This shows the new setting or state.
☰	Click this icon to display a greater or lesser number of configuration fields.

13.7 Group Settings

Use this screen to change your general group settings, such as the group name and members. Click **Group-wide** > **Group-wide manage** > **Group settings** to access this screen.

Figure 288 Group-wide > Group-wide manage > Group settings



Group-wide > Configure > Settings

Settings

Group information

Group name: Zyxel

Description

Group members

Organizations: Nebula_Org2, TestOrg2

Note: You could select organizations own by you to join Group.

Delete this group

You can delete this group only when:

+ No any Pro Pack organization belong to it

+ AutoVPN is off

The following table describes the labels in this screen.

Table 223 Group-wide > Group-wide manage > Group settings

LABEL	DESCRIPTION
Group name	Enter a descriptive name for the group.
Description	Enter a description for the group.
Group members	Click in the box to add an organization to the group. Click X to remove an organization from the group. Note: You must be the group owner, and each group must have a Pro license.
Delete this group	Click this to delete the group. Note: You can only delete a group if it contains no organizations, and **Hub to Hub VPN** is disabled at **Group-wide** > **Group-wide manage** > **Org-to-Org VPN**.

PART V
MSP

CHAPTER 14
MSP

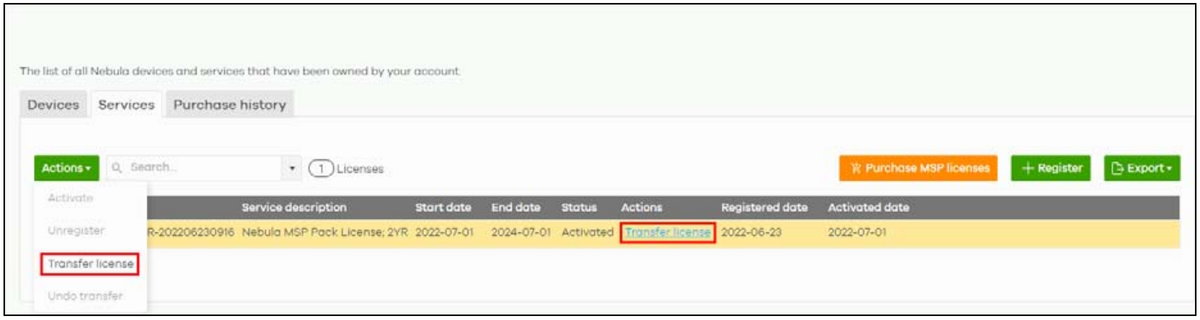
14.1 Overview

The **MSP** (Managed Services Provider) menus allow you to view the summary of organizations and change the branding on NCC.

An MSP license that expires will keep the previous settings in MSP but disable the MSP features.

An MSP license can be transferred to another MSP administrator. Click the More icon at the top right-hand corner of the **Dashboard** screen and click the **Services** tab to view the **Status** of MSP licenses. To transfer an MSP license, select the MSP license and click **Actions** > **Transfer license**. Alternatively, click **Transfer license** under **Actions**.

Figure 289 Transfer an MSP License



The list of all Nebula devices and services that have been owned by your account.

	Service description	Start date	End date	Status	Actions	Registered date	Activated date
R-202206230916	Nebula MSP Pack License; 2YR	2022-07-01	2024-07-01	Activated	Transfer license	2022-06-23	2022-07-01

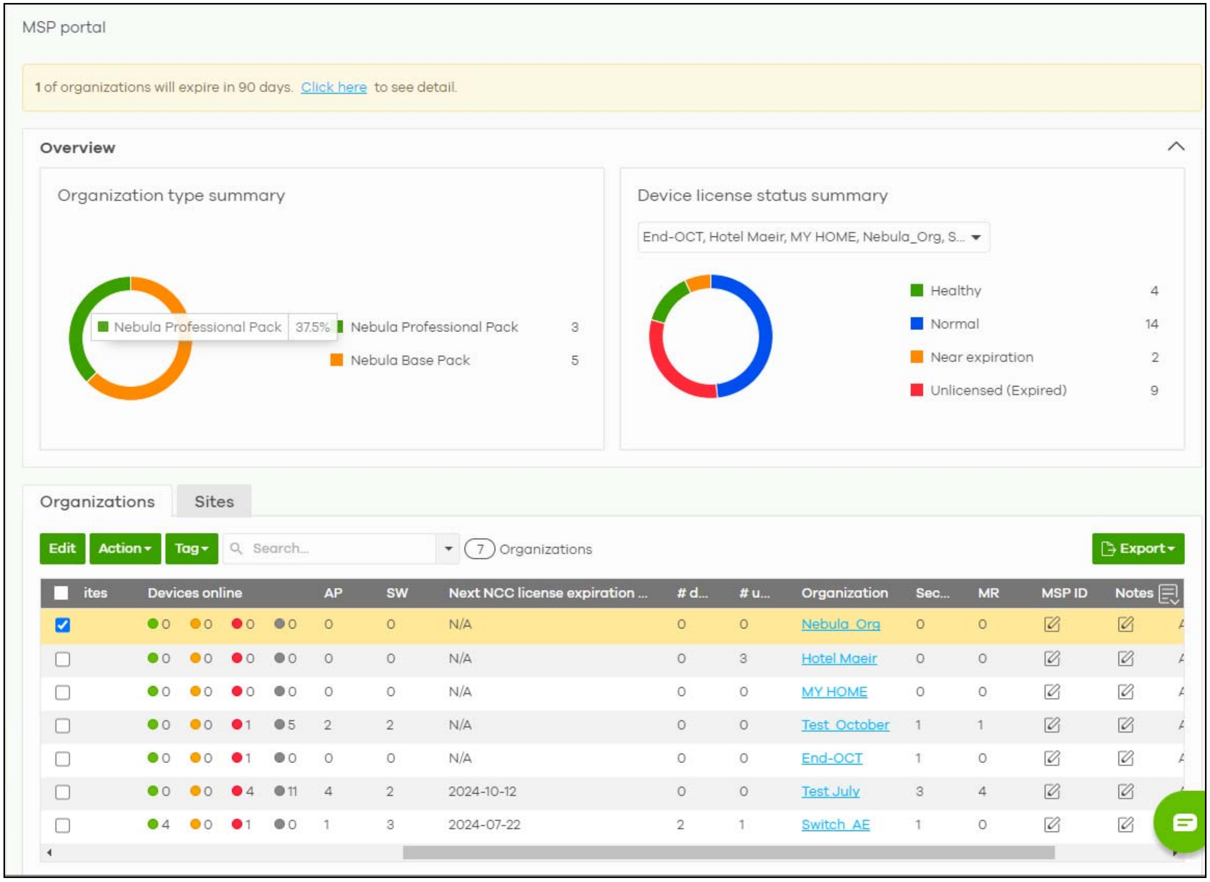
Note: To see these menus, assign an MSP license to your NCC login account.

14.2 MSP Portal

This screen lists every organization to which your account has at least read-only access.

To access this screen, select **MSP portal** from the **Organization** drop-down list box in the title bar, or click **MSP cross-org** > **MSP cross-org manage** > **MSP portal** in the navigation panel.

Figure 290 MSP cross-org > MSP cross-org manage > MSP portal



MSP portal

1 of organizations will expire in 90 days. Click here to see detail.

Overview

Organization type summary

🟩 Nebula Professional Pack	3
🟧 Nebula Base Pack	5

Device license status summary

End-OCT, Hotel Maeir, MY HOME, Nebula_Org, S...

🟩 Healthy	4
🟦 Normal	14
🟧 Near expiration	2
🟥 Unlicensed (Expired)	9

Organizations | Sites

Edit | Action | Tag | Search... | 7 Organizations | Export

☐	ites	Devices online	AP	SW	Next NCC license expiration ...	# d...	# u...	Organization	Sec...	MR	MSP ID	Notes
☑		● 0 ● 0 ● 0 ● 0	0	0	N/A	0	0	Nebula_Org	0	0	✎	✎
☐		● 0 ● 0 ● 0 ● 0	0	0	N/A	0	3	Hotel Maeir	0	0	✎	✎
☐		● 0 ● 0 ● 0 ● 0	0	0	N/A	0	0	MY HOME	0	0	✎	✎
☐		● 0 ● 0 ● 1 ● 5	2	2	N/A	0	0	Test_October	1	1	✎	✎
☐		● 0 ● 0 ● 1 ● 0	0	0	N/A	0	0	End-OCT	1	0	✎	✎
☐		● 0 ● 0 ● 4 ● 11	4	2	2024-10-12	0	0	Test July	3	4	✎	✎
☐		● 4 ● 0 ● 1 ● 0	1	3	2024-07-22	2	1	Switch_AE	1	0	✎	✎

The following table describes the labels in this screen.

Table 224 MSP cross-org > MSP cross-org manage > MSP portal

LABEL	DESCRIPTION
Organization type summary	This pie chart shows the total number of the organization mode (for example, x PRO, x Plus, x Base organizations).
Device license status summary	This pie chart shows the total number of Nebula managed devices with NCC and ATP licenses only. You can select the organization to display in the drop-down list. Click a particular color in the pie chart to show the details of the licenses of the selected organizations.
Organizations	

Table 224 MSP cross-org > MSP cross-org manage > MSP portal (continued)

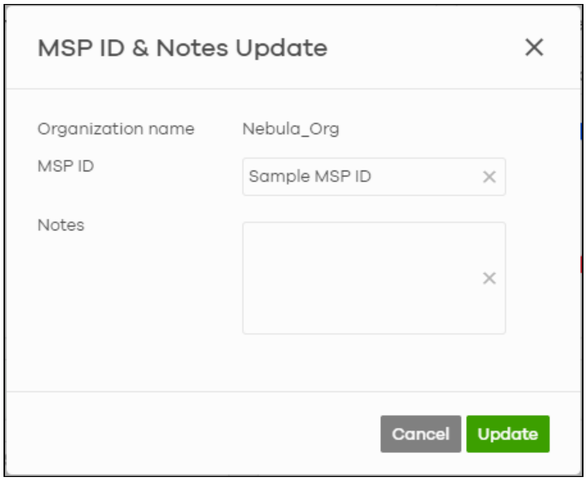
LABEL	DESCRIPTION
Edit	Click the **Edit** button to open a screen where you can change the **MSP ID** and **Notes** of the Organization. See Table 214 on page 725 for more information on **MSP ID** and **Notes** criteria.  MSP ID & Notes Update Organization name: Nebula_Org MSP ID: Sample MSP ID Notes:
Action	Perform and action on the selected Nebula organization. • **Deactivate CSM**. Select the organization(s) and click this button to disable CSM (Cloud-Saving Mode). See Section 1.7 on page 62 for more information on Cloud-saving mode. • **Restrict/allow device ownership takeover**. Select this to open a screen where you can allow/prohibit the transfer of Nebula Device to another administrator's organization by using the Nebula Mobile app. Click this switch to the right to prohibit Nebula Device transfer between administrators.
Tag	Assign a name to an organization or to a group of organizations. 1. Select the organizations. The **Tag** button will be enabled. 2. Click **Tag**. 3. In the **Add** field, enter a tag (up to 32 alphanumeric characters and spaces are allowed). 4. Click **+Add new**. Then **Add** to confirm. To remove the tag assigned to an organization or to a group of organizations. 1. Select the organization with an assigned tag. 2. Click **Tag**. 3. Enter the name of the tag. As you type along, NCC will automatically show the names of tags that matches. 4. Select the tag. Then click **Remove**.
Search	Specify your desired filter criteria to filter the list of organizations and organization status.
matches in	This shows the number of organizations that match your filter criteria after you perform a search.
Organizations	This shows the number of organizations that you can manage.
*	Click this to select all rows. Alternatively, click a row to go to the **Sites** tab that will show the sites belonging to the organization.

Table 224   MSP cross-org > MSP cross-org manage > MSP portal (continued)

LABEL	DESCRIPTION
Status	This shows the status of Nebula Devices in the organization. • Green: All Nebula Devices are online and have no alerts. • Orange: Some Nebula Devices have alerts. • Red: Some Nebula Devices are offline. • Gray: All Nebula Devices have been offline for 7 days or more. • White: No Nebula Devices in this organization. • ☁ : This organization is in Cloud-saving mode.
NCC license status	This shows the license status of Nebula Devices in the organization. • Green: All Nebula Devices with over 1 year licenses. • Blue: Any Nebula Device with over 90 days but less than 1 year license together with another Nebula Device with over 1 year license. • Orange: Any Nebula Device with license that will expire in 90 days together with another Nebula Device with over 90 days license. • Red: Any Nebula Device with an expired license or is unlicensed. • Gray: No Nebula Devices in this organization.
Organization	This shows the descriptive name of the organization. Click an **Organization** to go to the **Organization-wide** > **Organization-wide manage** > **Organization portal** screen. Hover the mouse over the name of the Organization to display the site information window. Clicking a **Site name** will go to the **Site-wide** > **Dashboard** screen.
Type	This shows your NCC version type.
Tag	This shows the tag name assigned to this organization. Otherwise, the organization does not have a tag.
Sites	This shows the number of sites belonging to this organization.
Devices online	This shows the number of Nebula Devices in this organization which are online (green), have recently had alerts (orange), recently went offline (red), or have been offline for more than 6 days (gray).
AP	This shows the number of Nebula access points connected to the sites in this organization.
SW	This shows the number of Nebula switches connected to the sites in this organization.
Security appliance	This shows the number of Nebula security appliances connected to the sites in this organization.
MR	This shows the number of Nebula mobile routers connected to the sites in this organization.
Device ownership takeover	This shows **Allow** if the Nebula Device can transfer to another administrator's organization using the Nebula Mobile app. This shows **Restrict** if the Nebula Device cannot transfer to another administrator's organization using the Nebula Mobile app.
MSP ID	This shows the customer ID used by the administrator of the organization on another system. For example, CRM (Customer Relationship Management) and ERP (Enterprise Resource Planning) systems.
Notes	This shows the user-specified description of the MSP ID.
Payment mode	This shows the payment method of the NCC license if you arranged a special payment method with Zyxel. If you bought the license through the Zyxel webstore or a third-party vendor, the value will be blank.

Table 224 MSP cross-org > MSP cross-org manage > MSP portal (continued)

LABEL	DESCRIPTION
Next NCC license expiration date	This shows the date when the license will expire, or **N/A** when there is no Nebula-managed device in the organization. For example, if you have two Nebula Devices in the organization: • Nebula Device 1 is with NCC license expiration date on 2022/10/1 • Nebula Device 2 is with NCC license expiration date on 2022/11/1 This field will show the nearest expiration date '2022/10/1'.
# devices will expire in 90 days	This shows the number of Nebula-managed devices with licenses that will expire in 90 days or less in this organization.
# unused NCC license	This shows the number of unused NCC (Nebula Control Center) licenses in this organization.
▤	Click this icon to display a greater or lesser number of configuration fields.
Export	Click this button to save the MSP Portal list as a CSV or XML file to your computer.
Sites	
Search	Specify your desired filter criteria to filter the list of sites.
matches in	This shows the number of sites that match your filter criteria after you perform a search.
sites	This shows the number of sites that you can manage.
*	Click this to select all rows.
Status	This shows the status of Nebula Devices in the site. • Green: All Nebula Devices are online and have no alerts. • Orange: Some Nebula Devices have alerts. • Red: Some Nebula Devices are offline. • Gray: All Nebula Devices have been offline for 7 days or more. • White: No Nebula Devices in this site.
Organization	This shows the descriptive name of the organization.
Site	This shows the descriptive name of the site. Clicking a site name will go to the **Site-wide** > **Dashboard** screen.
Tags	This shows the tag name assigned to this site. Otherwise, the site does not have a tag.
Devices	This shows the number of Nebula Devices connected to the site.
Offline devices	This shows the number of Nebula Devices in this site which are offline.
% Offline	This shows the percentage of Nebula Devices in this site which are offline.
Template	This shows the name of the template that is bound to a site.
▤	Click this icon to display a greater or lesser number of configuration fields.
Export	Click this button to save the MSP Portal list as a CSV or XML file to your computer.

14.3 Admins & Teams

The Admins & teams enables you to assign an administrator or a group of administrators (a team) to multiple organizations at the same time. This is faster than configuring administrators for each organization at **Organization-wide** > **Administrators**, especially if you have a large number of organizations.

14.3.1 Administrator Privilege Priority

You can configure organization administrator privileges on the following screens:

- **MSP cross-org** > **MSP cross-org manage** > **Admins & teams** > **Admins**
- **MSP cross-org** > **MSP cross-org manage** > **Admins & teams** > **Teams**
- **Group-wide** > **Group-wide manage** > **Administrators**
- **Organization-wide** > **Administrators**

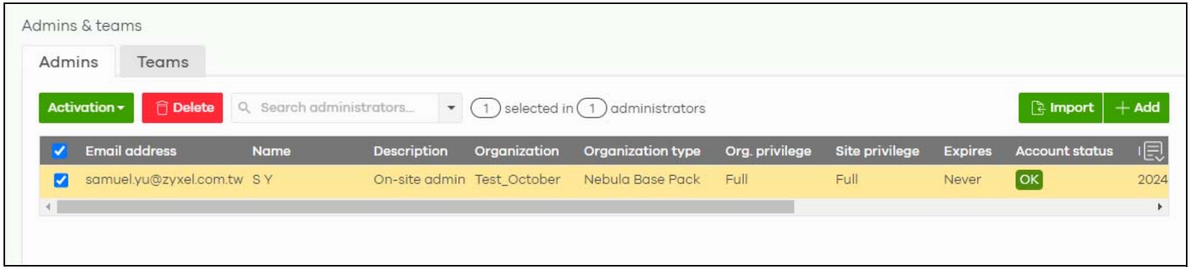
If an NCC account has different administrator privileges configured on different screens, then the highest privilege level takes priority.

Example, account User1 has four different privilege levels configured for organization Org1 on the four screens above: None, Read-Only, Full, Full (Delegate). User1's final privilege level for Org1 is Full (Delegate).

14.3.2 Admins Screen

The admins screen allows you to assign an administrator account to multiple organizations. To access this screen, click **MSP cross-org** > **MSP cross-org manage** > **Admins & teams** > **Admins**.

Figure 291 MSP cross-org > MSP cross-org manage > Admins & teams > Admins



Admins & teams

Admins | Teams

Activation ▾ | Delete | Search administrators... ▾ | 1 selected in 1 administrators | Import | + Add

☑	Email address	Name	Description	Organization	Organization type	Org. privilege	Site privilege	Expires	Account status	
☑	samuel.yu@zyxel.com.tw	S Y	On-site admin	Test_October	Nebula Base Pack	Full	Full	Never	OK	2024

The following table describes the labels in this screen.

Table 225 MSP cross-org > MSP cross-org manage > Admins & teams > Admins

LABEL	DESCRIPTION
Activation	Click this button to **Activate**/**Deactivate** the selected accounts. Then, click **Apply**.
Delete	Click this button to remove group administrator privileges for the selected accounts.
Search	Specify your desired filter criteria to filter the list of administrator accounts.
N administrators	This shows the number of administrator accounts (N) in the list.

Table 225 MSP cross-org > MSP cross-org manage > Admins & teams > Admins (continued)

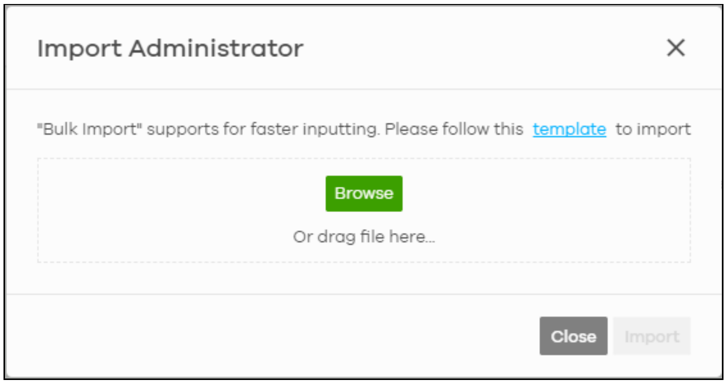
LABEL	DESCRIPTION
Import	Click this button to create administrator accounts in bulk by importing a complete list of all new administrators in an Excel file. Click **template** to view and use the file format.  Import Administrator "Bulk Import" supports for faster inputting. Please follow this template to import
Add	Click this button to create a new group administrator account.
Email address	This shows the email address of the administrator account.
Name	This shows the name of the administrator account.
Description	This shows the user-specified description for the administrator account.
Organization	This shows the name of the organization in which the privileges apply.
Organization type	This shows the license tier of the organization.
Org. privilege	This shows the privileges the administrator has within the specified organization. **Full**: the administrator can edit settings, create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula Devices in the organization. **Read-only:** the administrator account has no write access to the organization, but can be a site administrator. **Delegate owner's authority**: The administrator account has delegated owner privileges. This type of account can perform all of the same actions as the organization owner, except for the following: • Delete organization • Transfer organization ownership • Assign delegate owner privileges to an administrator account
Site privilege	This shows the privileges the administrator has within the specified site. **Full**: the administrator can edit settings, create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula Devices in the site. **Read-only:** the administrator account has no write access to the site, but can be a site administrator. **Monitor-only**: the administrator can view the site's monitor pages for Nebula Access Points, Ethernet Switches, and Security Appliances only. The configuration pages are hidden from view. **Installer**: the administrator can register Nebula Devices at this site. **Guest Ambassador**: the administrator can create, remove or manage guest accounts using the **Cloud authentication** screen.

Table 225   MSP cross-org > MSP cross-org manage > Admins & teams > Admins (continued)

LABEL	DESCRIPTION
Expires	This shows how long the account is valid. **Never expire** – this account never expires. **Expire on** – this specifies the date the account is valid.
Account status	This shows whether the administrator account has been validated (**OK**). It shows **Deactivated** if an administrator account has been created but cannot be used. This may happen since you can only have up to 5 active administrator account in NCC base tier.
Last access time (UTC)	This shows the last date and time traffic was sent from the administrator account.
Create date (UTC)	This shows the date and time the administrator account was created.
Status change date (UTC)	This shows the last date and time the administrator account status was changed.
Creator	This shows the name of the MSP user account that added the privilege settings.
📝	Click this icon to display a greater or lesser number of configuration fields.

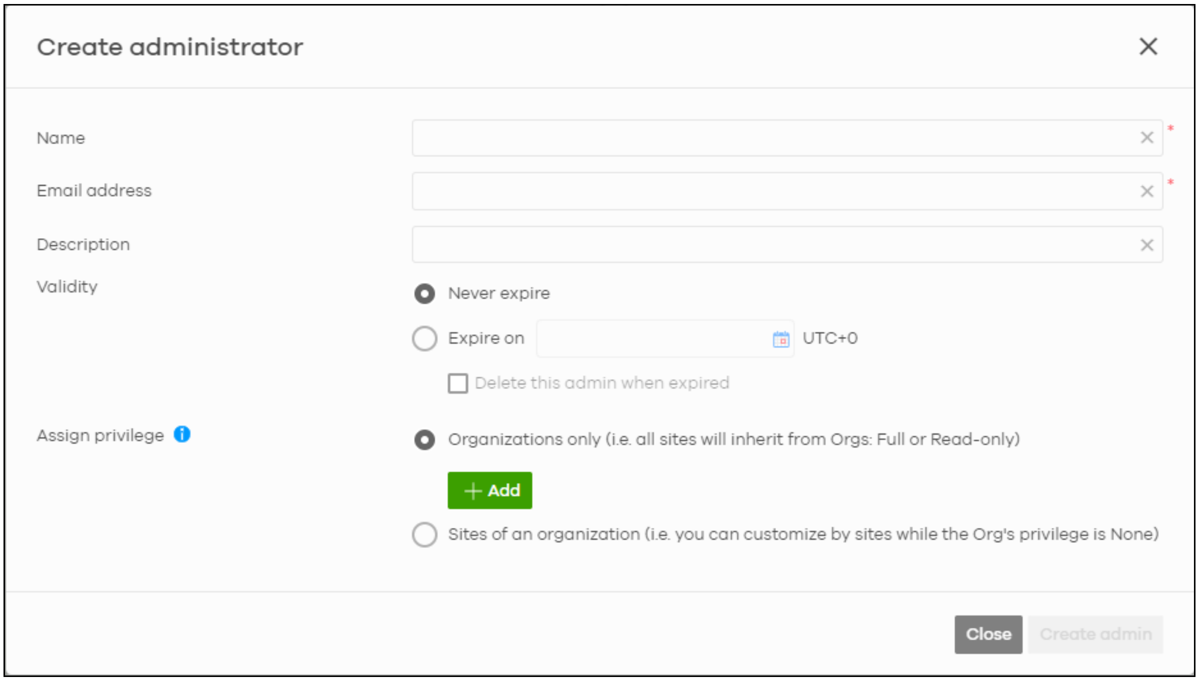
14.3.3 Create/Update Administrator

In the **MSP cross-org** > **MSP cross-org manage** > **Admins & teams** > **Admins** screen, click the **Add** button to add a new administrator account, or double-click an existing account entry to modify the account settings.

Note: NCC does not count the administrators created in Admin & teams to the Base tier and Nebula Plus Pack number of administrator account limit.

An NCC account with an MSP license can add administrators (with/without an MSP license) to the Base tier and Nebula Plus Pack organizations without limit.

Figure 292 MSP cross-org > MSP cross-org manage > Admins & teams > Admins: Create/Update administrator



Create administrator ×

Name	× *
Email address	× *
Description	×
Validity	● Never expire ○ Expire on UTC+0 □ Delete this admin when expired
Assign privilege	● Organizations only (i.e. all sites will inherit from Orgs: Full or Read-only) + Add ○ Sites of an organization (i.e. you can customize by sites while the Org's privilege is None)

The following table describes the labels in this screen.

Table 226 MSP cross-org > MSP cross-org manage > Admins & teams > Admins: Create/Update administrator

LABEL	DESCRIPTION
Name	Enter a descriptive name for the administrator account. Enter up to 100 characters in this field including special characters inside the square quotes [~!@#$%^&*()_+{}|:"<>?–=[]\;',./].
Email address	Enter the email address of the administrator account, which is used to log into the NCC. This field is read-only if you are editing an existing account.
Description	Enter a description for this administrator. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Validity	Specify how long the account is valid. Choices are: **Never expire** – select this if the account never expire. **Expire on** – select this to specify the date the account can no longer access the organization. Select **Delete this admin when expired** to remove this account from the administrator list when the **Expire on** date has been reached. Otherwise, this account will remain on the administrator list with an inactivated status.
Assign privilege	
Organization only	Select this to assign the account privileges to all the sites in the selected organizations. Only organizations belonging to an MSP account with full privileges can be selected.
Organization	Select one or more organizations to assign the account privileges to. Note: If no organization is selected, then the administrator cannot access any organization until an organization is assigned full privileges.

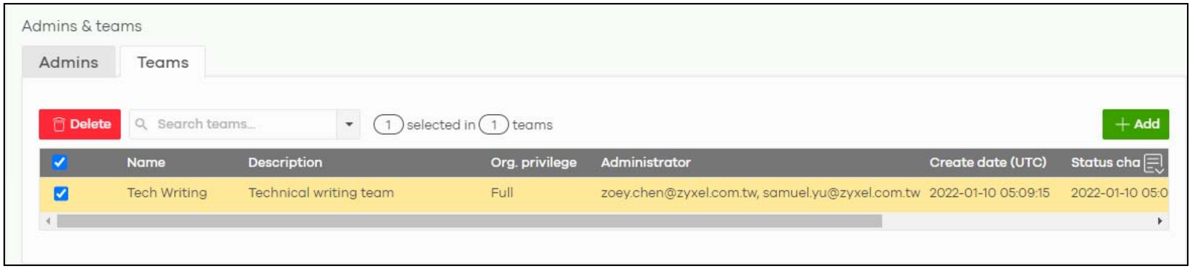
Table 226 MSP cross-org > MSP cross-org manage > Admins & teams > Admins: Create/Update administrator (continued)

LABEL	DESCRIPTION
Privilege	Select the privileges the administrator has within the selected organizations. **Full**: the administrator can edit settings, create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula Devices in the organization. **Read-only:** the administrator account has no write access to the organization, but can be a site administrator.
Activate	Select **Yes** to enable the account or **No** to temporarily disable the account.
🗑	Click the remove icon to delete the current set of admin privileges.
Add	Add administrator privileges for an organization.
Sites of an organization	Select this to assign the account privileges to the site(s) in the selected organization. Only organizations belonging to an MSP account with full privileges can be selected.
Organization	Select an organization to assign the account privileges to.
Sites	Select one or more sites to assign the account privileges to.
Site privilege	Select the privileges the administrator has within the selected sites. **Full**: the administrator can edit settings, create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula Devices in the site. **Read-only:** the administrator account has no write access to the site, but can be a site administrator. **Monitor-only**: the administrator can view the site's monitor pages for Nebula Access Points, Ethernet Switches, and Security Appliances only. The configuration pages are hidden from view. **Installer**: the administrator can register Nebula Devices at this site. **Guest Ambassador**: the administrator can create, remove or manage guest accounts using the **Cloud authentication** screen.
Activate	Select **Yes** to enable the account or **No** to temporarily disable the account.
🗑	Click the remove icon to delete the current set of admin privileges.
Add	Add administrator privileges for the site(s) in an organization.
Close	Click this button to exit this screen without saving.
Create admin/ Update admin	Click this button to save your changes and close the screen.

14.3.4 Teams Screen

The team screen allows you to assign administrator privileges to a group of NCC accounts (a team). To access this screen, click **MSP cross-org** > **MSP cross-org manage** > **Admins & teams** > **Teams**.

Figure 293 MSP cross-org > MSP cross-org manage > Admins & teams > Teams



☑	Name	Description	Org. privilege	Administrator	Create date (UTC)	Status cha
☑	Tech Writing	Technical writing team	Full	zoey.chen@zyxel.com.tw, samuel.yu@zyxel.com.tw	2022-01-10 05:09:15	2022-01-10 05:0

The following table describes the labels in this screen.

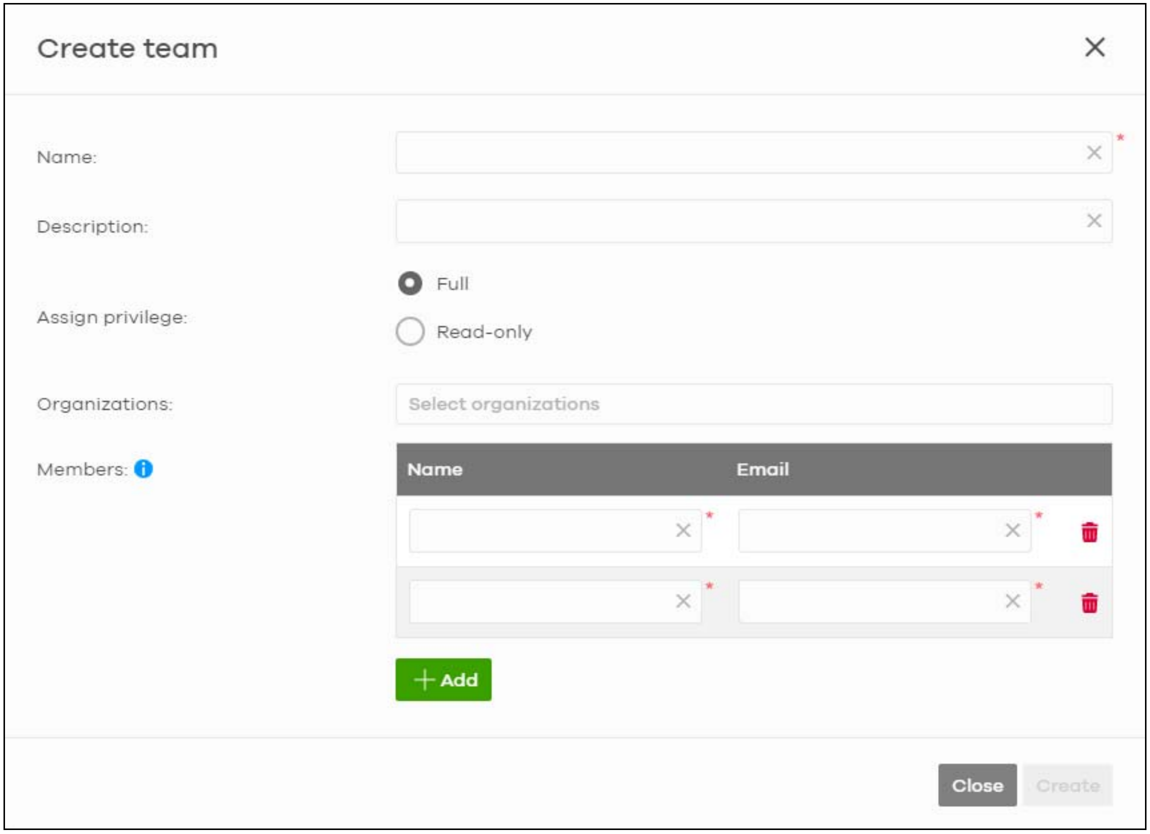
Table 227 MSP cross-org > MSP cross-org manage > Admins & teams > Teams

LABEL	DESCRIPTION
Delete	Click this button to remove the selected teams.
Search	Specify your desired filter criteria to filter the list of teams.
N teams	This shows the number of teams (N) in the list.
Add	Click this button to create a new administrator team.
	Select an entry's checkbox to select a specific team. Otherwise, select the checkbox in the table heading row to select all teams.
Name	This shows the name of the team.
Description	This shows a description of the team.
Org. privilege	This shows the privileges the team has within the specified organizations. **Full**: the administrator can edit settings, create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula Devices in the organization. **Read-only:** the administrator account has no write access to the organization, but can be a site administrator.
Organization	This shows the names of the organizations in which the privileges apply.
Administrator	This shows a list of the administrators in the team.
Create date (UTC)	This shows the date and time the team was created.
Status change date (UTC)	This shows the last date and time the team status was changed.
Creator	This shows the name of the MSP user account that added the privilege settings.
▤	Click this icon to display a greater or lesser number of configuration fields.

14.3.5 Create/Update Team

In the **MSP cross-org** > **MSP cross-org manage** > **Admins & teams** > **Teams** screen, click the **Add** button to add a new administrator team, or double-click an existing team entry to modify its settings.

Figure 294 MSP cross-org > MSP cross-org manage > Admins & teams > Teams: Create/Update team



Create team

Name: *

Description:

Assign privilege: ● Full ○ Read-only

Organizations: Select organizations

Members:

Name	Email
*	*
*	*

The following table describes the labels in this screen.

Table 228 MSP cross-org > MSP cross-org manage > Admins & teams > Teams: Create/Update team

LABEL	DESCRIPTION
Name	Enter a descriptive name for the team. Enter up to 15 characters in this field including special characters inside the square quotes [~!@#$%^&*()_+{}|:"<>?–=[]\;',./].
Description	Enter a description of the team, for example their role or membership. Enter up to 64 characters for this field including special characters inside the square quotes [~!@#$%^&*()_+{}|:"<>?–=[]\;',./].
Assign privilege	Select the privileges the team members have within the selected organizations. **Full**: Each member of the team can edit settings, create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula Devices in the organization. **Read-only:** Each member of the team has no write access to the organization, but can be a site administrator.
Organization	Select one or more organizations to assign the team privileges to. An organization can belong to multiple teams.
Members	
Name	Enter a descriptive name for the members. Enter up to 15 characters for this field including special characters inside the square quotes [~!@#$%^&*()_+{}|:"<>?–=[]\;',./].
Email address	Enter the email address of the members who can log into the NCC.
🗑	Click the remove icon to delete the current set of admin privileges.
Add	Add another NCC account to this team.

Table 228 MSP cross-org > MSP cross-org manage > Admins & teams > Teams: Create/Update team

LABEL	DESCRIPTION
Close	Click this button to exit this screen without saving.
Create/Update	Click this button to save your changes and close the screen.

14.4 Cross-org synchronization

The Cross-org synchronization screen allows you to copy settings or a site from one organization to another. You can also move Nebula Devices with its settings to another organization.

14.4.1 Cross-Org setting sync

Cross-org sync copies the following items from one organization to another organization:

- Organization-wide settings
- Administrators
- Cloud Authentication accounts (Users and MAC)
- Configuration templates

Your account must have **owner** or **organization-full** privileges in both source and destination organizations. When copying organization-wide settings, the following settings will not be overwritten if they are already configured in the destination organization:

- **Organization-wide** > **Organization-wide manage** > **Organization settings** > **Country**
- **Organization-wide** > **Organization-wide manage** > **Organization settings** > **Login IP ranges**
- Administrators privileges (when source and destination organizations have the same admin account)
- Cloud Authentication account privileges (when source and destination organizations have the same Cloud Authentication account)

When copying configuration templates:

- No sites are bound to the new template site.
- If the destination organization has a template with the same name, then the new template will have a number appended to the end of its name.

14.4.2 Cross-Org site clone

Cross-org site clone copies a site and all of its settings from one organization to another. Your account must have **owner** or **organization-full** privileges in both source and destination organizations.

If the destination organization has a site with the same name, then the new site will have a number appended to the end of its name.

The following table describes the Nebula Device (Access Point, Switch, Security Firewall) during cross-org site clone.

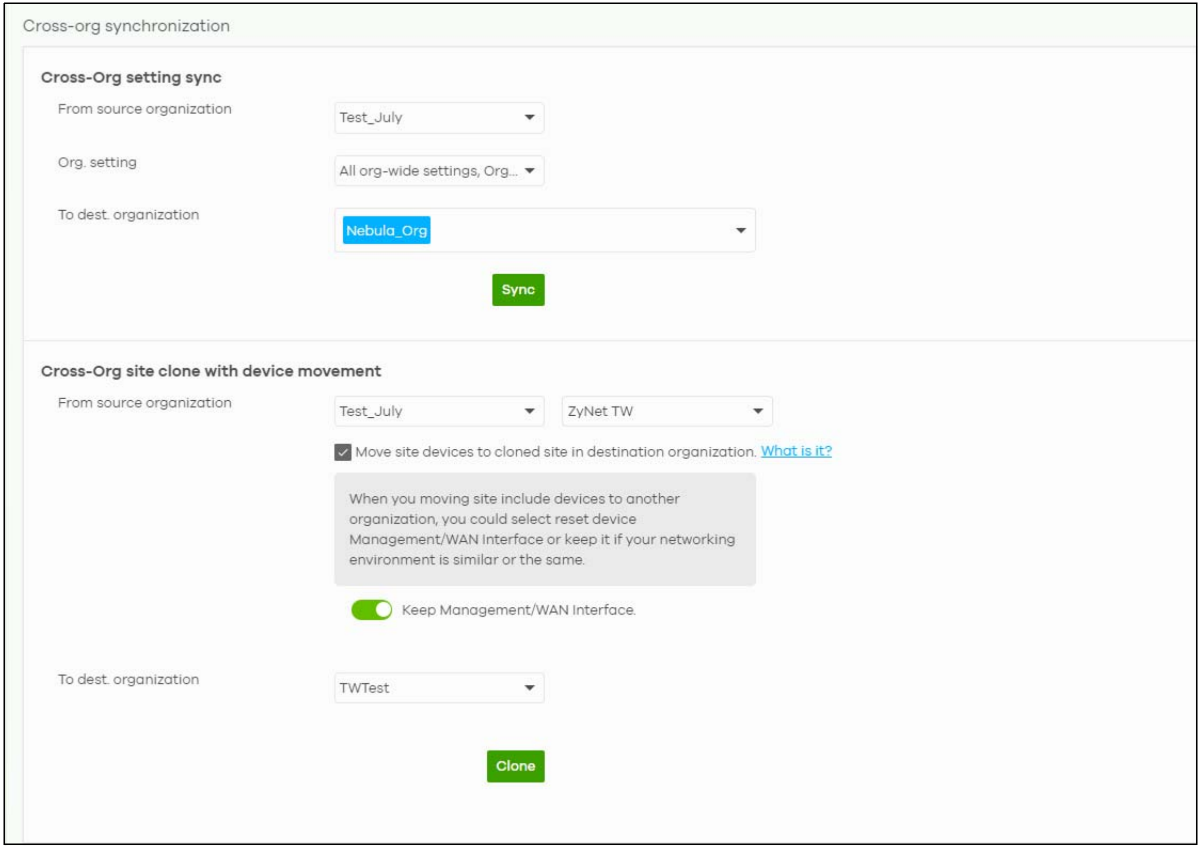
Table 229 Nebula Device Cross-org Site Clone

NEBULA DEVICE	CROSS-ORG SITE CLONE	MOVE NEBULA DEVICE TO CLONED SITE – ENABLED	KEEP MANAGEMENT/WAN INTERFACE – ENABLED
Access Point (AP)	When enabled: • AP site-wide configuration is cloned • Individual AP configuration is NOT cloned (for example, radio settings)	When enabled: AP site-wide configuration and individual AP configuration are cloned (for example, radio settings)	When enabled: AP site-wide configuration and individual AP configuration are cloned (for example, radio settings)
Switch	When enabled: • Switch site-wide configuration is cloned • Individual Switch configuration is NOT cloned (for example, IGMP) • Switch port configuration is NOT cloned	When enabled: • Switch site-wide configuration is cloned • Individual Switch configuration is cloned (for example, IGMP) • Switch port configuration is cloned	When enabled: • Switch site-wide configuration is cloned • Individual Switch configuration is cloned (for example, IGMP) • Switch port configuration is cloned
Security Firewall	When enabled, the site-to-site VPN settings are reset.	When enabled, the site-to-site VPN settings are reset.	When enabled, the site-to-site VPN settings are reset.

14.4.3 Cross-org synchronization Screen

Use this screen to configure cross-org synchronization and cross site clones.

Figure 295 MSP cross-org > MSP cross-org manage > Cross-org synchronization



Cross-org synchronization

Cross-Org setting sync

From source organization: Test_July

Org. setting: All org-wide settings, Org...

To dest. organization: Nebula_Org

Cross-Org site clone with device movement

From source organization: Test_July, ZyNet TW

☑ Move site devices to cloned site in destination organization. What is it?

When you moving site include devices to another organization, you could select reset device Management/WAN Interface or keep it if your networking environment is similar or the same.

Keep Management/WAN Interface.

To dest. organization: TWTest

The following table describes the labels in this screen.

Table 230 MSP cross-org > MSP cross-org manage > Cross-org synchronization

LABEL	DESCRIPTION
Cross-Org setting sync	
From source organization	Select the organization to copy settings from.
Org. setting	Select the settings that you want to copy from the source to the destination organization. Select **All org-wide settings** to copy everything.
To dest. organization	Select the organization to copy settings to.
Sync	Click this to copy the selected settings from the source to the destination organization.
Cross-Org site clone with device movement	
From source organization	Select the organization to copy settings from. Then select one or more sites. Select **All sites** to copy all sites from the source to the destination organization. Select **Move site devices to cloned site in destination organization** to include the Nebula Devices. Enable **Keep Management/WAN interface** to copy the WAN connection settings for the Nebula Devices to the destination organization.
To dest. organization	Select the organization to copy the selected sites to.
Clone	Click this to copy the selected organization and sites from the source to the destination organization.

14.5 Backup and Restore

Use these screens to back up your current Nebula Device's configurations to NCC, or restore a previously saved configuration. Click **MSP** > **MSP cross-org manage** > **Backup & restore** to access these screens.

Note: At the time of writing, you can do the following:
– In Cloud mode, back up a Security Firewall's running configuration to NCC and restore a running configuration from NCC to a Security Firewall
– In Cloud Monitoring mode, back up a Security Firewall's local Web Configurator settings to NCC and restore a local Web Configurator settings from NCC to a Security Firewall
– In Cloud mode, back up a Security Router's running configuration to NCC and restore a running configuration from NCC to a Security Router.
You cannot use the local Web Configurator settings in Cloud Monitoring mode to restore the running configuration of the Nebula Device in Cloud mode. Likewise, you cannot use the running configuration in Cloud mode to restore the local Web Configurator settings of the Nebula Device in Cloud Monitoring mode.

Note: A maximum of 10 backups are allowed per site. This includes the backups done in the **MSP** > **MSP cross-org manage** > **Backup & restore** and **Site-wide** > **Devices** > **Firewall**: **Live tools**: **Backup & Restore** screens. NCC will automatically remove the oldest backup after exceeding 10 backups.

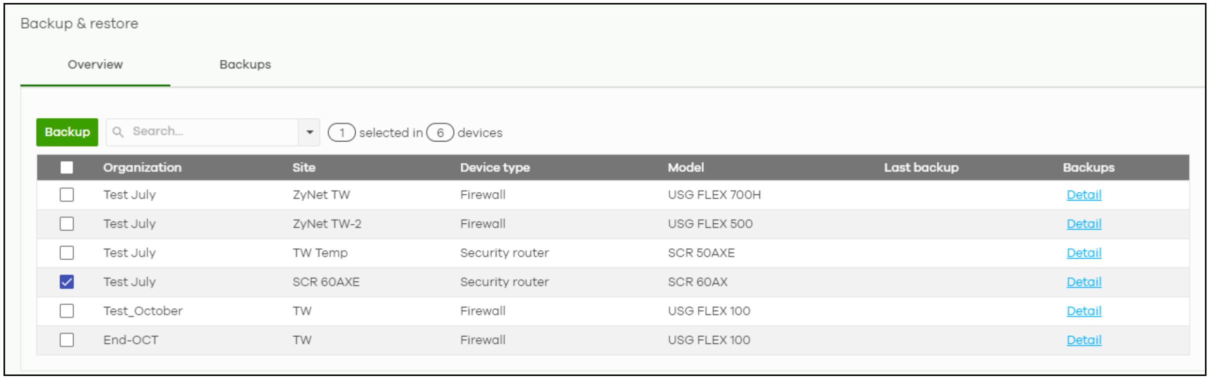
Note: A backup done in the **MSP** > **MSP cross-org manage** > **Backup & restore** screen is also added to the **Site-wide** > **Devices** > **Firewall**: **Live tools**: **Backup & Restore** screen.
A manual or scheduled back up done in the **Site-wide** > **Devices** > **Firewall**: **Live tools**: **Backup & Restore** screen is also added to the **MSP** > **MSP cross-org manage** > **Backup & restore** screen.

Note: The backups will be removed from NCC when the site it belongs to is deleted.

14.5.0.1 Backup and Restore Overview Screen

Use this screen to perform a backup or view a list of previous backups and the details. Click **MSP** > **MSP cross-org manage** > **Backup & restore** > **Overview** to access this screen.

Figure 296 MSP > MSP cross-org manage > Backup & restore > Overview



Backup & restore

Overview Backups

Backup | Search... | (1) selected in (6) devices

☐	Organization	Site	Device type	Model	Last backup	Backups
☐	Test July	ZyNet TW	Firewall	USG FLEX 700H		Detail
☐	Test July	ZyNet TW-2	Firewall	USG FLEX 500		Detail
☐	Test July	TW Temp	Security router	SCR 50AXE		Detail
☑	Test July	SCR 60AXE	Security router	SCR 60AX		Detail
☐	Test_October	TW	Firewall	USG FLEX 100		Detail
☐	End-OCT	TW	Firewall	USG FLEX 100		Detail

The following table describes the labels in this screen.

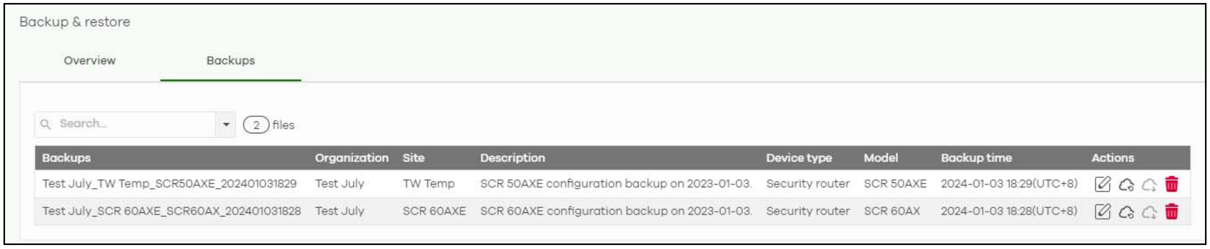
Table 231 MSP > MSP cross-org manage > Backup & restore > Overview

LABEL	DESCRIPTION
Backup	Click this button to create a new backup of the current configuration of the Nebula Device to the NCC.
Search	Select the filter criteria to filter the list of Nebula Devices.
N devices	This shows how many Nebula Devices (N) match the filter criteria and how many Nebula Devices of the selected type are created in total.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Organization	This shows the descriptive name of organization.
Site	This shows the descriptive name of site.
Device type	This shows the type of Nebula Device.
Model	This shows the model name of the Nebula Device.
Last backup	This shows the date and time the backup was saved on the NCC server.
Backups	Click **Detail** to go to the **Backups** screen. See the next section for details.

14.5.0.2 Backup and Restore Backups Screen

Use this screen to restore a backup to your Nebula Device. Click **MSP** > **MSP cross-org manage** > **Backup & restore** > **Backups** to access this screen.

Figure 297 MSP > MSP cross-org manage > Backup & restore > Backups



Backups	Organization	Site	Description	Device type	Model	Backup time	Actions
Test July_TW Temp_SCR50AXE_202401031829	Test July	TW Temp	SCR 50AXE configuration backup on 2023-01-03.	Security router	SCR 50AXE	2024-01-03 18:29(UTC+8)	
Test July_SCR 60AXE_SCR60AX_202401031828	Test July	SCR 60AXE	SCR 60AXE configuration backup on 2023-01-03.	Security router	SCR 60AX	2024-01-03 18:28(UTC+8)	

The following table describes the labels in this screen.

Table 232 MSP > MSP cross-org manage > Backup & restore > Backups

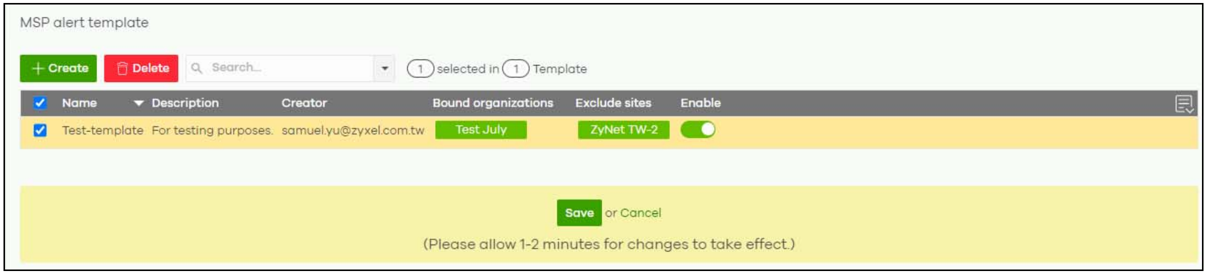
LABEL	DESCRIPTION
Search	Select the filter criteria to filter the list of backups.
N files	This shows how many backups (N) match the filter criteria and how many Nebula Devices of the selected type are created in total.
Backups	This shows the automatically generated filename of the backup. The format is "Organization name_Site name_Nebula Device model_backup date and time". Note: NCC hides the backup when all compatible Nebula Device(s) are removed from the site. Note: A hidden Security Appliance backup is displayed again when any model of a Security Appliance is added to the site.
Organization	This shows the descriptive name of the organization.
Site	This shows the descriptive name of the site.
Description	This shows the user-specified description entered during the backup.
Device type	This shows the type of Nebula Device.
Model	This shows the model name of the Nebula Device.
Backup time	This shows the date and time of the site, and when the backup was done.
Actions	Click the Edit icon to change the description. You can use alphanumeric and ()+/:=?!*#@$_%- characters, up to 512 characters. Click the Restore icon to restore a previously saved local GUI or Cloud configurations from NCC to the Nebula Device. Note: To restore Cloud configurations, the Nebula Device can be online or offline. To restore local GUI settings, the Nebula Device must be online. Click the Download icon to download the configuration file to your computer or laptop. Click the Delete icon to remove a previously saved local GUI or Cloud settings from NCC.

14.6 MSP Alert Templates

The MSP administrator can configure MSP alert template to monitor Nebula Devices for unexpected events (for example, online / offline events). This screen will list the alert templates you have created. See Section 14.6.1 on page 758 for details on creating an alert template.

To access this screen, click **MSP cross-org** > **MSP cross-org manage** > **Alert templates** in the navigation panel.

Figure 298 MSP cross-org > MSP cross-org manage > Alert templates



MSP alert template

1 selected in 1 Template

☑	Name	Description	Creator	Bound organizations	Exclude sites	Enable
☑	Test-template	For testing purposes.	samuel.yu@zyxel.com.tw	Test July	ZyNet TW-2	●

(Please allow 1-2 minutes for changes to take effect.)

The following table describes the labels in this screen.

Table 233 MSP cross-org > MSP cross-org manage > Alert templates

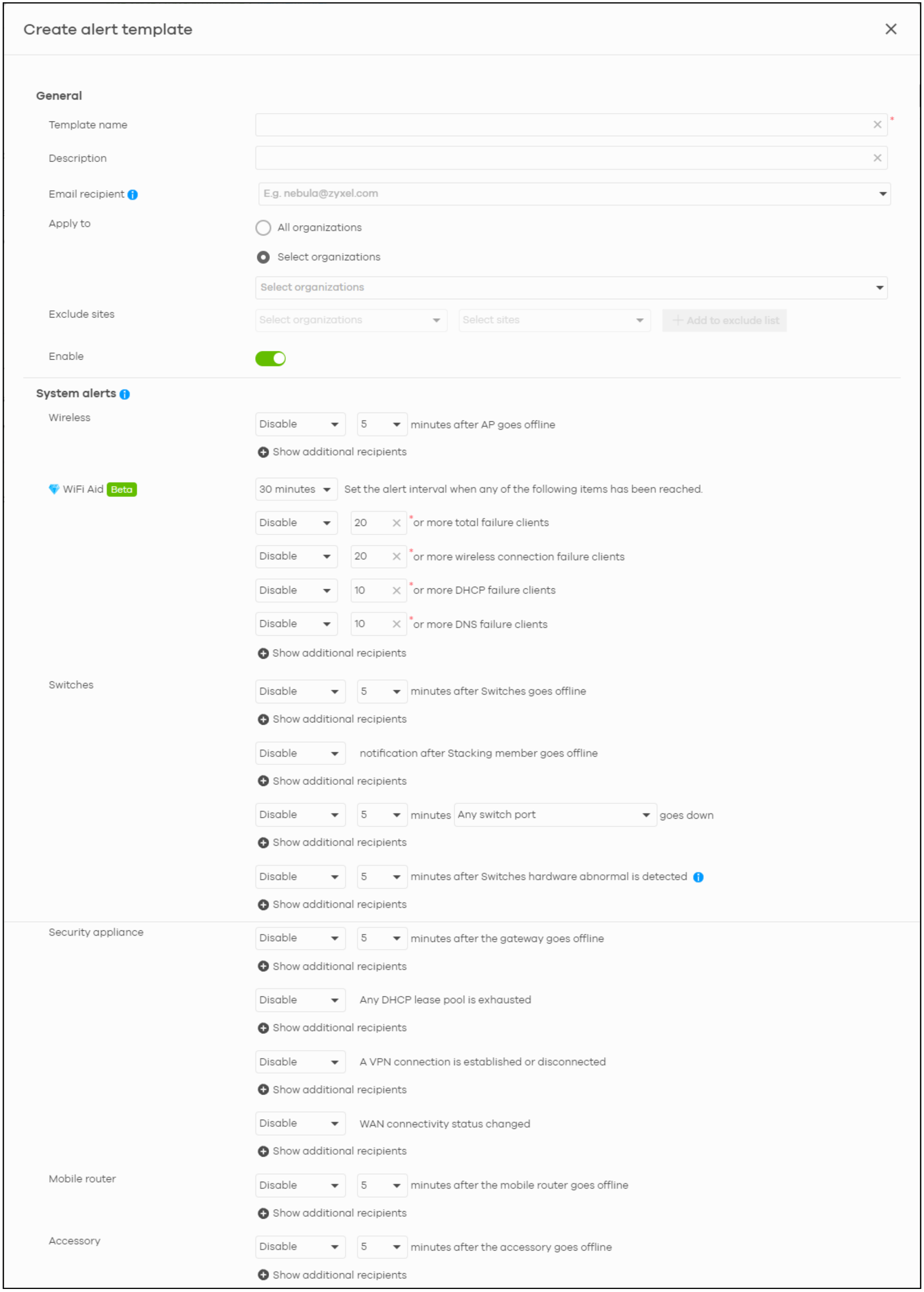
LABEL	DESCRIPTION
+ Create	Click this button to add a new alert template (see Section 14.6.1 on page 758).
Delete	Click this button to remove alert templates already created.
Search	Specify your desired search criteria to filter the list of alerts.
selected in	This shows the number of alerts that match your filter criteria after you perform a search.
Template	This shows the number of alert templates you have created.
Name	This shows a descriptive name of the alert template.
Description	This shows more details on the alert template.
Creator	This shows your email address.
Bound organizations	This shows **All organizations** or a list of the selected organizations to send alerts to.
Exclude sites	This shows the sites that will not receive any alerts.
Enable	Click this to activate the alert template.
Note: To edit the **Name**, **Description**, **Creator**, **Bound organizations**, and **Exclude sites** fields, just click the field and the **Update alert** screen will appear.	

14.6.1 Alert Settings

Use this screen to set which alerts are created and emailed, and set the email addresses to which an alert is sent. Click **MSP cross-org** > **MSP cross-org manage** > **Alert templates** > **Create** to access this screen.

Note: NCC's Smart Alert Engine uses knowledge of network topology and cross-device functionality to only generate alerts for unexpected events. This helps avoids unnecessary emails and notifications.
For example, an AP is receiving power from a PoE switch. If the AP loses power because its Ethernet cable is disconnected, NCC generates an alert. If the AP loses power because the switch has a PoE schedule that disables power to the AP, NCC does not generate an alert.

Figure 299 MSP cross-org > MSP cross-org manage > Alert templates > Create/Update alert



Create alert template

General

Template name: *

Description:

Email recipient: E.g. nebula@zyxel.com

Apply to: ○ All organizations

● Select organizations

Select organizations

Exclude sites: Select organizations | Select sites | + Add to exclude list

Enable: On

System alerts

Wireless: Disable | 5 minutes after AP goes offline

Show additional recipients

WiFi Aid Beta: 30 minutes. Set the alert interval when any of the following items has been reached.

Disable | 20 * or more total failure clients

Disable | 20 * or more wireless connection failure clients

Disable | 10 * or more DHCP failure clients

Disable | 10 * or more DNS failure clients

Show additional recipients

Switches: Disable | 5 minutes after Switches goes offline

Show additional recipients

Disable | notification after Stacking member goes offline

Show additional recipients

Disable | 5 minutes | Any switch port | goes down

Show additional recipients

Disable | 5 minutes after Switches hardware abnormal is detected

Show additional recipients

Security appliance: Disable | 5 minutes after the gateway goes offline

Show additional recipients

Disable | Any DHCP lease pool is exhausted

Show additional recipients

Disable | A VPN connection is established or disconnected

Show additional recipients

Disable | WAN connectivity status changed

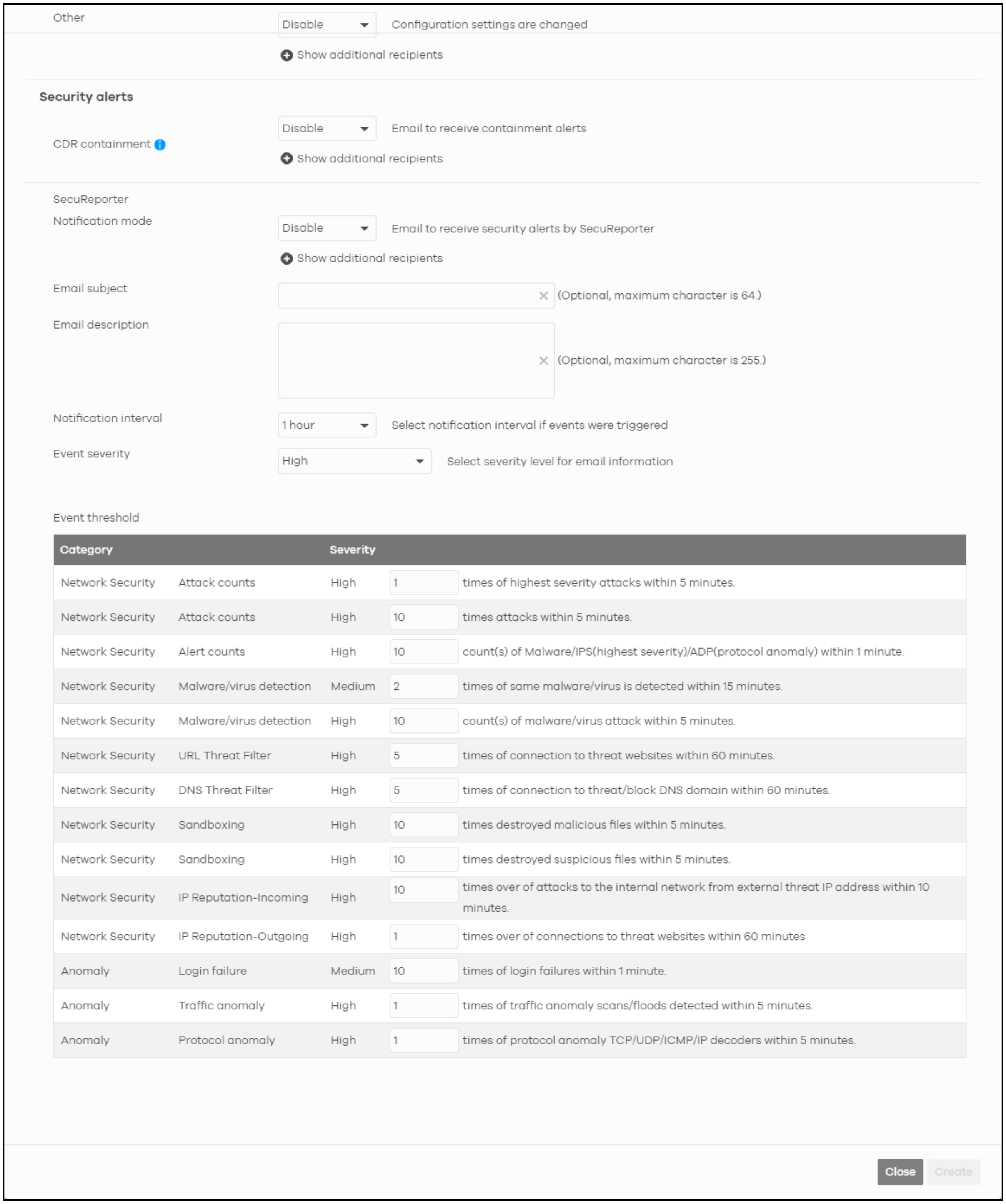
Show additional recipients

Mobile router: Disable | 5 minutes after the mobile router goes offline

Show additional recipients

Accessory: Disable | 5 minutes after the accessory goes offline

Show additional recipients



Other | Disable | Configuration settings are changed

Show additional recipients

Security alerts

CDR containment | Disable | Email to receive containment alerts

Show additional recipients

SecuReporter

Notification mode | Disable | Email to receive security alerts by SecuReporter

Show additional recipients

Email subject | (Optional, maximum character is 64.)

Email description | (Optional, maximum character is 255.)

Notification interval | 1 hour | Select notification interval if events were triggered

Event severity | High | Select severity level for email information

Event threshold

Category		Severity		
Network Security	Attack counts	High	1	times of highest severity attacks within 5 minutes.
Network Security	Attack counts	High	10	times attacks within 5 minutes.
Network Security	Alert counts	High	10	count(s) of Malware/IPS(highest severity)/ADP(protocol anomaly) within 1 minute.
Network Security	Malware/virus detection	Medium	2	times of same malware/virus is detected within 15 minutes.
Network Security	Malware/virus detection	High	10	count(s) of malware/virus attack within 5 minutes.
Network Security	URL Threat Filter	High	5	times of connection to threat websites within 60 minutes.
Network Security	DNS Threat Filter	High	5	times of connection to threat/block DNS domain within 60 minutes.
Network Security	Sandboxing	High	10	times destroyed malicious files within 5 minutes.
Network Security	Sandboxing	High	10	times destroyed suspicious files within 5 minutes.
Network Security	IP Reputation-Incoming	High	10	times over of attacks to the internal network from external threat IP address within 10 minutes.
Network Security	IP Reputation-Outgoing	High	1	times over of connections to threat websites within 60 minutes
Anomaly	Login failure	Medium	10	times of login failures within 1 minute.
Anomaly	Traffic anomaly	High	1	times of traffic anomaly scans/floods detected within 5 minutes.
Anomaly	Protocol anomaly	High	1	times of protocol anomaly TCP/UDP/ICMP/IP decoders within 5 minutes.

The following table describes the labels in this screen.

Table 234 MSP cross-org > MSP cross-org manage > Alert templates > Create/Update alert

LABEL	DESCRIPTION
General	
Template name	Enter a descriptive name for the alert template (up to 64 alphanumeric characters including spaces).

Table 234 MSP cross-org > MSP cross-org manage > Alert templates > Create/Update alert (continued)

LABEL	DESCRIPTION
Description	Enter more details of the alert template (up to 64 alphanumeric characters including spaces).
Email recipient	Enter the email addresses to which you want to send alerts.
Apply to	Select **All organizations** or specify the selected organizations to send alerts to.
Exclude sites	Select the sites in organizations that will not receive any alerts.
Enable	Click this to activate the alert template.
System alerts	
Notification Type	For each alert, you can set how to receive alert notifications: • **Email**: Alert notifications are sent by email to configured recipients. • **In-app Push**: Alert notifications are sent to site administrators who are logged into the Nebula Mobile app. This type of notification is not available for some features. • **Both**: Alert notifications are sent by email and app notification. • **Disable**: No alerts are sent.
Show additional recipients	Add additional user accounts who will receive email and in-app notifications for the alert.
Hide additional recipients	Do not show the additional user accounts who will receive email and/or in-app notifications for the alert.
System Alerts	
Wireless	Specify how long in minutes the NCC waits before generating and sending an alert when an access point goes offline.
WiFi Aid	Specify how long (15/30 minutes / 1 hour) the NCC waits before generating and sending an alert. Select the items to have the NCC generate and send an alert by email when the following events has reached the threshold (maximum 999): • WiFi clients with failed connection attempts (WiFi connection / DHCP failures / DNS failures). • WiFi clients with failed WiFi connection attempts. • WiFi clients with DHCP failures. • WiFi clients with DNS failures.
Switches	Specify how long in minutes (5/10/15/30/60) the NCC waits before generating and sending an alert when a port or a Switch or a stacking member goes offline, when the Switch temperature rises above the threshold, or the fan is functioning above the normal speed.
Security appliance	Specify how long in minutes the NCC waits before generating and sending an alert when the following events occur: • A security firewall, security gateway, or security router goes offline. • Any DHCP pool on the security firewall, security gateway, or security router runs out of IP addresses to assign. • A VPN connection to or from the security firewall, security gateway, or security router is created or terminated. • The WAN connectivity goes offline.
Mobile router / Accessory	Specify how long in minutes the NCC waits before generating and sending an alert when a mobile router or accessory goes offline.
Other	Specify whether to send an alert each time configuration settings are changed.
Security alerts	
CDR containment	Specify whether to send an alert each time a CDR block or containment action is triggered.
Show additional recipients	Add additional user accounts who will receive email and in-app notifications for the alert.
SecuReporter	

Table 234 MSP cross-org > MSP cross-org manage > Alert templates > Create/Update alert (continued)

LABEL	DESCRIPTION
Notification mode	Select whether to receive email security reports from SecuReporter.
Show additional recipients	Add additional user accounts who will receive email and in-app notifications for the alert.
Email subject	Enter an email title here.
Email description	Enter a description of the emails to be sent here. For example, maybe these emails are just for high severity events.
Notification interval	Specify how often to receive a SecuReporter report. If no security events were triggered, SecuReporter will not send a report.
Event severity	Select the severity level of events that will be included in each report.
Event threshold	This table lists the events that trigger SecuReporter security alerts. You can set the alert threshold. For example, X count(s) of malware/virus attack within 5 minutes means SecuReporter includes a report in the email if the total number of combined malware and virus detection events exceed X within a 5 minute time period.

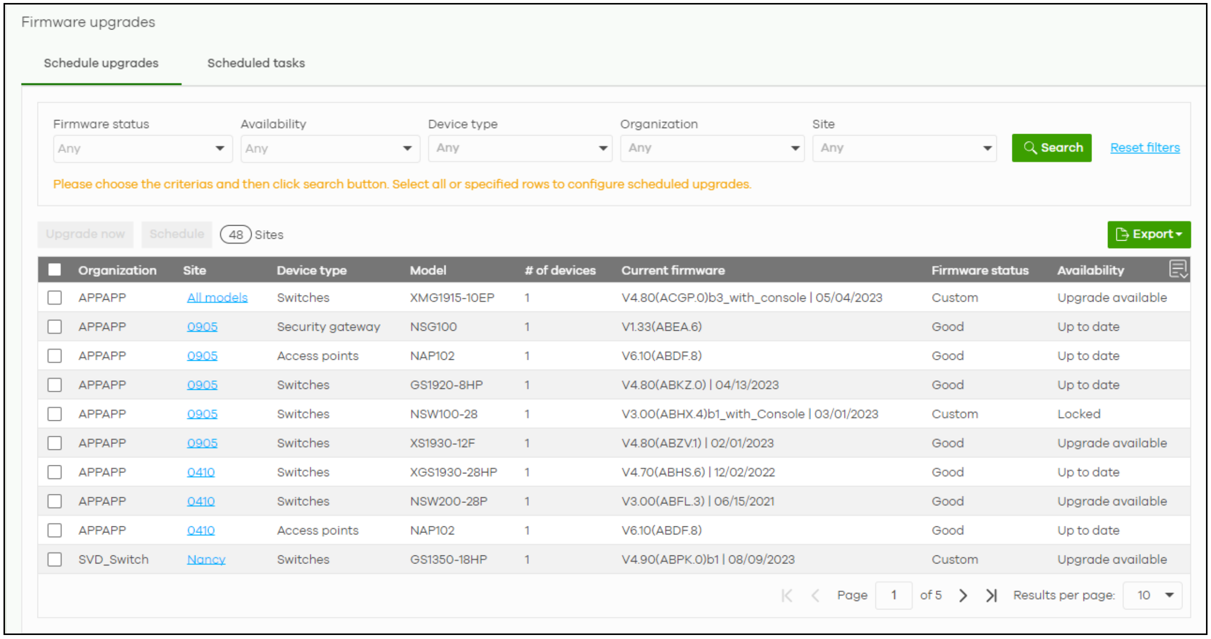
14.7 Firmware Upgrades

Use these screens to upgrade the firmware or schedule firmware upgrades for Nebula Devices in different organizations and different sites. Click **MSP** > **MSP cross-org manage** > **Firmware upgrades** to access the screens.

14.7.1 Schedule Upgrades Screen

Use this screen to view or schedule firmware upgrade for Nebula Devices within each organization and site. You can set different schedules for each Nebula Device models. Click **MSP** > **MSP cross-org manage** > **Firmware upgrades** > **Schedule upgrades** to access this screen.

Figure 300 MSP > MSP cross-org manage > Firmware upgrades > Schedule upgrades



Please choose the criterias and then click search button. Select all or specified rows to configure scheduled upgrades.

□	Organization	Site	Device type	Model	# of devices	Current firmware	Firmware status	Availability
□	APPAPP	All models	Switches	XMG1915-10EP	1	V4.80(ACGP.0)b3_with_console | 05/04/2023	Custom	Upgrade available
□	APPAPP	0905	Security gateway	NSG100	1	V1.33(ABEA.6)	Good	Up to date
□	APPAPP	0905	Access points	NAP102	1	V6.10(ABDF.8)	Good	Up to date
□	APPAPP	0905	Switches	GS1920-8HP	1	V4.80(ABKZ.0) | 04/13/2023	Good	Up to date
□	APPAPP	0905	Switches	NSW100-28	1	V3.00(ABHX.4)b1_with_Console | 03/01/2023	Custom	Locked
□	APPAPP	0905	Switches	XS1930-12F	1	V4.80(ABZV.1) | 02/01/2023	Good	Upgrade available
□	APPAPP	0410	Switches	XGS1930-28HP	1	V4.70(ABHS.6) | 12/02/2022	Good	Up to date
□	APPAPP	0410	Switches	NSW200-28P	1	V3.00(ABFL.3) | 06/15/2021	Good	Upgrade available
□	APPAPP	0410	Access points	NAP102	1	V6.10(ABDF.8)	Good	Up to date
□	SVD_Switch	Nancy	Switches	GS1350-18HP	1	V4.90(ABPK.0)b1 | 08/09/2023	Custom	Upgrade available

You can select Nebula Devices by firmware status and availability, device type, by organization and by site. For example, you can upgrade all model C Switches in Organization A and all model D APs in Organization B with **Critical** firmware status. Select **Critical** in **Firmware status**, **Switches** + **Access points** in **Device type**, A + B in **Organization**, then click **Search**.

Click the **Site** to view the **Site-wide** > **Configure** > **Firmware management** screen.

Note: This is a MSP Pack feature. If your MSP Pack license expires, scheduled firmware upgrades will still run.

14.7.2 Firmware Upgrade Priority

NCC prioritizes the different Nebula Device firmware upgrade schedules from highest to lowest as follows:

1. Individual Nebula Device upgrade schedule (set at **MSP** > **MSP cross-org manage** > **Firmware upgrades** > **Schedule upgrades**).
2. Individual Nebula Device upgrade schedule (set at **Organization-wide** > **Organization-wide manage** > **Firmware management** > **Devices**).
3. MSP, organization-wide or site-wide upgrade schedule. If you set all 3, the most recently set takes priority.
4. NCC default per-device upgrade schedule and default site-wide upgrade schedule. The default upgrade schedule is 14 days after new firmware is released.

The following table describes the labels in this screen.

Table 235 MSP > MSP cross-org manage > Firmware upgrades > Schedule upgrades

LABEL	DESCRIPTION
Firmware status	You can filter to display specific Nebula Devices by their firmware status. By default, only the Nebula Devices with the **Critical** firmware status are displayed. Select **Good** to display the Nebula Devices running a stable firmware and no immediate action is required. Select **Warning** to display the Nebula Devices with a newer firmware available and immediate action is recommended. The newer firmware may contain security enhancements, features, and performance improvements. Select **Critical** to display the Nebula Devices with a newer firmware available and immediate action is required. The existing firmware may have security vulnerabilities or lack key performance improvements. Select **Custom** to display the Nebula Devices running a firmware with specialized features unavailable to the general public.
Availability	Select to show the Nebula Devices with **Up to date** firmware, or with firmware update available for the Nebula Device (**Upgrade available**), or with a specific version of firmware installed by Zyxel customer support (**Locked**). By default, all available firmware is displayed (**Any**).
Device type	Select the type of Nebula Device. By default, all the Nebula Devices are displayed (**Any**).
Organization	Select an organization(s) managed by the MSP account. By default, all the organizations are displayed (**Any**).
Site	Select a site(s) in your organization. By default, all the sites are displayed (**Any**).
Search	Click this button after specifying your filter criteria in the **Firmware status**, **Availability**, **Device type**, **Organization** and **Site** fields.
Upgrade Now	Click this to upgrade the firmware on all selected organizations immediately. This button is selectable only when firmware update is available for the Nebula Devices for the selected organizations.
Schedule	Click this to run the wizard to set a specific date and time to upgrade the Nebula Devices firmware on the selected organizations. After running the wizard, the **Scheduled tasks** screen appears with the schedule you set. Nebula Devices are upgraded according to the time zone of the site they are in.
Export	Click this button to save the firmware schedule upgrade list as a CSV or XML file to your computer.
Note: Drag the following column headings to change the order. Click the column heading to change the sorting, ascending or descending order.	
*	Click this to select all the rows in this table.
Organization	This shows which organization the Nebula Device is in.
Site	This shows which site the Nebula Device is in. Click the site name to go to the site's **Firmware management**: **Overview**.
Device type	This shows the type of Nebula Device.
Model	This shows the model name of the Nebula Device.
# of devices	This shows the number of aggregated Nebula Device models in the organization for a particular upgrade schedule. For example, 10 NWA50AX in organization A will display as '10' in this field.
Current firmware	This shows the version number of the firmware the Nebula Device is currently running. It shows **N/A** when the Nebula Device goes offline and its firmware version is unavailable.

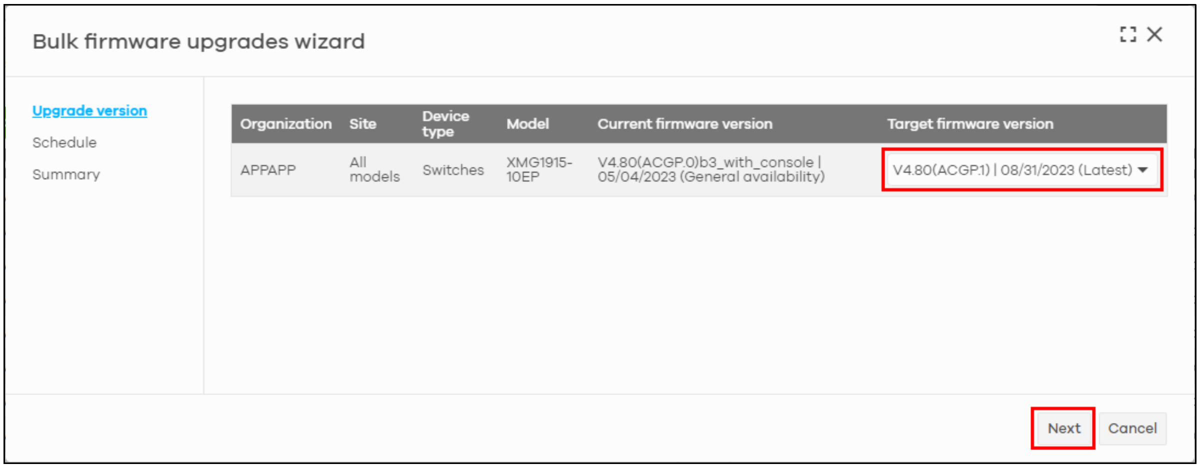
Table 235 MSP > MSP cross-org manage > Firmware upgrades > Schedule upgrades (continued)

LABEL	DESCRIPTION
Firmware status	This shows the status of the Nebula Device's firmware. • **Good**: The Nebula Device is running a stable firmware and no immediate action required. • **Warning**: A newer firmware is available for the Nebula Device, and immediate action is recommended. The newer firmware may contain security enhancements, features, and performance improvements. • **Critical**: A newer firmware is available for the Nebula Device, and immediate action is required. The existing firmware may have security vulnerabilities or lack key performance improvements. • **Custom**: The Nebula Device is running a firmware with specialized features unavailable to the general public.
Availability	This shows whether the firmware on the Nebula Device is **Up to date**, there is firmware update available for the Nebula Device (**Upgrade available**), or Zyxel customer support has installed a specific version of firmware (**Locked**).
☰	Click this icon to show and hide columns in the table.

14.7.3 Bulk Firmware Upgrade Wizard

Use this wizard to set a specific date and time to upgrade firmware to the selected Nebula Devices. Follow the steps below to use the wizard.

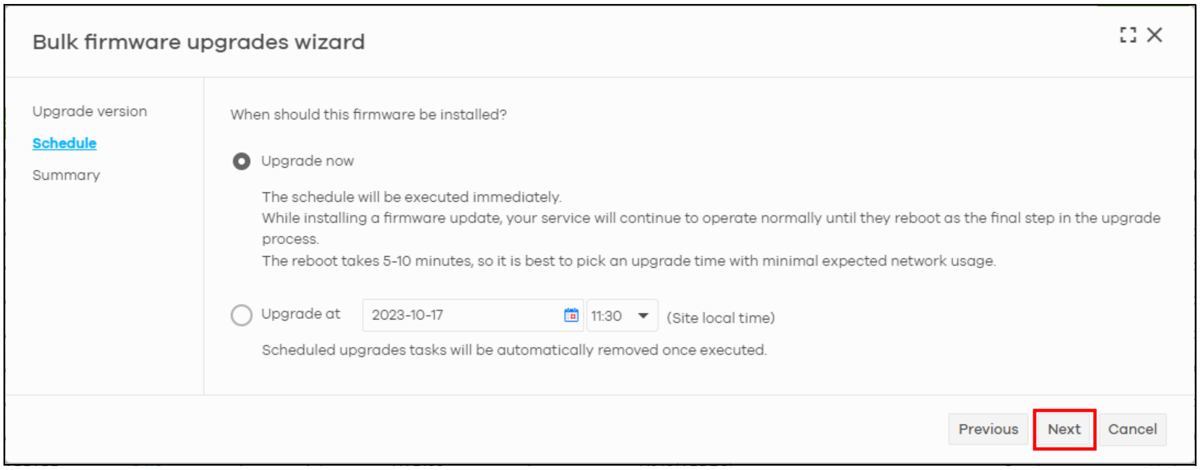
1 Click **MSP** > **MSP cross-org manage** > **Firmware upgrades** > **Schedule**. Select the **Target firmware version**, then click **Next**.



Bulk firmware upgrades wizard

Organization	Site	Device type	Model	Current firmware version	Target firmware version
APPAPP	All models	Switches	XMG1915-10EP	V4.80(ACGP.0)b3_with_console | 05/04/2023 (General availability)	V4.80(ACGP.1) | 08/31/2023 (Latest)

2 You can set a time to upgrade firmware for your Nebula Devices to overwrite the site-wide settings by selecting **Upgrade now** to upgrade immediately. If you do not want to upgrade the firmware immediately, you can choose **Upgrade at** to set up a specific date and time for a one time upgrade. The date and time are based on the site's local time zone. Then, click **Next**.



Bulk firmware upgrades wizard

When should this firmware be installed?

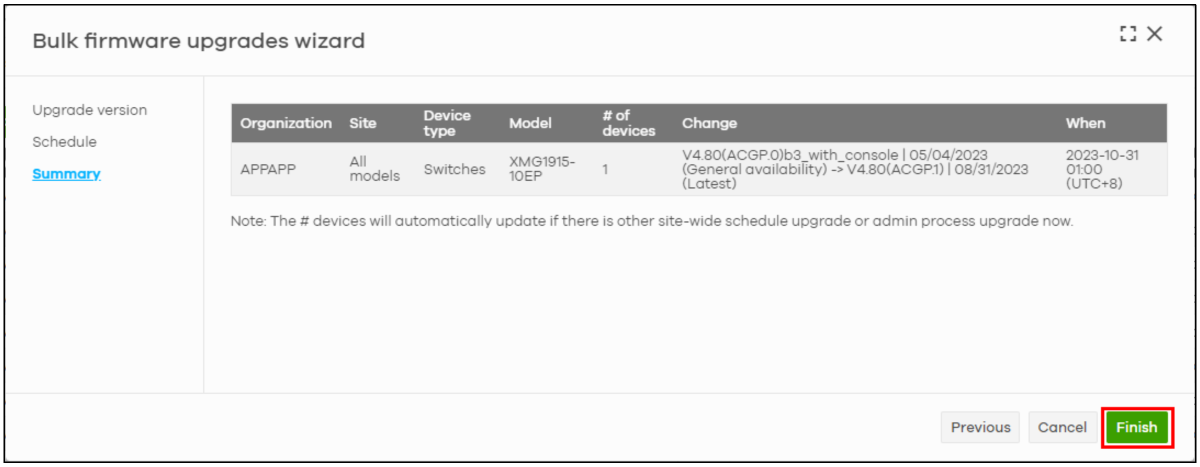
● Upgrade now

The schedule will be executed immediately.
While installing a firmware update, your service will continue to operate normally until they reboot as the final step in the upgrade process.
The reboot takes 5-10 minutes, so it is best to pick an upgrade time with minimal expected network usage.

○ Upgrade at 2023-10-17 11:30 (Site local time)

Scheduled upgrades tasks will be automatically removed once executed.

3 The **Summary** screen appears. Click **Finish** to exit the wizard.



Bulk firmware upgrades wizard

Organization	Site	Device type	Model	# of devices	Change	When
APPAPP	All models	Switches	XMG1915-10EP	1	V4.80(ACGP.0)b3_with_console | 05/04/2023 (General availability) -> V4.80(ACGP.1) | 08/31/2023 (Latest)	2023-10-31 01:00 (UTC+8)

Note: The # devices will automatically update if there is other site-wide schedule upgrade or admin process upgrade now.

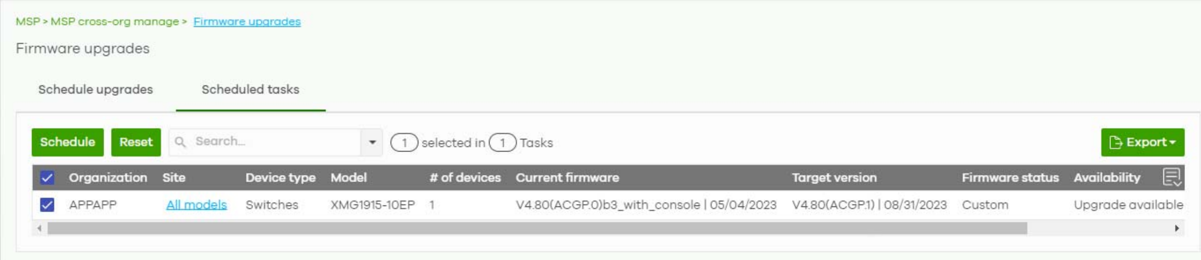
14.7.4 Scheduled Tasks Screen

Use this screen to change/reset to default the firmware upgrade schedule for the Nebula Devices. Click **MSP** > **MSP cross-org manage** > **Firmware upgrades** > **Scheduled tasks** to access this screen.

Note: You can change a scheduled task anytime before execution. After execution scheduled task(s) are removed.

Note: Changes to the **Site-wide** > **Configure** > **Firmware management** settings will be applied automatically to the **Scheduled tasks** screens. For example, when you upgrade a Nebula Device firmware to the latest version using the site-wide **Firmware management** screen, this Nebula Device will be removed automatically from the count for **# of devices**.

Figure 301 MSP > MSP cross-org manage > Firmware upgrades > Scheduled tasks



☑	Organization	Site	Device type	Model	# of devices	Current firmware	Target version	Firmware status	Availability
☑	APPAPP	All models	Switches	XMG1915-10EP	1	V4.80(ACGP.0)b3_with_console | 05/04/2023	V4.80(ACGP.1) | 08/31/2023	Custom	Upgrade available

The following table describes the labels in this screen.

Table 236 MSP > MSP cross-org manage > Firmware upgrades > Scheduled tasks

LABEL	DESCRIPTION
Schedule	Click this to run the wizard to set a specific date and time to upgrade firmware to Nebula Devices in the selected organizations and sites. Note: Nebula Devices are upgraded according to the time zone of the site they are in.
Reset	Select one or more Nebula Devices, and then click **Reset** to remove the Nebula Devices from the scheduled task list. The Nebula Devices will follow the site-wide firmware management settings.
Organization/Site/ Device type/Model/ Target version/ Firmware status/ Availability	Specify your desired filter criteria to filter the list of Nebula Devices.
Export	Click this button to save the firmware upgrade scheduled tasks list as a CSV or XML file to your computer.
Note: Drag the following column headings to change the order. Click the column heading to change the sorting, ascending or descending order.	
*	Click this to select all the rows in this table.
Organization	This shows which organization the Nebula Device is in.
Site	This shows which site the Nebula Device is in. Click the site name to go to the site's **Firmware management**: **Overview**.
Device type	This shows the type of Nebula Device.
Model	This shows the model name of the Nebula Device.
# of devices	This shows the number of Nebula Devices in the organization for a particular **Schedule status**. Click this to change the schedule.
Current firmware	This shows the version number of the firmware the Nebula Device is currently running. It shows **N/A** when the Nebula Device goes offline and its firmware version is not available.
Target version	This shows the version number of the new firmware for the Nebula Device.

Table 236   MSP > MSP cross-org manage > Firmware upgrades > Scheduled tasks (continued)

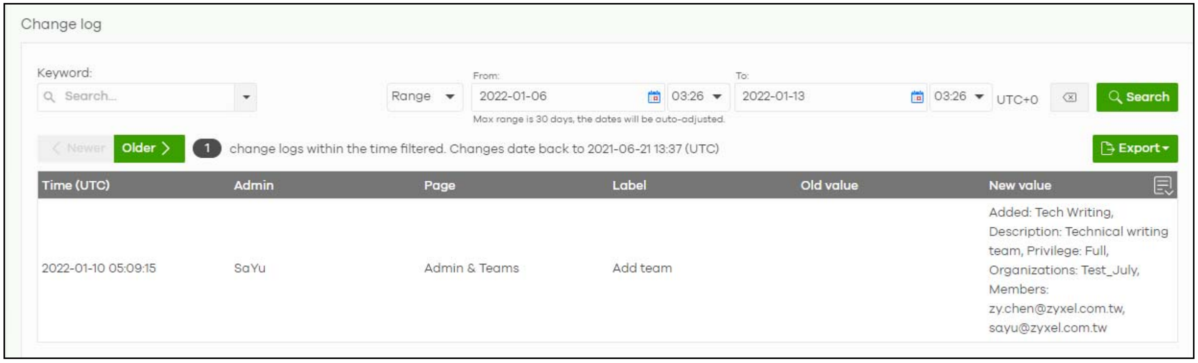
LABEL	DESCRIPTION
Firmware status	The status shows **Good** if the Nebula Device is running a stable firmware and no immediate action is required. The status shows **Warning** if a newer firmware is available and immediate action is recommended. The newer firmware may contain security enhancements, new features, and performance improvements. The status shows **Critical** if a newer firmware is available and immediate action is required. The firmware may have security vulnerabilities or lack key performance improvements. The status shows **Custom** if the Nebula Device is running a firmware with specialized features unavailable to the general public. The status changes to **Upgrading...** after you click **Upgrade Now** to install the firmware immediately.
Availability	This shows whether the firmware on the Nebula Device is **Up to date**, there is firmware update available for the Nebula Device (**Upgrade available**), or a specific version of firmware installed by Zyxel customer support (**Locked**).
Schedule	This shows the date and time when a new firmware upgrade will occur. If there is no date nor time, it shows: • **Follow upgrade time** and the Nebula Device sticks to the site-wide schedule, or • **No** when the firmware on the Nebula Device is up-to-date, or • The Nebula Device goes offline and its firmware status is unavailable. A lock icon displays for a specific schedule created for the Nebula Device, which means upgrade of the Nebula Device firmware will not follow the time configured for all Nebula Devices in the site.
☰	Click this icon to display a greater or lesser number of configuration fields.

14.8 Change Log

Use this screen to view logged messages for changes in the **Admins & teams** and **Cross-org synchronization** screens. Click **MSP cross-org** > **MSP cross-org manage** > **Change log** to access this screen.

When the log is full, it deletes older entries one by one to make room for newer ones.

Figure 302   MSP cross-org > MSP cross-org manage > Change log



Change log

Keyword: Search...

Range

From: 2022-01-06 03:26

To: 2022-01-13 03:26 UTC+0

Max range is 30 days, the dates will be auto-adjusted.

1 change logs within the time filtered. Changes date back to 2021-06-21 13:37 (UTC)

Time (UTC)	Admin	Page	Label	Old value	New value
2022-01-10 05:09:15	SaYu	Admin & Teams	Add team		Added: Tech Writing, Description: Technical writing team, Privilege: Full, Organizations: Test_July, Members: zy.chen@zyxel.com.tw, sayu@zyxel.com.tw

The following table describes the labels in this screen.

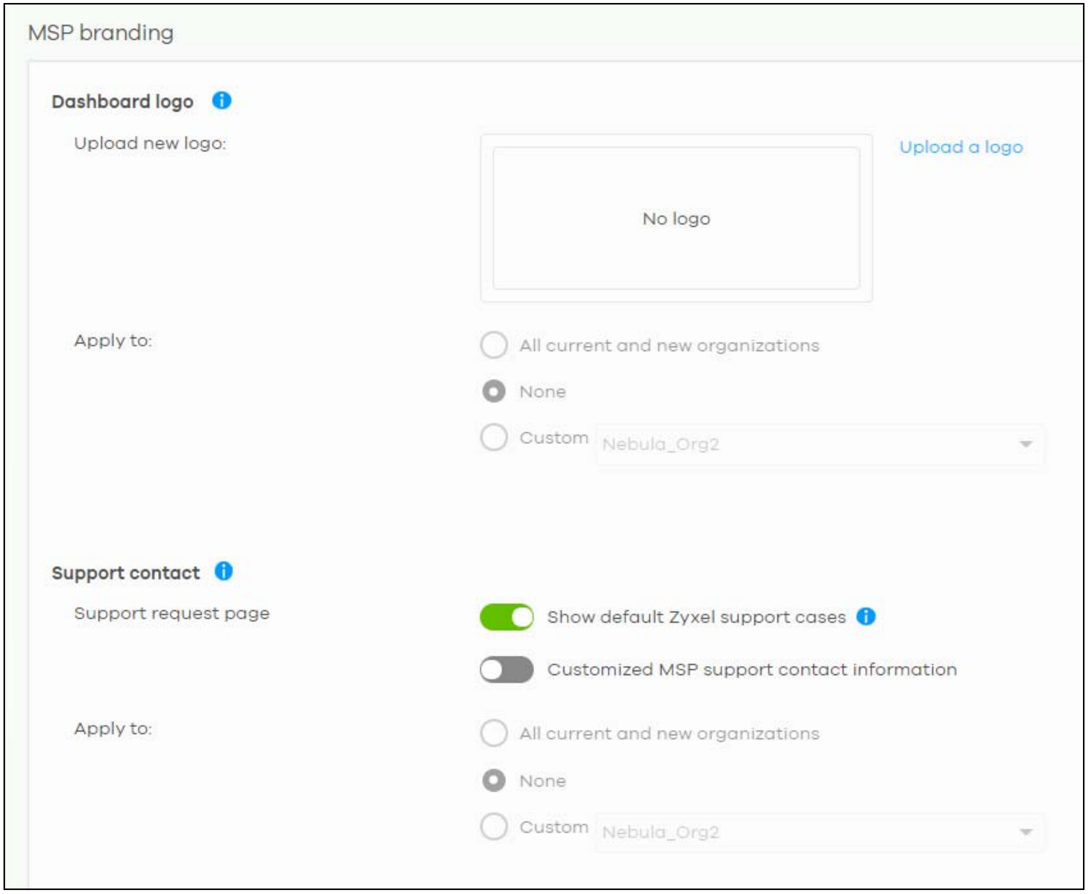
Table 237   MSP cross-org > MSP cross-org manage > Change log

LABEL	DESCRIPTION
Keyword	Enter a keyword or specify one or more filter criteria to filter the list of log entries.
Range/Before	Select a filtering option, set a date, and then click **Search** to filter log entries by date. **Range**: Display log entries from the first specified date to the second specified date. **Before**: Display log entries from the beginning of the log to the selected date.
Search	Click this to update the list of logs based on the search criteria.
Reset filters ⌫	Click this to return the search criteria to the previously saved time setting.
Newer/Older	Click to sort the log messages by most recent or oldest.
N change logs within the time filtered.	This shows the total number of the log messages that match the search criteria. It also shows the date and time the very first log was created.
Export	Click this button to download the log list as a CSV or XML file to your computer.
Time (UTC)	This shows the date and time in UTC+00:00 (or UTC+0) when the log was recorded. UTC is a standard time for use around the world (formerly known as Greenwich Mean Time or GMT). UTC is an international abbreviation that is neither French nor English. It means both "Temps Universel Coordonné" and "Coordinated Universal Time".
Page	This shows the name of the NCC menu in which the change was made.
Label	This shows the action that triggered the log entry
Old value	This shows the old setting or state that was overwritten with the new value.
New value	This shows the new setting or state.
☰	Click this icon to display a greater or lesser number of configuration fields.

14.9 MSP Branding

The **Dashboard logo** section of this screen allows organization owners to replace the Nebula Control Center logo with a new MSP logo. The **Support contact** section allows addition of a customized message or MSP contact information in the **Help** > **Support** request page. To access this screen, click **MSP cross-org** > **MSP cross-org manage** > **MSP branding**.

Figure 303   MSP cross-org > MSP cross-org manage > MSP branding



MSP branding

Dashboard logo

Upload new logo: No logo Upload a logo

Apply to:
○ All current and new organizations
● None
○ Custom Nebula_Org2

Support contact

Support request page
● Show default Zyxel support cases
○ Customized MSP support contact information

Apply to:
○ All current and new organizations
● None
○ Custom Nebula_Org2

The following table describes the labels in this screen.

Table 238   MSP cross-org > MSP cross-org manage > MSP branding

LABEL	DESCRIPTION
Dashboard logo	
Upload new logo	Click this to browse for the location of the image file to be used as your dashboard logo. • Allowed image file formats: JPG/JPEG, PNG, GIF. • Maximum image file size: 200 KB. • NCC converts the image file to a 160 x 44 pixel logo after uploading.
Replace this logo	Click this to browse for the location of the image file to replace your current dashboard logo.
Remove this logo	Click this to remove your current dashboard logo.
Apply to	Select **All current and new PRO organizations** to apply the logo to all Nebula Professional Pack organization dashboards. Select **Custom** to choose which Nebula Professional Pack organization to apply the logo. Select **None** if you only wish to upload the image file but will not apply it yet.
Support contact	
Support request page	
Show default Zyxel support cases	Select **ON** to display the standard Zyxel support contact information in the **Help** > **Support request** screen. Organization owners can choose to hide the default **Help** > **Support** screen section to only show their information to clients. But the organization owner and administrators with full privilege will still see the hidden default screen section.

Table 238 MSP cross-org > MSP cross-org manage > MSP branding (continued)

LABEL	DESCRIPTION
Customized MSP support contact information	Create your own support contact information. Enter up to 1000 characters in this field including special characters inside the square quotes [~!@#$%^&*()_+{}|:”<>?–=[]\;’,./].
Apply to	Select **All current and new PRO organizations** to apply the support contact information to all Nebula Professional Pack organization **Help** > **Support request** screens. Select **Custom** to choose which Nebula Professional Pack organization to apply the support contact information. Select **None** if you only wish to save the settings but will not apply it yet.

PART VI

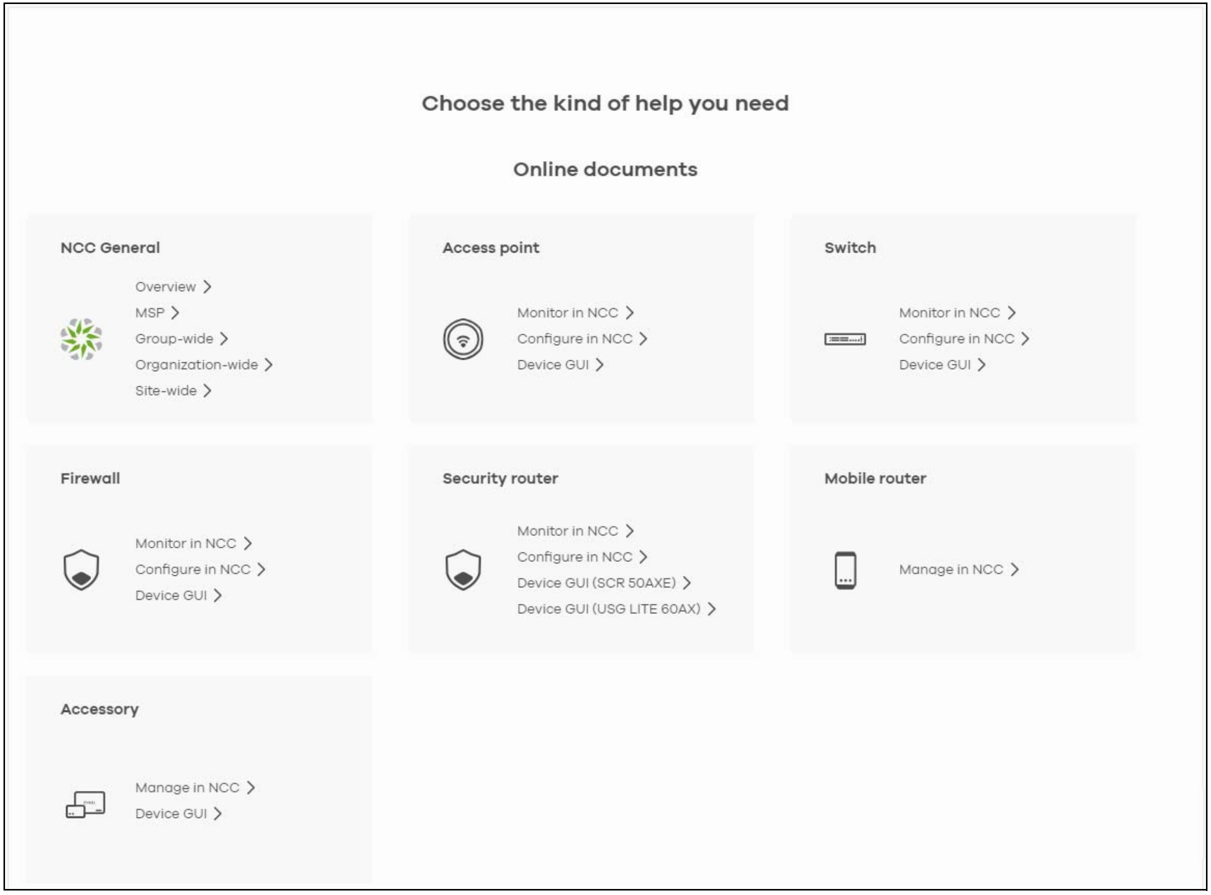
Troubleshooting and Appendices

CHAPTER 15
Help

15.1 Online documents

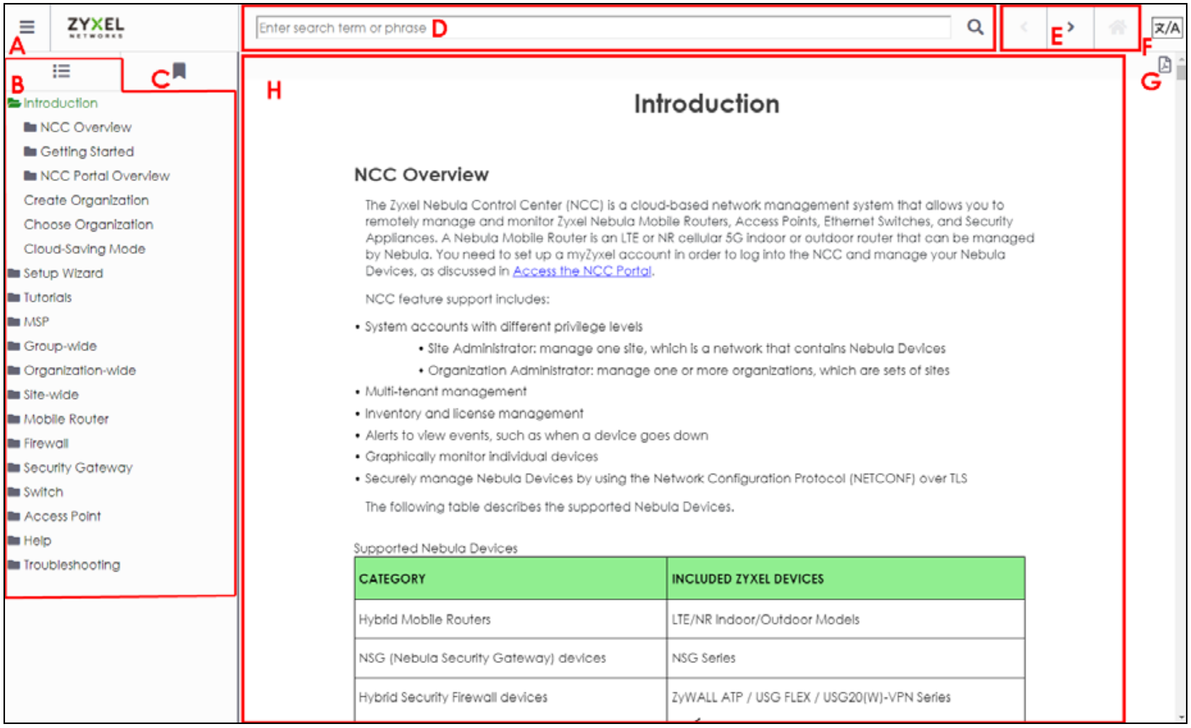
Click **Help** > **Online documents** to view the online help for NCC and NCC-compatible devices. For example, to view the Security Firewall Series configuration and hardware information, locate the online help under **Firewall**.

Figure 304 Help > Online documents



The following summarizes how to navigate the **Online documents** screen. The **Online documents** screen is divided into these parts:

Figure 305 Online Documents Overview



Introduction

NCC Overview

The Zyxel Nebula Control Center (NCC) is a cloud-based network management system that allows you to remotely manage and monitor Zyxel Nebula Mobile Routers, Access Points, Ethernet Switches, and Security Appliances. A Nebula Mobile Router is an LTE or NR cellular 5G indoor or outdoor router that can be managed by Nebula. You need to set up a myZyxel account in order to log into the NCC and manage your Nebula Devices, as discussed in Access the NCC Portal.

NCC feature support includes:

- System accounts with different privilege levels
  - Site Administrator: manage one site, which is a network that contains Nebula Devices
  - Organization Administrator: manage one or more organizations, which are sets of sites
- Multi-tenant management
- Inventory and license management
- Alerts to view events, such as when a device goes down
- Graphically monitor individual devices
- Securely manage Nebula Devices by using the Network Configuration Protocol (NETCONF) over TLS

The following table describes the supported Nebula Devices.

Supported Nebula Devices

CATEGORY	INCLUDED ZYXEL DEVICES
Hybrid Mobile Routers	LTE/NR Indoor/Outdoor Models
NSG (Nebula Security Gateway) devices	NSG Series
Hybrid Security Firewall devices	ZyWALL ATP / USG FLEX / USG20(W)-VPN Series

- A – Hide/Show the Contents Menu/Index
- B – Contents Menu
- C – Index
- D – Search Bar
- E – Navigation Buttons
- F – Google Translate Button
- G – Download Content PDF Button
- H – Content Page

The following table shows the description of the online documents parts.

Table 239 Online Documents Overview

LABEL	DESCRIPTION
A	Click to hide or show the contents menu and Index.
B	This shows a menu of the content topics. Click a topic heading to display its content in the main screen.
C	Click this to show the Index panel. Click an index entry to view its description.
D	Enter a keyword to search and display the related section(s) in the online document.
E	These are the navigation buttons. • Click the Previous button to display the previous chapter in the online document. • Click the Next button to display the next chapter in the online document. • Click the Home button to display the first chapter in the online document.
F	Click this to view the translated content page. You can click Google Translate anywhere in a content page, but you must be at the top of the content page to choose a language. The bottom right of the content page has a ‘Back to top’ arrow to get there.

Table 239 Online Documents Overview (continued)

LABEL	DESCRIPTION
G	Click this to download content in a PDF file. You must be at the top of the content page to click the PDF icon.
H	The content of the online document is displayed here.

15.2 Troubleshooting Tips

To find suggestions to solve problems you might encounter with NCC and Nebula Devices, go to Chapter 16 on page 780 for more information.

15.2.1 Firewall Information

Click **Help** > **Support tools** > **Firewall information** to view information required for firewall rules to allow management traffic between NCC and Nebula Devices on your sites. Click **Export** to export the information to a CSV or XML file.

Note: The **Firewall Information** page for a Security Gateway will show its FQDN (fully qualified domain name) and service ports. The FQDN is the complete domain name of Nebula Cloud Management on the Internet.

The following table shows the sample information required for firewall rules at the time of writing.

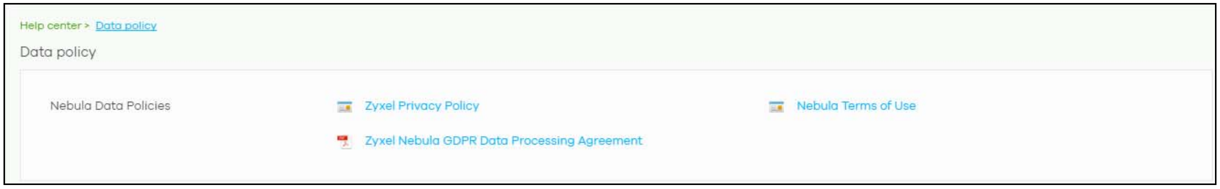
Table 240 Sample Information Required for Firewall Rules

SERVICE	FQDN	IP ADDRESS	PORT	PROTOCOL
Nebula Cloud Management (NETCONF)	d.nebula.zyxel.com	34.247.112.130, 52.210.12.1, 52.48.115.44, 54.73.103.137, 63.32.141.172, 63.35.107.114	4335 / 6667	TCP
Nebula Cloud Management	s.nebula.zyxel.com	Dynamic	443	TCP
Network Time Protocol	*.pool.ntp.org	Dynamic	123	UDP
Nebula Cloud Management (Zero Touch Provisioning)	d-a.nebula.zyxel.com	Dynamic	443	TCP
Nebula Cloud Management (Configure related service for USG FLEX series)	d-cp.nebula.zyxel.com	34.254.181.105, 52.212.114.133	4335	TCP
Nebula Cloud Management (Monitor related service for USG FLEX series)	d-mp.nebula.zyxel.com	52.18.204.70, 54.220.154.85, 63.34.155.16	443	TCP

15.2.2 Data Policy

Click **Help** > **Support tools** > **Data Policy** to view and download NCC GDPR data policy, privacy policy, and terms of use.

Figure 306 Help > Support tools > Data Policy



Help center > Data policy

Data policy

Nebula Data Policies

Zyxel Privacy Policy

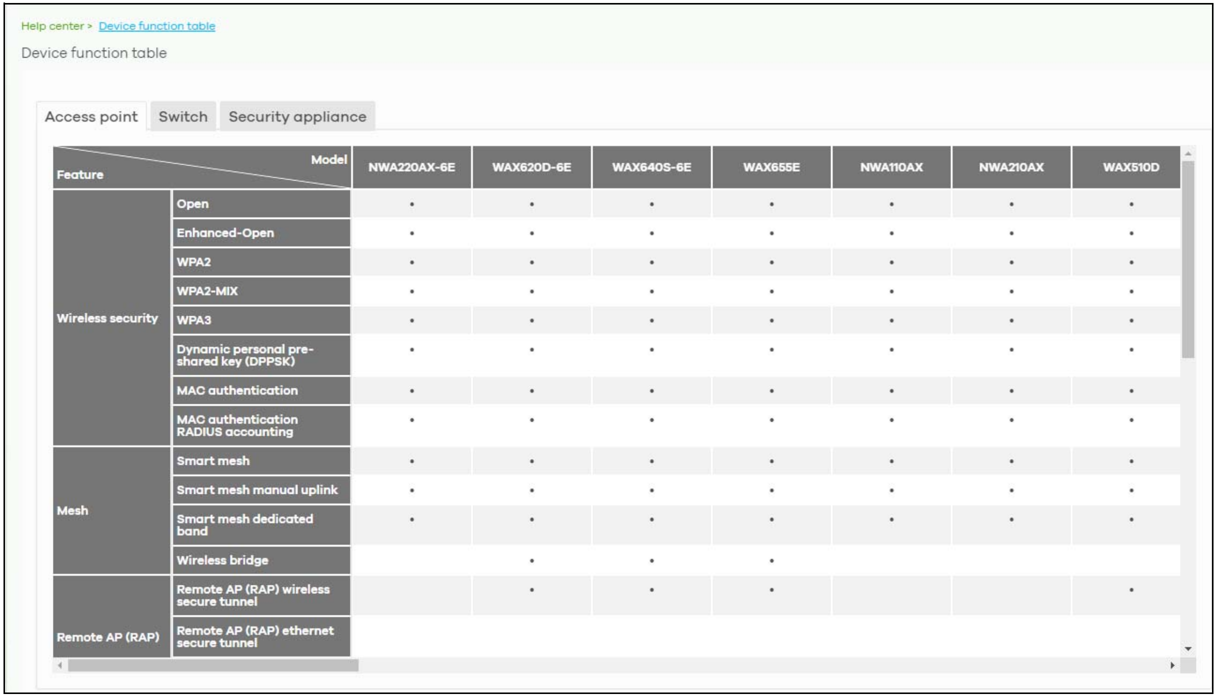
Zyxel Nebula GDPR Data Processing Agreement

Nebula Terms of Use

15.3 Device Function Table

Click **Help** > **Support tools** > **Device function table** to view a list of NCC-compatible Access Points, Switches, Security Gateway, and Security Firewall devices at the time of writing. The table also includes which features each Nebula Device supports.

Figure 307 Help > Support tools > Device function table



Help center > Device function table

Device function table

Feature	Model	NWA220AX-6E	WAX620D-6E	WAX640S-6E	WAX655E	NWA110AX	NWA210AX	WAX510D
Wireless security	Open	•	•	•	•	•	•	•
	Enhanced-Open	•	•	•	•	•	•	•
	WPA2	•	•	•	•	•	•	•
	WPA2-MIX	•	•	•	•	•	•	•
	WPA3	•	•	•	•	•	•	•
	Dynamic personal pre-shared key (DPPSK)	•	•	•	•	•	•	•
	MAC authentication	•	•	•	•	•	•	•
	MAC authentication RADIUS accounting	•	•	•	•	•	•	•
Mesh	Smart mesh	•	•	•	•	•	•	•
	Smart mesh manual uplink	•	•	•	•	•	•	•
	Smart mesh dedicated band	•	•	•	•	•	•	•
	Wireless bridge		•	•	•			
Remote AP (RAP)	Remote AP (RAP) wireless secure tunnel		•	•	•			•
	Remote AP (RAP) ethernet secure tunnel							

15.4 Support Forum

Click **Help** > **Still need help?** > **Support community** to go to Zyxel Nebula Community, where you can get the latest Nebula information and have conversations with other people by posting your messages.

15.5 Support Request

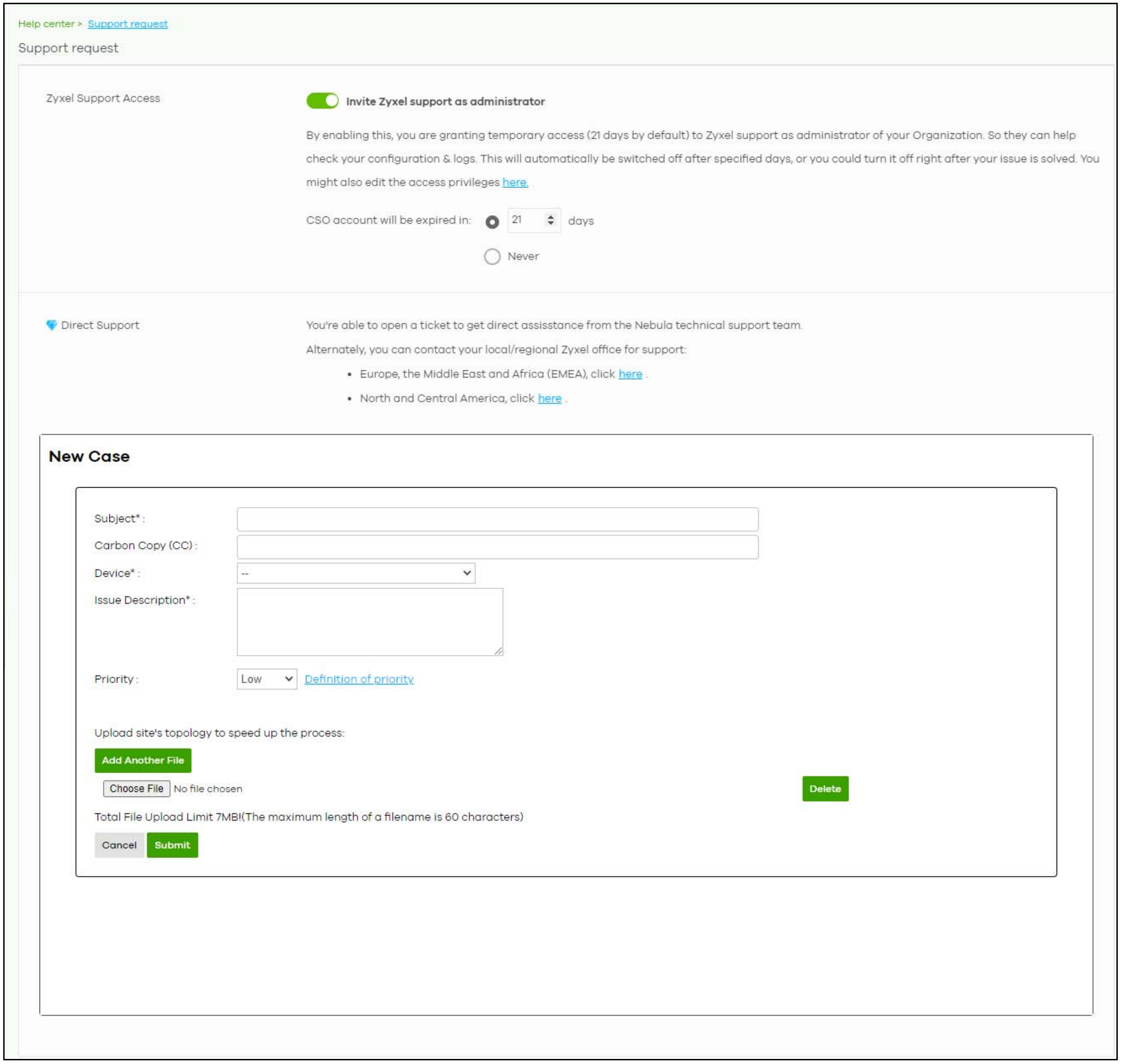
If you need Zyxel customer support to help you find answers and/or solve problems, you can submit a ticket through the NCC.

Note: It is suggested that you check this user’s guide first to seek help and then go to the Zyxel Nebula Community before you use this screen to send a ticket.

Click **Help** > **Still need help?** > **Support request** to access this screen. The screen varies depending on whether you select to view the ticket details or create a new ticket.

Note: **Direct Support** for opening a ticket to get direct assistance from the Nebula technical support team is only available for Nebula Pro Pack license.

Figure 308 Help > Still need help?: Support request



Help center > Support request

Support request

Zyxel Support Access

Invite Zyxel support as administrator

By enabling this, you are granting temporary access (21 days by default) to Zyxel support as administrator of your Organization. So they can help check your configuration & logs. This will automatically be switched off after specified days, or you could turn it off right after your issue is solved. You might also edit the access privileges here.

CSO account will be expired in: ● 21 days

○ Never

Direct Support

You're able to open a ticket to get direct assisstance from the Nebula technical support team.

Alternately, you can contact your local/regional Zyxel office for support:

- Europe, the Middle East and Africa (EMEA), click here .
- North and Central America, click here .

New Case

Subject* :	
Carbon Copy (CC) :	
Device* :	--
Issue Description* :	
Priority :	Low — Definition of priority

Upload site's topology to speed up the process:

Total File Upload Limit 7MB!(The maximum length of a filename is 60 characters)

The following table describes the labels in this screen.

Table 241 Help > Still need help?: Support Request

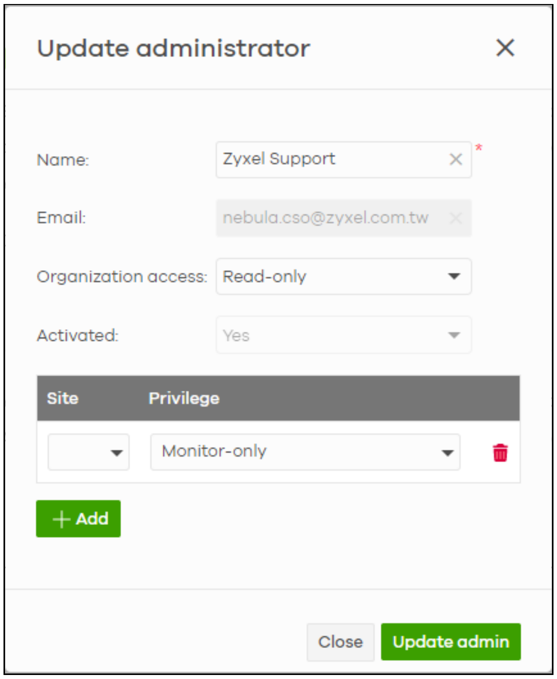
LABEL	DESCRIPTION
Zyxel Support Access Invite Zyxel support as administrator	Select **ON** to allow the Zyxel customer support account to access your organization temporarily, so that they can help check your configurations and log messages. At the time of writing, the support account will be deactivated automatically after 21 days. You can set the number of days, or select **Never**. If you select **ON**, you can click **here** to change the support account's name and access right to the organization and sites.  Update administrator Name: Zyxel Support Email: nebula.cso@zyxel.com.tw Organization access: Read-only Activated: Yes Site | Privilege Monitor-only
My Cases	
↻	Click this button to reload the data-related frames for this section on the page.
Open/Closed	Select to view the details about the tickets that are still open or closed.
Case Number	This shows the number of the eITS ticket.
Created	This shows the first date and time the ticket was created.
Last Updated	This shows the last date and time the ticket was updated.
Creator	This shows the account name of the administrator that created this ticket.
Subject	This shows the subject of the ticket.
Priority	This shows the severity level of the ticket.
Status	This shows whether the ticket is open or closed.
Engineer	This shows the name of the support person who handles the ticket.
New Case	Click this button if you want to issue a new ticket. The following fields then appear allowing you to provide the necessary information and describe the issue encountered.
Subject	Enter the subject of the ticket.
Carbon Copy (CC)	Enter the email address of the person you would like to receive a copy of the case.
Device	Select the NCC or the name of the Nebula Device that cannot work properly.
Issue Description	Enter a complete and detailed description of your issue.

Table 241 Help > Still need help?: Support Request (continued)

LABEL	DESCRIPTION
Priority	Select the severity level of the ticket. Click the **Definition of priority** link to see how to correctly identify a ticket’s severity level. This can help to get your problem solved quickly.
Add Another File	Click this button to upload another file.
Choose File/ Browse...	Click this button to locate the file you want to upload for reference.
Delete	Click this button to remove the file you just uploaded before submitting the ticket.
Cancel	Click this button to close the **New Case** section without saving.
Submit	Click this button to send your ticket to the Zyxel customer support.

CHAPTER 16
Troubleshooting

This chapter offers some suggestions to solve problems you might encounter with NCC and Nebula Devices.

- To see how to do things in NCC, go to the Tutorials section.
- To know how to manage Mobile Routers in NCC, go to Section 10.2 on page 632 for more information.
- To know how to monitor Security Appliances in NCC, go to Section 8.2 on page 466 (Security Firewalls) or Section 9.2 on page 576 (Security Gateways) for more information.
- To know how to configure Security Appliances in NCC, go to Section 8.3 on page 474 (Security Firewalls) or Section 9.3 on page 584 (Security Gateways) for more information.
- To know how to monitor Switches in NCC, go to Section 6.2 on page 349 for more information.
- To know how to configure Switches in NCC, go to Section 6.3 on page 362 for more information.
- To know how to monitor Access Points in NCC, go to Section 5.2 on page 305 for more information.
- To know how to configure Access Points in NCC, go to Section 5.3 on page 317 for more information.

I cannot register the Zyxel Device in NCC.

Check if your Zyxel Device supports Nebula by locating the Nebula QR code on the Zyxel Device label or package box.

I cannot access the NCC portal.

- Check that you are using the correct URL:
  - NCC: https://nebula.zyxel.com/
- Make sure your computer's Ethernet card is installed and functioning properly.
- Check that you have Internet access. In your computer, click **Start**, **(All) Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, type 'ping' followed by a website such as 'zyxel.com'. If you get a reply, try to ping 'nebula.zyxel.com'.
- Make sure you are using the correct web browser that supports HTML5. View the browser in full screen mode to display the NCC portal properly. Browsers supported are:
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

I cannot log into the NCC portal.

Open your web browser and go to *https://nebula.zyxel.com*. Sign in with the correct email and password. Click **Sign Up** if you do not have a Zyxel Account and create an account.

I cannot access a Nebula Device that I have registered in NCC or the Nebula Device appears offline in NCC.

- Check if the TCP/UDP port is blocked by your network's firewall rule or ISP. Click **Help** > **Support tools** > **Firewall information** to view information required for firewall rules to allow management traffic between NCC and Nebula Devices on your sites.
- Check the Nebula Device's hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local customer support.
- Make sure the Nebula Device is connected to the Internet.
- For Mobile Routers, make sure a valid SIM card is inserted in the SIM card slot.
- Make sure the Mobile Router is located where the cellular signal is strong.
- For ZyWALL USG FLEX / ATP / USG20(W)-VPN Series devices with **Nebula native mode** as the deployment method, make sure you perform the steps for **Nebula native mode** on the Nebula Device; see Section 2.1.8.1 on page 69 for information.
  If you select **Zero Touch Provision mode** as the deployment method. Make sure you perform the steps for **Zero Touch Provision mode** on the Nebula Device, see Section 2.1.8.2 on page 69 for information.
- Check if the WAN IP address is configured on the Nebula Device.
- Check if the Nebula Device can access the NCC server's domain through SSH/Console and enter 'nslookup d.nebula.zyxel.com'. If the Nebula Device shows 'unknown host', check your DNS server setting or use '8.8.8.8' as the DNS server on the Nebula Device.
- The Nebula Devices will apply the site-wide password after getting online on NCC. Check the login credential by going to **Site-wide** > **Configure** > **Site settings**: **Local credentials**.
- Specify the **Port** number and click **Establish** using **Remote Access** in the following screens to obtain real-time logs and data from the Nebula Device.
  - **Site-wide** > **Devices** > **Access points**
  - **Site-wide** > **Devices** > **Security router**
  - **Site-wide** > **Devices** > **Firewall**
  - **Site-wide** > **Devices** > **Security gateway**

Note: **Remote Access** to Nebula Access Points is available to the organization owner, organization administrators with full privileges, and site administrators with full privileges in Nebula Pro Pack license only.
Remote Access to Nebula Security Firewalls and Security Gateways is available to the organization owner in Nebula Pro Pack license only.

- Make sure that your Nebula Device can connect to the NCC by checking your network's firewall/ security settings. The following ports must be allowed:

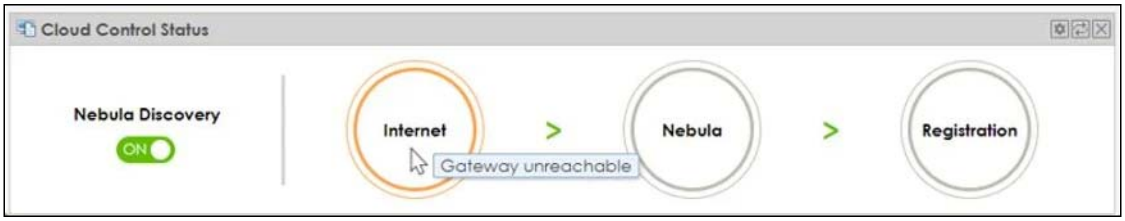
  - TCP: 22, 443, 4335 and 6667

Note: Go to **Help** > **Support tools** > **Firewall information** to find the latest port information.

- Make sure that your Nebula Device can synchronize with NTP (Network Time Protocol) through the following port:
  - UDP: 123
- Make sure that your Nebula Device can resolve the Nebula Cloud Management (NETCONF) domain name d.nebula.zyxel.com.
- Changing the **MTU** (Maximum Transmission Unit) size in **Site-wide** > **Configure** > **Firewall** > **Interface** > **WAN/LAN interface configuration** may cause the Nebula Switches to appear offline. Make sure that the MTU size is not smaller than 1500 bytes.

I cannot see my Nebula Devices in the NCC Dashboard or the corresponding Nebula Device monitor page.

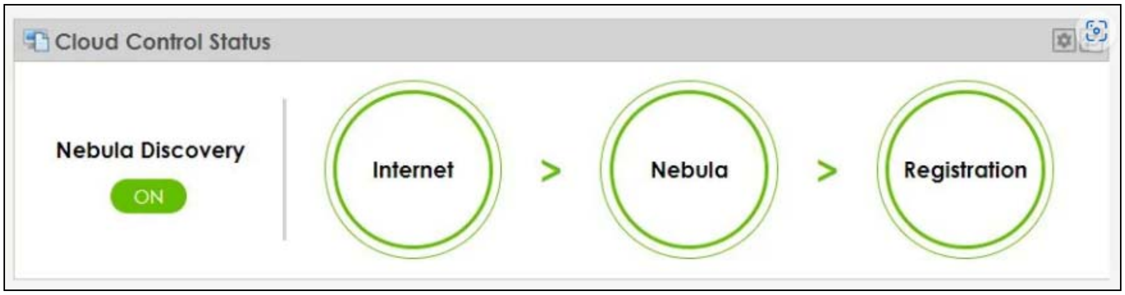
- Check the Nebula Device's local Web Configurator's **Dashboard**. The **Cloud Control Status** displays the status of the Nebula Device's Internet and NCC connection and registration status. Make sure that the Nebula Device has **NCC Discovery** enabled.
- If the Nebula Device cannot connect to the Internet or NCC, hover the mouse over the **Internet** circle to check the error message. Check your local network settings.



- Make sure that your Nebula Device can connect to the NCC by checking your network's firewall/ security settings. The following ports must be allowed:
  - TCP: 22, 443, 4335 and 6667
  - UDP: 123

Note: Go to **Help** > **Support tools** > **Firewall information** to find the latest port information.

- Make sure that you have registered your Nebula Devices with the NCC. See Section 12.2.1 on page 659.
- Make sure that you have created an organization and site and added the Nebula Devices to the site. See Create Organization on page 57.
- When the Nebula Device is online in NCC, all circles are green.



I made the mistake of assigning a license to a Nebula Device and the license is in **Active**/**Queued** status. Can I **Undo assign**?

No, **Undo assign** can only apply to an **Inactive** license. Select **Transfer license** to transfer the license to the correct Nebula Device.

I have already transferred a license to a Nebula Device. Why is the organization still in the grace period or Base tier?

Not all Nebula Devices in the organization have been assigned a license. Check if you have assigned a valid Plus or Professional license to all unlicensed Nebula Devices in the organization.

- In **Organization-wide** > **License & inventory** > **Overview**, click **Upgrade Now** to upgrade the organization to Plus or Professional tier.
- Alternatively, remove the unlicensed Nebula Device(s) from the organization.

My organization is now in Cloud-saving mode; how can I disable it?

There are two ways to disable Cloud-saving mode.

- Click the **Cloud-saving mode** switch in the **Welcome back** pop-up window.
  Then click **Close** to turn off Cloud-saving mode for the organization.
- A banner displays when NCC is in Cloud-saving mode.
  Click the **You could change mode here** link in the NCC banner.
  Click the **Cloud-saving mode** switch in the **Cloud-saving mode** pop-up window.
  Then click **Close** to turn off Cloud-saving mode for the organization.

I want to place my Nebula Device on the right location on Google maps.

If your Nebula Device has a public IPv4 address, Google Maps can use Geo IP to approximatively locate your Nebula Device. If your Nebula Device has an IPv6 address or a private IPv4 address or you want locate the Nebula Device more exactly, use one of the following methods.

- Select **Use the following address or coordinates** to enter the complete address or coordinates of the Nebula Device in **Site-wide** > **Devices** > **Firewall** / **Security gateway** / **Switches** / **Access points**: details: **Map**: **Position device**.
- Select **Get my location from web browser** to use the public IP address of the computer accessing the NCC portal.
- Drag-and-drop your Nebula Device directly on the Google map.

I cannot set up Secure WiFi in NCC.

- Make sure the Nebula Security Firewall and Nebula Access points are in the same NCC site.
- Make sure a Secure WiFi license is assigned to the Nebula Security Firewall.
- Make sure to configure the **Remote AP Setting** of each Remote Access Point before booting up the Remote Access Point in the remote site. See Table 19 on page 220.
- The maximum number of Remote Access points depends on the Nebula Security Firewall.

Table 242 Maximum Remote Access Points (at the time of writing)

CAPACITY	USG FLEX 50 / USG20-VPN / USG20W-VPN	USG FLEX 100 / USG FLEX 100W / ATP100 / ATP100W	USG FLEX 200 / ATP200	USG FLEX 500 / ATP500	ATP700	USG FLEX 700 / ATP800
Maximum IPSec Tunnel	10	40	90	250	450	450
Maximum Remote AP	No support	6	10	18	66	130

The mesh extender does not appear online on **Status** in **Site-wide** > **Devices** > **Access points**.

- Click **Reconnect** in **Site-wide** > **Devices** > **Access points**: **Uplink AP** to re-establish connection.
- Make sure your Nebula Device supports smart mesh. To view the list of Nebula Devices that support smart mesh, go to **Help** > **Device function table**.

After adding a mesh extender to a site, the mesh extender cannot connect to a mesh controller.

- Make sure you enable **AP Smart Mesh** in **Site-wide** > **Configure** > **Access points** > **AP & port settings**. See Section 5.3.7 on page 344 for more information.

Note: For more information about smart mesh, see Section 5.1.1 on page 303.

The mesh extender does not broadcast the mesh controller SSID.

- Make sure you enable **Downlink** in **Site-wide** > **Devices** > **Access points**: **Details**. See Section 4.3.1.1 on page 218 for more information.
- To enhance your mesh extender's connectivity, maintain an **Uplink signal** strength above -65 dBm. You can check this in **Site-wide** > **Devices** > **Access points**.

None of the Nebula Device LEDs turn on.

- Make sure that you have the power cord connected to the Nebula Device and plugged in to an appropriate power source. Make sure you have the Nebula Device turned on.
- Check all cable connections. See the related Quick Start Guide.
- If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local customer support.

The Nebula Device PWR LED is red.

- The Nebula Device has a power-related error. Disconnect and reconnect the power cord. Make sure that you are using the included power cord for the Nebula Device and it is plugged into an appropriate power source. See the related Quick Start Guide.
- If the LED is still red, you may have a hardware problem. In this case, you should contact your local customer support.

I need to replace a defective Nebula Device on my stacking system. I want to keep the NCC configurations.

- Contact your vendor about the faulty Nebula Device.
- Do NOT remove or swap the faulty Nebula Device in NCC.
- Contact Zyxel Customer Support to keep the faulty Nebula Device's port configuration and apply it to the new Nebula Device.

When I click **Upgrade now** in the **Site-wide** > **Configure** > **Firmware management** or **Organization-wide** > **Organization-wide manage** > **Firmware management** screens, I get an **Upgrade system firmware failed**.

- Make sure the DNS server used by your Nebula Device can resolve the domain name 'firmware.nebula.zyxel.com'.
- Make sure there are no firewall policies restricting access to 'firmware.nebula.zyxel.com' and that the firewall allows connection to TCP port 443.
- If there is no firewall policy restricting access, log in to the Nebula Device Web Configurator to get the technical support log from the following location:
  - For an Access Point, go to **MAINTENANCE** > **Diagnostics** > **Diagnostic** > **Collect now**.

- For a Switch, go to **MAINTENANCE** > **Tech-Support** > **All**.
- For a Security Router, there is no technical support log.
- For a Security Firewall, go to **MAINTENANCE** > **Diagnostics Info** > **Collect now**.
- For a Security Gateway, go to **MAINTENANCE** > **Diagnostics** > **Collect** > **Collect now** > **Files**.
- For a Mobile Router, there is no technical support log.

- Contact Zyxel Customer Support for help.

Note: The **Upgrade now** option is available only when the selected Nebula Devices have a new firmware available.

The smartphone app cannot find and communicate with the IoT (Internet of Thing) device over WiFi.

- Go to **Site-wide** > **Configure** > **WiFi SSID settings** to configure a separate WiFi network for the IoT device(s).
- Go to **Site-wide** > **Configure** > **Access points** > **SSID advanced settings** and select the separate WiFi network in the previous step. Select **WPA Personal With WPA2** in **Security options**.
- Select the **2.4GHz band** in **Band mode**. The smartphone with IoT app and IoT device must connect to an SSID on the 2.4 GHz band. This enhances the connectivity and performance of IoT devices.
- Disable 802.11k/v/r in **Assisted roaming** and **802.11r**. This prevents the Nebula Device from steering IoT devices to the 5 GHz band.
- Disable **Layer 2 isolation** in **Advanced settings**. An IoT device's MAC address that is not in the **Layer 2 isolation** table will not be able to communicate with other devices in the same WiFi network when layer-2 isolation is enabled.

Note: When layer-2 isolation is enabled, click **Add** to enter a MAC address of a IoT device you want to allow access to other devices in the same WiFi network.

- Disable **Intra-BSS traffic blocking** in **Advanced settings**. This allows direct communication between IoT devices from within the same WiFi network.
- Go to **Site-wide** > **Configure** > **WiFi SSID settings**. Configure the same **Tagging** for the same WiFi network and the **Tag** for the Nebula Device in **Site-wide** > **Devices** > **Access points**. For example, tagging Nebula Device A with "Lobby" in **Site-wide** > **Devices** > **Access points** and assigning the "Lobby" tag to "SSID_lobby" in **Site-wide** > **Configure** > **WiFi SSID settings** means that Nebula Device A will broadcast "SSID_lobby."
- Go to **Site-wide** > **Configure** > **Radio settings** and disable **Allow 802.11ax/ac/n stations only**. This allows the IEEE 802.11a/b/g IoT devices to connect.

A WiFi client device cannot connect to a Nebula Device WiFi.

- Check the WiFi LED status to make sure the Nebula Device WiFi is on.
- Make sure the WiFi client is within transmission range of a Nebula Device.
- Make sure the WiFi client entered the correct SSID (Service Set IDentifier) and pre-shared key (PSK). Go to **Site-wide** > **Configure** > **WiFi SSID settings** for the correct SSID and PSK.
- Make sure your WiFi client is using the same WiFi security type (PSK or open) as the Nebula Device.

- Make sure the WiFi adapter on your WiFi client is working. Right-click your WiFi client computer's network adapter and then select **Properties** to check the network adapter status.
- Make sure the WiFi adapter on your WiFi client is IEEE 802.11-compatible. Make sure it supports the same WiFi standard as the Nebula Device 2.4G/5G radio.
- Select **MAC authentication fallback** in **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**: **Sign-in method**. If MAC authentication fails, the WiFi client will use web authentication with a user name and password.

  Example Scenario: When MAC authentication fails.
  A WiFi client tries to connect to a WiFi network using MAC authentication (RADIUS server). If MAC authentication fails, the WiFi client will fall back to web authentication. The WiFi client must provide a user name and password for web authentication.

A client device's WiFi connection is slow and intermittent.

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other WiFi devices.

To optimize the speed and quality of a WiFi connection, you can:

- Move the client WiFi device closer to a Nebula Device if the signal strength is low.
- Reduce WiFi interference caused by other WiFi networks or surrounding wireless electronics such as cordless phones.
- Reduce the number of WiFi clients connecting to the same Nebula Device simultaneously, or add additional Nebula Devices if necessary.
- Try closing some programs that use the Internet on the WiFi client, especially peer-to-peer applications. If a WiFi client is sending or receiving a lot of information, it may have too many programs open that use the Internet.
- Place a Nebula Device where there are minimum obstacles (such as walls and ceilings) between a Nebula Device and a WiFi client. Avoid placing a Nebula Device inside any box that might block WiFi signals. See How to Position Multiple Nebula Devices (for Nebula Access Points only) for more tips on selecting the best position to minimize signal interference for multiple Nebula Devices (access points).

- Go to **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**: **Advanced settings** and turn on IEEE 802.11r fast roaming on the Nebula Device. 802.11r fast roaming reduces the delay when the clients switch from one Nebula Device to another by storing the security keys on all Nebula Devices in a network. Information from an original association is passed to the new Nebula Device when the clients roam. The clients do not need to perform the 802.1x authentication process again.

I enabled **AP traffic log** in **Site-wide** > **Configure** > **Site settings: Reporting**, and I want to restrict the type of logs from my Nebula Device (for example, no debug logs).

- At the time of writing, Nebula Devices will log all events. You will not be able to restrict the type of logs written.
- You can choose the type of logs to generate only in Standalone mode by doing the following:

- Log in to the Nebula Access Point's Web Configurator.

Note: If NCC is managing or has managed a Nebula Device, check **Local credentials** in **Site-wide** > **Configure** > **Site settings** for the Nebula Device's current password.

- Go to **Configuration** > **Log & Report** > **Log Setting** > **Active Log Summary**.
- Select what information to include in the system log.

My Mac OS computer will not display the captive portal page for logging in.

- Enter "http://neverssl.com" in the **Location** or **Address** field of your browser. This allows you to access the NCC login page by bypassing SSL (Secure Sockets Layer). SSL creates an encrypted link between a web server and a web browser.

I am unable to access a Nebula Device in Standalone mode after removing (unregistering) the Nebula Device from NCC.

- Make sure the Nebula Device has been removed from your organization. Go to **Organization-wide** > **License & inventory** > **Devices**. Select the Nebula Device, click **Actions**, then click **Remove from organization**. Click **Yes** to confirm, or click the delete icon to remove the Nebula Device.
- Make sure to reset the Zyxel Device to its factory-default settings. This will remove the current configuration.

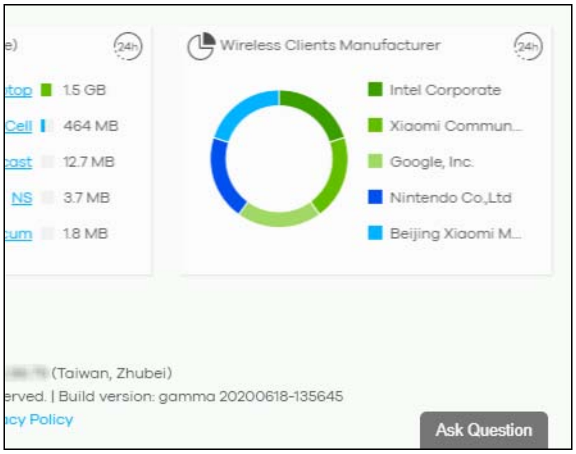
You should now be able to access the Zyxel Device's Web Configurator in Standalone mode.

16.1 Getting More Troubleshooting Help

Go to *support.zyxel.com* at the Zyxel website for other technical information on the NCC.

16.2 NCC Live Chat

Clicking the **Ask Question** button at the bottom of NCC window prompts you to search for a solution on the Zyxel forum, and then connects you to a Zyxel technical support agent. If a technical support agent is not available, you can fill in a form to send your question to Zyxel by email.



Note: This is an NCC Professional Pack feature.

Live chat might be limited to a certain number of hours per day. The time that live chat is available varies depending on your country.

APPENDIX A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

For Zyxel Communication offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Network offices, see *https://www.zyxel.com/index.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com*

Asia

China

- Zyxel Communications Corporation–China Office
- *https://www.zyxel.com/cn/sc*

India

- Zyxel Communications Corporation–India Office
- *https://www.zyxel.com/in/en-in*

Kazakhstan

- Zyxel Kazakhstan
- *https://www.zyxel.com/ru/ru*

Korea

- Zyxel Korea Co., Ltd.
- *http://www.zyxel.kr/*

Malaysia

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Philippines

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Singapore

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com/tw/zh*

Thailand

- Zyxel Thailand Co., Ltd.
- *https://www.zyxel.com/th/th*

Vietnam

- Zyxel Communications Corporation–Vietnam Office
- *https://www.zyxel.com/vn/vi*

Europe

Belarus

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Belgium (Netherlands)

- Zyxel Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

Bulgaria

- Zyxel Bulgaria

- *https://www.zyxel.com/bg/bg*

Czech Republic

- Zyxel Communications Czech s.r.o.
- *https://www.zyxel.com/cz/cs*

Denmark

- Zyxel Communications A/S
- *https://www.zyxel.com/dk/da*

Finland

- Zyxel Communications
- *https://www.zyxel.com/fi/fi*

France

- Zyxel France
- *https://www.zyxel.com/fr/fr*

Germany

- Zyxel Deutschland GmbH.
- *https://www.zyxel.com/de/de*

Hungary

- Zyxel Hungary & SEE
- *https://www.zyxel.com/hu/hu*

Italy

- Zyxel Communications Italy S.r.l.
- *https://www.zyxel.com/it/it*

Norway

- Zyxel Communications A/S
- *https://www.zyxel.com/no/no*

Poland

- Zyxel Communications Poland
- *https://www.zyxel.com/pl/pl*

Romania

- Zyxel Romania
- *https://www.zyxel.com/ro/ro*

Russian Federation

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Slovakia

- Zyxel Slovakia
- *https://www.zyxel.com/sk/sk*

Spain

- Zyxel Iberia
- *https://www.zyxel.com/es/es*

Sweden

- Zyxel Communications A/S
- *https://www.zyxel.com/se/sv*

Switzerland

- Studerus AG
- *https://www.zyxel.com/ch/de-ch*
- *https://www.zyxel.com/fr/fr*

Turkey

- Zyxel Turkey A.S.
- *https://www.zyxel.com/tr/tr*

UK

- Zyxel Communications UK Ltd.
- *https://www.zyxel.com/uk/en-gb*

Ukraine

- Zyxel Ukraine
- *https://www.zyxel.com/ua/uk-ua*

South America

Argentina

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Brazil

- Zyxel Communications Brasil Ltda.

- *https://www.zyxel.com/br/pt*

Colombia

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Ecuador

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

South America

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Middle East

Israel

- Zyxel Communications Corp.
- *https://il.zyxel.com*

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- *https://www.zyxel.com/us/en-us*

APPENDIX B
Legal Information

Copyright

Copyright © 2025 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Viewing Certifications

Go to *http://www.zyxel.com* to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at *http://www.zyxel.com/web/support_warranty_info.php*.

Registration

Register your product online at *www.zyxel.com* to receive email notices of firmware upgrades and related information.

Index