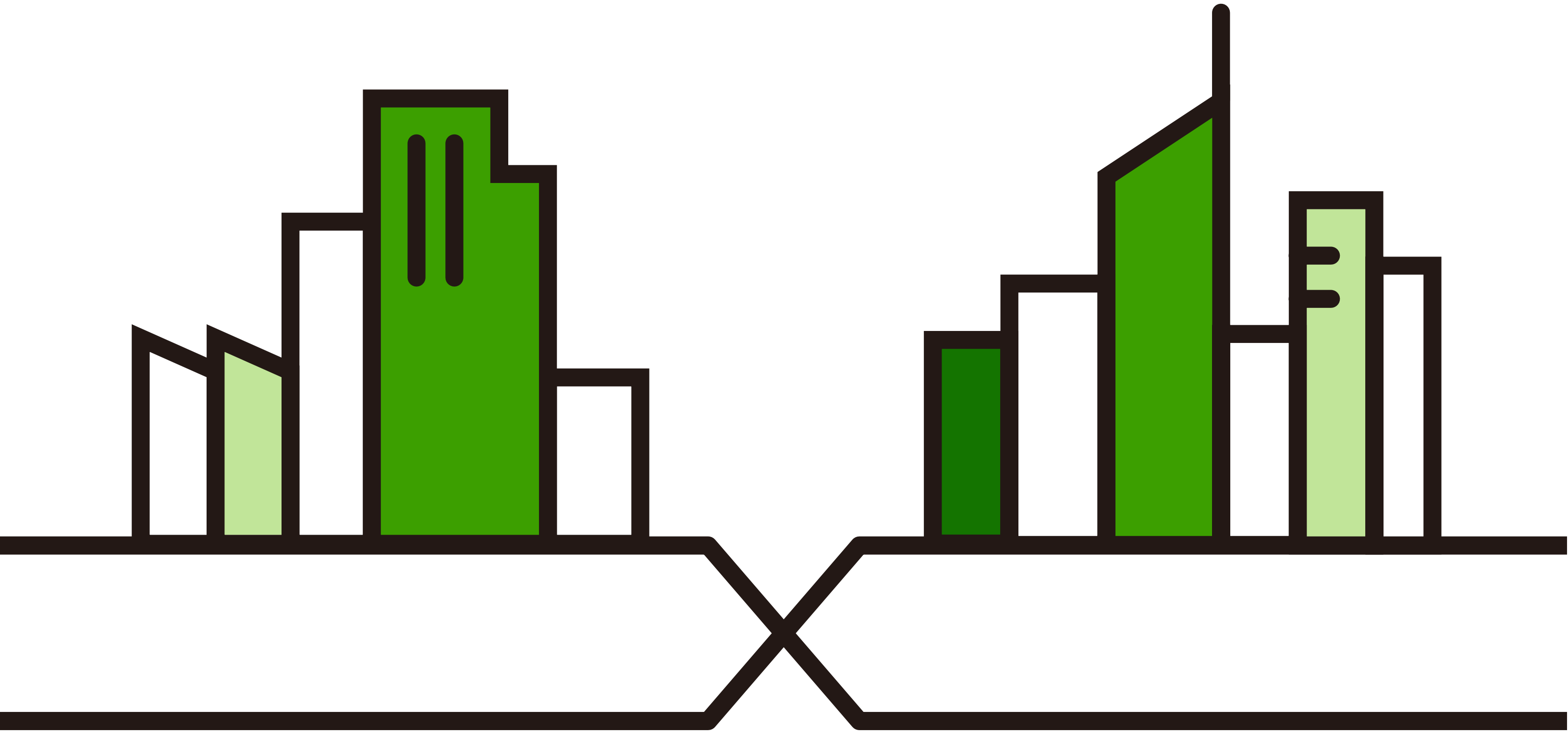
User's Guide

NCC

Nebula Control Center

Default Login Details	
NCC URL	https://nebula.zyxel.com
User Name	myZyxel account name
Password	myZyxel account password

Version 17.00 Edition 1, 04/2023



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.

Related Documentation

- Nebula Device Quick Start Guide

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

- 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, 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 Section 1.2.2 on page 24.

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
Security Gateways	NSG Series
Hybrid Security Firewalls	ZyWALL ATP / USG FLEX / 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

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

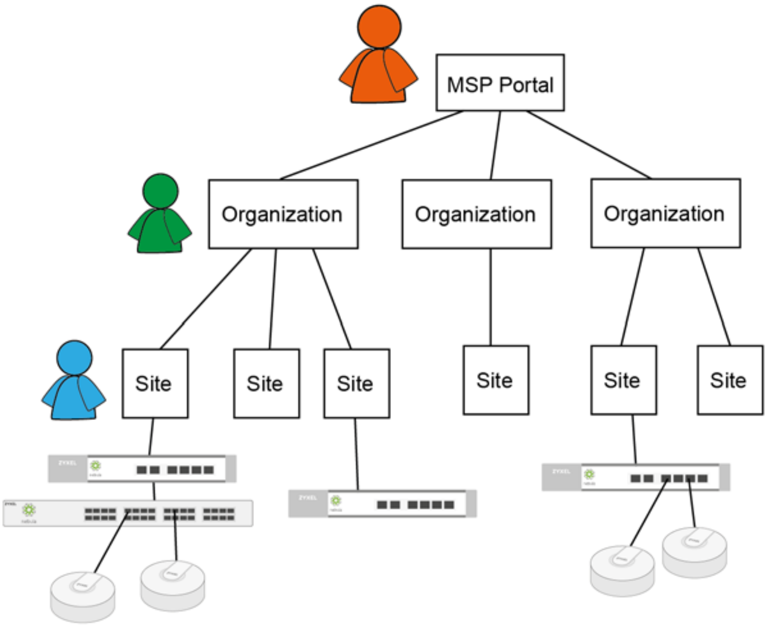
A hybrid device can operate in either standalone or Nebula cloud management mode. When the hybrid device is in standalone mode, it can be configured and managed by the Web Configurator. When the hybrid device is in Nebula cloud management mode, it can be managed and provisioned by the Zyxel Nebula Control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

1.1.1 MSP (Managed Services Provider) Portal

If you have an MSP license (as discussed in Section 13.1 on page 570), 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.

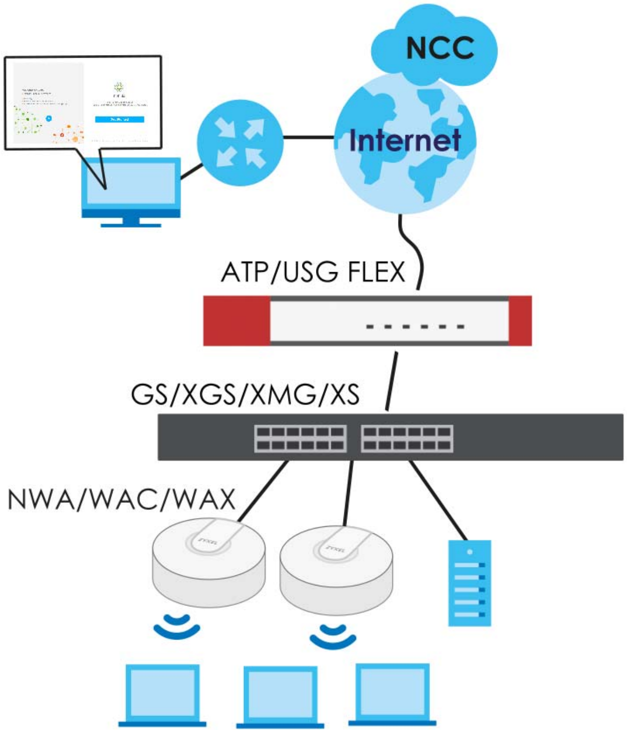
- A site can have multiple Nebula Devices, but can only belong to one organization.
- A site can be managed by more than one site or organization administrator.
- An organization can contain multiple sites and can be managed by more than one organization administrator.
- A myZyxel.com account can be an organization administrator and/or site administrator in the NCC (see Section 11.3 on page 508).
- A site administrator can manage more than one site.

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

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

In the following example, Nebula managed devices, such as the NAP102 or the NSW100-28P, are deployed in two separate networks (Site A and Site B). With the NCC organization administrator account, you can remotely manage and monitor all Nebula Devices even when they are located at different places.

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 17.
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 17.
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.
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.

Table 2 Licenses Summary (continued)

LICENSE	CATEGORY	ASSIGN TO	DESCRIPTION
UTM Security Pack	Security Service	USG FLEX devices	Unlocks security services, such as anti-malware, content filtering, URL threat filter, IP reputation, sandboxing, IPS (Intrusion Prevention System), application patrol, SecuReporter, CDR (Collaborative Detection & Response), and security profile sync (see Section 11.4.5 on page 527 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 filtering, 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 17.
Gold Security Pack	Organization and Security Service	USG FLEX devices except USG20-VPN / USG20W-VPN / USG FLEX 50	Unlocks security services, such as content filtering, 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 filtering, 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.
SCR Pro Pack	Organization and Security Service	SCR 50AXE	Unlocks security services, such as web filtering, Ransomware Prevention Premium, and all advanced features within the Nebula Device's organization. For details on Pro features, see Section 1.1.4.2 on page 17.

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)	
New site configuration clone	No	No	Yes	Organization-wide > Create site	
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	
Site/Switch configuration backup and restore	No	No	Yes	Organization-wide > Organization-wide manage > Configuration management	

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
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	No	Yes	Yes	Site-wide > Configure > Alert settings	
Per-device firmware upgrade schedules	No	Yes	Yes	Site-wide > Configure > Firmware management	

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
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 > WiFi 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]	
Facebook WiFi	Configure in NCC	No	Yes	Site-wide > Configure > Access points > SSID advanced settings	
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 access	
IP Source Guard	No	No	Yes	Site-wide > Configure > Switches > Switch settings	
Nebula cloud authentication	Yes	Yes	Yes	Site-wide > Configure > Switches > Authentication	
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
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

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
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
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

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 11.2.7 on page 502 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.

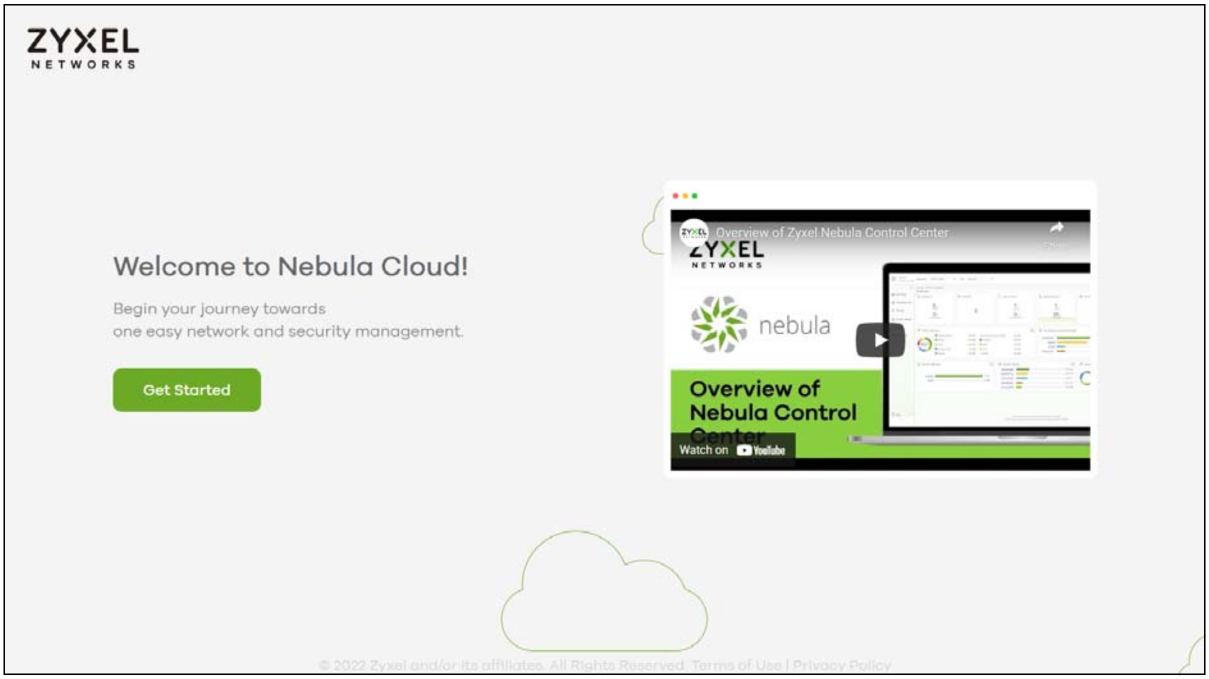
1.2.1 Connect Nebula Managed Devices

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**.



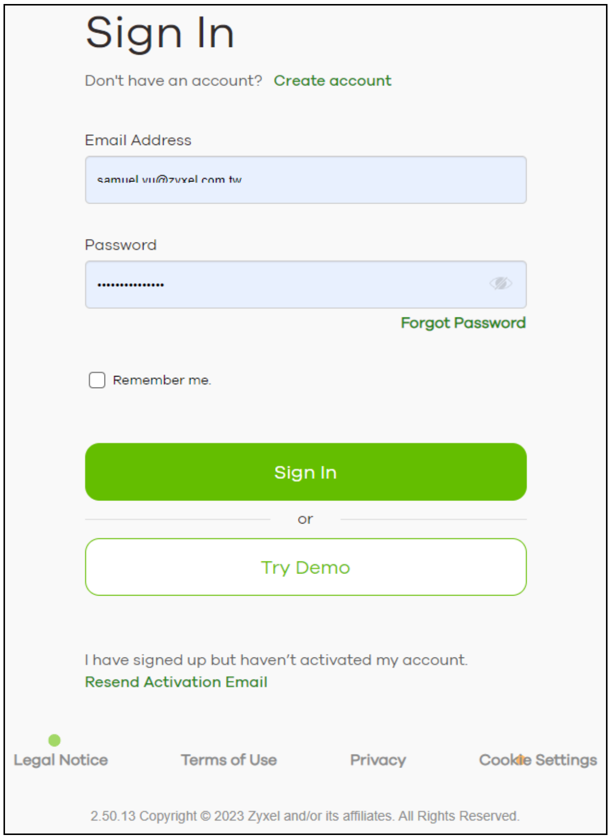
Welcome to Nebula Cloud!

Begin your journey towards
one easy network and security management.

ZYXEL NETWORKS
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

Note: The NCC requires a myZyxel account before you can register and manage Nebula Devices. Log into the NCC with your myZyxel account. Click **Create account** if you do not have a myZyxel account and create an account with your existing email address.

2 Enter the **Email Address** and **Password**, and then click **Sign In**.



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

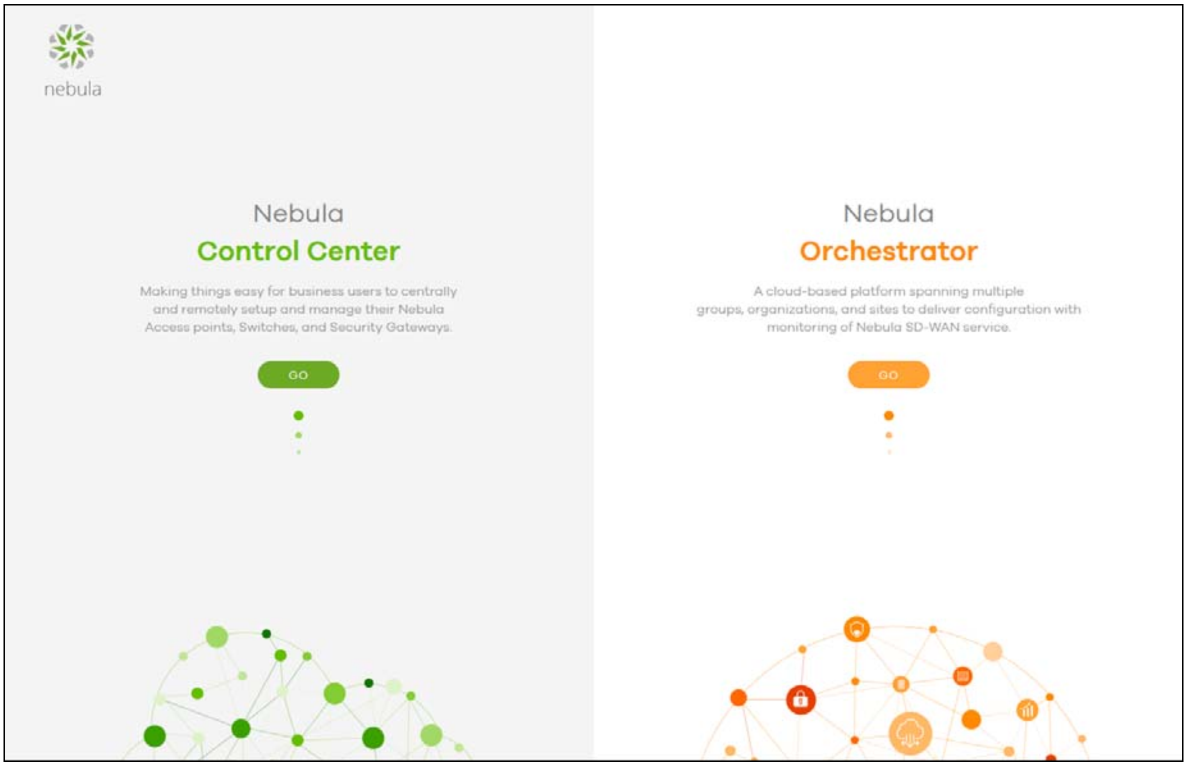
I have signed up but haven't activated my account.
Resend Activation Email

Legal Notice Terms of Use Privacy Cookie Settings

2.50.13 Copyright © 2023 Zyxel and/or its affiliates. All Rights Reserved.

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

3 Click **Go** under **Nebula Control Center** to log in to NCC.



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.

GO

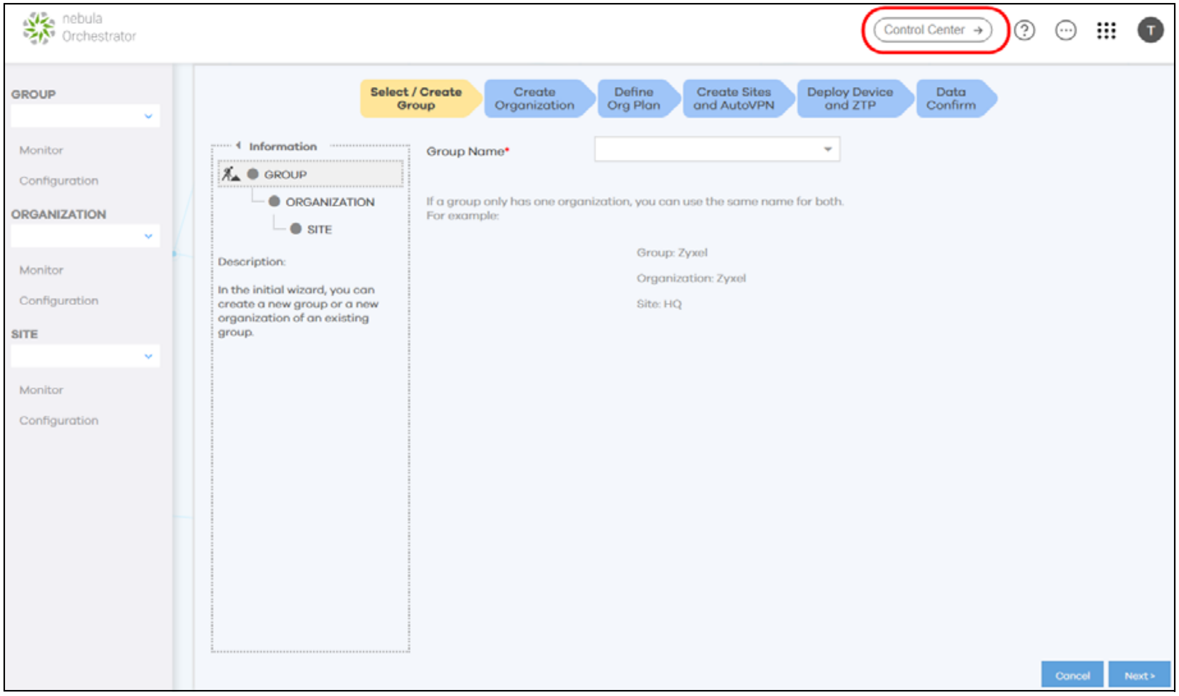
Nebula
Orchestrator

A cloud-based platform spanning multiple groups, organizations, and sites to deliver configuration with monitoring of Nebula SD-WAN service.

GO

Alternatively, click **Go** under **Nebula Orchestrator** to 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.

Figure 2 Nebula SD-WAN (Orchestrator)



Group Name*

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:

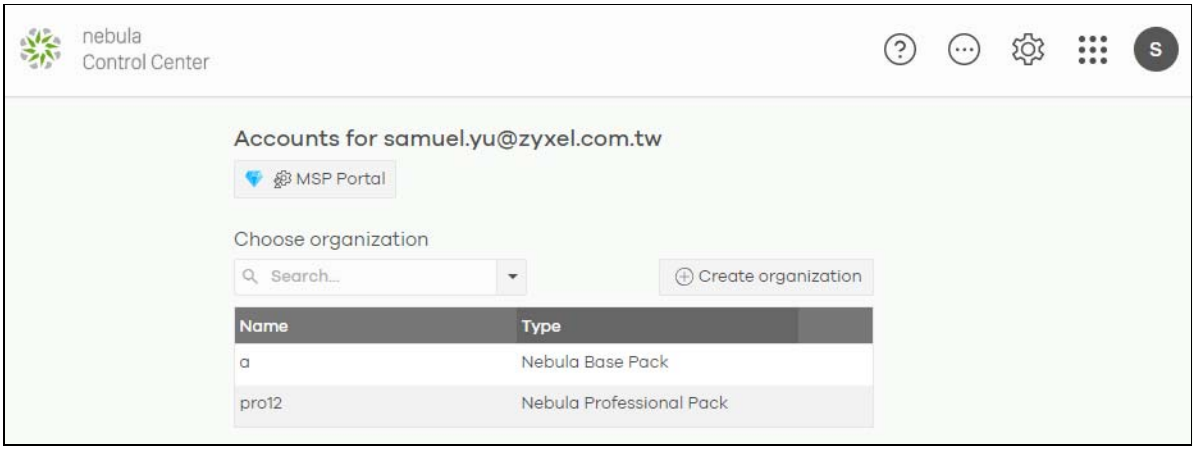
Group: Zyxel

Organization: Zyxel

Site: HQ

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

4 Click **Create organization** to create a new organization. If this is the first time you have logged into NCC, proceed to step 10.
If you have more than one organization, click a row to select the organization you want to manage.

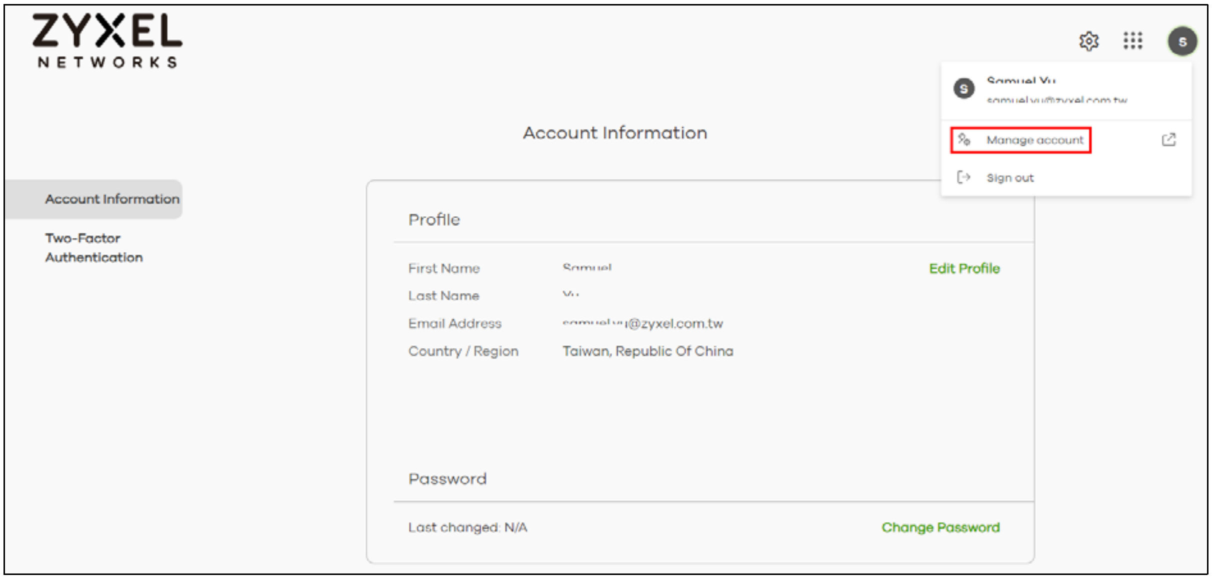


Accounts for samuel.yu@zyxel.com.tw

Choose organization

Name	Type
a	Nebula Base Pack
pro12	Nebula Professional Pack

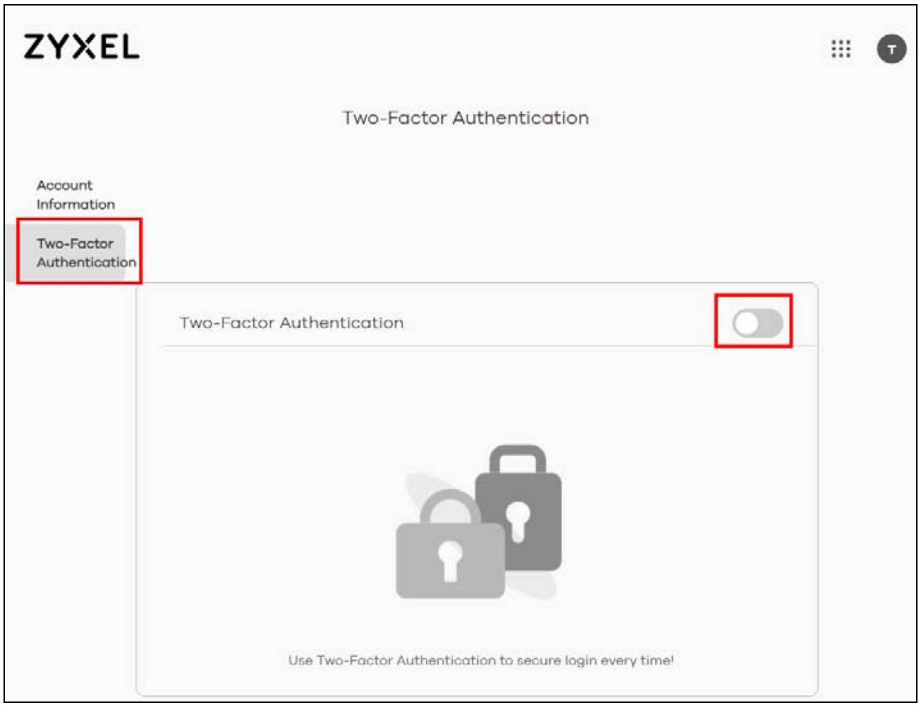
5 The NCC supports two-factor authentication (2FA) to add a second layer of security to your account. Click **Manage account** to enable Two-factor authentication on the following page. Otherwise, you can skip 2FA and go to step 10 directly.



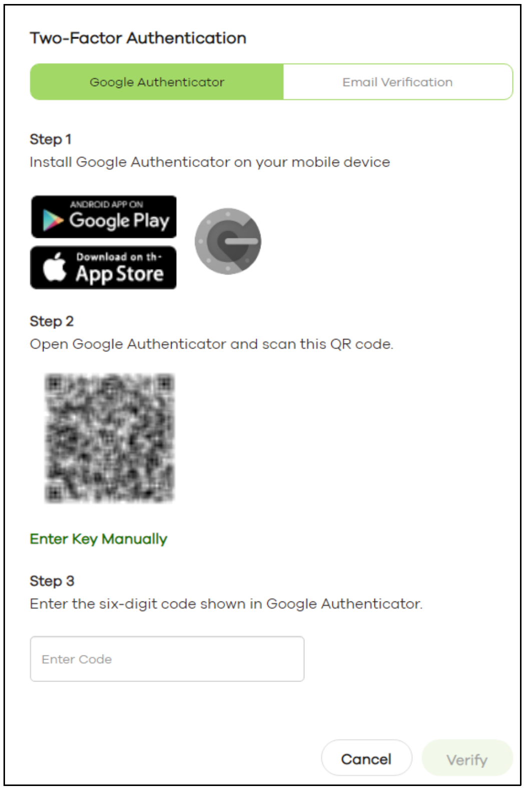
First Name Samuel
Last Name Yu
Email Address samuel.yu@zyxel.com.tw
Country / Region Taiwan, Republic Of China

Last changed: N/A

6 Click **Two-Factor Authentication** and then click the switch to enable Two-Factor Authentication.


ZYXEL
Two-Factor Authentication
Account Information
Two-Factor Authentication
Two-Factor Authentication
Use Two-Factor Authentication to secure login every time!

7 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

Google Authenticator | Email Verification

Step 1
Install Google Authenticator on your mobile device

Step 2
Open Google Authenticator and scan this QR code.

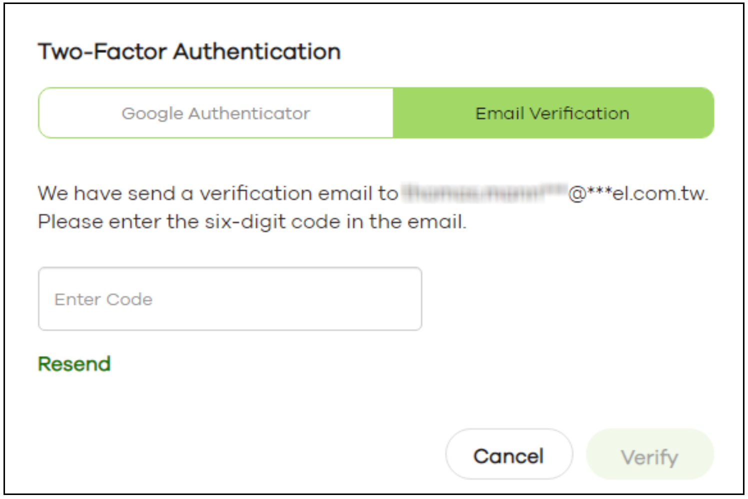
Enter Key Manually

Step 3
Enter the six-digit code shown in Google Authenticator.

Enter Code

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

If you select **Email Verification**, an email is sent to your myZyxel account's email address. Enter the code exactly as it appears in the email and click **Verify**.

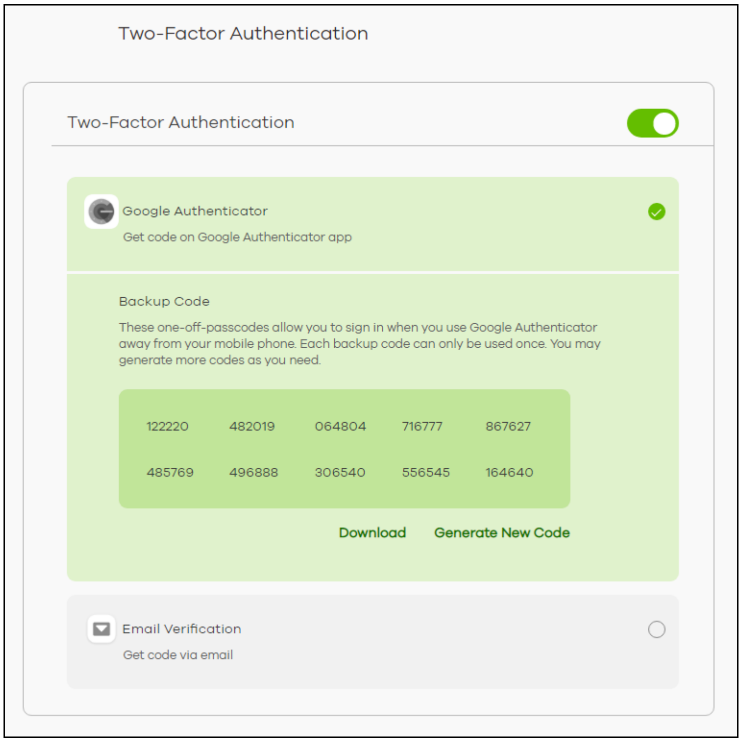


Two-Factor Authentication

We have send a verification email to [redacted]@***el.com.tw.
Please enter the six-digit code in the email.

8 Enter the verification code to get 10 backup codes, which help regain access to your account in case your smartphone is not available for 2FA the next time you need to log in again.

Note: If you generate a new set of backup codes, the old set will become inactive.



Two-Factor Authentication

Two-Factor Authentication

Google Authenticator

Get code on Google Authenticator app

Backup Code

These one-off-passcodes allow you to sign in when you use Google Authenticator away from your mobile phone. Each backup code can only be used once. You may generate more codes as you need.

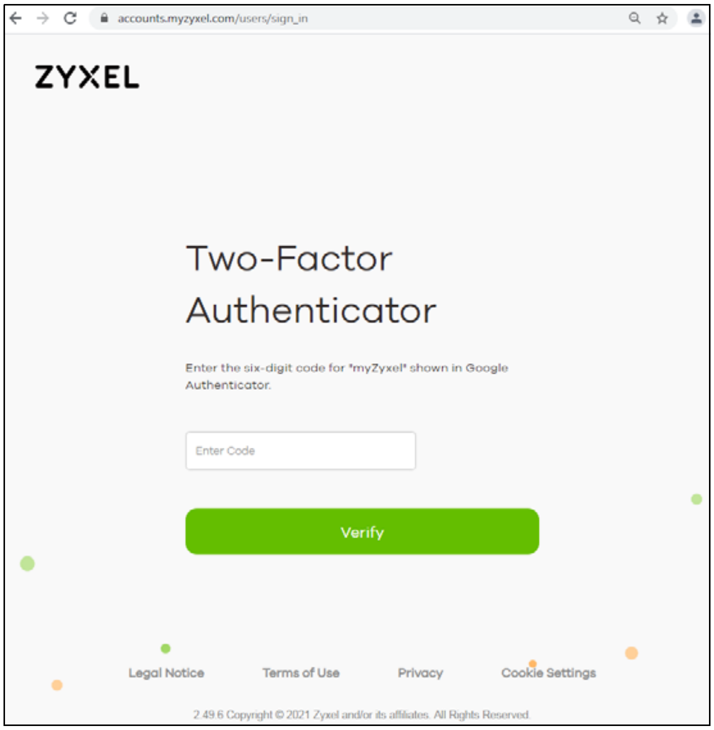
122220	482019	064804	716777	867627
485769	496888	306540	556545	164640

Email Verification

Get code via email

Write down or print out the backup codes for your account. You can enter the backup code on the NCC web page to authenticate your identity at the next login. Each code can only work once. Click **Download** to download the backup codes.

9 To re-log in Nebula after the **Two-Factor Authentication** is enabled. Go to **Applications** > **Nebula** and then enter a code to log in your Nebula account.



accounts.myzyxel.com/users/sign_in

ZYXEL

Two-Factor Authenticator

Enter the six-digit code for "myZyxel" shown in Google Authenticator.

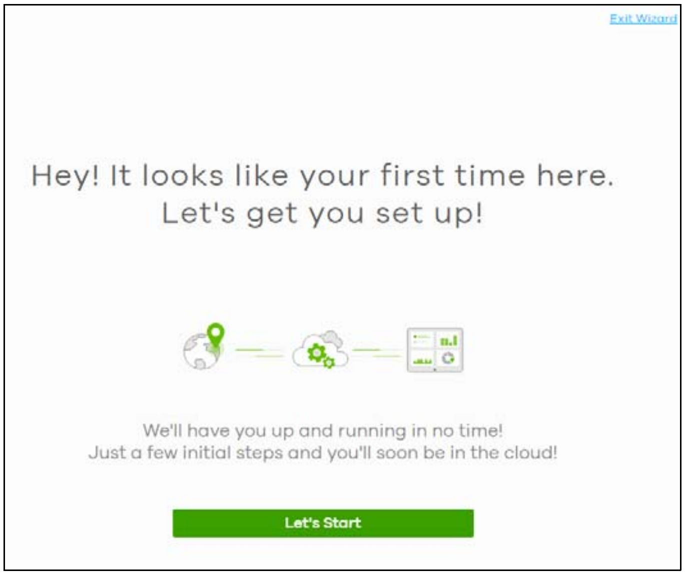
Enter Code

Verify

Legal Notice Terms of Use Privacy Cookie Settings

2.49.6 Copyright © 2021 Zyxel and/or its affiliates. All Rights Reserved.

10 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 46 for how to use the wizard.



Exit Wizard

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

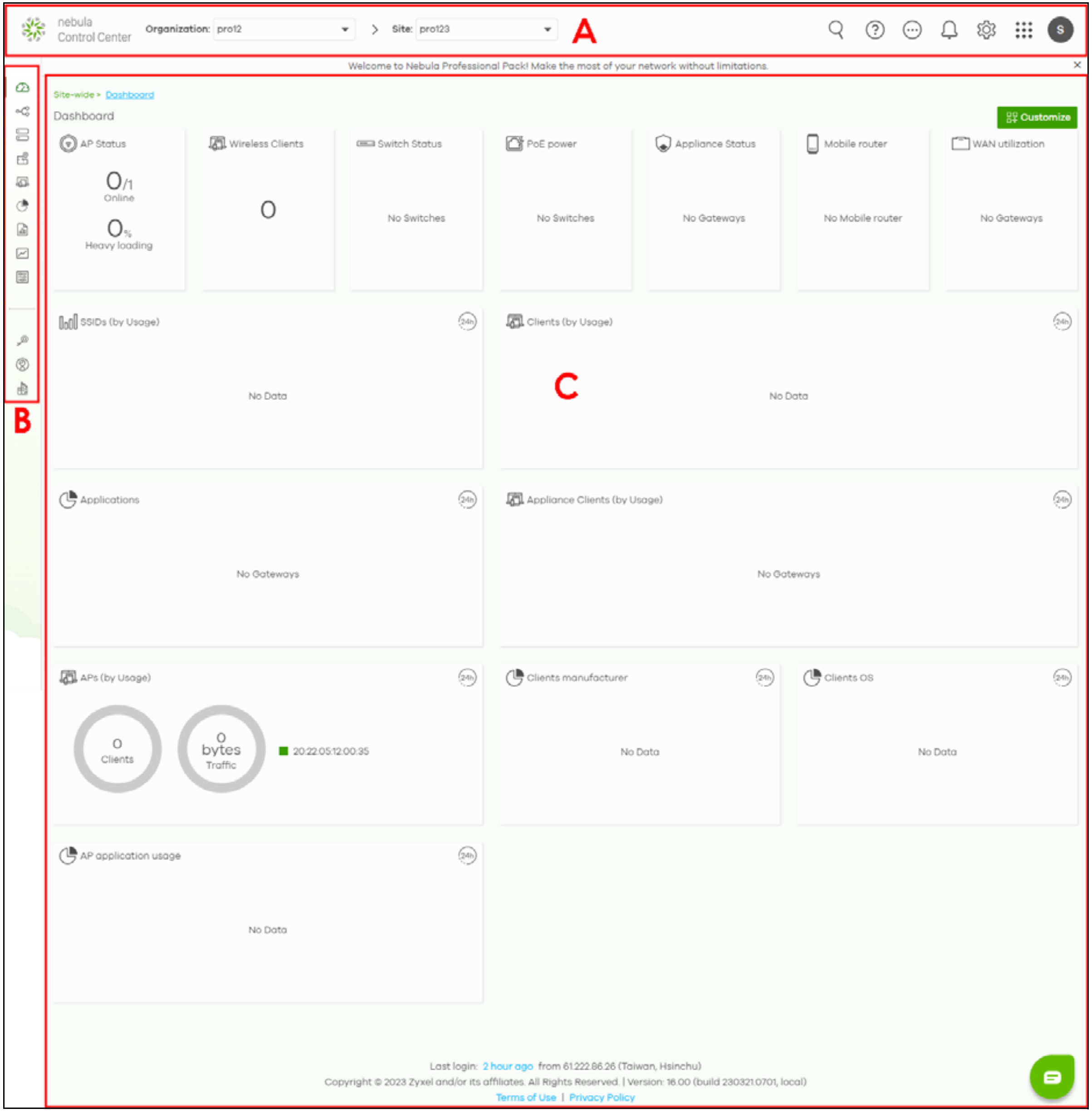
We'll have you up and running in no time!
Just a few initial steps and you'll soon be in the cloud!

Let's Start

1.3 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



Welcome to Nebula Professional Pack! Make the most of your network without limitations.

Last login: 2 hour ago from 61.222.86.26 (Taiwan, Hsinchu)

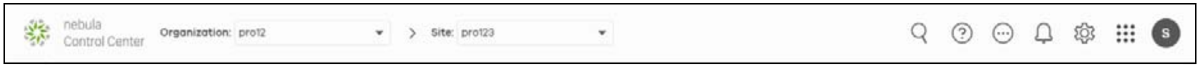
Copyright © 2023 Zyxel and/or its affiliates. All Rights Reserved. | Version: 16.00 (build 230321.0701, local)

- A – Title Bar
- B – Navigation Panel
- C – Main Screen

1.3.1 Title Bar

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

Figure 4 NCC Title Bar



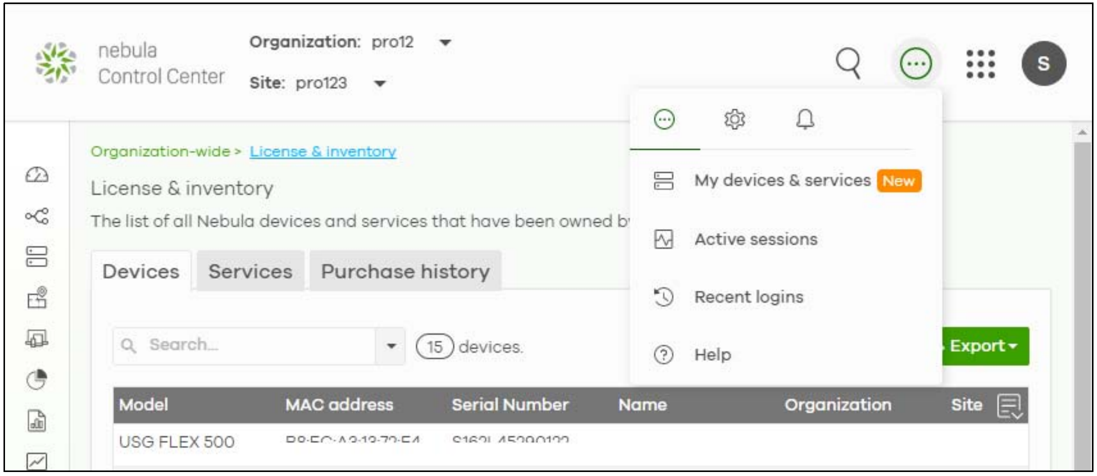
The icons provide the following functions.

Table 4 NCC Title Bar

LABEL	DESCRIPTION
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 12.1.1 on page 557.
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.
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 log messages.
Settings	Click this to select a display language for the screens, or change the theme between dark and light mode.
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



The list of all Nebula devices and services that have been owned b

15 devices.

Model	MAC address	Serial Number	Name	Organization	Site
USG FLEX 500	B8:EC:A3:13:72:E4	S162L45290122			

1.3.1.1 Site/Organization/Group

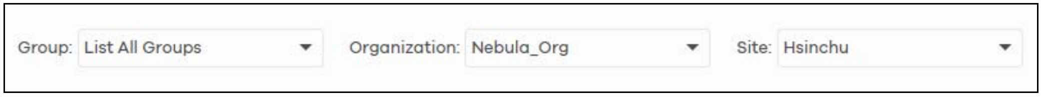
Select the site, organization and group that you want to manage.

- 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 13.2 on page 570).

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 43).
- If you need to have more sites, select **Create site** from the **Site** drop-down list box to create a new one.

Figure 6 NCC Title Bar: Group/Organization/Site



Group: List All Groups

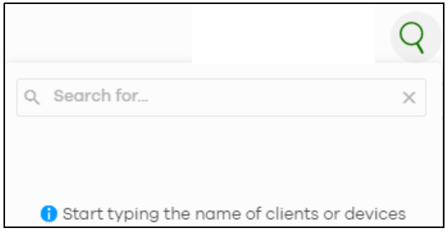
Organization: Nebula_Org

Site: Hsinchu

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

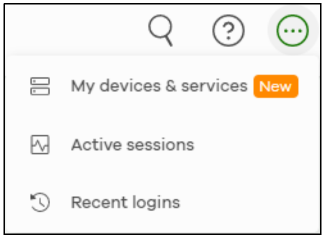


Start typing the name of clients or devices

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



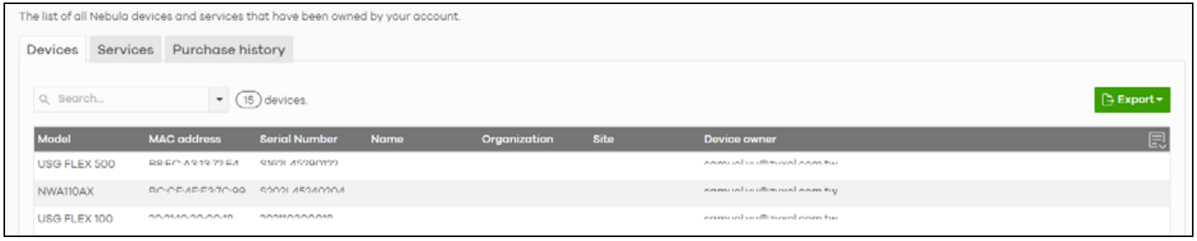
The following table describes this menu.

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, 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 > MSP cross-org manage > Admins & teams > Admins in Section 13.5.2 on page 581 for details on the organization privileges.

Figure 9 My Devices

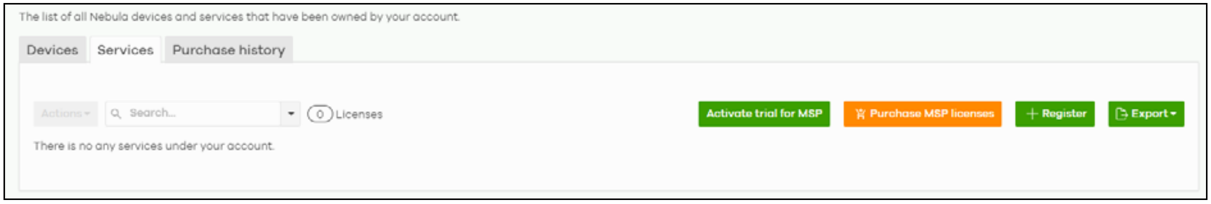


The list of all Nebula devices and services that have been owned by your account.

Model	MAC address	Serial Number	Name	Organization	Site	Device owner
USG FLEX 500	[illegible]	[illegible]				[illegible]
NWA110AX	[illegible]	[illegible]				[illegible]
USG FLEX 100	[illegible]	[illegible]				[illegible]

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 My Services

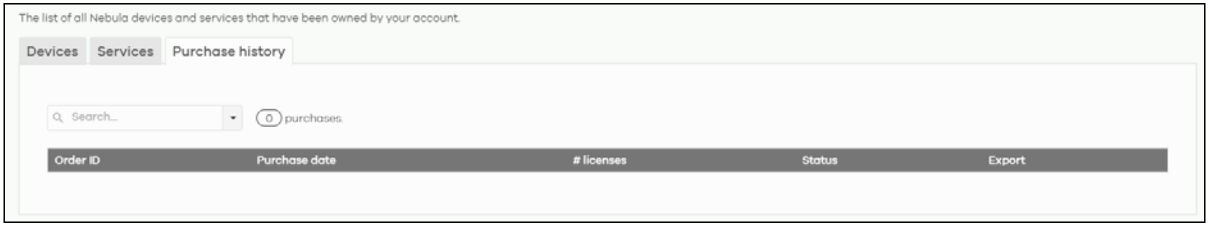


The list of all Nebula devices and services that have been owned by your account.

There is no any services under your account.

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



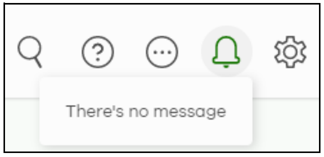
The list of all Nebula devices and services that have been owned by your account.

Order ID	Purchase date	# licenses	Status	Export

1.3.1.4 Notifications

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

Figure 12 NCC Notification

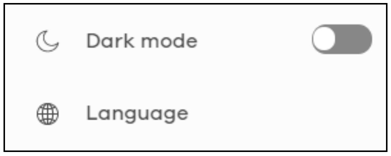


There's no message

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 13 Settings

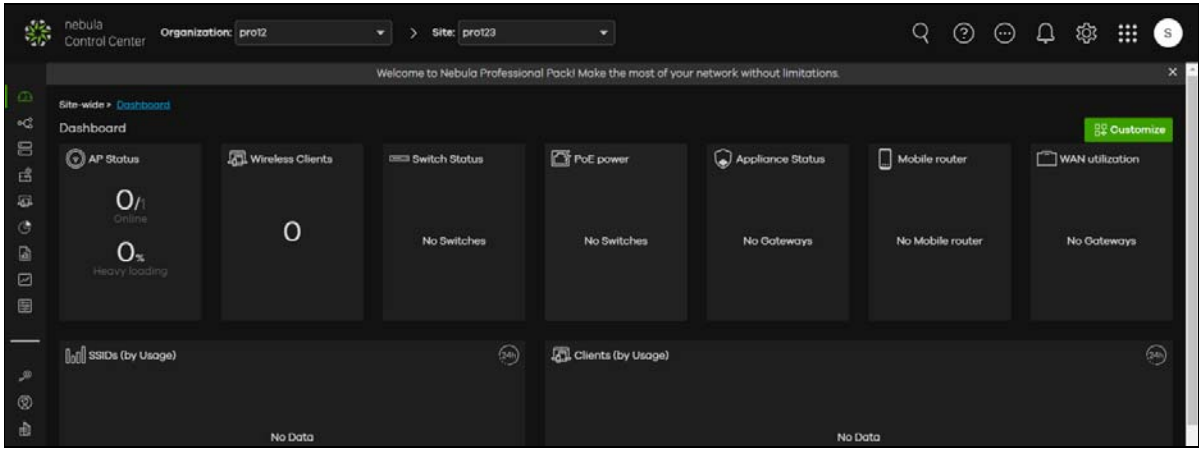


The following table describes this menu.

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.

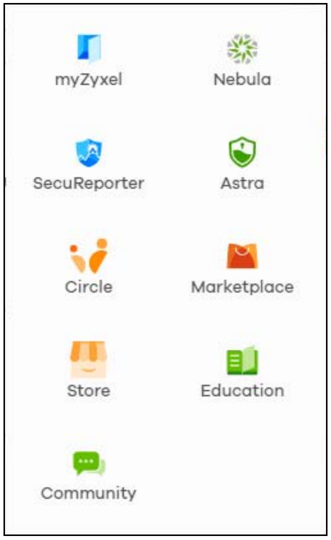
Figure 14 Dark Mode



1.3.1.6 Applications

Click this to display a list of related NCC links.

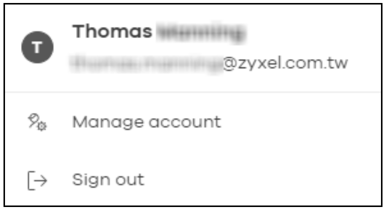
Figure 15 Related NCC Links



1.3.1.7 Account

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

Figure 16 Account



The following table describes this menu.

Table 7 Account Menu

LABEL	DESCRIPTION
Manage account	Click this to edit your account settings at myZyxel.
Sign out	Sign out of NCC.

1.3.2 Navigation Panel

Use the NCC menu items to configure network management for each site, organization and/or Nebula Device. Click the arrow («) on the upper right corner of the navigation panel to collapse or expand the navigation panel menus.

Table 8 Navigation Menus Overview

LABEL	DESCRIPTION
Use these menus to set up customer networks.	
Site-wide	Manage Nebula Devices in a site.
Organization -wide	Manage multiple network sites within an organization.

Table 8 Navigation Menus Overview (continued)

LABEL	DESCRIPTION
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.	
Mobile router	Manage the Zyxel LTE/NR devices.
Security router	Manage the SCR 50AXE.
Security gateway	Manage the ZyWALL NSG devices.
Firewall	Manage the ZyWALL ATP, USG FLEX, and USG20(W)-VPN devices (firewalls).
Switch	Manage the Zyxel Switches.
Access point	Manage the Zyxel APs (Access Points).
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 9 NCC Menu Summary

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
Site-wide	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	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.

Table 9 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
	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.
	Summary report	Use this menu to view network statistics specific to Access Points in the site.
	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.
	Threat report	Use this menu to view statistics for threat management categories.
	VPN connections	Use this menu to view status of the site-to-site VPN connections.
	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 filtering, 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 Appliance. 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 filtering, Intrusion Detection and Prevention (IDP), application patrol, and anti-virus.
	Summary report	Use this menu to view network statistics specific to the Security Appliance in the site.
	Containment list	Use this menu to view and manage Nebula Devices contained by CDR (Collaborative Detection & Response).
	Site features logs	Use this menu to view log messages about configuration changes made by the NCC for the site.

Table 9 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
	Configure	
	WiFi SSID settings	Use this menu to view and configure SSID settings and authentication methods.
	Access points	
	SSID advanced settings	Use this menu to configure network access, traffic options and advanced settings for SSID profiles.
	Captive portal customization	Use this menu to configure captive portal settings for SSID profiles.
	SSID availability	Use this menu to configure SSID visibility settings and set whether the SSID is enabled or disabled on each day of the week.
	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.
	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 9 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.
	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.
	Interface	Use this menu to configure interface address, subnet mask and VLAN ID settings on the Security Firewall.
	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 filtering 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.
	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.

Table 9 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
	Security gateway	
	Interface addressing	Use this menu to configure network mode, port grouping, interface address, static route and DDNS settings on the Security Appliance.
	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 filtering and block access to specific web sites. You can also enable Anti-virus and Intrusion Detection and Prevention (IDP) on the Security Appliance.
	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 Appliance 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 Appliance can use in authenticating users. You can also specify walled garden web site links for all interfaces on the Security Appliance.
	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 9 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 filtering 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 9 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.
	Cross-org synchronization	Use this menu to sync or clone organization-wide settings from a source organization to a destination organization.
	Alert templates	Use this menu to configure **MSP alert template**s to monitor Nebula Devices for unexpected events (for example, online or offline events).
	Admins & teams	Use this menu to create administrators or groups of administrators (teams) and view their login details.
	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 at myZyxel 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 11.2 on page 492.

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.

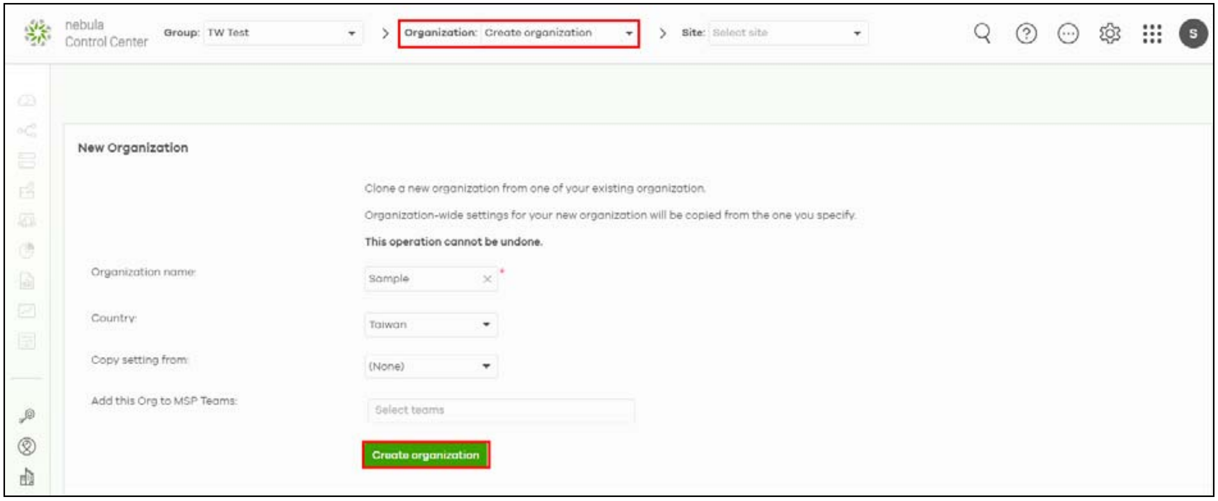
1 Click **Create Organization** from the **Organization** drop-down list box in the title bar. The Wizard starts. See Chapter 2 on page 46 for detailed information about how to use the wizard to create an organization and site. Otherwise, click **Exit Wizard** to close the wizard and display the **Create 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 17 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

Create organization

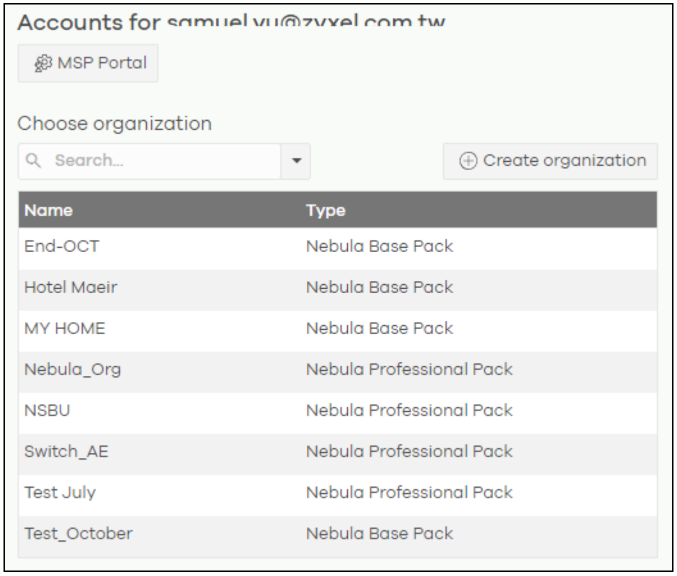
5 Choose whether to activate a one-month trial of Nebula Pro Pack and Nebula Security Services for the organization. For example, USG FLEX 700, Secure WiFi License, 1MO; USG FLEX 700, UTM Security Pack License, 1MO; Nebula Professional Pack License, 1MO.

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 18 Choose Organization



Accounts for samuel.yu@zyxel.com.tw

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 Cloud-Saving Mode

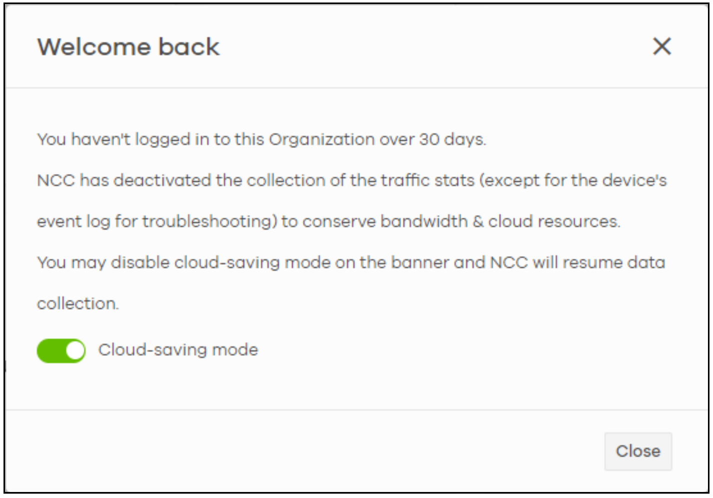
If you do not log into a base (free) license tier organization for over 30 days, the organization automatically enters Cloud-saving mode to save your network bandwidth and cloud resources.

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 19 Cloud-saving mode



Welcome back

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

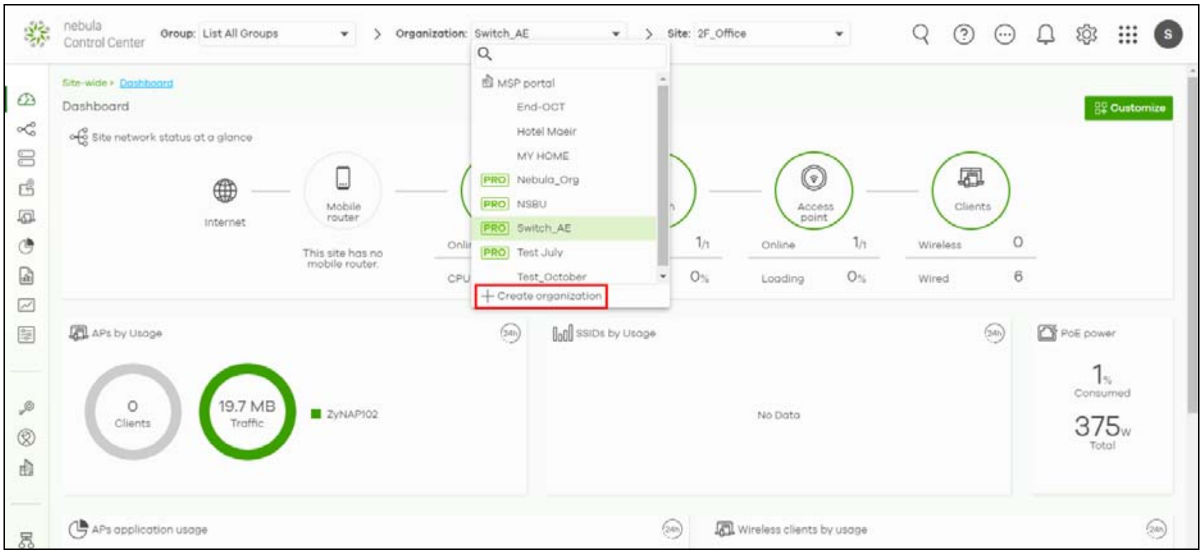
NCC has deactivated the collection of the traffic stats (except for the device's event log for troubleshooting) to conserve bandwidth & cloud resources.

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

CHAPTER 2 Setup Wizard

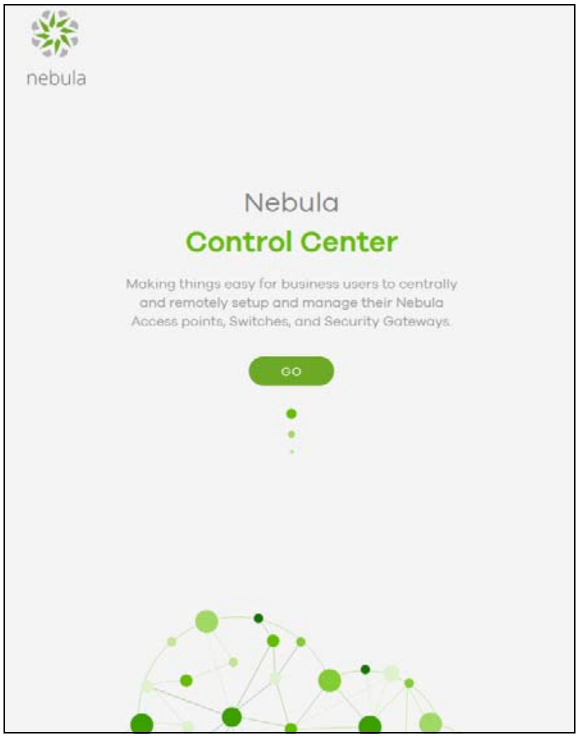
2.1 Setup Wizard

- 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

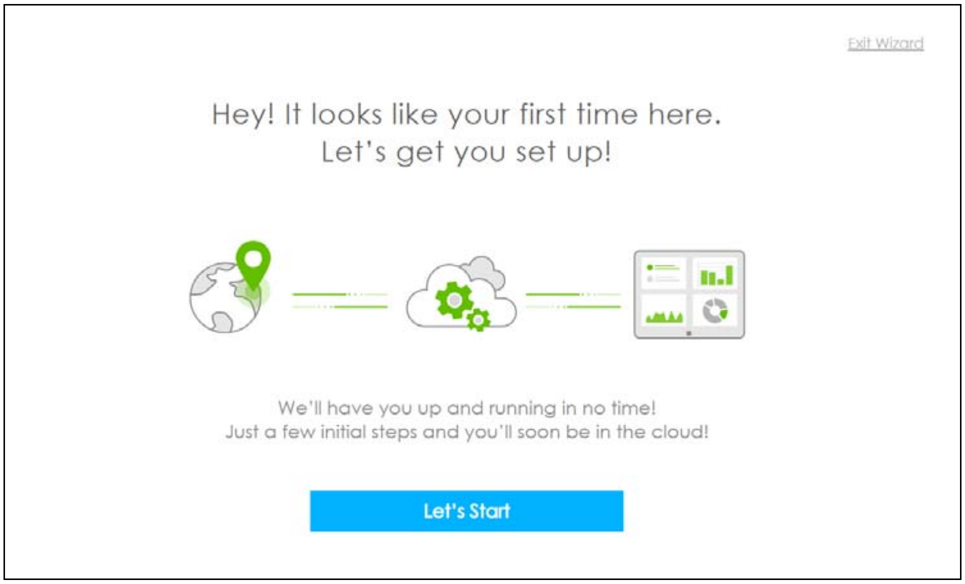
1 After logging in to https://nebula.zyxel.com, the following screen appears. Click **GO** to start the NCC wizard.



Nebula
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!

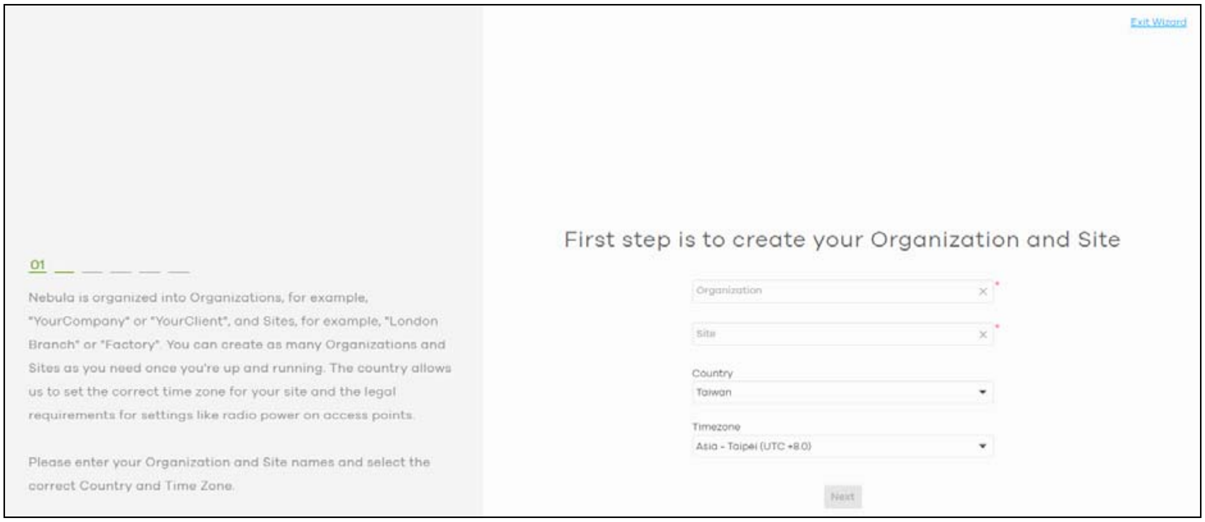
Note: This screen will appear only if you have not created a new organization.

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.



Nebula is organized into Organizations, for example, "YourCompany" or "YourClient", and Sites, for example, "London Branch" or "Factory". You can create as many Organizations and Sites as you need once you're up and running. The country allows us to set the correct time zone for your site and the legal requirements for settings like radio power on access points.

Please enter your Organization and Site names and select the correct Country and Time Zone.

First step is to create your Organization and Site

Organization *

Site *

Country: Taiwan

Timezone: Asia - Taipei (UTC +8.0)

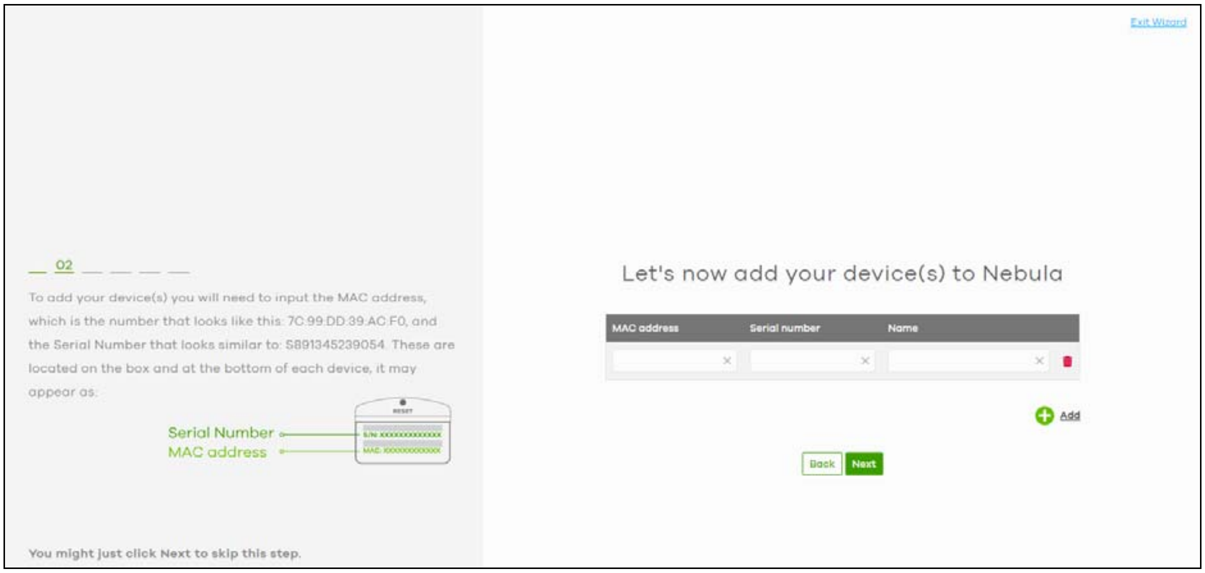
2.1.3 Step 3: Add Your Nebula Devices

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.



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

2.1.4 Step 4: 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).

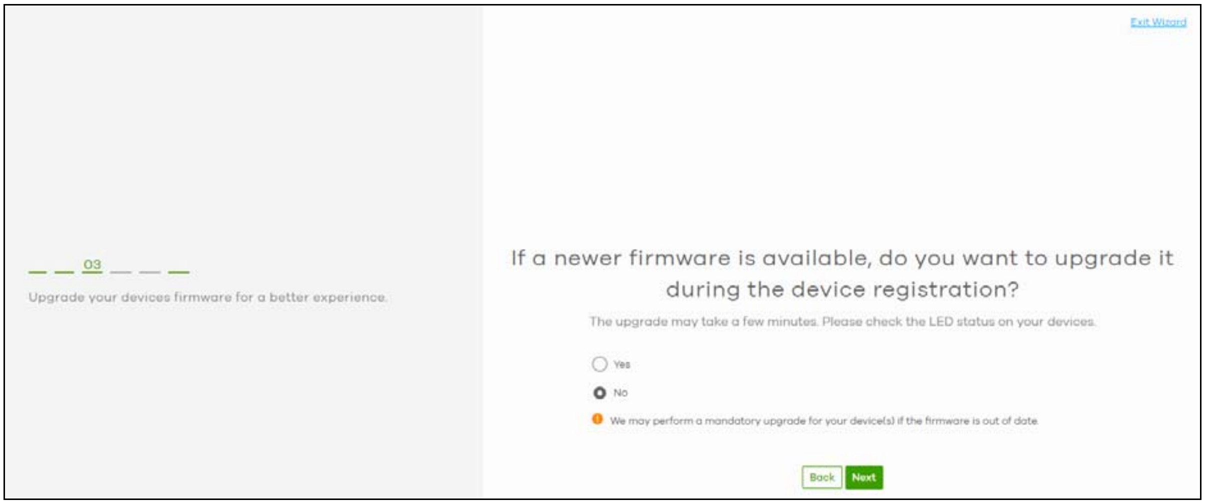
Even if you choose not to upgrade the firmware, NCC will still perform a mandatory upgrade to **Stable** firmware version if the Nebula Device's firmware have security vulnerabilities, and/or lack key performance improvements. See Table 176 on page 538 for the description of a **Stable** firmware.

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

Table 10 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 / Firewalls / Security Gateways	The mandatory firmware upgrade occurs after registering the Nebula Device on NCC.

Click **Next** to proceed.



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

We may perform a mandatory upgrade for your device(s) if the firmware is out of date.

2.1.5 Step 5: Set up your WiFi Network

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

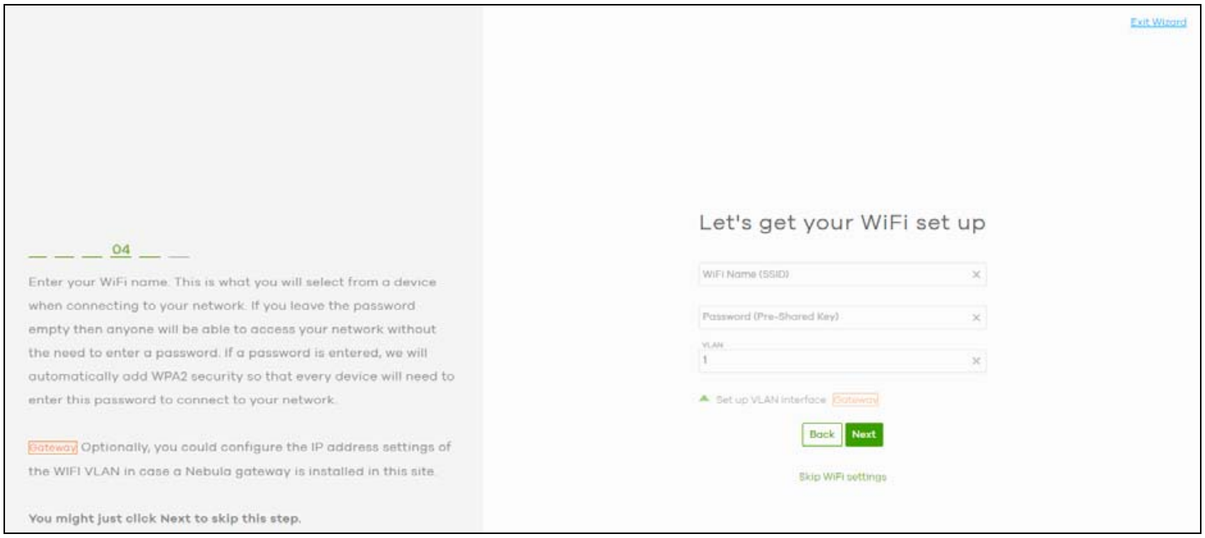
You can also leave the fields blank and click **Next** to move on to the next step without setting up the main WiFi network.

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

Set up VLAN interface Gateway

2.1.6 Step 6: 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.

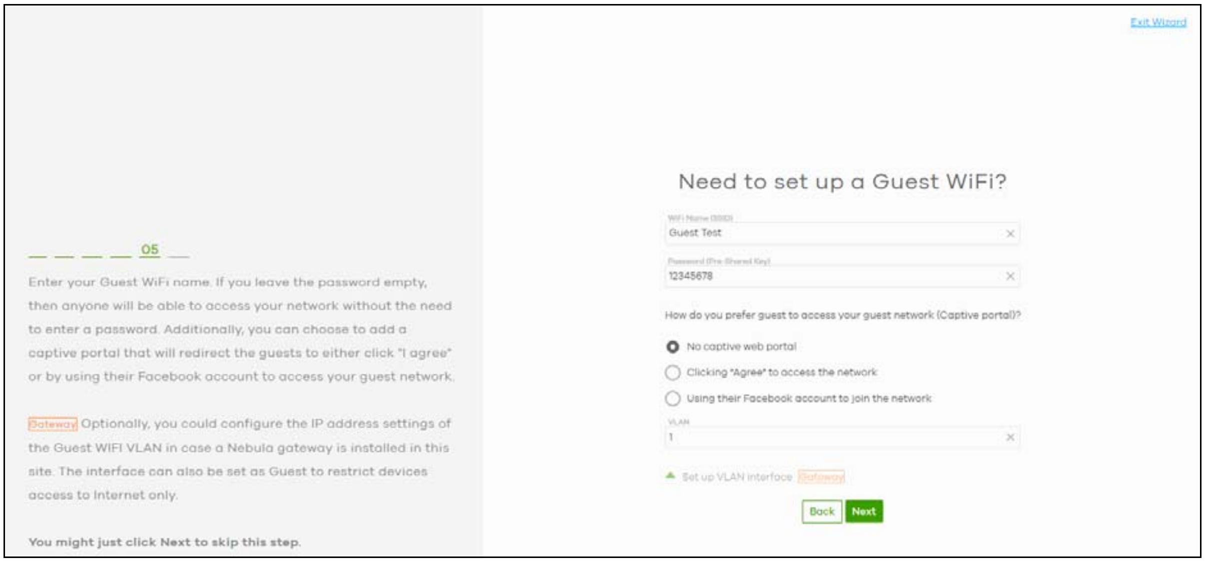
Note: If you do not enable any WiFi security, your network is accessible to any WiFi networking device that is within range.

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.

Need to set up a Guest WiFi?

WiFi Name (SSID): Guest Test

Password (Pre-Shared Key): 12345678

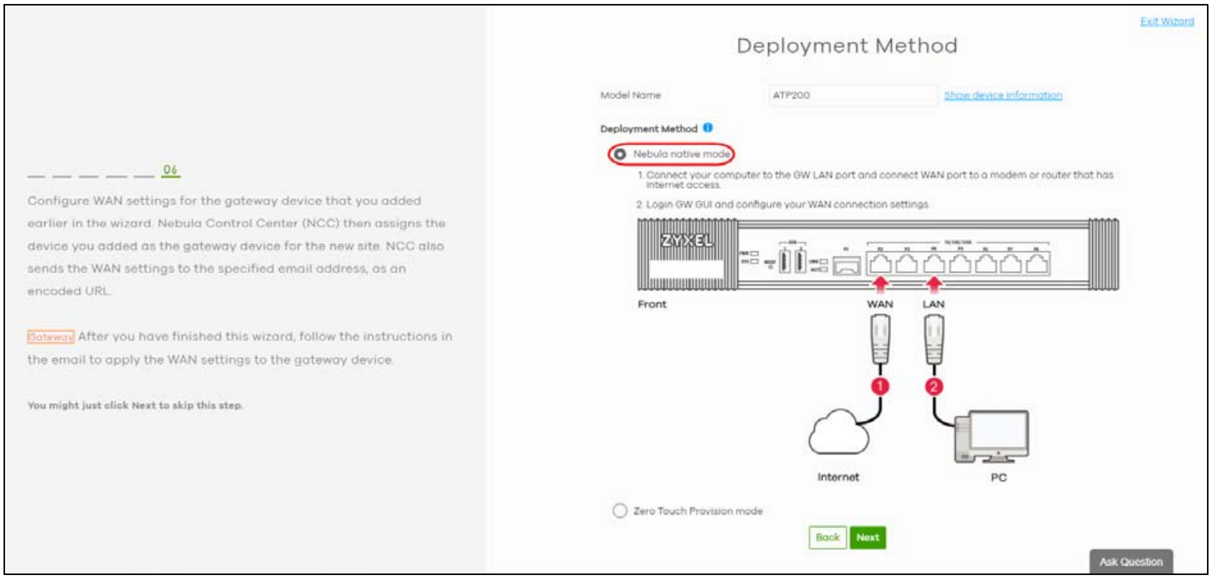
How do you prefer guest to access your guest network (Captive portal)?

● No captive web portal
○ Clicking "Agree" to access the network
○ Using their Facebook account to join the network

VLAN: 1

2.1.7 Step 7: 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.

Deployment Method

Model Name: ATP200

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

2.1.7.1 Nebula Native Mode

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

2.1.7.2 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).

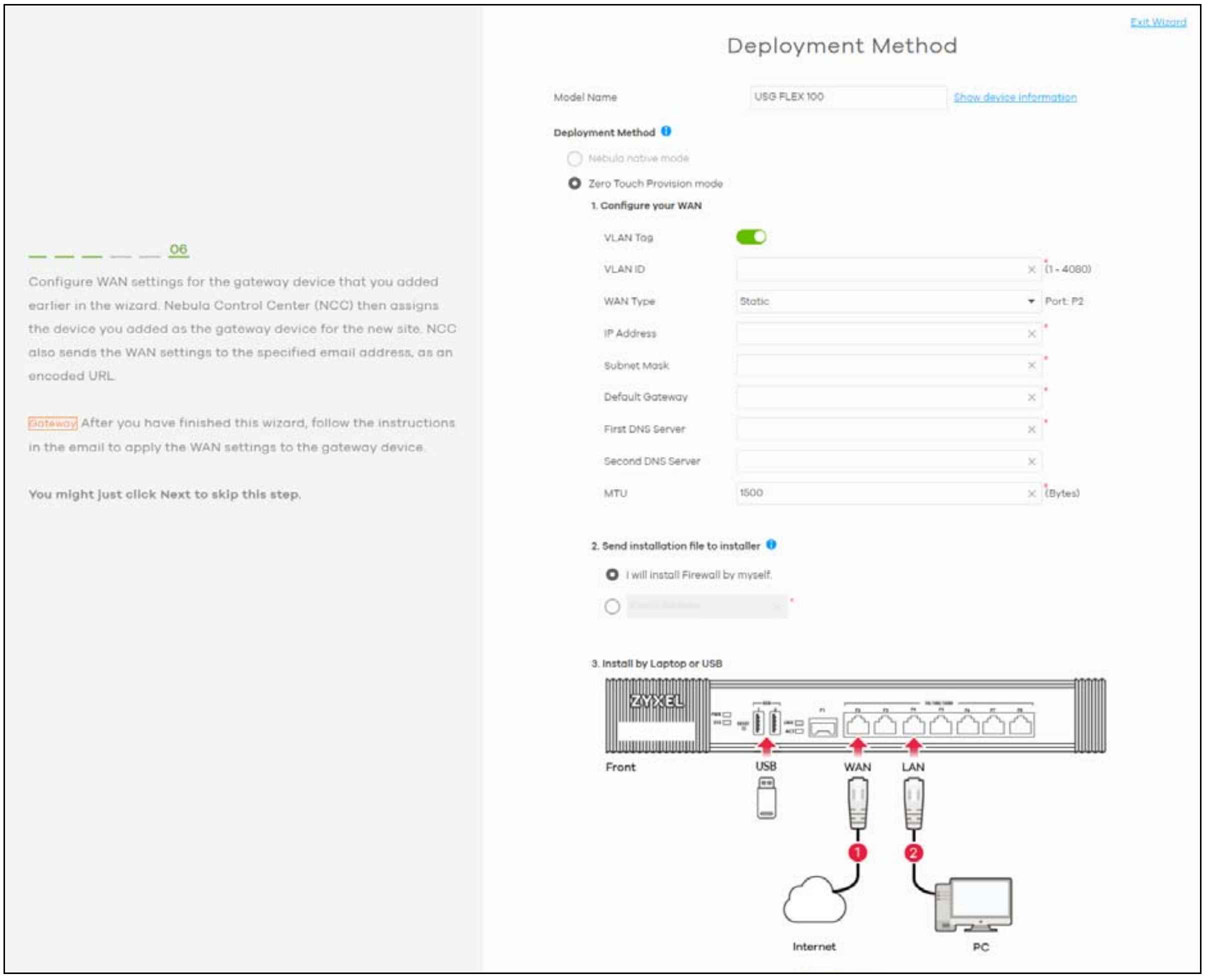
Note: Configure the VLAN ID and WAN interface for the Nebula Device exactly as your ISP gave it to you.

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

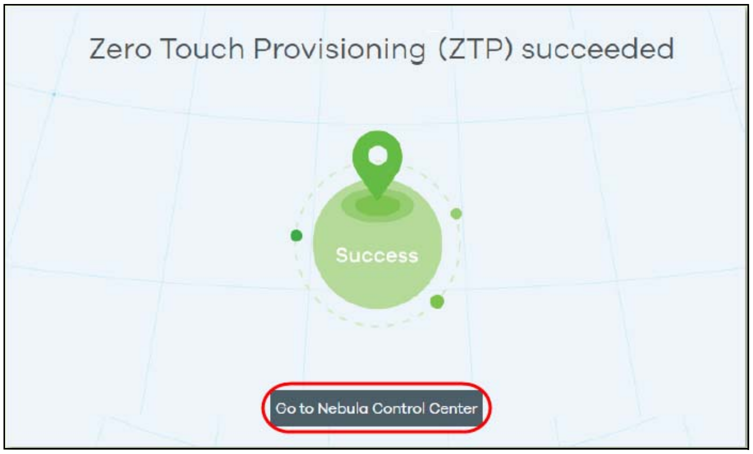
1 Back up the current configuration (in case you want to return to On Premises mode later).

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.

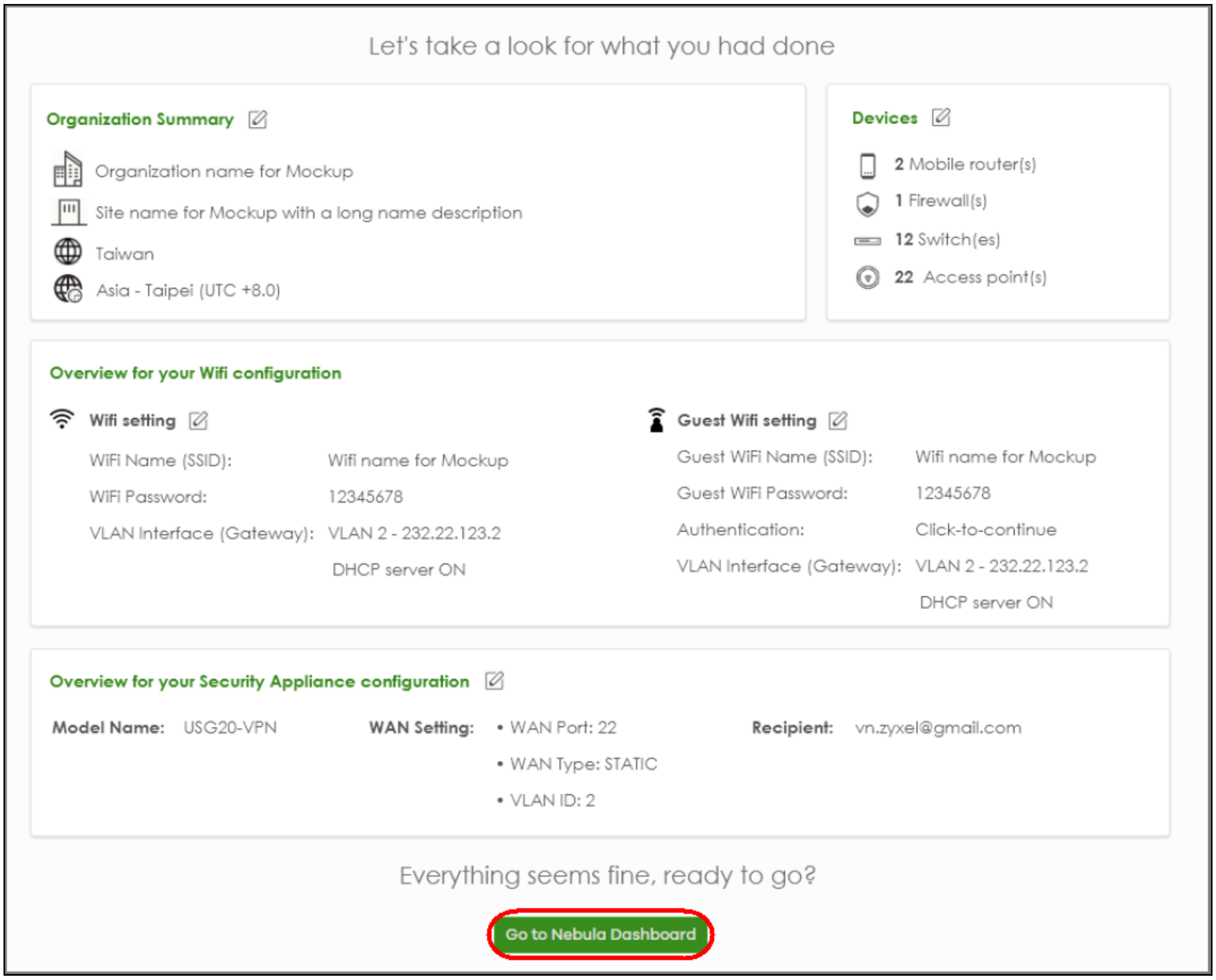
Note: Refer to the Nebula Device User's Guide for more information.

2.1.8 Step 8: 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 name for Mockup

Site name for Mockup with a long name description

Taiwan

Asia - Taipei (UTC +8.0)

Devices

2 Mobile router(s)

1 Firewall(s)

12 Switch(es)

22 Access point(s)

Overview for your Wifi configuration

Wifi setting

WiFi Name (SSID):	Wifi name for Mockup
WiFi Password:	12345678
VLAN Interface (Gateway):	VLAN 2 - 232.22.123.2 DHCP server ON

Guest Wifi setting

Guest WiFi Name (SSID):	Wifi name for Mockup
Guest WiFi Password:	12345678
Authentication:	Click-to-continue
VLAN Interface (Gateway):	VLAN 2 - 232.22.123.2 DHCP server ON

Overview for your Security Appliance configuration

Model Name: USG20-VPN

WAN Setting:
- WAN Port: 22
- WAN Type: STATIC
- VLAN ID: 2

Recipient: vn.zyxel@gmail.com

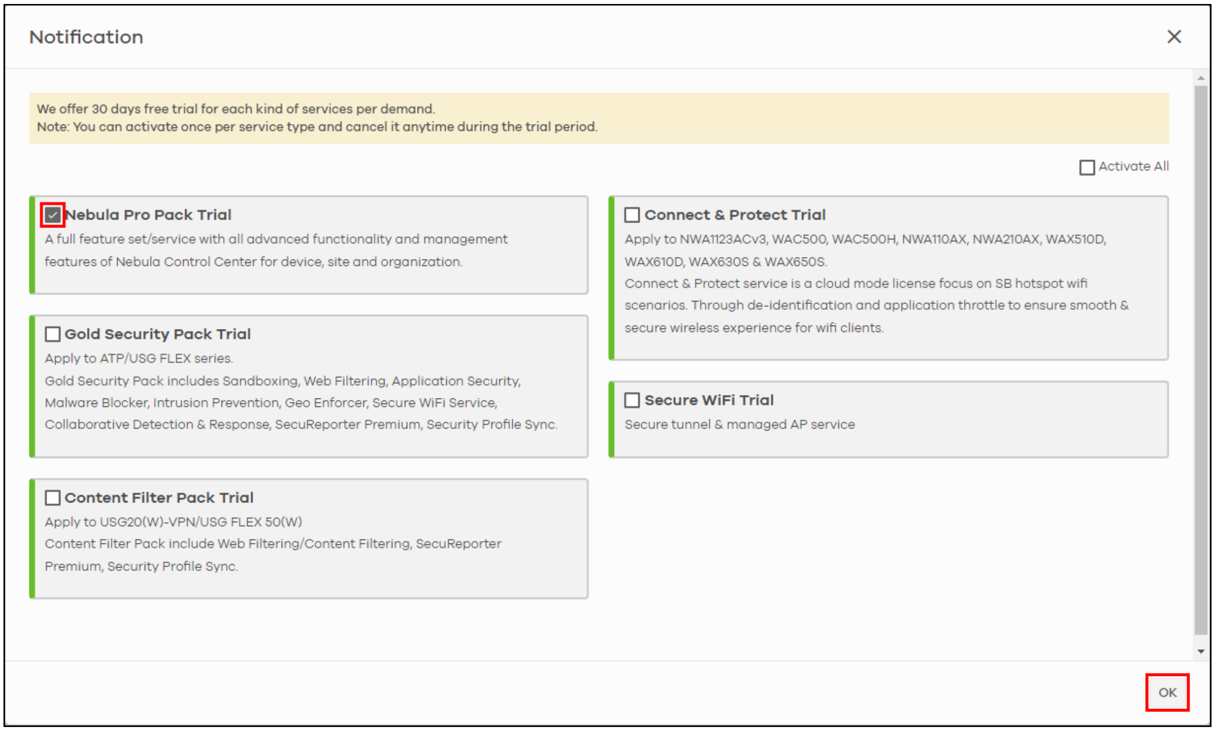
Everything seems fine, ready to go?

2.1.9 Step 9: Activate the Trial License(s)

After setting up the wizard, the following screen will appear. 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 11.2.8 on page 505 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 **OK**. NCC will send you an email reminding you to purchase the full license when the trial is close to expiring.



Notification

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.

□ 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.

□ **Connect & Protect Trial**
Apply to NWA1123ACv3, WAC500, WAC500H, NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S & WAX650S.
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.

□ **Gold Security Pack Trial**
Apply to ATP/USG FLEX series.
Gold Security Pack includes Sandboxing, Web Filtering, Application Security, Malware Blocker, Intrusion Prevention, Geo Enforcer, Secure WiFi Service, Collaborative Detection & Response, SecuReporter Premium, Security Profile Sync.

□ **Secure WiFi Trial**
Secure tunnel & managed AP service

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

Note: To set the administrator privileges, see Section 13.5.1 on page 581 for more information.

CHAPTER 3 Tutorials

3.1 Overview

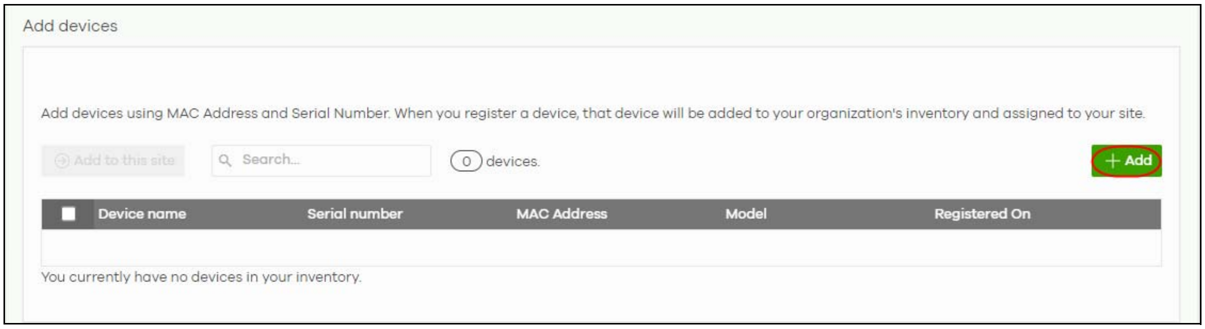
This chapter shows you how to use the NCC's various features.

- 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
- Reset the Nebula Password
- Change an Organization and/or Site Name
- Maintain Firmware
- 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
- Resolve WiFi Connection Problems (for Nebula APs 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)
- Configure DHCP Domain Name (for Security Firewalls in Nebula)

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

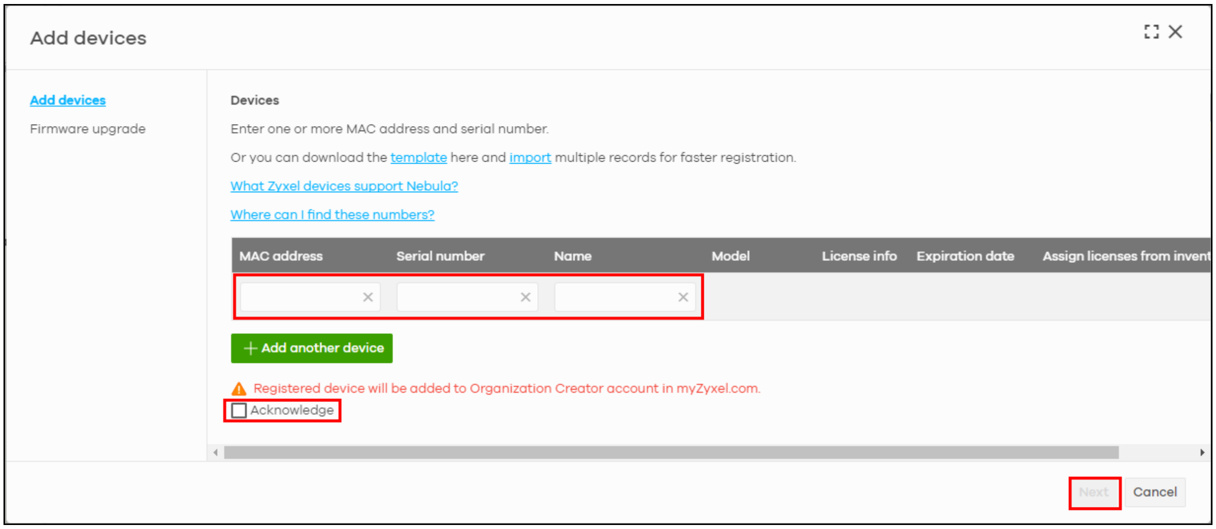
Add devices using MAC Address and Serial Number. When you register a device, that device will be added to your organization's inventory and assigned to your site.

☐	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.



Add devices

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 17 for a summary of NCC licenses.

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

Table 11 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
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 device
Site-wide	SCR Pro	SCR 50AXE

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

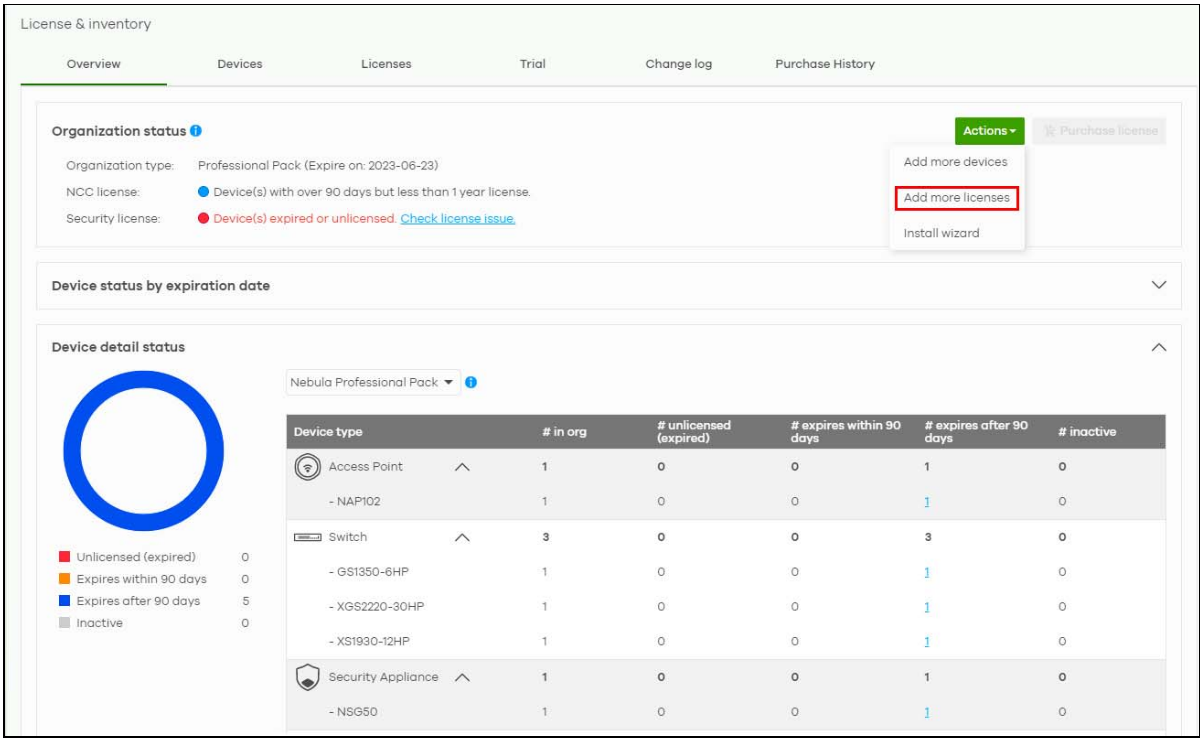
The following are the license states in NCC.

- Active – the license pack is assigned to a Nebula Device, is activated, and is in use (expiration countdown/timer has started).
- Queued – the license pack is assigned to a Nebula Device, is activated, but not yet in use.
- Inactive – the license pack is assigned to a Nebula Device, but is not yet activated in NCC.
- Unused – The license pack is assigned to an organization, but is not yet assigned to a Nebula Device and not yet activated in NCC.

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**.



Organization status

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

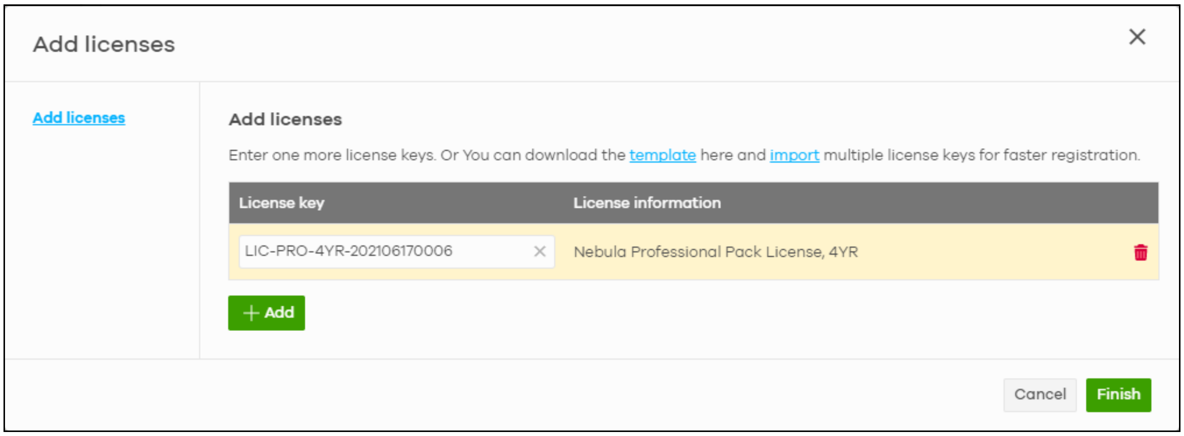
Device detail status

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	1	0	0	1	0
- NSG50	1	0	0	1	0

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



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

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.

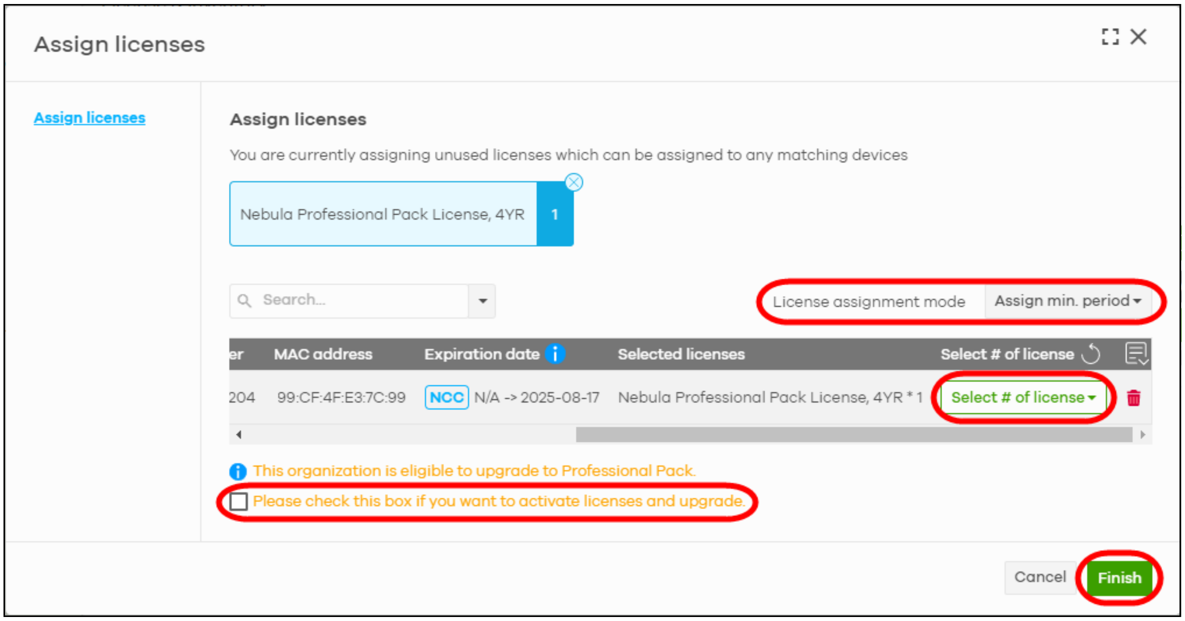
6 Clear any license that you do not want added to the Nebula Device.

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

Assign licenses

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

Nebula Professional Pack License, 4YR 1

Search...

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

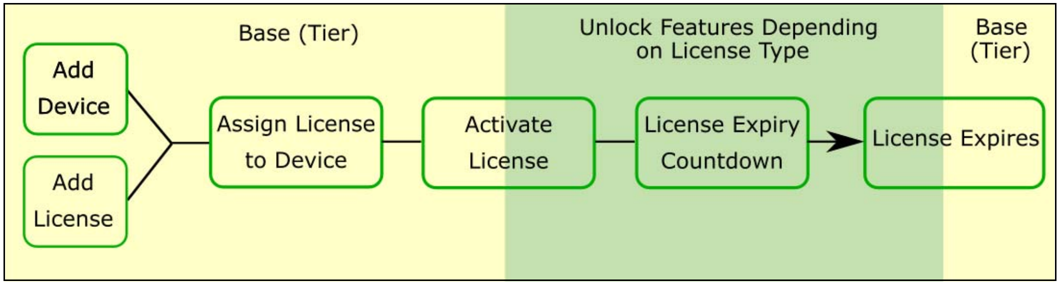
This organization is eligible to upgrade to Professional Pack.

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

Cancel Finish

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

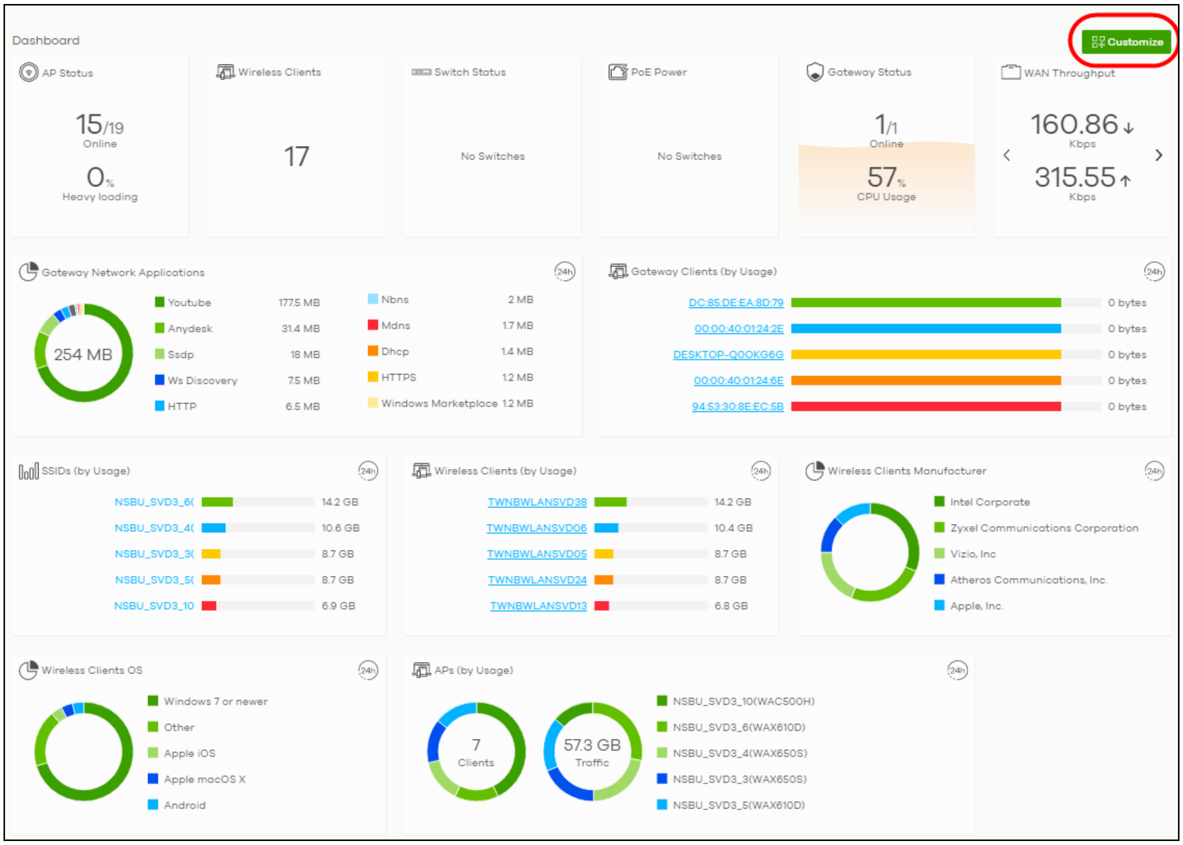
Figure 20 License Activation Process



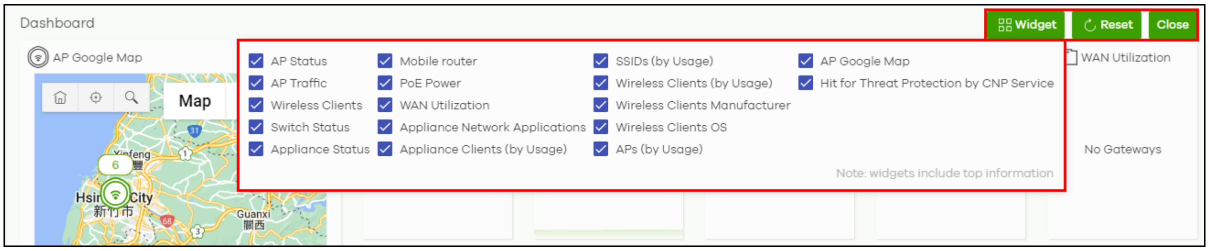
3.4 Monitor a Site

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.

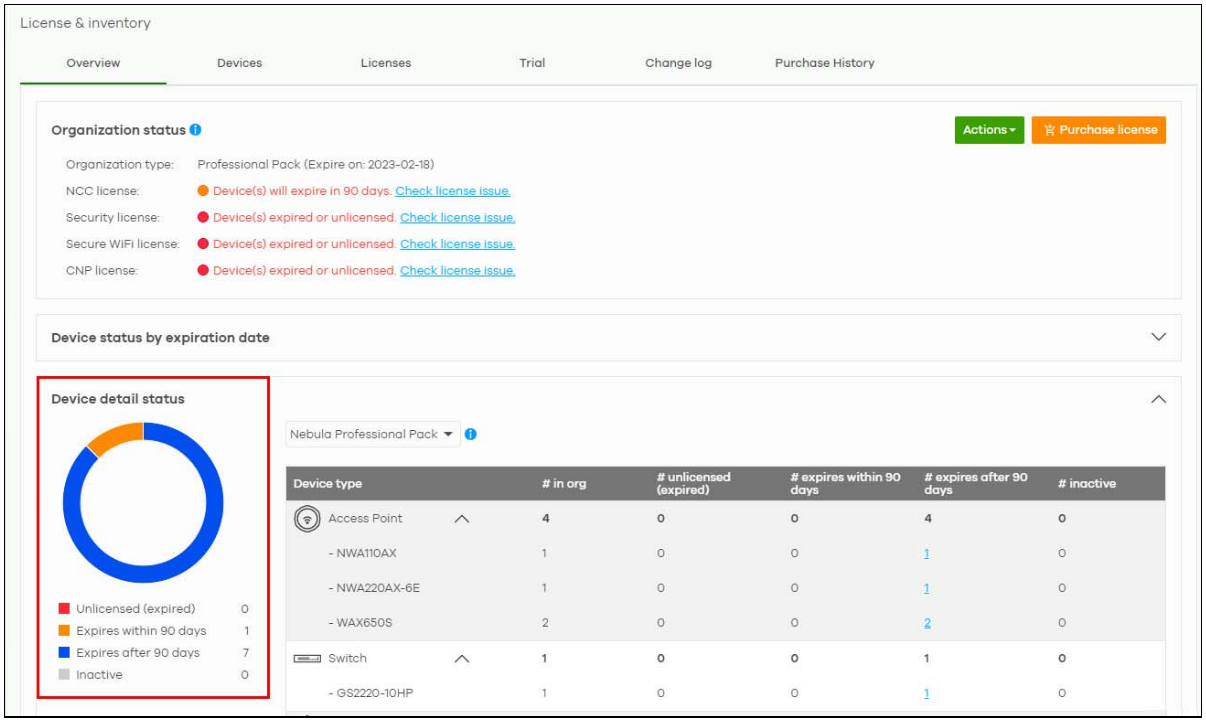


☑ AP Status
☑ AP Traffic
☑ Wireless Clients
☑ Switch Status
☑ Appliance Status
☑ Mobile router
☑ PoE Power
☑ WAN Utilization
☑ Appliance Network Applications
☑ Appliance Clients (by Usage)
☑ SSIDs (by Usage)
☑ Wireless Clients (by Usage)
☑ Wireless Clients Manufacturer
☑ Wireless Clients OS
☑ APs (by 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.



License & inventory

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

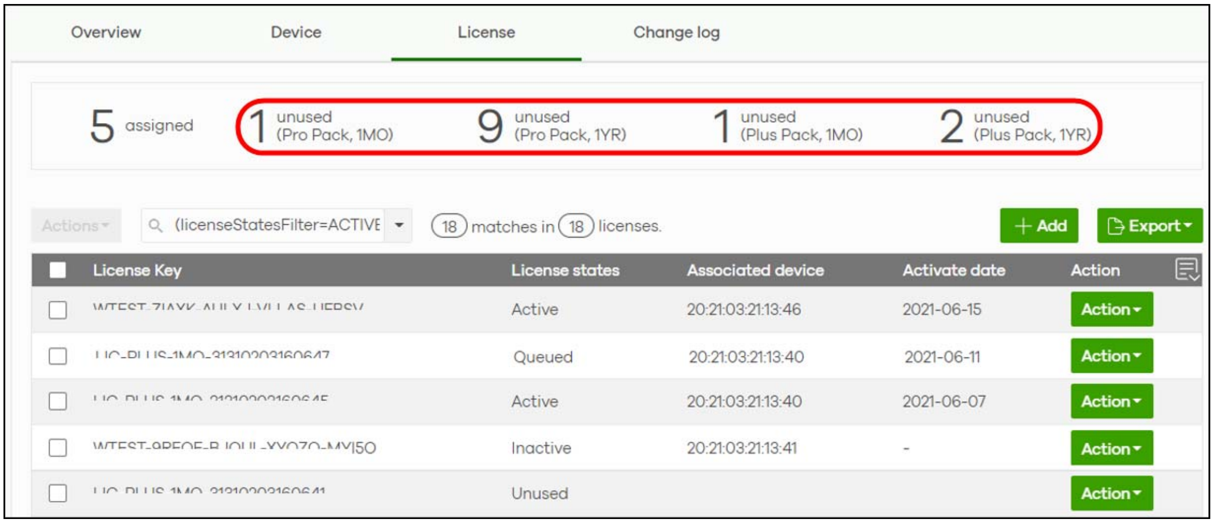
The license health is shown in the **Device detail status** and the following are the definition:

- 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 23 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)

(licenseStatesFilter=ACTIVE 18 matches in 18 licenses.

☐	License Key	License states	Associated device	Activate date	Action
☐	WTEST-ZIAYK-ALILY-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-RJOLJI-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 check box and click **Action**. Then click **Assign license**. See Section 3.3.3 on page 59 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 23 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:

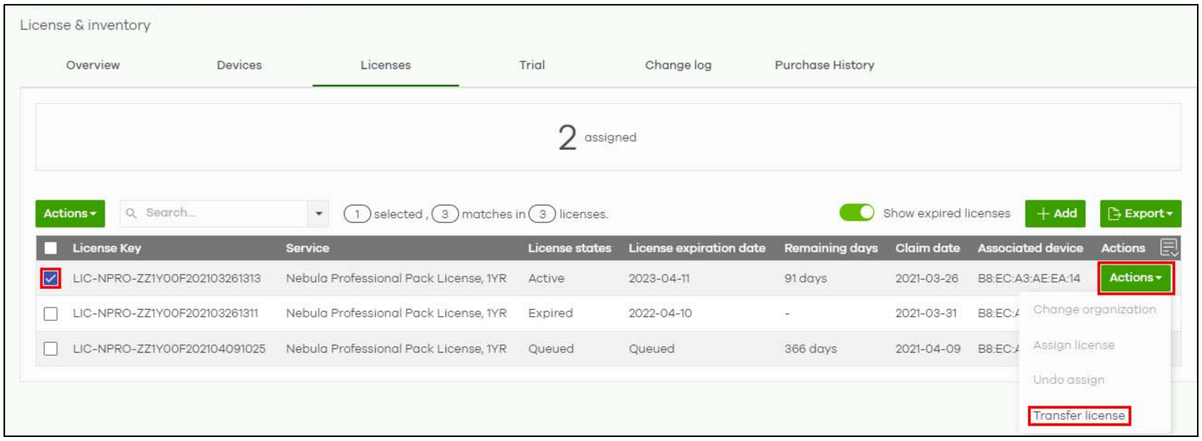
- The Nebula Devices must have the same owner.
- Bundled, Trial, and Promotion licenses cannot be transferred. (See Table 159 for more information.)
- If the license transfer causes the Nebula Devices in the organization to be without a valid license, the organization automatically downgrades to the 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 ▾

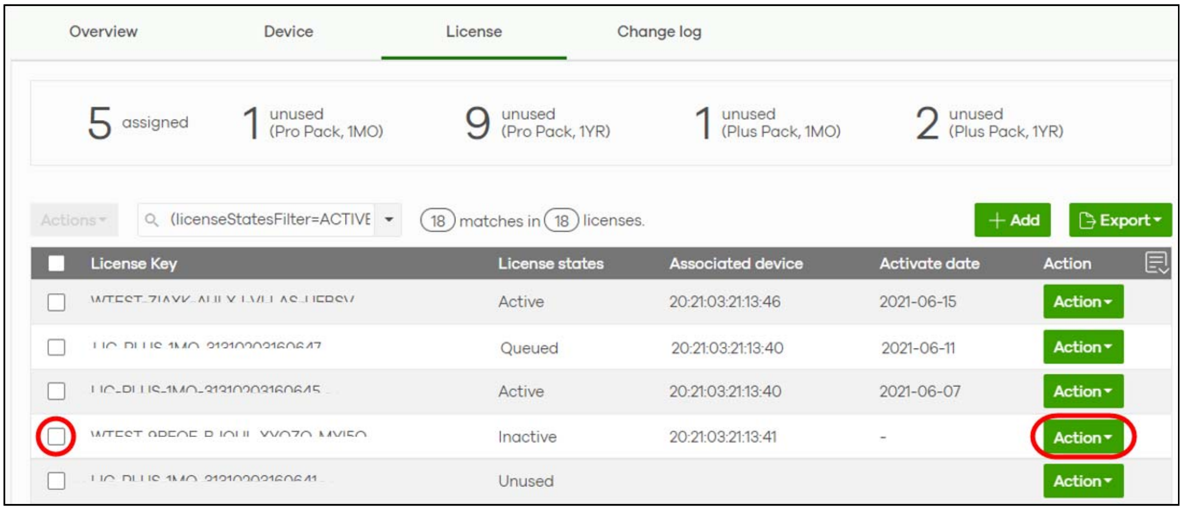
☐	License Key	Service	License states	License expiration date	Remaining days	Claim date	Associated device	Actions
☑	LIC-NPRO-ZZ1Y00F202103261313	Nebula Professional Pack License, 1YR	Active	2023-04-11	91 days	2021-03-26	B8:EC:A3:AE:EA:14	Actions ▾
☐	LIC-NPRO-ZZ1Y00F202103261311	Nebula Professional Pack 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-LVLI-AS-UFBSV	Active	20:21:03:21:13:46	2021-06-15	Action ▾
☐	LIC-PLUS-1MO-21210203160647	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-9BFOF-DJOUL-XYQZO-MYI5Q	Inactive	20:21:03:21:13:41	-	Action ▾
☐	LIC-PLUS-1MO-21210203160641	Unused			Action ▾

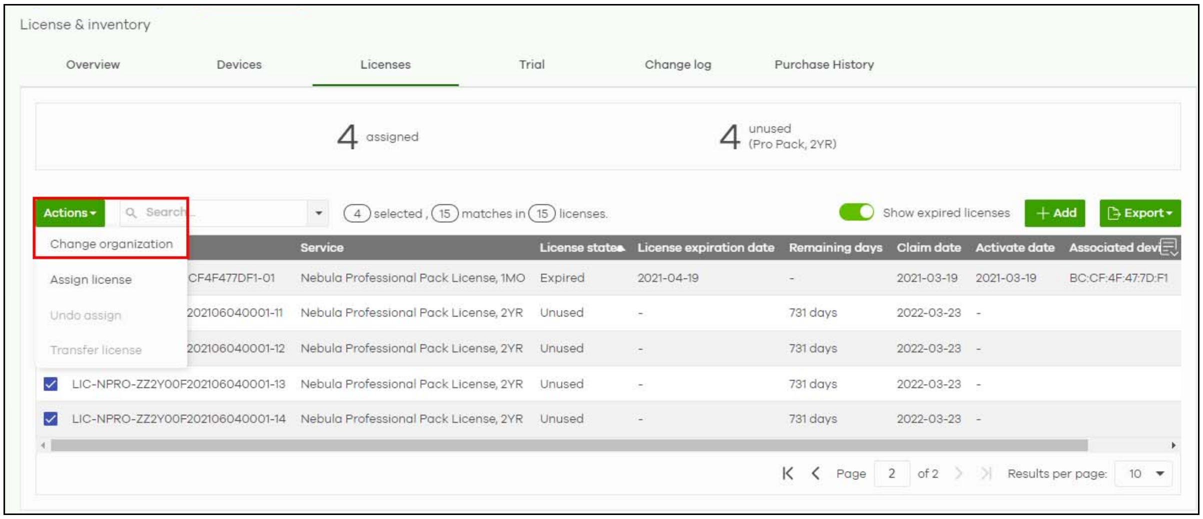
3.7.3 Transfer a License to a Different Organization

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

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

4 assigned

4 unused (Pro Pack, 2YR)

Actions ▾ | Search...

(4) selected , (15) matches in (15) licenses.

Show expired licenses | + Add | Export ▾

Change organization

Assign license

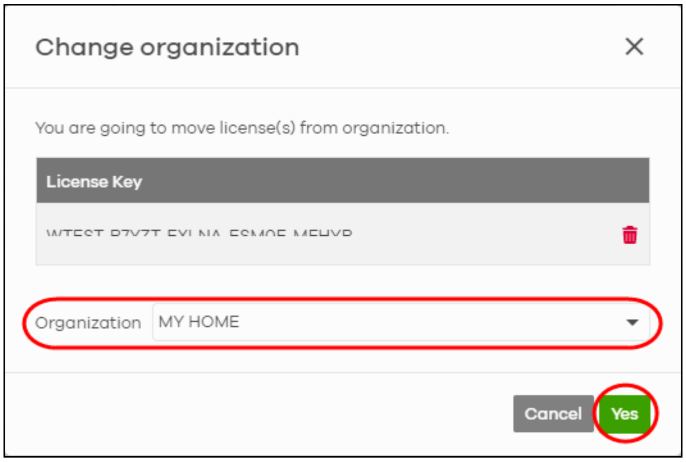
Undo assign

Transfer license

		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-P7V7T-EYLNA-ESMOE-MEHYP

Organization: MY HOME

Cancel | Yes

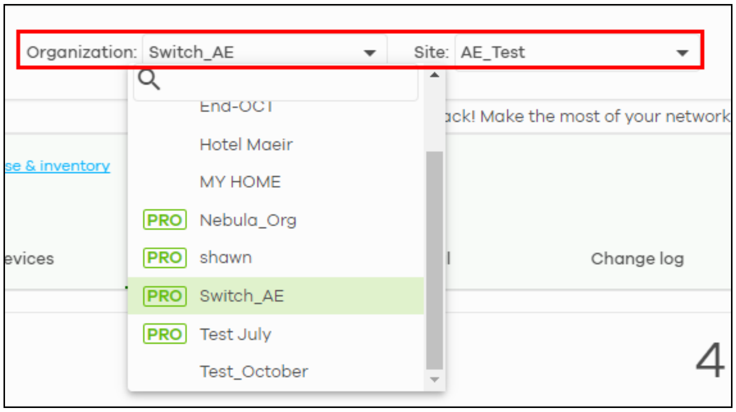
You have successfully transferred a license to another organization, but without assigning it to a Nebula Device yet.

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:

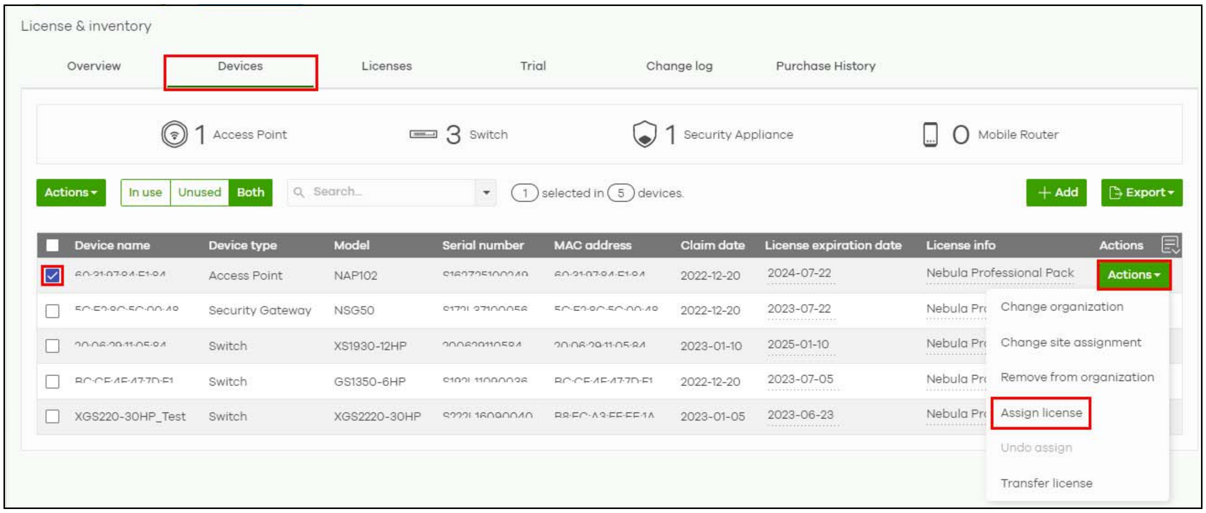
1 Perform the steps mentioned in Transfer a License to a Different Organization.

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



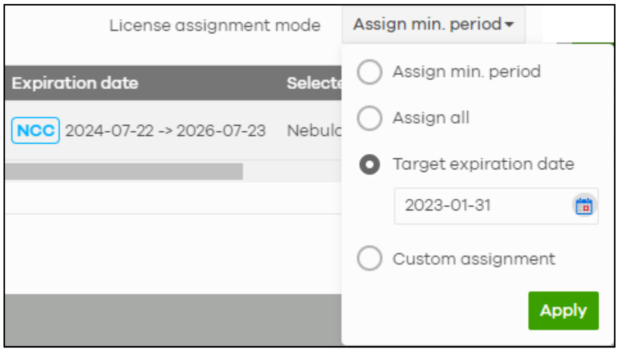
3 Go to the **Organization-wide** > **Configure** > **License & inventory** > **Device** screen.

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



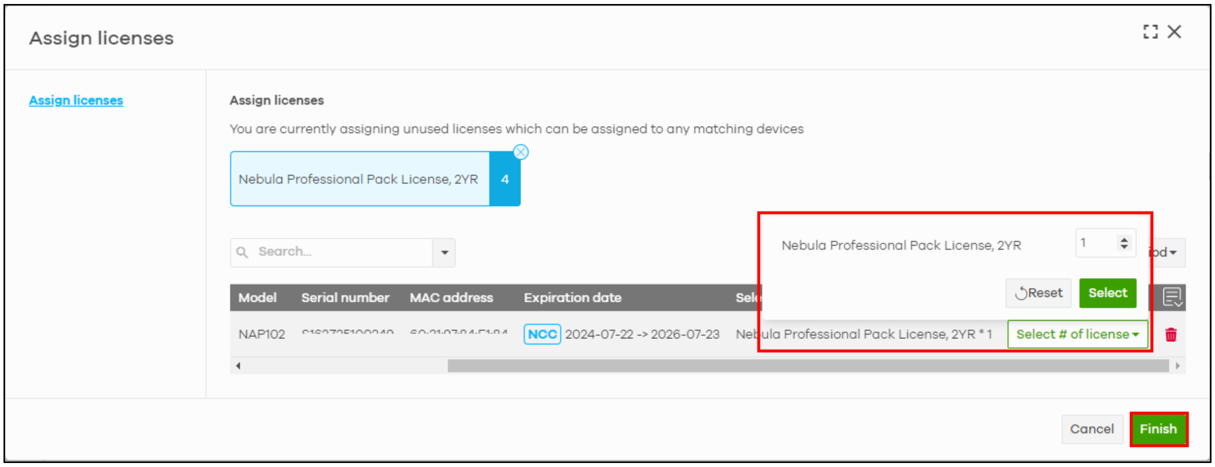
	Device name	Device type	Model	Serial number	MAC address	Claim date	License expiration date	License info	Actions
☑	60:31:07:94:E1:94	Access Point	NAP102	S162725100240	60:31:07:94:E1:94	2022-12-20	2024-07-22	Nebula Professional Pack	Actions
□	5C:E2:8C:5C:00:48	Security Gateway	NSG50	S172L37100056	5C:E2:8C:5C:00:48	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:E1	Switch	GS1350-6HP	S192L11090036	BC:CF:4F:47:7D:E1	2022-12-20	2023-07-05	Nebula Pro	
□	XGS220-30HP_Test	Switch	XGS2220-30HP	S222L16090040	B8:EC:A3:EE: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

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

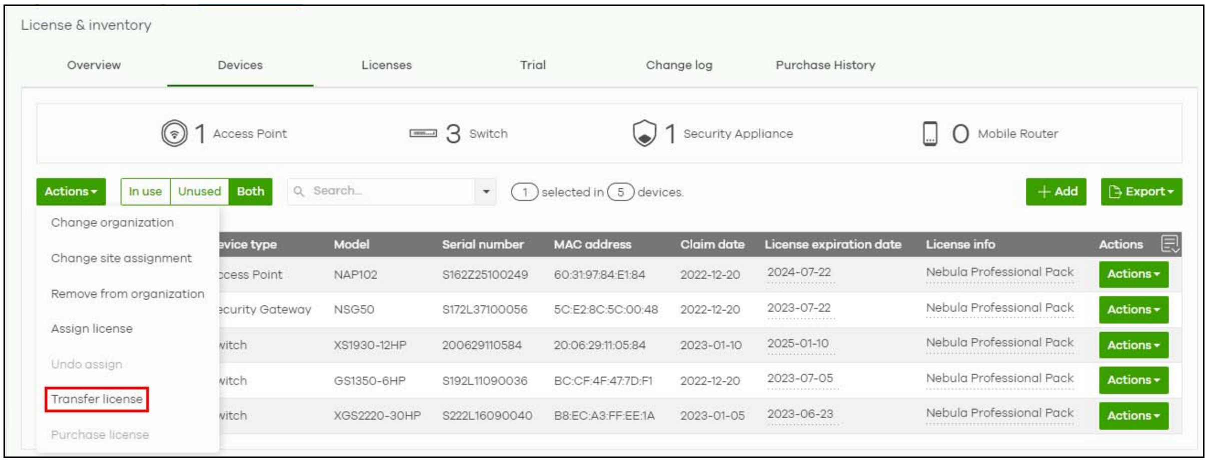
To transfer a license(s) to a Nebula Device in the new organization, do the following:

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**.



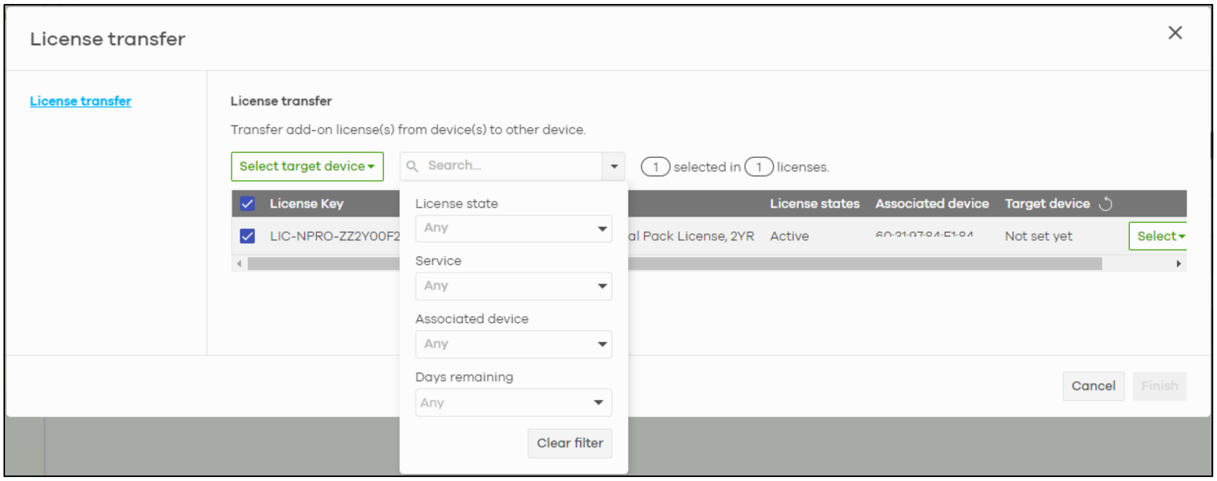
License & inventory

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 transfer

License transfer

Transfer add-on license(s) from device(s) to other device.

1 selected in 1 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

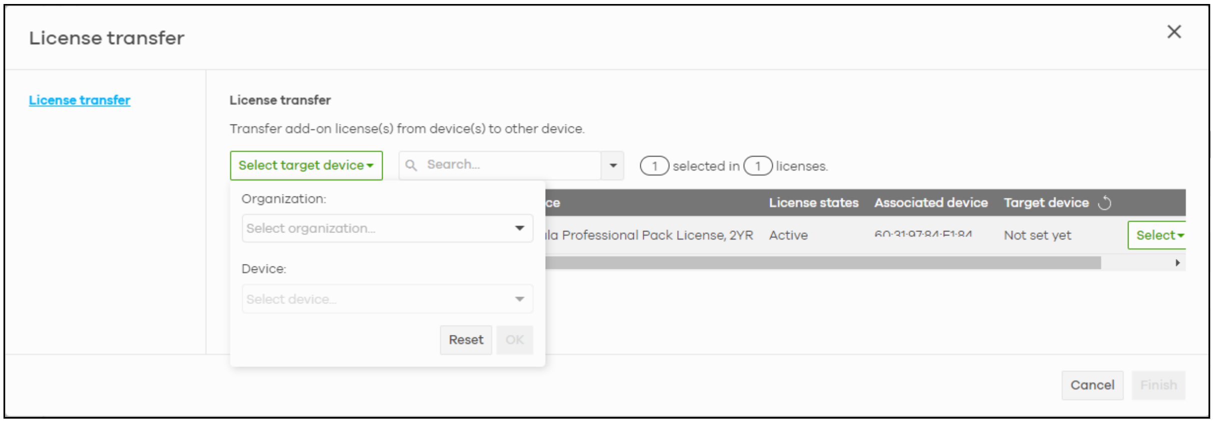
License state: Any

Service: Any

Associated device: Any

Days remaining: Any

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.



License transfer

License transfer

Transfer add-on license(s) from device(s) to other device.

1 selected in 1 licenses.

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

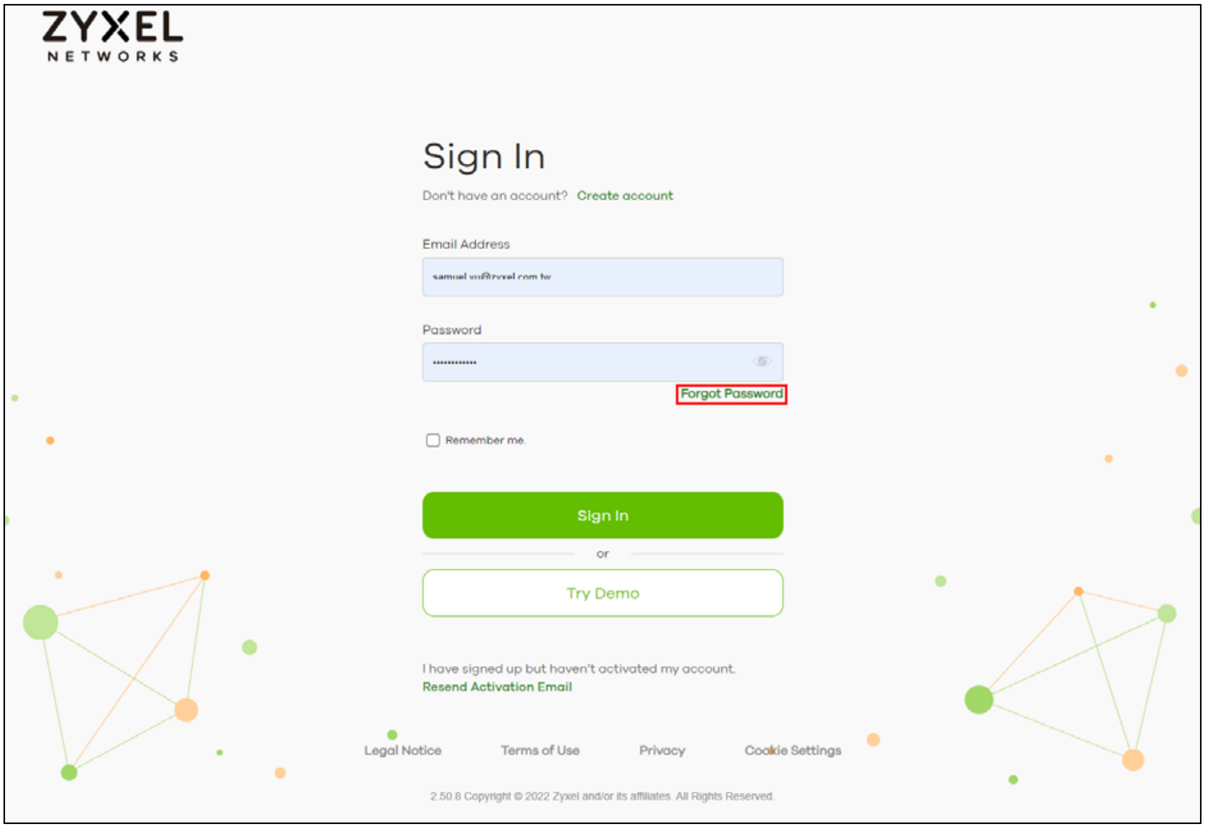
Organization: Select organization...

Device: Select device...

3.8 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

••••••••••••

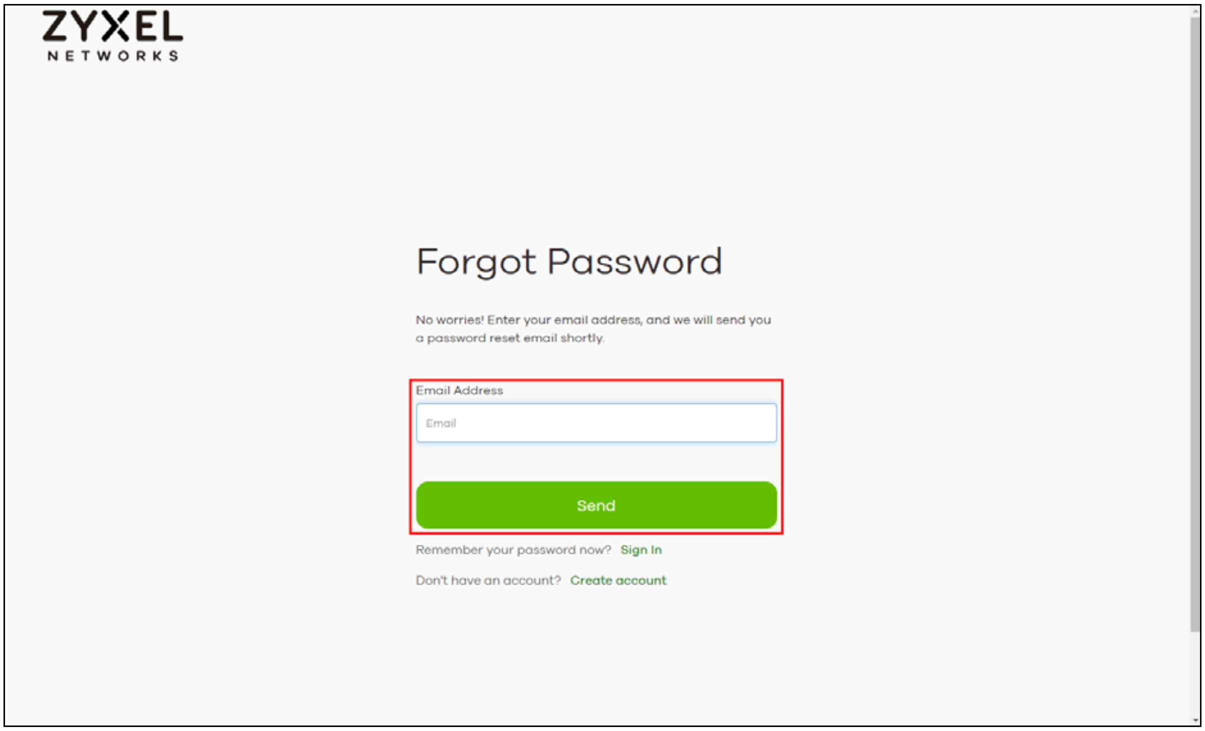
Forgot Password

□ Remember me.

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

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

2 Enter your myZyxel 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.

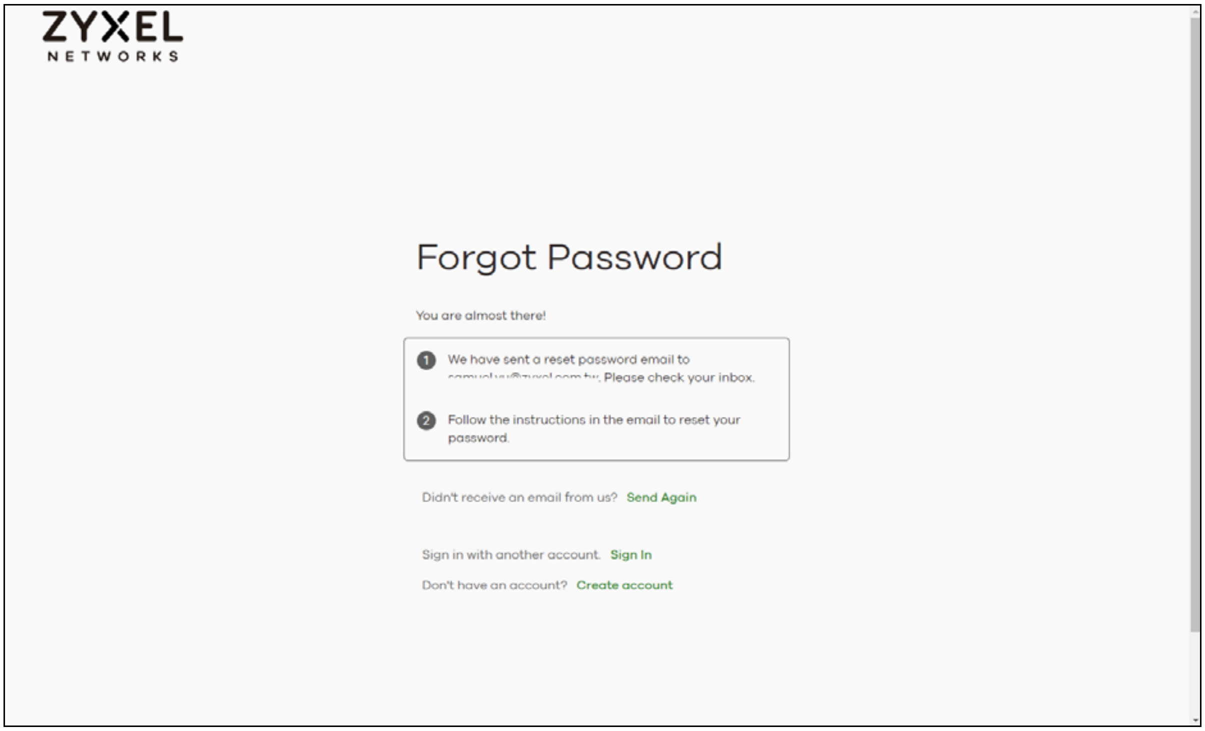
Email Address

Email

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 [redacted]. Please check your inbox.

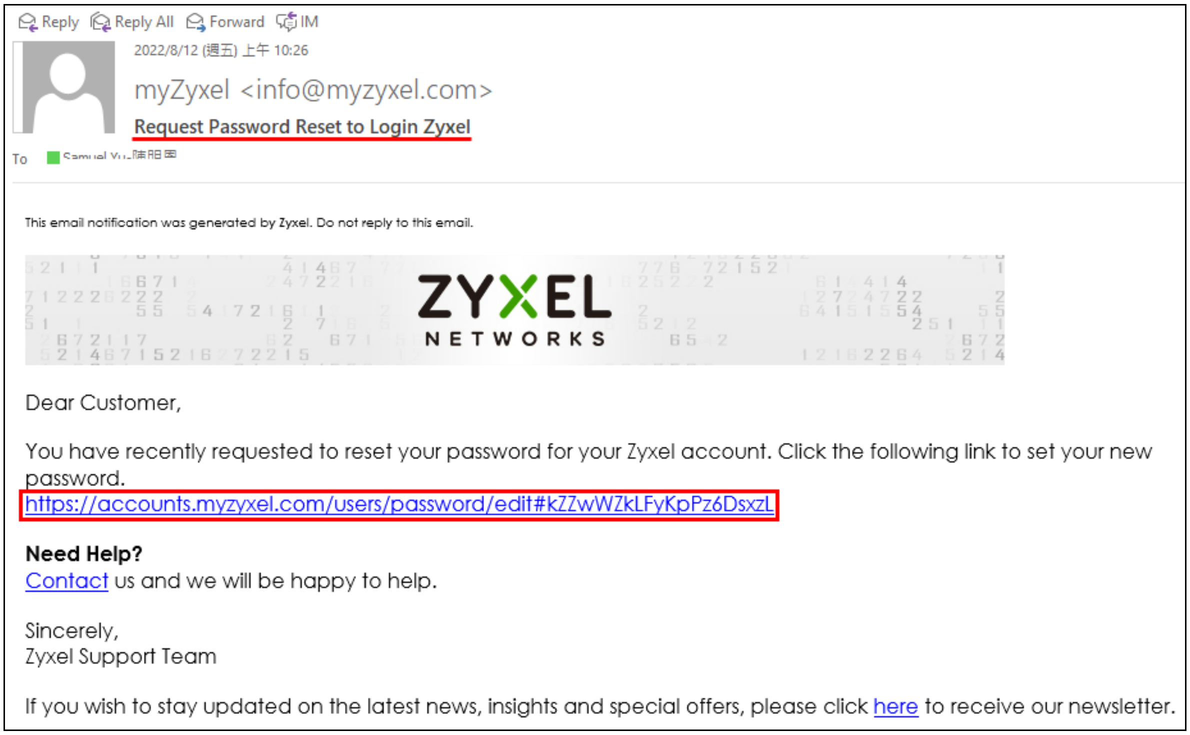
2 Follow the instructions in the email to reset your password.

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 [redacted]

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

Dear Customer,

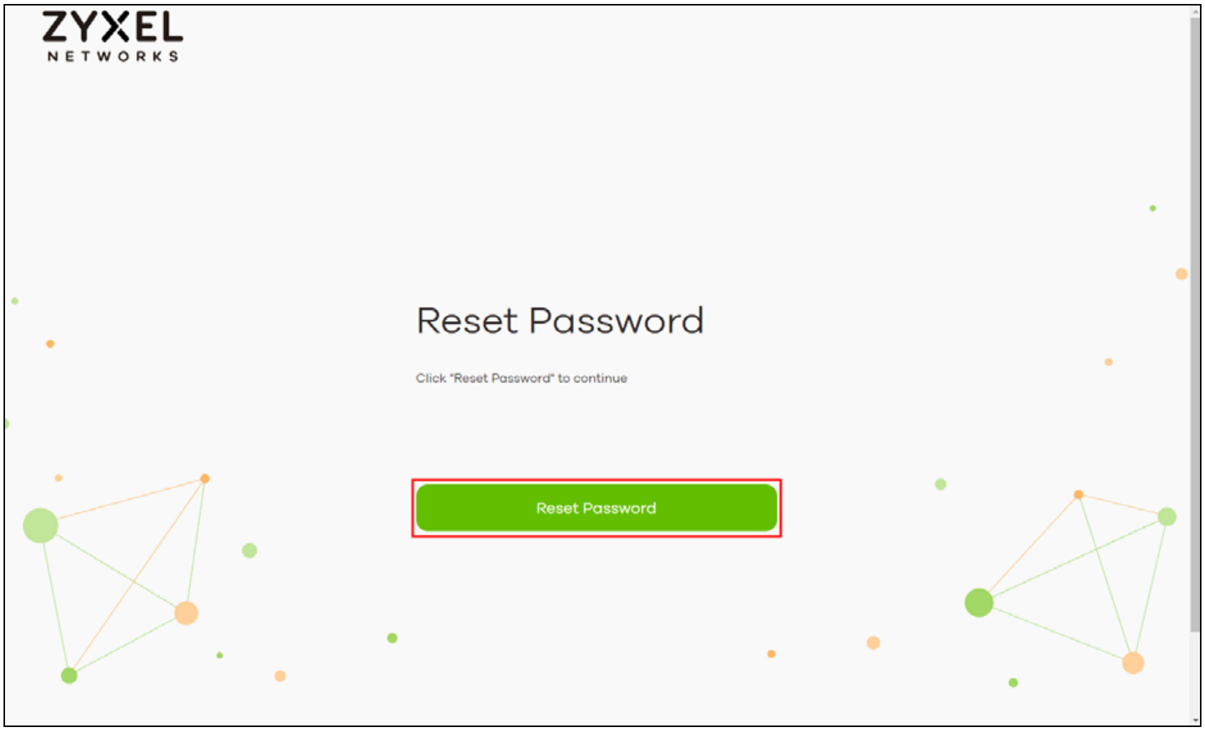
You have recently requested to reset your password for your Zyxel account. Click the following link to set your new password.
https://accounts.myzyxel.com/users/password/edit#kZZwWZkLFyKpPz6DsxzL

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.

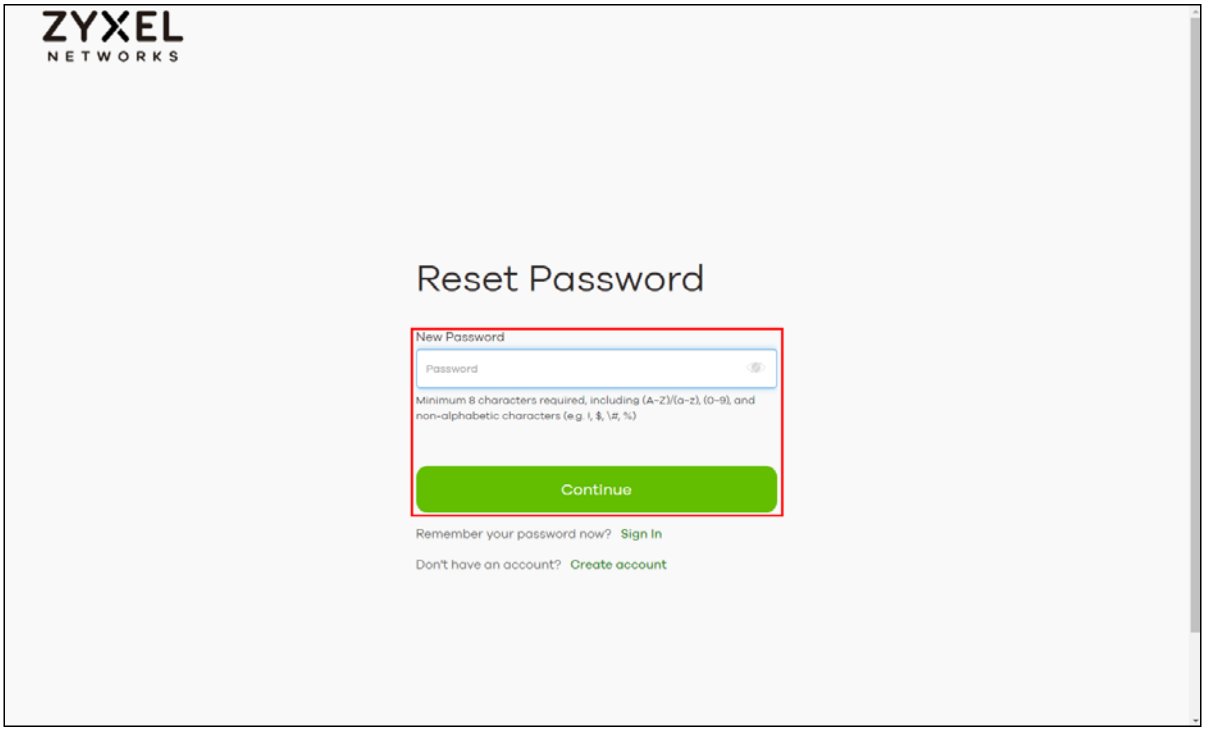
4 The following screen appears. Click **Reset Password**.



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

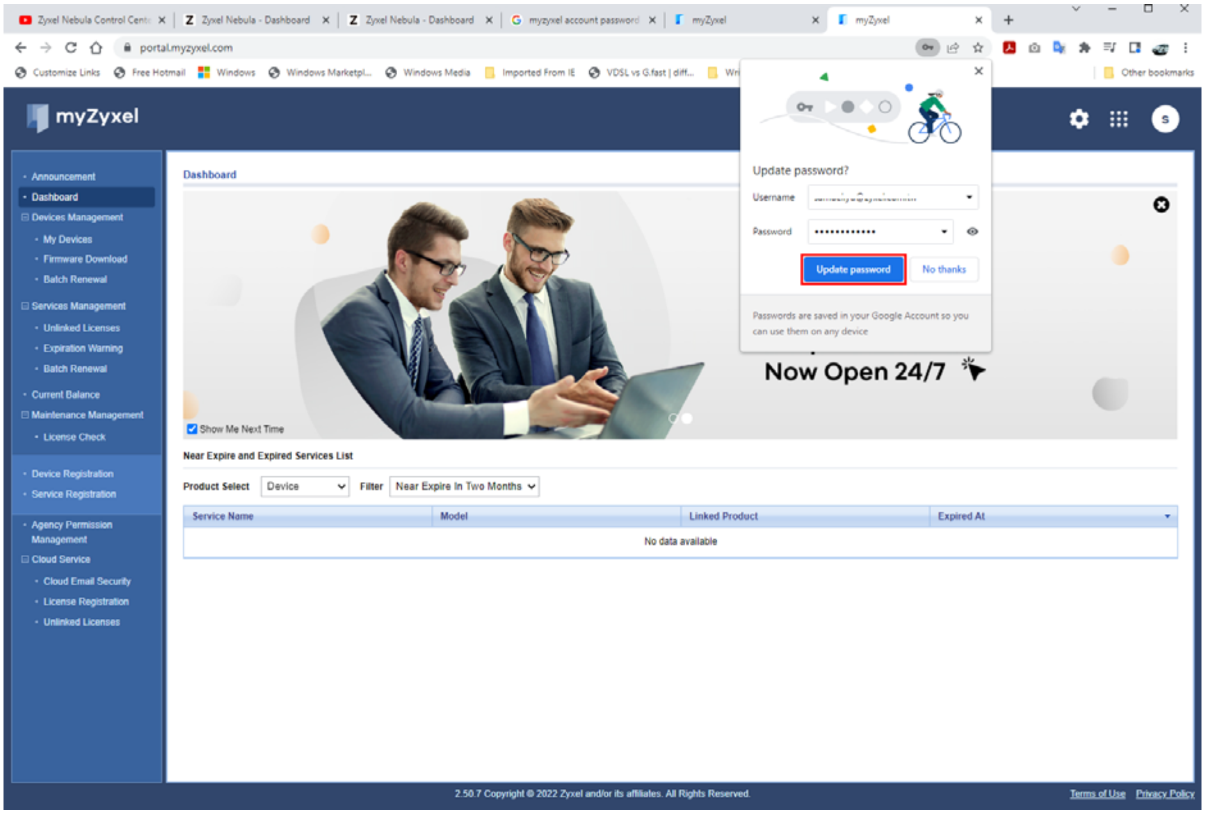
Password

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**.

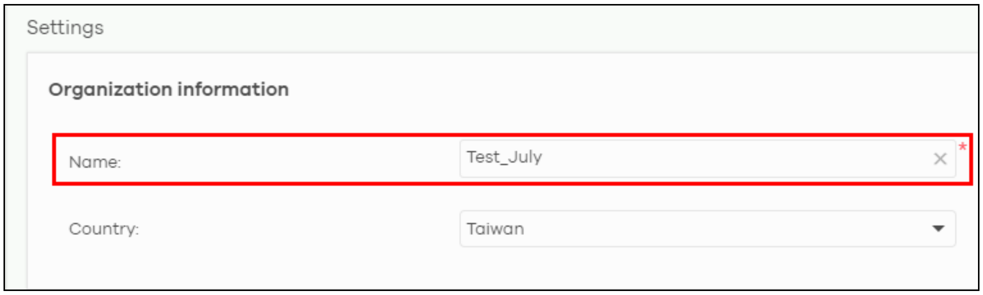


3.9 Change an Organization and/or Site Name

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

Organization Name

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



Settings

Organization information

Name: Test_July

Country: Taiwan

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

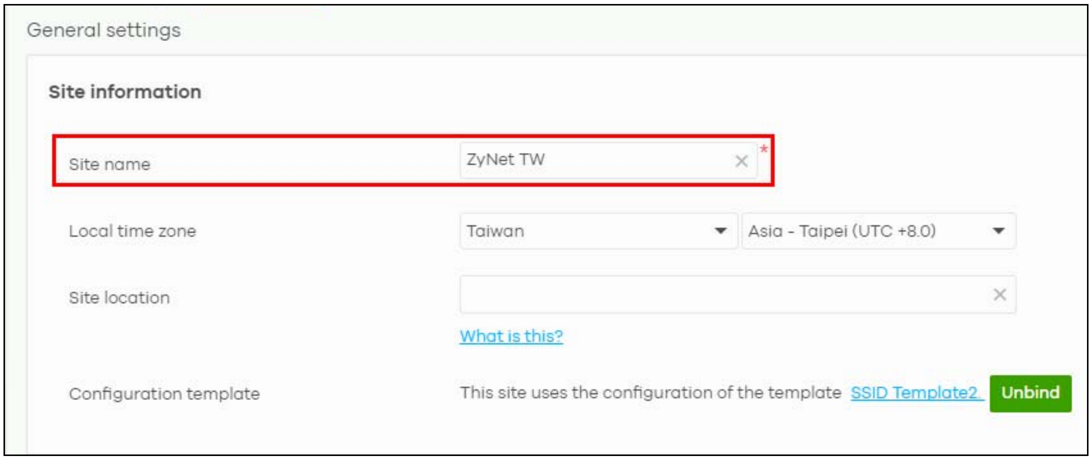
Note: NCC does not allow duplicate organization name.

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.

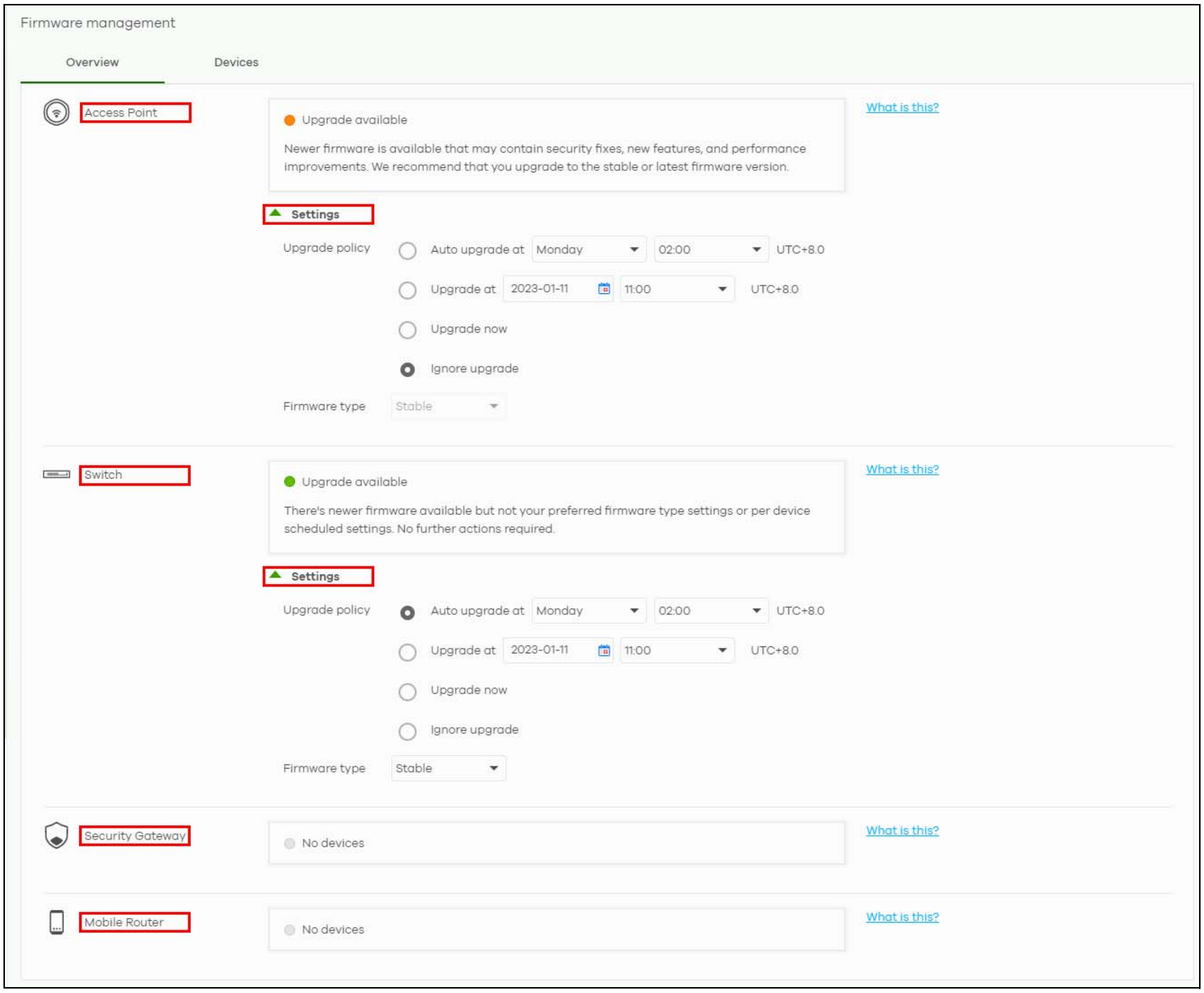
Note: Changing the site name will not affect the Nebula Devices configuration in NCC.

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

3.10 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, 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

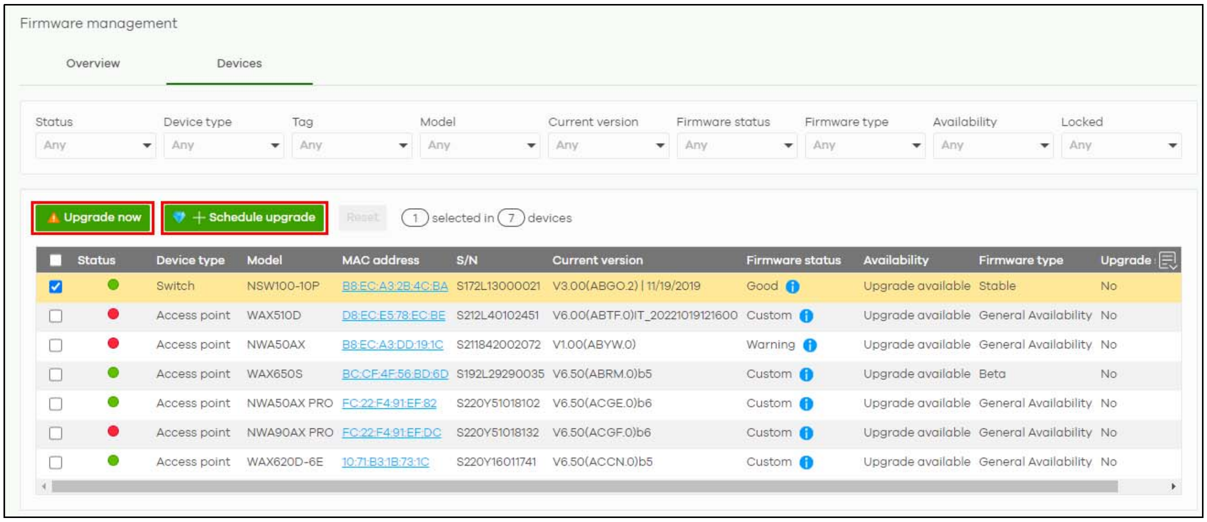
What is this?

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	Device type	Tag	Model	Current version	Firmware status	Firmware type	Availability	Locked
Any	Any	Any	Any	Any	Any	Any	Any	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.

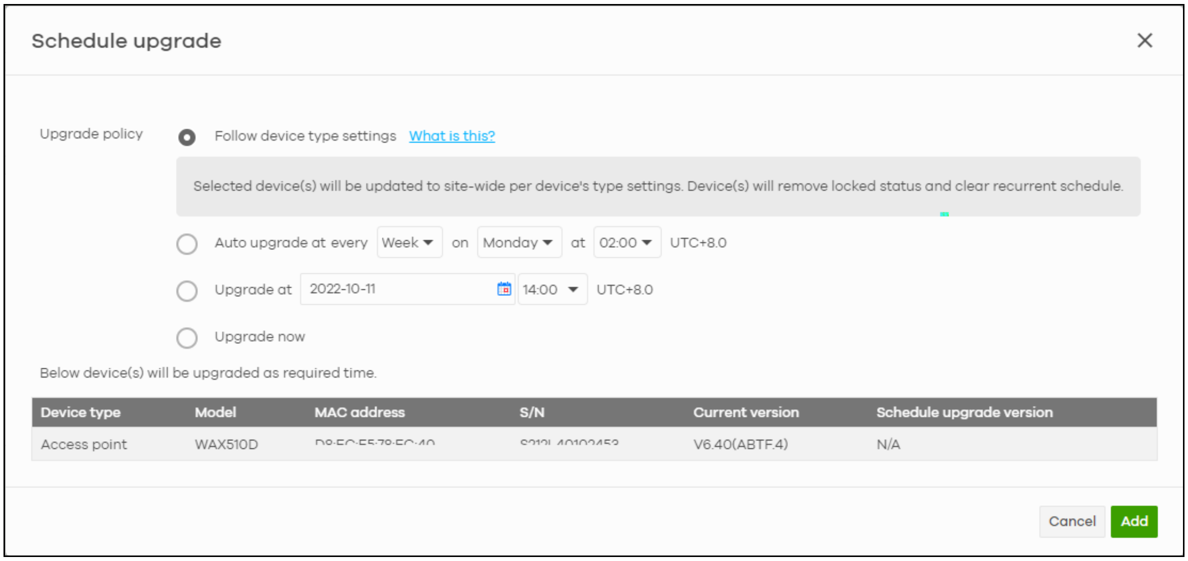
Note: Due to network bandwidth and number of Nebula Devices per site, not all Nebula Devices may get the firmware upgrade on the specified date/time.

- 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

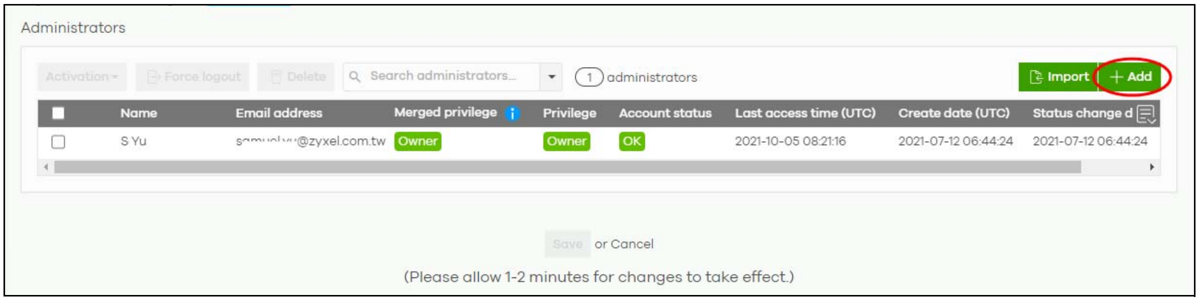
Below device(s) will be upgraded as required time.

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 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

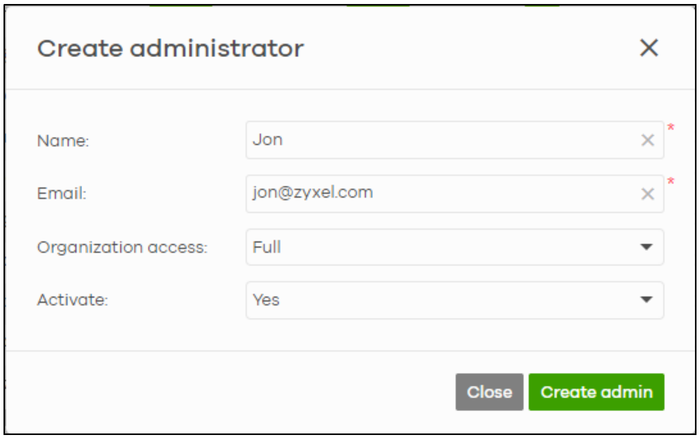
□	Name	Email address	Merged privilege	Privilege	Account status	Last access time (UTC)	Create date (UTC)	Status change d
□	S Yu	samuelyu@zyxel.com.tw	Owner	Owner	OK	2021-10-05 08:21:16	2021-07-12 06:44:24	2021-07-12 06:44:24

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

2 Enter the **Name** and **Email** of a myZyxel account. Assign the **Organization access** (**Full**, **Read-Only**, **None**). See Table 202 on page 581 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.

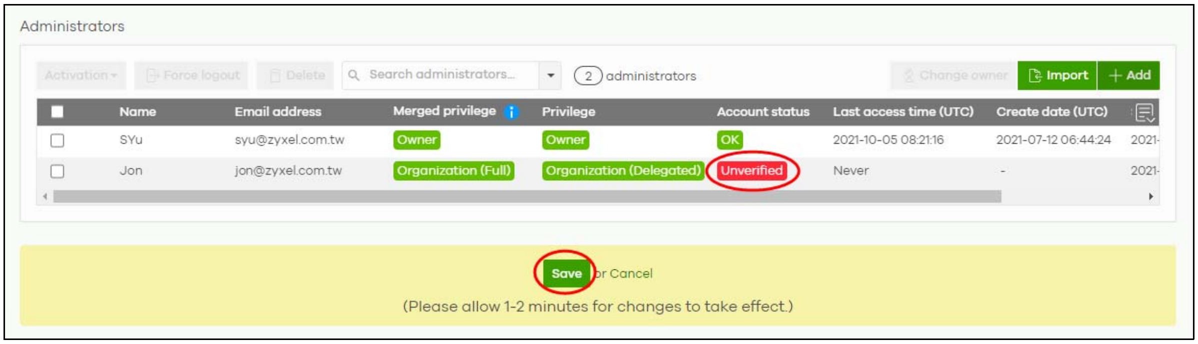
Select **Yes** if you wish to **Activate** the account administrator. Alternatively, select **No** if you wish to create an account administrator, but activate at a later time. The click **Create admin**.



Create administrator

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

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

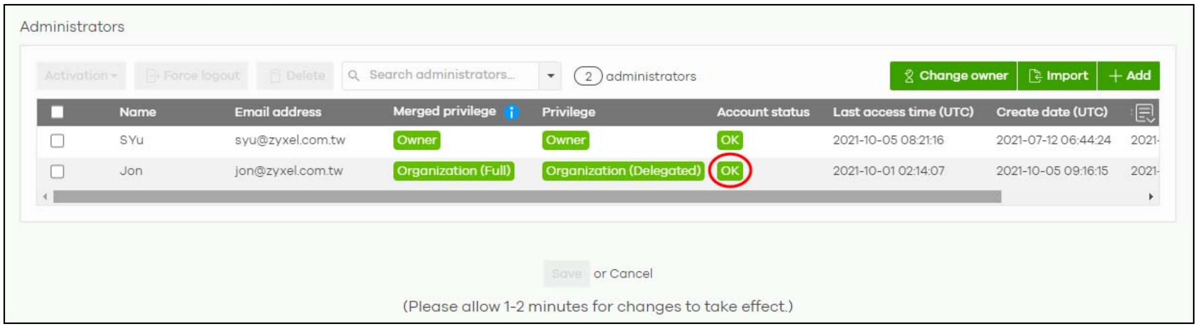


Administrators

□	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.



☐	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
☐	Jon	jon@zyxel.com.tw	Organization (Full)	Organization (Delegated)	OK	2021-10-01 02:14:07	2021-10-05 09:16:15

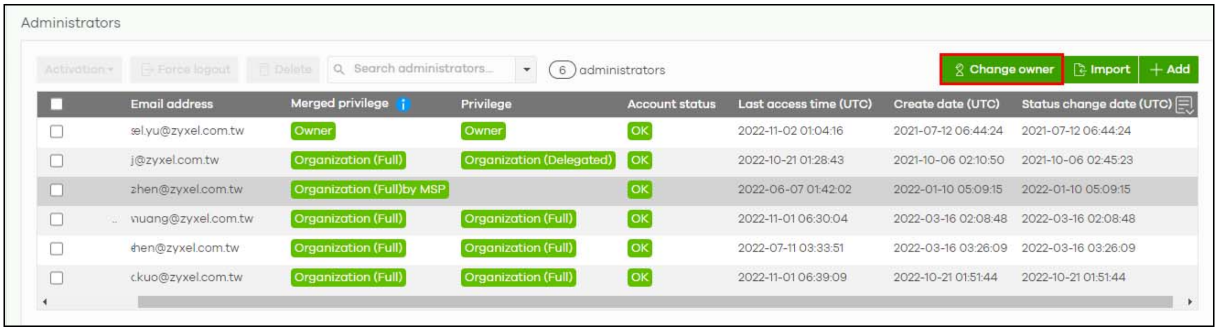
(Please allow 1-2 minutes for changes to take effect.)

3.12 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.

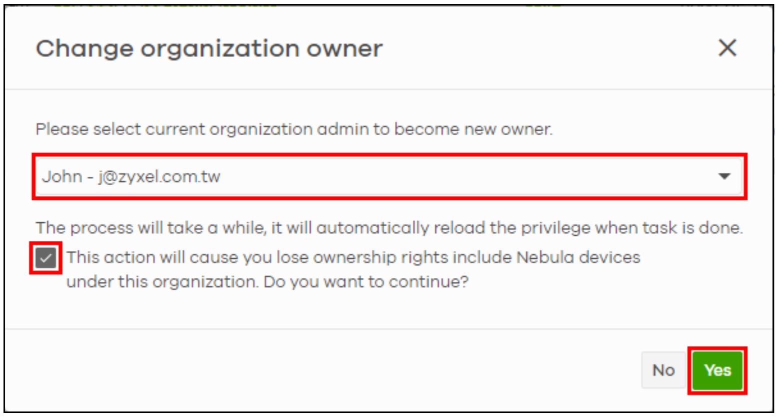
Note: Only the owner can transfer ownership of an organization to another administrator. See Section 3.11 on page 76 if you want to transfer management of your Nebula Devices only.

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



☐	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.



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.

3.13 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 202 on page 581 for details on organization privileges).

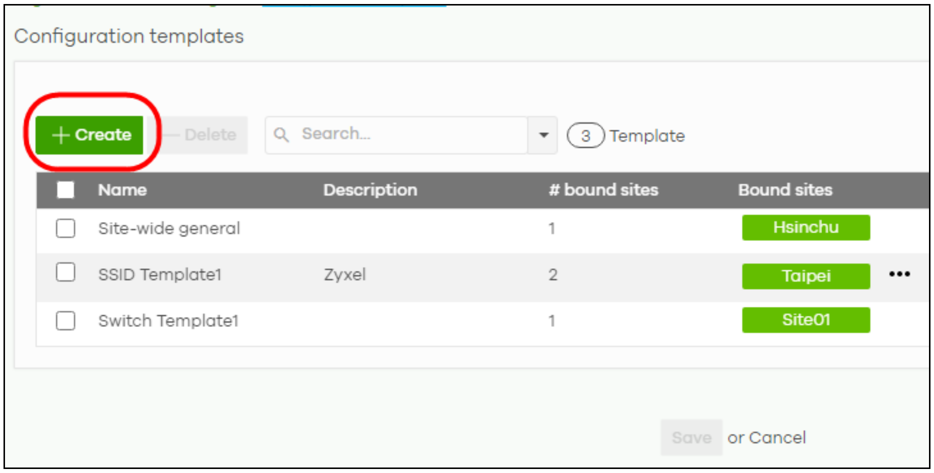
1 Create and Bind a Template Site/Setting

2 Duplicate and Import a Template Setting to a Site

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

3.13.1 Create and Bind a Template Site/Setting

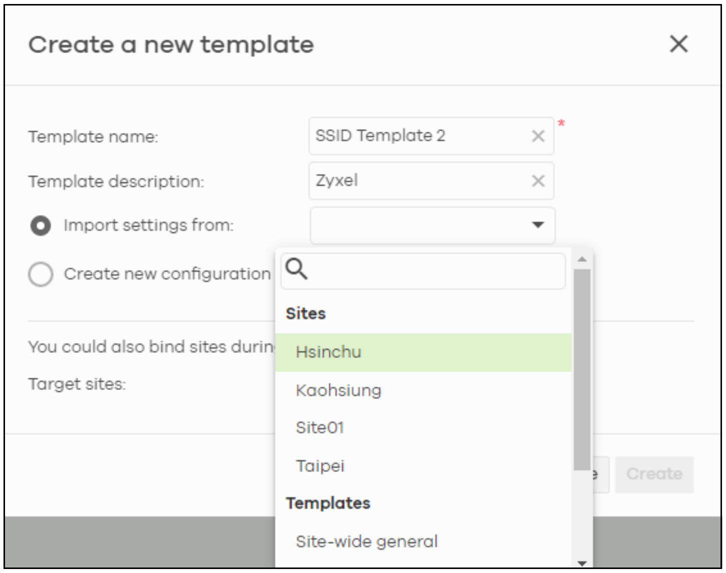
1 Go to the **Organization-wide** > **Organization-wide manage** > **Configuration templates** screen. Click **+Create**.



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**.



Create a new template

Template name: SSID Template 2 *

Template description: Zyxel

● Import settings from:

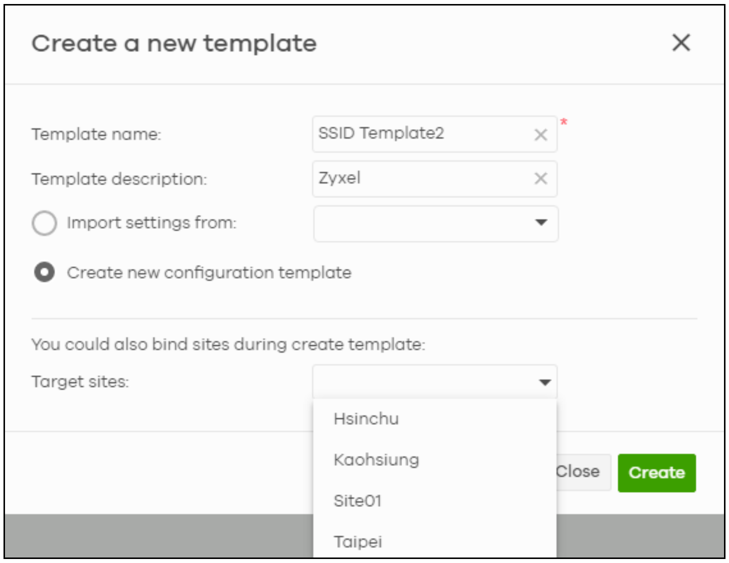
○ Create new configuration

You could also bind sites durin

Target sites:

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.



Create a new template

Template name: SSID Template2 *

Template description: Zyxel

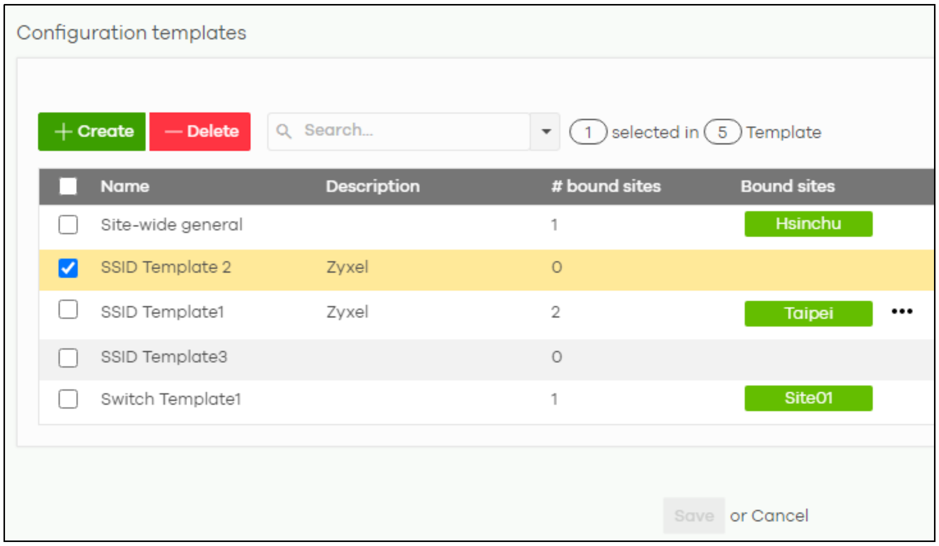
○ Import settings from:

● Create new configuration template

You could also bind sites during create template:

Target sites:

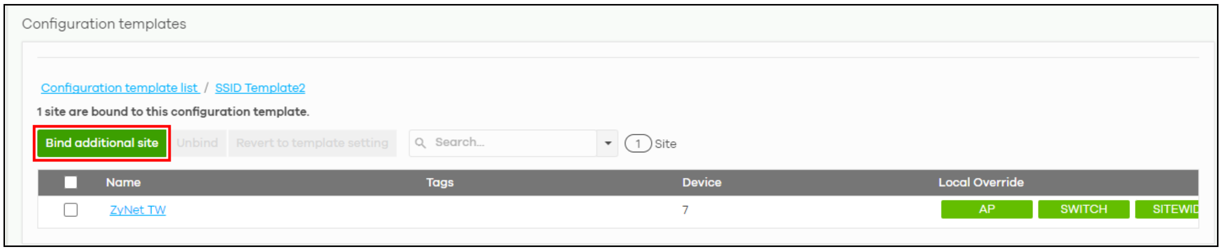
If you skip this step, you can bind a template to a site later. Go to the **Organization-wide** > **Organization-wide manage** > **Configuration templates** screen. Select the template you want to use and then click the row with the template that you want to bind to a site.



Configuration templates

☐	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.



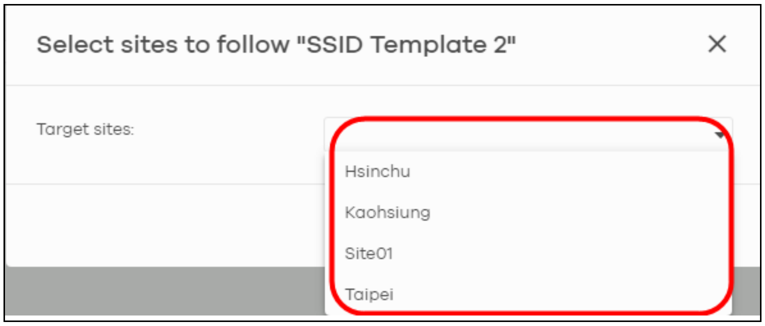
Configuration templates

Configuration template list / SSID Template2

1 site are bound to this configuration template.

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

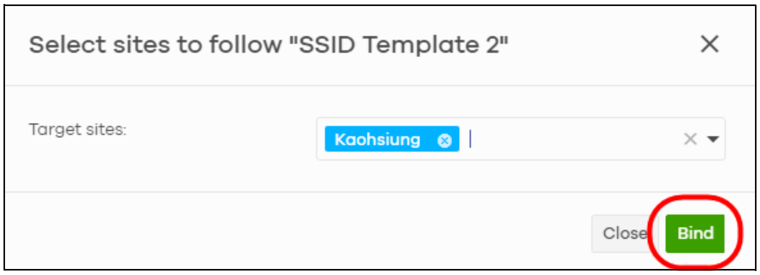
5 The following screen appears. Click the **Target sites** drop-down list box.



Select sites to follow "SSID Template 2"

Target sites:

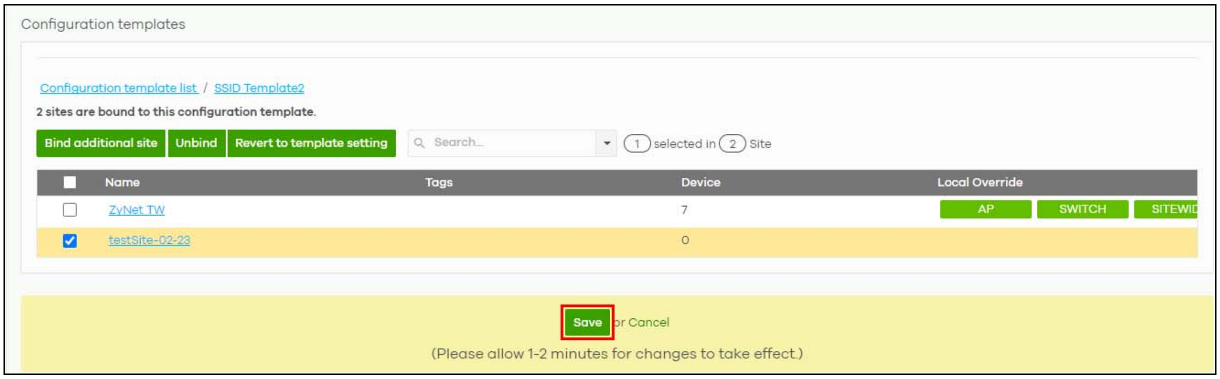
6 Select a site from the **Target sites** drop-down box list and then click **Bind**.



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.

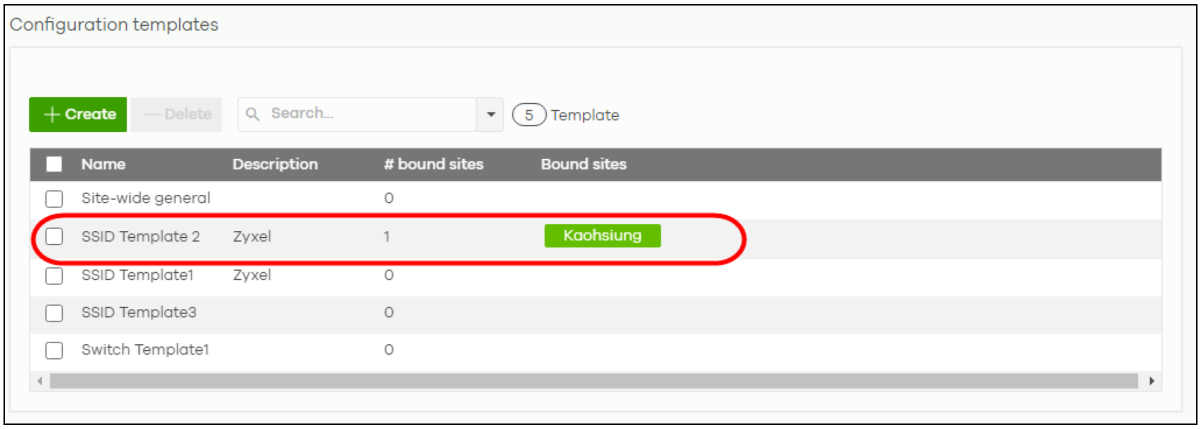
Bind additional site | Unbind | Revert to template setting | Search... | 1 selected in 2 Site

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

Save or Cancel

(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.

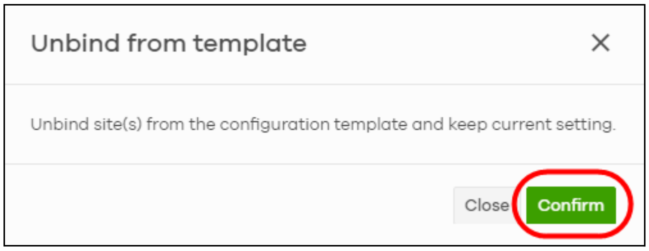


Configuration templates

+ Create | — Delete | Search... | 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.

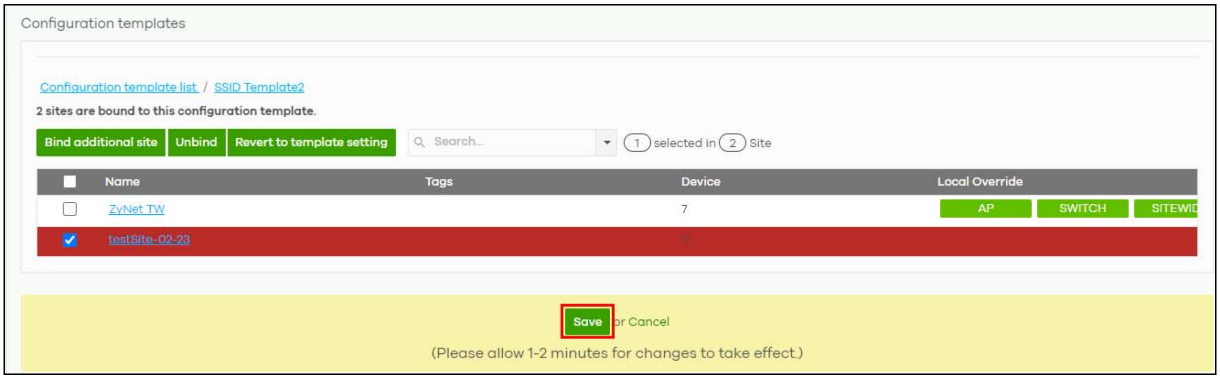


Unbind from template

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

Close | Confirm

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



Configuration templates

Configuration template list / SSID Template2

2 sites are bound to this configuration template.

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

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

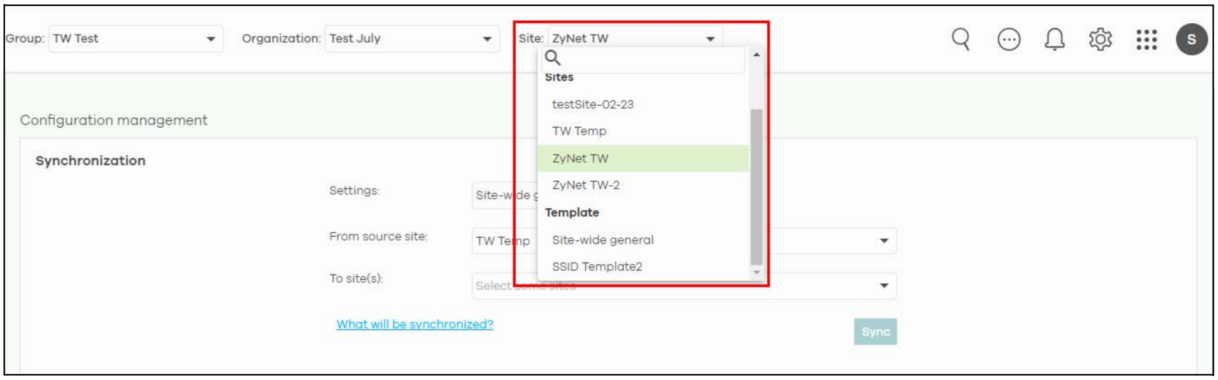
3.13.2 Duplicate and Import a Template Setting to a Site

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

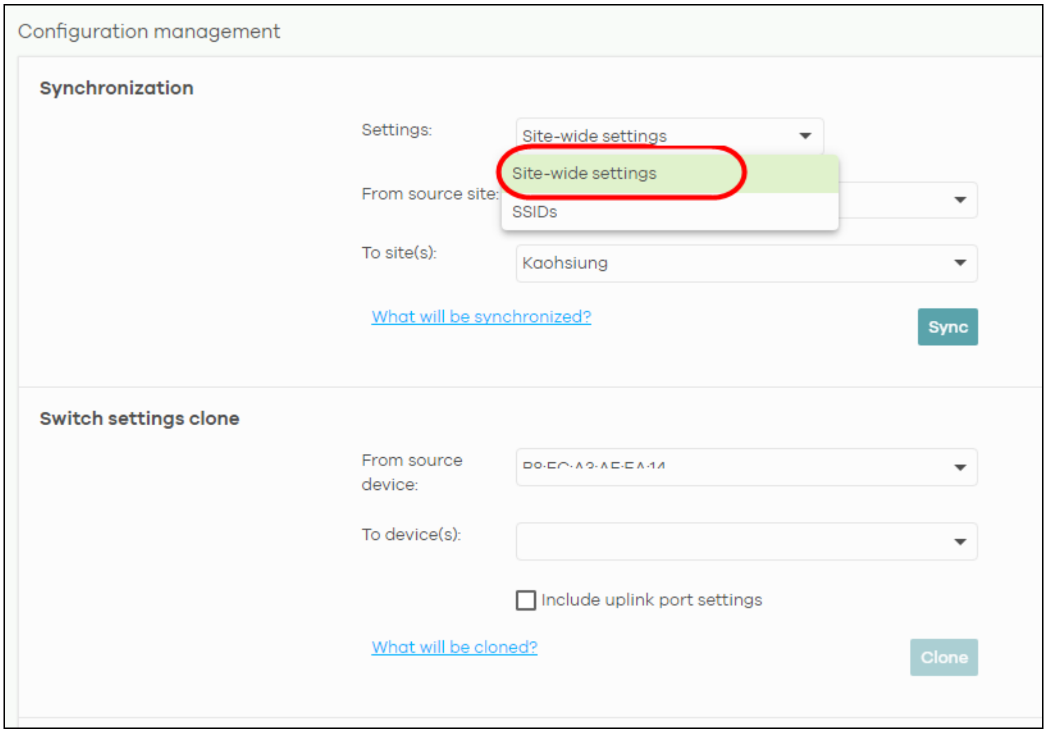
Synchronization

Settings: Site-wide g

From source site: TW Temp

To site(s): Select

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

From source site:

To site(s): Kaohsiung

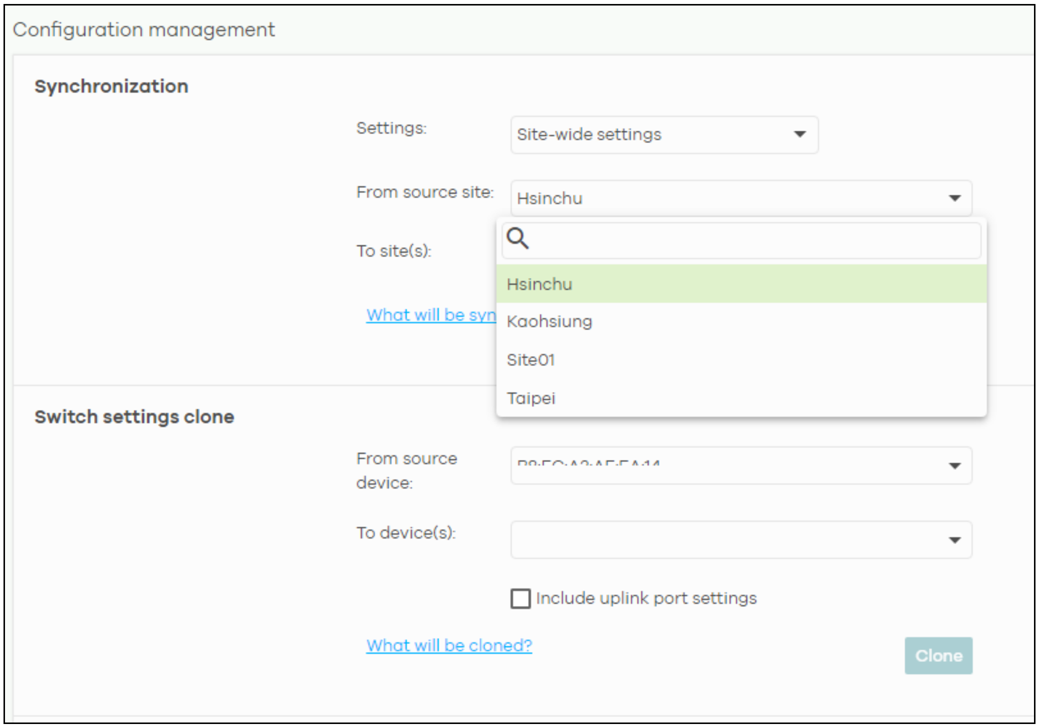
Switch settings clone

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

To device(s):

□ Include uplink port settings

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

To site(s):

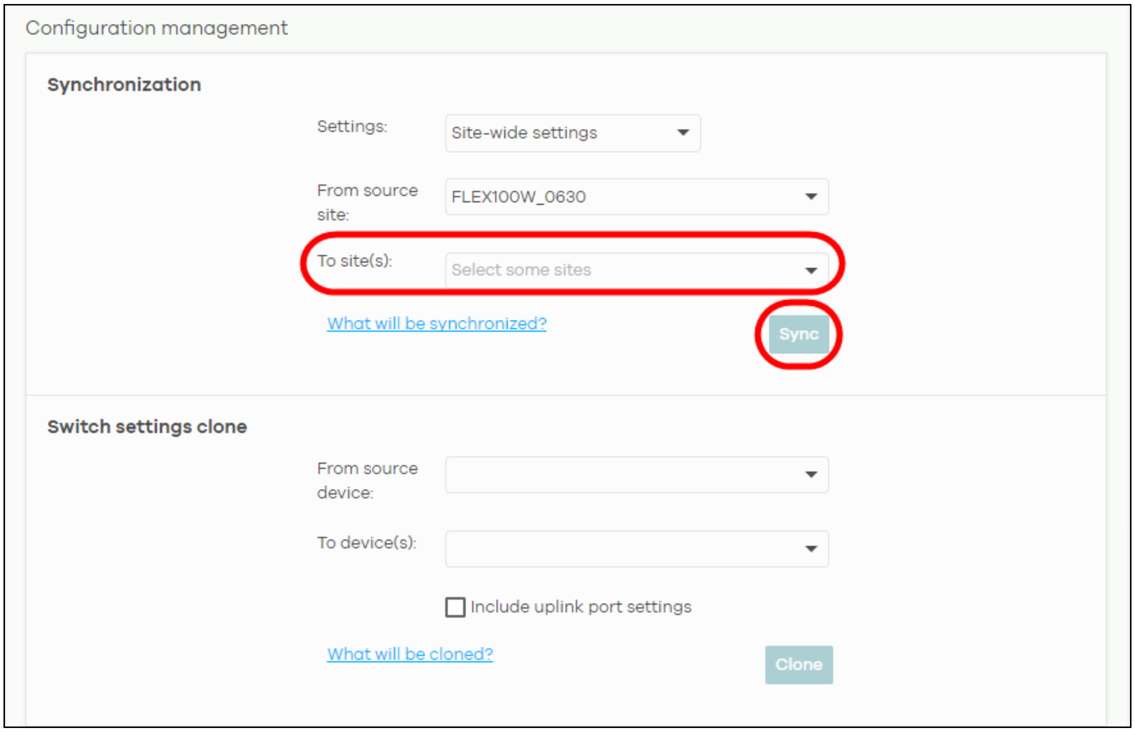
Switch settings clone

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

To device(s):

□ Include uplink port settings

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

Switch settings clone

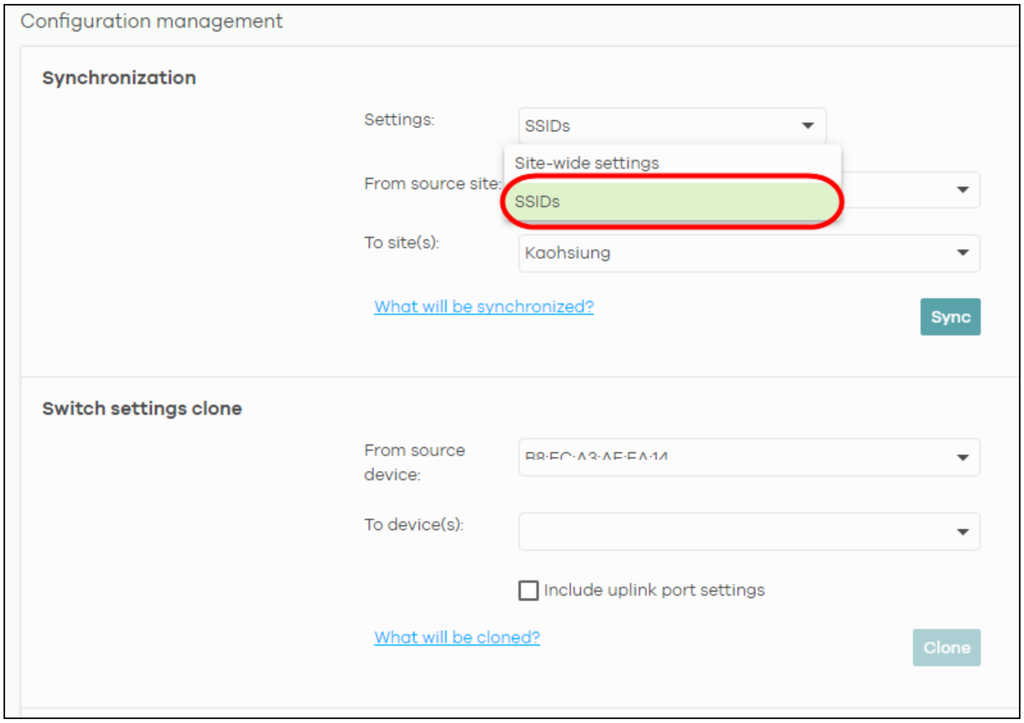
From source device:

To device(s):

□ Include uplink port settings

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

From source site:

To site(s): Kaohsiung

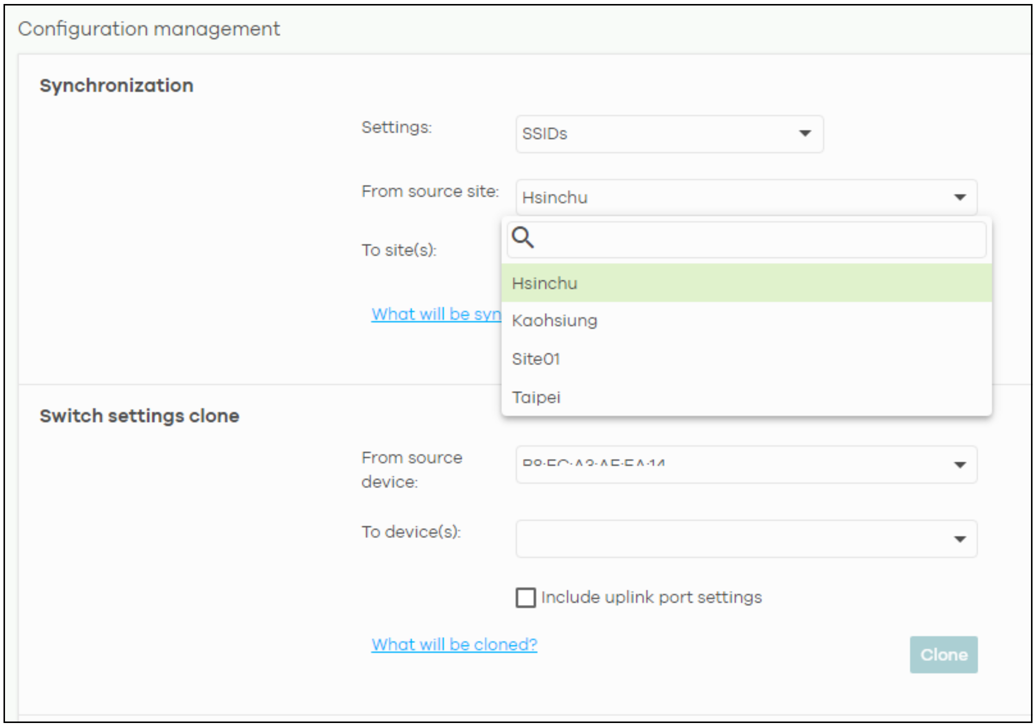
Switch settings clone

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

To device(s):

□ Include uplink port settings

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):

- Hsinchu
- Kaohsiung
- Site01
- Taipei

What will be syn

Switch settings clone

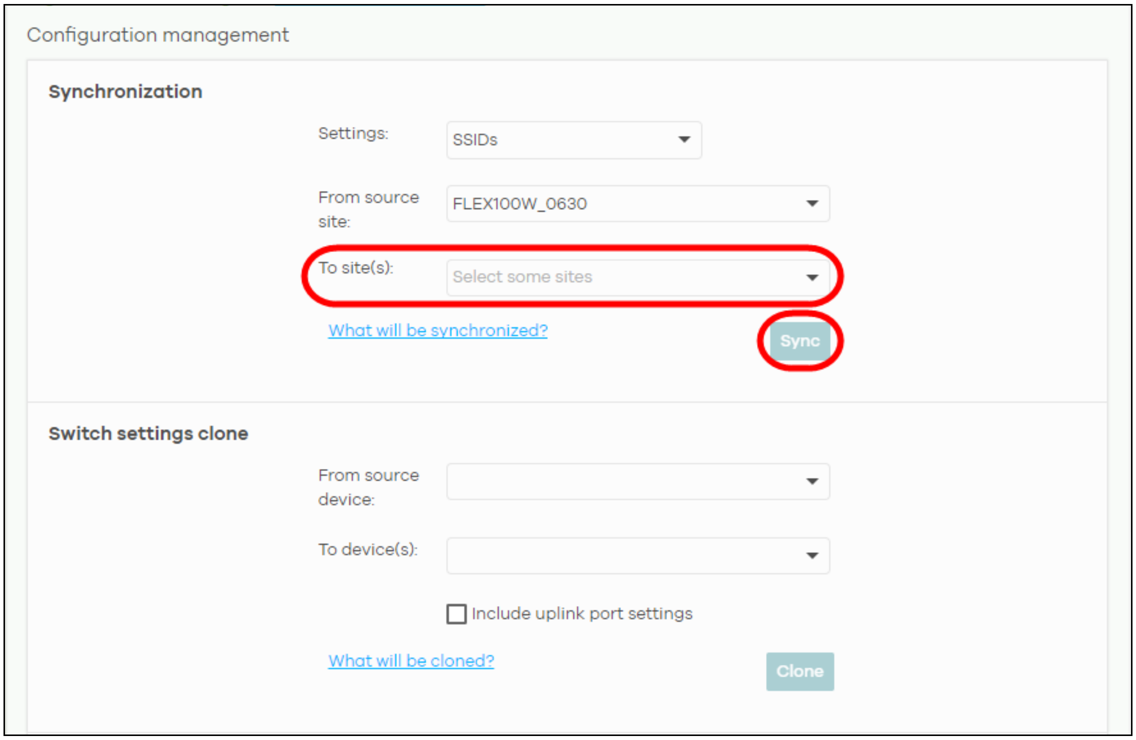
From source device: B8:EC:A3:AE:EA:14

To device(s):

□ Include uplink port settings

What will be cloned?

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

What will be synchronized?

Switch settings clone

From source device:

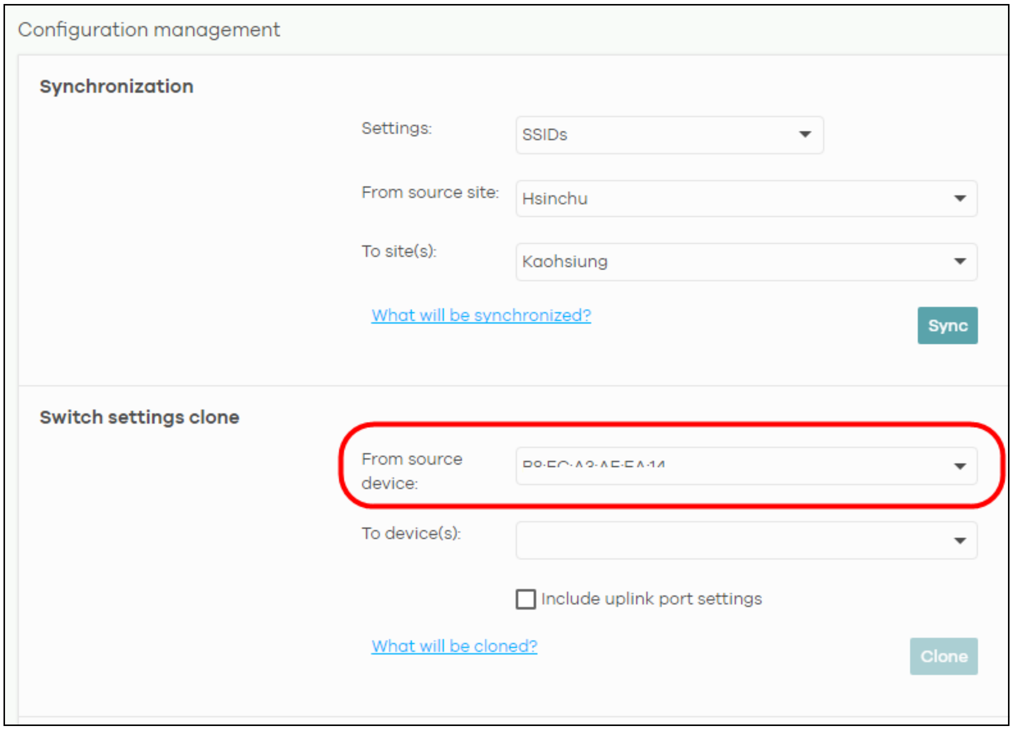
To device(s):

□ Include uplink port settings

What will be cloned?

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

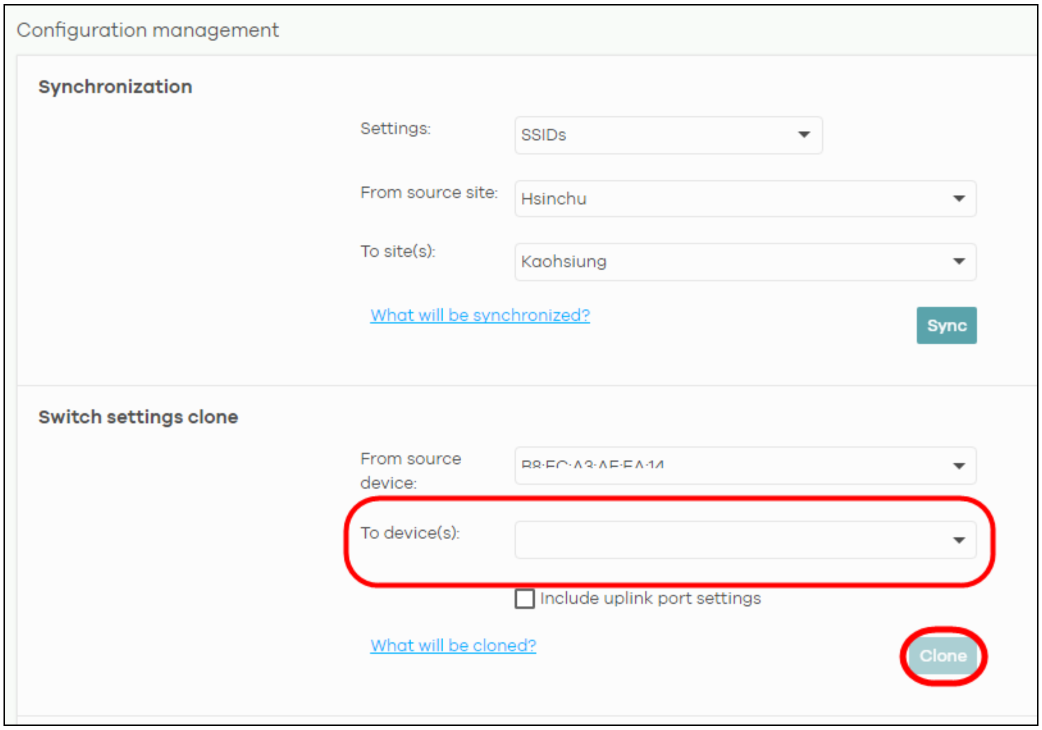
Switch settings clone

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

To device(s):

☐ Include uplink port settings

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?

Switch settings clone

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

To device(s):

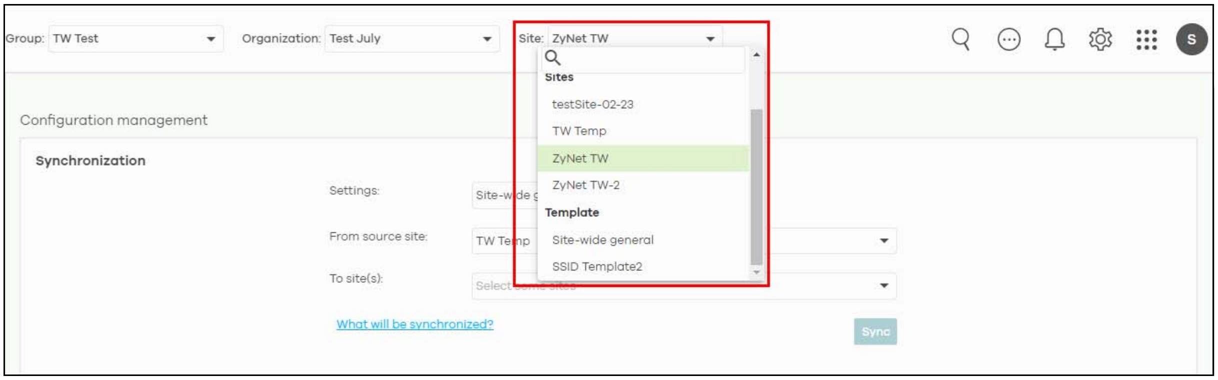
□ Include uplink port settings

What will be cloned?

3.13.3 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

Configuration management

Synchronization

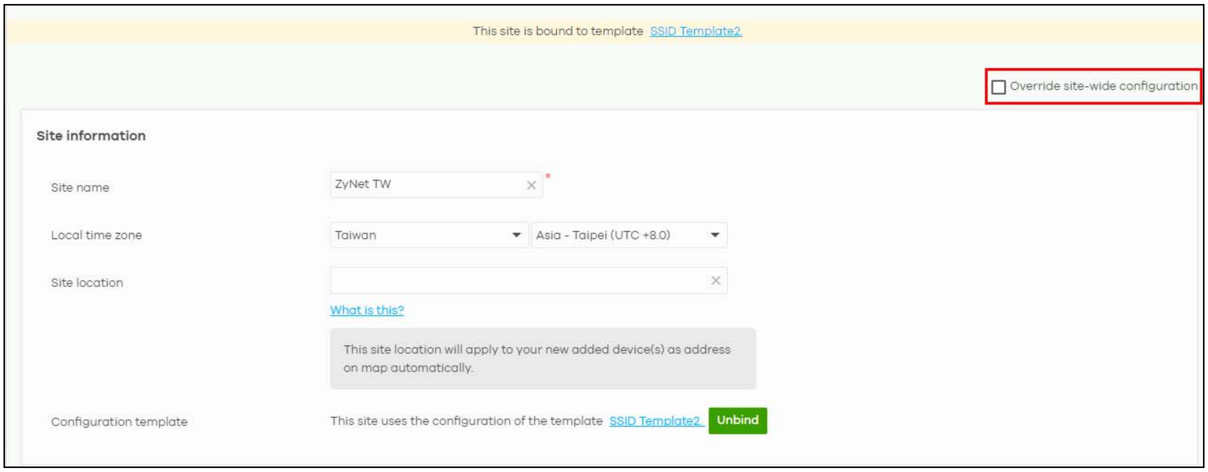
Settings: Site-wide g

From source site: TW Temp

To site(s): Select some sites

What will be synchronized?

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)

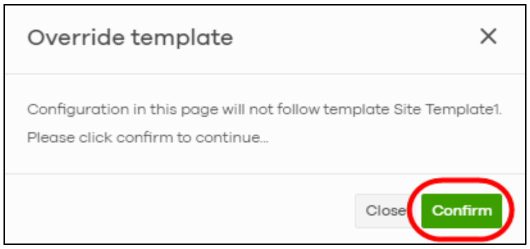
Site location:

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

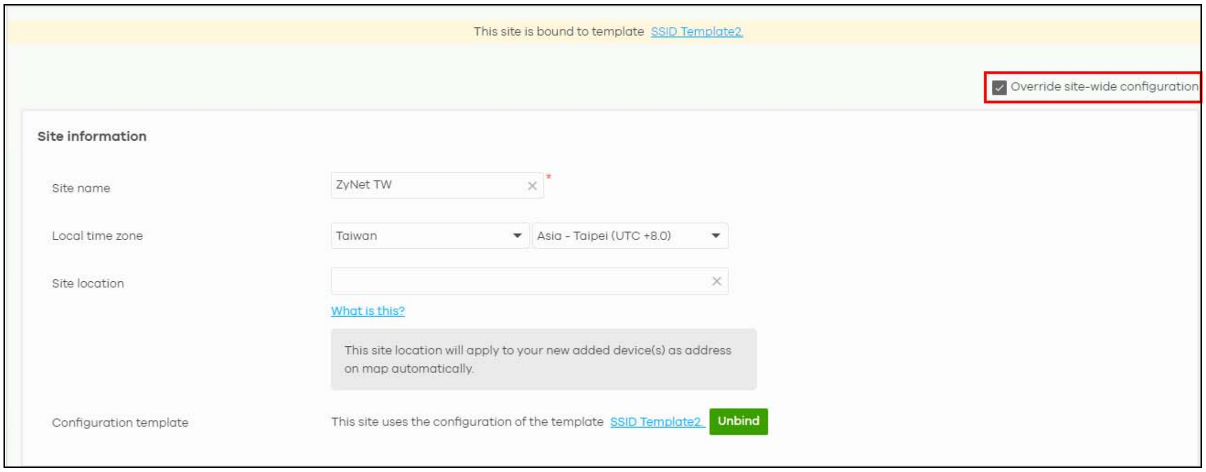
2 The following screen appears. Click **Confirm** to continue.



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)

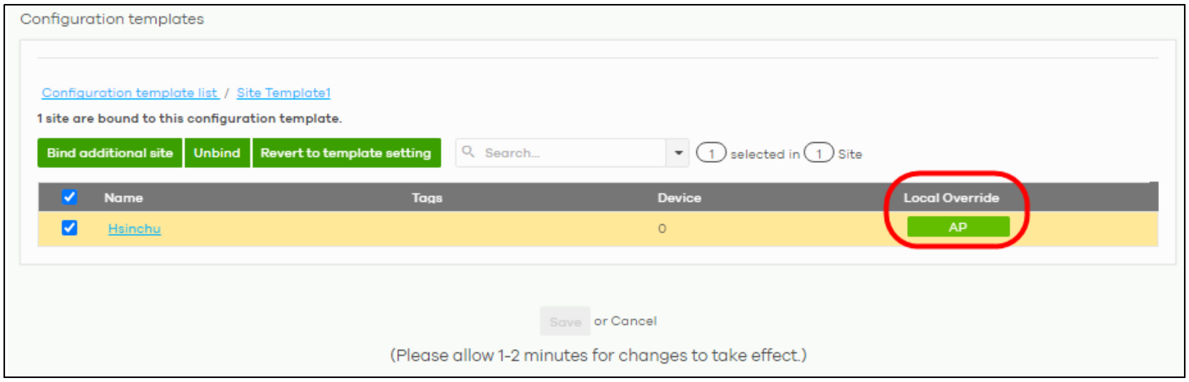
Site location:

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

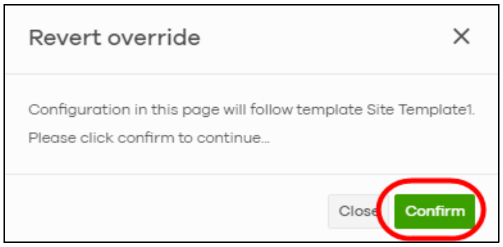
Configuration template list / Site Template1

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.



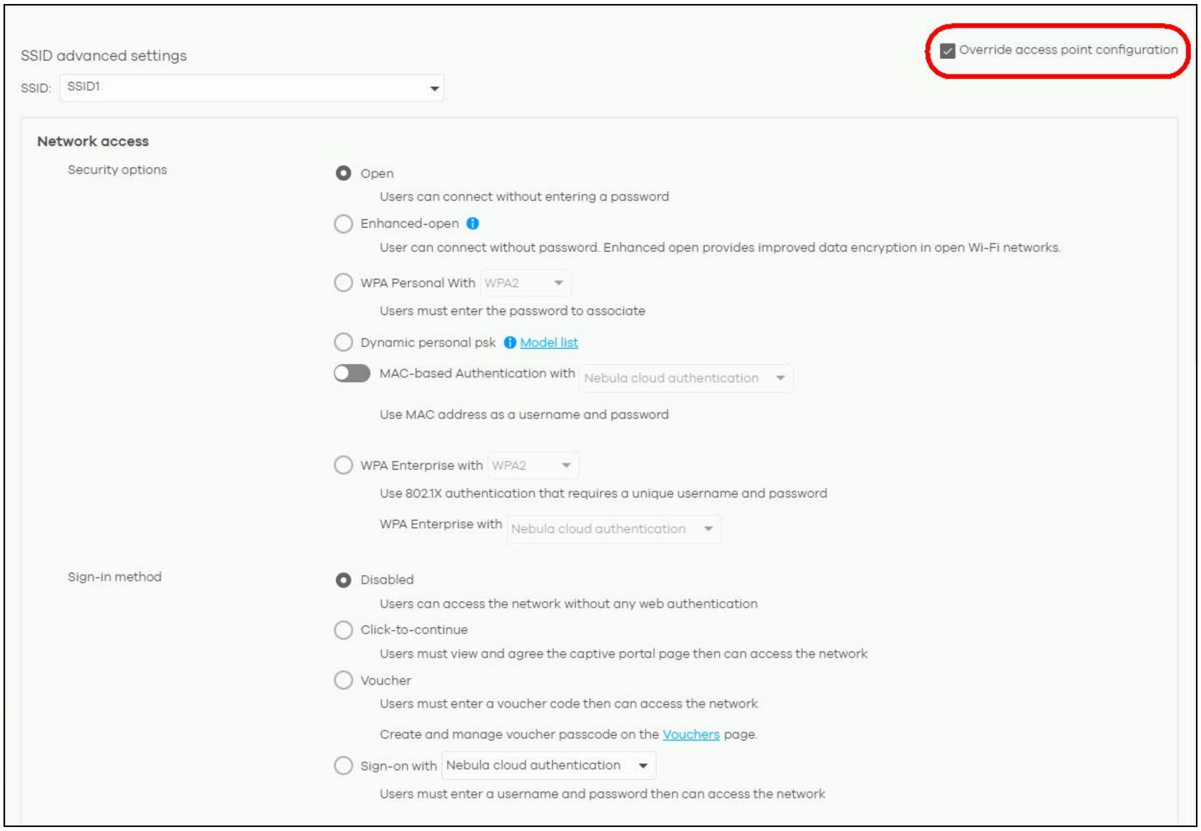
Revert override

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

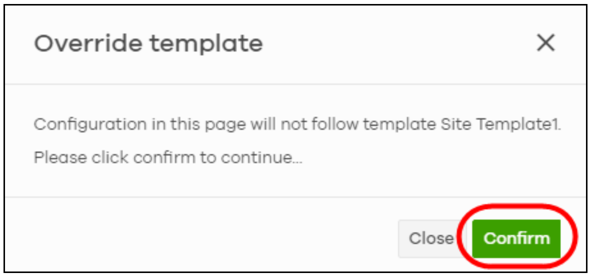
● Disabled
Users can access the network without any web authentication

○ 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.

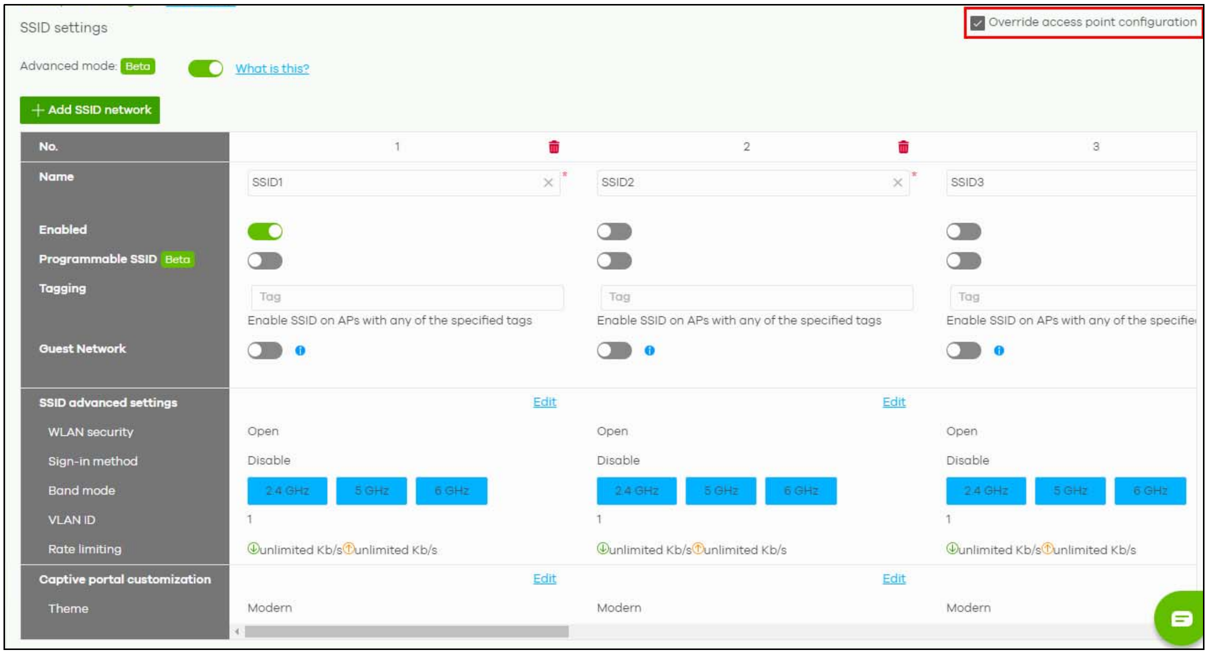


Override template

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

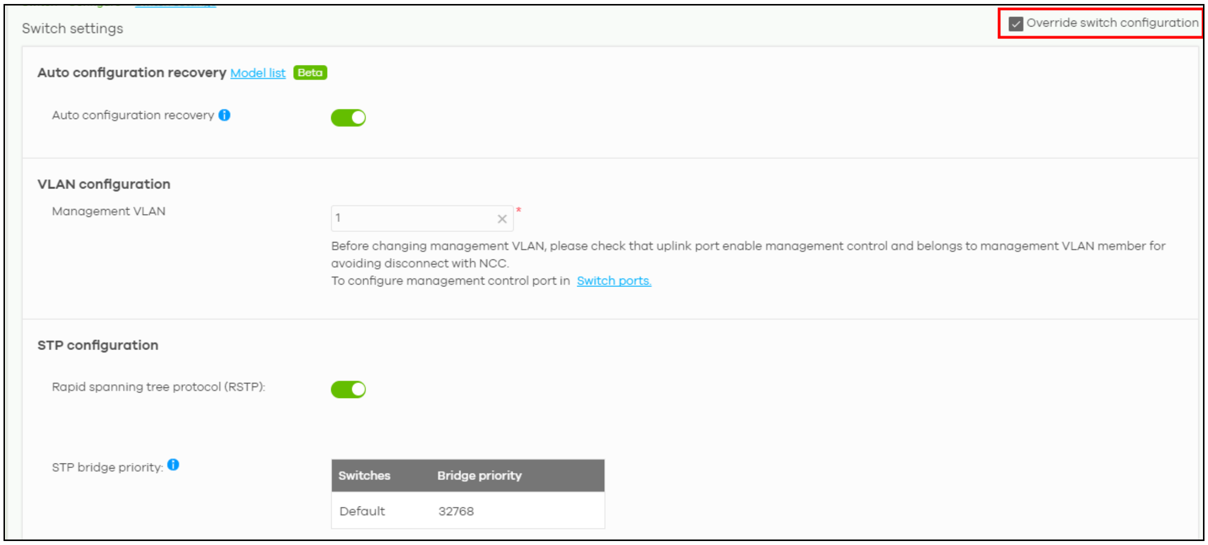
Advanced mode: Beta

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

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.

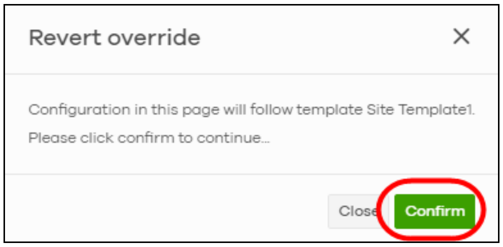
STP configuration

Rapid spanning tree protocol (RSTP): ●

STP bridge priority:

Switches	Bridge priority
Default	32768

4 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

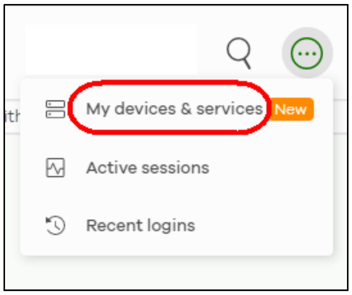
Configuration in this page will follow template Site Template1. Please click confirm to continue...

3.14 Activate an MSP License

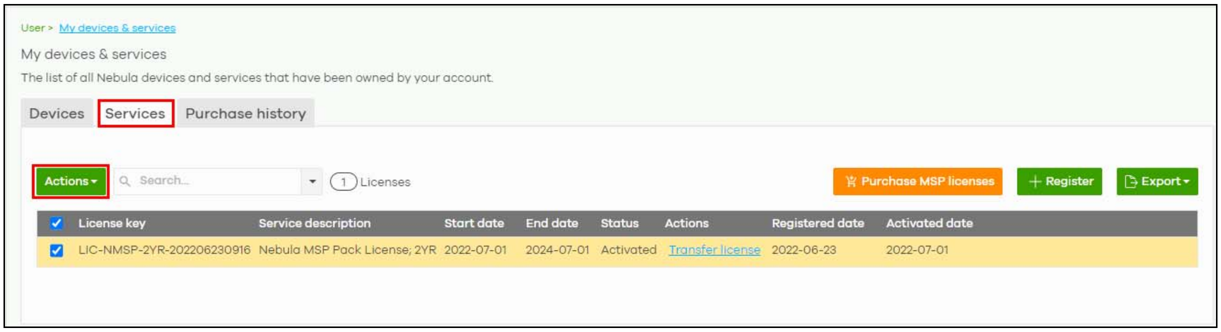
You must have an NCC account and an MSP license pack to activate an MSP license.

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 13 on page 570 for details on the MSP menus).

3.15 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.

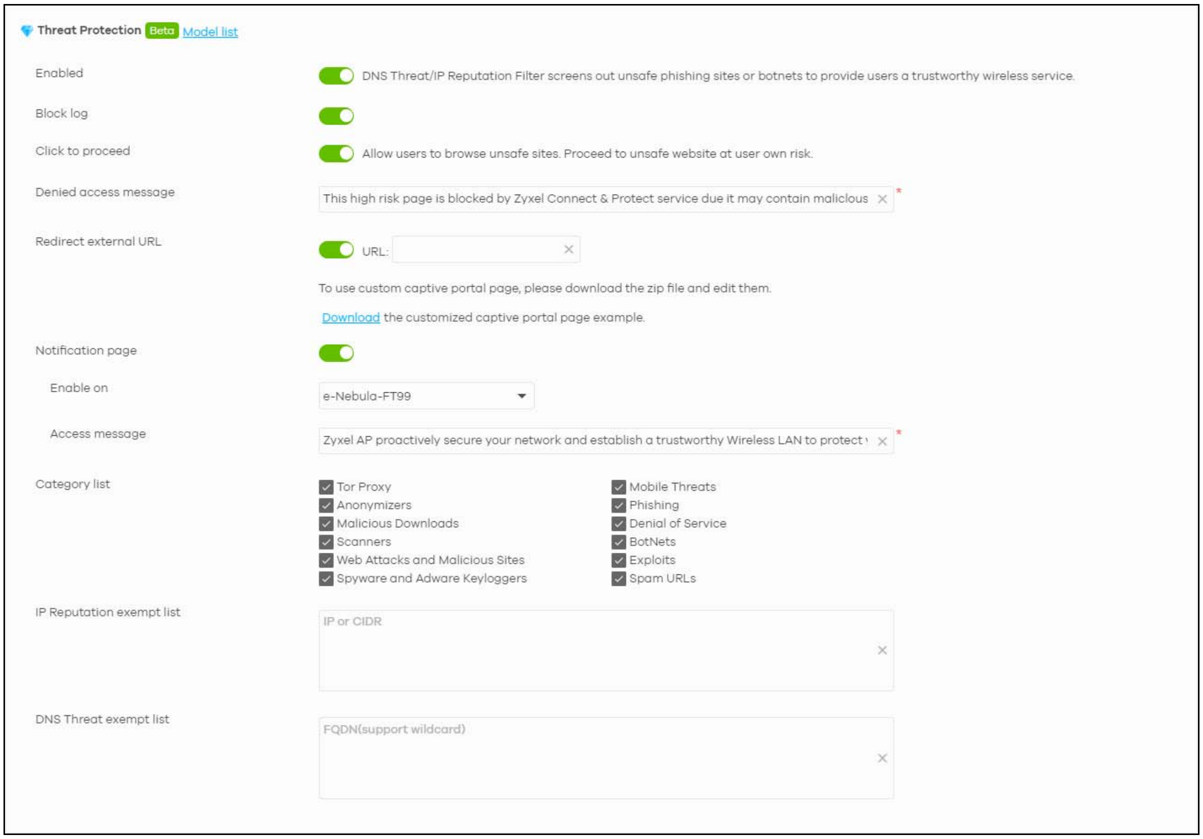
3.15.1 Threat Protection

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 268 for details on how to configure the **Threat Protection** fields.



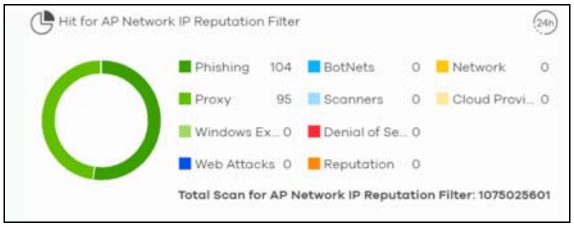
Threat Protection Beta Model list

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.


Hit for AP Network IP Reputation Filter

🟩	Phishing	104	🟦	BotNets	0	🟨	Network	0
🟩	Proxy	95	🟦	Scanners	0	🟨	Cloud Provi...	0
🟩	Windows Ex...	0	🟥	Denial of Se...	0			
🟦	Web Attacks	0	🟧	Reputation	0			

Total Scan for AP Network IP Reputation Filter: 1075025601

3.15.2 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**.

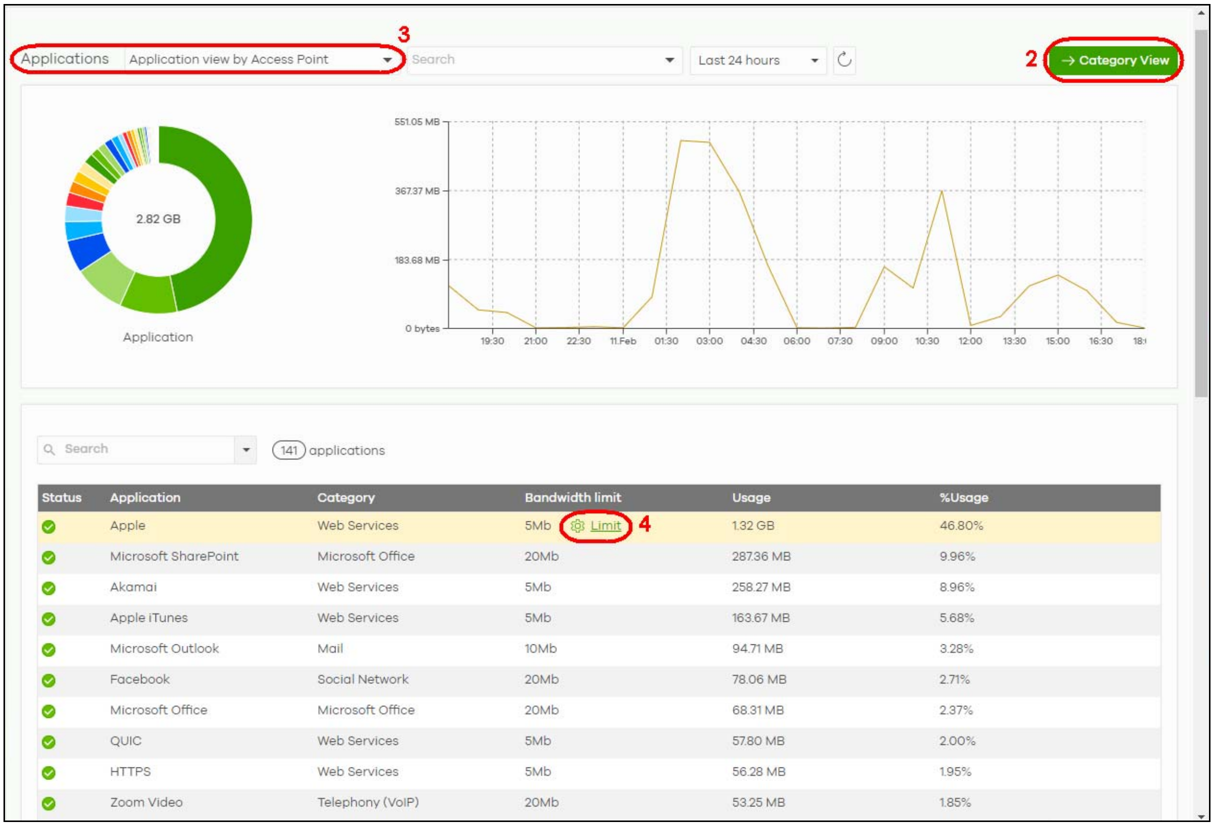
You need to purchase the CNP Plus license to enable application visibility & optimization. To configure application visibility & optimization, do the following:

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

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

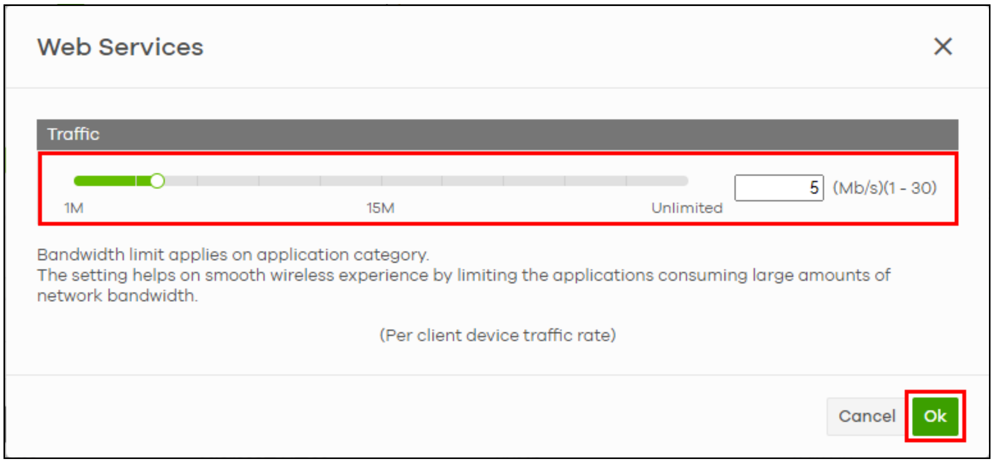
3 Select **Application View by Access Point** in the **Applications** field.

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**).

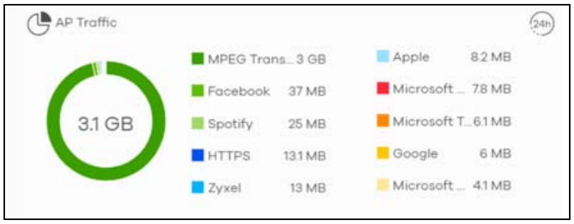


Bandwidth limit applies on application category.
The setting helps on smooth wireless experience by limiting the applications consuming large amounts of network bandwidth.

(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.



3.16 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.

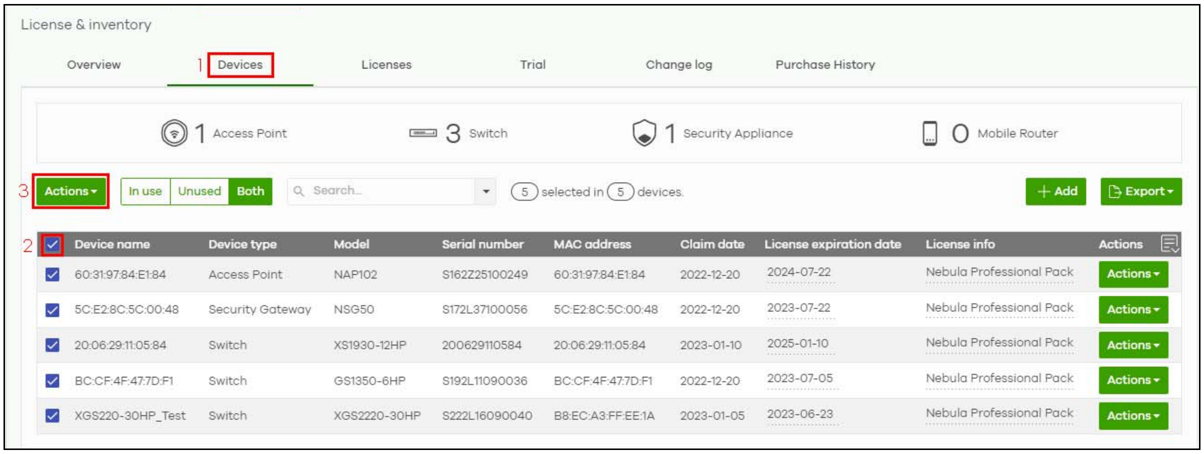
To delete an Organization from the NCC, do the following:

3.16.1 Remove All Nebula Devices

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

2 Click the check box (2) to select all Nebula Devices.

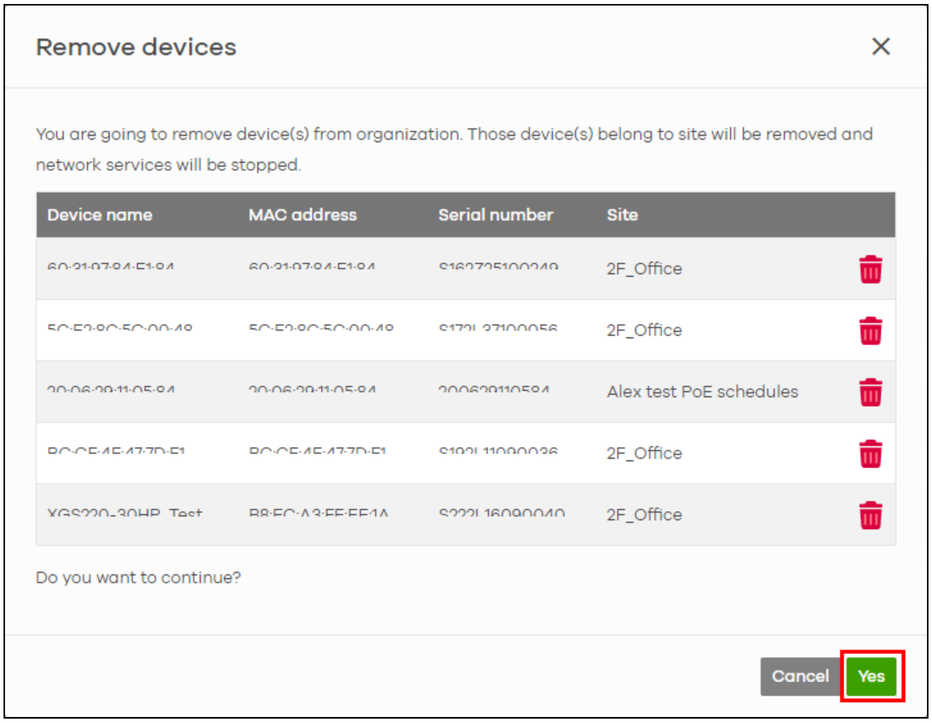
3 Click the **Actions** button (3).



☑	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.



Remove devices

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	S162725100249	2F_Office
5C:E2:8C:5C:00:48	5C:E2:8C:5C:00:48	S172L27100056	2F_Office
20:06:29:11:05:84	20:06:29:11:05:84	200629110584	Alex test PoE schedules
BC:CF:4F:47:7D:E1	BC:CF:4F:47:7D:E1	S192L11090036	2F_Office
XGS220-30HP_Test	B8:EC:A3:FF:EE:1A	S222L16090040	2F_Office

Do you want to continue?

3.16.2 Transfer All Licenses

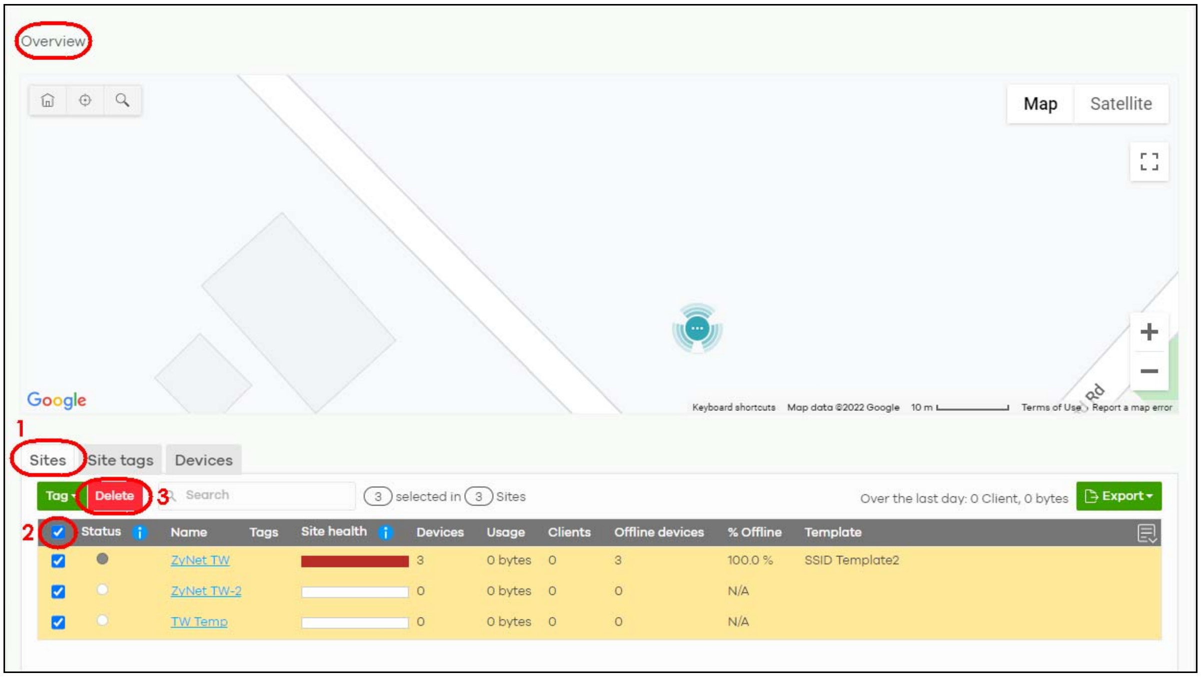
See Section 3.7 on page 64 in this chapter for information on how to transfer licenses assigned to an organization and Nebula Device to another Nebula Device in a different organization.

3.16.3 Delete All Sites

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

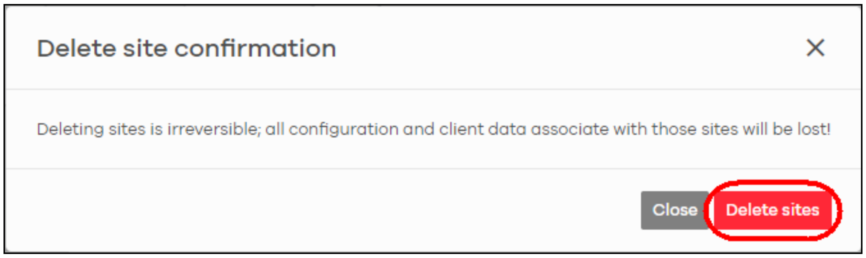
2 Click the check box (2) to select all sites.

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



☑	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.



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

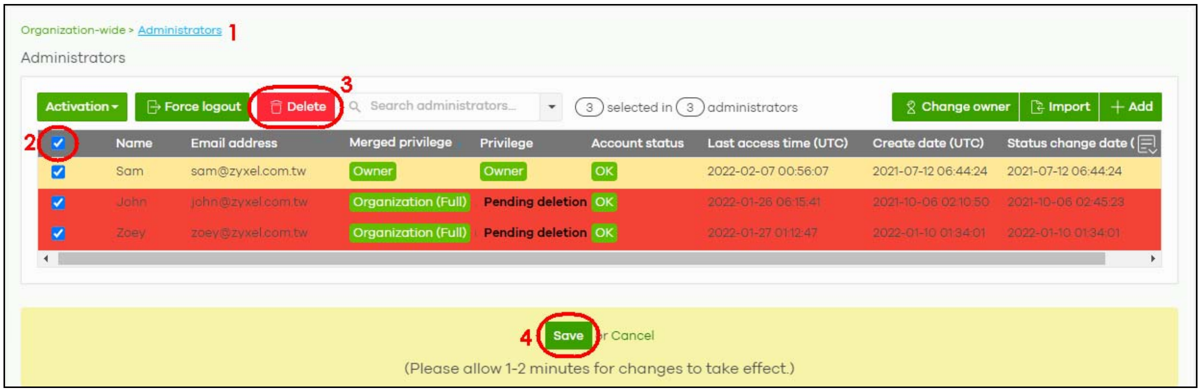
3.16.4 Delete All Administrators

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

2 Click the check box to select all administrators (2).

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

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



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.)

3.16.5 Remove All Users

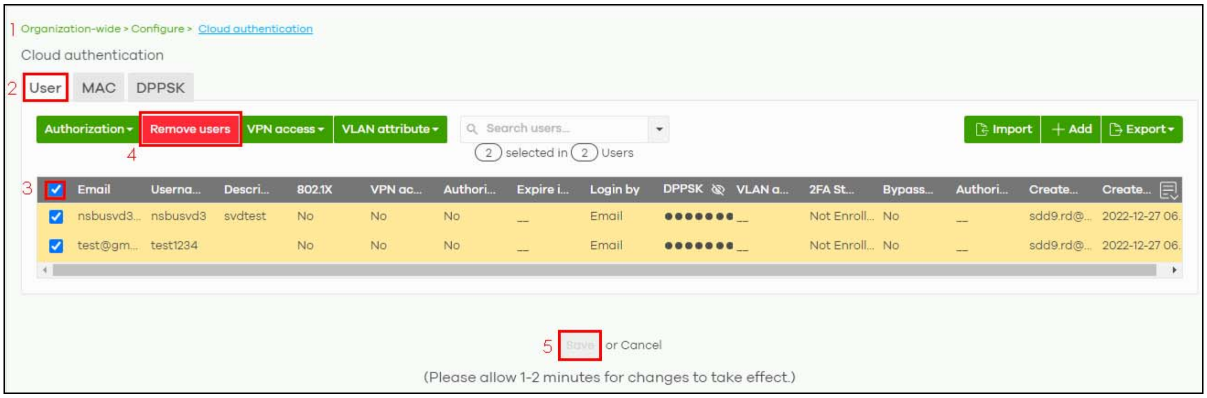
1 Go to **Organization-wide** > **Organization-wide manage** > **Cloud authentication** (1).

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

3 Click the check box to select all users (3).

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

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



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.

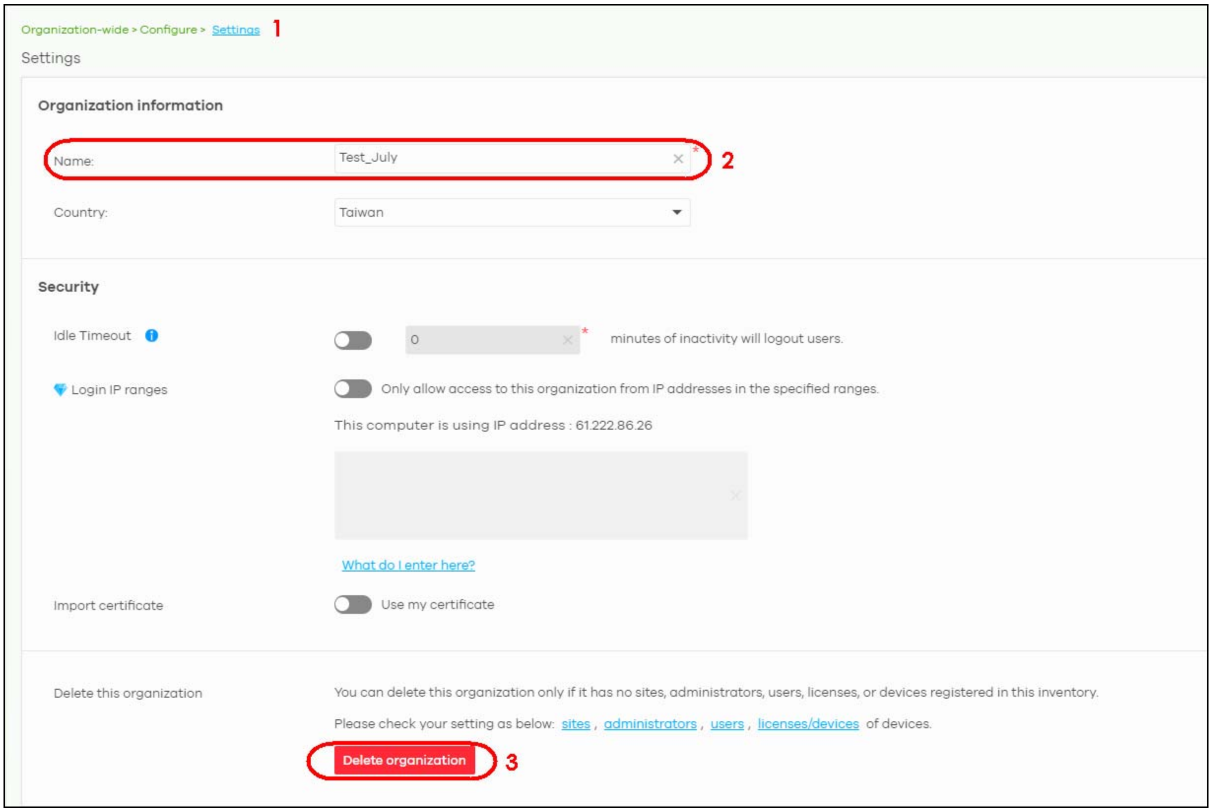
(Please allow 1-2 minutes for changes to take effect.)

3.16.6 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

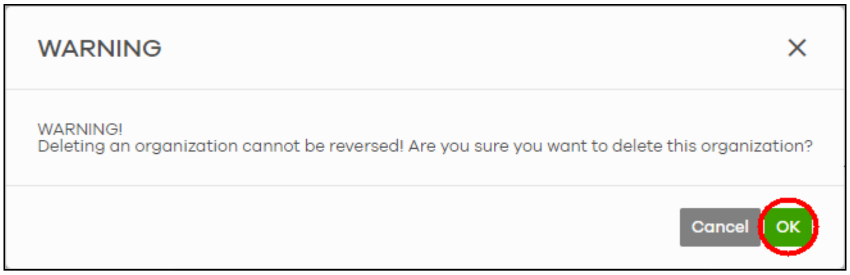
What do I enter here?

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.

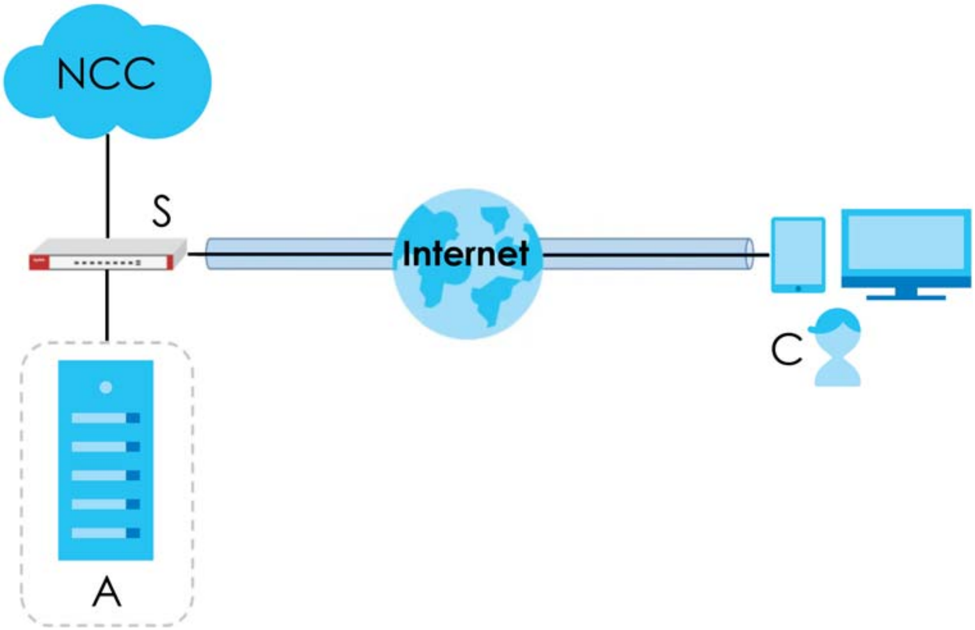


WARNING

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

3.17 Remote Access VPN Setup

The following figure illustrates a secure VPN channel configured through Nebula. 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:

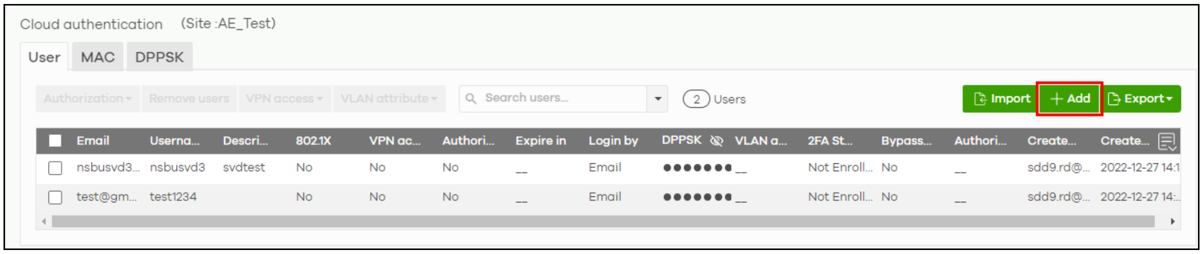
- Create a VPN user
- Enable the remote access VPN rule for IPSec VPN client
- Check the connection in Nebula.

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.

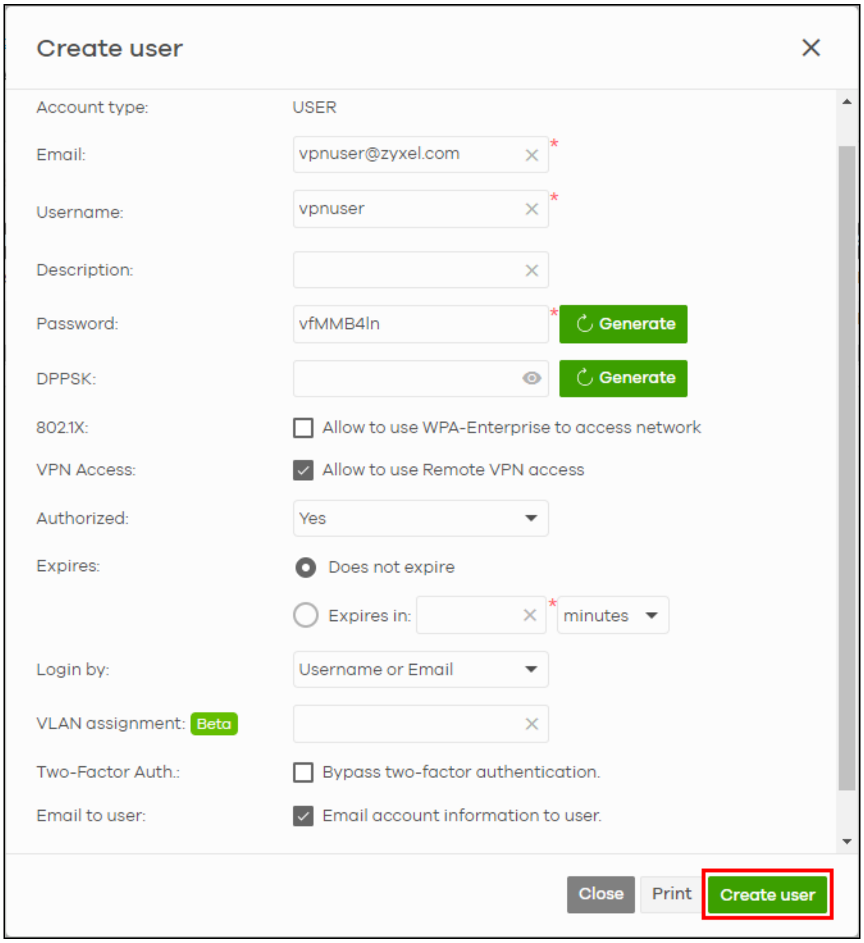
3.17.1 Create a VPN User

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


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:...

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 * Generate

DPPSK: Generate

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

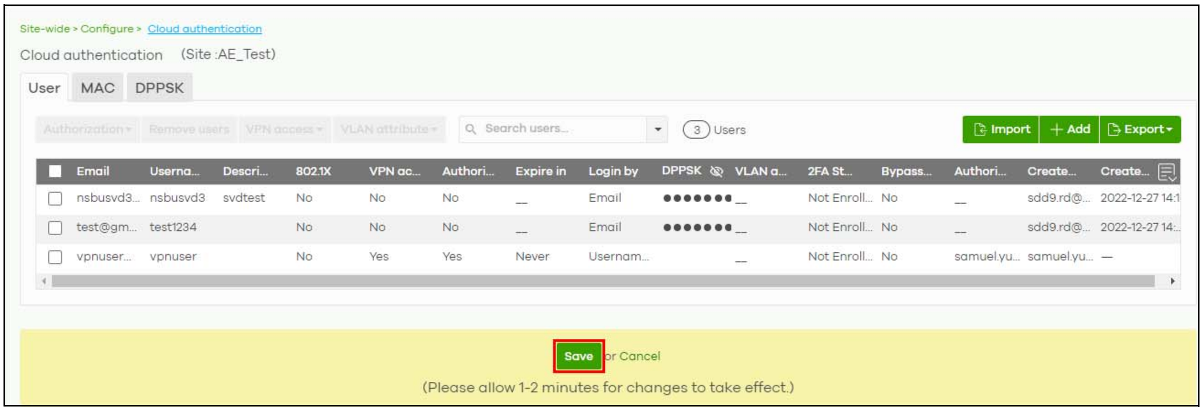
Login by: Username or Email

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)

3 Users

	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...	—

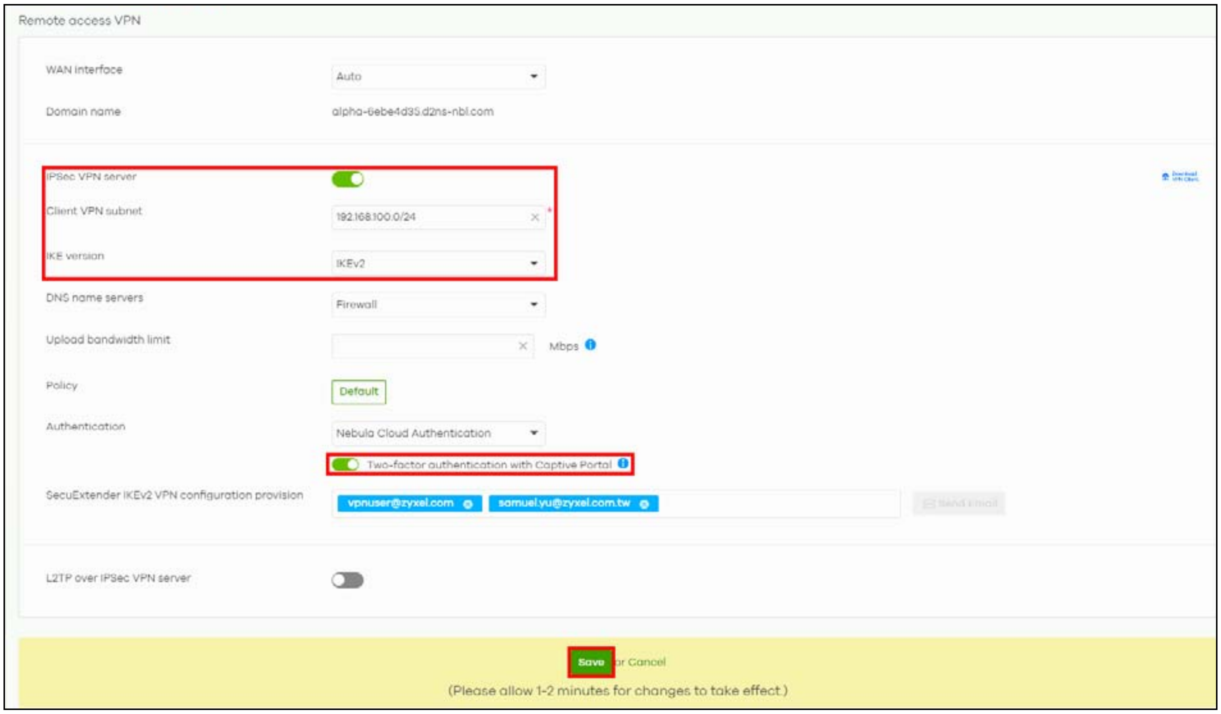
Save or Cancel

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

3.17.2 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: ON

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: ON

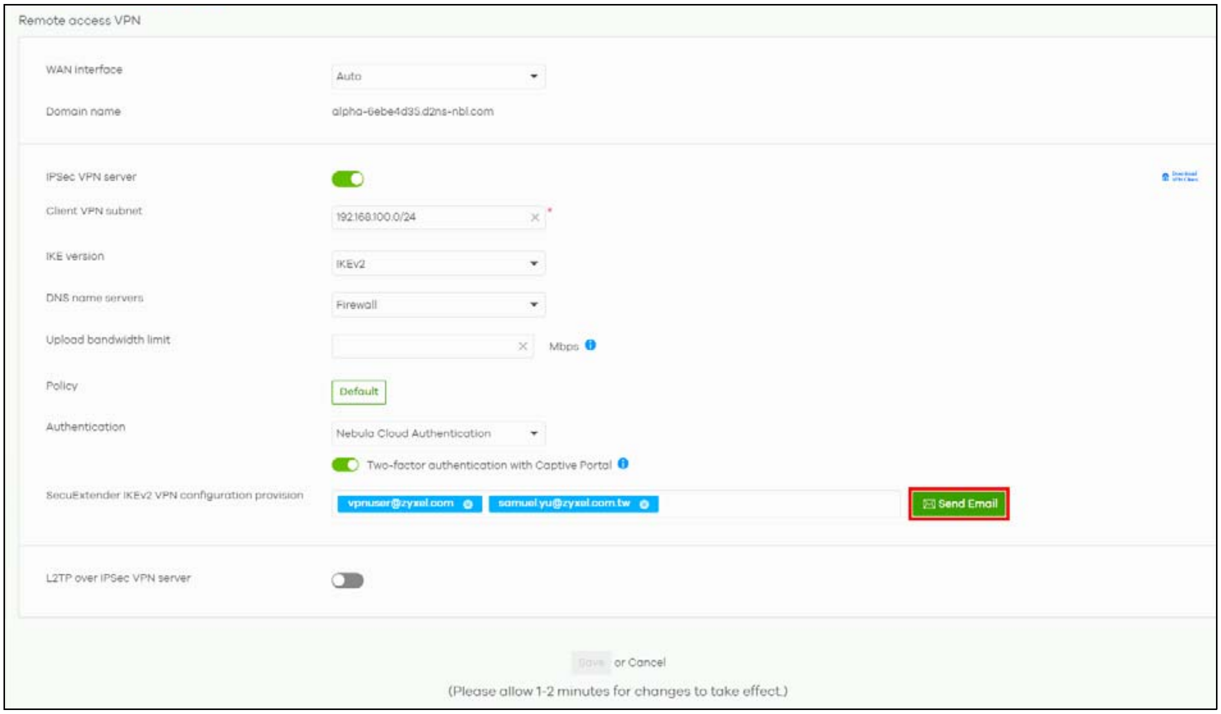
SecuExtender IKEv2 VPN configuration provision: vpnuser@zyxel.com, samuel.yu@zyxel.com.tw

L2TP over IPSec VPN server: OFF

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: ON

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: ON

SecuExtender IKEv2 VPN configuration provision: vpnuser@zyxel.com, samuel.yu@zyxel.com.tw

Send Email

L2TP over IPSec VPN server: OFF

Save or Cancel

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

3.17.3 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**).

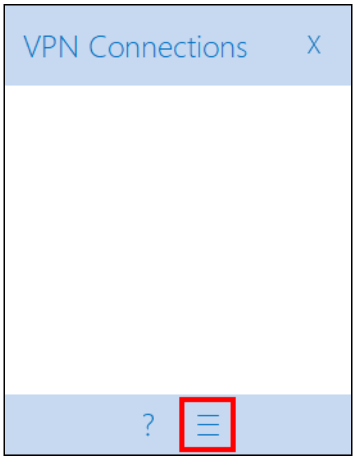
2 Click the link in the **Configuration for SecuExtender IPSec VPN Client** email for instructions on installing the SecuExtender and activating the license key. The **How to activate SecuExtender license key after your online purchase** webpage appears.

- 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.

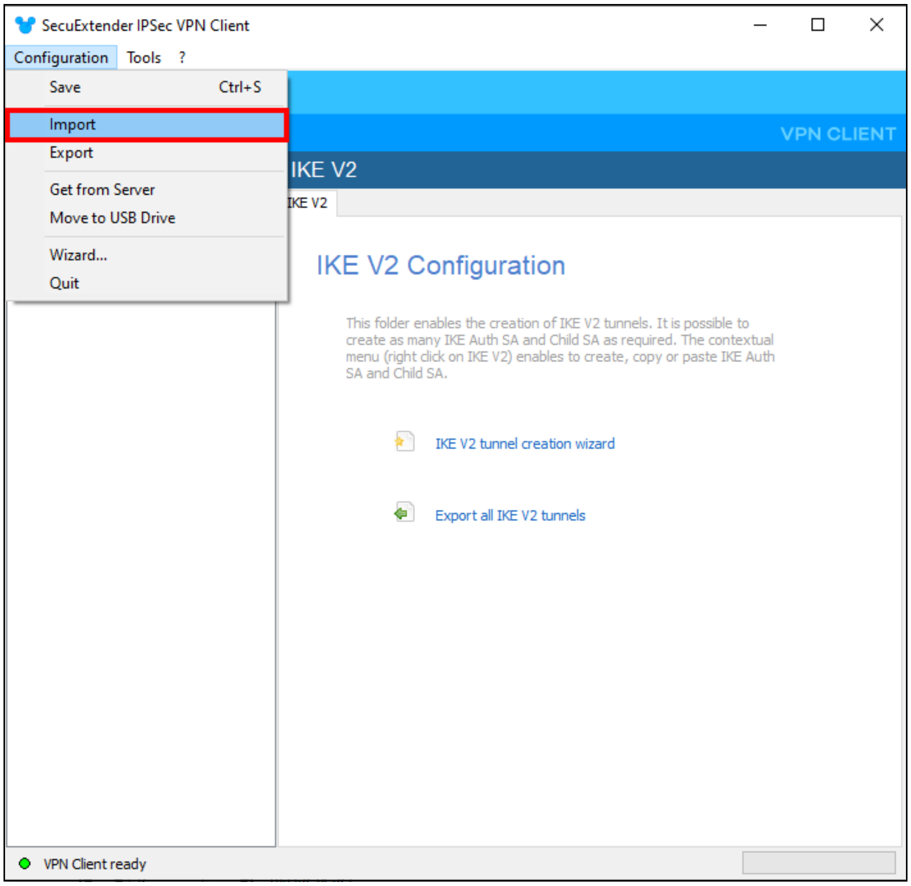
3.17.4 Import the VPN Configuration File

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.



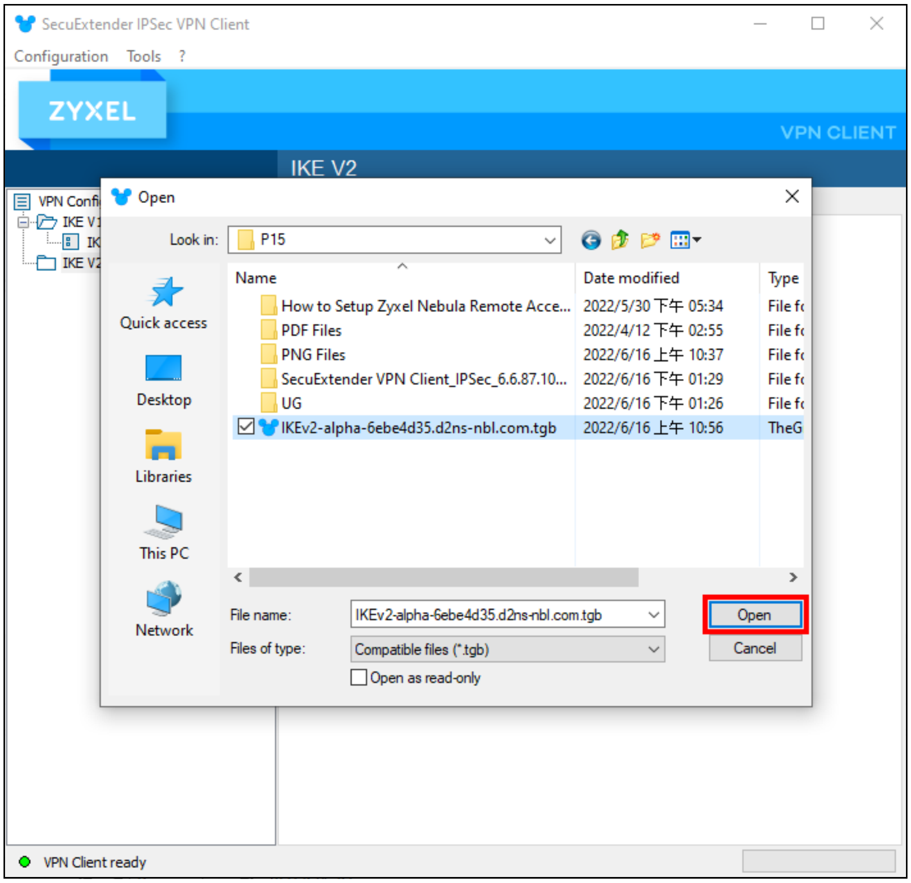
3 Click **Configuration** > **Import**.



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.

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

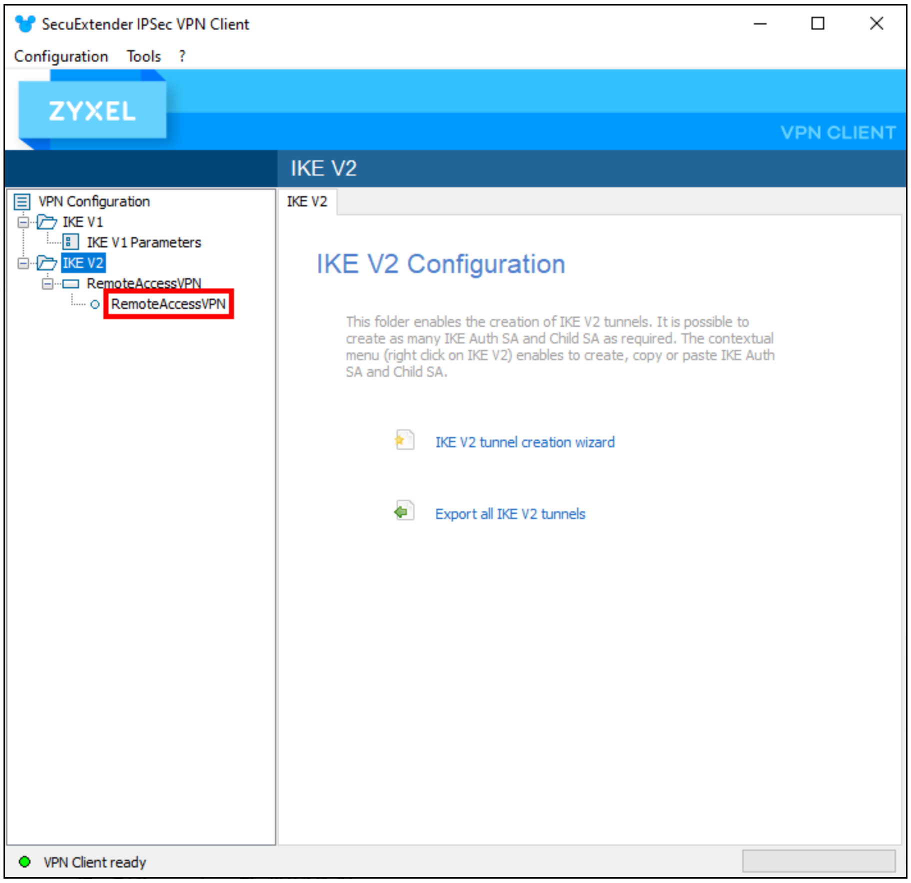
Name	Date modified	Type
How to Setup Zyxel Nebula Remote Acce...	2022/5/30 下午 05:34	File fc
PDF Files	2022/4/12 下午 02:55	File fc
PNG Files	2022/6/16 上午 10:37	File fc
SecuExtender VPN Client_IPSec_6.6.87.10...	2022/6/16 下午 01:29	File fc
UG	2022/6/16 下午 01:26	File fc
☑ IKEv2-alpha-6ebe4d35.d2ns-nbl.com.tgb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

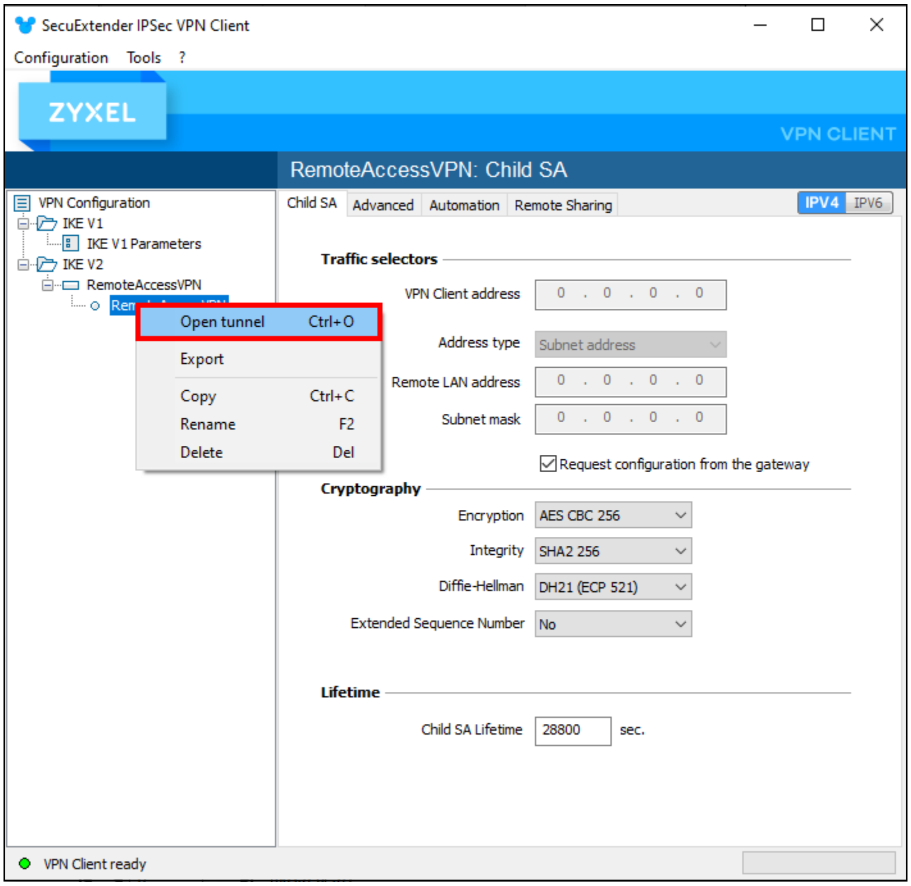


IKE V2 Configuration

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.

3.17.5 Open the VPN Tunnel

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



SecuExtender IPSec VPN Client

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)

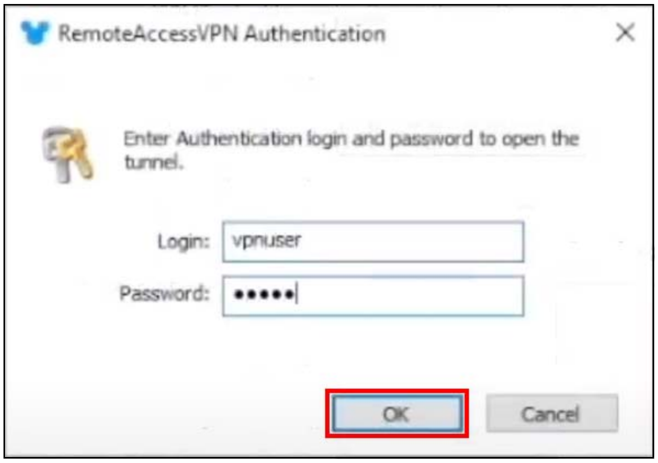
Extended Sequence Number: No

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**.



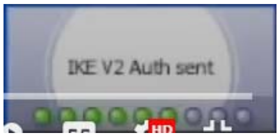
RemoteAccessVPN Authentication

Enter Authentication login and password to open the tunnel.

Login: vpnuser

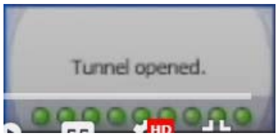
Password: •••••

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



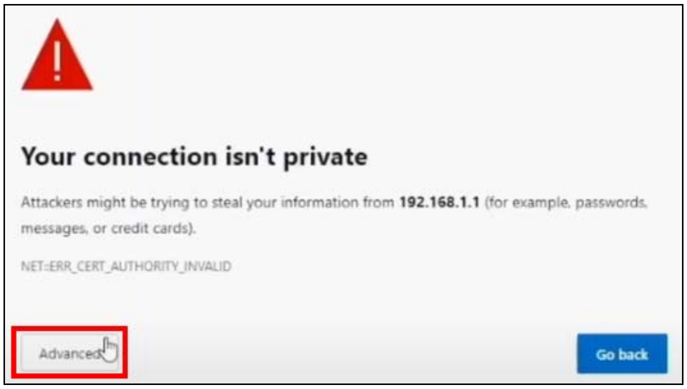
IKE V2 Auth sent

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**.

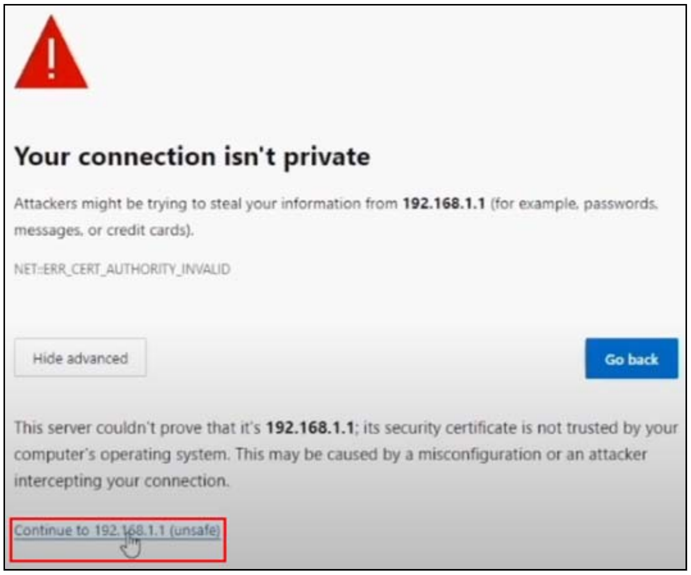
3 When **Your connection isn't private** appears on the web browser, click **Advanced** to continue.


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

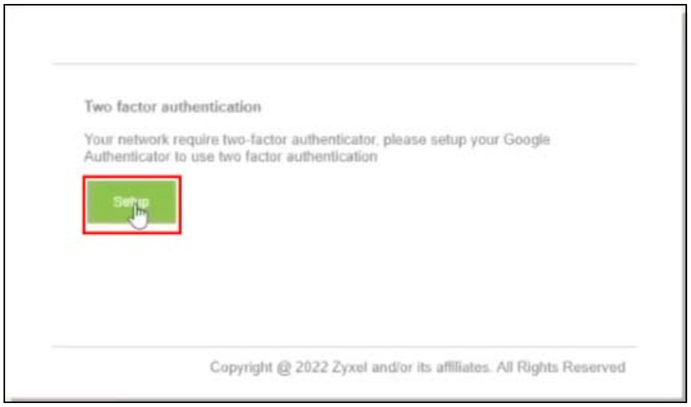
Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards).

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.

3.17.6 Set Up Two Factor Authentication to Bind the User Account

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

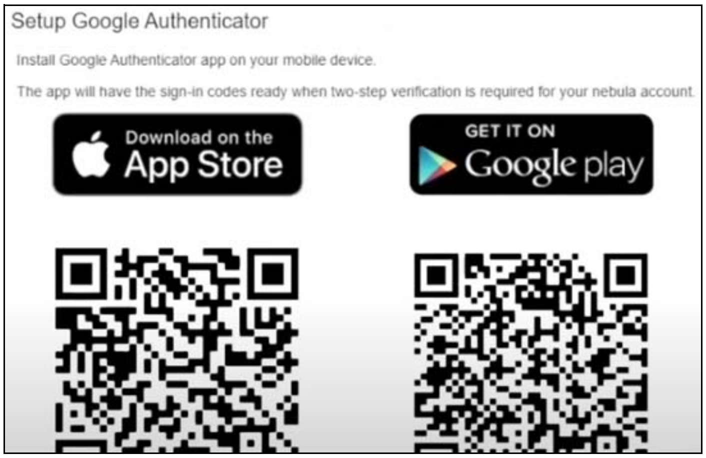


Two factor authentication

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**.

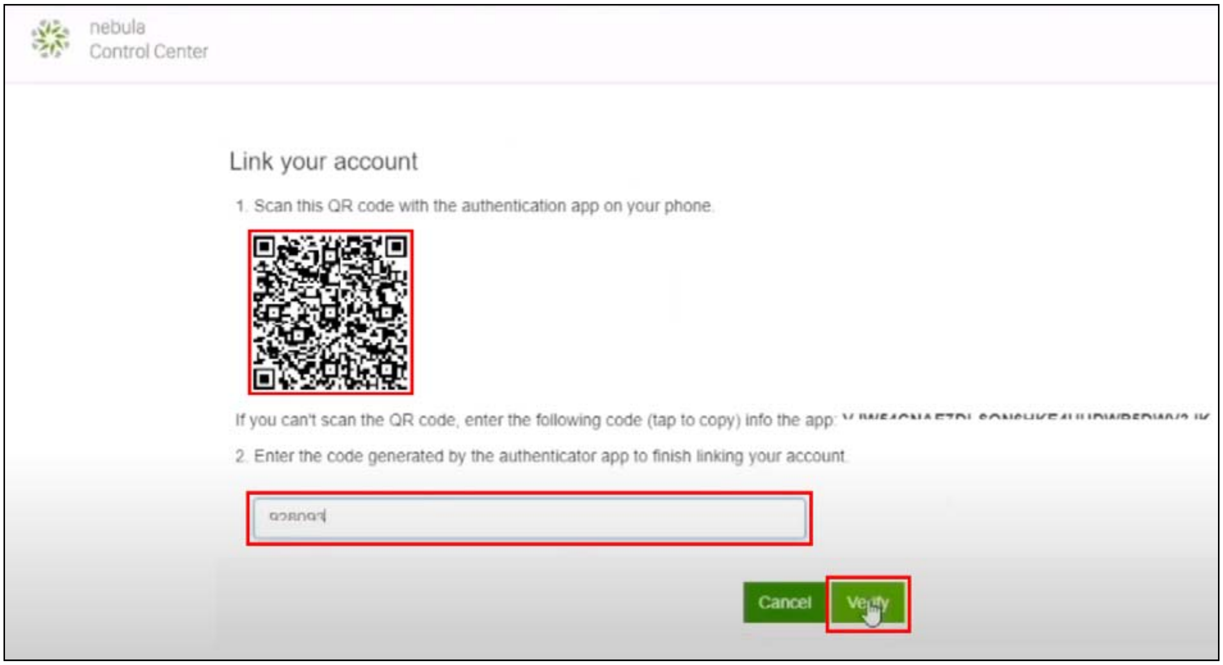


Setup Google Authenticator

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**.



Link your account

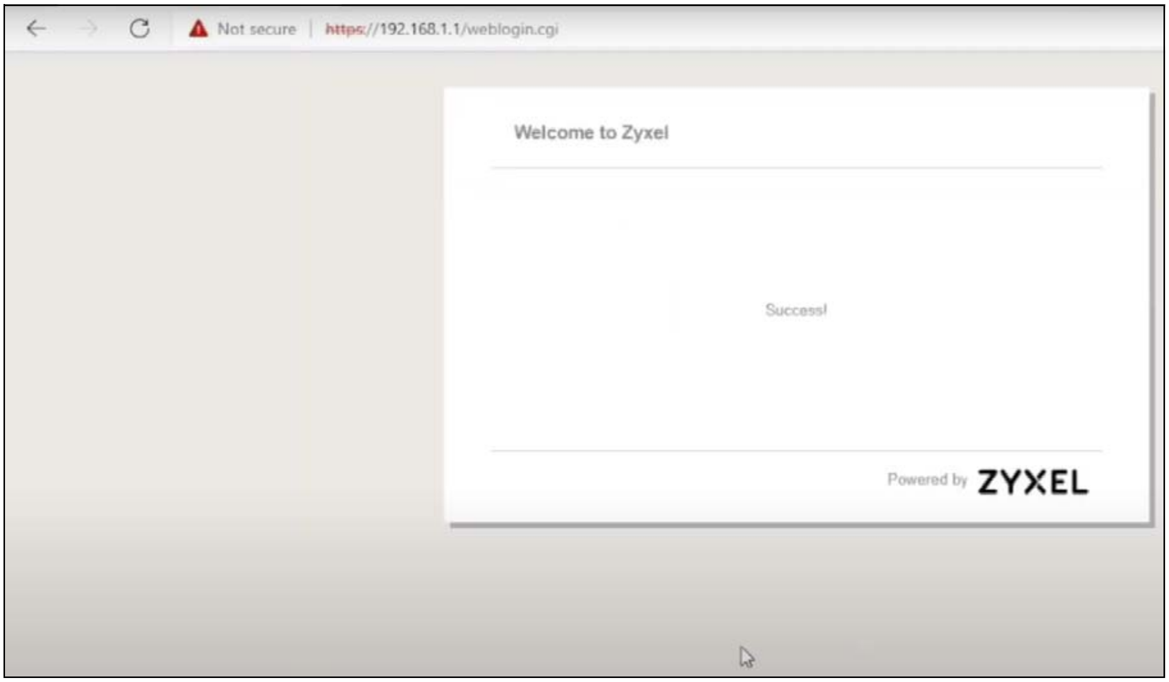
1. Scan this QR code with the authentication app on your phone.

If you can't scan the QR code, enter the following code (tap to copy) into 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.

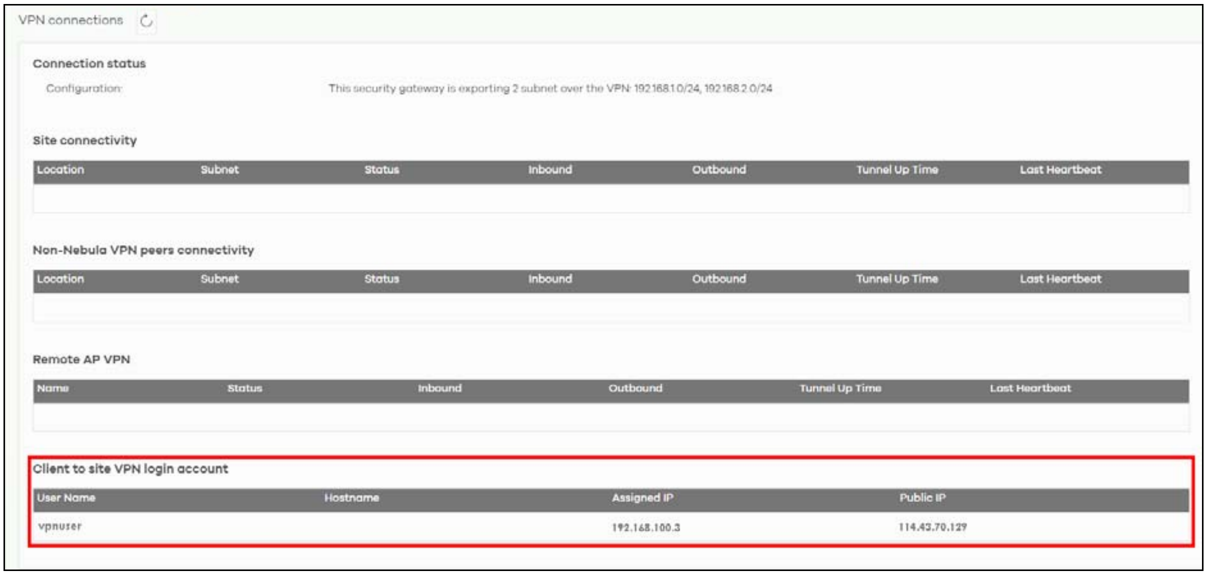


Welcome to Zyxel

Success!

3.17.7 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

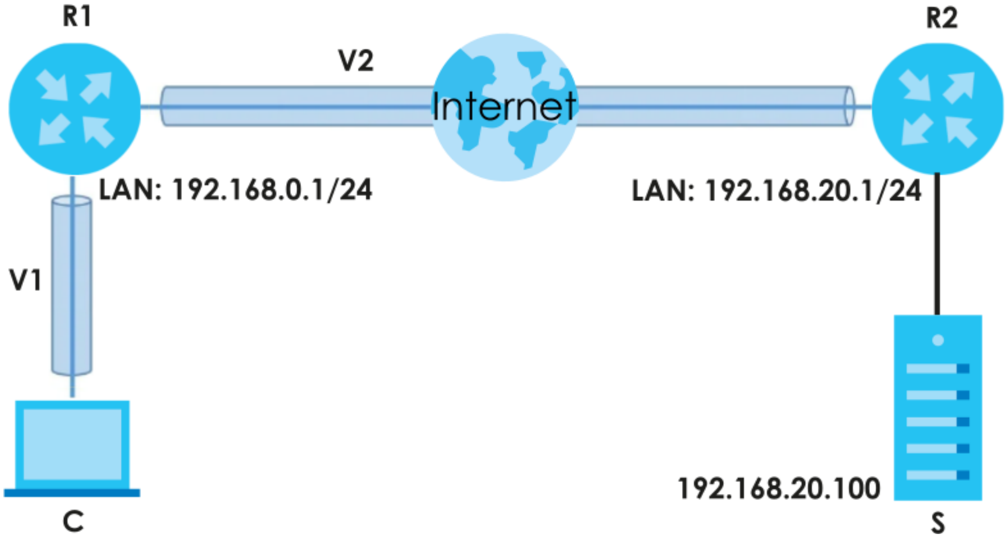
Client to site VPN login account

User Name	Hostname	Assigned IP	Public IP
vpnuser		192.168.100.3	114.43.70.129

3.18 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).



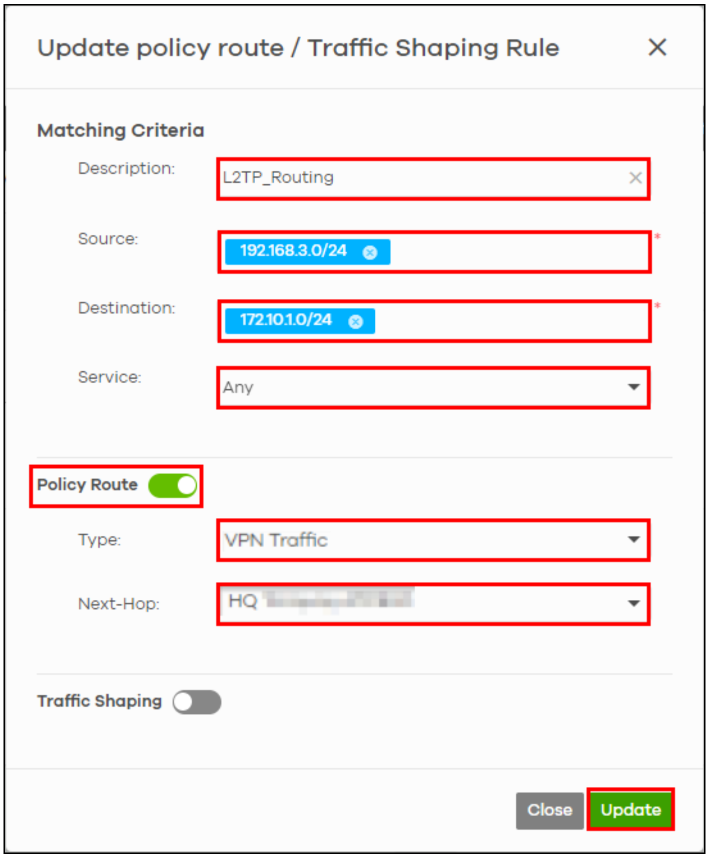
You can set up a VPN site-to-site tunnel to a cloud computing service like Microsoft Azure. To route L2TP traffic between your site and Microsoft Azure site, do the following:

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 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

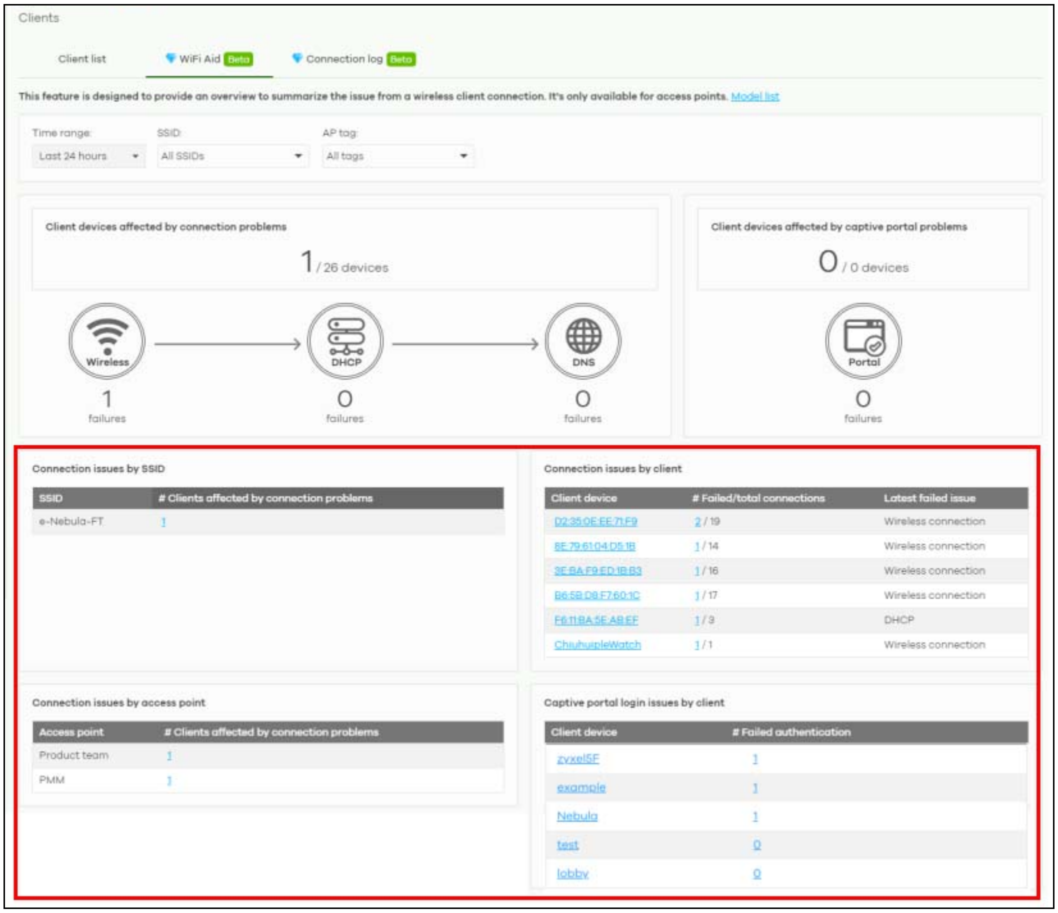
3.19 Resolve WiFi Connection Problems (for Nebula APs only)

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



Clients

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 / 26 devices

Client devices affected by captive portal problems

0 / 0 devices

Connection issues by SSID

SSID	# Clients affected by connection problems
e-Nebula-FT	1

Connection issues by client

Client device	# Failed/total connections	Latest failed issue
D2:35:0E:EE:71:F9	2 / 19	Wireless connection
8E:79:61:04:D5:1B	1 / 14	Wireless connection
3E:BA:F9:ED:1B:B3	1 / 16	Wireless connection
B6:5B:D8:F7:60:1C	1 / 17	Wireless connection
F6:11:BA:5E:AB:EF	1 / 3	DHCP
ChiuhupleWatch	1 / 1	Wireless connection

Connection issues by access point

Access point	# Clients affected by connection problems
Product team	1
PMM	1

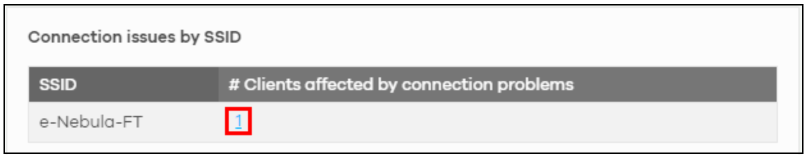
Captive portal login issues by client

Client device	# Failed authentication
zyxel5F	1
example	1
Nebula	1
test	0
lobby	0

Connection Issues by SSID

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

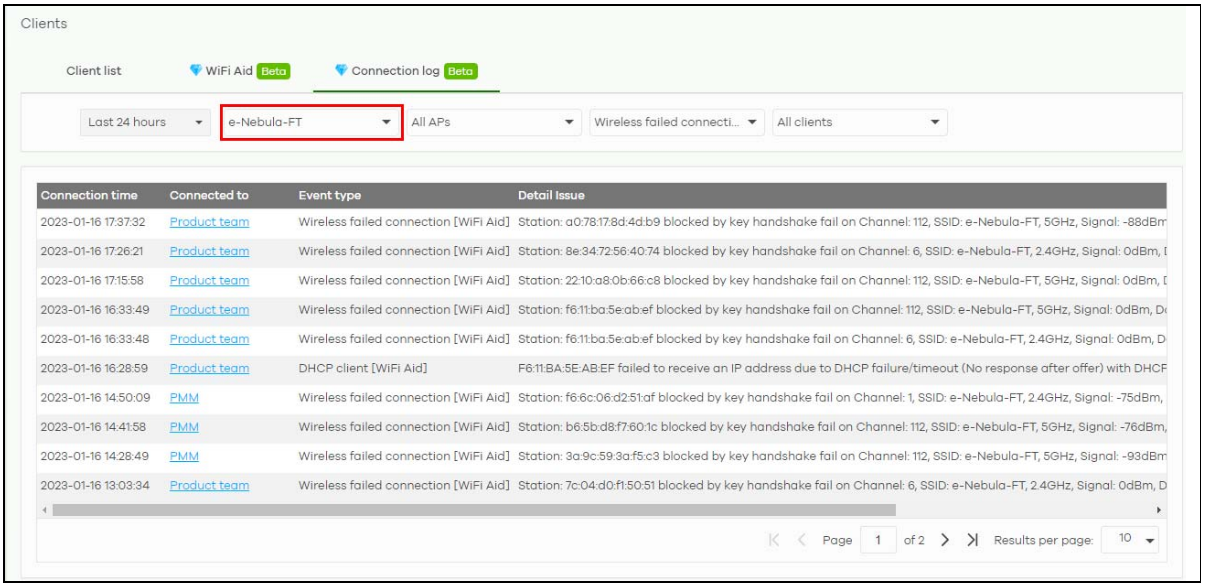
1 Click a hyperlink in the **# Clients affected by connection problems** column.



Connection issues by SSID

SSID	# Clients affected by connection problems
e-Nebula-FT	1

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



Last 24 hours | e-Nebula-FT | All APs | Wireless failed connecti... | All clients

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, D
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, D
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

Page 1 of 2 Results per page: 10

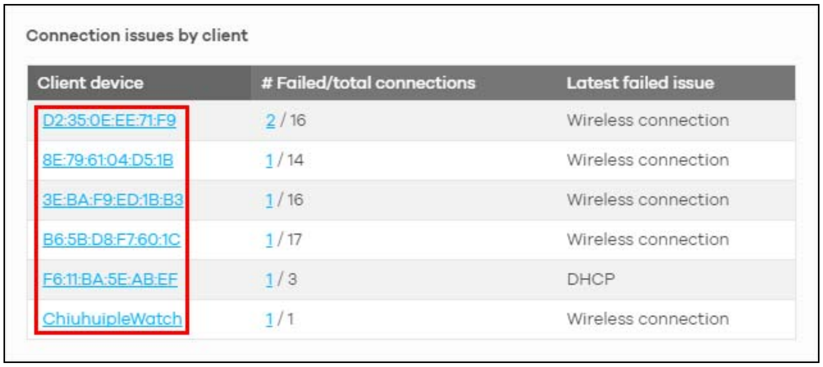
2 Use the following information listed in chronological order to resolve WiFi connection issues.

- **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 client/DNS failures – numerator) over the number of total connection attempts (denominator). The list displays the WiFi client with the most connection failures first, in descending order.

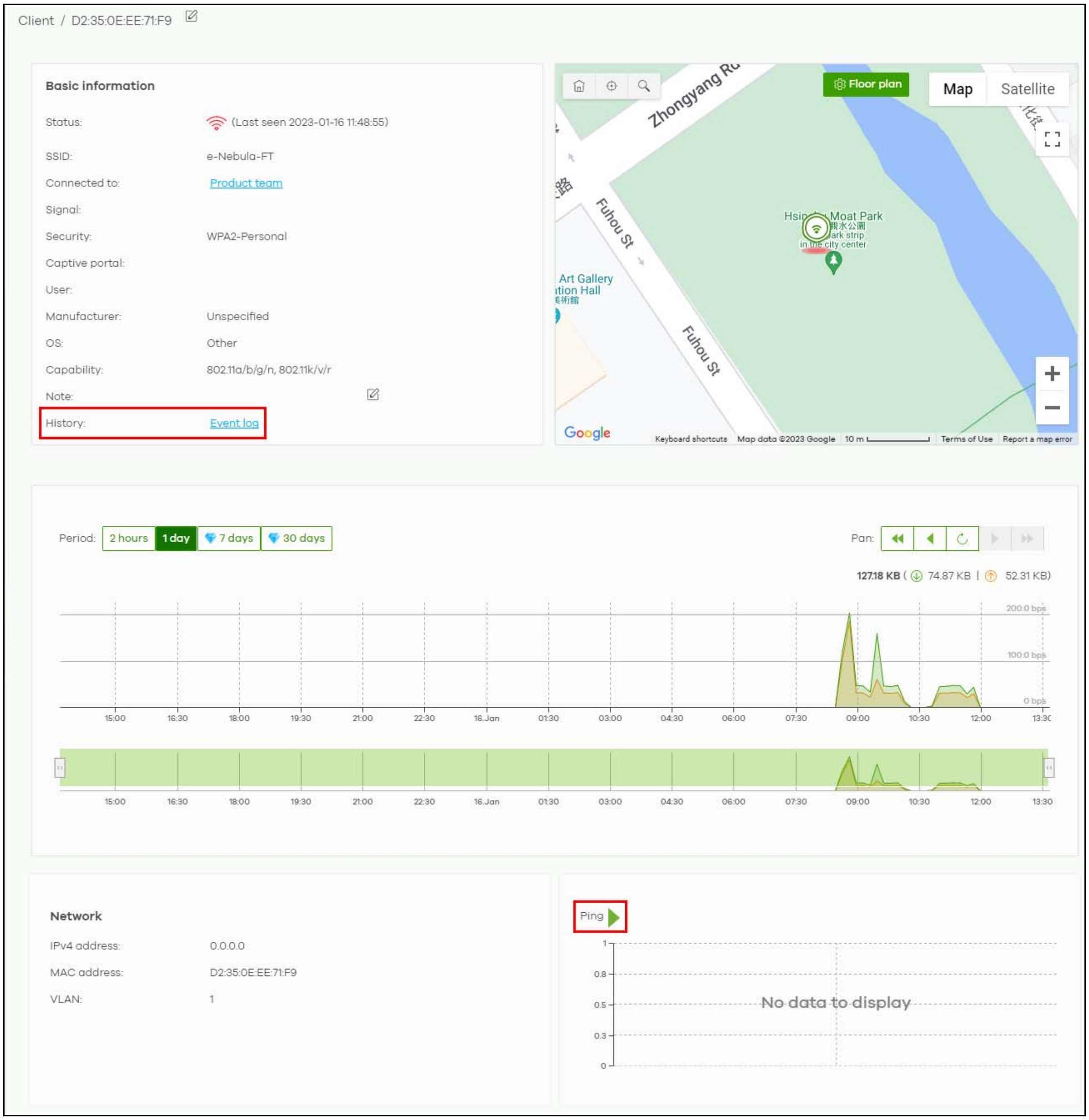
1 Click a hyperlink in the **Client device** column.



Connection issues by client

Client device	# Failed/total connections	Latest failed issue
D2:35:0E:EE:71:F9	2 / 16	Wireless connection
8E:79:61:04:D5:1B	1 / 14	Wireless connection
3E:BA:F9:ED:1B:B3	1 / 16	Wireless connection
B6:5B:D8:F7:60:1C	1 / 17	Wireless connection
F6:11:BA:5E:AB:EF	1 / 3	DHCP
ChiuhuipleWatch	1 / 1	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

Network

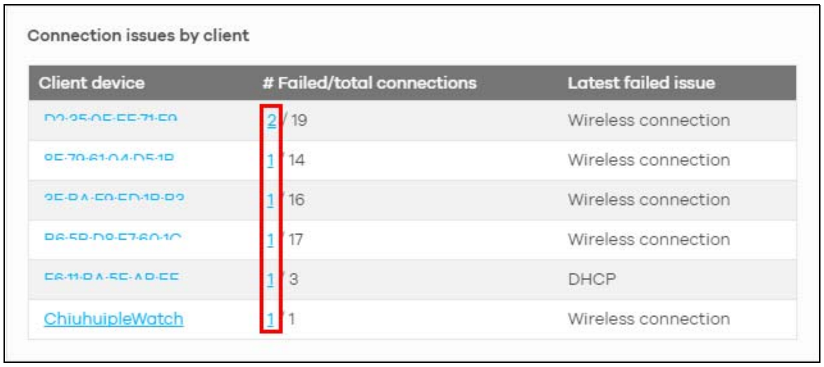
IPv4 address:	0.0.0.0
MAC address:	D2:35:0E:EE:71:F9
VLAN:	1

2 Use the information in this screen to identify the WiFi client with connection issues. See Table 24 on page 196 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.

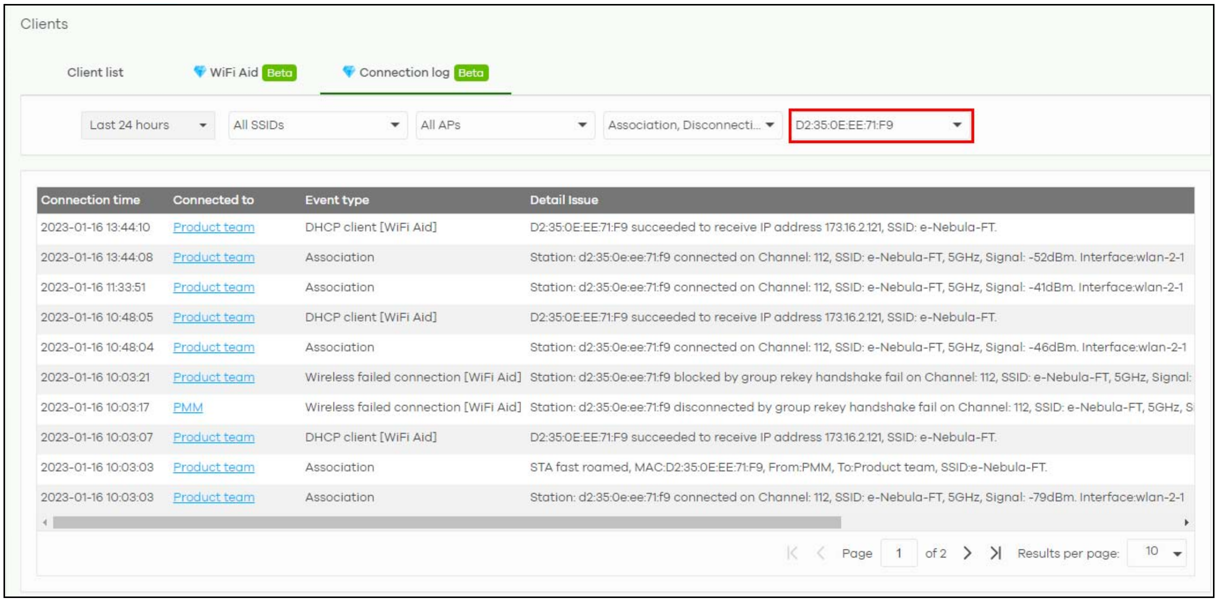
5 Click the numerator hyperlink in the **# Failed/total connections** column.



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
D6-5B-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** > **Monitor** > **Site features logs** screen appears showing all related event logs between APs and WiFi clients. See Section on page 115 on using the information listed in chronological order to resolve WiFi connection issues.



Clients

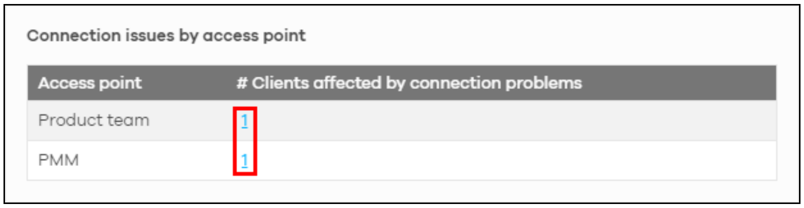
Last 24 hours | All SSIDs | All APs | Association, Disconnecti... | D2:35:0E:EE:71:F9

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 client/DNS failures listed according to access point. The list displays the access point with the most connection failures first, in descending order.

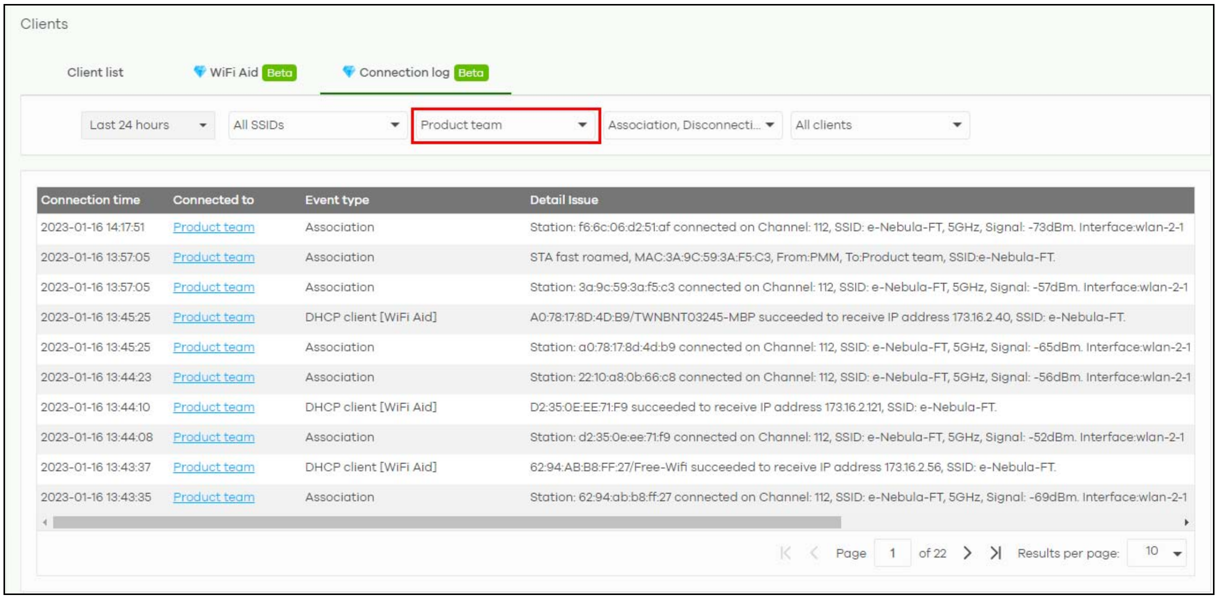
1 Click a hyperlink in the # **Clients affected by connection problems** column of a specific AP.



Connection issues by access point

Access point	# Clients affected by connection problems
Product team	1
PMM	1

The **Site-wide** > **Monitor** > **Site features logs** screen appears showing all related event logs between a specific AP (for example, Product team) and its WiFi clients. See Section on page 115 on using the information listed in chronological order to resolve WiFi connection issues.

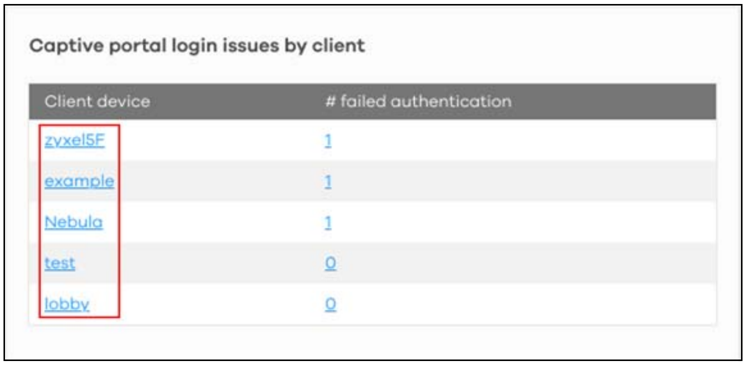


Connection time	Connected to	Event type	Detail Issue
2023-01-16 14:17:51	Product team	Association	Station: f6:6c:06:d2:51:af connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -73dBm. Interface:wlan-2-1
2023-01-16 13:57:05	Product team	Association	STA fast roamed, MAC:3A:9C:59:3A:F5:C3, From:PMM, 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 hotspot authentication. The list displays the WiFi client that failed hotspot authentication the most number of times first, in descending order.

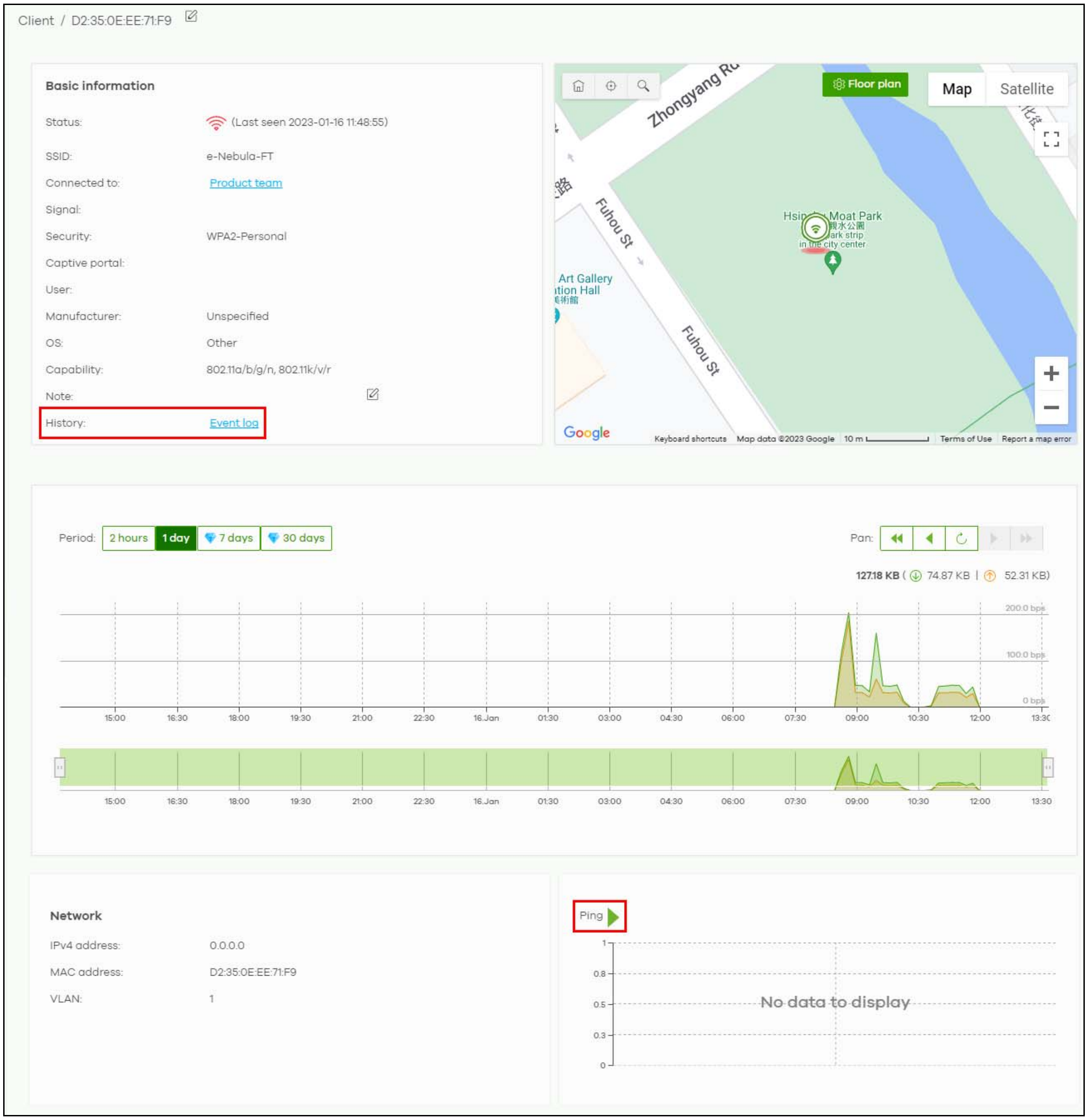
1 Click a hyperlink in the **Client device** column.



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 116 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

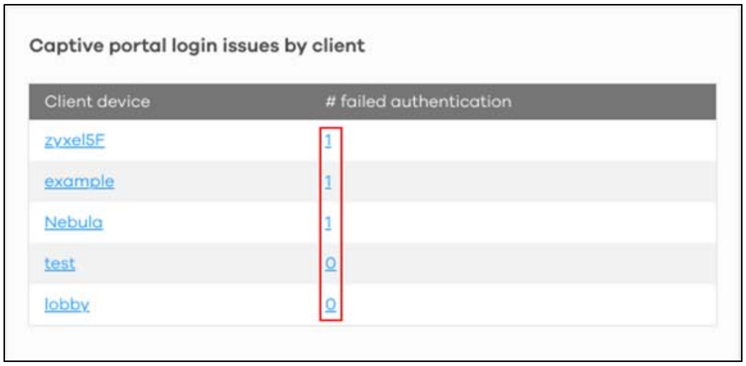
Ping

2 Use the information in this screen to identify the WiFi client with connection issues. See Table 24 on page 196 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.

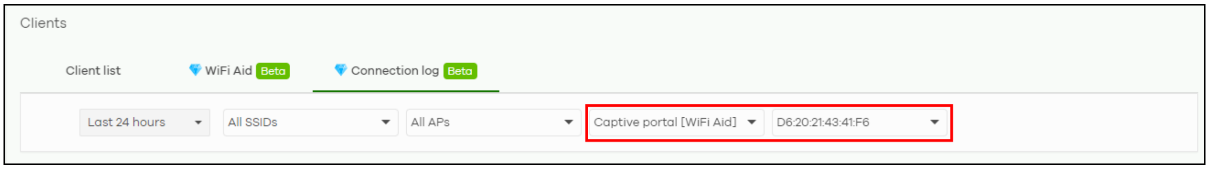
5 Click the hyperlink in the **# Failed Authentication** column.



Captive portal login issues by client

Client device	# failed authentication
zyxel5F	1
example	1
Nebula	1
test	0
lobby	0

The **Site-wide** > **Monitor** > **Site features logs** screen appears showing all related event logs of a specific client device with failed hotspot authentication event type.



Clients

Client list | WiFi Aid Beta | Connection log Beta

Last 24 hours | All SSIDs | All APs | Captive portal [WiFi Aid] | D6:20:21:43:41:F6

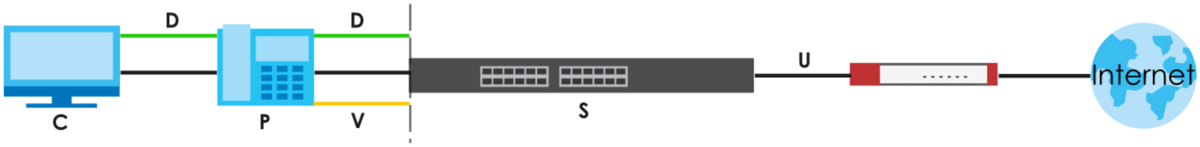
6 Use the following information listed in chronological order to resolve failed hotspot authentication issues.

- **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.

3.20 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).



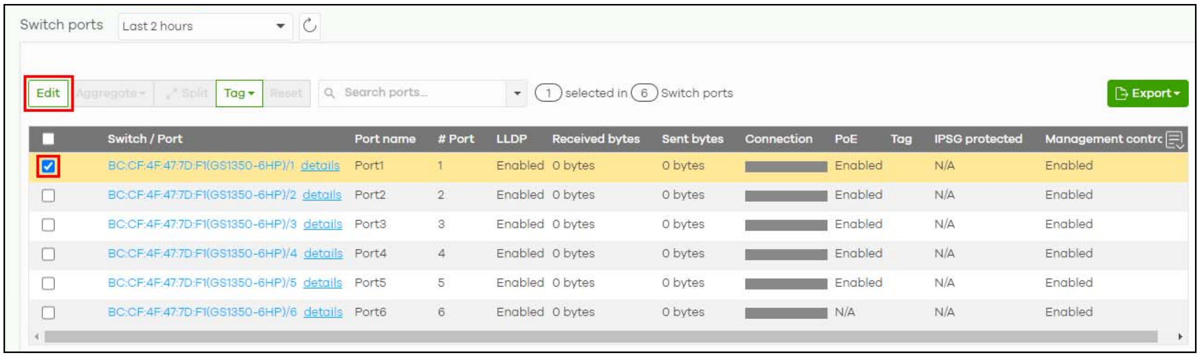
The Nebula Device will add a VLAN tag for voice packets (V) and data packets (D) separately after receiving them. Then forward the voice packets (V) and data packets (D) to the uplink port (U). This section shows you how to separate data packets (D) and voice packets (V) between a VoIP device (P) and computer (C), without having to assign a VLAN tag.

- Configure the Nebula Device Ports
- Configure the Voice VLAN

3.20.1 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**.



Switch ports Last 2 hours

Edit Aggregate Split Tag Reset Search ports... 1 selected in 6 Switch ports Export

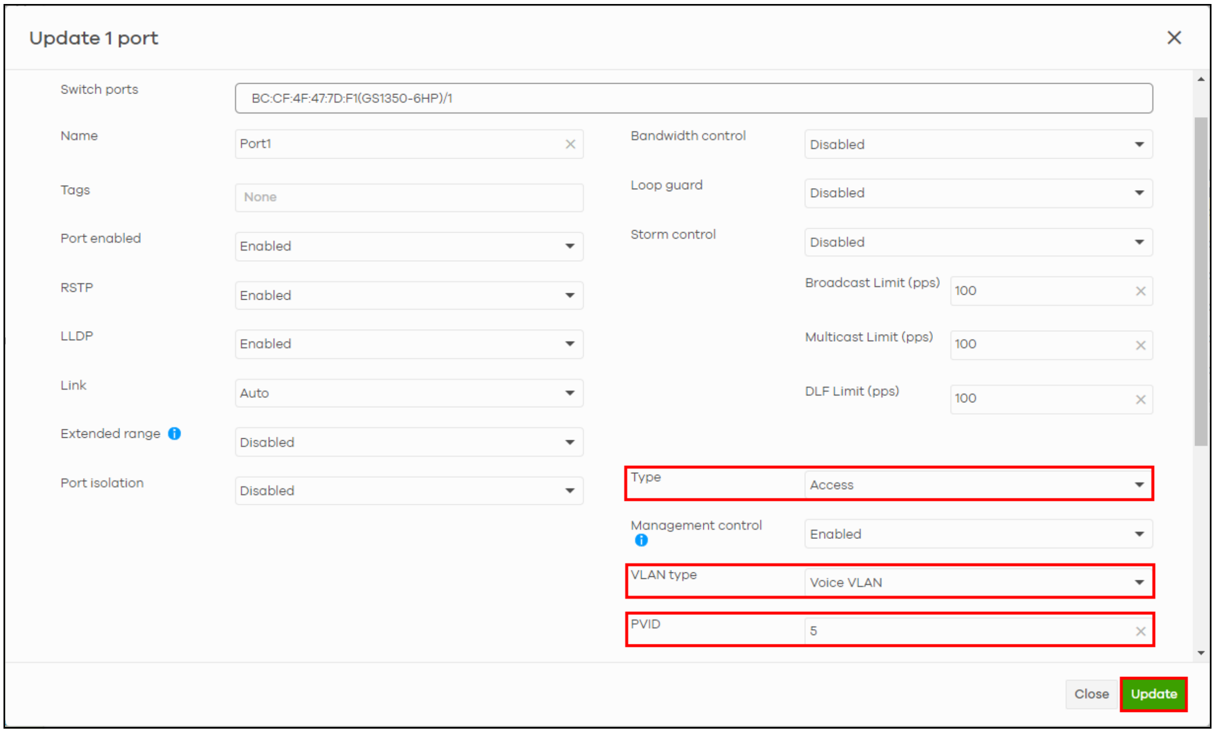
	Switch / Port	Port name	# Port	LLDP	Received bytes	Sent bytes	Connection	PoE	Tag	IPSG protected	Management contrc
☑	BC:CF:4F:47:7D:F1(GS1350-6HP)/1 details	Port1	1	Enabled	0 bytes	0 bytes		Enabled		N/A	Enabled
□	BC:CF:4F:47:7D:F1(GS1350-6HP)/2 details	Port2	2	Enabled	0 bytes	0 bytes		Enabled		N/A	Enabled
□	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		
Port isolation	Disabled	Type	Access
		Management control	Enabled
		VLAN type	Voice VLAN
		PVID	5

Close Update

3.20.2 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.

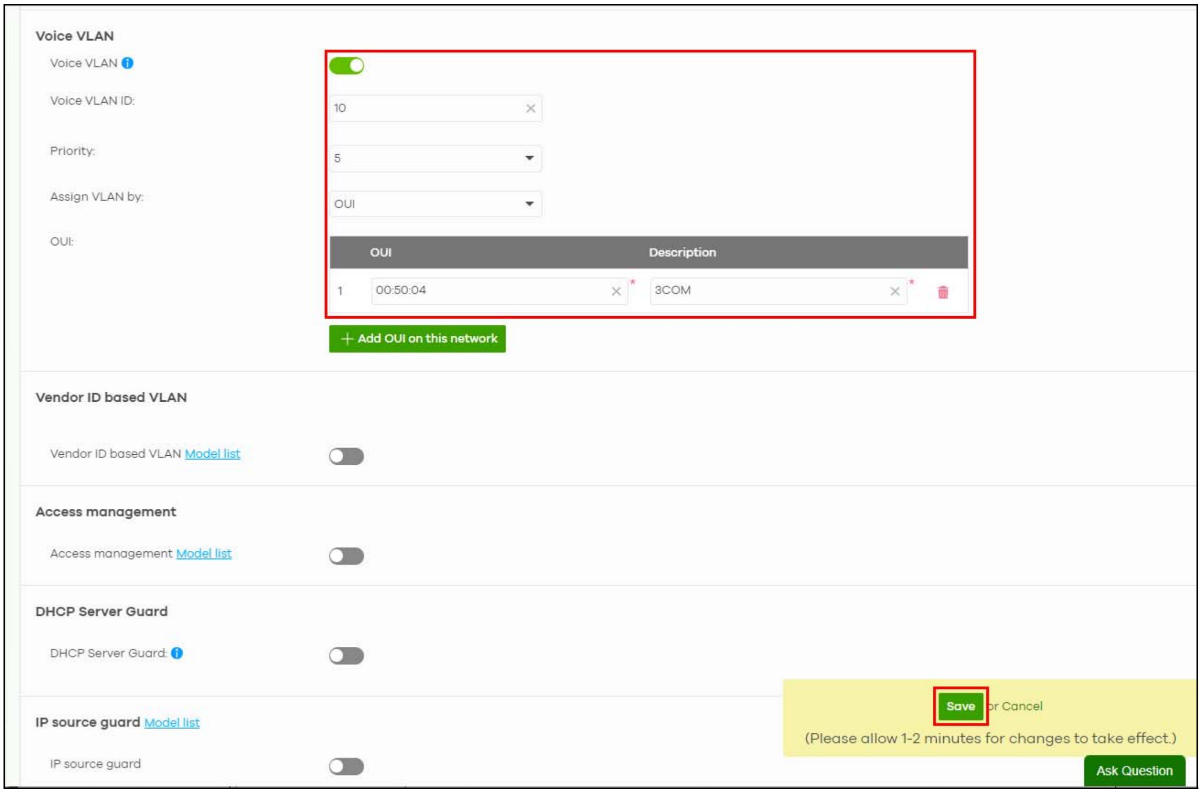
4 Enter a **Voice VLAN ID**.

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: on

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: off

Access management

Access management Model list: off

DHCP Server Guard

DHCP Server Guard: off

IP source guard Model list

IP source guard: off

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

8 Then click **Save**.

3.21 Manage IPTV (for Nebula Switches only)

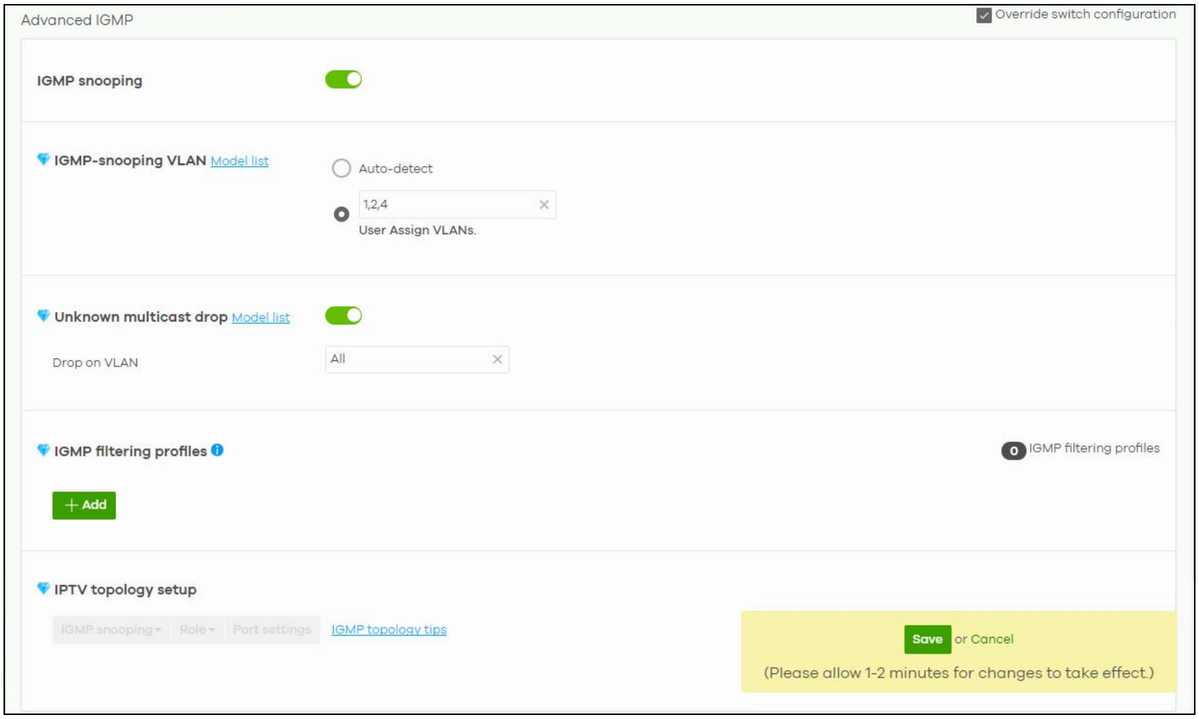
This section shows you how to configure IPTV settings and view IPTV reports:

- Set up the VLAN for IPTV
- Define the Role of a Switch

- Configure the Channel Profile and Naming

3.21.1 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: on

IGMP-snooping VLAN Model list
○ Auto-detect
● 1,2,4
User Assign VLANs.

Unknown multicast drop Model list: on

Drop on VLAN: All

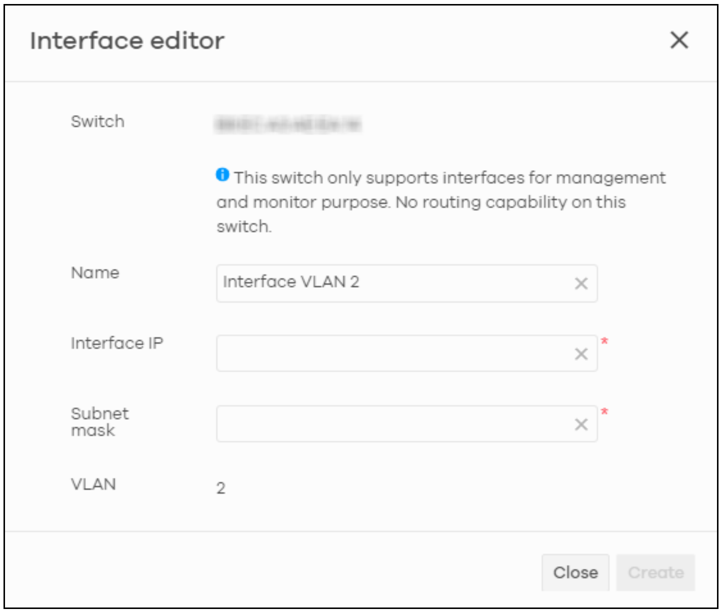
IGMP filtering profiles

0 IGMP filtering profiles

IPTV topology setup

(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.



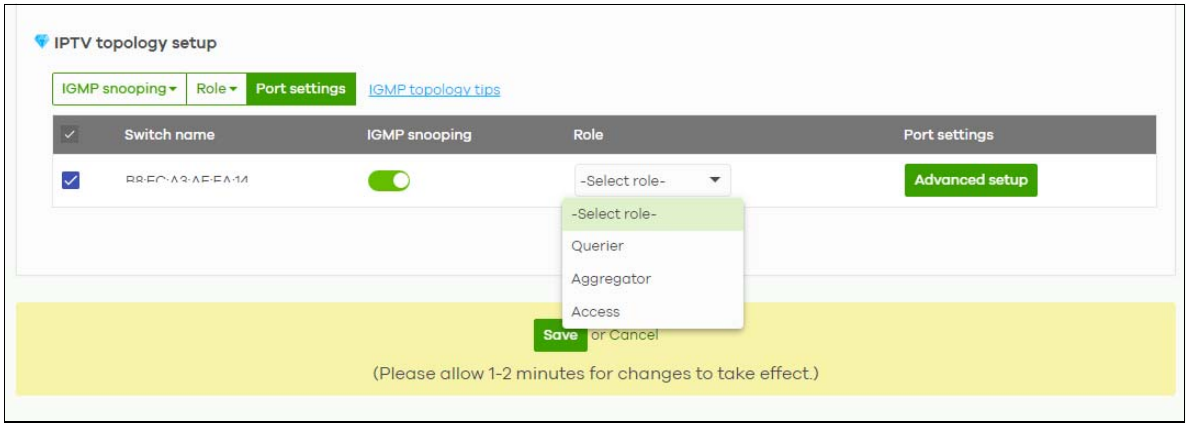
Interface editor

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

3.21.2 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.



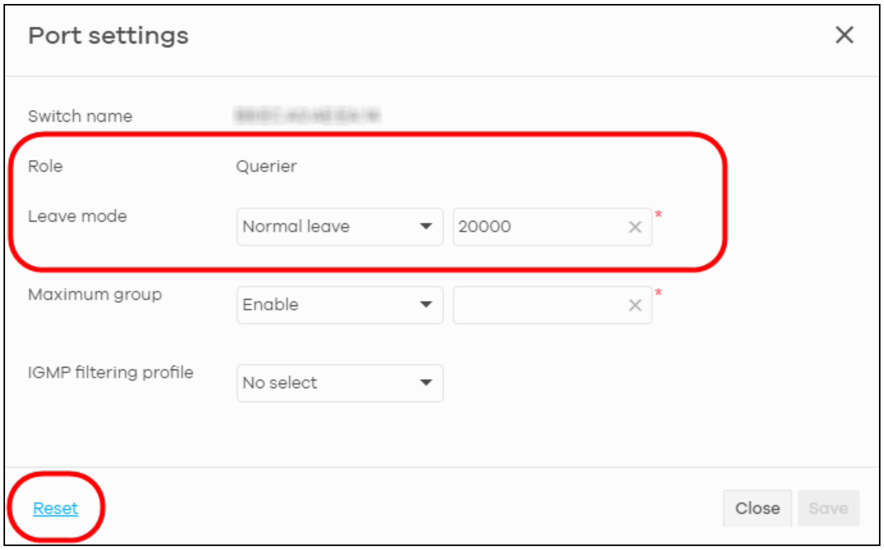
IPTV topology setup

☑	Switch name	IGMP snooping	Role	Port settings
☑	B8:EC:A3:AE:FA:14	●	-Select role-	Advanced setup

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

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.

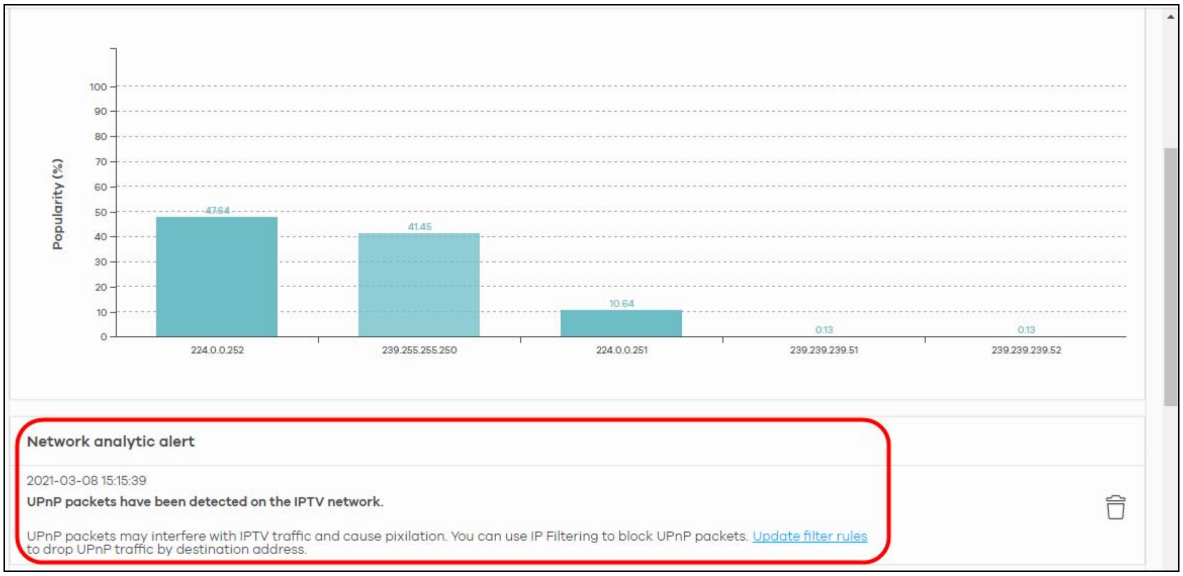
Note: You can click **Reset** to reset the port settings to default.



Port settings

Switch name	[redacted]	
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.



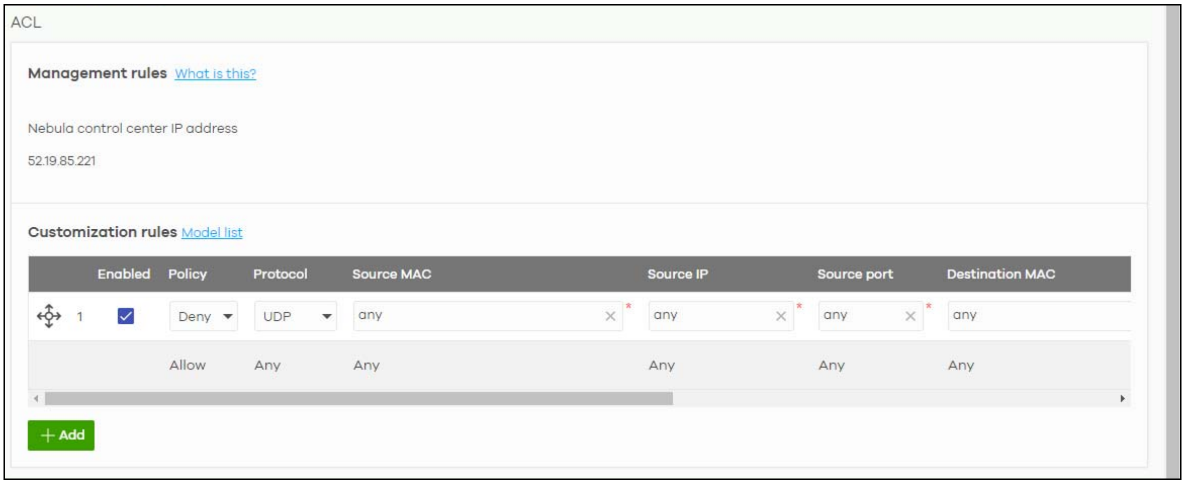
Network analytic alert

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

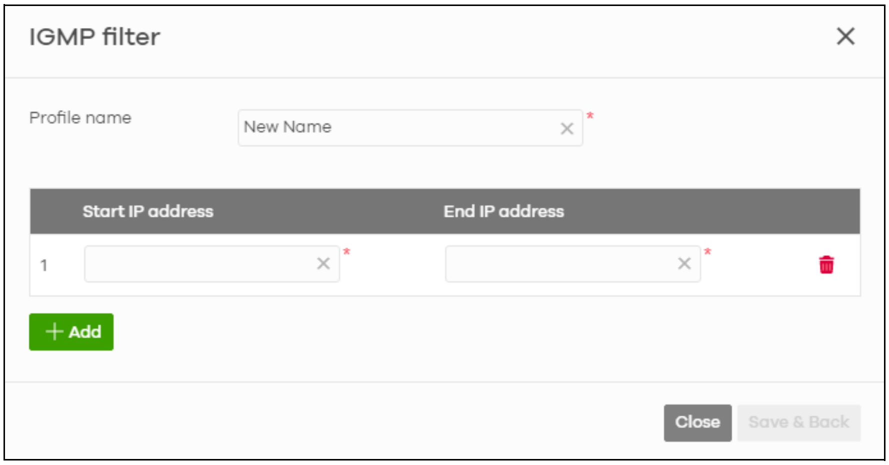
Customization rules Model list

	Enabled	Policy	Protocol	Source MAC	Source IP	Source port	Destination MAC
1	☑	Deny	UDP	any	any	any	any
		Allow	Any	Any	Any	Any	Any

3.21.3 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.

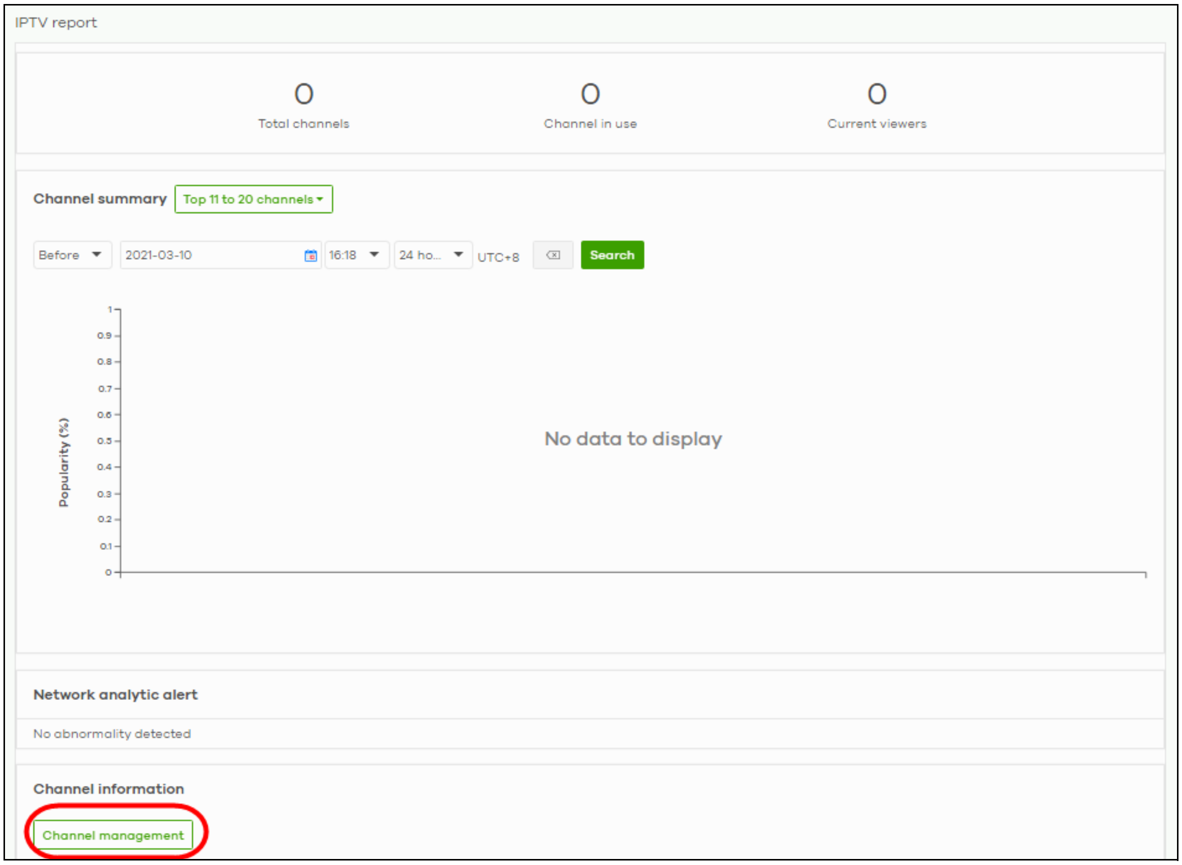


IGMP filter

Profile name: New Name

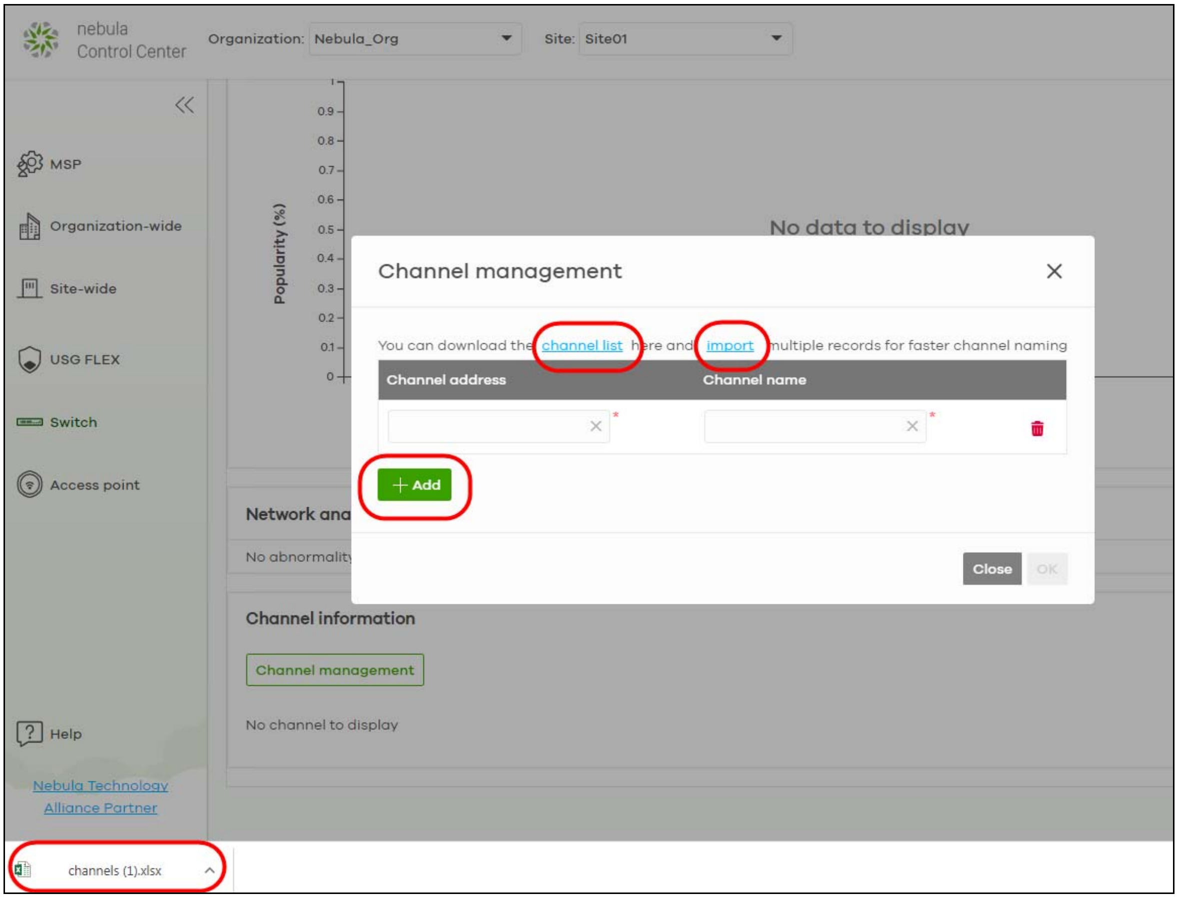
	Start IP address	End IP address
1		

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**.



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.

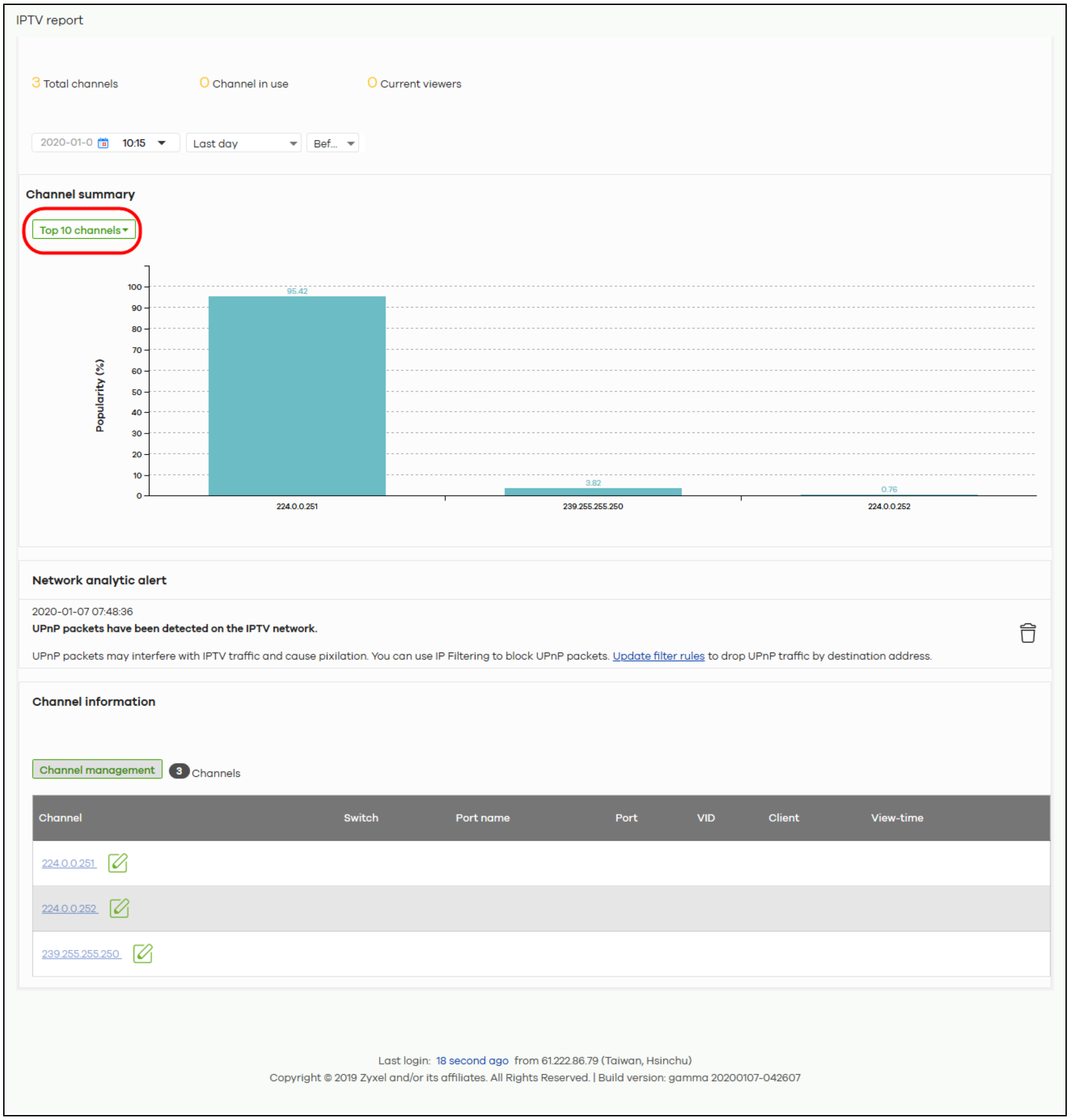


Channel management

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

3.22 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

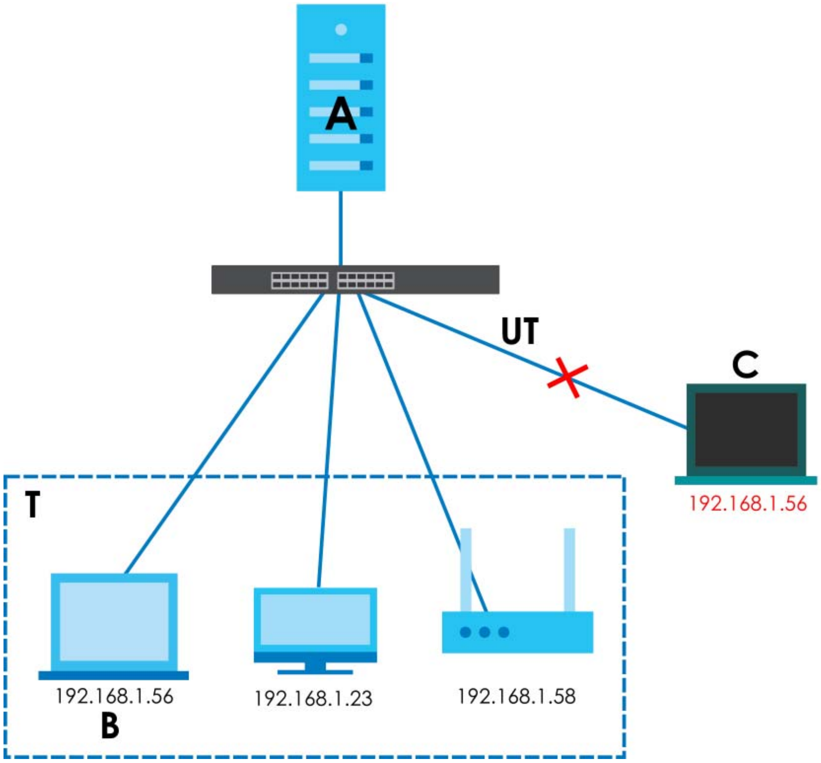
The Nebula Device only allows an authorized DHCP server on a trusted port to assign IP addresses. Unauthorized DHCP servers will not be able to assign IP addresses to network clients. When the Nebula Device receives a DHCP server packet from an authorized DHCP server, it inspects the packet and records 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.

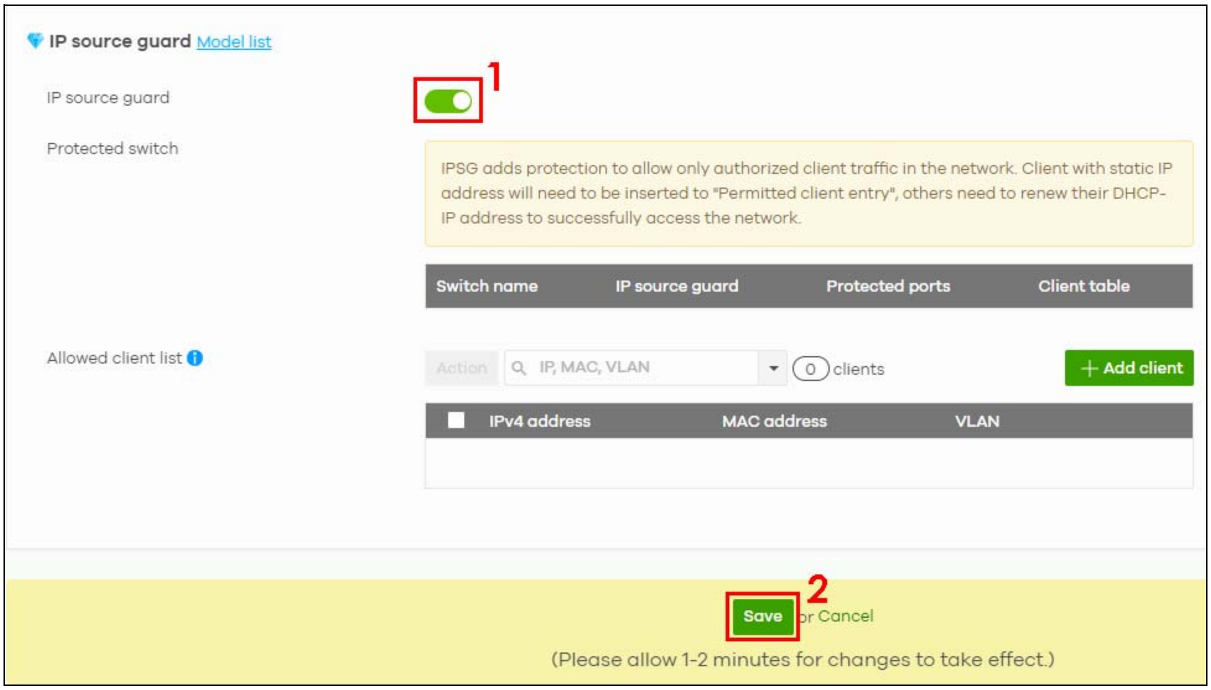
If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

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.



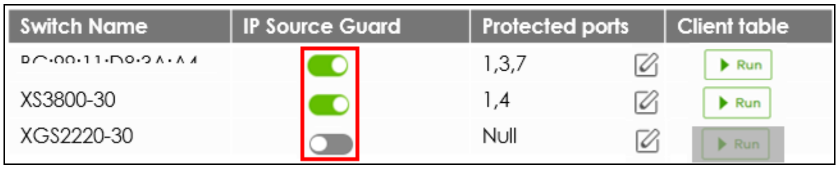
IPSG adds protection to allow only authorized client traffic in the network. Client with static IP address will need to be inserted to "Permitted client entry", others need to renew their DHCP-IP address to successfully access the network.

Switch name	IP source guard	Protected ports	Client table

□	IPv4 address	MAC address	VLAN

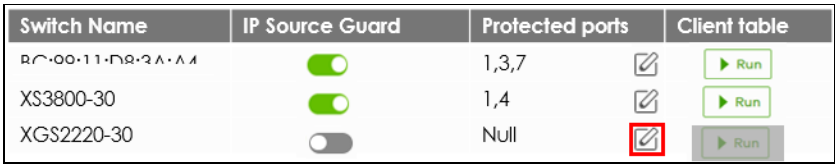
(Please allow 1-2 minutes for changes to take effect.)

2 Click the IP Source Guard switch to enable/disable **IP source guard** for the specific registered Nebula Device(s) in your site.



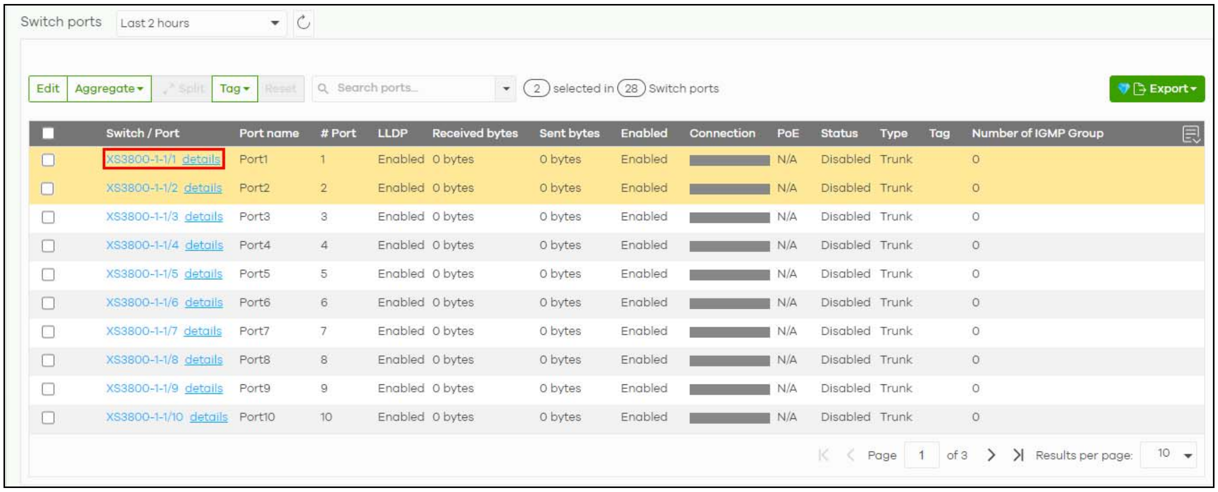
Switch Name	IP Source Guard	Protected ports		Client table
BC:99:11:D8:3A:A4	●	1,3,7	✎	▶ Run
XS3800-30	●	1,4	✎	▶ Run
XGS2220-30	○	Null	✎	▶ Run

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.

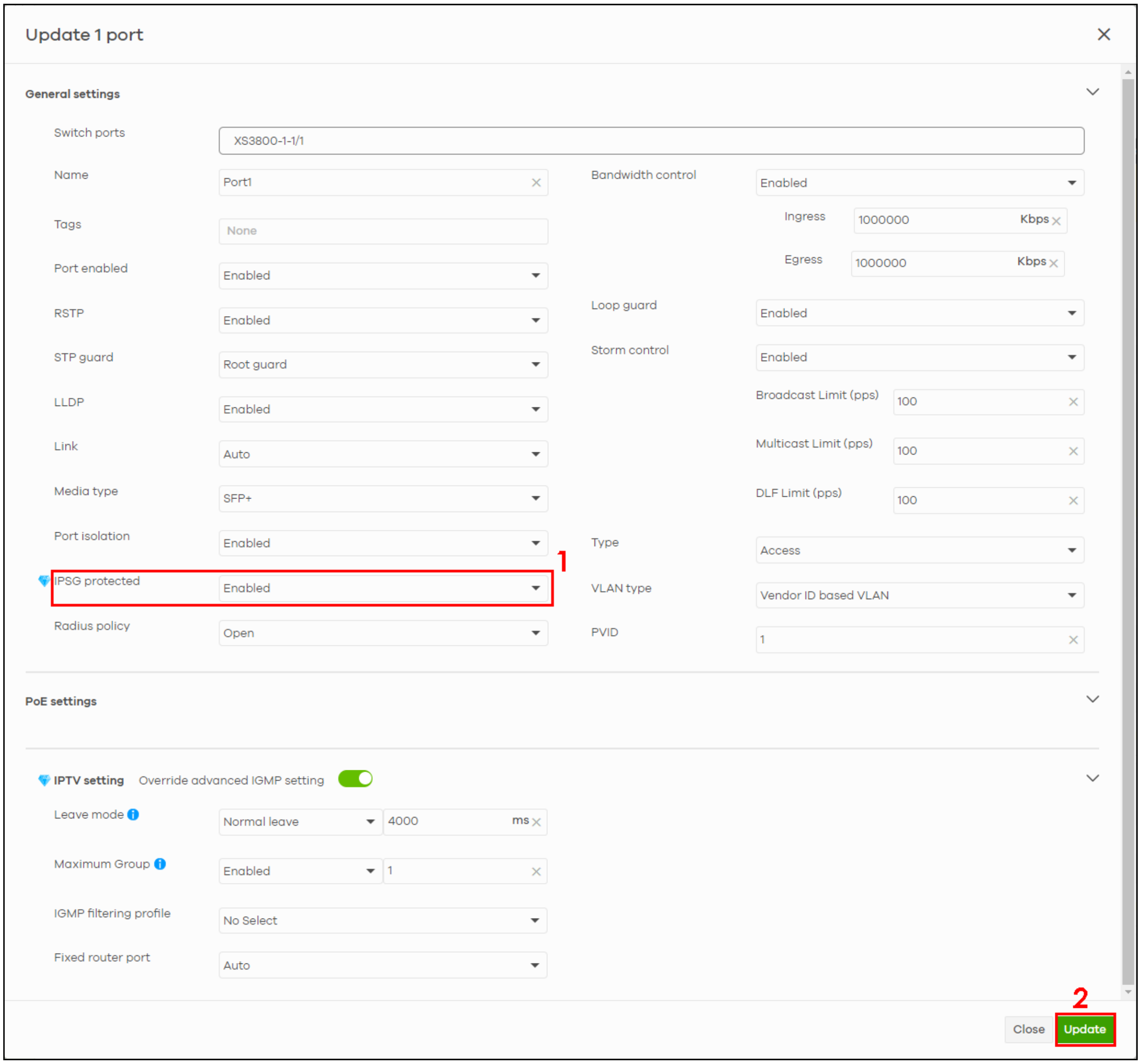


□	Switch / Port	Port name	# Port	LLDP	Received bytes	Sent bytes	Enabled	Connection	PoE	Status	Type	Tag	Number of IGMP Group
□	XS3800-1-1/1 details	Port1	1	Enabled	0 bytes	0 bytes	Enabled	▬	N/A	Disabled	Trunk		0
□	XS3800-1-1/2 details	Port2	2	Enabled	0 bytes	0 bytes	Enabled	▬	N/A	Disabled	Trunk		0
□	XS3800-1-1/3 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

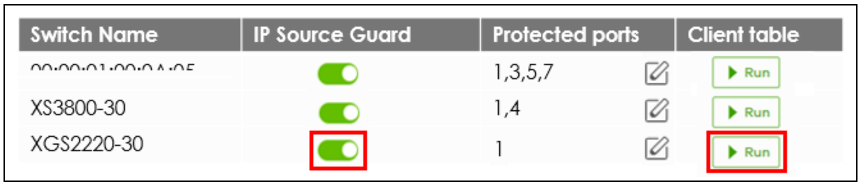
Switch ports	XS3800-1-1/1		
Name	Port1	Bandwidth control	Enabled
Tags	None	Ingress	1000000 Kbps
		Egress	1000000 Kbps
Port enabled	Enabled		
RSTP	Enabled	Loop guard	Enabled
STP guard	Root guard	Storm control	Enabled
LLDP	Enabled	Broadcast Limit (pps)	100
Link	Auto	Multicast Limit (pps)	100
Media type	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

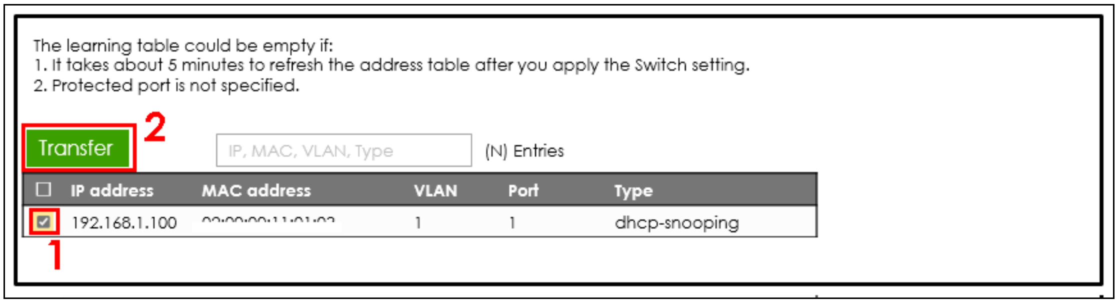
Leave mode	Normal leave	4000 ms
Maximum Group	Enabled	1
IGMP filtering profile	No Select	
Fixed router port	Auto	

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

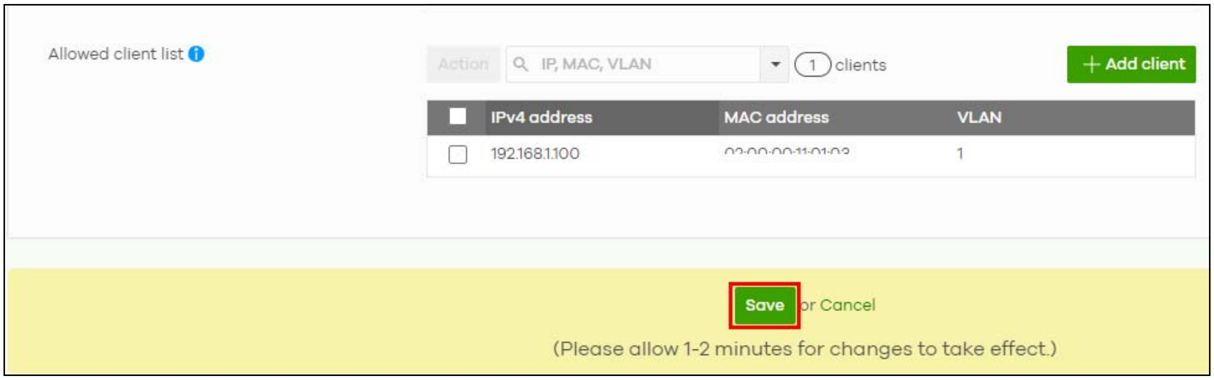
7 A merged list window appears. Click to select the port and then click **Transfer**.



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

3.23 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**.

3.24 Set Up Dynamic VLAN With RADIUS (for Nebula Switches only)

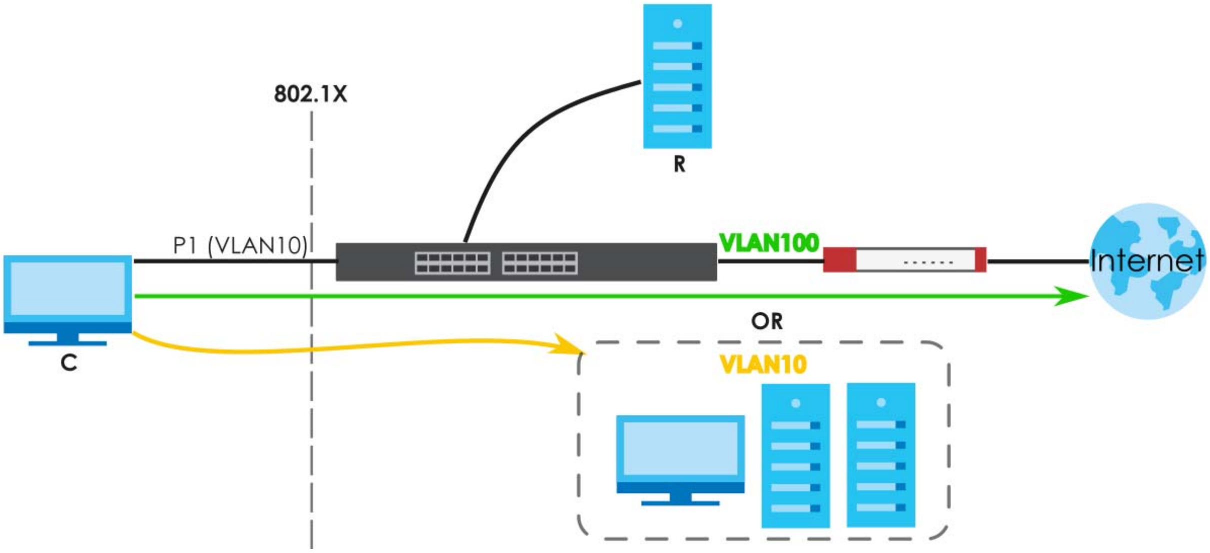
In this example, VLAN10 is configured on port 1 (P1) of the Nebula Device. The user creates the following two accounts in the RADIUS server (R):

- 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.

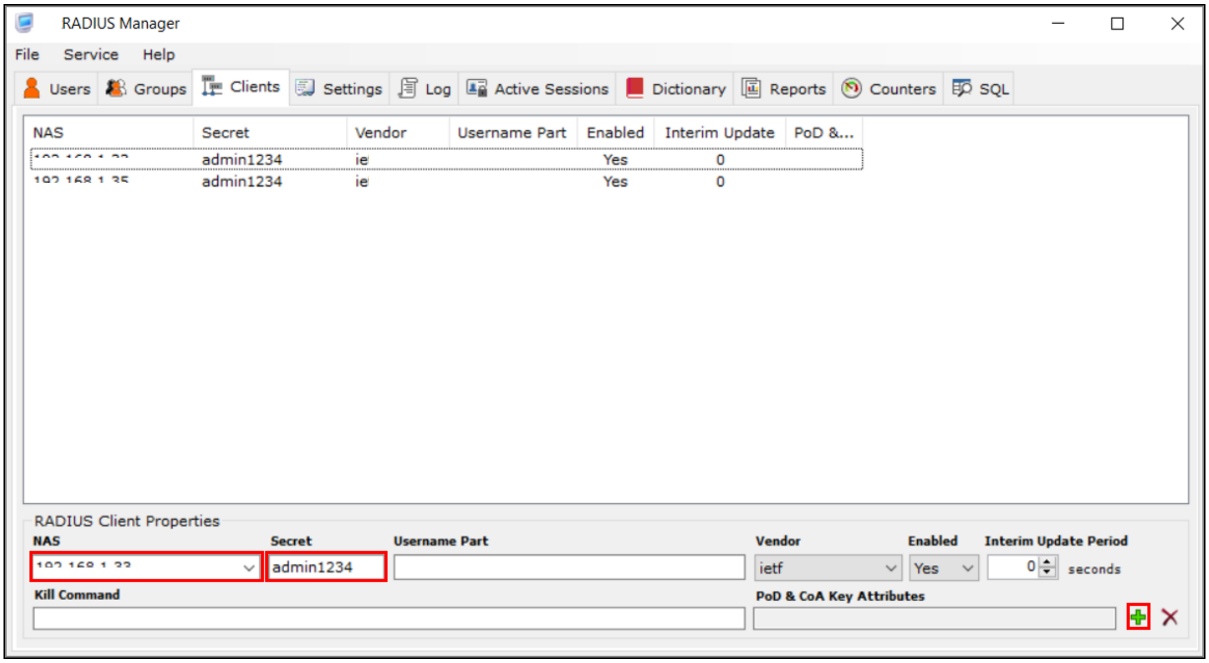
Scenario 2:
The login account passes IEEE 802.1x port authentication without dynamic VLAN assignment. Client (C) will connect to the network through VLAN10.

Figure 21 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.

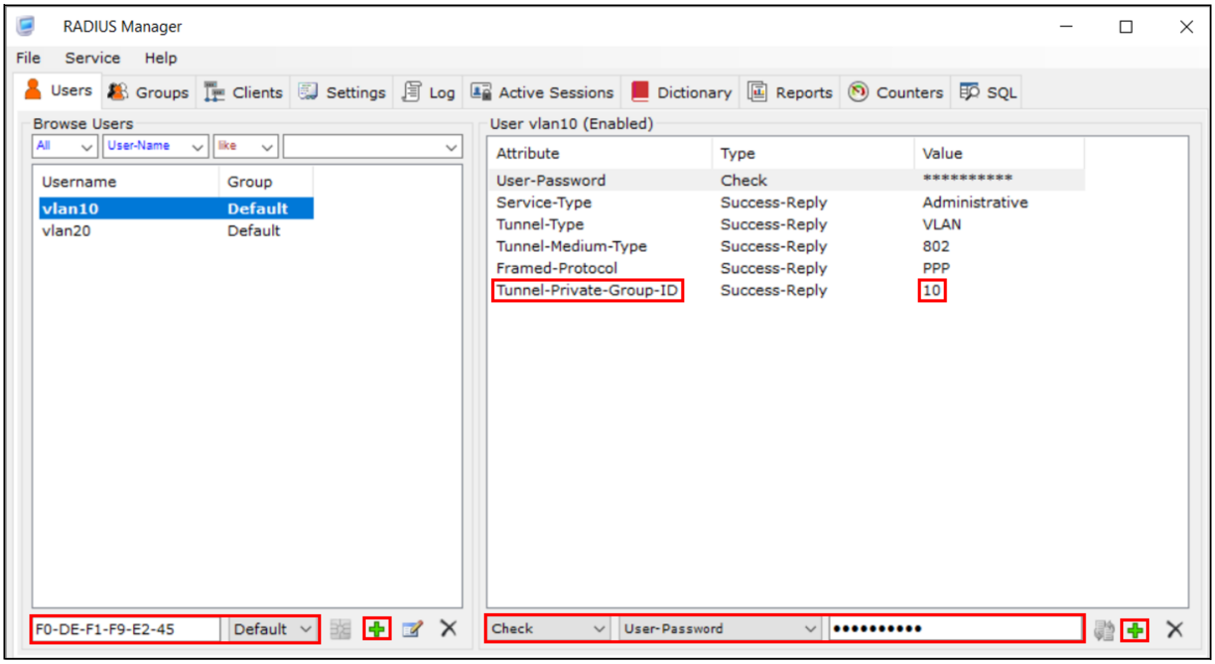

RADIUS Manager
File Service Help
Users Groups Clients Settings Log Active Sessions Dictionary Reports Counters SQL

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	

RADIUS Client Properties

NAS: 192.168.1.33
Secret: admin1234
Username Part:
Vendor: ietf
Enabled: Yes
Interim Update Period: 0 seconds
Kill Command:
PoD & CoA Key Attributes:

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.


RADIUS Manager
File Service Help
Users Groups Clients Settings Log Active Sessions Dictionary Reports Counters SQL
Browse Users
All
User-Name
like

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.

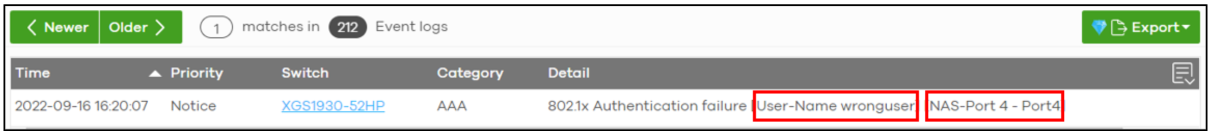
5a Select the uplink port and click **Edit**.

5b In the **Update # port** screen, select **Trunk** in **Type**.
Enter the dynamic VLAN(s) in **Allowed VLANs**. Then click **Update**.

3.25 Monitor Dynamic VLAN Using Event Logs (for Nebula Switches only)

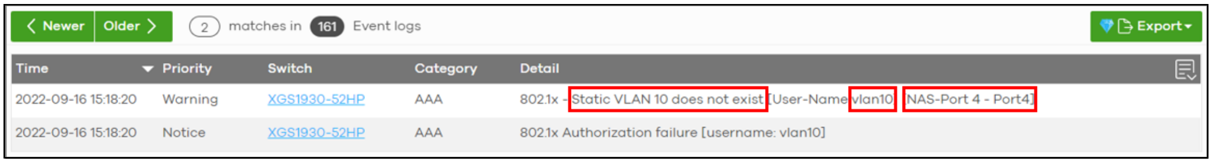
Go to **Site-wide** > **Monitor** > **Switches** > **Event log** to monitor dynamic VLANs. The following are example dynamic VLAN-related event logs:

- User submits an incorrect 802.1X credential (wrong user name on the client port ‘Port4’).



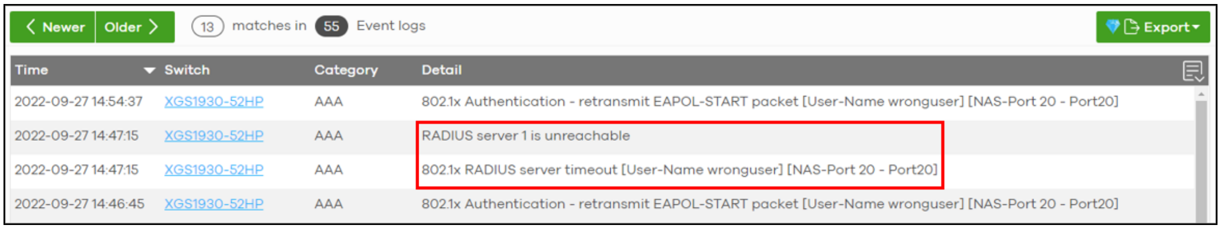
Time	Priority	Switch	Category	Detail
2022-09-16 16:20:07	Notice	XGS1930-52HP	AAA	802.1x Authentication failure [User-Name wronguser] [NAS-Port 4 - Port4]

- 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’).



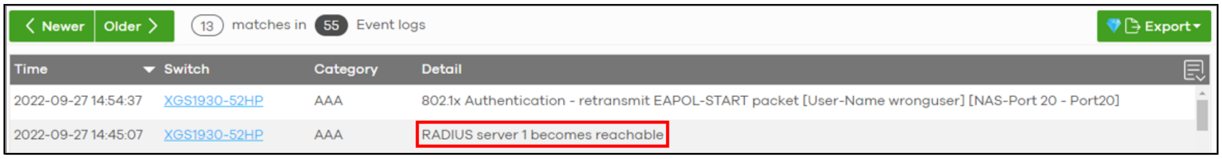
Time	Priority	Switch	Category	Detail
2022-09-16 15:18:20	Warning	XGS1930-52HP	AAA	802.1x - Static VLAN 10 does not exist [User-Name vlan10] [NAS-Port 4 - Port4]
2022-09-16 15:18:20	Notice	XGS1930-52HP	AAA	802.1x Authorization failure [username: vlan10]

- 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

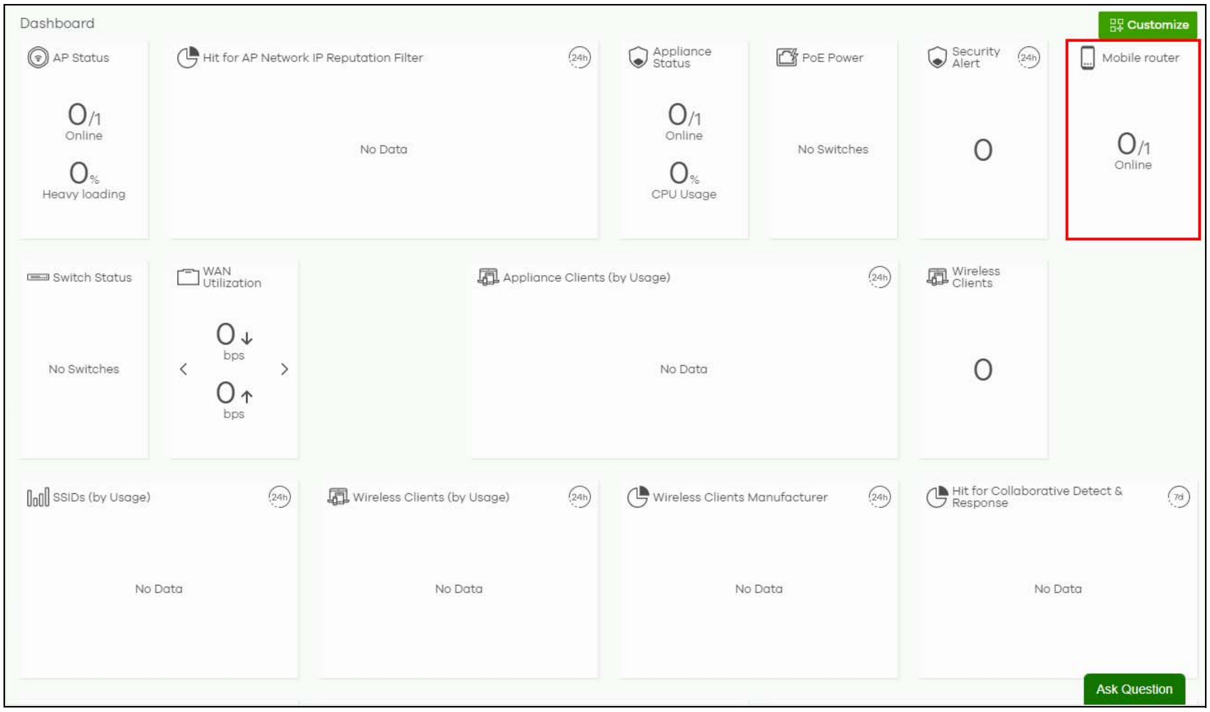
3.26 Register a Nebula Device (mobile router) in Nebula

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 46 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.

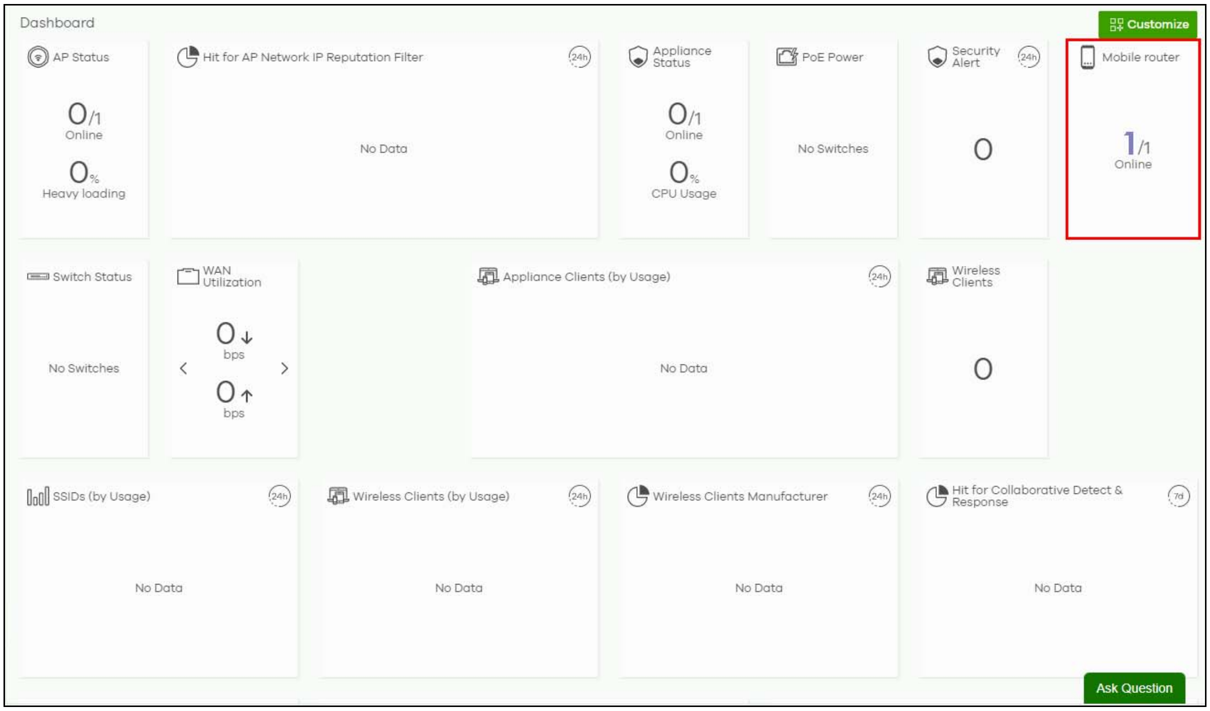


Insert the SIM Card

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.

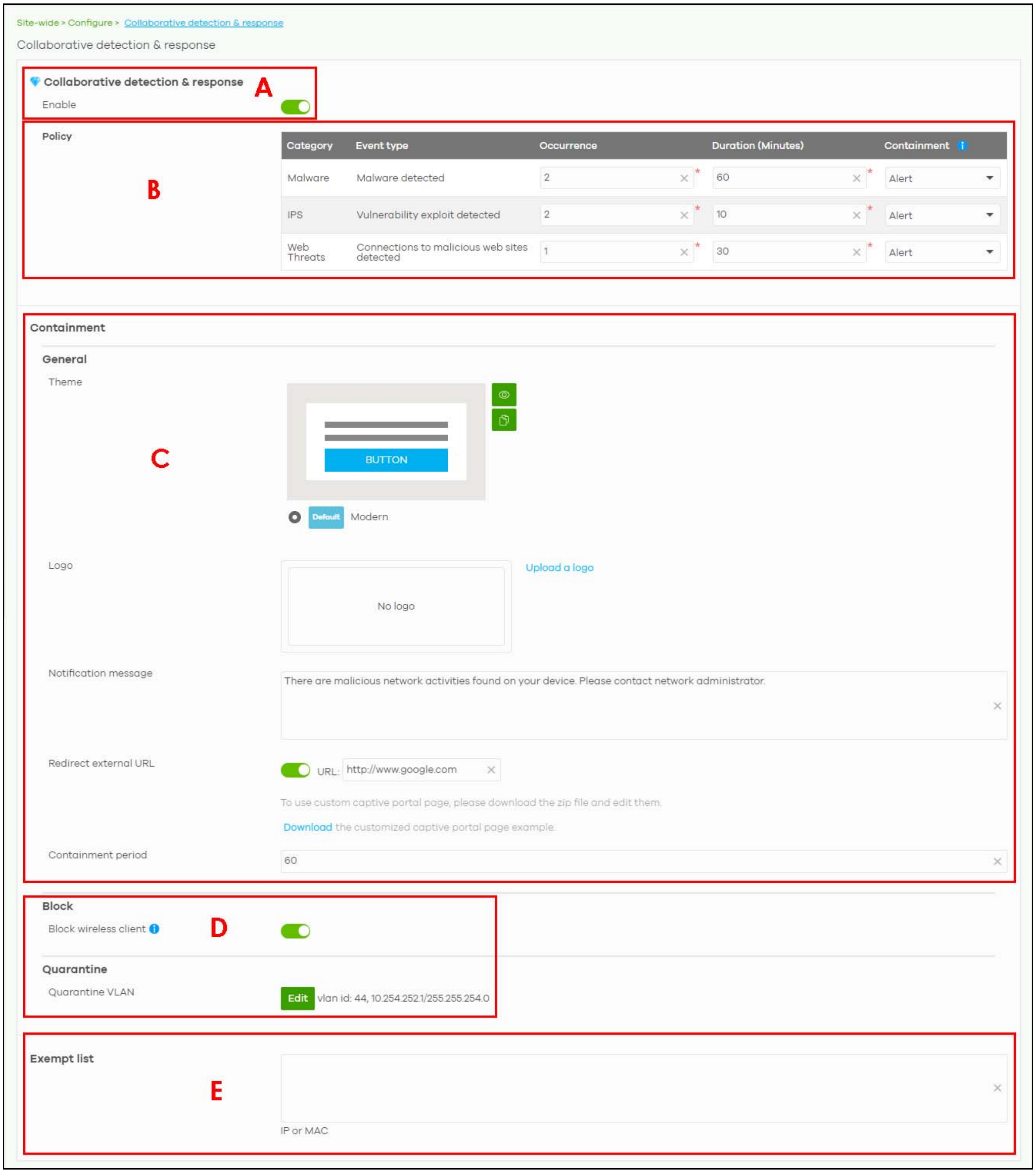
Note: Its login password and settings are then overwritten with what you have configured in the Nebula web portal. To access the Web Configurator when the Nebula Device is in Cloud mode, use the Nebula Local credentials password to login. The **Local credentials**: **Password** can be found in **Site-wide** > **Configure** > **Site settings** > **Device configuration**.

3.27 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 232 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 39 on page 226 for more information.

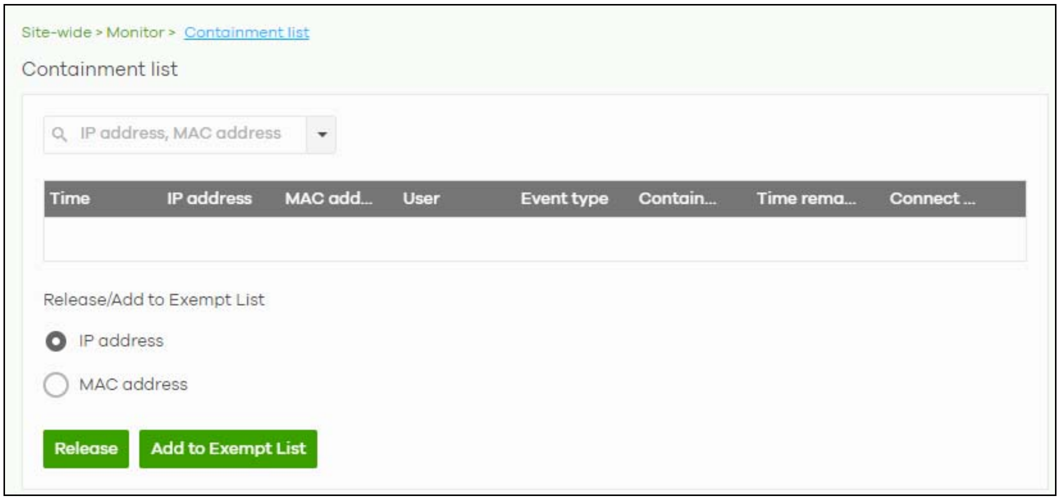
3 Configure the containment alert (**Theme**), customized pop-up (**Notification message**) for the client blocked by CDR, and the (**Containment Period**) time interval (refer to the **C** part in the above figure).

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.



Time	IP address	MAC add...	User	Event type	Contain...	Time rema...	Connect ...

3.28 Deploy With Nebula Native Mode (for Security Firewalls in Nebula)

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).

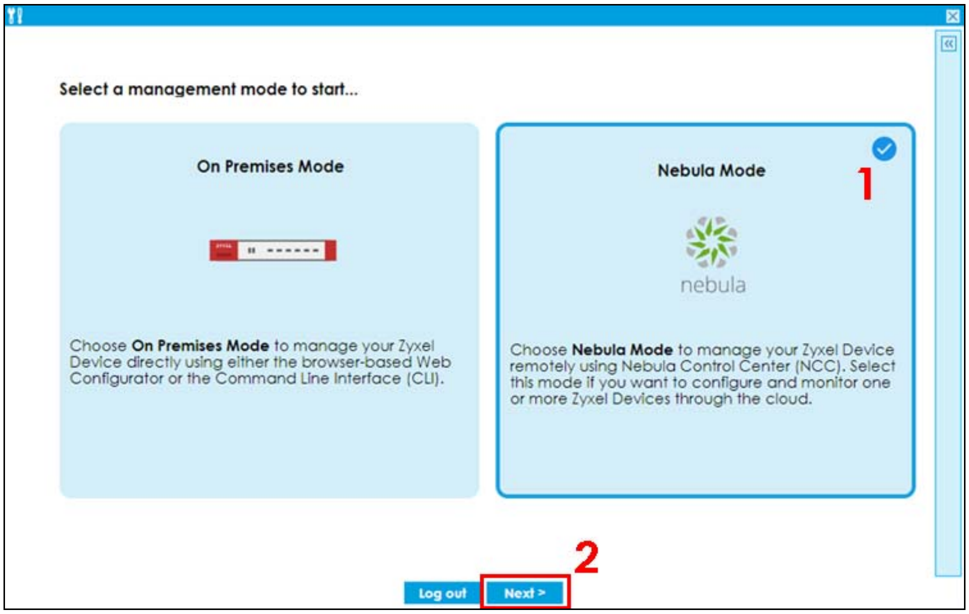
Note: Apply the factory-default settings on the SF before switching to cloud mode. Only the following two settings can be changed after resetting:

- 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...

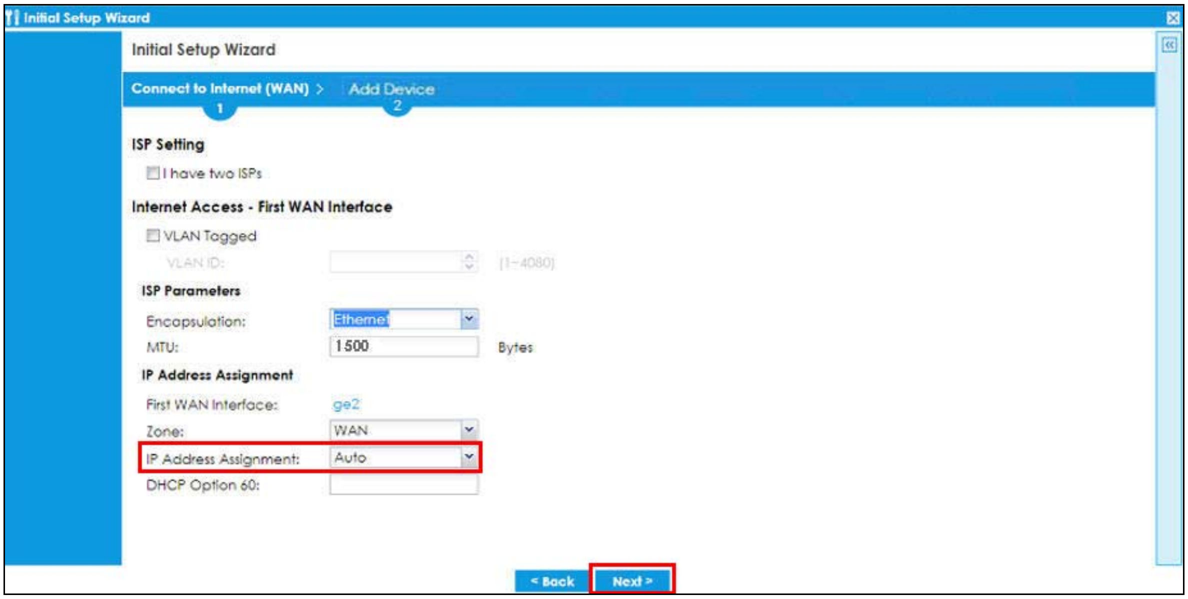
On Premises Mode

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**.



ISP Setting

☐ I have two ISPs

Internet Access - First WAN Interface

☐ VLAN Tagged

VLAN ID: (1~4080)

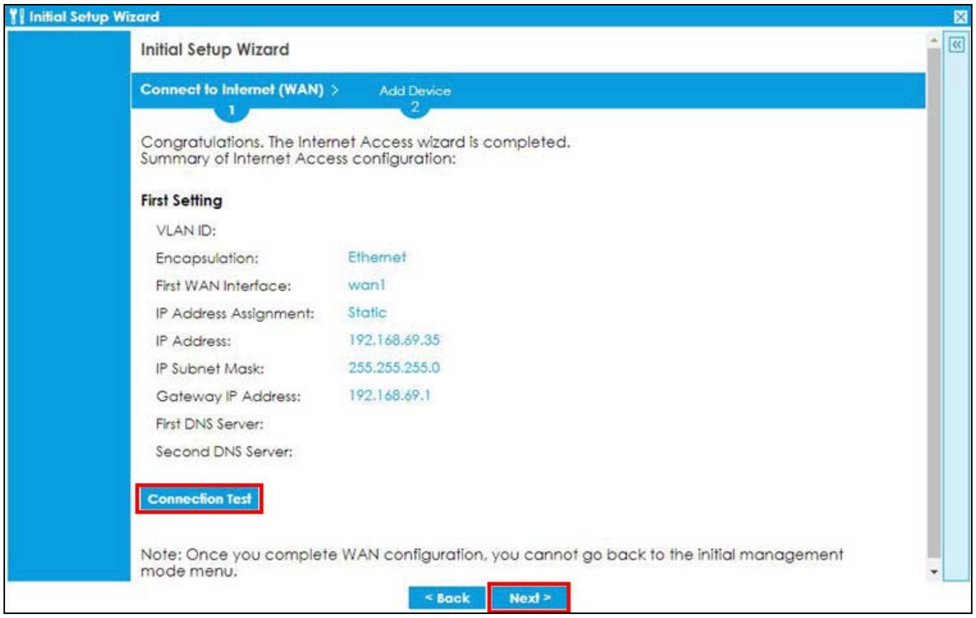
ISP Parameters

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**.



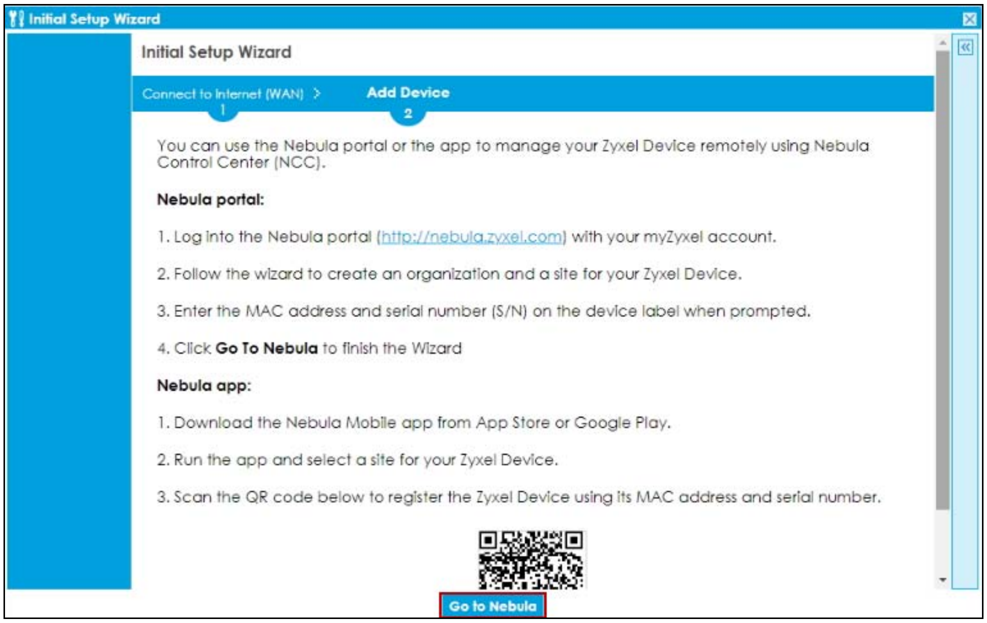
Congratulations. The Internet Access wizard is completed.
Summary of Internet Access configuration:

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:

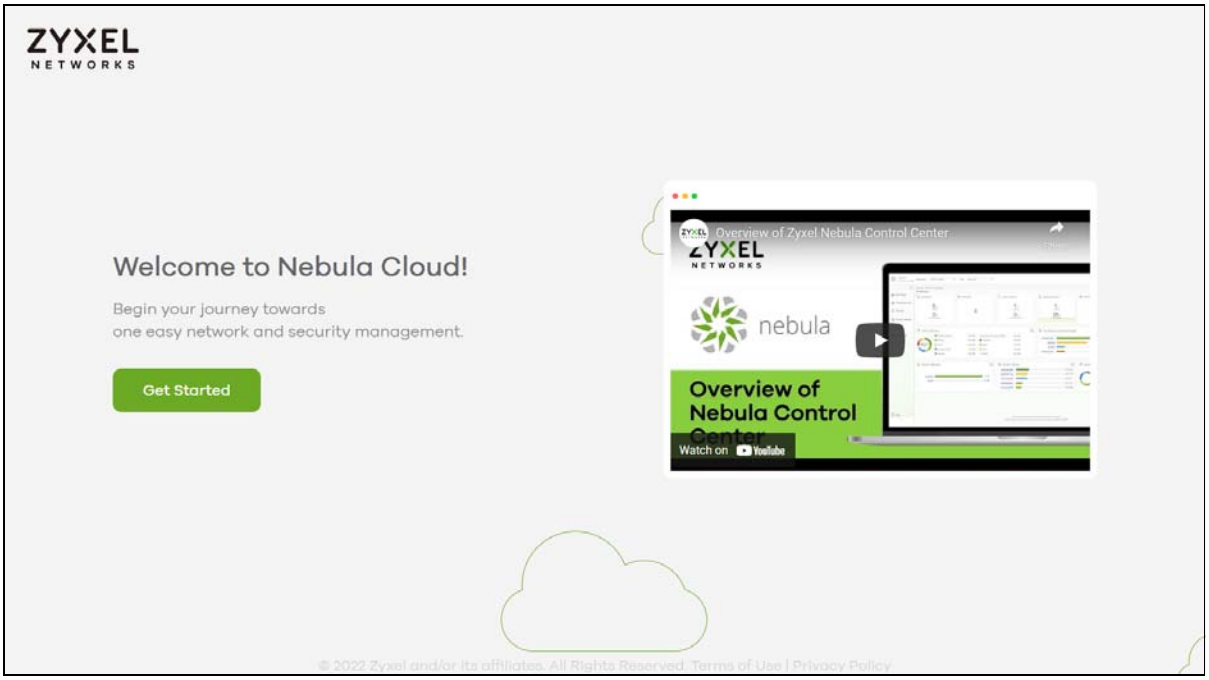
1. Download the Nebula Mobile app from App Store or Google Play.

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**.


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

Welcome to Nebula Cloud!

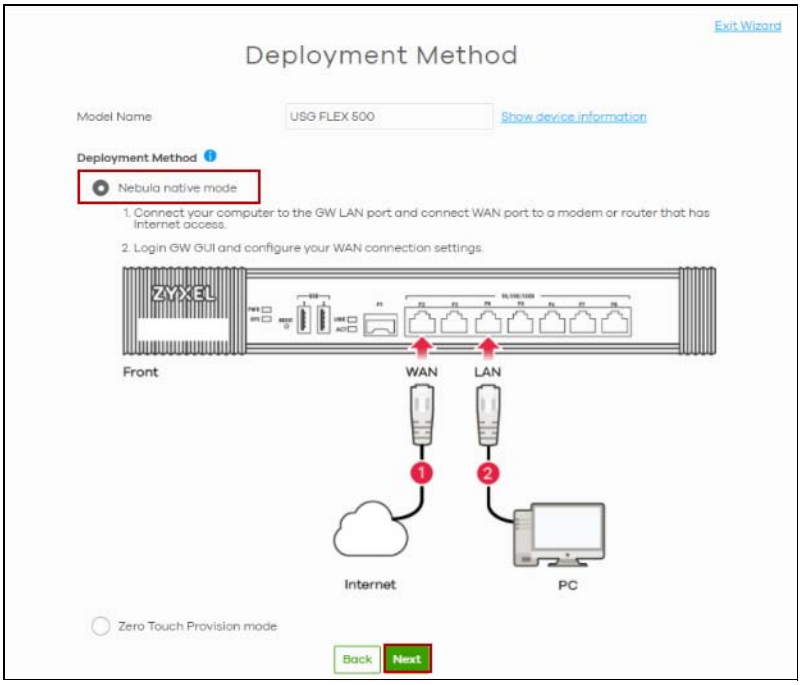
Begin your journey towards
one easy network and security management.

© 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 46 for more information on using the wizard.

Note: Make sure to select **Nebula native mode** as the **Deployment Method** in the Setup Wizard.

Nebula native mode may be un-clickable (grayed-out) if your Nebula Device do NOT support it. Select **Zero Touch Provision mode** instead (see Section 2.1.7 on page 51 for more information on the ZTP deployment method).



Exit Wizard

Deployment Method

Model Name: USG FLEX 500 — Show device information

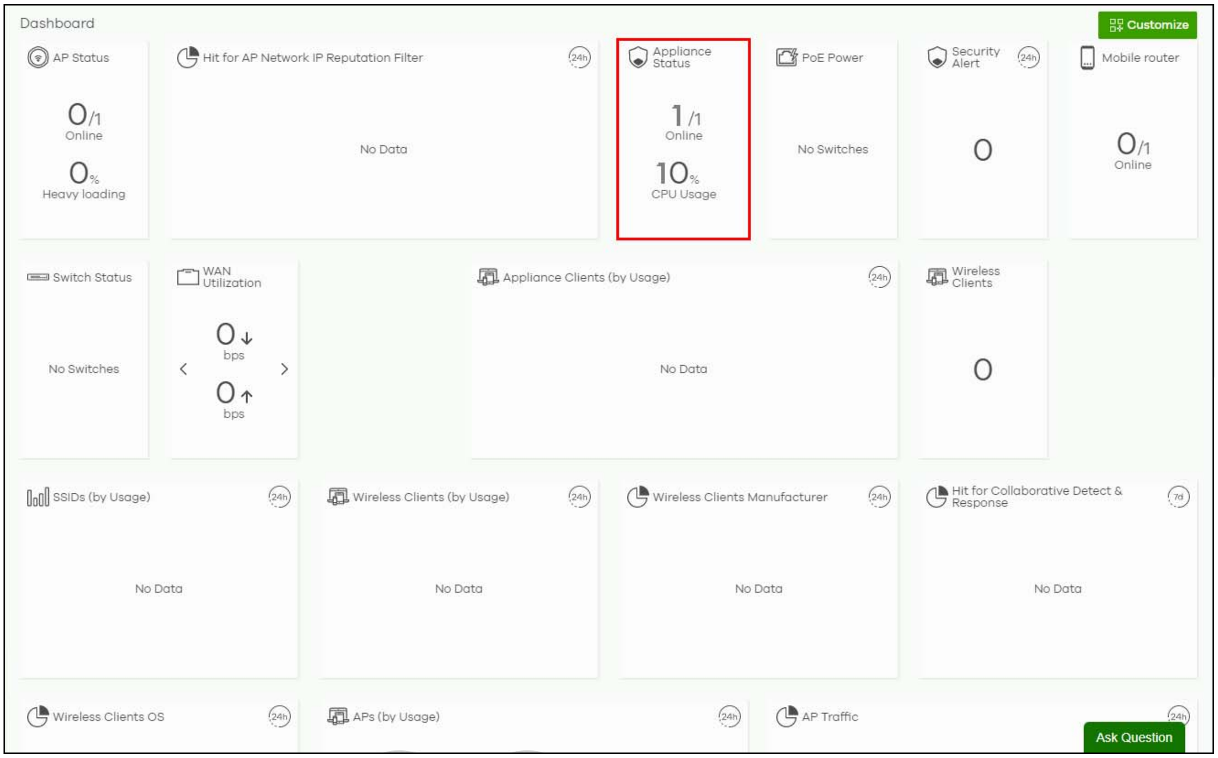
Deployment Method

● 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

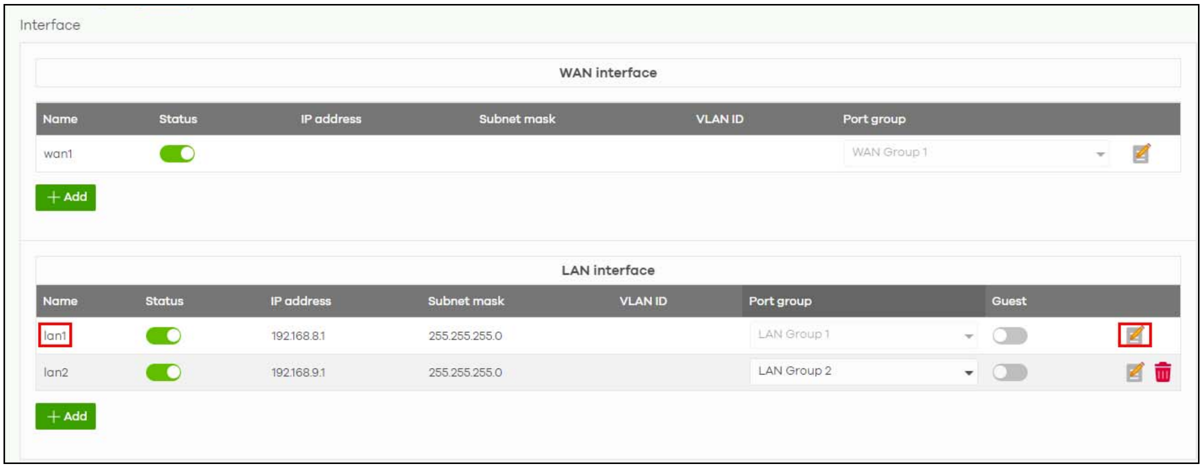
3 After configuring the Setup Wizard, close the Nebula Control Center welcome message to go to the Nebula portal dashboard. **1/1 Online** will show on **Appliance Status**. This means that one SF is registered in Nebula and is online.



3.29 Configure DHCP Domain Name (for Security Firewalls in Nebula)

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 **Firewall** > **Configure** > **Interface**. Click the Edit icon for the **lan1** interface to open the **Site-wide** > **Configure** > **Firewall** > **Interface** > **LAN interface configuration** screen.


Interface

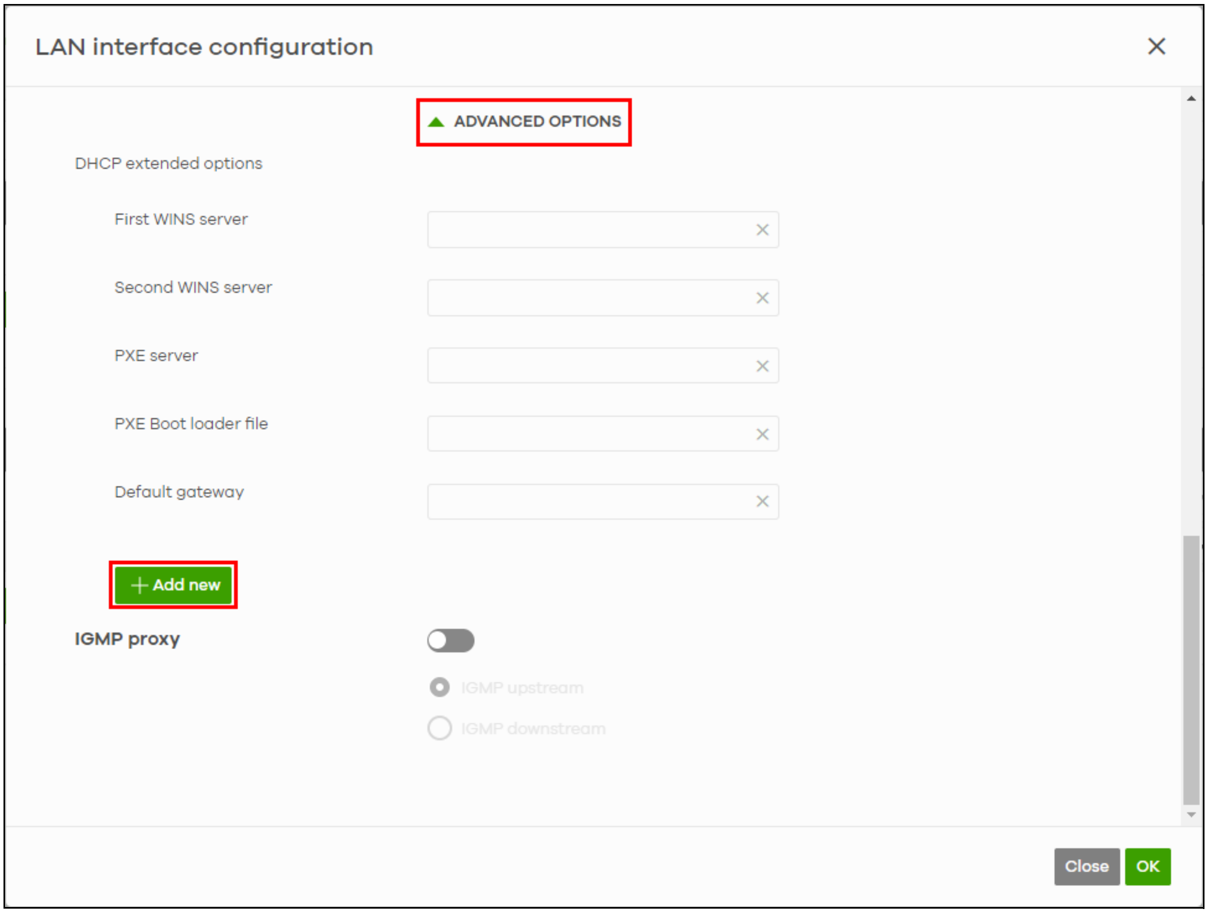
WAN interface

Name	Status	IP address	Subnet mask	VLAN ID	Port group
wan1					WAN Group 1

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	

2 Click **ADVANCED OPTIONS**. Then click **+Add new** to open the **Site-wide** > **Configure** > **Firewall** > **Interface** > **LAN interface configuration**: **DHCP option** screen.

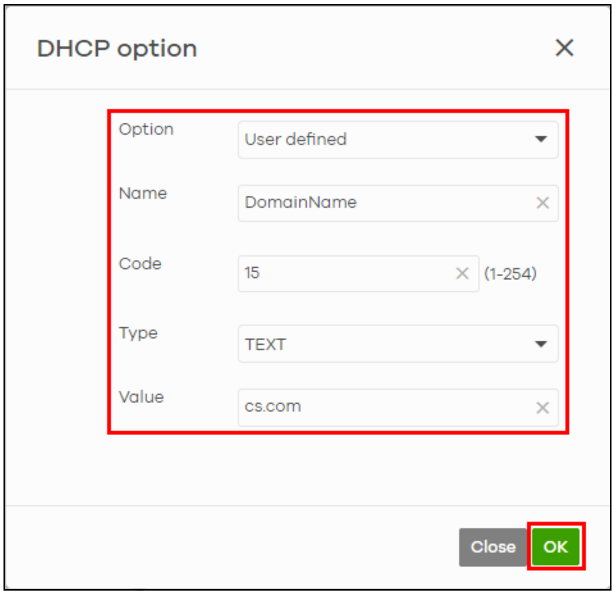

LAN interface configuration

▲ ADVANCED OPTIONS

DHCP extended options

First WINS server	
Second WINS server	
PXE server	
PXE Boot loader file	
Default gateway	

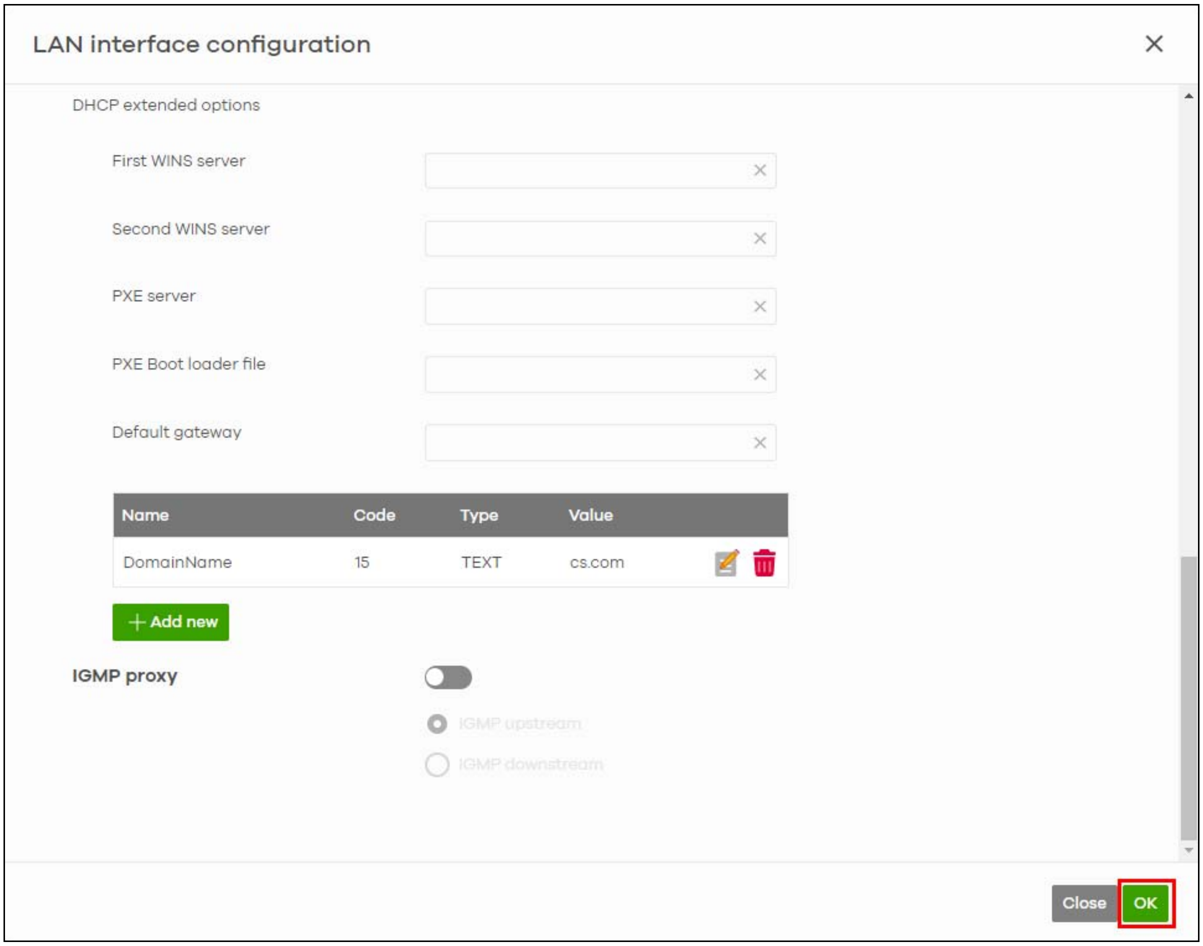
3 Select **User defined** as the DHCP **Option** that you want to add in the DHCP packets sent through the LAN interface. Select **TEXT** for the **Type**, enter a descriptive **Name** to identify and the **Code** number of the selected DHCP option (**15**, for setting the Domain Name). See *https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.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**.



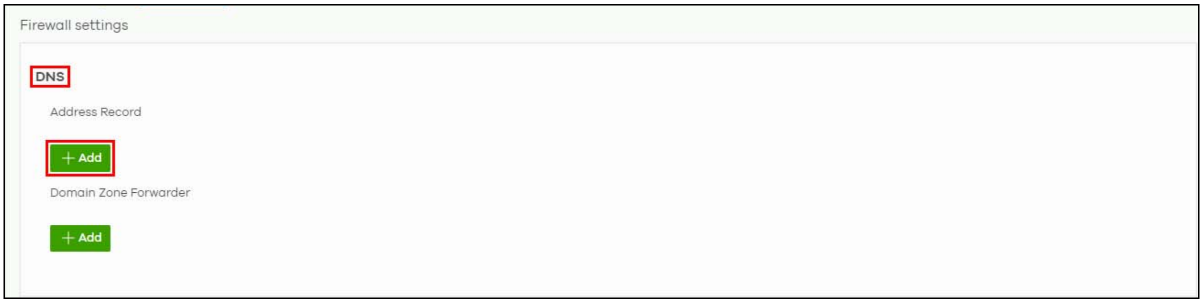
LAN interface configuration

DHCP extended options

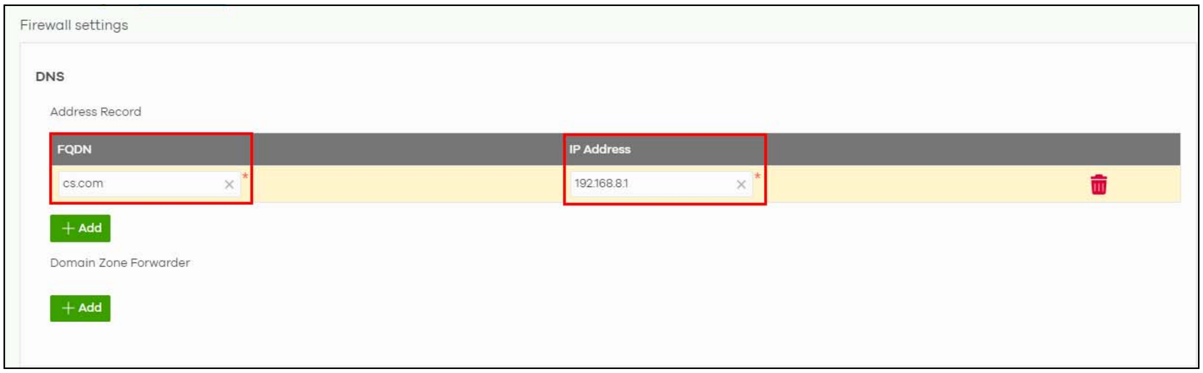
First WINS server	
Second WINS server	
PXE server	
PXE Boot loader file	
Default gateway	

Name	Code	Type	Value
DomainName	15	TEXT	cs.com

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.



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.

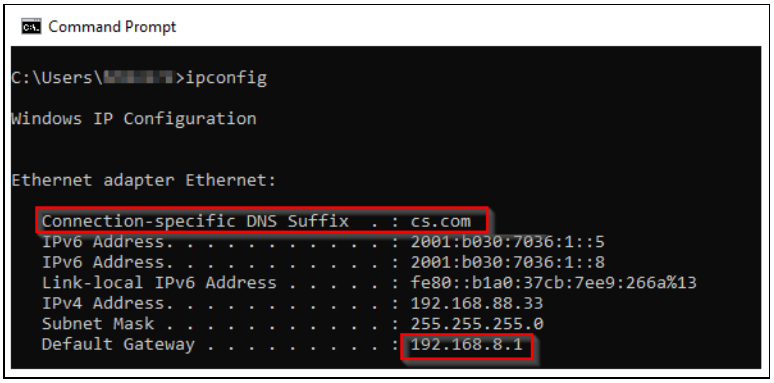


FQDN	IP Address
cs.com	192.168.8.1

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
```

PART II

Manage by Site Deployment

CHAPTER 4 Site-wide

4.1 Dashboard

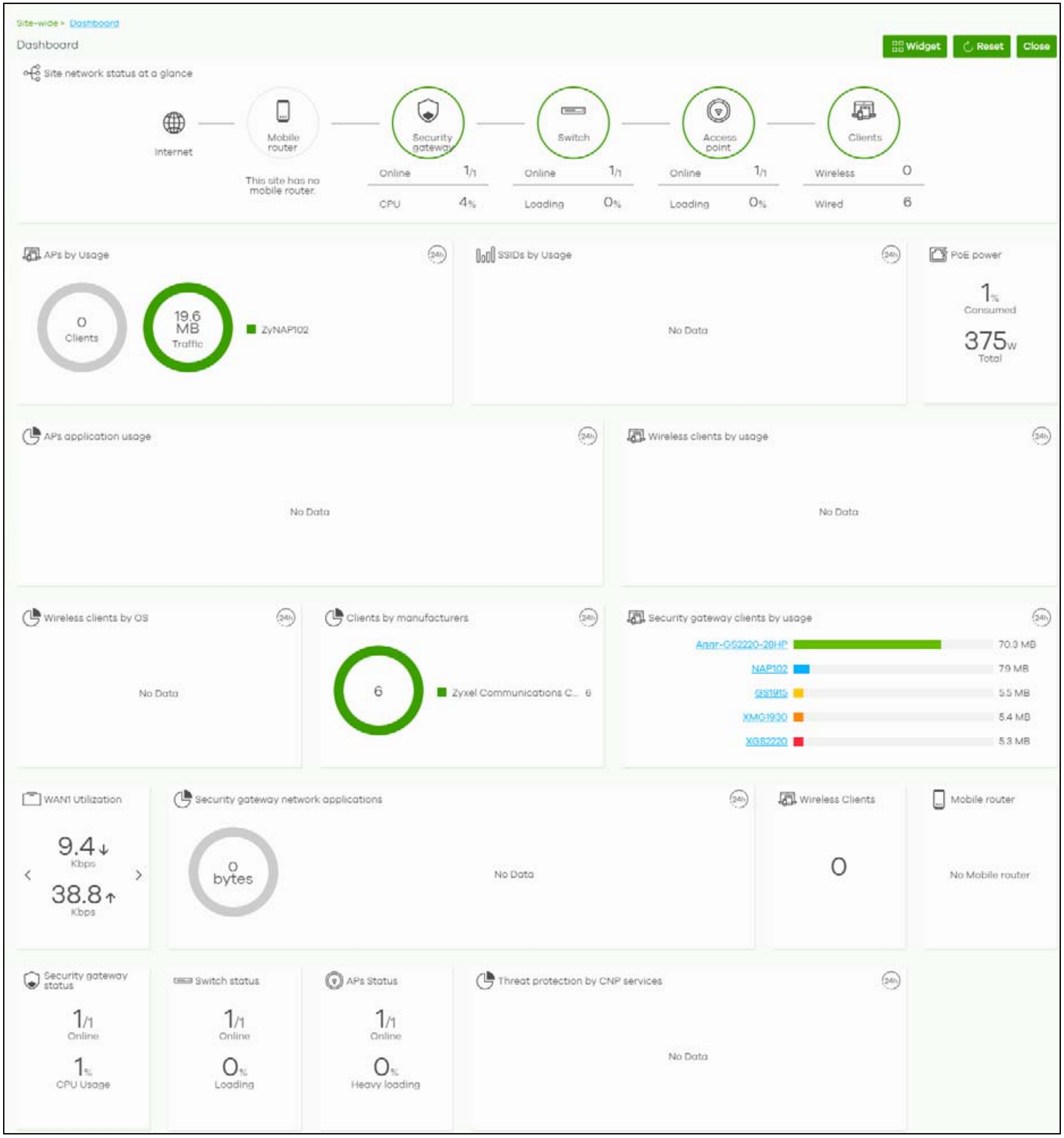
If a site is created and selected, the **Dashboard** is always the first menu you see when you log into the NCC. You can also click **Site-wide** > **Dashboard** to access this screen.

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 22 Site-wide > Dashboard



The following table describes the labels in this screen.

Table 12 Site-wide > Dashboard

LABEL	DESCRIPTION
APs 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.
Wireless clients	This shows the number of WiFi clients currently connected to the managed access points.
Switch 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.

Table 12 Site-wide > Dashboard (continued)

LABEL	DESCRIPTION
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 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.
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.
Security alert	This shows the total number of the latest alerts sent to the administrator in the last 24 hours.
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.
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.
Wireless 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.
Wireless 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.
Wireless 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 which use this operating system.
APs 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.
APs application usage	This shows the usage statistic of the top ten applications used in the site in the past 24 hours.
APs 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.

4.2 Topology

Use this screen to view the links between Nebula Devices in the site. Click **Site-wide** > **Topology** to access this screen.

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).

Move the pointer over a node to view detailed Nebula Device information, such as its name, model number, number of connected clients, and MAC address. Click **Reboot** to restart the Nebula Device.

Move the pointer over a link to view link details, such as type (Ethernet or wireless mesh), speed, and data usage from the past 24 hours. If the link is supplying power to a node using Power over Ethernet (PoE), you can click **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.

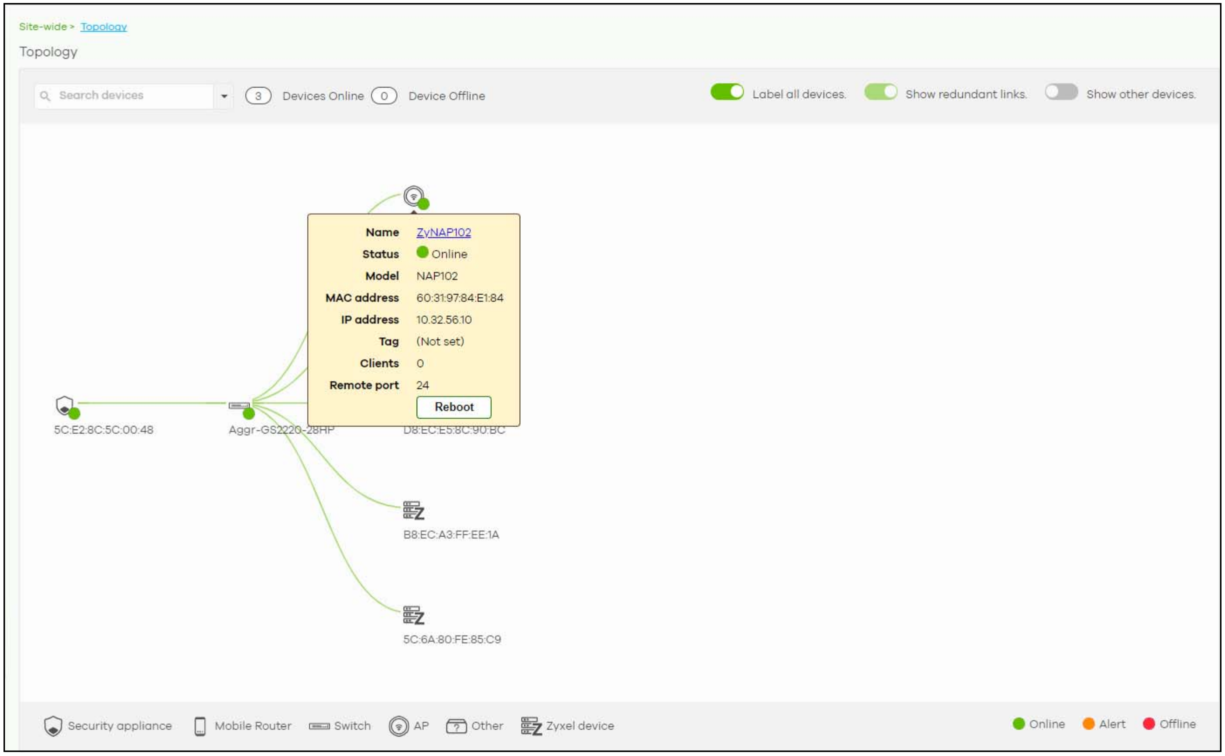
Enable **Label all devices** to show Nebula Device information, such as MAC address in the network topology diagram.

Enable **Show redundant links** to display the secondary connection between two nodes, if any.

Enable **Show other devices** to also display the Nebula Devices that are connected to your network but cannot be identified by the NCC. This on/off switch is configurable only when there is a non-Nebula Device installed in the network and detected by the NCC through LLDP packets.

Zyxel device is a device manufactured by Zyxel but not registered at the NCC or unable to work in Nebula cloud management mode.

Figure 23 Site-wide > Topology



Site-wide > Topology

Topology

Search devices ▾ (3) Devices Online (0) Device Offline

Label all devices. Show redundant links. Show other devices.

Name	ZyNAP102
Status	● Online
Model	NAP102
MAC address	60:31:97:84:E1:84
IP address	10.32.56.10
Tag	(Not set)
Clients	0
Remote port	24

Reboot

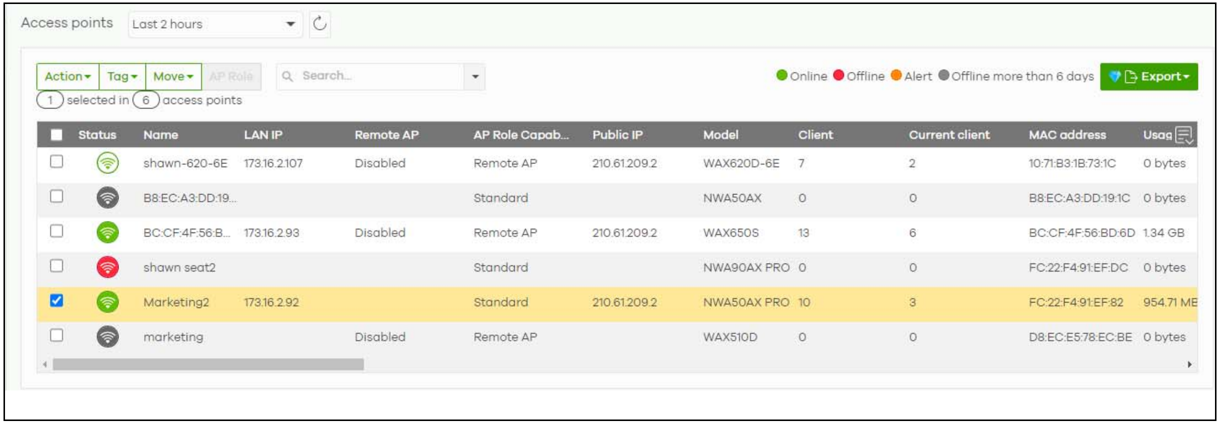
4.3 Devices

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 24 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 13 Site-wide > Devices > Access points

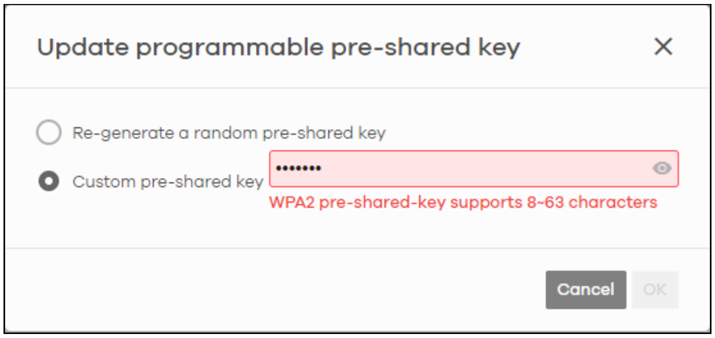
LABEL	DESCRIPTION
Access points	Select to view device information and connection status in the past two hours, day, week or month.
↻	Click this button to reload the data-related frames on this page.
Action	Perform an action on the selected Nebula Devices.
Reboot	Select this to restart the Nebula Device.
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 Cancel OK Note: **Programmable SSID** must be enabled in **Site-wide** > **Configure** > **WiFi SSID**.

Table 13 Site-wide > Devices > Access points (continued)

LABEL	DESCRIPTION
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. • 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 full duplex mode or when the Nebula Device is in a **Limited Power mode**.
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.

Table 13 Site-wide > Devices > Access points (continued)

LABEL	DESCRIPTION
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**).
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 14 on page 161 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 235.
Uplink	This shows whether the Nebula Device is connected to the gateway through a wired Ethernet connection or WiFi connection.

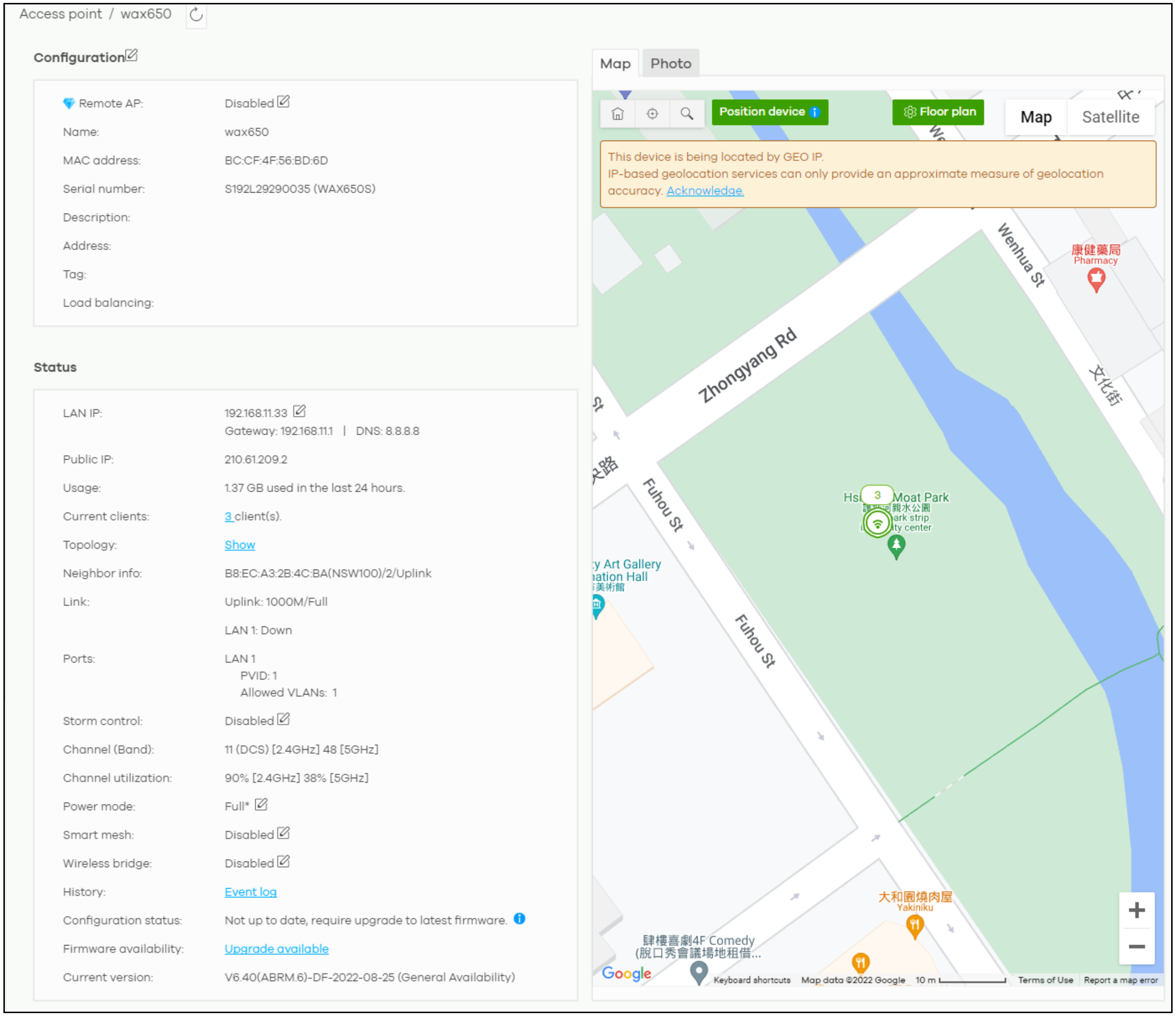
Table 13 Site-wide > Devices > Access points (continued)

LABEL	DESCRIPTION
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.
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 25 Site-wide > Devices > Access points: Details Part 1



Access point / wax650

Configuration

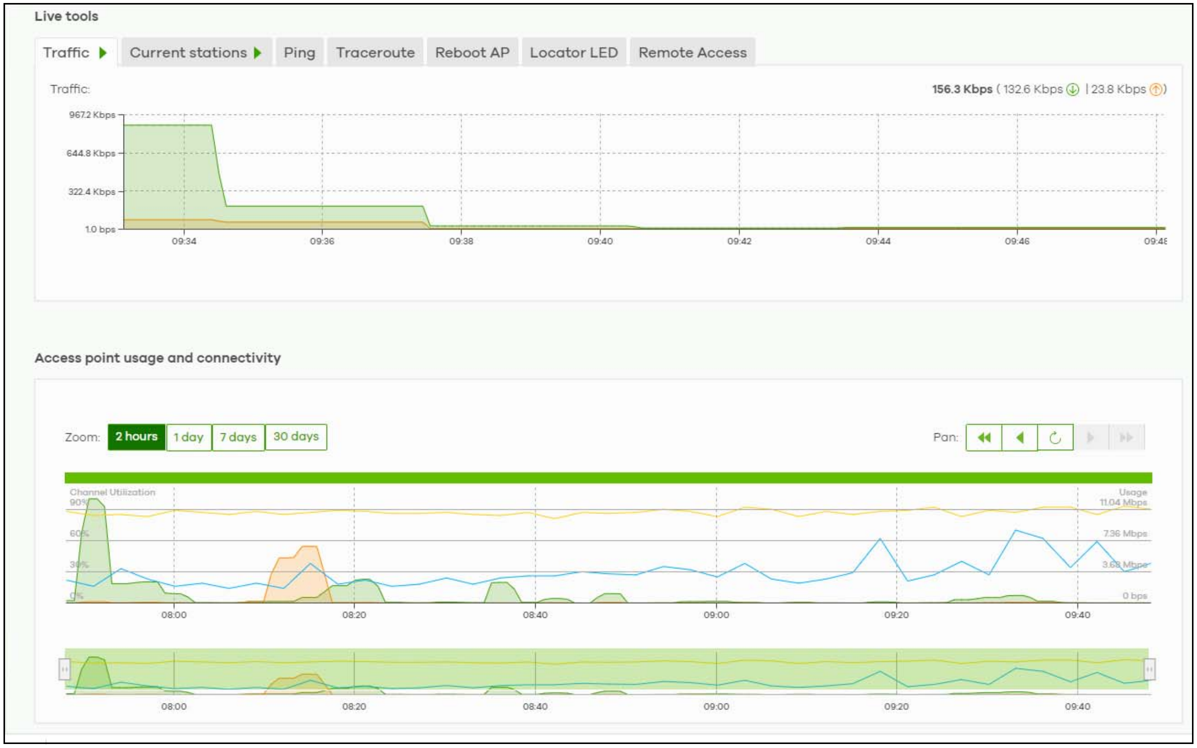
Remote AP:	Disabled
Name:	wax650
MAC address:	BC:CF:4F:56:BD:6D
Serial number:	S192L29290035 (WAX650S)
Description:	
Address:	
Tag:	
Load balancing:	

Status

LAN IP:	192.168.11.33 Gateway: 192.168.11.1 | DNS: 8.8.8.8
Public IP:	210.61.209.2
Usage:	1.37 GB used in the last 24 hours.
Current clients:	3 client(s).
Topology:	Show
Neighbor info:	B8:EC:A3:2B:4C:BA(NSW100)/2/Uplink
Link:	Uplink: 1000M/Full LAN 1: Down
Ports:	LAN 1 PVID: 1 Allowed VLANs: 1
Storm control:	Disabled
Channel (Band):	11 (DCS) [2.4GHz] 48 [5GHz]
Channel utilization:	90% [2.4GHz] 38% [5GHz]
Power mode:	Full*
Smart mesh:	Disabled
Wireless bridge:	Disabled
History:	Event log
Configuration status:	Not up to date, require upgrade to latest firmware.
Firmware availability:	Upgrade available
Current version:	V6.40(ABRM.6)-DF-2022-08-25 (General Availability)

This device is being located by GEO IP.
IP-based geolocation services can only provide an approximate measure of geolocation accuracy. Acknowledge.

Figure 26 Site-wide > Devices > Access points: Details Part 2



The following table describes the labels in this screen.

Table 14 Site-wide > Devices > Access points: Details

LABEL	DESCRIPTION
↻	Click this button to reload the data-related frames on this page.
Configuration	
Click the edit configuration icon to change the Nebula Device name, description, tags, load balancing, and address. You can also move the Nebula Device to another site or remove.	

Table 14 Site-wide > Devices > Access points: Details (continued)

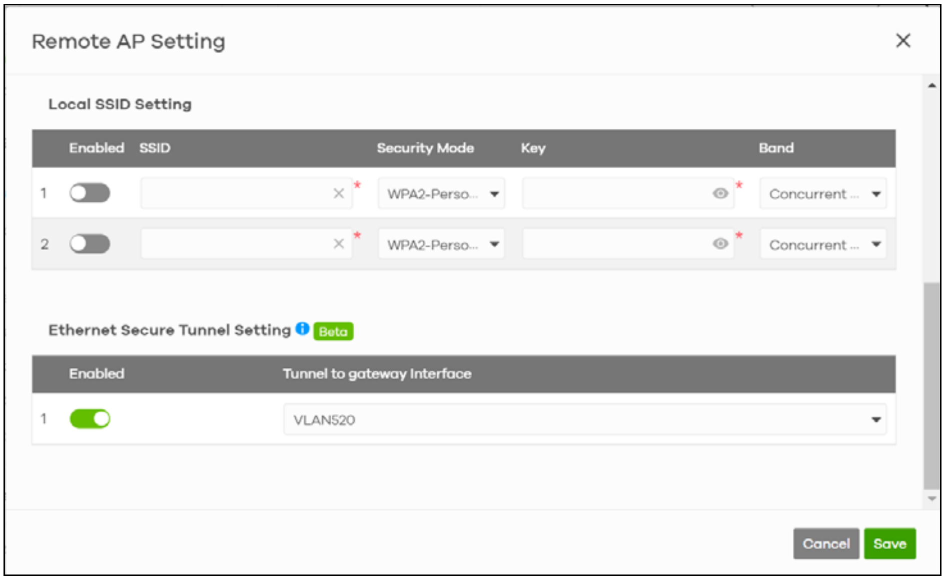
LABEL	DESCRIPTION
Remote AP	Click this to enable or disable the **Remote AP** feature. **Remote AP** enables the site's Security Appliance to connect to the Nebula Device through a secure VPN tunnel. This allows you to set up VPN-enabled WiFi Nebula Devices in remote locations, such as in a branch office 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 5.3.1 on page 247 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.
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.
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.
Status	

Table 14   Site-wide > Devices > Access points: Details (continued)

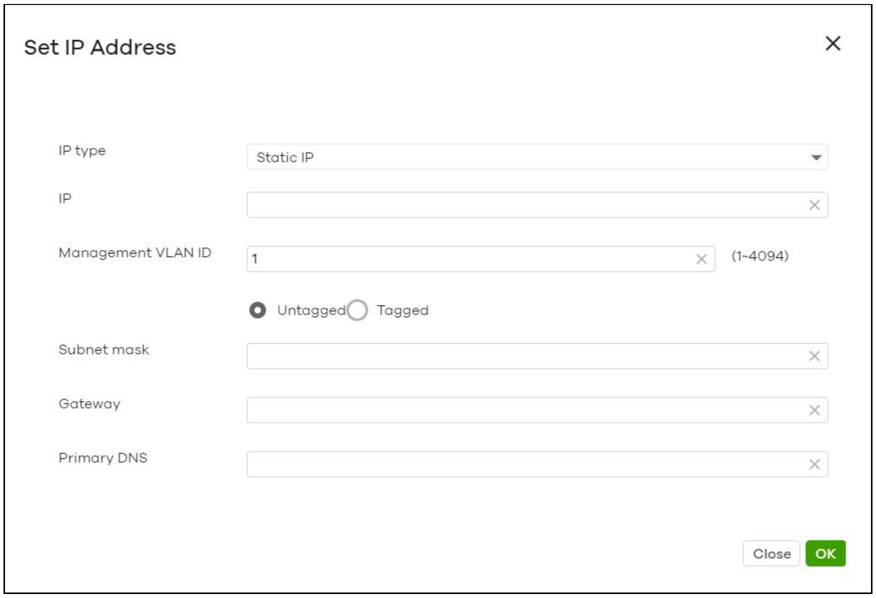
LABEL	DESCRIPTION
LAN IP	This shows the local (LAN) IP address of the Nebula Device. It also shows the IP addresses of the gateway and DNS server. Click the edit icon to open a screen where you can change the IP addresses, VLAN ID number and tagging setting.  Set IP Address IP type: Static IP IP Management VLAN ID: 1 (1~4094) ● Untagged ○ Tagged Subnet mask Gateway Primary DNS Close OK
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 155.
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 271 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.
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.

Table 14 Site-wide > Devices > Access points: Details (continued)

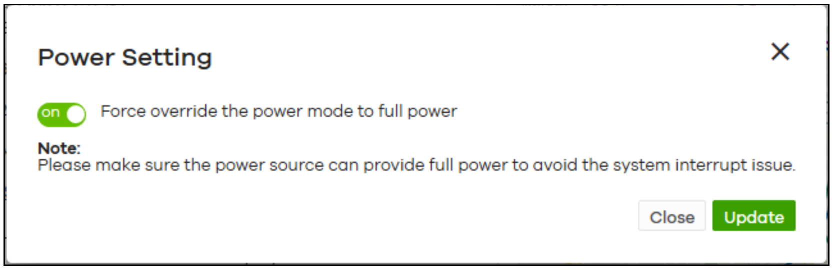
LABEL	DESCRIPTION
Power mode	This shows **Full** when the Nebula Device receives power directly through a power outlet. This shows **Full (Power by DC)** when the Nebula Device receives power using a power adapter. This shows **Full (Power by PoE)** when the Nebula Device receives power through a PoE 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 233. To view the list of Nebula Devices that support smart mesh, go to **Help** > **Device function table**.

Table 14   Site-wide > Devices > Access points: Details (continued)

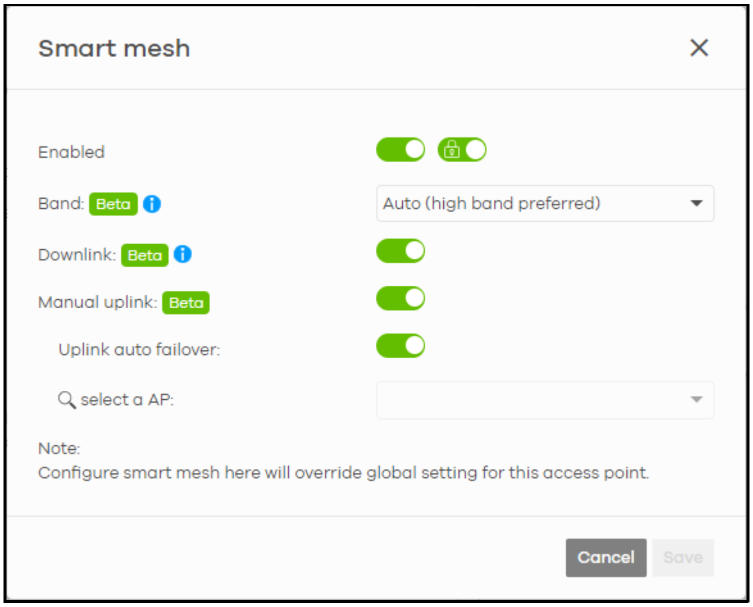
LABEL	DESCRIPTION
Edit	Edit the Nebula Device's Smart Mesh settings.  Smart mesh Enabled Band: Beta Auto (high band preferred) Downlink: Beta Manual uplink: Beta Uplink auto failover: select a AP: Note: Configure smart mesh here will override global setting for this access point.
Enabled	Enable or disable 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.
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.
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 a 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 235. Note: Wireless bridge can only work when smart mesh is enabled in this screen.
Edit	Edit the Nebula Device's wireless bridge settings.

Table 14 Site-wide > Devices > Access points: Details (continued)

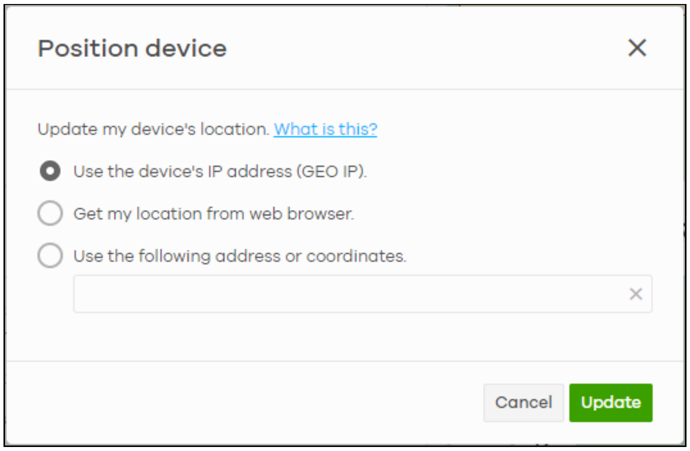
LABEL	DESCRIPTION
Enabled	Enable or disable wireless bridge on the Nebula Device. Note: If Smart Mesh is disabled for the site in NCC, then enabling wireless bridge automatically enables Smart Mesh on the Nebula Device.
Allowed VLANs	Enter the IDs of the VLANs that the Nebula Device will forward over 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 271.
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.
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.
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.

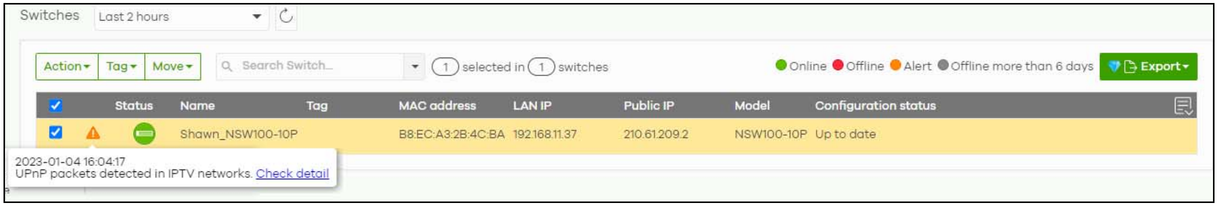
Table 14   Site-wide > Devices > Access points: Details (continued)

LABEL	DESCRIPTION
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 AP	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 Access	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.
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.	
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 27   Site-wide > Devices > Switches



☑	Status	Name	Tag	MAC address	LAN IP	Public IP	Model	Configuration status
☑	⚠	Shawn_NSW100-10P		B8:EC:A3:2B:4C:BA	192.168.11.37	210.61.209.2	NSW100-10P	Up to date

2023-01-04 16:04:17
UPnP packets detected in IPTV networks. Check detail

The following table describes the labels in this screen.

Table 15   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.

Table 15 Site-wide > Devices > Switches (continued)

LABEL	DESCRIPTION
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.
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 75 on page 312 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.
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.
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.

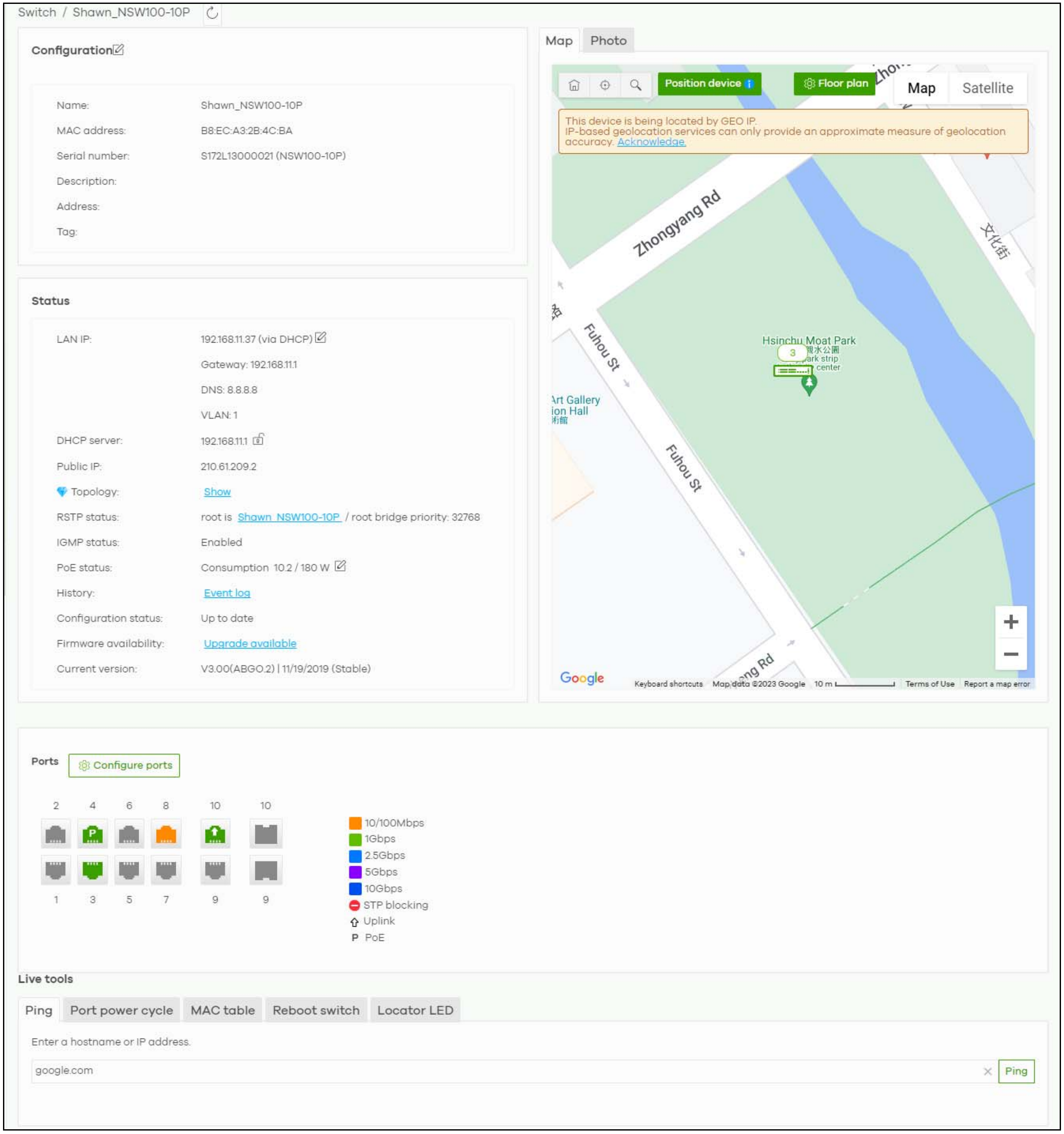
Table 15 Site-wide > Devices > Switches (continued)

LABEL	DESCRIPTION
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.
Usage	This shows the amount of data that has been 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 28 Site-wide > Devices > Switches: Switch Details



Switch / Shawn_NSW100-10P

Configuration

Name:	Shawn_NSW100-10P
MAC address:	B8:EC:A3:2B:4C:BA
Serial number:	S172L13000021 (NSW100-10P)
Description:	
Address:	
Tag:	

Status

LAN IP:	192.168.11.37 (via DHCP) Gateway: 192.168.11.1 DNS: 8.8.8.8 VLAN: 1
DHCP server:	192.168.11.1
Public IP:	210.61.209.2
Topology:	Show
RSTP status:	root is Shawn_NSW100-10P / root bridge priority: 32768
IGMP status:	Enabled
PoE status:	Consumption 10.2 / 180 W
History:	Event log
Configuration status:	Up to date
Firmware availability:	Upgrade available
Current version:	V3.00(ABGO.2) | 11/19/2019 (Stable)

Map | Photo

Position device | Floor plan | Map | Satellite

This device is being located by GEO IP.
IP-based geolocation services can only provide an approximate measure of geolocation accuracy. Acknowledge.

Ports Configure ports

🟧 10/100Mbps
🟩 1Gbps
🟦 2.5Gbps
🟪 5Gbps
🟦 10Gbps
⛔ STP blocking
⇧ Uplink
P PoE

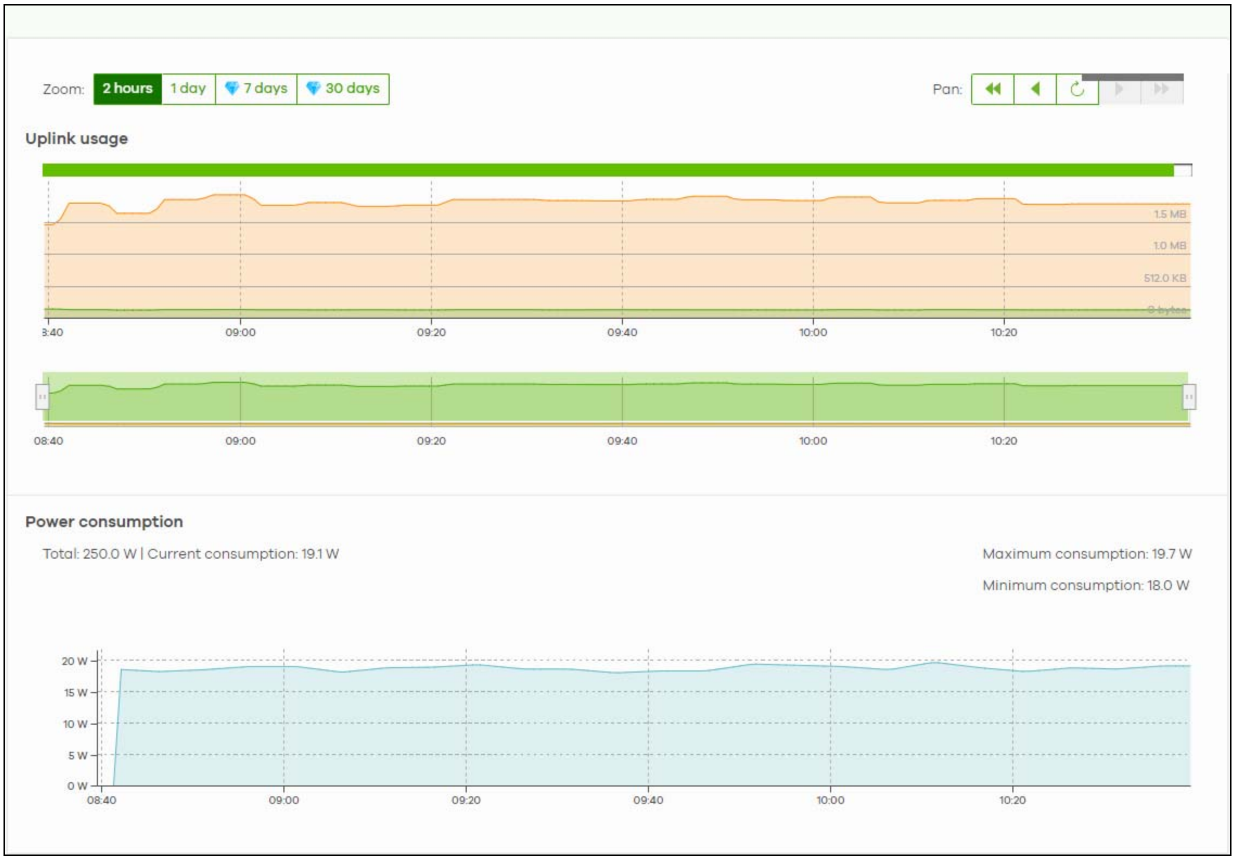
Live tools

Ping | Port power cycle | MAC table | Reboot switch | Locator LED

Enter a hostname or IP address.

google.com

Ping



Uplink usage

Power consumption

Total: 250.0 W | Current consumption: 19.1 W

Maximum consumption: 19.7 W

Minimum consumption: 18.0 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 16 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.
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	

Table 16   Site-wide > Devices > Switches: Switch Details (continued)

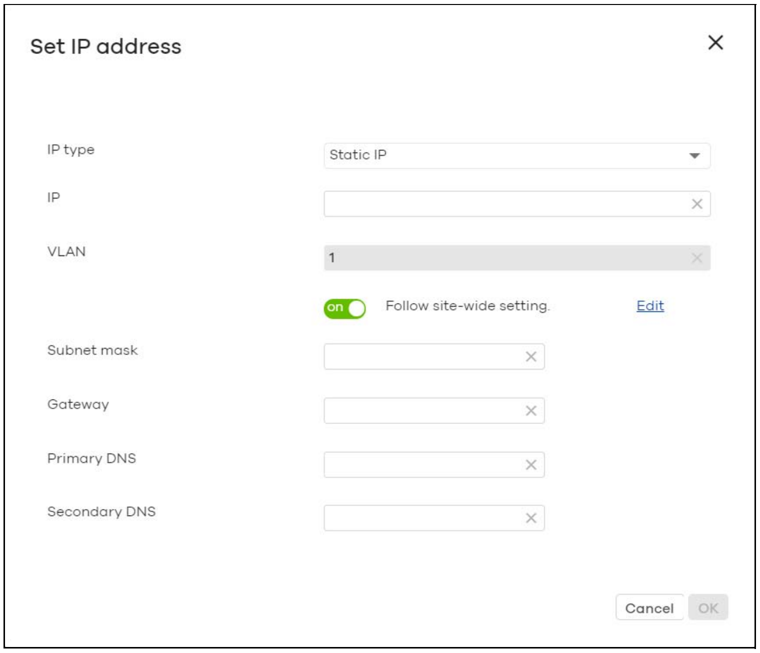
LABEL	DESCRIPTION
LAN IP	This shows the local (LAN) IP address of the Nebula Device. It also shows the IP addresses of the gateway and DNS servers. Click the edit icon to open a screen where you can change the IP address, VLAN ID number and DNS server settings.  Set IP address IP type: Static IP IP: VLAN: 1 on Follow site-wide setting. Edit Subnet mask: Gateway: Primary DNS: Secondary DNS:
DHCP server	This shows the IP address of the DHCP server.
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 155.
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 and 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. Click the edit icon to open the **PoE Configuration** screen. See Section 4.3.2.2 on page 175.
History	Click **Event log** to go to the **Site-wide** > **Monitor** > **Switches** > **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.

Table 16 Site-wide > Devices > Switches: Switch Details (continued)

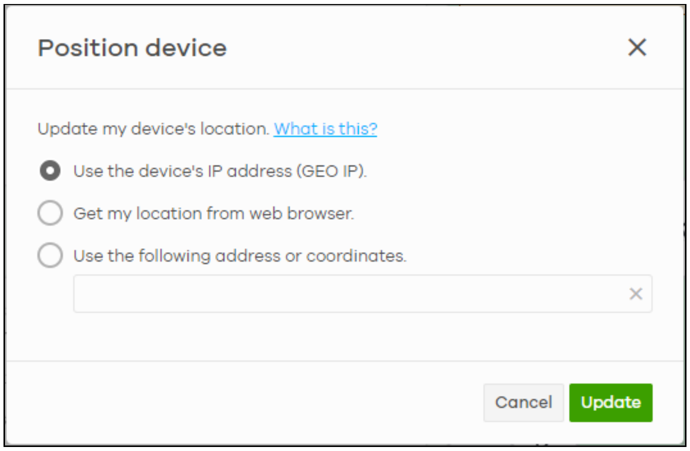
<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></tr>
<tr><td>Map</td><td>This shows the location of the Nebula Device on Google map (<b>Map</b> view or <b>Satellite</b> imagery view) or on a floor plan. Click <b>Floor plan</b> to display a list of existing floor plans. Each floor plan has a drawing that shows the rooms scaled and viewed from above. Drag-and-drop your Nebula Device directly on the Google map or click <b>Position device</b> 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 <b>GEO IP</b> to use the public IP address of the Nebula Device.
• Select <b>Get my location from web browser</b> to use the public IP address of the computer accessing the NCC portal.
• Select <b>Use the following address or coordinates</b> to enter the complete address or coordinates of the Nebula Device.
Note: Nebula Devices that are offline cannot use GEO IP.</td></tr>
<tr><td>Photo</td><td>This shows the photo of the Nebula Device. Click <b>Add</b> to upload one or more photos. Click <b>x</b> to remove a photo.</td></tr>
<tr><td colspan="2">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 175. 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 (#0079FF): 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.</td></tr>
<tr><td>Name</td><td>This shows the Nebula Device name configured in NCC.</td></tr>
<tr><td>Status</td><td>This shows the connection status of the port.</td></tr>
<tr><td>Type</td><td>This shows the port type (<b>Trunk</b> or <b>Access</b>), PVID, and allowed VLANs.</td></tr>
<tr><td>Speed</td><td>This shows the current connection speed of the port. If the speed is unavailable, this displays "Ethernet".</td></tr>
<tr><td>LLDP</td><td>This shows the LLDP information received on the port.</td></tr>
<tr><td>Reset</td><td>This button only appears when the PoE port is connected to a PD (powered device). Follow the prompt and click <b>Confirm</b> to reboot the PD connected to this port.
Note: This button is not available for an uplink port.</td></tr>
</table>

Table 16 Site-wide > Devices > Switches: Switch Details (continued)

LABEL	DESCRIPTION
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 288.
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**.
Port Power Cycle	Enter the number of the ports and click the **Reset** button to disable and enable the 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 switch	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 Access	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 Access** 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 12 hours, day, week, month, 3 months or 6 months.
Pan	Click to move backward or forward by one day or week.
Power Consumption	

Table 16 Site-wide > Devices > Switches: Switch Details (continued)

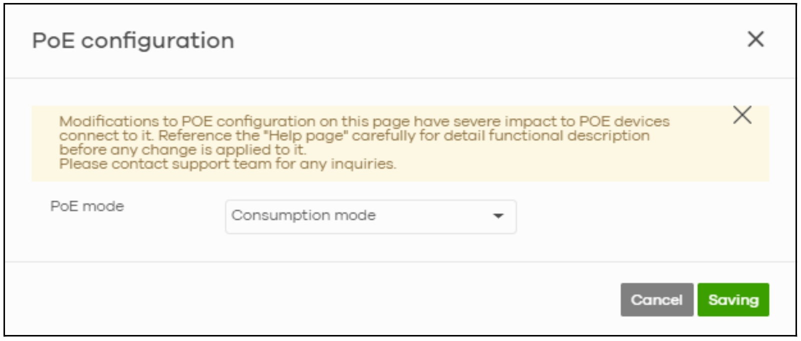
LABEL	DESCRIPTION
	Select to view the Nebula Device power consumption in the past two hours, day, week or month.
	This shows the current, total, maximum and minimum power consumption of the Nebula Device.
y-axis	The y-axis shows how much power is used in Watts.
x-axis	The x-axis shows the time period over which the power consumption is recorded.

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 288.

Figure 29 Site-wide > Devices > Switches: Switch Details: 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.

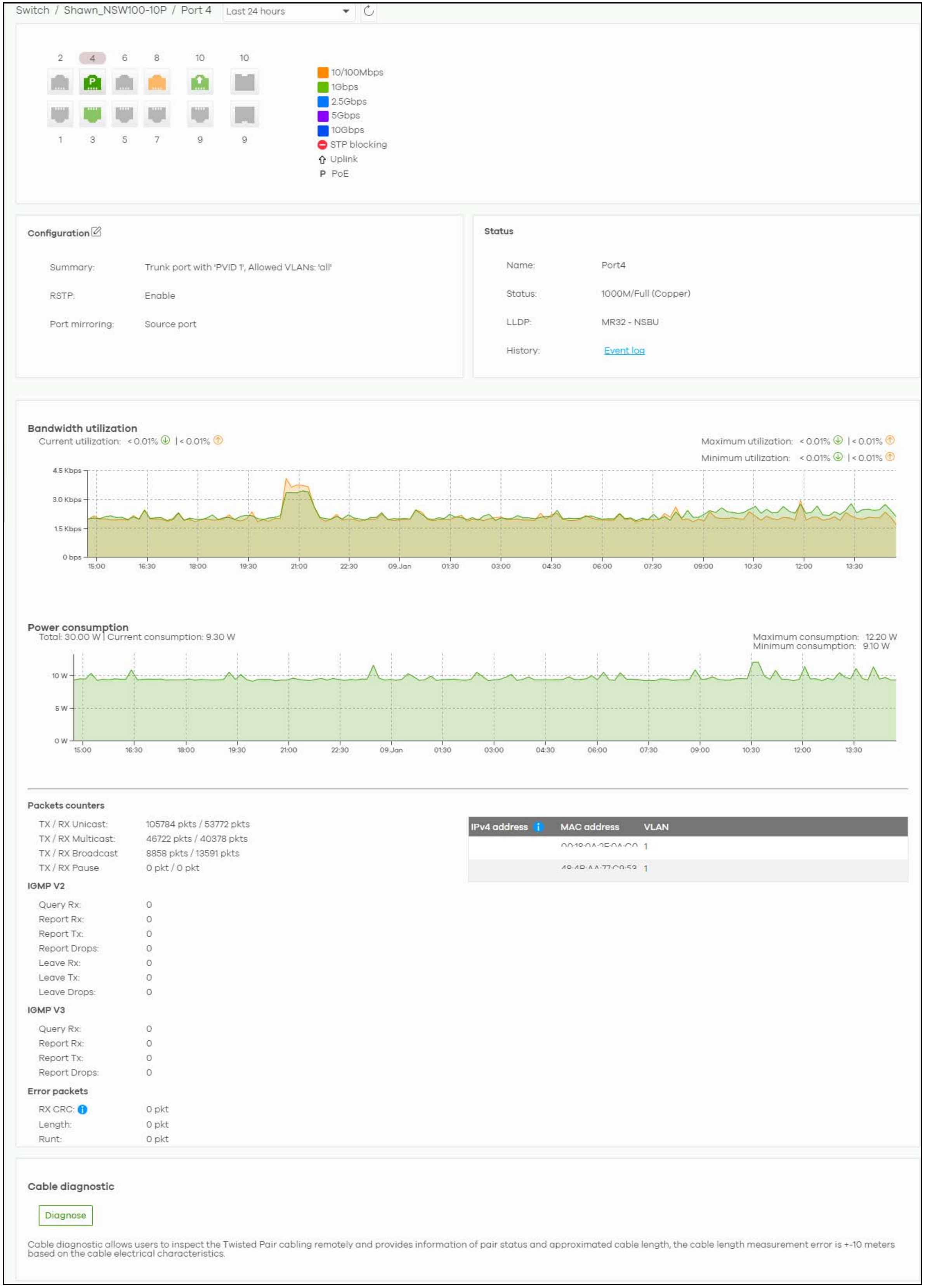
Table 17 Site-wide > Devices > Switches: Switch Details: PoE Configuration

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 30 Site-wide > Devices > Switches: Switch Details: Port Details



Switch / Shawn_NSW100-10P / Port 4 Last 24 hours

🟧 10/100Mbps
🟩 1Gbps
🟦 2.5Gbps
🟪 5Gbps
🟦 10Gbps
⛔ STP blocking
⇧ Uplink
P PoE

Configuration

Summary:	Trunk port with 'PVID 1', Allowed VLANs: 'all'
RSTP:	Enable
Port mirroring:	Source port

Status

Name:	Port4
Status:	1000M/Full (Copper)
LLDP:	MR32 - NSBU
History:	Event log

Bandwidth utilization

Current utilization: < 0.01% ⇩ | < 0.01% ⇧

Maximum utilization: < 0.01% ⇩ | < 0.01% ⇧

Minimum utilization: < 0.01% ⇩ | < 0.01% ⇧

Power consumption

Total: 30.00 W | Current consumption: 9.30 W

Maximum consumption: 12.20 W

Minimum consumption: 9.10 W

Packets counters

TX / RX Unicast:	105784 pkts / 53772 pkts
TX / RX Multicast:	46722 pkts / 40378 pkts
TX / RX Broadcast	8858 pkts / 13591 pkts
TX / RX Pause	0 pkt / 0 pkt

IPv4 address	MAC address	VLAN
	00:18:0A:25:0A:C0	1
	48:4B:AA:77:C9:53	1

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

Diagnose

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 18 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 (#0079FF): 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 288.	
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 18 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.

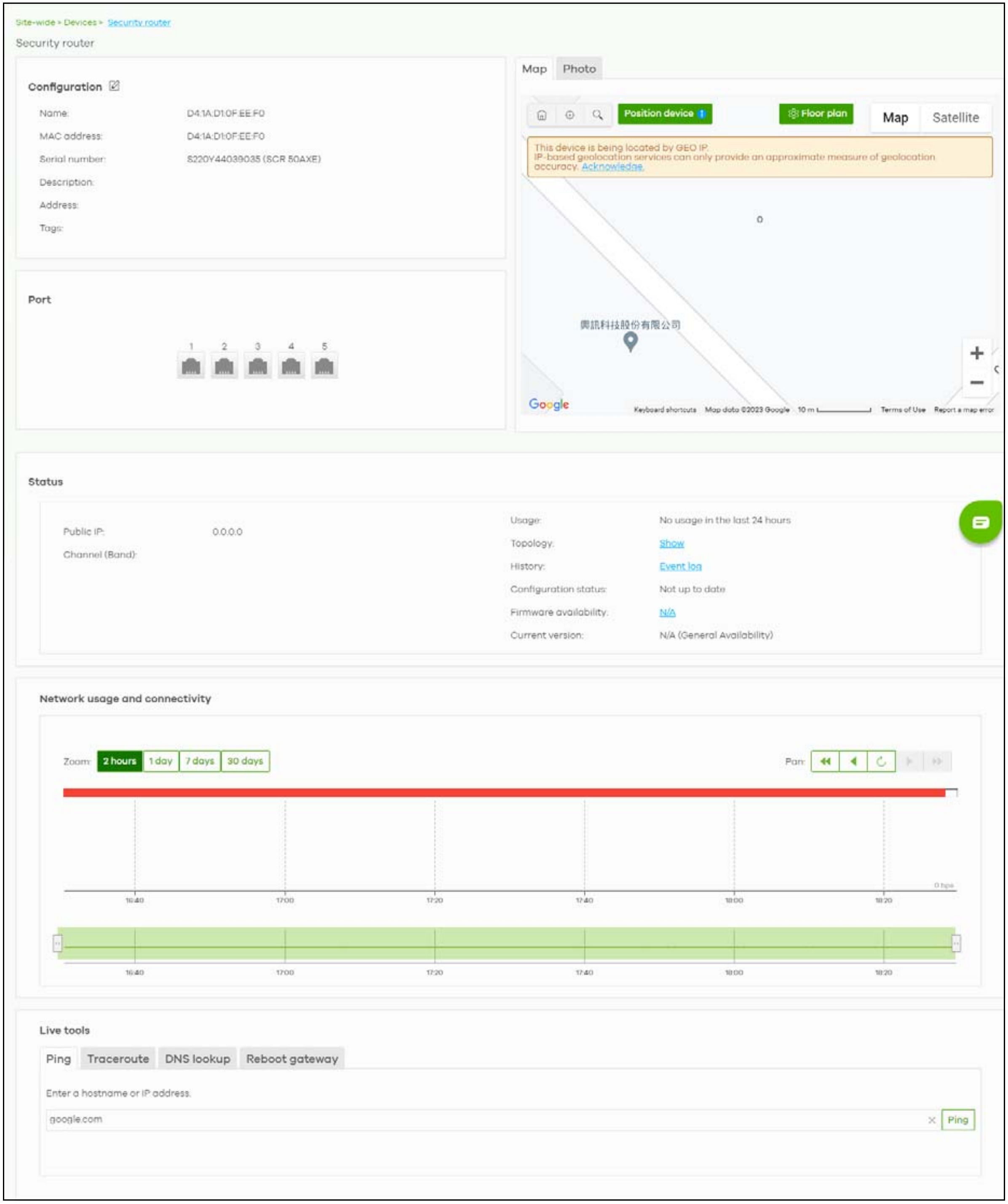
Table 18 Site-wide > Devices > Switches: Switch Details: Port Details (continued)

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 31 Site-wide > Devices > Security routerl



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 19 Site-wide > Devices > Security router

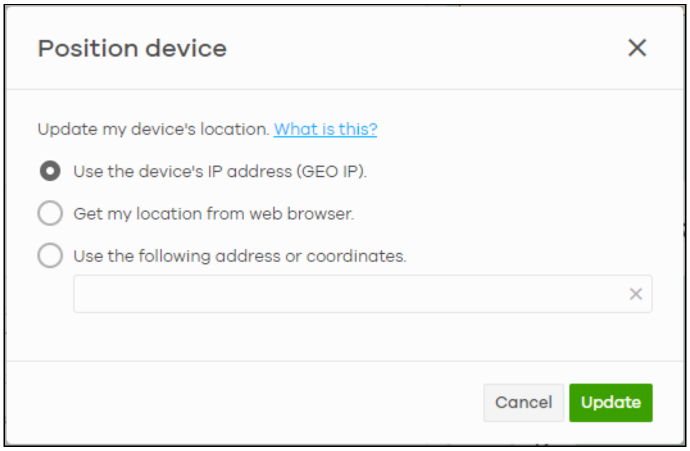
LABEL	DESCRIPTION
Configuration Click the edit icon to change the Nebula Device name, description, tags and address (physical location). You can also move the Nebula Device to another site or remove.	
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of 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.

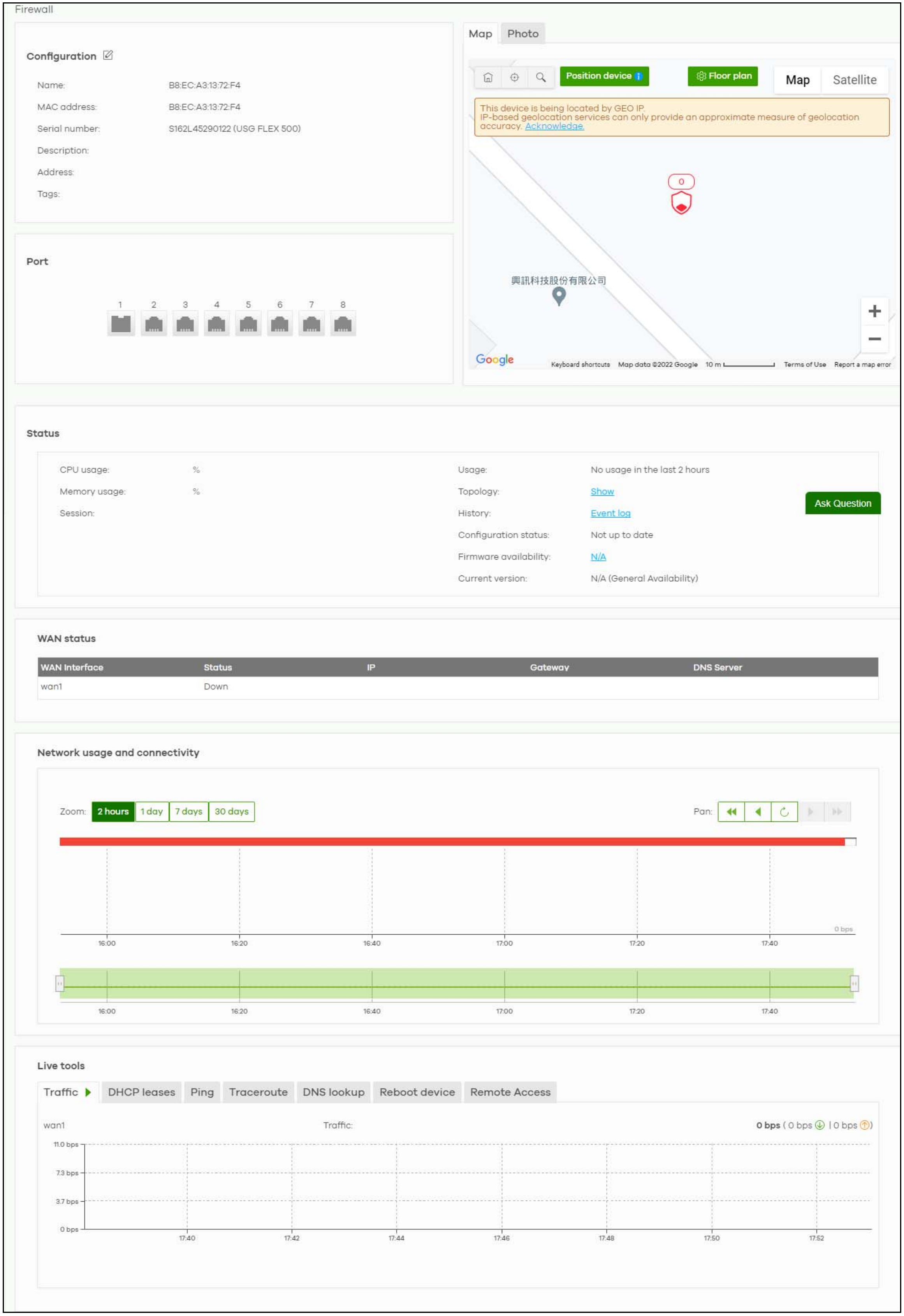
Table 19 Site-wide > Devices > Security router (continued)

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 155.
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.
Reboot gateway	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 32 Site-wide > Devices > Firewall



Firewall

Configuration

Name:	B8:EC:A3:13:72:F4
MAC address:	B8:EC:A3:13:72:F4
Serial number:	S162L45290122 (USG FLEX 500)
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

CPU usage:	%	Usage:	No usage in the last 2 hours
Memory usage:	%	Topology:	Show
Session:		History:	Event log
		Configuration status:	Not up to date
		Firmware availability:	N/A
		Current version:	N/A (General Availability)

WAN status

WAN Interface	Status	IP	Gateway	DNS Server
wan1	Down			

Network usage and connectivity

Live tools

wan1 Traffic: **0 bps** (0 bps | 0 bps)

The following table describes the labels in this screen.

Table 20 Site-wide > Devices > Firewall

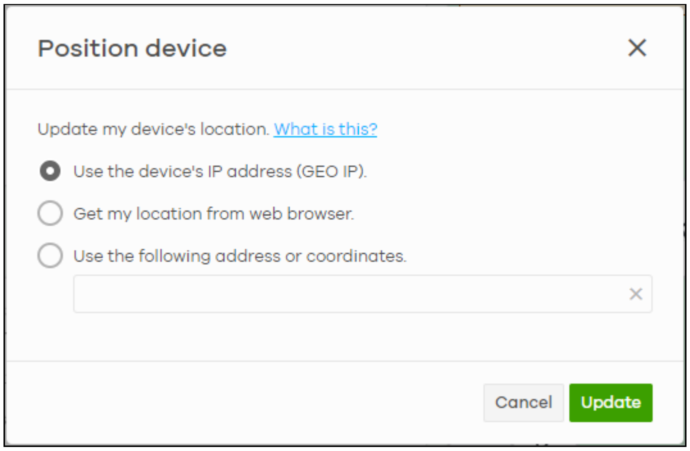
LABEL	DESCRIPTION
Configuration Click the edit icon to change the Nebula Device name, description, tags and address (physical location). You can also move the Nebula Device to another site or remove.	
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device's WAN port.
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.
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	

Table 20 Site-wide > Devices > Firewall (continued)

LABEL	DESCRIPTION
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.
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 155.
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	
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 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	
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.

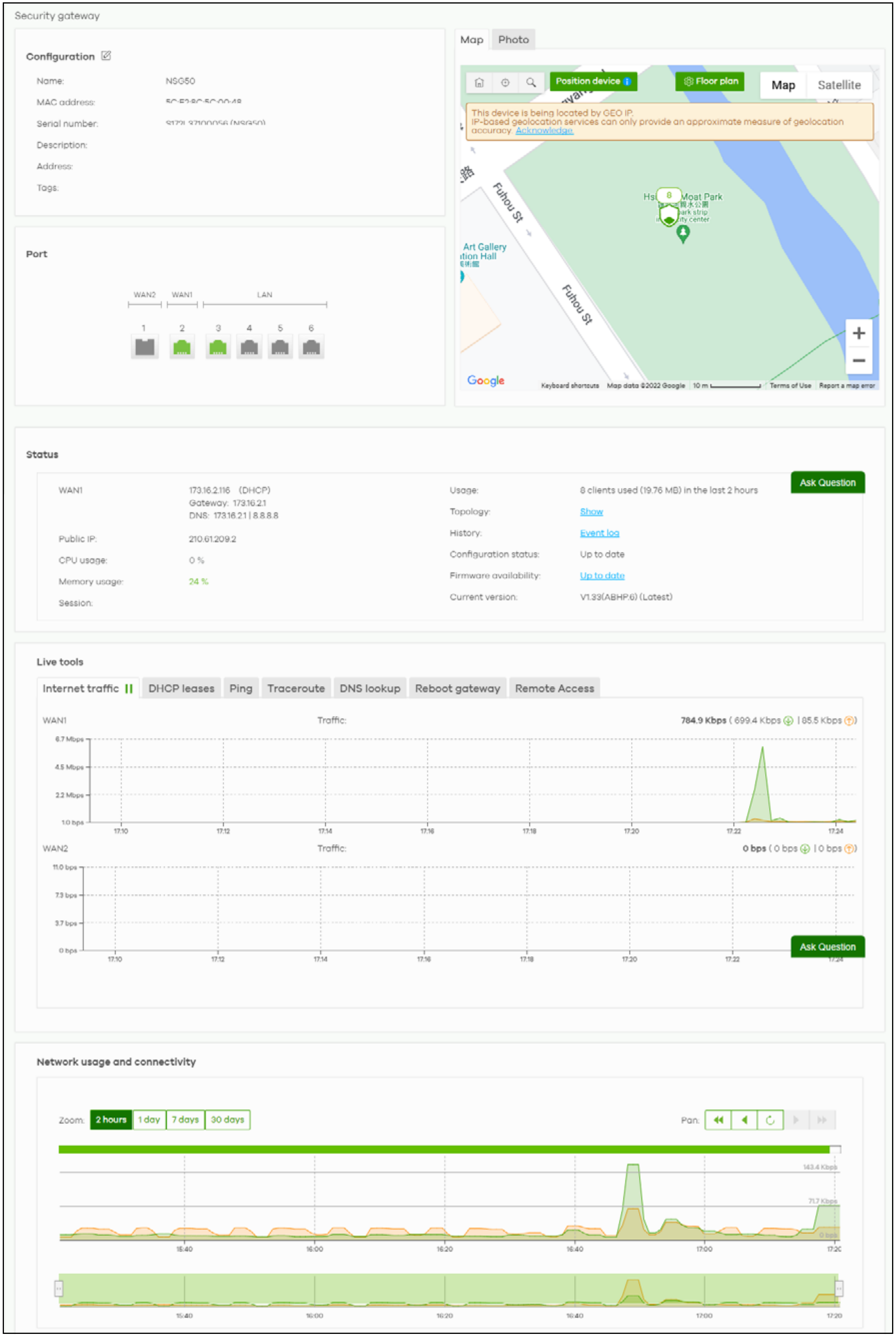
Table 20 Site-wide > Devices > Firewall (continued)

LABEL	DESCRIPTION
Reboot device	Click the **Reboot** button to restart the Nebula Device.
Remote Access	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**.

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 33 Site-wide > Devices > Security gateway



Security gateway

Configuration

Name: NSG50

MAC address: 5C-E2-8C-5C-00-48

Serial number: S172L37100056 (NSG50)

Description:

Address:

Tags:

Port

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: 0 %

Memory usage: 24 %

Session:

Usage: 8 clients used (19.76 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: 784.9 Kbps (699.4 Kbps | 85.5 Kbps)

WAN2 Traffic: 0 bps (0 bps | 0 bps)

Network usage and connectivity

The following table describes the labels in this screen.

Table 21 Site-wide > Devices > Security gateway

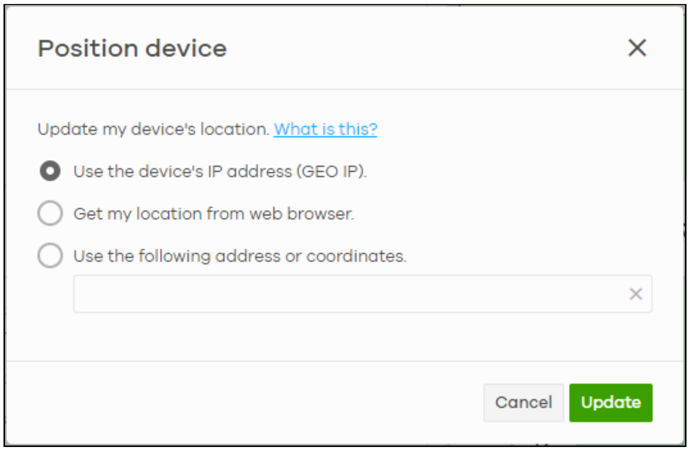
LABEL	DESCRIPTION
Configuration Click the edit icon to change the Nebula Device name, description, tags and address. You can also move the Nebula Device to another site or remove.	
Name	This shows the descriptive name of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
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.
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.
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 21 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.
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 155.
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.
Reboot gateway	Click the **Reboot** button to restart the Nebula Device.
Remote Access	This option is available only for the Nebula Device owner. Establish a remote connection by specifying the **Port** number and clicking **Establish**.
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.

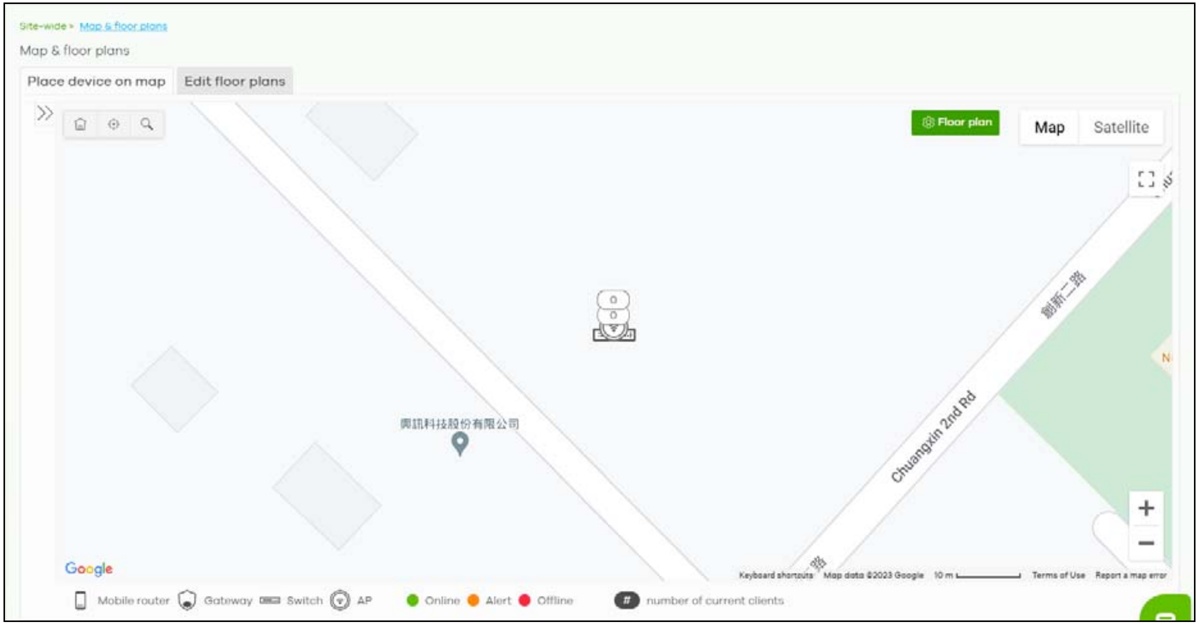
4.3.6 Mobile Router

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.

4.4 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.

Figure 34 Site-wide > Map & floor plans



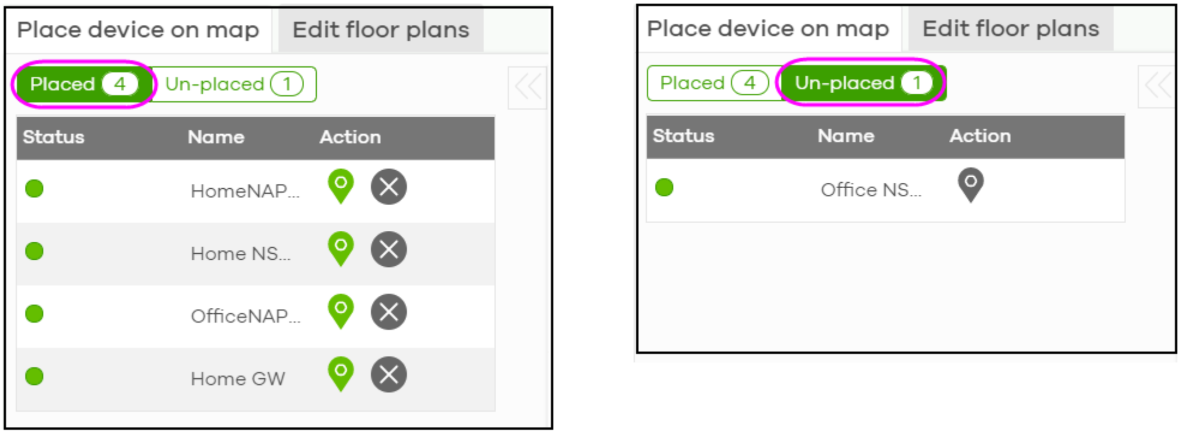
Place device on map

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 35 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

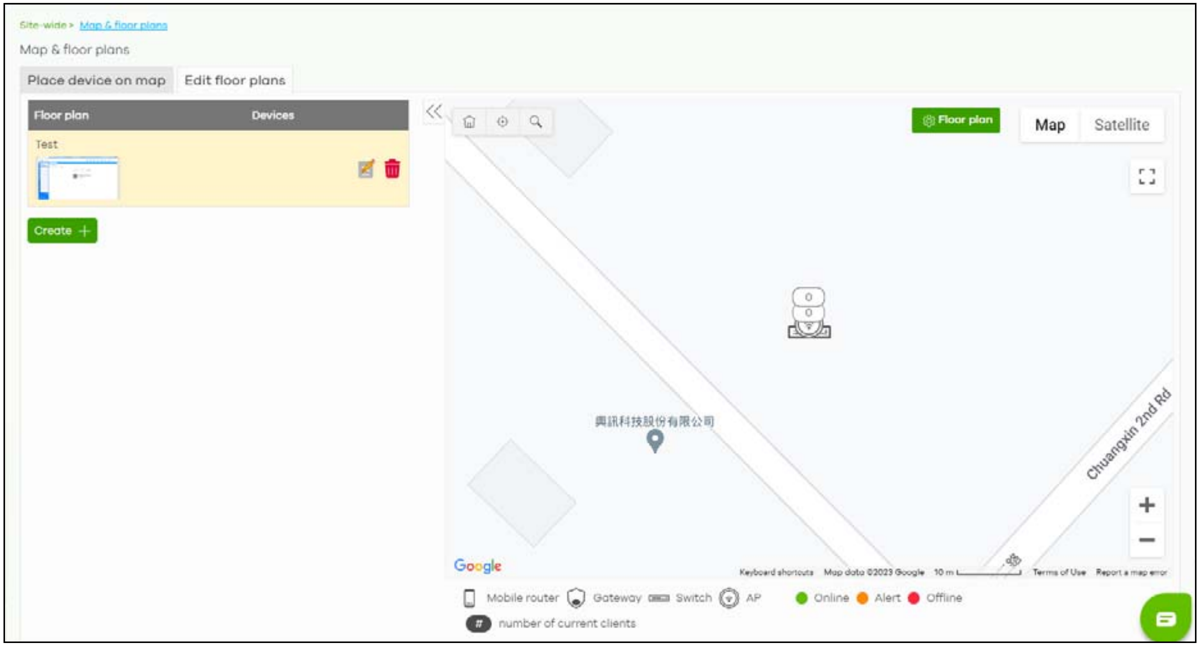
Status	Name	Action
●	Office NS...	📍

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 36 Site-wide > Map & floor plans: Edit floor plans



Site-wide > Map & floor plans

Map & floor plans

Place device on map | Edit floor plans

Floor plan	Devices
Test	

The following table describes the labels in this screen.

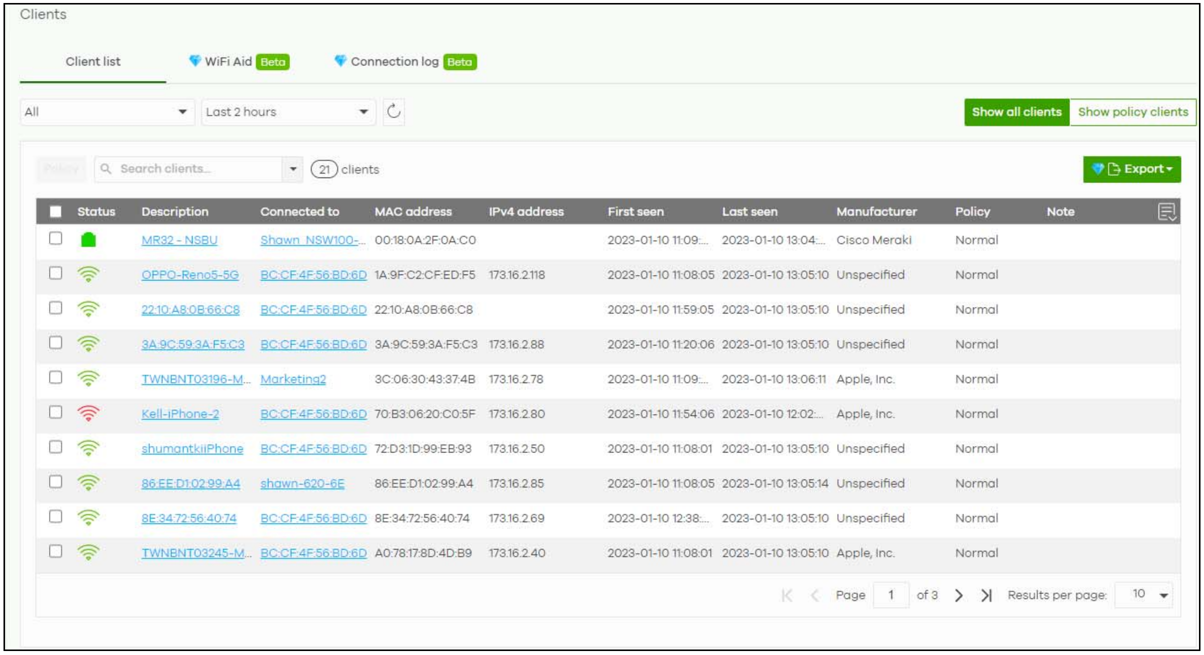
Table 22   Site-Wide > Map & floor plans: Edit floor plans

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, mobile routers) in the site. You can also block or allow clients. Click **Site-wide** > **Clients** to access this screen.

Figure 37   Site-wide > Clients > Client list



Clients

Client list | WiFi Aid Beta | Connection log Beta

All ▾ | Last 2 hours ▾ | ↻ | Show all clients | Show policy clients

Policy | Search clients... ▾ | 21 clients | Export ▾

☐	Status	Description	Connected to	MAC address	IPv4 address	First seen	Last seen	Manufacturer	Policy	Note
☐	■	MR32 - NSBU	Shawn_NSW100-...	00:18:0A:2F:0A:C0		2023-01-10 11:09:...	2023-01-10 13:04:...	Cisco Meraki	Normal	
☐	📶	OPPO-Reno5-5G	BC:CF:4F:56:BD:6D	1A:9F:C2:CF:ED:F5	173.16.2.118	2023-01-10 11:08:05	2023-01-10 13:05:10	Unspecified	Normal	
☐	📶	22:10:A8:0B:66:C8	BC:CF:4F:56:BD:6D	22:10:A8:0B:66:C8		2023-01-10 11:59:05	2023-01-10 13:05:10	Unspecified	Normal	
☐	📶	3A:9C:59:3A:F5:C3	BC:CF:4F:56:BD:6D	3A:9C:59:3A:F5:C3	173.16.2.88	2023-01-10 11:20:06	2023-01-10 13:05:10	Unspecified	Normal	
☐	📶	TWNBNT03196-M...	Marketing2	3C:06:30:43:37:4B	173.16.2.78	2023-01-10 11:09:...	2023-01-10 13:06:11	Apple, Inc.	Normal	
☐	📶	Kell-iPhone-2	BC:CF:4F:56:BD:6D	70:B3:06:20:C0:5F	173.16.2.80	2023-01-10 11:54:06	2023-01-10 12:02:...	Apple, Inc.	Normal	
☐	📶	shumantkiiPhone	BC:CF:4F:56:BD:6D	72:D3:1D:99:EB:93	173.16.2.50	2023-01-10 11:08:01	2023-01-10 13:05:10	Unspecified	Normal	
☐	📶	86:EE:D1:02:99:A4	shawn-620-6E	86:EE:D1:02:99:A4	173.16.2.85	2023-01-10 11:08:05	2023-01-10 13:05:14	Unspecified	Normal	
☐	📶	8E:34:72:56:40:74	BC:CF:4F:56:BD:6D	8E:34:72:56:40:74	173.16.2.69	2023-01-10 12:38:...	2023-01-10 13:05:10	Unspecified	Normal	
☐	📶	TWNBNT03245-M...	BC:CF:4F:56:BD:6D	A0:78:17:8D:4D:B9	173.16.2.40	2023-01-10 11:08:01	2023-01-10 13:05:10	Apple, Inc.	Normal	

Page 1 of 3 | Results per page: 10 ▾

The following table describes the labels in this screen.

Table 23   Site-wide > Clients > Client list

LABEL	DESCRIPTION
Client list	Select to filter the list of clients, based on what type of Nebula Device (access point, Switch, Security Appliance, mobile router) the client is connected to. You can also set a time; the list shows each client's connection status in the past two hours or past 24 hours.
↻	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 23 Site-wide > Clients > Client list (continued)

LABEL	DESCRIPTION
Show policy clients	Click this to show clients that have a white-listed or blocked 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. • **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. • **To specific SSID:** Selectively apply captive portal authentication to specific SSIDs on an AP. • **Normal**: The selected clients have no policies applied to them.
Search clients	Specify your desired filter criteria to filter the list of clients.
N clients	This shows the number of clients (N) connected to the gateway in the site network.
Export	Click this button to save the client list as a CSV or XML file to your computer.
General fields	
	Select an entry's check box to select a specific client. Otherwise, select the check box 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.
Description	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 194 and wired: Section 4.5.0.2 on page 196.
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 client. Click the MAC address to display the individual client statistics. See wireless: Section 4.5.0.1 on page 194 and wired: Section 4.5.0.2 on page 196.
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.

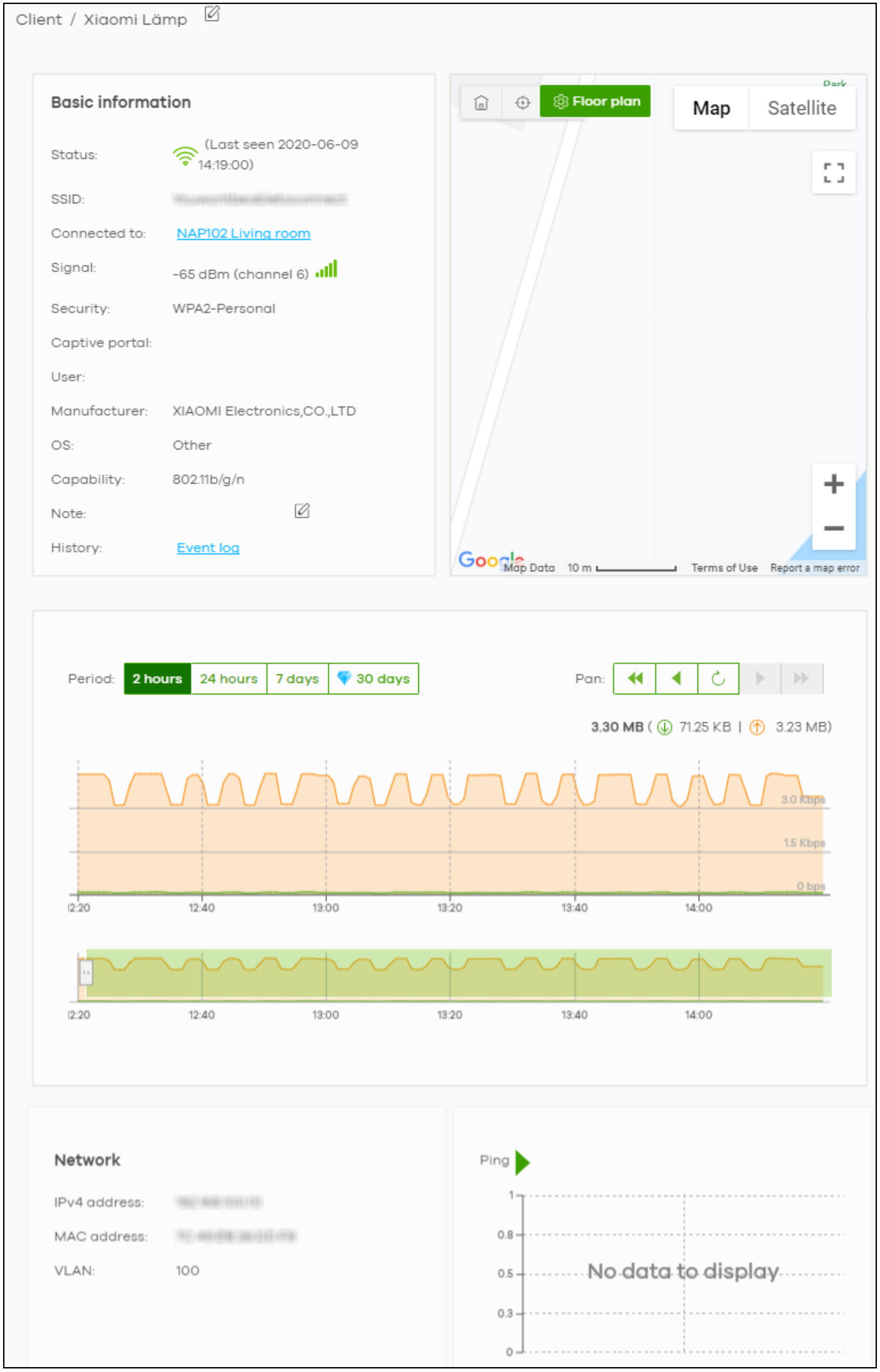
Table 23 Site-wide > Clients > Client list (continued)

LABEL	DESCRIPTION
Note	This shows additional information about the client.
☰	Click this icon to display a greater or lesser number of configuration fields.

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 38 Site-wide > Clients > Clients list: WiFi Client Details



Client / Xiaomi Lämp

Basic information

Status:	(Last seen 2020-06-09 14:19:00)
SSID:	[redacted]
Connected to:	NAP102 Living room
Signal:	-65 dBm (channel 6)
Security:	WPA2-Personal
Captive portal:	
User:	
Manufacturer:	XIAOMI Electronics,CO.,LTD
OS:	Other
Capability:	802.11b/g/n
Note:	
History:	Event log

Period: 2 hours 24 hours 7 days 30 days

3.30 MB (71.25 KB | 3.23 MB)

Network

IPv4 address:	[redacted]
MAC address:	[redacted]
VLAN:	100

The following table describes the labels in this screen.

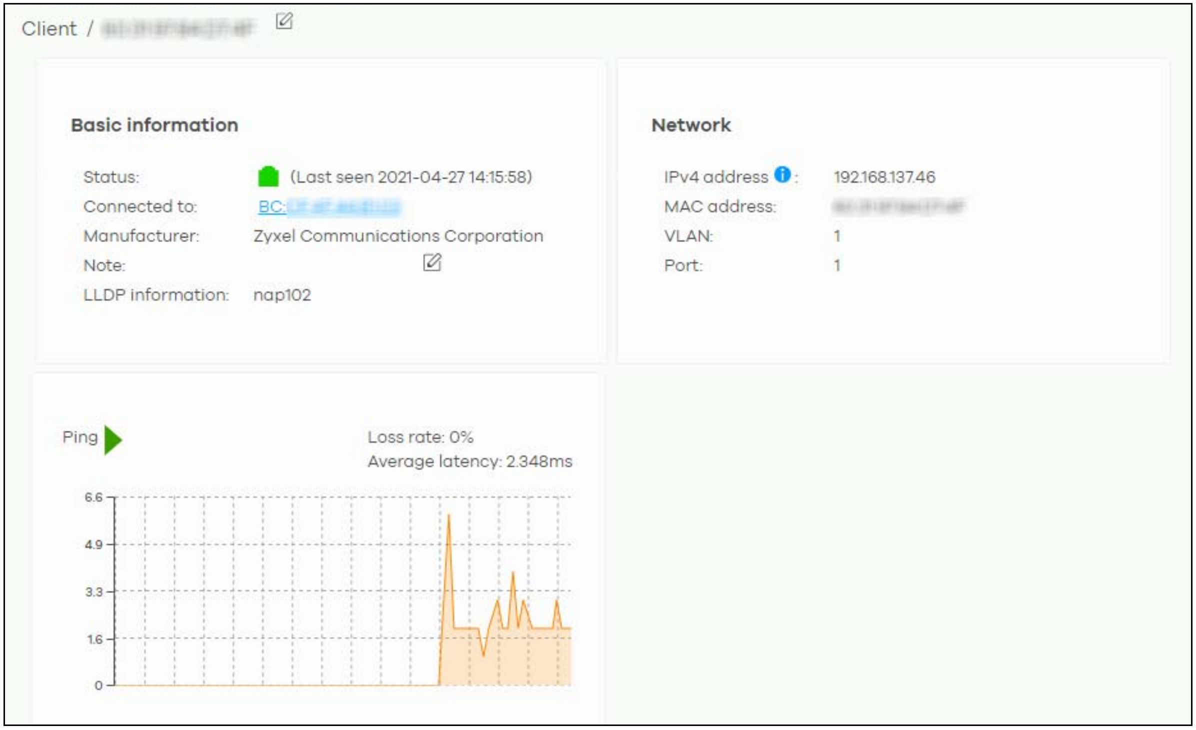
Table 24 Site-wide > Clients > Clients list: WiFi Client Details

LABEL	DESCRIPTION
Client	Click the edit icon to change the client name.
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 159.
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.
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	
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 39 Site-wide > Clients > Clients list: Wired Client Details



Client / [redacted]

Basic information

Status: 🟩 (Last seen 2021-04-27 14:15:58)
Connected to: BC:[redacted]
Manufacturer: Zyxel Communications Corporation
Note:
LLDP information: nap102

Network

IPv4 address: 192.168.137.46
MAC address: [redacted]
VLAN: 1
Port: 1

Loss rate: 0%
Average latency: 2.348ms

The following table describes the labels in this screen.

Table 25 Site-wide > Clients > Clients list: Wired Client Details

LABEL	DESCRIPTION
Client	Click the edit icon to change the client name.
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.
Connected to	This shows the name of the Security Appliance to which the client is connected.
Manufacturer	This shows the manufacturer of the client device.
Note	Enter information about this Nebula Device, for yourself or for other administrators.
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.
Port	This shows the port number of the Nebula Device the client is connected.
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.

4.5.1 WiFi Aid

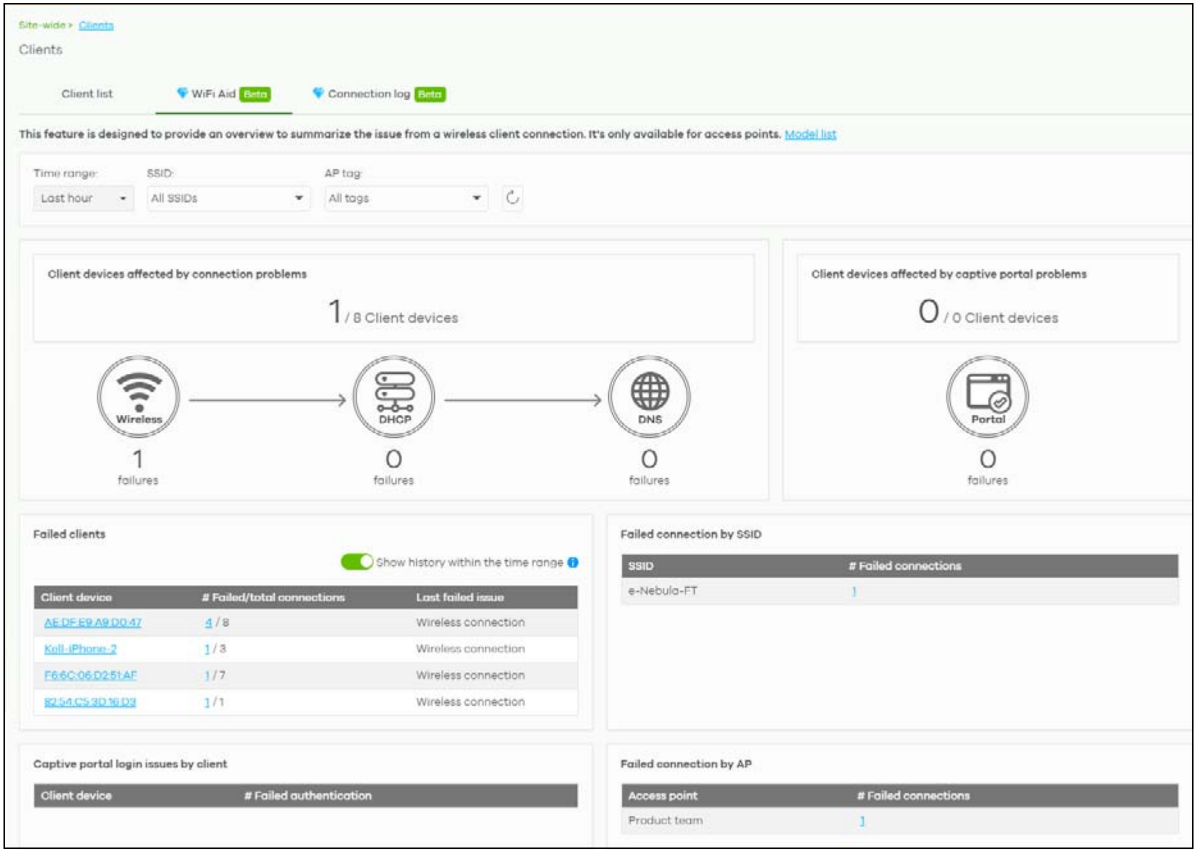
The **WiFi Aid** screen displays the number of WiFi clients that cannot connect to an AP(s) in a site. It also displays the number of WiFi clients who cannot authenticate in a hotspot (captive portal) or who have timed out.

Use this screen to identify connection problems between WiFi clients and supported AP(s). Click **Site-wide** > **Clients** > **WiFi Aid** to access this screen.

Note: This feature is available if you have the Nebula Pro Pack license only.

Note: After a WiFi client successfully connects to the Nebula Device, NCC will not count past connection failures.

Figure 40 Site-wide > Clients > WiFi Aid



Site-wide > Clients

Clients

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 hour

SSID: All SSIDs

AP tag: All tags

Client devices affected by connection problems

1 / 8 Client devices

Client devices affected by captive portal problems

0 / 0 Client devices

Failed clients

Show history within the time range

Client device	# Failed/total connections	Last failed issue
AE:DF:E9:A9:D0:47	4 / 8	Wireless connection
Kall-iPhone-2	1 / 3	Wireless connection
F6:6C:06:D2:51:AF	1 / 7	Wireless connection
82:54:C5:3D:16:D3	1 / 1	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

The following table describes the labels in this screen.

Table 26 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 WiFi networks (**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 **Access point** > **Monitor** > **Access points**. Click the Refresh icon to update this screen.
Client devices affected by connection problems	This chart displays the number of WiFi clients with the following connection problems. • **Wireless** failures. This displays the number of WiFi clients that failed association to an AP or failed authentication. • **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. • **DNS** failures. This displays the number of WiFi clients that failed DNS query due to DNS timeout from a DNS server.
Client devices affected by captive portal problems	This chart displays the number of WiFi clients that failed hotspot authentication. 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 client/DNS failures – numerator) over the number of total connection attempts (denominator). 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 192 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 204 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 client/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 204 for more information on this screen.
Captive portal login issues by client	This table displays the list of WiFi clients with the corresponding number of failed hotspot authentication. The list displays the WiFi client that failed hotspot authentication the most number of times 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 192 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 204 for more information on this screen.
Failed connection by AP	This table displays the number of WiFi clients with WiFi connection/DHCP client/DNS failures in each access point. The list displays the access point with the most connection failures first, in descending order. Clicking the hyperlink in the **# Failed connection** column will direct you to the **Site-wide** > **Monitor** > **Connection log** screen. See Section 4.8 on page 204 for more information on this screen.

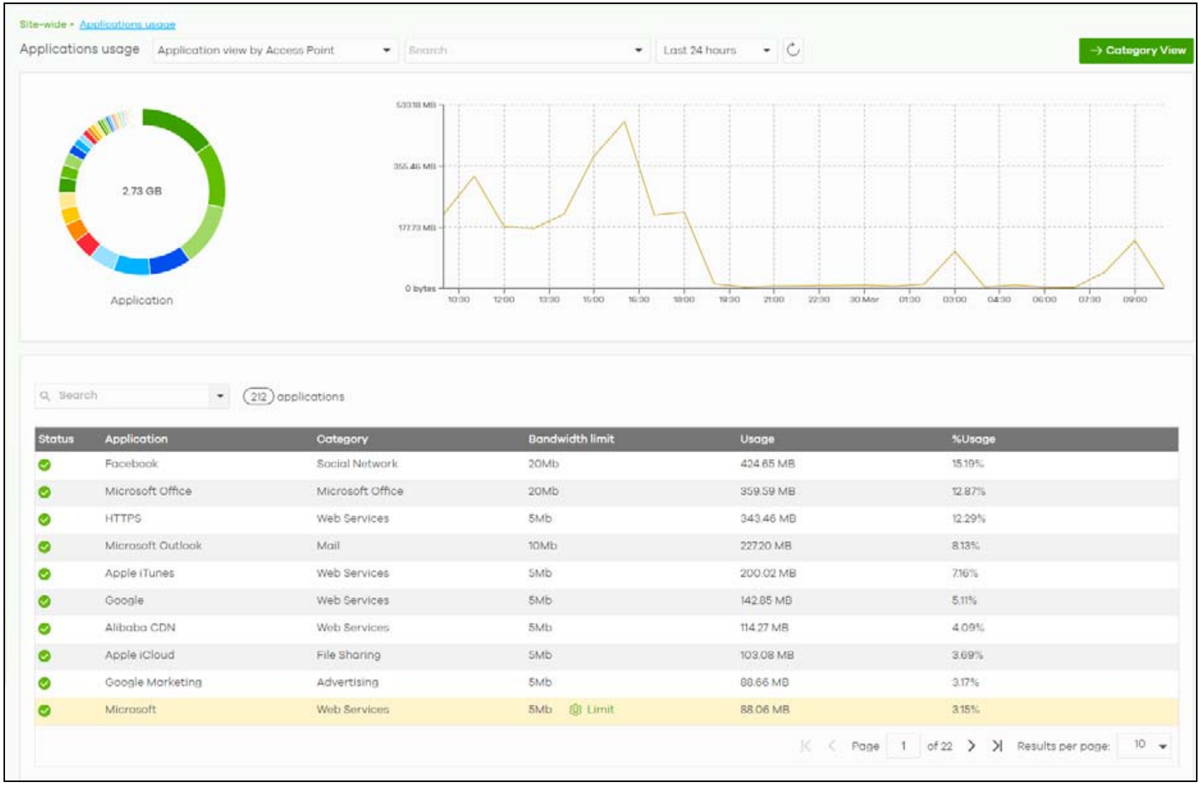
4.6 Applications Usage

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.

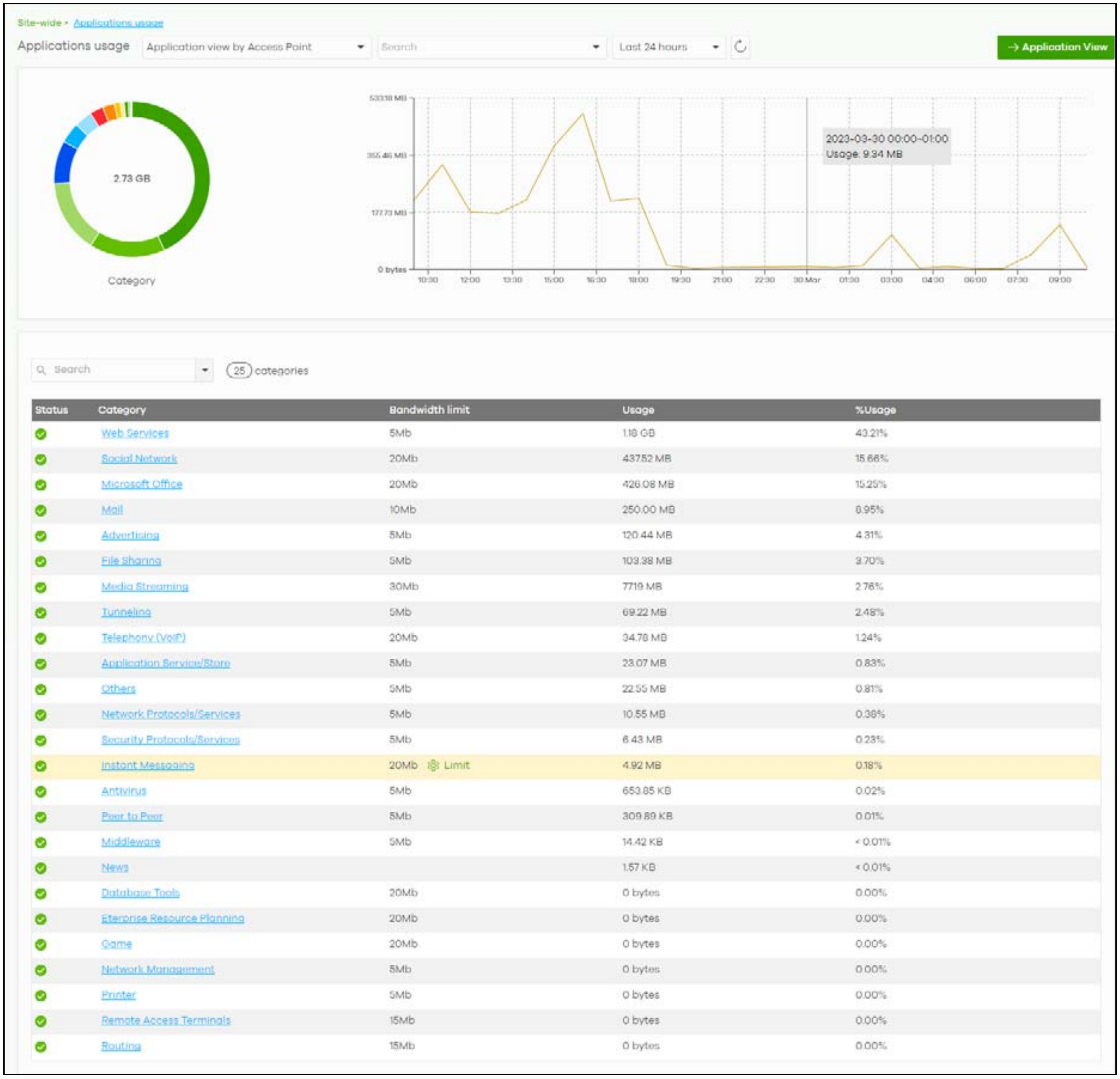
Note: You can view this screen by application or by category.

Figure 41 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%

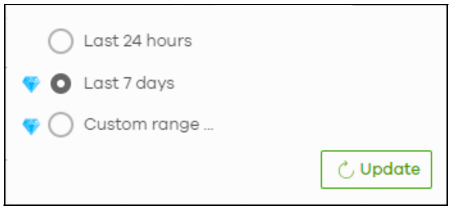
Figure 42 Site-wide > Applications usage: Category View



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 27 Site-wide > Applications usage

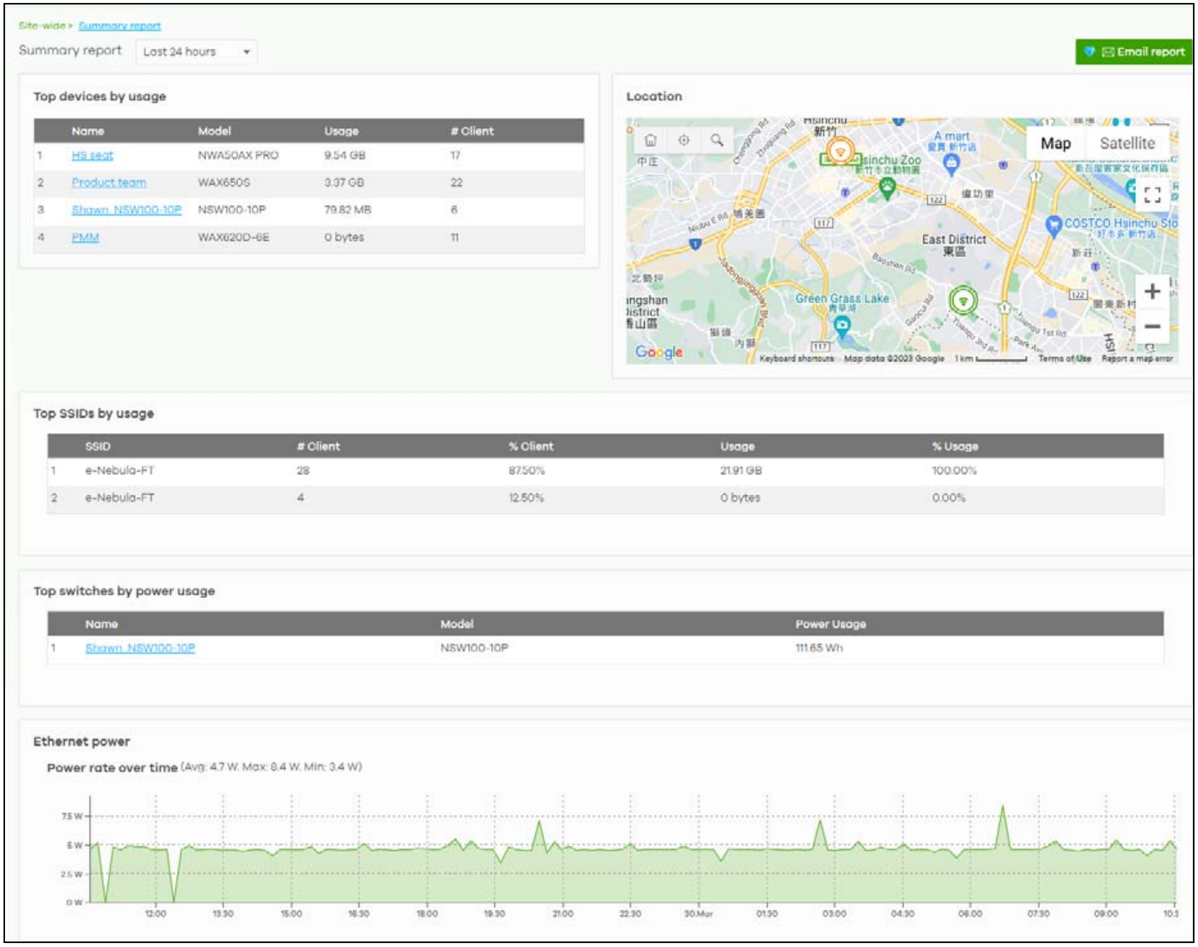
LABEL	DESCRIPTION
Applications	In Application view, select to view all applications of Nebula Security Appliances / Nebula Access Points, or only applications with bandwidth or block policies applied to Nebula Security Appliances. In Category view, select to view all applications of Nebula Security Appliances / 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 43 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 28 Site-wide> Summary report

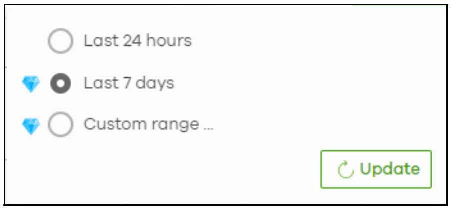
LABEL	DESCRIPTION
Summary report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ● Last 7 days ○ Custom range ... Update
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
Top devices by usage	
	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.
Model	This shows the model number of the Nebula Device.

Table 28 Site-wide> Summary report (continued)

LABEL	DESCRIPTION
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.	
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

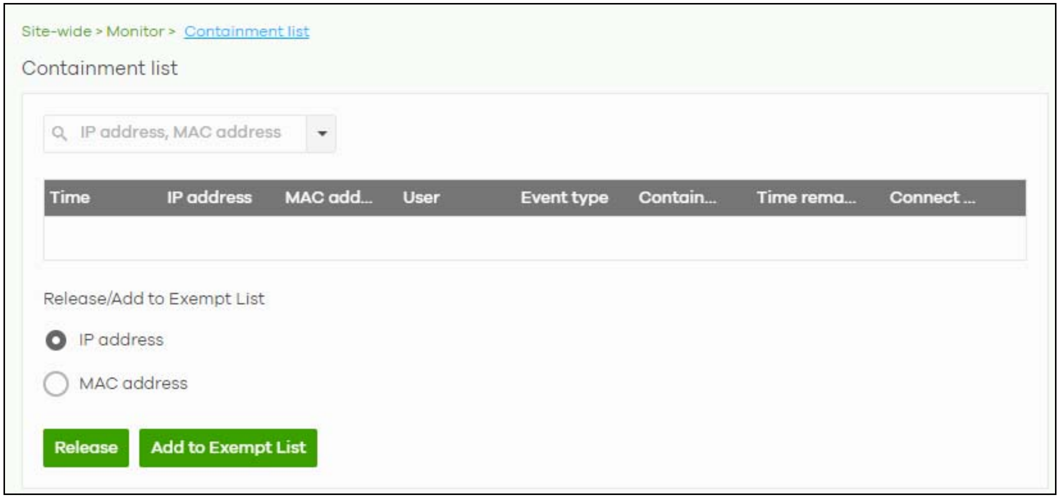
Use the **Monitor** menus to check the site features logs and containment list of the Nebula Devices for the selected site. Please click the following links to go to the respective Nebula Devices **Monitor** menus.

- Access points (Section 5.2 on page 235)
- Switches (Section 6.2 on page 276)
- Security router (Section 7.2 on page 316)
- Mobile router (Section 10.4 on page 479)
- Firewall (Section 8.2 on page 342)
- Security gateway (Section 9.2 on page 414)

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 44 Site-wide > Monitor > Containment list



The following table describes the labels in this screen.

Table 29 Site-wide > Monitor > Containment list

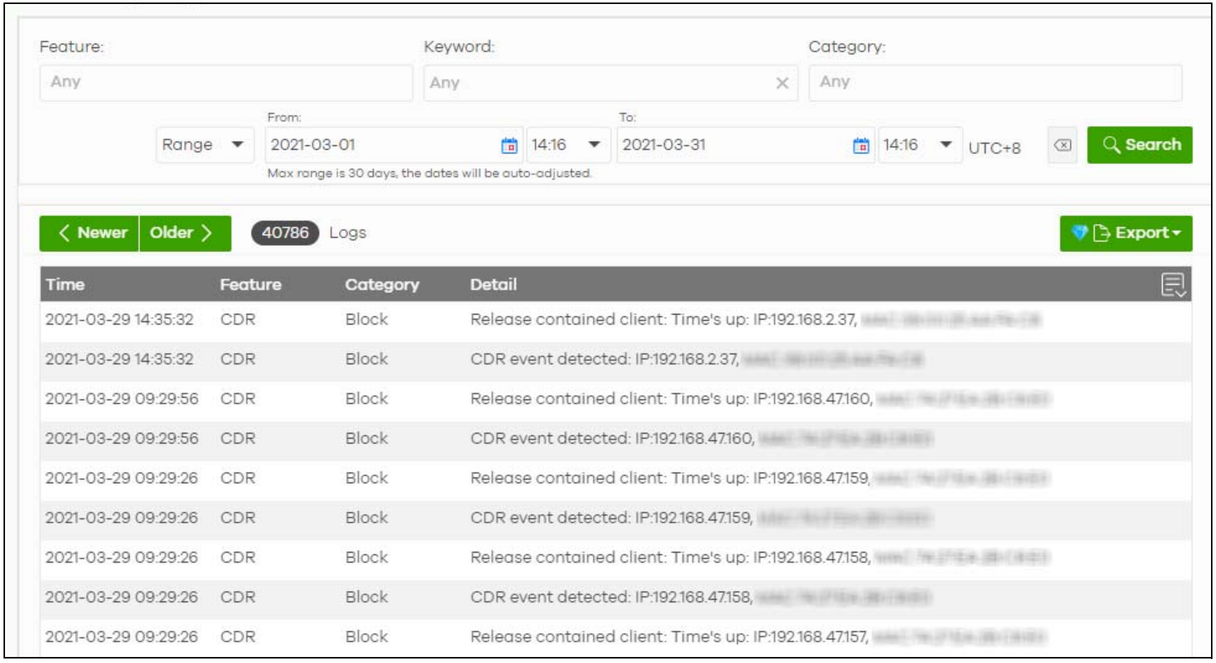
LABEL	DESCRIPTION
Search	Enter a MAC or IP address to filter the list of clients.
Time	This field displays the date and time CDR contained this client.
IP address	This field displays the IPv4 address of the client contained by CDR.
MAC address	This field displays the MAC address of the client contained 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 45 Site-wide > Monitor > Site features logs



Feature: Any

Keyword: Any

Category: Any

Range From: 2021-03-01 14:16 To: 2021-03-31 14:16 UTC+8

Max range is 30 days, the dates will be auto-adjusted.

40786 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 30 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 30 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.

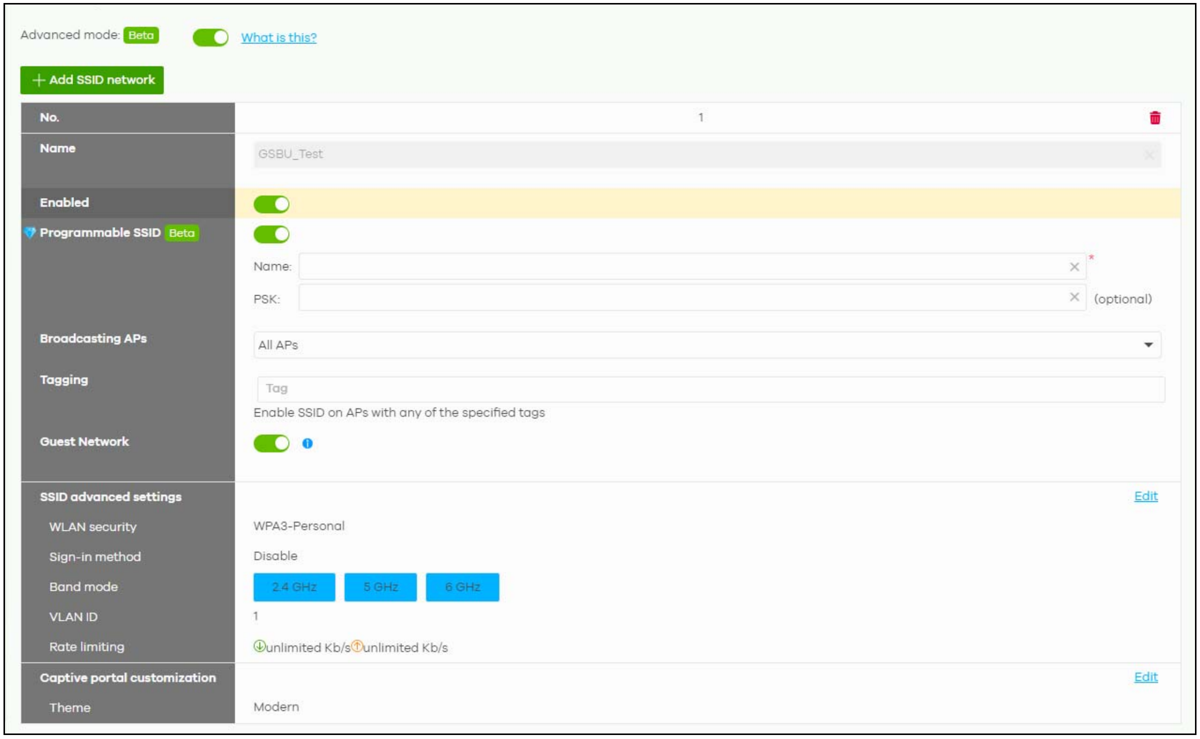
- Access points (Section 5.3 on page 247)
- Switches (Section 6.3 on page 288)
- Security router (Section 7.3 on page 319)
- Mobile router (Section 10.2 on page 471)
- Firewall (Section 8.3 on page 350)
- Security gateway (Section 9.3 on page 422)

4.9.1 WiFi SSID Settings

This screen allows you to configure up to eight 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** > **WiFi SSID settings** to access this screen.

Figure 46 Site-wide > Configure > WiFi SSID settings



Advanced mode: Beta — What is this?

+ Add SSID network

No.	1
Name	GSBU_Test
Enabled	
Programmable SSID Beta	Name: PSK: (optional)
Broadcasting APs	All APs
Tagging	Tag Enable SSID on APs with any of the specified tags
Guest Network	
SSID advanced settings	Edit
WLAN security	WPA3-Personal
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

The following table describes the labels in this screen.

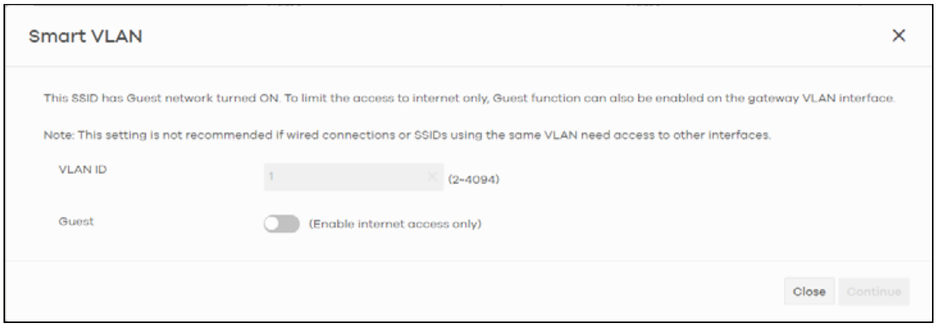
Table 31 Site-wide > Configure > WiFi SSID settings

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
No.	This shows the index number of this profile.
delete	Click this icon to remove the SSID profile.
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.
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 31 Site-wide > Configure > WiFi 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**.
Broadcasting APs	Select **All APs** or specify the AP to use this SSID profile.
Tagging	Enter or select the tags you created for Nebula Devices in the **Site-wide** > **Devices** > **Access points / Security router / Mobile router** screen. The SSID profile will only be applied to Nebula Devices with the specified tag. If you leave this field blank, this SSID profile will be applied to all Nebula Devices in the site.

Table 31 Site-wide > Configure > WiFi SSID settings (continued)

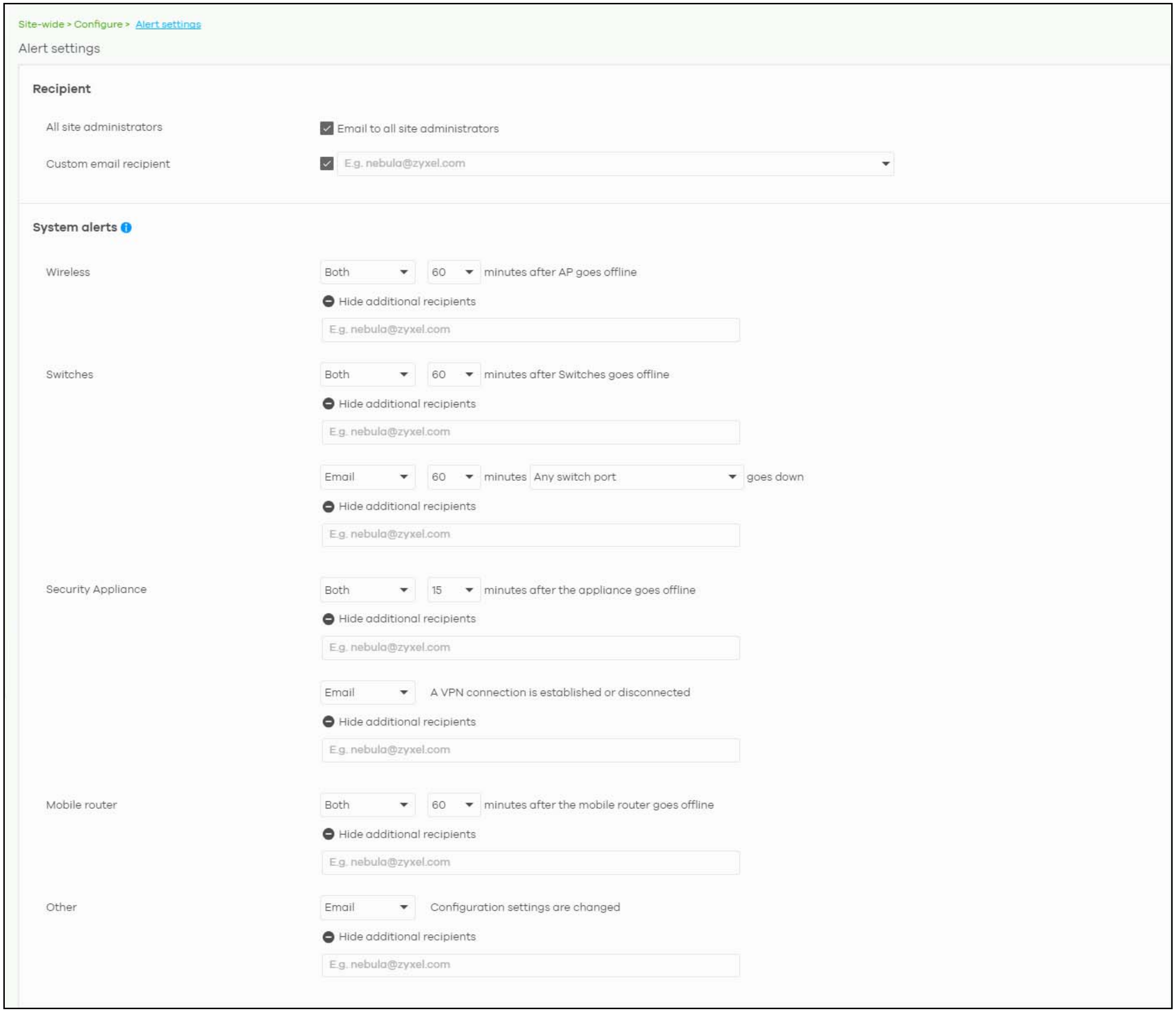
LABEL	DESCRIPTION
Guest Network	Select On to set this WiFi network as a guest network. Layer 2 isolation and intra-BSS blocking are automatically enabled on the SSID. WiFi clients connecting to this SSID can access the Internet through the Nebula Device but cannot directly connect to the LAN or the WiFi 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 5.3.1 on page 247. 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)
SSID advanced 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 48 on page 249 for more information on assisted roaming and U-APSD.
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.
Captive portal customization	
Edit	Click this button to go to the **Captive portal** screen and configure the captive portal settings. See Section 5.3.2 on page 256.
Theme	If captive portal is enabled, this shows the name of the captive portal page used in this profile.

4.9.2 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 47 Site-Wide > Configure > Alert settings



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
Wireless: Both | 60 | minutes after AP goes offline
Hide additional recipients
E.g. nebula@zyxel.com
Switches: Both | 60 | minutes after Switches goes offline
Hide additional recipients
E.g. nebula@zyxel.com
Email | 60 | minutes | Any switch port | goes down
Hide additional recipients
E.g. nebula@zyxel.com
Security Appliance: Both | 15 | minutes after the appliance goes offline
Hide additional recipients
E.g. nebula@zyxel.com
Email | A VPN connection is established or disconnected
Hide additional recipients
E.g. nebula@zyxel.com
Mobile router: Both | 60 | minutes after the mobile router goes offline
Hide additional recipients
E.g. nebula@zyxel.com
Other: Email | Configuration settings are changed
Hide additional recipients
E.g. nebula@zyxel.com

The following table describes the labels in this screen.

Table 32 Site-Wide > Configure > Alert settings

LABEL	DESCRIPTION
Recipient	
All site administrators	Select this to send alerts to all site administrators for the current site.
Custom email recipient	Enter the email addresses to which you want to send alerts.

Table 32 Site-Wide > Configure > Alert settings (continued)

LABEL	DESCRIPTION
Notification Type	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. • **Disabled**: No alerts are sent.
Show additional recipients	Add additional user accounts who will receive email and 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 AP becomes offline.
Switches	Specify how long in minutes the NCC waits before generating and sending an alert when a port or a Switch goes offline.
Security Appliance	Select the check box to have the NCC generate and send an alert by email when the following events occur: • A Security Appliance goes offline. • Any DHCP pool on the Security Appliance runs out of IP addresses. • A VPN connection to or from the Security Appliance is established or disconnected. • The WAN connectivity status changed.
Mobile router	Specify how long in minutes the NCC waits before generating and sending an alert when a mobile router goes offline.
Other	Specify whether to send an alert each time configuration settings are changed.

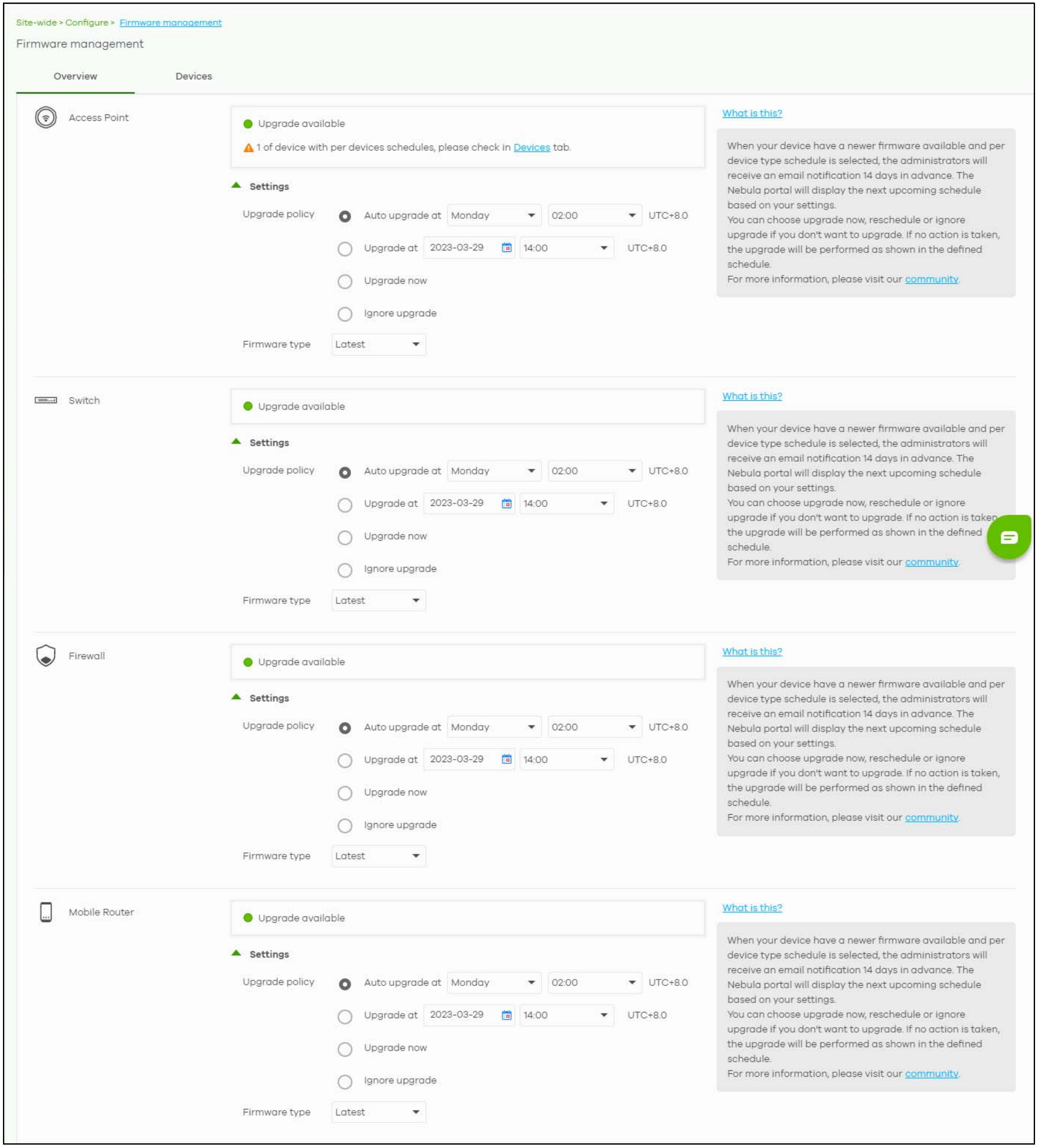
4.9.3 Firmware Management

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.

4.9.3.1 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 48 Site-Wide > Configure > Firmware management > Overview



Site-wide > Configure > Firmware management

Firmware management

Overview | Devices

Access Point

● Upgrade available

⚠ 1 of device with per devices schedules, please check in Devices tab.

▲ **Settings**

Upgrade policy ● Auto upgrade at Monday 02:00 UTC+8.0
○ Upgrade at 2023-03-29 14:00 UTC+8.0
○ Upgrade now
○ Ignore upgrade

Firmware type: Latest

What is this?

When your device have a newer firmware available and per device type schedule is selected, the administrators will receive an email notification 14 days in advance. The Nebula portal will display the next upcoming schedule based on your settings.
You can choose upgrade now, reschedule or ignore upgrade if you don't want to upgrade. If no action is taken, the upgrade will be performed as shown in the defined schedule.
For more information, please visit our community.

Switch

● Upgrade available

▲ **Settings**

Upgrade policy ● Auto upgrade at Monday 02:00 UTC+8.0
○ Upgrade at 2023-03-29 14:00 UTC+8.0
○ Upgrade now
○ Ignore upgrade

Firmware type: Latest

What is this?

When your device have a newer firmware available and per device type schedule is selected, the administrators will receive an email notification 14 days in advance. The Nebula portal will display the next upcoming schedule based on your settings.
You can choose upgrade now, reschedule or ignore upgrade if you don't want to upgrade. If no action is taken the upgrade will be performed as shown in the defined schedule.
For more information, please visit our community.

Firewall

● Upgrade available

▲ **Settings**

Upgrade policy ● Auto upgrade at Monday 02:00 UTC+8.0
○ Upgrade at 2023-03-29 14:00 UTC+8.0
○ Upgrade now
○ Ignore upgrade

Firmware type: Latest

What is this?

When your device have a newer firmware available and per device type schedule is selected, the administrators will receive an email notification 14 days in advance. The Nebula portal will display the next upcoming schedule based on your settings.
You can choose upgrade now, reschedule or ignore upgrade if you don't want to upgrade. If no action is taken, the upgrade will be performed as shown in the defined schedule.
For more information, please visit our community.

Mobile Router

● Upgrade available

▲ **Settings**

Upgrade policy ● Auto upgrade at Monday 02:00 UTC+8.0
○ Upgrade at 2023-03-29 14:00 UTC+8.0
○ Upgrade now
○ Ignore upgrade

Firmware type: Latest

What is this?

When your device have a newer firmware available and per device type schedule is selected, the administrators will receive an email notification 14 days in advance. The Nebula portal will display the next upcoming schedule based on your settings.
You can choose upgrade now, reschedule or ignore upgrade if you don't want to upgrade. If no action is taken, the upgrade will be performed as shown in the defined schedule.
For more information, please visit our community.

The following table describes the labels in this screen.

Table 33 Site-Wide > Configure > Firmware management > Overview

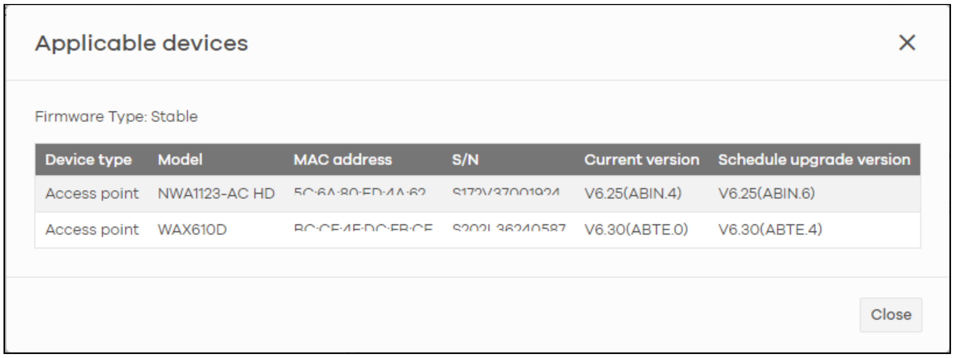
LABEL	DESCRIPTION
Access Point / Switch / Security router / Firewall or Security Gateway / Mobile Router	
Upgrade available	This shows the status of the Nebula Device's firmware in your site. • **Up to date** is displayed if all the Nebula Device(s) of a particular type (for example, all Switches) in 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 Device type | Model | MAC address | S/N | Current version | Schedule upgrade version Access point | NWA1123-AC HD | 5C:6A:80:ED:4A:62 | S172V37001924 | V6.25(ABIN.4) | V6.25(ABIN.6) Access point | WAX610D | BC:CF:4F:DC:FB:CE | S202L36240587 | V6.30(ABTE.0) | V6.30(ABTE.4) • **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.

Table 33 Site-Wide > Configure > Firmware management > Overview (continued)

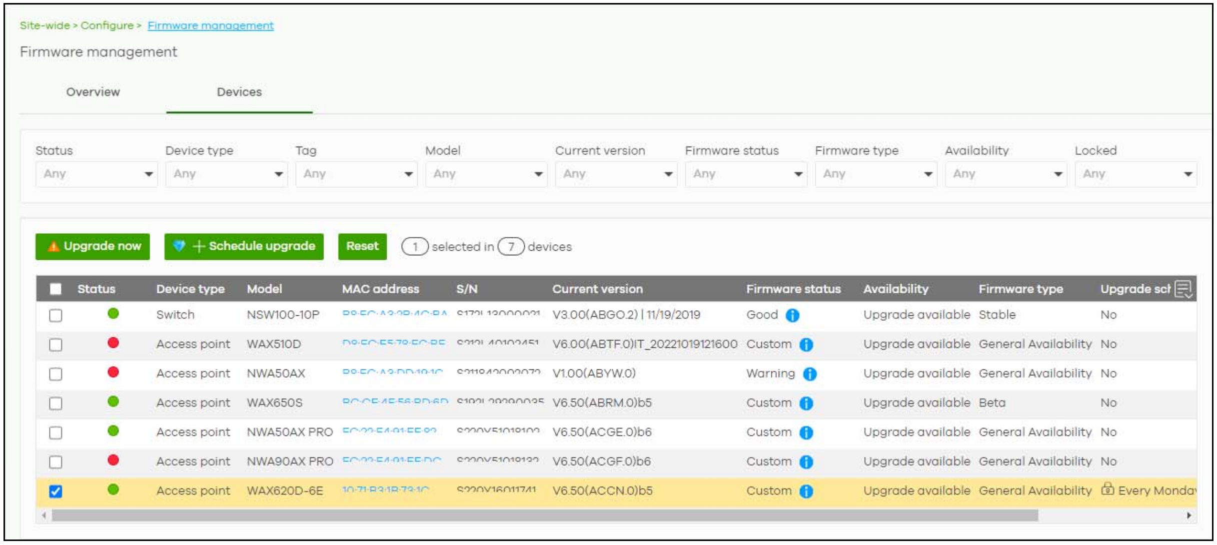
LABEL	DESCRIPTION
Settings	Create a schedule for each Nebula Device type. The following **Upgrade policy** are available: • Select **Auto upgrade at** to create a recurring schedule. With a recurring schedule, NCC will check and install the firmware when a new firmware release is available for each Nebula 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.

4.9.3.2 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 49 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 sc
☐	●	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	S192L20290035	V6.50(ABRM.0)b5	Custom	Upgrade available	Beta	No
☐	●	Access point	NWA50AX PRO	FC:22:F4:01:FF:82	S220Y51018102	V6.50(ACGE.0)b6	Custom	Upgrade available	General Availability	No
☐	●	Access point	NWA90AX PRO	FC:22:F4:01:FF: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	Every Monda

The following table describes the labels in this screen.

Table 34   Site-wide > Configure > Firmware management > Devices

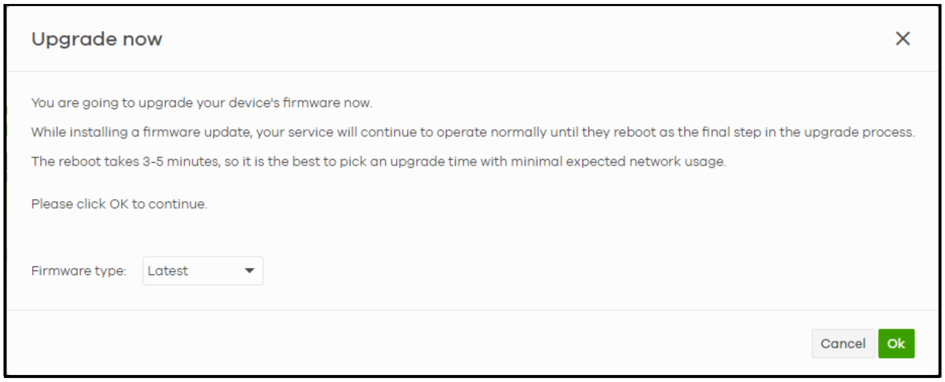
<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></tr>
<tr><td>Upgrade Now</td><td>

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 **Firmware type** to be installed.

- 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.



Upgrade now

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.

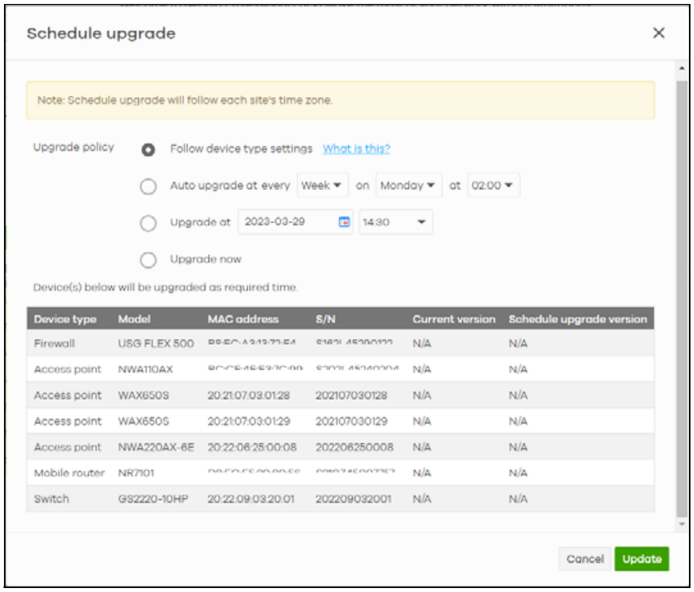
Firmware type: Latest

</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 side-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.

<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 34 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 firmware and no immediate action is required. The installed firmware does not have the latest features but provides the smoothest operation. 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.
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 34 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.

4.9.4 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.

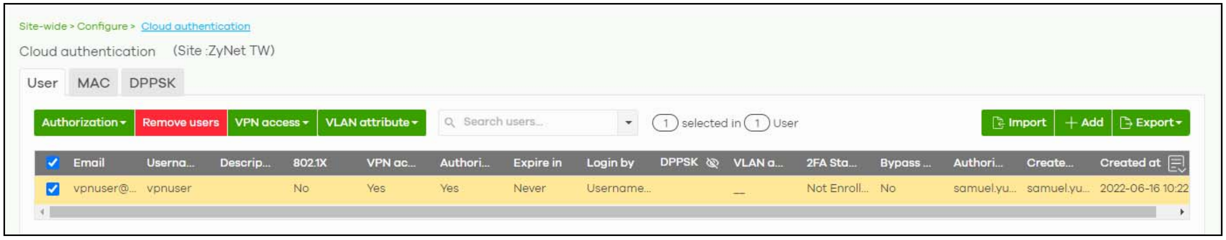
Note: The changes you made in this screen apply only to the current site. To change the cloud authentication settings for all sites in the organization, go to **Organization-wide** > **Organization-wide manage** > **Cloud Authentication** (see Section 4.9 on page 207).

Note: For more information on user account types, see Section 11.4.7.1 on page 541.

4.9.4.1 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 50 Site-wide > Configure > Cloud Authentication > User



Site-wide > Configure > Cloud authentication

Cloud authentication (Site :ZyNet TW)

☑	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 35 Site-wide > Configure > Cloud Authentication > User

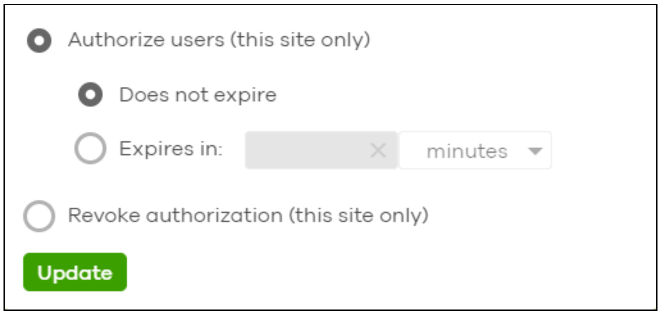
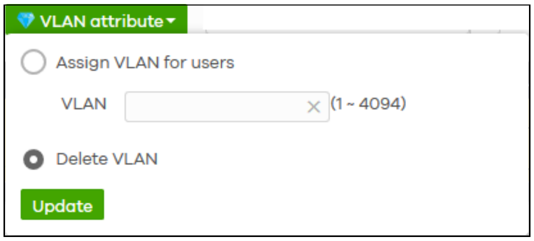
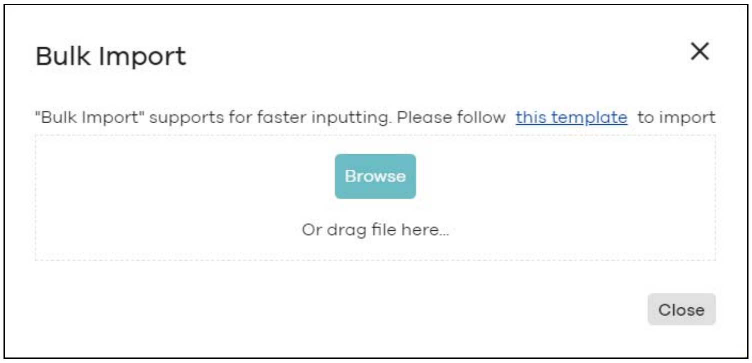
LABEL	DESCRIPTION
Authorization	Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (this site only) ● Does not expire ○ Expires in: minutes ○ Revoke authorization (this site only) Update
Remove users	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 4.9.4.2 on page 221.
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.

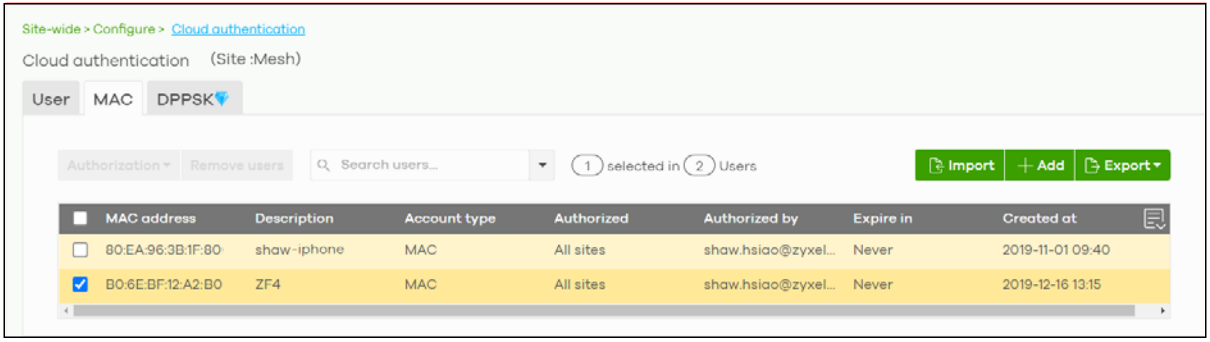
Table 35 Site-wide > Configure > Cloud Authentication > User (continued)

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.

4.9.4.2 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 51 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 36 Site-wide > Configure > Cloud Authentication > MAC

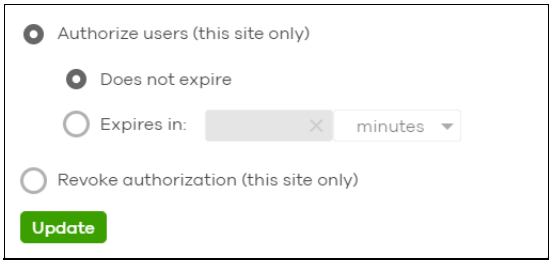
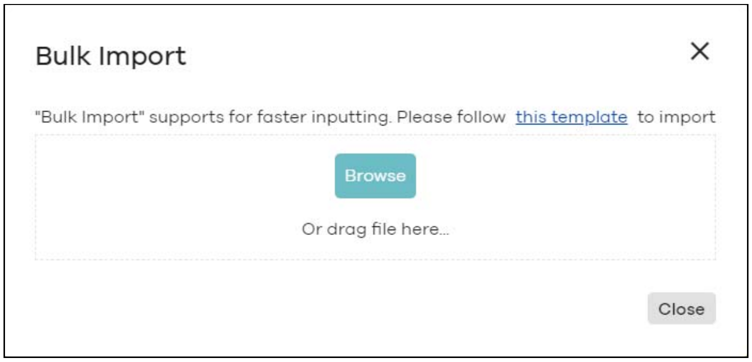
LABEL	DESCRIPTION
Authorization	Select one or more than one account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (this site only) ● Does not expire ○ Expires in: minutes ○ Revoke authorization (this site only) Update
Remove users	Select 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 4.9.4.3 on page 223.
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.

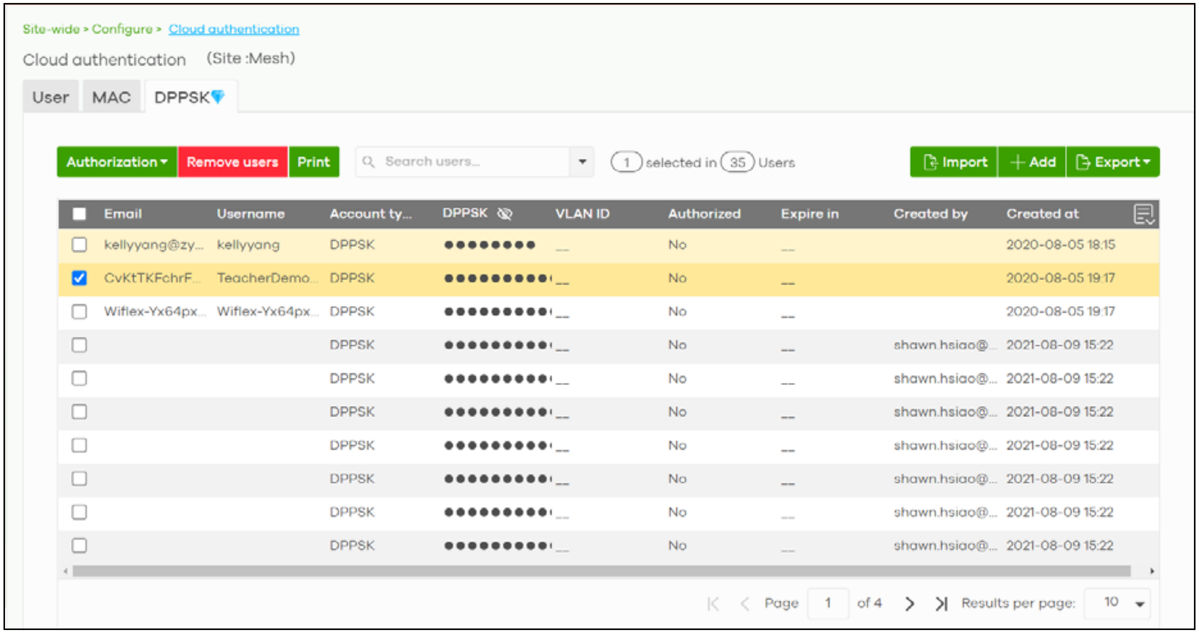
Table 36   Site-wide > Configure > Cloud Authentication > MAC (continued)

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.

4.9.4.3 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 52   Site-wide > Configure > Cloud Authentication > DPPSK



□	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

The following table describes the labels in this screen.

Table 37   Site-wide > Configure > Cloud Authentication > DPPSK

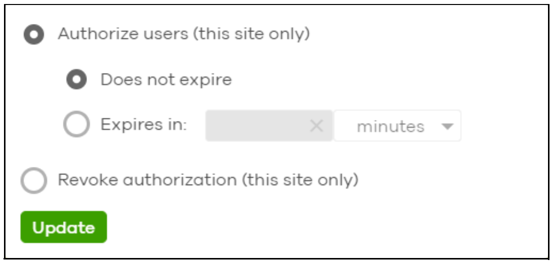
LABEL	DESCRIPTION
Authorization	Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (this site only) ● Does not expire ○ Expires in: minutes ○ Revoke authorization (this site only) Update
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.

Table 37 Site-wide > Configure > Cloud Authentication > DPPSK (continued)

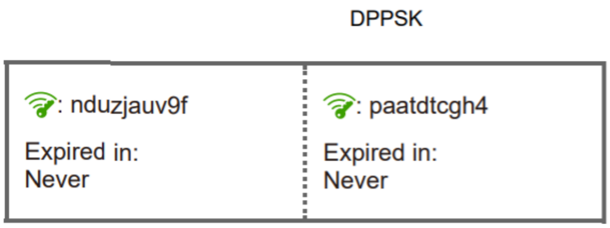
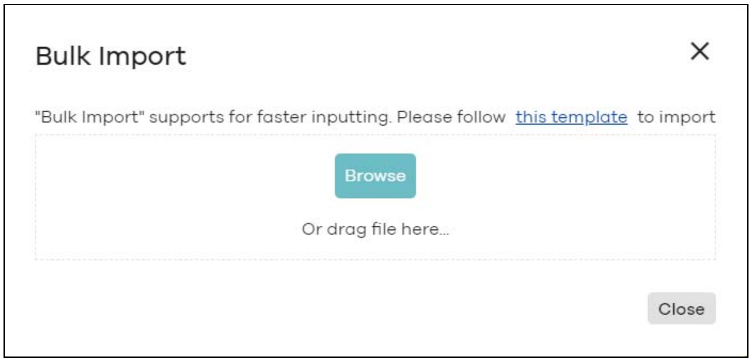
LABEL	DESCRIPTION
Print	Click this button to print the unique dynamic personal pre-shared key (DPPSK) and expiry time of each selected user account. The account details can be cut into cards, and then given to users in order to grant them WiFi network access.  DPPSK : nduzjauv9f Expired in: Never : paatdtcgh4 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 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 11.4.7.7 on page 550. • Batch create DPPSK: See Section 11.4.7.8 on page 551.
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 37 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.

4.9.5 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.

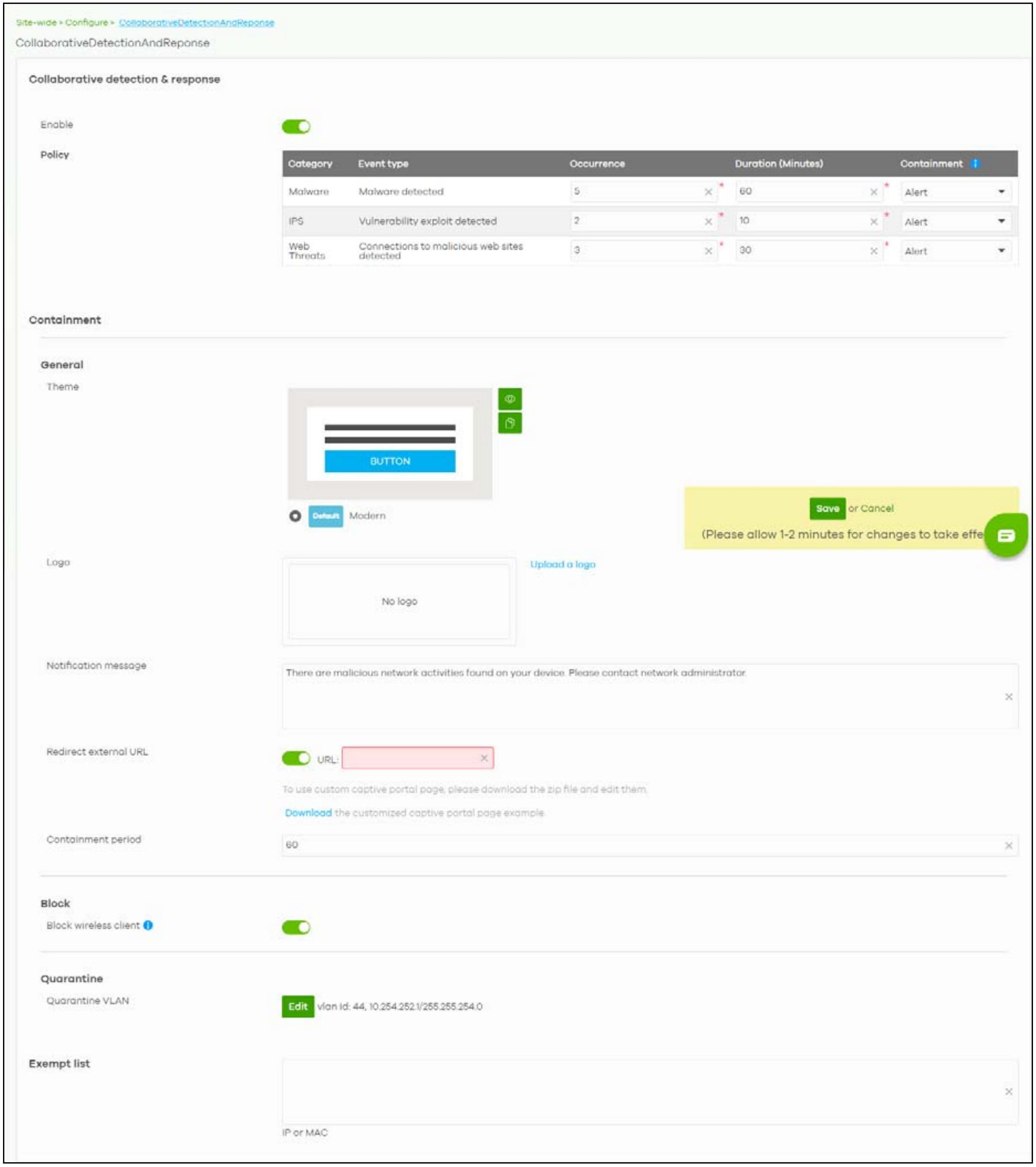
Note: To use the CDR feature, a Gold/UTM Security Pack license and a Nebula Pro Pack license is required.

The following table shows the CDR feature with/without a Gold/UTM Security Pack license.

Table 38 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 53 Site-wide > Configure > Collaborative Detection & Response



Site-wide > Configure > CollaborativeDetectionAndReponse

CollaborativeDetectionAndReponse

Collaborative detection & response

Enable

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

Upload a logo

Notification message

There are malicious network activities found on your device. Please contact network administrator.

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.

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

The following table describes the labels in this screen.

Table 39 Site-wide > Configure > Collaborative Detection & Response

LABEL	DESCRIPTION
Collaborative detection & response	
Enable	Select this check box 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 39 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 Filtering 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 39 Site-wide > Configure > Collaborative Detection & Response (continued)

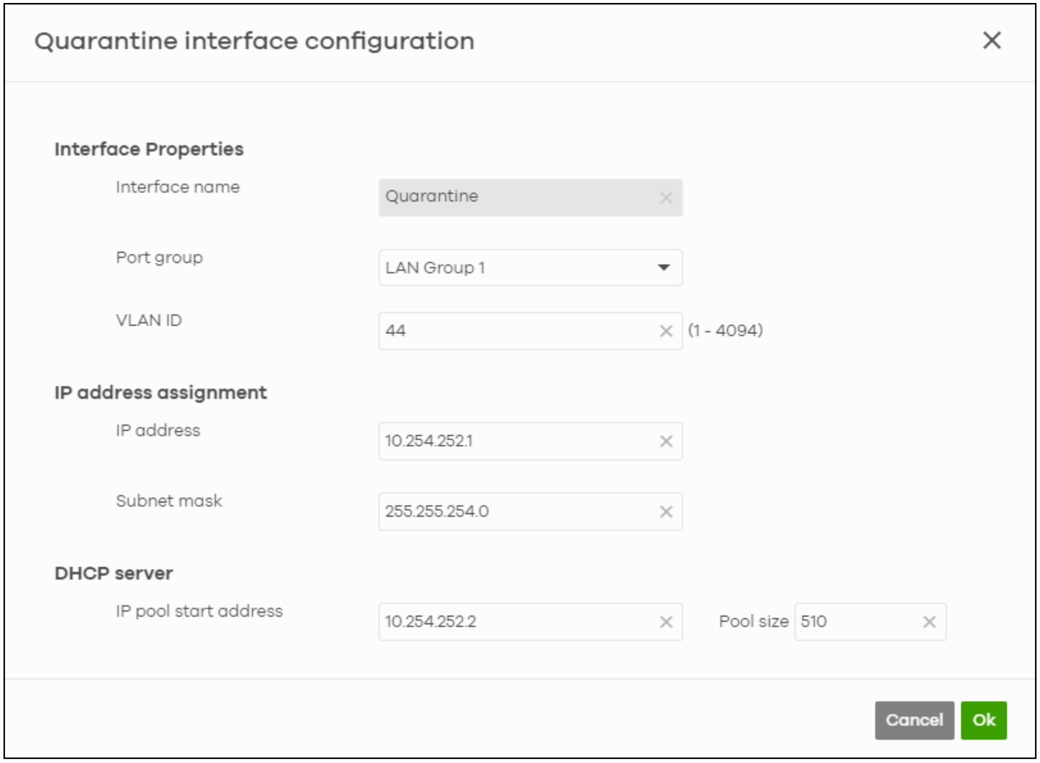
LABEL	DESCRIPTION
Quarantine	
Quarantine VLAN	Click **Set** to configure a VLAN in order to isolate traffic from suspect clients. Traffic from a suspect client is broadcast to all members in the VLAN.
Exempt list	Enter IPv4 and /or MAC addresses of client devices that are exempt from CDR checking.

4.9.6 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 54 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 40 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)

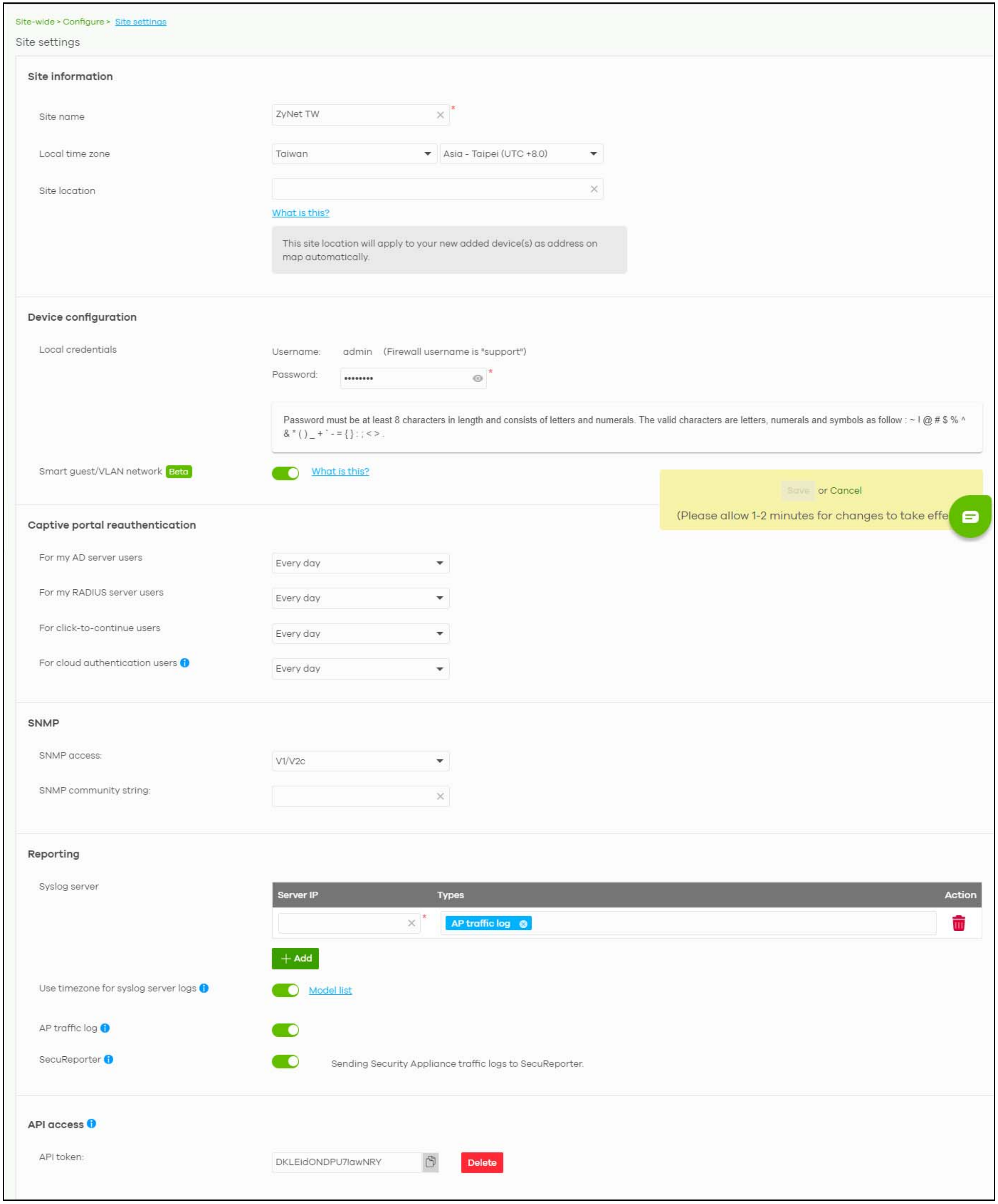
Table 40 Site-wide > Configure > Collaborative detection & response > Containment > Quarantine

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.

4.9.7 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 55 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 41 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 **Gateway 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. **Gateway traffic log** includes the traffic information (such as its source, destination or usage) of the Security Appliance clients.
Action	Click the **Delete** icon to remove the entry.

Table 41 Site-wide > Configure > Site settings (continued)

LABEL	DESCRIPTION
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 5.3.1 on page 247.
SecuReporter	Click **On** to enable this feature. This allows the NCC to send traffic logs to SecuReporter. 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.

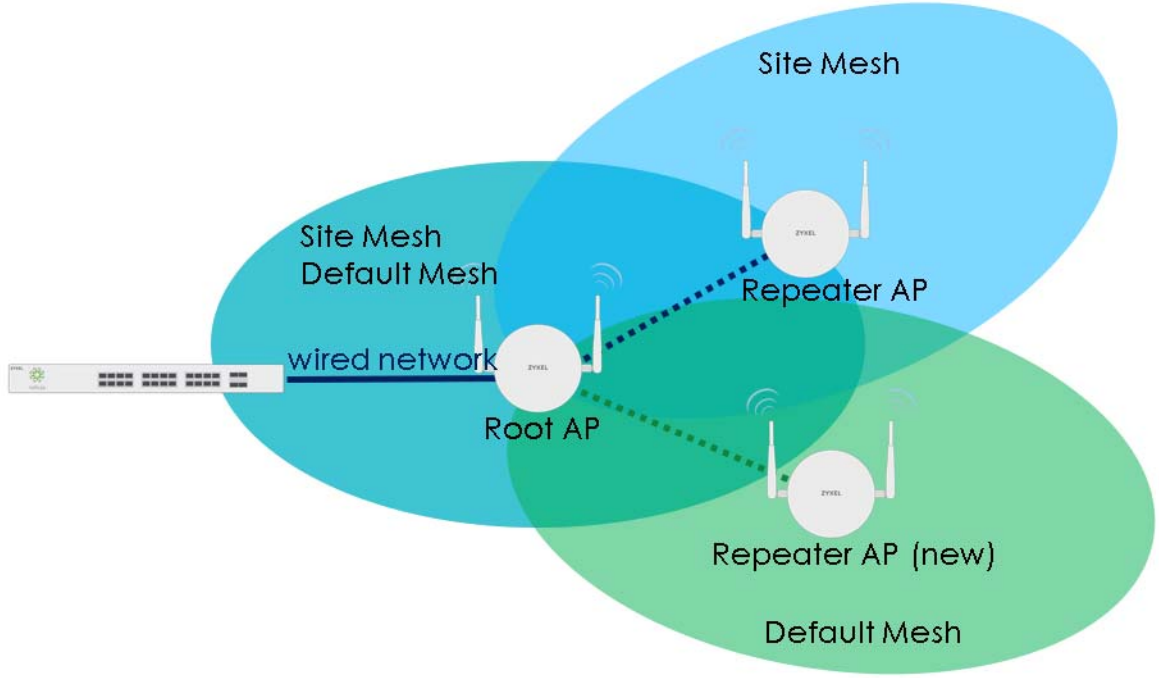
Table 42 Features/Fields Supported on Specific Nebula Devices Only

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 156 for more information.
Wired stations		
WPA3 in **Security options**	NWA110AX, WAX510D, WAX650S	Click **Site-wide** > **Configure** > **Access points** > **SSID advanced settings**. See Section 5.3.1 on page 247 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 274 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 56 Nebula Smart Mesh



Smart Mesh assigns a role to each Nebula Device depending on its connection method.

- **Root AP**: A Nebula Device (mesh controller) that is connected to the network by Ethernet and can reach the gateway device.
- **Repeater AP**: 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

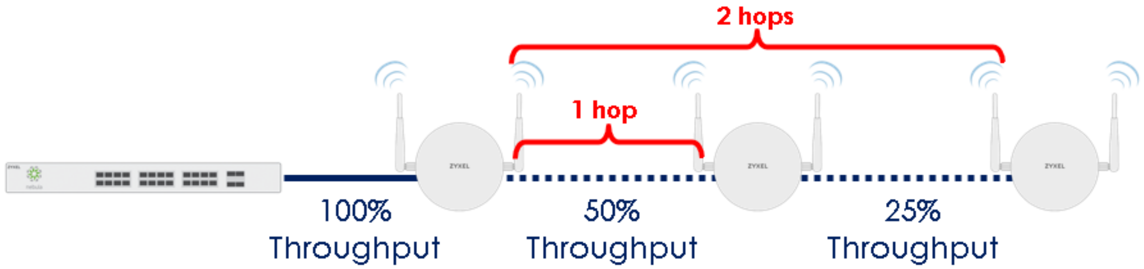
After you add a Nebula Device to an NCC site and then turn it on, the new Nebula Device automatically connects to a mesh network called the **default mesh**. The Nebula Device then tries to connect to a mesh controller and contact NCC. After the Nebula Device successfully contacts NCC and joins the site, 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 57 Nebula Smart Mesh Wireless Hops

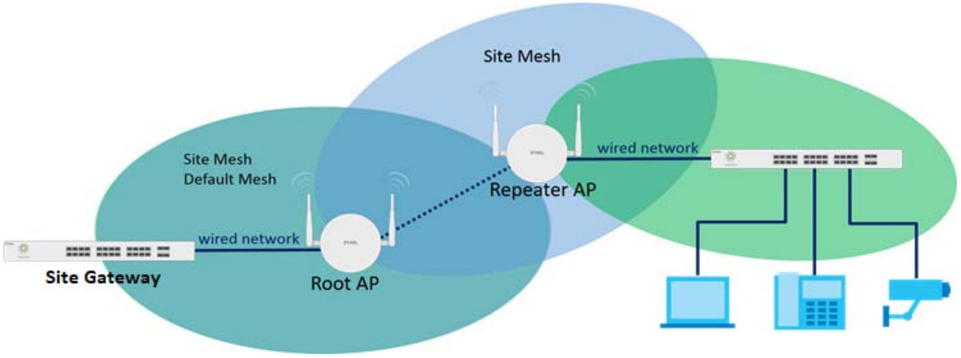


5.1.2.2 Wireless Bridge

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 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 through the Nebula Device's WiFi connection.

Figure 58 Nebula Smart Mesh Wireless Bridge



5.2 Monitor

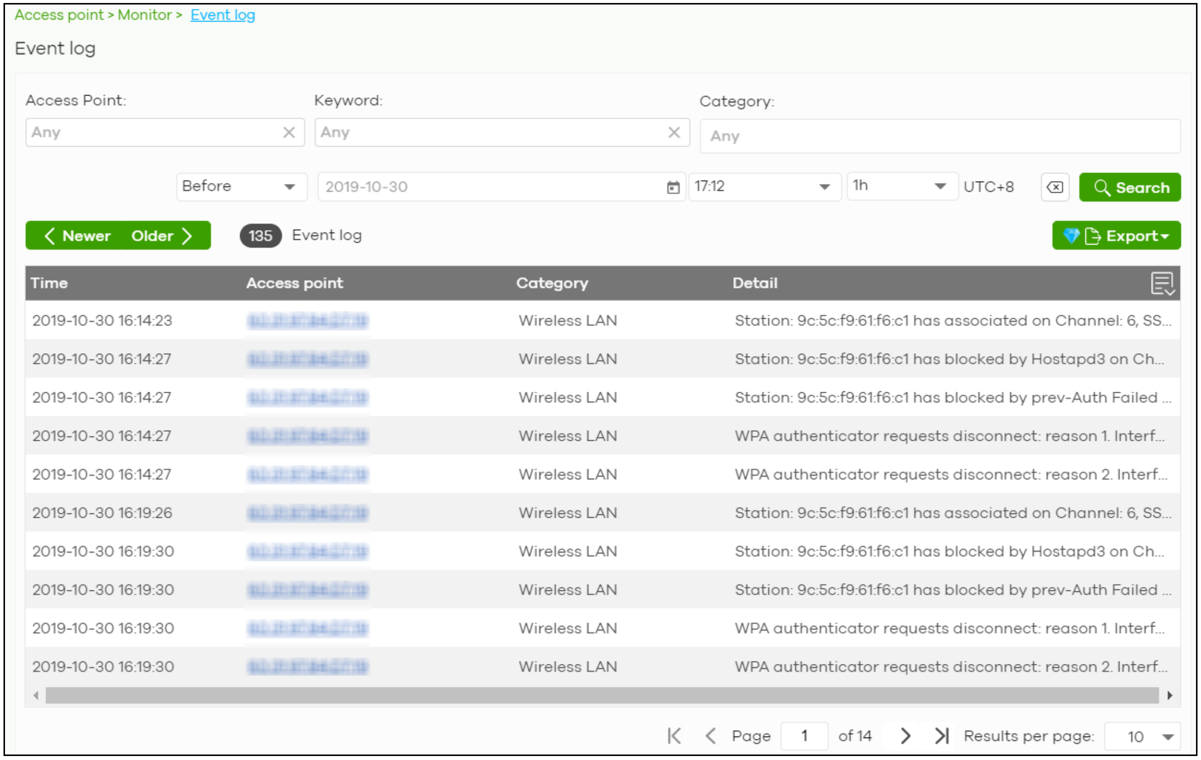
Use the **Monitor** menus to check Nebula Device event log messages and summary report for Nebula Devices in the selected site.

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 59 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.

Note: You can only enable voucher authentication for one SSID per site.

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 12.3.1 on page 538.

2. Go to **Site-wide** > **Configure** > **WiFi SSID**, select the SSID, and then under **Sign-in method** select **Voucher**. For details, see Section 12.3.2 on page 540.

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 239.

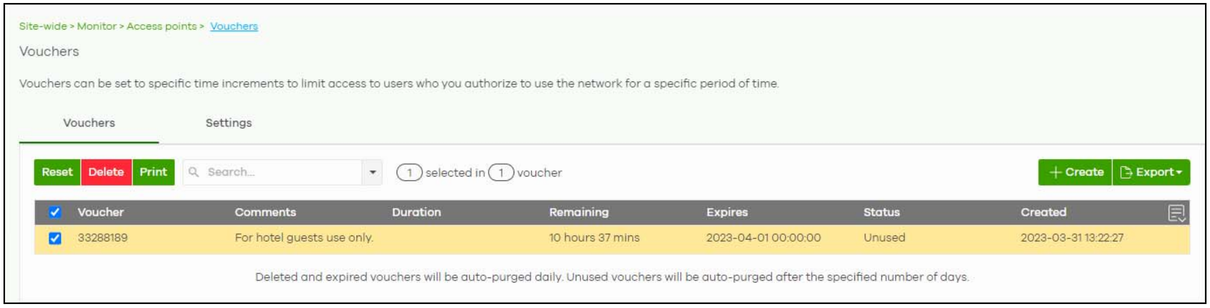
4. Go to **Site-wide** > **Monitor** > **Access points** > **Vouchers,** and then click **Create** to create one or more vouchers.

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 60 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 43 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. You can modify how vouchers look when printed at **Site-wide** > **Configure** > **General settings**.
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 238.
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.

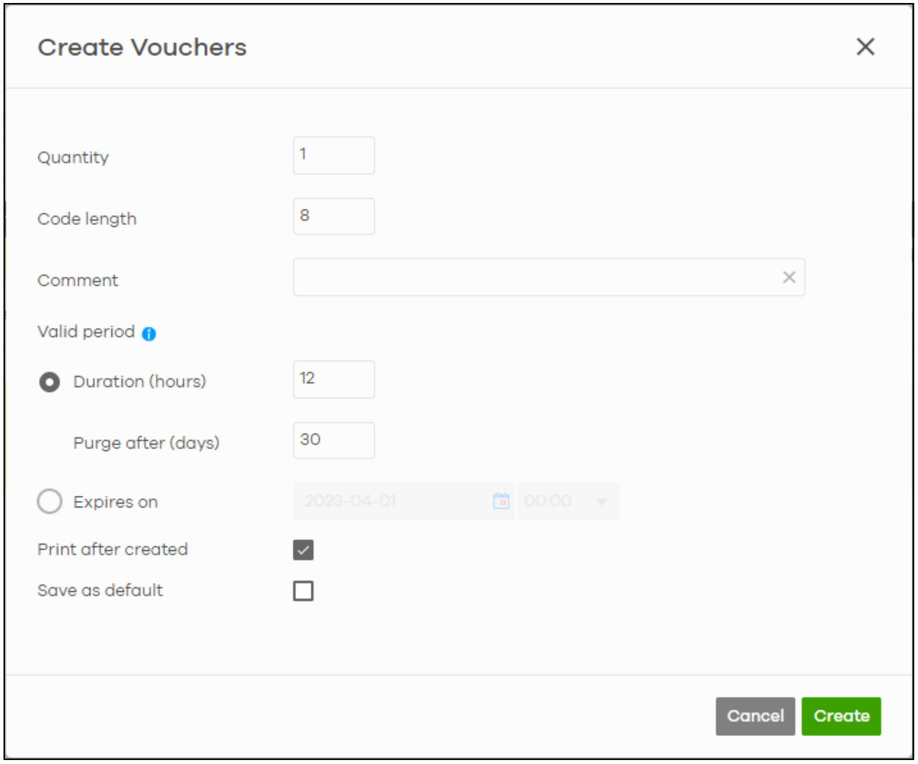
Table 43 Site-wide > Monitor > Vouchers (continued)

LABEL	DESCRIPTION
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 61 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 44 Site-wide > Monitor > Vouchers > Create

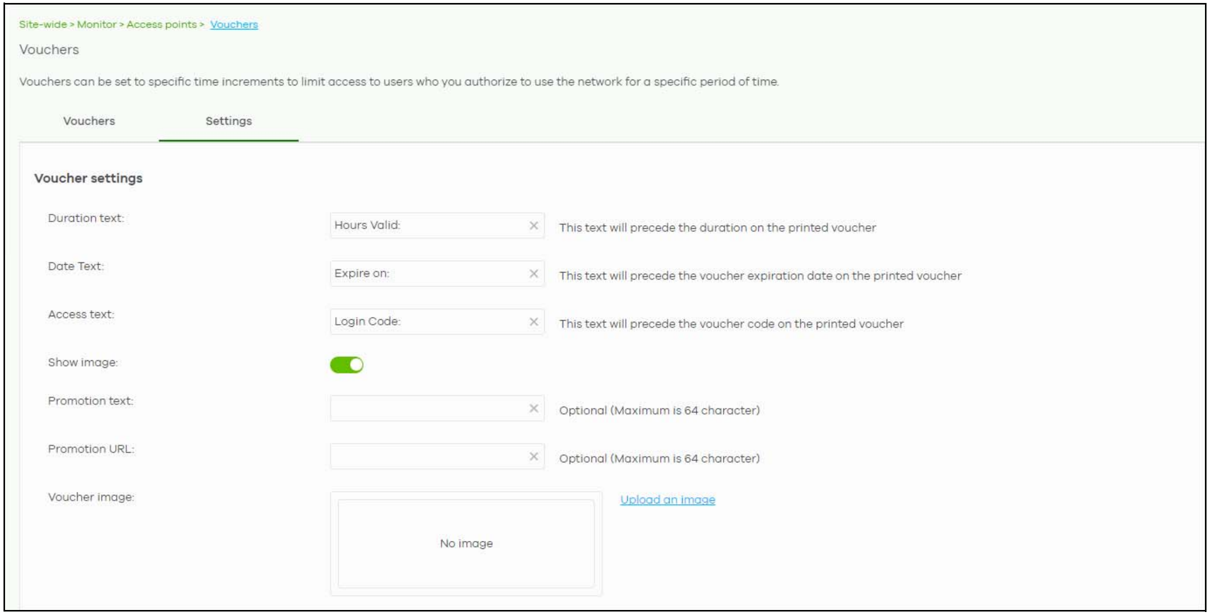
LABEL	DESCRIPTION
Quantity	Sets the number of vouchers you want to create. The valid range for this setting is 1 – 999.
Code length	Sets the length of the unique code on each voucher. The valid range for this setting is 6 – 10.
Comment	Enter information about the voucher that might be useful for other 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 1 – 72.
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**.
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 12.3.2 on page 540.

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 62 Site-wide > Monitor > Access points > Voucher > Settings



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 settings

Duration text: Hours Valid: — This text will precede the duration on the printed voucher

Date Text: Expire 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: ●

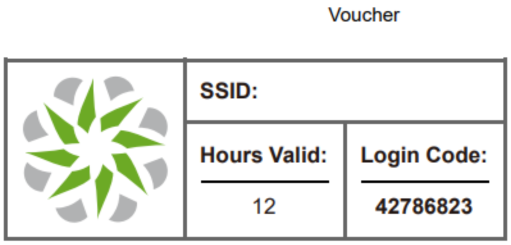
Promotion text: — Optional (Maximum is 64 character)

Promotion URL: — Optional (Maximum is 64 character)

Voucher image: No image — Upload an image

The following table describes the labels in this screen.

Table 45 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 236.
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.
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

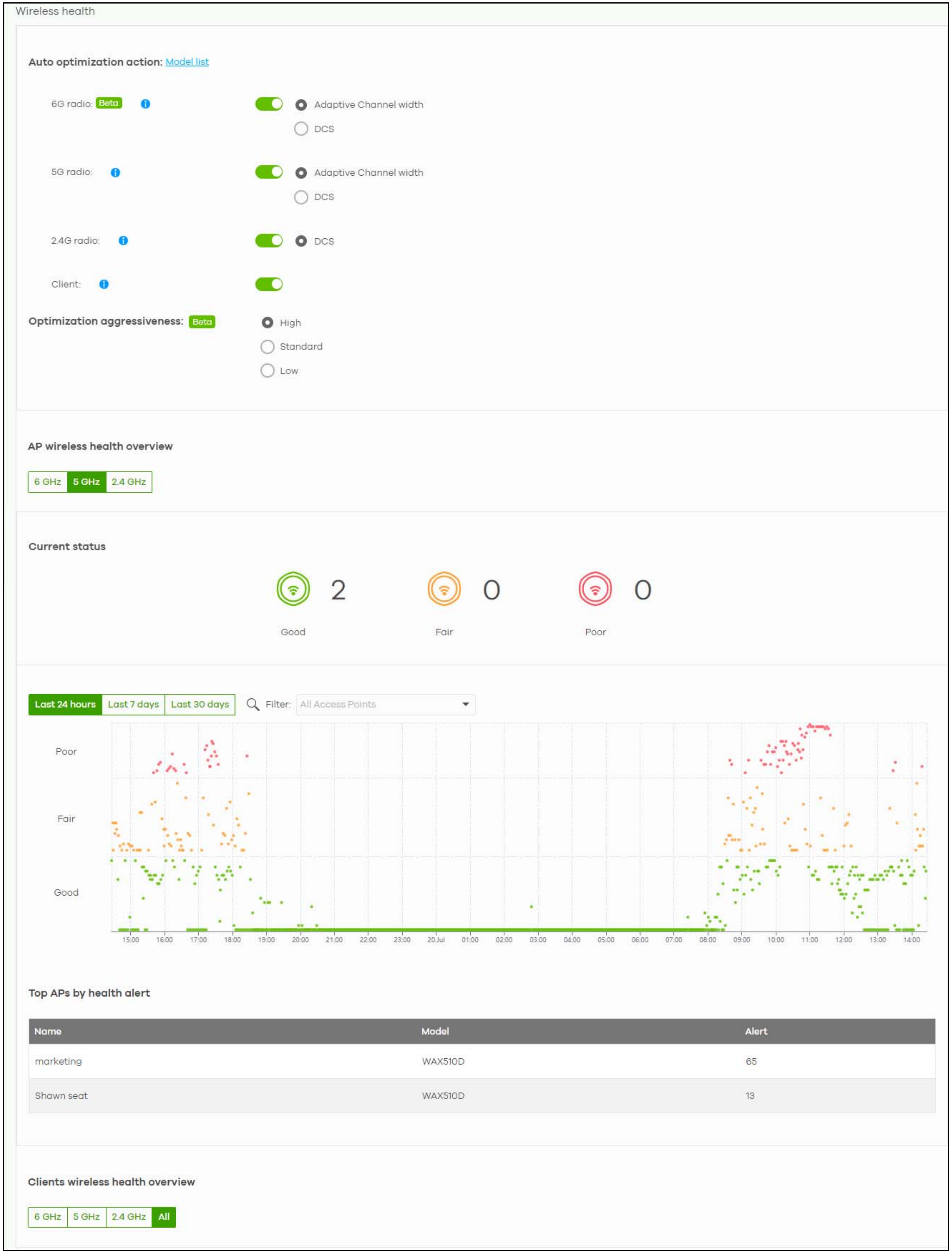
This screen lets you monitor the health of WiFi networks for your Nebula Devices and connected WiFi clients.

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 63 Site-wide > Monitor > Access points > Wireless health



Wireless health

Auto optimization action: Model list

6G radio: Beta — ● Adaptive Channel width ○ DCS

5G radio: — ● Adaptive Channel width ○ DCS

2.4G radio: — ● DCS

Client:

Optimization aggressiveness: Beta — ● High ○ Standard ○ Low

AP wireless health overview

6 GHz | **5 GHz** | 2.4 GHz

Current status

Good	Fair	Poor
2	0	0

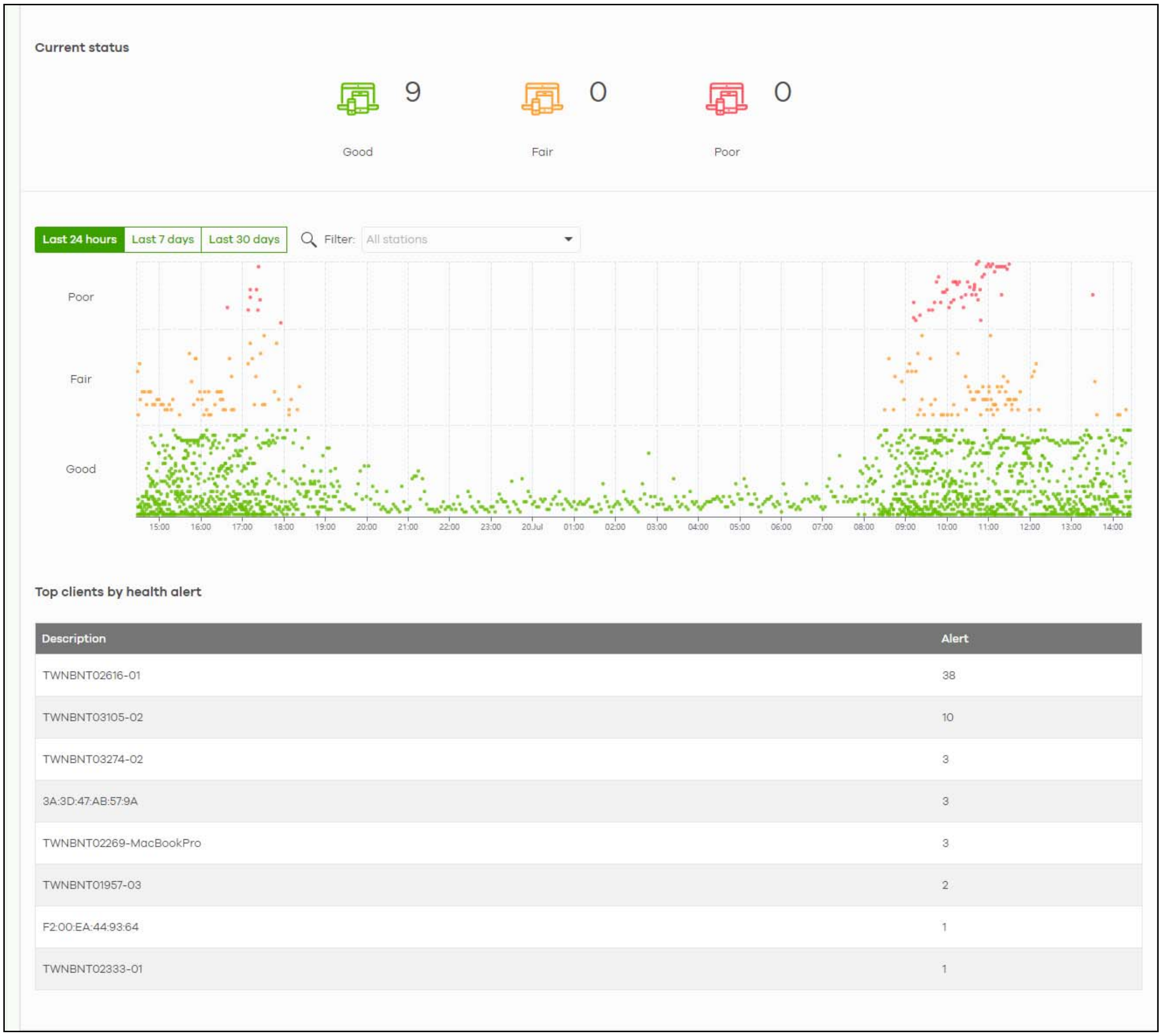
Last 24 hours | Last 7 days | Last 30 days — Filter: All Access Points

Top APs by health alert

Name	Model	Alert
marketing	WAX510D	65
Shawn seat	WAX510D	13

Clients wireless health overview

6 GHz | 5 GHz | 2.4 GHz | **All**



Current status

9	0	0
Good	Fair	Poor

Top clients by health alert

Description	Alert
TWNBNT02616-01	38
TWNBNT03105-02	10
TWNBNT03274-02	3
3A:3D:47:AB:57:9A	3
TWNBNT02269-MacBookPro	3
TWNBNT01957-03	2
F2:00:EA:44:93:64	1
TWNBNT02333-01	1

The following table describes the labels in this screen.

Table 46 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.

Table 46 Site-wide > Monitor > Access points > Wireless health (continued)

LABEL	DESCRIPTION
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 Move the cursor over the information icon to view the supported Nebula Device model list.	
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.
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.

Table 46 Site-wide > Monitor > Access points > Wireless health (continued)

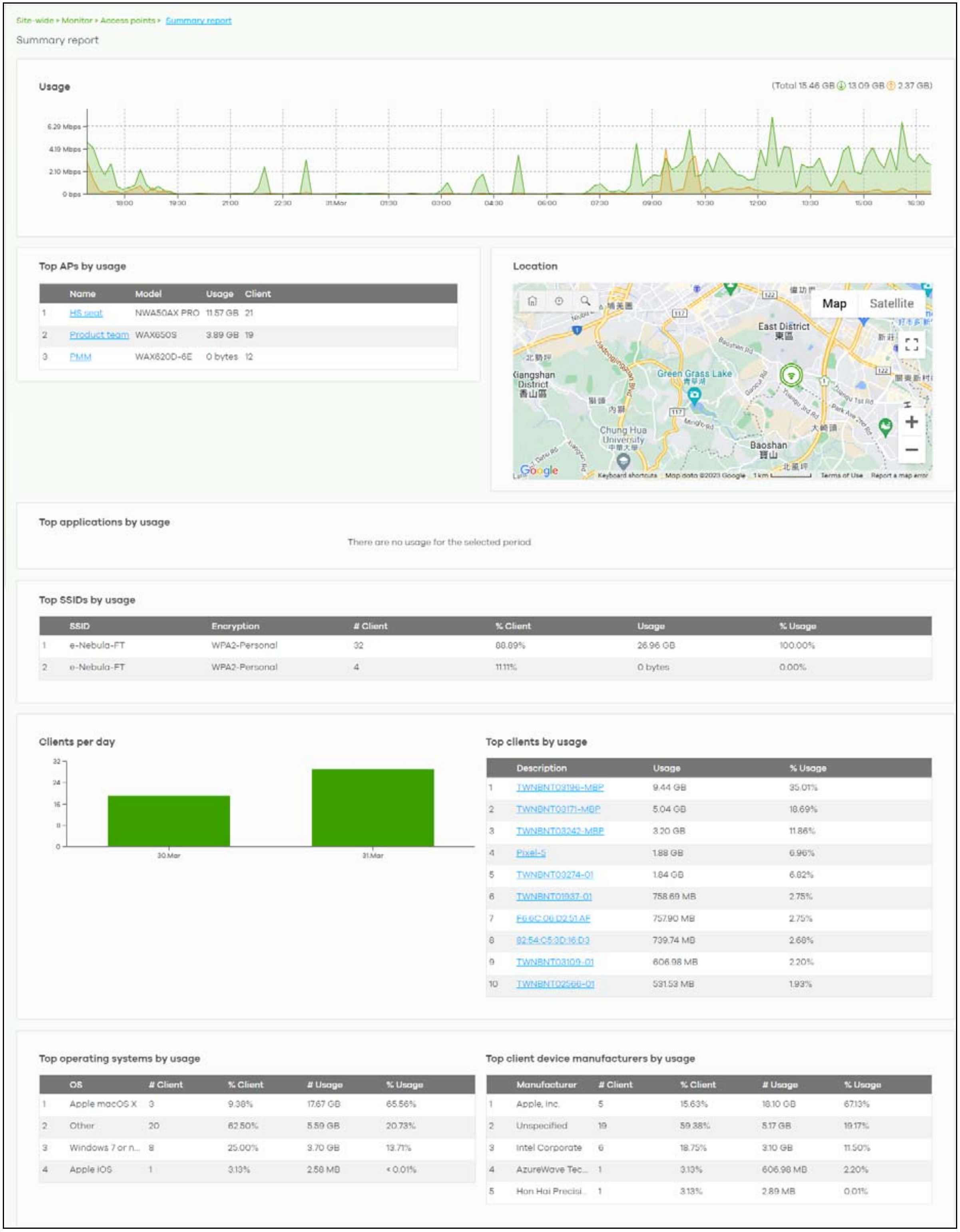
LABEL	DESCRIPTION
Client health	Select to view the health of all WiFi clients which are connected to the supported Nebula Devices using the 6 GHz, 5 GHz or 2.4 GHz band. You can select to view the health report for the past day, week or month, as well as filter the WiFi station to view.
y-axis	The y-axis 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 64 Site-wide > Monitor > Access points > Summary report



Site-wide > Monitor > Access points > Summary report

Summary report

Usage

(Total 15.46 GB ⬇ 13.09 GB ⬆ 2.37 GB)

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

Location

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%

Clients per day

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 47 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 47 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

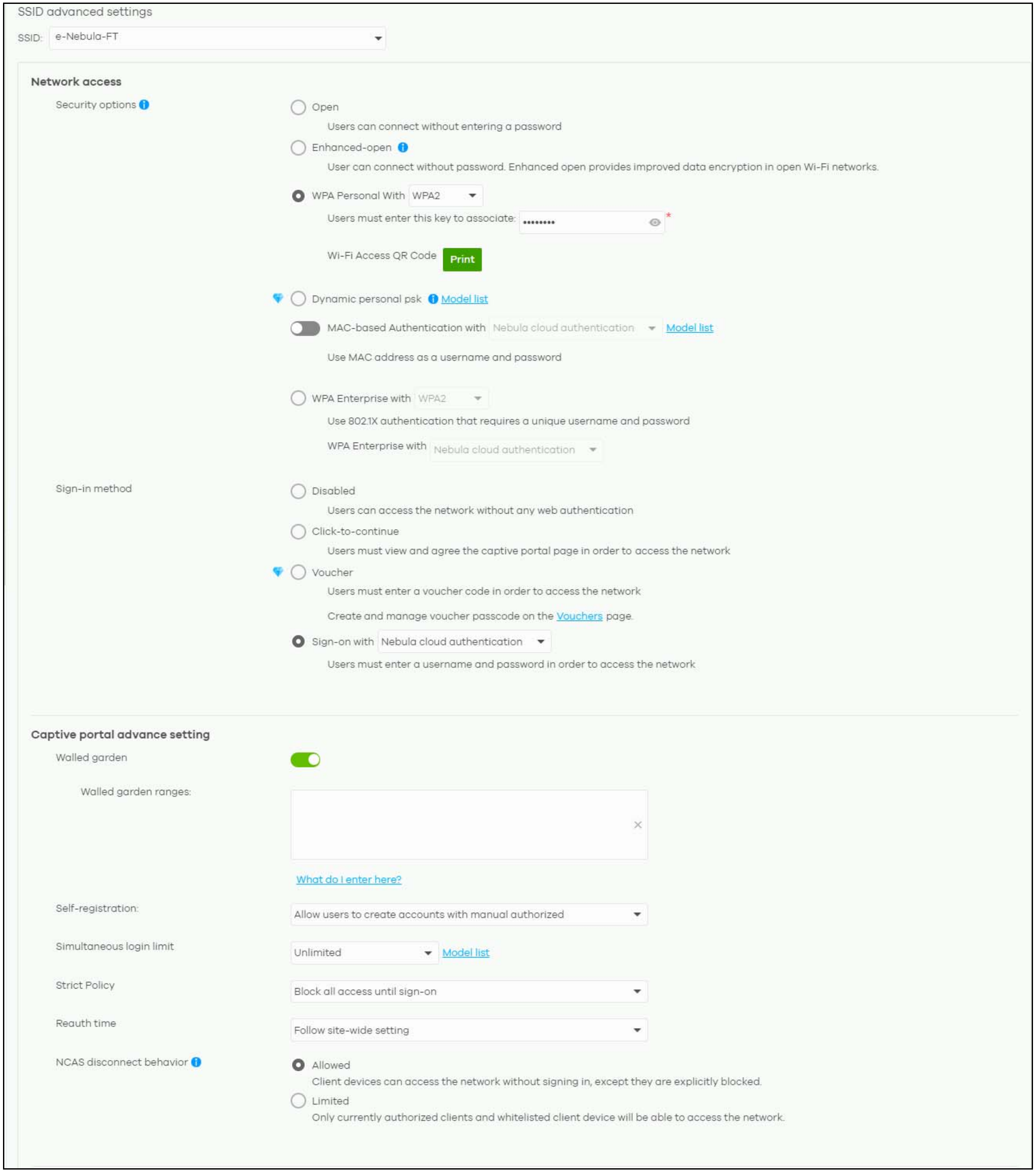
Use the **Configure** menus to set the WiFi security settings for Nebula Devices of the selected site.

5.3.1 SSID Advanced Settings

Use this screen to configure the WiFi security, L2 isolation, intra-BSS traffic blocking and walled garden settings for the SSID profiles.

Click **Site-wide** > **Configure** > **Access points** > **SSID advanced settings** to access this screen.

Figure 65 Site-wide > Configure > Access points > SSID advanced settings Part 1



SSID advanced settings

SSID: e-Nebula-FT

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

○ Dynamic personal psk

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 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 Nebula cloud authentication
Users must enter a username and password in order to access the network

Captive portal advance setting

Walled garden

Walled garden ranges:

Self-registration: Allow users to create accounts with manual authorized

Simultaneous login limit Unlimited

Strict Policy Block all access until sign-on

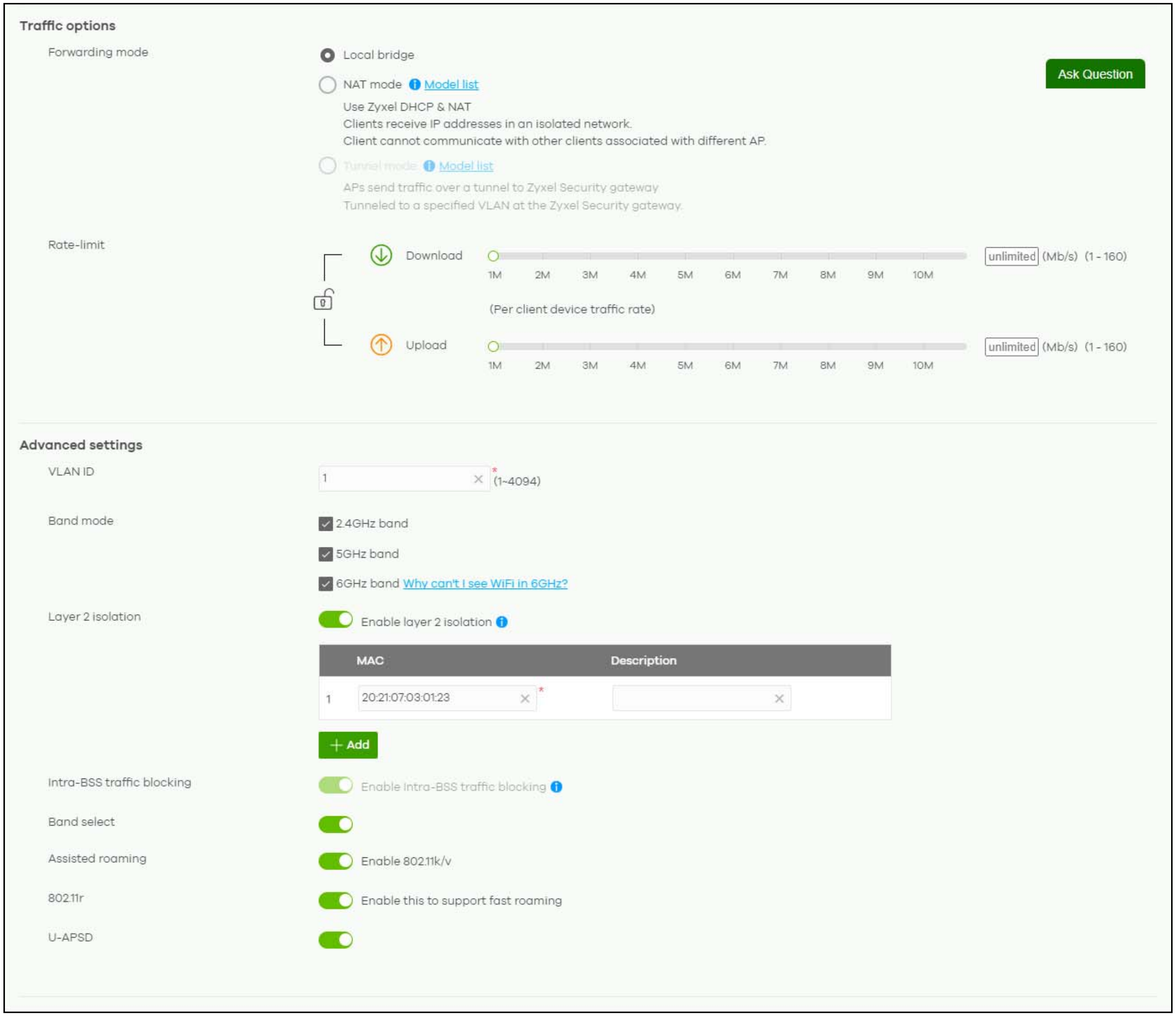
Reauth time Follow site-wide setting

NCAS disconnect behavior

● Allowed
Client devices can access the network without signing in, except they are explicitly blocked.

○ Limited
Only currently authorized clients and whitelisted client device will be able to access the network.

Figure 66 Site-wide > Configure > Access points > SSID advanced settings Part 2



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

☑ 2.4GHz band

☑ 5GHz band

☑ 6GHz band Why can't I see WiFi in 6GHz?

Layer 2 isolation — Enable layer 2 isolation

	MAC	Description
1	20:21:07:03:01:23	

+ Add

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

The following table describes the labels in this screen.

Table 48 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.
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 555.

Table 48 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 64 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. 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 11.4.7.3 on page 544. • For details on creating organization DPPSK users, see Section 4.9 on page 207. 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 48 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 236. Note: Vouchers cannot be enabled if Dynamic Personal Pre-Shared Key (DPPSK) or WPA Enterprise are enabled. You can only enable voucher authentication for one SSID per site. 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. • select **Facebook Wi-Fi** to let users check in to a business on Facebook for free Internet access after connecting to the Nebula Device's WiFi network. Users then have the option to like the Facebook fan page. You should already have set up a Facebook fan page associated with the business location. Click **here** to open the Facebook WiFi configuration screen in a new window, where you can select the Facebook Page associated with your location and configure bypass mode and session length.

Table 48 Site-wide > Configure > Access points > SSID advanced settings (continued)

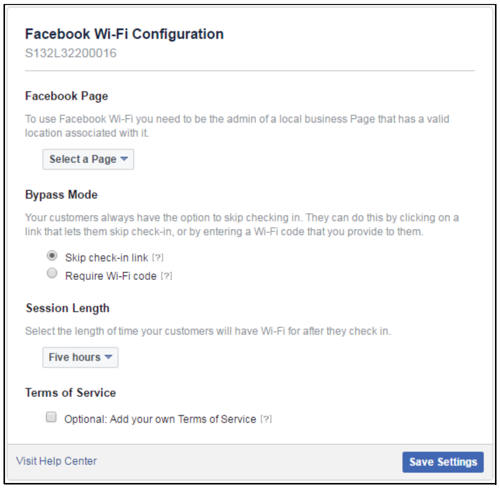
LABEL	DESCRIPTION
Sign-in method (continued)	 Facebook Wi-Fi Configuration S132L32200016 Facebook Page To use Facebook Wi-Fi you need to be the admin of a local business Page that has a valid location associated with it. Select a Page ▾ Bypass Mode Your customers always have the option to skip checking in. They can do this by clicking on a link that lets them skip check-in, or by entering a Wi-Fi code that you provide to them. ● Skip check-in link [?] ○ Require Wi-Fi code [?] Session Length Select the length of time your customers will have Wi-Fi for after they check in. Five hours ▾ Terms of Service □ Optional: Add your own Terms of Service [?] Visit Help Center Save Settings Note: When the NCC license of the organization expires, the SSID configured with Facebook WiFi will be disabled automatically. To enable the SSID again, change its authentication method or register with a new license key.
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. 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	If the RADIUS server requires the Nebula Device to provide the Network Access Server identifier attribute with a specific value, enter it here.
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.

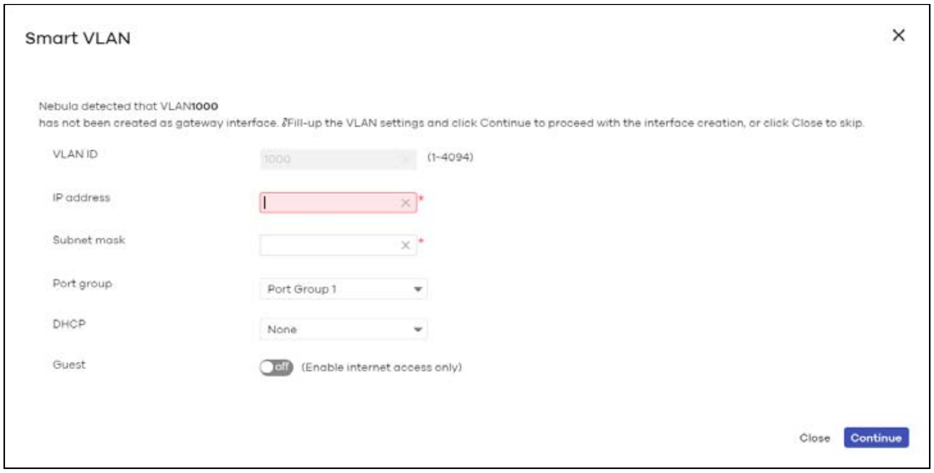
Table 48 Site-wide > Configure > Access points > SSID advanced settings (continued)

LABEL	DESCRIPTION
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.
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	

Table 48 Site-wide > Configure > Access points > SSID advanced settings (continued)

LABEL	DESCRIPTION
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.
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	

Table 48 Site-wide > Configure > Access points > SSID advanced settings (continued)

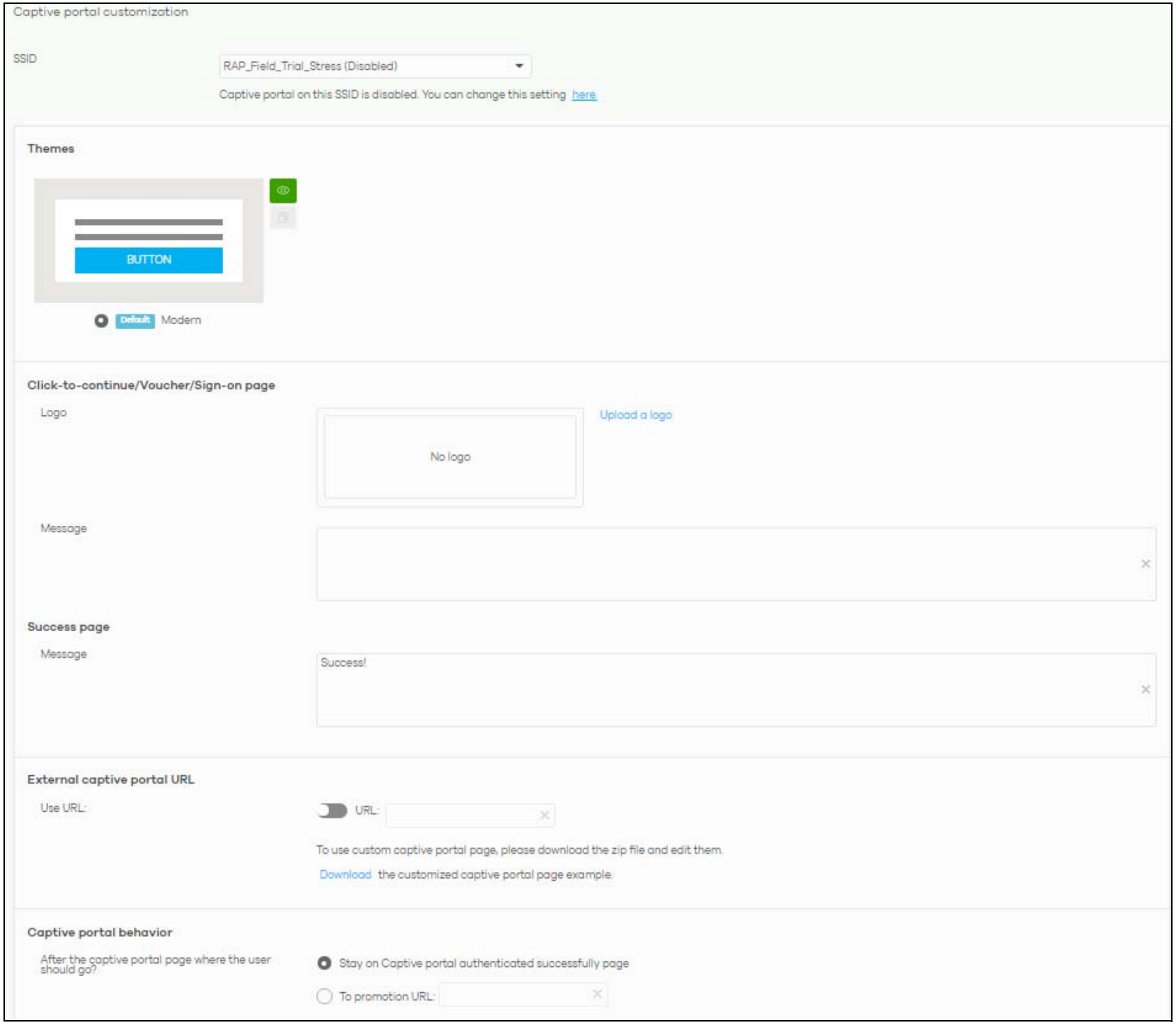
LABEL	DESCRIPTION
VLAN ID	Enter the ID number of the VLAN to which the SSID belongs. Note: If you have a Nebula Security Appliance installed in the site but did not configure an identical VLAN interface on the gateway, **Smart Guest/VLAN network tip, click here**. displays. Click **here** to open a screen 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.
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: 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 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.

5.3.2 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.

Click **Site-wide** > **Configure** > **Access points** > **Captive portal customization** to access this screen.

Figure 67 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

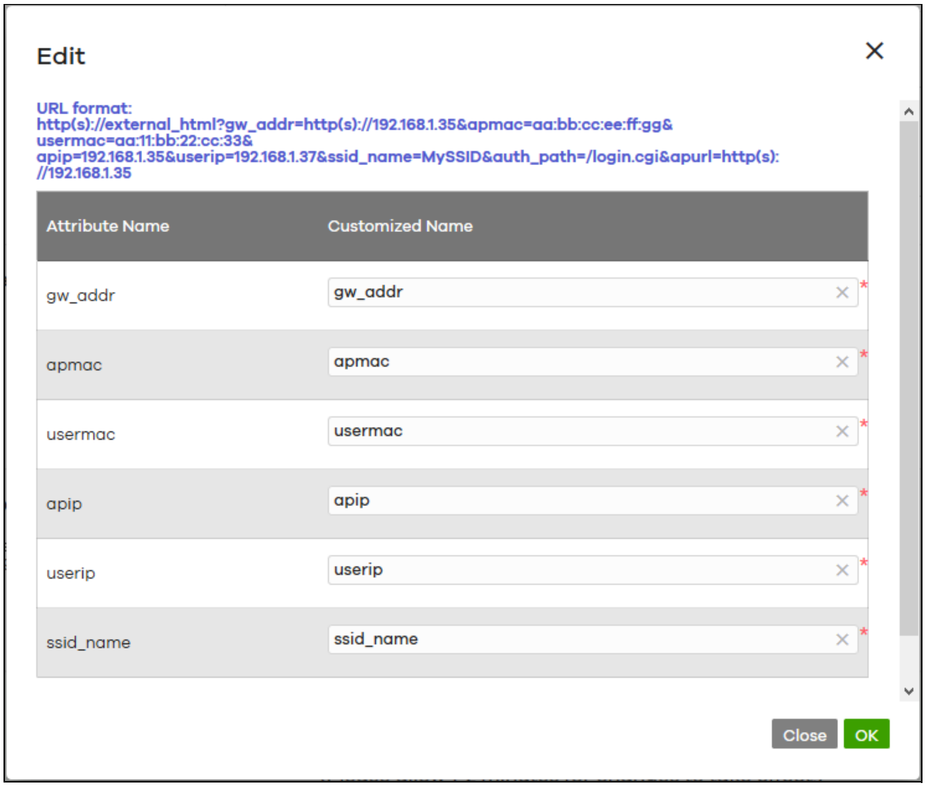
○ To promotion URL:

The following table describes the labels in this screen.

Table 49 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 5.3.2.1 on page 258. • 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	

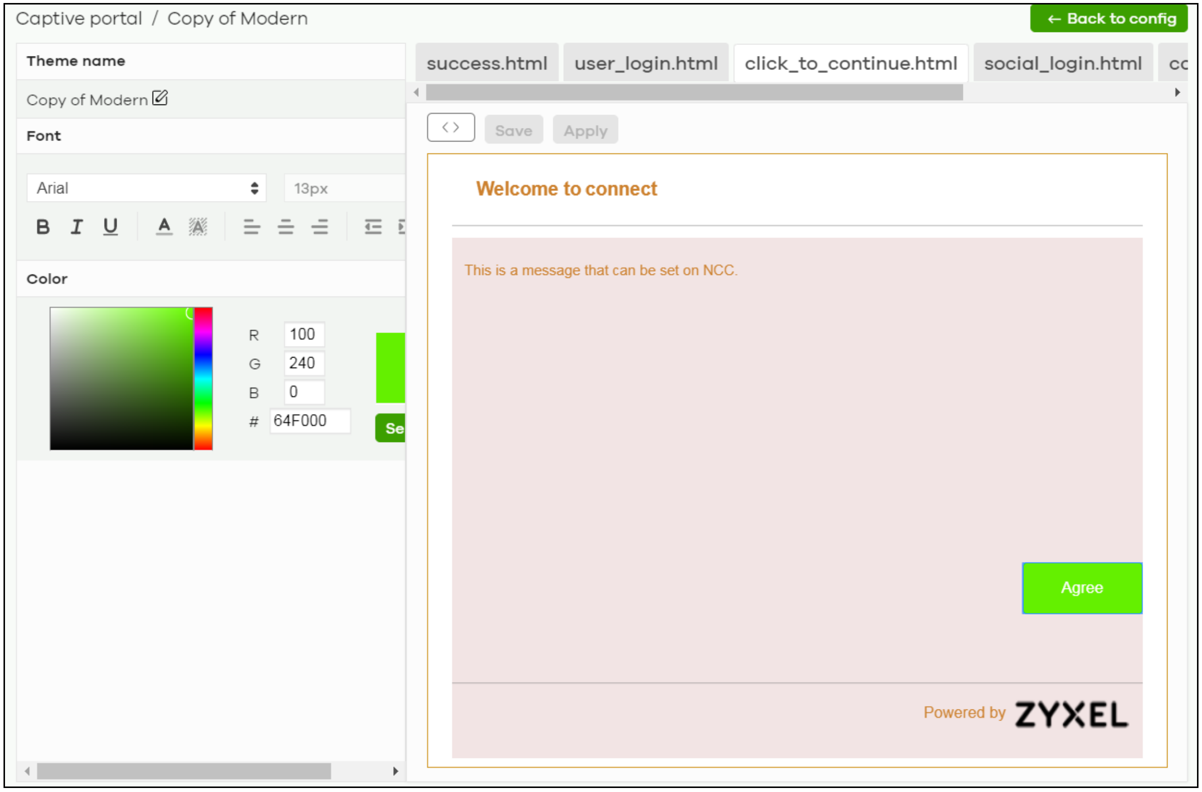
Table 49 Site-wide > Configure > Access points > Captive portal customization (continued)

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
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**.

5.3.2.1 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 68 Site-wide > Configure > Access points > Captive portal: Edit



Theme name

Copy of Modern

Font

Arial 13px

Color

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.

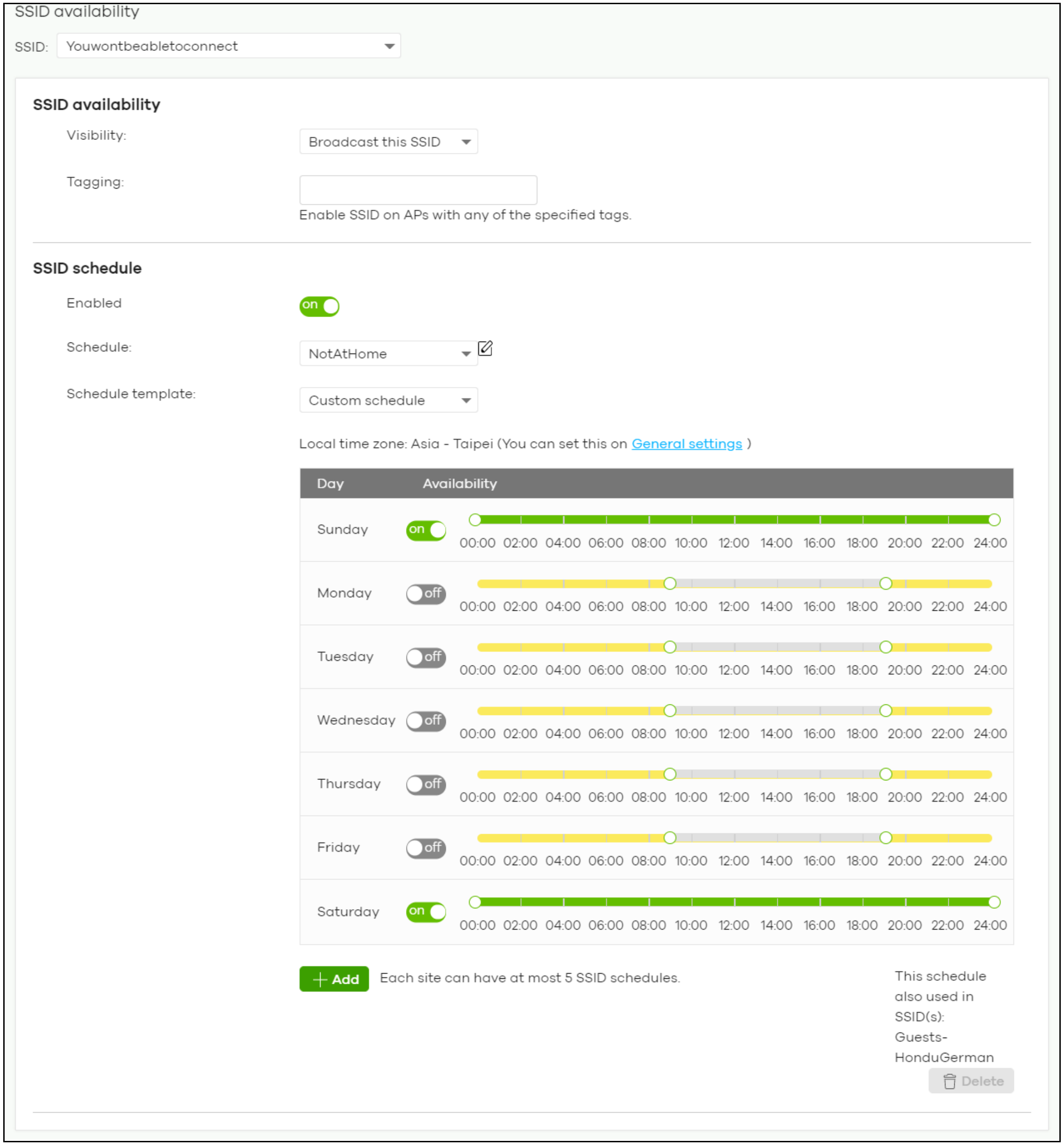
Table 50 Site-wide > Configure > Access points > Captive portal: Edit

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.

5.3.3 SSID Availability

Use this screen to configure SSID availability and the schedules which can be applied to the SSIDs. The SSID is enabled or disabled at the specified time. Click **Site-wide** > **Configure** > **Access points** > **SSID availability** to access this screen.

Figure 69 Site-wide > Configure > Access points > SSID availability



SSID availability

SSID: Youwontbeabletoconnect

SSID availability

Visibility: Broadcast this SSID

Tagging:

Enable SSID on APs with any of the specified tags.

SSID schedule

Enabled: on

Schedule: NotAtHome

Schedule template: Custom schedule

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

Day	Availability
Sunday	on
Monday	off
Tuesday	off
Wednesday	off
Thursday	off
Friday	off
Saturday	on

+ Add Each site can have at most 5 SSID schedules.

This schedule also used in SSID(s): Guests-HonduGerman

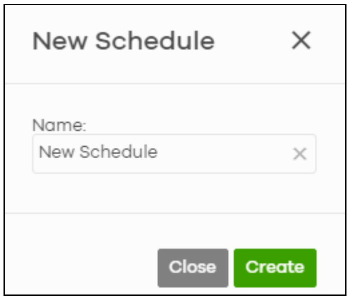
Delete

The following table describes the labels in this screen.

Table 51 Site-wide > Configure > Access points > SSID availability

LABEL	DESCRIPTION
SSID	Select the SSID profile to which the settings you configure here is applied.
SSID availability	

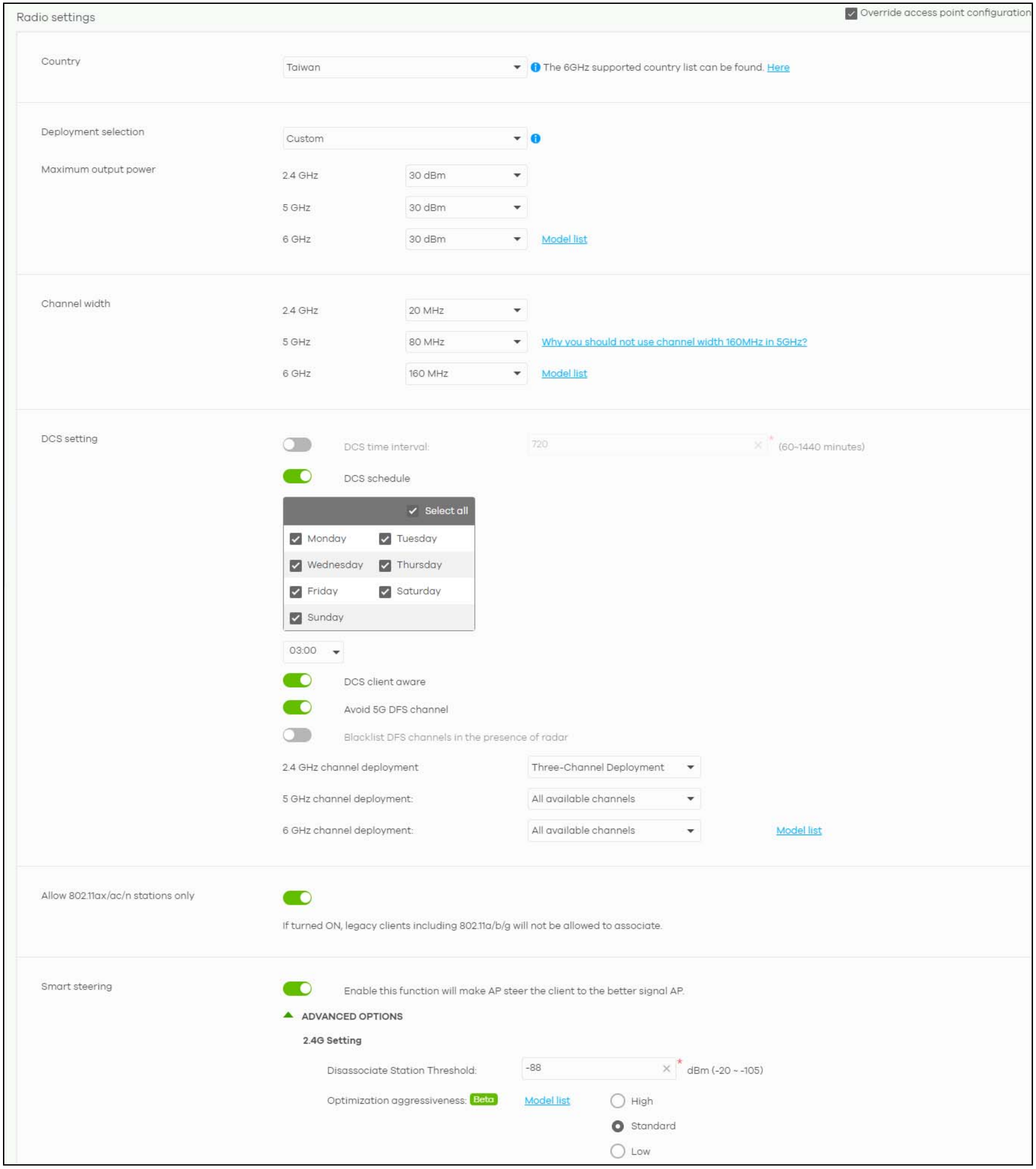
Table 51 Site-wide > Configure > Access points > SSID availability (continued)

LABEL	DESCRIPTION
Visibility	Select **Hide this SSID** 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. Not all WiFi clients respect this flag and display it anyway. Otherwise, select **Broadcast this SSID**. 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 (these vary by client, client connectivity software, and operating system).
Tagging	Enter the tags you created for Nebula Devices in the **Site-wide** > **Devices** > **Access points** screen. The SSID profile will only be applied to Nebula Devices with the specified tag. If you leave this field blank, this SSID profile will be applied to all Nebula Devices in the site.
SSID schedule	
Enabled	Click **On** 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 **On** to enable the SSID at the specified time on this day. Otherwise, select **Off** 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.

5.3.4 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 70 Site-wide > Configure > Access points > Radio settings



Radio settings ☑ Override access point configuration

Country: Taiwan ▾ — The 6GHz 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 160MHz in 5GHz?
- 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

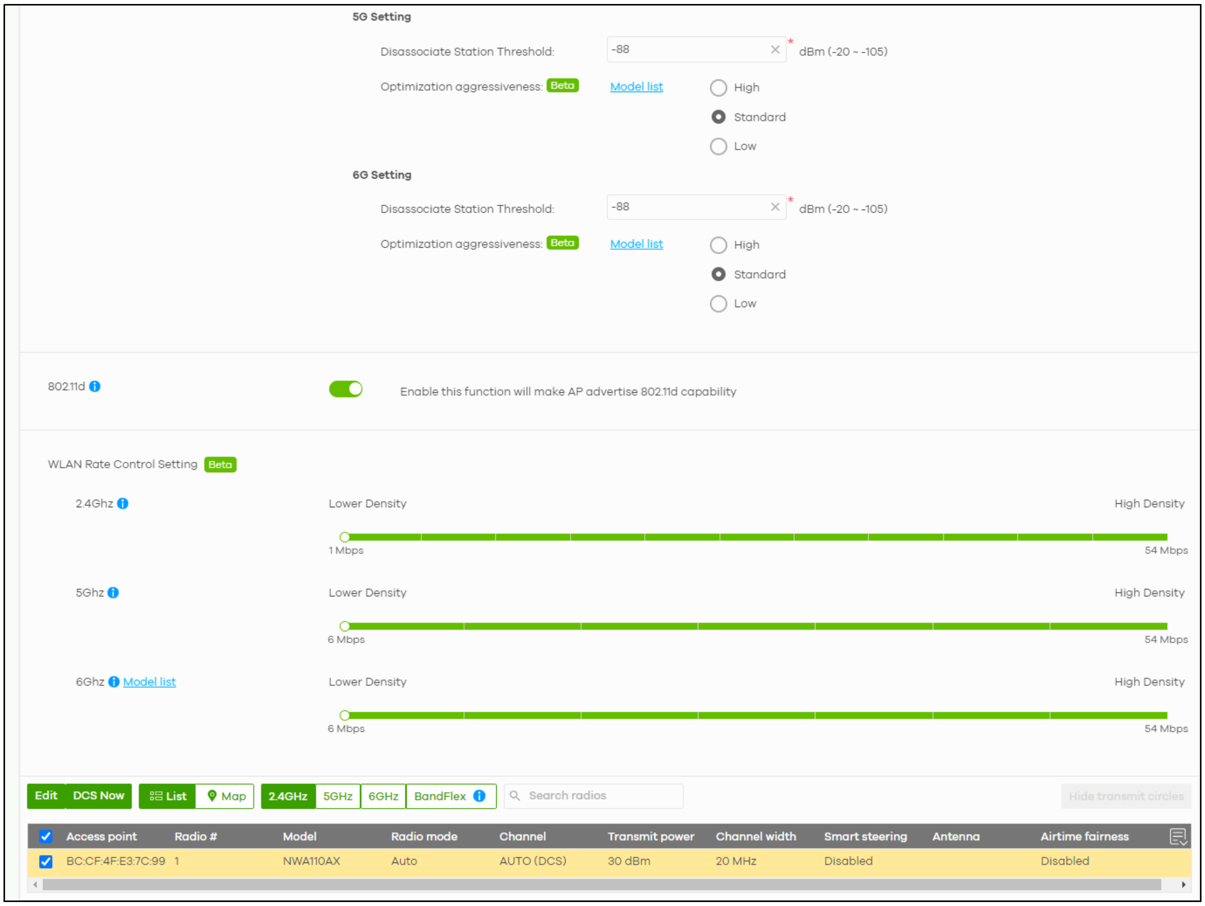
Allow 802.11ax/ac/n stations only

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 Beta

2.4Ghz: Lower Density — High Density; 1 Mbps — 54 Mbps

5Ghz: Lower Density — High Density; 6 Mbps — 54 Mbps

6Ghz Model list: Lower Density — High Density; 6 Mbps — 54 Mbps

☑	Access point	Radio #	Model	Radio mode	Channel	Transmit power	Channel width	Smart steering	Antenna	Airtime fairness
☑	BC:CF:4F:E3:7C:99	1	NWA110AX	Auto	AUTO (DCS)	30 dBm	20 MHz	Disabled		Disabled

The following table describes the labels in this screen.

Table 52 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 52 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. 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 bandwidth to 160 MHz for the whole site. To configure a Nebula Device to use 160 MHz, 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 52 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.
WLAN Rate Control Setting	

Table 52 Site-wide > Configure > Access points > Radio settings (continued)

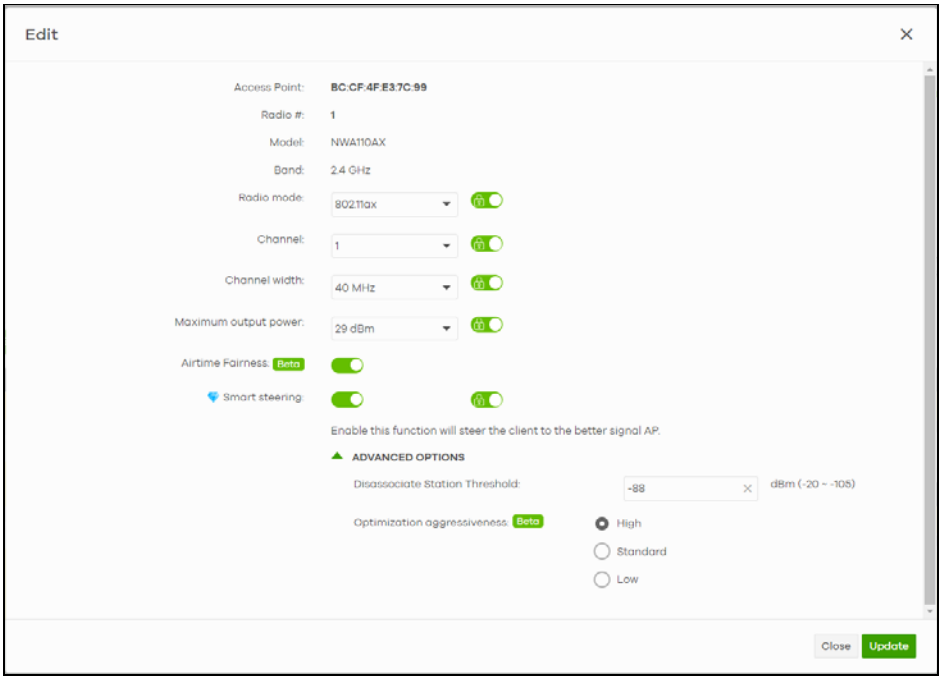
LABEL	DESCRIPTION
2.4Ghz/5Ghz/6Ghz	Sets the minimum data rate that 2.4 GHz, 5 GHz, and 6 GHz WiFi clients can connect to the Nebula Device, in Mbps. Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that 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.
2.4GHz	Click this to display the connected Nebula Devices using the 2.4 GHz frequency band.
5GHz	Click this to display the connected Nebula Devices using the 5 GHz frequency band.
6GHz	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 52 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 53 Radio Deployment Selection and Corresponding Parameters

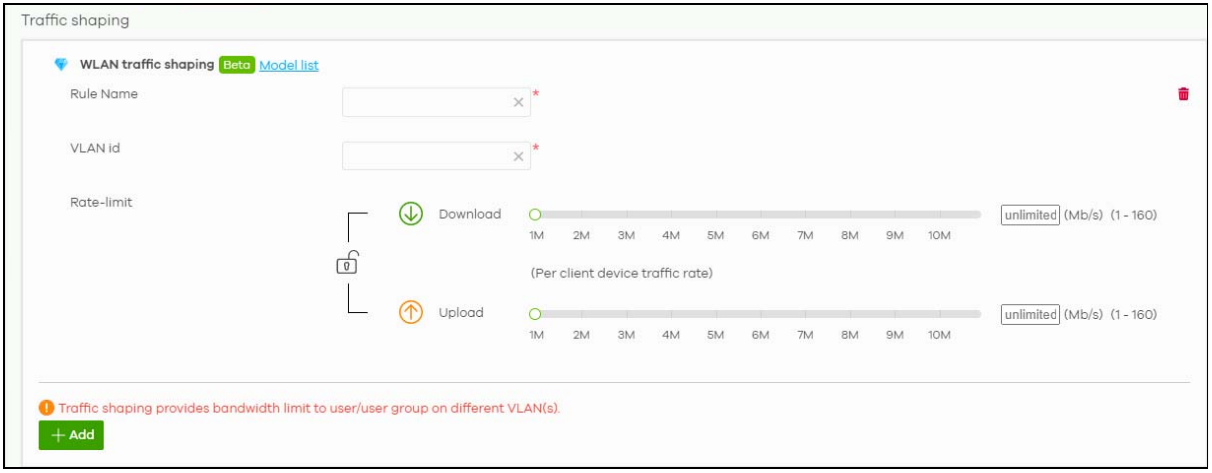
DEPLOYMENT		HIGH DENSITY	MODERATE DENSITY	LOW DENSITY	SINGLE AP
Number of APs		More than 10	6 – 9	2 – 5	1
Power (dBm)	2G	12	15	20	30 20 (EU)
	5G	15	18	30	30
	6G	18	21	30	30
Channel width (MHz)	5G	20	40	80	80
	6G	80	160	160	160
Avoid 5G DFS channel / Blacklist DFS channels in the presence of radar		Disabled / 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 71 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)

Traffic shaping provides bandwidth limit to user/user group on different VLAN(s).

+ Add

The following table describes the labels in this screen.

Table 54 Site-wide > Configure > Access points > Traffic shaping

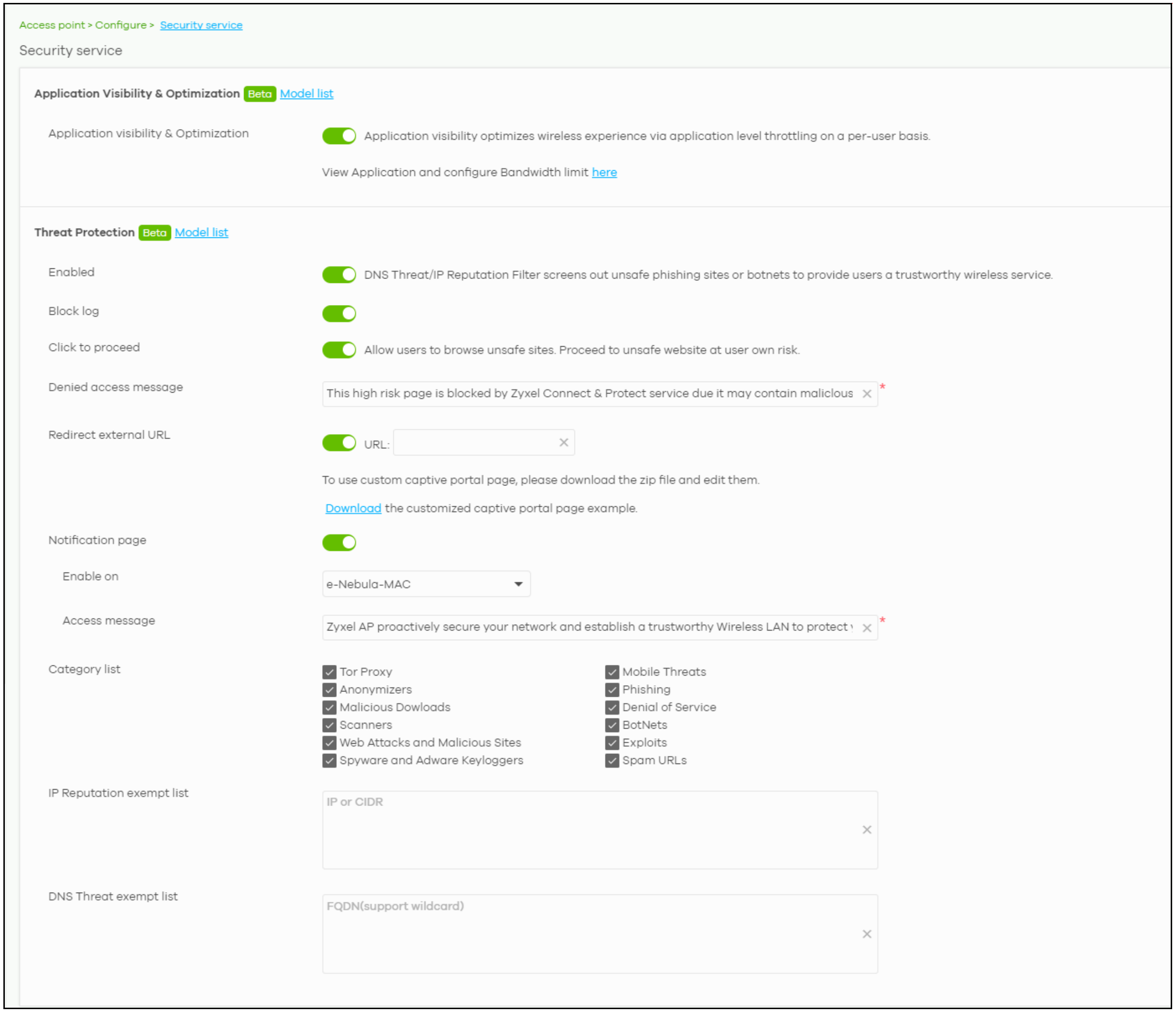
LABEL	DESCRIPTION
WLAN traffic shaping	
Rule Name	Enter the name of the traffic shaping rule. The name is used to refer to the traffic shaping rule. You may use 1 – 31 alphanumeric characters, underscores(_), or dashes (-). This value is case-sensitive.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely 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 72 Site-wide > Configure > Access points > Security service



Access point > Configure > 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 55 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 55   Site-wide > Configure > Access points > Security service (continued)

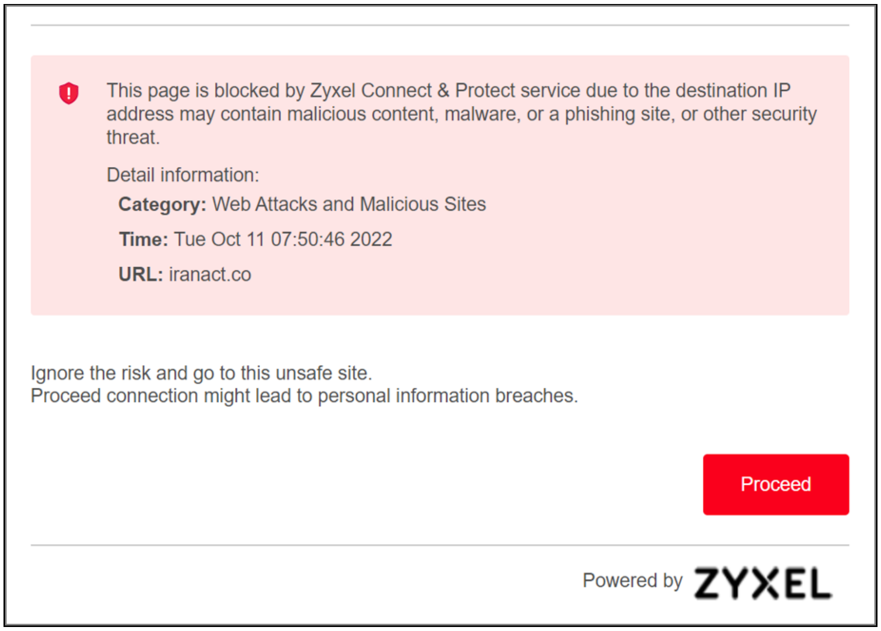
LABEL	DESCRIPTION
Enabled	Select this option to allow inspection of DNS queries made by clients on your network and turn on IP blocking on the Nebula Device. When you enable the DNS threat service, your Nebula Device inspects the DNS queries against a database of blocked or allowed Fully Qualified Domain 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 55 Site-wide > Configure > Access points > Security service (continued)

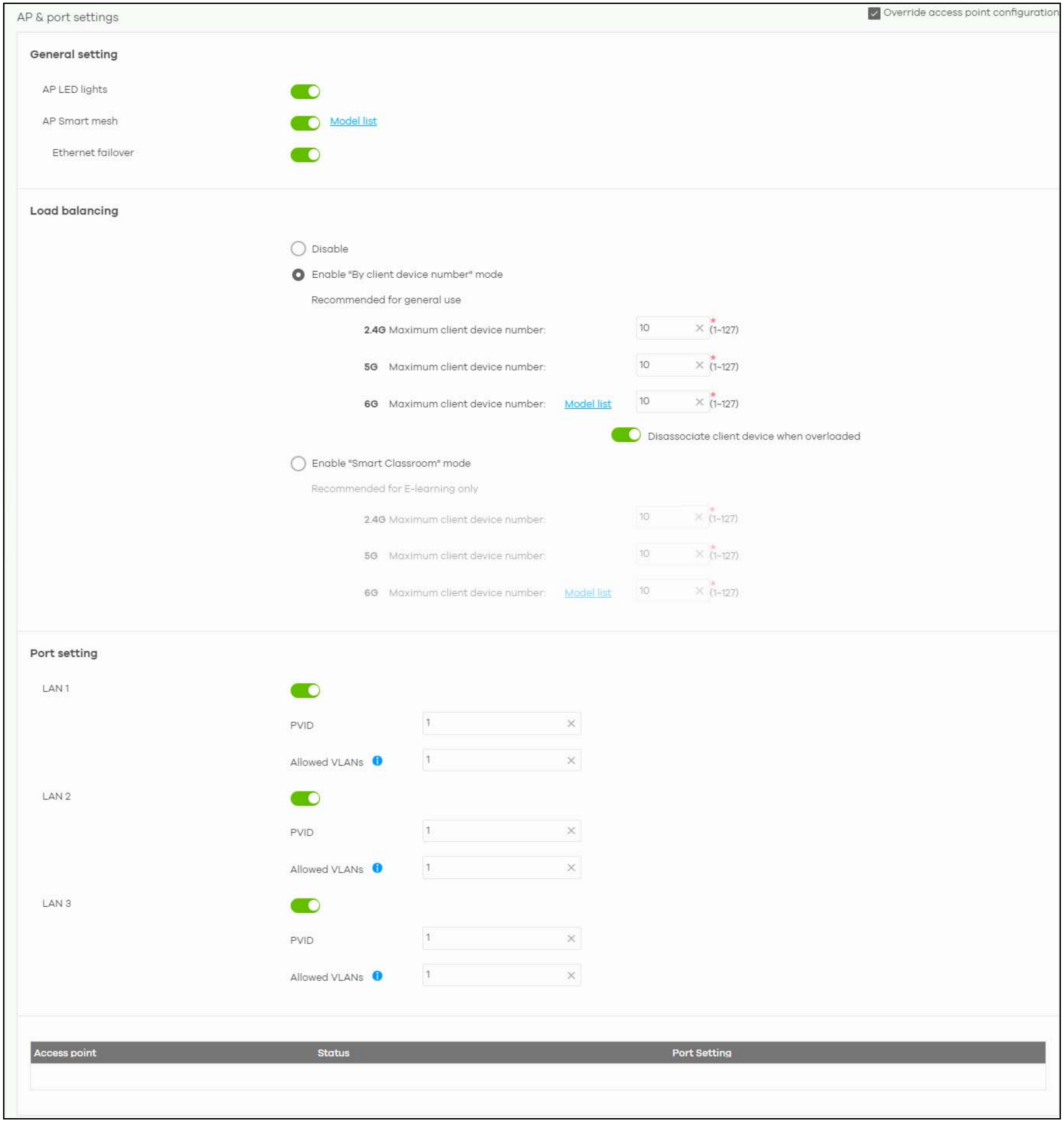
LABEL	DESCRIPTION
Category list	Select the categories of packets that come from the Internet and are known to pose a security threat to users or their computers.
IP Reputation exempt list	Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this 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 73 Site-wide > Configure > Access points > AP & port settings



AP & port settings

☑ Override access point configuration

General setting

AP LED lights

AP Smart mesh Model list

Ethernet failover

Load balancing

○ Disable

● Enable "By client device number" mode

Recommended for general use

2.4G Maximum client device number: 10 * (1~127)

5G Maximum client device number: 10 * (1~127)

6G Maximum client device number: Model list 10 * (1~127)

Disassociate client device when overloaded

○ Enable "Smart Classroom" mode

Recommended for E-learning only

2.4G Maximum client device number: 10 * (1~127)

5G Maximum client device number: 10 * (1~127)

6G Maximum client device number: Model list 10 * (1~127)

Port setting

LAN 1

PVID 1

Allowed VLANs 1

LAN 2

PVID 1

Allowed VLANs 1

LAN 3

PVID 1

Allowed VLANs 1

Access point	Status	Port Setting

The following table describes the labels in this screen.

Table 56 Site-wide > Configure > Access points > AP & port settings

LABEL	DESCRIPTION
General setting	
AP LED lights	Click to turn on or off the LEDs on the Nebula Devices.

Table 56 Site-wide > Configure > Access points > AP & port settings (continued)

LABEL	DESCRIPTION
AP 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 233. 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 159. 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 159.
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 233.
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.
Maximum client device number	Enter the threshold number of client devices 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.
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.
Maximum client device number	Enter the threshold number of client devices 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.

Table 56 Site-wide > Configure > Access points > AP & port settings (continued)

LABEL	DESCRIPTION
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. 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**.

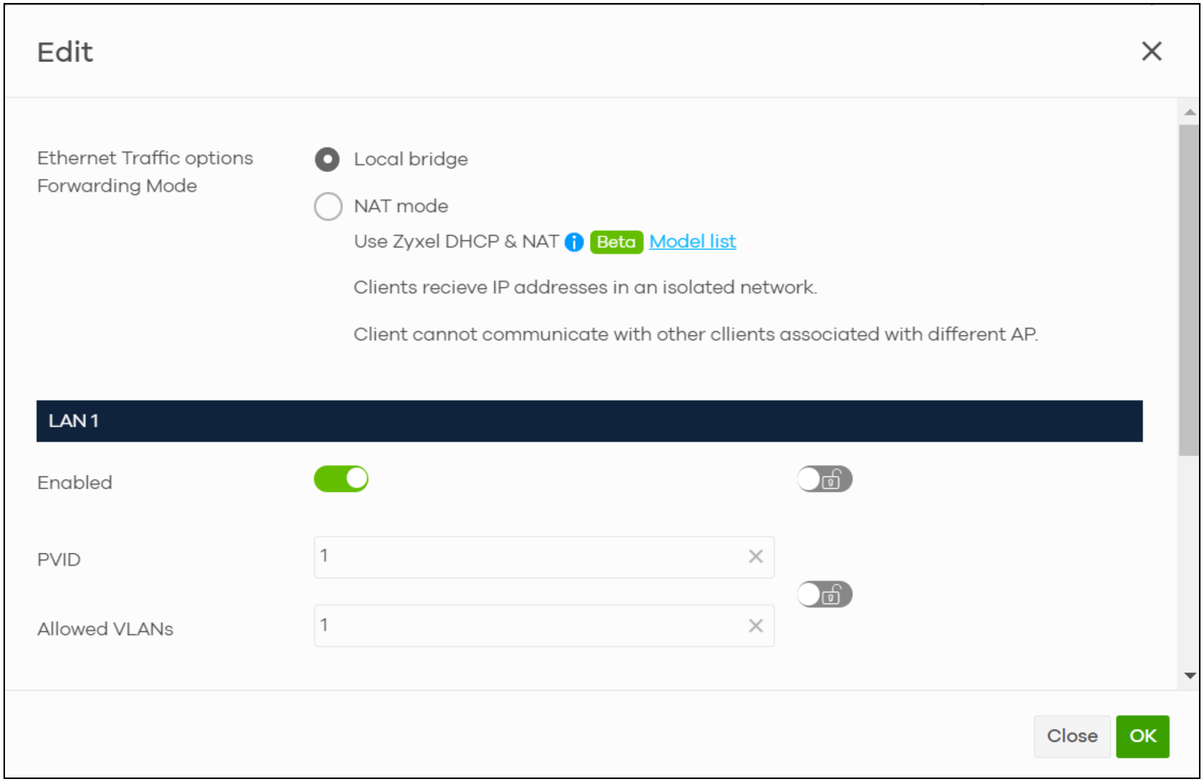
The following Nebula Device features do not work when NAT mode is enabled:

- 802.11r (see Table 48 on page 249 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 74 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. To view the list of Nebula Devices that can be managed through NCC, go to **Help** > **Support tools** > **Device function table**.

6.2 Monitor

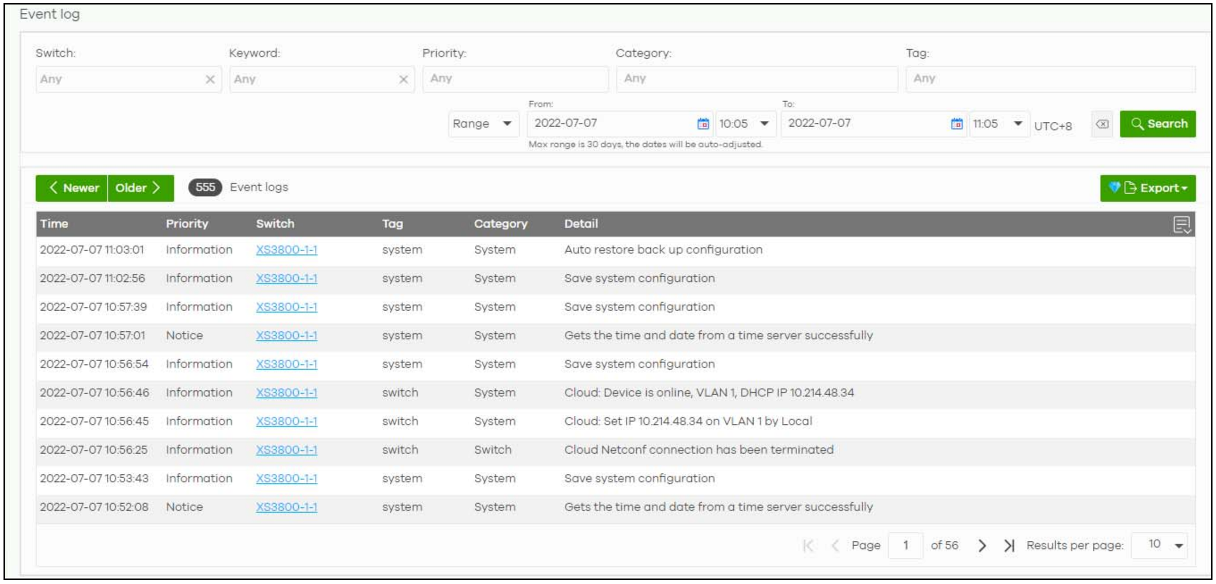
Use the **Monitor** menus to check the Nebula Device information, client information, event log messages and summary report for Nebula Devices in the selected site.

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 75 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

Max range is 30 days, the dates will be auto-adjusted.

555 Event logs

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

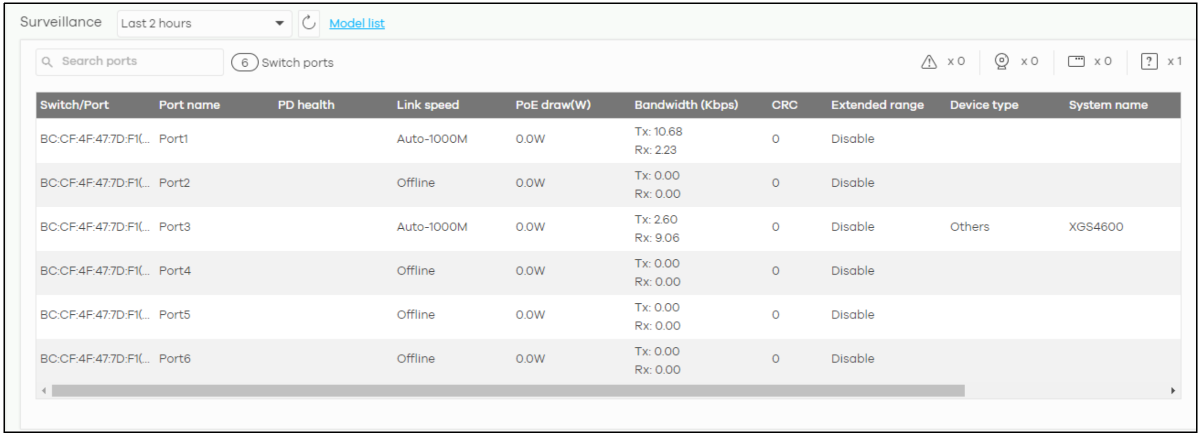
Page 1 of 56 Results per page: 10

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 76 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 57 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.
▭	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 288.
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.

Table 57   Site-wide > Monitor > Switches > Surveillance (continued)

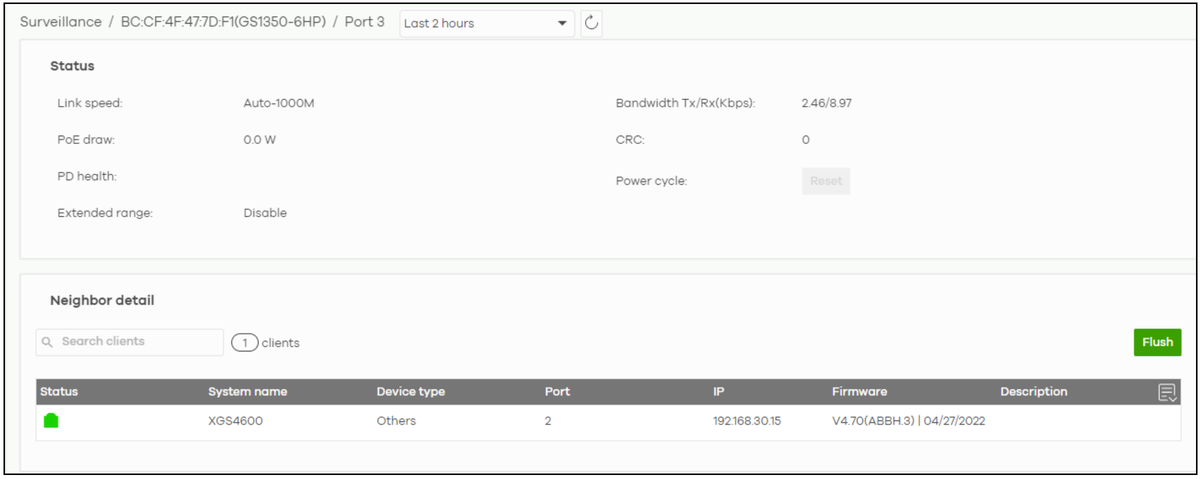
LABEL	DESCRIPTION
PoE draw(W)	This shows the total power that the connected PD draws from the port, in watts. This allows you to plan and use within the power budget of the Nebula Device.
Bandwidth (Kbps)	Tx shows the number of kilobytes per second transmitted on this port. Rx shows the number of kilobytes 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 77   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

PoE draw: 0.0 W

PD health:

Extended range: Disable

Bandwidth Tx/Rx(Kbps): 2.46/8.97

CRC: 0

Power cycle: Reset

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 58   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.

Table 58 Site-wide > Monitor > Switches > Surveillance > Port Details (continued)

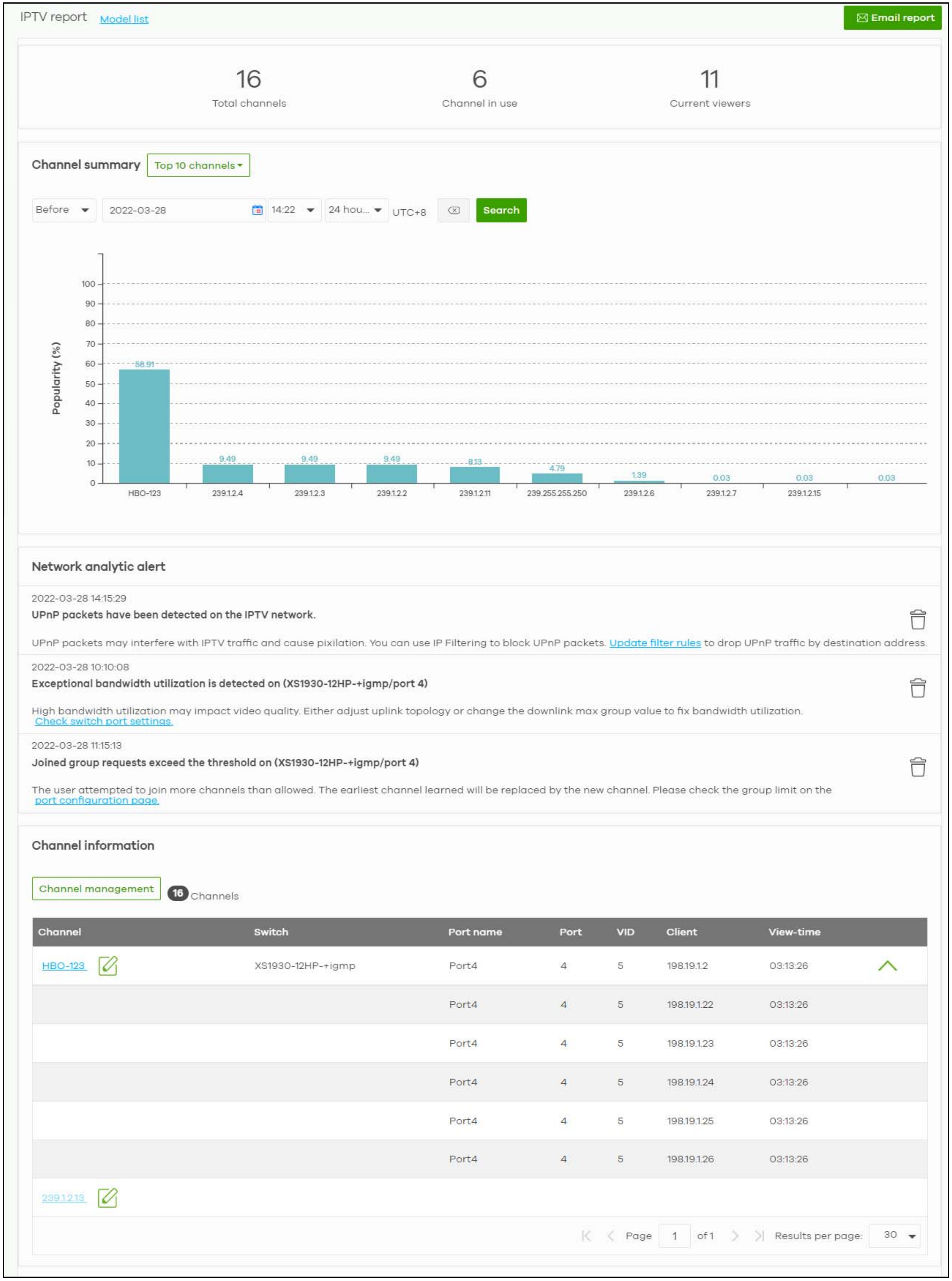
LABEL	DESCRIPTION
PD health	This shows the status of auto PD recovery on this port. • Red: The Nebula Device failed to get information from the PD connected to the port using LLDP, or the connected PD did not respond to the Nebula Device's ping requests. • Yellow: The Nebula Device is restarting the 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 288.
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 cycle	Click **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.
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 78 Site-wide > Monitor > Switches > IPTV Report



16	6	11
Total channels	Channel in use	Current viewers

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 59 Site-wide > Monitor > Switches > IPTV Report

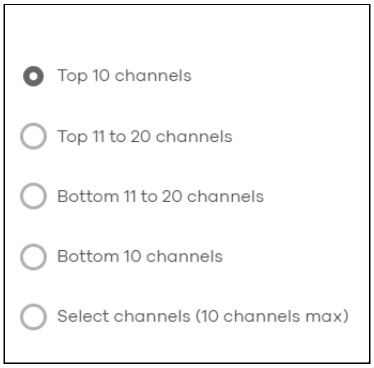
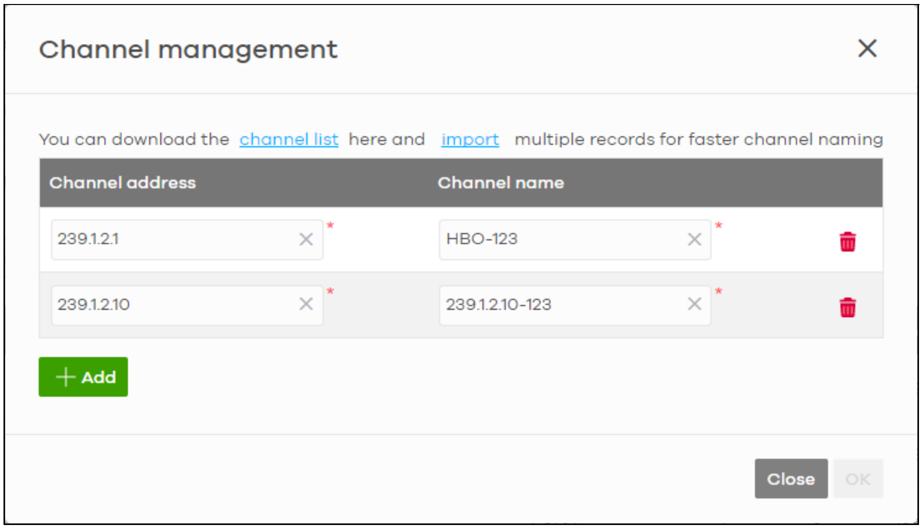
LABEL	DESCRIPTION
IPTV report	Click **Model list** to show the **Non-supported model list**. Click **See more** to go to the **Help** > **Support tools** > **Device function table** screen.
Email report	Click this button to send channel summary report by email, change the report logo and set email schedules.
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	

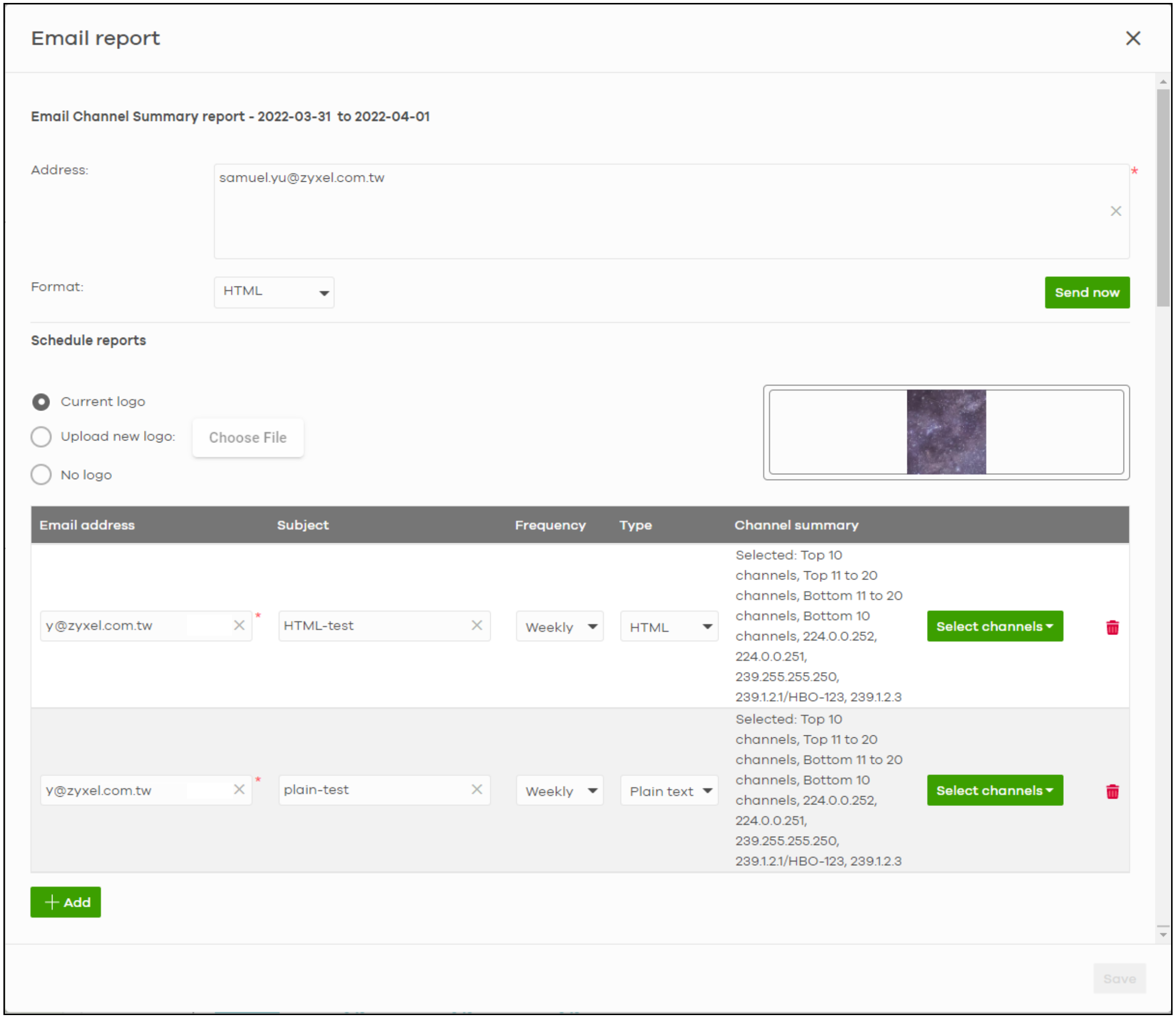
Table 59   Site-wide > Monitor > Switches > IPTV Report (continued)

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 | Channel name 239.1.2.1 | HBO-123 239.1.2.10 | 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 284.
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 79 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: Choose File

○ No logo

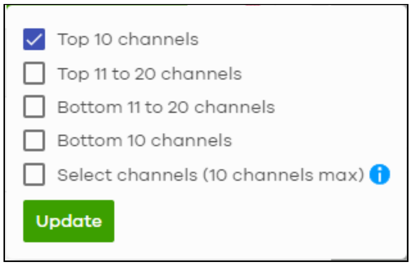
Email address	Subject	Frequency	Type	Channel summary
y@zyxel.com.tw	HTML-test	Weekly	HTML	Selected: Top 10 channels, Top 11 to 20 channels, Bottom 11 to 20 channels, Bottom 10 channels, 224.0.0.252, 224.0.0.251, 239.255.255.250, 239.1.2.1/HBO-123, 239.1.2.3
y@zyxel.com.tw	plain-test	Weekly	Plain text	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 60 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.

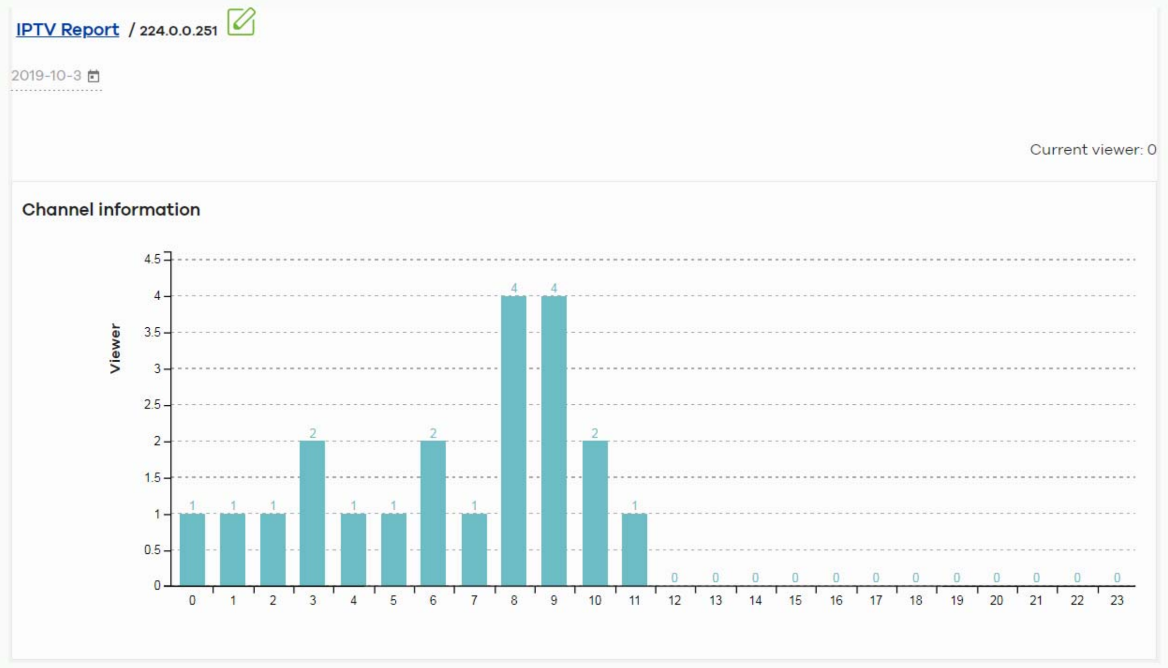
Table 60 Site-wide > Monitor > Switches > IPTV Report: Email report (continued)

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 80 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 61 Switches > Monitor > Switches > IPTV Report: Channel Information

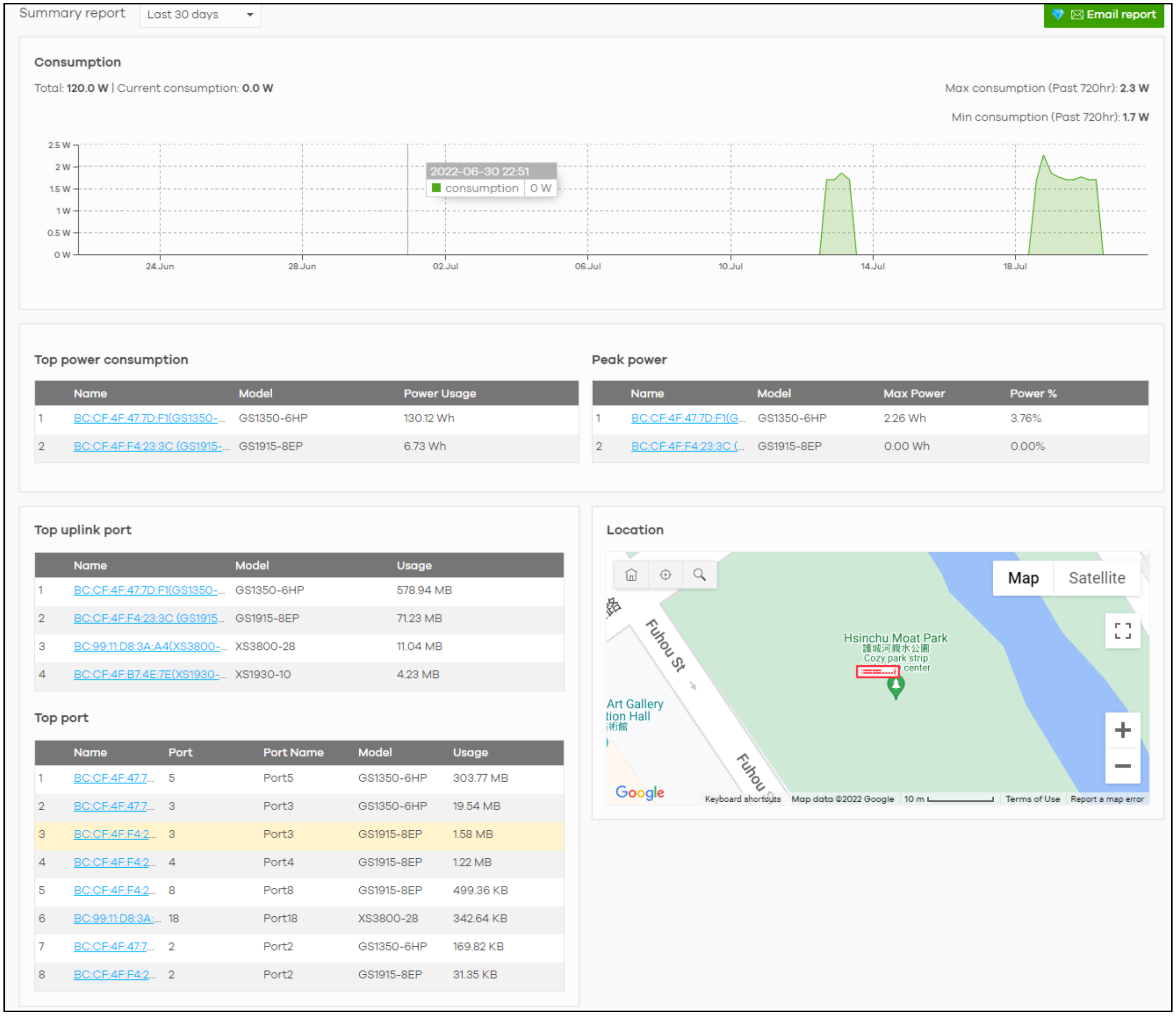
LABEL	DESCRIPTION
	Select a specific date to display only the clients who watch the IPTV channel on that day.
Current Viewer	This shows the number of clients who are currently watching the IPTV channel.
y-axis	The y-axis shows the number of clients watching the IPTV channel.
x-axis	The x-axis shows the 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 81 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 62 Site-wide > Monitor > Switches > Summary Report

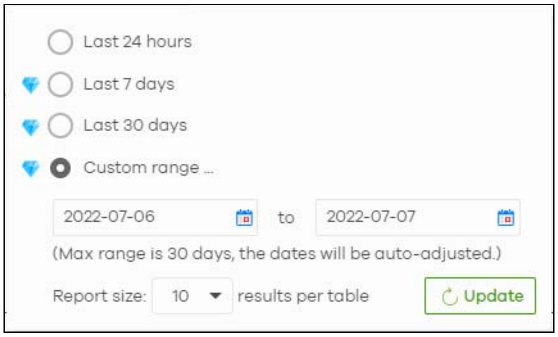
LABEL	DESCRIPTION
Switch – Summary report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ○ Last 7 days ○ Last 30 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 62 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.	

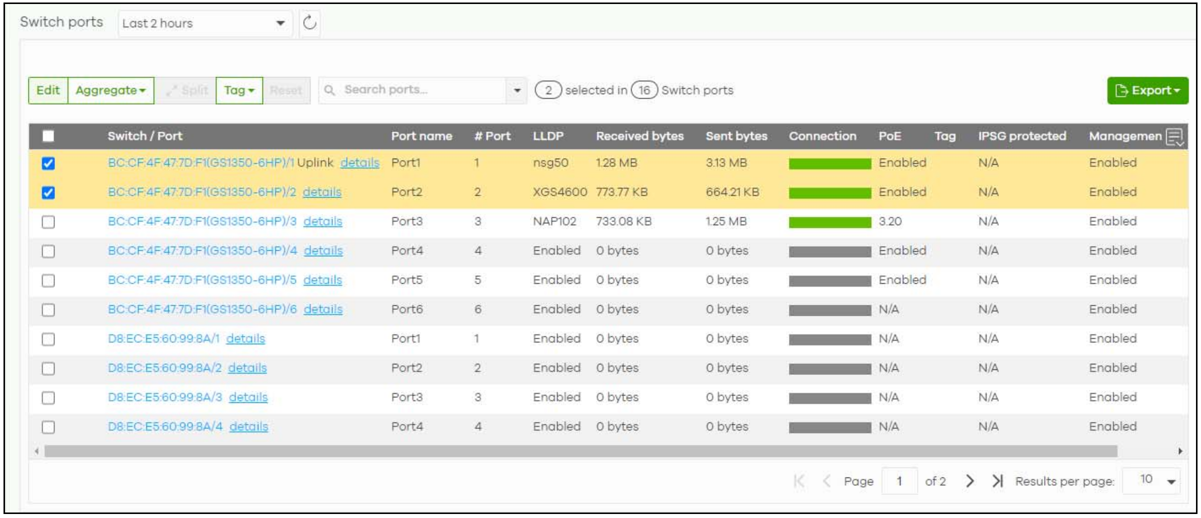
6.3 Configure

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 82 Site-wide > Configure > Switches > Switch ports



2 selected in 16 Switch ports

☐	Switch / Port	Port name	# Port	LLDP	Received bytes	Sent bytes	Connection	PoE	Tag	IPSG protected	Managemen
☑	BC:CF:4F:47:7D:F1(GS1350-6HP)/1 Uplink details	Port1	1	nsg50	1.28 MB	3.13 MB	🟩	Enabled		N/A	Enabled
☑	BC:CF:4F:47:7D:F1(GS1350-6HP)/2 details	Port2	2	XGS4600	773.77 KB	664.21 KB	🟩	Enabled		N/A	Enabled
☐	BC:CF:4F:47:7D:F1(GS1350-6HP)/3 details	Port3	3	NAP102	733.08 KB	1.25 MB	🟩	3.20		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
☐	D8:EC:E5:60:99:8A/1 details	Port1	1	Enabled	0 bytes	0 bytes	▬	N/A		N/A	Enabled
☐	D8:EC:E5:60:99:8A/2 details	Port2	2	Enabled	0 bytes	0 bytes	▬	N/A		N/A	Enabled
☐	D8:EC:E5:60:99:8A/3 details	Port3	3	Enabled	0 bytes	0 bytes	▬	N/A		N/A	Enabled
☐	D8:EC:E5:60:99:8A/4 details	Port4	4	Enabled	0 bytes	0 bytes	▬	N/A		N/A	Enabled

Page 1 of 2 Results per page: 10

The following table describes the labels in this screen.

Table 63 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.

Table 63 Site-wide > Configure > Switches > Switch ports (continued)

LABEL	DESCRIPTION
Aggregate	Select more than one port and click this button to group the physical ports into one logical higher-capacity link.
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.
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 169 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**. Click **details** to display the port details screen. See Section 4.3.2.1 on page 169.
Port name	This shows the descriptive name of the 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.

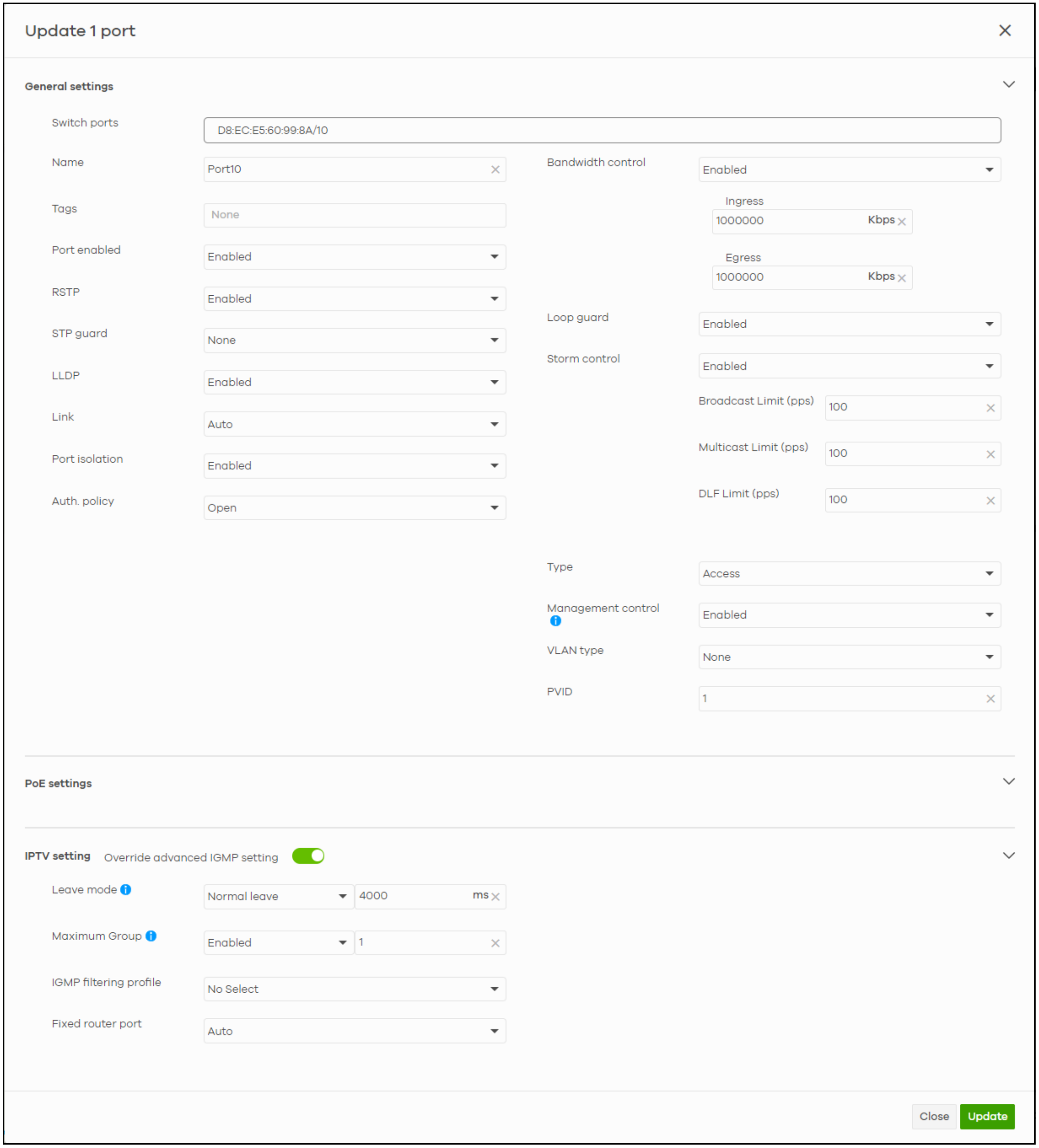
Table 63 Site-wide > Configure > Switches > Switch ports (continued)

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 (#0079FF): 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.
Management control	This shows if management control is enabled on this port. See Table 64 on page 292 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 83 Site-wide > Configure > Switches > Switch ports: Edit



Update 1 port

General settings

Switch ports: D8:EC:E5:60:99:8A/10

Name: Port10

Tags: None

Port enabled: Enabled

RSTP: Enabled

STP guard: None

LLDP: Enabled

Link: Auto

Port isolation: Enabled

Auth. policy: Open

Bandwidth control: Enabled

Ingress: 1000000 Kbps

Egress: 1000000 Kbps

Loop guard: Enabled

Storm control: Enabled

Broadcast Limit (pps): 100

Multicast Limit (pps): 100

DLF Limit (pps): 100

Type: Access

Management control: Enabled

VLAN type: None

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

The following table describes the labels in this screen.

Table 64 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 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 on the ports.
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**.
LLDP	Select to enable or disable LLDP on the ports.
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.
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.
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 73 on page 308 for more information on authentication policy type. See Section 6.3.6 on page 306 for more information on configuring authentication policy. Select **Open** if you do NOT want to enable port authentication on the ports.
Bandwidth Control	Select to enable or disable bandwidth control on the 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.

Table 64 Site-wide > Configure > Switches > Switch ports: Edit (continued)

LABEL	DESCRIPTION
Loop guard	Select to enable or disable loop guard on the ports. Note: The loop guard feature cannot be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.
Storm Control	Select to enable or disable broadcast storm control on the ports.
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.
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 through which the device management VLAN traffic is allowed. Note: Make sure to enable this for an uplink port to maintain connection with Nebula.
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 6.3.8 on page 310.
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 3.24 on page 136 for the steps in setting up dynamic VLAN with RADIUS. See Section 3.25 on page 138 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 64 Site-wide > Configure > Switches > Switch ports: Edit (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 **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.
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.

Table 64 Site-wide > Configure > Switches > Switch ports: Edit (continued)

LABEL	DESCRIPTION
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	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.
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	
Overwrite 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.

Table 64   Site-wide > Configure > Switches > Switch ports: Edit (continued)

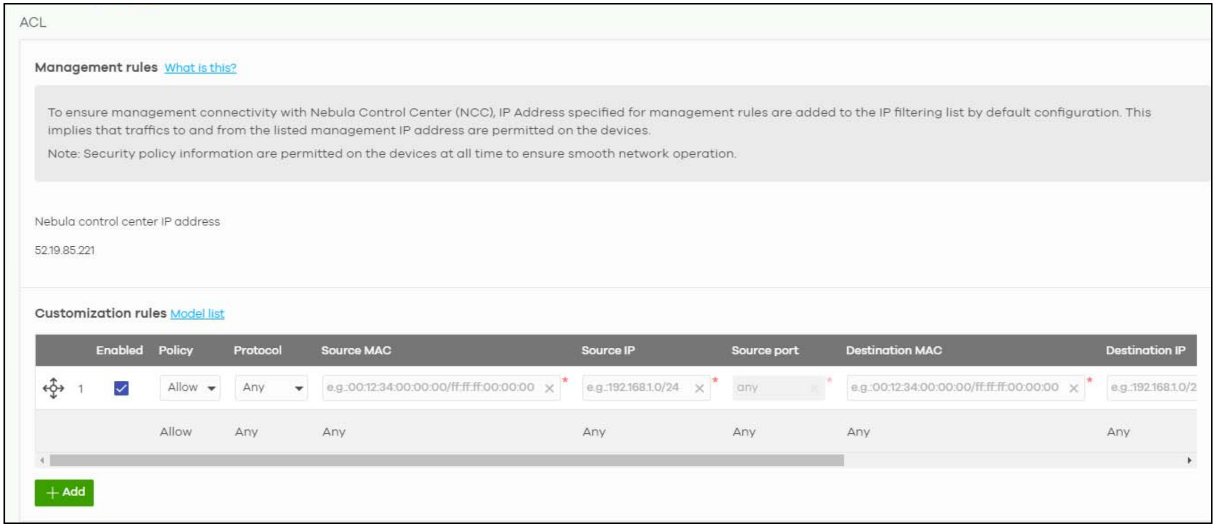
LABEL	DESCRIPTION
Leave Mode	Select **Immediate Leave** to remove this port from the multicast tree immediately when an IGMP leave message is received on this port. Select this option if there is only one host connected to this port. Select **Normal Leave** or **Fast Leave** and enter an IGMP normal/fast 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.

6.3.2 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 84 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

The following table describes the labels in this screen.

Table 65 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 check box to turn on the rule. Otherwise, clear the check box 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.

6.3.3 IP & Routing

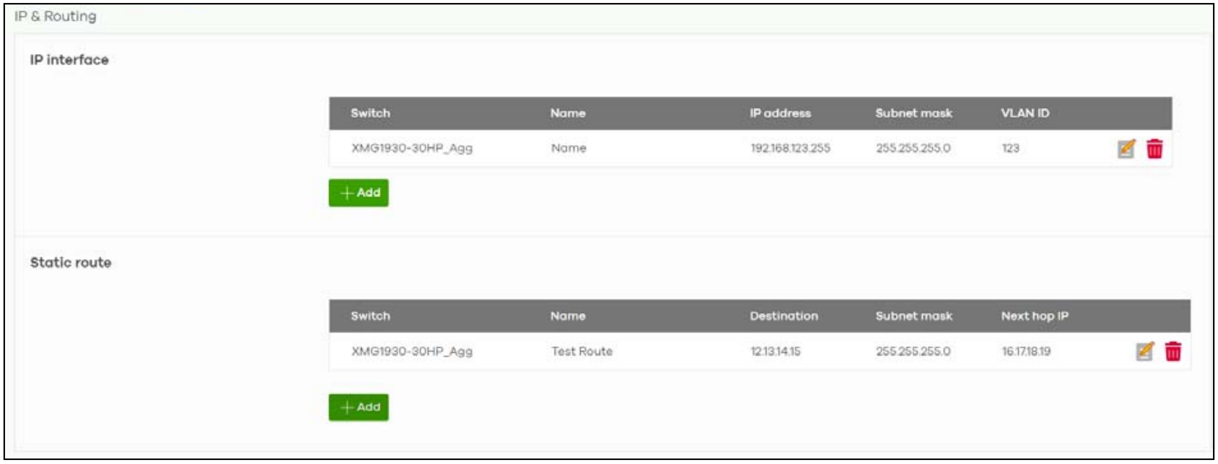
This screen enables you to create IP interfaces and static routes on Nebula Devices in the site. This allows you to do the following:

- 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.

Click **Site-wide** > **Configure** > **Switches** > **IP & Routing** to access this screen.

Figure 85 Site-wide > Configure > Switches > IP & Routing



Switch	Name	IP address	Subnet mask	VLAN ID	
XMG1930-30HP_Agg	Name	192.168.123.255	255.255.255.0	123	📝 🗑

Switch	Name	Destination	Subnet mask	Next hop IP	
XMG1930-30HP_Agg	Test Route	12.13.14.15	255.255.255.0	16.17.18.19	📝 🗑

The following table describes the labels in this screen.

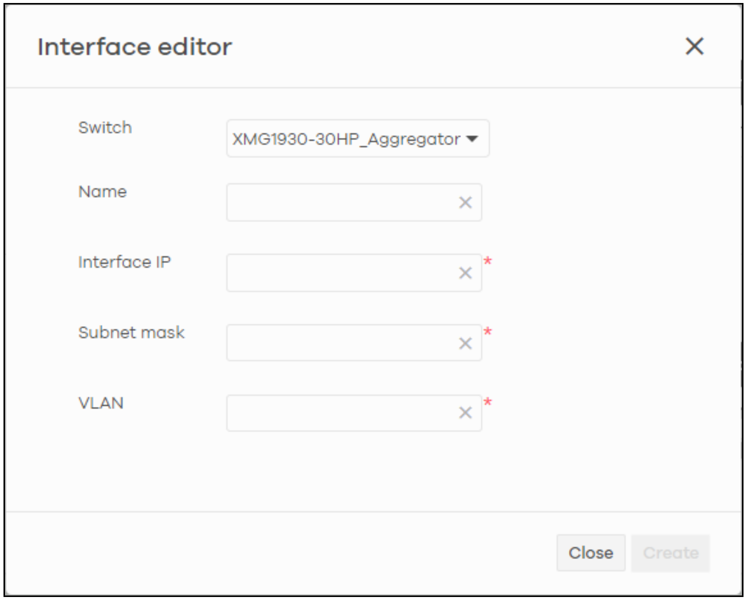
Table 66 Site-wide > Configure > Switches > IP & Routing

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).
📝	Click this icon to modify the interface.
🗑	Click this icon to delete the interface.
VLAN ID	This shows the ID number of the VLAN with which the interface (network) is associated.
+ 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.

6.3.3.1 Add IP Interface

Click the **+ Add** button on the **Site-wide** > **Configure** > **Switches** > **IP & Routing** > **IP Interface** screen to access this screen.

Figure 86 Site-wide > Configure > Switches > IP & Routing > IP Interface > Add



Interface editor

Switch: XMG1930-30HP_Aggregator

Name

Interface IP *

Subnet mask *

VLAN *

The following table describes the labels in this screen.

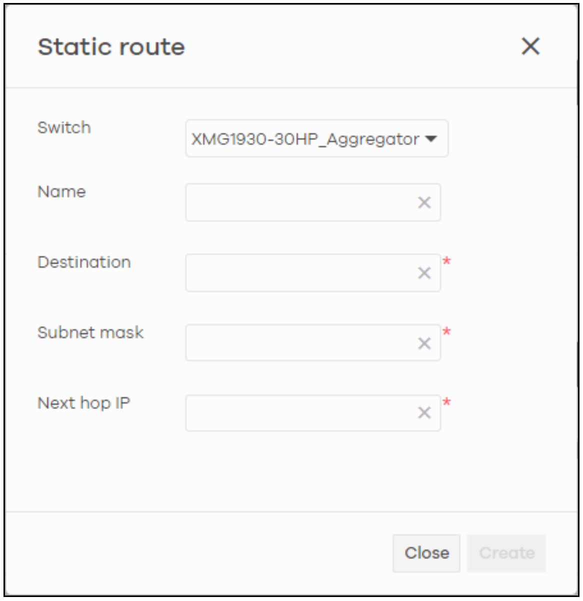
Table 67 Site-wide > Configure > Switches > IP & Routing > IP Interface > Add

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.
IP address	Inter the IP address of the interface (network).
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.
Close	Click **Close** to exit this screen without saving.
Create	Click **Create** to save your changes and create the interface.

6.3.3.2 Add Static Route

Click the **+ Add** button on the **Site-wide** > **Configure** > **Switches** > **IP & Routing** > **Static Route** screen to access this screen.

Figure 87   Site-wide > Configure > Switches > IP & Routing > Static Route > Add



The following table describes the labels in this screen.

Table 68   Site-wide > Configure > Switches > IP & Routing > Static Route > Add

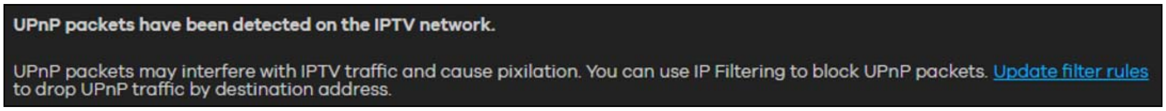
LABEL	DESCRIPTION
Switch	Select a Nebula Device in the site on which to create the interface.
Name	Enter a descriptive name for this route.
Destination	Specifies the IP network address of the final destination.
Subnet mask	Enter the IP subnet mask.
Next hop IP	Enter the IP address of the next-hop gateway.
Close	Click **Close** to exit this screen without saving.
Create	Click **Create** to save your changes and create the static route.

6.3.4 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.

6.3.4.1 Configuring ONVIF Discovery

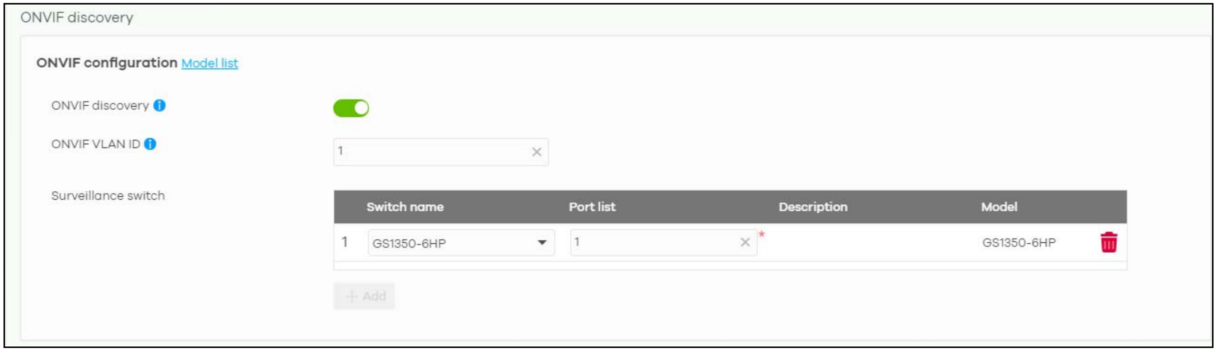
Follow these steps to configure ONVIF discovery within a site.

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.

6.3.4.2 ONVIF Discovery Screen

Click **Site-wide** > **Configure** > **Switches** > **ONVIF discovery** to access this screen.

Figure 88 Site-wide > Configure > Switches > ONVIF discovery



ONVIF discovery

ONVIF configuration Model list

ONVIF discovery ●

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 69 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.

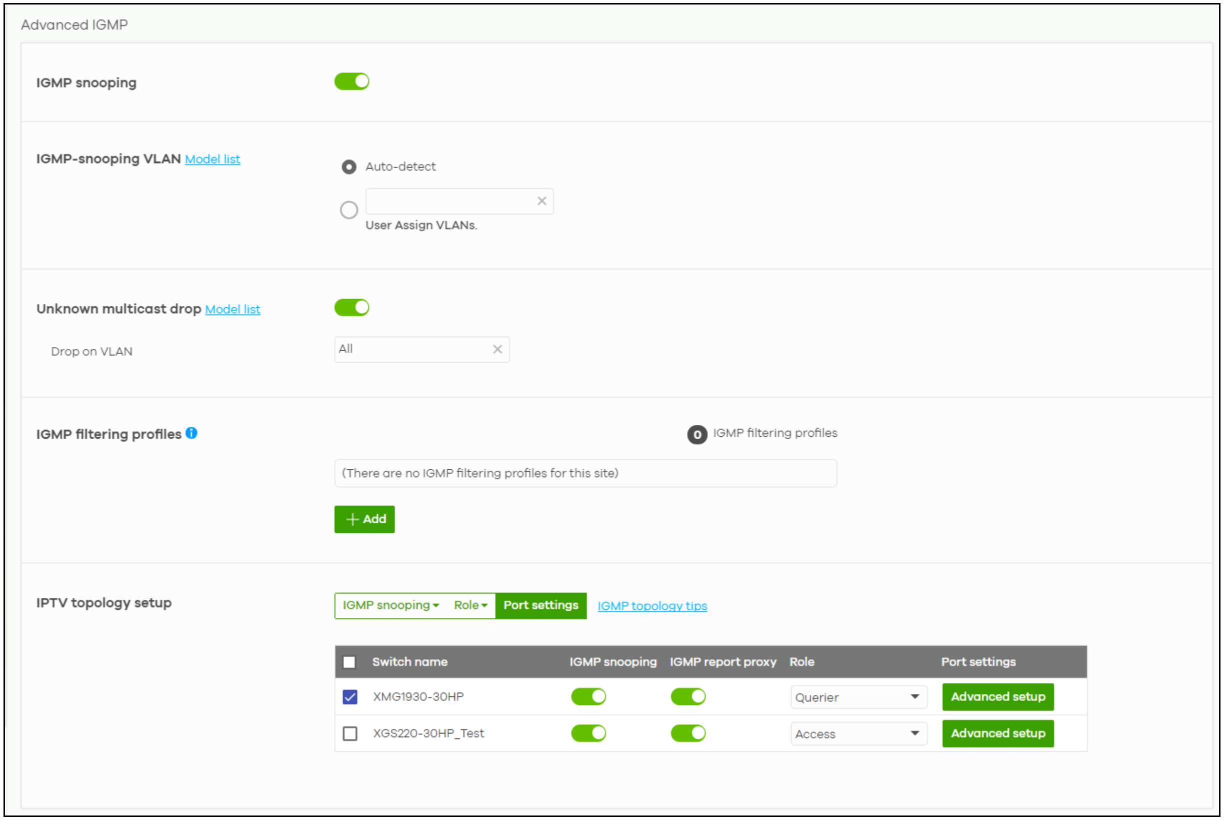
6.3.5 Advanced IGMP

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 89 Site-wide > Configure > Switches > Advanced IGMP



Advanced IGMP

IGMP snooping

IGMP-snooping VLAN

● Auto-detect

○ ×
User Assign VLANs.

Unknown multicast drop

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 70 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 6.3.5.1 on page 304.
🗑	Click the remove icon to delete the profile.
+Add	Click this button to create a new profile. See Section 6.3.5.1 on page 304.
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 6.3.5.2 on page 305.
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 6.3.5 on page 302 for more information on IGMP snooping.

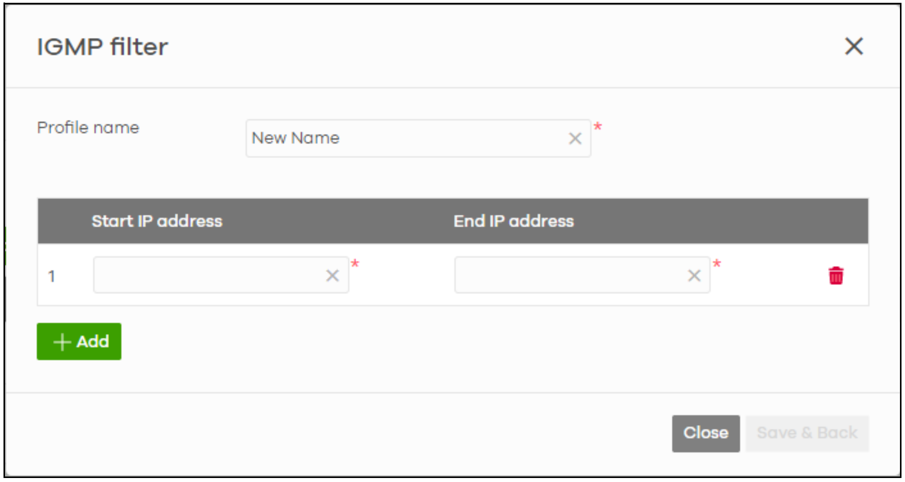
Table 70 Site-wide > Configure > Switches > Advanced IGMP (continued)

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 6.3.5.2 on page 305.
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.

6.3.5.1 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 90 Site-wide > Configure > Switches > Advanced IGMP: Add IGMP Filtering Profile



IGMP filter

Profile name: New Name *

	Start IP address	End IP address	
1	*	*	🗑

The following table describes the labels in this screen.

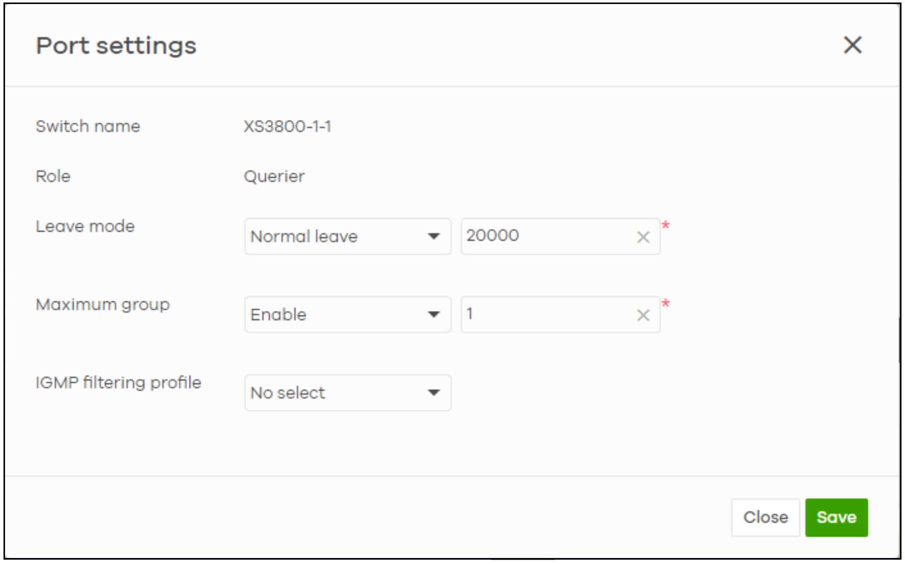
Table 71 Site-wide > Configure > Switches > Advanced IGMP: Add/Edit IGMP Filtering Profile

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.

6.3.5.2 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 91 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 72 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 72 Site-wide > Configure > Switches > Advanced IGMP: Port settings (continued)

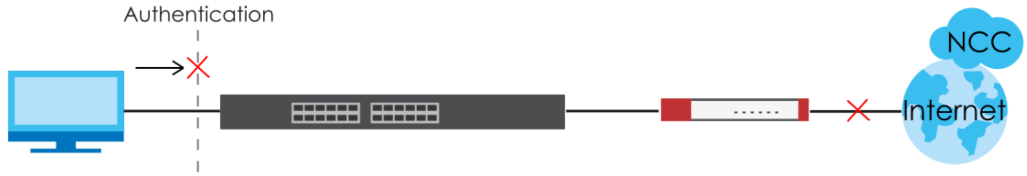
LABEL	DESCRIPTION
Leave mode	Select **Immediate Leave** to set the Nebula Device to remove this port from the multicast tree immediately when an IGMP leave message is received on this port. Select this option if there is only one host connected to this port. Select **Normal Leave** or **Fast Leave** 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.

6.3.6 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.

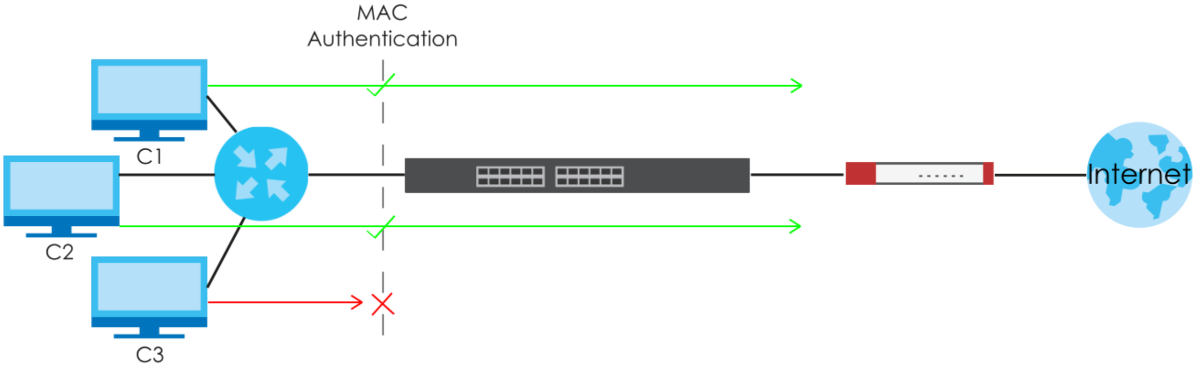
Note: Network traffic from clients will be denied when the Nebula cloud authentication server (NCAS) cannot be reached.

Figure 92 NCAS Disconnect Behavior



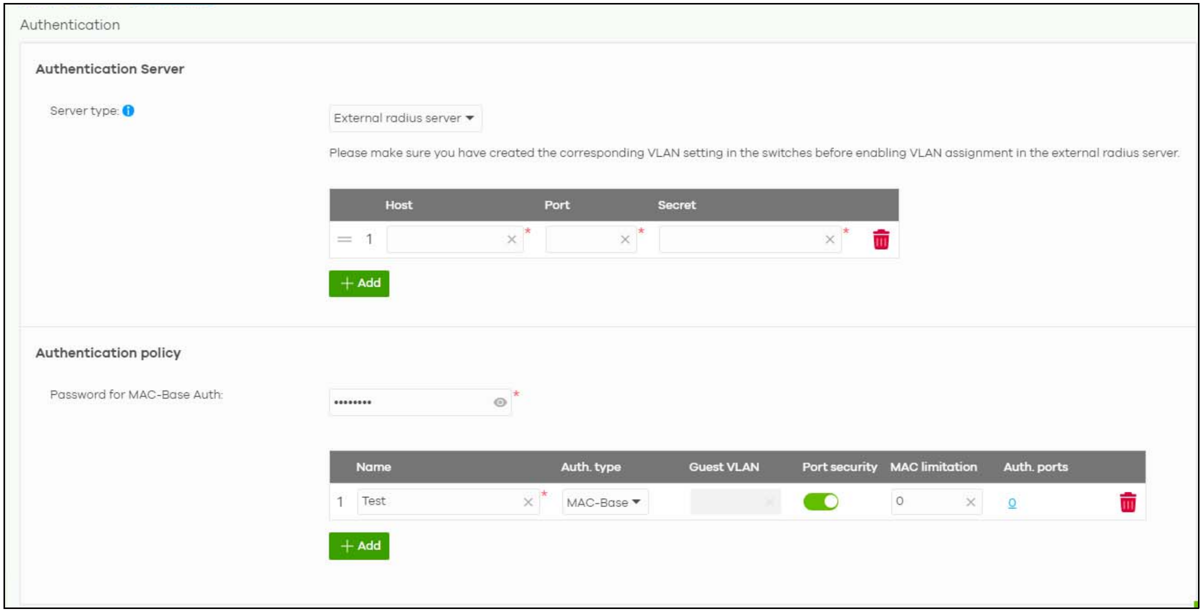
The following figure shows an example Nebula Device with ports enabled for MAC authentication. Clients 1 and 2 (C1, C2) passes MAC authentication (authorized). Client 3 (C3) fails MAC authentication (not authorized).

Figure 93 MAC Authentication Application



Click **Site-wide** > **Configure** > **Switches** > **Authentication** to access this screen.

Figure 94 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 73   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 3.23 on page 135 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 73 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 that may be learned on a port.
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.

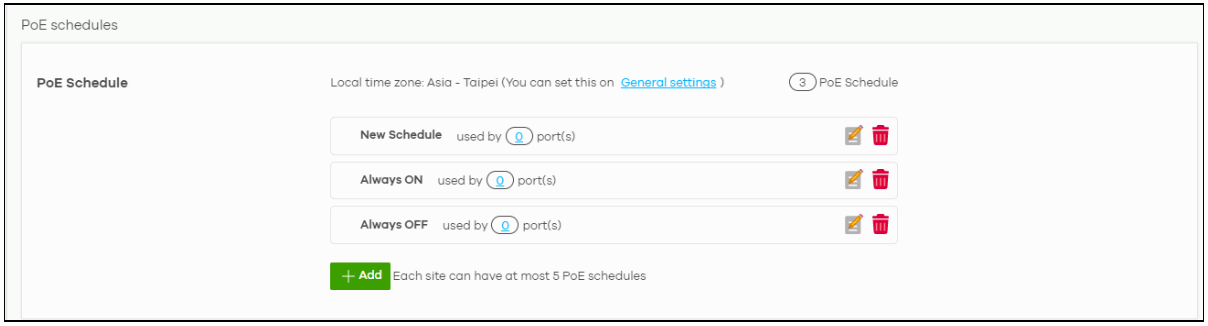
6.3.7 PoE Schedules

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 6.3.7.1 on page 309.

Figure 95 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)

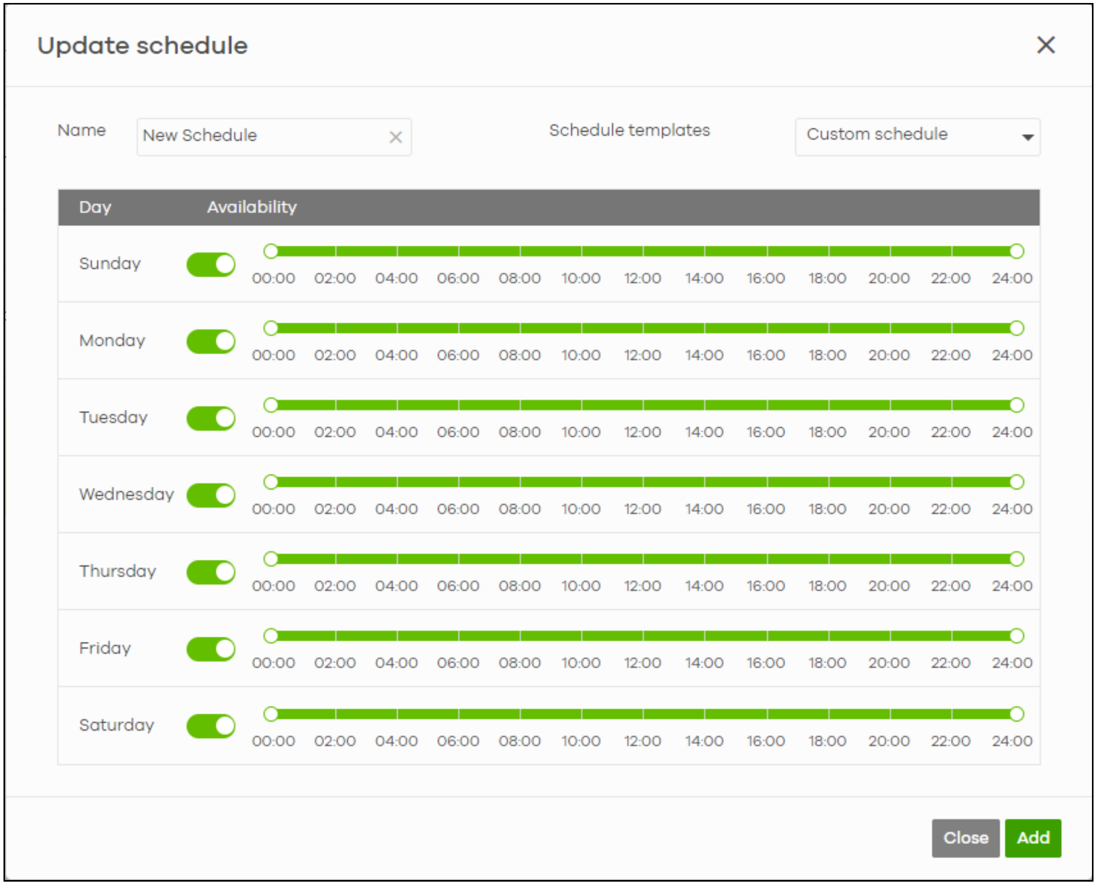
Always OFF used by 0 port(s)

+ Add Each site can have at most 5 PoE schedules

6.3.7.1 Create new schedule

Click the **Add** button in the **Site-wide** > **Configure** > **Switches** > **PoE schedules** screen to access this screen.

Figure 96 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 74 Site-wide > Configure > Switches > PoE schedules: Add

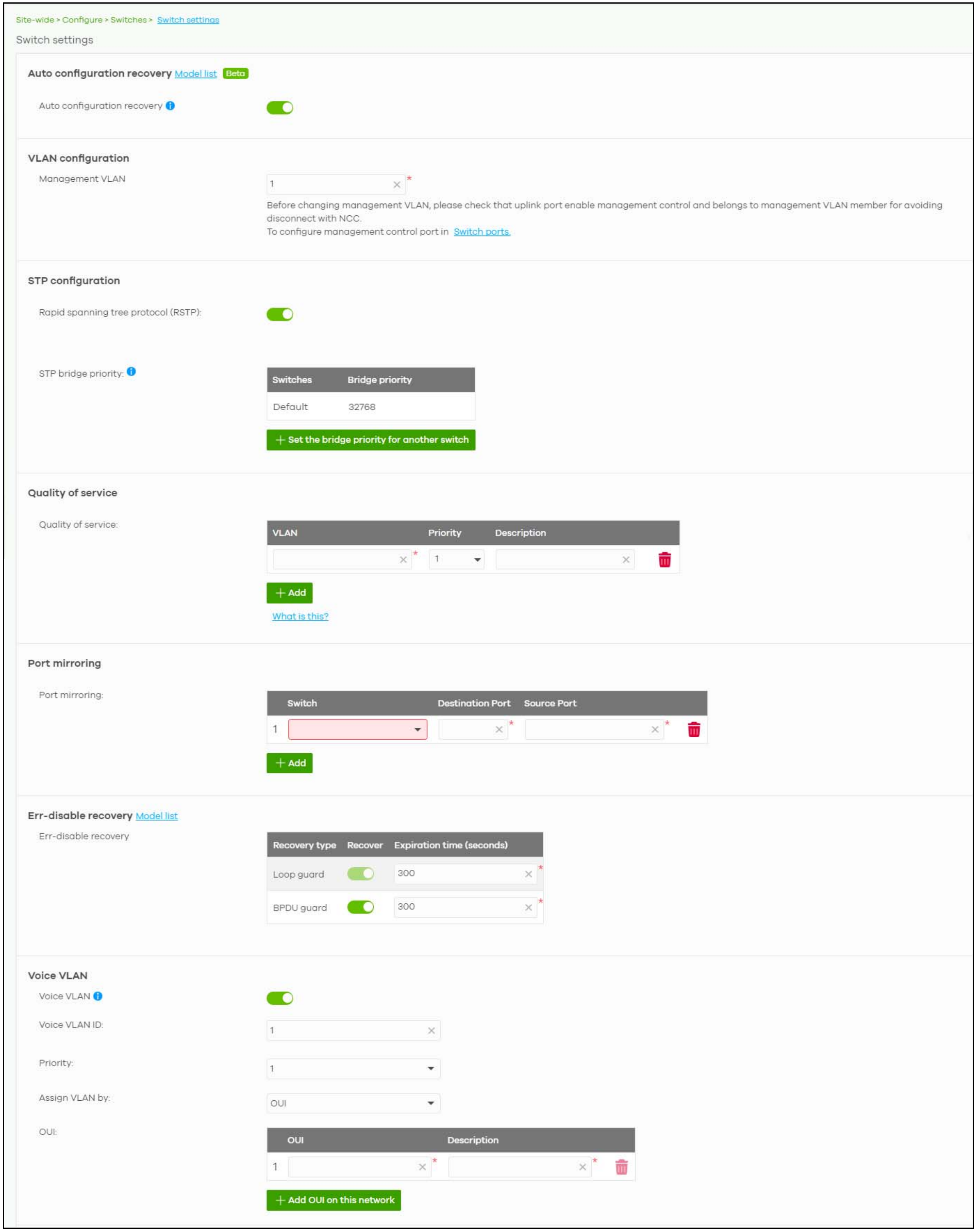
LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identification purposes.
Schedule templates	Select a pre-defined schedule template or select **Custom schedule** and manually configure the day and time at which PoE is enabled.
Day	This shows the day of the week.
Availability	Click **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.

6.3.8 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 97 Site-wide > Configure > Switches > Switch settings



Site-wide > Configure > Switches > Switch settings

Switch settings

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

+ Set the bridge priority for another switch

Quality of service

Quality of service:

VLAN	Priority	Description
*	1	

+ Add

What is this?

Port mirroring

Port mirroring:

	Switch	Destination Port	Source Port
1		*	*

+ Add

Err-disable recovery Model list

Err-disable recovery

Recovery type	Recover	Expiration time (seconds)
Loop guard	●	300 *
BPDU guard	●	300 *

Voice VLAN

Voice VLAN ⓘ ●

Voice VLAN ID: 1

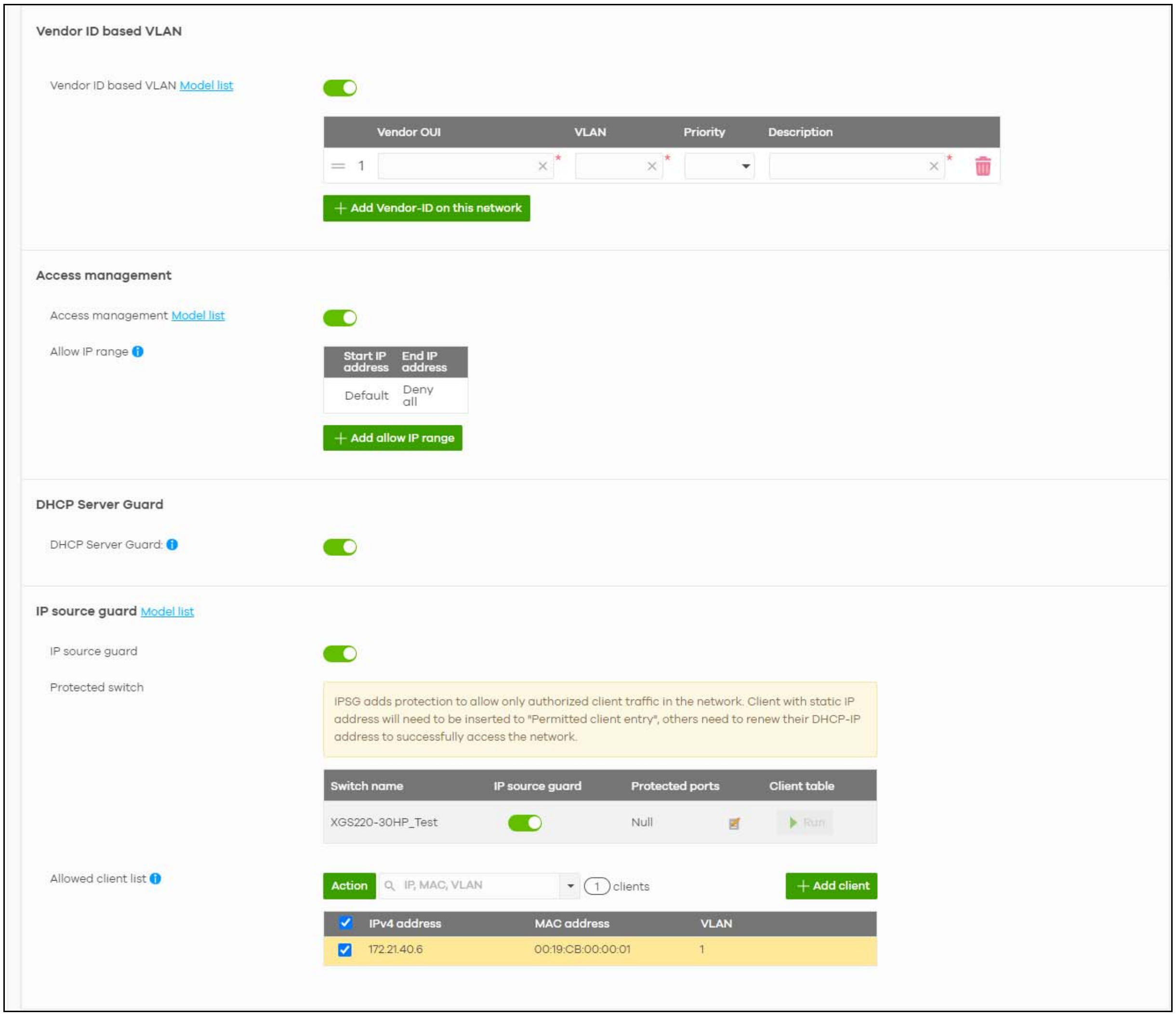
Priority: 1

Assign VLAN by: OUI

OUI:

	OUI	Description
1	*	*

+ Add OUI on this network



Vendor ID based VLAN

Vendor ID based VLAN Model list

	Vendor OUI	VLAN	Priority	Description
1				

+ Add Vendor-ID on this network

Access management

Access management Model list

Allow IP range

Start IP address	End IP address
Default	Deny all

+ Add allow IP range

DHCP Server Guard

DHCP Server Guard:

IP source guard Model list

IP source guard

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
XGS220-30HP_Test		Null	Run

Allowed client list

Action IP, MAC, VLAN 1 clients + Add client

☑	IPv4 address	MAC address	VLAN
☑	172.21.40.6	00:19:CB:00:00:01	1

The following table describes the labels in this screen.

Table 75 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	

Table 75 Site-wide > Configure > Switches > Switch settings (continued)

LABEL	DESCRIPTION
Management 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	
Port mirroring	Click **Add** to create a new entry. Select the Nebula Device 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.
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.

Table 75 Site-wide > Configure > Switches > Switch settings (continued)

LABEL	DESCRIPTION
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	
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.

Table 75 Site-wide > Configure > Switches > Switch settings (continued)

LABEL	DESCRIPTION
Protected switch	This shows the Nebula Device(s). • Select **On** to enable IP source guard protection on the Nebula Device. 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 288 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 **Actions** > **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 **Actions** > **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.

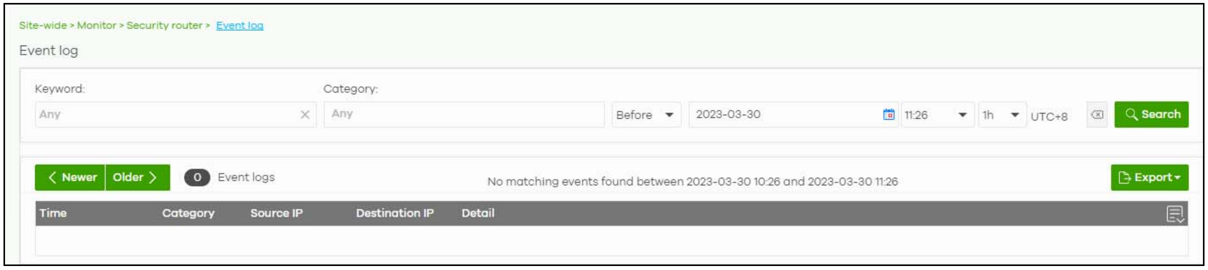
7.2.1 Event Log

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 98 Site-wide > Monitor > Security router > Event log



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

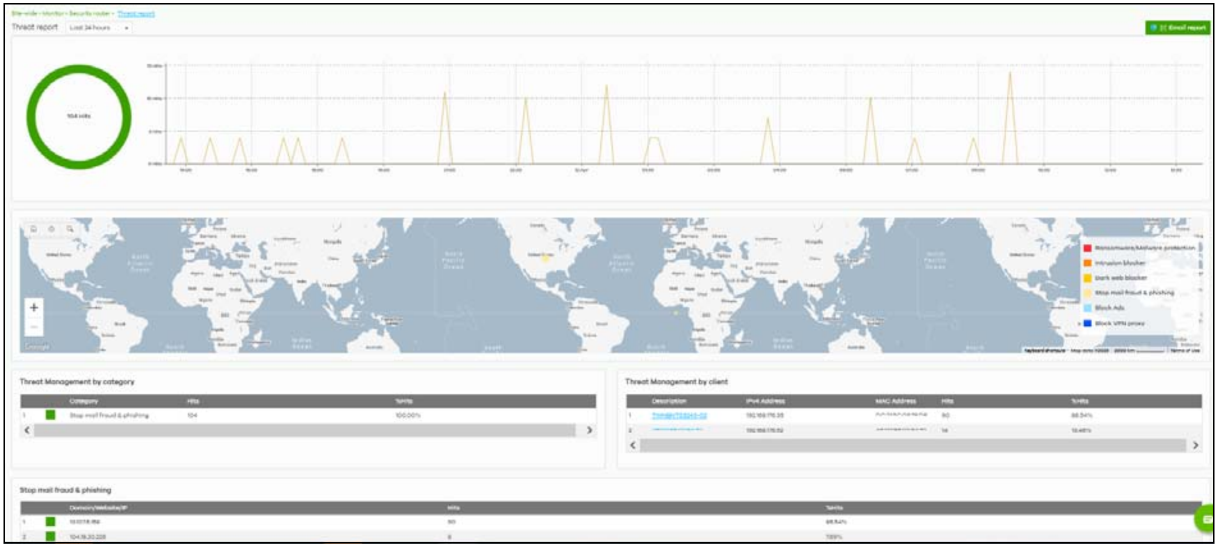
No matching events found between 2023-03-30 10:26 and 2023-03-30 11:26

Time	Category	Source IP	Destination IP	Detail

7.2.2 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 99 Site-wide > Monitor > Security router > Threat report



The following table describes the labels in this screen.

Table 76 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 Management by category	
Category	This shows the name of the category to which the threat belongs. Click the **Category** to display the individual category statistics table. The category statistics table includes the following fields: • **Domain/Website/IP** • **Hits** • **%Hits**
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.
Threat Management 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. The client statistics table includes the following fields: • **Domain/Website/IP** • **Category** • **Hits** • **%Hits**
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.

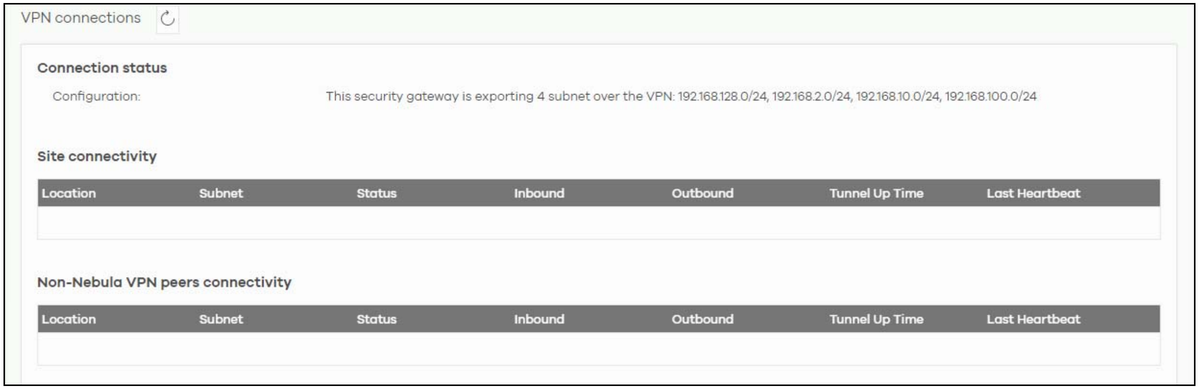
7.2.3 VPN Connections

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 332 for more information.

Click **Site-wide** > **Monitor** > **Security router** > **VPN connections** to access this screen.

Figure 100 Site-wide > Monitor > Security router > VPN connections



VPN connections

Connection status

Configuration: This security gateway is exporting 4 subnet over the VPN: 192.168.128.0/24, 192.168.2.0/24, 192.168.10.0/24, 192.168.100.0/24

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

The following table describes the labels in this screen.

Table 77 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.

Table 77   Site-wide > Monitor > Security router > VPN connections (continued)

LABEL	DESCRIPTION
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.

7.3 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.

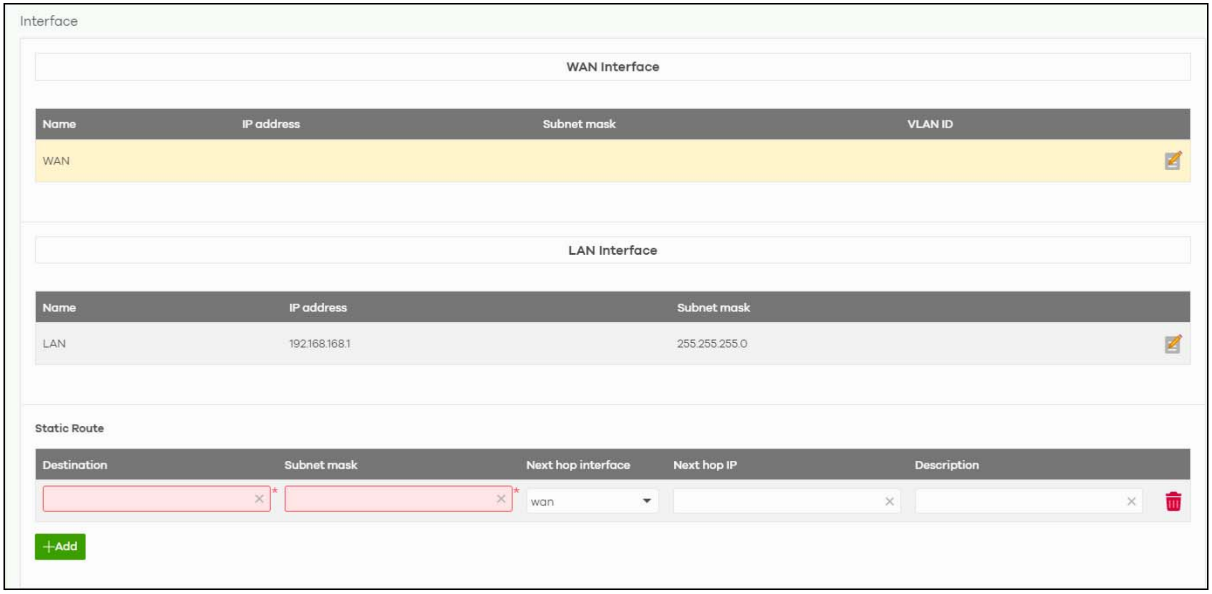
Note: Only one Security Router is allowed per site.

7.3.1 Interface

Use this screen to configure network interfaces on the Nebula Device. An interface consists of a port group, a VLAN ID, and an IP address, plus other configuration settings.

To access this screen, click **Site-wide** > **Configure** > **Security router** > **Interface**.

Figure 101   Site-wide > Configure > Security router > Interface



Interface

WAN Interface

Name	IP address	Subnet mask	VLAN ID
WAN			

LAN Interface

Name	IP address	Subnet mask
LAN	192.168.168.1	255.255.255.0

Static Route

Destination	Subnet mask	Next hop interface	Next hop IP	Description
		wan		

The following table describes the labels in this screen.

Table 78   Site-wide > Configure > Security router > Interface

LABEL	DESCRIPTION
WAN Interface	
Name	This field is read-only.
IP address	This shows the IP address for this interface.

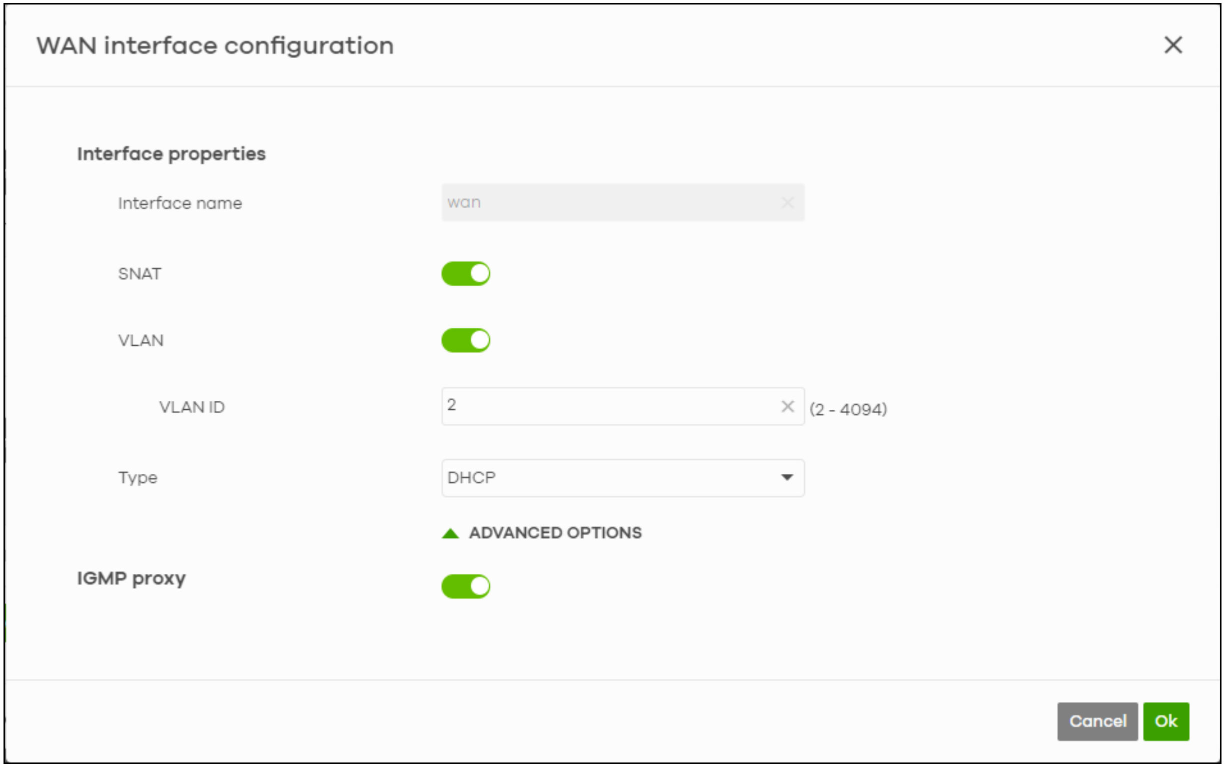
Table 78 Site-wide > Configure > Security router > Interface (continued)

LABEL	DESCRIPTION
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.)
✎	Click the edit icon to modify the 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.
✎	Click the edit icon to modify it.
Static Route	
Destination	Enter the destination IP address.
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.
✎	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.

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 102 Site-wide > Configure > Security router > Interface > WAN interface configuration



WAN interface configuration

Interface properties

Interface name: wan

SNAT: On

VLAN: On

VLAN ID: 2 (2 - 4094)

Type: DHCP

IGMP proxy: On

The following table describes the labels in this screen.

Table 79 Site-wide > Configure > Security router > Interface > WAN interface configuration

LABEL	DESCRIPTION
Interface properties	
Interface name	Specify a name for the WAN interface.
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.

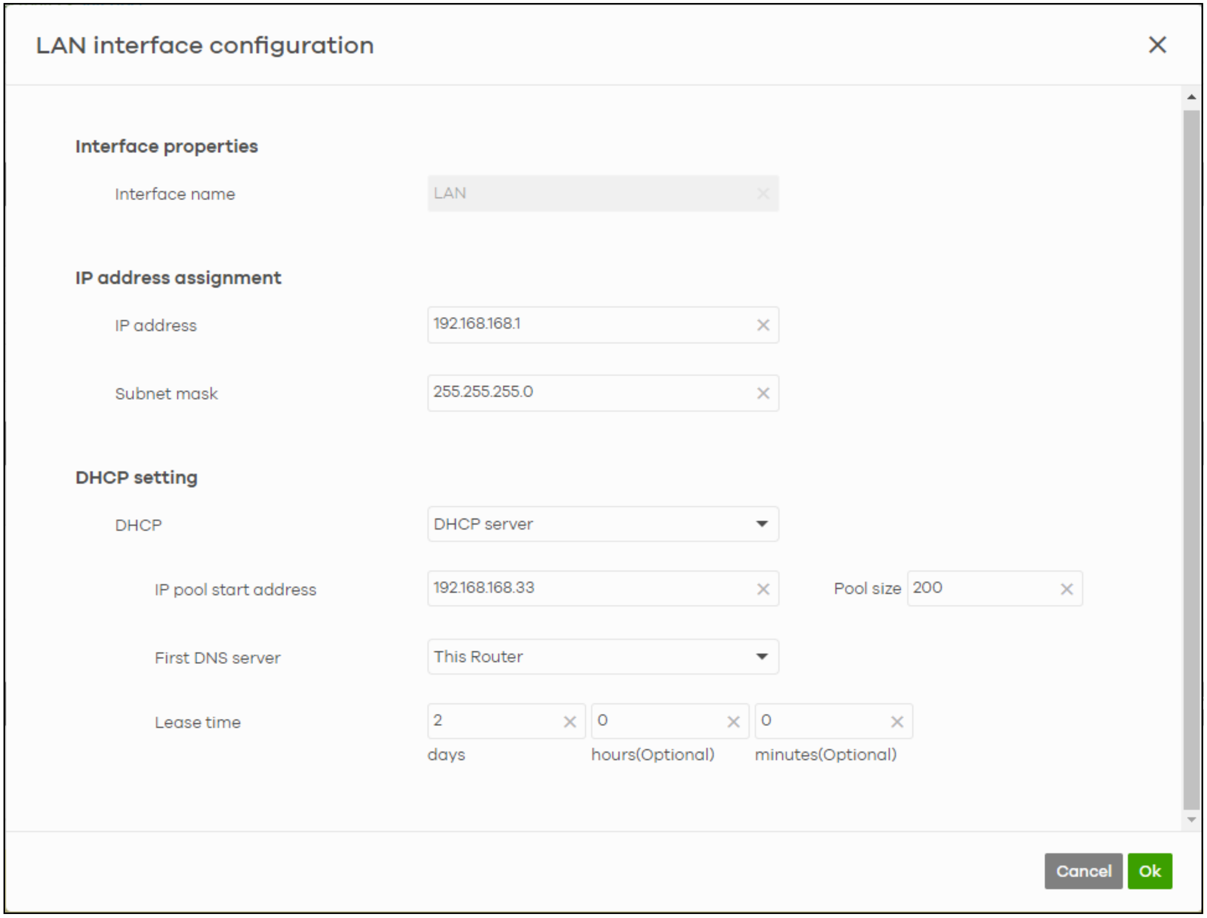
Table 79 Site-wide > Configure > Security router > Interface > WAN interface configuration (continued)

LABEL	DESCRIPTION
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	
Connection trigger	Select when to have the Nebula Device establish the PPP connection. **Auto connect** – select this to not let the connection time out. **On demand** – select this to automatically bring up the connection when the Nebula Device receives packets destined for the Internet.
PPPoE passthrough	Select this to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP through the Nebula Device. Each host can have a separate account and a public WAN IP address. PPPoE passthrough is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE passthrough if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
IGMP proxy	Select this to allow the Nebula Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
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 103 Site-wide > Configure > Security router > Interface > LAN interface configuration



LAN interface configuration

Interface properties

Interface name: LAN

IP address assignment

IP address: 192.168.168.1

Subnet mask: 255.255.255.0

DHCP setting

DHCP: DHCP server

IP pool start address: 192.168.168.33

Pool size: 200

First DNS server: This Router

Lease time: 2 days, 0 hours(Optional), 0 minutes(Optional)

The following table describes the labels in this screen.

Table 80 Site-wide > Configure > Security router > Interface > LAN interface configuration

LABEL	DESCRIPTION
Interface properties	
Interface name	Specify a name for the LAN interface.
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.
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.

Table 80 Site-wide > Configure > Security router > Interface > LAN interface configuration (continued)

LABEL	DESCRIPTION
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	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.
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.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

7.3.2 Threat Management

Use this screen to enable the threat management categories such as:

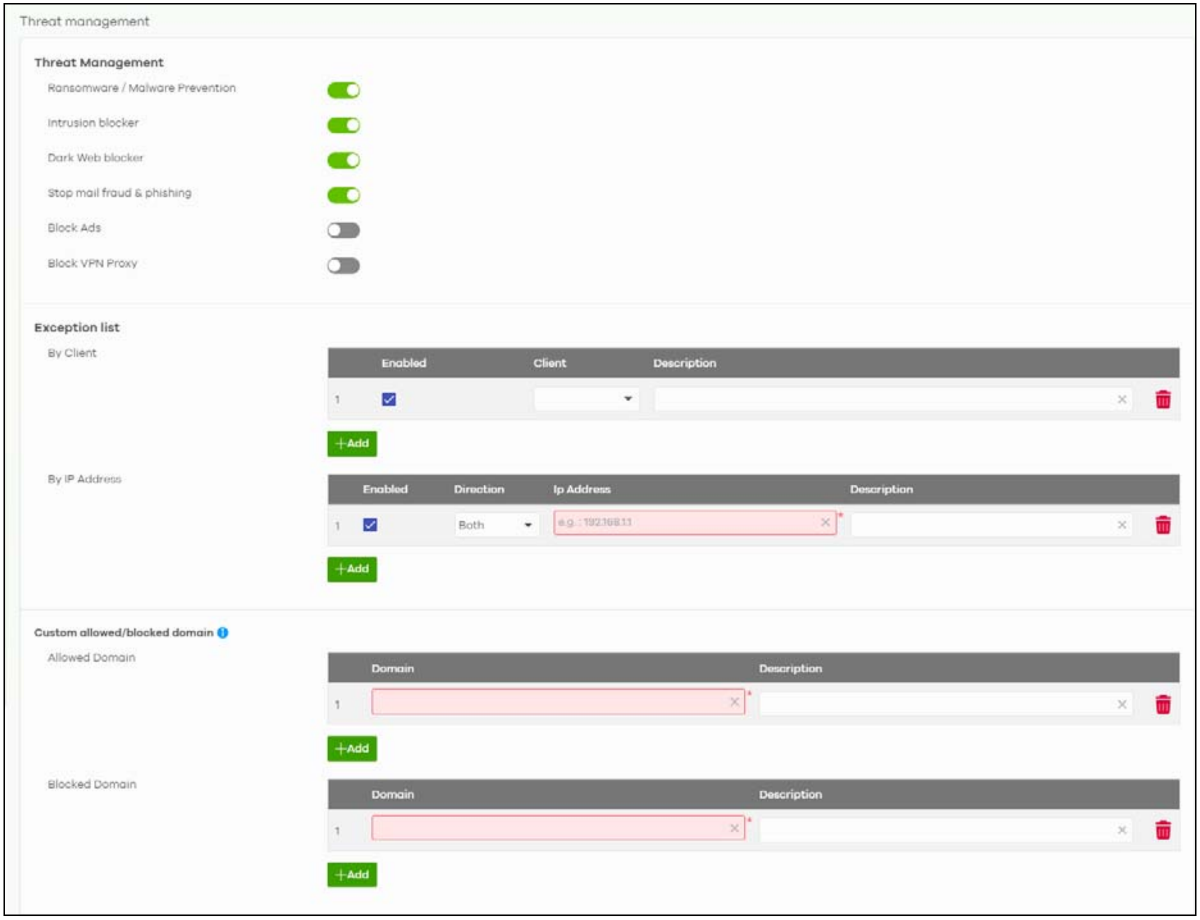
- Ransomware and malware prevention that protects LAN clients from accessing or downloading harmful web contents.
- Intrusion blocker that prevents personal data theft in your network.
- Dark Web blocker that prevents unauthorized access from TOR proxies to the LAN clients.
- Stop mail fraud and phishing 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 104 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	☑		

By IP Address

	Enabled	Direction	Ip Address	Description
1	☑	Both	e.g.: 192.168.1.1	

Custom allowed/blocked domain

Allowed Domain

	Domain	Description
1		

Blocked Domain

	Domain	Description
1		

The following table describes the labels in this screen.

Table 81 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 81 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 194 and Section 4.5.0.2 on page 196 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 81 Site-wide > Configure > Security router > Threat management (continued)

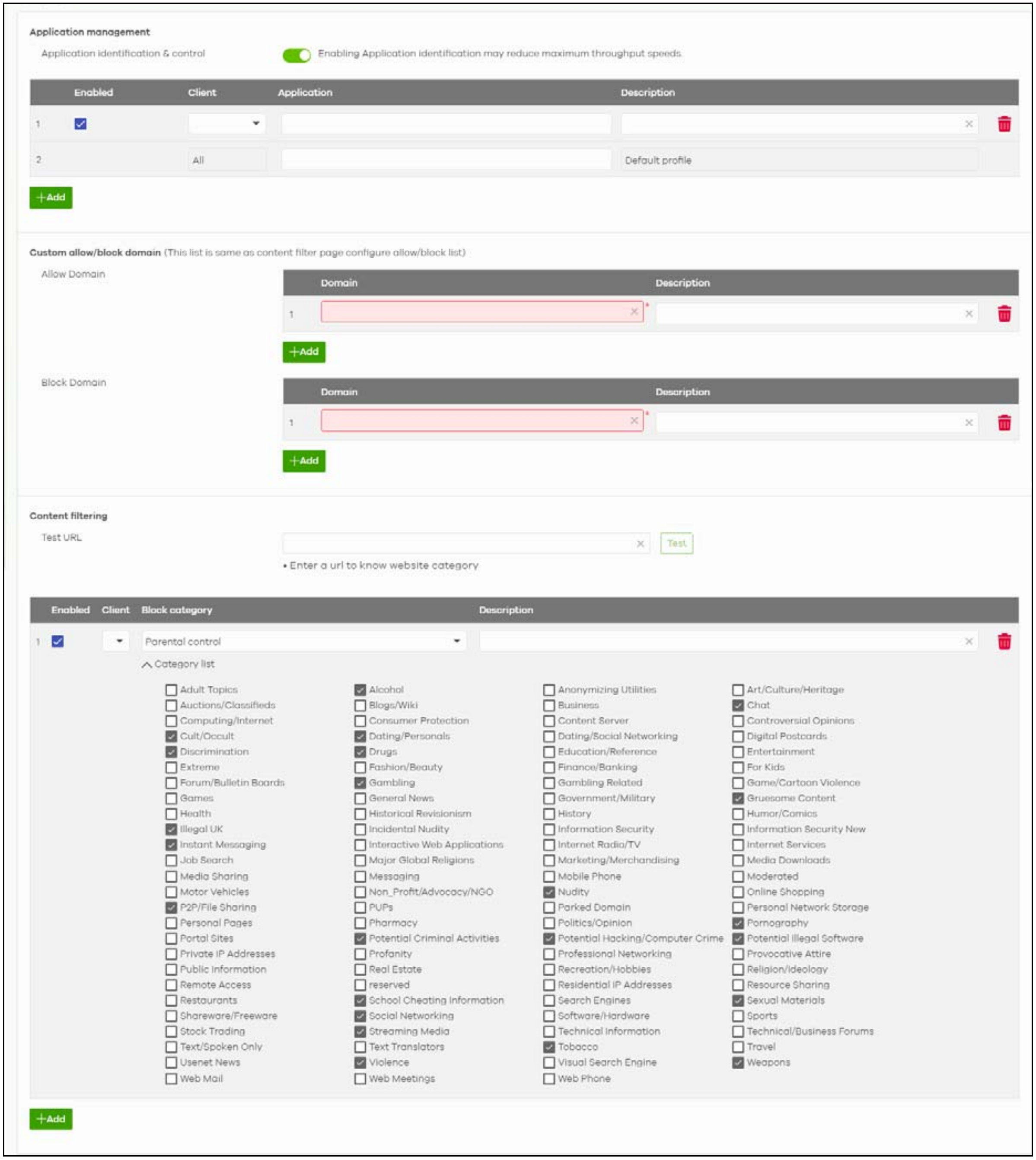
LABEL	DESCRIPTION
Allowed Domain	If you want to access any site, regardless of their content rating, add them to this list. **Domain** – Enter the host name, such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains 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 Filtering 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 filtering.

Figure 105 Site-wide > Configure > Security router > Traffic management



Application management

Application identification & control — ● Enabling Application identification may reduce maximum throughput speeds

	Enabled	Client	Application	Description
1	☑	▾		
2		All		Default profile

+Add

Custom allow/block domain (This list is same as content filter page configure allow/block list)

Allow Domain

	Domain	Description
1	*	

+Add

Block Domain

	Domain	Description
1	*	

+Add

Content filtering

Test URL [ ] Test

- Enter a url to know website category

	Enabled	Client	Block category	Description
1	☑	▾	Parental control ▾	

^ Category list

□ Adult Topics
□ Auctions/Classifieds
□ Computing/Internet
☑ Cult/Occult
☑ Discrimination
□ Extreme
□ Forum/Bulletin Boards
□ Games
□ Health
☑ Illegal UK
☑ Instant Messaging
□ Job Search
□ Media Sharing
□ Motor Vehicles
☑ P2P/File Sharing
□ Personal Pages
□ Portal Sites
□ Private IP Addresses
□ Public Information
□ Remote Access
□ Restaurants
□ Shareware/Freeware
□ Stock Trading
□ Text/Spoken Only
□ Usenet News
□ Web Mail

☑ Alcohol
□ Blogs/Wiki
□ Consumer Protection
☑ Dating/Personals
☑ Drugs
□ Fashion/Beauty
☑ Gambling
□ General News
□ Historical Revisionism
□ Incidental Nudity
□ Interactive Web Applications
□ Major Global Religions
□ Messaging
□ Non_Profit/Advocacy/NGO
□ PUPs
□ Pharmacy
☑ Potential Criminal Activities
□ Profanity
□ Real Estate
□ reserved
☑ School Cheating Information
☑ Social Networking
☑ Streaming Media
□ Text Translators
☑ Violence
□ Web Meetings

□ Anonymizing Utilities
□ Business
□ Content Server
□ Dating/Social Networking
□ Education/Reference
□ Finance/Banking
□ Gambling Related
□ Government/Military
□ History
□ Information Security
□ Internet Radio/TV
□ Marketing/Merchandising
□ Mobile Phone
☑ Nudity
□ Parked Domain
□ Politics/Opinion
☑ Potential Hacking/Computer Crime
□ Professional Networking
□ Recreation/Hobbies
□ Residential IP Addresses
□ Search Engines
□ Software/Hardware
□ Technical Information
☑ Tobacco
□ Visual Search Engine
□ Web Phone

□ Art/Culture/Heritage
☑ Chat
□ Controversial Opinions
□ Digital Postcards
□ Entertainment
□ For Kids
□ Game/Cartoon Violence
☑ Gruesome Content
□ Humor/Comics
□ Information Security New
□ Internet Services
□ Media Downloads
□ Moderated
□ Online Shopping
□ Personal Network Storage
☑ Pornography
☑ Potential Illegal Software
□ Provocative Attire
□ Religion/Ideology
□ Resource Sharing
☑ Sexual Materials
□ Sports
□ Technical/Business Forums
□ Travel
☑ Weapons

+Add

The following table describes the labels in this screen.

Table 82 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**.
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box to turn off the rule.
Client	Select **All** or select a client to apply the rule.
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.
Custom allow/block domain	
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 **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 **Add** to create a domain name profile.
Content filtering	
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 Filtering 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 82 Site-wide > Configure > Security router > Traffic management (continued)

LABEL	DESCRIPTION
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box 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.

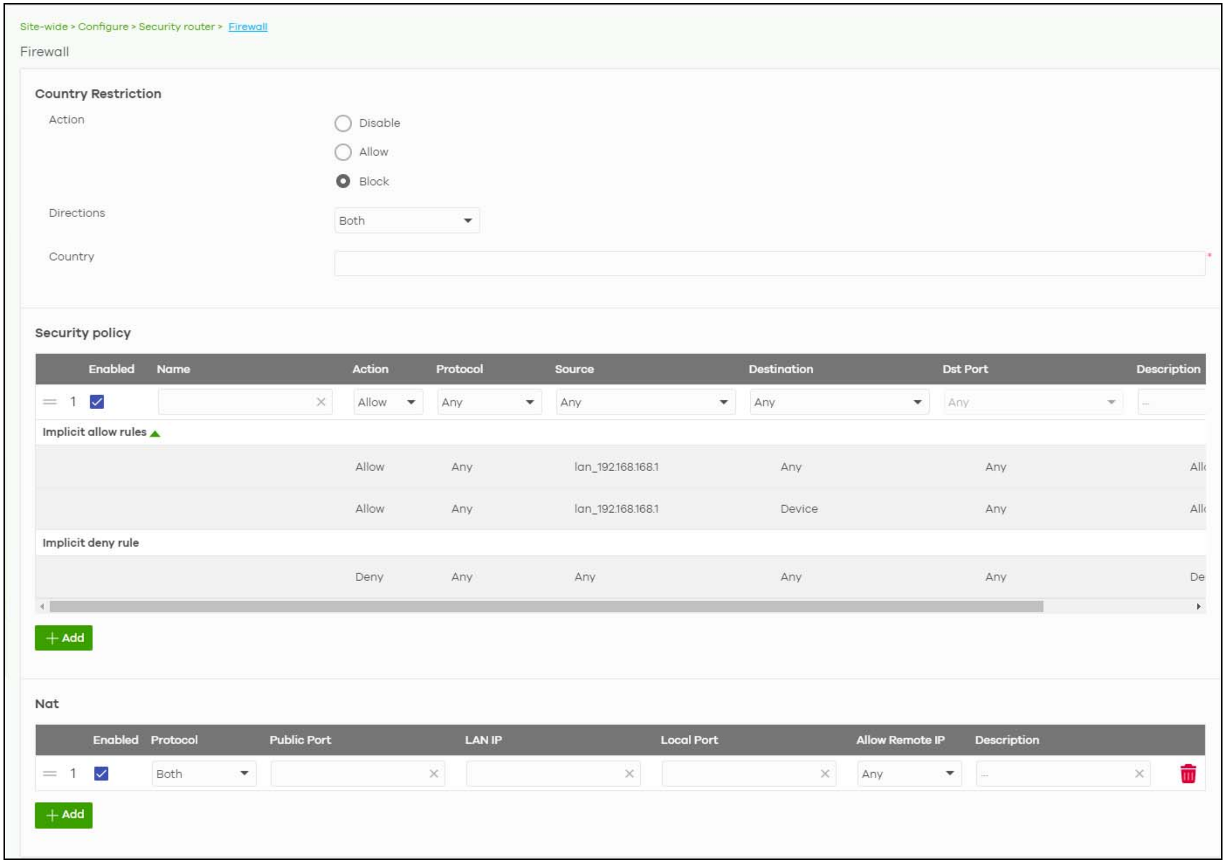
In addition, this screen allows you to create new NAT rules and edit/delete existing NAT rules.

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 106 Site-wide > Configure > Security router > Firewall



Site-wide > Configure > Security router > Firewall

Firewall

Country Restriction

Action: ○ Disable ○ Allow ● Block

Directions: Both

Country:

Security policy

	Enabled	Name	Action	Protocol	Source	Destination	Dst Port	Description
1	☑		Allow	Any	Any	Any	Any	--
Implicit allow rules ▲								
			Allow	Any	lan_192168.1681	Any	Any	All
			Allow	Any	lan_192168.1681	Device	Any	All
Implicit deny rule								
			Deny	Any	Any	Any	Any	De

+ Add

Nat

	Enabled	Protocol	Public Port	LAN IP	Local Port	Allow Remote IP	Description
1	☑	Both				Any	--

+ Add

The following table describes the labels in this screen.

Table 83 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 check box to turn on the rule. Otherwise, clear the check box 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.

Table 83 Site-wide > Configure > Security router > Firewall (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 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 check box to turn on the rule. Otherwise, clear the check box to turn off the rule.
Protocol	Select the IP protocol to which this rule applies. Choices are: **TCP**, **UDP**, and **Both**.
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. Select **Any** to allow all IP addresses.
Description	Enter the descriptive name of the policy of up to 60 printable ASCII characters.
🗑	Click this icon to remove the profile.
Add	Click this button to create a new schedule profile.

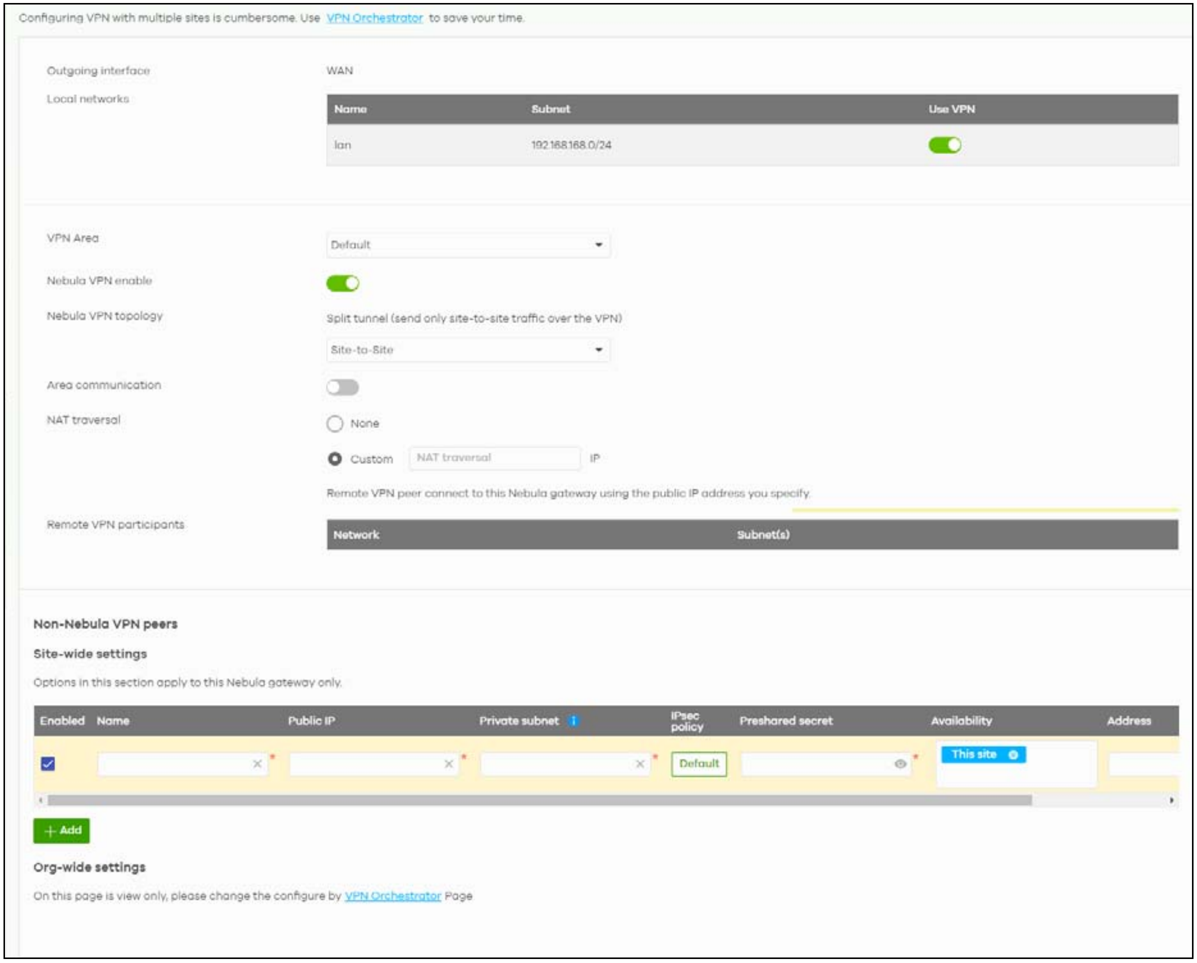
7.3.5 Site-to-Site VPN

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 107 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 84 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.
VPN Area	Select the VPN area of the site. For details, see Section 11.4.4.2 on page 524.
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	Click this to select a topology for the VPN area. For details on topologies, see Section 11.4.4.1 on page 523. 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.

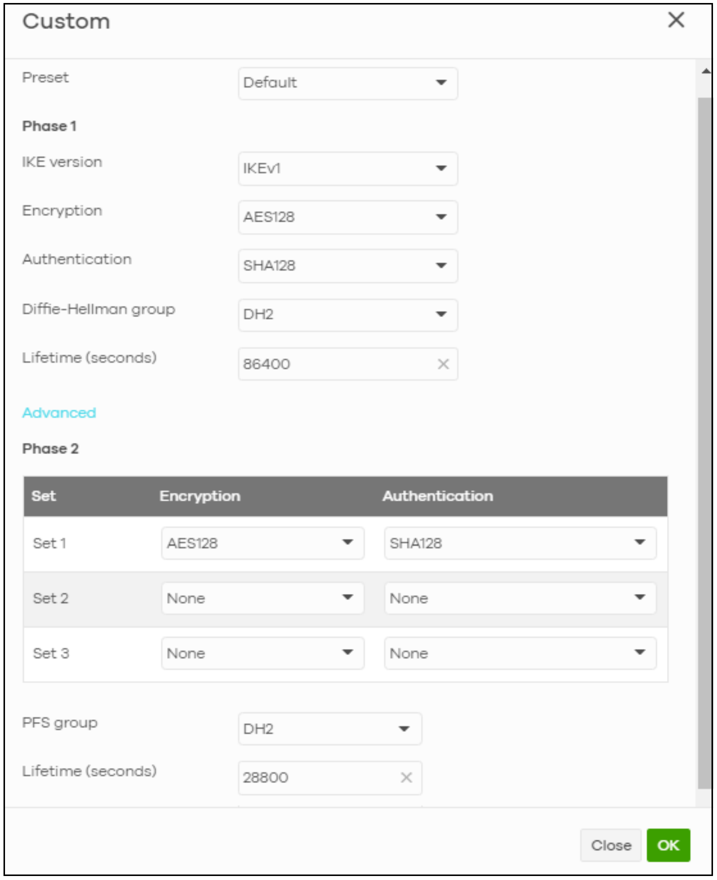
Table 84 Site-wide > Configure > Security router > Site-to-Site VPN (continued)

LABEL	DESCRIPTION
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. 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 check box 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 7.3.5.1 on page 334 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 108 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 85 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 85 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 85 Site-wide > Configure > Security router > Site-to-Site VPN: IPsec Policy (continued)

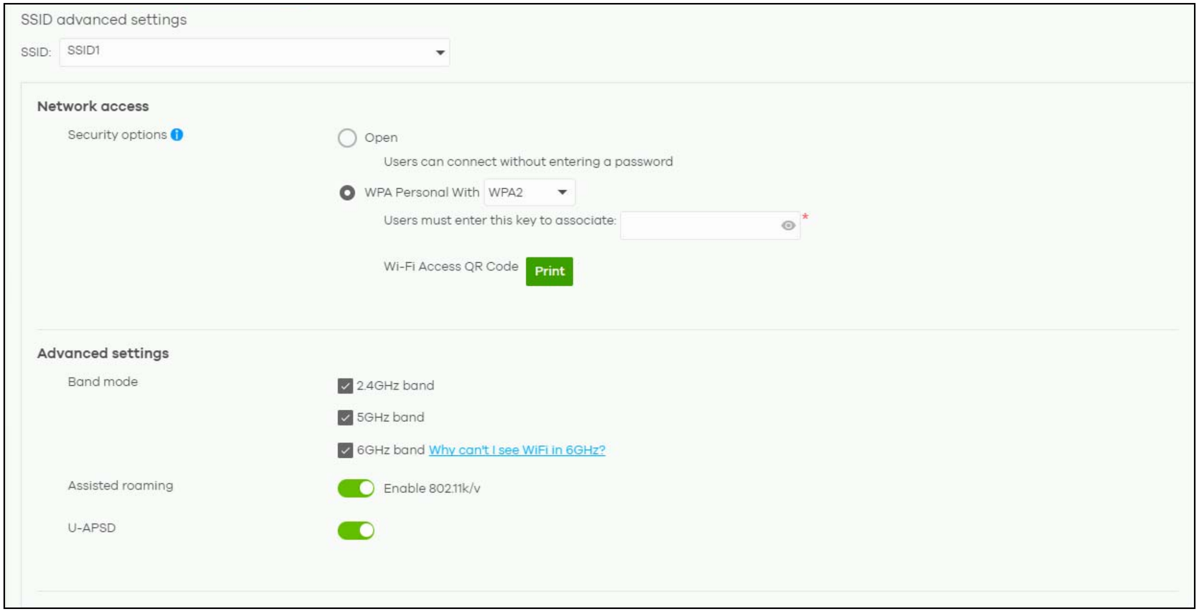
LABEL	DESCRIPTION
Encryption	Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **(None)** – no encryption key or algorithm **DES** – a 56-bit key with the DES encryption algorithm **3DES** – a 168-bit key with the DES encryption algorithm **AES128** – a 128-bit key with 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 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. NCC will redirect to the **Site-wide** > **Configure** > **Access points** > **SSID advanced settings** screen.

Figure 109 Site-Wide > Configure > Access points > SSID advanced settings



SSID advanced settings

SSID: SSID1

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

Band mode

☑ 2.4GHz band

☑ 5GHz band

☑ 6GHz band Why can't I see WiFi in 6GHz?

Assisted roaming: Enable 802.11k/v

U-APSD

The following table describes the labels in this screen.

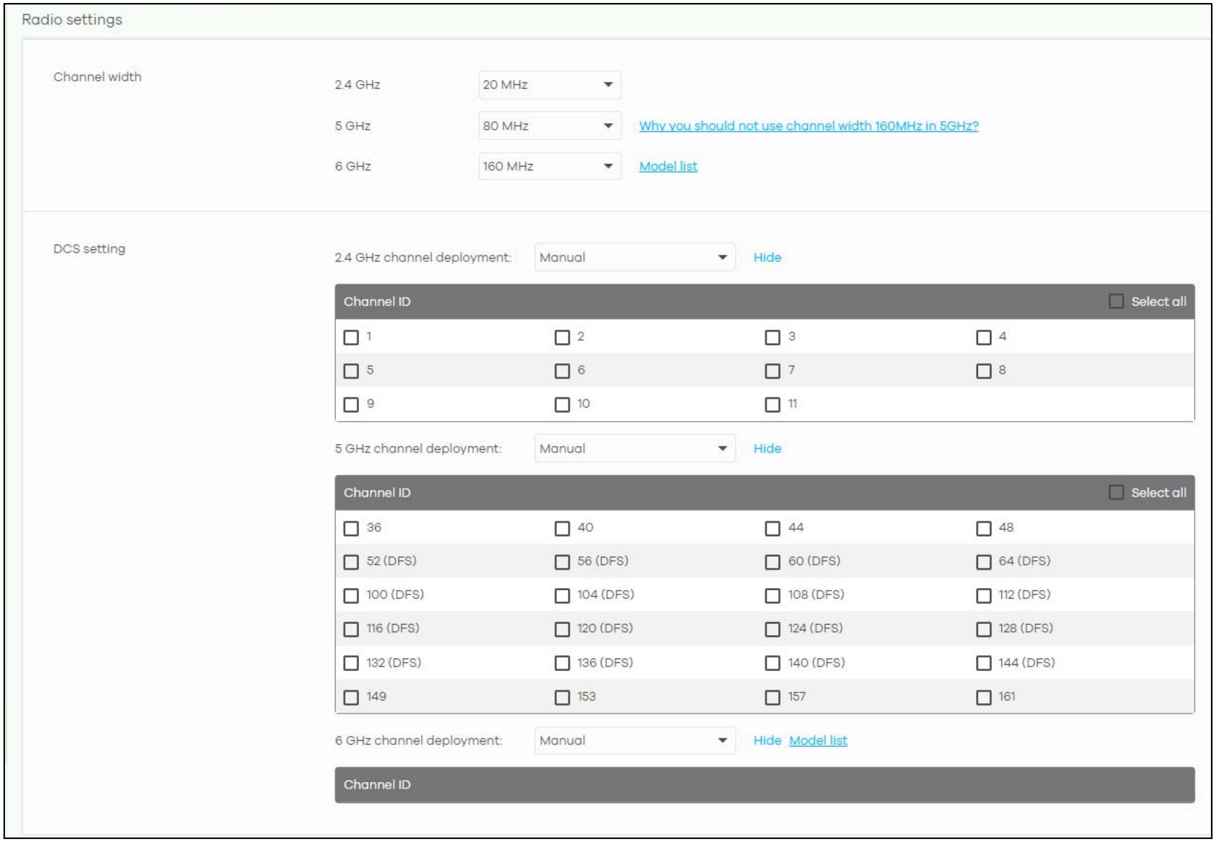
Table 86 Site-Wide > Configure > Access points > SSID advanced settings

LABEL	DESCRIPTION
SSID advanced settings	Select the SSID profile to which the settings you configure here is applied.
Network access	
Security options	Select **Open** to allow any client to associate this network without any data encryption or authentication. Select **WPA Personal With (WPA2/WPA3)** and enter a pre-shared key from 8 to 64 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. Click **Print** to display the QR code that includes the password for quick access. You can save the QR code as PDF.
Advanced settings	
Band mode	Select to have the SSID use either **2.4GHz band**, **5GHz band**, or **6GHz band** only.
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.
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.

7.3.7 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. NCC will redirect to the **Site-wide** > **Configure** > **Access points** > **Radio settings** screen.

Figure 110 Site-wide > Configure > Access points > Radio settings



Radio settings

Channel width

- 2.4 GHz: 20 MHz
- 5 GHz: 80 MHz — Why you should not use channel width 160MHz in 5GHz?
- 6 GHz: 160 MHz — Model list

DCS setting

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

Channel ID

The following table describes the labels in this screen.

Table 87 Site-wide > Configure > Access points > Radio settings

LABEL	DESCRIPTION
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	
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 87 Site-wide > Configure > Access points > Radio settings (continued)

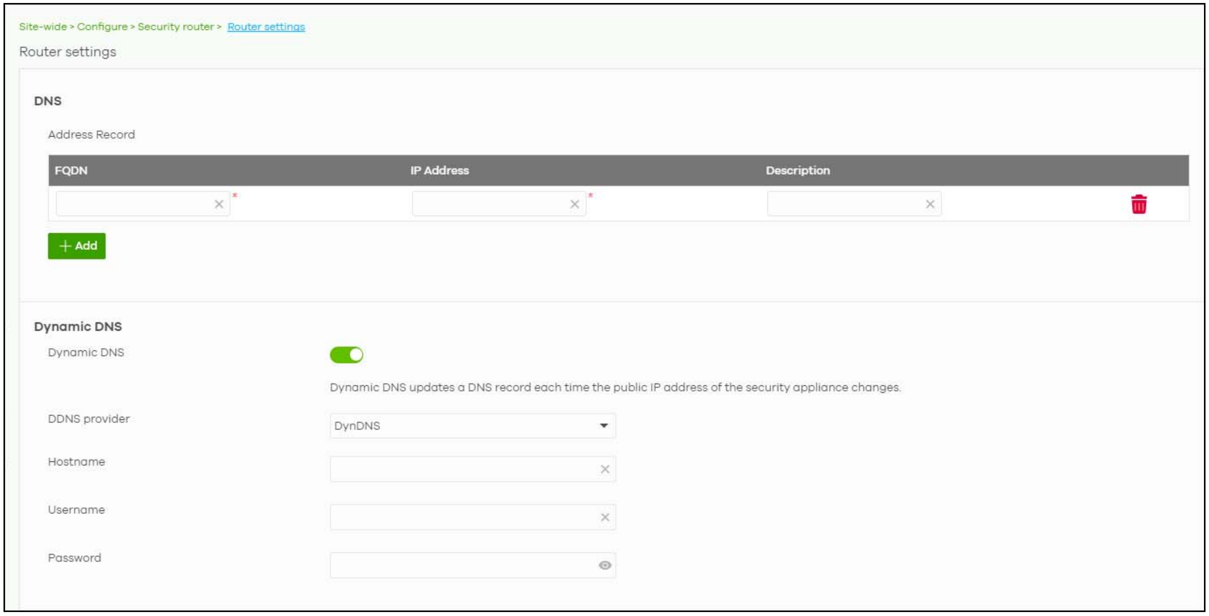
LABEL	DESCRIPTION
5 GHz channel deployment	Select how you want to specify the channels the Nebula Device switches between for 5 GHz operation. Select **All available channels** to have the Nebula Device automatically select the best channel. Select **Manual** to select the individual channels the Nebula 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.

7.3.8 Router Settings

Use this screen to configure DNS settings.

Click **Site-wide** > **Configure** > **Security router** > **Router settings** to access this screen.

Figure 111 Site-wide > Configure > Security router > Router settings



Site-wide > Configure > Security router > Router settings

Router settings

DNS

Address Record

FQDN	IP Address	Description

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

The following table describes the labels in this screen.

Table 88 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 "*." 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 60 printable ASCII characters.
🗑	Click this icon to remove the entry.
Add	Click this button to create a new entry.
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 used when you registered your domain name.
Password	Enter the password provided by the DDNS provider.

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 192.

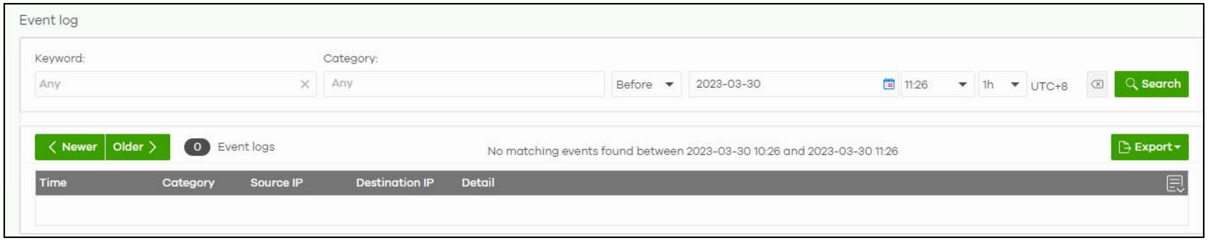
8.2.2 Event Log

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 112 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

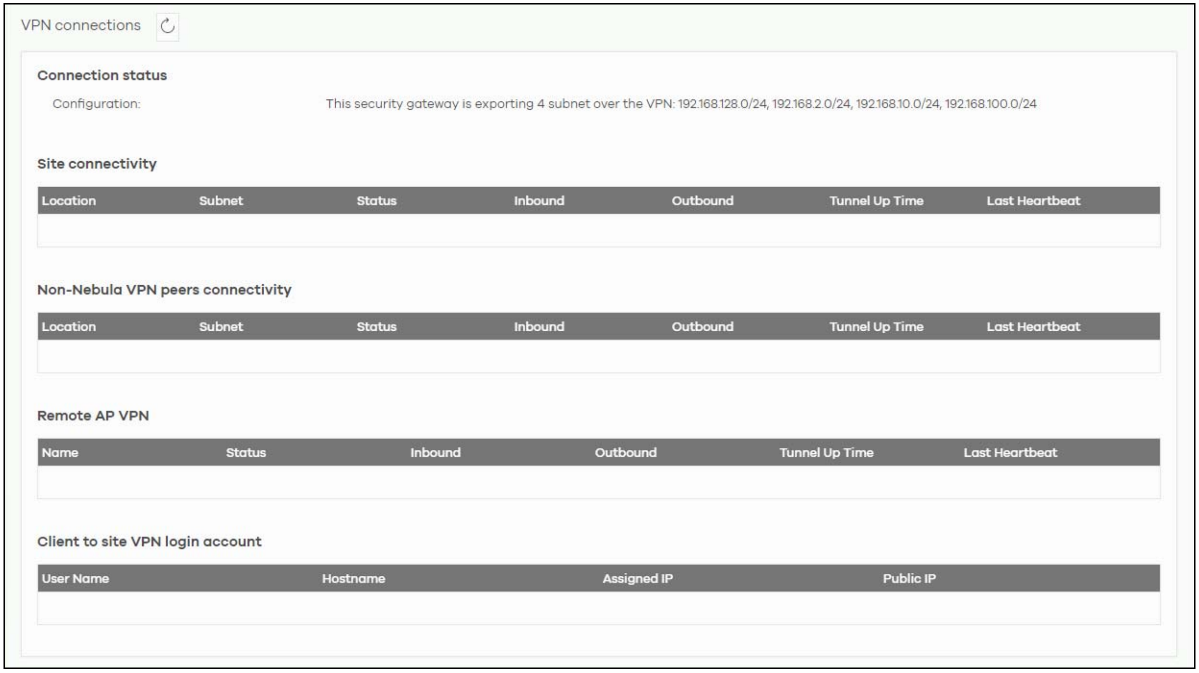
8.2.3 VPN Connections

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 8.3.5 on page 365 for more information.

Click **Site-wide** > **Monitor** > **Firewall** > **VPN connections** to access this screen.

Figure 113 Site-wide > Monitor > Firewall > VPN connections



VPN connections

Connection status

Configuration: This security gateway is exporting 4 subnet over the VPN: 192.168.128.0/24, 192.168.2.0/24, 192.168.10.0/24, 192.168.100.0/24

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

The following table describes the labels in this screen.

Table 89 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.
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	

Table 89 Site-wide > Monitor > Firewall > VPN connections (continued)

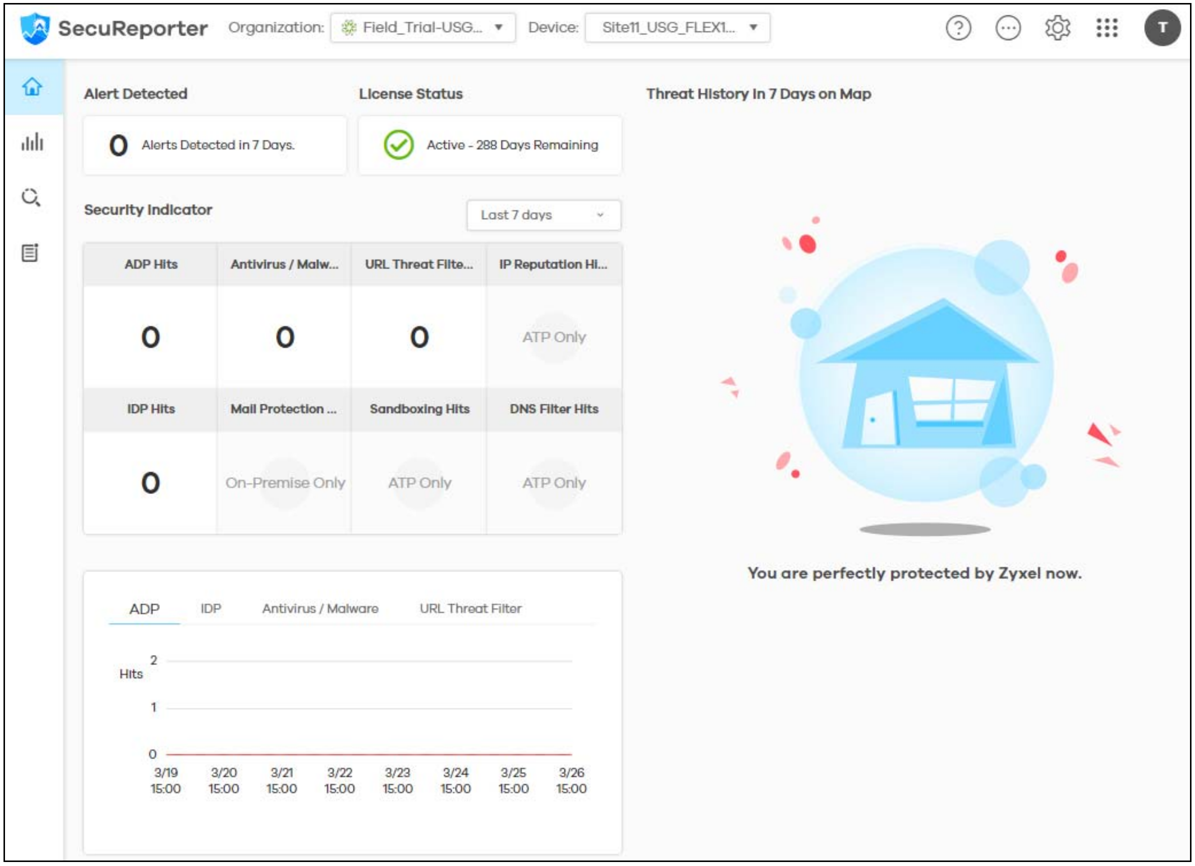
LABEL	DESCRIPTION
Location	This shows the name of the site to which the Non-Nebula peer gateway (Zyxel or non-Zyxel IPSec VPN gateway and Cloud VPN (Azure VPN or AWS VPN)) is assigned. Click the name to go to the **Site-wide** > **Configure** > **Firewall** > **Site-to-Site VPN** screen, where you can modify the VPN settings.
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 filtering, 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 114 Site-wide > Monitor > Firewall > SecuReporter



SecuReporter Organization: Field_Trial-USG... Device: Site11_USG_FLEX1...

Alert Detected

0 Alerts Detected in 7 Days.

License Status

Active - 288 Days Remaining

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

Threat History In 7 Days on Map

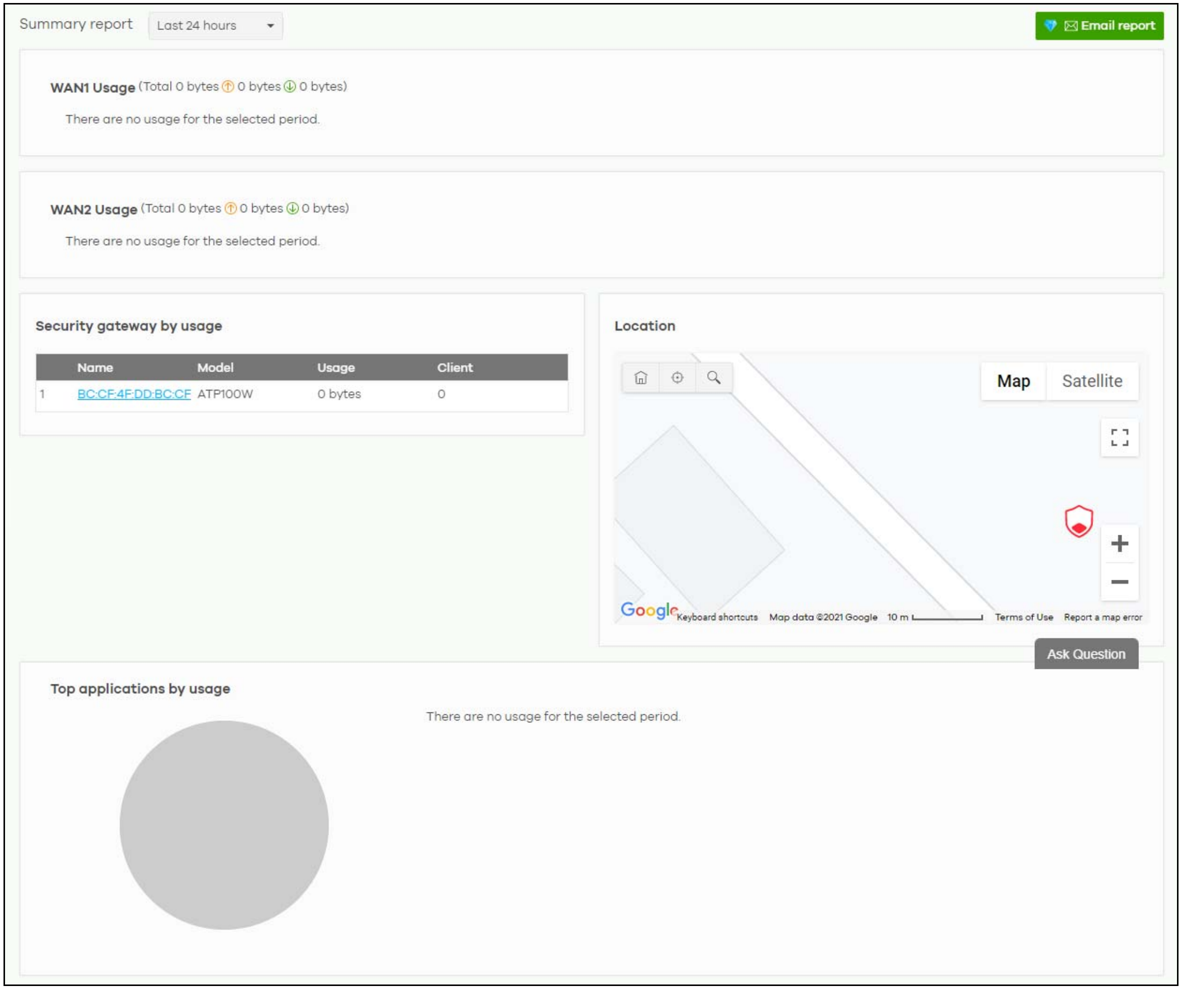
You are perfectly protected by Zyxel now.

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 115 Site wide > Monitor > Firewall > Summary 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.

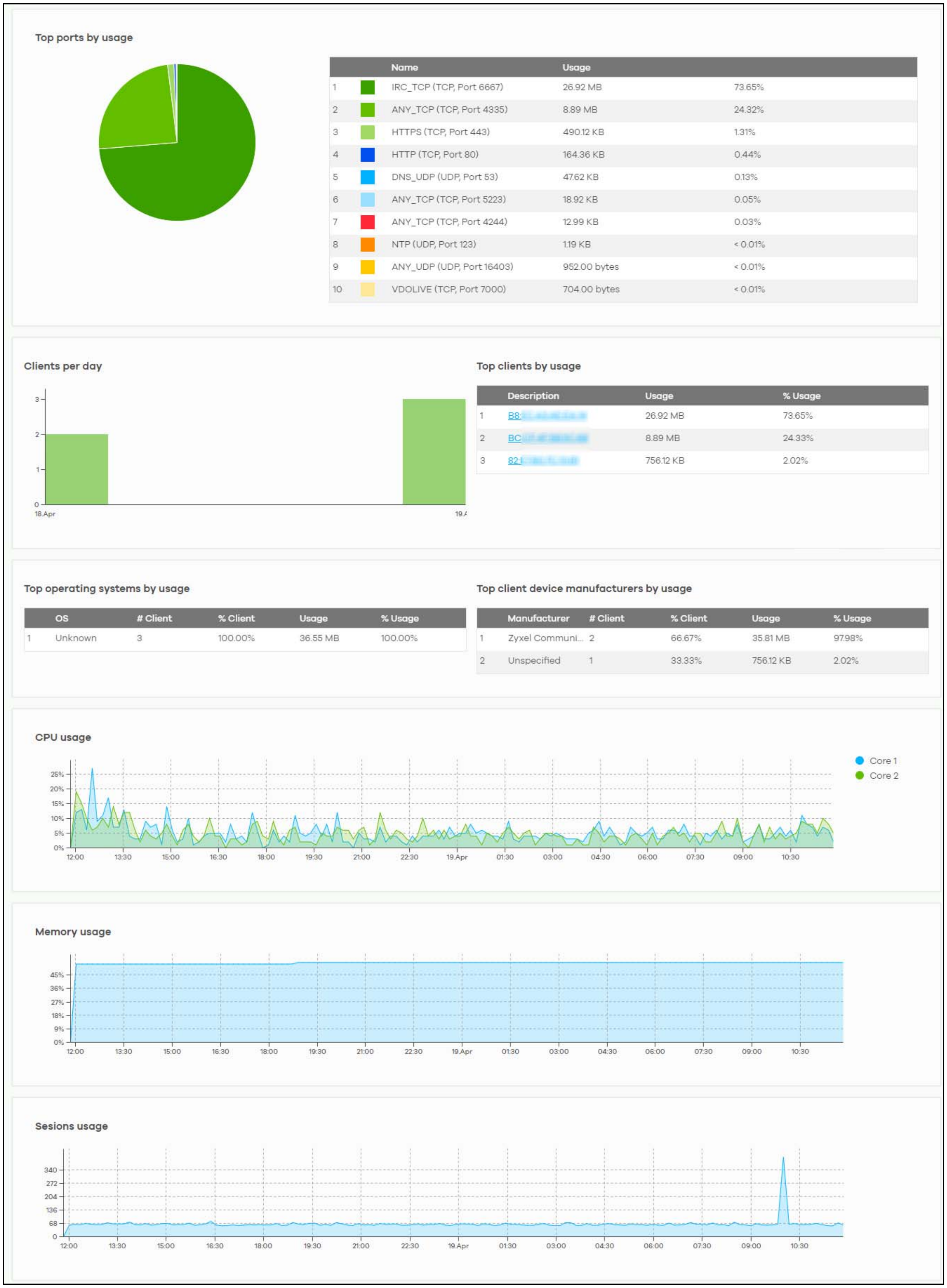
Security gateway by usage

	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 90 Site-wide > Monitor > Firewall > Summary report

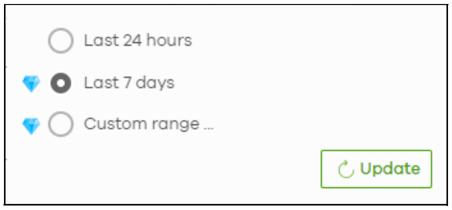
LABEL	DESCRIPTION
Security gateway – Summary report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ● Last 7 days ○ 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 90   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

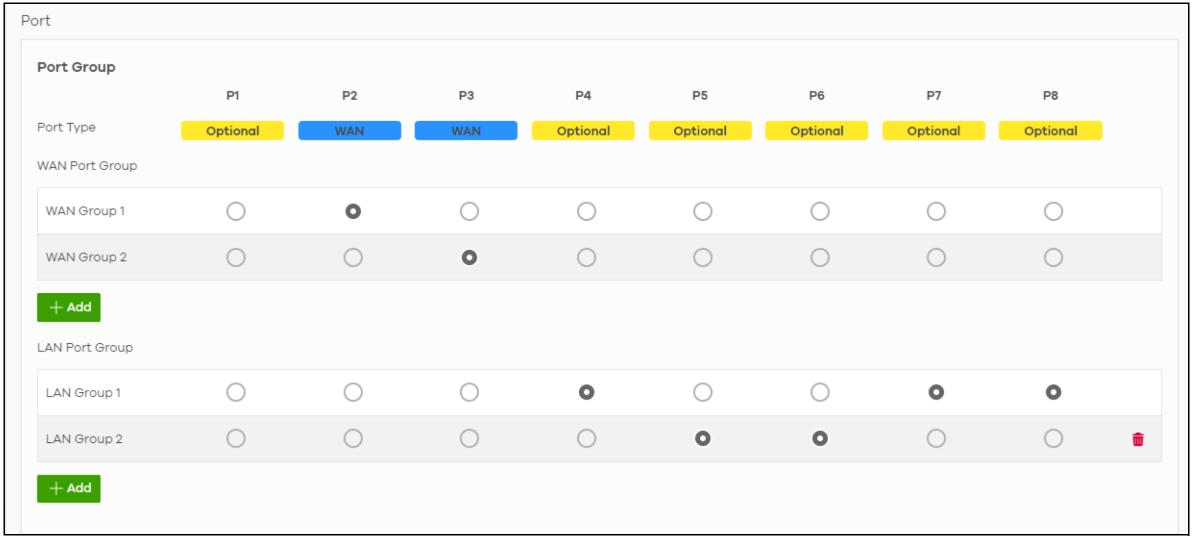
Use the **Configure** menus to configure interface addressing, firewall, site-to-site VPN, captive portal, traffic shaping, authentication server and other gateway settings for the Nebula Device of the selected site.

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 116 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	○	○	●	○	○	○	○	○	
+ Add									
LAN Port Group									
LAN Group 1	○	○	○	●	○	○	●	●	
LAN Group 2	○	○	○	○	●	●	○	○	🗑
+ Add									

The following table describes the labels in this screen.

Table 91 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 13 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 91 Site-wide > Configure > Firewall > Port (continued)

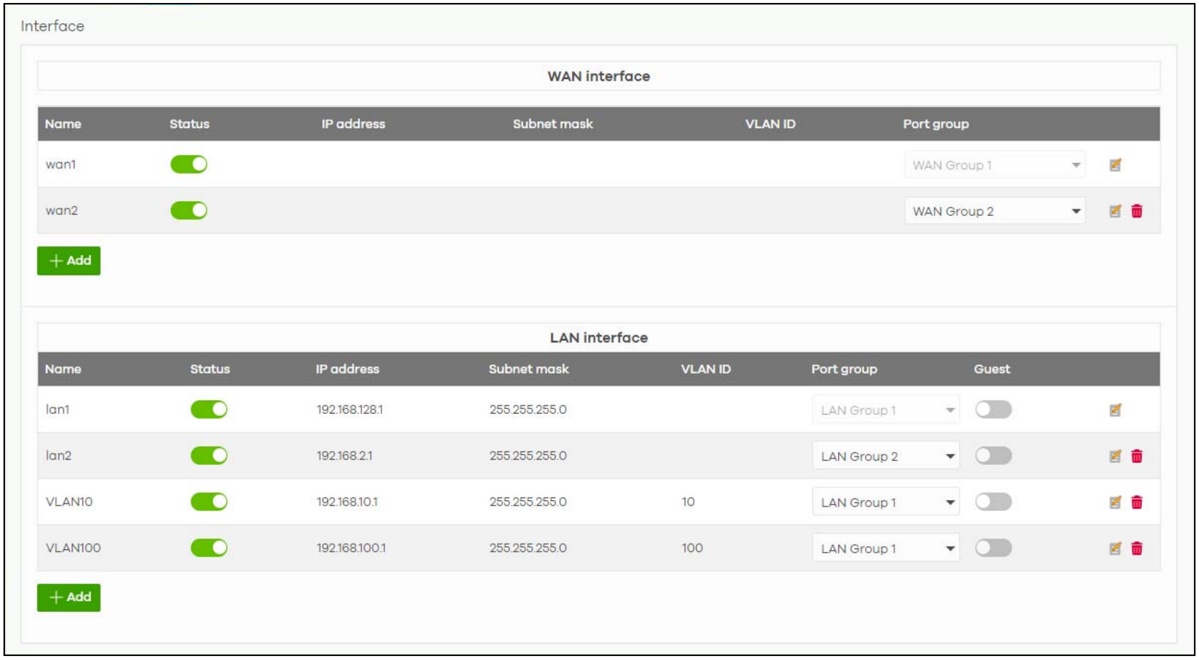
LABEL	DESCRIPTION
Add	Click this button to create a new WAN port group.
LAN Port Group	
LAN Group 1	This shows the name of the LAN port group.
🗑	Click this icon to remove a LAN port group.
Add	Click this button to create a new LAN port group.
Close	Click **Close** to exit this screen without saving.
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 117 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 92 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.

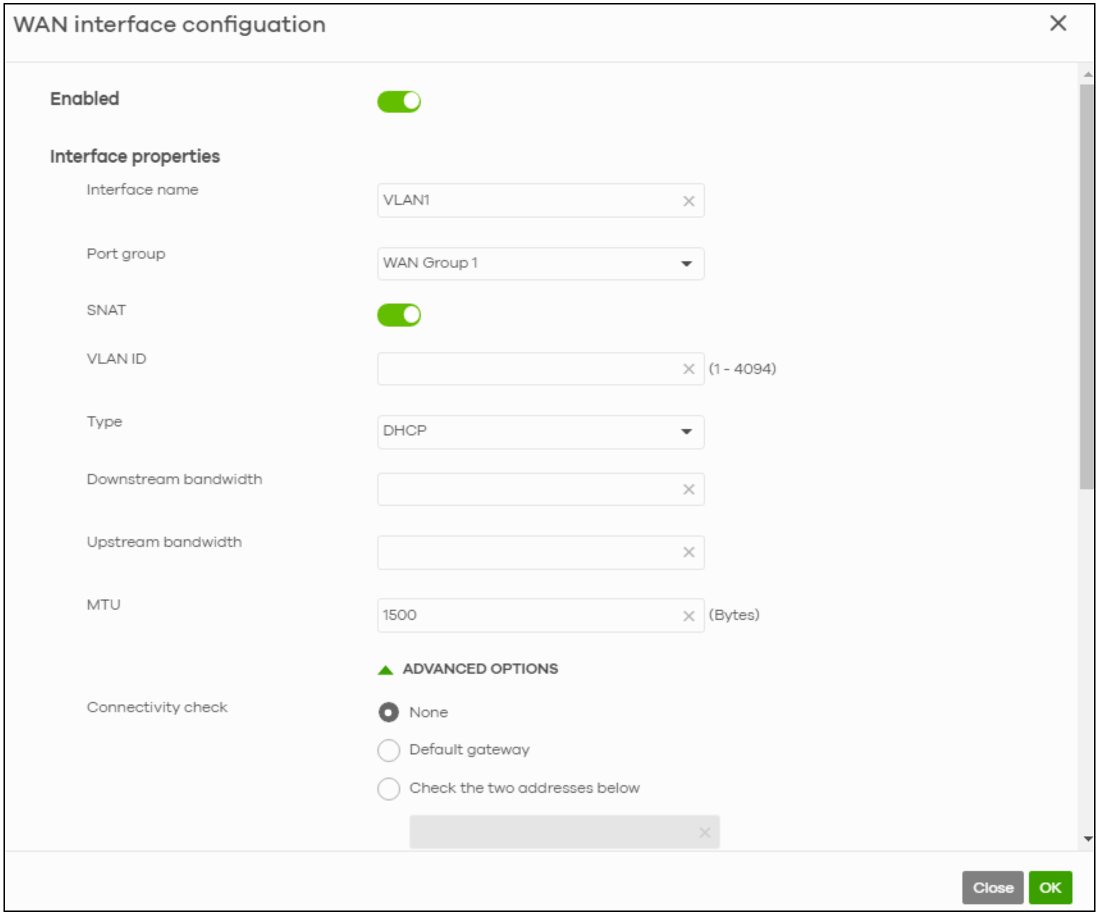
Table 92 Site-wide > Configure > Firewall > Interface (continued)

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 to (network) 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 to (network) belong.
Guest	Select **On** 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.
✎	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 118 Site-wide > Configure > Firewall > Interface > WAN interface configuration



WAN interface configuation

Enabled: ON

Interface properties

Interface name: VLAN1

Port group: WAN Group 1

SNAT: ON

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 93 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 to (network) 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 93 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.
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	
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.

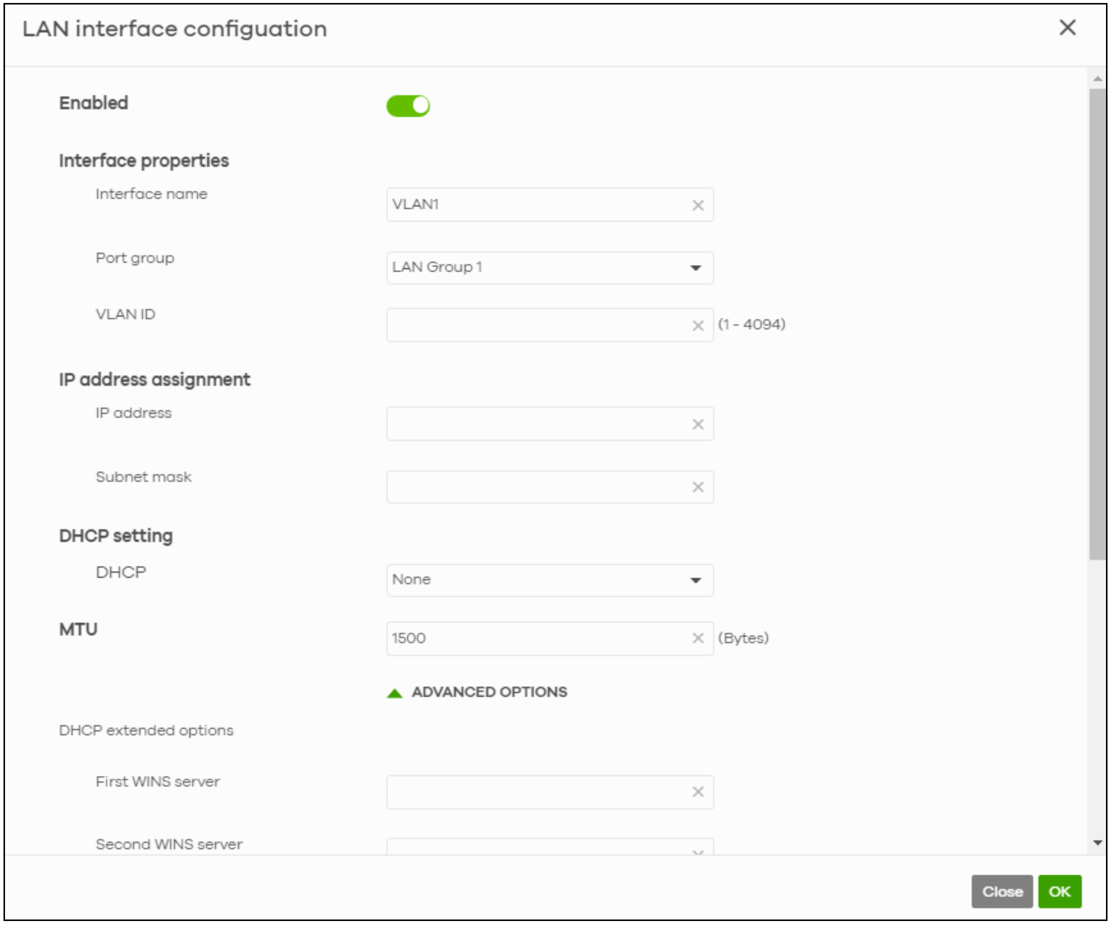
Table 93 Site-wide > Configure > Firewall > Interface > WAN interface configuration (continued)

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.
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 119 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)

▲ ADVANCED OPTIONS

DHCP extended options

First WINS server:

Second WINS server:

The following table describes the labels in this screen.

Table 94 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 to (network) 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.
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 94 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.
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.
Add New	Click this to create an entry in the Static DHCP table.
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	

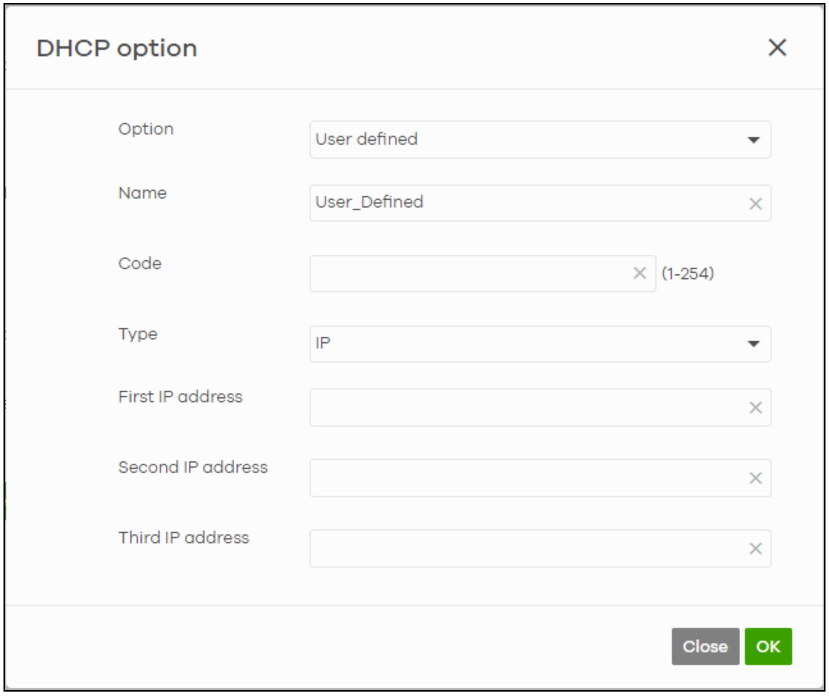
Table 94 Site-wide > Configure > Firewall > Interface > LAN interface configuration (continued)

LABEL	DESCRIPTION
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 120 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 95 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.

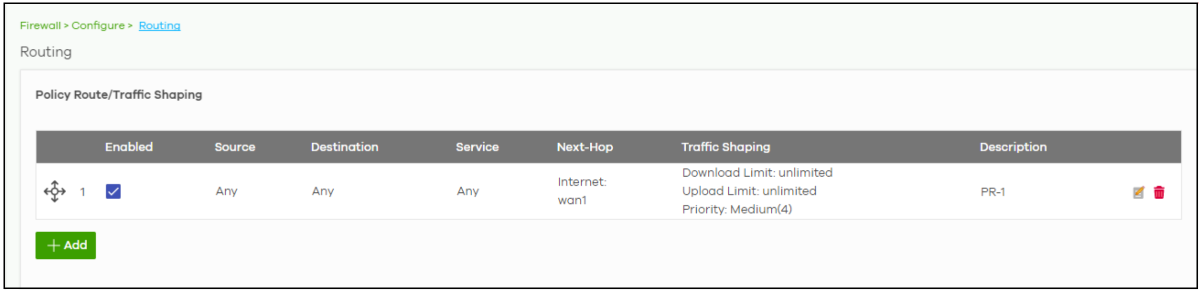
8.3.3 Routing

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 121 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	✎ 🗑

+ Add

The following table describes the labels in this screen.

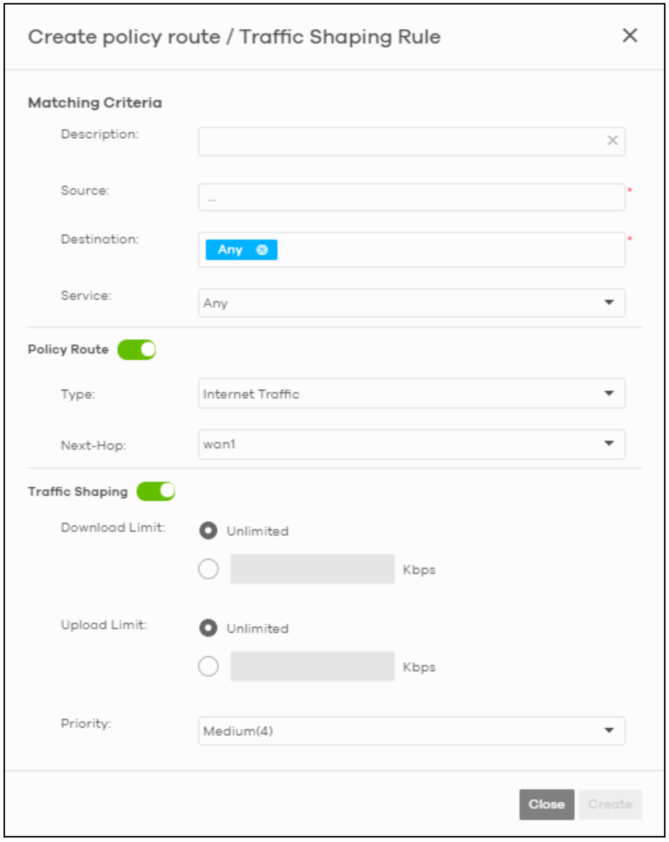
Table 96 Site-wide > Configure > Firewall > Routing: Policy Route/Traffic Shaping

LABEL	DESCRIPTION
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box 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.
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 8.3.7.1 on page 380 for more information.

8.3.3.1 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 122 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 97 Site-wide > Configure > Firewall > Routing: Policy Route/Traffic Shaping: Add/Edit

LABEL	DESCRIPTION
Matching Criteria	
Description	Enter a descriptive name for the rule.
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 use at the same time. Multiple FQDNs are not supported.

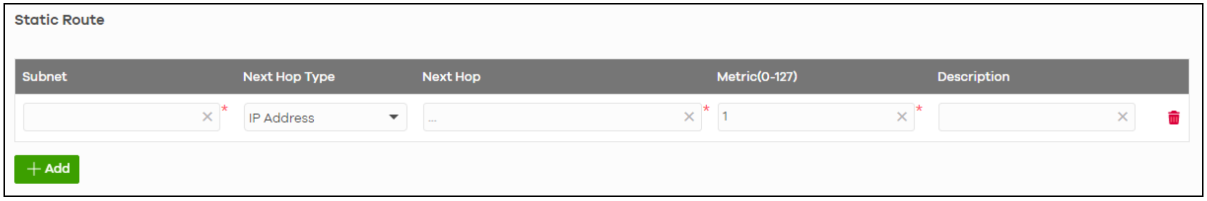
Table 97 Site-wide > Configure > Firewall > Routing: Policy Route/Traffic Shaping: Add/Edit (continued)

LABEL	DESCRIPTION
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 11.4.4.3 on page 524 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.

8.3.3.2 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 123 Site-wide > Configure > Firewall > Routing: Static Route



Static Route

Subnet	Next Hop Type	Next Hop	Metric(0-127)	Description
	IP Address	...	1	

The following table describes the labels in this screen.

Table 98 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.

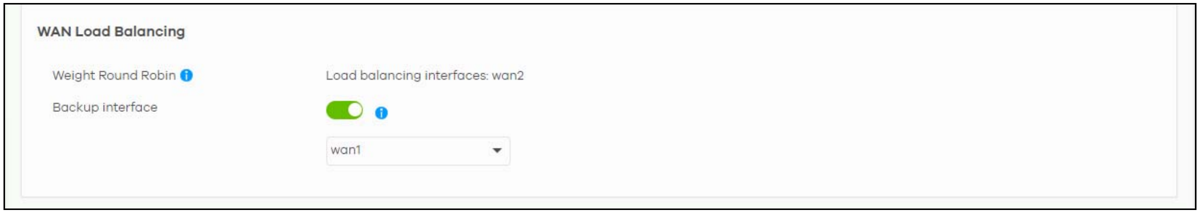
8.3.3.3 WAN Load Balancing

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 124 Site-wide > Configure > Firewall > Routing: WAN Load Balancing



WAN Load Balancing

Weight Round Robin: Load balancing interfaces: wan2

Backup interface: ● wan1

The following table describes the labels in this section.

Table 99 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.

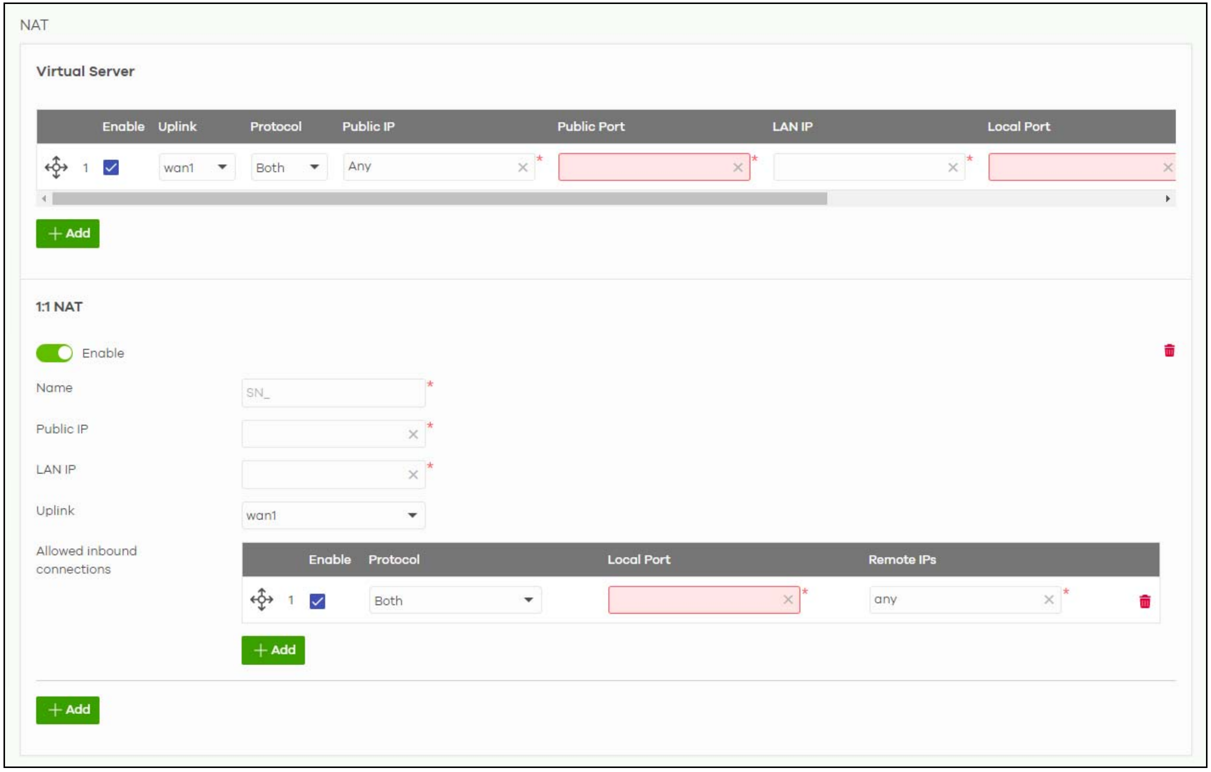
8.3.4 NAT

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 a NAT rule, based on the NAT setting NCC will automatically add the incoming security policy (firewall) rule.

To access this screen, click **Site-wide** > **Configure** > **Firewall** > **NAT**. The following screen appears, providing a summary of the existing NAT rules.

Figure 125 Site-wide > Configure > Firewall > NAT



NAT

Virtual Server

		Enable	Uplink	Protocol	Public IP	Public Port	LAN IP	Local Port
✥	1	☑	wan1	Both	Any *	*	*	

+ Add

1:1 NAT

Enable

Name	SN_ *
Public IP	*
LAN IP	*
Uplink	wan1
Allowed inbound connections	

		Enable	Protocol	Local Port	Remote IPs
✥	1	☑	Both	*	any *

+ Add

+ Add

The following table describes the labels in this screen.

Table 100 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 check box to turn on the rule. Otherwise, clear the check box 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.

Table 100   Site-wide > Configure > Firewall > NAT (continued)

LABEL	DESCRIPTION
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 check box to turn on the rule. Otherwise, clear the check box 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.
🗑	Click the remove icon to delete it.
Add	Click this to create a new entry.

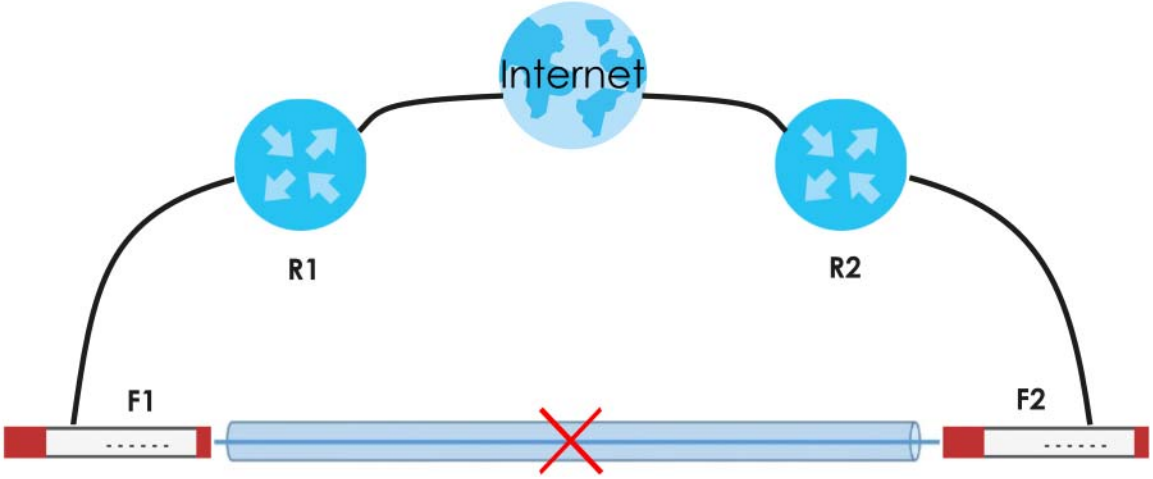
8.3.5 Site-to-Site VPN

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. Use this screen to configure a VPN rule.

Note: Site-to-site VPN does not support both VPN sites behind NAT mode.

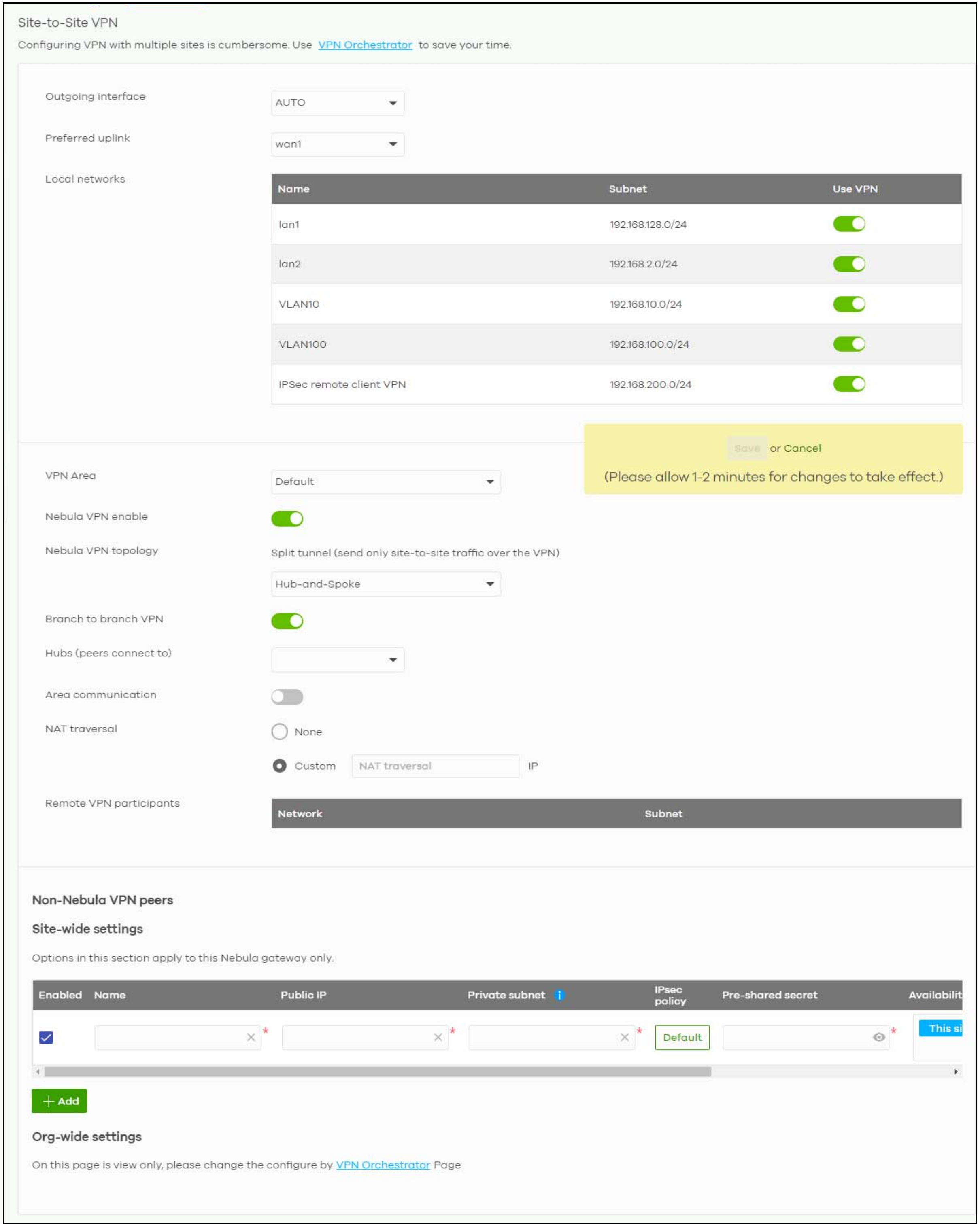
The following figure shows two routers (R1, R2) with NAT mode enabled. Site-to-site VPN between the two Firewall devices (F1, F2) is not allowed.

Figure 126 Two VPN Sites Behind NAT Example



Click **Site-wide** > **Configure** > **Firewall** > **Site-to-Site VPN** to access this screen.

Figure 127 Site-wide > Configure > Firewall > Site-to-Site VPN



Site-to-Site VPN

Configuring VPN with multiple sites is cumbersome. Use VPN Orchestrator to save your time.

Outgoing interface: AUTO

Preferred uplink: wan1

Local networks

Name	Subnet	Use VPN
lan1	192.168.128.0/24	●
lan2	192.168.2.0/24	●
VLAN10	192.168.10.0/24	●
VLAN100	192.168.100.0/24	●
IPSec remote client VPN	192.168.200.0/24	●

Save or Cancel

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

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: ○ None

● Custom NAT traversal IP

Remote VPN participants

Network	Subnet

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	Availabilit
☑	*	*	*	Default	*	This si

+ 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 101 Site-wide > Configure > Firewall > Site-to-Site VPN

LABEL	DESCRIPTION
Outgoing Interface	Select the WAN interface to which the VPN connection is going. Select **AUTO** to use all available WAN interfaces to build the VPN tunnel.
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. 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**.
VPN Area	Select the VPN area of the site. For details, see Section 11.4.4.2 on page 524.
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	Click this to select a topology for the VPN area. For details on topologies, see Section 11.4.4.1 on page 523. Select disable to disable VPN connections for all sites in the VPN area.
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 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**.
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.
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 check box 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 8.3.8.1 on page 394 for detailed information.

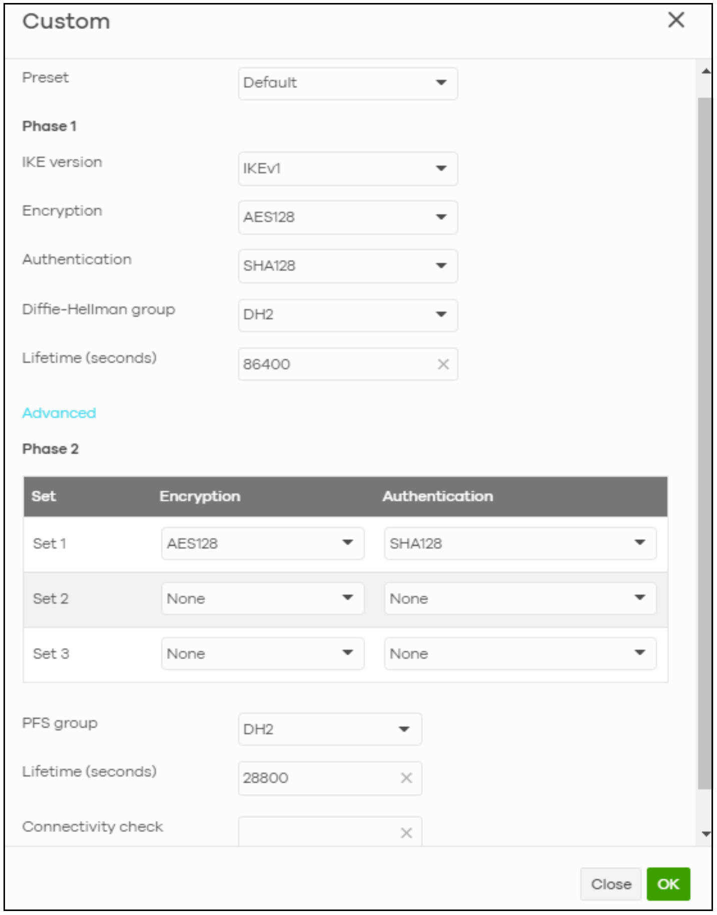
Table 101 Site-wide > Configure > Firewall > Site-to-Site VPN (continued)

LABEL	DESCRIPTION
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.

8.3.5.1 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 128 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

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 102 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 **DH2** – use a 1024-bit random number **DH5** – use a 1536-bit random number **DH14** – use a 2048-bit random number 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.
Local ID	Enter an identifier used to identify the Nebula Device during authentication. This can be an IP address or hostname.

Table 102 Site-wide > Configure > Firewall > Site-to-Site VPN: IPsec Policy (continued)

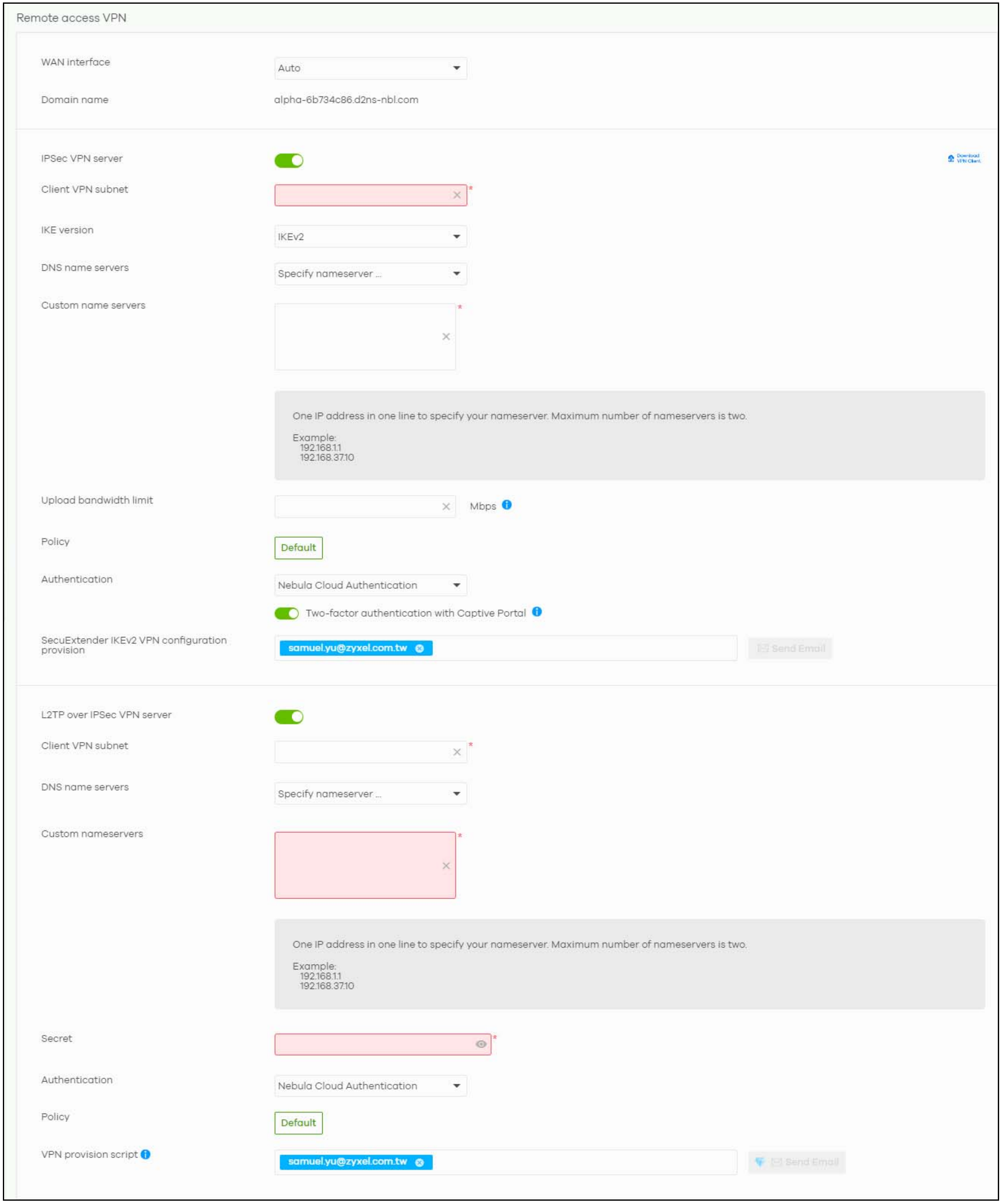
LABEL	DESCRIPTION
Peer ID	Enter an identifier used to identify the remote IPSec router during authentication. This can be an IP address or hostname.
Phase2	Phase 2 uses the SA that was established in phase 1 to negotiate SAs for IPSec.
Encryption	Select which key size and encryption algorithm to use 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.

8.3.6 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** > **Firewall** > **Remote access VPN** to access this screen.

Figure 129 Site-wide > Configure > Firewall > Remote access VPN



Remote access VPN

WAN interface: Auto

Domain name: alpha-6b734c86.d2ns-nbl.com

IPSec VPN server

Client VPN subnet: *

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

Two-factor authentication with Captive Portal

SecuExtender IKEv2 VPN configuration provision: samuel.yu@zyxel.com.tw

L2TP over IPSec VPN server

Client VPN subnet: *

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

Secret: *

Authentication: Nebula Cloud Authentication

Policy: Default

VPN provision script: samuel.yu@zyxel.com.tw

The following table describes the labels in this screen.

Table 103 Site-wide > Configure > Firewall > Remote access VPN

LABEL	DESCRIPTION
WAN interface	Select the WAN interface which VPN users connect to.
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.
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.
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 nameservers	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.
Secret	Enter the pre-shared key (password) which is used to set up the VPN tunnel. The password should be 8 – 32 characters.
Policy	Configure custom VPN tunnel settings. For details, see Section 8.3.6.1 on page 374.
Authentication	Select how the Nebula Device authenticates a remote user before allowing access to the VPN tunnel.
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.
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.
L2TP over IPSec 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.
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.
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.

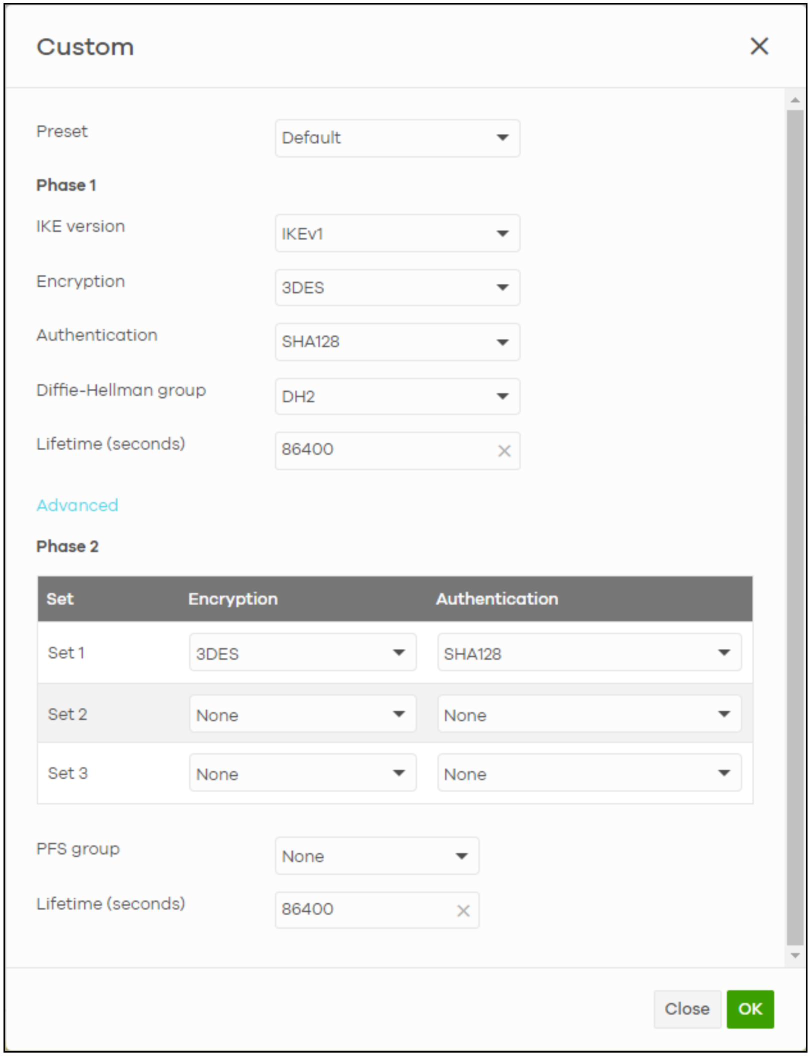
Table 103   Site-wide > Configure > Firewall > Remote access VPN (continued)

LABEL	DESCRIPTION
Policy	Configure custom VPN tunnel settings. For details, see Section 8.3.6.1 on page 374.
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.

8.3.6.1 Remote Access VPN > Custom VPN Policy

Click **Default** in **Site-wide** > **Configure** > **Firewall** > **Remote access VPN** > **Policy** to open the following screen.

Figure 130 Site-wide > Configure > Firewall > Remote access VPN: Default



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 104 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	

Table 104 Site-wide > Configure > Firewall > Remote access VPN: Default (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 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 **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 **DH2** – use a 1024-bit random number **DH5** – use a 1536-bit random number **DH14** – use a 2048-bit random number 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.

Table 104 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 **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.
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.

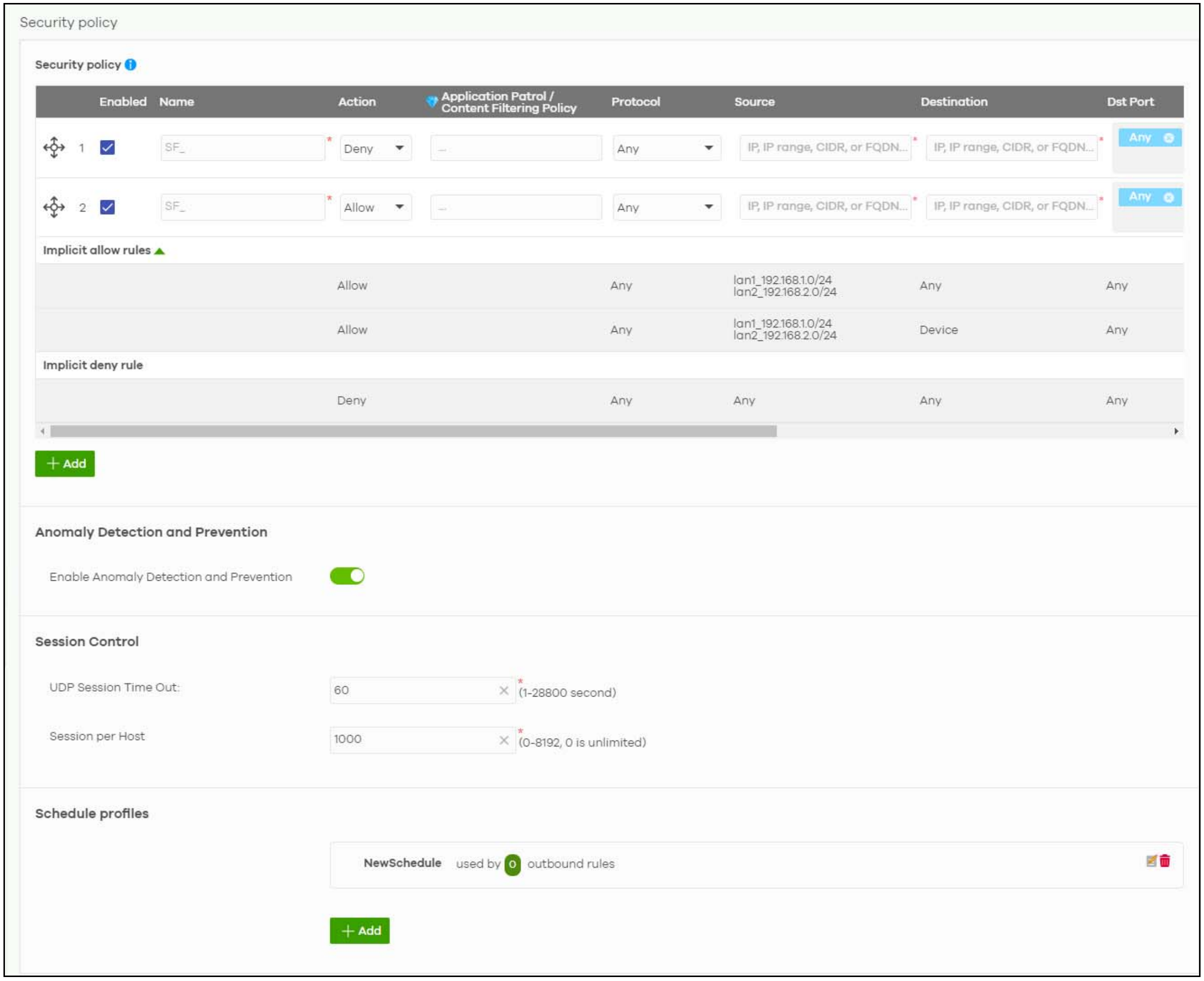
8.3.7 Security Policy

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 filtering, 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 131 Site-wide > Configure > Firewall > Security policy



Security policy

Security policy

		Enabled	Name	Action	Application Patrol / Content Filtering Policy	Protocol	Source	Destination	Dst Port
✥	1	☑	SF_ *	Deny	...	Any	IP, IP range, CIDR, or FQDN... *	IP, IP range, CIDR, or FQDN... *	Any ⊗
✥	2	☑	SF_ *	Allow	...	Any	IP, IP range, CIDR, or FQDN... *	IP, IP range, CIDR, or FQDN... *	Any ⊗
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

UDP Session Time Out: 60 * (1-28800 second)

Session per Host 1000 * (0-8192, 0 is unlimited)

Schedule profiles

NewSchedule used by 0 outbound rules

The following table describes the labels in this screen.

Table 105 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 check box to turn on the rule. Otherwise, clear the check box 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.

Table 105 Site-wide > Configure > Firewall > Security policy (continued)

LABEL	DESCRIPTION
Application Patrol/ Content Filtering Policy	Click the "**+**" to add an Application Patrol or Content Filtering 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 8.3.7.1 on page 380 for how to create an Application Patrol profile. Content Filtering controls access to specific web sites or web content. See Section 8.3.7.2 on page 381 for how to create a Content Filtering profile.
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 use 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. • 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	

Table 105   Site-wide > Configure > Firewall > Security policy (continued)

LABEL	DESCRIPTION
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.
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 8.3.7.3 on page 384 for more information.

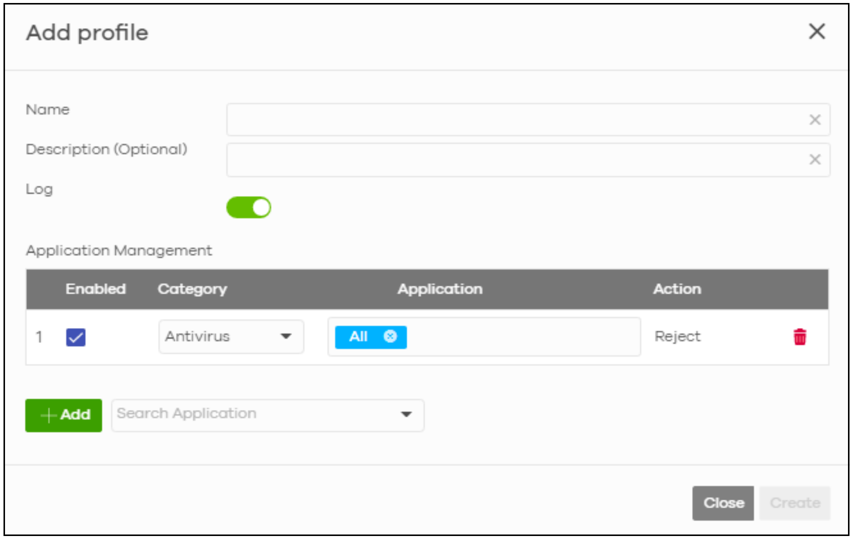
8.3.7.1 Add an Application Patrol Profile

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 **Organization-wide** > **Organization-wide manage** > **Security profile sync** 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 132 Organization-wide > Organization-wide manage > Security profile sync > Application patrol: Add an Application Profile



Add profile

Name

Description (Optional)

Log

Application Management

	Enabled	Category	Application	Action	
1	☑	Antivirus	All	Reject	🗑

The following table describes the labels in this screen.

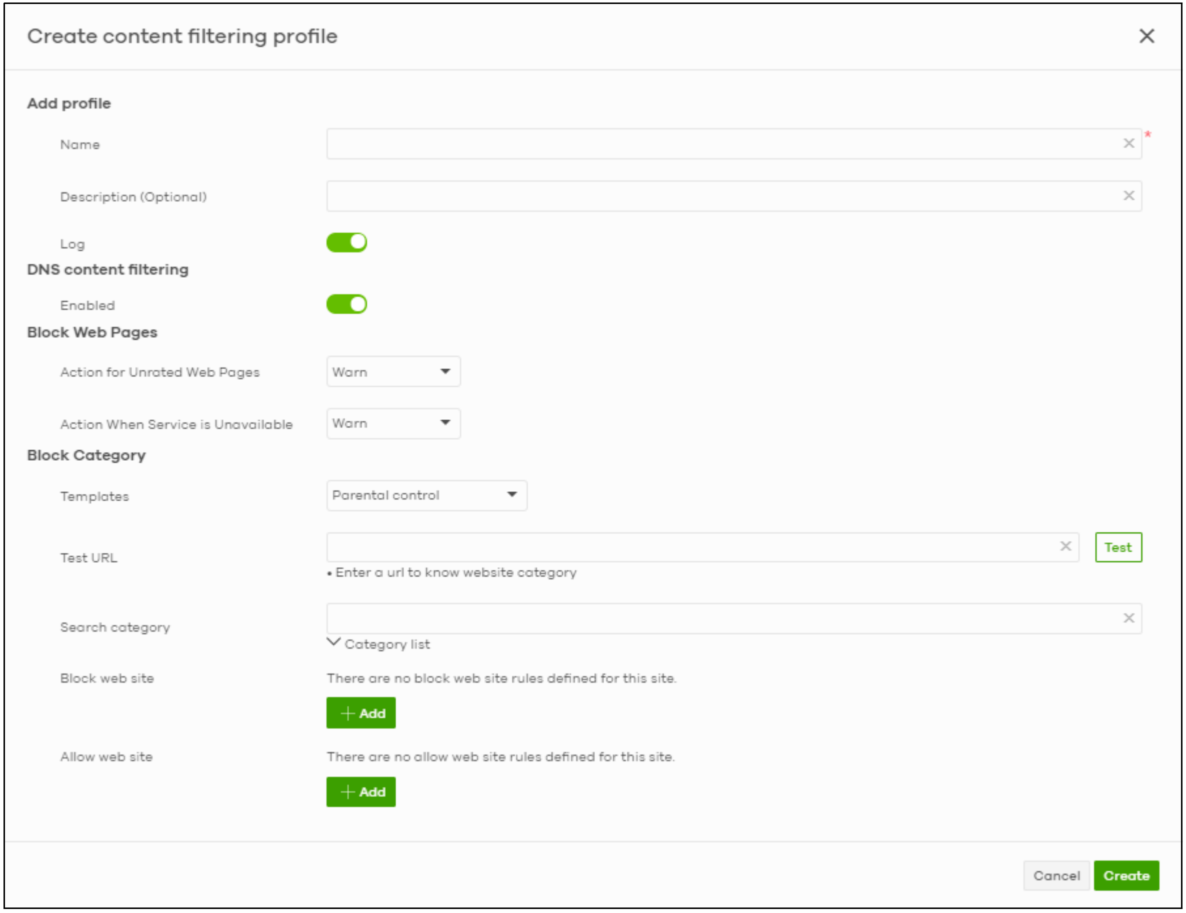
Table 106 Organization-wide > Organization-wide manage > Security profile sync > Application patrol: Add an Application Profile

LABEL	DESCRIPTION
Name	Enter a name for this profile for identification purposes.
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 check box to turn on the rule. Otherwise, clear the check box 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.
🗑	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.

8.3.7.2 Add a Content Filtering Profile

Click "**+**" in the **Application Patrol/Content Filtering Policy** section of the **Organization-wide > Organization-wide manage > Security profile sync > Content filtering: Create content filtering profile** screen to access this screen.

Figure 133 Organization-wide > Organization-wide manage > Security profile sync > Content filtering: Create content filtering profile



Create content filtering profile

Add profile

Name

Description (Optional)

Log

DNS content filtering

Enabled

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: There are no block web site rules defined for this site.

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

The following table describes the labels in this screen.

Table 107 Organization-wide > Organization-wide manage > Security profile sync > Content filtering: Create content filtering profile

LABEL	DESCRIPTION
Name	Enter a name for this profile for identification purposes.
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 Filtering	Select whether to enable DNS content filtering, 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.
Block Web Pages	

Table 107 Organization-wide > Organization-wide manage > Security profile sync > Content filtering: Create content filtering profile (continued)

LABEL	DESCRIPTION
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 filtering database is unavailable. Select **Block** to block access to any requested web page if the external content filtering database is unavailable. Select **Warn** to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable. The following are possible causes for the external content filtering server not being available: • There is no response from the external content filtering 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 filtering database. • There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering'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. 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 Filtering 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.
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.
Custom 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.

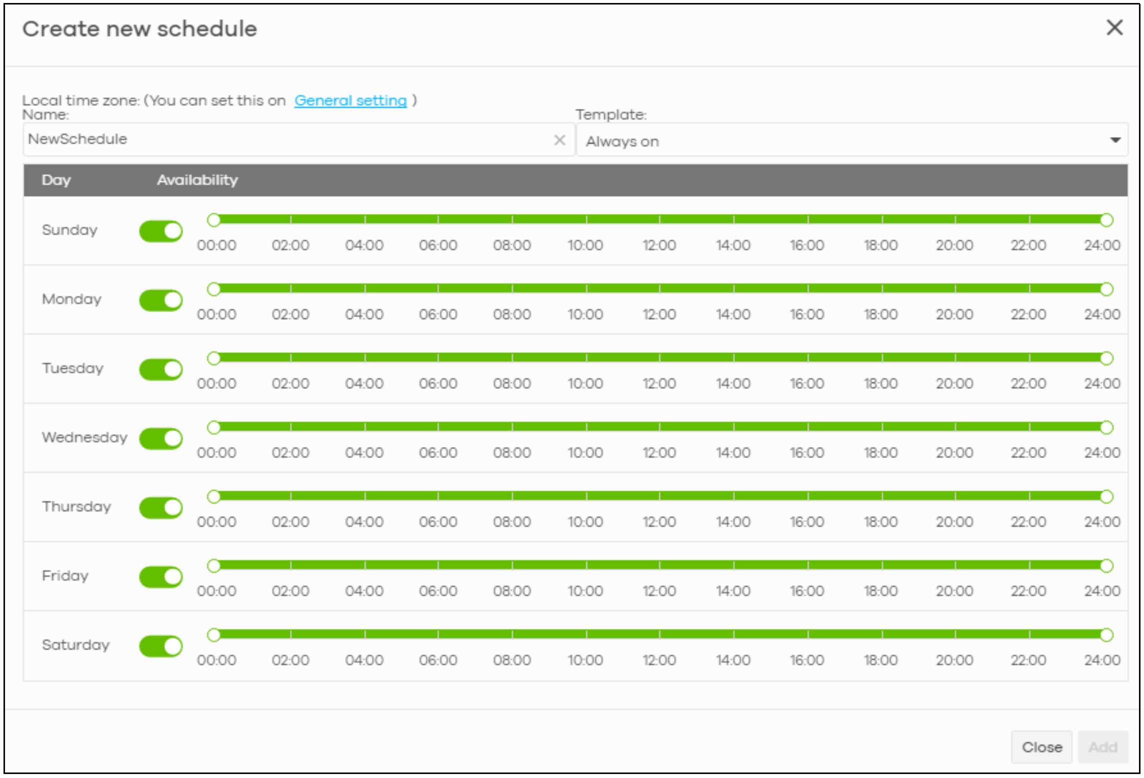
Table 107 Organization-wide > Organization-wide manage > Security profile sync > Content filtering: Create content filtering profile (continued)

LABEL	DESCRIPTION
Custom 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.

8.3.7.3 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 134 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	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

The following table describes the labels in this screen.

Table 108   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.

8.3.8 Security Service

Use this screen to enable or disable the features available in the security pack for your Nebula Device, such as content filtering, 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.

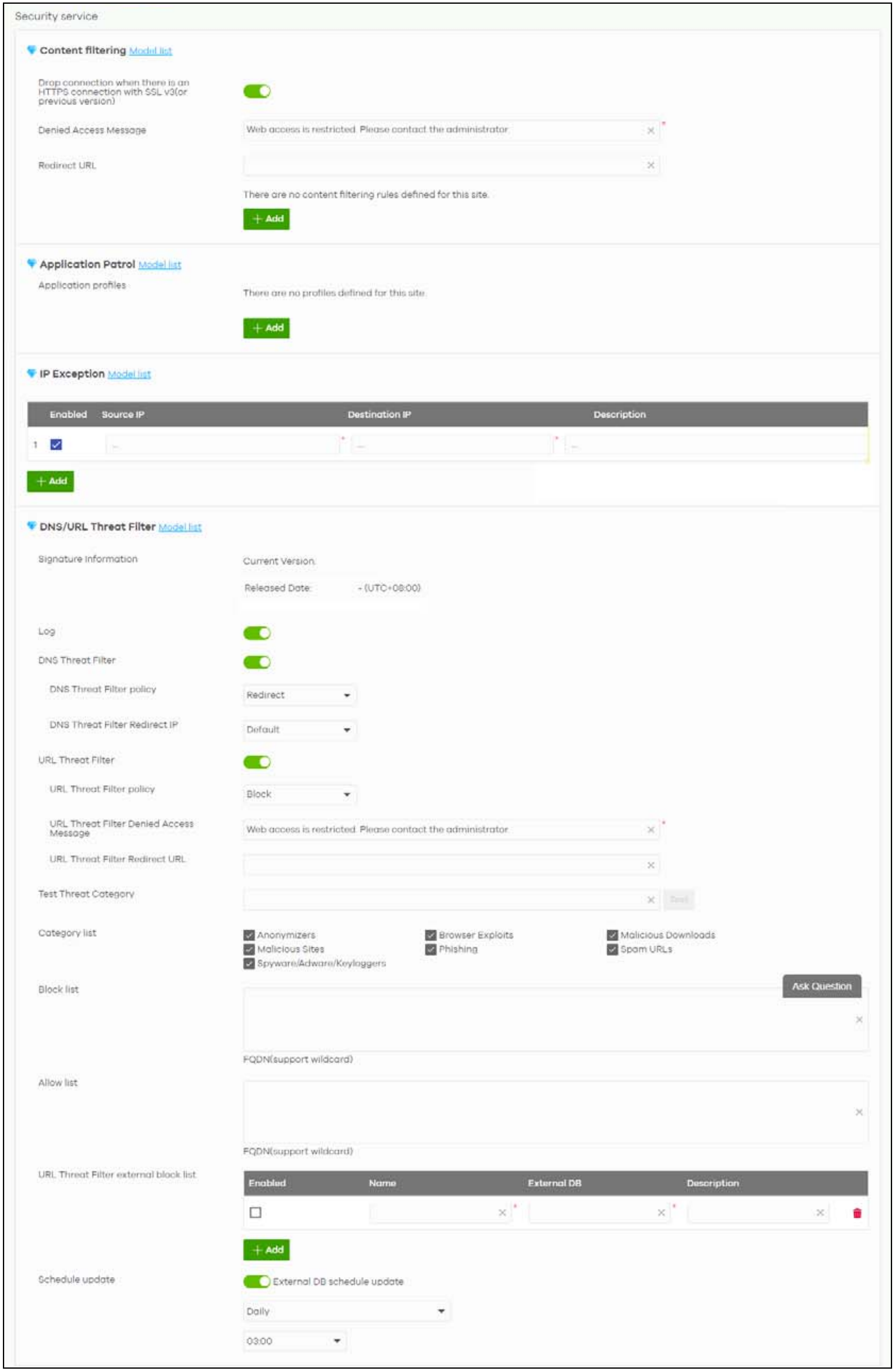
Content filtering allows you to block access to specific web sites. It can also block access to specific categories of web site content. IDP can detect malicious or suspicious packets used in network-based intrusions and respond instantaneously. Anti-virus helps protect your connected network from virus/spy-ware infection.

Click **Site-wide** > **Configure** > **Firewall** > **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.

Note: If Security Profile Sync (SPS) is enabled, you cannot configure security settings on this screen. For details, see Section 11.4.5 on page 527.

Figure 135   Site-wide > Configure > Firewall > Security service



Security service

Content filtering 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:

There are no content filtering rules defined for this site.

+ Add

Application Patrol Model list

Application profiles: There are no profiles defined for this site.

+ Add

IP Exception Model list

	Enabled	Source IP	Destination IP	Description
1	☑	--	--	--

+ Add

DNS/URL Threat Filter Model list

Signature Information: Current Version:
Released Date: - (UTC+08:00)

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)

Ask Question

Allow list:

FQDN(support wildcard)

URL Threat Filter external block list:

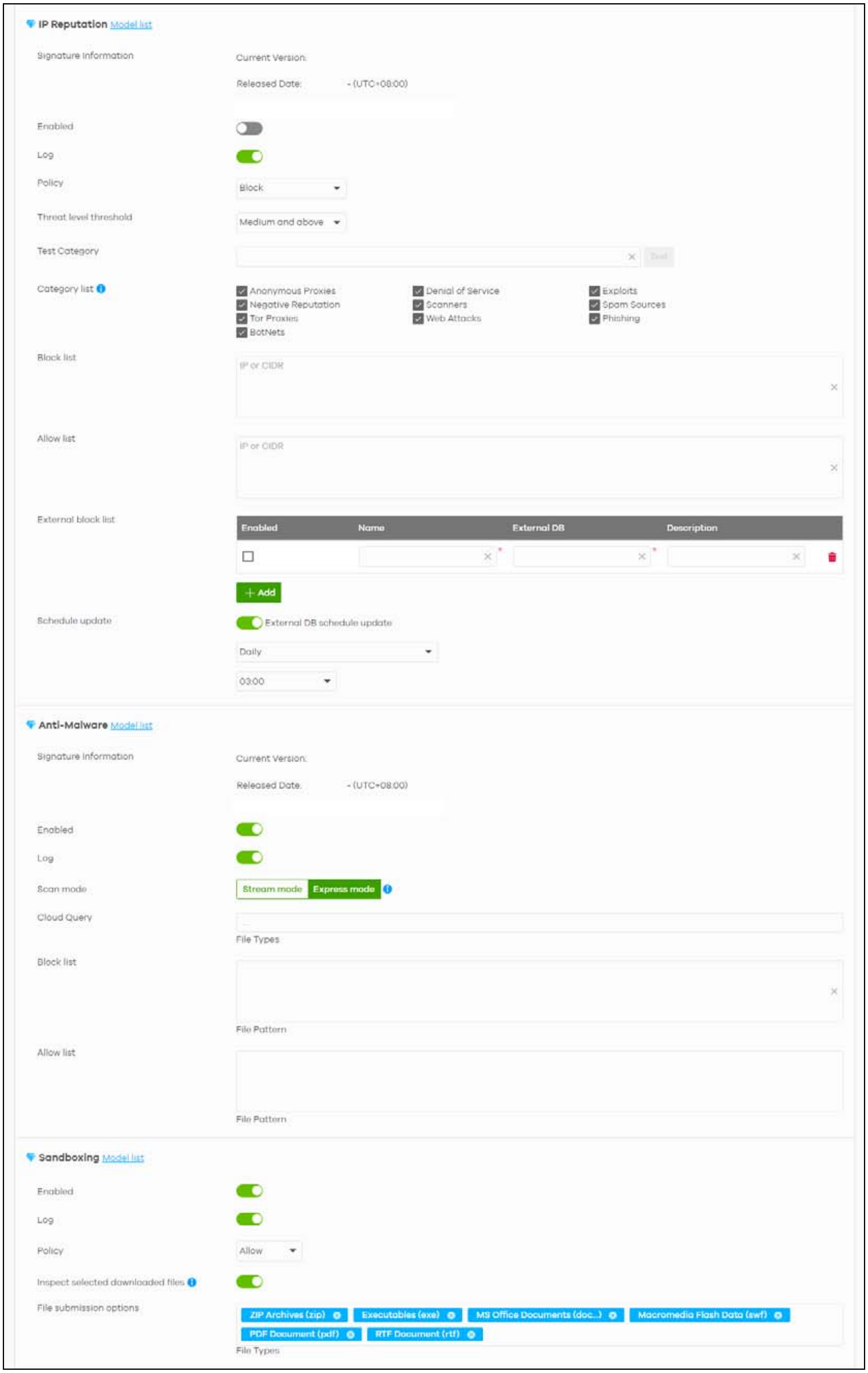
Enabled	Name	External DB	Description
□			

+ Add

Schedule update: On External DB schedule update

Daily

03:00



IP Reputation Model list

Signature information	Current Version: Released Date: - (UTC+08:00)
Enabled	Off
Log	On
Policy	Block
Threat level threshold	Medium and above
Test Category	Test
Category list	☑ Anonymous Proxies ☑ Negative Reputation ☑ Tor Proxies ☑ BotNets ☑ Denial of Service ☑ Scanners ☑ Web Attacks ☑ Exploits ☑ Spam Sources ☑ Phishing
Block list	IP or CIDR
Allow list	IP or CIDR
External block list	

Enabled	Name	External DB	Description
□			

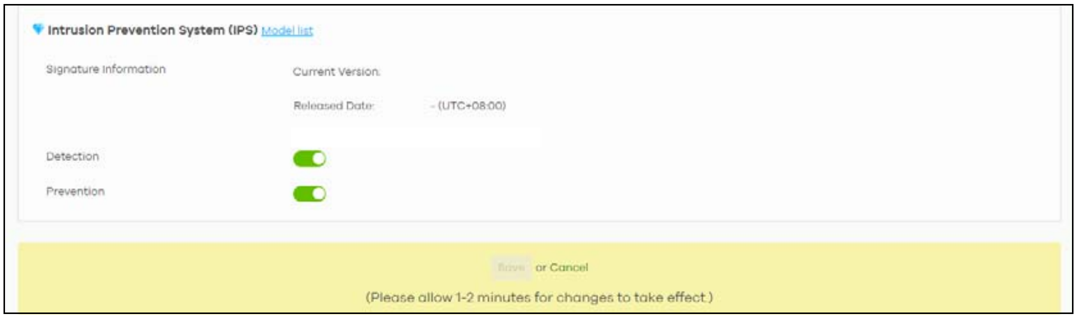
Schedule update	On External DB schedule update Daily 03:00

Anti-Malware Model list

Signature information	Current Version: Released Date: - (UTC+08:00)
Enabled	On
Log	On
Scan mode	Stream mode / Express mode
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
File submission options	ZIP Archives (zip) Executables (exe) MS Office Documents (doc...) Macromedia Flash Data (swf) PDF Document (pdf) RTF Document (rtf) File Types



Intrusion Prevention System (IPS) Model list

Signature Information Current Version:

Released Date: - (UTC+08:00)

Detection

Prevention

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

The following table describes the labels in this screen.

Table 109 Site-wide > Configure > Firewall > Security service

LABEL	DESCRIPTION
Content Filtering	
Drop connection when 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.
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 filtering 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 filtering profile. See Section 8.3.7.2 on page 381 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 8.3.8.2 on page 397 for more information.
IP Exception	
Enabled	Select the check box 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.

Table 109   Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
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.
Signature information	This shows the **Current Version** of the DNS/URL threat definition and the **Released Date**.
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 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.
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.

Table 109 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
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.
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	

Table 109 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
Signature information	This shows the **Current Version** of the signature set the Nebula Device is using and the **Released Date**.
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.
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 check box 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.

Table 109 Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
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 myZyxel, register your Nebula Device and then subscribe for IP reputation 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.
Anti-Malware	
Signature information	This shows the **Current Version** of the signature set the Nebula Device is using and the **Released Date**.
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 (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 check box 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 check box, the Nebula Device deletes compressed files that use password encryption. Select this check box 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 check box enabled. The Nebula Device classifies the firmware package as a file that cannot be decompressed and then deletes it. Clear this check box when you download a firmware package from the Zyxel website. It is okay to upload a firmware package to the Nebula Device with the check box selected.
Cloud Query	Select the Cloud Query supported file types for the Nebula Device to scan for viruses.

Table 109   Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
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.
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.

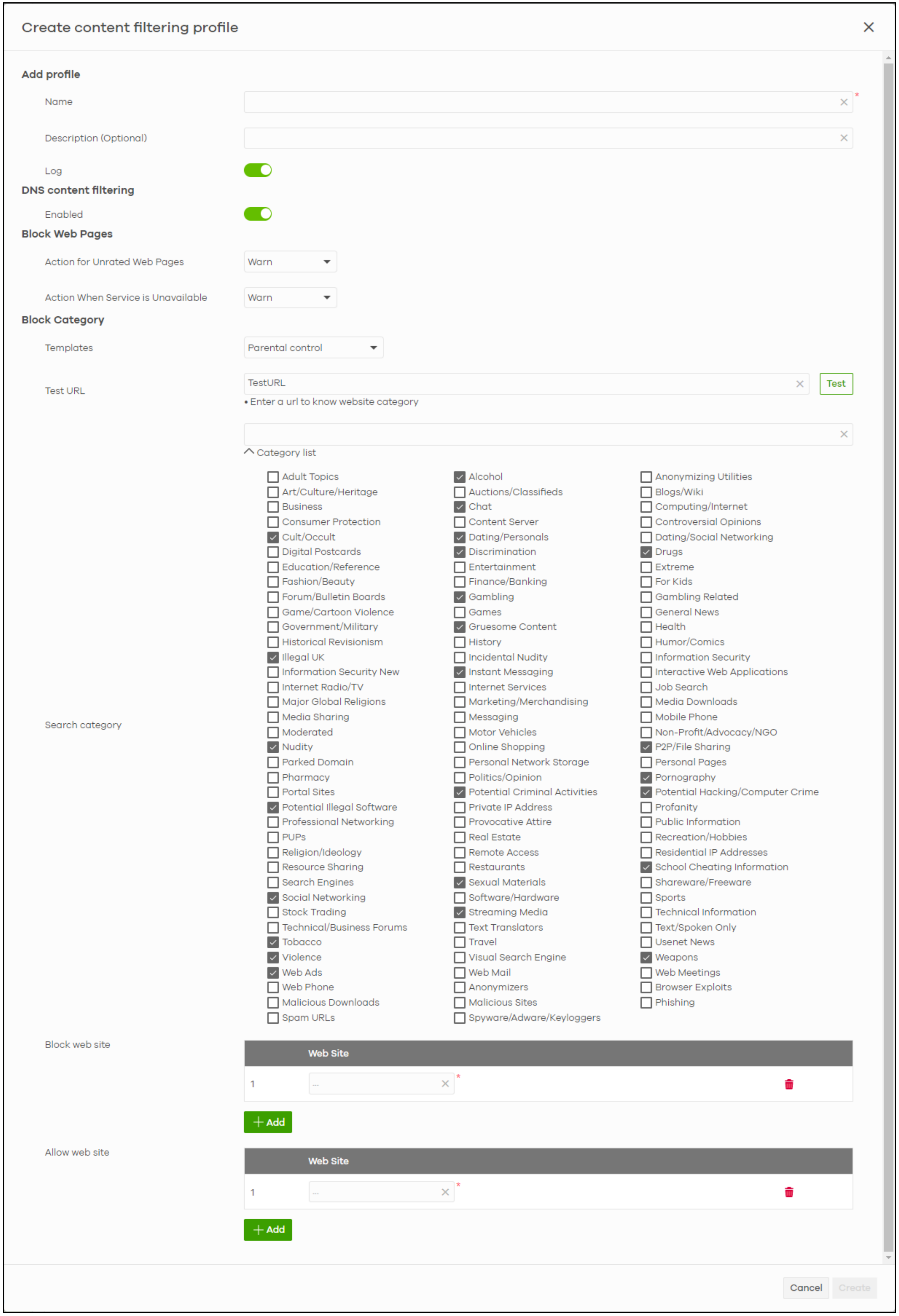
Table 109   Site-wide > Configure > Firewall > Security service (continued)

LABEL	DESCRIPTION
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 Detection/Prevention	
Signature information	This shows the **Current Version** of the signature set the Nebula Device is using and the **Released Date**.
Detection	Select **On** to enable Detection.
Prevention	Select **On** to enable Prevention.

8.3.8.1 Create a Content Filtering Profile

Click the **Add** button in the **Content Filtering** section of the **Site-wide** > **Configure** > **Firewall** > **Security service** screen to access this screen.

Figure 136 Site-wide > Configure > Firewall > Security service > Content Filtering: Add/Edit



Create content filtering profile ✕

Add profile

Name:

Description (Optional):

Log

DNS content filtering

Enabled

Block Web Pages

Action for Unrated Web Pages: Warn

Action When Service is Unavailable: Warn

Block Category

Templates: Parental control

Test URL: TestURL [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
- □ Malicious Downloads
- □ Spam URLs
- ☑ 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
- □ Anonymizers
- □ Malicious Sites
- □ Spyware/Adware/Keyloggers
- □ 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
- □ Browser Exploits
- □ Phishing

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 110 Site-wide > Configure > Firewall > Security service > Content Filtering: Add/Edit

LABEL	DESCRIPTION
Add profile	
Name	This column lists the names of the content filter profile rule.
Description (Optional)	This column lists the description of the content filter profile rule.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed above.
DNS content filtering	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 filtering will either drop the DNS query or reply to the user with a fake DNS response.
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 filtering database is unavailable. Select **Block** to block access to any requested web page if the external content filtering database is unavailable. Select **Warn** to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable. The following are possible causes for the external content filtering server not being available: •There is no response from the external content filtering 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 filtering database. •There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering'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 filtering 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.

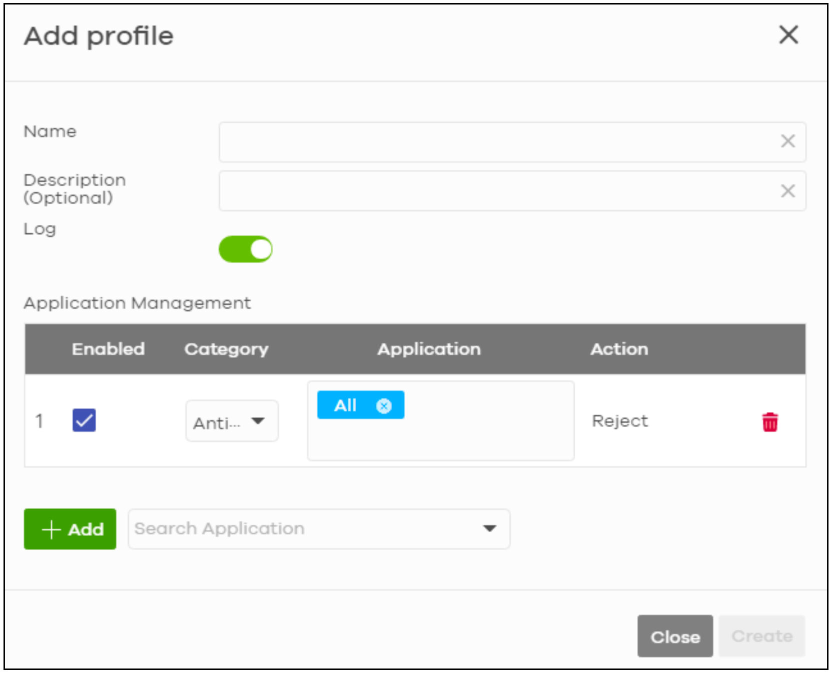
Table 110 Site-wide > Configure > Firewall > Security service > Content Filtering: Add/Edit (continued)

LABEL	DESCRIPTION
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 Filtering 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.

8.3.8.2 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 137 Site-wide > Configure > Firewall > Security service > Application Patrol: Add/Edit



	Enabled	Category	Application	Action	
1	☑	Anti...	All	Reject	🗑

The following table describes the labels in this screen.

Table 111 Site-wide > Configure > Firewall > Security service > Application Patrol: Add/Edit

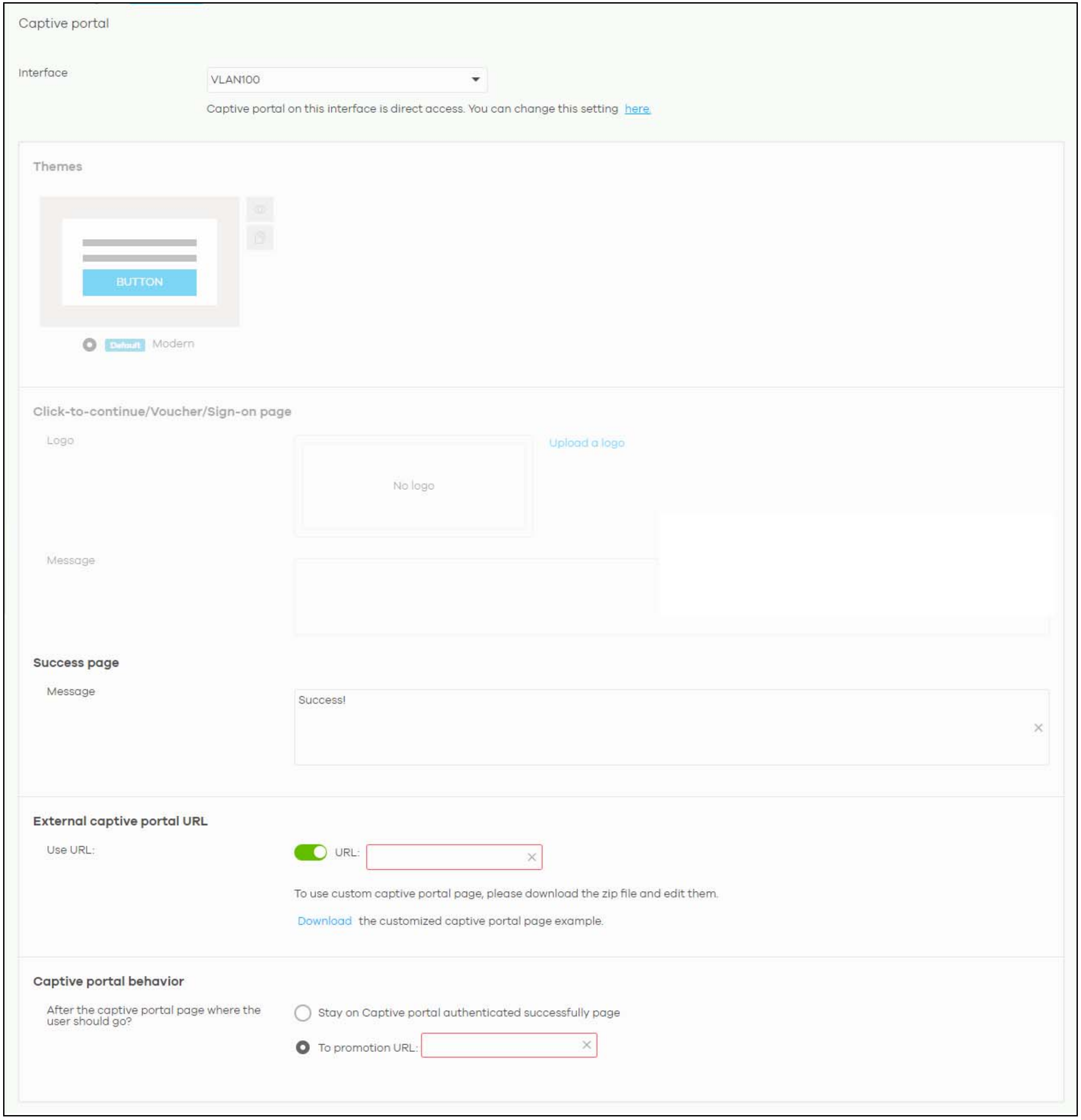
LABEL	DESCRIPTION
Add profile	
Name	This column lists the names of the application patrol profile rule.
Description (Optional)	This column lists the description of the application patrol profile rule.
Log	Select whether to have the Nebula Device generate a log when the policy is matched to the criteria listed above.
Application Management	
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box 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 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 138 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

● 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.

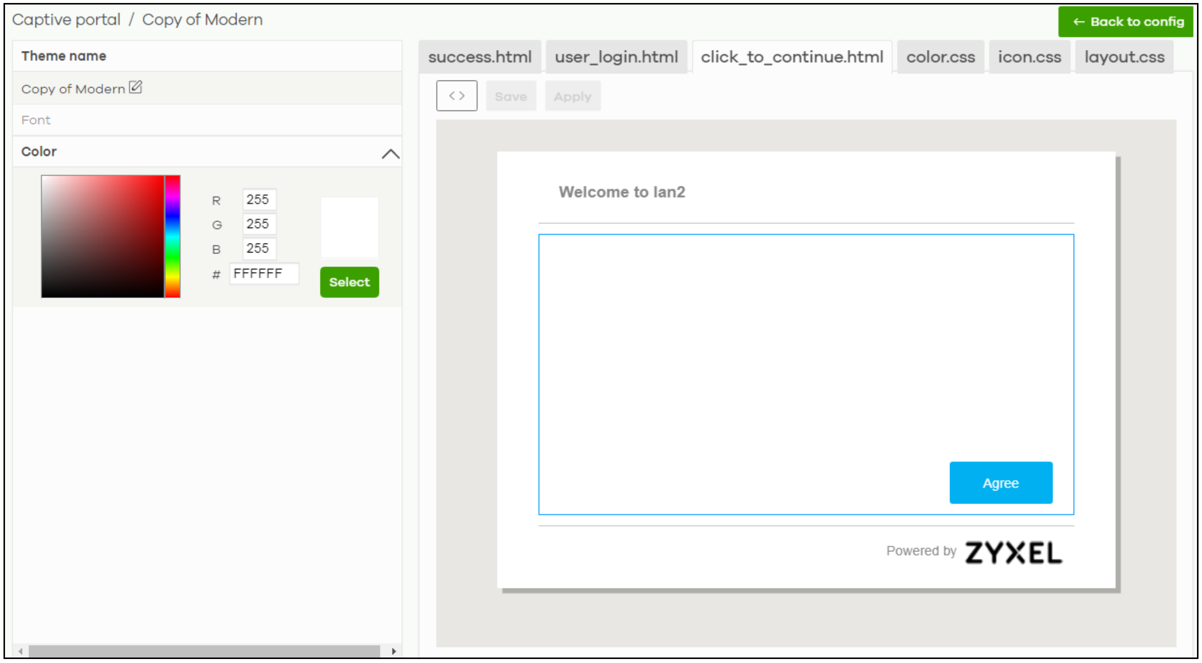
Table 112   Site-wide > Configure > Firewall > Captive portal

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 8.3.9.1 on page 400. • 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**.

8.3.9.1 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 139 Site-wide > Configure > Firewall > Captive portal: Edit



R 255
G 255
B 255
FFFFFF

Welcome to lan2

The following table describes the labels in this screen.

Table 113 Site-wide > Configure > Firewall > Captive portal: Edit

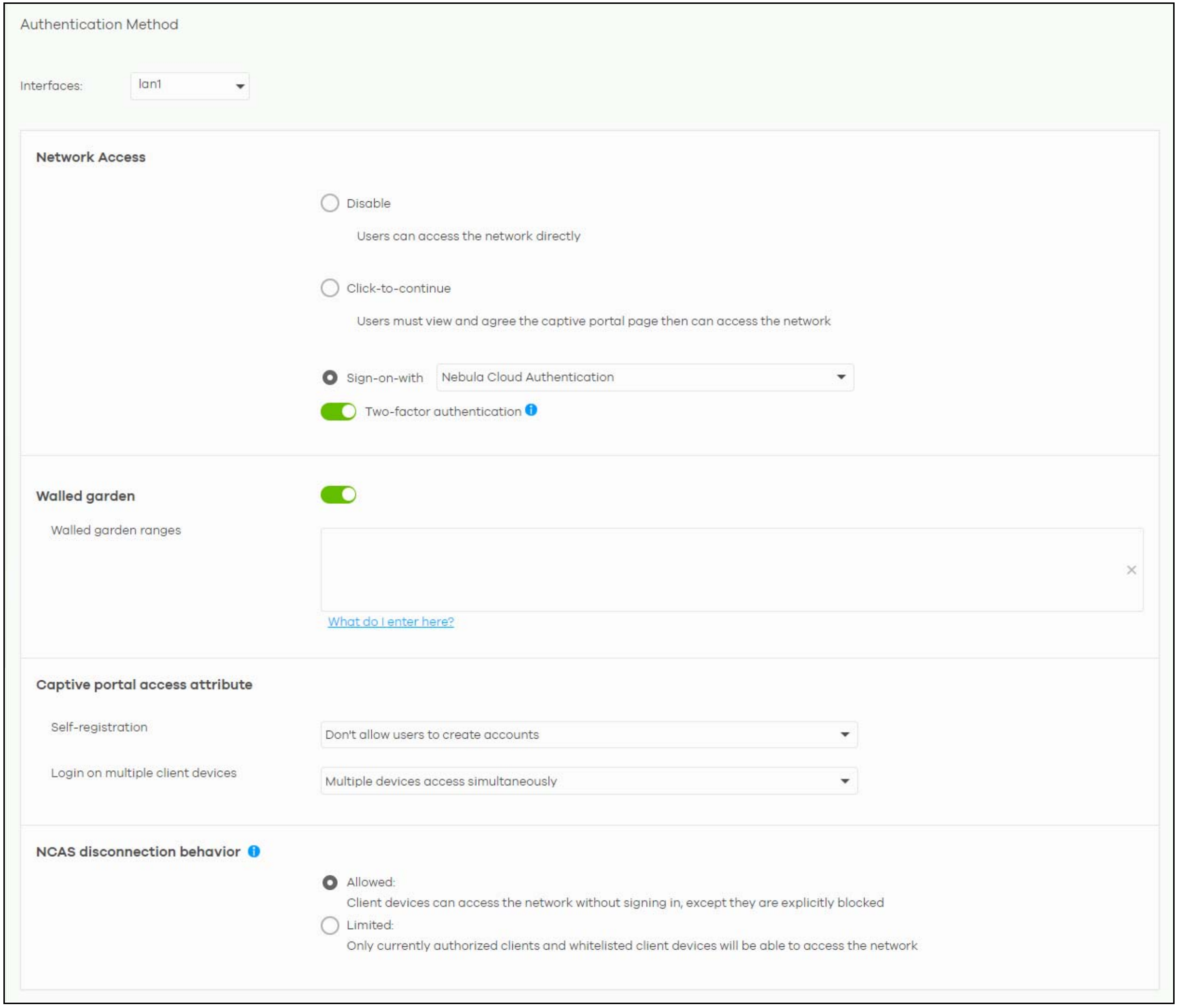
LABEL	DESCRIPTION
Back to config	Click this button to return to the **Captive portal** screen.
Theme name	This shows the name of the theme. Click the edit icon to change it.
Font	Click the arrow to hide or display the configuration fields. To display this section and customize the font type and/or size, 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.

8.3.10 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 140 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 114 Site-wide > Configure > Firewall > Authentication method

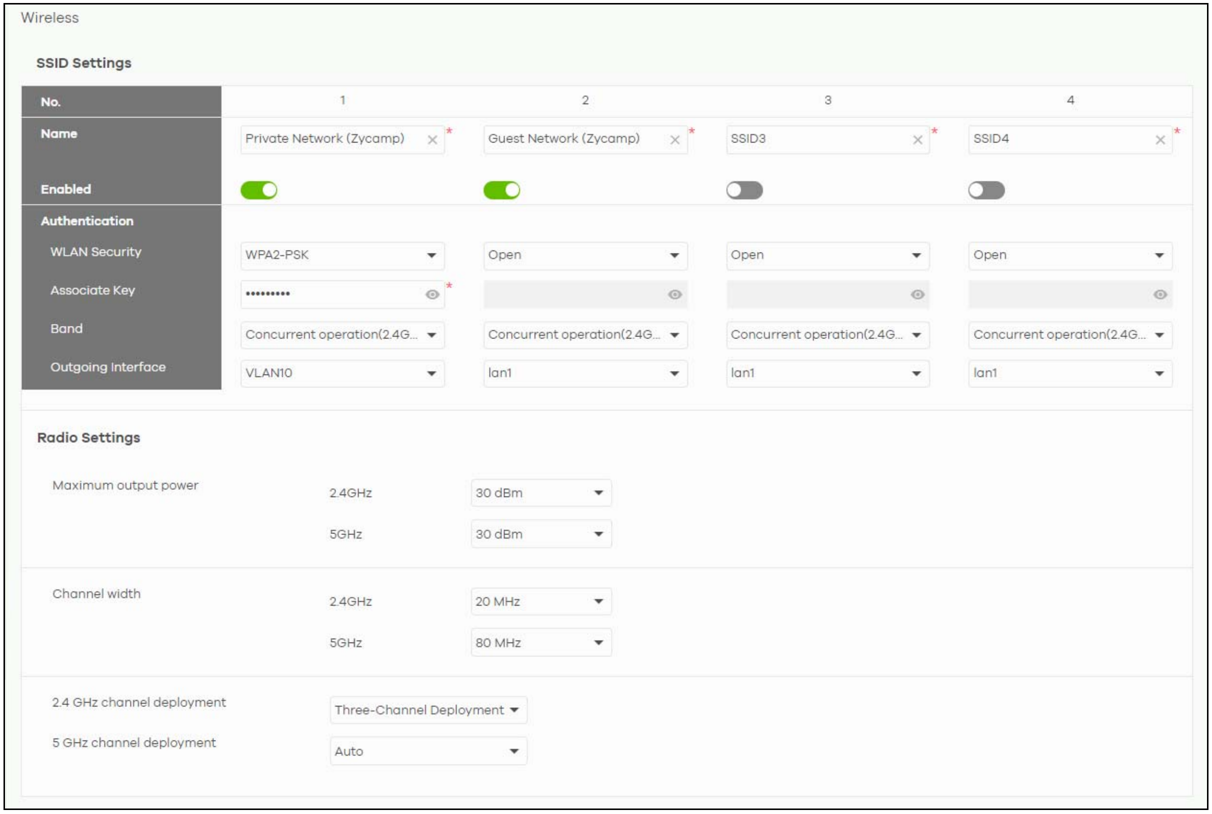
LABEL	DESCRIPTION
Interfaces	Select the Nebula Device's interface (network) to which the settings you configure here is applied.
Network Access	Select **Disable** to turn off web authentication. Select **Click-to-continue** to block network traffic until a client agrees to the policy of user agreement. 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 8.3.12 on page 405). 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.

8.3.11 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 141 Site-wide > Configure > Firewall > Wireless



Wireless

SSID Settings

No.	1	2	3	4
Name	Private Network (Zycamp)	Guest Network (Zycamp)	SSID3	SSID4
Enabled	On	On	Off	Off
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 115 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 115 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.

8.3.12 Firewall Settings

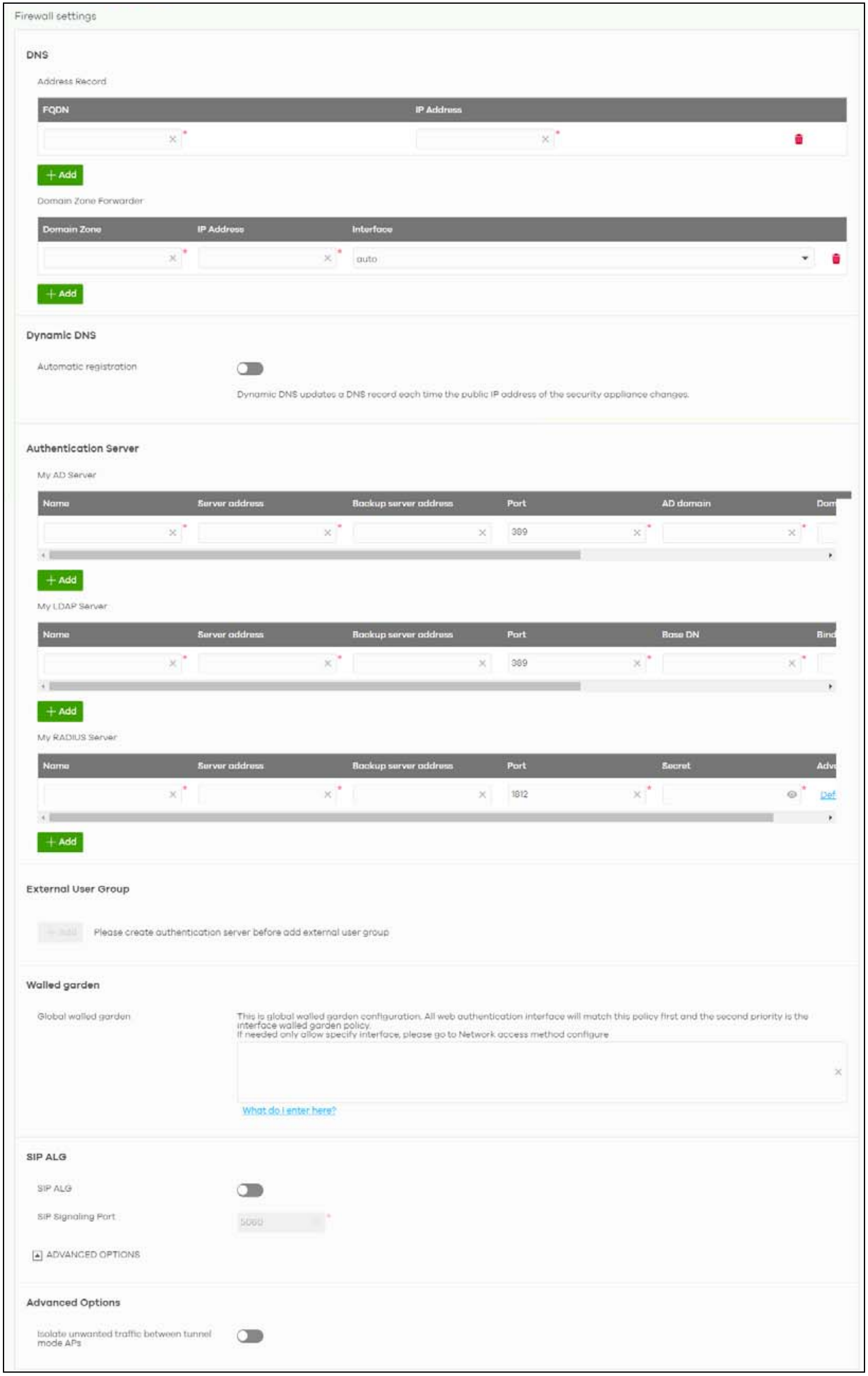
Use this screen to configure DNS settings and external AD (Active Directory), RADIUS, or LDAP server that the Nebula Device can use for authenticating users.

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 142 Site-wide > Configure > Firewall > Firewall settings



Firewall settings

DNS

Address Record

FQDN	IP Address

Domain Zone Forwarder

Domain Zone	IP Address	Interface
		auto

Dynamic DNS

Automatic registration

Dynamic DNS updates a DNS record each time the public IP address of the security appliance changes.

Authentication Server

My AD Server

Name	Server address	Backup server address	Port	AD domain	Dom
			389		

My LDAP Server

Name	Server address	Backup server address	Port	Base DN	Bind
			389		

My RADIUS Server

Name	Server address	Backup server address	Port	Secret	Adv
			1812		Def

External User Group

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?

SIP ALG

SIP ALG

SIP Signaling Port 5060

Advanced Options

Isolate unwanted traffic between tunnel mode APs

The following table describes the labels in this screen.

Table 116   Site-wide > Configure > Firewall > Firewall 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 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.
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 8.3.12.3 on page 413.
🗑	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.

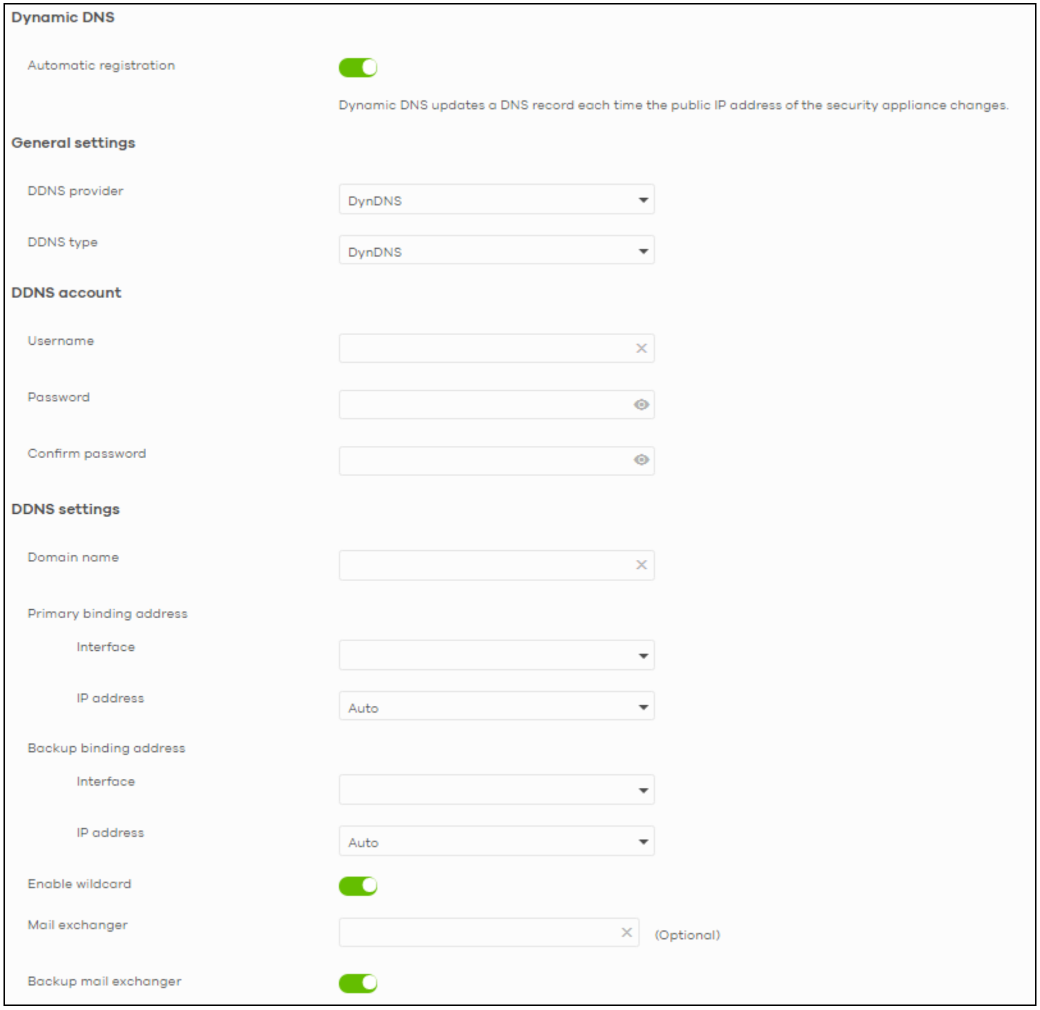
Table 116 Site-wide > Configure > Firewall > Firewall settings (continued)

LABEL	DESCRIPTION
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 8.3.12.3 on page 413.
🗑	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.
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 8.3.12.3 on page 413.
🗑	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.
Advanced Options	
Isolate unwanted traffic between tunnel mode APs	Select **On** to block broadcast and multicast traffic coming from Remote APs (RAPs).

8.3.12.1 Dynamic DNS

Enable **Dynamic DNS** to open the **Site-wide** > **Configure** > **Firewall** > **Firewall settings: Dynamic DNS** screen.

Figure 143 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.

General settings

DDNS provider: DynDNS

DDNS type: DynDNS

DDNS account

Username:

Password:

Confirm password:

DDNS settings

Domain name:

Primary binding address

Interface:

IP address: Auto

Backup binding address

Interface:

IP address: Auto

Enable wildcard: On

Mail exchanger: (Optional)

Backup mail exchanger: On

The following table describes the labels in this screen.

Table 117 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.
General 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.

Table 117 Site-wide > Configure > Firewall > Firewall settings: Dynamic DNS (continued)

LABEL	DESCRIPTION
DDNS type	Select the type of DDNS service you are using. Select **DynDNS custom** to create your own DDNS service and configure the **DynDNS** and **DDNS static** fields below. If the DDNS provider is **Dynu**, you can select the account type of **DynuBasic** or **DynuPremium**.
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.
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 117 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 check box 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 customize** 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 customize** 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 customize** 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/

8.3.12.2 SIP ALG

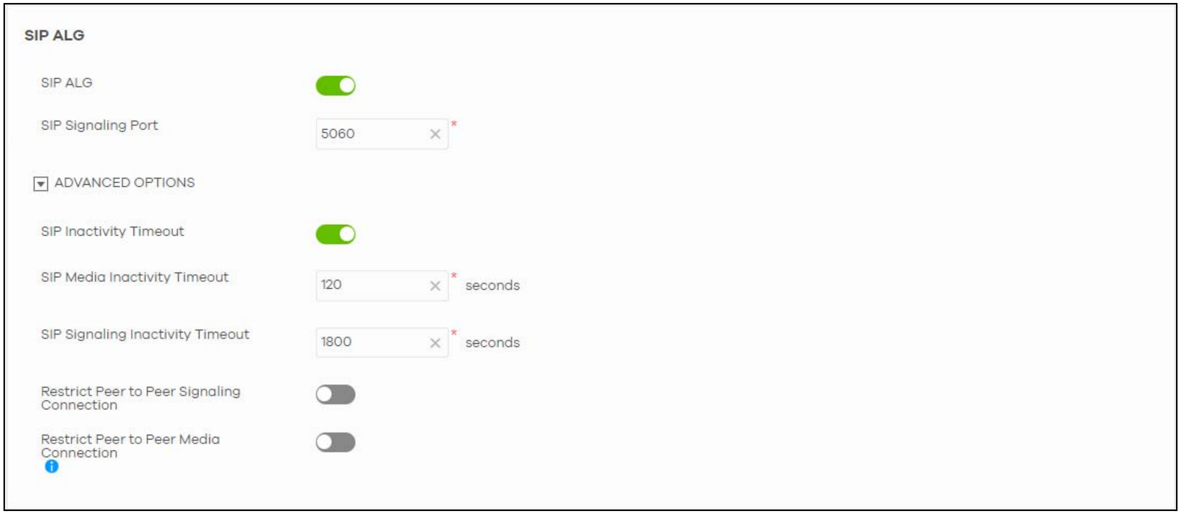
Application Layer Gateway (ALG) allows the following applications to operate properly through the NCC's NAT.

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 144 Site-wide > Configure > Firewall > Firewall settings: SIP ALG



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

Restrict Peer to Peer Signaling Connection

Restrict Peer to Peer Media Connection

The following table describes the labels in this screen.

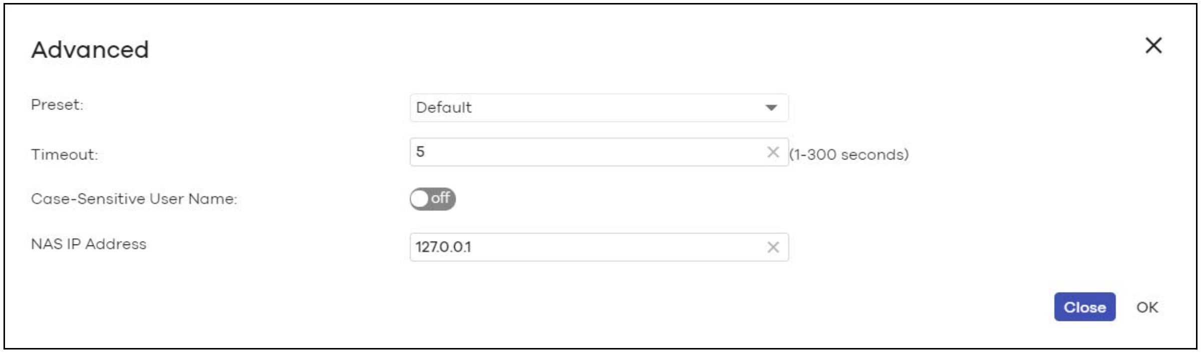
Table 118 Site-wide > Configure > Firewall > Firewall settings: SIP ALG

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.
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.

8.3.12.3 Advanced Settings

Click the **Advanced** column in the **Site-wide** > **Configure** > **Firewall** > **Firewall settings** screen to access this screen.

Figure 145 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 119 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	If the RADIUS server requires the Nebula Device to provide the Network Access Server identifier attribute with a specific value, enter it here.
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.

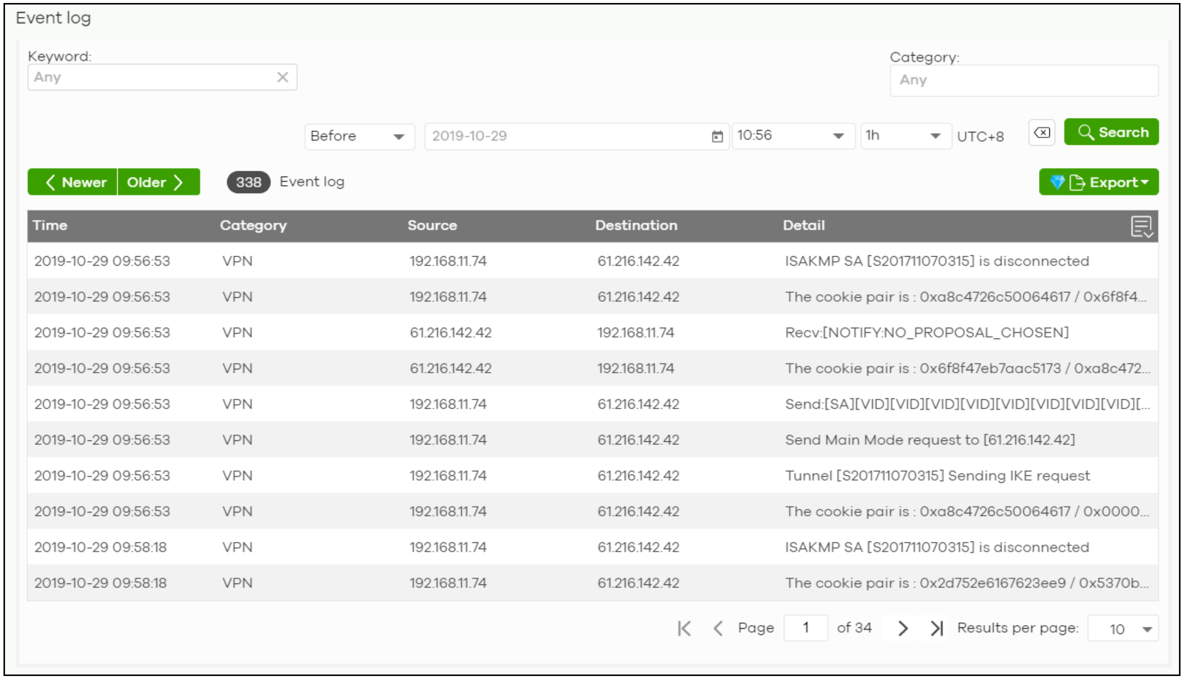
9.2.1 Event Log

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 146 Site-wide > Monitor > Security gateway > Event log



Event log

Keyword: Any

Category: Any

Before | 2019-10-29 | 10:56 | 1h | UTC+8 | Search

< Newer | Older > | 338 Event log | Export

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

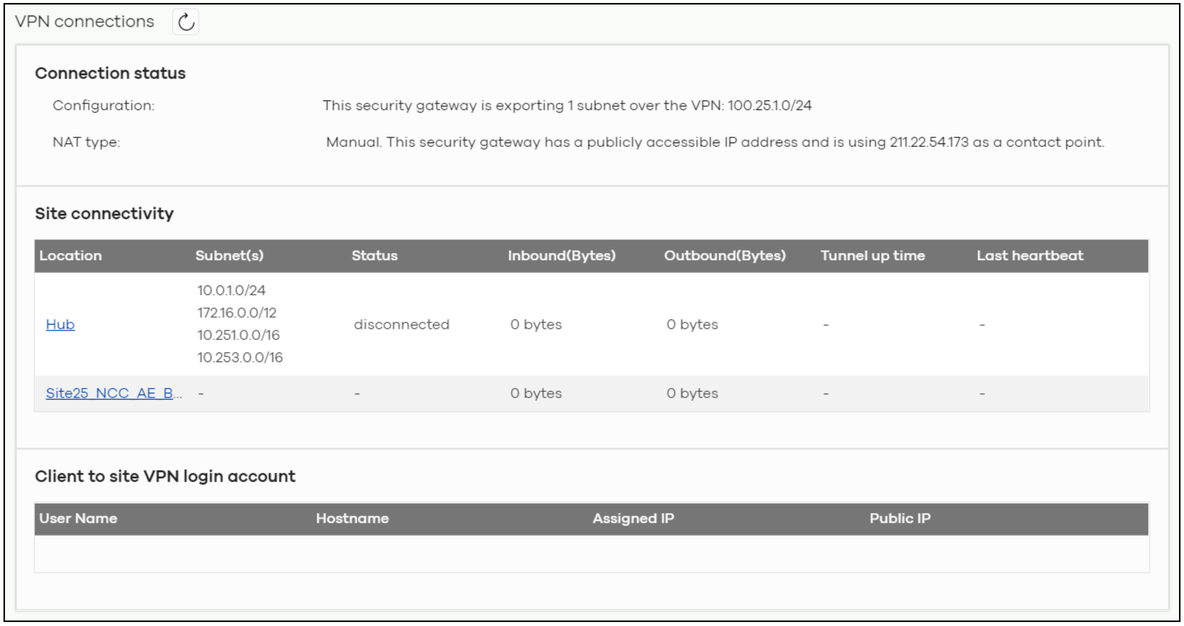
9.2.2 VPN Connections

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 449 for more information.

Click **Site-wide** > **Monitor** > **Security gateway** > **VPN Connections** to access this screen.

Figure 147 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 120 Site-wide > Monitor > Security gateway > VPN Connections

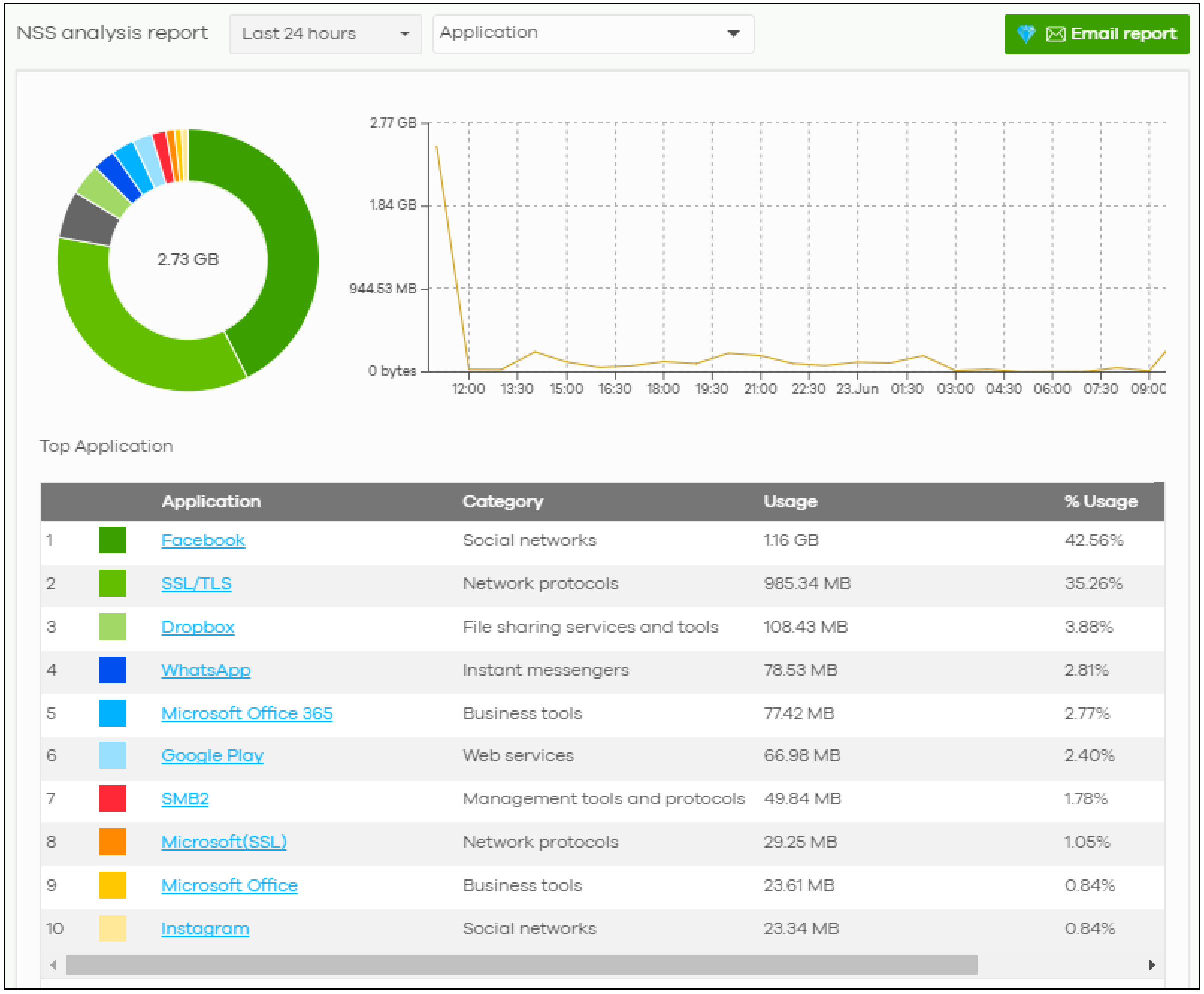
LABEL	DESCRIPTION
↻	Click this button to reload the data-related frames on this page.
Connection Status	
Configuration	This shows the number and address of the local networks behind the Nebula Device, on which the computers are allowed to use the VPN tunnel.
NAT Type	This shows the public IP address 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.
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 filtering, 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 148 Site-wide > Monitor > Security gateway > NSS Analysis 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 121 Site-wide > Monitor > Security gateway > NSS Analysis Report

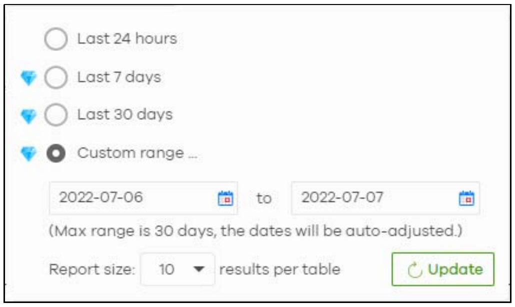
LABEL	DESCRIPTION
Security Appliance – NSS Analysis	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ○ Last 7 days ○ 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 Update
	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.

Table 121 Site-wide > Monitor > Security gateway > NSS Analysis Report (continued)

LABEL	DESCRIPTION
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 414.
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 filtering 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.
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 414.
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.	

Table 121 Site-wide > Monitor > Security gateway > NSS Analysis Report (continued)

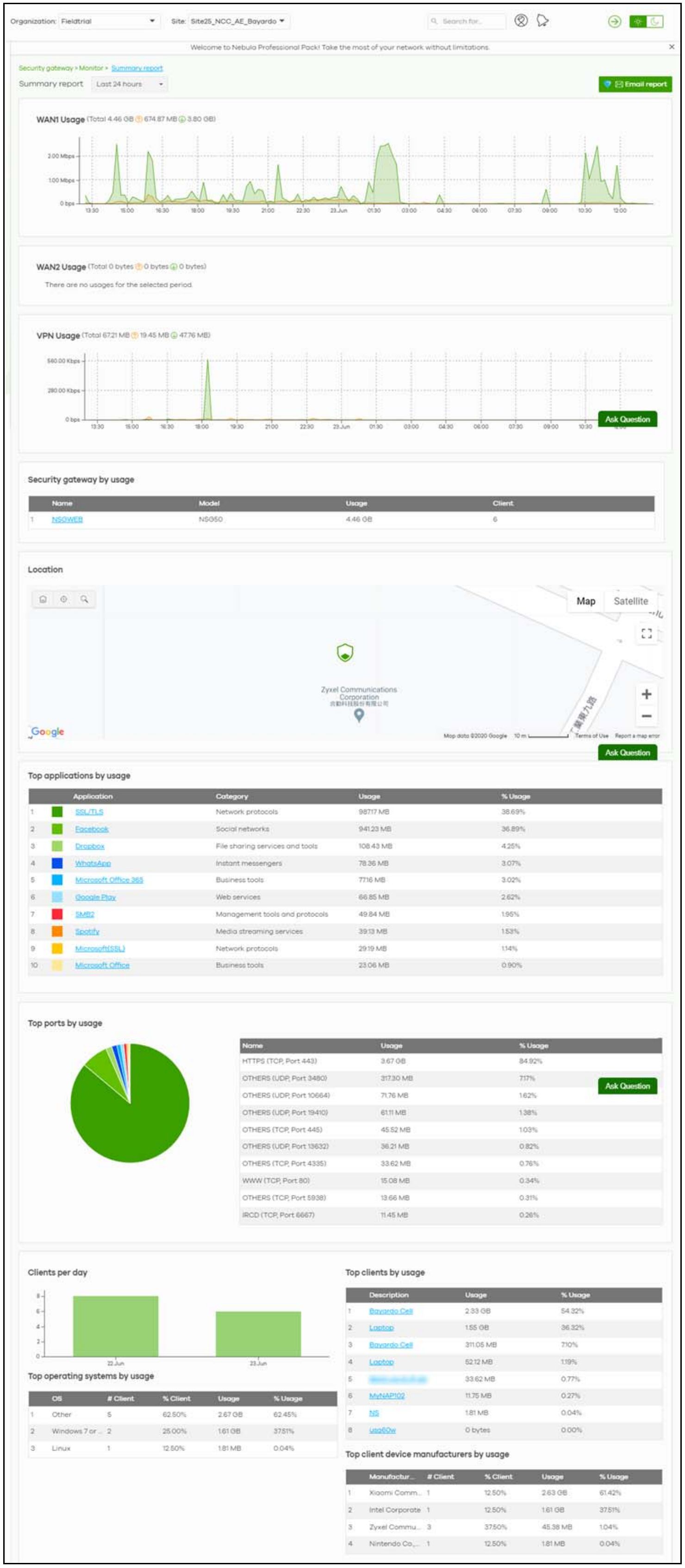
LABEL	DESCRIPTION
y-axis	The y-axis shows the total number of viruses that the gateway has detected.
x-axis	The x-axis shows the time period over which the virus is detected.
Virus Name	This shows the name of the virus that the Nebula Device has detected and blocked. Click a virus name to view the IPv4 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 414.
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 149   Site-wide > Monitor > Security gateway > Summary report



Welcome to Nebula Professional Pack! Take the most of your network without limitations.

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 122 Site-wide > Monitor > Security gateway > Summary report

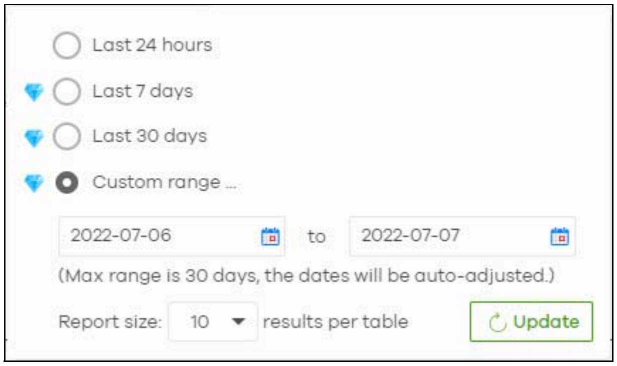
LABEL	DESCRIPTION
Security gateway – Summary report	Select to view the report for the past day, week or month. Alternatively, select **Custom range...** to specify a time period the report will span. You can also select the number of results you want to view in a table.  ○ Last 24 hours ○ Last 7 days ○ 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 122 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.

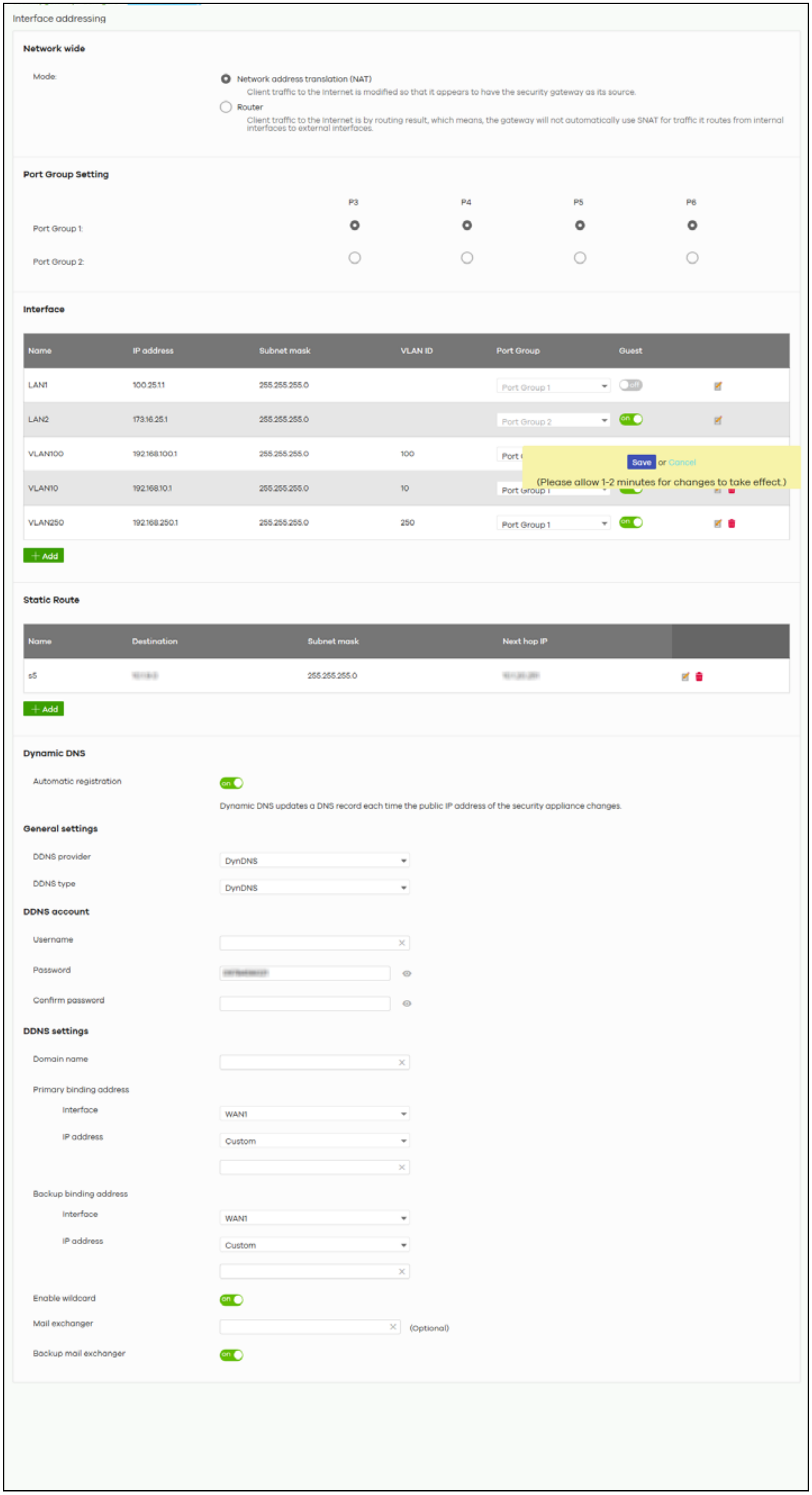
Note: Only one Security Appliance is allowed per site.

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 446.

Figure 150 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

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

Static Route

Name	Destination	Subnet mask	Next hop IP
s5	[redacted]	255.255.255.0	[redacted]

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 123   Site-wide > Configure > Security gateway > Interface addressing

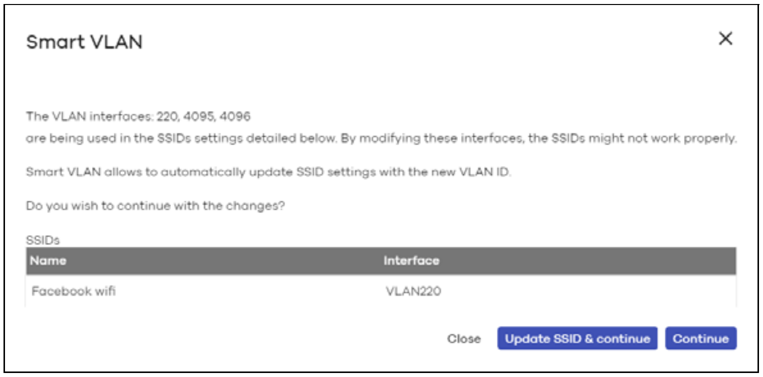
LABEL	DESCRIPTION
Network wide	
Mode	Select **Network address translation (NAT)** to have the Nebula Device automatically use SNAT for traffic it routes from internal interfaces to external interfaces. Select **Router** to have the Nebula Device forward packets according to the routing policies. The 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** > **General 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 123 Site-wide > Configure > Security gateway > Interface addressing (continued)

LABEL	DESCRIPTION
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 427 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 427 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 437 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 437 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.

Table 123 Site-wide > Configure > Security gateway > Interface addressing (continued)

LABEL	DESCRIPTION
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: 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 check box 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.

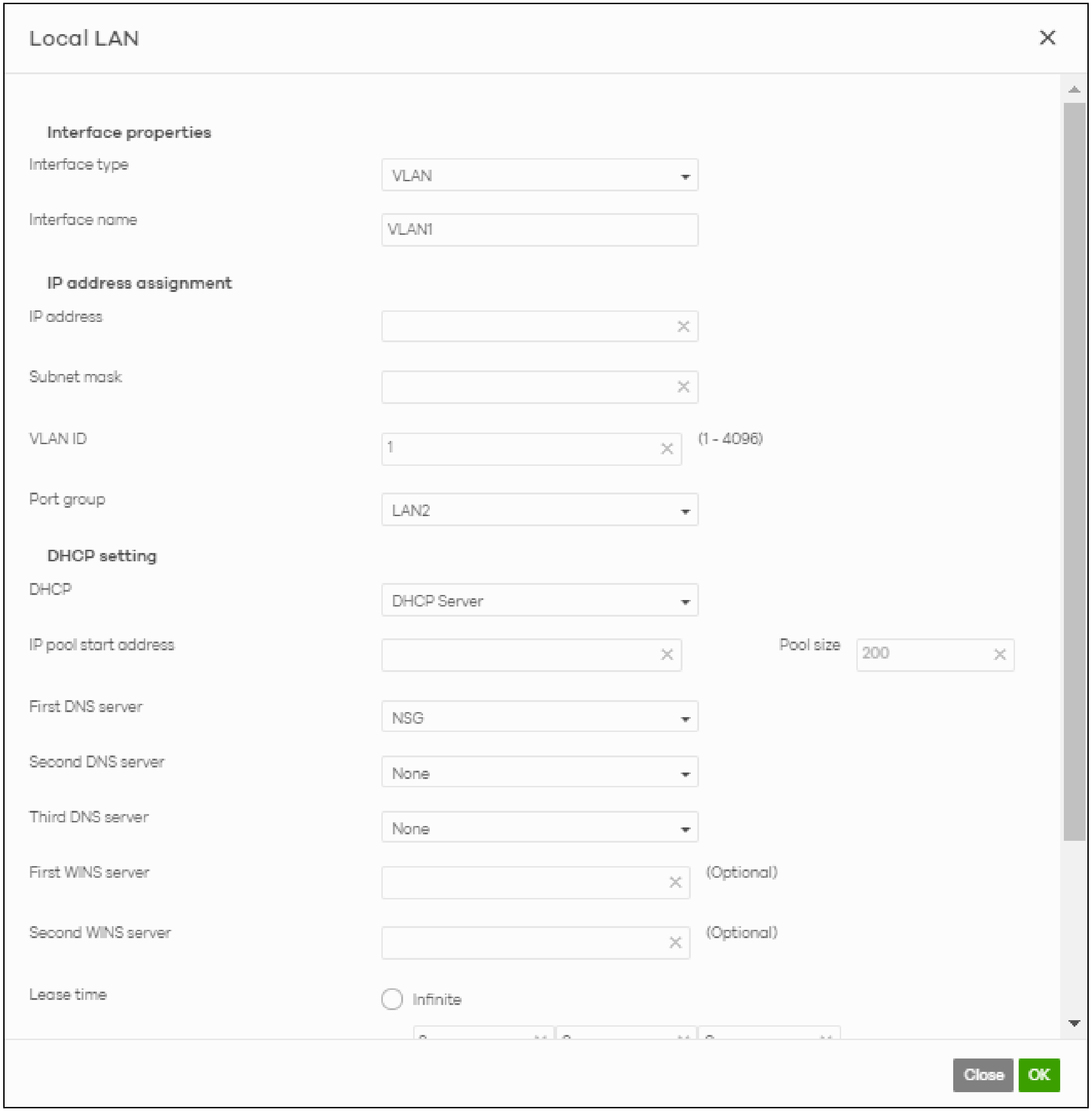
Table 123 Site-wide > Configure > Security gateway > Interface addressing (continued)

LABEL	DESCRIPTION
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 151 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 124 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.

Table 124 Site-wide > Configure > Security gateway > Interface addressing: Local LAN (VLAN)

LABEL	DESCRIPTION
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 to (network) 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.
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.

Table 124   Site-wide > Configure > Security gateway > Interface addressing: Local LAN (VLAN)

LABEL	DESCRIPTION
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 435 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.

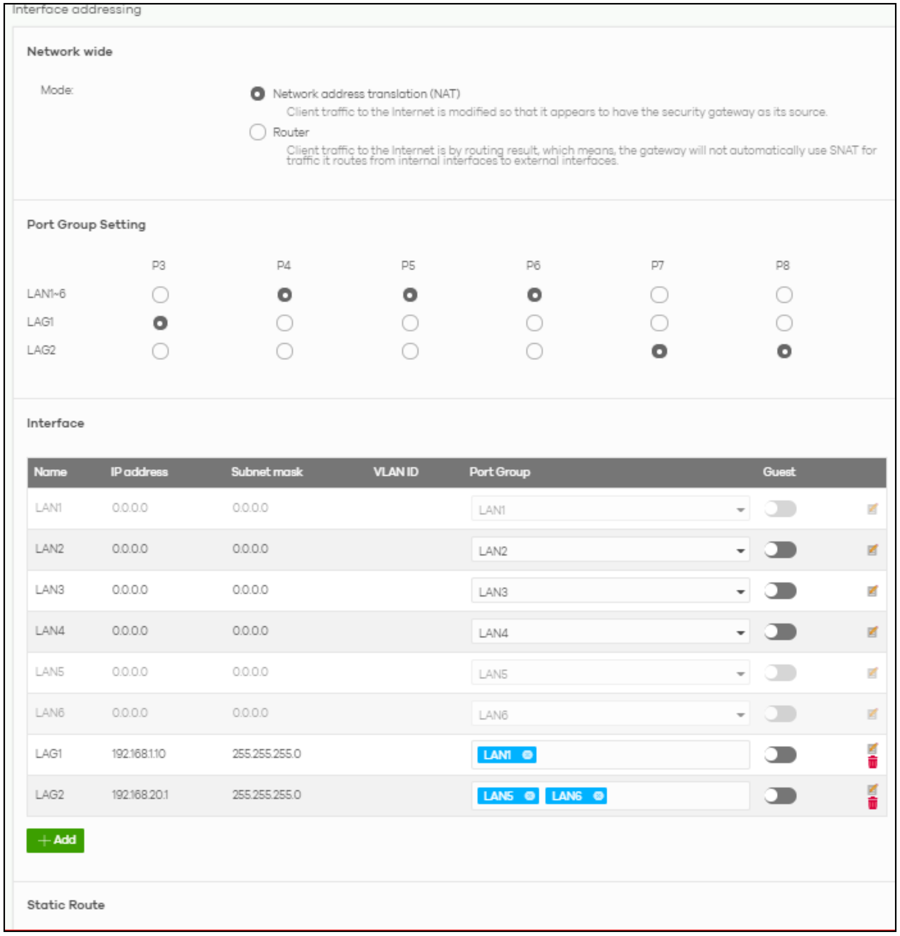
Ports in the group can all connect to a target simultaneously, combining their bandwidth. A LAG can also offer higher network availability; if any port in the group becomes disconnected, the LAG can continue sending data using another port.

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 152 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	

+ Add

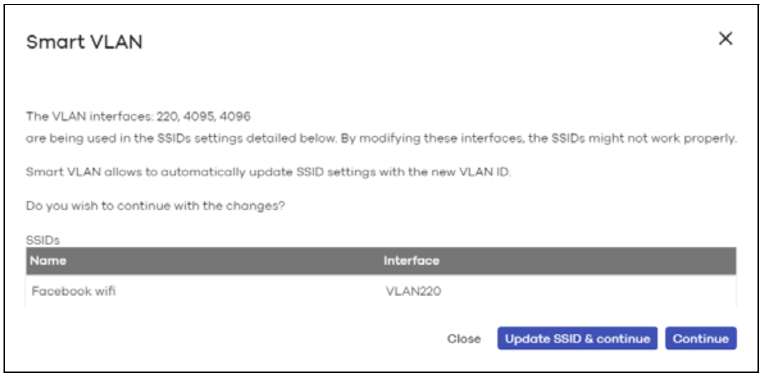
Static Route

The following table describes the labels in this screen.

Table 125 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).

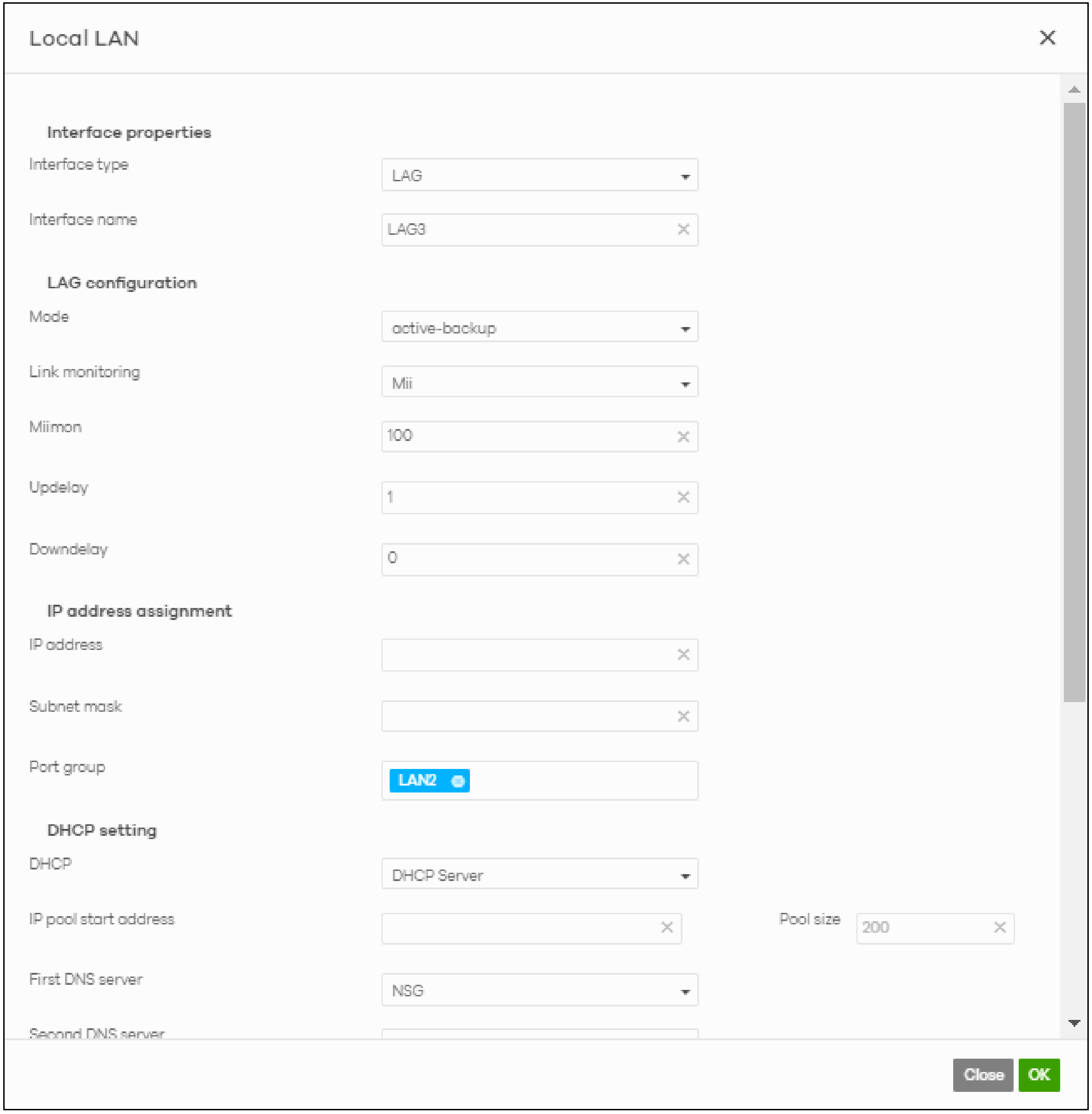
Table 125 Site-wide > Configure > Security gateway > Interface addressing (LAG Interface Type)

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** > **General 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** > **General 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 427 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 427. • For details on creating a link aggregation group, see Section 9.3.2.2 on page 432.

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 153 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 126 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 126 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 to (network) 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**.	

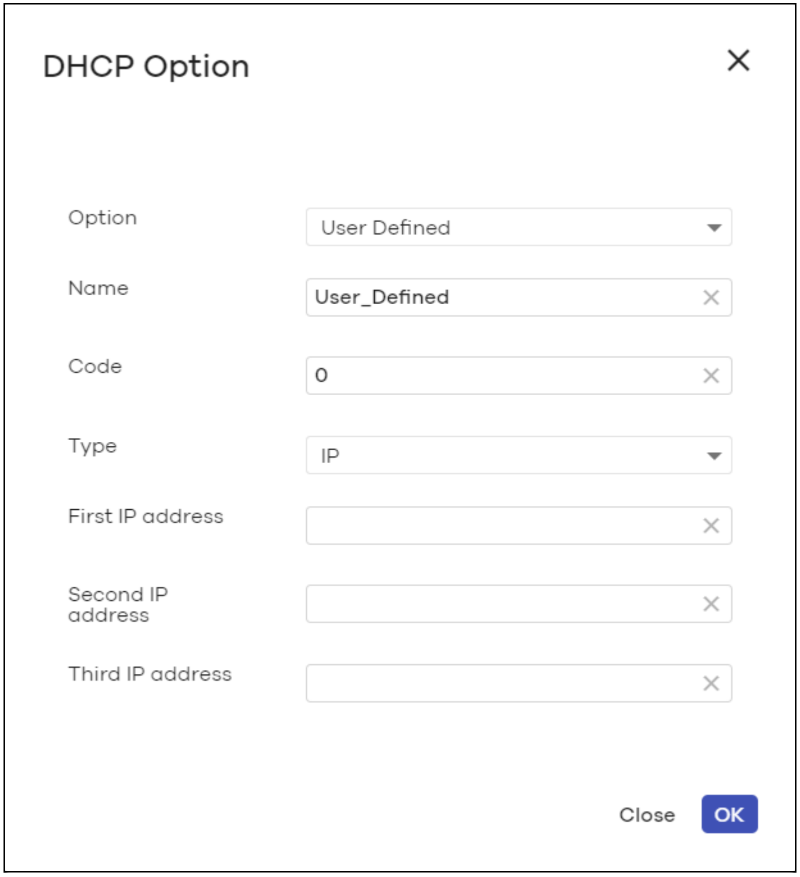
Table 126 Site-wide > Configure > Security gateway > Interface addressing: Local LAN (LAG Interface Type) (continued)

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 435 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 154 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 127 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.

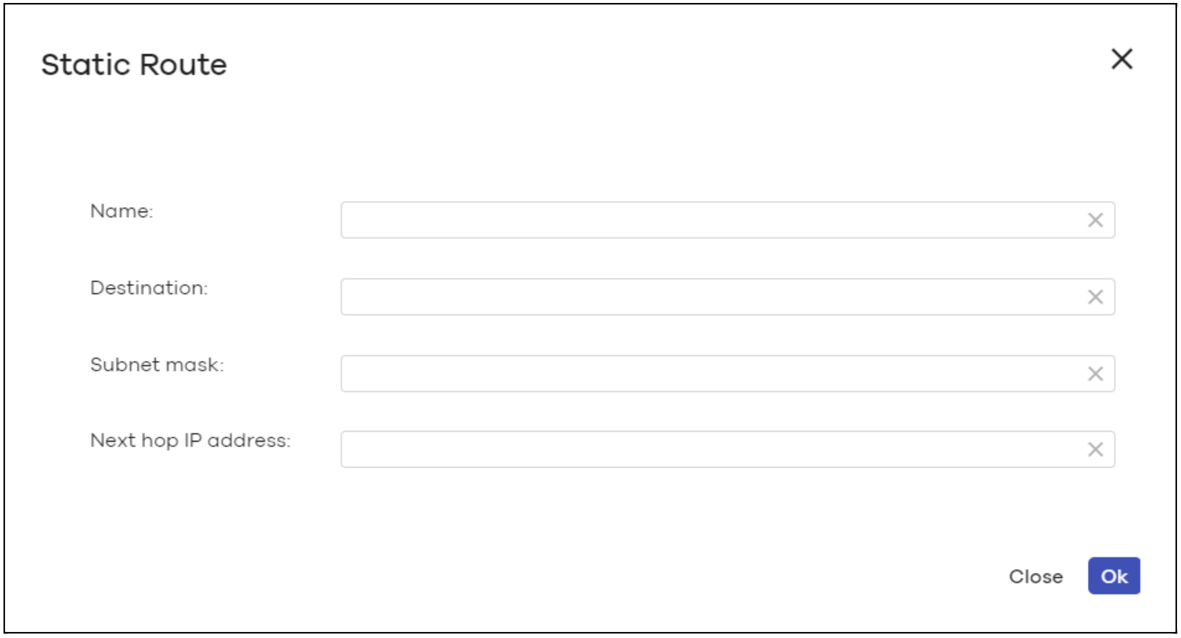
Table 127 Site-wide > Configure > Security gateway > Interface addressing: Local LAN: DHCP Option

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 155 Site-wide > Configure > Security gateway > Interface addressing: Static Route



The following table describes the labels in this screen.

Table 128 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.

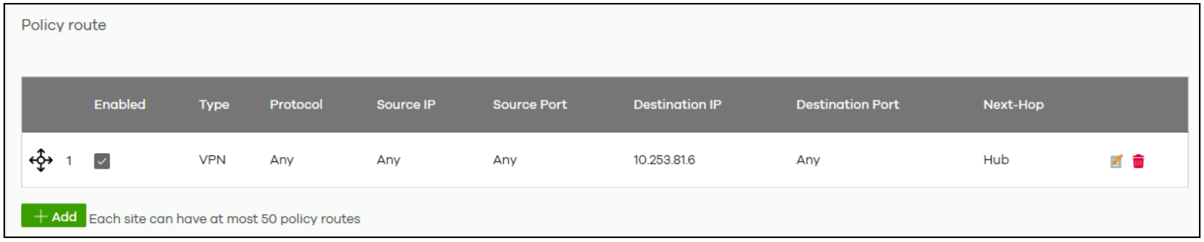
9.3.3 Policy Route

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 156 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.

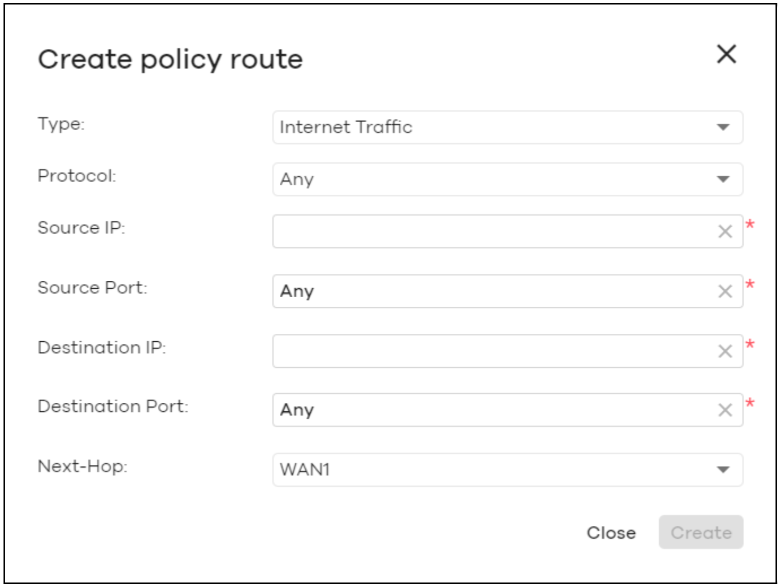
Table 129 Site-wide > Configure > Security gateway > Policy route

LABEL	DESCRIPTION
✥	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box 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 444 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 157 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 130 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.

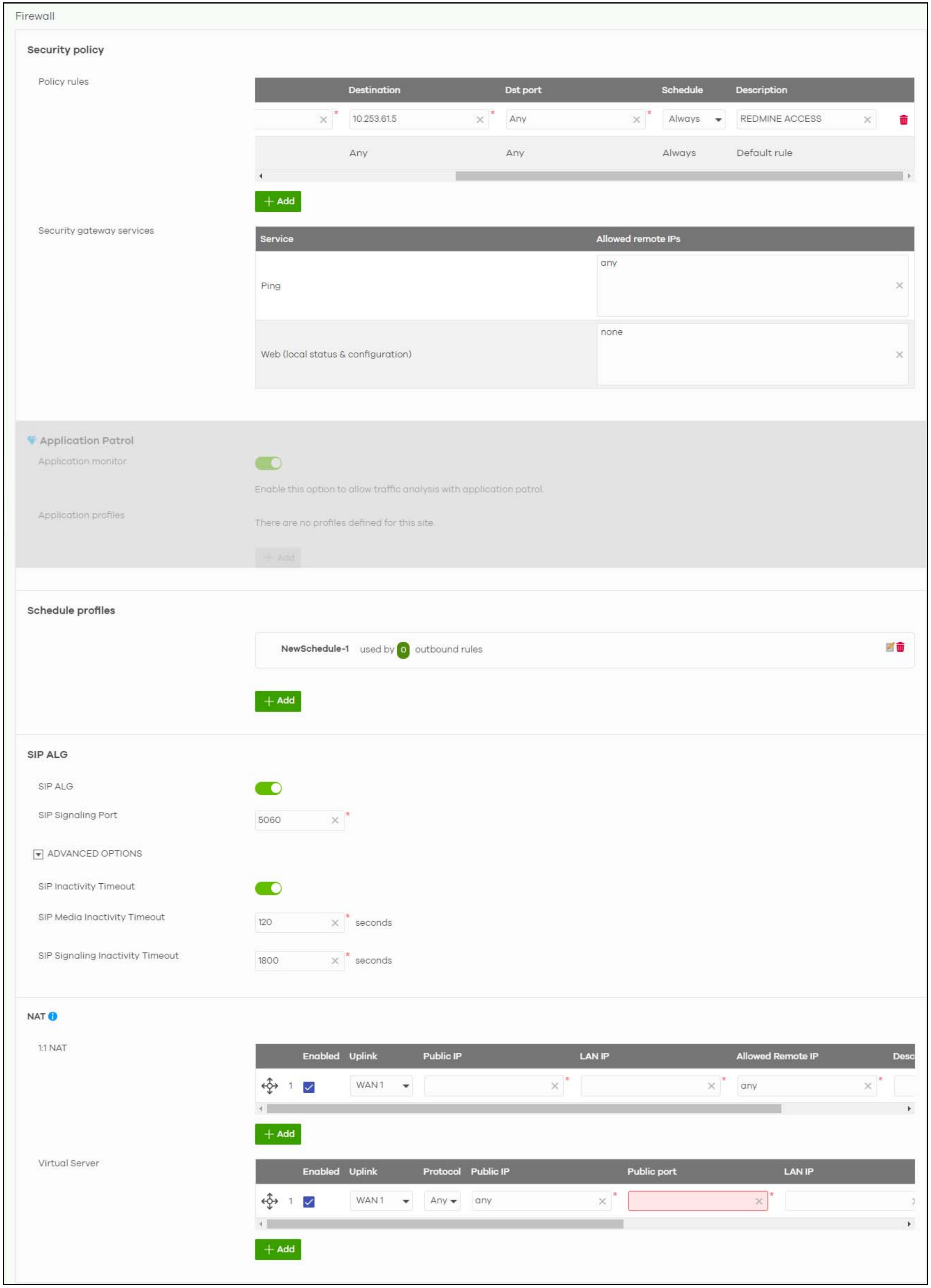
9.3.4 Firewall

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 158 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 131 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 check box to turn on the rule. Otherwise, clear the check box 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 444 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 444 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 131 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 445 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 check box to turn on the rule. Otherwise, clear the check box 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 131 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 check box to turn on the rule. Otherwise, clear the check box 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.

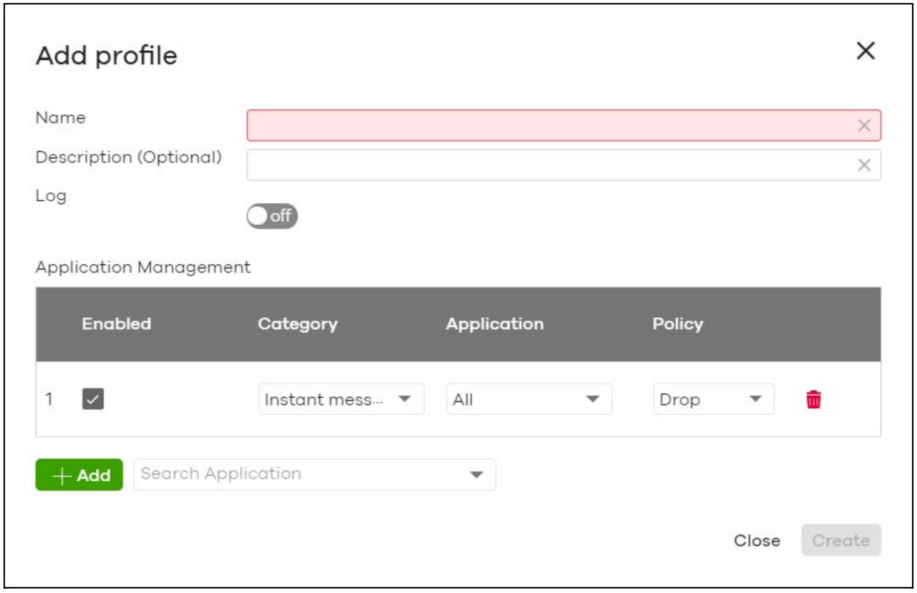
9.3.4.1 Add application patrol profile

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 159 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.

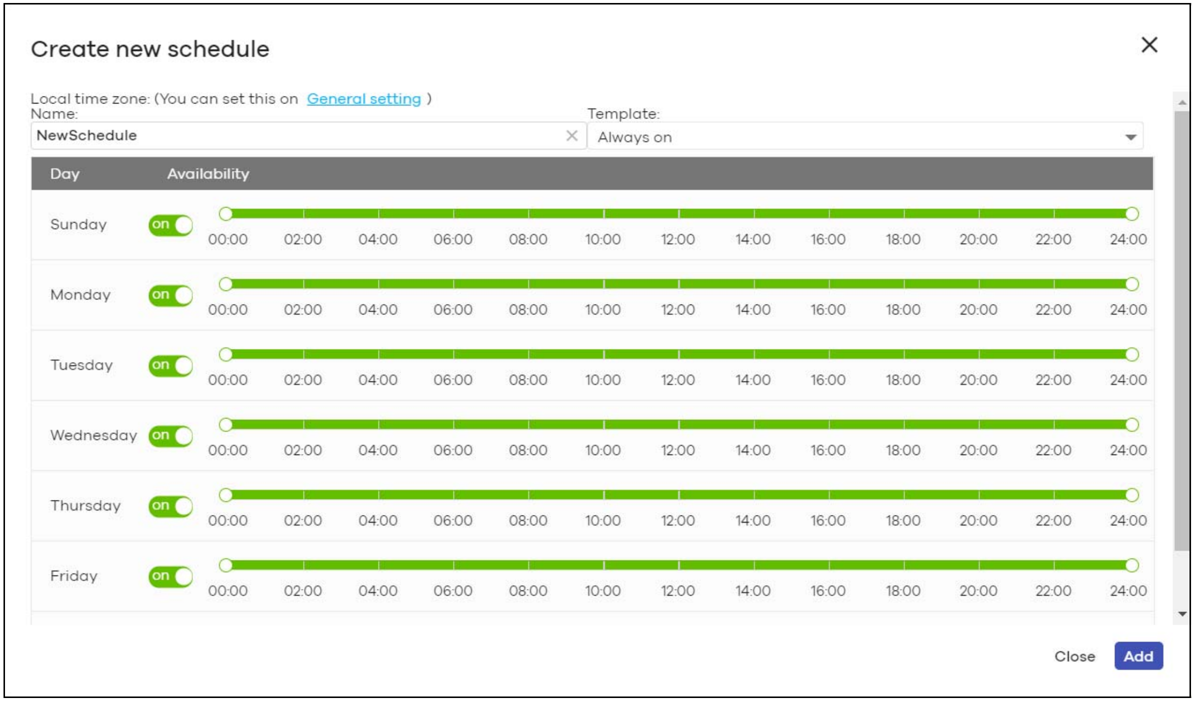
Table 132 Site-wide > Configure > Security gateway > Firewall: Add an application profile

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 check box to turn on the rule. Otherwise, clear the check box 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 160 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 133 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

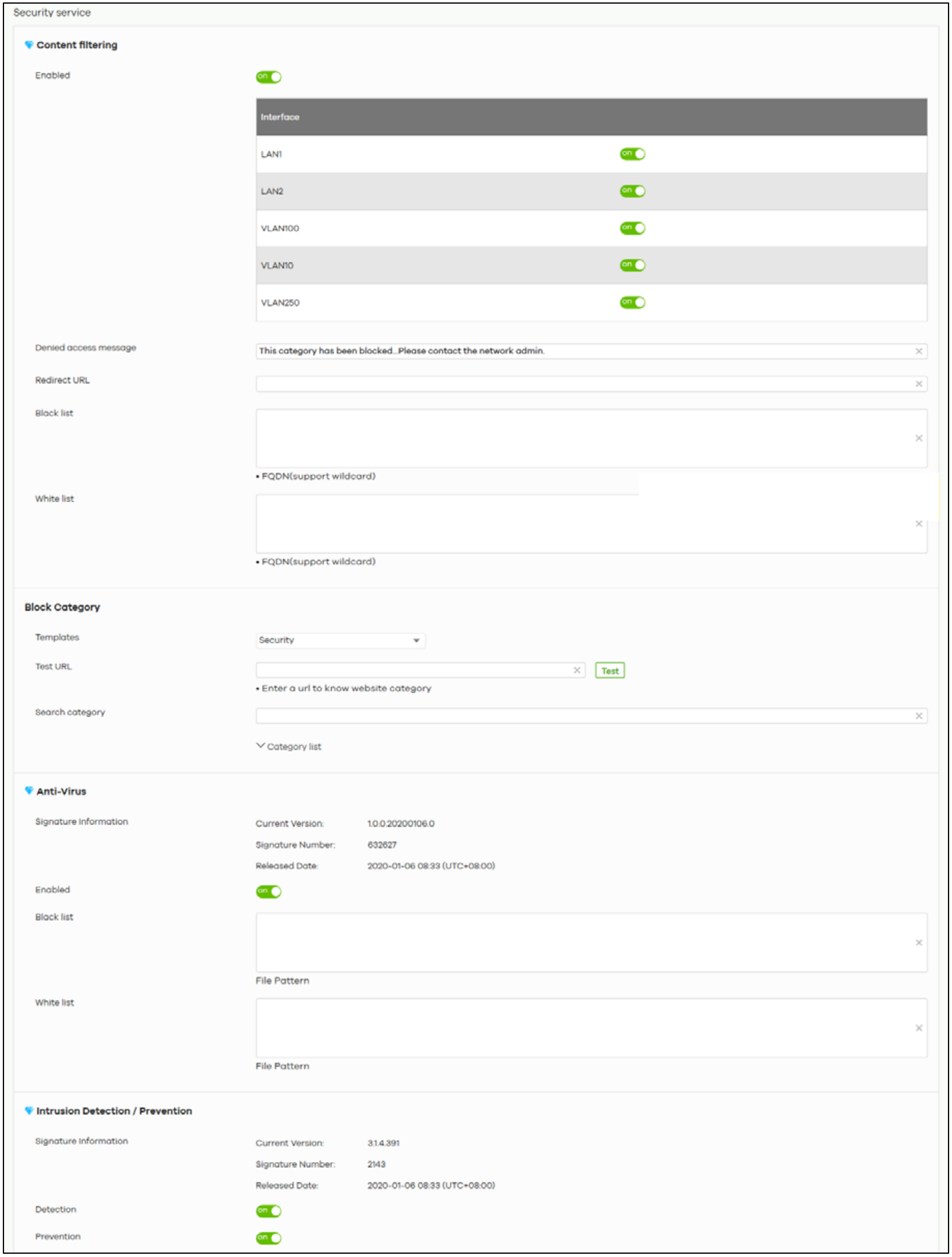
Use this screen to enable or disable the features available in the security pack for your Nebula Device, such as content filtering, Intrusion Detection and Prevention (IDP) and/or anti-virus. As to application patrol, go to the **Firewall** screen to configure it since you need to have a firewall rule for outbound traffic.

Content filtering 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 161 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 134 Site-wide > Configure > Security gateway > Security service

LABEL	DESCRIPTION
Content Filtering	
Enabled	Click **ON** to enable the content filtering 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 filtering 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 filtering 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 Filtering 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 134 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.

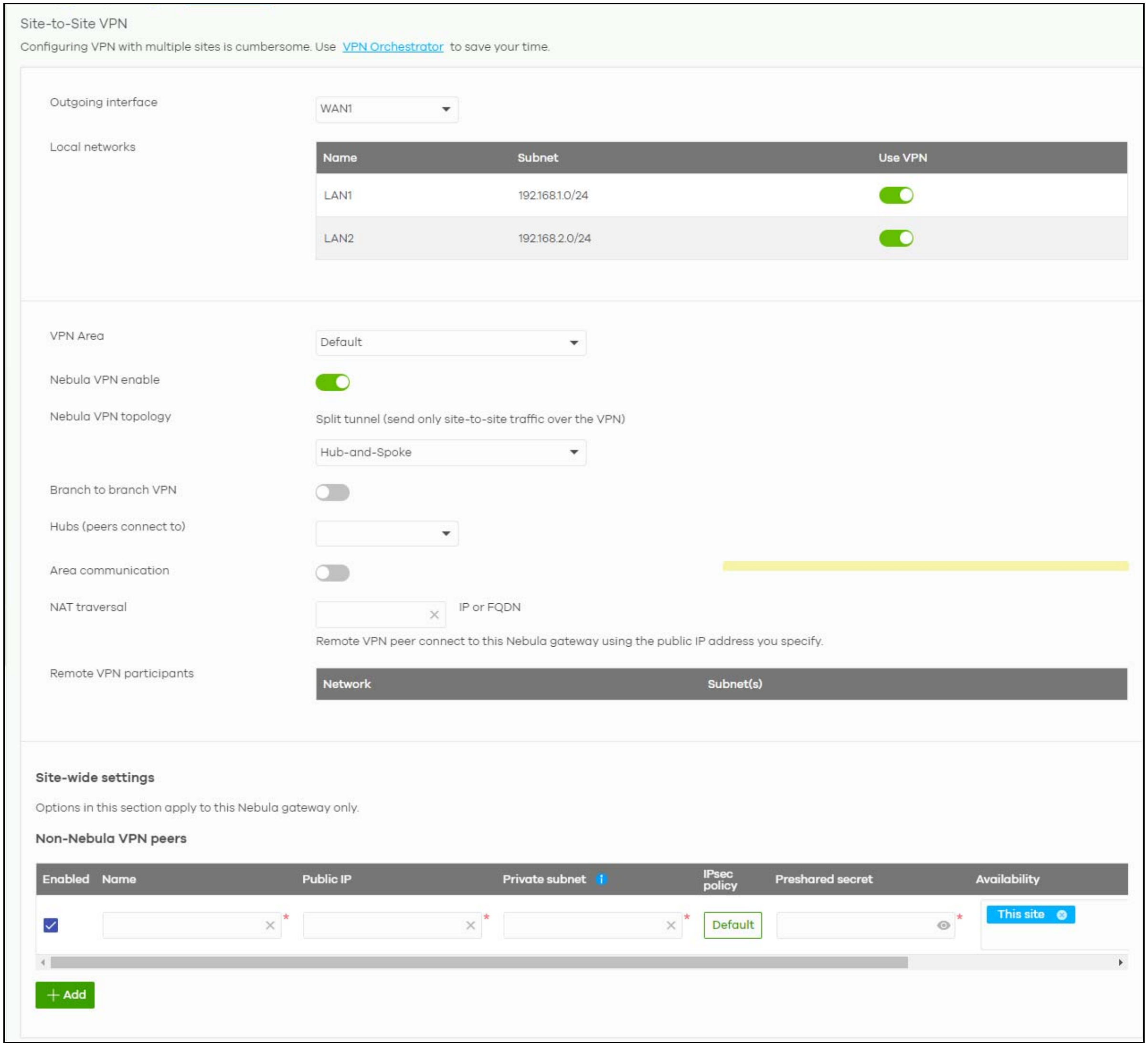
9.3.6 Site-to-Site VPN

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 162 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	On
LAN2	192.168.2.0/24	On

VPN Area: Default

Nebula VPN enable: On

Nebula VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

Hub-and-Spoke

Branch to branch VPN: Off

Hubs (peers connect to)

Area communication: Off

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 135 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 11.4.4.2 on page 524.

Table 135 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 check box to turn on the rule. Otherwise, clear the check box 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 452 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.

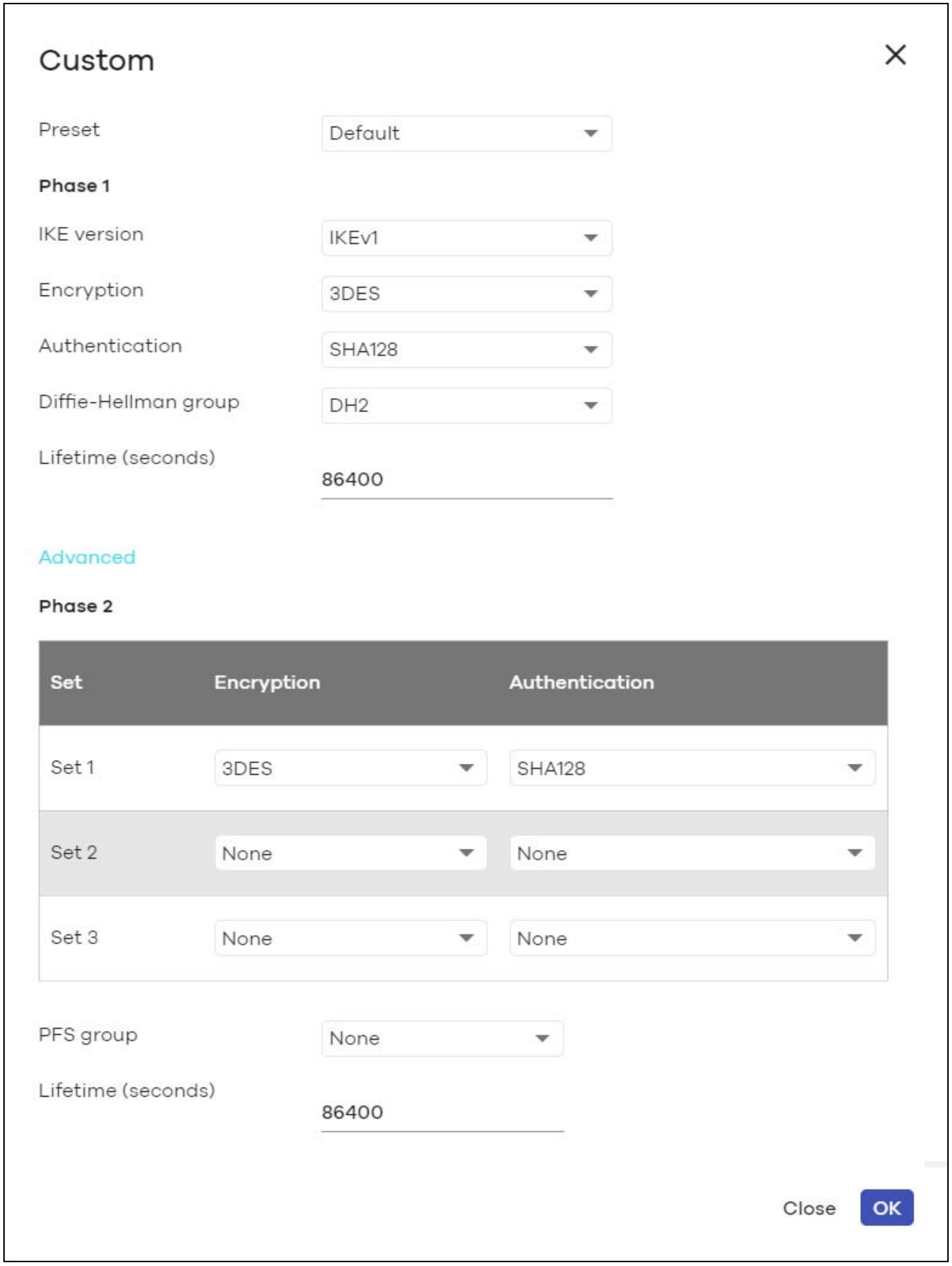
Table 135 Site-wide > Configure > Security gateway > Site-to-Site VPN (continued)

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 163   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 136   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 136 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 **DH2** – use a 1024-bit random number **DH5** – use a 1536-bit random number **DH14** – use a 2048-bit random number 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 136 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

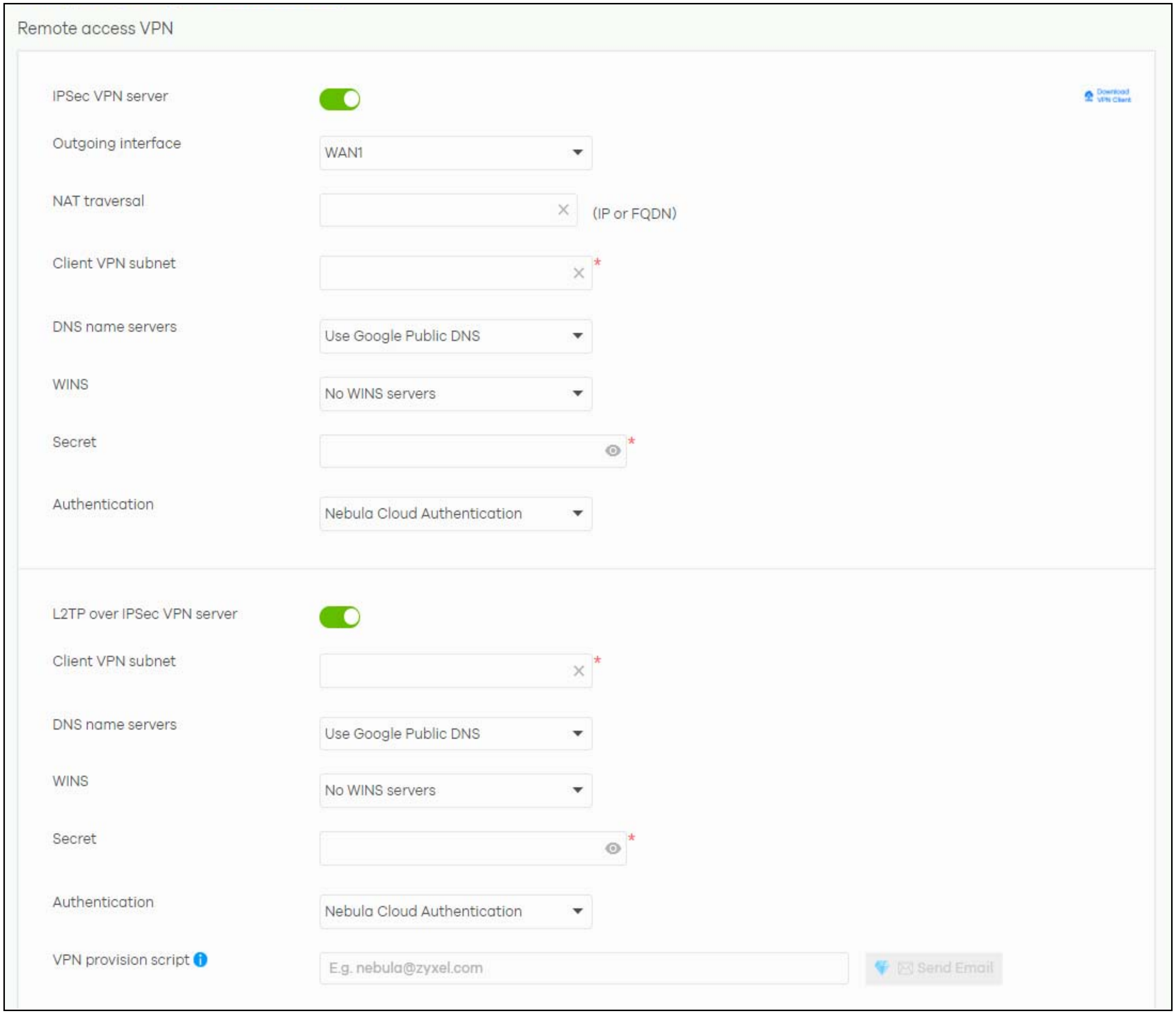
Use this screen to configure the VPN client settings.

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 164 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 137 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 137 Site-wide > Configure > Security gateway > Remote access VPN (continued)

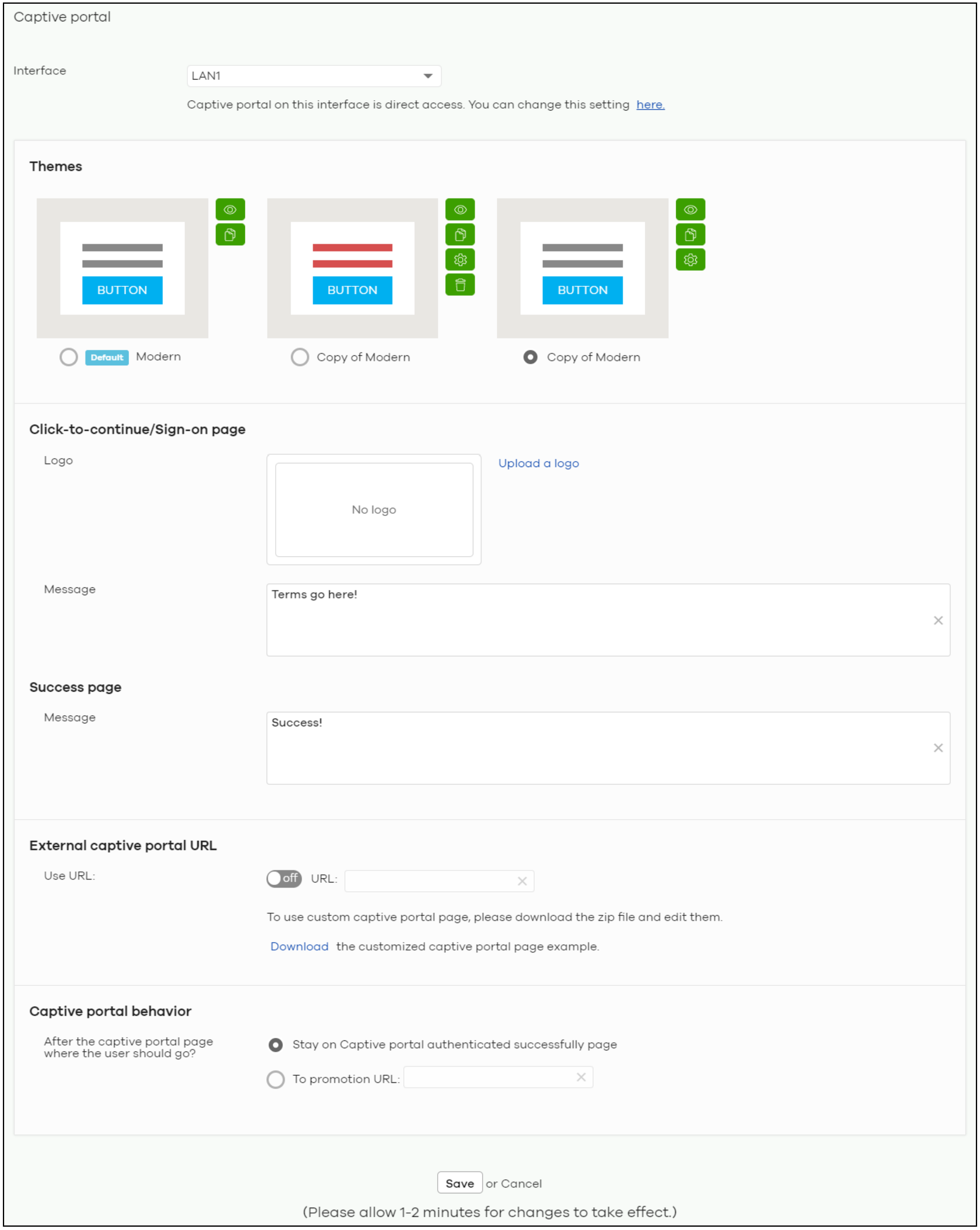
LABEL	DESCRIPTION
Authentication	Select how the Nebula Device authenticates a remote user before allowing access to the L2TP over IPSec VPN tunnel.
VPN provision script	Send an email to help automatically configure VPN settings on client devices so that the devices can remotely access this Nebula Device. 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 165 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.

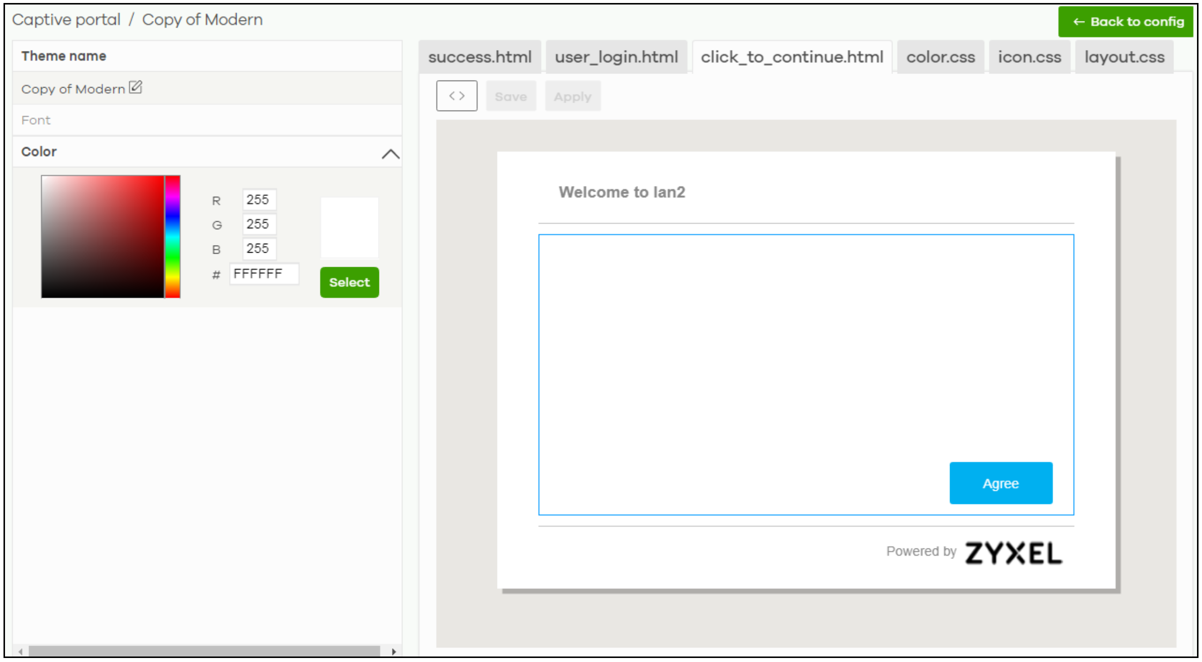
Table 138 Site-wide > Configure > Security gateway > Captive portal

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 460. • 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 166 Site-wide > Configure > Security gateway > Captive portal: Edit



The following table describes the labels in this screen.

Table 139 Site-wide > Configure > Security gateway > Captive portal: Edit

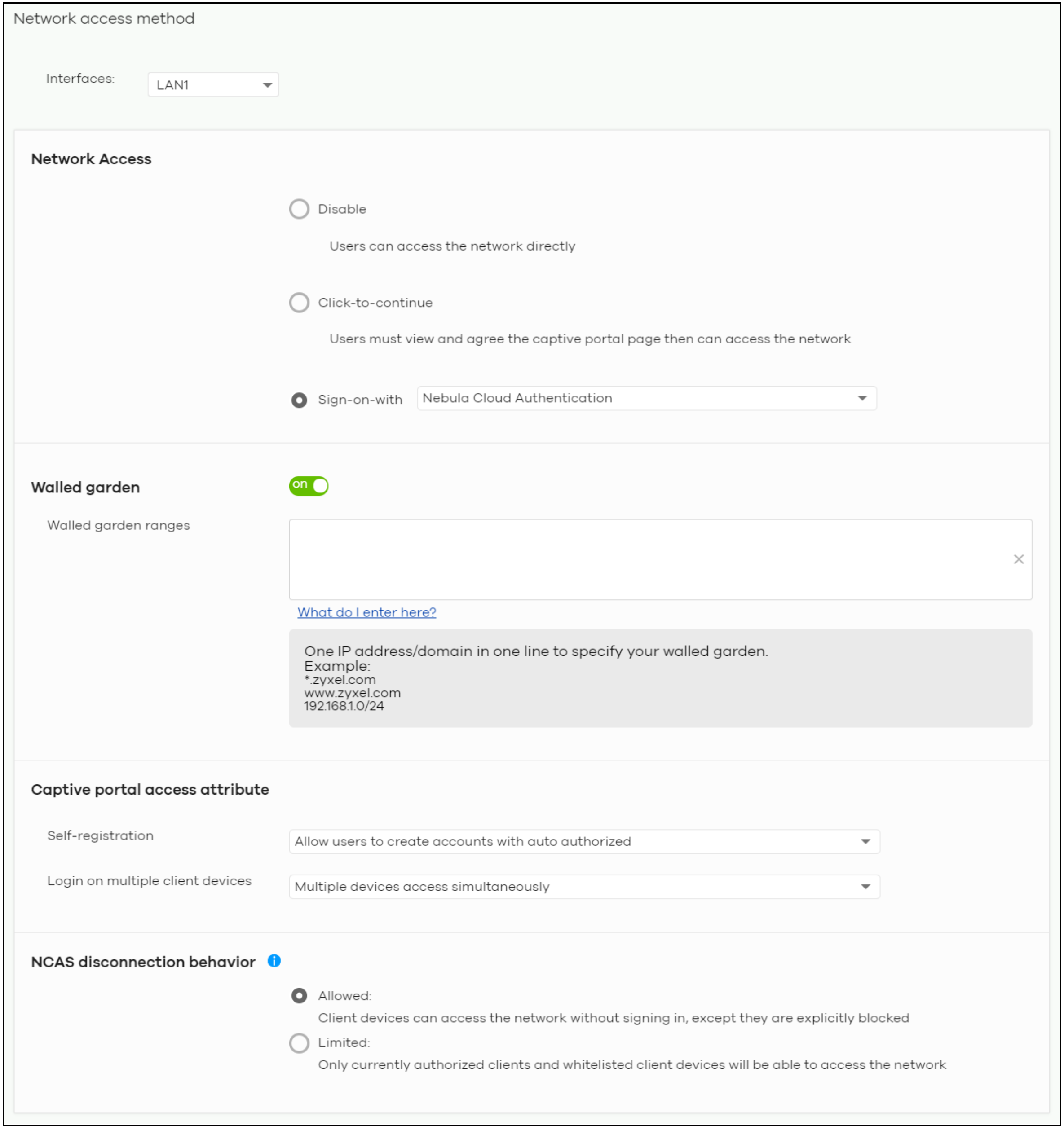
LABEL	DESCRIPTION
Back to config	Click this button to return to the **Captive portal** screen.
Theme name	This shows the name of the theme. Click the edit icon to change it.
Font	Click the arrow to hide or display the configuration fields. To display this section and customize the font type and/or size, 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 167 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

Walled garden ranges

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 140 Site-wide > Configure > Security gateway > Network access method

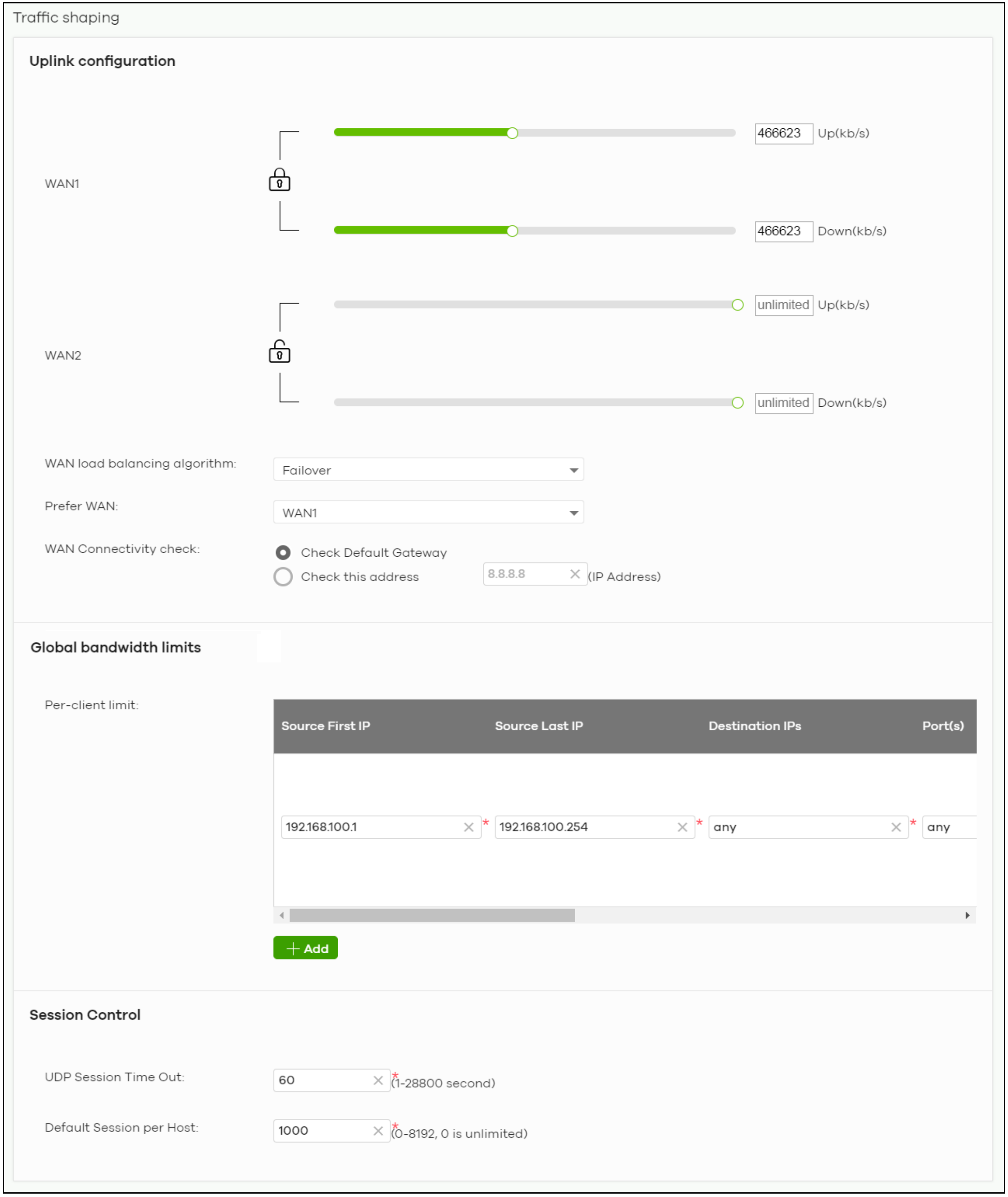
LABEL	DESCRIPTION
Interfaces	Select the Nebula Device's interface (network) to which the settings you configure here is applied.
Network Access	Select **Disable** to turn off web authentication. Select **Click-to-continue** to block network traffic until a client agrees to the policy of user agreement. 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 466). 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 168 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

Add

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 141 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 141 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

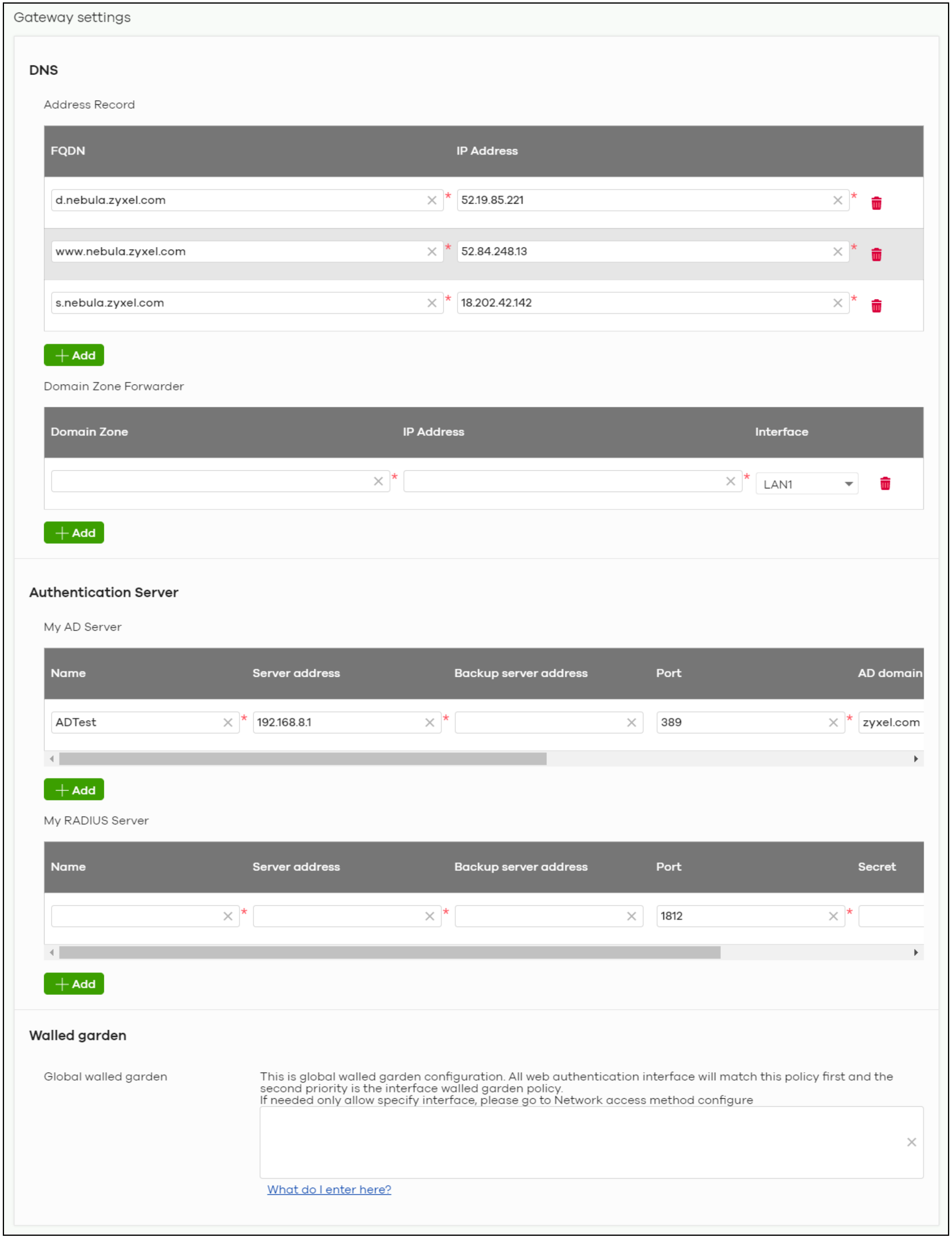
Use this screen to configure DNS settings and external AD (Active Directory) server or RADIUS server that the Nebula Device can use in authenticating users.

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 169 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

Domain Zone Forwarder

Domain Zone	IP Address	Interface
		LAN1

Authentication Server

My AD Server

Name	Server address	Backup server address	Port	AD domain
ADTest	192.168.8.1		389	zyxel.com

My RADIUS Server

Name	Server address	Backup server address	Port	Secret
			1812	

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 142   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 469.
🗑	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.

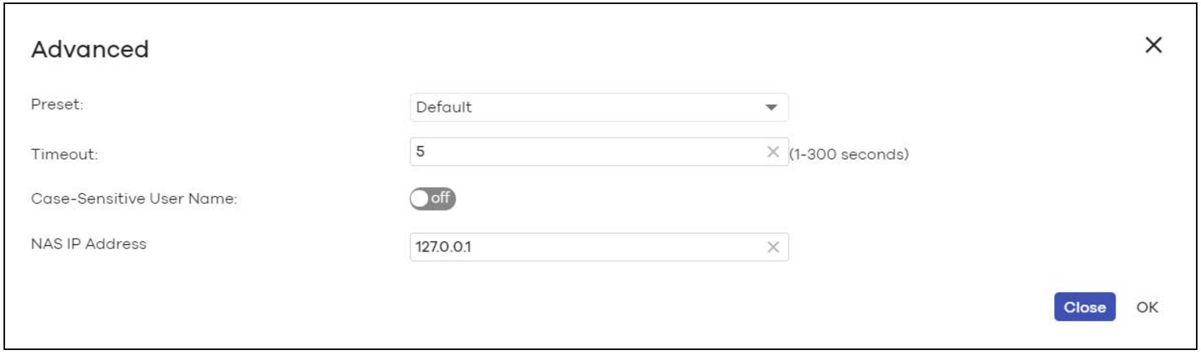
Table 142 Site-wide > Configure > Security gateway > Gateway settings (continued)

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 469.
🗑	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 170 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 143 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 143   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.

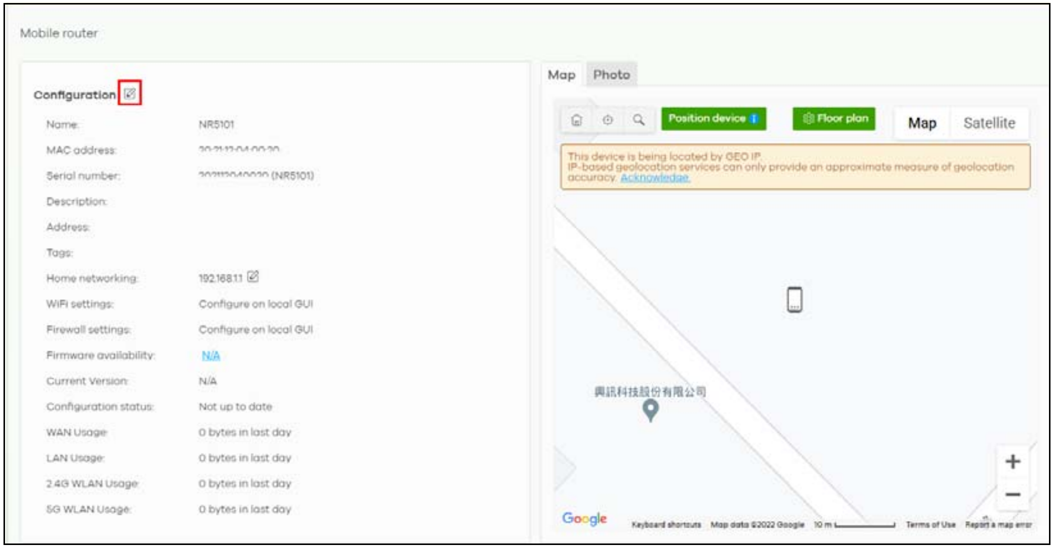
A Nebula Mobile Router is an LTE or NR cellular 5G indoor or outdoor router that can be managed by Nebula. It is referred to as a Nebula Device in this chapter. To identify whether your Nebula Device is an outdoor or indoor device and view the list of the Nebula Devices that can be managed through the NCC, go to **Help** > **Support tools** > **Device function table**.

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 171 Site-wide > Devices > Mobile router > Configuration (Indoor)



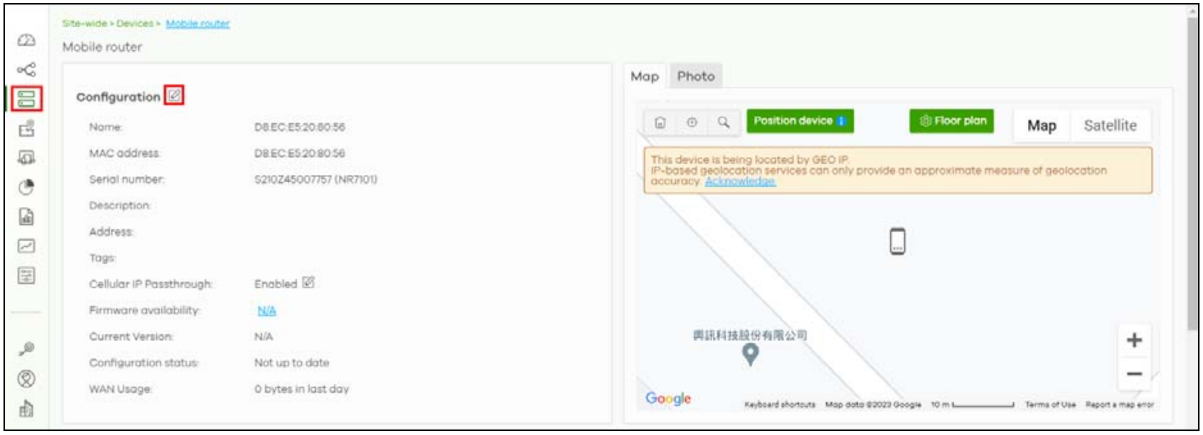
Mobile router

Configuration ✎

Name:	NR5101
MAC address:	[illegible]
Serial number:	[illegible] (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 172   Site-wide > Devices > Mobile router > Configuration (Outdoor)



Site-wide > Devices > Mobile router

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

Firmware availability: N/A

Current Version: N/A

Configuration status: Not up to date

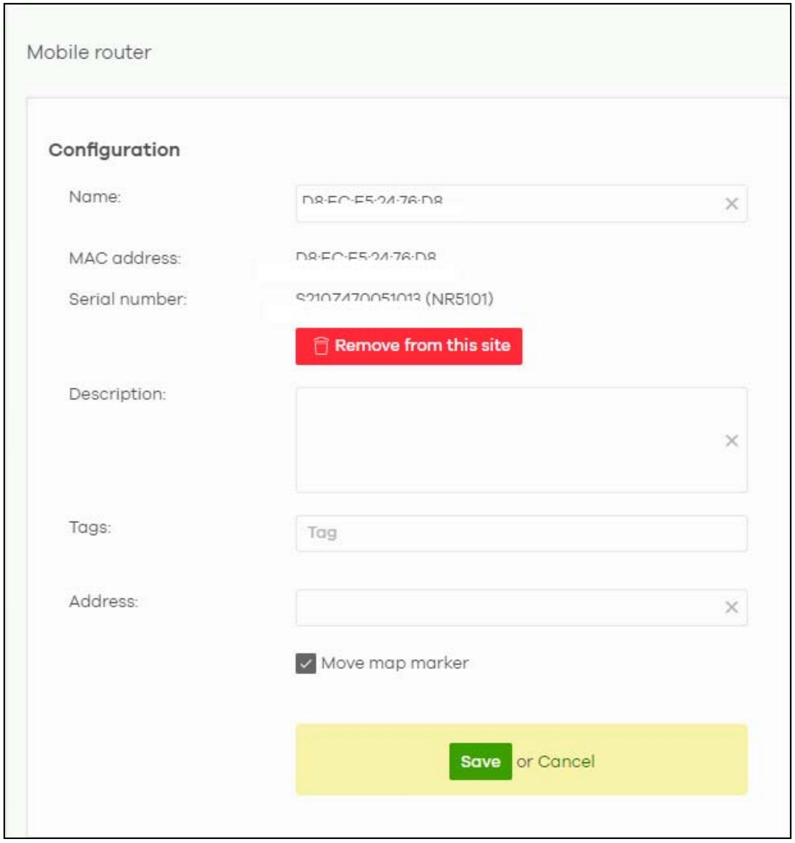
WAN Usage: 0 bytes in last day

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 173   Site-wide > Devices > Mobile router > Configuration: Edit



Mobile router

Configuration

Name: D8:EC:F5:24:76:D8

MAC address: D8:EC:F5:24:76:D8

Serial number: S210Z470051013 (NR5101)

Description:

Tags: Tag

Address:

☑ Move map marker

The following table describes the labels in this screen.

Table 144 Site-wide > Devices > Mobile router > Configuration: Edit

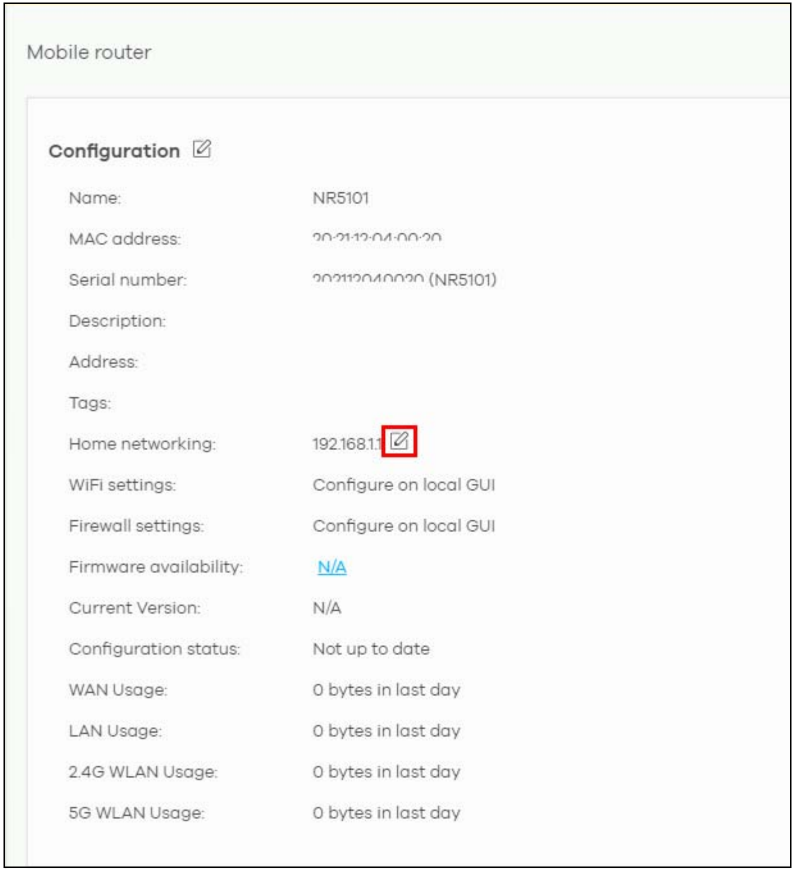
LABEL	DESCRIPTION
Configuration	
Name	Enter a descriptive name for the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
Serial number	This shows the serial number of the Nebula Device.
Description	Enter a user-specified description for the Nebula Device.
Tags	Enter a user-specified 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.

Note: Home Networking is only available for the LTE3301-PLUS and NR5101.

Figure 174 Site-wide > Devices > Mobile router > Configuration: Home networking (Indoor)



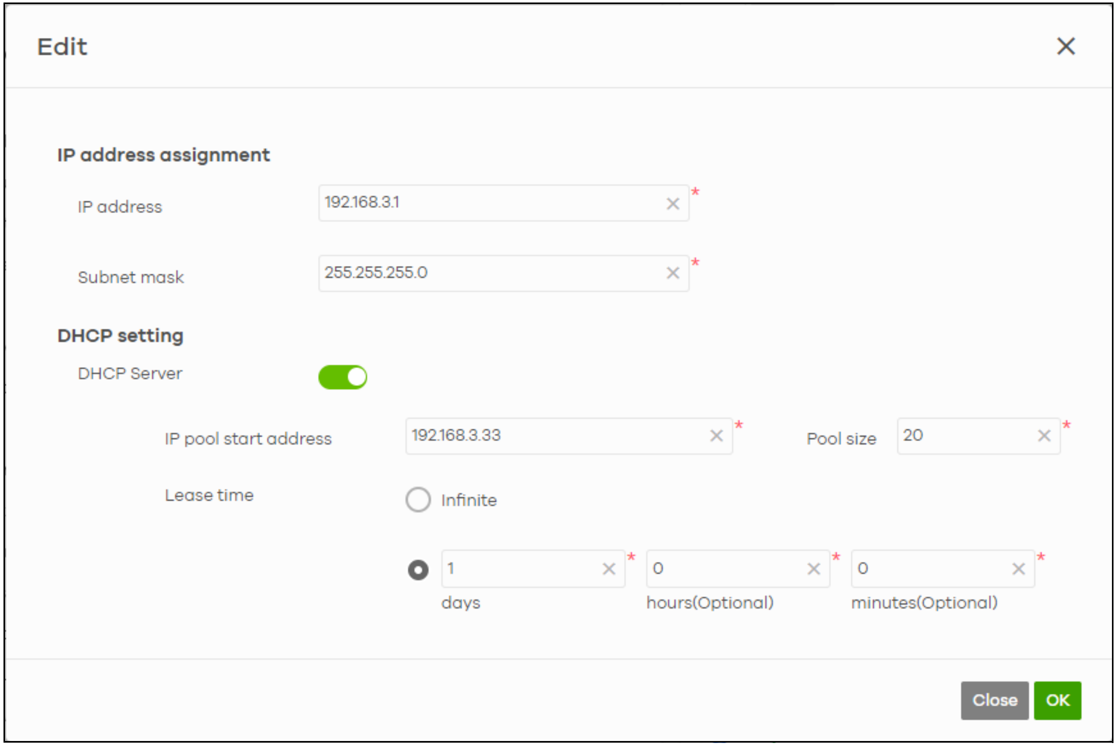
Mobile router

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

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 175 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 145 Site-wide > Devices > Mobile router > Configuration > Home networking: Edit

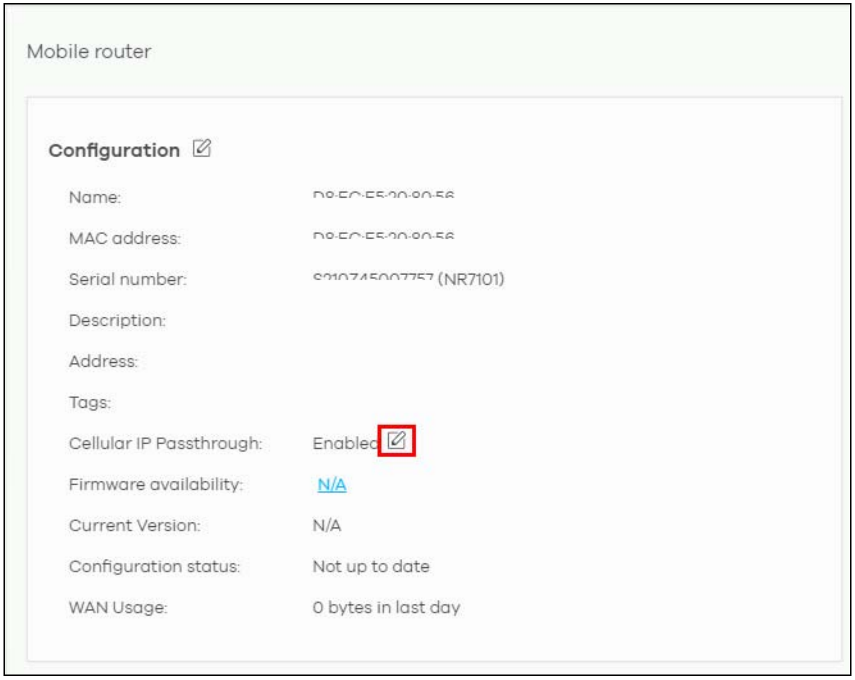
LABEL	DESCRIPTION
IP address assignment	
IP address	Enter the IP address for this interface.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
DHCP setting	
DHCP Server	Select 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.

Note: As of this writing, cellular IP passthrough is for NR7101 and LTE7461 only.

Figure 176 Site-wide > Devices > Mobile router > Configuration: Cellular IP Passthrough (Outdoor)



Mobile router

Configuration ✎

Name: D8:EC:E5:20:80:56

MAC address: D8:EC:E5:20:80:56

Serial number: S210745007757 (NR7101)

Description:

Address:

Tags:

Cellular IP Passthrough: Enabled ✎

Firmware availability: N/A

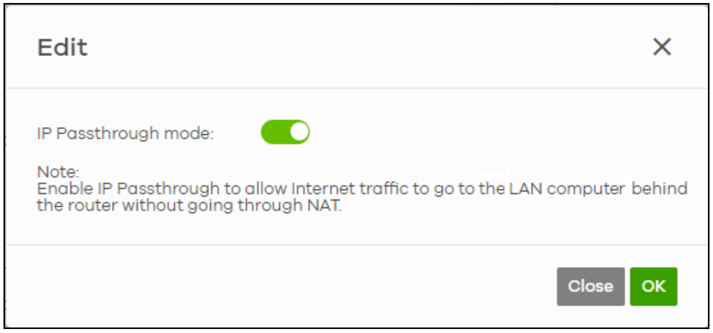
Current Version: N/A

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 177 Site-wide > Devices > Mobile router > Configuration > Cellular IP Passthrough: Edit



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 146   Site-wide > Devices > Mobile router > Configuration > Cellular IP Passthrough: Edit

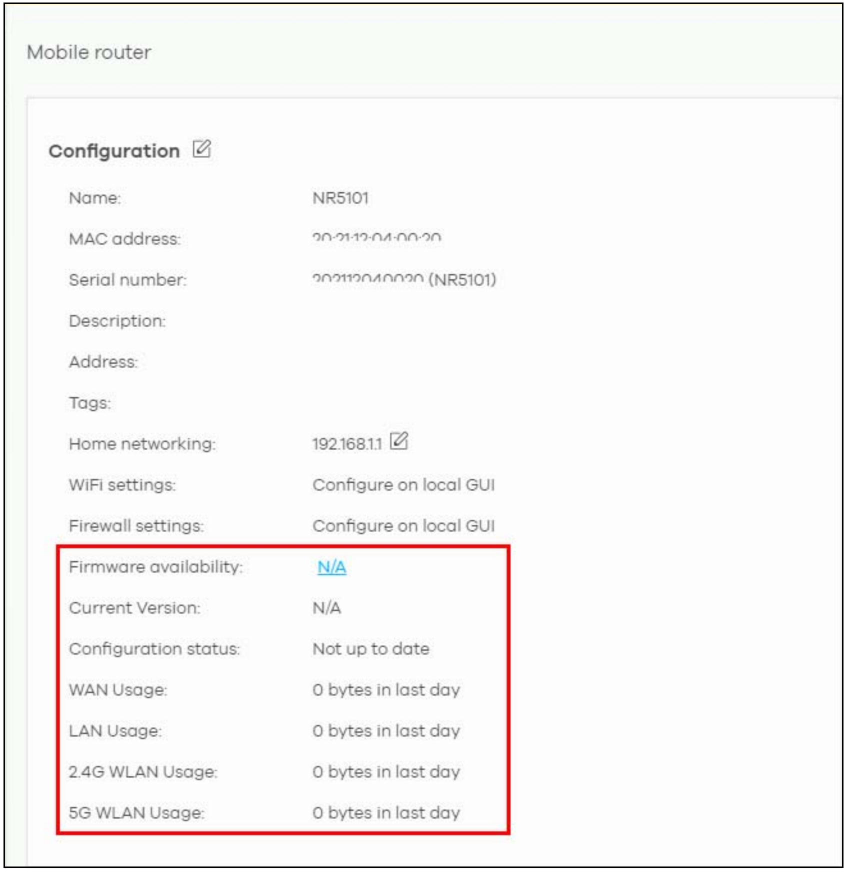
LABEL	DESCRIPTION
IP Passthrough mode	This displays if IP passthrough is enabled on the Nebula Device.
Close	Click **Close** to exit this screen without saving.
OK	Click **OK** to save your changes.

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 178   Site-wide > Devices > Mobile router > Configuration > Firmware status



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

The following table describes the labels in this screen.

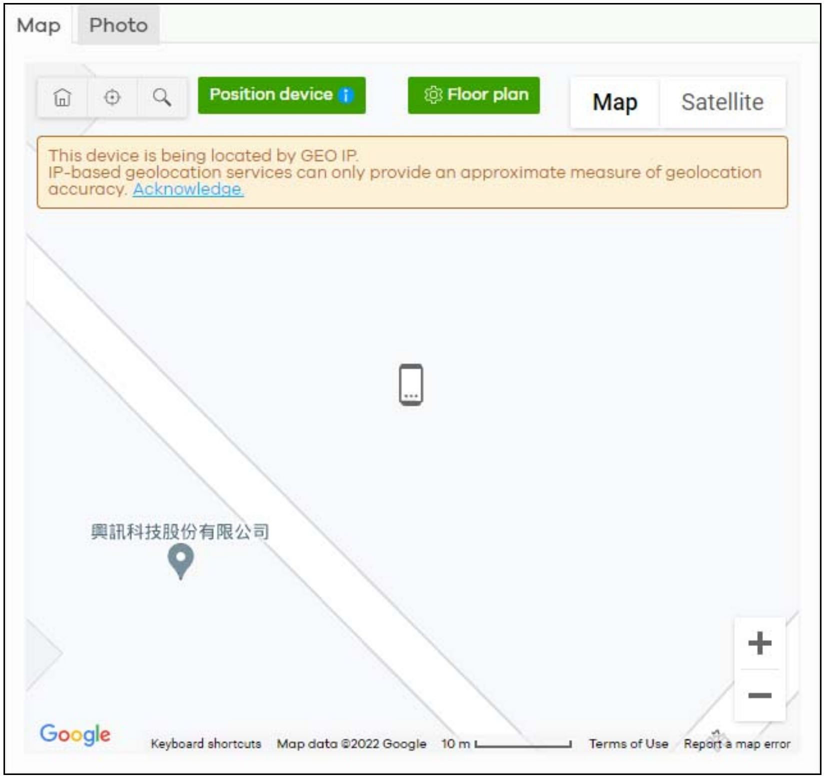
Table 147 Site-wide > Devices > Mobile router > Configuration > Firmware status

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.
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.

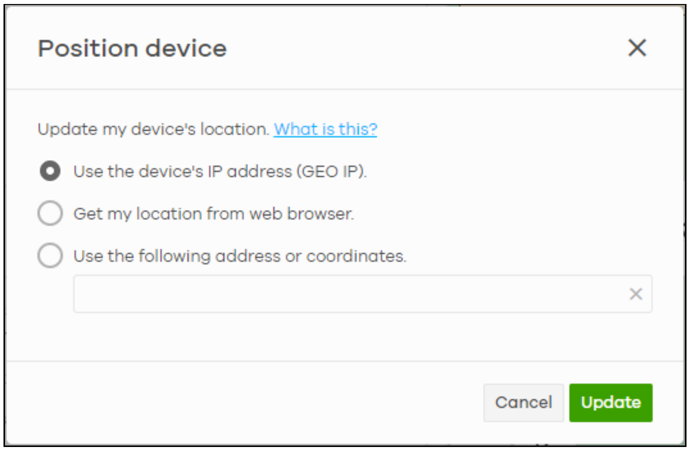
Figure 179 Site-wide > Devices > Mobile router > Map



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.

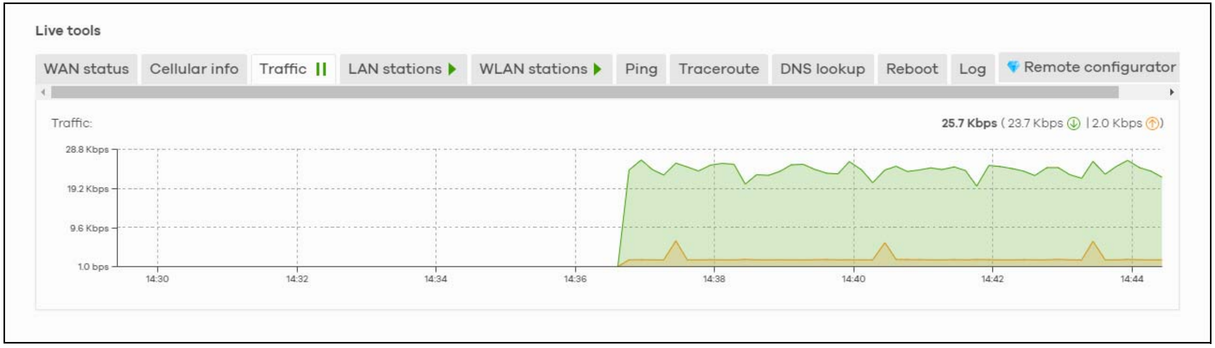
Table 148 Site-wide > Devices > Mobile router > Map/Photo

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 180 Site-wide > Devices > Mobile router > Live tools > Traffic (Example)



Live tools

Traffic: 25.7 Kbps (23.7 Kbps | 2.0 Kbps)

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.

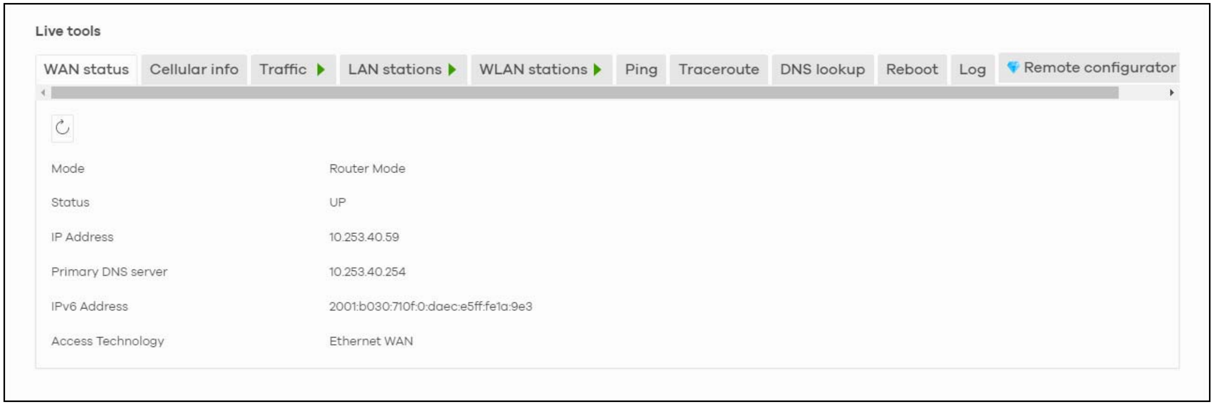
Table 149 Site-wide > Devices > Mobile router > Live tools

LABEL	DESCRIPTION
WAN Status	This shows the connection status of the Ethernet WAN interface. See Section 10.4.1 on page 480 for more information.
Cellular info	This shows the connection status of the cellular WAN interface. See Section 10.4.2 on page 481 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 488 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	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 181 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.

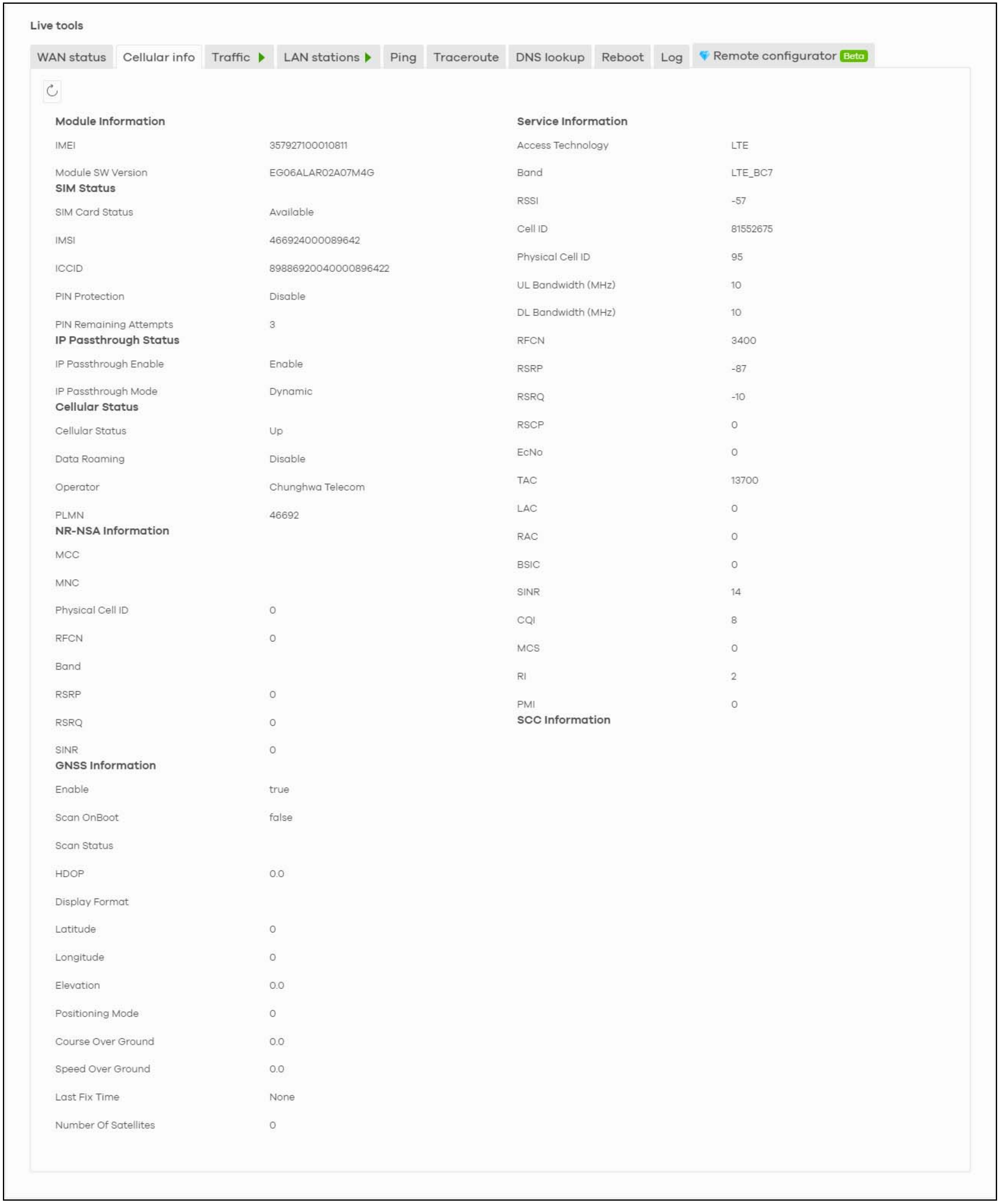
Table 150 Site-wide > Devices > Mobile router > Live tools > WAN status

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 182 Site-wide > Devices > Mobile router > Live tools > Cellular Info



Live tools

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 151 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 151 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 151 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 151 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 151 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.

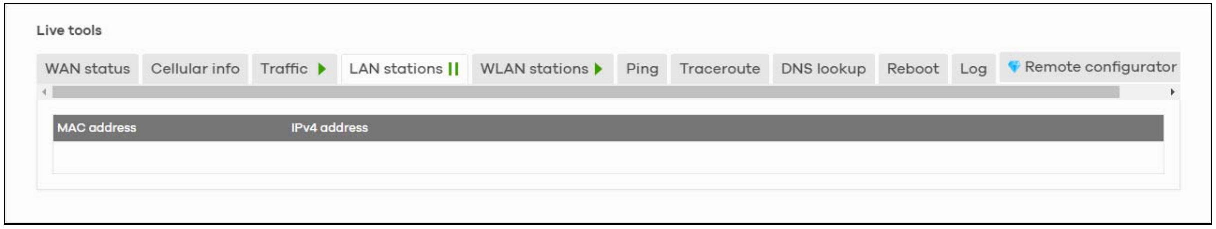
Table 151 Site-wide > Devices > Mobile router > Live tools > Cellular Info (continued)

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.
Longtitude	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 183 Site-wide > Devices > Mobile router > Live tools > LAN stations



The following table describes the labels in this screen.

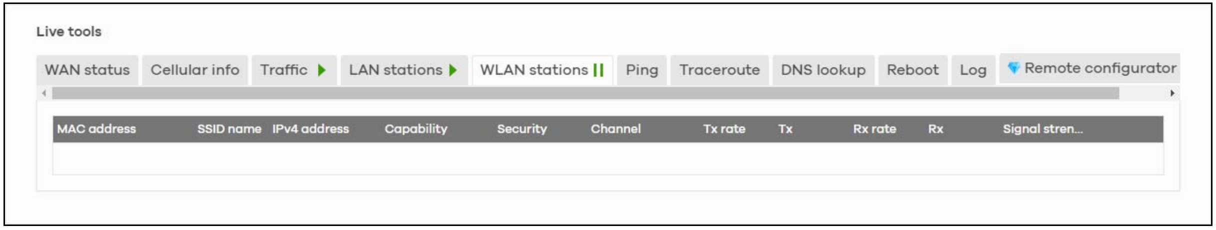
Table 152 Site-wide > Devices > Mobile router > Live tools > LAN stations

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 184 Site-wide > Devices > Mobile router > Live tools > WLAN stations



The following table describes the labels in this screen.

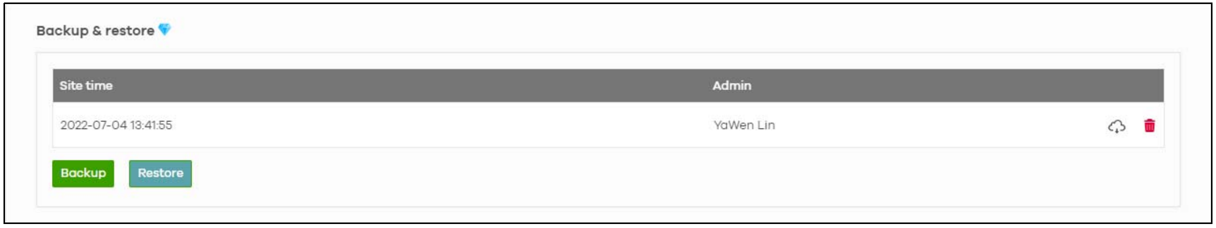
Table 153 Site-wide > Devices > Mobile router > Live tools > WLAN stations

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 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 185 Site-wide > Devices > Mobile router > Backup & restore



Backup & restore

Site time	Admin	
2022-07-04 13:41:55	YaWen Lin	☁ 🗑

Backup Restore

The following table describes the labels in this screen.

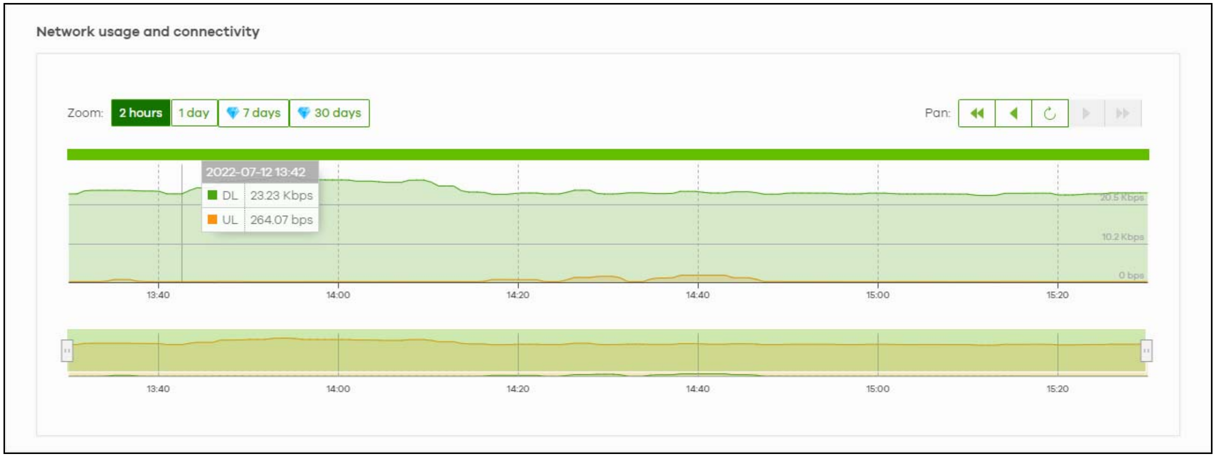
Table 154 Site-wide > Devices > Mobile router > Backup & restore

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.

10.6 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 186 Site-wide > Devices > Mobile router > Network usage and connectivity



The following table describes the labels in this screen.

Table 155 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.

PART III

Manage by Organization Deployment

CHAPTER 11
Organization-wide

11.1 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.

11.2 License & inventory

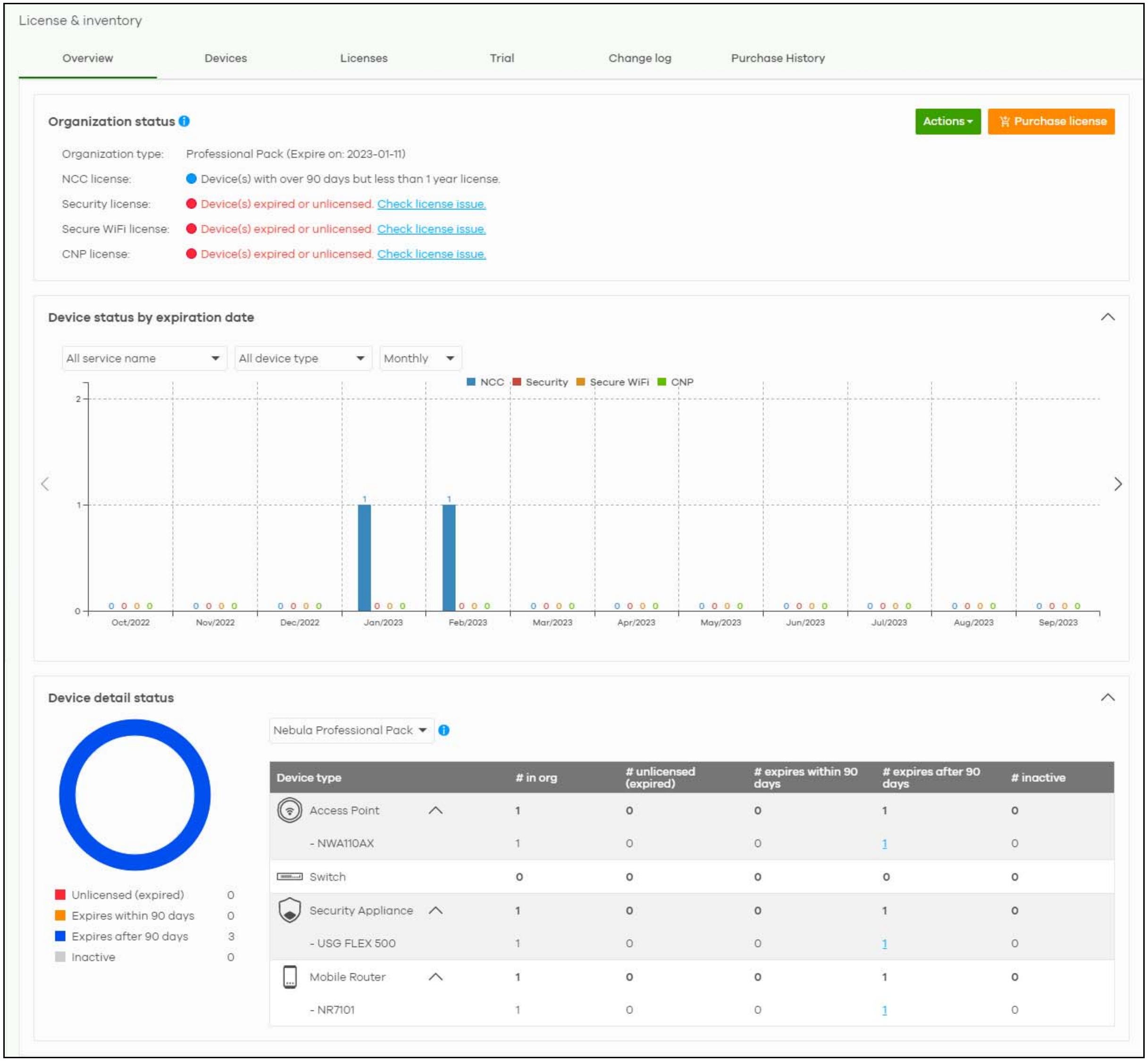
The following section describes license management screens in NCC.

Unused licenses can be transferred from a Nebula Device in an Organization to another Nebula Device in an Organization.

11.2.1 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 187 Organization-wide > License & inventory > Overview



License & inventory

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

Organization status

Actions ▾ | Purchase license

Organization type:	Professional Pack (Expire on: 2023-01-11)
NCC license:	● Device(s) with over 90 days but less than 1 year license.
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

All service name ▾ | All device type ▾ | Monthly ▾

Device detail status

🟥 Unlicensed (expired)	0
🟧 Expires within 90 days	0
🟦 Expires after 90 days	3
⬜ Inactive	0

Nebula Professional Pack ▾

Device type	# in org	# unlicensed (expired)	# expires within 90 days	# expires after 90 days	# inactive
Access Point	1	0	0	1	0
- NWA110AX	1	0	0	1	0
Switch	0	0	0	0	0
Security Appliance	1	0	0	1	0
- USG FLEX 500	1	0	0	1	0
Mobile Router	1	0	0	1	0
- NR7101	1	0	0	1	0

The following table describes the labels in this screen.

Table 156 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 11.2.2 on page 495. • **Add more licenses**: Add new licenses to the organization, by license key. For details, see Section 11.2.4 on page 496. • **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 11.2.5 on page 497.

Table 156 Organization-wide > License & inventory > Overview (continued)

LABEL	DESCRIPTION
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.
NSS/UTM 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.
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**, **Nebula Professional Pack**, **Nebula Plus Pack**, **Nebula Security Pack**, **UTM Security Pack**, or **Secure WiFi**: select the category of licenses to display. • **All device type**, **Access Point**, **Switch**, or **Security Gateway**: 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**, **Secure WiFi**, **Connect & Protect**).
Device type	This shows the category of Nebula Device (**Access points**, **Switches**, **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.
# near expiration in 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.

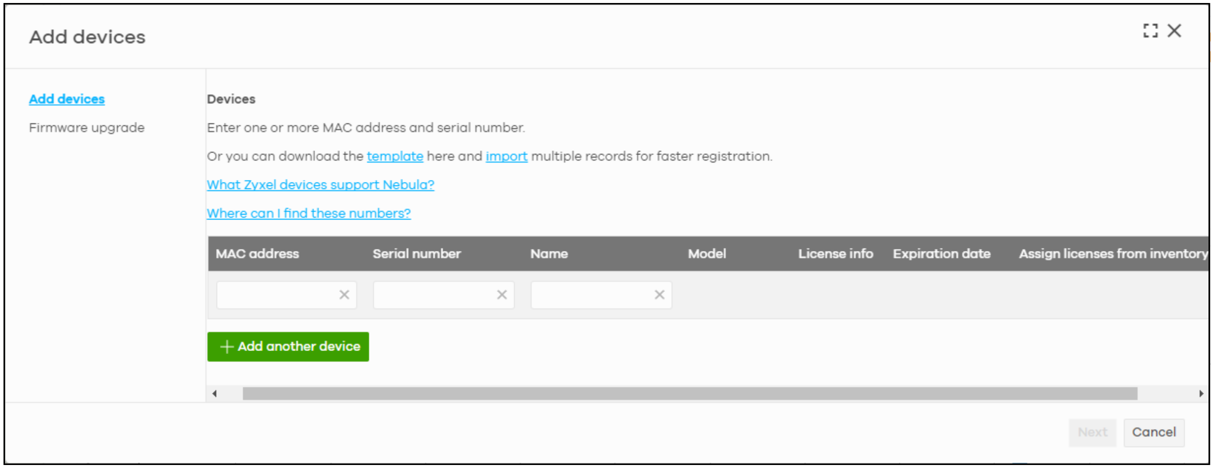
Table 156 Organization-wide > License & inventory > Overview (continued)

LABEL	DESCRIPTION
# expiration over 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.

11.2.2 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 188 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 157 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.
Expiration date	This shows the expiration date of the NCC license activated on the Nebula Device, if there is one.
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.

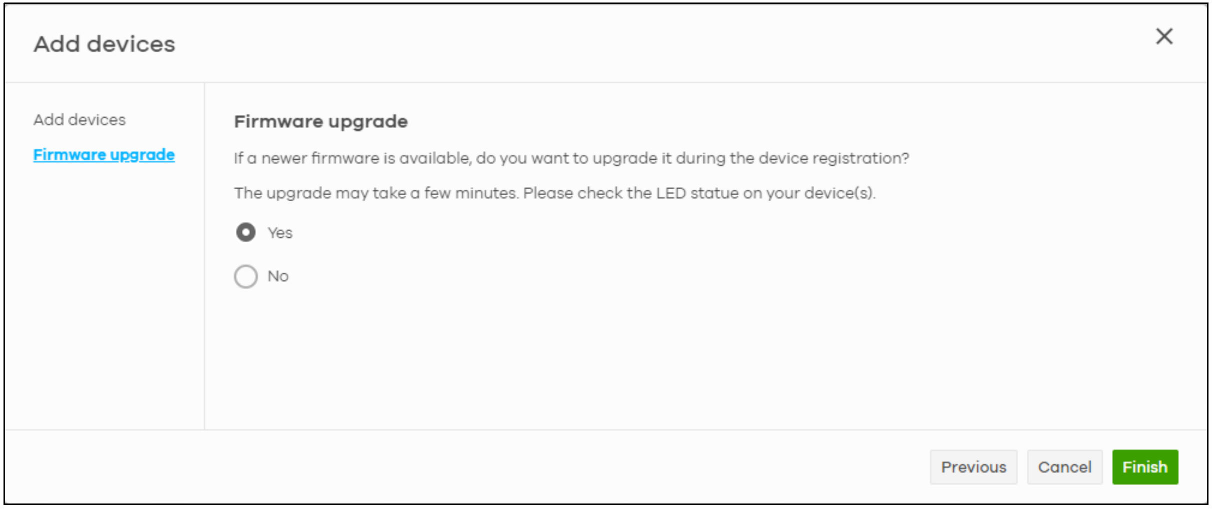
Table 157 Organization-wide > License & inventory > Overview: Add devices: Add devices (continued)

LABEL	DESCRIPTION
Acknowledge	Select this to confirm that your NCC account will be the owner of the new Nebula Devices.
Finish	Click this to add the Nebula Devices to the organization.
Cancel	Click this to close the screen without saving.

11.2.3 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 189 Organization-wide > License & inventory > Overview: Add devices: Firmware upgrade



Add devices

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

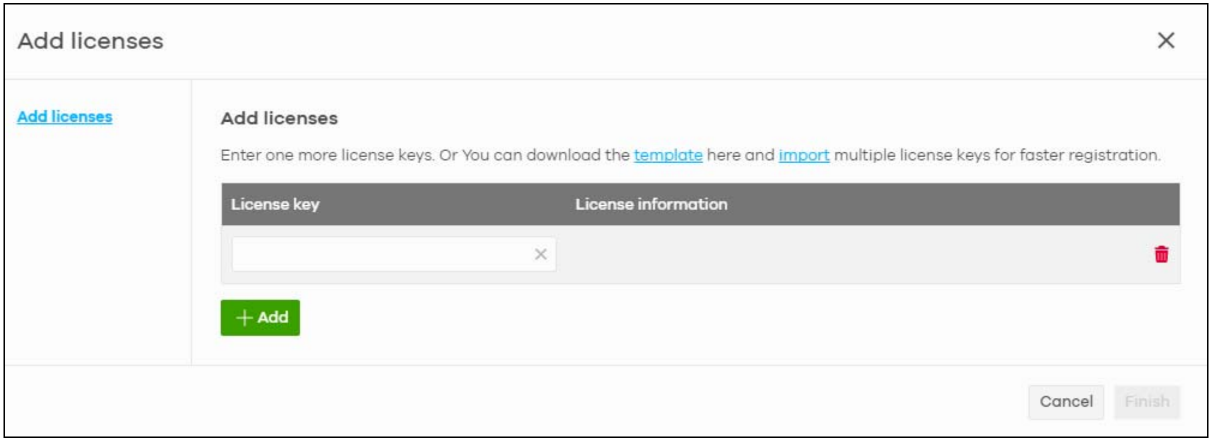
○ No

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.

11.2.4 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 190 Organization-wide > License & inventory > Overview: Add licenses



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.

The following table describes the labels in this screen.

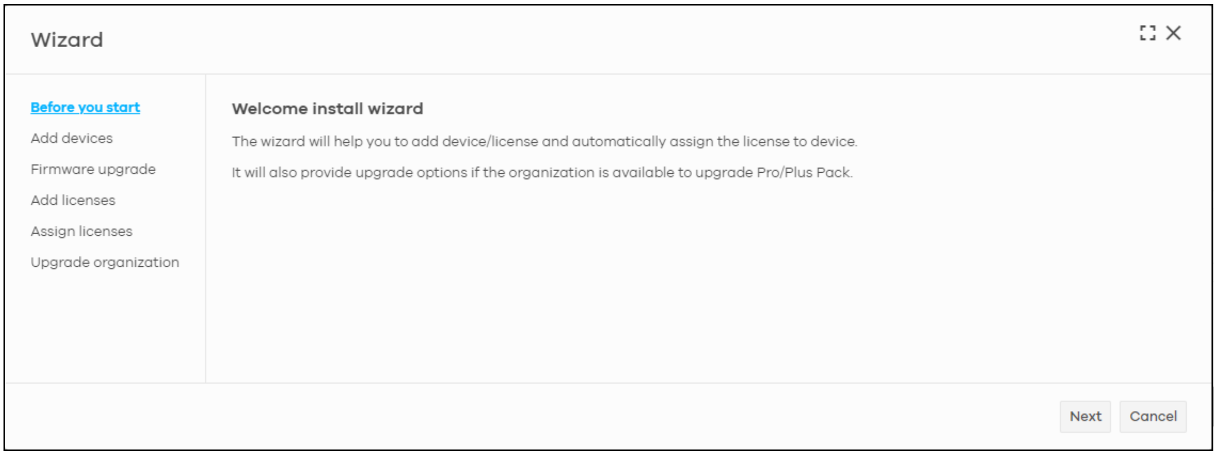
Table 158 Organization-wide > License & inventory > Overview: Add licenses

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.

11.2.5 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

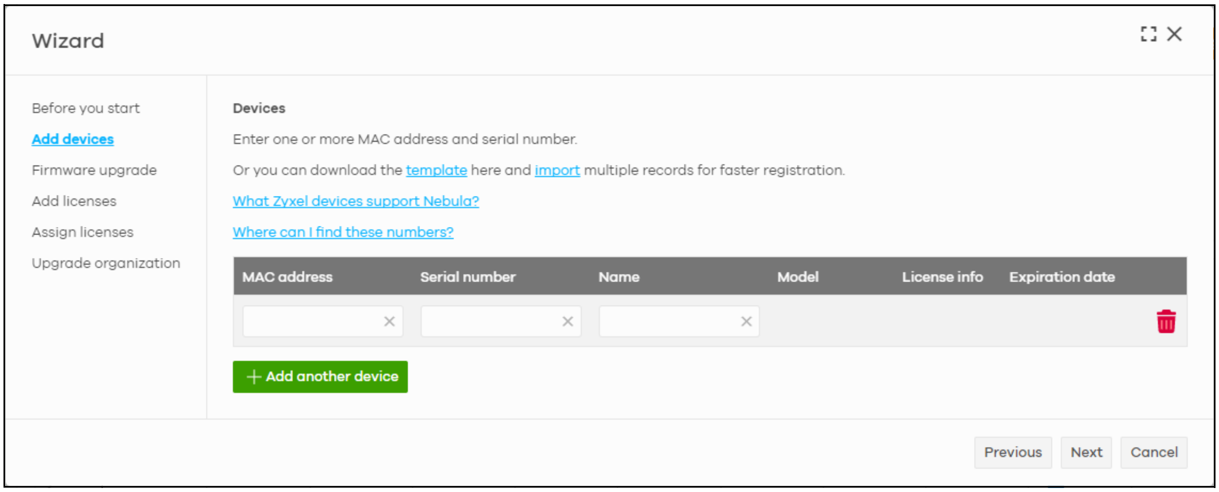
Before you start
Add devices
Firmware upgrade
Add licenses
Assign licenses
Upgrade organization

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 11.2.2 on page 495.



Wizard

Before you start
Add devices
Firmware upgrade
Add licenses
Assign licenses
Upgrade organization

Devices

Enter one or more MAC address and serial number.

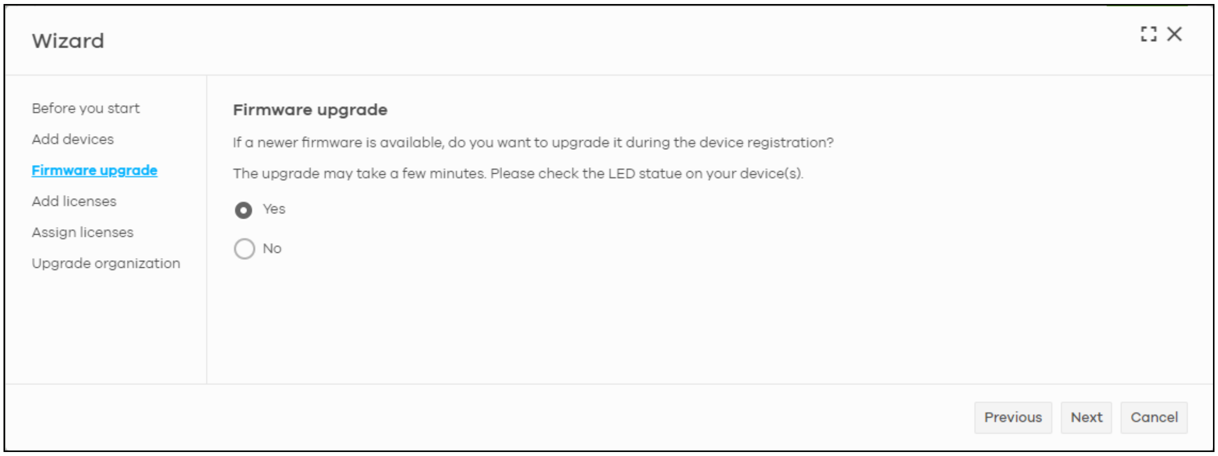
Or you can download the template here and import multiple records for faster registration.

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

Before you start
Add devices
Firmware upgrade
Add licenses
Assign licenses
Upgrade organization

Firmware upgrade

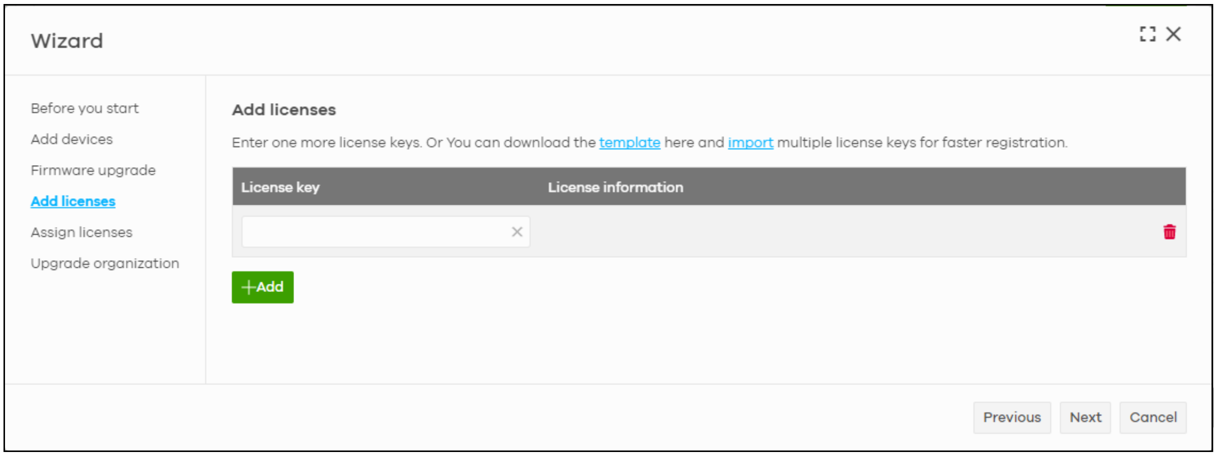
If a newer firmware is available, do you want to upgrade it during the device registration?

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 11.2.4 on page 496.



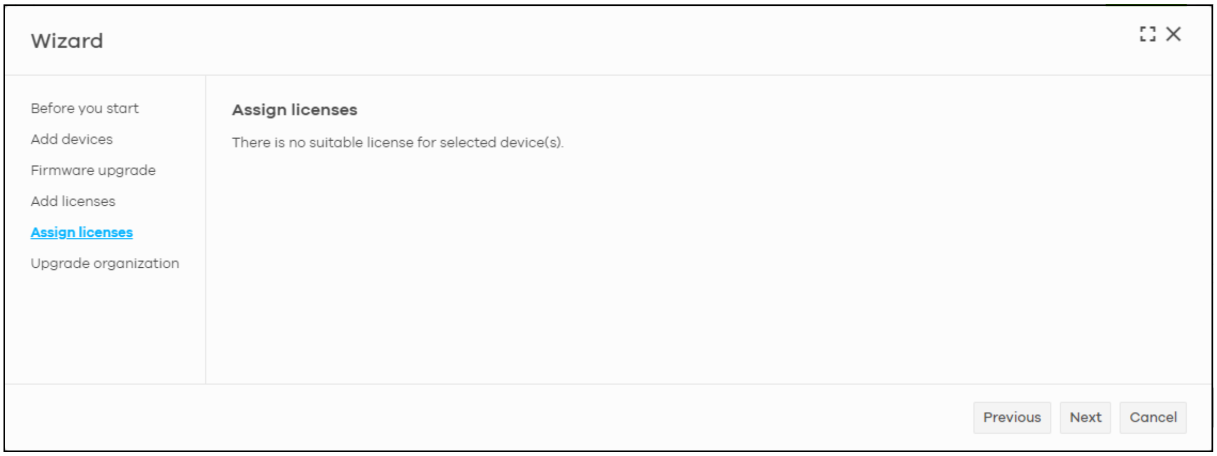
Wizard

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**.

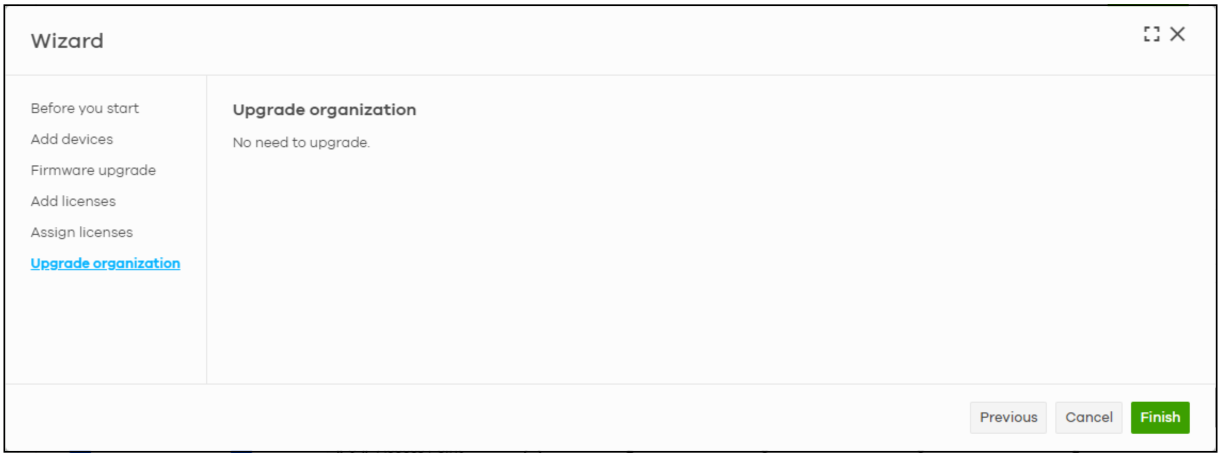


Wizard

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

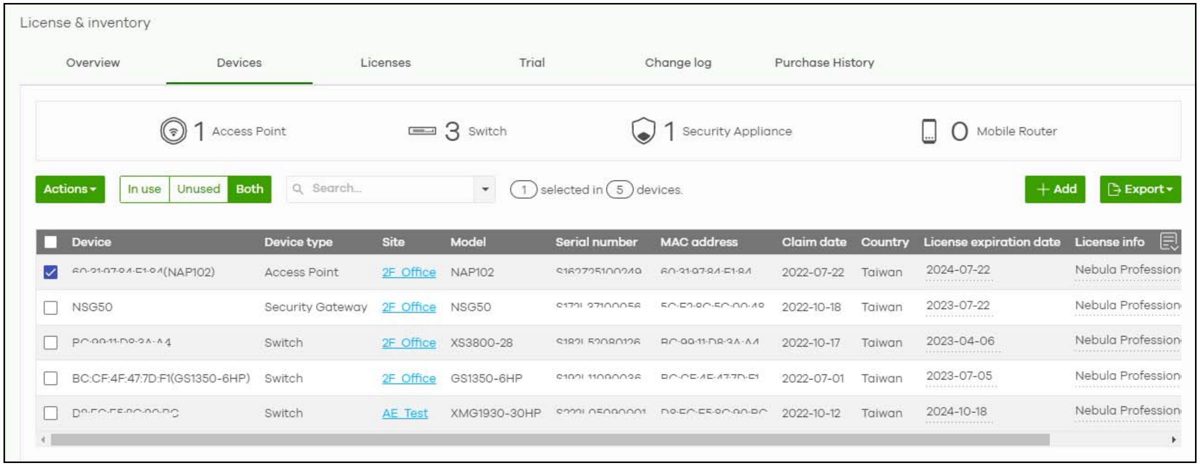
Upgrade organization

No need to upgrade.

11.2.6 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 191 Organization-wide > License & inventory > Devices



License & inventory

1 Access Point

3 Switch

1 Security Appliance

0 Mobile Router

1 selected in 5 devices.

☐	Device	Device type	Site	Model	Serial number	MAC address	Claim date	Country	License expiration date	License info
☑	60:31:97:84:E1:84(NAP102)	Access Point	2F_Office	NAP102	S162725100249	60:31:97:84:E1:84	2022-07-22	Taiwan	2024-07-22	Nebula Profession
☐	NSG50	Security Gateway	2F_Office	NSG50	S172L27100056	5C:E2:8C:5C:00:48	2022-10-18	Taiwan	2023-07-22	Nebula Profession
☐	BC:99:11:D8:3A:A4	Switch	2F_Office	XS3800-28	S182L52080126	BC:99:11:D8:3A:A4	2022-10-17	Taiwan	2023-04-06	Nebula Profession
☐	BC:CF:4F:47:7D:F1(GS1350-6HP)	Switch	2F_Office	GS1350-6HP	S192L11090036	BC:CF:4F:47:7D:F1	2022-07-01	Taiwan	2023-07-05	Nebula Profession
☐	D8:EC:E5:8C:90:BC	Switch	AE_Test	XMG1930-30HP	S222L05090001	D8:EC:E5:8C:90:BC	2022-10-12	Taiwan	2024-10-18	Nebula Profession

The following table describes the labels in this screen.

Table 159 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.

Table 159 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 13 for information on the supported Security Firewall devices), select the deployment method for management by Nebula (see Step 7: Set up the Deployment Method on page 51 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.
+ 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 11.2.2 on page 495.
Export	Click this button to save the Nebula Device list as a CSV or XML file to your computer.
	Select an entry's check box to select a specific Nebula Device. Otherwise, select the check box in the table heading row to select all Nebula Devices.
Device	This shows the hostname of the Nebula Device.
Device type	This shows the category of Nebula Device (**Access points**, **Switches**, **Security appliance**, **Firewall**, **Mobile router**) 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.

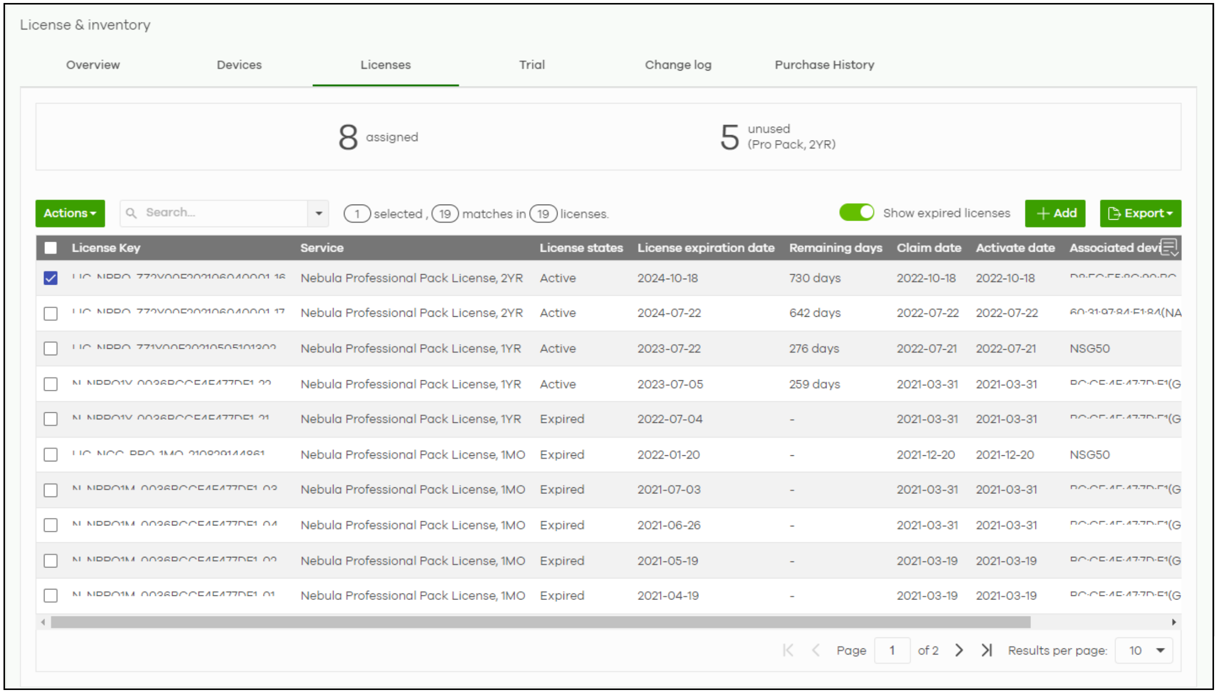
Table 159 Organization-wide > License & inventory > Devices (continued)

LABEL	DESCRIPTION
Claim 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 13 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.
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.
License 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 13 for information on the supported Security Firewall devices), select the deployment method for management by Nebula (see Step 7: Set up the Deployment Method on page 51 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.

11.2.7 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 192 Organization-wide > License & inventory > Licenses



License & inventory

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

8 assigned

5 unused (Pro Pack, 2YR)

Actions ▾ | Search... ▾ | 1 selected , 19 matches in 19 licenses. | Show expired licenses | + Add | Export ▾

□	License Key	Service	License states	License expiration date	Remaining days	Claim date	Activate date	Associated devi
☑	LIC-NPRO-772Y00E2021060400001-16	Nebula Professional Pack License, 2YR	Active	2024-10-18	730 days	2022-10-18	2022-10-18	D8:EC:E5:8C:00:BC
□	LIC-NPRO-772Y00E2021060400001-17	Nebula Professional Pack License, 2YR	Active	2024-07-22	642 days	2022-07-22	2022-07-22	60:31:97:84:E1:84(NA
□	LIC-NPRO-771Y00E20210505101302	Nebula Professional Pack License, 1YR	Active	2023-07-22	276 days	2022-07-21	2022-07-21	NSG50
□	N-NPRO1Y-0036BCCF4F477DE1-02	Nebula Professional Pack License, 1YR	Active	2023-07-05	259 days	2021-03-31	2021-03-31	BC:CF:4F:47:7D:E1(G
□	N-NPRO1Y-0036BCCF4F477DE1-01	Nebula Professional Pack License, 1YR	Expired	2022-07-04	-	2021-03-31	2021-03-31	BC:CF:4F:47:7D:E1(G
□	LIC-NCC-PRO-1MO-210829144861	Nebula Professional Pack License, 1MO	Expired	2022-01-20	-	2021-12-20	2021-12-20	NSG50
□	N-NPRO1M-0036BCCF4F477DE1-03	Nebula Professional Pack License, 1MO	Expired	2021-07-03	-	2021-03-31	2021-03-31	BC:CF:4F:47:7D:E1(G
□	N-NPRO1M-0036BCCF4F477DE1-04	Nebula Professional Pack License, 1MO	Expired	2021-06-26	-	2021-03-31	2021-03-31	BC:CF:4F:47:7D:E1(G
□	N-NPRO1M-0036BCCF4F477DE1-02	Nebula Professional Pack License, 1MO	Expired	2021-05-19	-	2021-03-19	2021-03-19	BC:CF:4F:47:7D:E1(G
□	N-NPRO1M-0036BCCF4F477DE1-01	Nebula Professional Pack License, 1MO	Expired	2021-04-19	-	2021-03-19	2021-03-19	BC:CF:4F:47:7D:E1(G

Page 1 of 2 | Results per page: 10

The following table describes the labels in this screen.

Table 160 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.

Table 160 Organization-wide > License & inventory > Licenses (continued)

LABEL	DESCRIPTION
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.
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 11.2.4 on page 496.
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: • **Active**: The license is assigned to a specific Nebula Device and activated. • **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.
License 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.
Claim 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.
Activate 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.

11.2.8 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 standard license during the trial period will cancel the trial. NCC activates inactive licenses when the associated trial has expired.

If you activate the Nebula Pro 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:

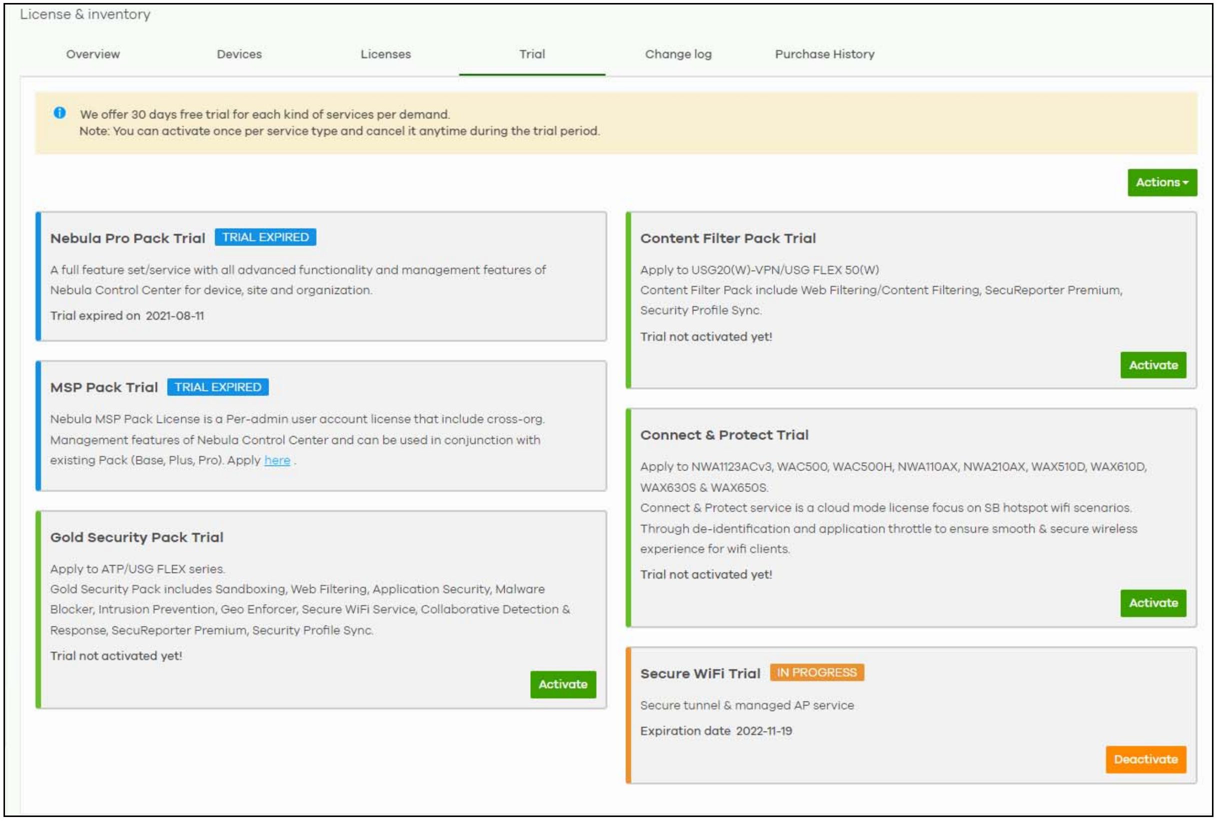
Table 161 Trial Licenses Summary

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 4.9.7 on page 229 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.
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.
Content Filter Pack Trial	This is for USG FLEX 50 /USG20-VPN / USG20W-VPN devices.
Connect & Protect (CNP) Trial	This allows you to manage small business WiFi hotspots using an NWA1123-ACv3, WAC500, WAC500H, NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, or WAX650S.

See Table 2 on page 16 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 193 Organization-wide > License & inventory > Trial



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

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

Trial not activated yet!

Content Filter Pack Trial

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

Trial not activated yet!

Connect & Protect Trial

Apply to NWA1123ACv3, WAC500, WAC500H, NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S & WAX650S.
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 not activated yet!

Secure WiFi Trial IN PROGRESS

Secure tunnel & managed AP service

Expiration date 2022-11-19

The following table describes the labels in this screen.

Table 162 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.
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.

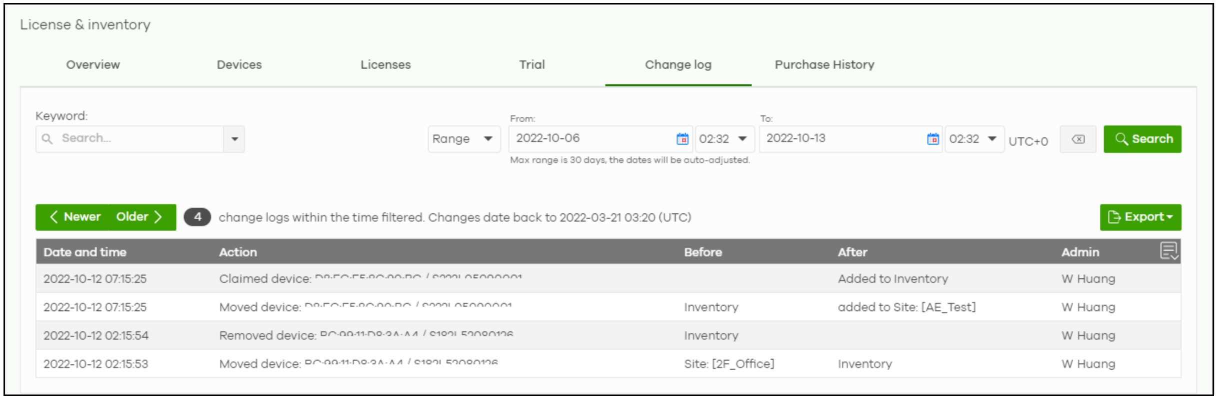
Table 162   Organization-wide > License & inventory > Trial (continued)

LABEL	DESCRIPTION
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.

11.2.9 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 194   Organization-wide > License & inventory > Change log



Keyword: Search...

Range From: 2022-10-06 02:32 To: 2022-10-13 02:32 UTC+0

Max range is 30 days, the dates will be auto-adjusted.

4 change logs within the time filtered. Changes date back to 2022-03-21 03:20 (UTC)

Date and time	Action	Before	After	Admin
2022-10-12 07:15:25	Claimed device: D8:EC:E5:8C:00:BC / S222L05000001		Added to Inventory	W Huang
2022-10-12 07:15:25	Moved device: D8:EC:E5:8C:00:BC / S222L05000001	Inventory	added to Site: [AE_Test]	W Huang
2022-10-12 02:15:54	Removed device: BC:99:11:D8:3A:A4 / S182L52080126	Inventory		W Huang
2022-10-12 02:15:53	Moved device: BC:99:11:D8:3A:A4 / S182L52080126	Site: [2F_Office]	Inventory	W Huang

The following table describes the labels in this screen.

Table 163   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".
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.

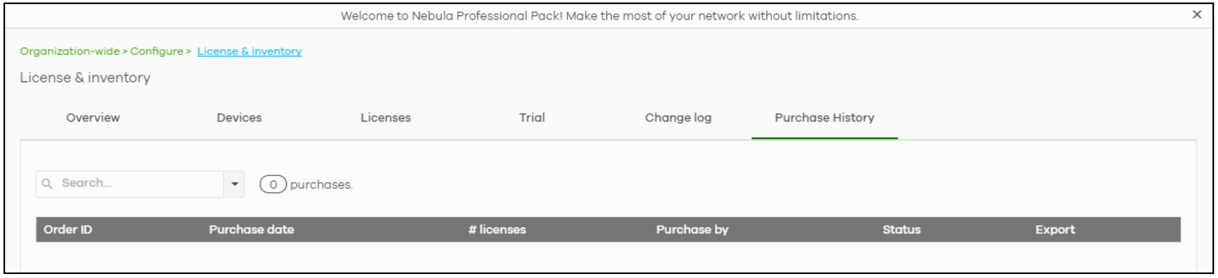
Table 163 Organization-wide > License & inventory > Change log (continued)

LABEL	DESCRIPTION
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.

11.2.10 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 195 Organization-wide > License & inventory > Purchase history



Welcome to Nebula Professional Pack! Make the most of your network without limitations. ×

Organization-wide > Configure > License & inventory

License & inventory

Overview Devices Licenses Trial Change log Purchase History

Search... 0 purchases.

Order ID	Purchase date	# licenses	Purchase by	Status	Export

The following table describes the labels in this screen.

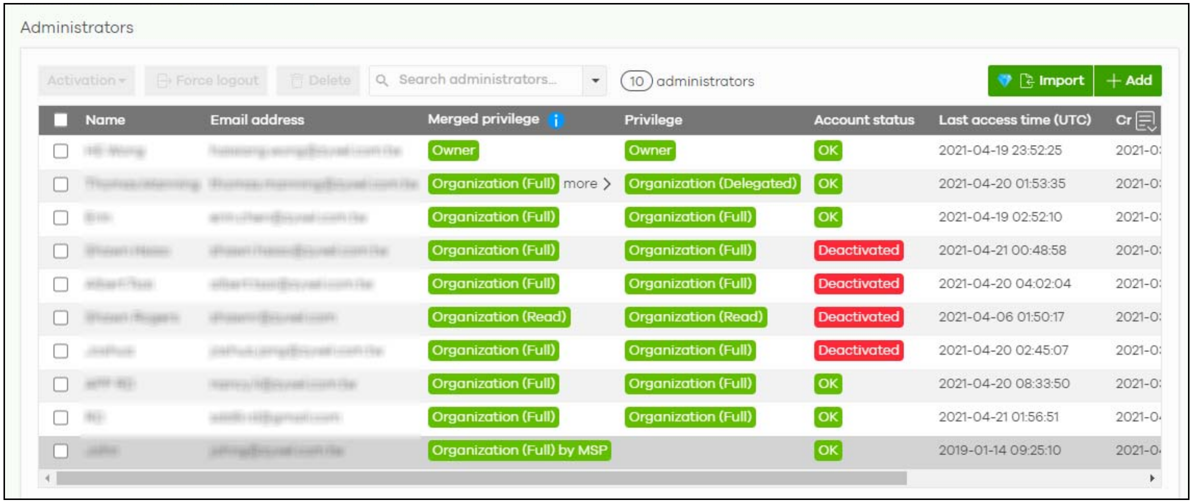
Table 164 Organization-wide > License & inventory > Purchase history

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.

11.3 Administrators

Use this screen to view, manage and create administrator accounts for the specified organization. Click **Organization-wide** > **Administrators** to access this screen.

Figure 196 Organization-wide > Administrators



Administrators

10 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 165 Organization-wide > Administrators

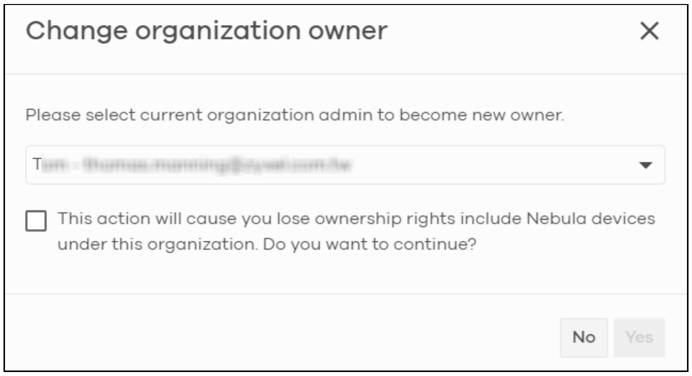
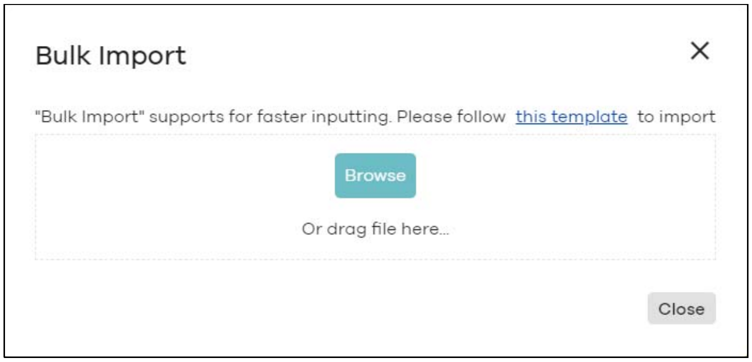
LABEL	DESCRIPTION
Activation	Click this button to **Activate**/**Deactivate** the selected accounts. Then click **Update**.
Force logout	Click this button to force the selected accounts to log out of the NCC.
Delete	Click this button to remove the selected accounts.
Search	Specify your desired filter criteria to filter the list of administrator accounts.
administrators	This shows the number of administrator accounts in the list.
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? No Yes 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.

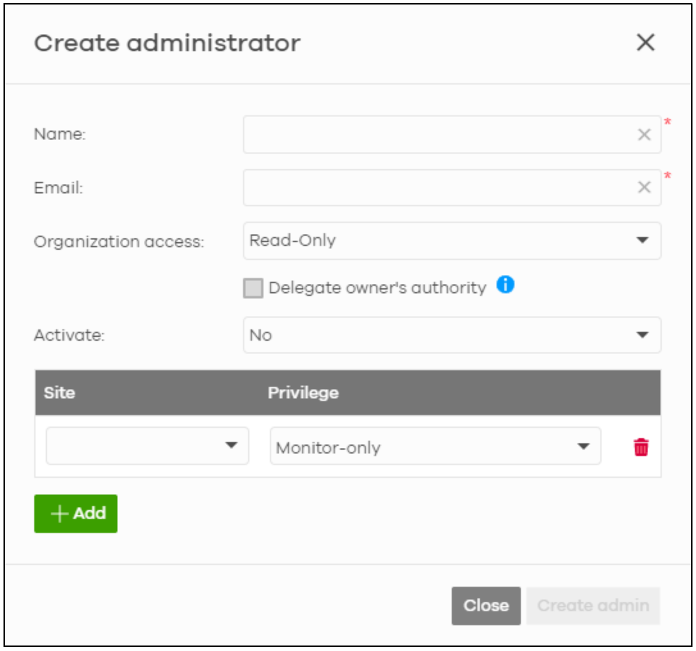
Table 165 Organization-wide > Administrators (continued)

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.  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 administrator account. See Section 11.3.0.1 on page 510.
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 13.5.1 on page 581.
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).
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.

11.3.0.1 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 197 Organization-wide > Administrator: Create/Update administrator



Create administrator

Name: *

Email: *

Organization access: Read-Only

□ Delegate owner's authority

Activate: No

Site	Privilege
	Monitor-only

The following table describes the labels in this screen.

Table 166 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.
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.
Activate	Select **Yes** to enable the account or **No** to temporarily disable the account.

Table 166 Organization-wide > Administrator: Create/Update administrator (continued)

LABEL	DESCRIPTION
YES, I want to do it.	The check box displays only when an administrator that has full access to the organization selects **No** in the **Activate** field to disable his/her own account. Note: After you select the check box 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 555). **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.

11.4 Organization-wide Manage

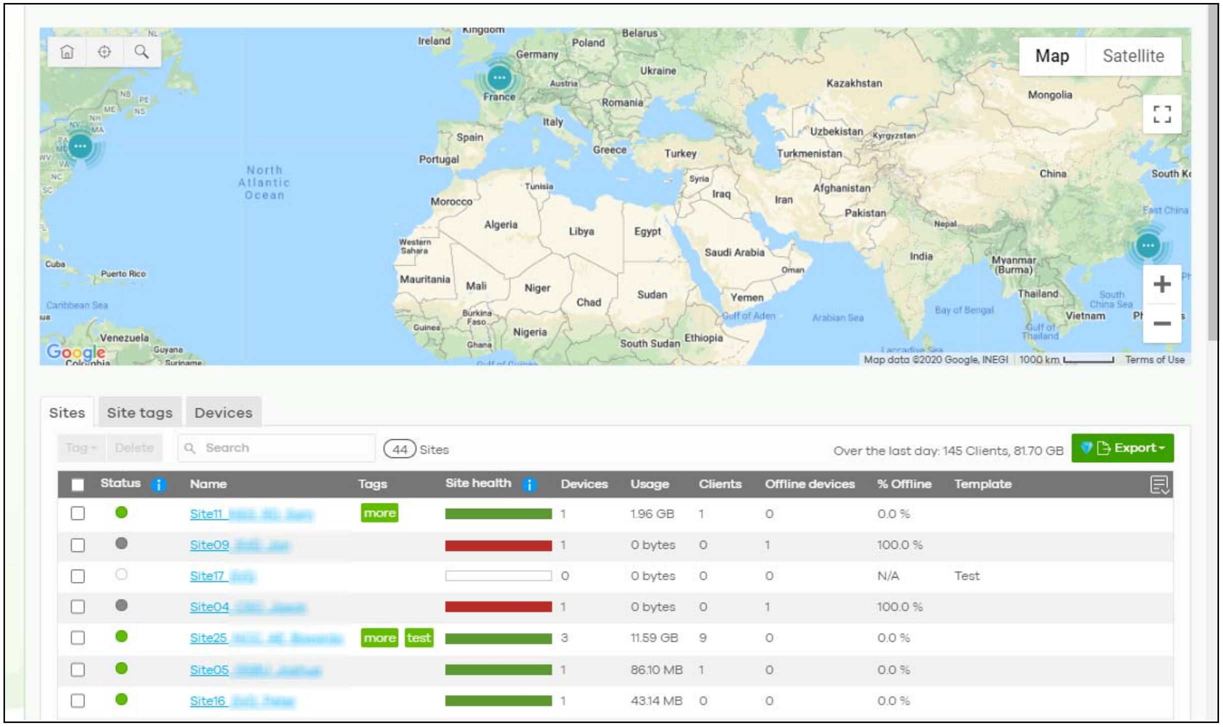
Use the **Organization-wide manage** menus to create new sites, register or unregister a Nebula Device, change organization general settings, and manage licenses, user accounts, administrator accounts or VPN members in the organization.

11.4.1 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.

Click **Organization-wide** > **Organization-wide manage** > **Organization portal** to access this screen.

Figure 198 Organization-wide > Organization-wide manage > Organization portal



Sites | Site tags | Devices

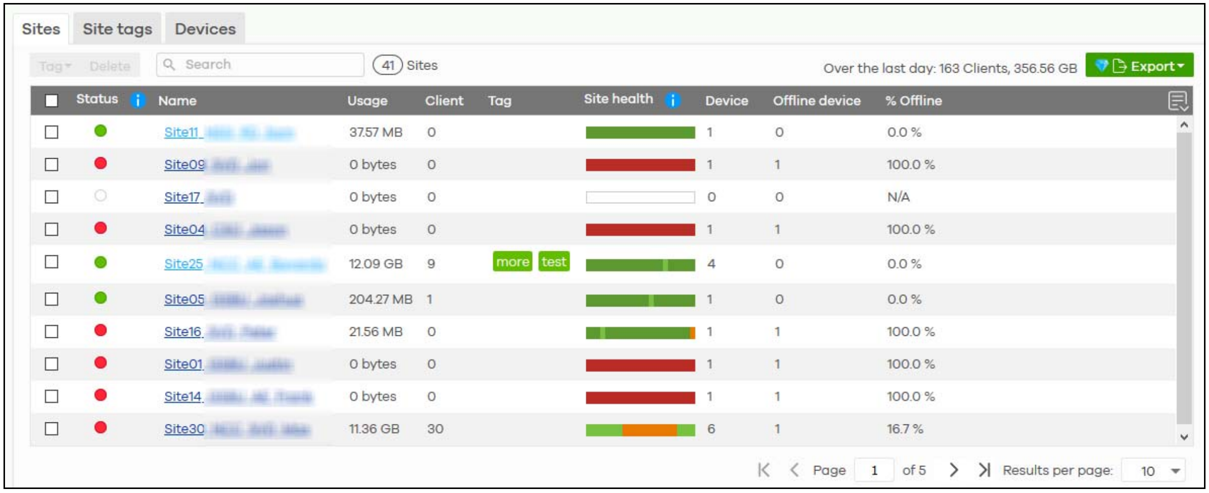
Tag ▾ | Delete | Search | (44) Sites | Over the last day: 145 Clients, 81.70 GB | Export ▾

☐	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 %	

11.4.1.1 Sites

Click the **Sites** tab in the **Overview** screen to view detailed information of the sites which are associated with the selected organization.

Figure 199 Organization-wide > Organization-wide manage > Organization portal: Sites



Sites | Site tags | Devices

Tag ▾ | Delete | Search | (41) Sites | Over the last day: 163 Clients, 356.56 GB | Export ▾

☐	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 167 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.

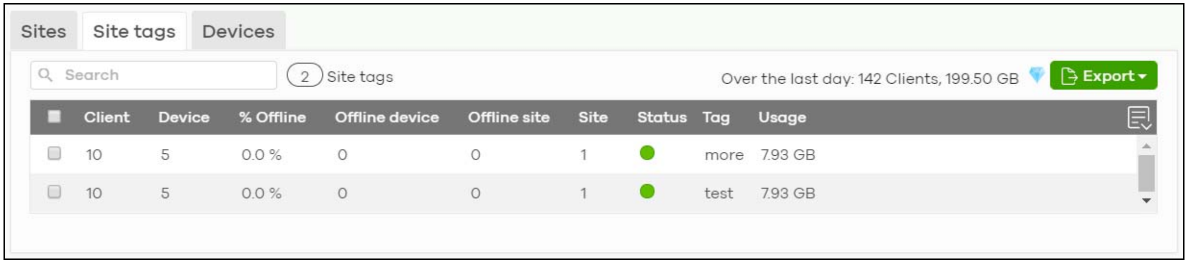
Table 167 Organization-wide > Organization-wide manage > Organization portal: Sites (continued)

LABEL	DESCRIPTION
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.
Client	This shows the number of clients connected to Nebula Devices in the site.
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.
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.

11.4.1.2 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 200 Organization-wide > Organization-wide manage > Organization portal: Site tags



■	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.

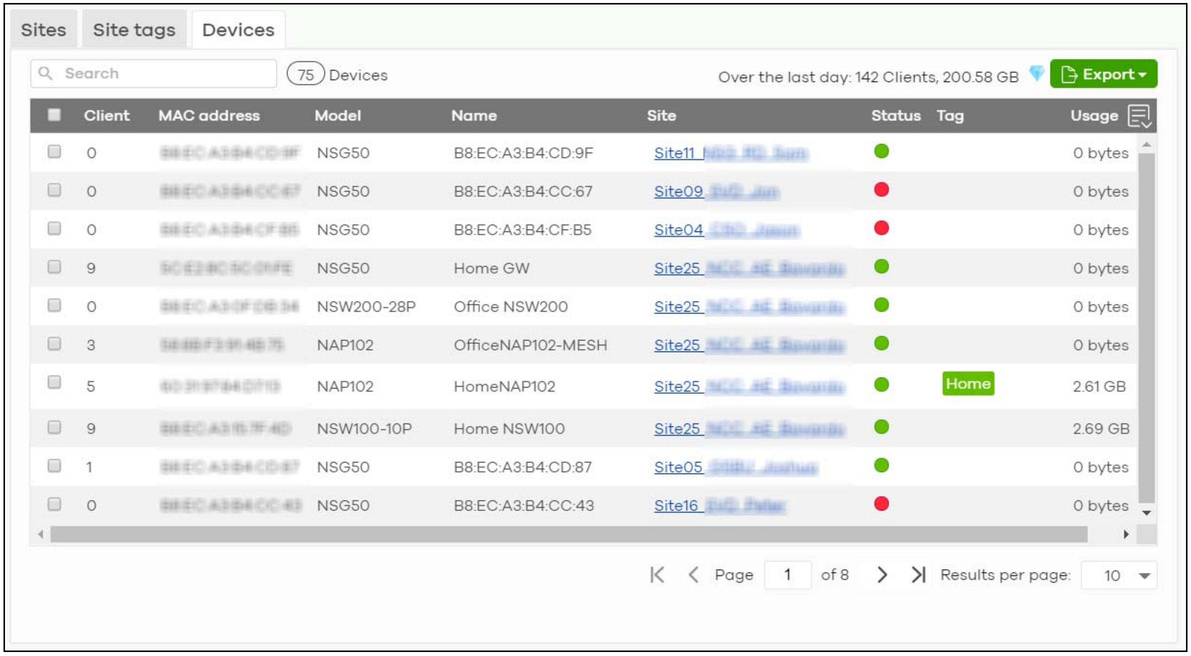
Table 168   Organization-wide > Organization-wide manage > Organization portal: Site tags

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.
Client	This shows the number of clients in sites with the specified tag.
Usage	This shows the total amount of data consumed in all sites with the specified tag.
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.

11.4.1.3 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 201 Organization-wide > Organization-wide manage > Organization portal: Devices



Sites | Site tags | Devices

Search | 75 Devices | Over the last day: 142 Clients, 200.58 GB | Export

□	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 169 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.
Client	This shows the number of the clients which are currently connected to the Nebula Device.
Usage	This shows the amount of data consumed by 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 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.

Table 169 Organization-wide > Organization-wide manage > Organization portal: Devices (continued)

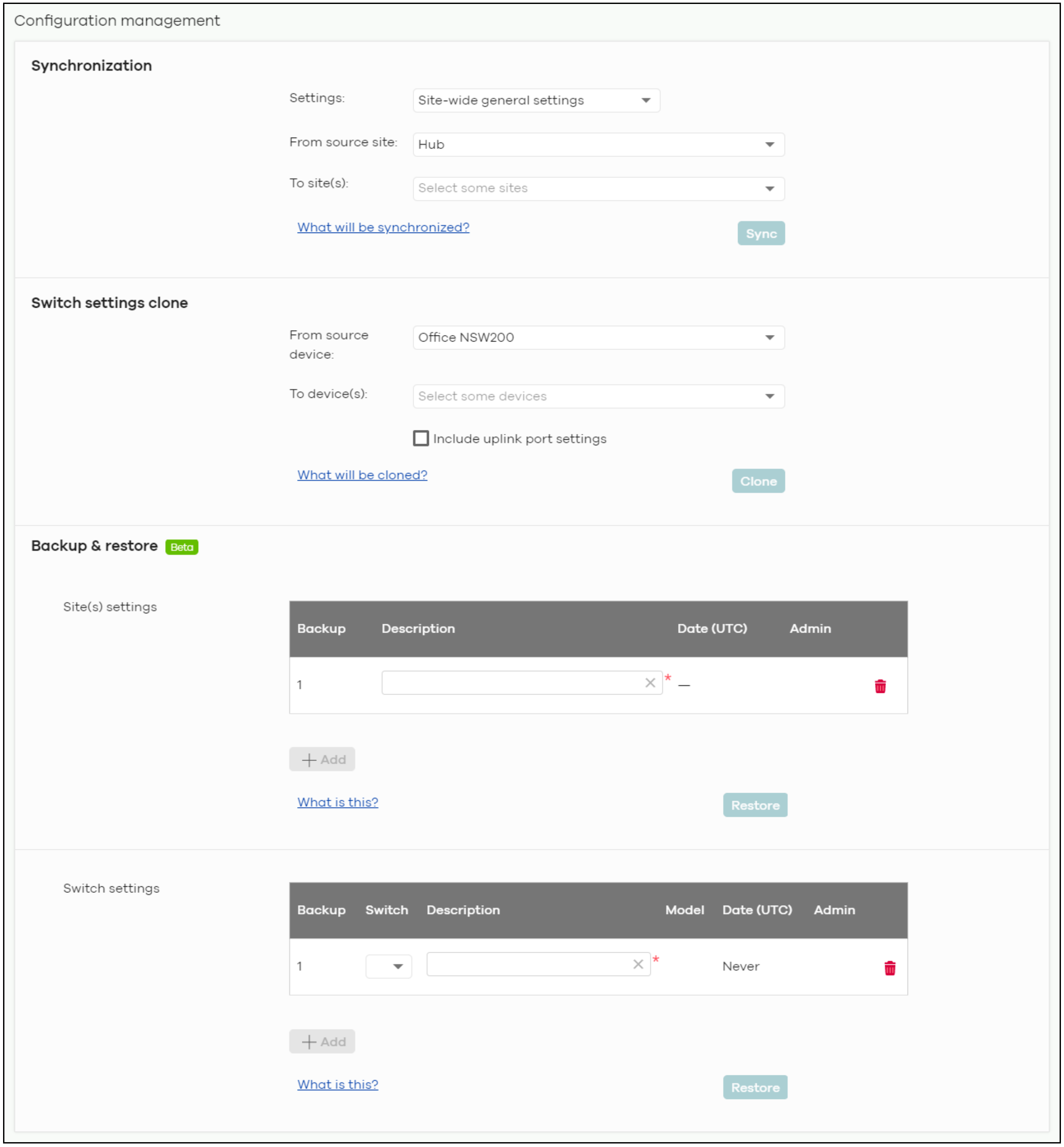
LABEL	DESCRIPTION
Public IP	This shows the global (WAN) IP address of the Nebula Device.
☰	Click this icon to display a greater or lesser number of configuration fields.

11.4.2 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 202 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

What will be synchronized?

Switch settings clone

From source device: Office NSW200

To device(s): Select some devices

□ Include uplink port settings

What will be cloned?

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 170 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 170 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.	
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.
Restore from backup	Select the backup you want to restore.

Table 170   Organization-wide > Organization-wide manage > Configuration management (continued)

LABEL	DESCRIPTION
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.

11.4.3 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 11.4.3.3 on page 522).

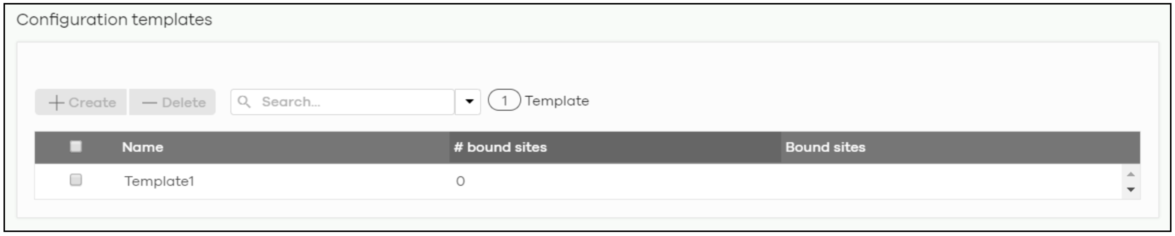
Use this screen to create and manage configuration templates. You can then bind or unbind a site from the template (see Section 11.4.3.1 on page 521).

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.

Click **Organization-wide** > **Organization-wide manage** > **Configuration templates** to access this screen.

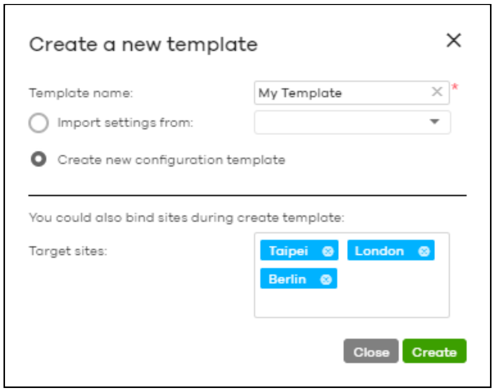
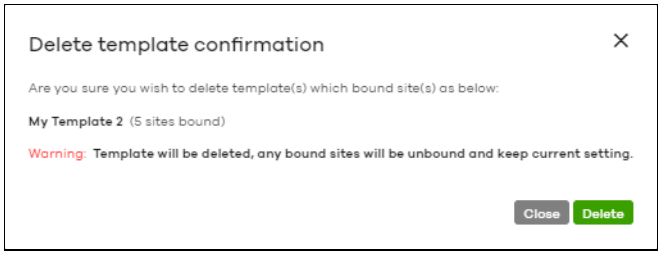
Figure 203   Organization-wide > Organization-wide manage > Configuration templates



□	Name	# bound sites	Bound sites
□	Template1	0	

The following table describes the labels in this screen.

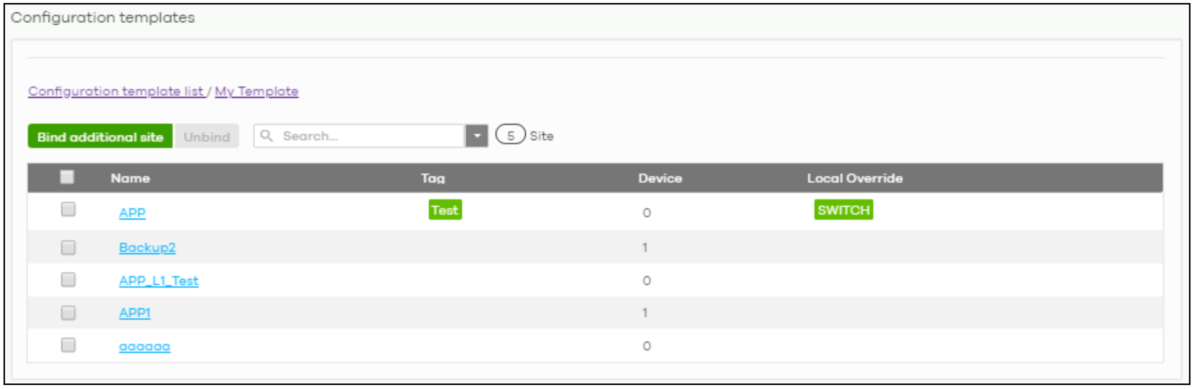
Table 171 Organization-wide > Organization-wide manage > Configuration templates

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 ⊗ Close Create
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. Close Delete
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.

11.4.3.1 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 204 Organization-wide > Organization-wide manage > Configuration templates: Template



Configuration templates

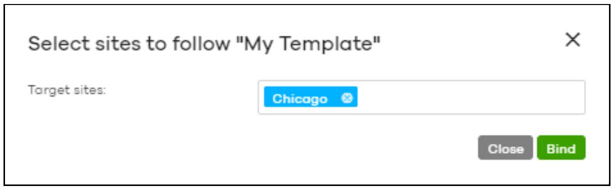
Configuration template list / My Template

Bind additional site | Unbind | Search... | 5 Site

☐	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 172 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.

11.4.3.2 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.

11.4.3.3 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 check box 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 check box is not selected, any changes of the same configuration screen in the template apply to the site.

11.4.3.4 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 291 for details.) after the Switch is bound to a profile, turn on the local override function (see Section 11.4.3.3 on page 522).

11.4.4 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.

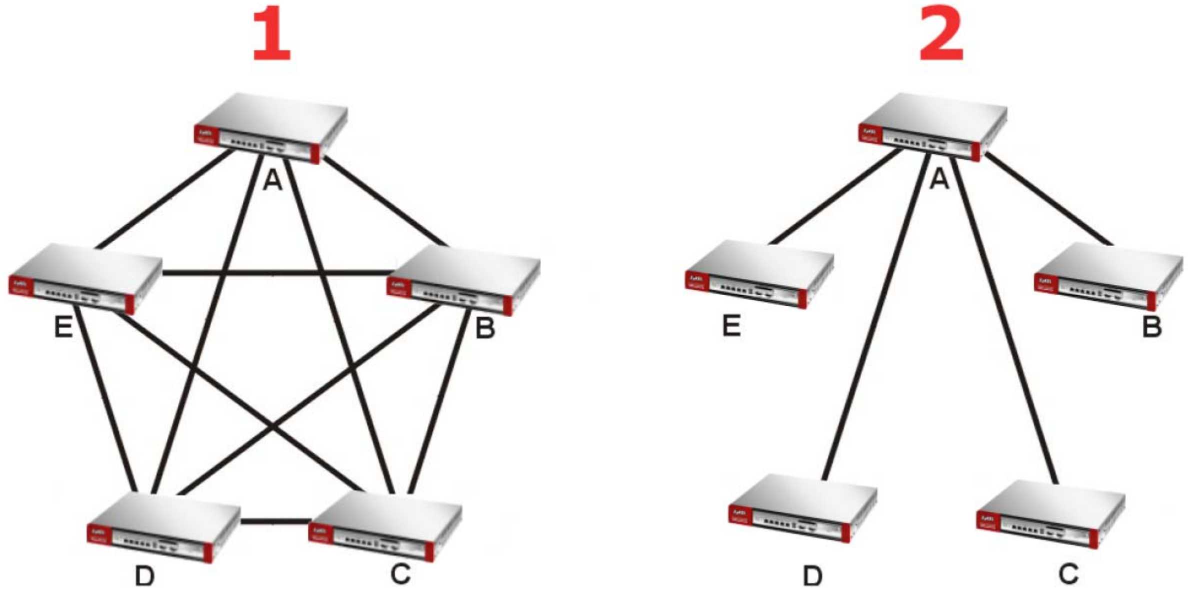
Note: You can manually create VPN connections between sites at **Site-wide** > **Configure** > **Security Gateway** > **Site-to-Site VPN** or **Site-wide** > **Configure** > **Firewall** > **Site-to-Site VPN**.

11.4.4.1 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 205 VPN Topologies (Fully Meshed and Hub-and-Spoke)



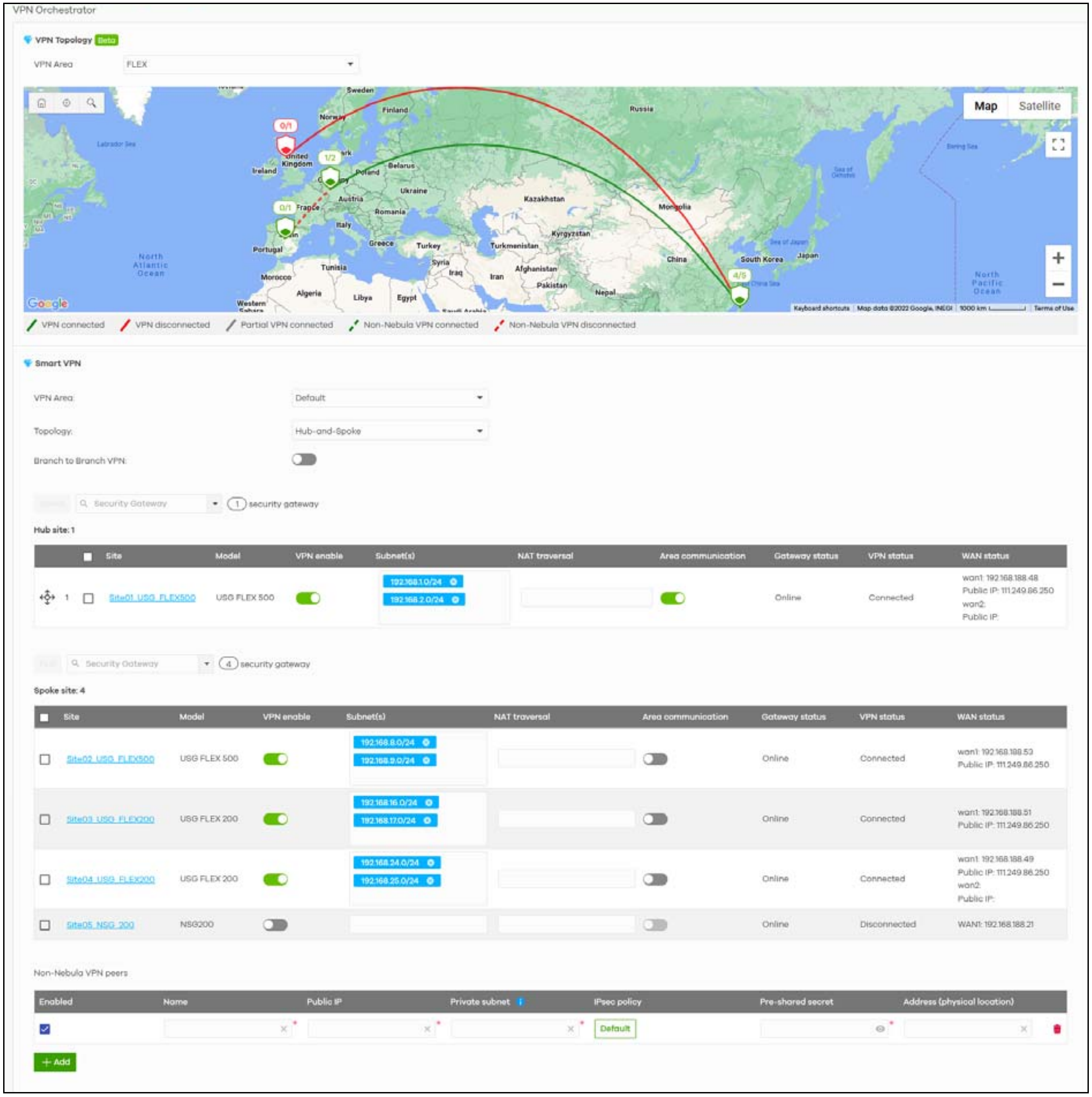
11.4.4.2 VPN Areas

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.

11.4.4.3 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.

Figure 206 Organization-wide > Organization-wide manage > VPN orchestrator



VPN Area: FLEX

/ VPN connected / VPN disconnected / Partial VPN connected / Non-Nebula VPN connected / Non-Nebula VPN disconnected

VPN Area: Default

Topology: Hub-and-Spoke

Branch to Branch VPN: ○

Security Gateway (1) security gateway

Hub site: 1

	□	Site	Model	VPN enable	Subnet(s)	NAT traversal	Area communication	Gateway status	VPN status	WAN status
1	□	Site01_USG_FLEX500	USG FLEX 500	●	192.168.1.0/24 192.168.2.0/24		●	Online	Connected	wan1: 192.168.188.48 Public IP: 111.249.86.250 wan2: Public IP:

Security Gateway (4) security gateway

Spoke site: 4

□	Site	Model	VPN enable	Subnet(s)	NAT traversal	Area communication	Gateway status	VPN status	WAN status
□	Site02_USG_FLEX500	USG FLEX 500	●	192.168.8.0/24 192.168.9.0/24		○	Online	Connected	wan1: 192.168.188.53 Public IP: 111.249.86.250
□	Site03_USG_FLEX200	USG FLEX 200	●	192.168.16.0/24 192.168.17.0/24		○	Online	Connected	wan1: 192.168.188.51 Public IP: 111.249.86.250
□	Site04_USG_FLEX200	USG FLEX 200	●	192.168.24.0/24 192.168.25.0/24		○	Online	Connected	wan1: 192.168.188.49 Public IP: 111.249.86.250 wan2: Public IP:
□	Site05_NSG_200	NSG200	○			○	Online	Disconnected	WAN1: 192.168.188.21

Non-Nebula VPN peers

Enabled	Name	Public IP	Private subnet	IPsec policy	Pre-shared secret	Address (physical location)
☑				Default		

The following table describes the labels in this screen.

Table 173 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.
Smart VPN	
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.

Table 173 Organization-wide > Organization-wide manage > VPN orchestrator (continued)

LABEL	DESCRIPTION
Topology	Click this to select a topology for the VPN area. For details on topologies, see Section 11.4.4.1 on page 523. 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.
Model	This shows the model of the site's Security Gateway device.
VPN enable	Click this to enable or disable site-to-site VPN on the site's Security Gateway. 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 Gateway.
NAT traversal	If the Security Gateway is behind a NAT router, enter the public IP address or the domain name that is configured and mapped to the Security Gateway 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 Gateway 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 Gateway.
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 check box 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 452 for detailed information.

Table 173 Organization-wide > Organization-wide manage > VPN orchestrator (continued)

LABEL	DESCRIPTION
Preshared secret	Enter a pre-shared key (password). The Nebula Security Gateway and peer gateway use the key to identify each other when they negotiate the IKE SA.
Address	Enter the address (physical location) of the Nebula Device.
🗑	Click the remove icon to delete the entry.

11.4.5 Security Profile Sync

Security profile sync allows you to share the same Security Firewall gateway 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**.

11.4.5.1 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 gateway device.

2. Configure security service settings for **Content filtering**, **Application Patrol**, **URL Threat Filter**, **Anti-Malware**, and **Intrusion Detection / Prevention**. Then click **Save**.
   All security settings are synced to the selected sites.

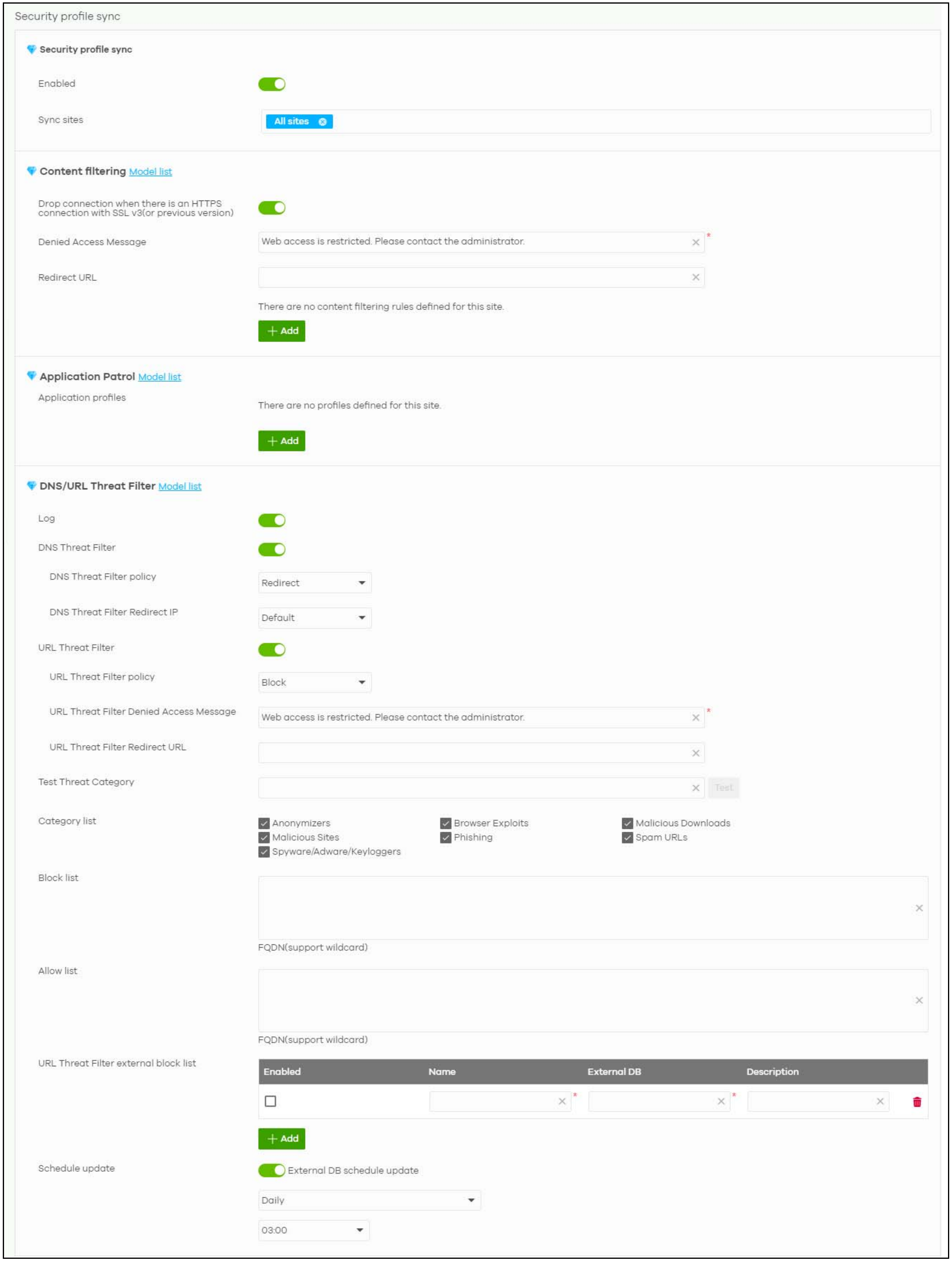
3. If you change the settings in the **Security profile sync** screen, the changes will be copied to all selected sites.

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**.

11.4.5.2 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 207 Organization-wide > Organization-wide manage > Security Profile Sync



Security profile sync

Security profile sync

Enabled	●
Sync sites	All sites ⊗

Content filtering 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	×

There are no content filtering rules defined for this site.

+ Add

Application Patrol Model list

Application profiles

There are no profiles defined for this site.

+ 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)

URL Threat Filter external block list

Enabled	Name	External DB	Description
□	× *	× *	×

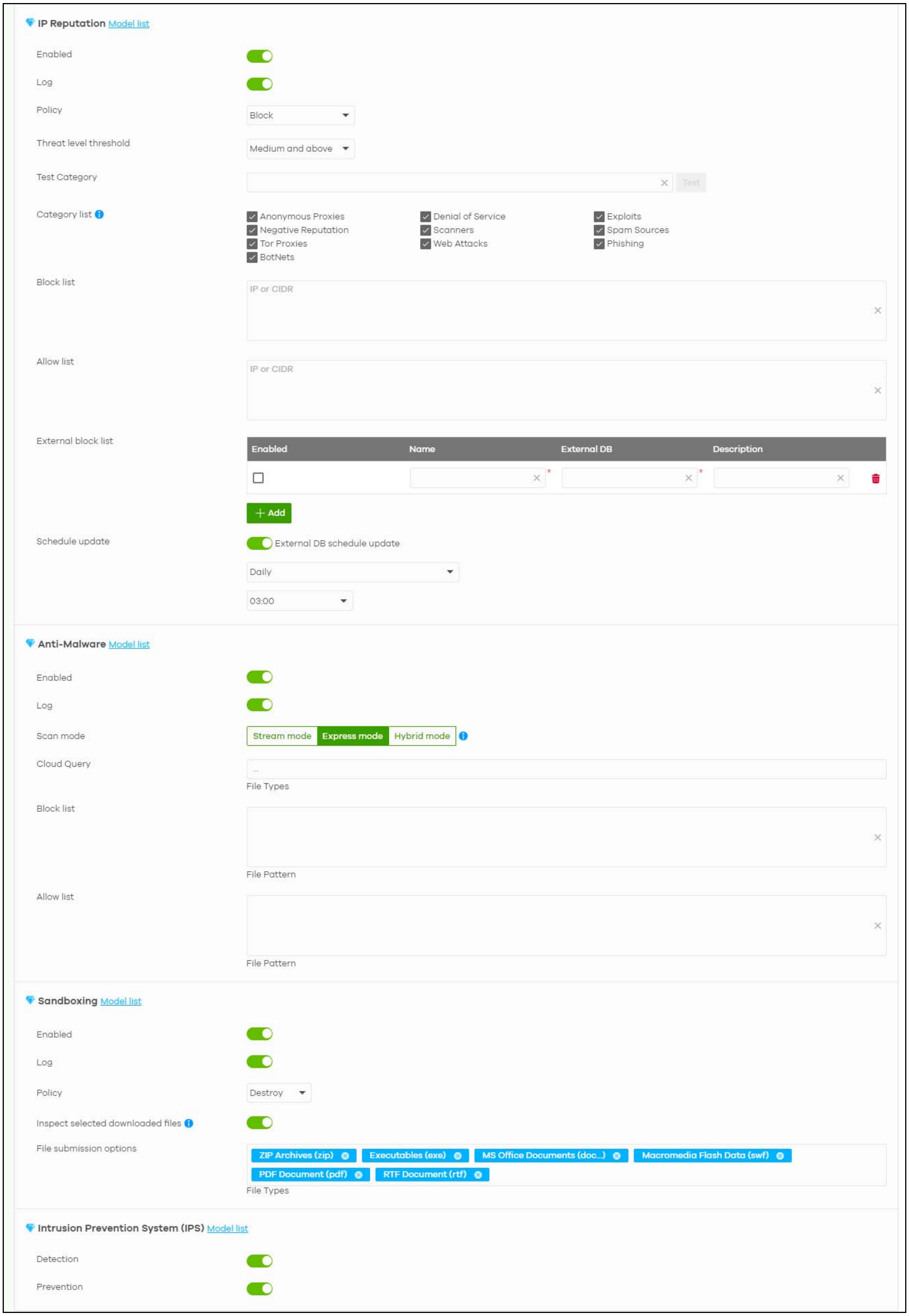
+ Add

Schedule update

● External DB schedule update

Daily

03:00



IP Reputation Model list

Enabled

Log

Policy: Block

Threat level threshold: Medium and above

Test Category

Category list

☑ Anonymous Proxies
☑ Negative Reputation
☑ Tor Proxies
☑ BotNets
☑ Denial of Service
☑ Scanners
☑ Web Attacks
☑ Exploits
☑ Spam Sources
☑ Phishing

Block list: IP or CIDR

Allow list: IP or CIDR

External block list

Enabled	Name	External DB	Description
□			

Schedule update: External DB schedule update

Daily

03:00

Anti-Malware Model list

Enabled

Log

Scan mode: Stream mode | Express mode | Hybrid mode

Cloud Query

File Types

Block list

File Pattern

Allow list

File Pattern

Sandboxing Model list

Enabled

Log

Policy: Destroy

Inspect selected downloaded files

File submission options: ZIP Archives (zip), Executables (exe), MS Office Documents (doc...), Macromedia Flash Data (swf), PDF Document (pdf), RTF Document (rtf)

File Types

Intrusion Prevention System (IPS) Model list

Detection

Prevention

The following table describes the labels in this screen.

Table 174   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 sync the security settings on this screen to. Select **All sites** to sync security settings with all sites in the organization. Note: You can only add sites that have a Security Firewall gateway device.
Content Filtering	
Drop connection when there is an HTTPS connection with SSL v3 (or previous version)	Select **On** to have the Security Gateway 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;/?:@&=+$\.–_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the security gateway just opens the web page you specified without showing a denied access message.
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Enabled	Select the check box to enable the content filtering 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 filtering profile. See Section 8.3.8.1 on page 394 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 8.3.8.2 on page 397 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.

Table 174 Organization-wide > Organization-wide manage > Security profile sync (continued)

LABEL	DESCRIPTION
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 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.
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;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the Nebula Device just opens the web page you specified without showing a denied access message.
URL Threat Filter Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0–9a–zA–Z;/?:@&=+$\.-_!~*'()%). 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.
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.

Table 174 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 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.
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.

Table 174 Organization-wide > Organization-wide manage > Security profile sync (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. Add the IPv4 addresses that the Nebula Device will allow the incoming packets.
External block list	
Enabled	Select this check box 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 myZyxel, register your Nebula Device and then subscribe for IP reputation 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.
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.

Table 174 Organization-wide > Organization-wide manage > Security profile sync (continued)

LABEL	DESCRIPTION
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.
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.

Table 174 Organization-wide > Organization-wide manage > Security profile sync (continued)

LABEL	DESCRIPTION
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 Detection/Prevention	
Detection	Select **On** to enable Detection.
Prevention	Select **On** to enable Prevention.

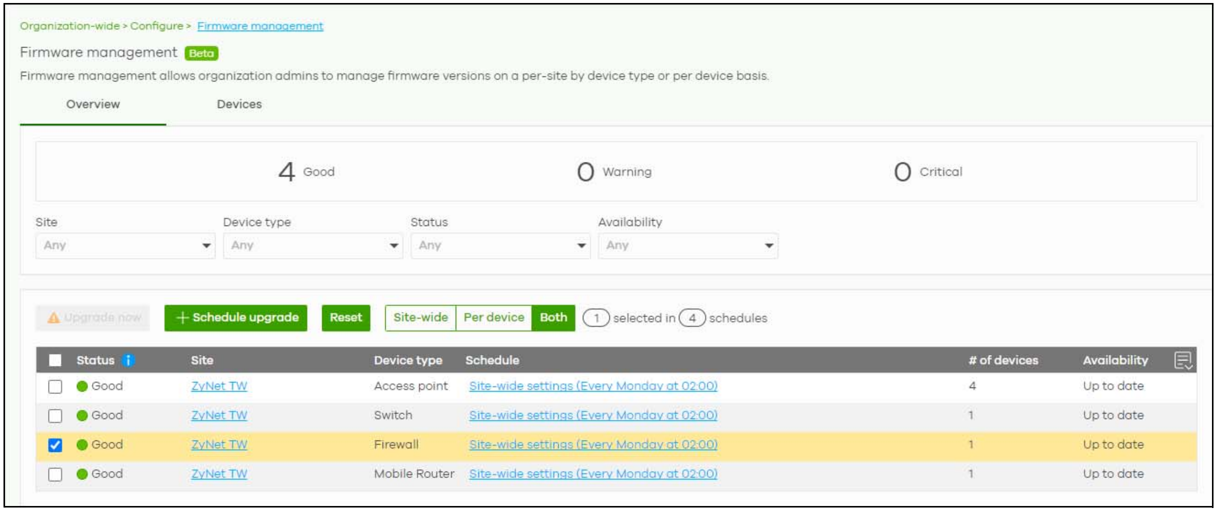
11.4.6 Firmware Management

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.

11.4.6.1 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 208 Organization-wide > Organization-wide manage > Firmware management > Overview



Organization-wide > Configure > Firmware management

Firmware management Beta

Firmware management allows organization admins to manage firmware versions on a per-site by device type or per device basis.

Overview Devices

4 Good 0 Warning 0 Critical

Site: Any
Device type: Any
Status: Any
Availability: Any

1 selected in 4 schedules

	Status	Site	Device type	Schedule	# of devices	Availability
□	● Good	ZyNet TW	Access point	Site-wide settings (Every Monday at 02:00)	4	Up to date
□	● Good	ZyNet TW	Switch	Site-wide settings (Every Monday at 02:00)	1	Up to date
☑	● Good	ZyNet TW	Firewall	Site-wide settings (Every Monday at 02:00)	1	Up to date
□	● Good	ZyNet TW	Mobile Router	Site-wide settings (Every Monday at 02:00)	1	Up to date

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, existing firmware upgrades will still run as scheduled.

11.4.6.2 Firmware Upgrade Priority

NCC prioritizes the different Nebula Device firmware upgrade schedules as follows, from highest to lowest:

1. Individual Nebula Device upgrade schedule (set at **Organization-wide** > **Organization-wide manage** > **Firmware management** > **Devices**).
2. Organization-wide or site-wide upgrade schedule. If both are set, the schedule that was most recently set takes priority.
3. NCC default per-device upgrade schedule and default site-wide upgrade schedule (14 days after new firmware is released).

11.4.6.3 Firmware Management Overview Screen

The following table describes the labels in this screen.

Table 175 Organization-wide > Organization-wide manage > Firmware management > Overview

LABEL	DESCRIPTION
Site	Select 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 status of the Nebula Device's firmware. By default, all the status are displayed (**Any**). Select **Good** to display the Nebula Devices running a stable firmware with 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, 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**). By default, all the available firmware are 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.

Table 175 Organization-wide > Organization-wide manage > Firmware management > Overview

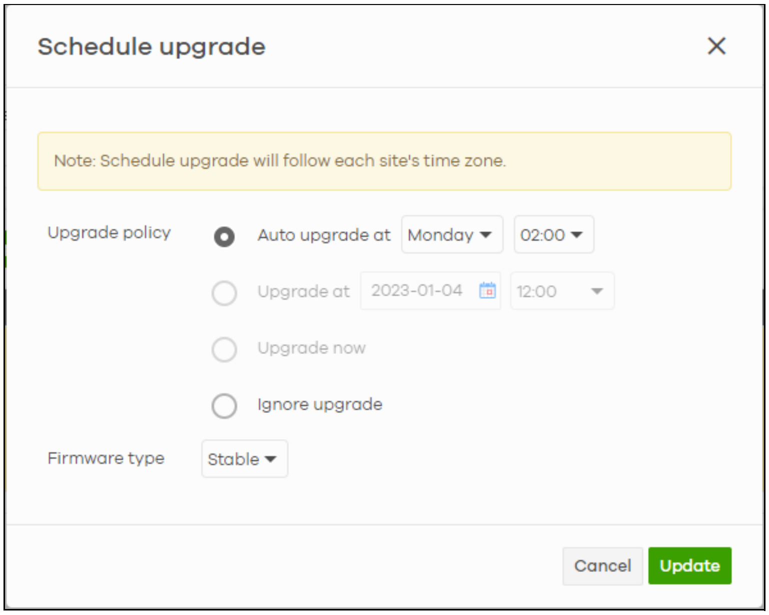
LABEL	DESCRIPTION
Schedule Upgrade	Click this to pop-up a window where you can set a specific date and time to upgrade the Nebula Devices firmware on the selected sites.  Schedule upgrade Note: Schedule upgrade will follow each site's time zone. Upgrade policy ● Auto upgrade at Monday 02:00 ○ Upgrade at 2023-01-04 12:00 ○ Upgrade now ○ Ignore upgrade Firmware type Stable Note: Nebula Devices are upgraded according to the time zone of the site they are in.
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	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 176 on page 538 for more information).

Table 175 Organization-wide > Organization-wide manage > Firmware management > Overview

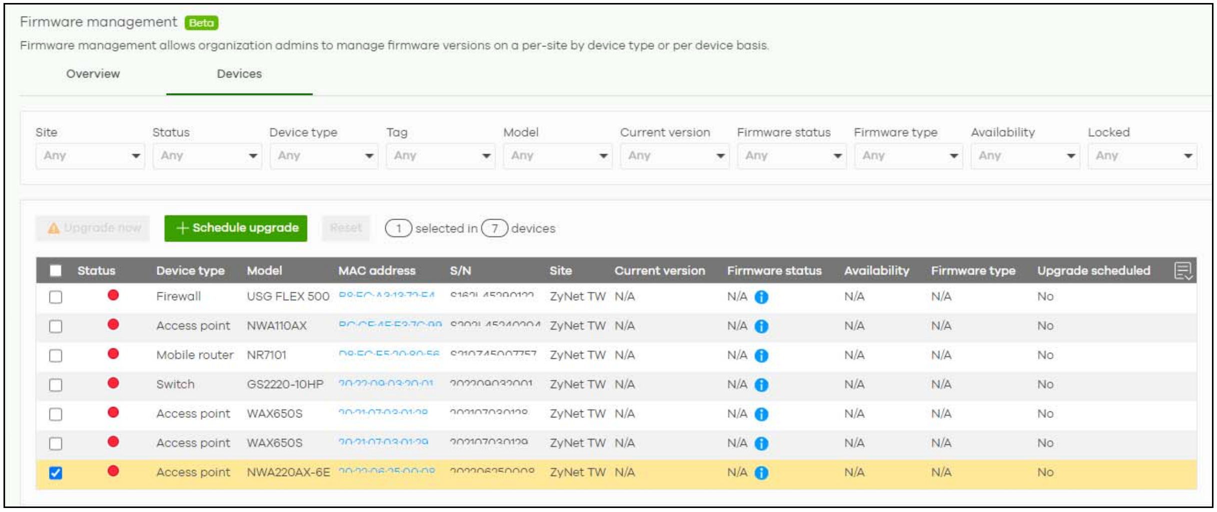
LABEL	DESCRIPTION
Availability	This shows whether the firmware on the Nebula Device is **Up to date**, there is firmware update available for the Nebula Device (**Upgrade available**), or a specific version of firmware has been installed by Zyxel customer support (**Locked**).
☰	Click this icon to show and hide columns in the table.

11.4.6.4 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 209 Organization-wide > Organization-wide manage > Firmware management > Devices



Firmware management Beta

Firmware management allows organization admins to manage firmware versions on a per-site by device type or per device basis.

Overview | Devices

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

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

☐	Status	Device type	Model	MAC address	S/N	Site	Current version	Firmware status	Availability	Firmware type	Upgrade scheduled
☐	●	Firewall	USG FLEX 500	[illegible]	[illegible]	ZyNet TW	N/A	N/A ⓘ	N/A	N/A	No
☐	●	Access point	NWA110AX	[illegible]	[illegible]	ZyNet TW	N/A	N/A ⓘ	N/A	N/A	No
☐	●	Mobile router	NR7101	[illegible]	[illegible]	ZyNet TW	N/A	N/A ⓘ	N/A	N/A	No
☐	●	Switch	GS2220-10HP	20:22:09:03:20:01	202209032001	ZyNet TW	N/A	N/A ⓘ	N/A	N/A	No
☐	●	Access point	WAX650S	20:21:07:03:01:28	202107030128	ZyNet TW	N/A	N/A ⓘ	N/A	N/A	No
☐	●	Access point	WAX650S	20:21:07:03:01:29	202107030129	ZyNet TW	N/A	N/A ⓘ	N/A	N/A	No
☑	●	Access point	NWA220AX-6E	20:22:06:25:00:08	202206250008	ZyNet TW	N/A	N/A ⓘ	N/A	N/A	No

The following table describes the labels in this screen.

Table 176 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.

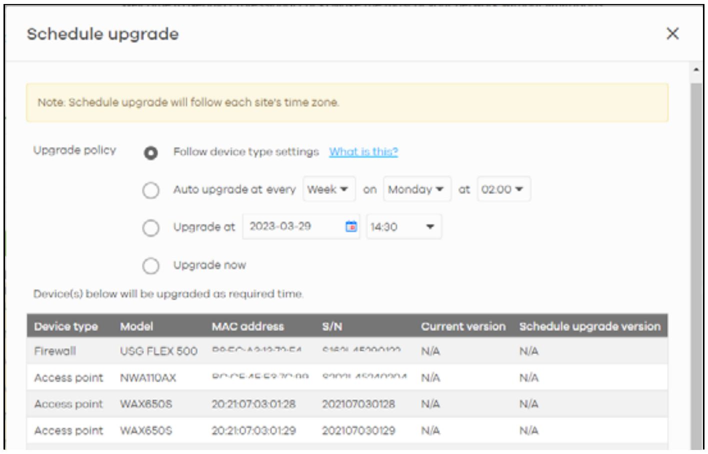
Table 176 Organization-wide > Organization-wide manage > Firmware management > Devices

<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></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 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.

<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>
</table>

</td></tr>
<tr><td>Reset</td><td>Select one or more Nebula Devices, and then click <b>Reset</b> to allow the Nebula Devices to follow the site-wide firmware management settings.</td></tr>
<tr><td>Status</td><td>

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.

</td></tr>
<tr><td>Device type</td><td>This shows the type of the Nebula Device.</td></tr>
<tr><td>Model</td><td>This shows the model number of the Nebula Device.</td></tr>
<tr><td>Tag</td><td>This shows the tag created and added to the Nebula Device.</td></tr>
<tr><td>Name</td><td>This shows the descriptive name of the Nebula Device.</td></tr>
<tr><td>MAC address</td><td>This shows the MAC address of the Nebula Device.</td></tr>
<tr><td>S/N</td><td>This shows the serial number of the Nebula Device.</td></tr>
<tr><td>Site</td><td>This shows the descriptive name of the site.</td></tr>
<tr><td>Current version</td><td>This shows the version number of the firmware the Nebula Device is currently running. It shows <b>N/A</b> when the Nebula Device goes offline and its firmware version is not available.</td></tr>
</table>

Table 176 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 177 on page 541 for an example **Firmware type** version progression example scenario.
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**).
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 177 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.

11.4.7 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 207).

11.4.7.1 User Account Types

NCC has the following types of user accounts. For details on using these accounts for WiFi and network authentication, see Section 5.3.1 on page 247.

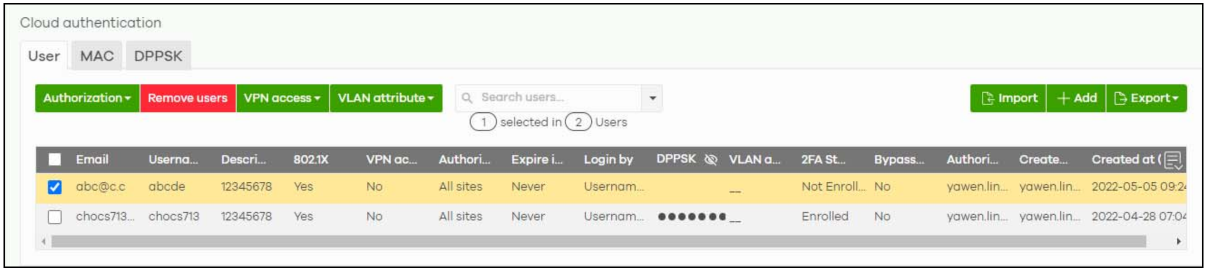
Table 178 Cloud Authentication: User Account Types

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

11.4.7.2 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 210 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 179 Organization-wide > Organization-wide manage > Cloud authentication > User

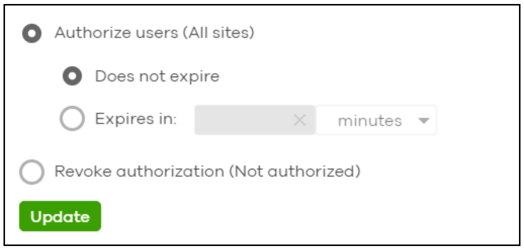
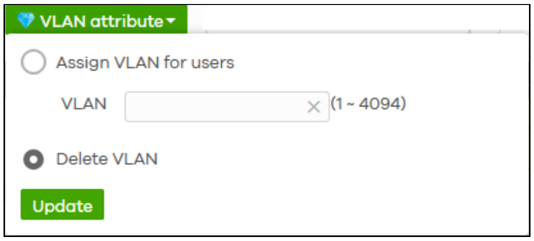
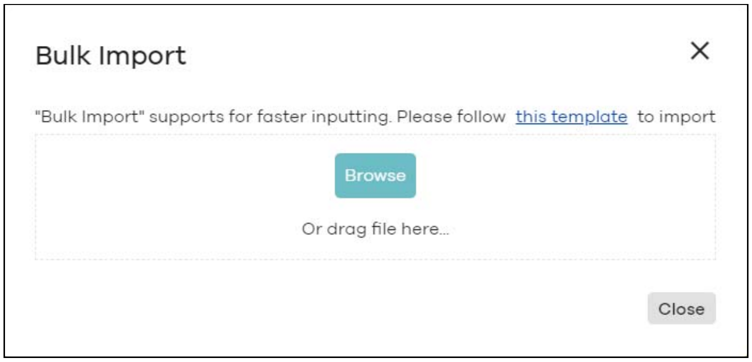
LABEL	DESCRIPTION
Authorization	Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (All sites) ● Does not expire ○ Expires in: minutes ○ Revoke authorization (Not authorized) Update
Remove users	Select 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.

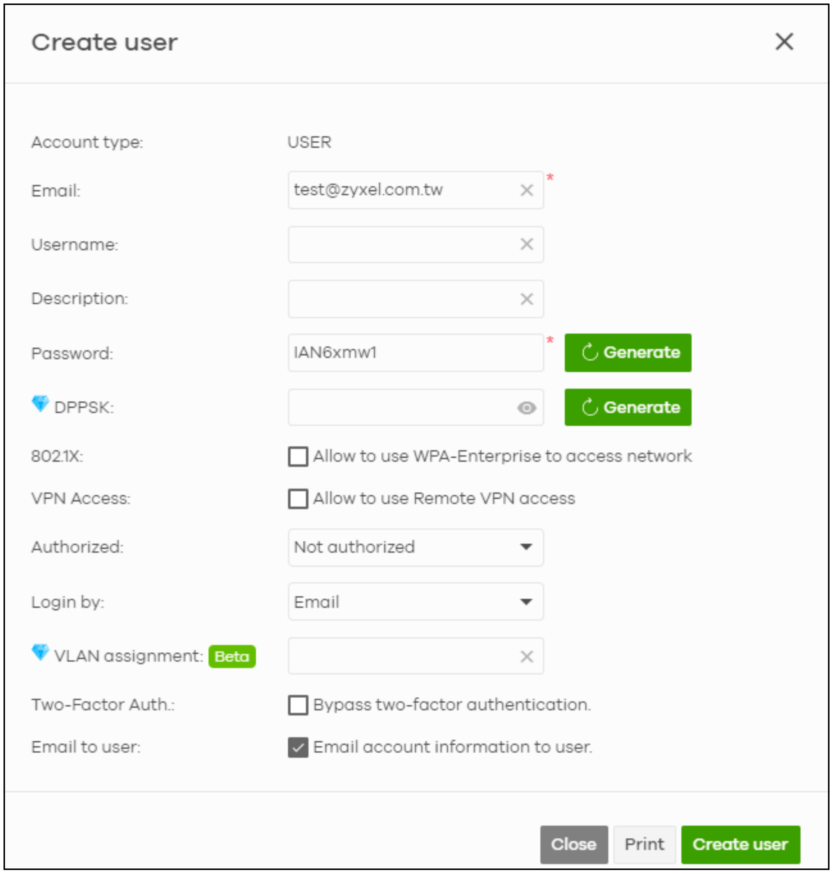
Table 179 Organization-wide > Organization-wide manage > Cloud authentication > User (continued)

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 Or drag file here...
Add	Click this button to create a new user account. See Section 11.4.7.3 on page 544.
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.

11.4.7.3 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 211 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
DPPSK:	
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 180 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.

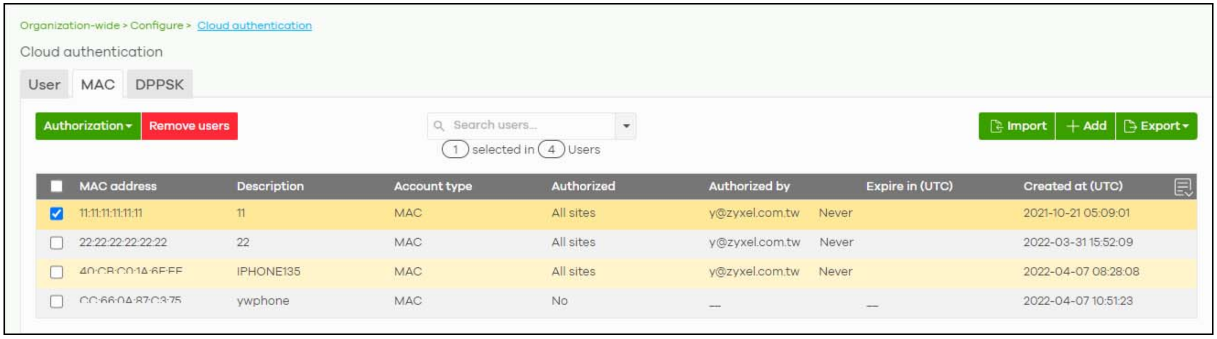
Table 180 Organization-wide > Organization-wide manage > Cloud authentication > User: Create/ Update user (continued)

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.

11.4.7.4 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 212 Organization-wide > Organization-wide manage > Cloud authentication > MAC



☐	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:66:04:87: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 181 Organization-wide > Organization-wide manage > Cloud authentication > MAC

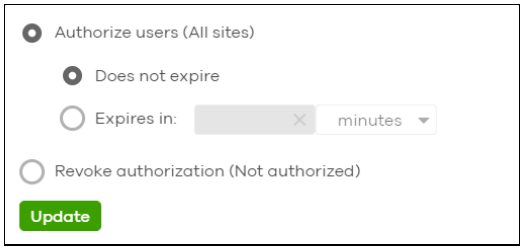
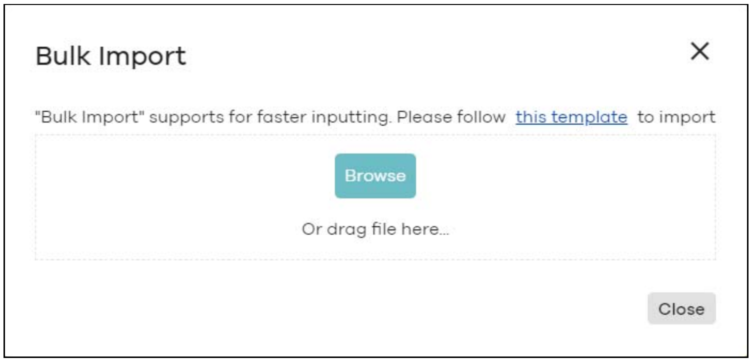
LABEL	DESCRIPTION
Authorization	Select one or more than one account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (All sites) ● Does not expire ○ Expires in: minutes ○ Revoke authorization (Not authorized) Update
Remove users	Select one 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 11.4.7.5 on page 547.
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.

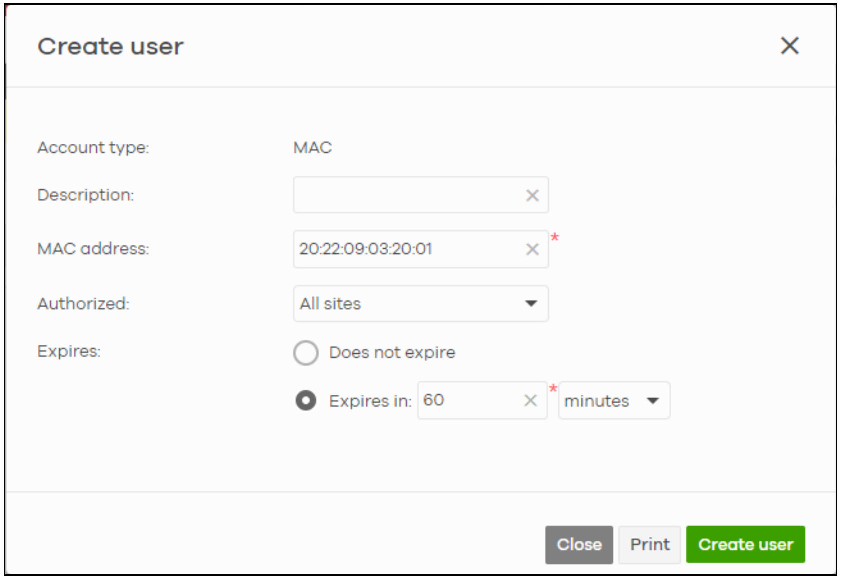
Table 181 Organization-wide > Organization-wide manage > Cloud authentication > MAC (continued)

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.

11.4.7.5 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 213 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.

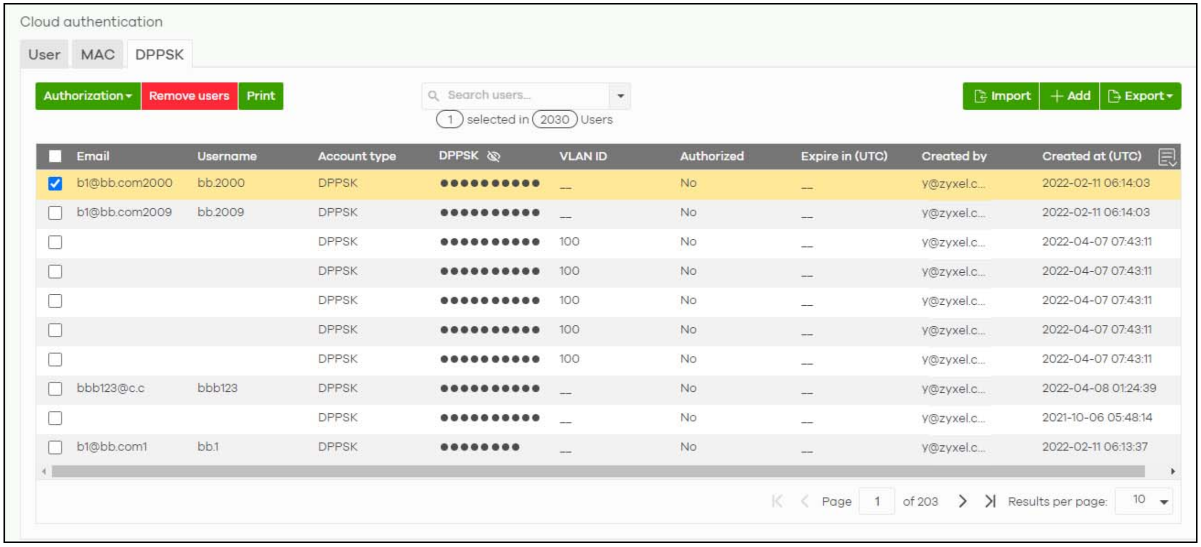
Table 182 Organization-wide > Organization-wide manage > Cloud authentication > MAC: Create/Update user

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.

11.4.7.6 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 214 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	bb1	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 183 Organization-wide > Organization-wide manage > Cloud authentication > DPPSK

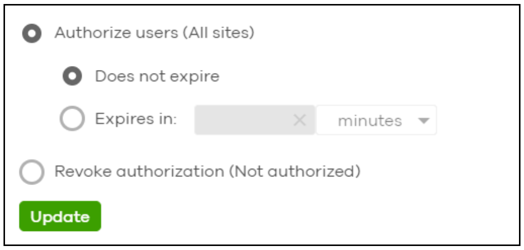
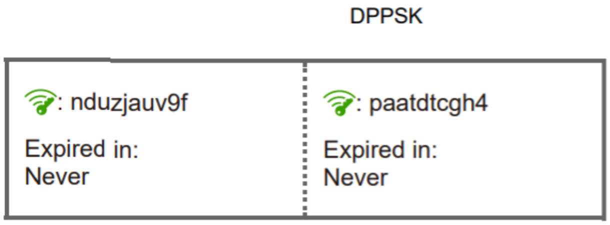
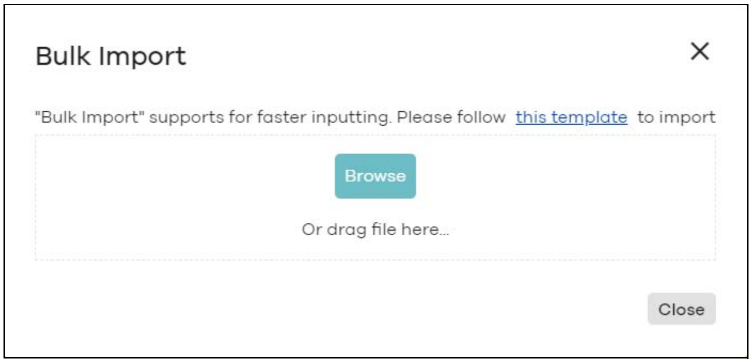
LABEL	DESCRIPTION
Authorization	Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.  ● Authorize users (All sites) ● Does not expire ○ Expires in: minutes ○ Revoke authorization (Not authorized)
Remove users	Select one 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
Add	Click this button to create a single new account, or a batch of accounts. • Single DPPSK: See Section 11.4.7.7 on page 550. • Batch create DPPSK: See Section 11.4.7.8 on page 551.
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.

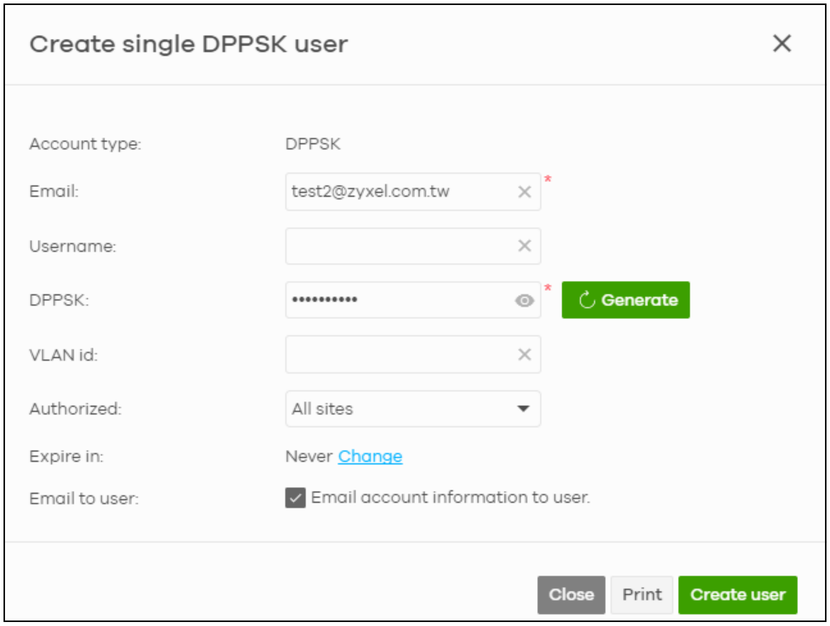
Table 183   Organization-wide > Organization-wide manage > Cloud authentication > DPPSK

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.

11.4.7.7 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 215   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.

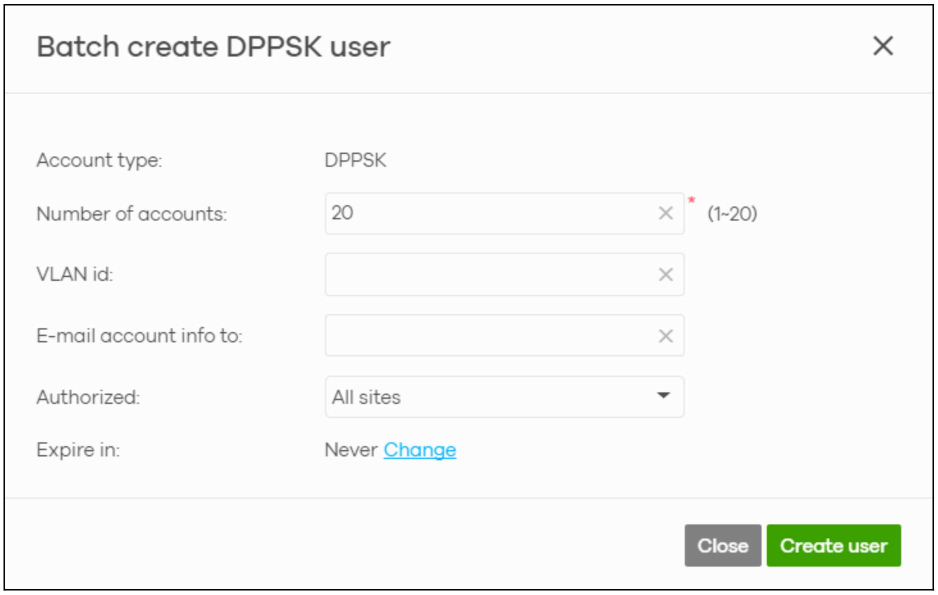
Table 184 Organization-wide > Organization-wide manage > Cloud authentication > DPPSK: Create/ Update DPPSK user

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.

11.4.7.8 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 216 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 185 Organization-wide > Organization-wide manage > Cloud authentication: Batch Create DPPSK

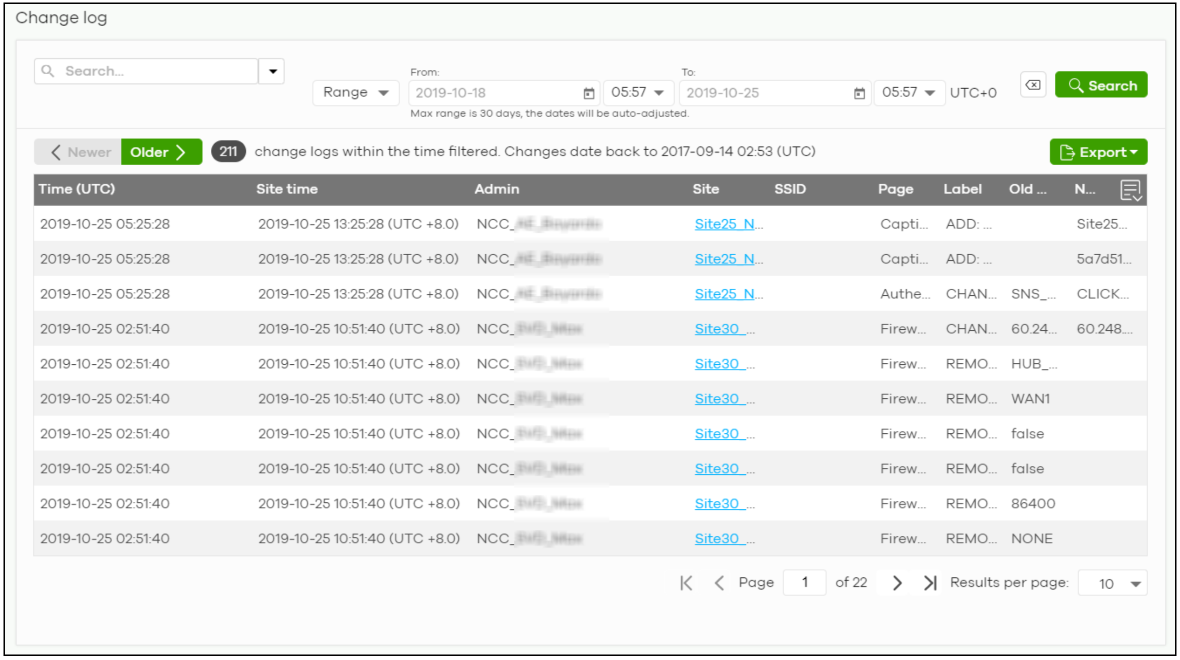
LABEL	DESCRIPTION
Number of accounts	Enter how many DPPSK user accounts you want to create.
VLAN id	Assign the users to a specific VLAN based on the user's dynamic personal pre-shared key (DPPSK).
E-mail account info to	Send a copy of each user account's dynamic personal pre-shared key (DPPSK) and expiry 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.

11.4.8 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 217 Organization-wide > Organization-wide manage > Change log



Change log

Search... ▾ Range ▾ From: 2019-10-18 05:57 ▾ To: 2019-10-25 05:57 ▾ UTC+0 Search

Max range is 30 days, the dates will be auto-adjusted.

< Newer Older > 211 change logs within the time filtered. Changes date back to 2017-09-14 02:53 (UTC) Export ▾

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	

Page 1 of 22 Results per page: 10 ▾

The following table describes the labels in this screen.

Table 186 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.

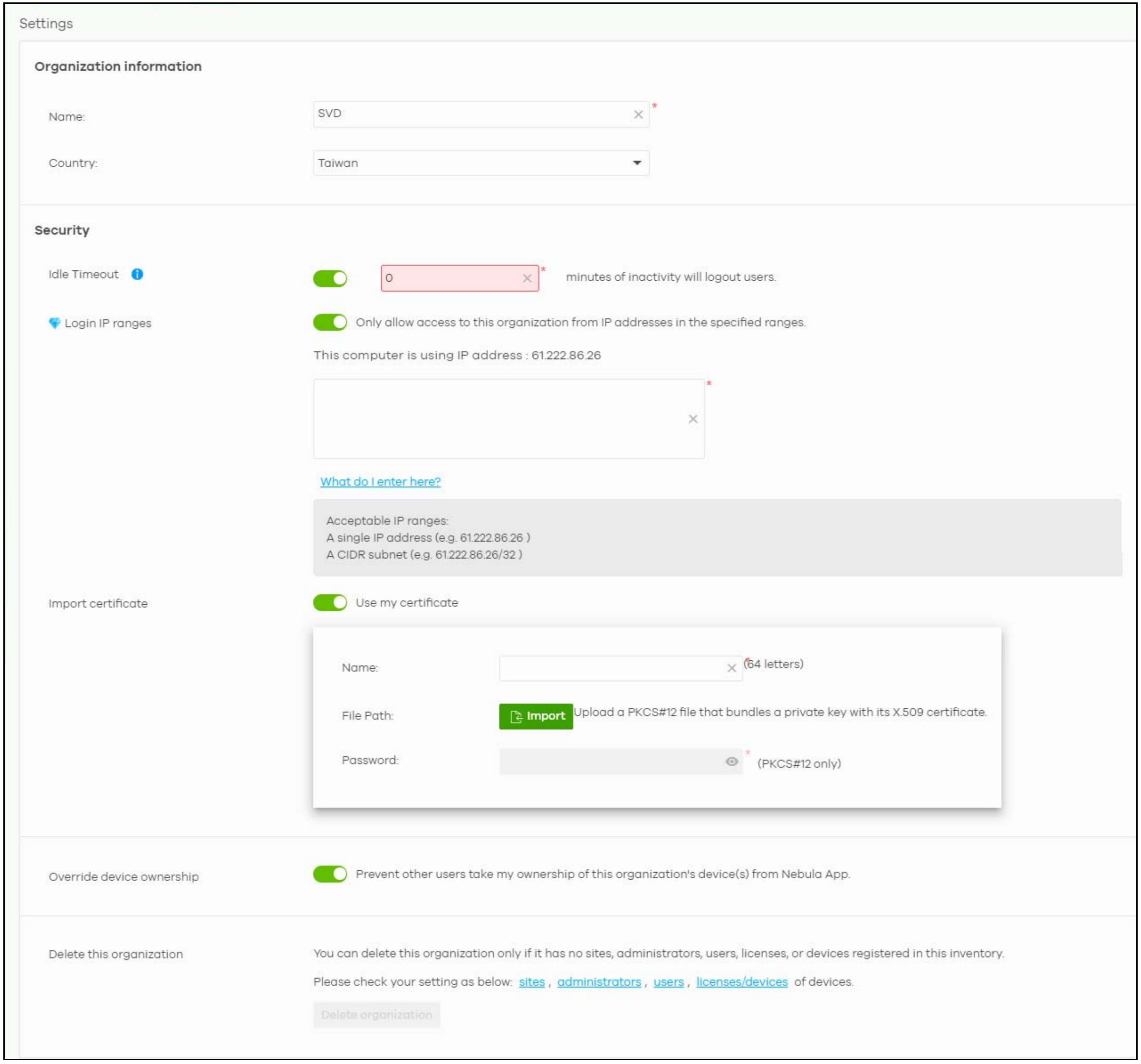
Table 186 Organization-wide > Organization-wide manage > Change log (continued)

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.

11.4.9 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 218 Organization-wide > Organization-wide manage > Organization settings



Settings

Organization information

Name: SVD *

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?

Acceptable IP ranges:
A single IP address (e.g. 61.222.86.26)
A CIDR subnet (e.g. 61.222.86.26/32)

Import certificate: Use my certificate

Name: (64 letters)

File Path: Import Upload a PKCS#12 file that bundles a private key with its X.509 certificate.

Password: (PKCS#12 only)

Override device ownership: Prevent other users take my ownership of this organization's device(s) from Nebula App.

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.

The following table describes the labels in this screen.

Table 187 Organization-wide > Organization-wide manage > Organization settings

LABEL	DESCRIPTION
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.
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.
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	
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.
Override device ownership	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.
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 12 Group-wide

12.1 Introduction

This chapter discusses the menus that you can use to monitor and manage your groups settings.

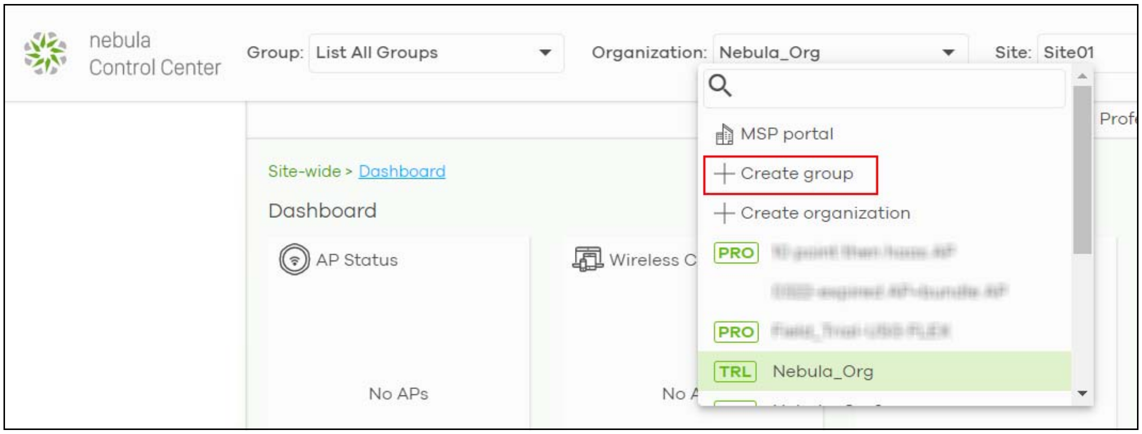
A group is a collection of two or more organizations. Groups allow you to view and manage multiple organizations, and create VPN links between groups in the organization.

12.1.1 Creating a Group

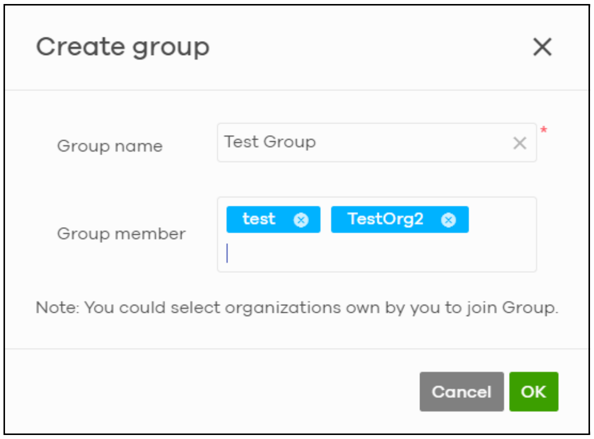
Follow the steps below to create a group.

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 *

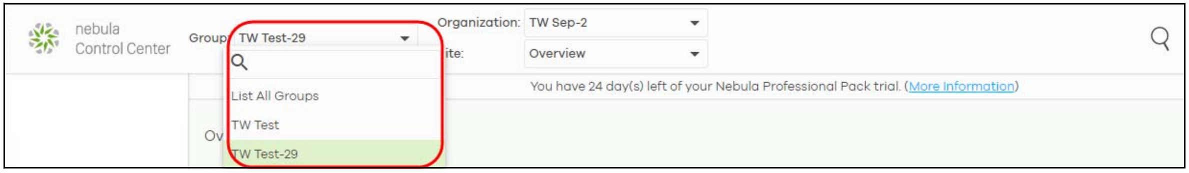
Group member: test, TestOrg2

Note: You could select organizations own by you to join Group.

12.1.2 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 219 Group-wide > Group-wide manage > Overview: Group

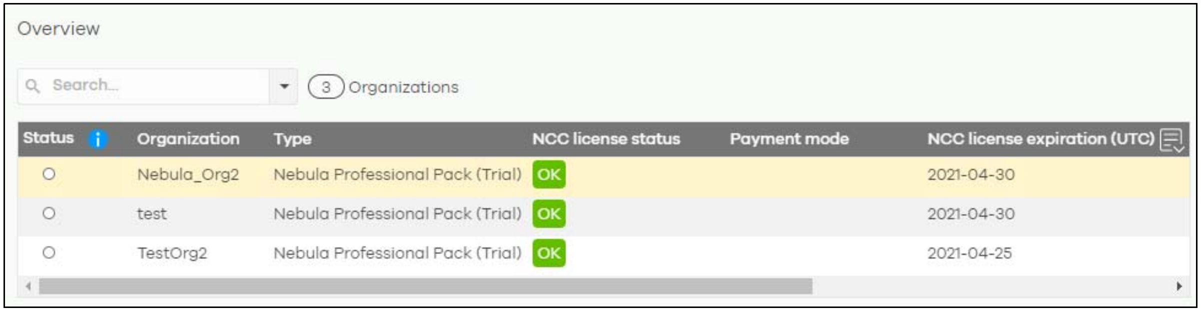


You have 24 day(s) left of your Nebula Professional Pack trial. (More information)

12.2 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 220 Group-wide > Group-wide manage > Group portal



Overview

Search... 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 188 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.

Table 188 Group-wide > Group-wide manage > Group portal (continued)

LABEL	DESCRIPTION
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.

12.3 Org-to-Org VPN

Org-to-Org VPN allows devices in different organizations in a group to access each other's services, such as a website, database, or ERP server, through VPN tunnels.

12.3.1 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.

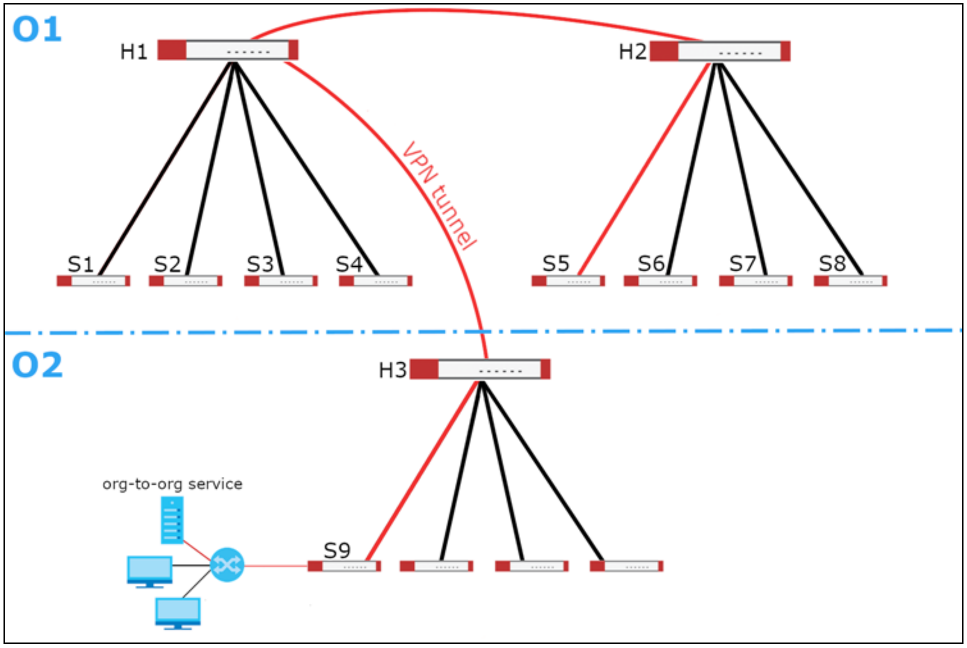
4 Click **+ Org-to-Org Service**, and add a server's fully qualified domain name (FQDN) and IP address.

5 Devices in the organizations included in the Org-to-Org VPN are now able to access the server by IP address or FQDN.

12.3.2 Org-to-Org VPN Example

Figure 221 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**.

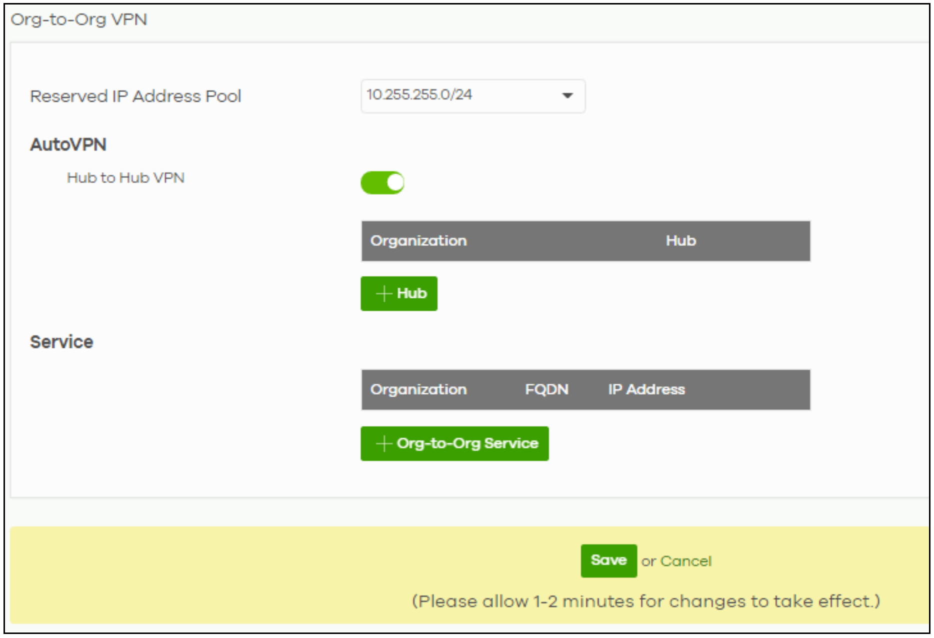
Figure 221 Org-to-Org VPN Example



12.3.3 Org-to-Org VPN Screen

Click **Group-wide** > **Group-wide manage** > **Org-to-Org VPN** to access this screen.

Figure 222 Group-wide > Group-wide manage > Org-to-Org VPN



Org-to-Org VPN

Reserved IP Address Pool: 10.255.255.0/24

AutoVPN

Hub to Hub VPN: On

Organization	Hub

+ Hub

Service

Organization	FQDN	IP Address

+ Org-to-Org Service

Save or Cancel

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

The following table describes the labels in this screen.

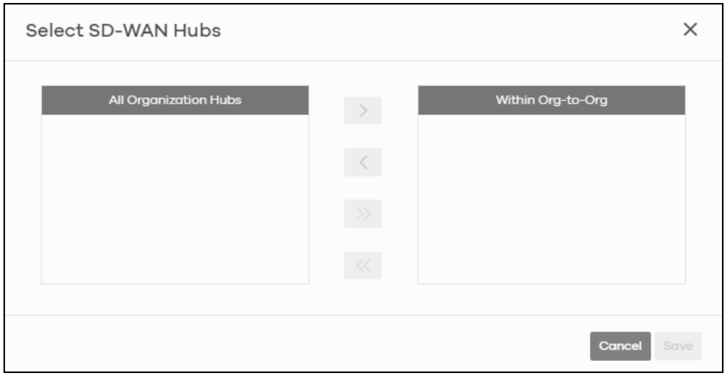
Table 189 Group-wide > Group-wide manage > Org-to-Org VPN

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.

12.3.4 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 223 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.

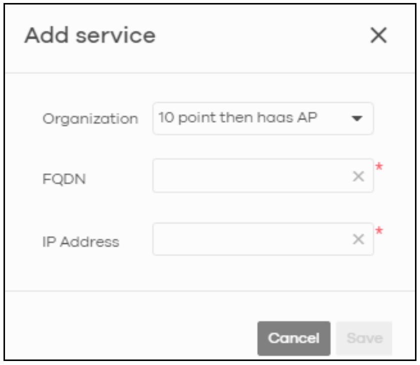
Table 190 Group-wide > Group-wide manage > Org-to-Org VPN: SD-WAN Hubs

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.

12.3.5 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 224 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.

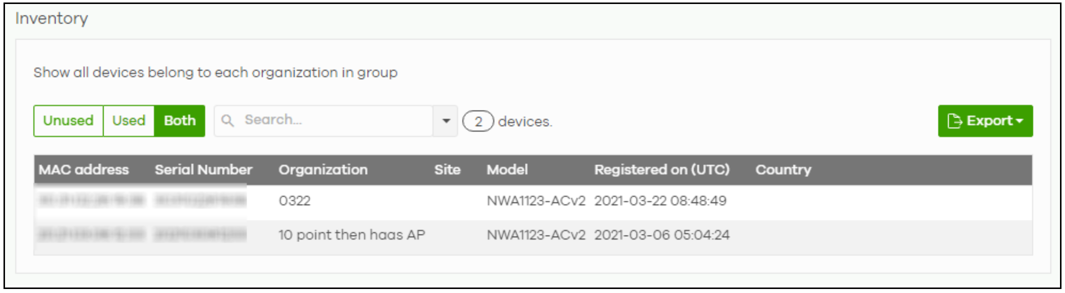
Table 191 Group-wide > Group-wide manage > Org-to-Org VPN: Service

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.

12.4 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 225 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 192 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.
Organization	This shows the organization of the Nebula Device.

Table 192   Group-wide > Group-wide manage > Inventory (continued)

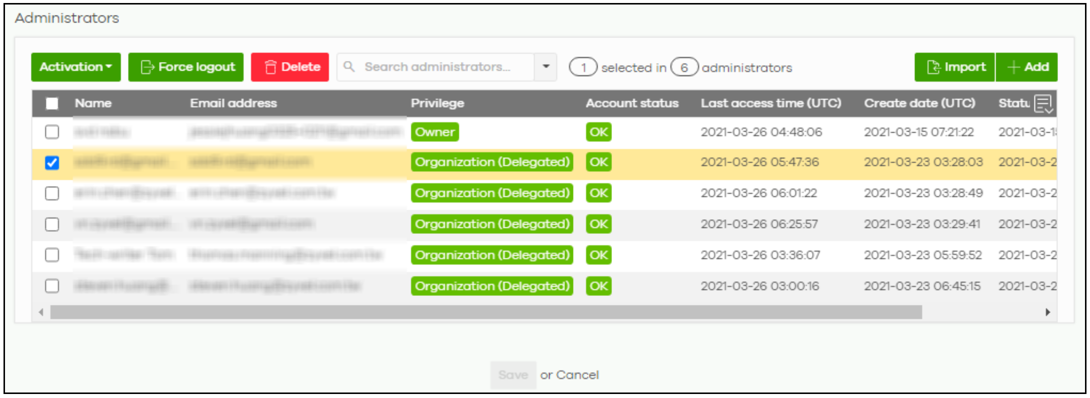
LABEL	DESCRIPTION
Site	This shows the name of the site to which the Nebula Device is connected.
Model	This shows the model number of the Nebula Device.
Registered on (UTC)	This shows the date and time that the Nebula Device was registered at the NCC.
Country	This shows the country where the Nebula Device is located.

12.5 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 226   Group-wide > Group-wide manage > Administrators



Administrators

Activation ▾ | Force logout | Delete | Search administrators... ▾ | (1) selected in (6) administrators | Import | + Add

■	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

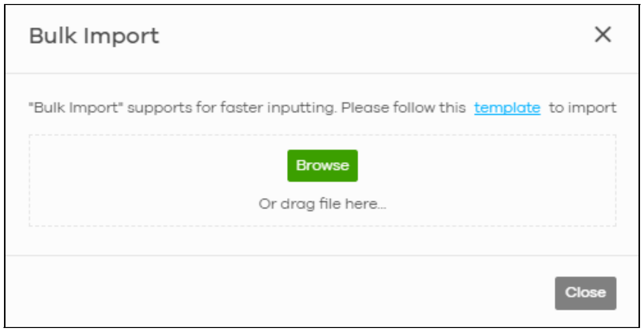
Save or Cancel

The following table describes the labels in this screen.

Table 193   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.

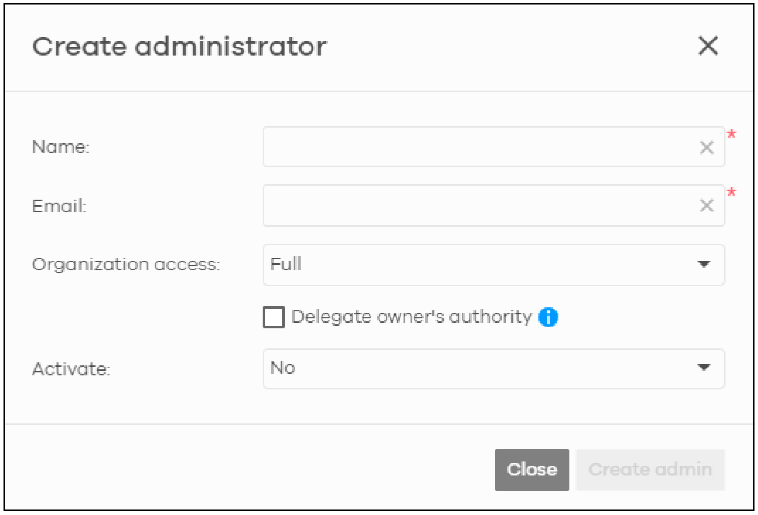
Table 193 Group-wide > Group-wide manage > Administrators (continued)

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.  "Bulk Import" supports for faster inputting. Please follow this template to import
Add	Click this button to create a new group administrator account. See Section 12.5.1 on page 565.
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.

12.5.1 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 227 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 194 Group-wide > Group-wide manage > Administrators: Create/Update administrator

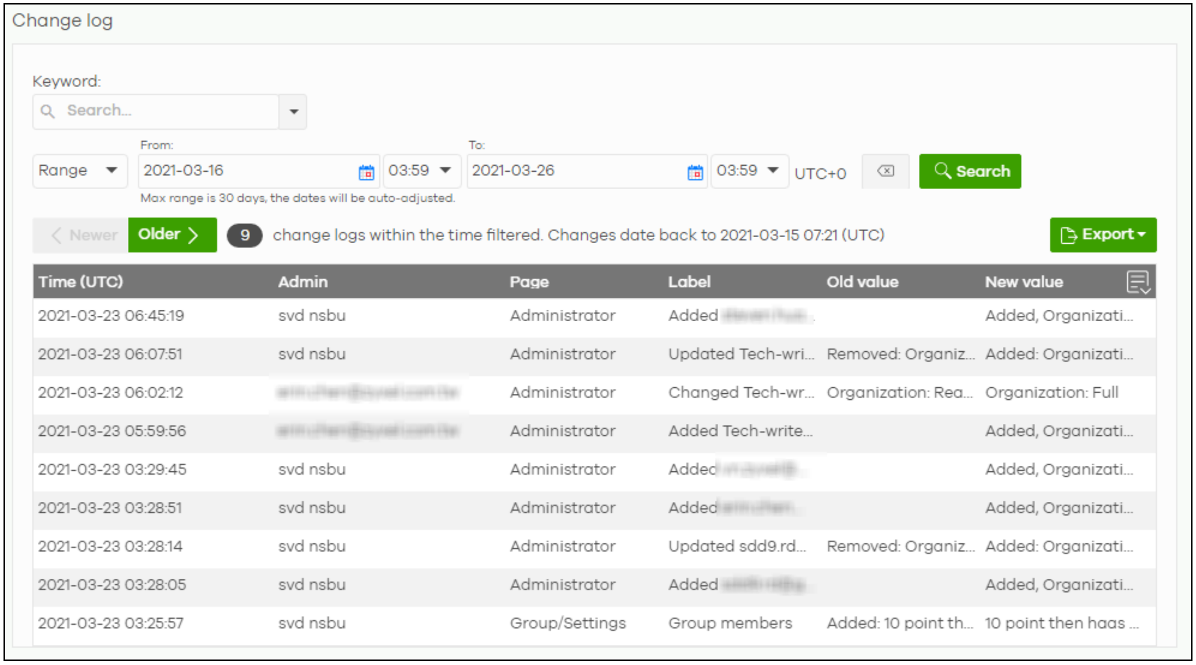
LABEL	DESCRIPTION
Name	Enter a descriptive name for the administrator account.
Email	Enter the email address of the administrator account, which is used to log into the NCC. This field is read-only if you are editing an existing account.
Organization access	This shows the privileges the administrator 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.

12.6 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 228 Group-wide > Group-wide manage > Change log



Change log

Keyword:

Search...

From: 2021-03-16 03:59 To: 2021-03-26 03:59 UTC+0

Range

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.

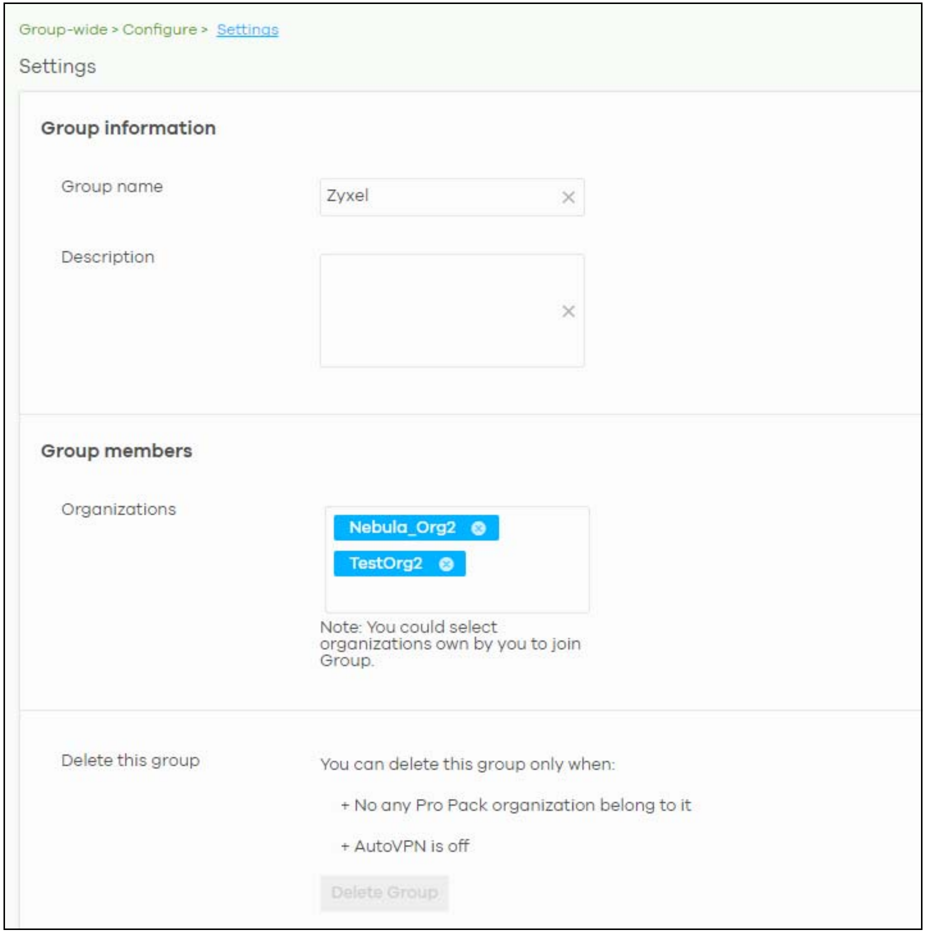
Table 195 Group-wide > Group-wide manage > Change log

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.

12.7 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 229 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 196 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 13 MSP

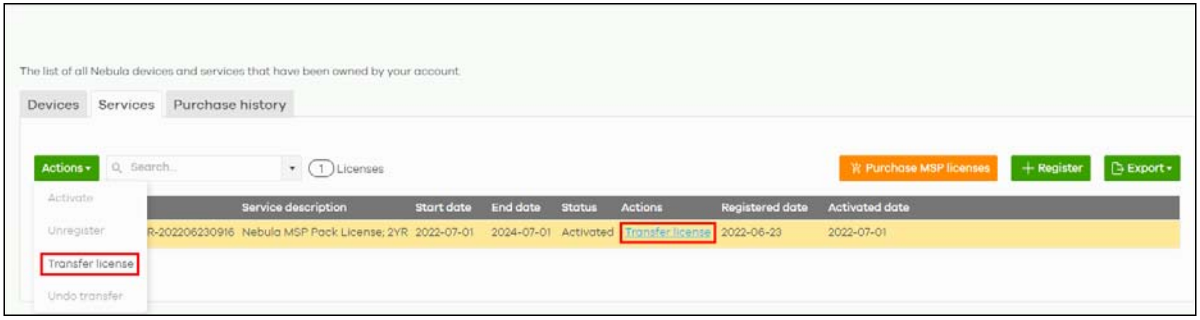
13.1 Overview

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 230 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

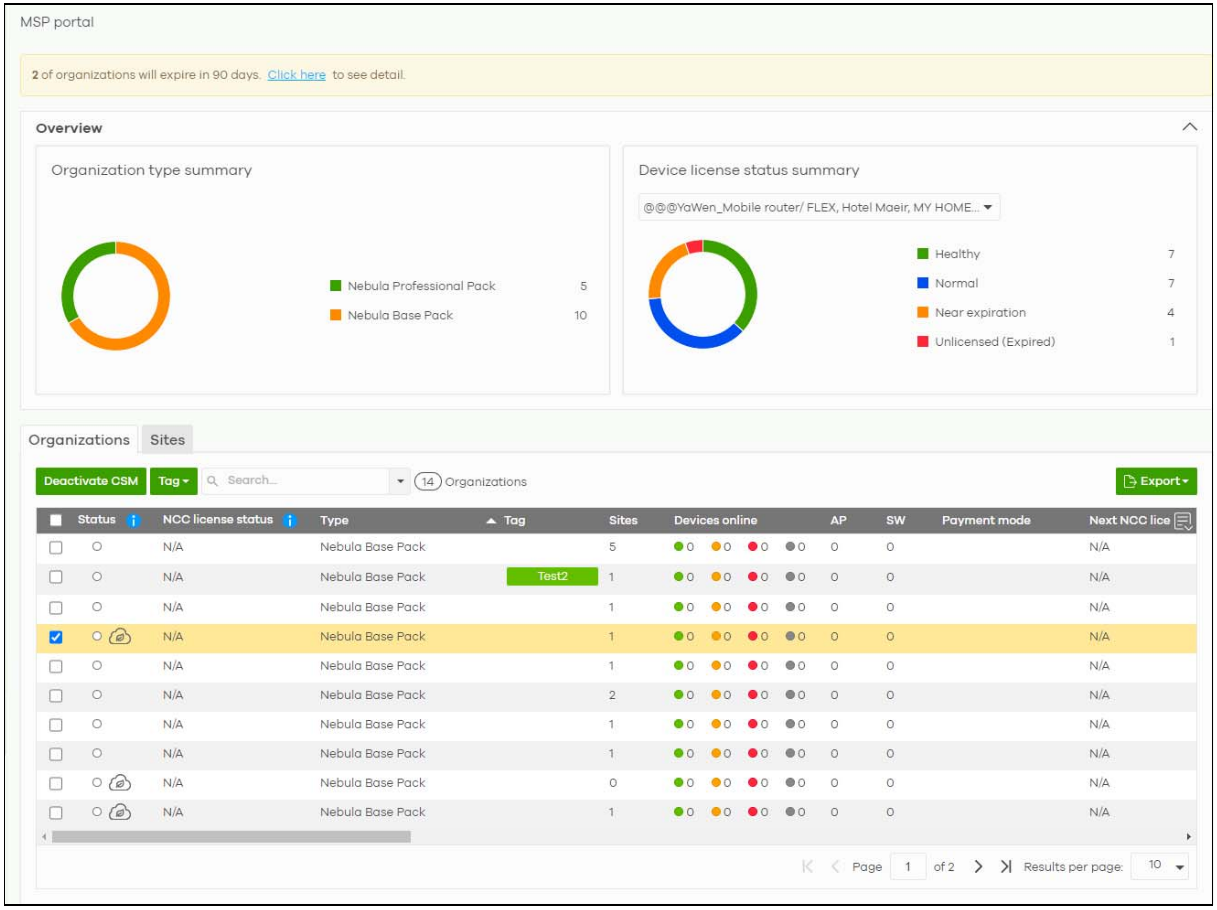
Note: To see these menus, assign an MSP license to your NCC login account.

13.2 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 231 MSP cross-org > MSP cross-org manage > MSP portal



MSP portal

2 of organizations will expire in 90 days. Click here to see detail.

Overview

Organization type summary

🟩 Nebula Professional Pack	5
🟧 Nebula Base Pack	10

Device license status summary

@@@YaWen_Mobile router/ FLEX, Hotel Maeir, MY HOME...

🟩 Healthy	7
🟦 Normal	7
🟧 Near expiration	4
🟥 Unlicensed (Expired)	1

14 Organizations

☐	Status	NCC license status	Type	Tag	Sites	Devices online	AP	SW	Payment mode	Next NCC lice
☐	○	N/A	Nebula Base Pack		5	●0 ●0 ●0 ●0	0	0		N/A
☐	○	N/A	Nebula Base Pack	Test2	1	●0 ●0 ●0 ●0	0	0		N/A
☐	○	N/A	Nebula Base Pack		1	●0 ●0 ●0 ●0	0	0		N/A
☑	○	N/A	Nebula Base Pack		1	●0 ●0 ●0 ●0	0	0		N/A
☐	○	N/A	Nebula Base Pack		1	●0 ●0 ●0 ●0	0	0		N/A
☐	○	N/A	Nebula Base Pack		2	●0 ●0 ●0 ●0	0	0		N/A
☐	○	N/A	Nebula Base Pack		1	●0 ●0 ●0 ●0	0	0		N/A
☐	○	N/A	Nebula Base Pack		1	●0 ●0 ●0 ●0	0	0		N/A
☐	○	N/A	Nebula Base Pack		0	●0 ●0 ●0 ●0	0	0		N/A
☐	○	N/A	Nebula Base Pack		1	●0 ●0 ●0 ●0	0	0		N/A

Page 1 of 2 Results per page: 10

The following table describes the labels in this screen.

Table 197 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	
Deactivate CSM	Select the organization(s) and click this button to disable CSM (Cloud-Saving Mode). See Section 1.6 on page 45 for more information on Cloud-saving mode.

Table 197 MSP cross-org > MSP cross-org manage > MSP portal (continued)

LABEL	DESCRIPTION
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.
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.

Table 197 MSP cross-org > MSP cross-org manage > MSP portal (continued)

LABEL	DESCRIPTION
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.
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.
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.

13.3 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.

13.3.1 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.

13.3.2 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.

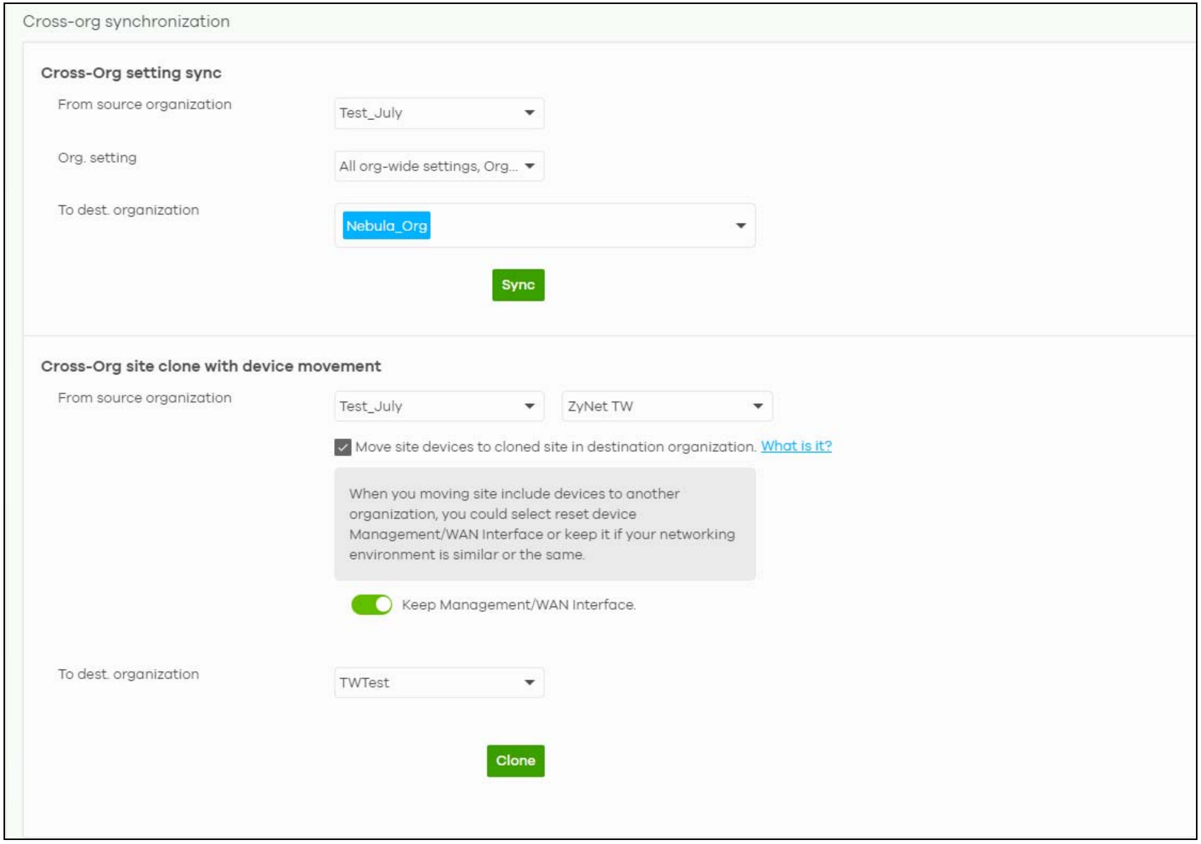
Table 198 Nebula Device Cross-org Site Clone

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.

13.3.3 Cross-org synchronization Screen

Use this screen to configure cross-org synchronization and cross site clones.

Figure 232 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. (on)

To dest. organization: TWTest

The following table describes the labels in this screen.

Table 199 MSP cross-org > MSP cross-org manage > Cross-org synchronization

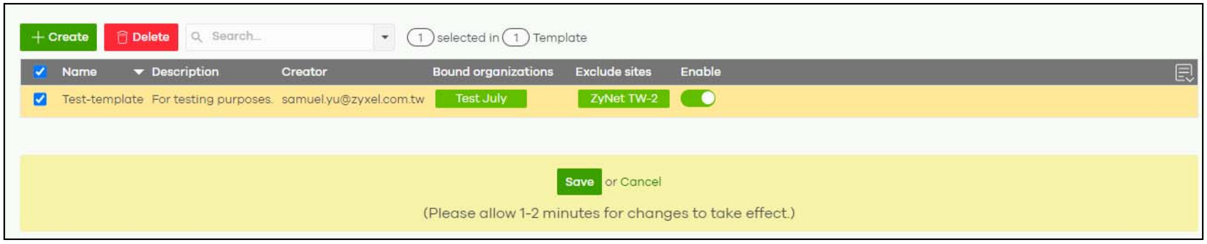
LABEL	DESCRIPTION
Cross-Org setting sync	
From source organization	Select the organization to copy settings from.
Org. setting	Select the settings that you want to copy from the source to the destination organization. Select **All org-wide settings** to copy everything.
To dest. organization	Select the 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.

13.4 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 13.4.1 on page 577 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 233 MSP cross-org > MSP cross-org manage > Alert templates



☑	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 200 MSP cross-org > MSP cross-org manage > Alert templates

LABEL	DESCRIPTION
+ Create	Click this button to add a new alert template (see Section 13.4.1 on page 577).
Delete	Click this button to remove alert templates already created.

Table 200 MSP cross-org > MSP cross-org manage > Alert templates (continued)

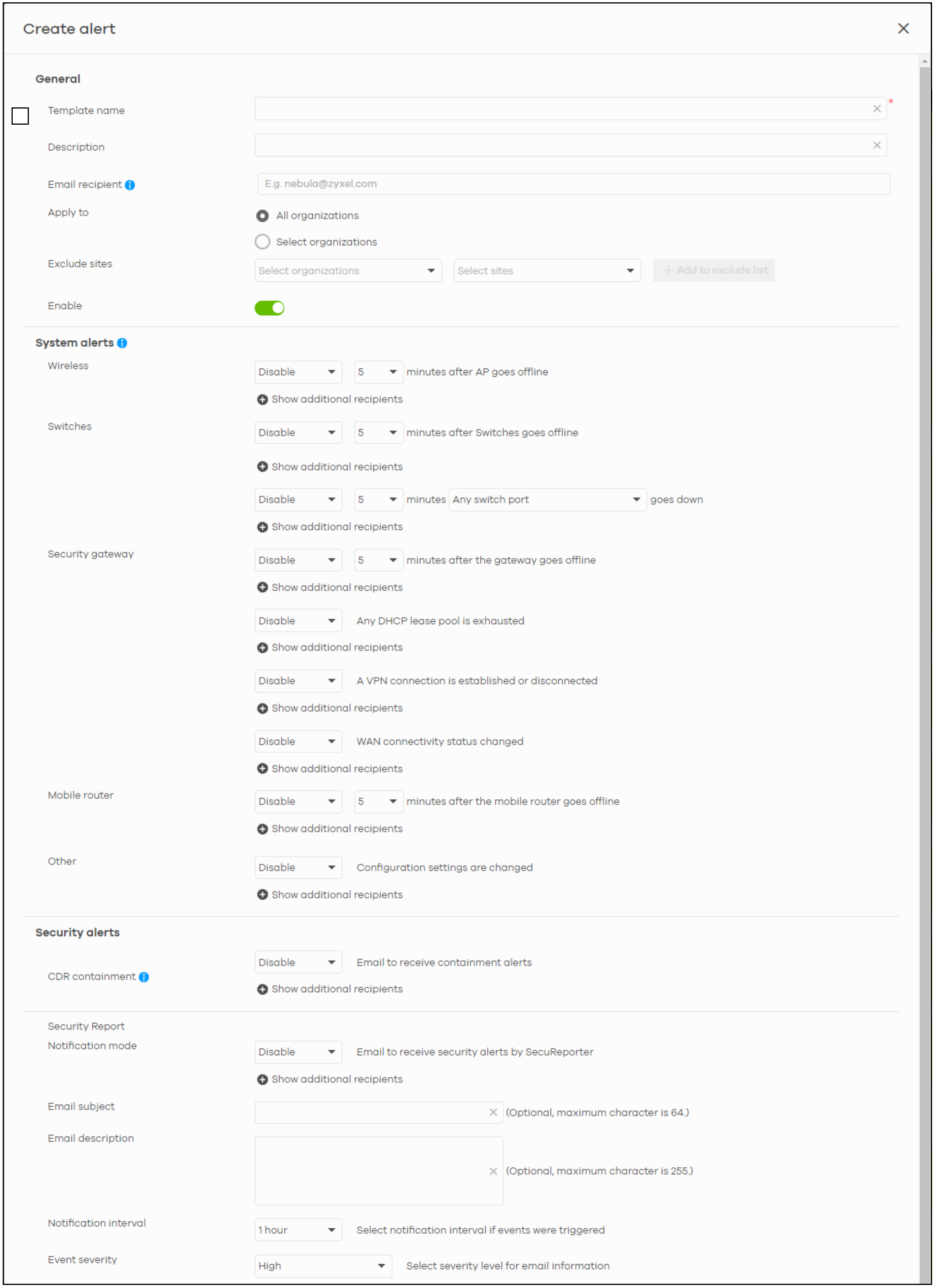
LABEL	DESCRIPTION
Search	Specify your desired search criteria to filter the list of alerts.
selected in	This shows the number of alerts that match your filter criteria after you perform a search.
Template	This shows the number of alert templates you have created.
Name	This shows a descriptive name of 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.	

13.4.1 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 234 MSP cross-org > MSP cross-org manage > Alert templates > Create/Update alert



Create alert

General

Template name *

Description

Email recipient: E.g. nebula@zyxel.com

Apply to: ● All 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

Switches
- Disable | 5 minutes after Switches goes offline
- Show additional recipients
- Disable | 5 minutes | Any switch port | goes down
- Show additional recipients

Security gateway
- 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

Other
- Disable | Configuration settings are changed
- Show additional recipients

Security alerts

CDR containment
- Disable | Email to receive containment alerts
- Show additional recipients

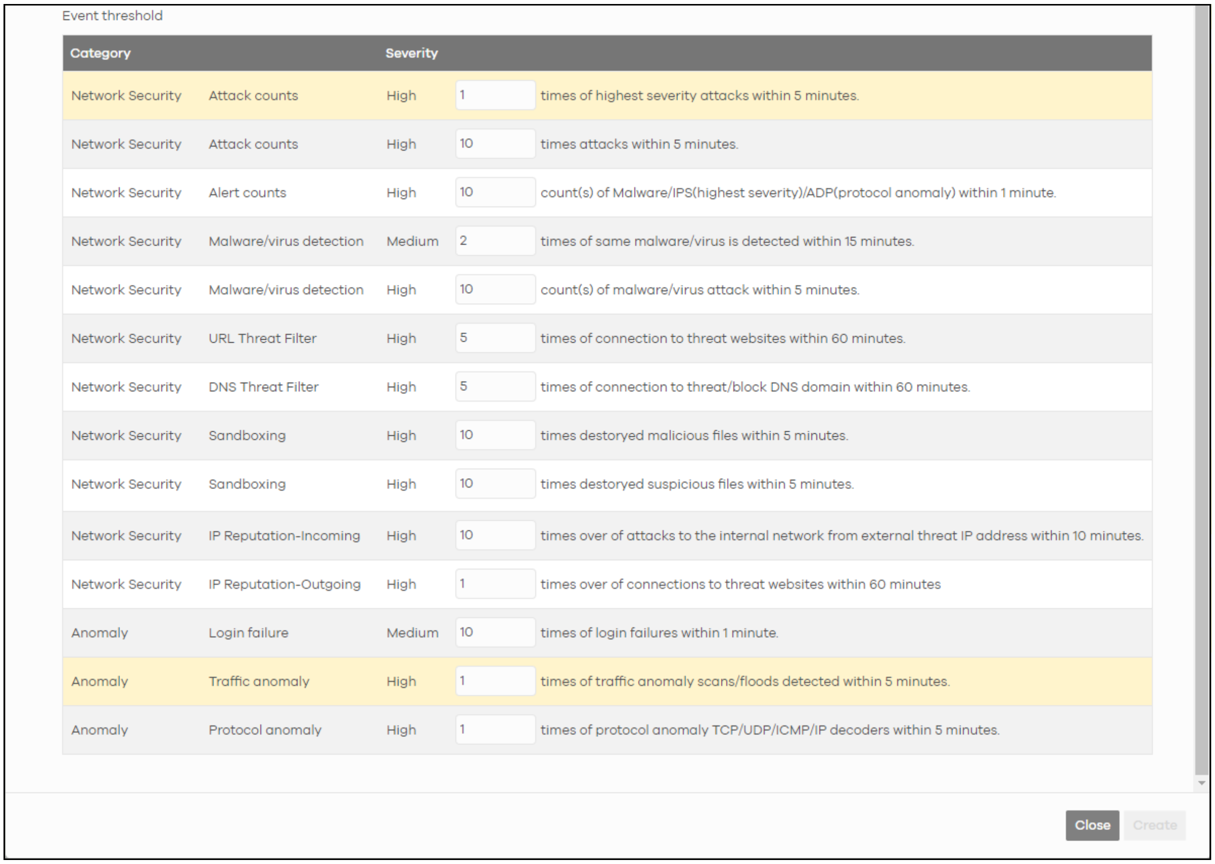
Security Report Notification mode
- Disable | Email to receive security alerts by SecuReporter
- Show additional recipients

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 destoryed malicious files within 5 minutes.
Network Security	Sandboxing	High	10	times destoryed 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 201 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).
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. Note: Recipients belonging to Base organizations will not receive email alerts, except if the recipient's account includes an MSP license. In general, only the organizations with activated MSP license will receive email alerts. For example, **ORG 1** is a Base tier organization, and **ORG 2** is a Professional tier organization. An MSP alert template is created to monitor AP offline events. If there are three email recipients in both **ORG 1** and **ORG 2** with the following licenses: • **REP 1** (recipient 1) has an account which includes an MSP license. • **REP 2** (recipient 2)and **REP 3** (recipient 3) has accounts which does not include an MSP license. When an AP offline event occurs, an email alert will only be sent to **REP 1** in **ORG 1**. While an email alert will be sent to all recipients (**REP 1**, **REP 2**, and **REP 3**) in **ORG 2**.
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.

Table 201 MSP cross-org > MSP cross-org manage > Alert templates > Create/Update alert (continued)

LABEL	DESCRIPTION
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. • **Disabled**: No alerts are sent.
Show additional recipients	Add additional user accounts who will receive email and 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.
Switches	Specify how long in minutes the NCC waits before generating and sending an alert when a port or a switch goes offline.
Security gateway	Specify how long in minutes the NCC waits before generating and sending an alert when the following events occur: • A gateway device goes offline. • Any DHCP pool on the gateway device runs out of IP addresses to assign. • A VPN connection to or from the gateway device is created or terminated. • The WAN connectivity goes offline.
Mobile router	Specify how long in minutes the NCC waits before generating and sending an alert when an mobile router 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.
Security Report	
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.

13.5 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.

13.5.1 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**

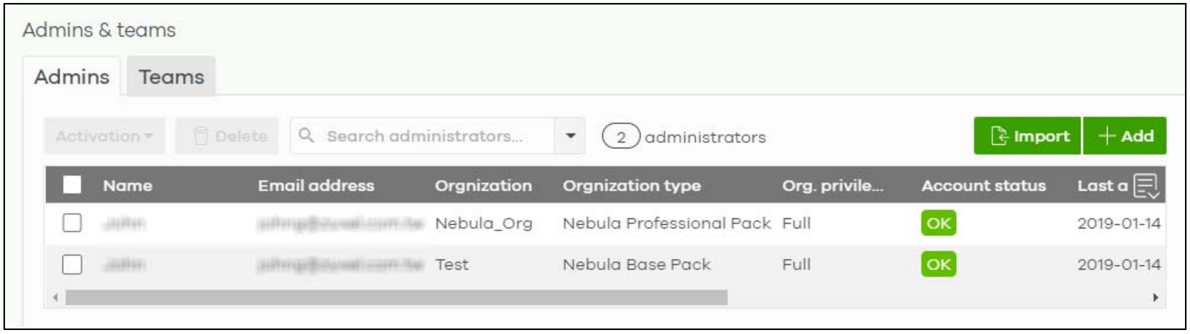
If an NCC account has different administrator privileges configured on different screens, then the highest privilege level takes priority.

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).

13.5.2 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 235 MSP cross-org > MSP cross-org manage > Admins & teams > Admins



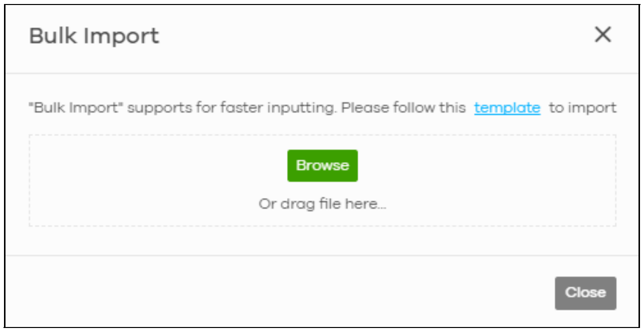
□	Name	Email address	Orgnization	Orgnization type	Org. privile...	Account status	Last a
□	[redacted]	[redacted]	Nebula_Org	Nebula Professional Pack	Full	OK	2019-01-14
□	[redacted]	[redacted]	Test	Nebula Base Pack	Full	OK	2019-01-14

The following table describes the labels in this screen.

Table 202 MSP cross-org > MSP cross-org manage > Admins & teams > Admins

LABEL	DESCRIPTION
Activation	Click this button to **Activate**/**Deactivate** the selected accounts. Then, click **Update**.
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.

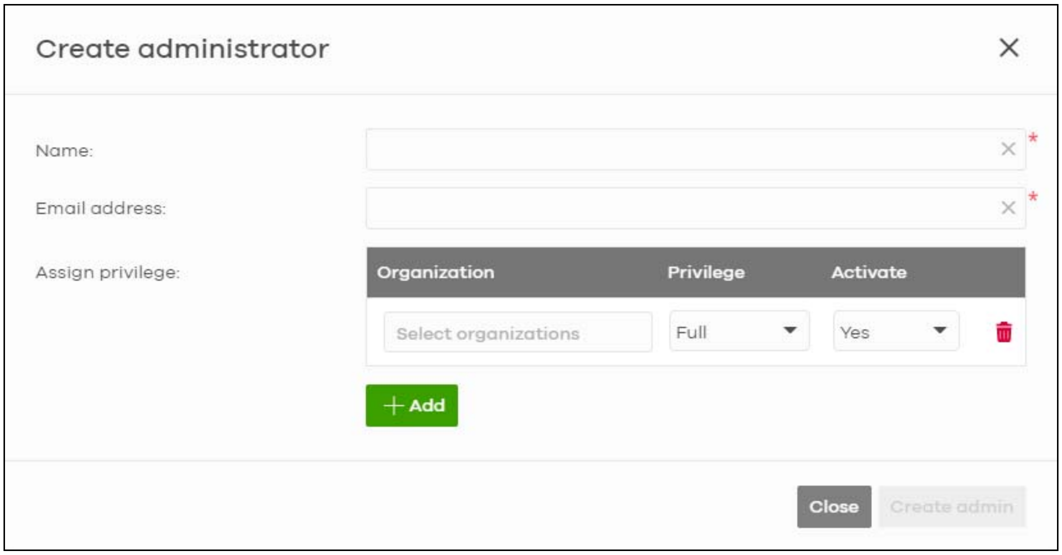
Table 202 MSP cross-org > MSP cross-org manage > Admins & teams > Admins (continued)

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 the file format.  Bulk Import "Bulk Import" supports for faster inputting. Please follow this template to import
Add	Click this button to create a new group administrator account.
Name	This shows the name of the administrator account.
Email address	This shows the email address of 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
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.

13.5.3 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.

Figure 236 MSP cross-org > MSP cross-org manage > Admins & teams > Admins: Create/Update administrator



Create administrator

Name:

Email address:

Assign privilege:

Organization	Privilege	Activate
Select organizations	Full	Yes

The following table describes the labels in this screen.

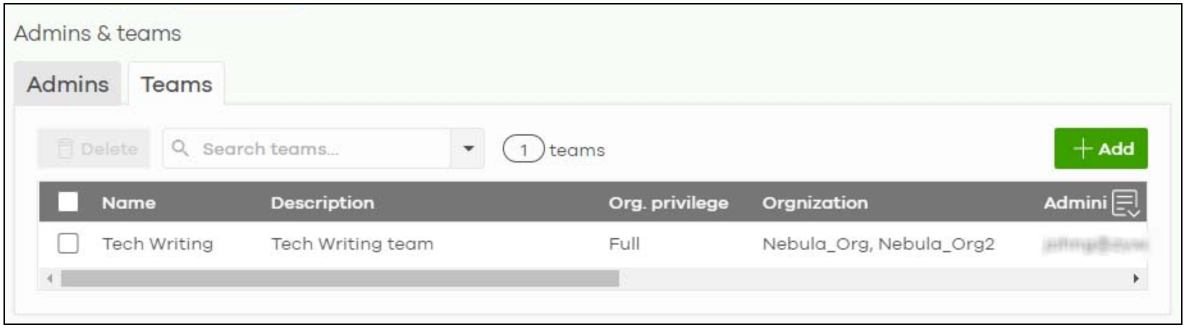
Table 203 MSP cross-org > MSP cross-org manage > Admins & teams > Admins: Create/Update administrator

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.
Assign privilege	
Organization	Select one or more organizations to assign the account privileges to. Only organizations belonging to an MSP account with full privileges can be selected. Note: If no organization is selected, then the administrator cannot access any organization until an organization is assigned full privileges.
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.
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.

13.5.4 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 237 MSP cross-org > MSP cross-org manage > Admins & teams > Teams



Admins & teams

Admins | Teams

Delete | Search teams... | 1 teams | + Add

☐	Name	Description	Org. privilege	Orgnization	Admini
☐	Tech Writing	Tech Writing team	Full	Nebula_Org, Nebula_Org2	[redacted]

The following table describes the labels in this screen.

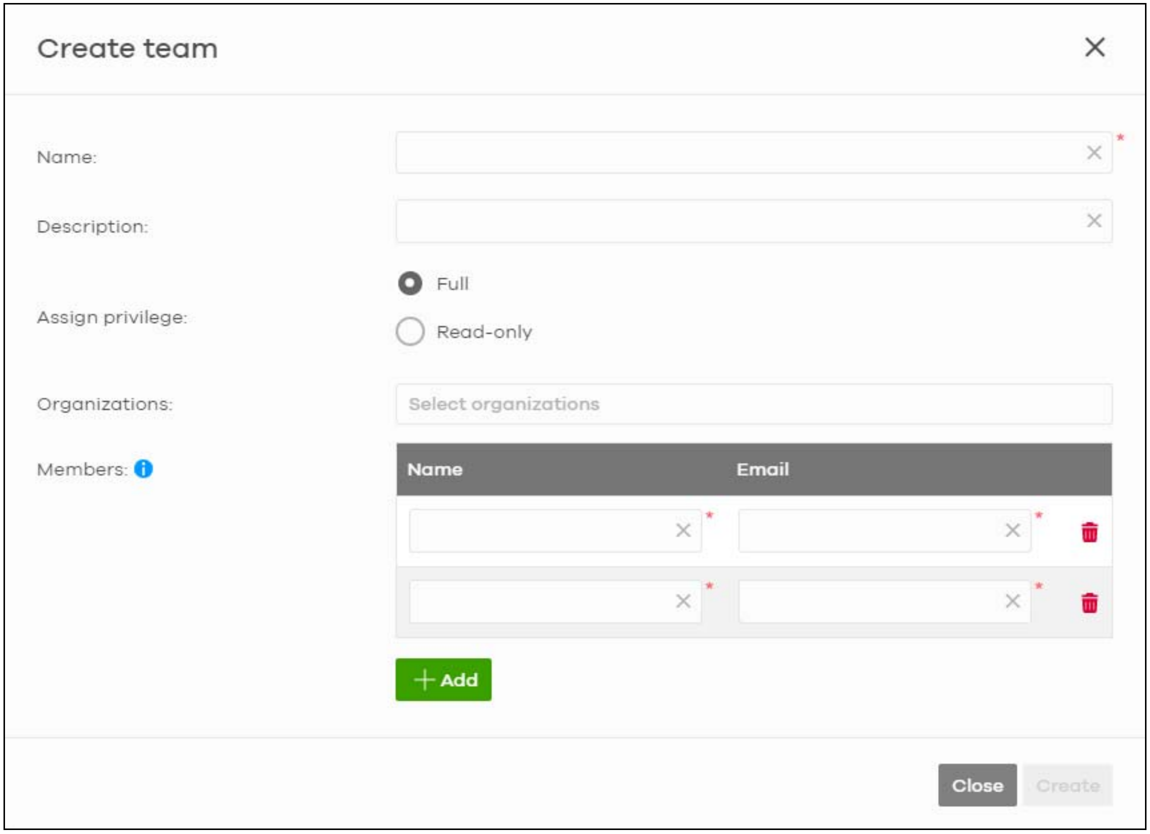
Table 204 MSP cross-org > MSP cross-org manage > Admins & teams > Teams

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 check box to select a specific team. Otherwise, select the check box 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.

13.5.5 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 238 MSP cross-org > MSP cross-org manage > Admins & teams > Teams: Create/Update team



The following table describes the labels in this screen.

Table 205 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 205   MSP cross-org > MSP cross-org manage > Admins & teams > Teams: Create/Update team

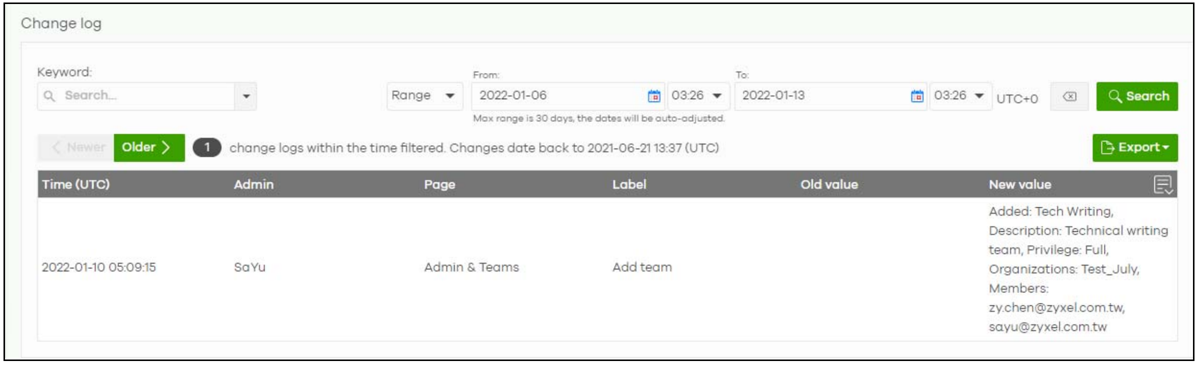
LABEL	DESCRIPTION
Close	Click this button to exit this screen without saving.
Create/Update	Click this button to save your changes and close the screen.

13.6 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 239   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 206   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

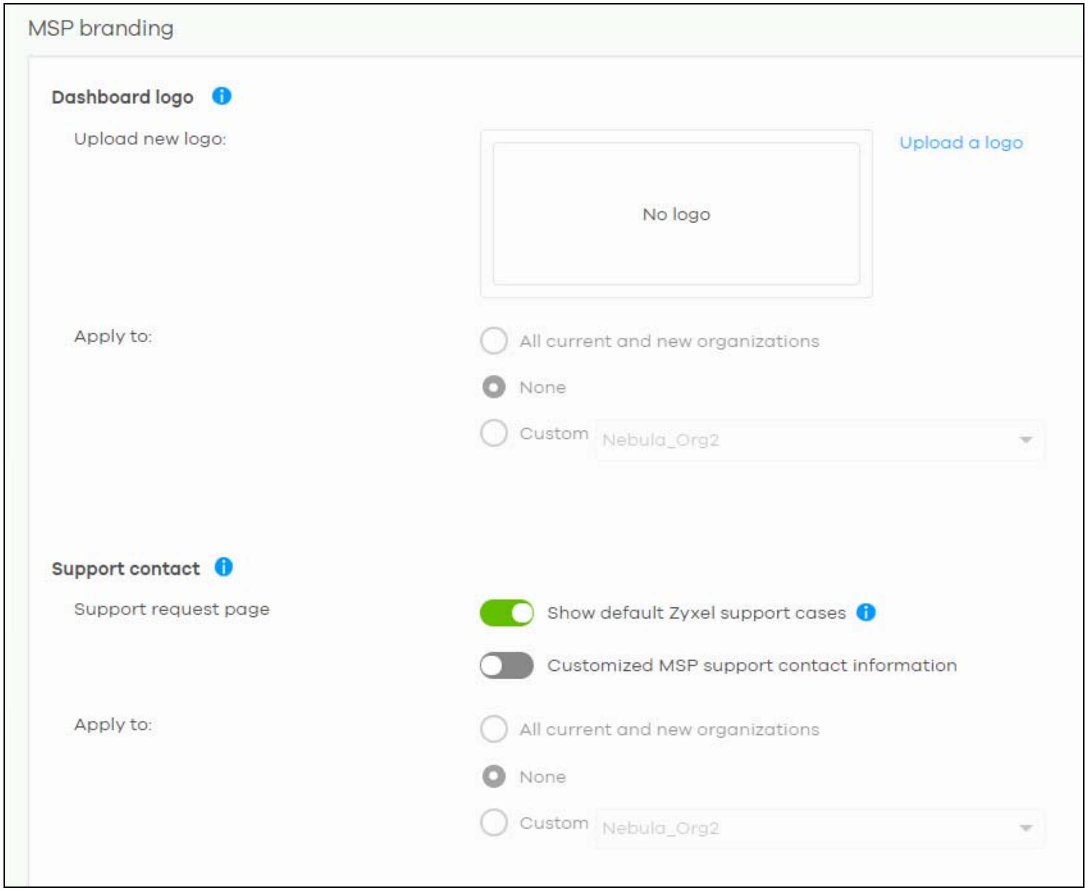
Table 206 MSP cross-org > MSP cross-org manage > Change log (continued)

LABEL	DESCRIPTION
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 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 240 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: On
Customized MSP support contact information: Off

Apply to:
○ All current and new organizations
● None
○ Custom Nebula_Org2

The following table describes the labels in this screen.

Table 207 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.
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

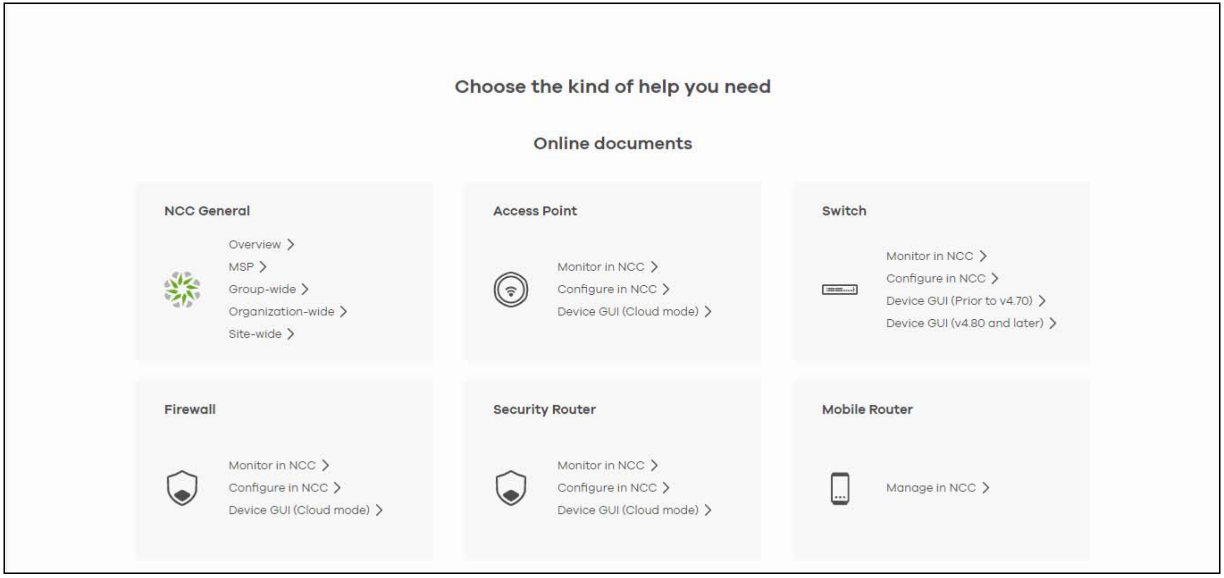
Troubleshooting and Appendices

CHAPTER 14 Help

14.1 Online documents

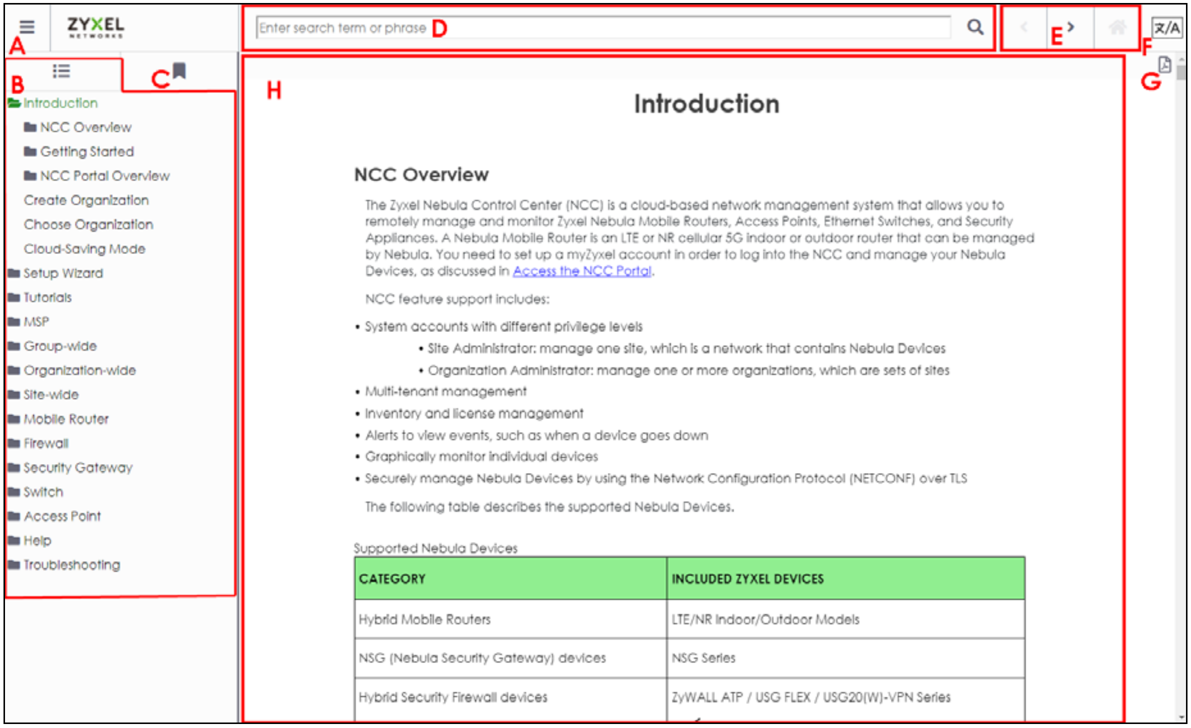
Click **Help** > **Online documents** to view the documentation for NCC and NCC-compatible devices. For example, to view the Security Firewall Series configuration and hardware information, locate the documents under **Firewall**.

Figure 241 Help > Online documents



The following summarizes how to navigate the online document screen. The online document screen is divided into these parts:

Figure 242 Online Document 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 document parts.

Table 208 Online Document 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 208 Online Document 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.

14.2 Troubleshooting Tips

To find suggestions to solve problems you might encounter with NCC and Nebula Devices, go to Chapter 15 on page 597 for more information.

14.2.1 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.

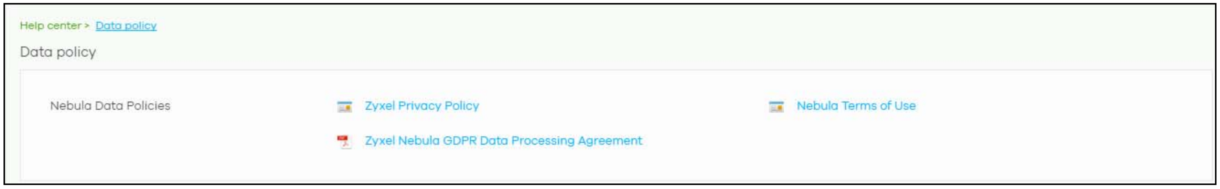
Table 209 Sample Information Required for Firewall Rules

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

14.2.2 Data Policy

Click **Help** > **Support tools** > **Data Policy** to view and download NCC GDPR data policy, privacy policy, and terms of use.

Figure 243 Help > Support tools > Data Policy



Help center > Data policy

Data policy

Nebula Data Policies

Zyxel Privacy Policy

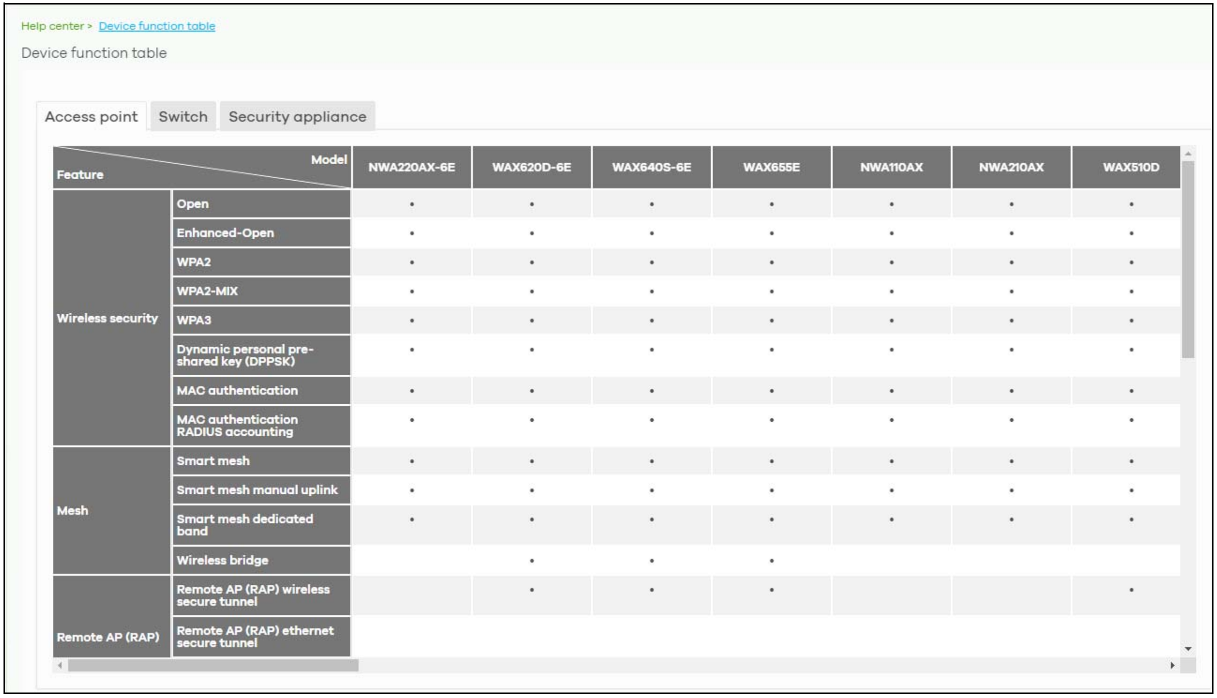
Zyxel Nebula GDPR Data Processing Agreement

Nebula Terms of Use

14.3 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 244 Help > Support tools > 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							

14.4 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.

14.5 Support Request

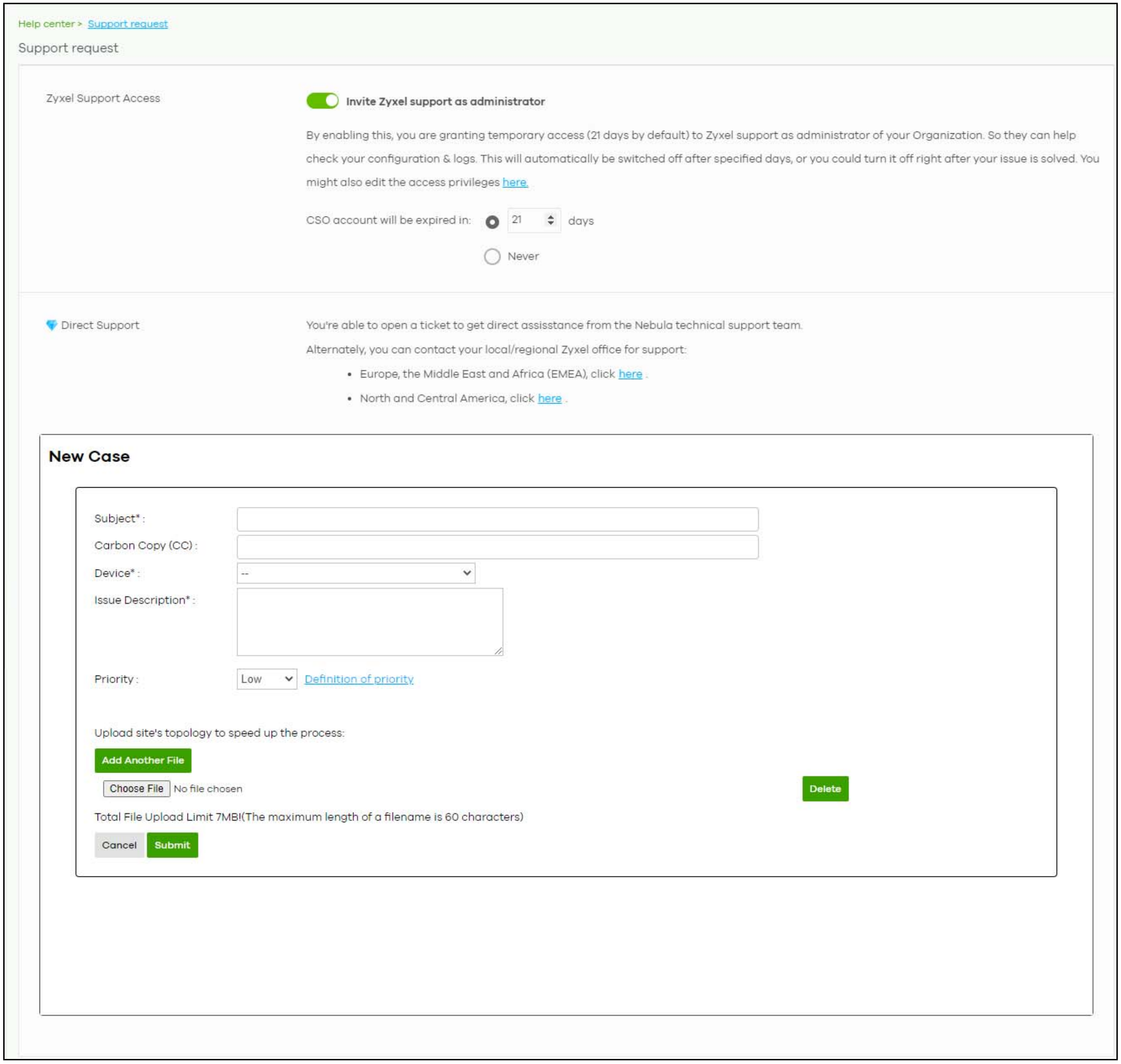
If you need Zyxel customer support to help you find answers and/or solve problems, you can submit a ticket through the NCC.

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 245 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 210   Help > Still need help?: Support Request

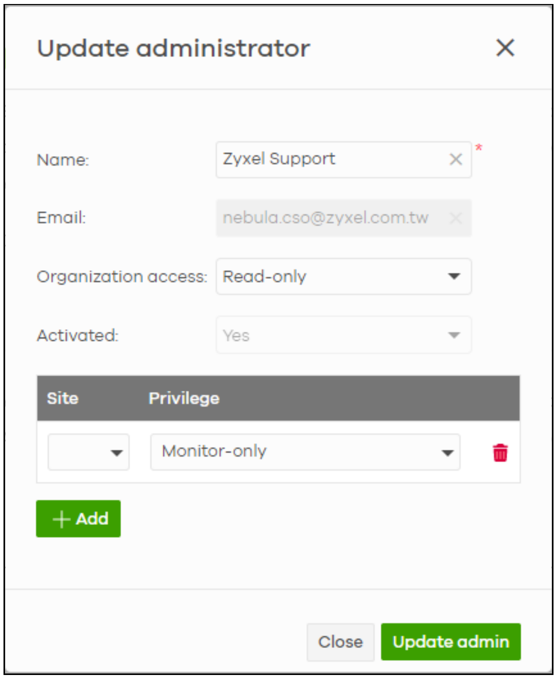
LABEL	DESCRIPTION
Zyxel Support Access Invite Zyxel support as administrator	Select **ON** to allow the Zyxel customer support account to access your organization temporarily, so that they can help check your configurations and log messages. At the time of writing, the support account will be deactivated 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 + Add Close · Update admin
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 210 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 15
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 471 for more information.
- To know how to monitor Security Appliances in NCC, go to Section 8.2 on page 342 (Security Firewalls) or Section 9.2 on page 414 (Security Gateways) for more information.
- To know how to configure Security Appliances in NCC, go to Section 8.3 on page 350 (Security Firewalls) or Section 9.3 on page 422 (Security Gateways) for more information.
- To know how to monitor Switches in NCC, go to Section 6.2 on page 276 for more information.
- To know how to configure Switches in NCC, go to Section 6.3 on page 288 for more information.
- To know how to monitor Access Points in NCC, go to Section 5.2 on page 235 for more information.
- To know how to configure Access Points in NCC, go to Section 5.3 on page 247 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 myZyxel account and create an account.

I cannot access a Nebula Device that I have registered 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.
- 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 2.1.7.1 on page 51 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 2.1.7.2 on page 51 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** > **Firewall**
  - **Site-wide** > **Devices** > **Security gateway**
  - **Site-wide** > **Devices** > **Access points**

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.

I cannot see my Nebula Devices in the NCC Dashboard or the corresponding Nebula Device monitor page.

- If your Nebula Device is a Zyxel Hybrid Switch (GS / XGS / XMG / XS Series), make sure that the Nebula Device is working in Nebula cloud management mode with NCC Discovery enabled.
  - For the Web Configurator version 4.70:
    Active is enabled in **Basic Setting** > **Cloud Management** > **Nebula Control Center Discovery**.
  - For the Web Configurator version 4.80:
    Nebula Control Center (NCC) Discovery is enabled in **SYSTEM** > **Cloud Management**.
- 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 11.2.1 on page 492.
- Make sure that you have created an organization and site and add the Nebula Devices to the site. See Create Organization on page 43.

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 14 on page 161.
- The maximum number of Remote Access points depends on the Nebula Security Firewall.

Table 211 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 271 for more information.

Note: For more information about smart mesh, see Section 5.1.1 on page 233.

The mesh extender does not broadcast the mesh controller SSID.

- Make sure you enable **Downlink** in **Site-wide** > **Monitor** > **Access points**: **Details**. See Section 4.3.1.1 on page 159 for more information.

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.

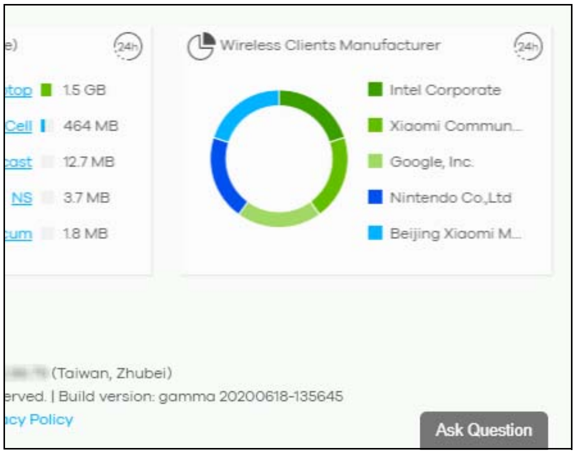
- The Nebula Device has a power-related error. Disconnect and reconnect the power cord. Make sure that you are using the included power cord for the Nebula Device and it is plugged into an appropriate power source. See the related Quick Start Guide.
- If the LED is still red, you may have a hardware problem. In this case, you should contact your local customer support.

15.1 Getting More Troubleshooting Help

Go to *support.zyxel.com* at the Zyxel website for other technical information on the NCC.

15.2 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

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