

# User's Guide

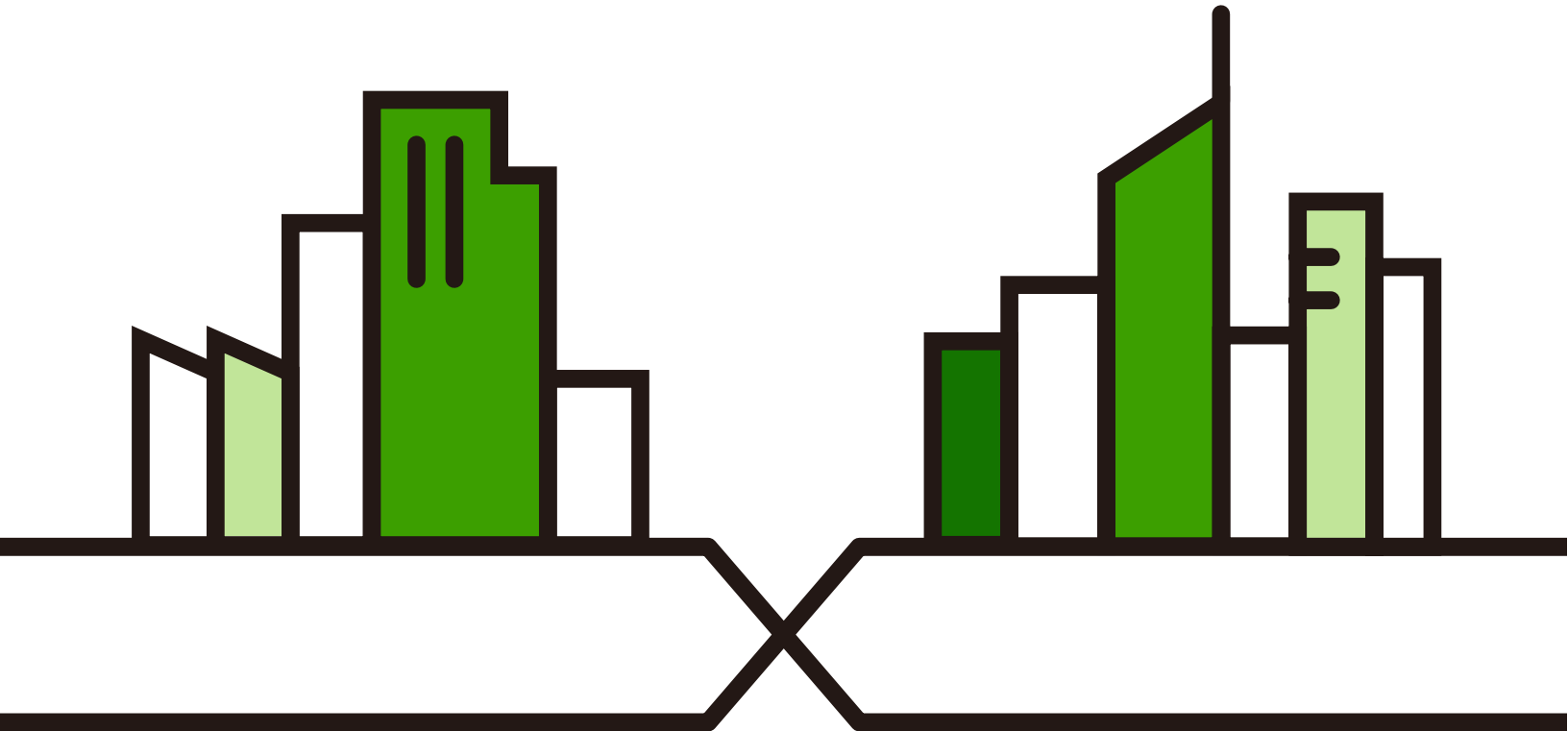
## NCC

Nebula Control Center

### Default Login Details

NCC URL	<a href="https://nebula.zyxel.com">https://nebula.zyxel.com</a>
User Name	myZyxel account name
Password	myZyxel account password

Version 16.00 Edition 1, 01/2023



---

**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

<b>Table of Contents</b> .....	<b>3</b>
<b>Part I: Introduction &amp; Getting Started Tutorials</b> .....	<b>11</b>
<b>Chapter 1</b>	
<b>Introduction</b> .....	<b>12</b>
1.1 NCC Overview .....	12
1.1.1 MSP (Managed Services Provider) Portal .....	13
1.1.2 Groups, Organizations, and Sites .....	13
1.1.3 Mobile Router, Firewall (Security Appliance), Switch, and Access Point .....	14
1.1.4 License Concept .....	14
1.2 Getting Started .....	22
1.2.1 Connect Nebula Managed Devices .....	23
1.2.2 Access the NCC Portal .....	23
1.3 NCC Portal Overview .....	29
1.3.1 Title Bar .....	30
1.3.2 Navigation Panel .....	35
1.4 Create Organization .....	42
1.5 Choose Organization .....	43
1.6 Cloud-Saving Mode .....	44
<b>Chapter 2</b>	
<b>Setup Wizard</b> .....	<b>45</b>
2.1 Setup Wizard .....	45
2.1.1 Step 1: Run the Wizard .....	45
2.1.2 Step 2: Create an Organization and Site .....	46
2.1.3 Step 3: Add Your Nebula Devices .....	47
2.1.4 Step 4: Upgrade your Nebula Device Firmware .....	48
2.1.5 Step 5: Set up your WiFi Network .....	48
2.1.6 Step 6: Set up a Guest WiFi Network .....	49
2.1.7 Step 7: Set up the Deployment Method .....	50
2.1.8 Step 8: View the Summary .....	53
2.1.9 Step 9: Activate the Trial License(s) .....	54
<b>Chapter 3</b>	
<b>Tutorials</b> .....	<b>56</b>
3.1 Overview .....	56
3.2 Add a Nebula Device .....	57

3.3 Activate and Assign a License for a Nebula Device, Site, or Organization .....	57
3.3.1 Bundled License and Add-on License .....	58
3.3.2 License States .....	58
3.3.3 License Activation Process .....	58
3.4 Monitor a Site .....	60
3.5 Know What Licenses are Set to Expire in My Site or Organization .....	61
3.6 Renew an Expired License .....	62
3.7 Transfer Licenses .....	63
3.7.1 Select Transferable Licenses .....	63
3.7.2 Undo Assigning a License .....	64
3.7.3 Transfer a License to a Different Organization .....	65
3.7.4 Assign a License to a Nebula Device in the New Organization .....	66
3.7.5 Transfer a License to a Nebula Device in a New Organization .....	68
3.8 Reset the Nebula Password .....	69
3.9 Change an Organization and/or Site Name .....	73
3.10 Maintain Firmware .....	74
3.11 Assign an Administrator to Manage a Nebula Device .....	76
3.12 Transfer the Ownership of the Organization .....	78
3.13 Manage a Configuration Template .....	79
3.13.1 Create and Bind a Template Site/Setting .....	79
3.13.2 Duplicate and Import a Template Setting to a Site .....	83
3.13.3 Enable the Override Site-wide Configuration (Local Override) Feature .....	89
3.14 Activate an MSP License .....	93
3.15 Configure CNP/CNP Plus Security Services .....	93
3.15.1 Threat Protection .....	94
3.15.2 Application Visibility & Optimization .....	95
3.16 Delete an Organization .....	97
3.16.1 Remove All Nebula Devices .....	97
3.16.2 Transfer All Licenses .....	98
3.16.3 Delete All Sites .....	98
3.16.4 Delete All Administrators .....	99
3.16.5 Remove All Users .....	100
3.16.6 Delete the Organization .....	100
3.17 Remote Access VPN Setup .....	101
3.17.1 Create a VPN User .....	102
3.17.2 Enable the Remote Access VPN Rule for IPSec VPN Client .....	103
3.17.3 VPN Setup by the VPN Client .....	105
3.17.4 Import the VPN Configuration File .....	105
3.17.5 Open the VPN Tunnel .....	108
3.17.6 Set Up Two Factor Authentication to Bind the User Account .....	110
3.17.7 Check the Connection in Nebula by the Administrator .....	112
3.18 Route L2TP VPN Traffic .....	113
3.19 Resolve WiFi Connection Problems (for Nebula APs only) .....	115

3.20 Configure Voice VLAN (for Nebula Switches only) .....	122
3.20.1 Configure the Nebula Device Ports .....	123
3.20.2 Configure the Voice VLAN .....	124
3.21 Manage IPTV (for Nebula Switches only) .....	125
3.21.1 Set up the VLAN for IPTV .....	125
3.21.2 Define the Role of a Switch .....	126
3.21.3 Configure the Channel Profile and Naming .....	128
3.22 Enable IP Source Guard (for Nebula Switches only) .....	131
3.23 Set Up MAC Authentication With NCAS (for Nebula Switches only) .....	136
3.24 Set Up Dynamic VLAN With RADIUS (for Nebula Switches only) .....	137
3.25 Monitor Dynamic VLAN Using Event Logs (for Nebula Switches only) .....	139
3.26 Register a Nebula Device (mobile router) in Nebula .....	140
3.27 Using Collaborative Detection and Response (CDR) .....	141
3.28 Deploy With Nebula Native Mode (for Security Firewalls in Nebula) .....	143
3.29 Configure DHCP Domain Name (for Security Firewalls in Nebula) .....	148

**Part II: MSP ..... 152**

**Chapter 4  
MSP ..... 153**

4.1 Overview .....	153
4.2 MSP Portal .....	153
4.3 Change Log .....	157
4.4 Create Organization .....	158
4.5 MSP Branding .....	159
4.6 Admins & Teams .....	160
4.6.1 Admins Screen .....	160
4.6.2 Teams Screen .....	163
4.6.3 Cross-org synchronization .....	166
4.7 MSP Alert Template .....	168
4.7.1 Alert Settings .....	169

**Part III: Manage by Deployment: Group, Organization, Site..... 173**

**Chapter 5  
Group-wide ..... 174**

5.1 Introduction .....	174
5.1.1 Creating a Group .....	174
5.1.2 Group-Wide Menu .....	175
5.2 Monitor .....	175

5.2.1 Overview .....	175
5.2.2 Inventory .....	176
5.2.3 Change Log .....	177
5.3 Configure .....	179
5.3.1 Group Settings .....	179
5.3.2 Org-to-Org VPN .....	180
5.3.3 Administrators .....	183
<b>Chapter 6</b>	
<b>Organization-wide .....</b>	<b>187</b>
6.1 Overview .....	187
6.2 Monitor .....	187
6.2.1 Organization Overview .....	187
6.2.2 Change Log .....	191
6.3 Configure .....	192
6.3.1 Organization Settings .....	192
6.3.2 Create Site .....	194
6.3.3 License & Inventory .....	195
6.3.4 Administrators .....	212
6.3.5 Cloud Authentication .....	216
6.3.6 Configuration Management .....	227
6.3.7 Configuration Template .....	230
6.3.8 Security Profile Sync .....	233
6.3.9 VPN Orchestrator .....	241
6.3.10 Firmware Management .....	245
<b>Chapter 7</b>	
<b>Site-wide .....</b>	<b>252</b>
7.1 Monitor .....	252
7.1.1 Dashboard .....	252
7.1.2 Clients .....	255
7.1.3 WiFi Aid .....	260
7.1.4 Connection Log .....	262
7.1.5 Containment List .....	263
7.1.6 Map & Floor Plans .....	264
7.1.7 Topology .....	266
7.1.8 Vouchers .....	267
7.1.9 Cloud Intelligence Logs .....	269
7.1.10 Summary Report .....	271
7.1.11 Applications .....	274
7.2 Configure .....	276
7.2.1 General Settings .....	277
7.2.2 Collaborative Detection & Response .....	280

7.2.3 Quarantine Interface Configuration .....	284
7.2.4 Alert Settings .....	285
7.2.5 Add Devices .....	288
7.2.6 Firmware Management .....	289
7.2.7 Cloud Authentication .....	296

**Part IV: Manage by Device Type ..... 303**

**Chapter 8  
Mobile Router .....304**

8.1 Overview .....	304
8.2 Configuration .....	304
8.2.1 Configuration: Edit .....	305
8.2.2 Home Networking .....	306
8.2.3 Cellular IP Passthrough .....	307
8.2.4 Firmware Status .....	309
8.3 Map/Photo .....	310
8.4 Live Tools .....	311
8.4.1 WAN Status .....	312
8.4.2 Cellular Info .....	313
8.4.3 LAN Stations .....	319
8.4.4 WLAN Stations .....	320
8.5 Backup & Restore .....	321
8.6 Network Usage and Connectivity .....	321

**Chapter 9  
Firewall .....323**

9.1 Overview .....	323
9.2 Monitor .....	323
9.2.1 Firewall .....	323
9.2.2 Clients .....	327
9.2.3 Event Log .....	327
9.2.4 VPN Connections .....	327
9.2.5 SecuReporter .....	329
9.2.6 Summary Report .....	330
9.3 Configure .....	335
9.3.1 Port .....	335
9.3.2 Interface .....	336
9.3.3 Routing .....	344
9.3.4 NAT .....	348
9.3.5 Site-to-Site VPN .....	350

---

9.3.6 Remote Access VPN .....	356
9.3.7 Security Policy .....	361
9.3.8 Security Service .....	369
9.3.9 Captive Portal .....	383
9.3.10 Authentication Method .....	386
9.3.11 Wireless .....	387
9.3.12 Firewall Settings .....	389
<b>Chapter 10</b>	
<b>Security Gateway .....</b>	<b>398</b>
10.1 Overview .....	398
10.2 Monitor .....	398
10.2.1 Security Appliance .....	398
10.2.2 Clients .....	401
10.2.3 Event Log .....	402
10.2.4 VPN Connections .....	402
10.2.5 NSS Analysis Report .....	404
10.2.6 Summary Report .....	406
10.3 Configure .....	409
10.3.1 Interface Addressing .....	409
10.3.2 Link Aggregation Groups .....	417
10.3.3 Policy Route .....	425
10.3.4 Firewall .....	426
10.3.5 Security Service .....	433
10.3.6 Site-to-Site VPN .....	436
10.3.7 Remote Access VPN .....	443
10.3.8 Captive Portal .....	445
10.3.9 Network Access Method .....	449
10.3.10 Traffic Shaping .....	450
10.3.11 Gateway Settings .....	453
<b>Chapter 11</b>	
<b>Switch .....</b>	<b>458</b>
11.1 Overview .....	458
11.2 Monitor .....	458
11.2.1 Switches .....	458
11.2.2 Clients .....	471
11.2.3 Event Log .....	471
11.2.4 IPTV Report .....	471
11.2.5 Surveillance .....	477
11.2.6 Surveillance Port Details .....	478
11.2.7 Summary Report .....	480
11.3 Configure .....	482



11.3.1 Switch Ports .....	482
11.3.2 ACL .....	490
11.3.3 IP & Routing .....	491
11.3.4 ONVIF Discovery .....	494
11.3.5 Advanced IGMP .....	496
11.3.6 Authentication .....	500
11.3.7 PoE Schedules .....	503
11.3.8 Switch Settings .....	504
<b>Chapter 12</b>	
<b>Access Point .....</b>	<b>510</b>
12.1 Overview .....	510
12.1.1 Nebula Smart Mesh .....	510
12.1.2 Smart Mesh Network Topology .....	511
12.2 Monitor .....	512
12.2.1 Access Points .....	512
12.2.2 Clients .....	524
12.2.3 Event Log .....	530
12.2.4 Wireless Health .....	530
12.2.5 Summary Report .....	534
12.3 Configure .....	538
12.3.1 SSID Settings .....	538
12.3.2 SSID Advanced Settings .....	540
12.3.3 Captive Portal Customization .....	549
12.3.4 SSID Availability .....	553
12.3.5 Radio Settings .....	554
12.3.6 Traffic Shaping .....	560
12.3.7 Security Service .....	561
12.3.8 AP & Port Settings .....	564
<b>Chapter 13</b>	
<b>Help .....</b>	<b>569</b>
13.1 Online documents .....	569
13.2 Troubleshooting Tips .....	571
13.2.1 Firewall Information .....	571
13.2.2 Data Policy .....	571
13.3 Device Function Table .....	572
13.4 Support Forum .....	572
13.5 Support Request .....	572
<b>Part V: Troubleshooting and Appendices .....</b>	<b>576</b>

<b>Chapter 14</b>	
<b>Troubleshooting</b> .....	<b>577</b>
14.1 Getting More Troubleshooting Help .....	581
14.2 NCC Live Chat .....	581
Appendix A Customer Support .....	582
Appendix B Legal Information .....	587
<b>Index</b> .....	<b>588</b>

---

# 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 23](#).

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
NSG (Nebula Security Gateway) devices	NSG Series
Hybrid Security Firewall devices	ZyWALL ATP / USG FLEX / USG20(W)-VPN Series  Note: The following Nebula Devices do NOT have a P1 port: <ul style="list-style-type: none"><li>• USG FLEX 50</li><li>• USG FLEX 100 rev 2.0</li><li>• ATP100 rev 2.0</li></ul>
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.

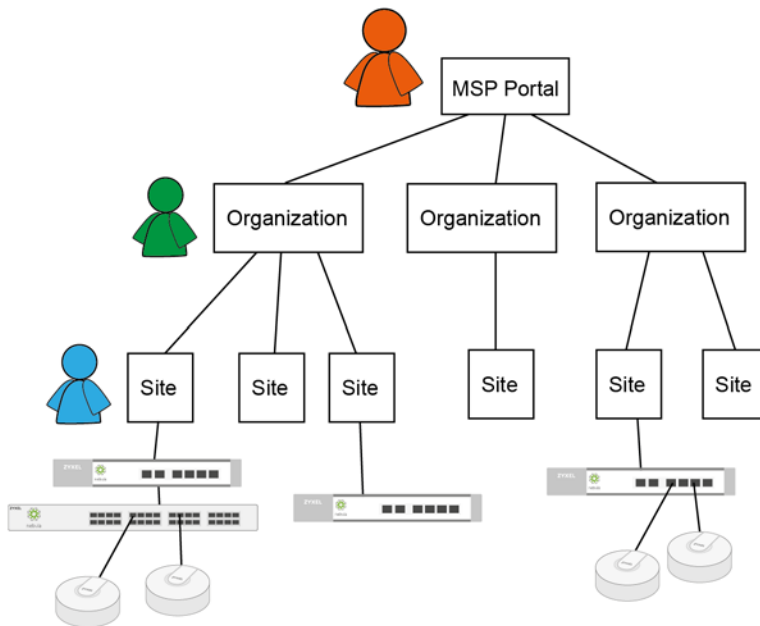
When the hybrid device is in Nebula cloud management mode, it can be managed and provisioned by the Zyxel Nebula Control Center (NCC).

### 1.1.1 MSP (Managed Services Provider) Portal

If you have an MSP license (as discussed in [Section 4.1 on page 153](#)), 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 Groups, Organizations, and Sites

To manage by how Nebula Devices are deployed, use the [Group-wide](#), [Organization-wide](#), and [Site-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.

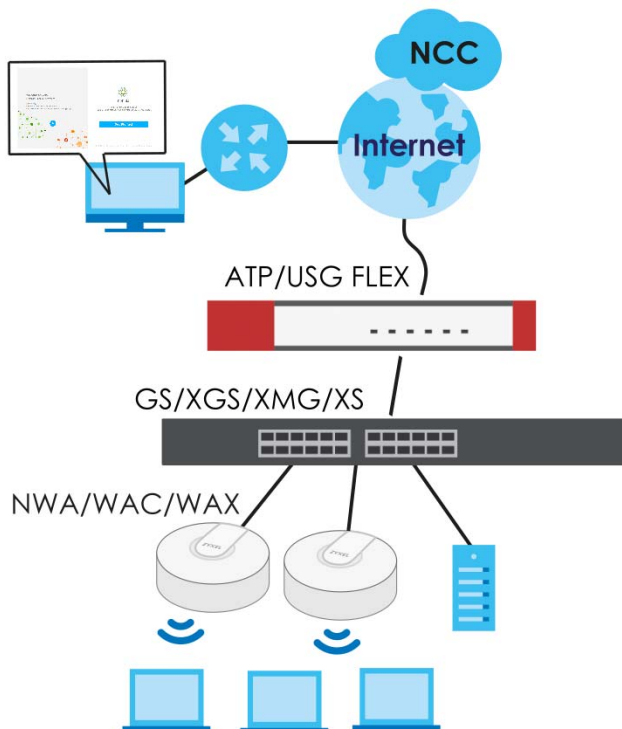
- A site can be managed by more than one site or organization administrator.
- An organization can contain multiple sites and can be managed by more than one organization administrator.
- A myZyxel.com account can be an organization administrator and/or site administrator in the NCC (see [Section 6.3.4 on page 212](#)).
- A site administrator can manage more than one site.

### 1.1.3 Mobile Router, Firewall (Security Appliance), Switch, and Access Point

To manage by Nebula Device type, use the [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 <a href="#">Section 1.1.4.2 on page 16</a> .
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 <a href="#">Section 1.1.4.2 on page 16</a> .
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 <b>More &gt; My devices &amp; services &gt; Services: Activate trial for MSP</b> .  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 <b>Nebula Professional Pack</b> and <b>Nebula Security Pack (NSS)</b> 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 <a href="#">Section 6.3.8 on page 233</a> 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 <a href="#">Section 1.1.4.2 on page 16</a> .
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 application visibility and threat protection using DNS and IP reputation filters.

### 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 > Monitor > Change log	
Login IPv4 address ranges for an organization	No	No	Yes	Organization-wide > Configure > Settings	
Number of admin accounts	5	8	Unlimited	Organization-wide > Configure > Administrators	
Number of cloud authentication accounts	50	100	Unlimited	Organization-wide > Configure > Cloud authentication	
Cloud authentication users with VLAN attribute	No	No	Yes	Organization-wide > Configure > Cloud authentication (Account type: User)	
Cloud Authentication DPPSK account type	No	No	Yes	Organization-wide > Configure > Cloud authentication (Account type: DPPSK)	
New site configuration clone	No	No	Yes	Organization-wide > Configure > Create site	
Site-wide settings sync	No	No	Yes	Organization-wide > Configure > Configuration management	
Switch settings clone	No	No	Yes	Organization-wide > Configure > Configuration management	
Site/Switch configuration backup and restore	No	No	Yes	Organization-wide > Configure > Configuration management	
Configuration templates	No	No	Yes	Organization-wide > Configure > 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 > Monitor > Clients	
WiFi aid	No	No	Yes	Site-wide > Monitor > Clients	

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
Connection log	No	No	Yes	Site-wide > Monitor > Clients Access point > Monitor > Clients	
Site-wide topology	No	Yes	Yes	Site-wide > Monitor > Topology	
Summary report email & schedule	No	Yes	Yes	Site-wide / Access point / Switch / Security gateway / Firewall > Monitor > Summary report	
Time period for summary reports	24 hours	7 days	365 days	Site-wide / Access point / Switch / Security gateway / Firewall > Monitor > Summary report	
Time period for device monitoring statistics	24 hours	7 days	365 days	Access point / Switch / Security gateway / Firewall > Monitor > Access Points / Switches / Security gateway / Firewall > [Select Access Points / Switches]	
Time period for client monitoring statistics	24 hours	7 days	365 days	Access point / Switch / Security gateway / Firewall > Monitor > Clients > [Select client]	
Time period for device event log access	24 hours	7 days	365 days	Access point / Switch / Security gateway / Firewall > Monitor > Event log	
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 > General 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	
Org-wide firmware upgrade	No	Yes	Yes	Organization-wide > Configure > Firmware management	

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
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	Device (for example, Access point) > Monitor > Device (for example, Access points) > [Select Device for example, AP] > Photo	
Remote CLI access	No	No	Yes	Access point / Security gateway / Firewall > Monitor > Access Points / Security gateway / Firewall [Select AP] Live tools	
Wireless health monitor and report	No	No	Yes	Access point > Monitor > Wireless health	
Programmable SSID/PSK	No	No	Yes	Access point > Configure > SSID settings	
Dynamic Personal Pre-Shared Key (DPPSK)	No	No	Yes	Access point > Configure > SSID advanced settings	
Vouchers as WiFi authentication credentials	No	Yes	Yes	Site-wide > Monitor > Vouchers  Site-wide > Configure > General settings  Access point > Configure > SSID advanced settings  Access point > Configure > Captive portal customization > [portal theme]	
Facebook WiFi	Configure in NCC	No	Yes	Access point > Configure > SSID advanced settings	
RADIUS accounting for captive portal	No	No	Yes	Access point > Configure > SSID advanced settings	
Customize RADIUS NAS ID	No	No	Yes	Access point > Configure > SSID advanced settings	
Customize portal redirect URL parameter	No	No	Yes	Access point > Configure > Captive portal customization	

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
Smart steering per AP	No	No	Yes	Access point > Configure > Radio settings > [Edit the selected Access Point]	
Bandwidth Management by VLAN interface	No	No	Yes	Access point > Configure > Traffic shaping	Currently supported on NWA1123ACv3, WAC500, WAC500H, NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, WAX650S
AP traffic log	No	No	Yes	Site-wide > Configure > General settings	
IPTV report	No	No	Yes	Switch > Monitor > IPTV report	
Advanced IGMP	No	No	Yes	Switch > Configure > Advanced IGMP	
Switch Surveillance Monitoring with ONVIF	No	No	Yes	Switch > Monitor > Surveillance	Currently only supported on GS1350 series switches
Extended PoE range	Yes	Yes	Yes	Switch > Configure > Switch ports > [select port]	Currently only supported on GS1350 series switches
Automatic PoE device recovery	No	Yes	Yes	Switch > Configure > Switch ports > [select port]	Currently only supported on GS1350, GS2220 and XGS2220 series switches
Port bandwidth control	Yes	Yes	Yes	Switch > Configure > Switch ports > [edit the selected port]	
Vendor ID-based VLAN	No	Yes	Yes	Switch > Configure > Switch settings	
IP interface and static route	No	No	Yes	Switch > Configure > IP & Routing	
Remote SSH in Live tools	No	No	Yes	Switch > Monitor > Switches: Switch Details > Live tools > Remote Access	Currently only supported on XS3800-28 and XGS2220 series v4.80 switches
IP Source Guard	No	No	Yes	Switch > Configure > Switch settings	Currently only supported on XS3800-28 and XGS2220 series v4.80 switches
Nebula cloud authentication	Yes	Yes	Yes	Switch > Configure > Authentication	Currently only supported on XGS1930 series v4.70 patch 5 switches

Table 3 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PROFESSIONAL	LOCATION	NOTES
IGMP report proxy	No	No	Yes	Switch > Configure > Advanced IGMP	Currently not supported on GS1915 series switches
Time period for security service (AV/App Patrol/CF/IDP/NSS) analysis report	24 hours	7 days	365 days	Security gateway > Monitor > NSS analysis report	Requires Nebula Security Gateway (NSG) Nebula Security Service (NSS) – Security Pack (SP) license
Traffic log archiving	No	No	Yes	Firewall > Monitor > SecuReporter	
VPN topology with traffic usage	No	No	Yes	Organization-wide > Configure > VPN Orchestrator	
Smart VPN	No	No	Yes	Organization-wide > Configure > VPN Orchestrator	
VPN provision script email	No	No	Yes	Security gateway / Firewall > Configure > 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	Access point > Monitor > Access points	Currently supported on NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S, WAX650S, NWA1123ACv3, WAC500, and WAC500H APs
Traffic logs to SecuReporter	No	No	Yes	Site-wide > Configure > General settings	Also available for Gold Security Pack, UTM Security Pack, and Content Filter Pack
Cellular IP Passthrough	No	No	Yes	Mobile Router > Configuration	Currently only supported on NR7101 and LTE7461
Remote configurator in Live tools	No	No	Yes	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 > Configure > License & inventory > License** and then click **+Add**. See [Section 6.3.3.7 on page 205](#) 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.

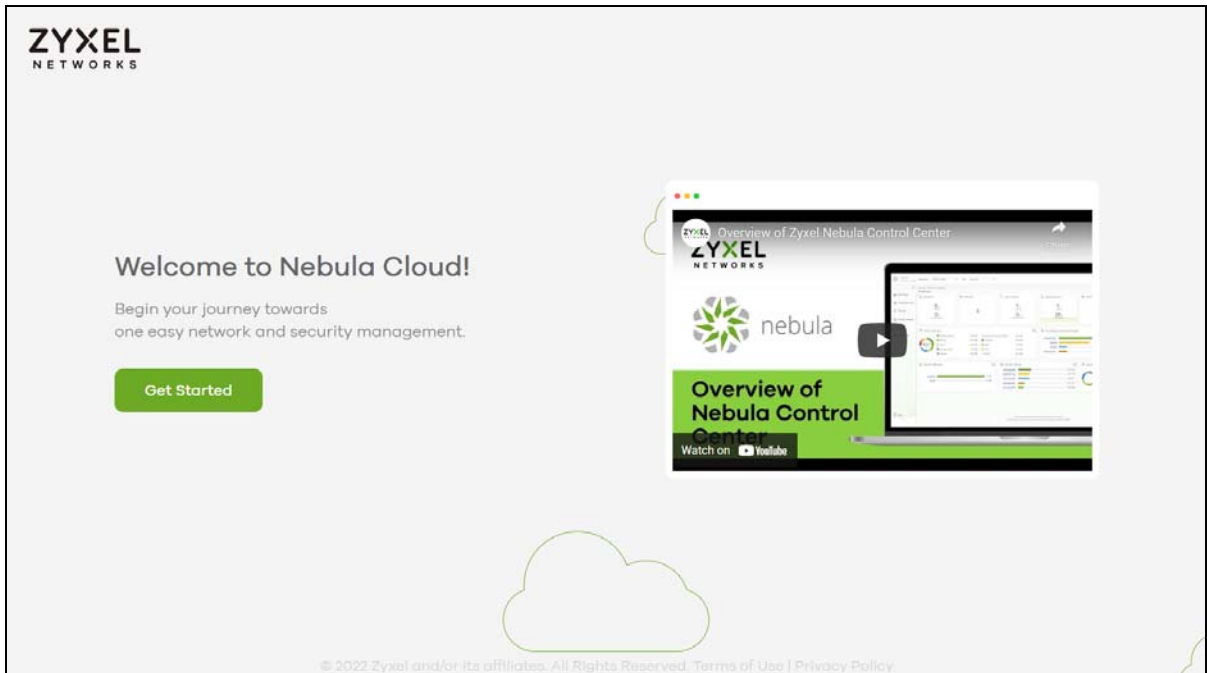
## 1.2.1 Connect Nebula Managed Devices

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**.



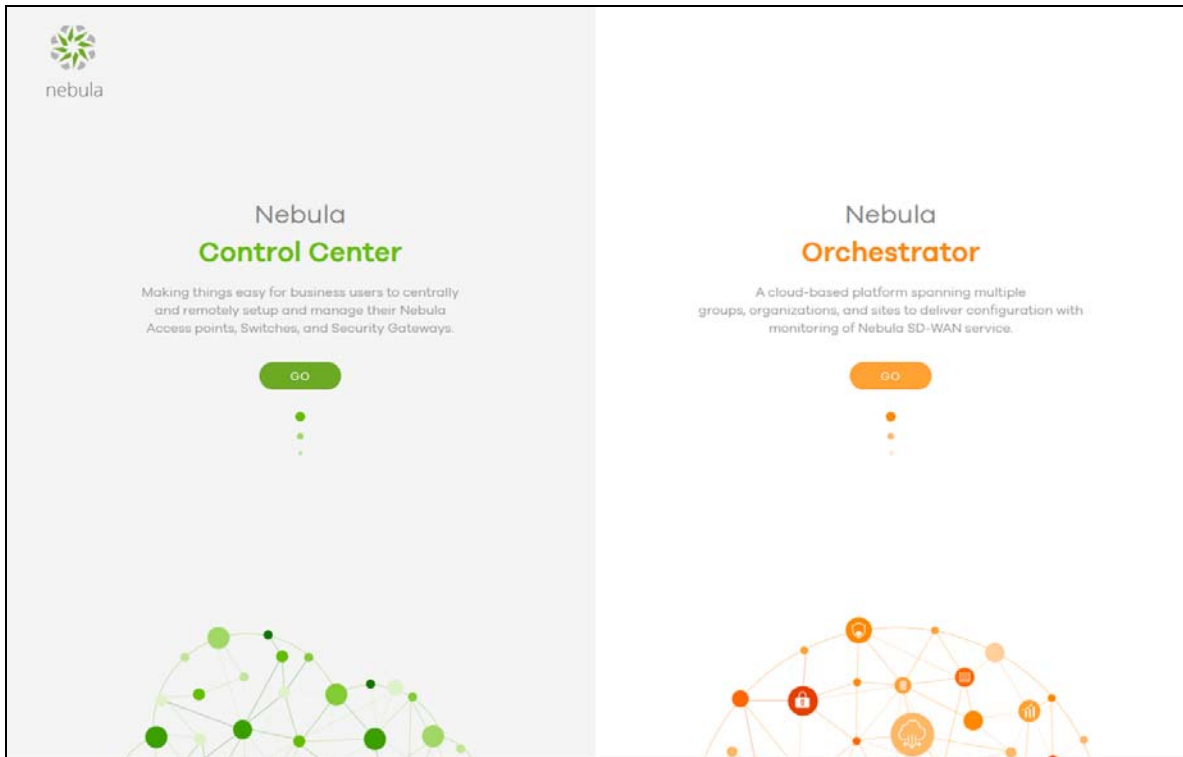
Note: The NCC requires a myZyXel account before you can register and manage Nebula Devices. Log into the NCC with your myZyXel account. Click **Create Account** if you do not have a myZyXel account and create an account with your existing email address.

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

The image shows a 'Sign In' form. At the top is the title 'Sign In'. Below it are two input fields: 'Email Address' containing 'syu@zyxel.com.tw' and 'Password' with a masked password and a visibility icon. A 'Forgot Password' link is to the right of the password field. Below the password field is a checked 'Remember me' checkbox. There are two buttons: a green 'Sign In' button and a white 'Try Demo' button. Below the buttons is a message: 'I have signed up but haven't activated my account. Resend Activation Email'. At the bottom left is a link 'Don't have an account? Create account'. At the bottom are links for 'Legal Notice', 'Terms of Use', 'Privacy', and 'Cookie Settings'. At the very bottom is a copyright notice: '2.49.12 Copyright © 2021 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.

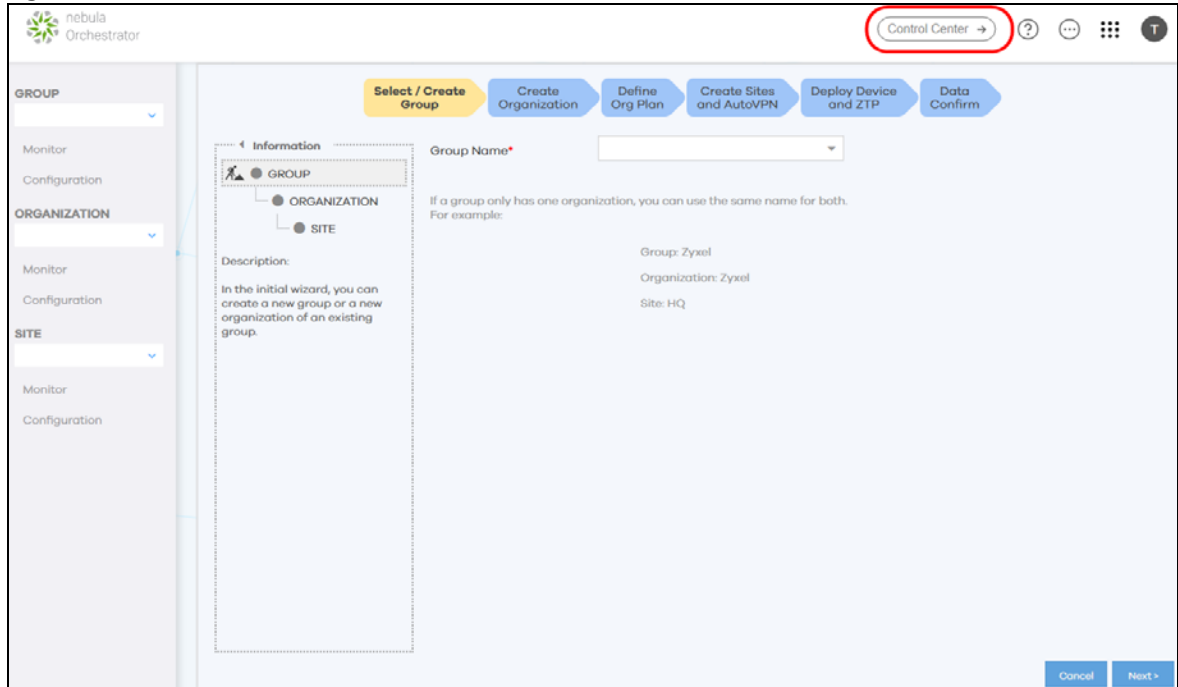
- 3 Click **Go** under Nebula Control Center to log in to NCC.



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.

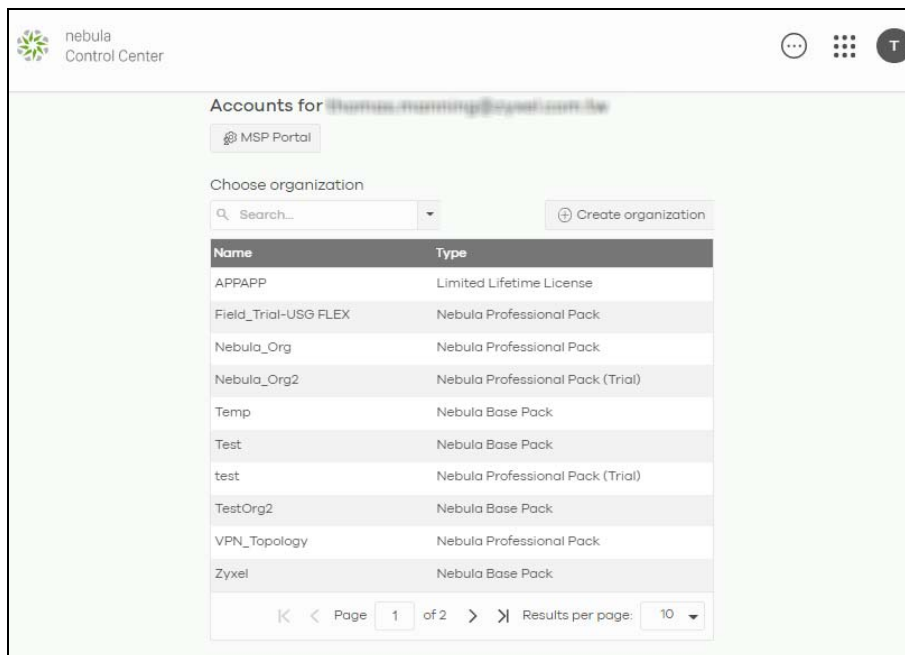


Figure 2 Nebula SD-WAN (Orchestrator)

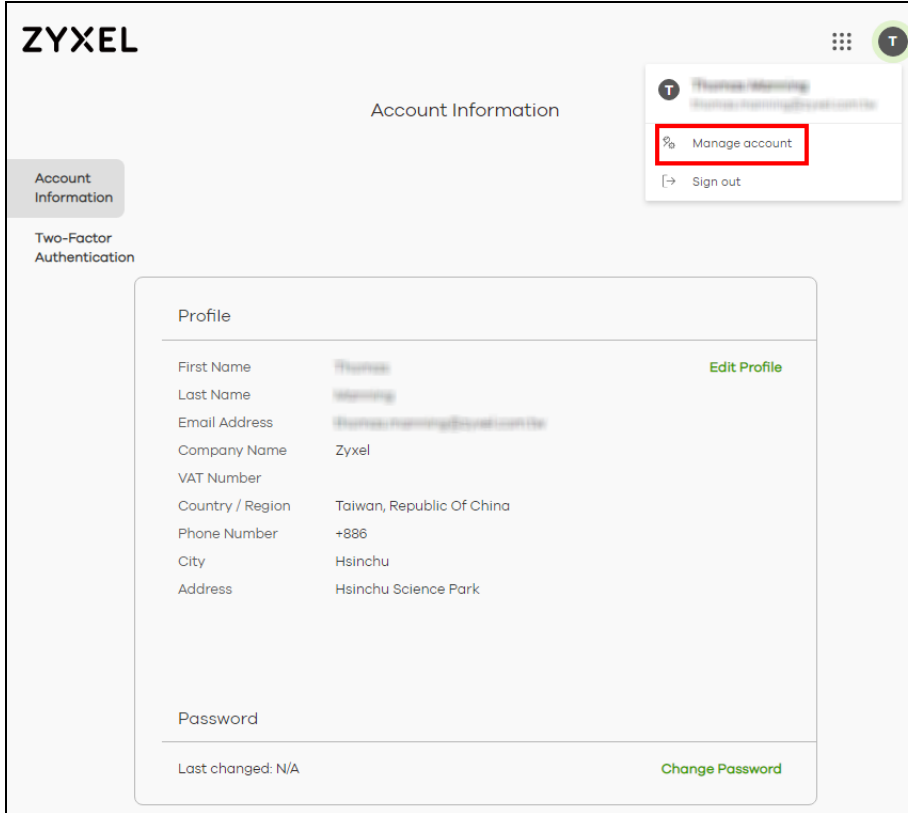


You can click **Control Center** to go back to the NCC platform.

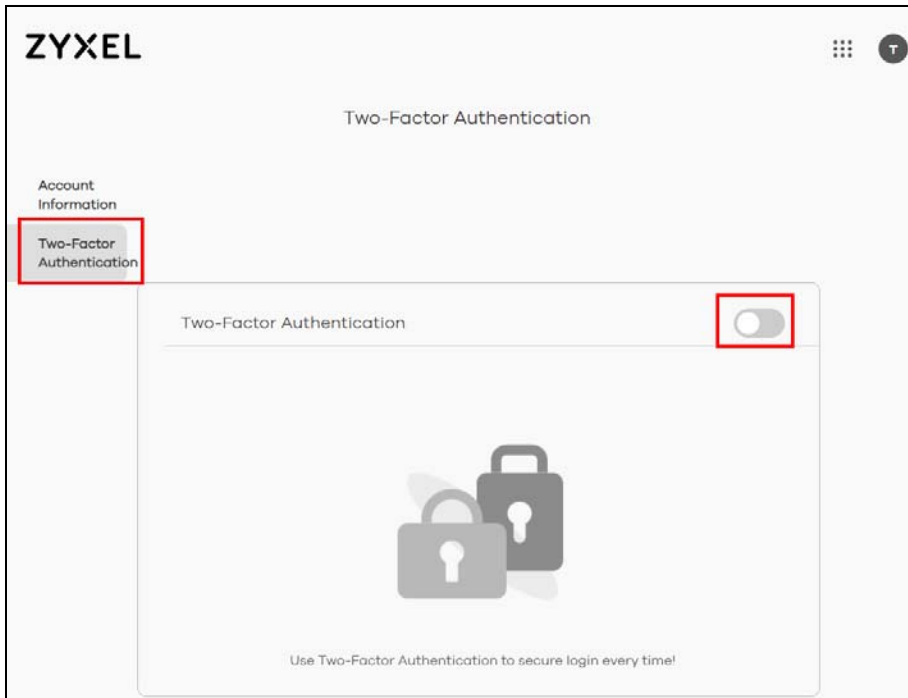
- 4 Click **Create organization** to create a new organization. If this is the first time you have logged into NCC, proceed to step 10. If you have more than one organization, click a row to select the organization you want to manage.



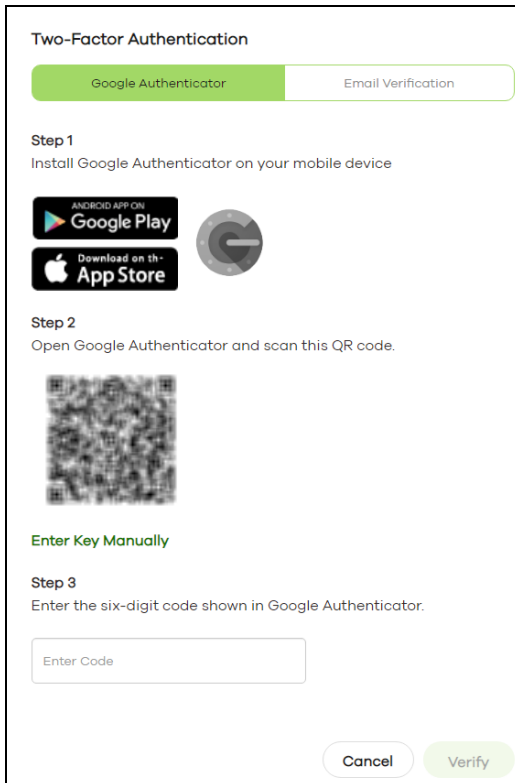
- 5 The NCC supports two-factor authentication (2FA) to add a second layer of security to your account. Click **Manage account** to enable Two-factor authentication on the following page. Otherwise, you can skip 2FA and go to step 10 directly.



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



- 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.



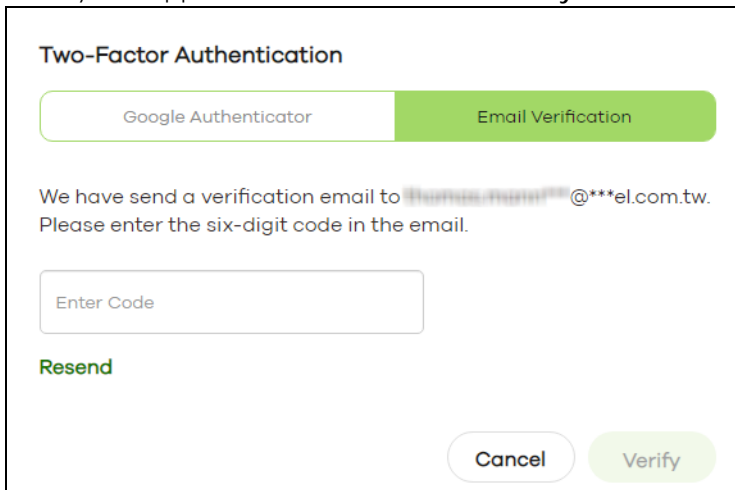
The screenshot shows a "Two-Factor Authentication" screen. At the top, there are two tabs: "Google Authenticator" (selected) and "Email Verification". Below the tabs, the screen is divided into three steps:

- Step 1:** "Install Google Authenticator on your mobile device". It features buttons for "Google Play" and "App Store", along with a circular icon containing a right-pointing arrow.
- Step 2:** "Open Google Authenticator and scan this QR code." It displays a square QR code.
- Step 3:** "Enter the six-digit code shown in Google Authenticator." It includes a text input field labeled "Enter Code" and "Enter Key Manually" text above it.

At the bottom of the screen, there are two buttons: "Cancel" and "Verify".

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

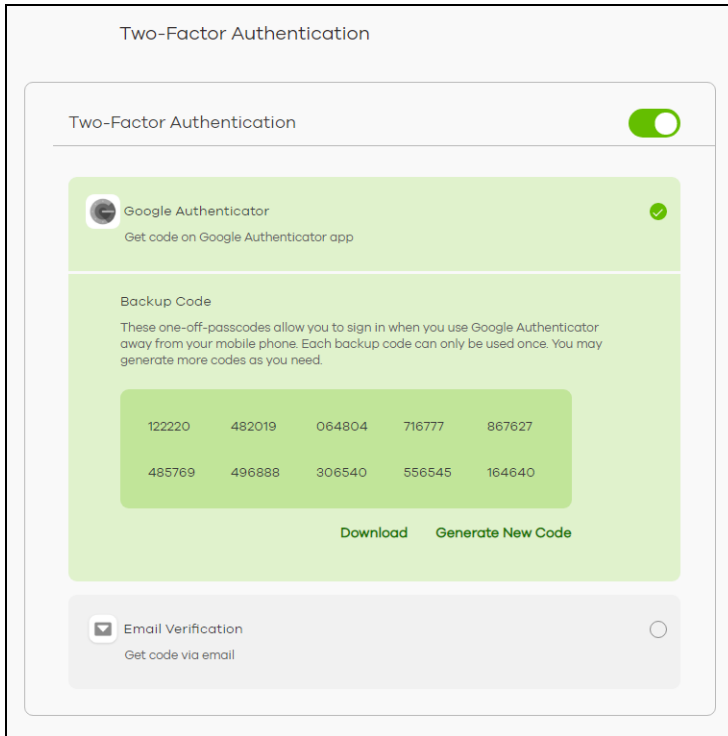
If you select **Email Verification**, an email is sent to your myZyxel account's email address. Enter the code exactly as it appears in the email and click **Verify**.



The screenshot shows the "Two-Factor Authentication" screen with the "Email Verification" tab selected. The text below the tabs reads: "We have send a verification email to [redacted]@\*\*\*el.com.tw. Please enter the six-digit code in the email." Below this text is a text input field labeled "Enter Code". A "Resend" link is visible below the input field. At the bottom, there are "Cancel" and "Verify" buttons.

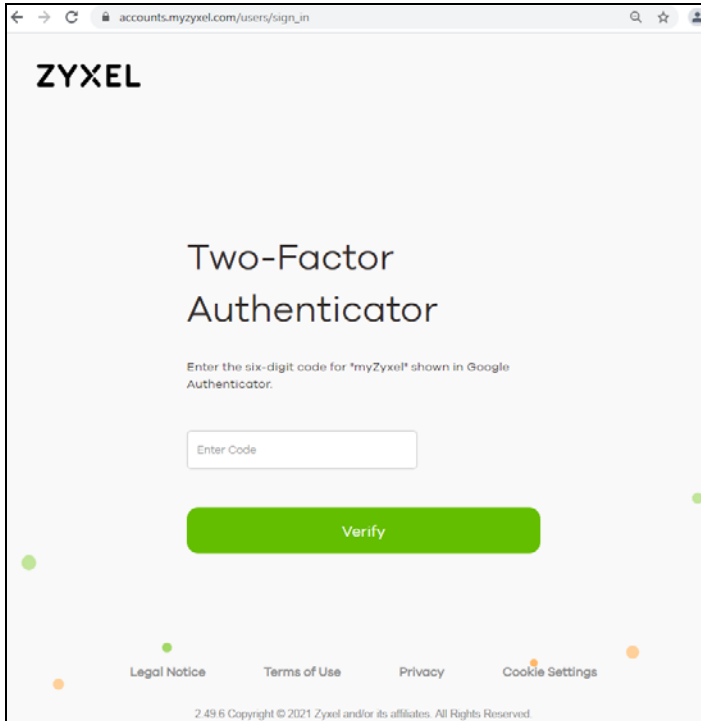
- 8 Enter the verification code to get 10 backup codes, which help regain access to your account in case your smartphone is not available for 2FA the next time you need to log in again.

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

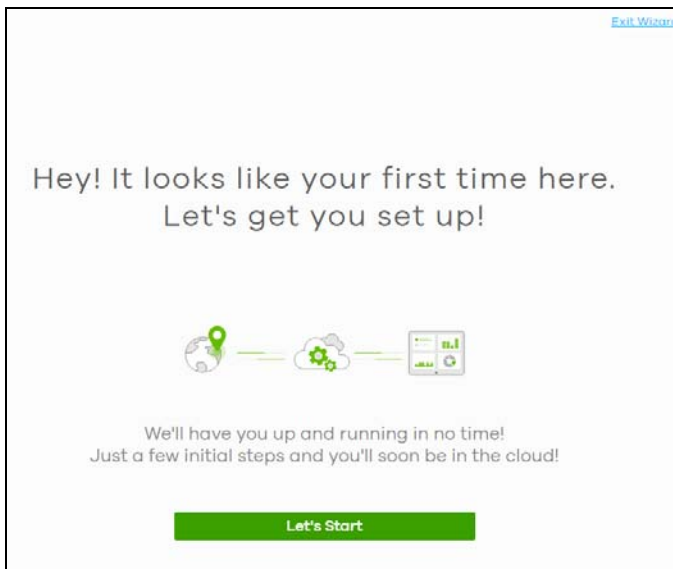


Write down or print out the backup codes for your account. You can enter the backup code on the NCC web page to authenticate your identity at the next login. Each code can only work once. Click **Download** to download the backup codes.

- 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.



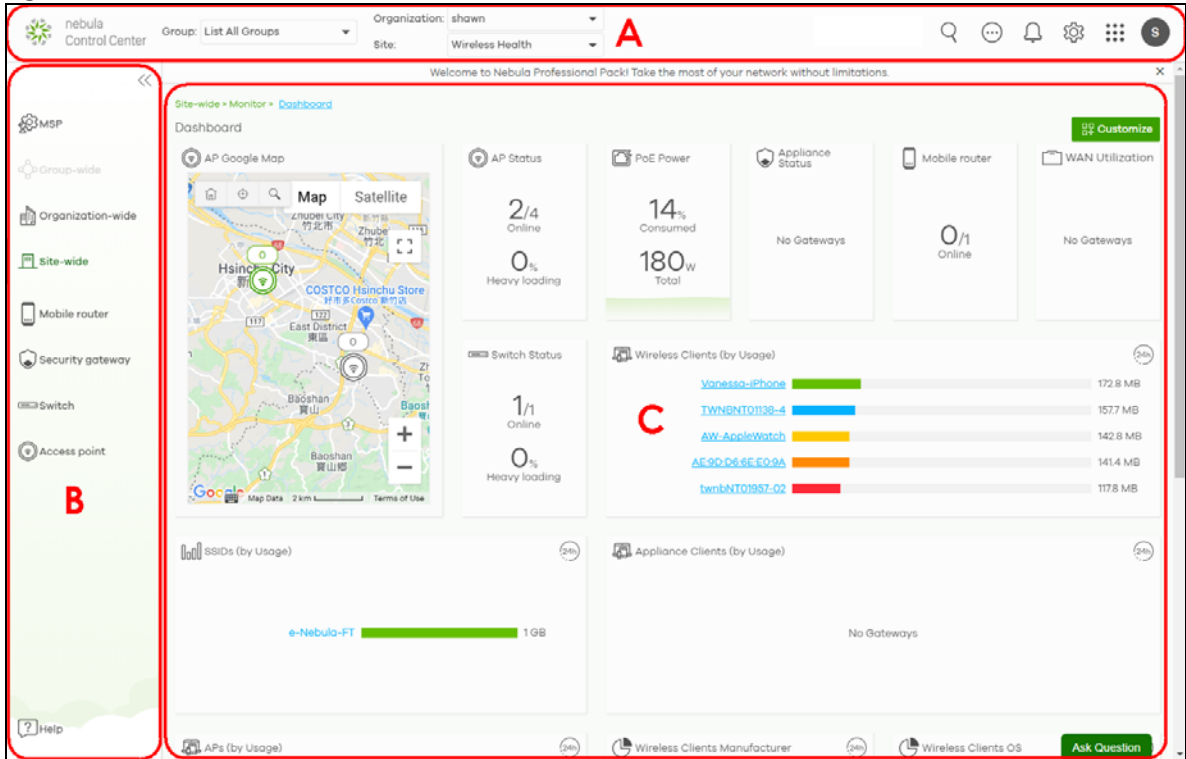
- 10 If this is the first time you have logged into NCC, the setup wizard welcome screen displays. You need to create your organization and sites, register Nebula Devices and associate them with a site. See [Chapter 2 on page 45](#) for how to use the wizard.



## 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



- 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

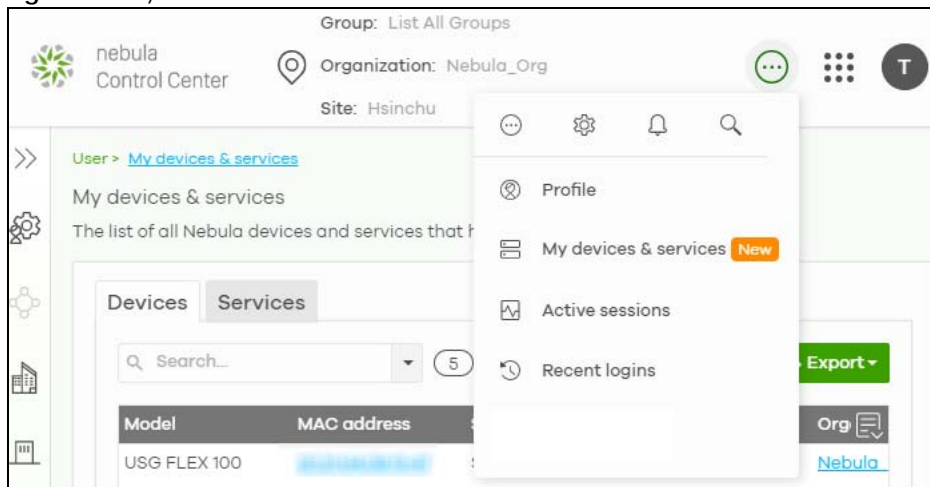
LABEL	DESCRIPTION
Group	This shows the name of the groups you are managing, if your NCC account has an MSP license. Click to choose another group if you have multiple groups.  Note: To create a group, you must be the owner of two or more Pro pack organizations that are not currently assigned to a group, as discussed in <a href="#">Section 5.1.1 on page 174</a> .
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.

Table 4 NCC Title Bar (continued)

LABEL	DESCRIPTION
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, CNC, Circle, Marketplace, and the Forum.
Account	Click this to manage your NCC account settings, or to sign out of NCC.

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

Figure 5 Layout of the Title Bar



### 1.3.1.1 Group/Organization/Site

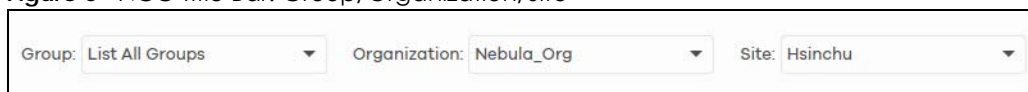
Select the group, organization and site that you want to manage.

- 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 4.2 on page 153](#)).

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 42](#)).
- If you need to have more sites, select **Create site** from the **Site** drop-down list box to create a new one (see [Section 6.3.2 on page 194](#)).

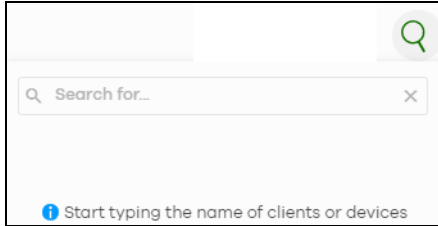
Figure 6 NCC Title Bar: Group/Organization/Site



### 1.3.1.2 Search

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

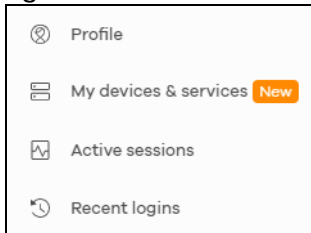
Figure 7 Search



### 1.3.1.3 More

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

Figure 8 More



The following table describes this menu.

Table 5 Login Account Menu

LABEL	DESCRIPTION
Profile	This shows account information, such as name, address, and phone number.
My devices & services	This shows a list of all Nebula Devices in NCC that have your login account as the owner. You can filter the list of Nebula Devices by name, serial number, model, or organization. You can also register licenses to your account, such as an MSP license.
Active sessions	Shows all active web browser sessions for this login account. Click <b>End Session</b> 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 > Configure > Admins & teams > Admins](#) in [Section 4.6.1](#) on page 160 for details on the organization privileges.



Figure 9 My Devices

User > [My devices & services](#)

My devices & services

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

Devices Services Purchase history

Q Search... 3 devices. [Export](#)

Model	MAC address	Serial Number	Name	Organization	Site	Device owner
USG FLEX 500	88FC-A31973EA	61829145300193		<a href="#">Test_July</a>	<a href="#">ZyNet_TW</a>	snmuel.vu@nubul.com.tw
NR7101	08FC-EE502058	6210745007757		<a href="#">Test_July</a>	<a href="#">ZyNet_TW</a>	snmuel.vu@nubul.com.tw
NWA110AX	80CE-A5597006	6200145310004		<a href="#">Test_July</a>	<a href="#">ZyNet_TW</a>	snmuel.vu@nubul.com.tw

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

User > [My devices & services](#)

My devices & services

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

Devices Services Purchase history

[Actions](#) Q Search... 2 Licenses [Purchase MSP licenses](#) [+ Register](#) [Export](#)

License key	Service description	Start date	End date	Status	Actions	Registered date	Activated date
<input checked="" type="checkbox"/> LIC-TRIAL-366DAYS-1624282655326	Nebula MSP Pack License, Trial	2021-06-21	2022-06-22	Expired		2021-06-21	2021-06-21
<input type="checkbox"/> LIC-NMSP-2YR-202206230916	Nebula MSP Pack License, 2YR	2022-07-01	2024-07-01	Activated	<a href="#">Transfer license</a>	2022-06-23	2022-07-01

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

User > [My devices & services](#)

My devices & services

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

Devices Services Purchase history

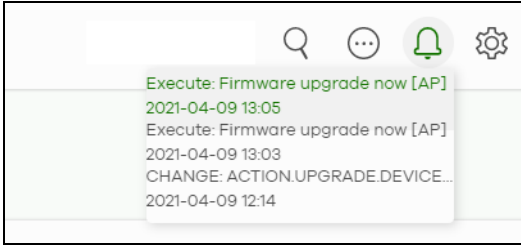
Q Search... 0 purchases.

Order ID	Purchase date	# licenses	Status	Export
----------	---------------	------------	--------	--------

### 1.3.1.4 Notifications

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

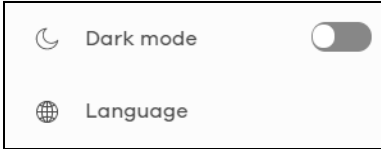
Figure 12 NCC Notification



### 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

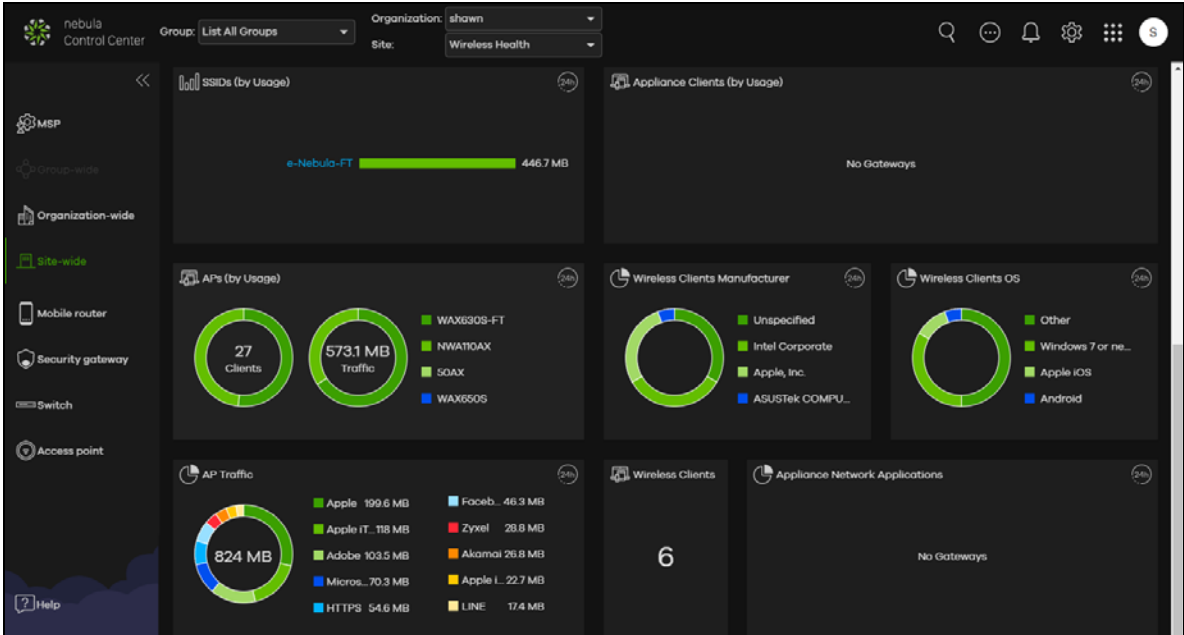


The following table describes this menu.

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.

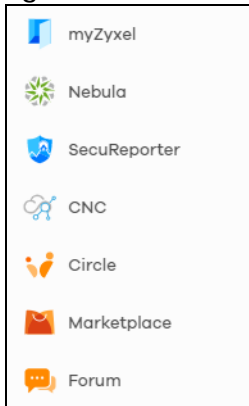
Figure 14 Dark Mode



### 1.3.1.6 Applications

Click this to display a list of related NCC links.

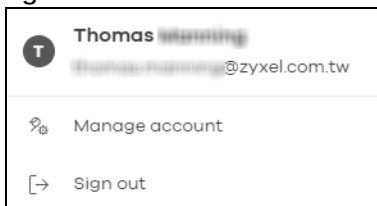
**Figure 15** Related NCC Links



### 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.	
MSP	Create multiple organizations and change the branding and assign administrators to multiple organizations.
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.

Table 8 Navigation Menus Overview (continued)

LABEL	DESCRIPTION
Organization-wide	Manage multiple network sites within an organization.
Site-wide	Manage Nebula Devices in a site.
Use these menus to set up customer Nebula Devices.	
Mobile router	Manage Zyxel LTE/NR devices.
Security gateway	Manage ZyWALL NSG devices (firewalls).
Firewall	Manage ZyWALL ATP, USG FLEX, and USG20(W)-VPN devices (firewalls).
Switch	Manage Zyxel Switches.
Access point	Manage 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
MSP	Monitor	
	MSP portal	Use this menu to create multiple organizations and change the branding and assign administrators to multiple organizations.
	Change log	Use this menu to view log messages about configuration changes in the <b>Admins &amp; teams</b> and <b>Cross-org synchronization</b> screens.
	Configure	
	Create organization	Use this menu to create a new organization or copy settings from an existing organization.
	MSP branding	Use this menu to upload/replace/remove the dashboard logo. You can also set the support contact details.
	Admins & teams	Use this menu to create administrators or groups of administrators (teams) and view their login details.
	Cross-org synchronization	Use this menu to sync or clone organization-wide settings from a source organization to a destination organization.
	MSP alert template	Use this menu to configure <b>MSP alert templates</b> to monitor Nebula Devices for unexpected events (for example, online or offline events).
Group-wide	Monitor	
	Overview	Use this menu to view organization and license details of a selected 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.
	Change log	Use this menu to view log messages about configuration changes in the group.
	Configure	
	Settings	Use this menu to configure group information and group members.
	Org-to-Org VPN	Use this menu to view and manage VPNs between members in the group.
	Administrators	Use this menu to view, remove, or create a new administrator account for the selected group.

Table 9 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
Organization-wide	Monitor	
	Overview	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.
	Change log	Use this menu to view log messages about configuration changes in this organization.
	Configure	
	Settings	Use this menu to configure security settings or delete the organization.
	Create site	Use this menu to create a new site.
	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.
	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.
	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.
	Security profile sync	Use this menu to synchronize the settings of URL threat filter, anti-malware and content filtering on the selected gateways.
	VPN Orchestrator	Use this menu to view and manage VPNs created for the selected organization.
Firmware management	Use this menu to upgrade firmware or schedule firmware upgrades for Nebula Devices in the organization.	

Table 9 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
Site-wide	Monitor	
	Dashboard	Use this menu to view Nebula Device connection status and traffic summary.
	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, Security Firewalls) 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.
	Containment list	Use this menu to view and manage Nebula Devices contained by CDR (Collaborative Detection & Response).
	Map & floor plans	Use this menu to locate Nebula Devices on a world map or on a floor plan.
	Topology	Use this menu to view Nebula managed-device connections in your network.
	Vouchers	Use this menu to create and manage vouchers that allow WiFi network access
	Cloud intelligent logs	Use this menu to view log messages about configuration changes made by the NCC for the site.
	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.
	Applications	Use this menu to view usage of applications such as Social Network, Telephony (VoIP), Advertising, News, Web Services in the network.
	Configure	
	General 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.
	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 at the time of writing.
	Alert settings	Use this menu to set which alerts are created and emailed or sent by the Zyxel Nebula app. You can also set the email addresses to which an alert is sent.
	Add devices	Use this menu to register a Nebula Device and add it to the site.
	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.
Mobile Router		Use this screen to monitor and configure the LTE/NR indoor/outdoor devices, managed by the NCC. The settings are applied when a Nebula Mobile Router is registered and added to the selected site.

Table 9 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
Security gateway		Use these menus to monitor and configure the Security Appliances, not including Security Firewall series, ATP series, and USG20(W)-VPN series, managed by the NCC. The settings are applied when a Nebula Security Appliance is registered and attached to the selected site.
	Monitor	
	Security gateway	Use this menu to view the detailed information about the Security Appliance of the selected site.
	Clients	Use this menu to view the connection status and detailed information about a client in the selected site.
	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.
	Configure	
	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.

Table 9 NCC Menu Summary (continued)

LEVEL 1	LEVEL 2 / LEVEL 3	FUNCTION
Firewall		Use these menus to monitor and configure the ZyWALL USG FLEX series, ATP series, and USG20(W)-VPN series devices, not including ZyWALL NSG series devices, managed by the NCC. The settings are applied when a Nebula Security Firewall is registered and attached to the selected site.
	Monitor	
	Firewall	Use this menu to view the detailed information about the Security Firewall of the selected site.
	Clients	Use this menu to view the connection status and detailed information of all wired and WiFi clients connected to Nebula Devices (Access Points, Security Firewall) in the site.
	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.
	Configure	
	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
Switch		Use these menus to monitor and configure the Switches managed by the NCC. The settings are applied when a Nebula Switch is registered and attached to the selected site.
	Monitor	
	Switches	Use this menu to view the list of Switches added to the site.
	Clients	Use this menu to view detailed information about the clients which are connecting to the Switches in the site.
	Event log	Use this menu to view all events on the Switch. An event is something that has happened to a Nebula managed device.
	IPTV report	Use this menu to view available IPTV channels and client information.
	Surveillance	Use this screen to view information about Powered Devices (PDs) connected to ports on the Switch.
	Summary report	Use this menu to view network statistics specific to Switches in the site.
	Configure	
	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
Access Point		Use these menus to monitor and configure the Access Points managed by the NCC. The settings are applied when a Nebula Access Point is registered and attached to the selected site.
	Monitor	
	Access points	Use this menu to view the list of Access Points added to the site.
	Clients	Use this menu to view WiFi clients which are connected to the Access Points in the site.
	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.
	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.
	Configure	
	SSID settings	Use this menu to view and configure SSID settings and authentication methods.
	SSID advanced settings	Use this menu to configure network access, traffic options 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.	

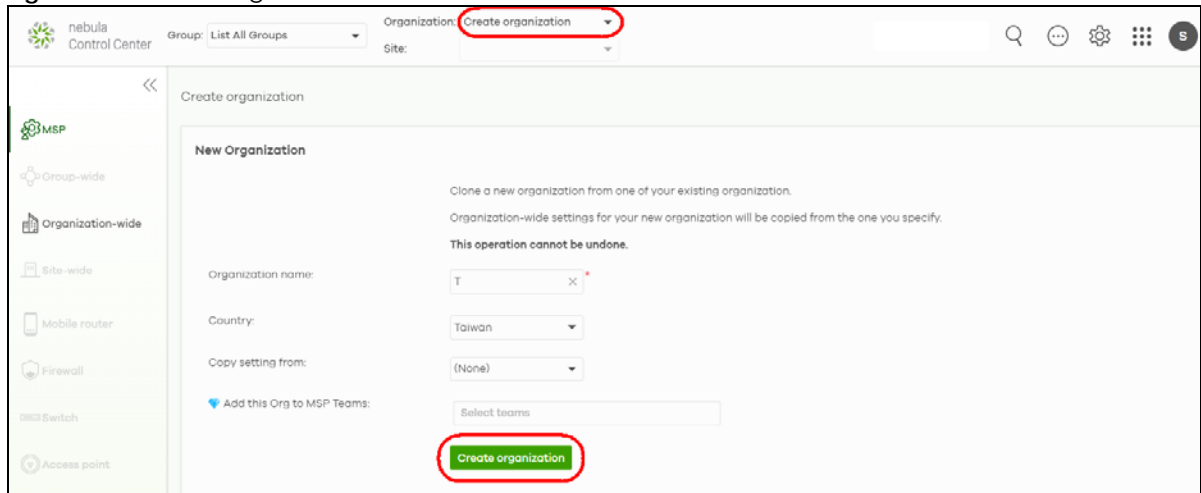
## 1.4 Create Organization

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 6.3.3 on page 195](#).

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 45](#) 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

The screenshot shows the Nebula Control Center interface. At the top, the title bar includes the Nebula logo, 'nebulas Control Center', a 'Group' dropdown set to 'List All Groups', an 'Organization' dropdown set to 'Create organization', and a 'Site' dropdown. The main content area is titled 'Create organization' and contains a 'New Organization' form. The form includes a warning: '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.' Below this, there are input fields for 'Organization name' (with 'T' entered), 'Country' (set to 'Taiwan'), and 'Copy setting from' (set to '(None)'). There is also a section for 'Add this Org to MSP Teams' with a 'Select teams' input field. At the bottom of the form is a green 'Create organization' button. The 'Organization' dropdown in the title bar and the 'Create organization' button are both circled in red.

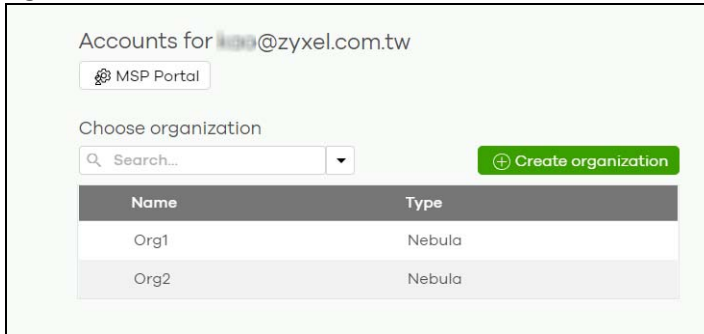
- 5 Choose whether to activate a one-month trial of Nebula Pro Pack and Nebula Security Services for the organization. For example, USG FLEX 700, Secure WiFi License, 1MO; USG FLEX 700, UTM Security Pack License, 1MO; Nebula Professional Pack License, 1MO.

## 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



## 1.6 Cloud-Saving Mode

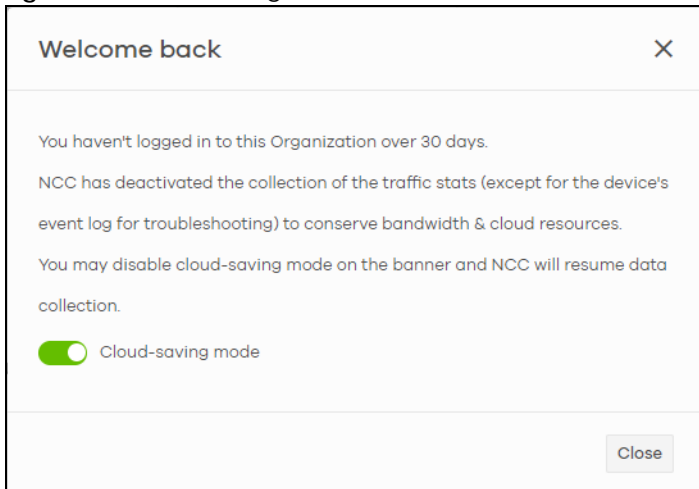
If you do not log into a base (free) license tier organization for over 30 days, the organization automatically enters Cloud-saving mode to save your network bandwidth and cloud resources.

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

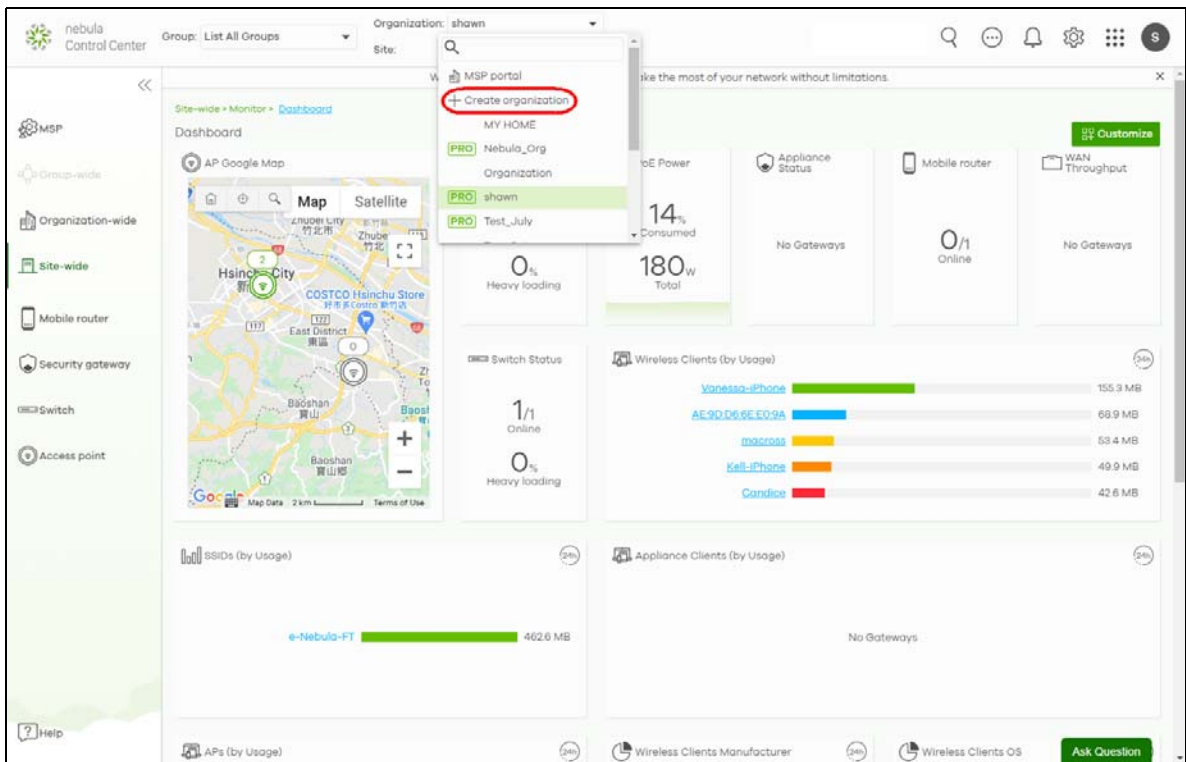


# CHAPTER 2

## Setup Wizard

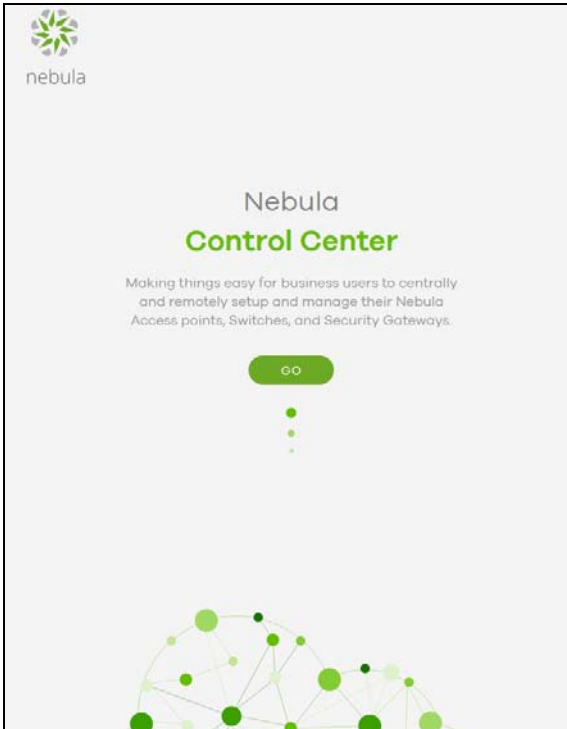
### 2.1 Setup Wizard

- 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.

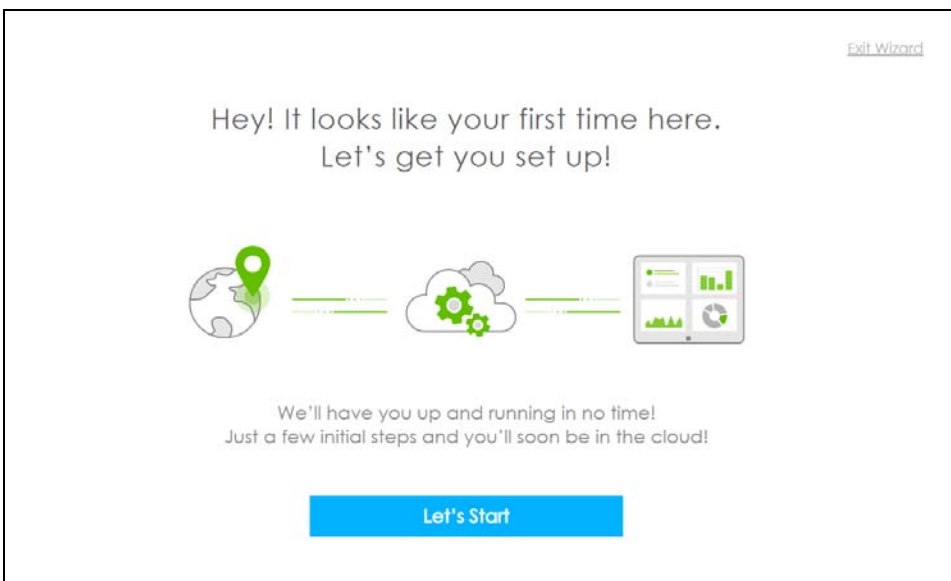


#### 2.1.1 Step1: Run the Wizard

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



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



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.

The screenshot shows the first step of the setup wizard. On the left, a progress indicator shows '01' followed by four dashes. Below it, text explains that Nebula is organized into Organizations and Sites, and provides instructions on how to create them. On the right, the main heading reads 'First step is to create your Organization and Site'. Below this heading are four input fields: 'Organization' (text input), 'Site' (text input), 'Country' (dropdown menu with 'Taiwan' selected), and 'Timezone' (dropdown menu with 'Asia - Taipei (UTC +8 0)' selected). A 'Next' button is located at the bottom right of the form area. An 'Exit Wizard' link is in the top right corner.

### 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.

The screenshot shows the second step of the setup wizard. On the left, a progress indicator shows '02' followed by three dashes. Below it, text explains that users need to input the MAC address and Serial Number for each device, and provides an example of how these are located on the device. A diagram shows a device with labels for 'Serial Number' and 'MAC address'. On the right, the main heading reads 'Let's now add your device(s) to Nebula'. Below this heading is a table with three columns: 'MAC address', 'Serial number', and 'Name'. Each column has an input field with an 'x' icon to clear the field. A red square icon is in the top right of the table. Below the table is a green '+ Add' button. At the bottom, there are 'Back' and 'Next' buttons. An 'Exit Wizard' link is in the top right corner.

## 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).

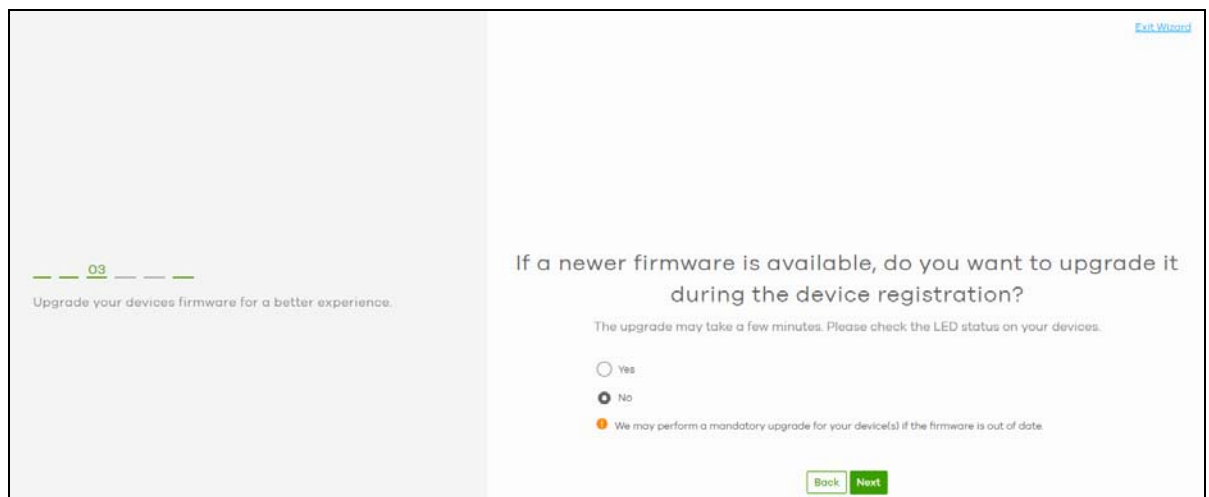
Even if you choose not to upgrade the firmware, NCC will still perform a mandatory upgrade to **Stable** firmware version if the Nebula Device's firmware have security vulnerabilities, and/or lack key performance improvements. See [Table 63 on page 248](#) for the description of a **Stable** firmware.

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.



## 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.

## 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.

[Exit Wizard](#)

### Need to set up a Guest WiFi?

----- 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.

**Tip** 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.

WiFi Name (SSID)

Guest Test

Password (The Shared Key)

12345678

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

No captive web portal

Clicking "Agree" to access the network

Using their Facebook account to join the network

VLAN

1

[Set up VLAN interface](#)

[Back](#) [Next](#)

## 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.

[Exit Wizard](#)

### Deployment Method

----- 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.

**Tip** 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.

Model Name

ATP200 [Show device information](#)

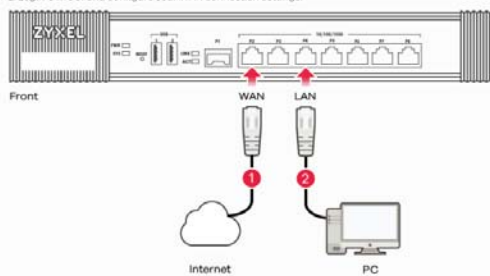
Deployment Method

Nebula native mode

Zero Touch Provision 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.



[Back](#) [Next](#)

[Ask Question](#)

### 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.

### Deployment Method [Exit Wizard](#)

Model Name:  [Show device information](#)

Deployment Method ?

Nebula native mode

Zero Touch Provision mode

**1. Configure your WAN**

VLAN Top:

VLAN ID:  (1-4080)

WAN Type:  Port: P2

IP Address:

Subnet Mask:

Default Gateway:

First DNS Server:

Second DNS Server:

MTU:  (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.



- 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**

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

**Overview for your Security Appliance configuration**

<b>Model Name:</b> USG20-VPN	<b>WAN Setting:</b> <ul style="list-style-type: none"> <li>• WAN Port: 22</li> <li>• WAN Type: STATIC</li> <li>• VLAN ID: 2</li> </ul>	<b>Recipient:</b> vn.zyxel@gmail.com
------------------------------	--	--------------------------------------

Everything seems fine, ready to go?

[Go to Nebula Dashboard](#)

### 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 6.3.3.8 on page 208](#) 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.

**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.

**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.

**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.

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

Note: To set the administrator privileges, see [Section 4.6.0.1 on page 160](#) 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 > Configure > Add devices** screen. Click **+Add**.

- 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.

## 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 16](#) 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	PRO / 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

### 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 > Configure > License & inventory**, click **Action > Add more licenses**.

Organization-wide > Configure > License & inventory

License & inventory

Overview Devices Licenses Trial Change log Purchase History

**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

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

■ Unlicensed (expired) 0  
■ Expires within 90 days 0  
■ Expires after 90 days 5  
■ Inactive 0

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

**Add licenses**

[Add licenses](#)

**Add licenses**

Enter one more license keys. Or you can download the [template](#) here and [import](#) multiple license keys for faster registration.

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

**+ Add**

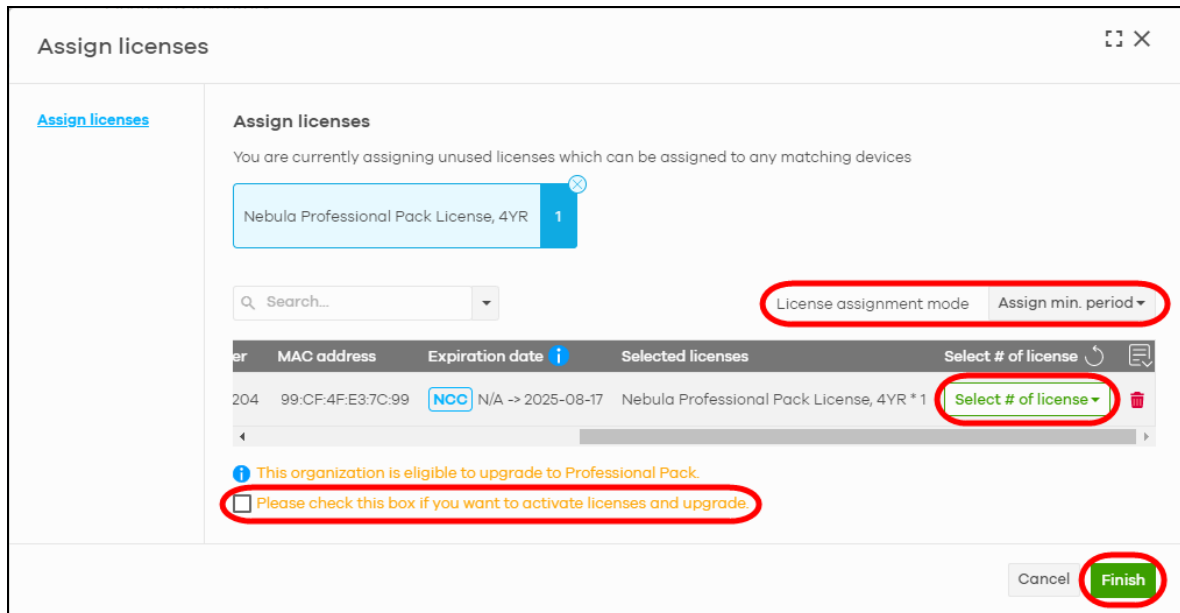
**Cancel Finish**

- 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.

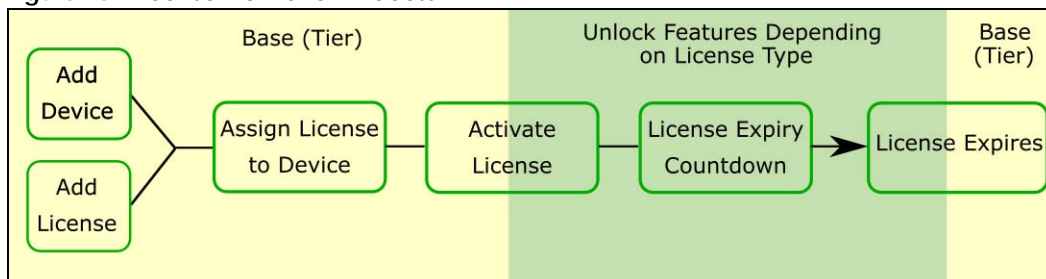
- In the **Organization-wide > Configure > License & inventory**, select the **Devices** tab.
- Locate the Nebula Device to assign a license(s). Click the **Actions** button and select **Assign license** on the device row.
- Clear any license that you do not want added to the Nebula Device.

- 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**.



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

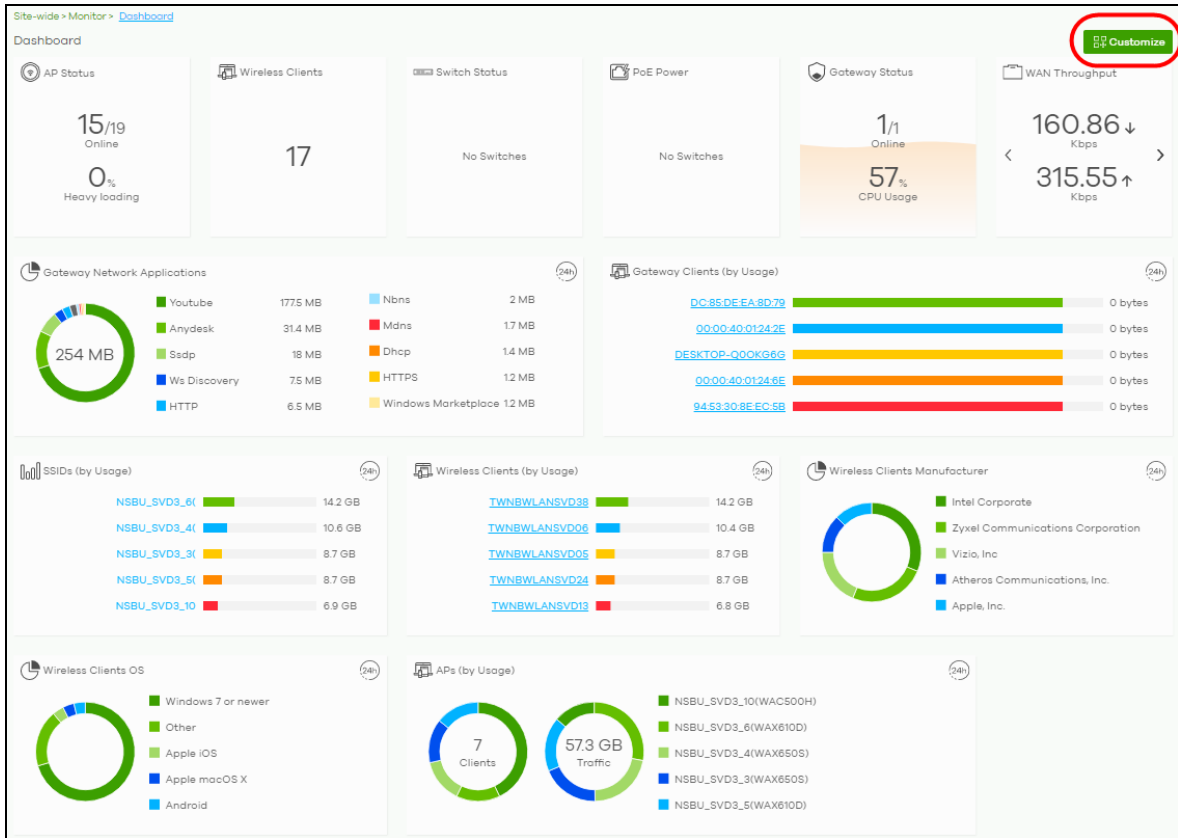
**Figure 20** License Activation Process



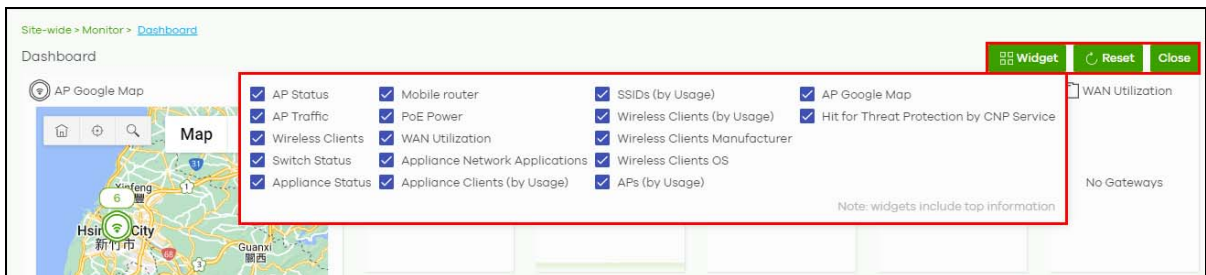
## 3.4 Monitor a Site

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 > Monitor > 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.



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

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

Organization-wide > Configure > [License & inventory](#)

License & inventory

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

**Organization status** Actions Purchase license

Organization type: Professional Pack (Expire on: 2023-02-18)

NCC license: ● Device(s) will expire in 90 days. [Check license issue](#)

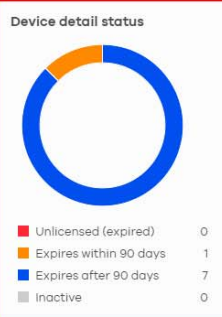
Security license: ● Device(s) expired or unlicensed. [Check license issue](#)

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 22](#) 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 > Configure > License & inventory** to view the available (unused) licenses assigned to your organization.

License Key	License states	Associated device	Activate date	Action
<input type="checkbox"/> WTEST-ZIAXK-AULXJ-VLLAS-UFBSV	Active	20:21:03:21:13:46	2021-06-15	Action ▾
<input type="checkbox"/> LIC-PLUS-1MO-31310203160647	Queued	20:21:03:21:13:40	2021-06-11	Action ▾
<input type="checkbox"/> LIC-PLUS-1MO-31310203160645	Active	20:21:03:21:13:40	2021-06-07	Action ▾
<input type="checkbox"/> WTEST-9RFQF-BJQUL-XYOZQ-MYI5O	Inactive	20:21:03:21:13:41	-	Action ▾
<input type="checkbox"/> 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 Keys** 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 58](#) 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 22](#) for details on a Nebula Device entering the grace period and what actions you must take.

## 3.7 Transfer Licenses

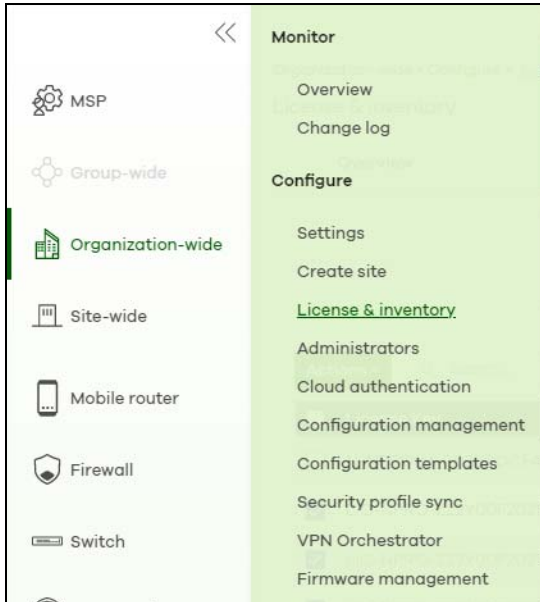
A license assigned to an organization and Nebula Device can be transferred to another Nebula Device in the same or different organization. The following guidelines apply when transferring licenses:

- The Nebula Devices must have the same owner.
- Bundled, Trial, and Promotion licenses cannot be transferred. (See [Table 41](#) 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.

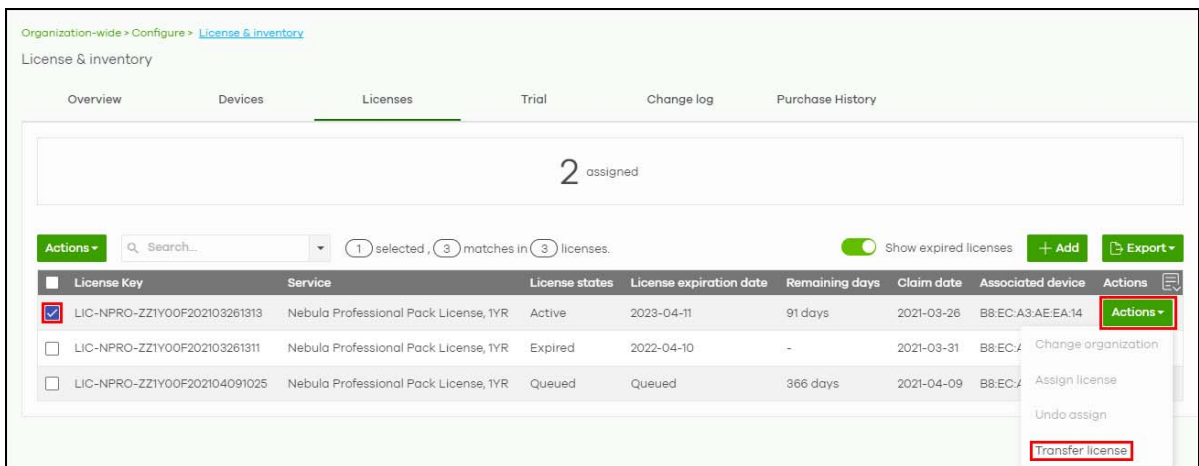
### 3.7.1 Select Transferable Licenses

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

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



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



### 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 ▾	Q (licenseStatesFilter=ACTIVE ▾)	(18) matches in (18) licenses.	+ Add Export ▾	
<input type="checkbox"/> License Key	License states	Associated device	Activate date	Action
<input type="checkbox"/> WTEST-ZIAXK-AULXJ-VLLAS-UFBSV	Active	20:21:03:21:13:46	2021-06-15	Action ▾
<input type="checkbox"/> LIC-PLUS-1MO-31310203160647	Queued	20:21:03:21:13:40	2021-06-11	Action ▾
<input type="checkbox"/> LIC-PLUS-1MO-31310203160645	Active	20:21:03:21:13:40	2021-06-07	Action ▾
<input checked="" type="checkbox"/> WTEST-9RFQF-BJQUL-XYOZQ-MYI50	Inactive	20:21:03:21:13:41	-	Action ▾
<input type="checkbox"/> LIC-PLUS-1MO-31310203160641	Unused			Action ▾

### 3.7.3 Transfer a License to a Different Organization

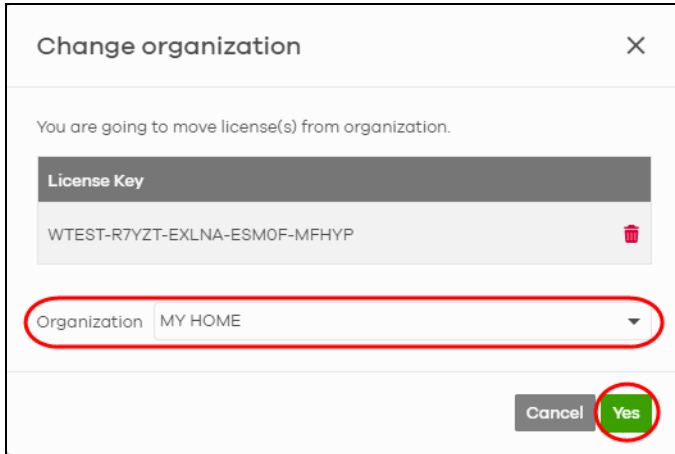
Only an **Unused** license (a license which is assigned to an organization but not assigned to a specific Nebula Device) can be transferred. Both source and destination organizations should belong to the same owner.

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

- 1 Perform the steps described in [Select Transferable Licenses](#).
- 2 With the licenses you want to transfer selected, click **Actions** and then click **Change organization**.

Overview	Devices	Licenses	Trial	Change log	Purchase History			
4 assigned	4 unused (Pro Pack, 2YR)							
Actions ▾	Q Search	(4) selected, (15) matches in (15) licenses.	Show expired licenses	+ Add	Export ▾			
Change organization	Service	License states	License expiration date	Remaining days	Claim date	Activate date	Associated dev	
Assign license	CF4F477DF1-01	Nebula Professional Pack License, 1MO	Expired	2021-04-19	-	2021-03-19	2021-03-19	BC:CF:4F:47:7D:F1
Undo assign	202106040001-11	Nebula Professional Pack License, 2YR	Unused	-	731 days	2022-03-23	-	
Transfer license	202106040001-12	Nebula Professional Pack License, 2YR	Unused	-	731 days	2022-03-23	-	
<input checked="" type="checkbox"/>	LIC-NPRO-ZZ2Y00F202106040001-13	Nebula Professional Pack License, 2YR	Unused	-	731 days	2022-03-23	-	
<input checked="" type="checkbox"/>	LIC-NPRO-ZZ2Y00F202106040001-14	Nebula Professional Pack License, 2YR	Unused	-	731 days	2022-03-23	-	

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

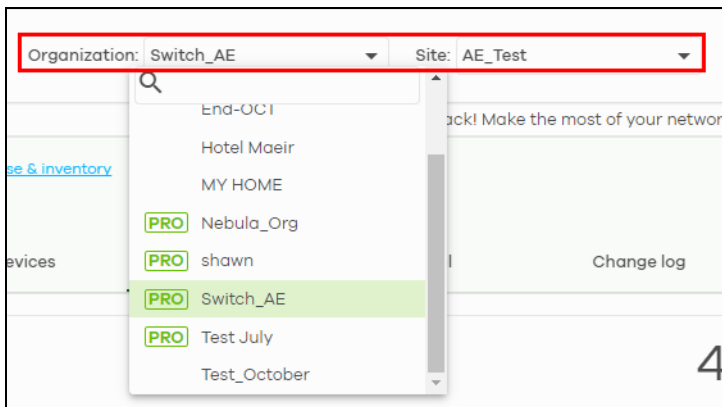


You have successfully transferred a license to another organization, but without assigning it to a Nebula Device yet.

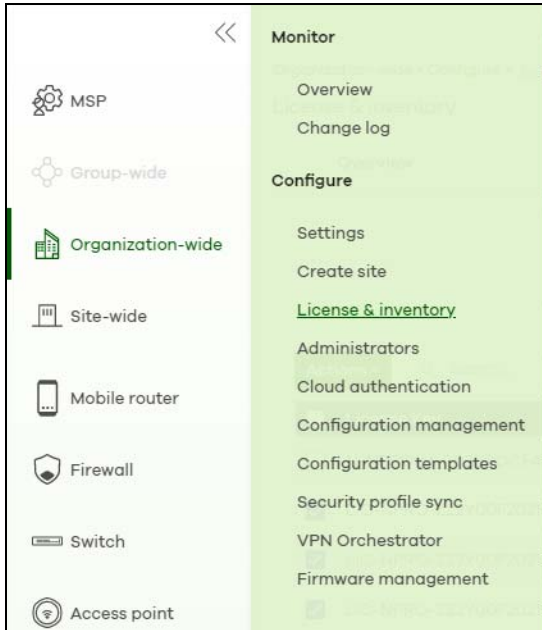
### 3.7.4 Assign a License to a Nebula Device in the New Organization

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

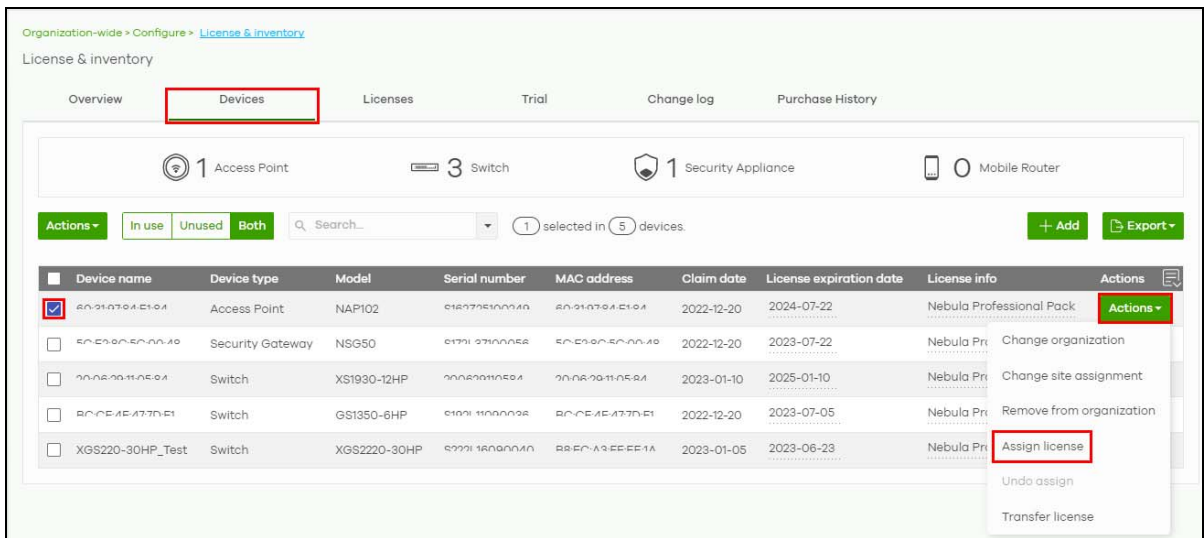
- 1 Perform the steps mentioned in [Transfer a License to a Different Organization](#).
- 2 Select the **Organization** and **Site** where the license is transferred.



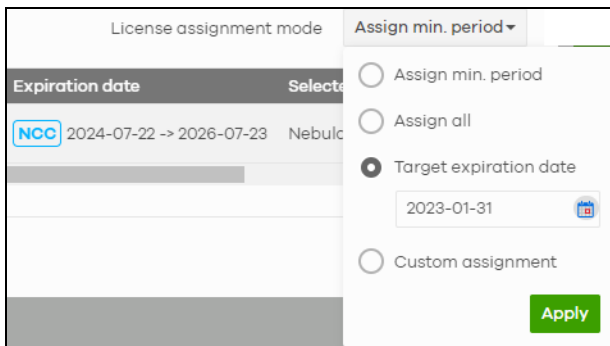
- 3 Go to the **Organization-wide > Configure > License & inventory > Device** screen.



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

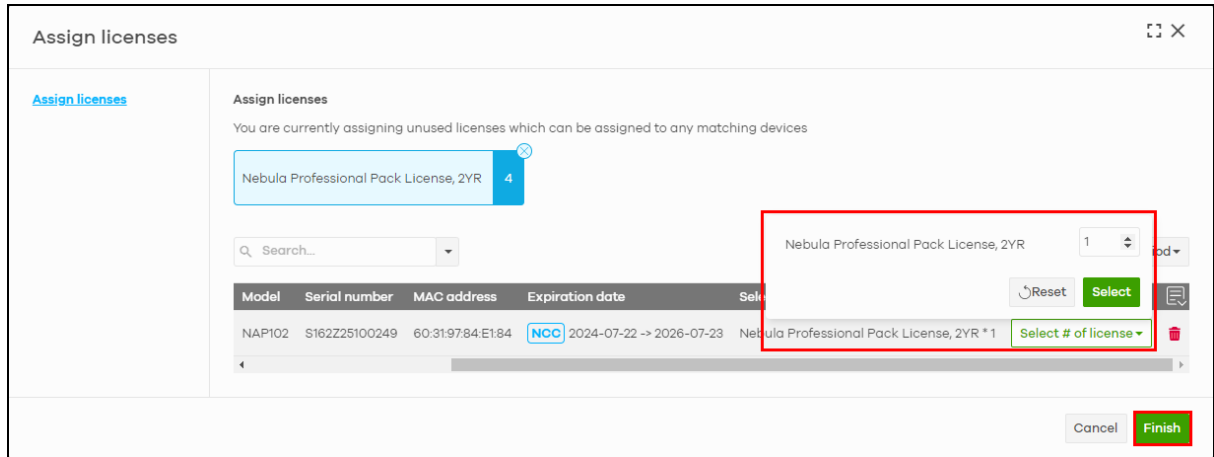


5 Select the **License assignment mode** to have NCC filter licenses that can be assigned.



- **Assign min. period** – one month license packs for your Nebula Device will be picked and displayed.

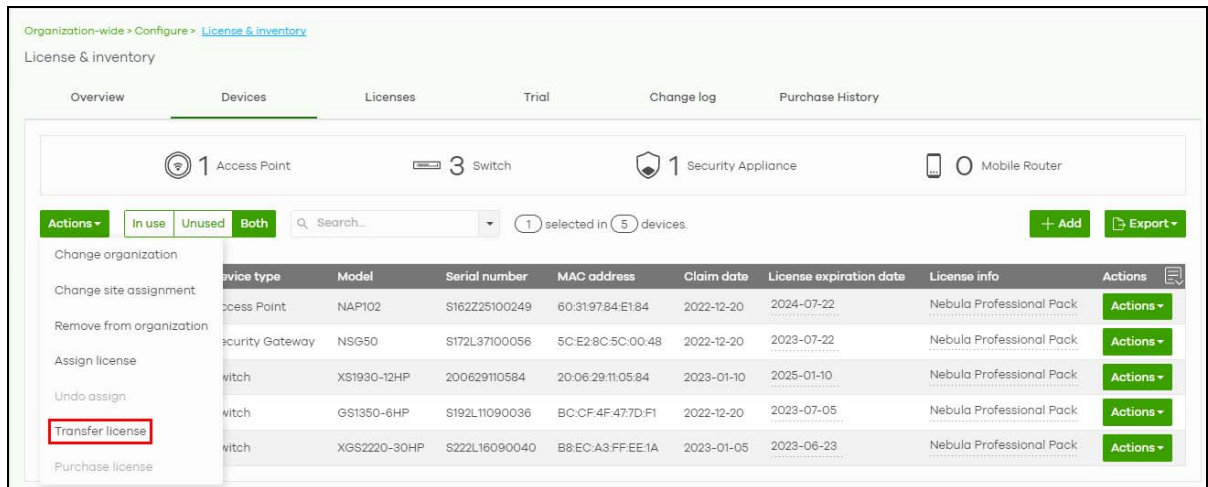
- **Assign all** – all licenses that can be assigned are displayed.
  - **Target expiration date** – all licenses that meet the expiry criteria you set and can be assigned are displayed.
  - **Custom assignment** – any change in value to **Assign min period** and **Assign all** licenses above will become 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**.



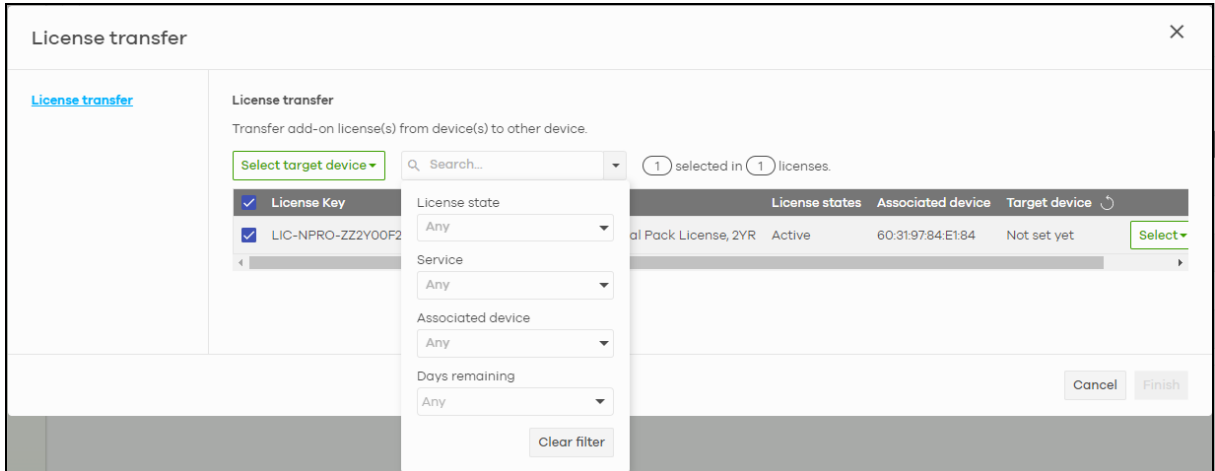
### 3.7.5 Transfer a License to a Nebula Device in a New Organization

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

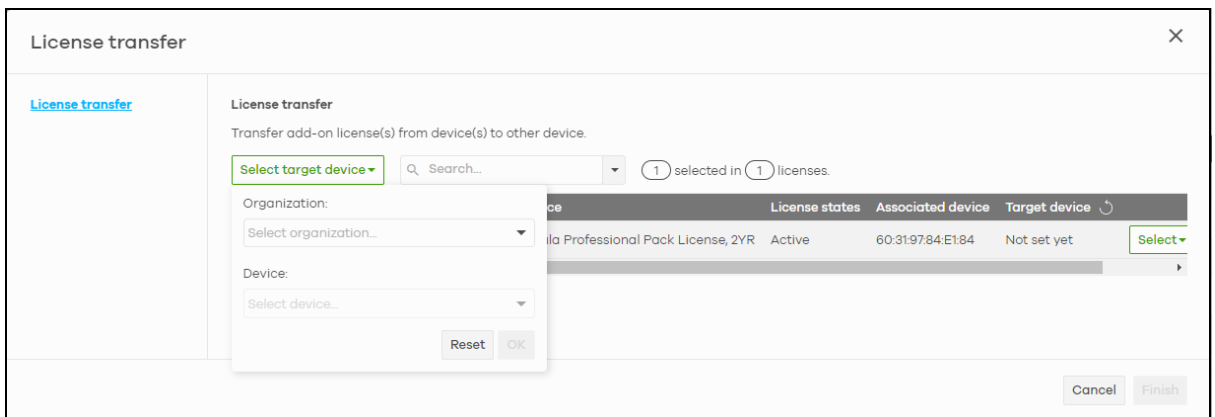
- 1 Perform the steps mentioned in [Assign a License to a Nebula Device in the New Organization](#).
- 2 Click **Organization-wide > Configure > License & inventory > Device** tab.
- 3 Select the devices with the license to be transferred.
- 4 Click **Actions** and select **Transfer License**.



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



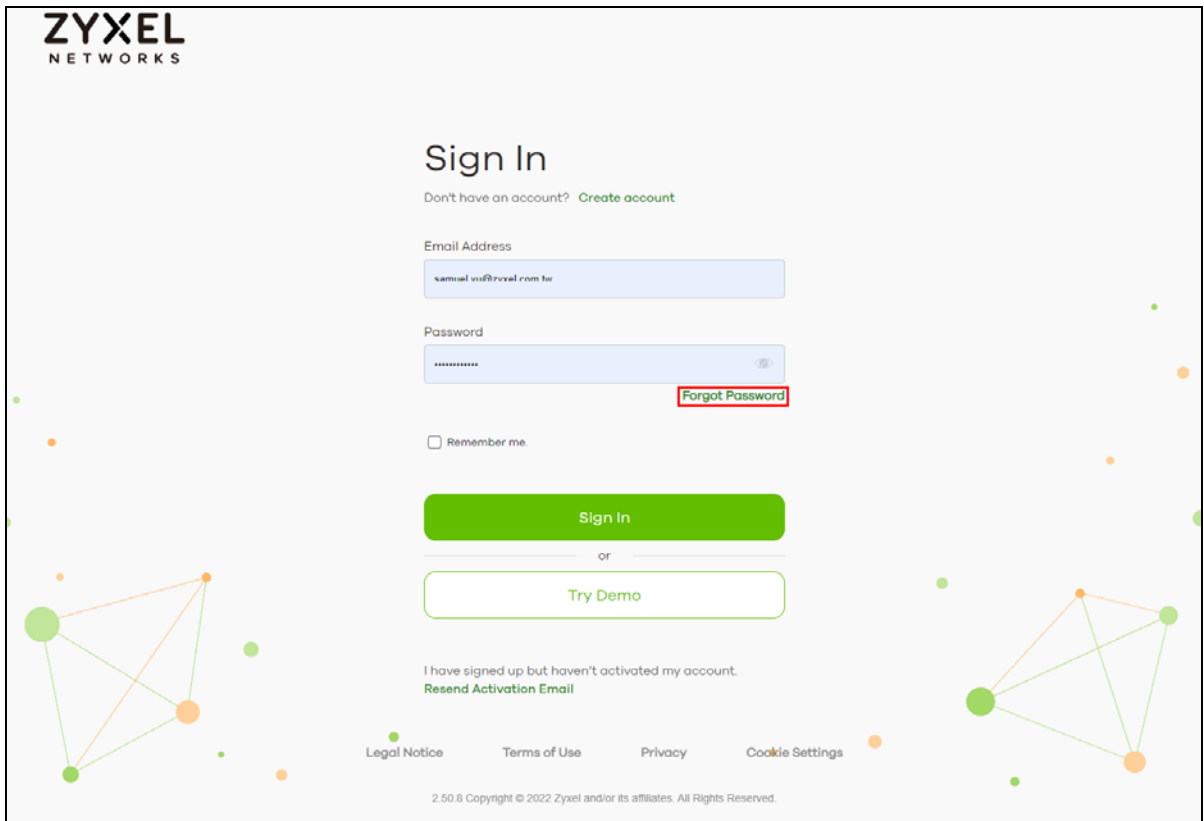
- 6 Click **Select target device** to transfer all licenses to one Nebula Device by selecting the same/different **Organization** and target **Device**. Then click **OK**. Or select the devices individually.



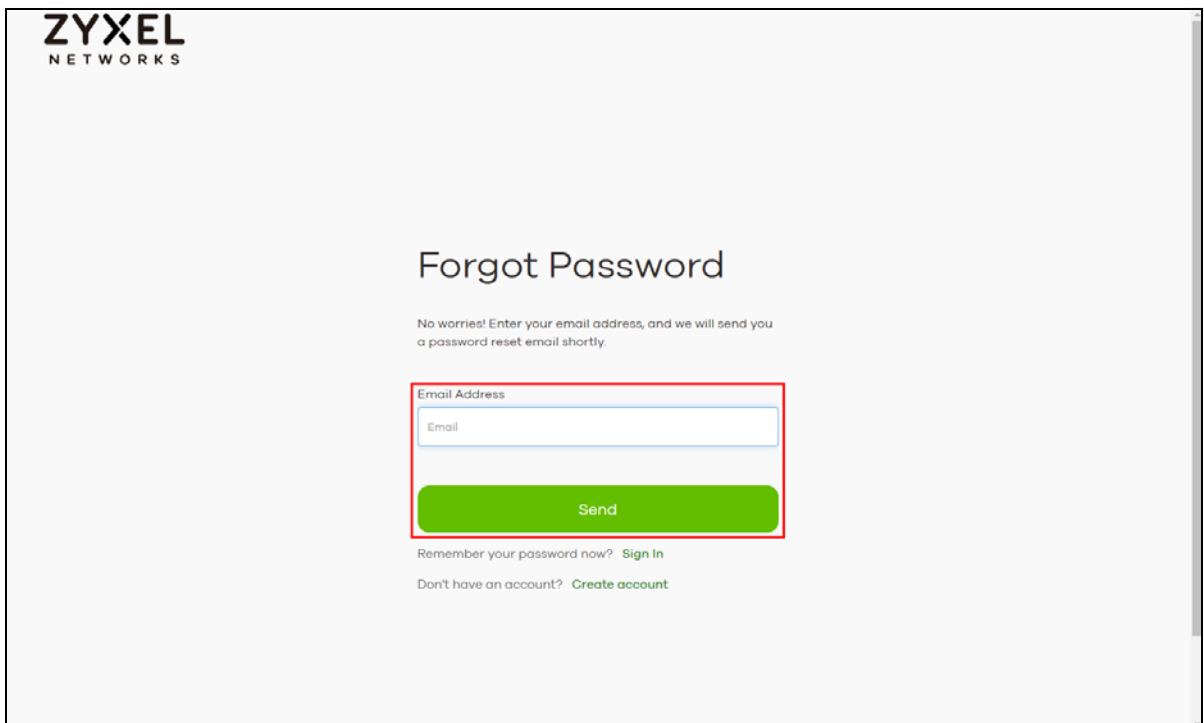
## 3.8 Reset the Nebula Password

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

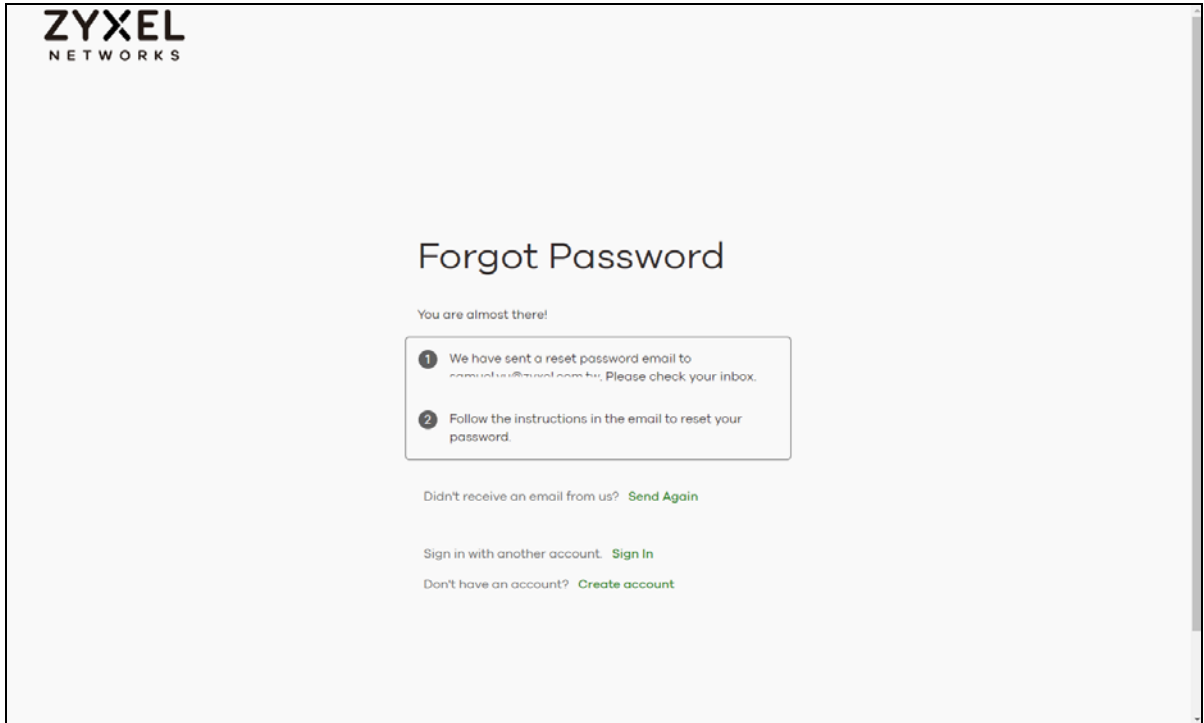
- 1 In the Nebula portal **Sign In** page, click **Forgot Password**.



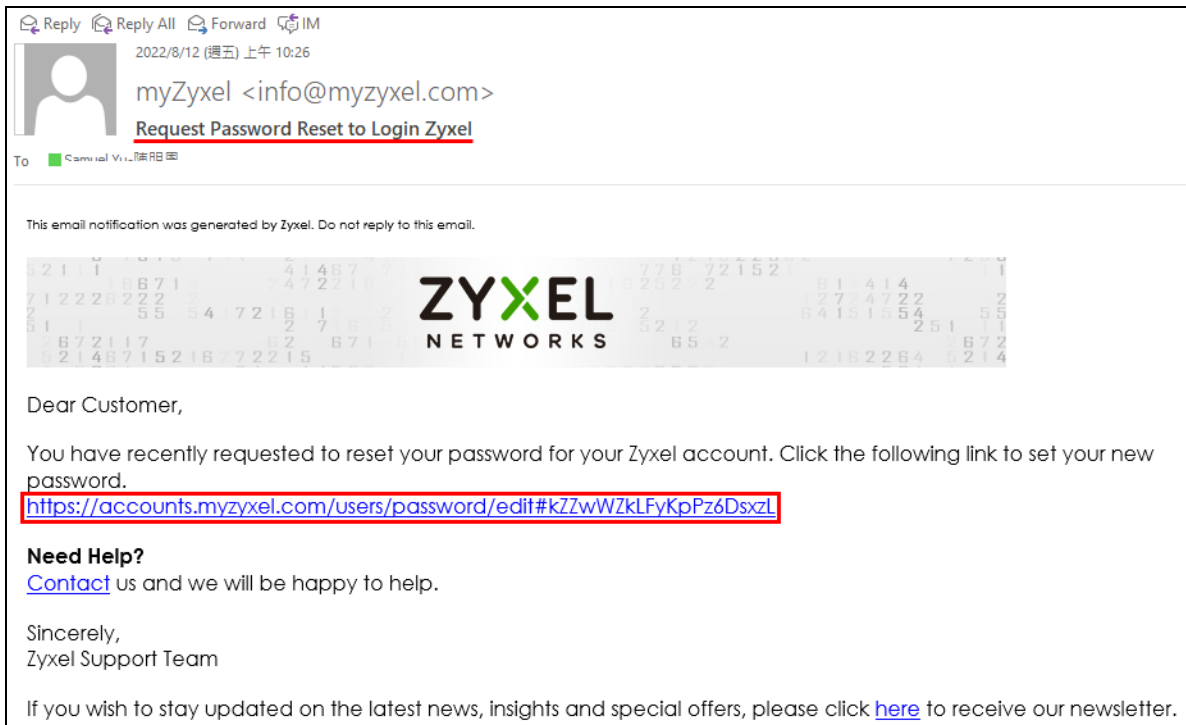
- 2 Enter your myZyxel account's email address, and then click **Send**.



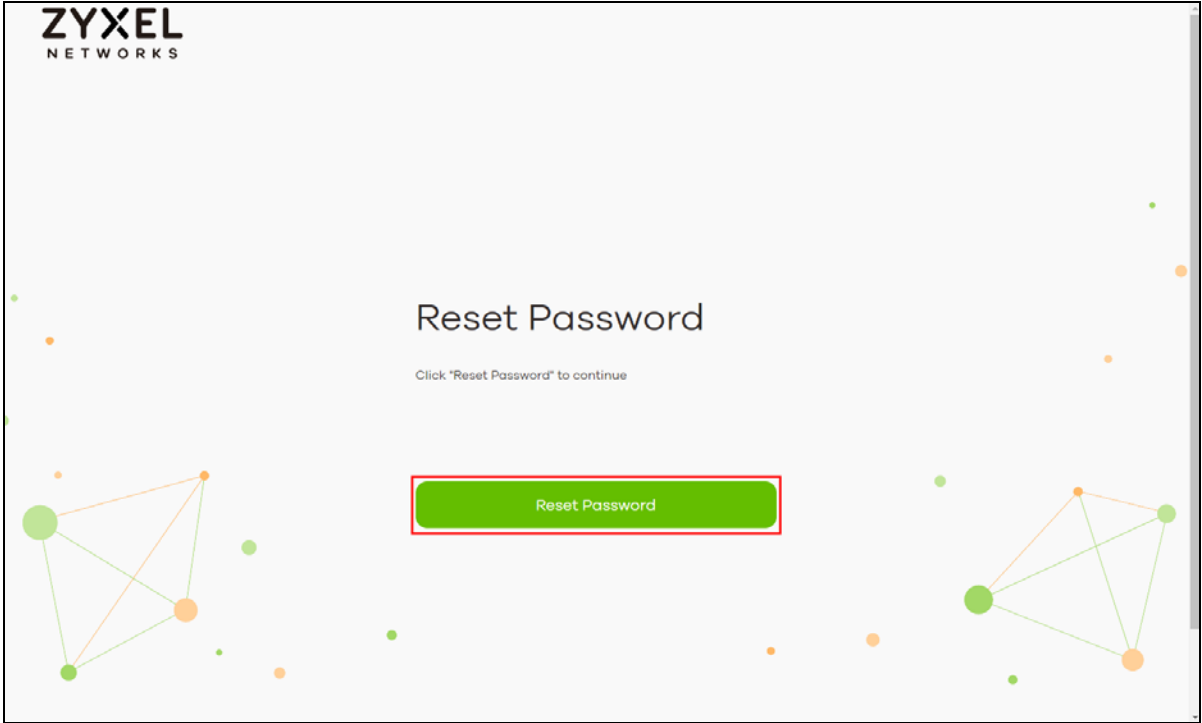
A reset password email has been sent notification appears.



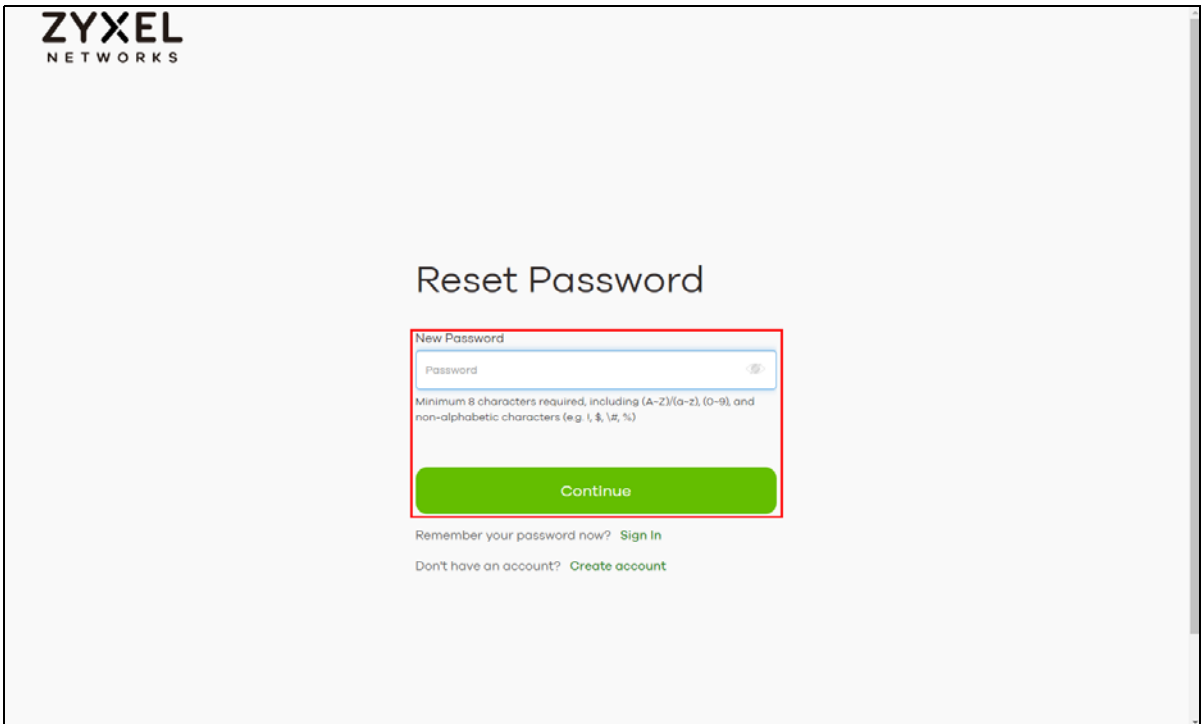
- 3 Click the link in the **Request Password Reset to Login ZyXel** email.



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

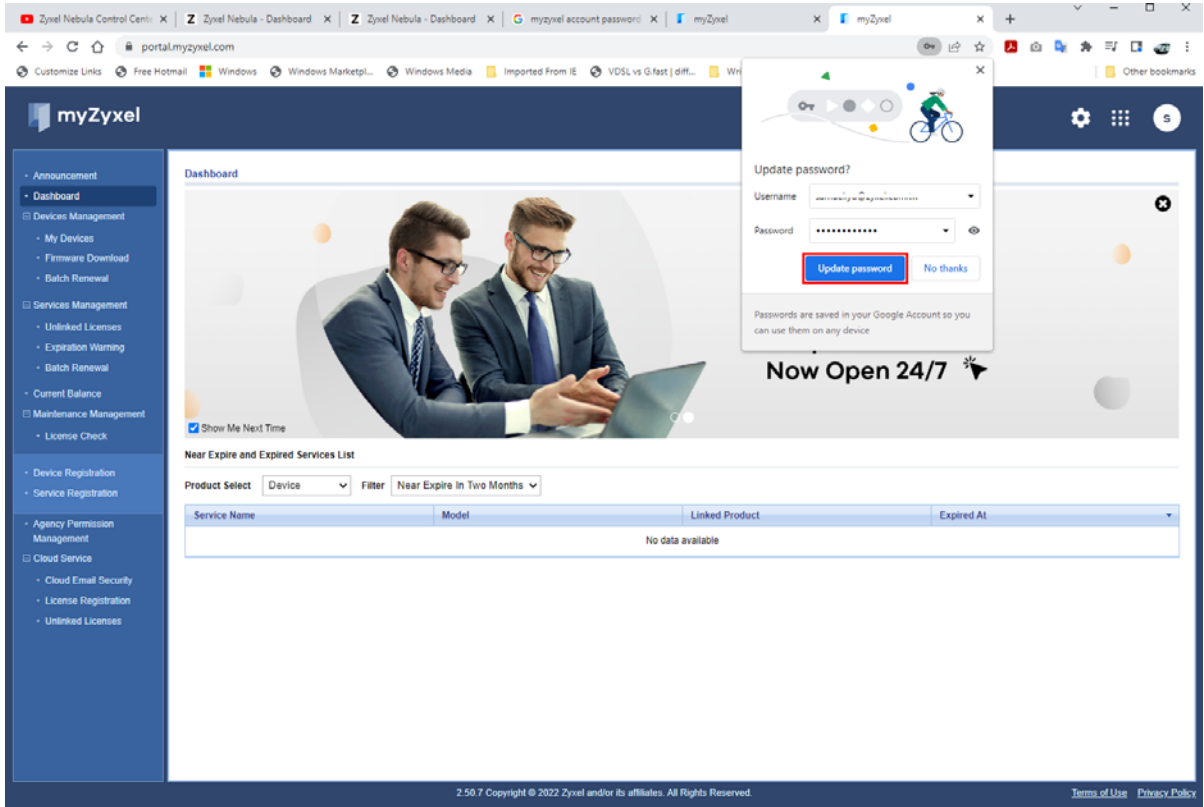


- 5 Enter the **New Password**. Use a minimum of 8 characters, including 0–9 a–z A–Z `~!@#\$\$%&\*(\_+={}|[];"/<> ?). Then click **Continue**.



- 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 > Configure > Settings**.

- 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 > General settings**.

The screenshot shows the 'General settings' page in NCC. Under the 'Site information' section, the 'Site name' field is highlighted with a red box and contains the text 'ZyNet TW'. Below it are two dropdown menus: 'Local time zone' set to 'Taiwan' and 'Site location' set to 'Asia - Taipei (UTC +8.0)'. A 'What is this?' link is visible at the bottom of the form.

- 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.

Site-wide > Configure > [Firmware management](#)

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?](#)

- 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.

Site-wide > Configure > [Firmware management](#)

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 Any

**Upgrade now** **+ Schedule upgrade**  1 selected in 7 devices

Status	Device type	Model	MAC address	S/N	Current version	Firmware status	Availability	Firmware type	Upgrade
<input checked="" type="checkbox"/>	Switch	NSW100-10P	B8:EC:A3:28:4C:BA	S172L13000021	V3.00(ABGO.2)   11/19/2019	Good	Upgrade available	Stable	No
<input type="checkbox"/>	Access point	WAX510D	D8:EC:E5:78:EC:BE	S212L40102451	V6.00(ABTF.0)   IT_20221019121600	Custom	Upgrade available	General Availability	No
<input type="checkbox"/>	Access point	NWA50AX	B8:EC:A3:DD:19:1C	S211942002072	V1.00(ABYW.0)	Warning	Upgrade available	General Availability	No
<input type="checkbox"/>	Access point	WAX650S	BC:CF:4F:56:BD:6D	S192L29290035	V6.50(ABRM.0)b5	Custom	Upgrade available	Beta	No
<input type="checkbox"/>	Access point	NWA50AX PRO	FC:22:F4:91:EF:82	S220Y51018102	V6.50(ACGE.0)b6	Custom	Upgrade available	General Availability	No
<input type="checkbox"/>	Access point	NWA90AX PRO	FC:22:F4:91:EF:DC	S220Y51018132	V6.50(ACGF.0)b6	Custom	Upgrade available	General Availability	No
<input type="checkbox"/>	Access point	WAX620D-6E	10:71:83:1B: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.

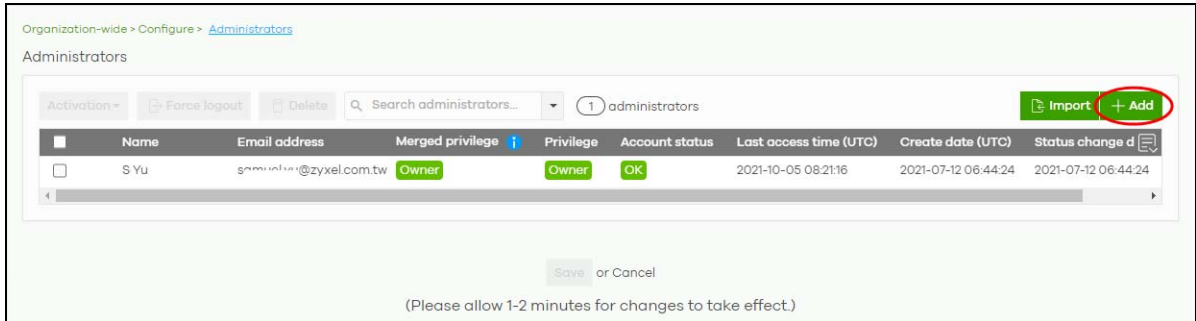
Device type	Model	MAC address	S/N	Current version	Schedule upgrade version
Access point	WAX510D	D8:EC:E5:78:EC:40	S212L40102453	V6.40(ABTF.4)	N/A

Cancel Add

## 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 > Configure > Administrators** screen. Click **+Add**.



- Enter the **Name** and **Email** of a myZyxel account. Assign the **Organization access (Full, Read-Only, None)**. See [Table 16 on page 161](#) 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** ✕

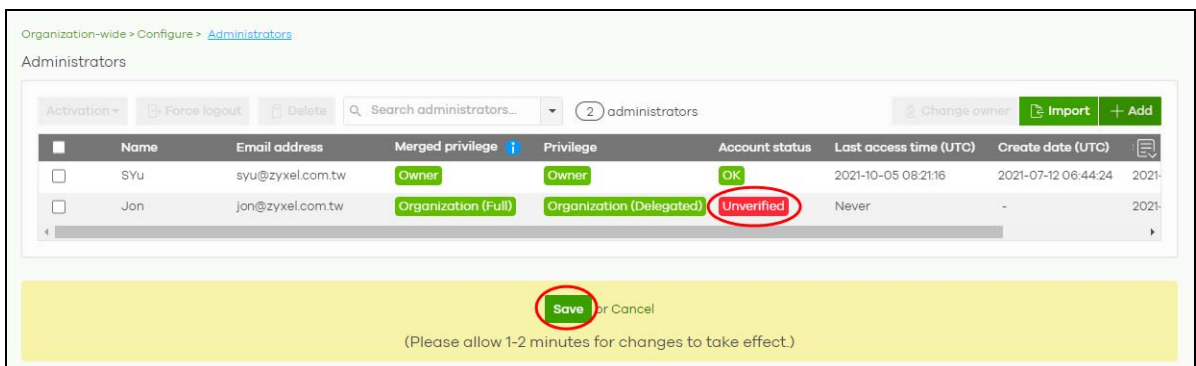
Name:  \*

Email:  \*

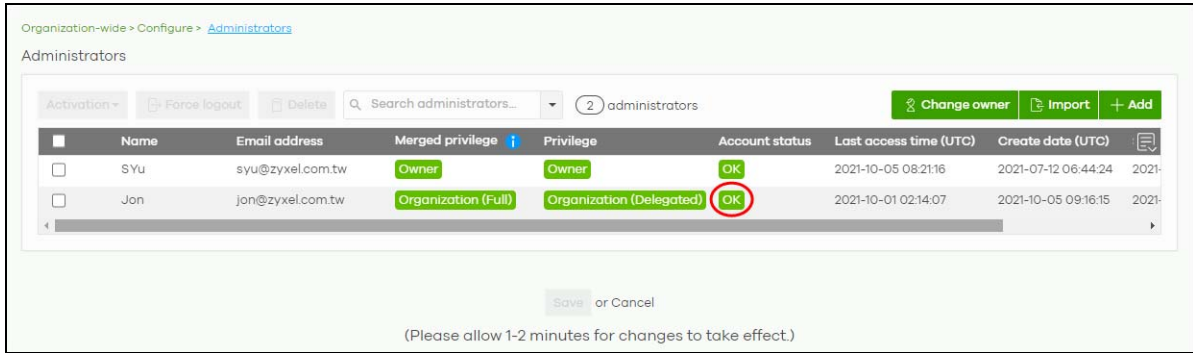
Organization access:

Activate:

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



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

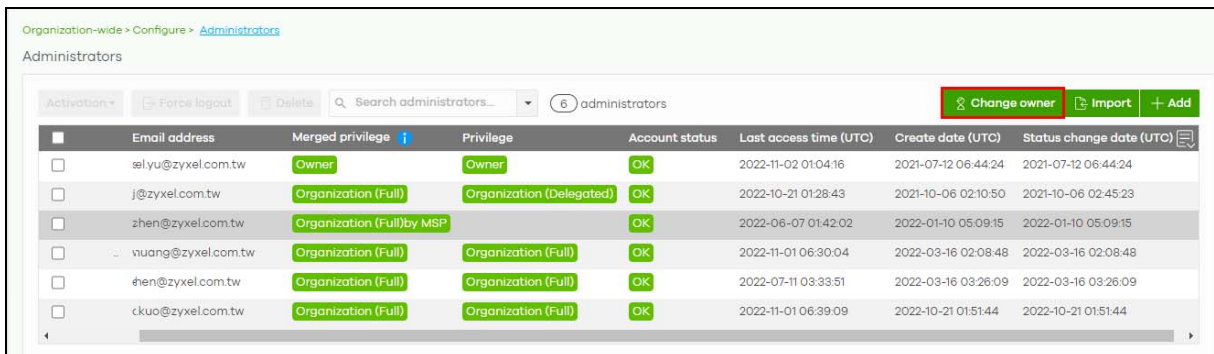


## 3.12 Transfer the Ownership of the Organization

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 > Configure > Administrators** screen. Click **Change owner**.



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

**Change organization owner** [X]

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?

No Yes

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 16 on page 161](#) 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 > Configure > Configuration templates** screen. Click **+Create**.

Organization-wide > Configure > Configuration templates

Configuration templates

+ Create Delete Search... 3 Template

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

Save or Cancel

- 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**.

The screenshot shows a dialog box titled "Create a new template". It has a close button (X) in the top right corner. The form contains the following fields and options:

- Template name:** A text input field containing "SSID Template 2" with a red asterisk indicating a required field.
- Template description:** A text input field containing "Zyxel".
- Import settings from:** A dropdown menu that is currently open, showing a search icon and a list of items. The list is divided into two sections: "Sites" (with "Hsinchu" highlighted) and "Templates" (with "Site-wide general").
- Create new configuration template:** A radio button that is selected.
- Target sites:** A dropdown menu with a downward arrow.
- Create:** A button located at the bottom right of the dialog.

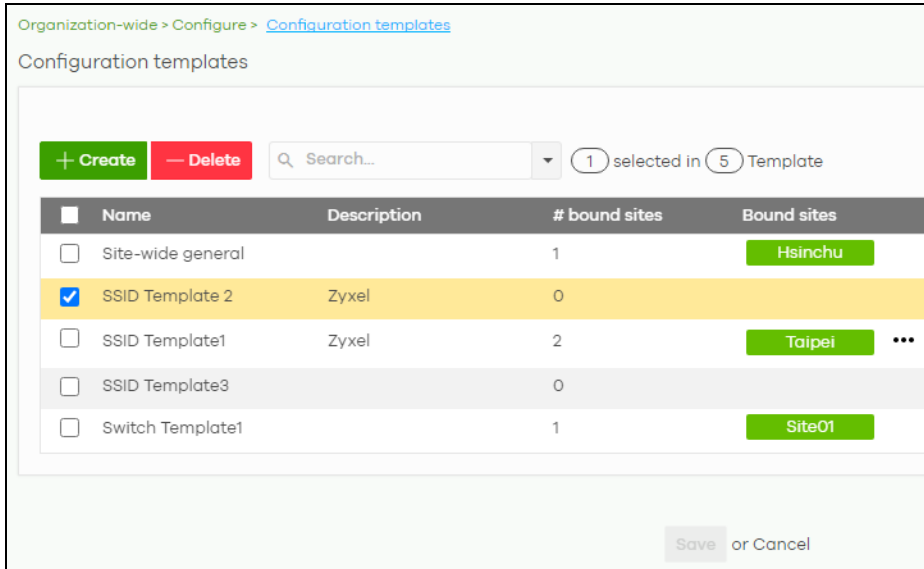
Note: Under **Import settings from**, select a site from **Sites** to copy a site's settings. Under **Import setting from**, select a template from **Templates** to copy a site's site-wide general setting, an Access Point's SSIDs setting or a Switch's port setting.

- 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.

The screenshot shows the same "Create a new template" dialog box. In this view, the "Import settings from" dropdown is closed, and the "Create new configuration template" radio button is selected. The "Target sites" dropdown is open, showing a list of sites: "Hsinchu", "Kaohsiung", "Site01", and "Taipei". The "Create" button is now highlighted in green, and a "Close" button is visible next to it.

If you skip this step, you can bind a template to a site later. Go to the **Organization-wide > Configure > 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.





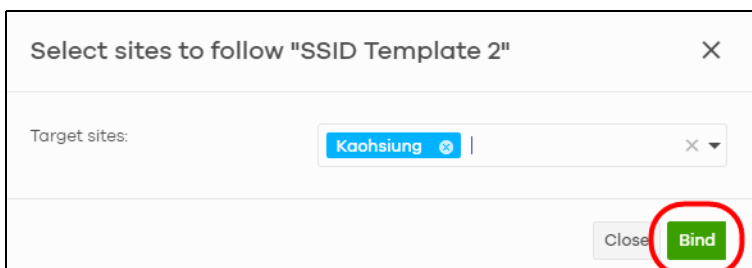
- 4 The following screen appears. Click **Bind additional site** to select the site you want to bind the template to.



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



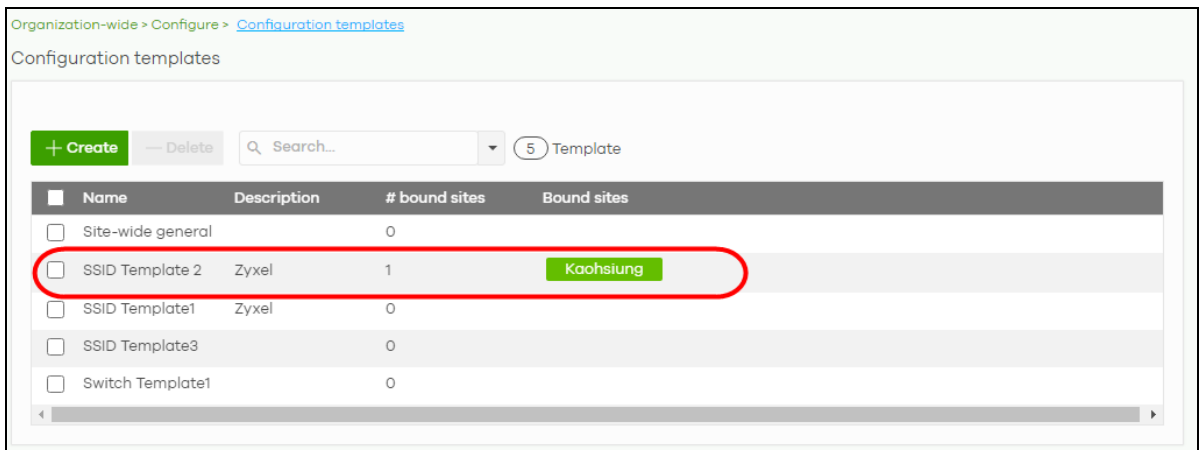
- 6 Select a site from the **Target sites** drop-down box list and then click **Bind**.



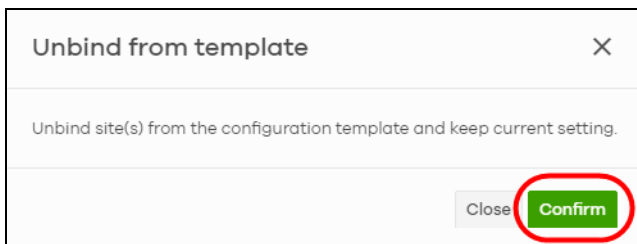
- 7 Click **Save** to save the changes.



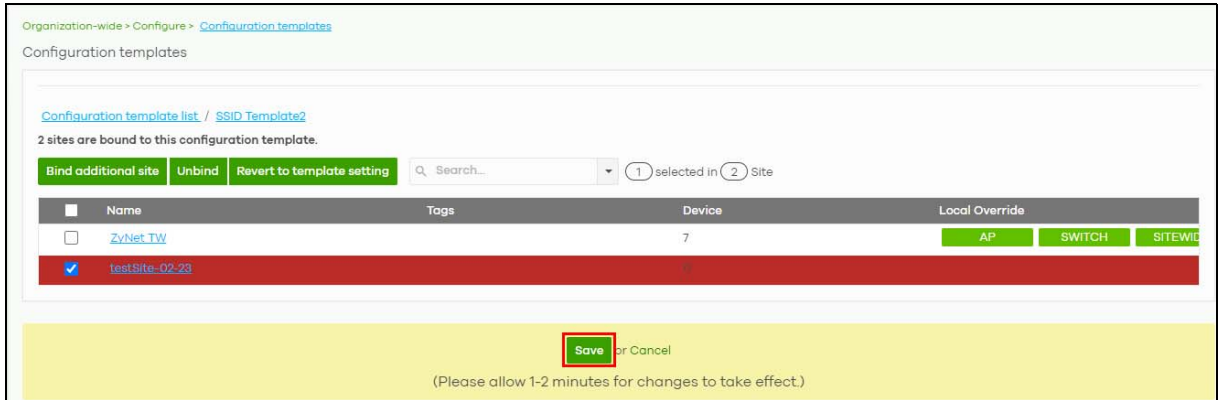
- 8 A configuration template is created as shown in the **Organization-wide > Configure > Configuration templates** screen.



- 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.



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



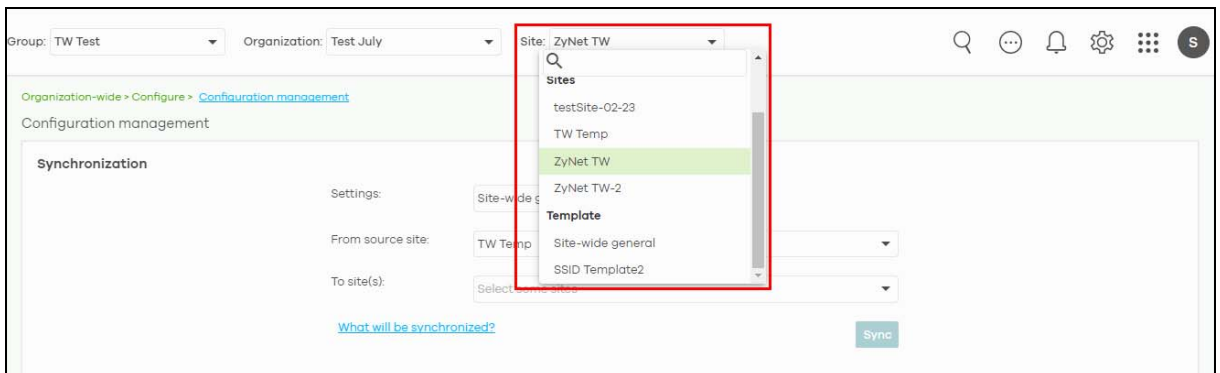
### 3.13.2 Duplicate and Import a Template Setting to a Site

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.



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

Organization-wide > Configure > [Configuration management](#)

Configuration management

### Synchronization

Settings:

From source site:

To site(s):

[What will be synchronized?](#)

### Switch settings clone

From source device:

To device(s):

Include uplink port settings

[What will be cloned?](#)

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

Organization-wide > Configure > [Configuration management](#)

Configuration management

### Synchronization

Settings:

From source site:

To site(s):

[What will be synchronized?](#)

### Switch settings clone

From source device:

To device(s):

Include uplink port settings

[What will be cloned?](#)

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

Organization-wide > Configure > [Configuration management](#)

Configuration management

**Synchronization**

Settings:

From source site:

To site(s):

[What will be synchronized?](#)

**Switch settings clone**

From source device:

To device(s):

Include uplink port settings

[What will be cloned?](#)

## An Access Point's SSID Setting

- 1 Go to **Organization-wide > Configure > 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.

Organization-wide > Configure > [Configuration management](#)

Configuration management

**Synchronization**

Settings: SSIDs

From source site: Site-wide general settings

From source site: SSIDs

To site(s): Kaohsiung

[What will be synchronized?](#)

**Sync**

---

**Switch settings clone**

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

To device(s):

Include uplink port settings

[What will be cloned?](#)

**Clone**

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

Organization-wide > Configure > [Configuration management](#)

Configuration management

**Synchronization**

Settings: SSIDs

From source site: Hsinchu

To site(s):

Hsinchu

Kaohsiung

Site01

Taipei

[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?](#)

**Clone**

- 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.

Organization-wide > Configure > [Configuration management](#)

Configuration management

**Synchronization**

Settings:

From source site:

To site(s):

[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 > Configure > 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.

Organization-wide > Configure > [Configuration management](#)

Configuration management

**Synchronization**

Settings:

From source site:

To site(s):

[What will be synchronized?](#)

---

**Switch settings clone**

From source device:

To device(s):

Include uplink port settings

[What will be cloned?](#)

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

Organization-wide > Configure > [Configuration management](#)

Configuration management

**Synchronization**

Settings:

From source site:

To site(s):

[What will be synchronized?](#)

---

**Switch settings clone**

From source device:

To device(s):

Include uplink port settings

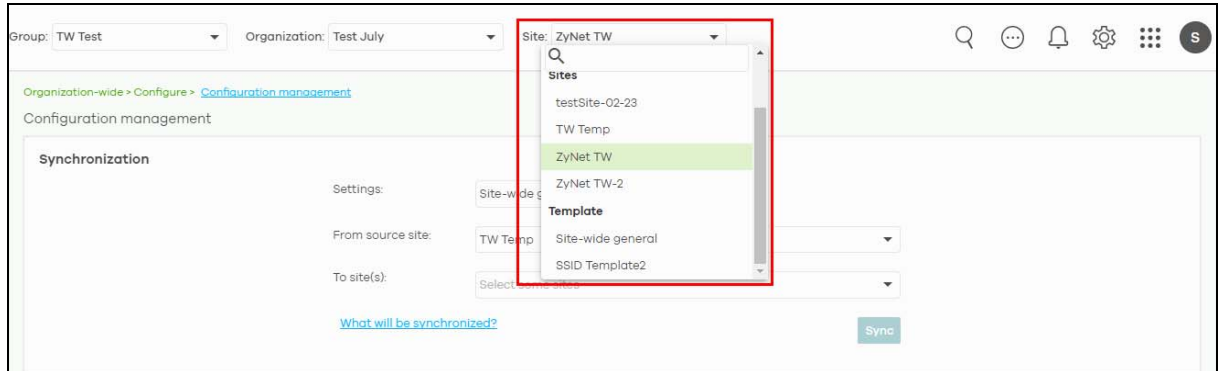
[What will be cloned?](#)



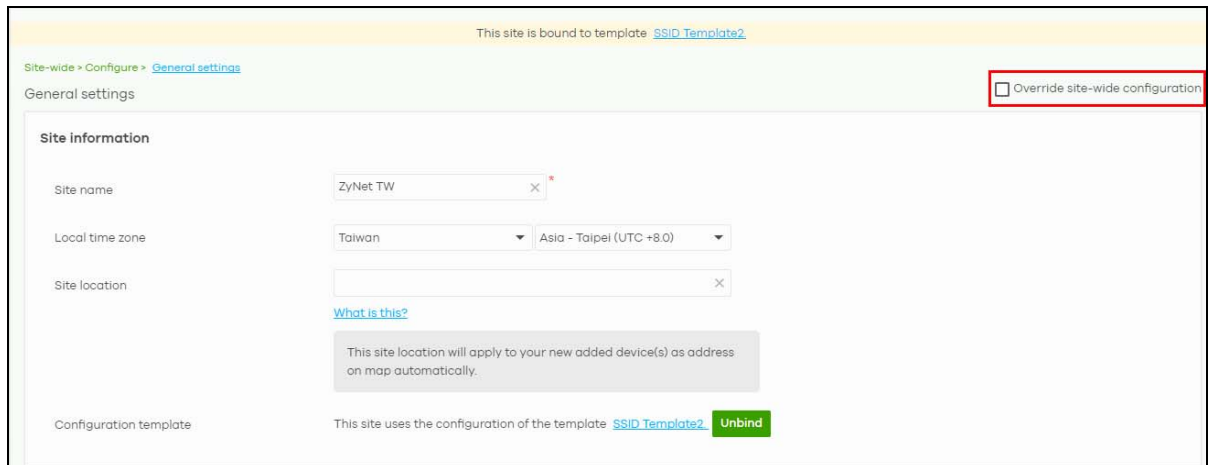
### 3.13.3 Enable the Override Site-wide Configuration (Local Override) Feature

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.

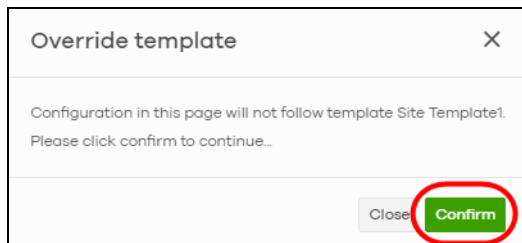
This section shows you how to enable the **Override site-wide configuration** feature to update site information. Select a bound site from the **Site** drop-down list box to edit the details of the selected site.



- 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.



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



- 3 In the **Site-wide > Configure > General 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](#).

Site-wide > Configure > [General settings](#)

General settings  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 > Configure > 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.

Organization-wide > Configure > [Configuration templates](#)

Configuration templates

[Configuration template list](#) / [Site Template1](#)

1 site are bound to this configuration template.

[Bind additional site](#) [Unbind](#) [Revert to template setting](#) Search... 1 selected in 1 Site

Name	Tags	Device	Local Override
<input checked="" type="checkbox"/> <a href="#">Hsinchu</a>		0	<a href="#">AP</a>

[Save](#) or [Cancel](#)

(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...

[Close](#) [Confirm](#)

## Overwrite the Access Point / Switch Setting

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

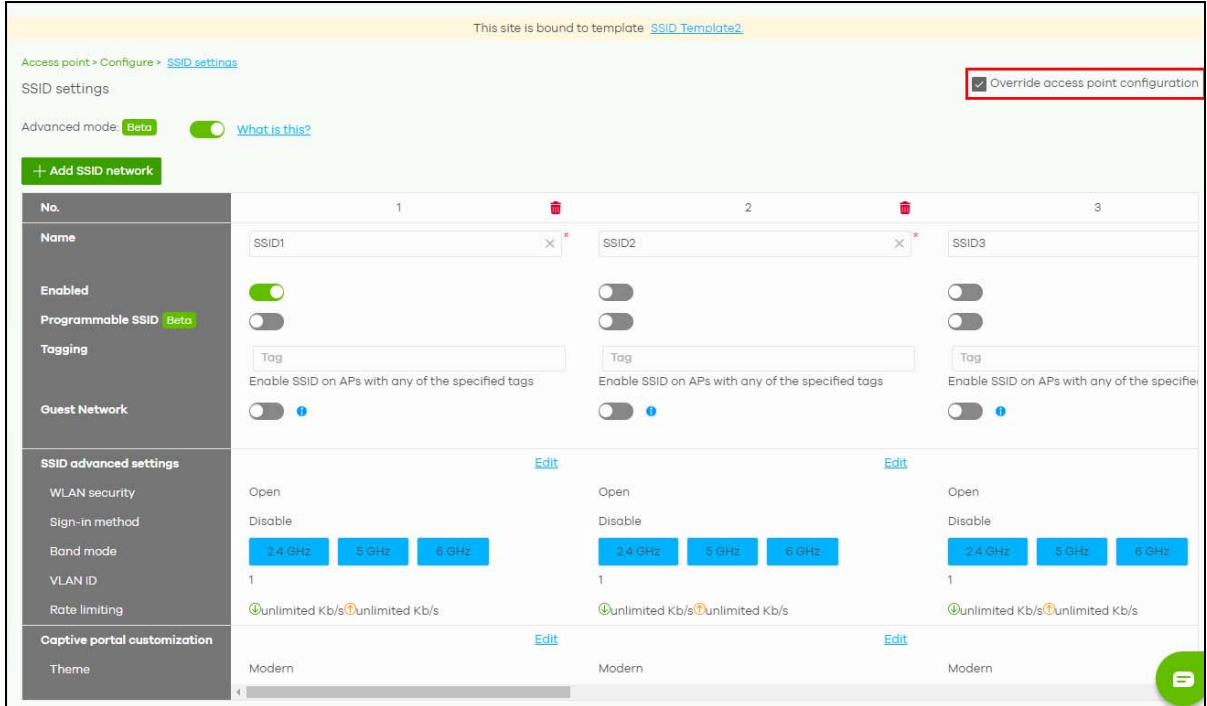
Note: If the local override configuration is enabled on one page, all configuration pages of the Nebula Devices in the selected site will be enabled.

The screenshot shows the 'SSID advanced settings' page. At the top right, there is a checkbox labeled 'Override access point configuration' which is checked and highlighted with a red circle. Below this, the 'Network access' section is visible, containing 'Security options' and 'Sign-in method' with various radio button and dropdown menu options.

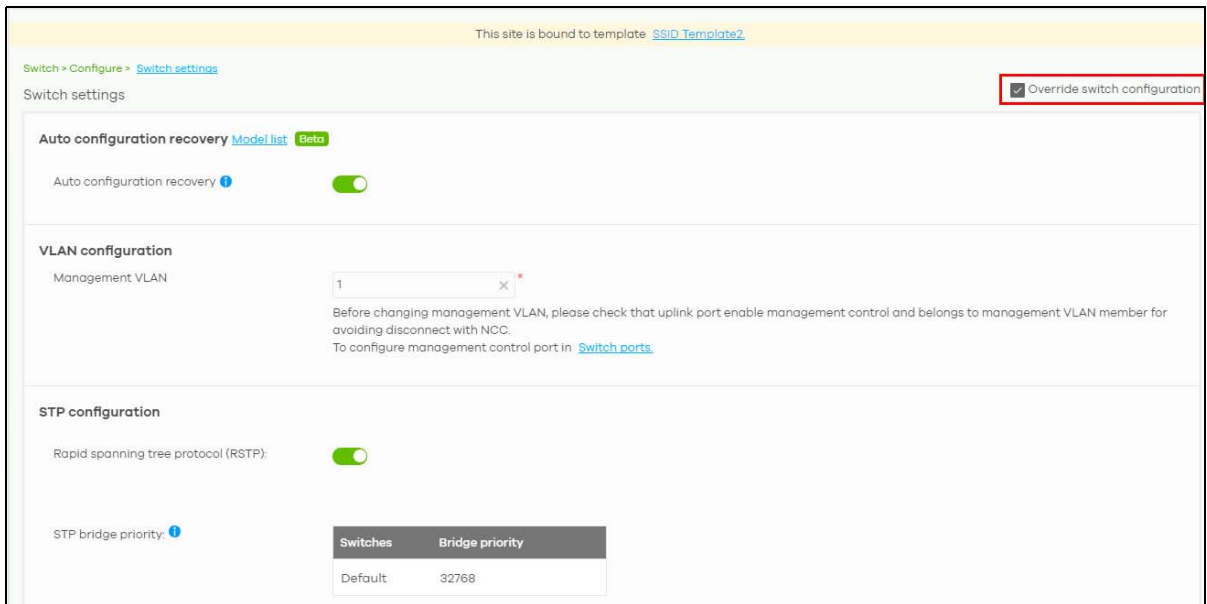
- 2 This allows a specific type of Nebula Device setting override. The following screen appears. Click **Confirm** to continue.

The screenshot shows a dialog box titled 'Override template'. The text inside reads: 'Configuration in this page will not follow template Site Template1. Please click confirm to continue...'. At the bottom right, there are two buttons: 'Close' and 'Confirm'. The 'Confirm' button is highlighted with a red circle.

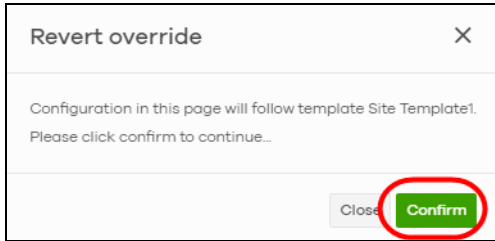
- 3 In **Access point > Configure > SSID settings**, edit your SSIDs, authentication or captive portal settings on the following page. Click **Save** to save the changes.



In the **Switch > Configuration > 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.



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

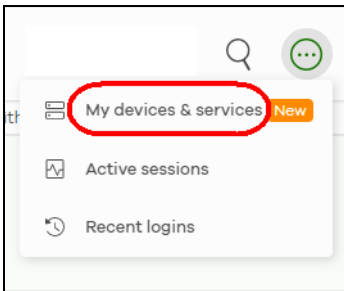


## 3.14 Activate an MSP License

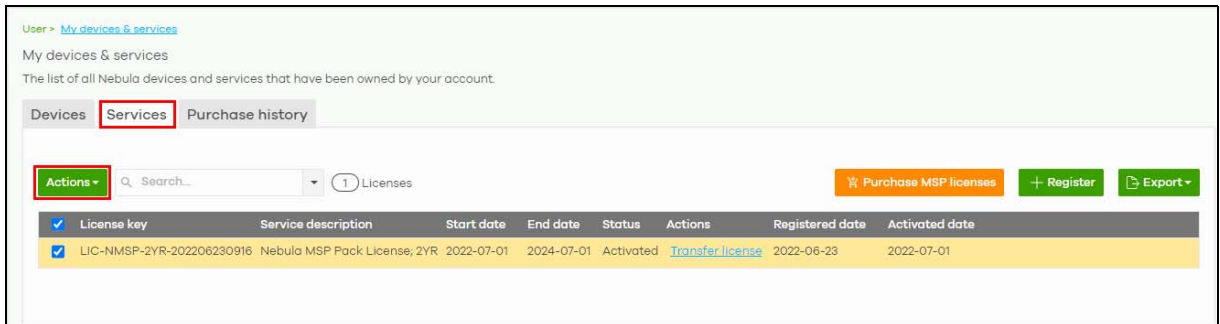
You must have an NCC account and an MSP license pack to activate an MSP license.

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.



- 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 4 on page 153](#) 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 **Access point > Configure > Security service**.
- 2 Refer to [Section 12.3.7 on page 561](#) for details on how to configure the **Threat Protection** fields.

The screenshot shows the 'Threat Protection' configuration page. The settings are as follows:

- 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:
- 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:**
- DNS Threat exempt list:**

- 3 Then click **Save**.

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

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



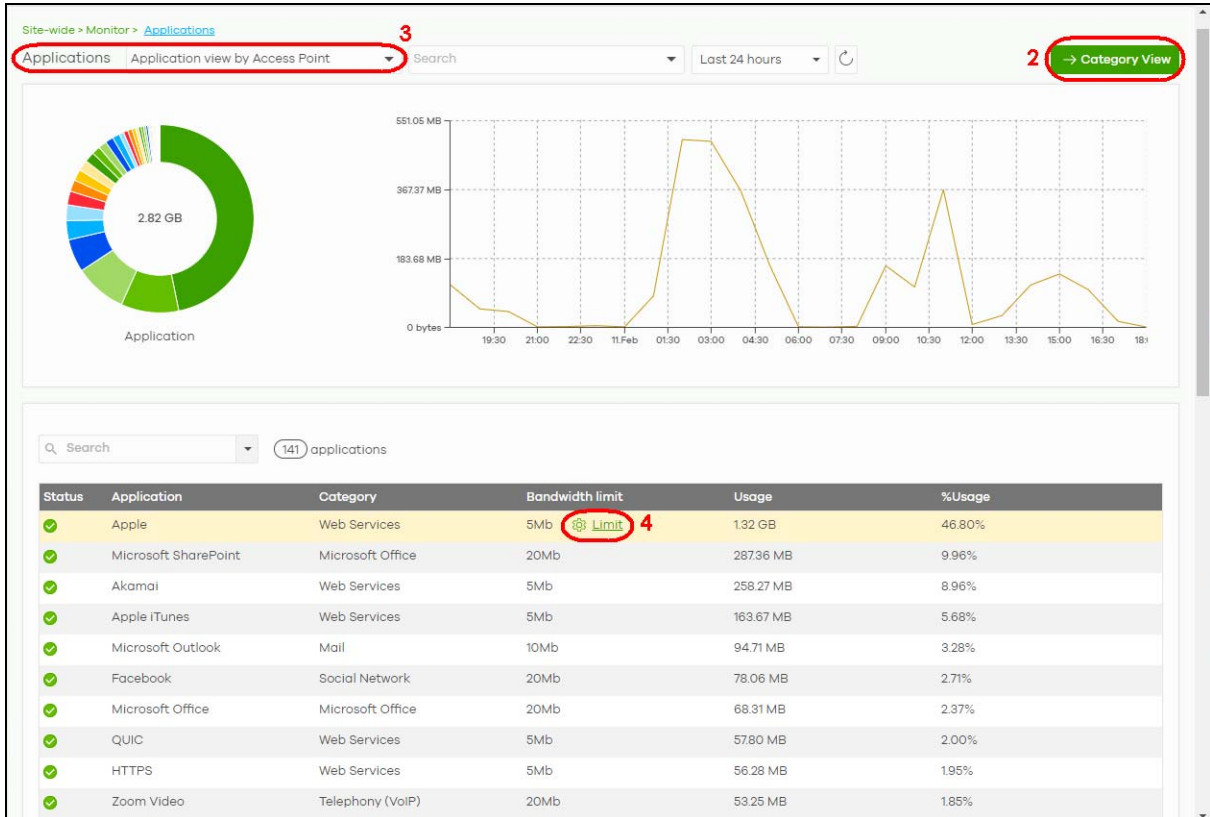
### 3.15.2 Application Visibility & Optimization

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.

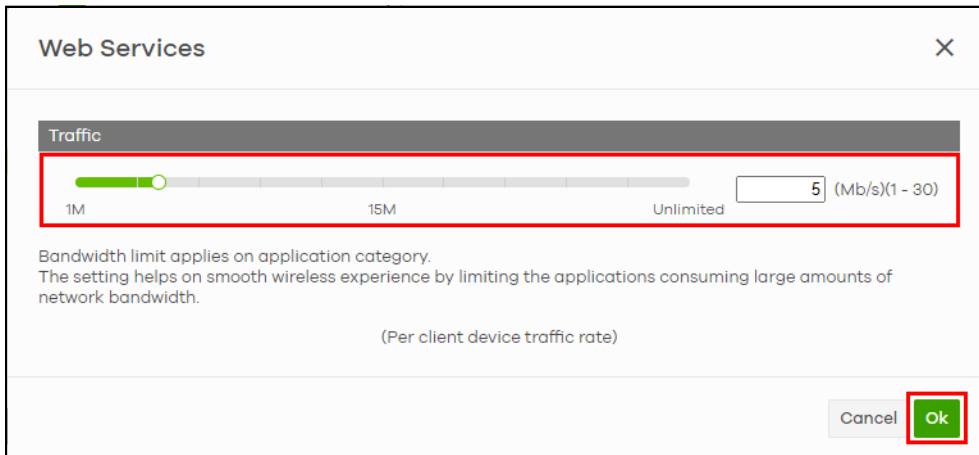
Application optimization is a way to limit the bandwidth usage of applications in the WiFi network. For example, applications that need real time traffic such as video streaming may use more resources. Use application optimization to limit the bandwidth used to stream video to prevent it from slowing 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 > Monitor > Applications > 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 > Monitor > Applications**.
- 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**.



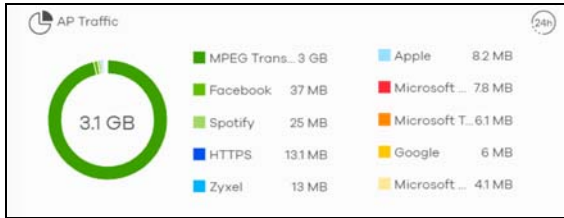
5 Use the slider or enter the **Traffic** allowed in **Mb/s** (1 – 30 or **Unlimited**).



6 Then click **Ok**.

To monitor the application bandwidth usage, go to **Site-wide > Monitor > Dashboard: AP Traffic** 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 > Configure > License & inventory > Devices** tab (1).
- 2 Click the check box (2) to select all Nebula Devices.
- 3 Click the **Actions** button (3).

Organization-wide > Configure > License & inventory

License & inventory

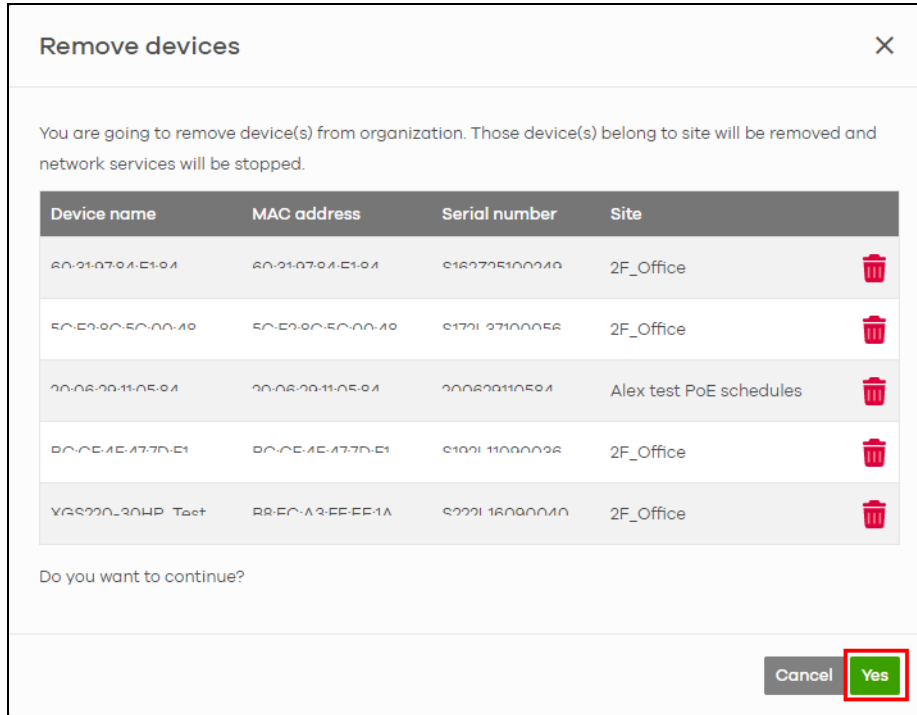
Overview **1 Devices** Licenses Trial Change log Purchase History

1 Access Point 3 Switch 1 Security Appliance 0 Mobile Router

3 Actions - In use Unused Both Search... 5 selected in 5 devices. + Add Export -

2	Device name	Device type	Model	Serial number	MAC address	Claim date	License expiration date	License info	Actions
<input checked="" type="checkbox"/>	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 -
<input checked="" type="checkbox"/>	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 -
<input checked="" type="checkbox"/>	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 -
<input checked="" type="checkbox"/>	BC:CF:4F:47:7D:F1	Switch	GS1350-8HP	S192L11090036	BC:CF:4F:47:7D:F1	2022-12-20	2023-07-05	Nebula Professional Pack	Actions -
<input checked="" type="checkbox"/>	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.

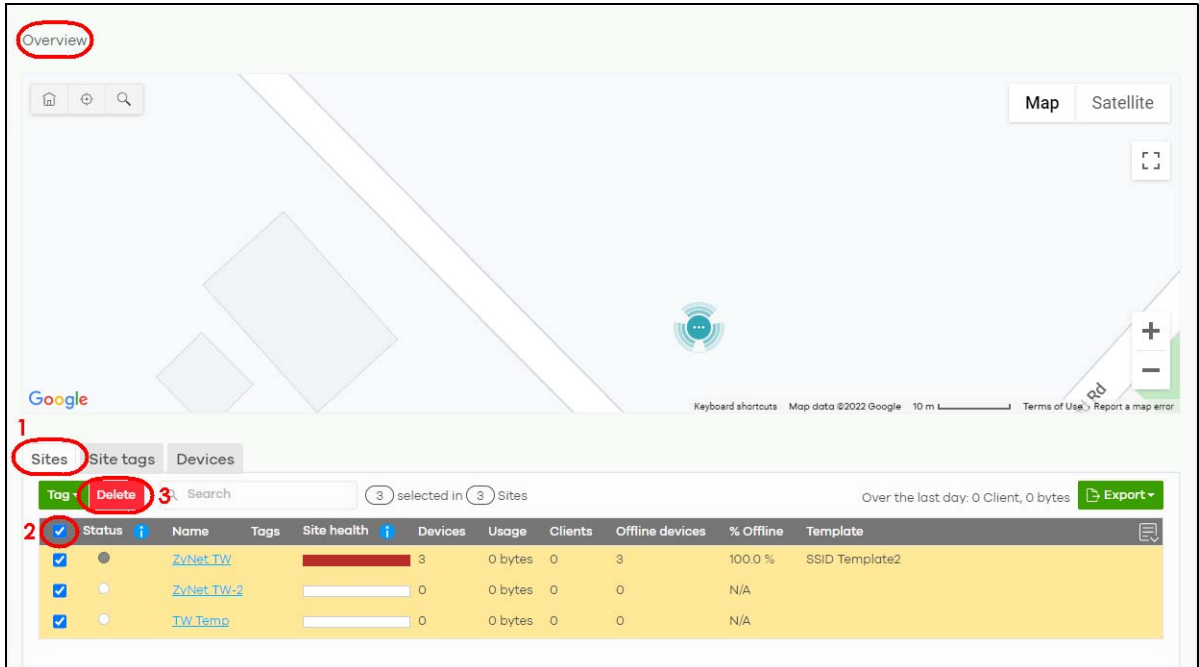


### 3.16.2 Transfer All Licenses

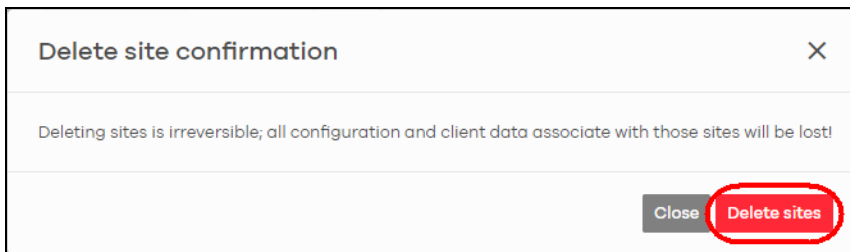
See [Section 3.7 on page 63](#) in this chapter for information on how to transfer licenses assigned to an organization and Nebula Device to another Nebula Device in a different organization.

### 3.16.3 Delete All Sites

- 1 Go to **Organization-wide > Monitor > Overview > Sites** tab (1).
- 2 Click the check box (2) to select all sites.
- 3 Click the **Delete** button (3) to remove all sites.

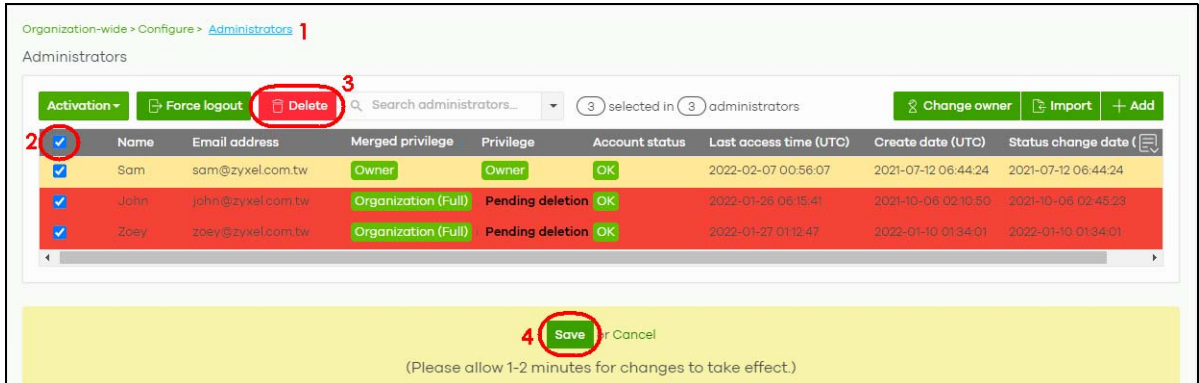


- 4 Click the **Delete sites** button to confirm.



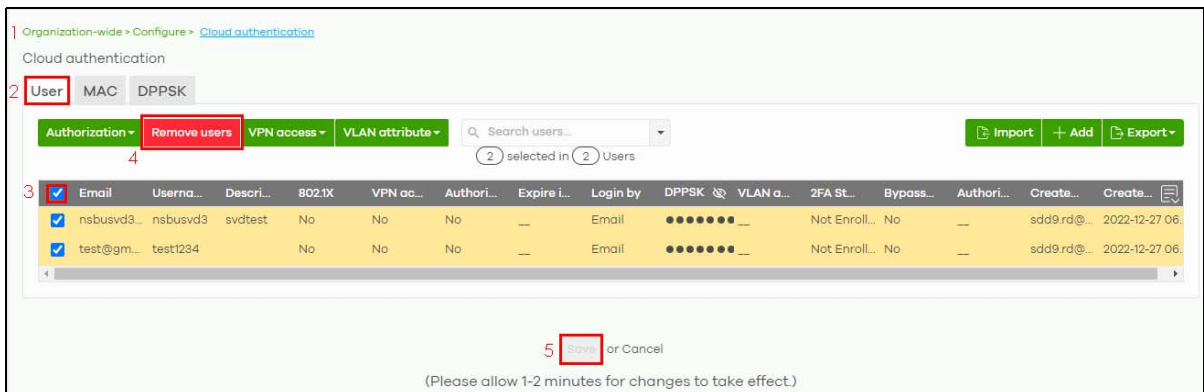
### 3.16.4 Delete All Administrators

- 1 Go to **Organization-wide > Configure > 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.



### 3.16.5 Remove All Users

- 1 Go to **Organization-wide > Configure > 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.



### 3.16.6 Delete the Organization

- 1 Go to **Organization-wide > Configure > 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 **1**

Settings

**Organization information**

Name:  **2**

Country:

**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

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.

**Delete organization** **3**

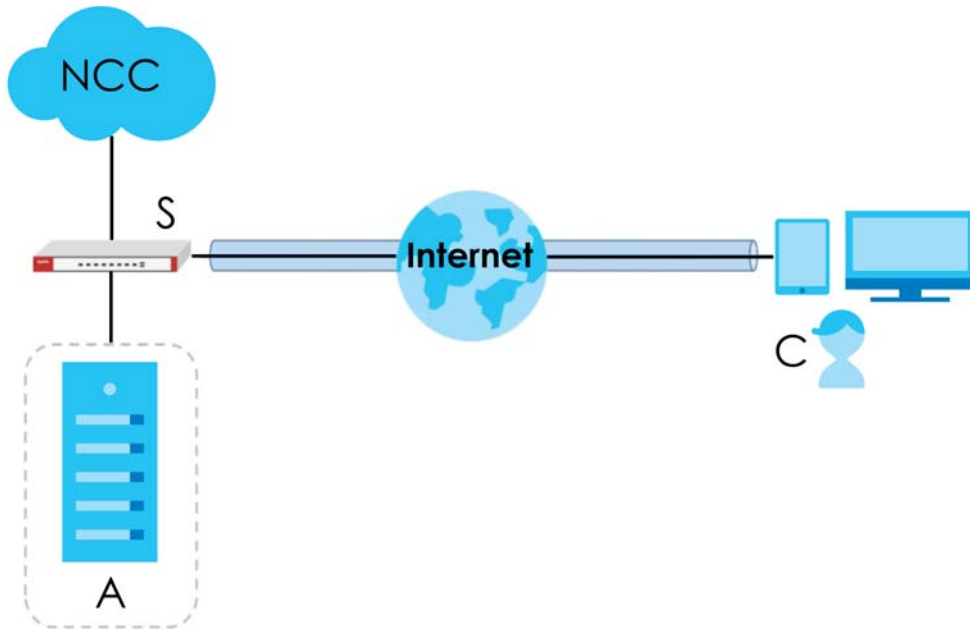
- 4 Click the **OK** button to confirm.

**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:

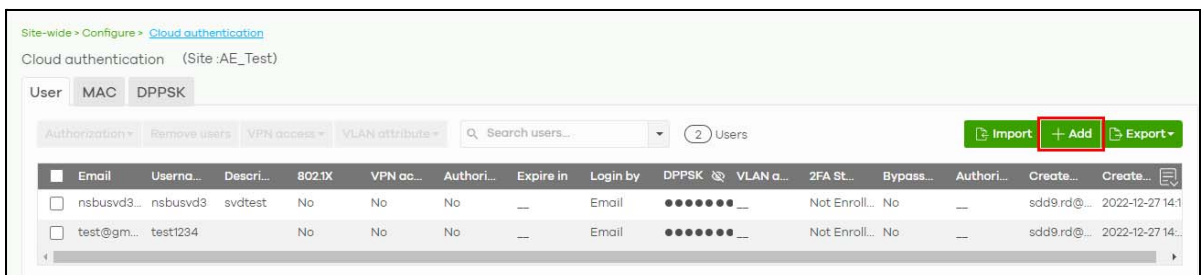
- Create a VPN user
- Enable the remote access VPN rule for IPSec VPN client
- Check the connection in Nebula.

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.



- 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.

**Create user**

3 Click Save.

Site-wide > Configure > Cloud authentication  
 Cloud authentication (Site :AE\_Test)

User MAC DPPSK

Authorization Remove users VPN access VLAN attribute Search users... 3 Users **Import + Add Export**

	Email	Username	Description	802.1X	VPN access	Authorized	Expires in	Login by	DPPSK	VLAN assignment	2FA Status	Bypass	Authorized	Create...	Create...
<input type="checkbox"/>	nsbusvd3...	nsbusvd3	svdtest	No	No	No	—	Email	●●●●●●	—	Not Enroll...	No	—	sdd9.rd@...	2022-12-27 14:1
<input type="checkbox"/>	test@gm...	test1234		No	No	No	—	Email	●●●●●●	—	Not Enroll...	No	—	sdd9.rd@...	2022-12-27 14:1
<input type="checkbox"/>	vpnuser...	vpnuser		No	Yes	Yes	Never	Username...	—	—	Not Enroll...	No	—	samuelyu...	—

**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 **Firewall > Configure > 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**.

The screenshot shows the 'Remote access VPN' configuration page. The 'IPSec VPN server' toggle is turned on and highlighted with a red box. Below it, the 'Client VPN subnet' is set to '192.168.100.0/24' and 'IKE version' is set to 'IKEv2'. The 'Authentication' dropdown is set to 'Nebula Cloud Authentication', and the 'Two-factor authentication with Captive Portal' toggle is also turned on and highlighted with a red box. The 'SecuExtender IKEv2 VPN configuration provision' field contains two email addresses: 'vpnuser@zyxel.com' and 'samuel.yu@zyxel.com.tw'. At the bottom, the 'Save' button is highlighted with a red box.

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

This screenshot is identical to the previous one, but the 'Send Email' button is now highlighted with a red box. The 'Save' button is no longer highlighted.

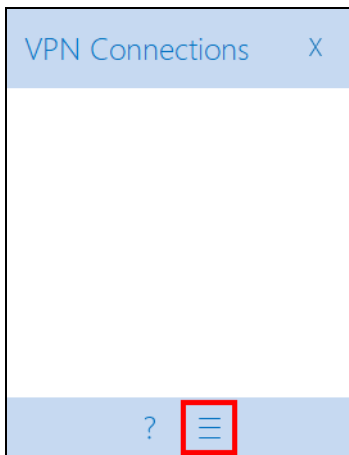


### 3.17.3 VPN Setup by the VPN Client

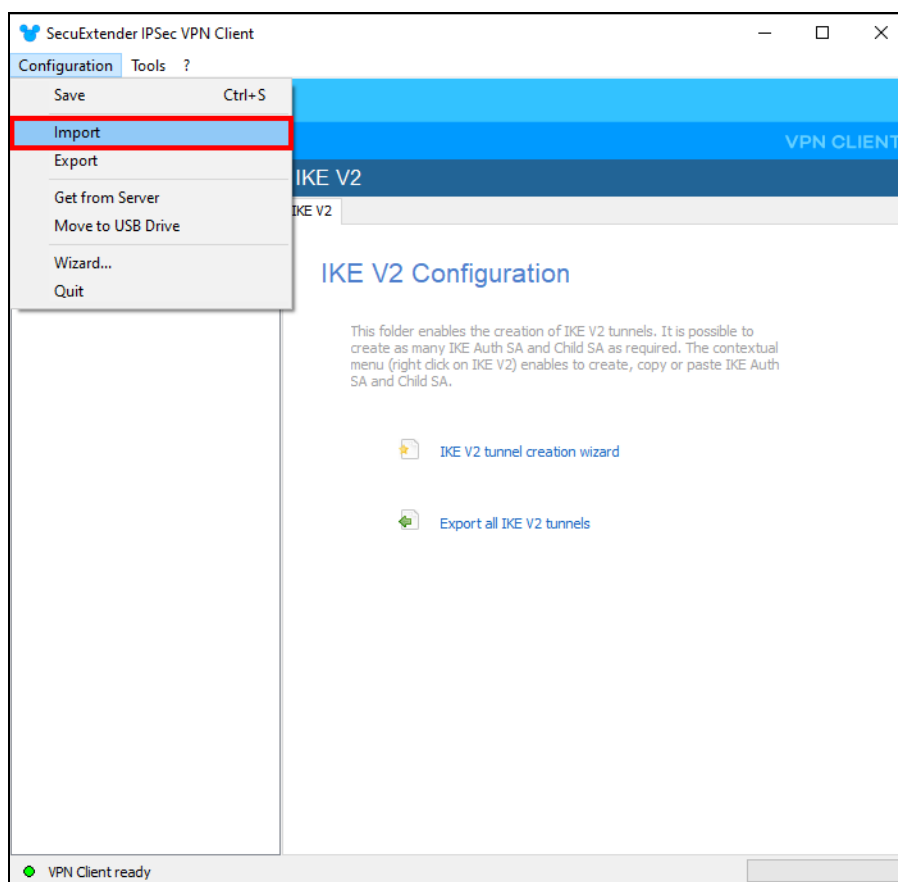
- 1 The VPN client should receive the following emails:
  - **Configuration for SecuExtender IPSec VPN Client** email with attached VPN configuration file (.tgb). Save the configuration file in your computer.
  - **Nebula Cloud Account Information** email with the following login information: **Email**, **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

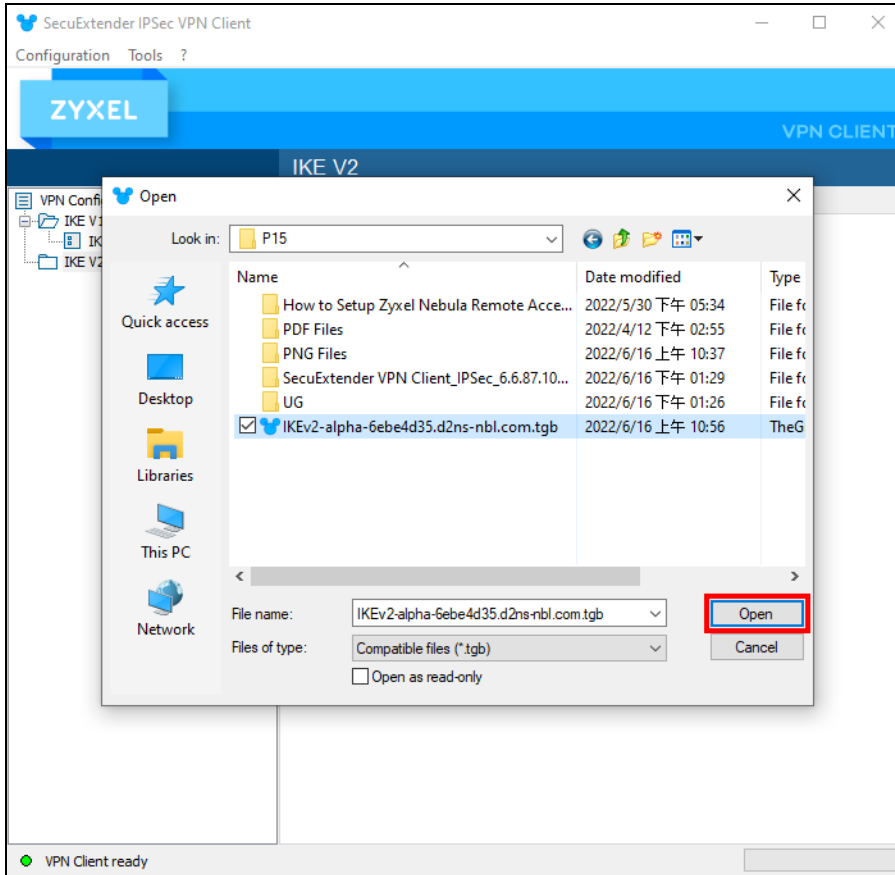
- 1 Save the attached VPN configuration file (.tgb) from the **Configuration for SecuExtender IPSec VPN Client** email on the VPN user's computer.
- 2 On your computer, open SecuExtender. Click the menu icon.



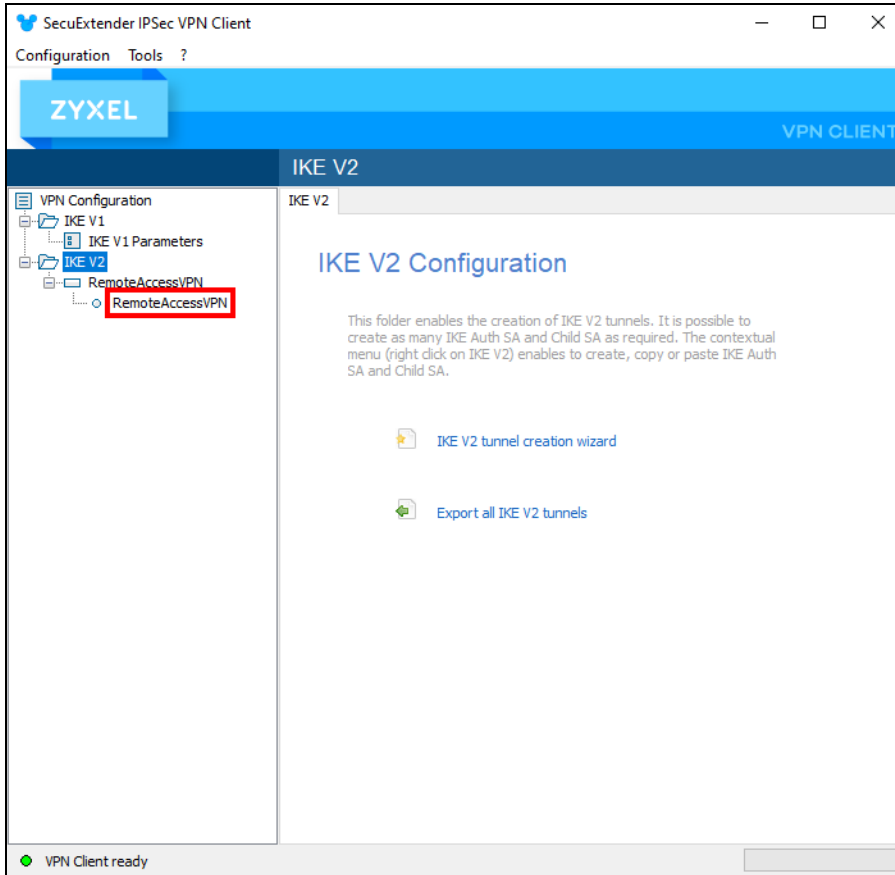
- 3 Click **Configuration > Import**.



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

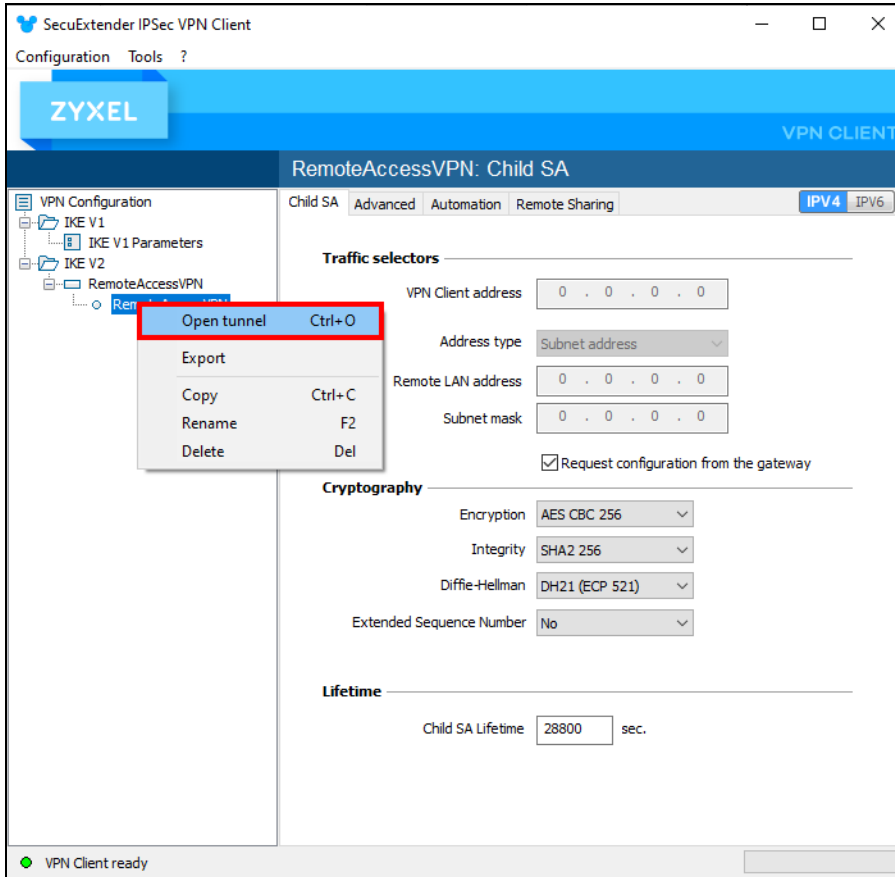


- 5 Click RemoteAccessVPN in VPN Configuration > IKE V2 > RemoteAccessVPN.

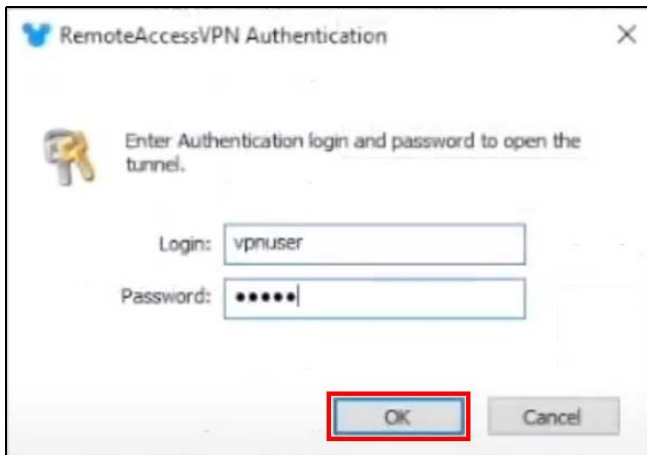


### 3.17.5 Open the VPN Tunnel

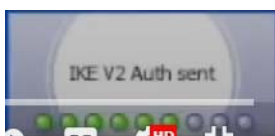
- 1 Right-click **RemoteAccessVPN** in **VPN Configuration > IKE V2 > RemoteAccessVPN** and click **Open tunnel**.



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



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

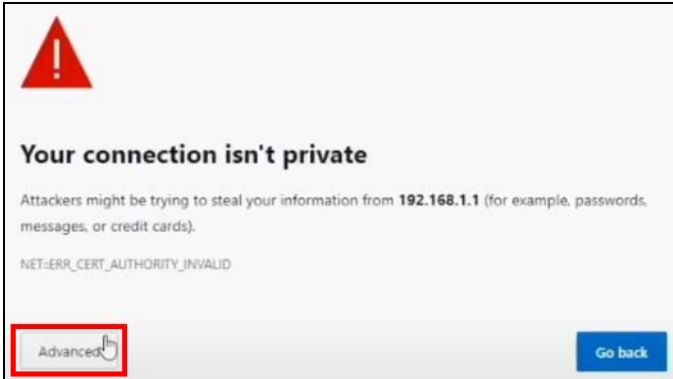


Wait until **Tunnel opened** appears on the lower right of the screen.

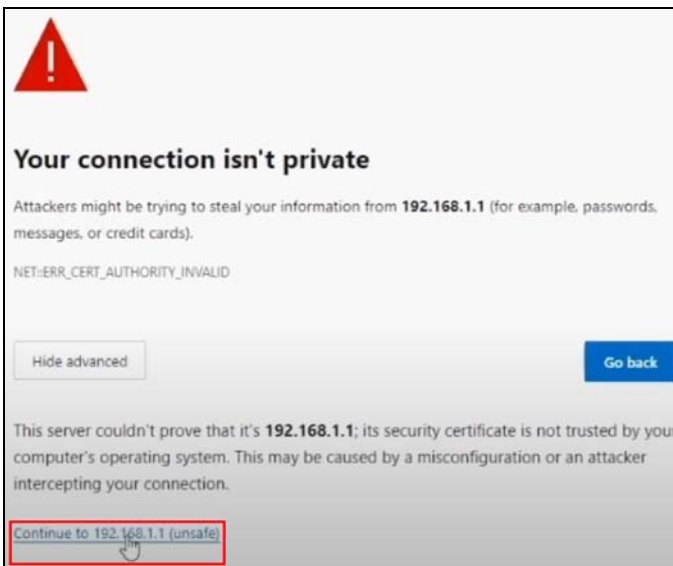


An IP address will now appear in **VPN Client address** to replace the previous **0.0.0.0**. The button lights green in front of **RemoteAccessVPN** in **VPN Configuration > IKE V2 > RemoteAccessVPN**.

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

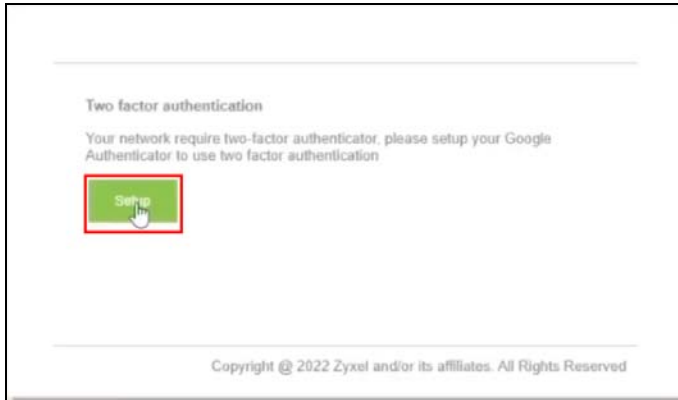


- 4 Click the **Continue to xxx.xxx.x.x (unsafe)** link on the bottom of the screen.

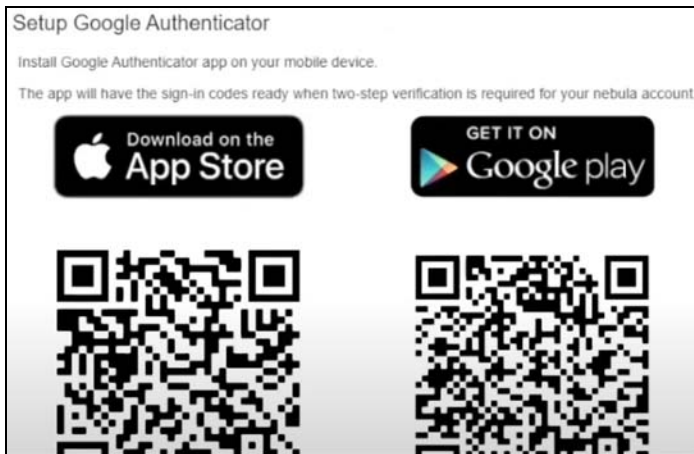


### 3.17.6 Set Up Two Factor Authentication to Bind the User Account

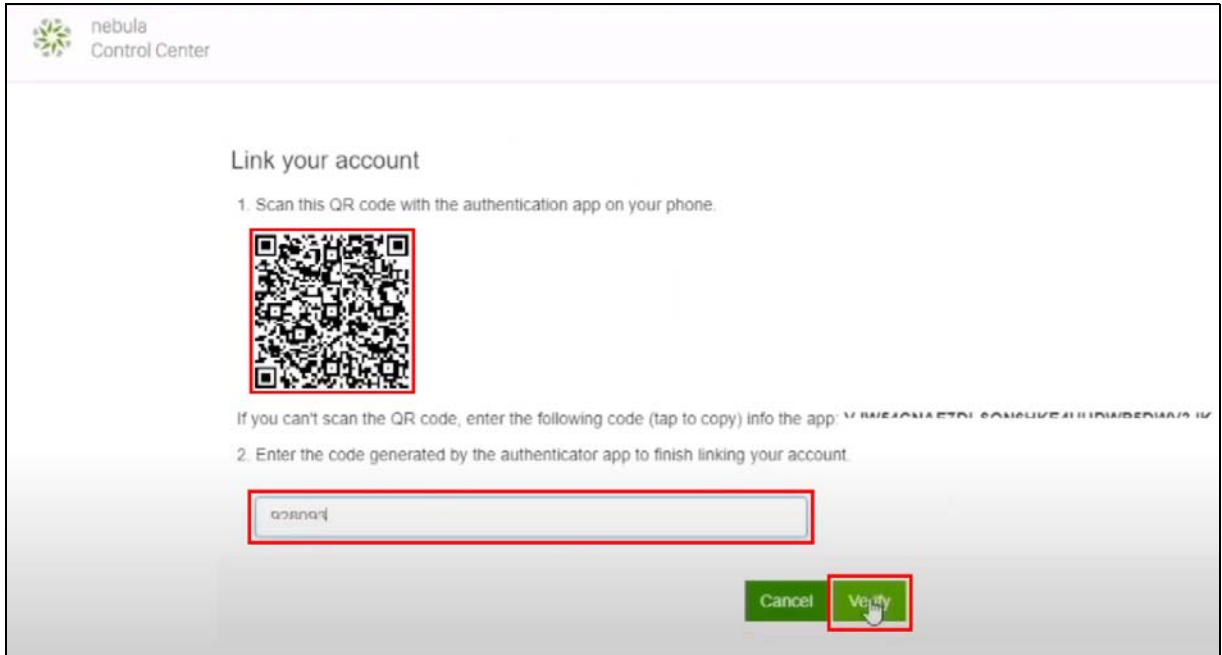
- 1 On the **Two factor authentication** screen, click **Setup**.



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

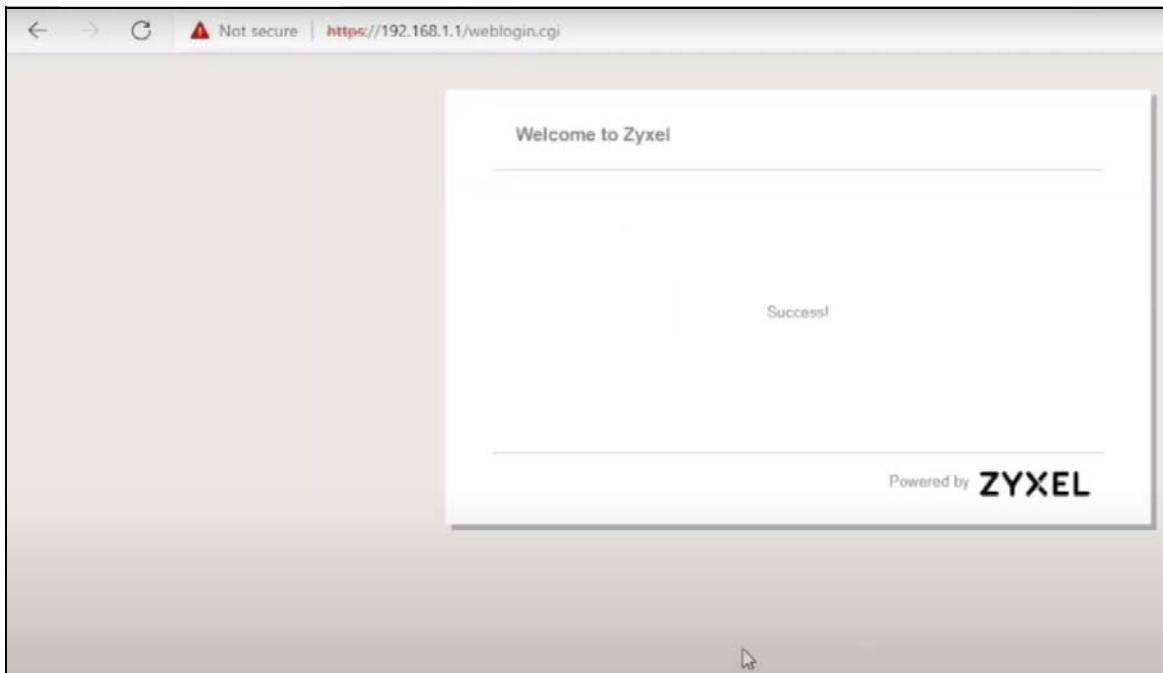


- 2 Use the **Google Authenticator** app to scan the QR code. The QR code contains the user account information created in step 2 of [Create a VPN User](#). Enter the code. Then click **Verify**.



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.



### 3.17.7 Check the Connection in Nebula by the Administrator

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



Firewall > Monitor > VPN connections

VPN connections

**Connection status**  
Configuration: This security gateway is exporting 2 subnet over the VPN: 192.168.10.0/24, 192.168.20.0/24

**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

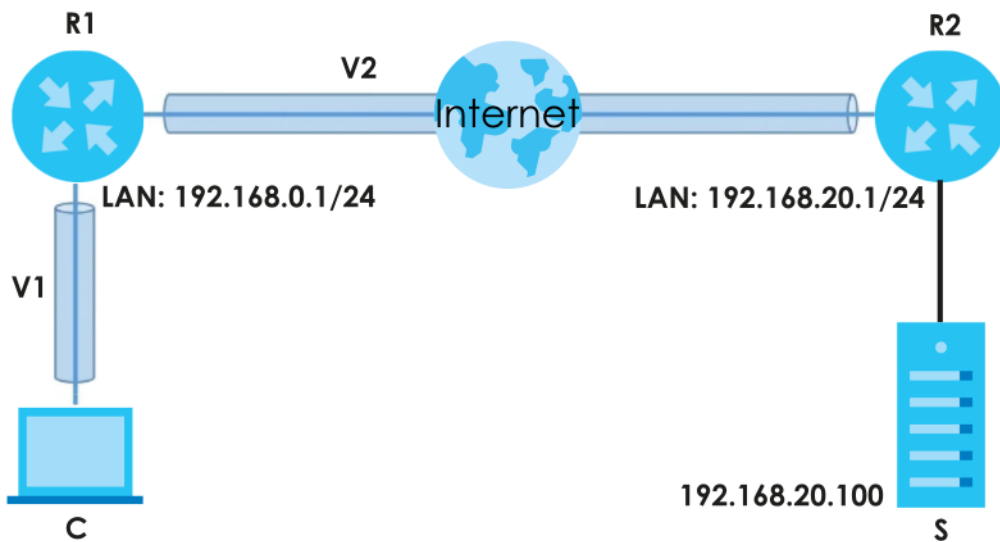
**Client to site VPN login account**

User Name	Hostname	Assigned IP	Public IP
vpnuser		192.168.100.3	114.42.70.127

### 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 **Firewall > Configure > Routing: Policy Route/Traffic Shaping: Add**.

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

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

Update policy route / Traffic Shaping Rule
✕

---

**Matching Criteria**

Description:

Source:

Destination:

Service:

---

**Policy Route**

Type:

Next-Hop:

---

Traffic Shaping

Update
Close

## 3.19 Resolve WiFi Connection Problems (for Nebula APs only)

The **WiFi Aid** tab in **Site-wide > Monitor > 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](#)

The screenshot displays the 'WiFi Aid' interface with the following sections:

- Client list:** Includes tabs for 'WiFi Aid' and 'Connection log'.
- Time range:** Set to 'Last 24 hours'.
- SSID:** Set to 'All SSIDs'.
- AP tag:** Set to 'All tags'.
- Client devices affected by connection problems:** Shows 1 / 26 devices. A flow diagram indicates 1 failure in the 'Wireless' category, 0 failures in 'DHCP', and 0 failures in 'DNS'.
- Client devices affected by captive portal problems:** Shows 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
EE-79-61-04-D5-18	1 / 14	Wireless connection
3E-8A-F9-ED-18-B3	1 / 16	Wireless connection
B6-58-D8-F7-60-1C	1 / 17	Wireless connection
F6-11-BA-5E-A9-EF	1 / 9	DHCP
ChuhumbleWatch	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
zyxel5E	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.

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

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

Site-wide > Monitor > Clients

Clients

Client list WiFi Aid Beta Connection log Beta

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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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, I
2023-01-16 17:15:58	<a href="#">Product team</a>	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, I
2023-01-16 16:33:49	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">PMM</a>	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	<a href="#">PMM</a>	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	<a href="#">PMM</a>	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	<a href="#">Product team</a>	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

- 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.

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

Connection issues by client

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

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

Site-wide > Monitor > Client > D2:35:0E:EE:71:F9  
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](#)

**Map**

Map | Satellite

Moat Park  
湖水公園  
Park strip  
in the city center

Art Gallery  
ation Hall  
美术馆

Zhongyang Rd  
Fujou St  
Fujou St

Google

Keyboard shortcuts | Map data ©2023 Google | 10 m | Terms of Use | Report a map error

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

Par:

12718 KB (↓) 74.87 KB (↑) 52.31 KB

200.0 bps  
100.0 bps  
0 bps

15:00 16:30 18:00 19:30 21:00 22:30 16:Jan 01:30 03:00 04:30 06:00 07:30 09:00 10:30 12:00 13:30

**Network**

IPv4 address: 0.0.0.0

MAC address: D2:35:0E:EE:71:F9

VLAN: 1

**Ping**

1  
0.8  
0.5  
0.3  
0

No data to display

- 2 Use the information in this screen to identify the WiFi client with connection issues. See [Table 67 on page 258](#) 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.

Client device	# Failed/total connections	Latest failed issue
<a href="#">D2:35:0E:EE:71:F9</a>	2 / 19	Wireless connection
<a href="#">8E:79:61:04:D5:1B</a>	1 / 14	Wireless connection
<a href="#">3E:BA:F9:ED:1B:83</a>	1 / 16	Wireless connection
<a href="#">B6:5B:D8:F7:60:1C</a>	1 / 17	Wireless connection
<a href="#">F6:11:BA:5E:AB:EF</a>	1 / 3	DHCP
<a href="#">ChihuahuaWatch</a>	1 / 1	Wireless connection

The **Site-wide > Monitor > Connection log** 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.

Site-wide > Monitor > Clients

Client list WiFi Aid Beta Connection log Beta

Last 24 hours | All SSIDs | All APs | Association, Disconnect... | [D2:35:0E:EE:71:F9](#)

Connection time	Connected to	Event type	Detail Issue
2023-01-16 13:44:10	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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: -46dBm. Interface:wlan-2-1
2023-01-16 10:03:17	<a href="#">PMM</a>	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, Signal: -46dBm. Interface:wlan-2-1
2023-01-16 10:03:07	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	Association	Station: d2:35:0e:ee:71:f9 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -79dBm. Interface:wlan-2-1

Page 1 of 2 | Results per page: 10

## 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.

Access point	# Clients affected by connection problems
<a href="#">Product team</a>	1
<a href="#">PMM</a>	1

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

Site-wide > Monitor > Clients

Clients

Client list WiFi Aid Beta Connection log Beta

Last 24 hours All SSIDs **Product team** Association, Disconnect... All clients

Connection time	Connected to	Event type	Detail
2023-01-16 14:17:51	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	Association	Station: 3a9c593a:f5c3 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -57dBm. Interface:wlan-2-1
2023-01-16 13:45:25	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	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	<a href="#">Product team</a>	Association	Station: 62:94:ab:b8:ff:27 connected on Channel: 112, SSID: e-Nebula-FT, 5GHz, Signal: -69dBm. Interface:wlan-2-1

Page 1 of 22 Results per page: 10

## 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
<a href="#">zyxelSF</a>	1
<a href="#">example</a>	1
<a href="#">Nebula</a>	1
<a href="#">test</a>	0
<a href="#">lobby</a>	0

The **Site-wide > Monitor > Client > 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.



Site-wide > Monitor > Client > D2:35:0E:EE:71:F9  
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](#)

**Map**

Map controls: Home, Refresh, Search, Floor plan, Map, Satellite, Full screen, Zoom in (+), Zoom out (-)

Location: Hsiang Moat Park (in the city center)

Other locations: Art Gallery Exhibition Hall

Map data ©2023 Google, 10 m

**Traffic History**

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

Par:

127.18 KB (↓ 74.87 KB | ↑ 52.31 KB)

Y-axis: 0 bps, 100.0 bps, 200.0 bps

X-axis: 15:00, 16:30, 18:00, 19:30, 21:00, 22:30, 16 Jan, 01:30, 03:00, 04:30, 06:00, 07:30, 09:00, 10:30, 12:00, 13:30

**Network**

IPv4 address: 0.0.0.0

MAC address: D2:35:0E:EE:71:F9

VLAN: 1

**Ping**

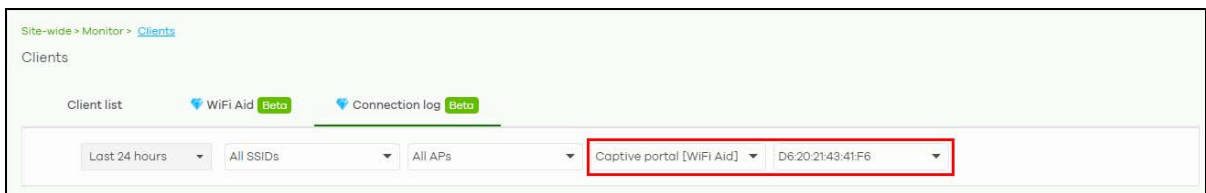
Y-axis: 0, 0.3, 0.5, 0.8, 1

No data to display

- 2 Use the information in this screen to identify the WiFi client with connection issues. See [Table 67 on page 258](#) 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.

Client device	# failed authentication
<a href="#">zyxel5F</a>	1
<a href="#">example</a>	1
<a href="#">Nebula</a>	1
<a href="#">test</a>	0
<a href="#">lobby</a>	0

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

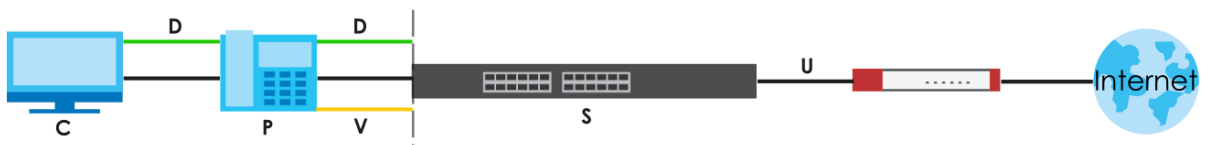


- 6 Use the following information listed in chronological order to resolve failed hotspot authentication issues.
  - **Connection time.** This shows the starting time period from which the event log occurred.
  - **Detail issue.** This shows a summary of the APs event logs in chronological order.

## 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).

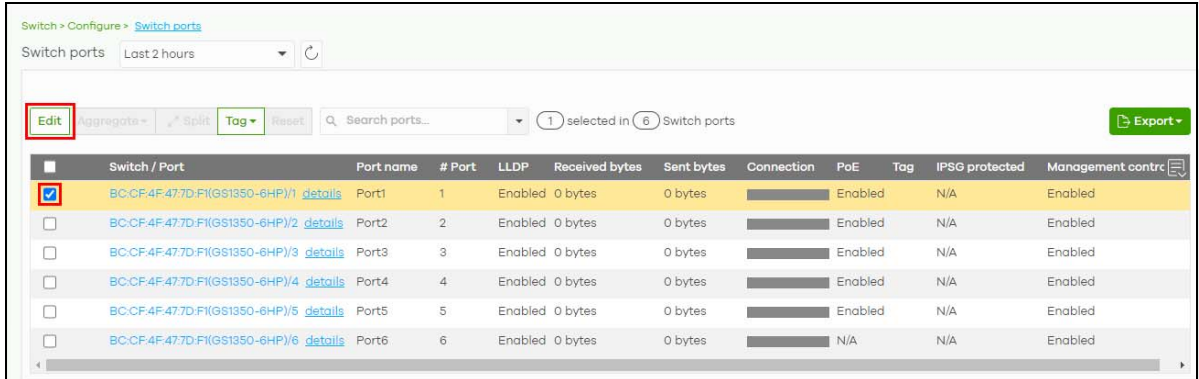


The Nebula Device will add a VLAN tag for voice packets (V) and data packets (D) separately after receiving them. Then forward the voice packets (V) and data packets (D) to the uplink port (U). This section shows you how to separate data packets (D) and voice packets (V) between a VoIP device (P) and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

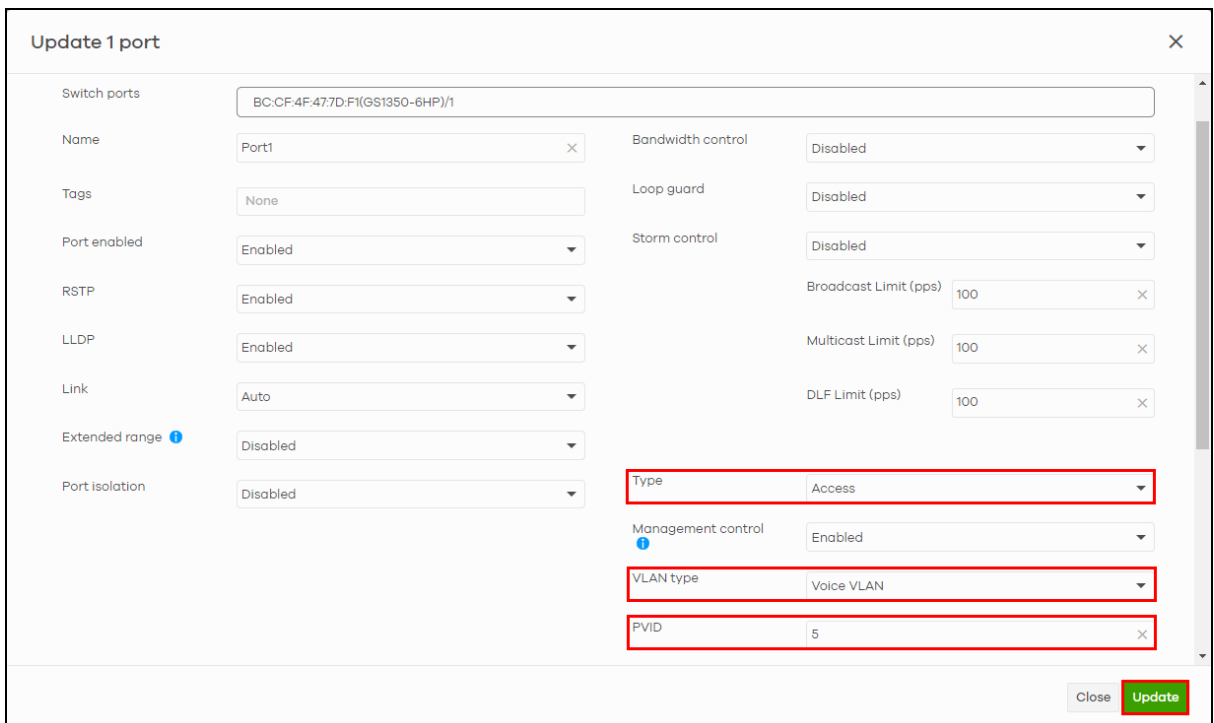
- [Configure the Nebula Device Ports](#)
- [Configure the Voice VLAN](#)

### 3.20.1 Configure the Nebula Device Ports

- 1 Go to **Switch > Configure > Switch ports**.
- 2 Select the port that connects to a VoIP device and click **Edit**.



- 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**.



## 3.20.2 Configure the Voice VLAN

- 1 Go to **Switch > Configure > Switch settings**.
- 2 Scroll to the **Voice VLAN** part of the screen.
- 3 Click the switch to enable the voice VLAN feature in the Nebula Device.
- 4 Enter a **Voice VLAN ID**.
- 5 Select the **Priority** of the voice VLAN from 1 to 6.
- 6 Select **OUI** in **Assign VLAN by**. The Nebula Device assigns the port connected to the VoIP device to the voice VLAN if the connected VoIP device's OUI matches any OUI in the list.
- 7 Enter the **OUI** address of the VoIP device. The OUI (Organizationally Unique Identifier) is the first three octets of the VoIP device's MAC address. By specifying the MAC address, the Nebula Device can identify voice traffic accordingly.

Note: The Nebula Device supports up to six vendor OUIs.

**Voice VLAN**

Voice VLAN 📘

Voice VLAN ID: 10

Priority: 5

Assign VLAN by: OUI

OUI:

OUI	Description
1 00:50:04 <input type="text"/>	3COM <input type="text"/>

[+ Add OUI on this network](#)

**Vendor ID based VLAN**

Vendor ID based VLAN [Model list](#)

**Access management**

Access management [Model list](#)

**DHCP Server Guard**

DHCP Server Guard 📘

**IP source guard** [Model list](#)

IP source guard

[Save](#) [Cancel](#)

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

[Ask Question](#)

- 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 **Switch > Configure > 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.

Switch > Configure > [Advanced IGMP](#)

Advanced IGMP  Override switch configuration

**IGMP snooping**

**IGMP-snooping VLAN** [Model list](#)

Auto-detect

1,2,4

User Assign VLANs.

**Unknown multicast drop** [Model list](#)

Drop on VLAN

**IGMP filtering profiles**

**IPTV topology setup**

[IGMP snooping](#) [Role](#) [Port settings](#) [IGMP topology tips](#)

or

(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 **Switch > Configure > 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.

### 3.21.2 Define the Role of a Switch

- 1 Go to the **Switch > Configure > Advanced IGMP** screen. Under **IPTV topology setup**, select a Switch you want to configure and select a **Role** to define the role of your Switch from the drop-down list box.

Note: Click the **IGMP topology tips** link to view information about Switch roles. If the role of the Switch is not defined accordingly, the IPTV performance will be greatly affected.

- 2 After you define the role of the Switch, click **Advanced setup** and the following screen appears. The **Leave mode** will show the default setting based on the role you select. But you can still go back to the **Advanced IGMP** screen to configure the **Role** and **Leave mode**. Under **Maximum group**, you can select **Enable** and enter the maximum number of channels allowed at a time. Otherwise, select **Disable**. Click **Save** to save the changes.

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

**Port settings**

Switch name: [Switch Name]

Role: Querier

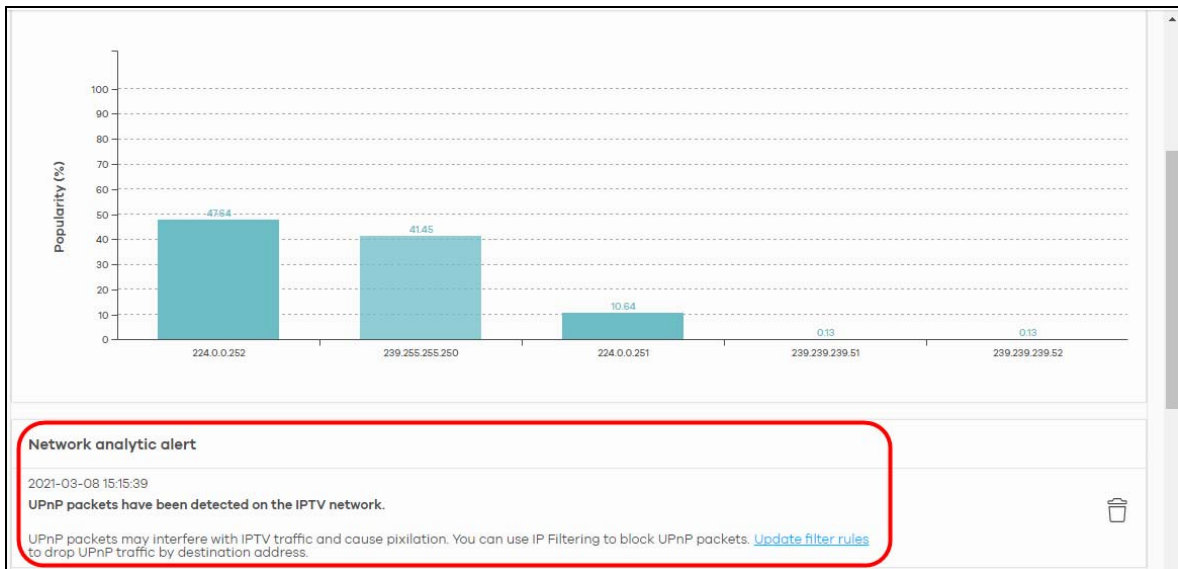
Leave mode: Normal leave (20000)

Maximum group: Enable

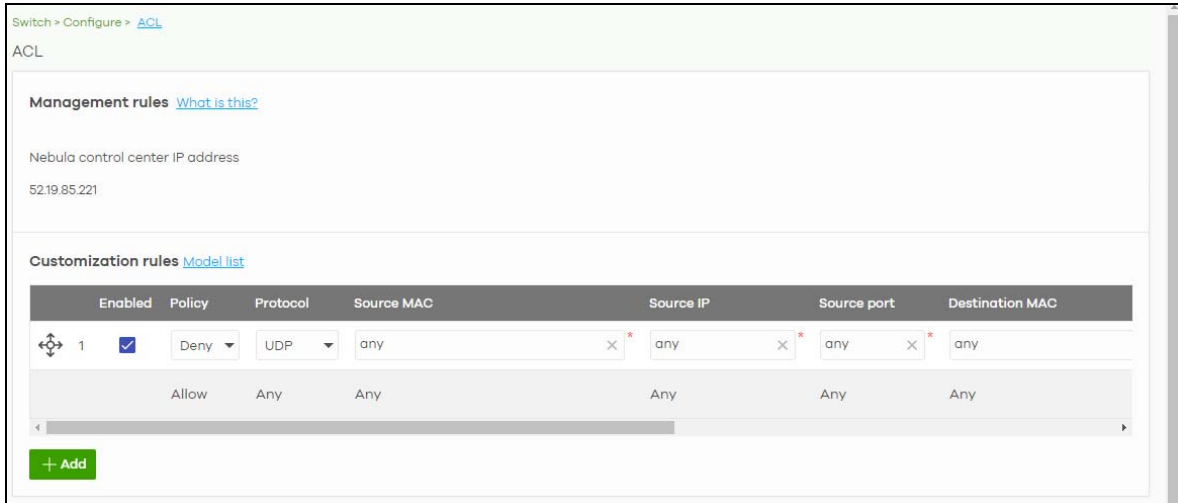
IGMP filtering profile: No select

Buttons: Reset, Close, Save

- 3 If a reminder of **Network analytic alert** appears on the **Switch > Monitor > 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 **Switch > Configure > ACL** screen to block these packets.



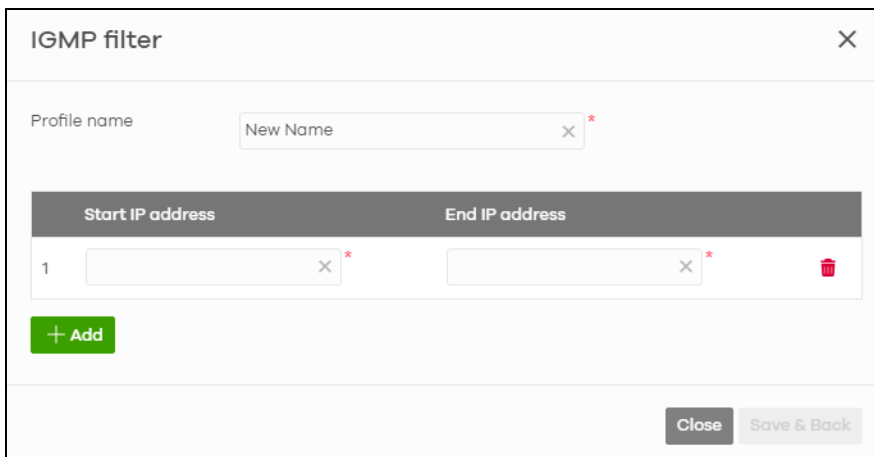
- 4 The **Update filter rules** link will lead you to the following screen. Click **Save** to save the default setting to block UPnP packets.



### 3.21.3 Configure the Channel Profile and Naming

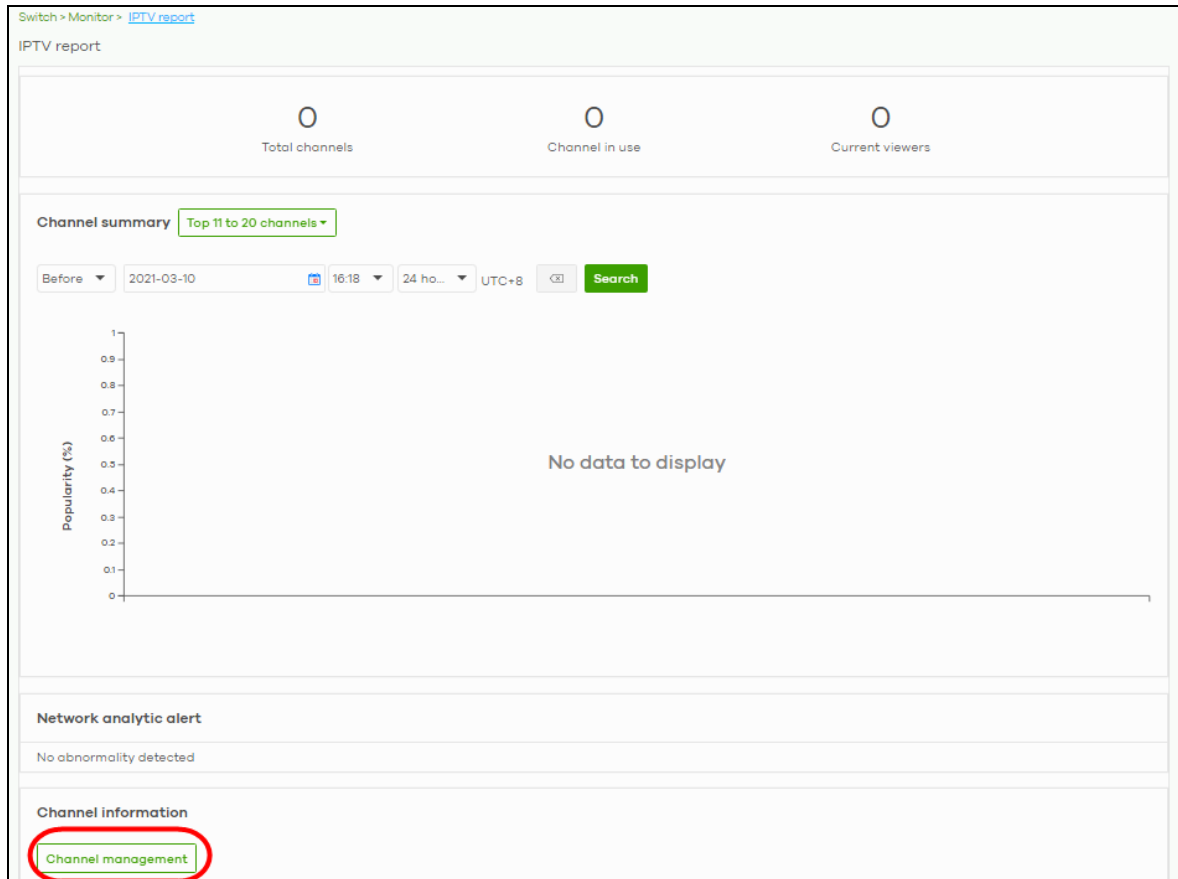
A channel profile is the IP address range allowed to receive IPTV channels. An IPTV channel is used to send video traffic to the IP addresses in the channel profile.

- 1 To set up a range of available IPTV channels, go to the **Switch > Configure > 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.

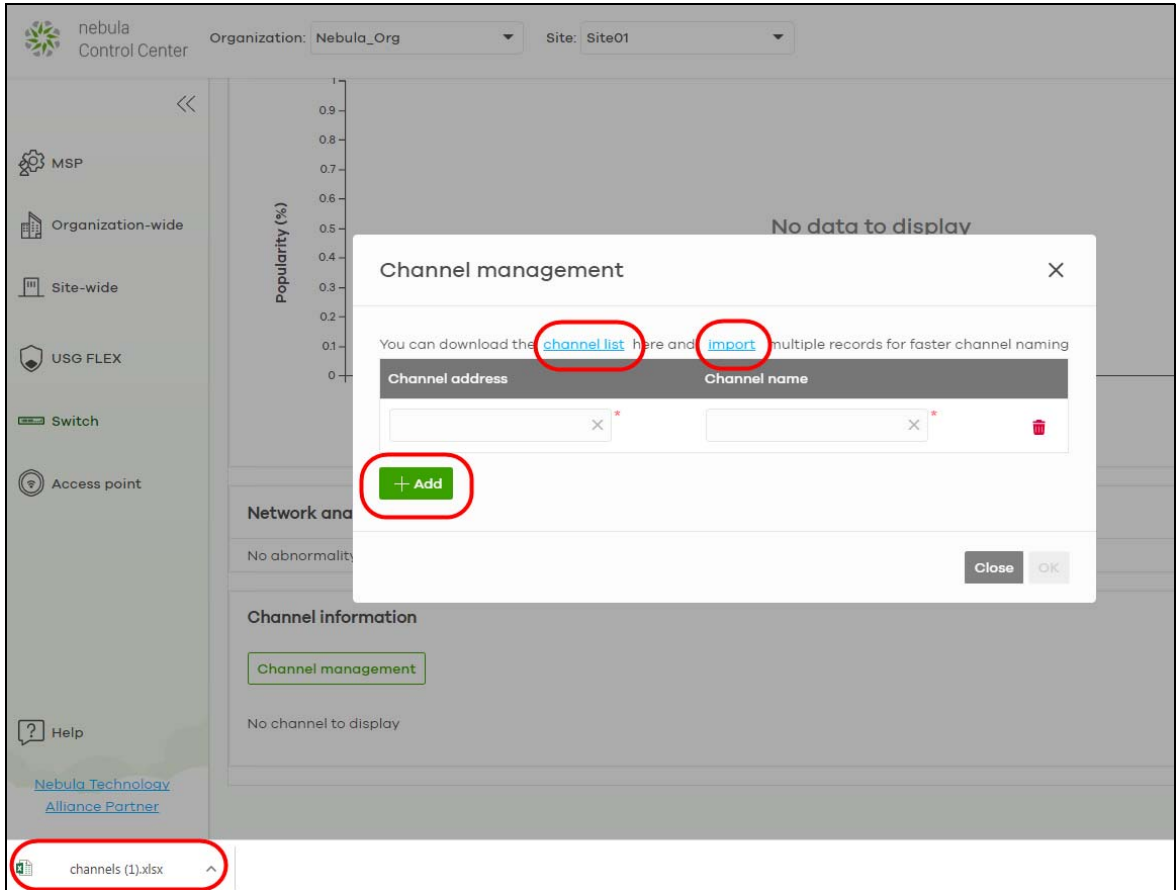


- 2 To edit the naming of the IPTV channels, go to the **Switch > Monitor > IPTV report** screen and click **Channel management** under **Channel information**.

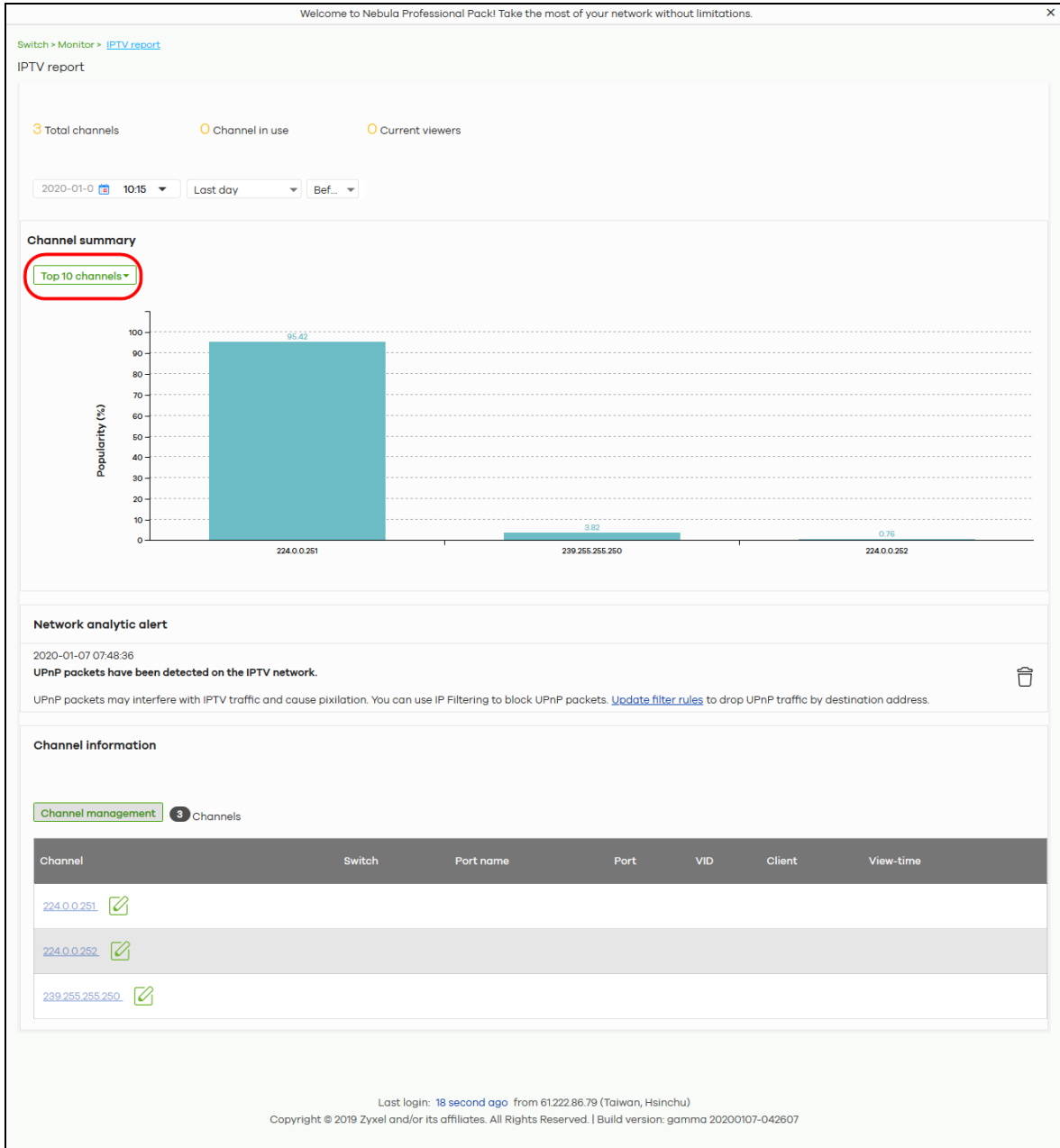




- 3 You can choose to either import an updated channel list (channels.xlsx), or enter/edit each **Channel address** and **Channel name** individually.
- Under **Channel management**, click **channel list** to download a blank Excel file template, edit accordingly and save it, and then click **import** 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.



- 4 To view the summary of the IPTV report, go to the **Switch > Monitor > IPTV report** screen. Click **Channel summary** to see the top or bottom viewed channels within the specified time period you choose.



## 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

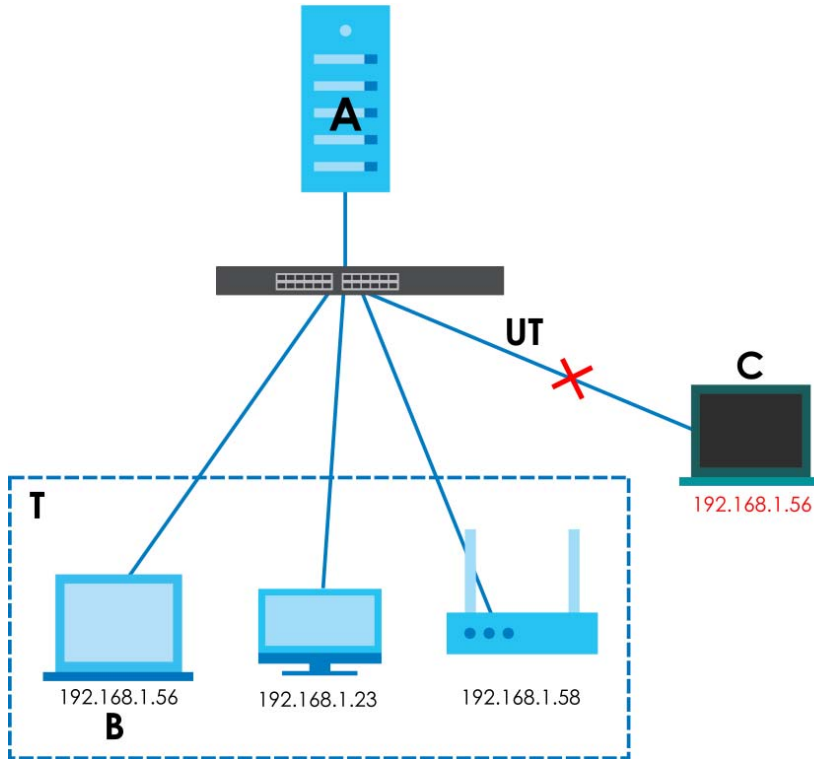
The Nebula Device only allows an authorized DHCP server on a trusted port to assign IP addresses. Unauthorized DHCP servers will not be able to assign IP addresses to network clients. When the Nebula Device receives a DHCP server packet from an authorized DHCP server, it inspects the packet and records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

**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

Allowed client list 1

Action  0 clients + Add client

IPv4 address	MAC address	VLAN

Save or Cancel

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

- 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	<input checked="" type="checkbox"/>	1,3,7	
XS3800-30	<input checked="" type="checkbox"/>	1,4	
XGS2220-30	<input type="checkbox"/>	Null	

- Click the edit icon to go to **Switch > Configure > 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	<input checked="" type="checkbox"/>	1,3,7	
XS3800-30	<input checked="" type="checkbox"/>	1,4	
XGS2220-30	<input type="checkbox"/>	Null	

- Click to select the port you want to enable IP source guard.

Switch > Configure > Switch ports

Switch ports Last 2 hours

Edit Aggregate Split Tag Reset Q Search ports... 2 selected in 28 Switch ports Export

Switch / Port	Port name	# Port	LLDP	Received bytes	Sent bytes	Enabled	Connection	PoE	Status	Type	Tag	Number of IGMP Group
<input checked="" type="checkbox"/> XS3800-1-1/1 <a href="#">details</a>	Port1	1	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
<input type="checkbox"/> XS3800-1-1/2 <a href="#">details</a>	Port2	2	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
<input type="checkbox"/> XS3800-1-1/3 <a href="#">details</a>	Port3	3	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
<input type="checkbox"/> XS3800-1-1/4 <a href="#">details</a>	Port4	4	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
<input type="checkbox"/> XS3800-1-1/5 <a href="#">details</a>	Port5	5	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
<input type="checkbox"/> XS3800-1-1/6 <a href="#">details</a>	Port6	6	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
<input type="checkbox"/> XS3800-1-1/7 <a href="#">details</a>	Port7	7	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
<input type="checkbox"/> XS3800-1-1/8 <a href="#">details</a>	Port8	8	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
<input type="checkbox"/> XS3800-1-1/9 <a href="#">details</a>	Port9	9	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0
<input type="checkbox"/> XS3800-1-1/10 <a href="#">details</a>	Port10	10	Enabled	0 bytes	0 bytes	Enabled		N/A	Disabled	Trunk		0

Page 1 of 3 Results per page: 10

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 **Switch > Configure > 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).

- In the **Update port** screen, select **Enabled** in **IPSG protected**. The **IPSG protected** field in the **Switch > Configure > Switch ports** table for the updated port will display **Enabled**.

### Update 1 port ✕

**General settings** ⌵

Switch ports	XS3800-1-1/1		
Name	Port1 <span>✕</span>	Bandwidth control	Enabled <span>⌵</span>
Tags	None	Ingress	1000000 Kbps <span>✕</span>
Port enabled	Enabled <span>⌵</span>	Egress	1000000 Kbps <span>✕</span>
RSTP	Enabled <span>⌵</span>	Loop guard	Enabled <span>⌵</span>
STP guard	Root guard <span>⌵</span>	Storm control	Enabled <span>⌵</span>
LLDP	Enabled <span>⌵</span>	Broadcast Limit (pps)	100 <span>✕</span>
Link	Auto <span>⌵</span>	Multicast Limit (pps)	100 <span>✕</span>
Media type	SFP+ <span>⌵</span>	DLF Limit (pps)	100 <span>✕</span>
Port isolation	Enabled <span>⌵</span>	Type	Access <span>⌵</span>
<b>IPSG protected</b>	<b>Enabled</b> <span>⌵</span>	VLAN type	Vendor ID based VLAN <span>⌵</span>
Radius policy	Open <span>⌵</span>	PVID	1 <span>✕</span>

**PoE settings** ⌵

**IPTV setting** Override advanced IGMP setting 🔴

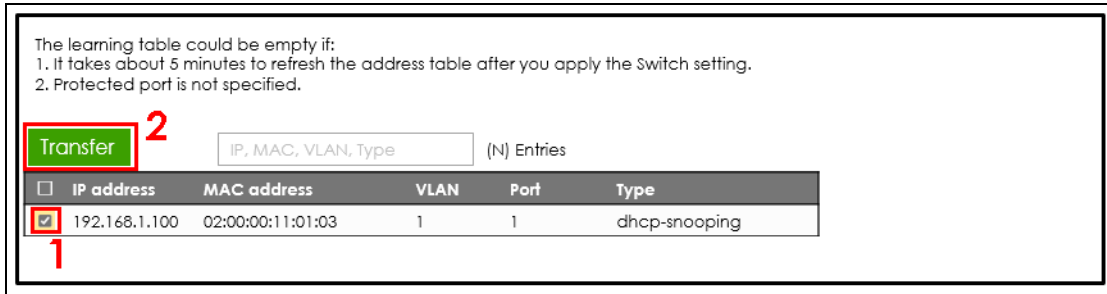
Leave mode <span>ℹ</span>	Normal leave <span>⌵</span>	4000 ms <span>✕</span>
Maximum Group <span>ℹ</span>	Enabled <span>⌵</span>	1 <span>✕</span>
IGMP filtering profile	No Select <span>⌵</span>	
Fixed router port	Auto <span>⌵</span>	

Close Update 2

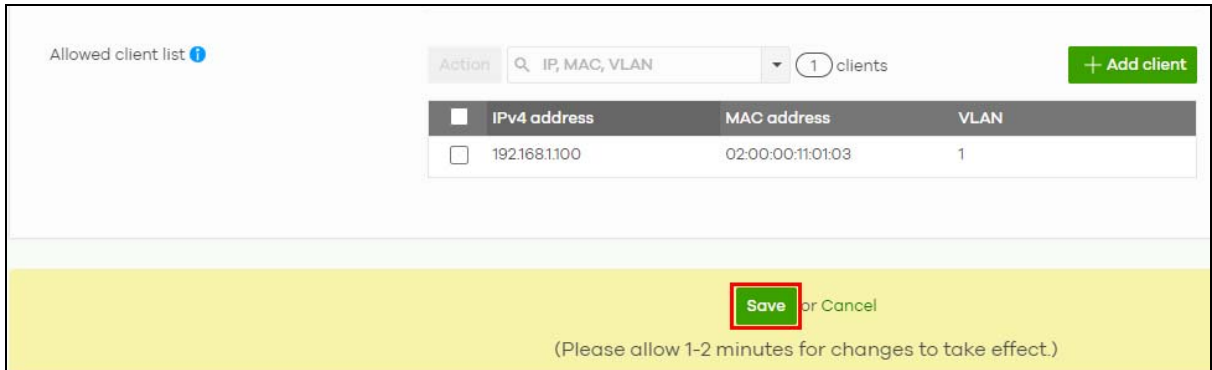
6 Click **Run**.

Switch Name	IP Source Guard	Protected ports		Client table
00:00:01:00:0A:05	<span style="color: green;">🔴</span>	1,3,5,7	☑	<span style="border: 1px solid green; padding: 2px 5px; color: green;">▶ Run</span>
XS3800-30	<span style="color: green;">🔴</span>	1,4	☑	<span style="border: 1px solid green; padding: 2px 5px; color: green;">▶ Run</span>
XGS2220-30	<span style="border: 1px solid red; color: green;">🔴</span>	1	☑	<span style="border: 1px solid red; padding: 2px 5px; color: green;">▶ Run</span>

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



- 8 The port with the particular IP and MAC addresses is added to the **Allowed client list**. Click **Save**.



## 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 **Switch > Configure > 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 **Switch > Configure > 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 > Configure > 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.

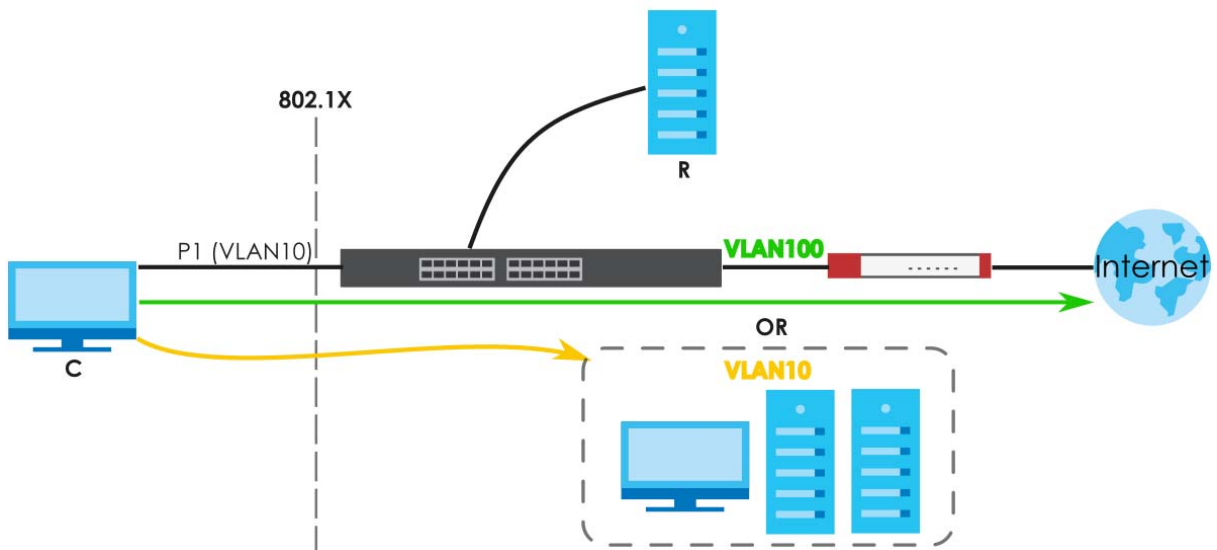
Scenario 1:

The login account passes IEEE 802.1x port authentication with dynamic VLAN assignment. Client (C) will connect to the network through VLAN100.

Scenario 2:

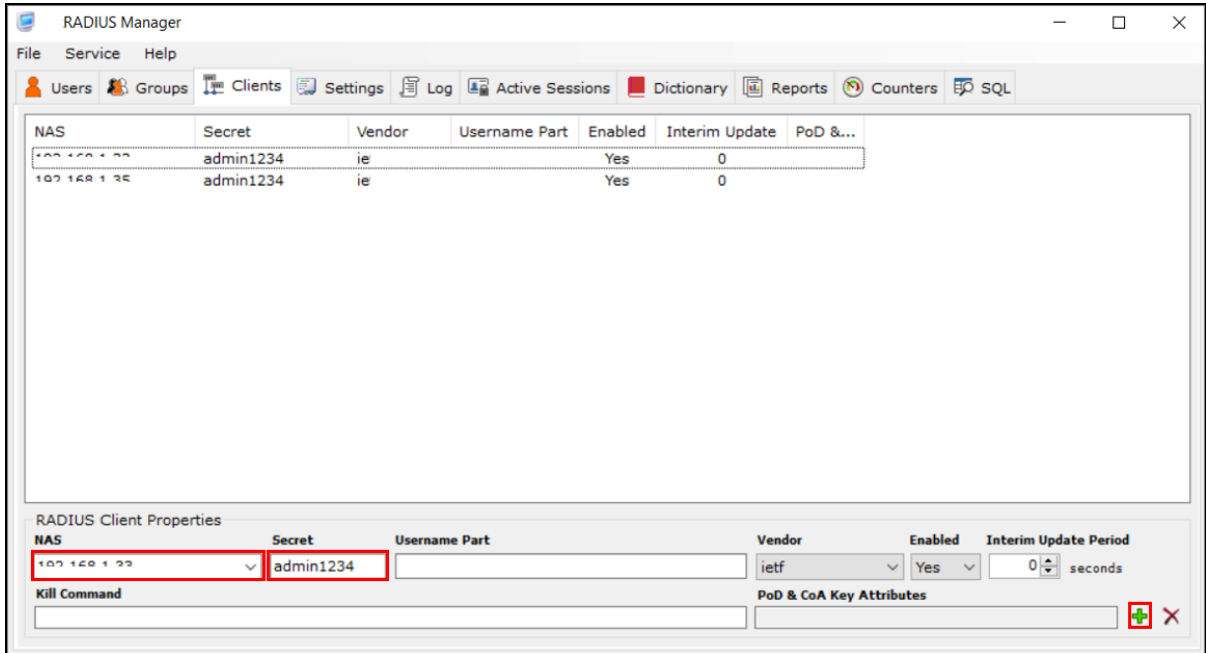
The login account passes IEEE 802.1x port authentication without dynamic VLAN assignment. Client (C) will connect to the network through VLAN10.

**Figure 21** IEEE 802.1x Port Authentication With and Without Dynamic VLAN Assignment Example

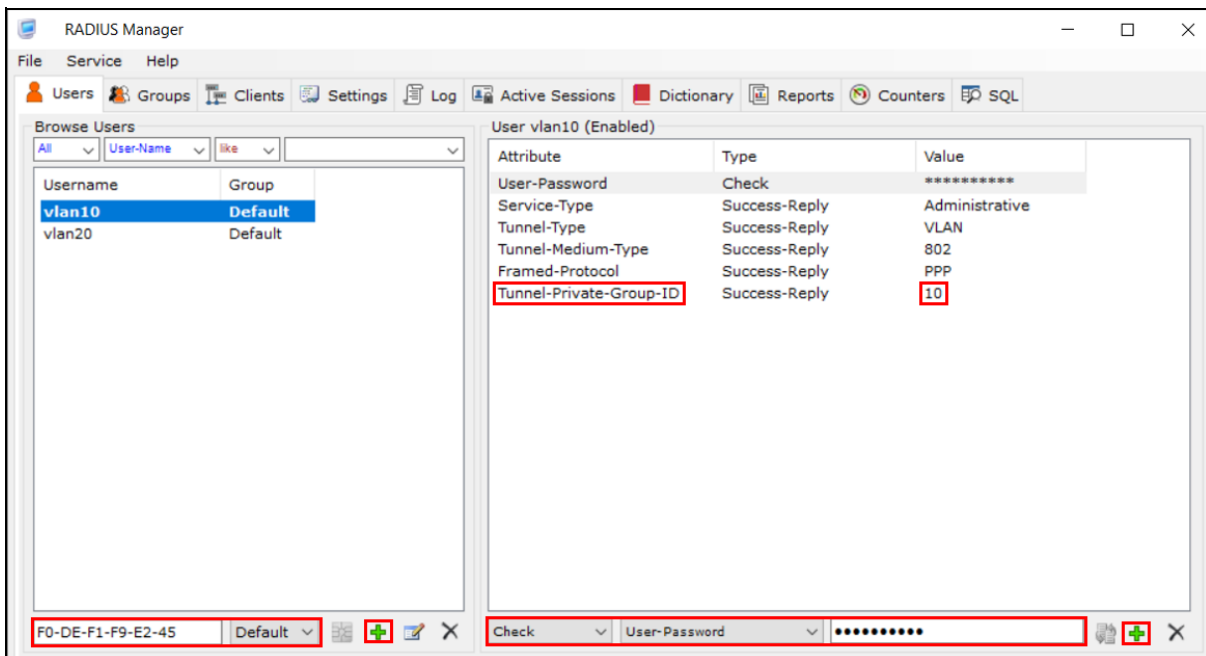


To set up dynamic VLAN with RADIUS, do the following:

- 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 **Switch > Configure > Authentication** screen. Then click the add (+) button.



- 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.



- 3 Go to **Switch > Configure > 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 **Switch > Configure > 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 **Switch > Configure > 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 **Switch > Monitor > 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	<a href="#">XGS1930-52HP</a>	AAA	802.1x Authentication - retransmit EAPOL-START packet [User-Name wronguser] [NAS-Port 20 - Port20]
2022-09-27 14:47:15	<a href="#">XGS1930-52HP</a>	AAA	RADIUS server 1 is unreachable
2022-09-27 14:47:15	<a href="#">XGS1930-52HP</a>	AAA	802.1x RADIUS server timeout [User-Name wronguser] [NAS-Port 20 - Port20]
2022-09-27 14:46:45	<a href="#">XGS1930-52HP</a>	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	<a href="#">XGS1930-52HP</a>	AAA	802.1x Authentication - retransmit EAPOL-START packet [User-Name wronguser] [NAS-Port 20 - Port20]
2022-09-27 14:45:07	<a href="#">XGS1930-52HP</a>	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 45](#) 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.

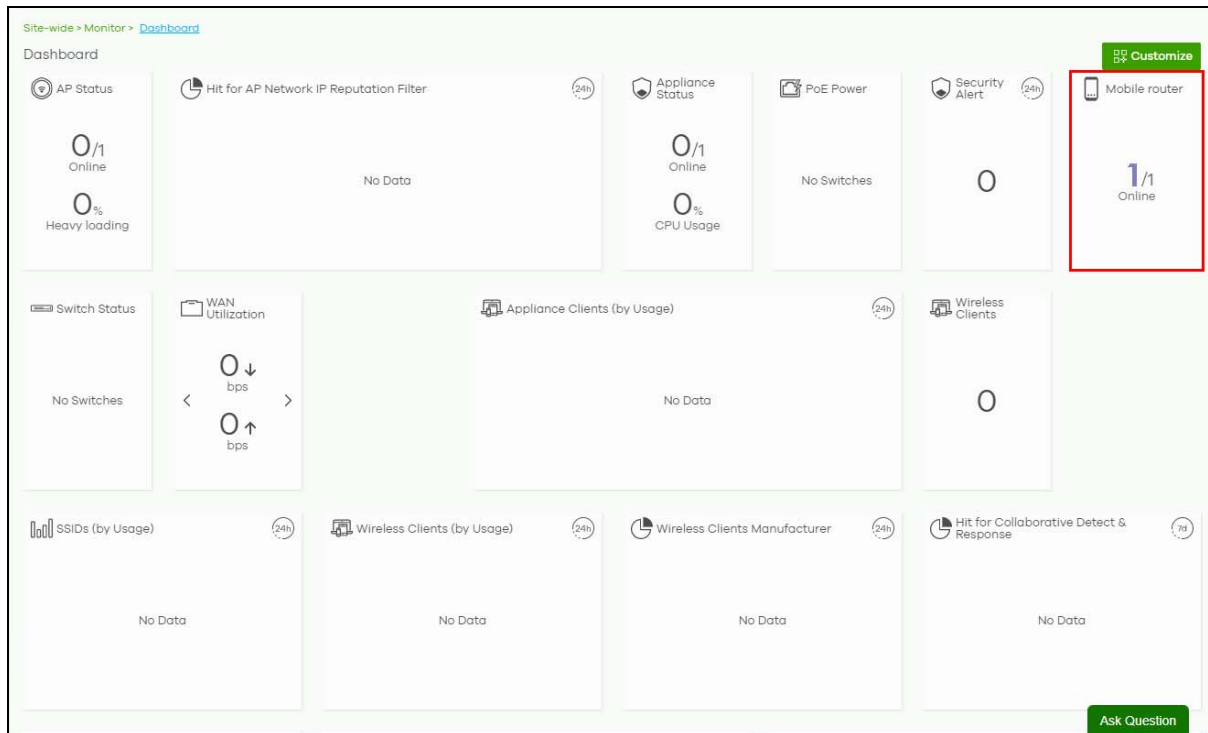
The screenshot shows the Nebula dashboard with various monitoring widgets. A red box highlights the 'Mobile router' widget, which displays '0/1 Online' and 'Heavy loading'. Other widgets include AP Status, Hit for AP Network IP Reputation Filter, Appliance Status, PoE Power, Security Alert, Switch Status, WAN Utilization, Appliance Clients (by Usage), Wireless Clients, SSIDs (by Usage), Wireless Clients (by Usage), Wireless Clients Manufacturer, and Hit for Collaborative Detect & Response.

## 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 > Monitor > 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 > General 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 [Collaborative Detection & Response on page 280](#) 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

**A** Collaborative detection & response  Enable

**B**

Policy	Category	Event type	Occurrence	Duration (Minutes)	Containment
	Malware	Malware detected	2 <input type="text"/> × *	60 <input type="text"/> × *	Alert
	IPS	Vulnerability exploit detected	2 <input type="text"/> × *	10 <input type="text"/> × *	Alert
	Web Threats	Connections to malicious web sites detected	1 <input type="text"/> × *	30 <input type="text"/> × *	Alert

**C**

**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:  ×

To use custom captive portal page, please download the zip file and edit them.  
[Download](#) the customized captive portal page example.

Containment period

60  ×

**D**

**Block**

Block wireless client:  **D**

**Quarantine**

Quarantine VLAN  **Edit**

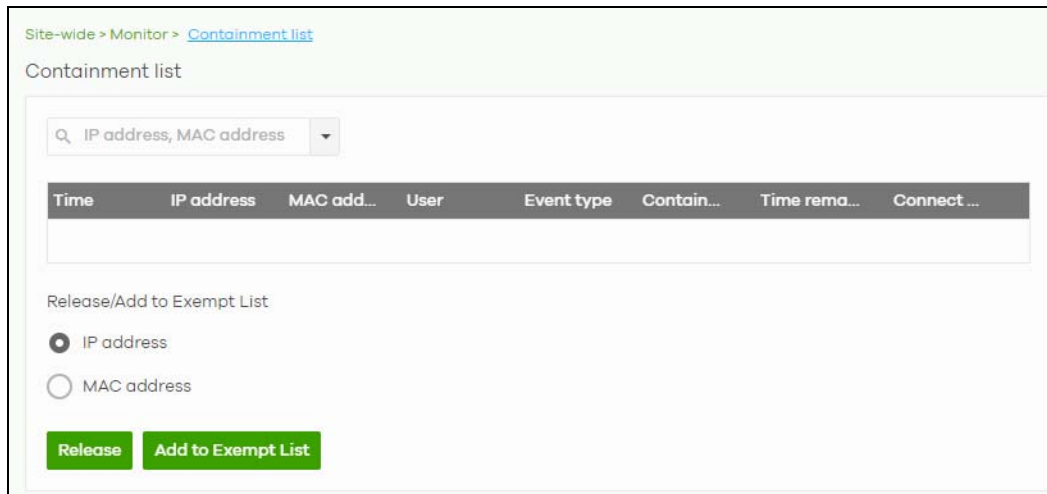
**E**

**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 80 on page 283](#) for more information.
- 3 Configure the containment alert (**Theme**), customized pop-up (**Notification message**) for the client blocked by CDR, and the (**Containment Period**) time interval (refer to the **C** part in the above figure).

- 4 In **Block**, set how long a suspect client should be blocked or quarantined (1 minute to 1 day (1,440 minutes)). Enter 0 to block a suspect client until released in **Site-wide > Monitor > Containment list**. In **Quarantine**, configure a VLAN in order to isolate traffic from suspect clients (refer to the **D** part in the figure for step 1).
- 5 Enter the IPv4 and/or MAC addresses of client device(s) that are exempt from CDR checking in **Exempt list** (refer to the **E** part in the figure for step 1).
- 6 To unblock a suspect client, go to **Site-wide > Monitor > Containment list**. Select a client, then
  - click **Release** to free the client from CDR containment, or
  - select an IPv4 address or MAC address, click **Add to Exempt List** and then click **OK** to release the client device from CDR containment. The client device's IP or MAC address is exempt from future CDR checking.



## 3.28 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.

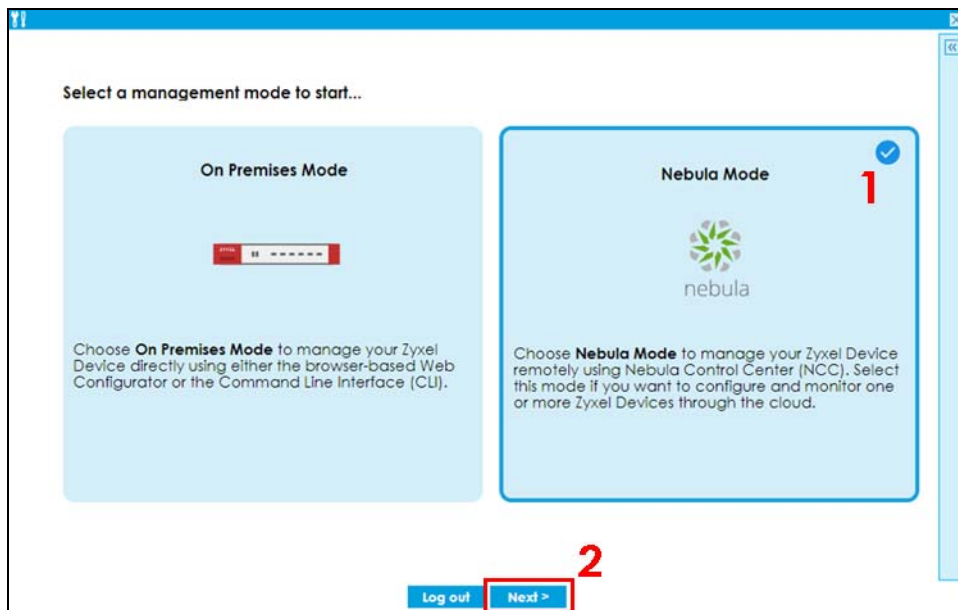
Press the **RESET** button on the SF panel (see the SF user's guide for more information).

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**.



- 3 Configure the WAN settings and click **Next**.

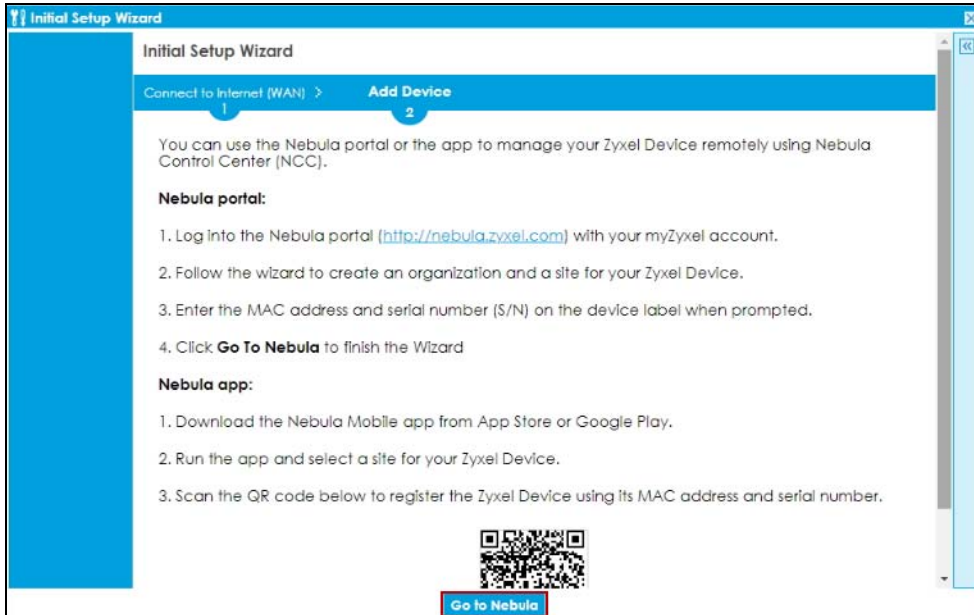


The screenshot shows the 'Initial Setup Wizard' window. The progress bar indicates step 1 'Connect to Internet (WAN)' is active, and step 2 'Add Device' is next. The 'ISP Setting' section has a checkbox for 'I have two ISPs' which is unchecked. The 'Internet Access - First WAN Interface' section has a checkbox for 'VLAN Tagged' which is unchecked. Below this is a 'VLAN ID' field with a dropdown arrow and a range of '[1-4080]'. The 'ISP Parameters' section includes 'Encapsulation' set to 'Ethernet', 'MTU' set to '1500' Bytes, and 'First WAN Interface' set to 'ge2'. The 'IP Address Assignment' section has 'Zone' set to 'WAN' and 'IP Address Assignment' set to 'Auto', which is highlighted with a red box. The 'DHCP Option 60' field is empty. At the bottom, there are '< Back' and 'Next >' buttons, with the 'Next >' button highlighted in red.

- 4 Click **Connection Test** to check that you can access the Internet and then click **Next**.

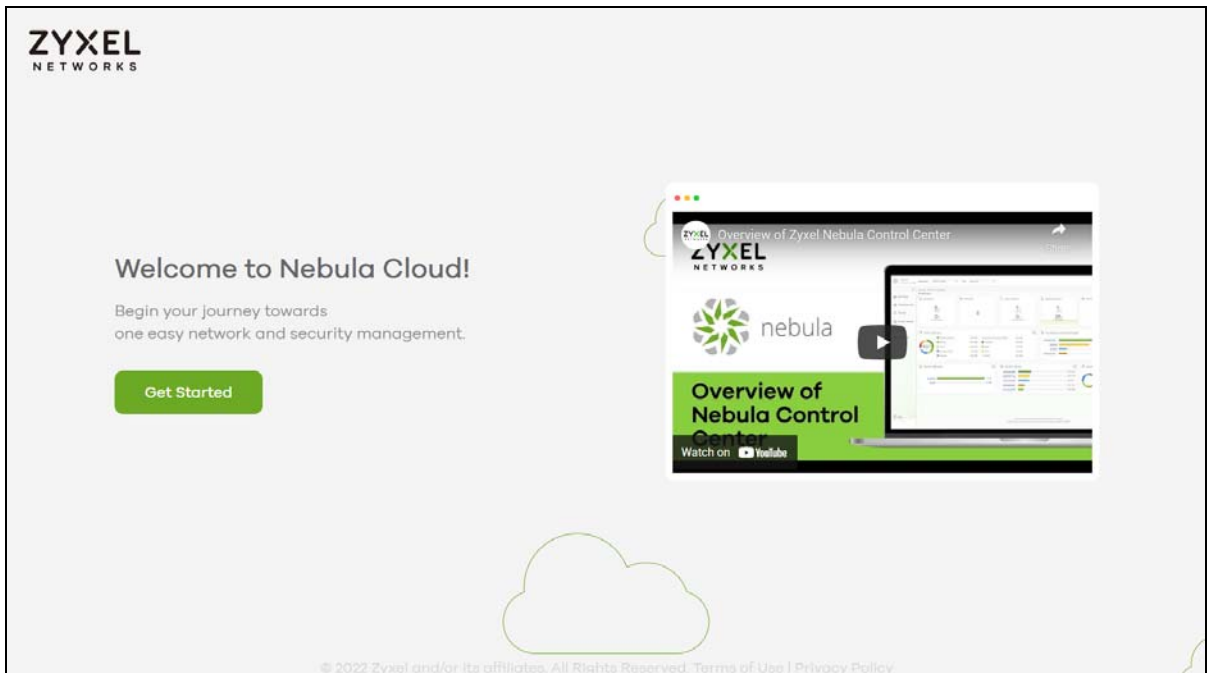
The screenshot shows the 'Initial Setup Wizard' window. The progress bar indicates step 1 'Connect to Internet (WAN)' is active, and step 2 'Add Device' is next. The main content area displays a message: 'Congratulations. The Internet Access wizard is completed. Summary of Internet Access configuration:'. Below this is the 'First Setting' section, which lists the following configuration details: '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:', and 'Second DNS Server:'. A red box highlights the 'Connection Test' button. At the bottom, there are '< Back' and 'Next >' buttons, with the 'Next >' button highlighted in red.

- 5 Click **Go to Nebula**.



## Nebula Configuration

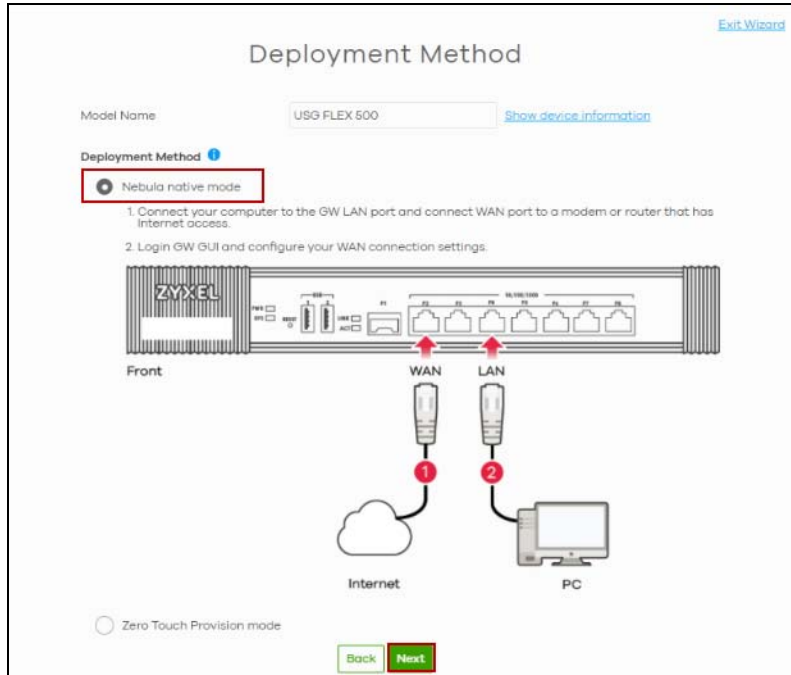
- 1 You will be redirected to the Nebula portal. Click **Get Started**.



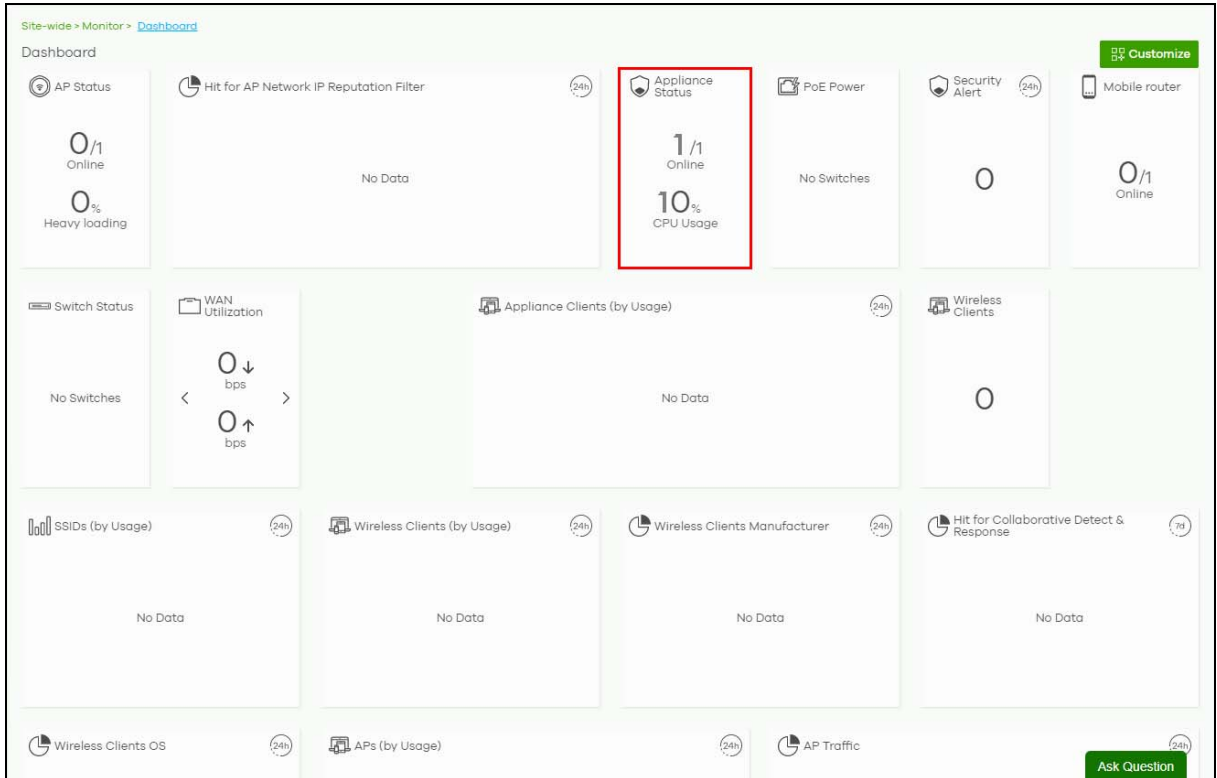
- 2 Use the Setup Wizard to create an organization and a site, and add the Nebula Device. See [Setup Wizard on page 45](#) for more information on using the wizard.

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 50](#) for more information on the ZTP deployment method).



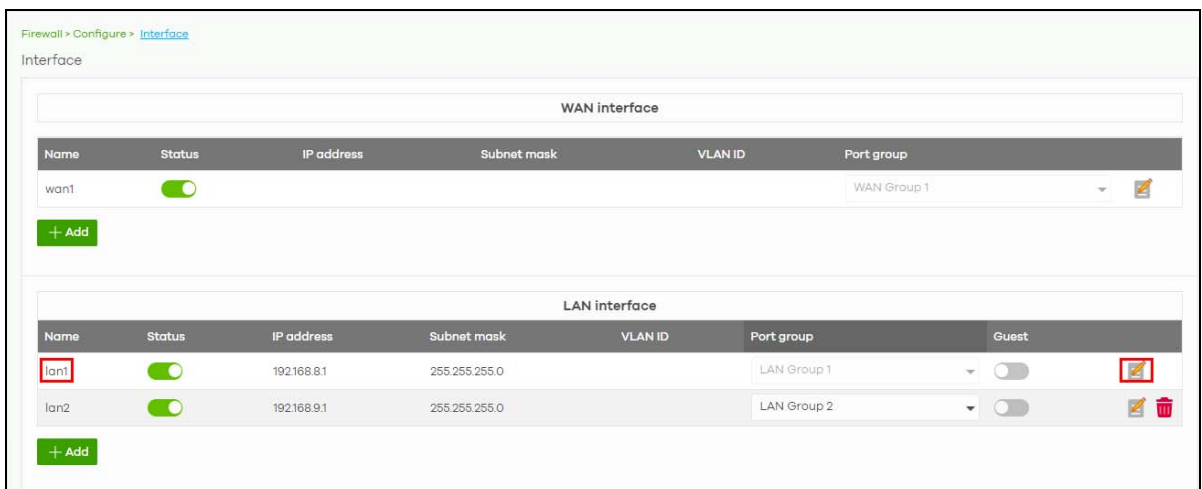
- 3 After configuring the Setup Wizard, close the Nebula Control Center welcome message to go to the Nebula portal dashboard. **1/1 Online** will show on **Appliance Status**. This means that one SF is registered in Nebula and is online.



## 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 **Firewall > Configure > Interface > LAN interface configuration** screen.



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

The screenshot shows the 'LAN interface configuration' dialog box. At the top, there is a tab labeled 'ADVANCED OPTIONS' with a green triangle icon, which is highlighted with a red box. Below this, the 'DHCP extended options' section contains five input fields: 'First WINS server', 'Second WINS server', 'PXE server', 'PXE Boot loader file', and 'Default gateway', each with a small 'x' icon to its right. Below these fields is a green button with a white plus sign and the text '+ Add new', also highlighted with a red box. Underneath, the 'IGMP proxy' section has a toggle switch that is currently turned off. Below the toggle are two radio button options: 'IGMP upstream' (which is selected) and 'IGMP downstream'. At the bottom right of the dialog, there are two buttons: 'Close' and 'OK'.

- 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** X

Option: User defined

Name: DomainName X

Code: 15 X (1-254)

Type: TEXT

Value: cs.com X

Close OK

- 4 A new user-defined DHCP option appears in **LAN interface configuration**. Click **OK**.

**LAN interface configuration** X

DHCP extended options

First WINS server X

Second WINS server X

PXE server X

PXE Boot loader file X

Default gateway X

Name	Code	Type	Value
DomainName	15	TEXT	cs.com

+ Add new

IGMP proxy

IGMP upstream

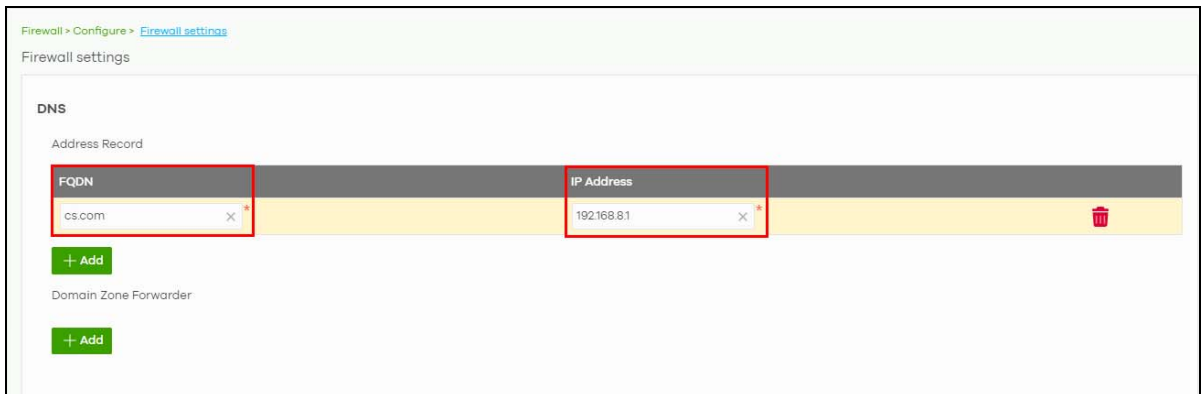
IGMP downstream

Close OK

- 5 Go to **Firewall > Configure > 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.



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\>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

## MSP

---



# CHAPTER 4

## MSP

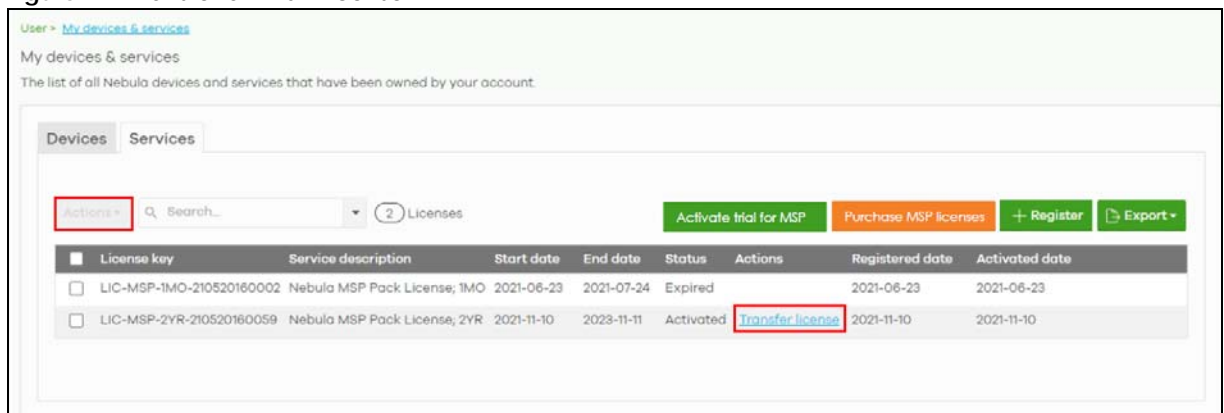
### 4.1 Overview

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 22** Transfer an MSP License



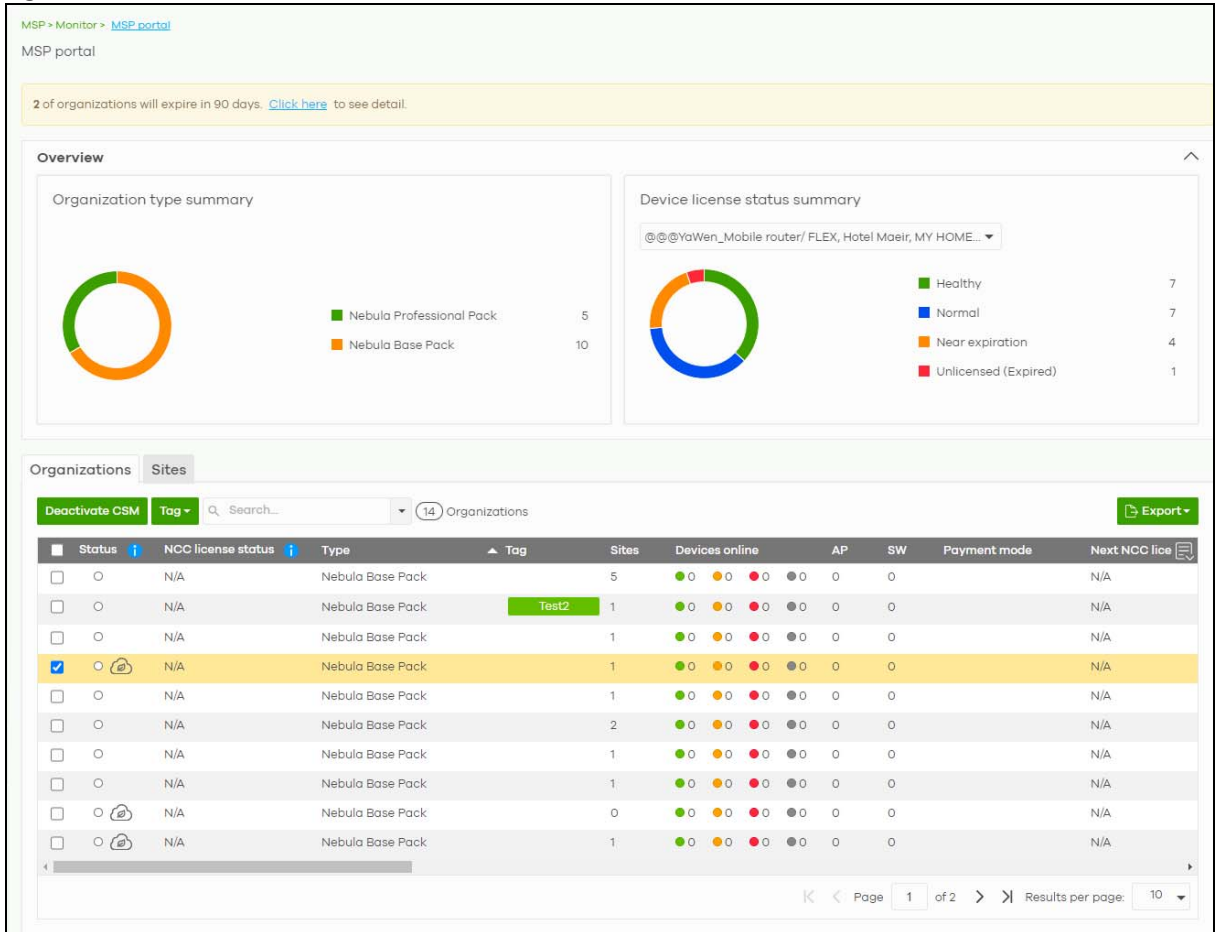
Note: To see these menus, assign an MSP license to your NCC login account.

### 4.2 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 > Monitor > MSP portal** in the navigation panel.

Figure 23 MSP > Monitor > MSP portal



The following table describes the labels in this screen.

Table 12 MSP > Monitor > 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 <a href="#">Section 1.6 on page 44</a> for more information on Cloud-saving mode.

Table 12 MSP &gt; Monitor &gt; MSP portal (continued)




LABEL	DESCRIPTION
Tag	<p>Assign a name to an organization or to a group of organizations.</p> <ol style="list-style-type: none"> <li>1. Select the organizations. The <b>Tag</b> button will be enabled.</li> <li>2. Click <b>Tag</b>.</li> <li>3. In the <b>Add</b> field, enter a tag (up to 32 alphanumeric characters and spaces are allowed).</li> <li>4. Click <b>+Add new</b>. Then <b>Add</b> to confirm.</li> </ol> <p>To remove the tag assigned to an organization or to a group of organizations.</p> <ol style="list-style-type: none"> <li>1. Select the organization with an assigned tag.</li> <li>2. Click <b>Tag</b>.</li> <li>3. Enter the name of the tag. As you type along, NCC will automatically show the names of tags that matches.</li> <li>4. Select the tag. Then click <b>Remove</b>.</li> </ol>
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.
*	<p>Click this to select all rows.</p> <p>Alternatively, click a row to go to the <b>Sites</b> tab that will show the sites belonging to the organization.</p>
Status	<p>This shows the status of Nebula Devices in the organization.</p> <ul style="list-style-type: none"> <li>• Green: All Nebula Devices are online and have no alerts.</li> <li>• Orange: Some Nebula Devices have alerts.</li> <li>• Red: Some Nebula Devices are offline.</li> <li>• Gray: All Nebula Devices have been offline for 7 days or more.</li> <li>• White: No Nebula Devices in this organization.</li> <li>•  : This organization is in Cloud-saving mode.</li> </ul>
NCC license status	<p>This shows the license status of Nebula Devices in the organization.</p> <ul style="list-style-type: none"> <li>• Green: All Nebula Devices with over 1 year licenses.</li> <li>• Blue: Any Nebula Device with over 90 days but less than 1 year license together with another Nebula Device with over 1 year license.</li> <li>• Orange: Any Nebula Device with license that will expire in 90 days together with another Nebula Device with over 90 days license.</li> <li>• Red: Any Nebula Device with an expired license or is unlicensed.</li> <li>• Gray: No Nebula Devices in this organization.</li> </ul>
Organization	This shows the descriptive name of the organization. Click an <b>Organization</b> to go to the <b>Organization-wide &gt; Monitor &gt; Overview</b> screen. Hover the mouse over the name of the Organization to display the site information window. Clicking a <b>Site name</b> will go to the <b>Site-wide &gt; Monitor &gt; Dashboard</b> 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 12 MSP &gt; Monitor &gt; MSP portal (continued)

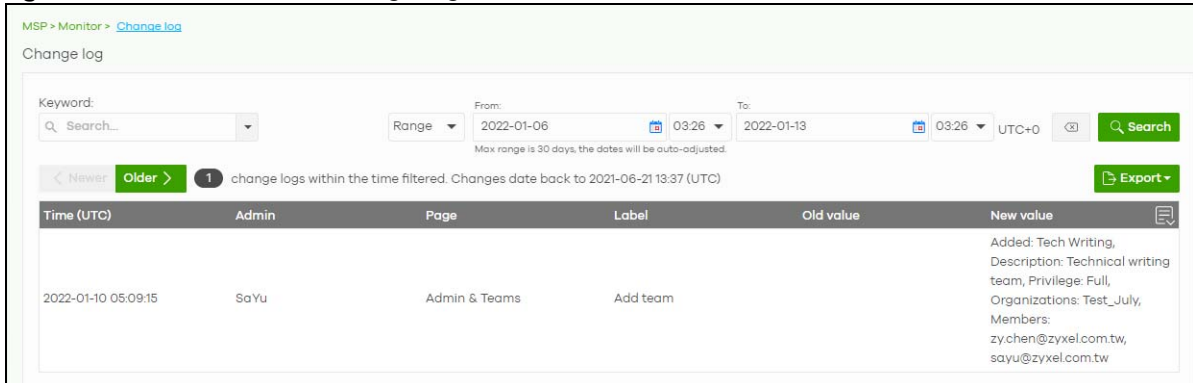
LABEL	DESCRIPTION
Devices online	This shows the number of Nebula Devices in this organization which are online (green), have recently had alerts (orange), recently went offline (red), or have been offline for more than 6 days (gray).
AP	This shows the number of Nebula access points connected to the sites 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 <b>N/A</b> when there is no Nebula-managed device in the organization.  For example, if you have two Nebula Devices in the organization: <ul style="list-style-type: none"> <li>• Nebula Device 1 is with NCC license expiration date on 2022/10/1</li> <li>• Nebula Device 2 is with NCC license expiration date on 2022/11/1</li> </ul> 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. <ul style="list-style-type: none"> <li>• Green: All Nebula Devices are online and have no alerts.</li> <li>• Orange: Some Nebula Devices have alerts.</li> <li>• Red: Some Nebula Devices are offline.</li> <li>• Gray: All Nebula Devices have been offline for 7 days or more.</li> <li>• White: No Nebula Devices in this site.</li> </ul>
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 <b>Site-wide &gt; Monitor &gt; Dashboard</b> 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.

## 4.3 Change Log

Use this screen to view logged messages for changes in the **Admins & teams** and **Cross-org synchronization** screens. Click **MSP > Monitor > 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 24** MSP > Monitor > Change log



The following table describes the labels in this screen.

**Table 13** MSP > Monitor > 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 <b>Search</b> to filter log entries by date. <b>Range:</b> Display log entries from the first specified date to the second specified date. <b>Before:</b> Display log entries from the beginning of the log to the selected date.
Search	Click this to update the list of logs based on the search criteria.
Reset filters 	Click this to return the search criteria to the previously saved time setting.
Newer/Older	Click to sort the log messages by most recent or oldest.
N change logs within the time filtered.	This shows the total number of the log messages that match the search criteria. It also shows the date and time the very first log was created.
Export	Click this button to download the log list as a CSV or XML file to your computer.
Time (UTC)	This shows the date and time in UTC+00:00 (or UTC+0) when the log was recorded.  UTC is a standard time for use around the world (formerly known as Greenwich Mean Time or GMT). UTC is an international abbreviation that is neither French nor English. It means both "Temps Universel Coordonné" and "Coordinated Universal Time".
Page	This shows the name of the NCC menu in which the change was made.
Label	This shows the action that triggered the log entry
Old value	This shows the old setting or state that was overwritten with the new value.
New value	This shows the new setting or state.
	Click this icon to display a greater or lesser number of configuration fields.

## 4.4 Create Organization

Use this screen to create an organization. You can copy the settings from an existing organization if you already created one. Click **MSP > Configure > Create organization** to access this screen.

Note: You have to contact Zyxel customer support if you need to remove an Organization from the NCC. But an administrator can remove Sites without customer support. Configure your organizations carefully. See [Section 3.16 on page 97](#) for information on removing an organization.

Note: There is no limit as to how many organizations you can create, but you can only activate a trial license for up to 10 new organizations every 90 days.

**Figure 25** MSP > Configure > Create organization

The following table describes the labels in this screen.

Table 14 MSP > Configure > Create organization

LABEL	DESCRIPTION
New Organization	
Organization name	Enter a name for your organization. Enter up to 100 characters in this field including special characters inside the square quotes [~!@#\$\$%^&*()+_{} :'"<>?-=[]\;'./].
Country	Select the country or region where the devices in the organization is located.  Note: This field is only for reference. It does not affect any other fields or features in NCC.
Copy setting from	If you already have one, or more than one organizations in your account and you want to copy the organization settings of an existing one, select the organization name.
Add this Org to MSP Teams	If you already have one, or more than one MSP teams ( <b>MSP &gt; Configure &gt; Admins &amp; teams</b> ) in your account and you want to add this organization to an existing one, select the MSP team.
Create organization	Click this button to add a new organization.

## 4.5 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 > Configure > MSP branding**.

**Figure 26** MSP > Configure > MSP branding

The following table describes the labels in this screen.

**Table 15** MSP > Configure > 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. <ul style="list-style-type: none"> <li>Allowed image file formats: JPG/JPEG, PNG, GIF.</li> <li>Maximum image file size: 200 KB.</li> <li>NCC converts the image file to a 160 x 44 pixel logo after uploading.</li> </ul>
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.

Table 15 MSP &gt; Configure &gt; MSP branding (continued)

LABEL	DESCRIPTION
Apply to	Select <b>All current and new PRO organizations</b> to apply the logo to all Nebula Professional Pack organization dashboards.  Select <b>Custom</b> to choose which Nebula Professional Pack organization to apply the logo.  Select <b>None</b> 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 <b>ON</b> to display the standard Zyxel support contact information in the <b>Help &gt; Support request</b> screen. Organization owners can choose to hide the default <b>Help &gt; Support</b> 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 <b>All current and new PRO organizations</b> to apply the support contact information to all Nebula Professional Pack organization <b>Help &gt; Support request</b> screens.  Select <b>Custom</b> to choose which Nebula Professional Pack organization to apply the support contact information.  Select <b>None</b> if you only wish to save the settings but will not apply it yet.

## 4.6 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 > Configure > Administrators**, especially if you have a large number of organizations.

### 4.6.0.1 Administrator Privilege Priority

You can configure organization administrator privileges on the following screens:

- **MSP > Configure > Admins & teams > Admins**
- **MSP > Configure > Admins & teams > Teams**
- **Group-wide > Configure > Administrators**
- **Organization-wide > Configure > Administrators**

If an NCC account has different administrator privileges configured on different screens, then the highest privilege level takes priority.

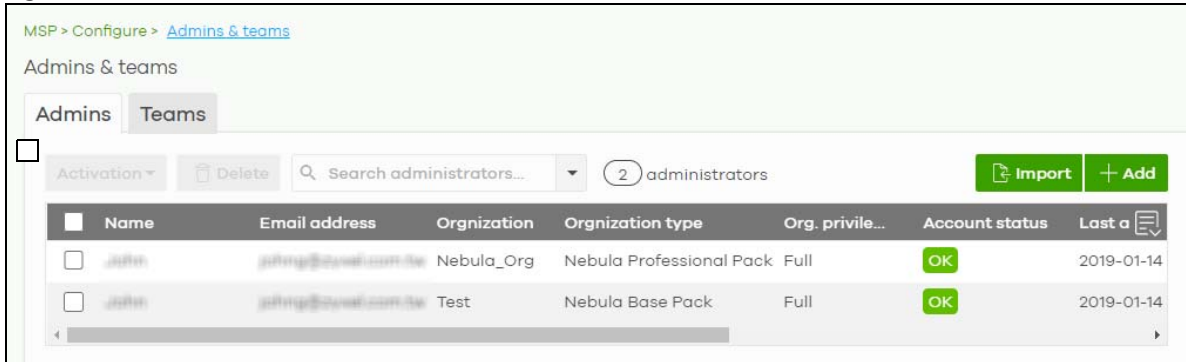
Example, account User1 has four different privilege levels configured for organization Org1 on the four screens above: None, Read-Only, Full, Full (Delegate). User1's final privilege level for Org1 is Full (Delegate).

### 4.6.1 Admins Screen

The admins screen allows you to assign an administrator account to multiple organizations. To access this screen, click **MSP > Configure > Admins & teams > Admins**.



Figure 27 MSP &gt; Configure &gt; Admins &amp; teams &gt; Admins




The following table describes the labels in this screen.

Table 16 MSP &gt; Configure &gt; Admins &amp; teams &gt; Admins

LABEL	DESCRIPTION
Activation	Click this button to <b>Activate/Deactivate</b> the selected accounts. Then, click <b>Update</b> .
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.
Import	Click this button to create administrator accounts in bulk by importing a complete list of all new administrators in an Excel file. Click <b>template</b> to view the file format. <div data-bbox="495 978 1125 1304" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><b>Bulk Import</b> <span style="float: right;">×</span></p> <p>"Bulk Import" supports for faster inputting. Please follow this <a href="#">template</a> to import</p> <div style="border: 1px dashed gray; padding: 5px; text-align: center;"> <p><b>Browse</b></p> <p>Or drag file here...</p> </div> <p style="text-align: right;"><b>Close</b></p> </div>
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.

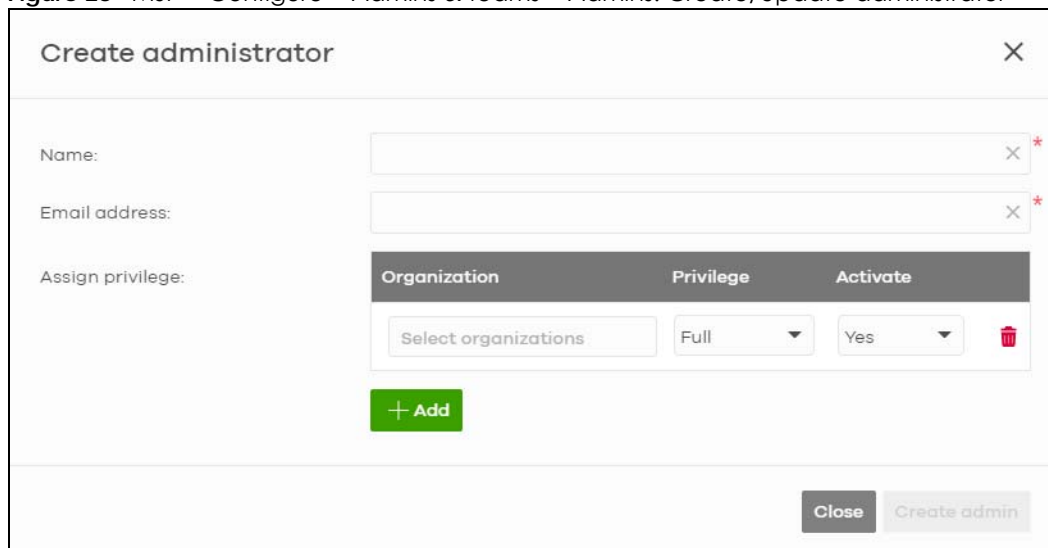
Table 16 MSP &gt; Configure &gt; Admins &amp; teams &gt; Admins (continued)

LABEL	DESCRIPTION
Org. privilege	<p>This shows the privileges the administrator has within the specified organization.</p> <p><b>Full:</b> 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.</p> <p><b>Read-only:</b> the administrator account has no write access to the organization, but can be a site administrator.</p> <p><b>Delegate owner's authority:</b> 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:</p> <ul style="list-style-type: none"> <li>• Delete organization</li> <li>• Transfer organization ownership</li> <li>• Assign delegate owner privileges to an administrator account</li> </ul>
Account status	This shows whether the administrator account has been validated ( <b>OK</b> ). It shows <b>Deactivated</b> 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.

#### 4.6.1.1 Create/Update Administrator

In the **MSP > Configure > 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 28 MSP &gt; Configure &gt; Admins &amp; teams &gt; Admins: Create/Update administrator



**Create administrator** ✕

Name:  ✕ \*

Email address:  ✕ \*

Assign privilege:


Organization	Privilege	Activate
Select organizations	Full ▼	Yes ▼ <span style="color: red;">✖</span>

+ Add

Close Create admin

The following table describes the labels in this screen.

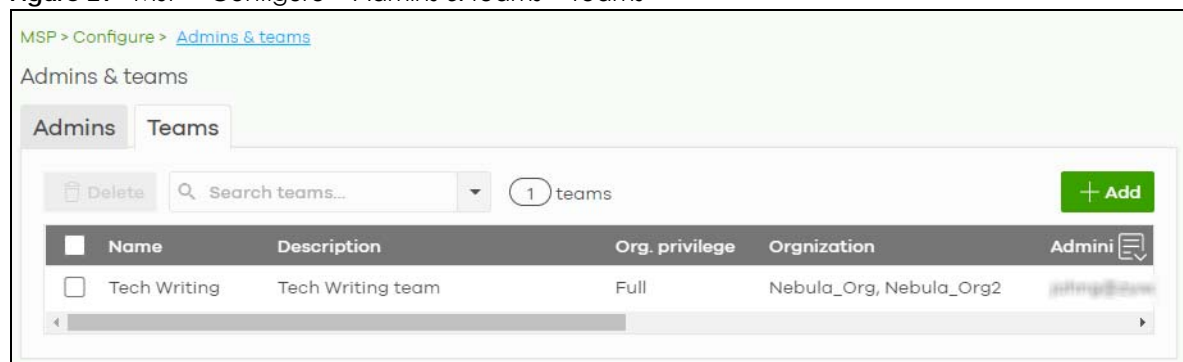
Table 17 MSP > Configure > Admins & teams > Admins: Create/Update administrator

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.  <b>Full:</b> 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.  <b>Read-only:</b> the administrator account has no write access to the organization, but can be a site administrator.
Activate	Select <b>Yes</b> to enable the account or <b>No</b> 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.

## 4.6.2 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 > Configure > Admins & teams > Teams**.

Figure 29 MSP > Configure > Admins & teams > Teams




The following table describes the labels in this screen.

Table 18 MSP > Configure > 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.

Table 18 MSP &gt; Configure &gt; Admins &amp; teams &gt; Teams (continued)

LABEL	DESCRIPTION
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.  <b>Full:</b> 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.  <b>Read-only:</b> 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.

#### 4.6.2.1 Create/Update Team

In the **MSP > Configure > 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 30** MSP > Configure > Admins & teams > Teams: Create/Update Team

The screenshot shows a 'Create team' form with the following elements:

- Name:** A text input field with a red asterisk indicating it is required.
- Description:** A text input field with a red asterisk indicating it is required.
- Assign privilege:** Two radio buttons: 'Full' (selected) and 'Read-only'.
- Organizations:** A dropdown menu labeled 'Select organizations'.
- Members:** A table with two columns: 'Name' and 'Email'. Each row has a red asterisk in the Name column and a red asterisk in the Email column. There are 'x' icons to delete each row and a red trash icon to delete the entire row. A green '+ Add' button is below the table.
- Buttons:** 'Close' and 'Create' buttons at the bottom right.

The following table describes the labels in this screen.

**Table 19** MSP > Configure > 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.  <b>Full:</b> 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.  <b>Read-only:</b> 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 19 MSP &gt; Configure &gt; Admins &amp; teams &gt; Teams: Create/Update Team (continued)

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.

## 4.6.3 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.

### 4.6.3.1 Cross-Org setting sync

Cross-org sync copies the following items from one MSP 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 > Configure > Settings > Country**
- **Organization-wide > Configure > 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.

### 4.6.3.2 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 20 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: <ul style="list-style-type: none"> <li>AP site-wide configuration is cloned</li> <li>Individual AP configuration is NOT cloned (for example, radio settings)</li> </ul>	When enabled: <ul style="list-style-type: none"> <li>AP site-wide configuration and individual AP configuration are cloned (for example, radio settings)</li> </ul>	When enabled: <ul style="list-style-type: none"> <li>AP site-wide configuration and individual AP configuration are cloned (for example, radio settings)</li> </ul>
Switch	When enabled: <ul style="list-style-type: none"> <li>Switch site-wide configuration is cloned</li> <li>Individual Switch configuration is NOT cloned (for example, IGMP)</li> <li>Switch port configuration is NOT cloned</li> </ul>	When enabled: <ul style="list-style-type: none"> <li>Switch site-wide configuration is cloned</li> <li>Individual Switch configuration is cloned (for example, IGMP)</li> <li>Switch port configuration is cloned</li> </ul>	When enabled: <ul style="list-style-type: none"> <li>Switch site-wide configuration is cloned</li> <li>Individual Switch configuration is cloned (for example, IGMP)</li> <li>Switch port configuration is cloned</li> </ul>
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.

### 4.6.3.3 Cross-org synchronization Screen

Use this screen to configure cross-org synchronization and cross site clones.

Figure 31 MSP &gt; Configure &gt; Cross-org synchronization

MSP > Configure > [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

Sync

**Cross-Org site clone with device movement**

From source organization: Test\_July ZyNet TW

Move site devices to cloned site in destination organization. [What is it?](#)

When you moving site include devices to another organization, you could select reset device Management/WAN Interface or keep it if your networking environment is similar or the same.

Keep Management/WAN Interface.

To dest. organization: TWTest

Clone

The following table describes the labels in this screen.

Table 21 MSP > Configure > Cross-org synchronization

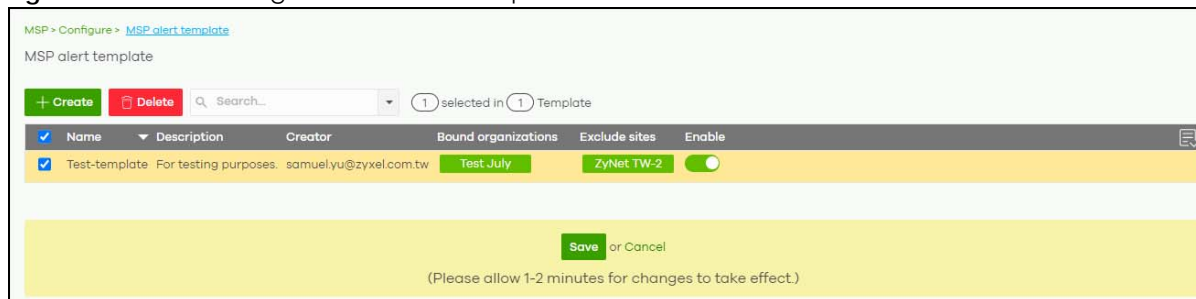
LABEL	DESCRIPTION
Cross-Org setting sync	
From source organization	Select the organization to copy settings from.
Org. setting	Select the settings that you want to copy from the source to the destination organization. Select <b>All org-wide settings</b> to copy everything.
To dest. organization	Select 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 <b>All sites</b> to copy all sites from the source to the destination organization.  Select <b>Move site devices to cloned site in destination organization</b> to include the Nebula Devices.  Enable <b>Keep Management/WAN interface</b> 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.

## 4.7 MSP Alert Template

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 4.7.1 on page 169](#) for details on creating an alert template.

To access this screen, click **MSP > Configure > MSP alert template** in the navigation panel.

Figure 32 MSP > Configure > MSP alert template





The following table describes the labels in this screen.

Table 22 MSP > Configure > MSP alert template

LABEL	DESCRIPTION
+ Create	Click this button to add a new alert template (see <a href="#">Section 4.7.1 on page 169</a> ).
Delete	Click this button to remove alert templates already created.
Search	Specify your desired search criteria to filter the list of alerts.
selected in	This shows the number of alerts that match your filter criteria after you perform a search.
Template	This shows the number of alert templates you have created.
Name	This shows a descriptive name of the alert template.
Description	This shows more details on the alert template.
Creator	This shows your email address.
Bound organizations	This shows <b>All organizations</b> 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 <b>Name</b> , <b>Description</b> , <b>Creator</b> , <b>Bound organizations</b> , and <b>Exclude sites</b> fields, just click the field and the <b>Update alert</b> screen will appear.	

## 4.7.1 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 > Configure > MSP alert template > 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 avoid 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 33 MSP &gt; Configure &gt; MSP alert template &gt; Create/Update alert

**Create alert**
✕

---

**General**

Template name

Description

Email recipient  ⓘ

Apply to   
 All organizations   
 Select organizations

Exclude sites

Enable

---

**System alerts**  ⓘ

Wireless   
  minutes after AP goes offline

Switches   
  minutes after Switches goes offline

minutes  goes down

Security gateway   
  minutes after the gateway goes offline

Any DHCP lease pool is exhausted

A VPN connection is established or disconnected

WAN connectivity status changed

Mobile router   
  minutes after the mobile router goes offline

Other   
 Configuration settings are changed

---

**Security alerts**

CDR containment  ⓘ   
 Email to receive containment alerts

---

Security Report

Notification mode   
 Email to receive security alerts by SecuReporter

Email subject   ⓘ (Optional, maximum character is 64.)

Email description   ⓘ (Optional, maximum character is 255.)

Notification interval   
 Select notification interval if events were triggered

Event severity   
 Select severity level for email information

Event threshold				
Category		Severity		
Network Security	Attack counts	High	<input type="text" value="1"/>	times of highest severity attacks within 5 minutes.
Network Security	Attack counts	High	<input type="text" value="10"/>	times attacks within 5 minutes.
Network Security	Alert counts	High	<input type="text" value="10"/>	count(s) of Malware/IPS(highest severity)/ADP(protocol anomaly) within 1 minute.
Network Security	Malware/virus detection	Medium	<input type="text" value="2"/>	times of same malware/virus is detected within 15 minutes.
Network Security	Malware/virus detection	High	<input type="text" value="10"/>	count(s) of malware/virus attack within 5 minutes.
Network Security	URL Threat Filter	High	<input type="text" value="5"/>	times of connection to threat websites within 60 minutes.
Network Security	DNS Threat Filter	High	<input type="text" value="5"/>	times of connection to threat/block DNS domain within 60 minutes.
Network Security	Sandboxing	High	<input type="text" value="10"/>	times destroyed malicious files within 5 minutes.
Network Security	Sandboxing	High	<input type="text" value="10"/>	times destroyed suspicious files within 5 minutes.
Network Security	IP Reputation-Incoming	High	<input type="text" value="10"/>	times over of attacks to the internal network from external threat IP address within 10 minutes.
Network Security	IP Reputation-Outgoing	High	<input type="text" value="1"/>	times over of connections to threat websites within 60 minutes
Anomaly	Login failure	Medium	<input type="text" value="10"/>	times of login failures within 1 minute.
Anomaly	Traffic anomaly	High	<input type="text" value="1"/>	times of traffic anomaly scans/floods detected within 5 minutes.
Anomaly	Protocol anomaly	High	<input type="text" value="1"/>	times of protocol anomaly TCP/UDP/ICMP/IP decoders within 5 minutes.

Close Create

The following table describes the labels in this screen.

Table 23 MSP > Configure > MSP alert template > 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	<p>Enter the email addresses to which you want to send alerts.</p> <p>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.</p> <p>For example, <b>ORG 1</b> is a Base tier organization, and <b>ORG 2</b> is a Professional tier organization. An MSP alert template is created to monitor AP offline events. If there are three email recipients in both <b>ORG 1</b> and <b>ORG 2</b> with the following licenses:</p> <ul style="list-style-type: none"> <li>• <b>REP 1</b> (recipient 1) has an account which includes an MSP license.</li> <li>• <b>REP 2</b> (recipient 2) and <b>REP 3</b> (recipient 3) has accounts which does not include an MSP license.</li> </ul> <p>When an AP offline event occurs, an email alert will only be sent to <b>REP 1</b> in <b>ORG 1</b>. While an email alert will be sent to all recipients (<b>REP 1</b>, <b>REP 2</b>, and <b>REP 3</b>) in <b>ORG 2</b>.</p>
Apply to	Select <b>All organizations</b> or specify the selected organizations to send alerts to.
Exclude sites	Select the sites in organizations that will not receive any alerts.

Table 23 MSP &gt; Configure &gt; MSP alert template &gt; 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: <ul style="list-style-type: none"> <li>• <b>Email:</b> Alert notifications are sent by email to configured recipients.</li> <li>• <b>In-app Push:</b> 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.</li> <li>• <b>Both:</b> Alert notifications are sent by email and app notification.</li> <li>• <b>Disabled:</b> No alerts are sent.</li> </ul>
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: <ul style="list-style-type: none"> <li>• A gateway device goes offline.</li> <li>• Any DHCP pool on the gateway device runs out of IP addresses to assign.</li> <li>• A VPN connection to or from the gateway device is created or terminated.</li> <li>• The WAN connectivity goes offline.</li> </ul>
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.

---

# PART III

## Manage by Deployment: Group, Organization, Site

---

# CHAPTER 5

## Group-wide

### 5.1 Introduction

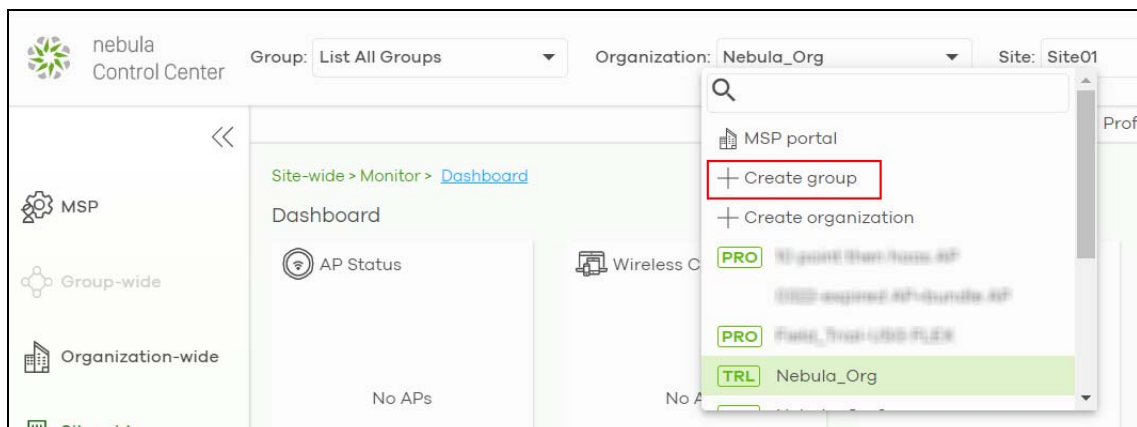
This chapter discusses the menus that you can use to monitor and manage your groups settings.

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.

#### 5.1.1 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** [X]

Group name: Test Group [X]

Group member: test [X] TestOrg2 [X]

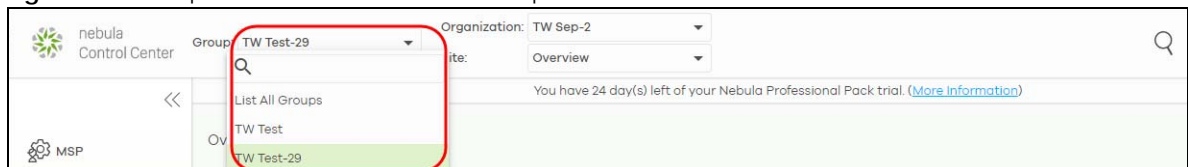
Note: You could select organizations own by you to join Group.

Cancel OK

## 5.1.2 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 34** Group > Monitor > Overview: Group



## 5.2 Monitor

The **Group** menus allow you to monitor and configure group settings, and also the inventories and logs of the sites and organizations in the group.

### 5.2.1 Overview

The overview screen allows you to view the status of organizations in a group. Click **Group-wide > Monitor > Overview** to access this screen.

**Figure 35** Group-wide > Monitor > Overview

Status	Organization	Type	NCC license status	Payment mode	NCC license expiration (UTC)
O	Nebula_Org2	Nebula Professional Pack (Trial)	OK		2021-04-30
O	test	Nebula Professional Pack (Trial)	OK		2021-04-30
O	TestOrg2	Nebula Professional Pack (Trial)	OK		2021-04-25

The following table describes the labels in this screen.

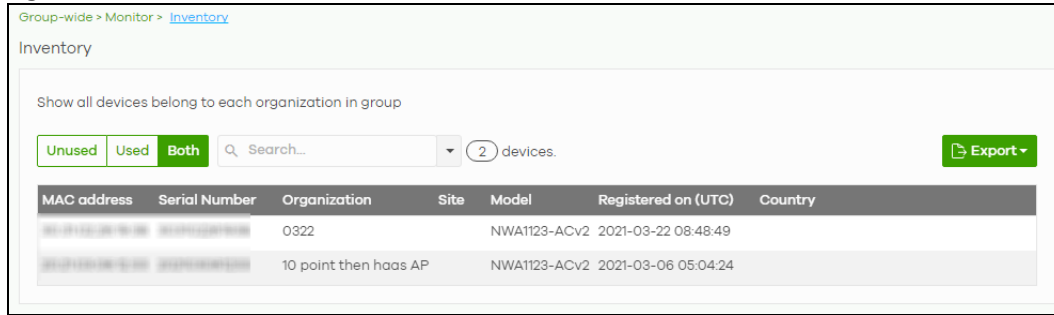
Table 24 Group-wide > Monitor > Overview

LABEL	DESCRIPTION
Search	Specify your desired filter criteria to filter the list of organizations.
matches in	This shows the number of organizations that match your filter criteria after you perform a search.
N Organizations	This shows the number of organizations (N) in the group.
Status	This shows the status of Nebula Devices in the organization. <ul style="list-style-type: none"> <li>Green: All Nebula Devices are online and have no alerts.</li> <li>Amber: One or more Nebula Devices have alerts.</li> <li>Red: One or more Nebula Devices are offline.</li> <li>Gray: All Nebula Devices have been offline for 7 days or more.</li> <li>White: No Nebula Devices.</li> </ul>
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 ( <b>OK</b> ), the license has expired and the organization downgraded from NCC Pro or Plus Pack to the base tier ( <b>Expired</b> ), or this is a free organization and an NCC license is not required ( <b>N/A</b> ).
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 <b>N/A</b> 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: <ul style="list-style-type: none"> <li>Green: The Nebula Device is online and has no alerts.</li> <li>Amber: The Nebula Device has alerts.</li> <li>Red: The Nebula Device has been offline for less than 7 days.</li> <li>Gray: The Nebula Device has been offline for 7 days or more.</li> </ul>
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.

## 5.2.2 Inventory

Use this screen to view all Nebula Devices in the organizations of the selected group. Click **Group-wide > Monitor > Inventory** to access this screen.



**Figure 36** Group-wide > Monitor > Inventory

The following table describes the labels in this screen.

**Table 25** Group-wide > Monitor > 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.
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.

### 5.2.3 Change Log

Use this screen to view logged messages for changes in all organizations in the group. Click **Group-wide > Monitor > 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 37 Group-wide &gt; Monitor &gt; Change log

Group-wide > Monitor > [Change log](#)

Change log

Keyword:

From: 2021-03-16 03:59 To: 2021-03-26 03:59 UTC+0

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

< Newer Older > 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 <del>Admin (Full)</del>		Added, Organizati...
2021-03-23 06:07:51	svd nsbu	Administrator	Updated Tech-wri...	Removed: Organiz...	Added: Organizati...
2021-03-23 06:02:12	svd nsbu	Administrator	Changed Tech-wr...	Organization: Rea...	Organization: Full
2021-03-23 05:59:56	svd nsbu	Administrator	Added Tech-write...		Added, Organizati...
2021-03-23 03:29:45	svd nsbu	Administrator	Added <del>Admin (Full)</del>		Added, Organizati...
2021-03-23 03:28:51	svd nsbu	Administrator	Added <del>Admin (Full)</del>		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 <del>Admin (Full)</del>		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 26 Group-wide &gt; Monitor &gt; 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 <b>Search</b> to filter log entries by date. <b>Range:</b> Display log entries from the first specified date to the second specified date. <b>Before:</b> 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 <input type="button" value="X"/>	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.
<input type="button" value="More"/>	Click this icon to display a greater or lesser number of configuration fields.

## 5.3 Configure

Use the **Configure** menus to create a new group and manage group general settings, administrator accounts and VPN members.

### 5.3.1 Group Settings

Use this screen to change your general group settings, such as the group name and members. Click **Group-wide > Configure > Settings** to access this screen.

**Figure 38** Group-wide > Configure > 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

Delete Group

The following table describes the labels in this screen.

**Table 27** Group-wide > Configure > Settings

LABEL	DESCRIPTION
Group name	Enter a descriptive name for the group.
Description	Enter a description for the group.

Table 27 Group-wide &gt; Configure &gt; Settings (continued)

LABEL	DESCRIPTION
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 <b>Hub to Hub VPN</b> is disabled at <b>Group-wide &gt; Configure &gt; Org-to-Org VPN</b> .

## 5.3.2 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.

### 5.3.2.1 Configure Org-to-Org VPN

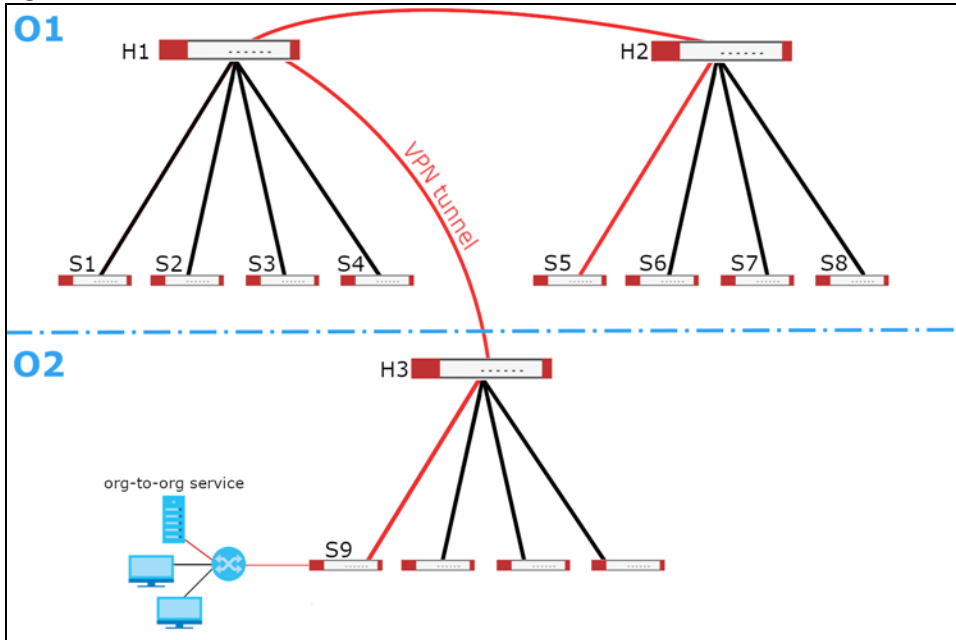
Follow the steps below to configure Org-to-Org VPN in the group.

- 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 > Configure > 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 > Configure > 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.

### 5.3.2.2 Org-to-Org VPN Example

[Figure 39](#) 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**.

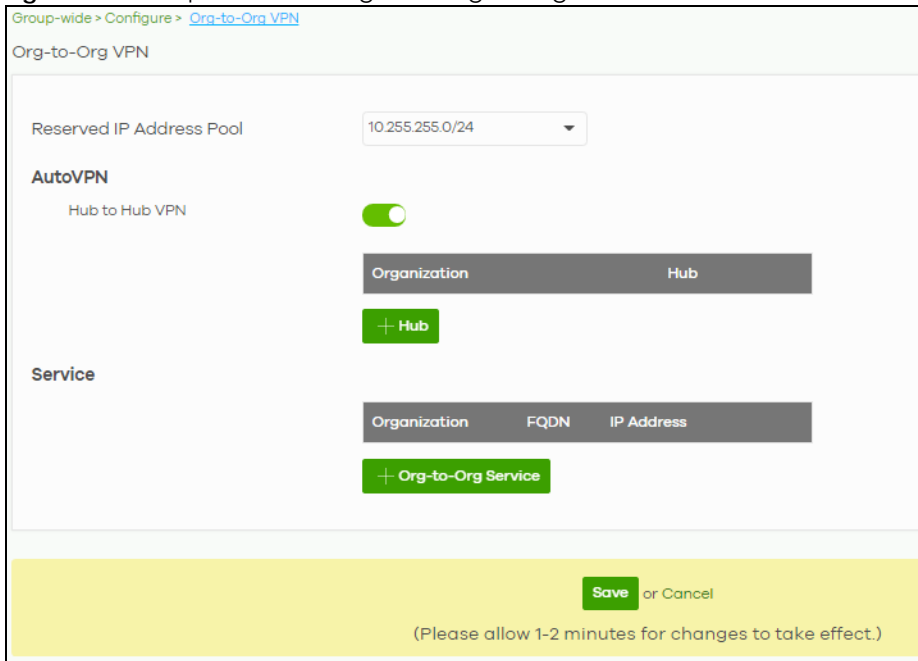
Figure 39 Org-to-Org VPN Example



### 5.3.2.3 Org-to-Org VPN Screen

Click **Group-wide > Configure > Org-to-Org VPN** to access this screen.

Figure 40 Group-wide > Configure > Org-to-Org VPN



The following table describes the labels in this screen.

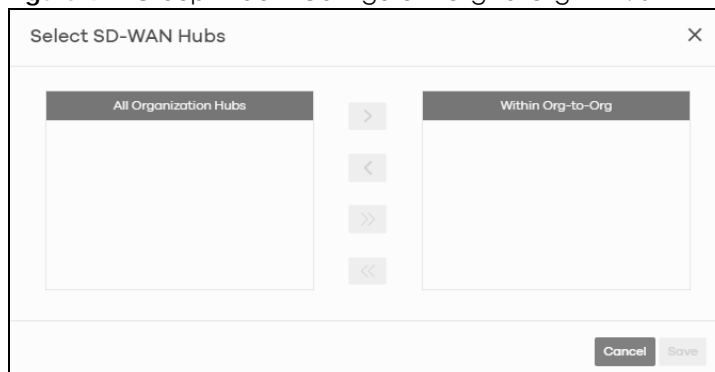
Table 28 Group-wide > Configure > Org-to-Org VPN

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 <b>On</b> 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 <b>Org-to-Org VPN</b> .
+Hub	Click this to set up which hub site you want to add to the <b>Org-to-Org VPN</b> .
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 <b>Cancel</b> to exit this screen without saving.

### 5.3.2.4 Add Hub

Click the **+Hub** button on the **Group-wide > Configuration > 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 41 Group-wide > Configure > 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 29 Group-wide > Configure > 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 <b>Cancel</b> to exit this screen without saving.
Save	Click <b>Save</b> to add the hubs to the org-to-org network.

### 5.3.2.5 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 42 Group-wide > Configure > Org-to-Org VPN: Service

The following table describes the labels in this screen.

Table 30 Group-wide > Configure > Org-to-Org VPN: Service

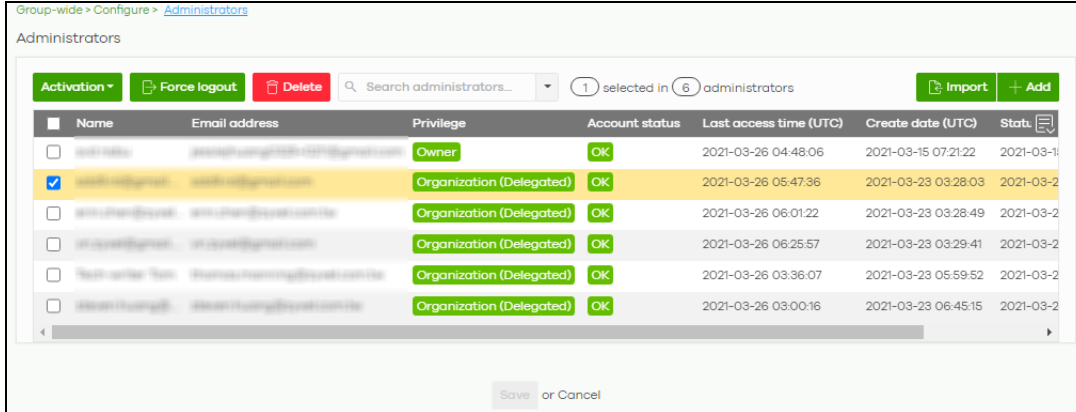
LABEL	DESCRIPTION
Organization	Select the organization to which the service you want to add is linked to.
FQDN	Enter the Fully-Qualified Domain Name (FQDN) associated with the service.  An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw 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 <b>Save</b> to allow access to the service through the org-to-org VPN.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

### 5.3.3 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 > Configure > Administrators** to access this screen.

Figure 43 Group-wide > Configure > Administrators




The following table describes the labels in this screen.

Table 31 Group-wide > Configure > Administrators

LABEL	DESCRIPTION
Activation	Click this button to <b>Activate/Deactivate</b> the selected accounts. Then, click <b>Update</b> .
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.
Import	Click this button to create administrator accounts in bulk by importing a complete list of all new administrators in an Excel file.  <div data-bbox="493 1066 1125 1392" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><b>Bulk Import</b> <span style="float: right;">✕</span></p> <p>"Bulk Import" supports for faster inputting. Please follow this <a href="#">template</a> to import</p> <div style="border: 1px dashed gray; padding: 5px; text-align: center; margin: 10px 0;"> <p><span style="background-color: #28a745; color: white; padding: 5px 10px;">Browse</span></p> <p>Or drag file here...</p> </div> <p style="text-align: right;"><span style="background-color: #6c757d; color: white; padding: 5px 10px;">Close</span></p> </div>
Add	Click this button to create a new group administrator account. See <a href="#">Section 5.3.3.1 on page 185</a> .
Name	This shows the name of the administrator account.
Email address	This shows the email address of the administrator account.



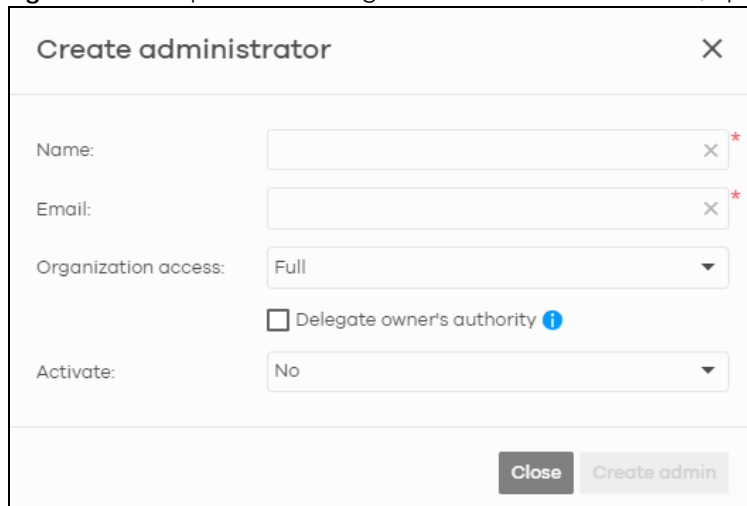
Table 31 Group-wide &gt; Configure &gt; Administrators (continued)

LABEL	DESCRIPTION
Privilege	<p>This shows the privileges the administrator has within all organizations in the group.</p> <p><b>Full:</b> 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.</p> <p><b>Read-only:</b> the administrator account has no write access to the organization, but can be a site administrator.</p> <p><b>Delegate owner's authority:</b> 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:</p> <ul style="list-style-type: none"> <li>• Delete organization</li> <li>• Transfer organization ownership</li> <li>• Assign delegate owner privileges to an administrator account.</li> </ul>
Account status	This shows whether the administrator account has been validated ( <b>OK</b> ). It shows <b>Deactivated</b> 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.

### 5.3.3.1 Create/Update Administrator

In the **Group-wide > Configure > 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 44** Group-wide > Configure > Administrators: Create/Update administrator



**Create administrator** ✕

---

Name:  ✕ \*

Email:  ✕ \*

Organization access: Full ▼

Delegate owner's authority ⓘ

Activate: No ▼

---

Close Create admin

The following table describes the labels in this screen.

Table 32 Group-wide > Configure > 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. <b>Full:</b> 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. <b>Read-only:</b> 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 <b>Organization access</b> is set to <b>Full</b> . 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: <ul style="list-style-type: none"> <li>• Delete organization</li> <li>• Transfer organization ownership</li> <li>• Assign delegate owner privileges to an administrator account.</li> </ul>
Activate	Select <b>Yes</b> to enable the account or <b>No</b> 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.

# CHAPTER 6

## Organization-wide

### 6.1 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.

### 6.2 Monitor

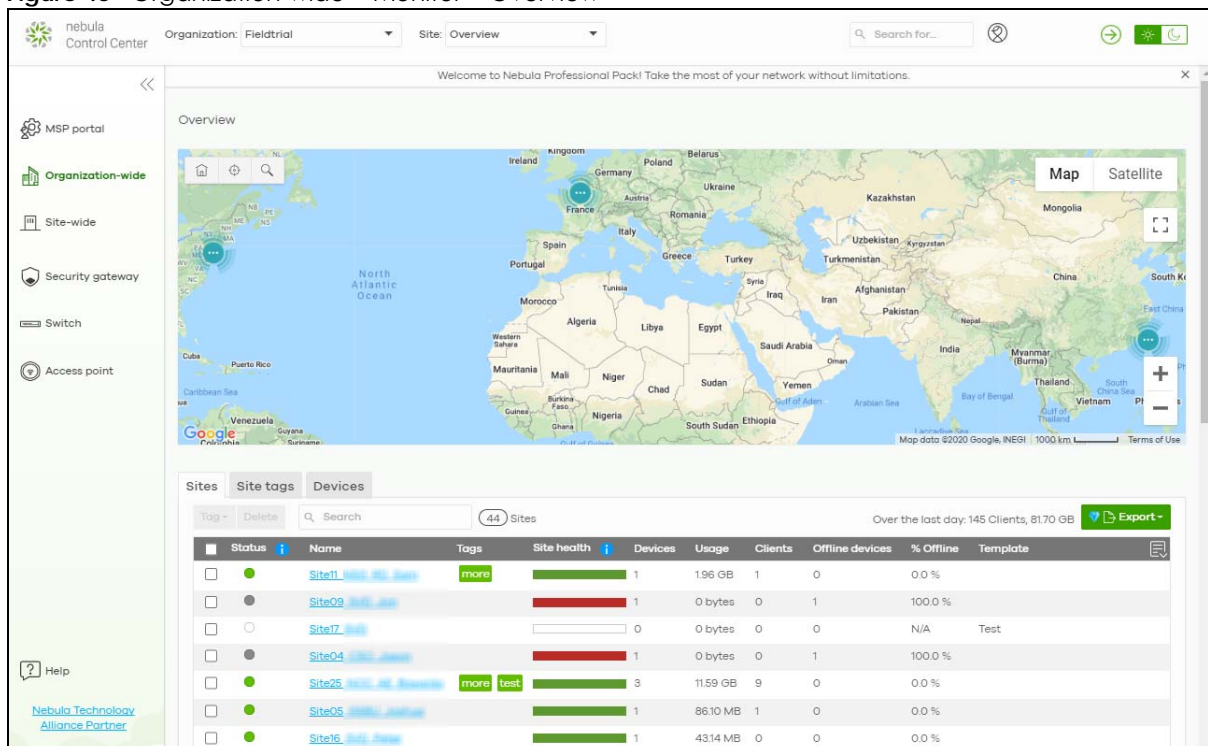
Use the **Monitor** menus to check the site and Nebula Device information and change logs for the selected organization.

#### 6.2.1 Organization Overview

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 > Monitor > Overview** to access this screen.

Figure 45 Organization-wide > Monitor > Overview



### 6.2.1.1 Sites

Click the **Sites** tab in the **Overview** screen to view detailed information of the sites which are associated with the selected organization.

**Figure 46** Organization-wide > Monitor > Overview: Sites


Status	Name	Usage	Client	Tag	Site health	Device	Offline device	% Offline
Green	Site11	37.57 MB	0		Green	1	0	0.0 %
Red	Site09	0 bytes	0		Red	1	1	100.0 %
White	Site17	0 bytes	0		White	0	0	N/A
Red	Site04	0 bytes	0		Red	1	1	100.0 %
Green	Site25	12.09 GB	9	more test	Green	4	0	0.0 %
Green	Site05	204.27 MB	1		Green	1	0	0.0 %
Red	Site16	21.56 MB	0		Red	1	1	100.0 %
Red	Site01	0 bytes	0		Red	1	1	100.0 %
Red	Site14	0 bytes	0		Red	1	1	100.0 %
Red	Site30	11.36 GB	30		Red	6	1	16.7 %

The following table describes the labels in this screen.

**Table 33** Organization-wide > Monitor > Overview: Sites

LABEL	DESCRIPTION
Tag	Select one or multiple sites and click this button to create a new tag for the sites or delete an existing tag.
Delete	Select the sites and click this button to remove it.
Search	Enter a key word as the filter criteria to filter the list of sites.
Sites	This shows the number of sites in this organization.
Over the last day	This shows how many clients are associated with the sites in this organization and the total amount of data transmitted or received by the clients in the past day.
Export	Click this button to save the site list as a CSV or XML file to your computer.
Status	This shows the status of Nebula Devices in the site. <ul style="list-style-type: none"> <li>Green: All Nebula Devices are online and have no alerts.</li> <li>Amber: Some Nebula Devices have alerts.</li> <li>Red: Some Nebula Devices are offline.</li> <li>Gray: All Nebula Devices have been offline for 7 days or more.</li> <li>White: No Nebula Devices.</li> </ul>
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. <ul style="list-style-type: none"> <li>Green: 95 – 100% network uptime</li> <li>Dark green: 75 – 95% network uptime</li> <li>Brown: 50 – 75% network uptime</li> <li>Red: &lt; 50% network uptime</li> <li>Grey: No uptime data</li> </ul>

Table 33 Organization-wide &gt; Monitor &gt; Overview: Sites (continued)

LABEL	DESCRIPTION
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.

### 6.2.1.2 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 47 Organization-wide &gt; Monitor &gt; Overview: Site tags

Client	Device	% Offline	Offline device	Offline site	Site	Status	Tag	Usage
10	5	0.0 %	0	0	1	Green	more	7.93 GB
10	5	0.0 %	0	0	1	Green	test	7.93 GB

The following table describes the labels in this screen.

Table 34 Organization-wide &gt; Monitor &gt; Overview: 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. <ul style="list-style-type: none"> <li>Green: All Nebula Devices are online and have no alerts.</li> <li>Amber: Some Nebula Devices have alerts.</li> <li>Red: Some Nebula Devices are offline.</li> <li>Gray: All Nebula Devices have been offline for 7 days or more.</li> <li>White: No Nebula Devices.</li> </ul>
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.

### 6.2.1.3 Devices

Click the **Devices** tab in the **Overview** screen to view the detailed information about Nebula Devices which are connected to the sites in the selected organization.

**Figure 48** Organization-wide > Monitor > Overview: Devices


Client	MAC address	Model	Name	Site	Status	Tag	Usage
0	B8EC:A3:B4:CD:9F	NSG50	B8.EC:A3.B4:CD:9F	Site11 <a href="#">NSG_40_Sum</a>	Green		0 bytes
0	B8EC:A3:B4:CC:67	NSG50	B8.EC:A3.B4:CC:67	Site09 <a href="#">NSG_40_Sum</a>	Red		0 bytes
0	B8EC:A3:B4:CF:B5	NSG50	B8.EC:A3.B4:CF:B5	Site04 <a href="#">NSG_40_Sum</a>	Red		0 bytes
9	8CE2B05C01FE	NSG50	Home GW	Site25 <a href="#">NSG_40_Sum</a>	Green		0 bytes
0	B8EC:A3:B4:0B:34	NSW200-28P	Office NSW200	Site25 <a href="#">NSG_40_Sum</a>	Green		0 bytes
3	B8B8F31A4675	NAP102	OfficeNAP102-MESH	Site25 <a href="#">NSG_40_Sum</a>	Green		0 bytes
5	40219784D713	NAP102	HomeNAP102	Site25 <a href="#">NSG_40_Sum</a>	Green	Home	2.61 GB
9	B8EC:A3:B4:7F:4D	NSW100-10P	Home NSW100	Site25 <a href="#">NSG_40_Sum</a>	Green		2.69 GB
1	B8EC:A3:B4:CD:87	NSG50	B8.EC:A3.B4:CD:87	Site05 <a href="#">NSG_40_Sum</a>	Green		0 bytes
0	B8EC:A3:B4:CC:43	NSG50	B8.EC:A3.B4:CC:43	Site16 <a href="#">NSG_40_Sum</a>	Red		0 bytes

The following table describes the labels in this screen.

**Table 35** Organization-wide > Monitor > Overview: 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. <ul style="list-style-type: none"> <li>Green: The Nebula Device is online.</li> <li>Amber: The Nebula Device recently had alerts.</li> <li>Red: The Nebula Device was recently offline.</li> <li>Gray: The Nebula Device has been offline for more than 6 days.</li> </ul>
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.

Table 35 Organization-wide > Monitor > Overview: Devices (continued)

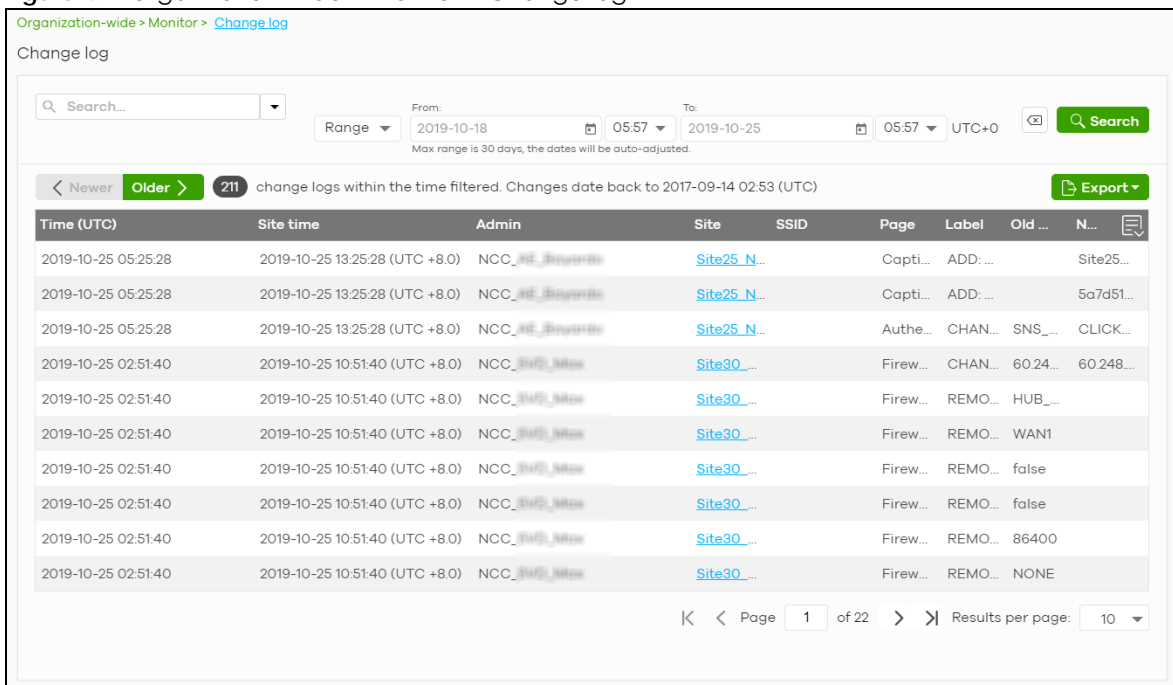
LABEL	DESCRIPTION
Configuration status	This shows whether the configuration on the Nebula Device is up-to-date.
Connectivity	This shows the Nebula Device connection status.  The red time slot indicates the connection to the NCC is down, and the green time slot indicates the connection is up. Move the cursor over a time slot to see the actual date and time when a Nebula Device is connected or disconnected.
Public IP	This shows the global (WAN) IP address of the Nebula Device.
	Click this icon to display a greater or lesser number of configuration fields.

## 6.2.2 Change Log

Use this screen to view logged messages for changes in the specified organization. Click **Organization-wide > Monitor > 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 49 Organization-wide > Monitor > Change log



Organization-wide > Monitor > [Change log](#)

Change log

Search... Range 2019-10-18 05:57 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_...@...@...	Site25_N...		Capti...	ADD: ...		Site25...
2019-10-25 05:25:28	2019-10-25 13:25:28 (UTC +8.0)	NCC_...@...@...	Site25_N...		Capti...	ADD: ...		5a7d51...
2019-10-25 05:25:28	2019-10-25 13:25:28 (UTC +8.0)	NCC_...@...@...	Site25_N...		Authe...	CHAN... SNS...		CLICK...
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_...@...@...	Site30_...		Firew...	CHAN... 60.24...		60.248...
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_...@...@...	Site30_...		Firew...	REMO... HUB...		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_...@...@...	Site30_...		Firew...	REMO... WAN1		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_...@...@...	Site30_...		Firew...	REMO... false		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_...@...@...	Site30_...		Firew...	REMO... false		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_...@...@...	Site30_...		Firew...	REMO... 86400		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_...@...@...	Site30_...		Firew...	REMO... NONE		

Page 1 of 22 Results per page: 10

The following table describes the labels in this screen.

Table 36 Organization-wide > Monitor > 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 <b>Range</b> to set a time range or select <b>Before</b> 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.

Table 36 Organization-wide &gt; Monitor &gt; Change log (continued)

LABEL	DESCRIPTION
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.
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.

## 6.3 Configure

Use the **Configure** 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.

### 6.3.1 Organization Settings

Use this screen to change your general organization settings, such as the organization name and security. Click **Organization-wide > Configure > Settings** to access this screen.



Figure 50 Organization-wide &gt; Configure &gt; Settings

Organization-wide > Configure > Settings

Settings

**Organization information**

Name:  ✕ \*

Country:  ▼

**Security**

Idle Timeout ?   ✕ \* 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 37 Organization-wide &gt; Configure &gt; 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.
<b>Security</b>	
Idle timeout	Select <b>ON</b> and enter the number of minutes each user can be logged in and idle before the NCC automatically logs out the user.  Select <b>OFF</b> if you do not want the NCC to log out idle users.

Table 37 Organization-wide &gt; Configure &gt; Settings (continued)

LABEL	DESCRIPTION
Login IP ranges	<p>Select <b>ON</b> and specify the IP address range of the computers from which an administrator is allowed to log into the NCC.</p> <p>Select <b>OFF</b> to allow any IP address of the computer from which an administrator can log into the NCC.</p>
Import certificate	
Use my certificate	Select <b>ON</b> 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	Select <b>ON</b> to prevent others from changing the ownership of the Nebula Device in your organization by simply scanning the QR code through the Nebula Mobile app. You can still transfer or unregister the Nebula Device through your myZyxel account.
Delete this organization	<p>Click the <b>Delete organization</b> button to remove the organization when it does not have any sites, Nebula Devices or users.</p> <p>Note: You will be redirected to the <b>Choose organization</b> page after this organization is deleted.</p>

### 6.3.2 Create Site

After an organization is created, click **Organization-wide > Configure > Create Site** to add a site (network) to your organization.

- 1 Enter a descriptive name of up to 64 printable characters for the site.
- 2 If you already have one or more than one sites in the organization and you want to copy the site settings of an existing one, select the **Clone from** check box and then the site name.  
If you have created a configuration template (see [Section 6.3.7 on page 230](#)), you can select to bind the new site to the specified template.
- 3 Select the type of Security Gateway that you will add to the site (see [Table 1 on page 12](#) for the supported Security Gateways). You can skip this selection if you do NOT plan to add a Security Gateway at the moment.
- 4 Choose the time zone of the site's location.
- 5 Click **Create site** to add the new site to your organization.

**Figure 51** Organization-wide > Configure > Create Site

Organization-wide > Configure > [Create site](#)

Create site

Site name:

Configuration:  Default configuration  
 Clone from   
 Bind to template

Local time zone:

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

1 selected in 1 devices. [+ Register](#)

<input checked="" type="checkbox"/>	Device name	Serial Number	MAC address	Model
<input checked="" type="checkbox"/>	202112-04-00:15	202112040015	202112-04-00:15	NR5101

[Create site](#)

- You will be re-directed to the **Site-wide > Configure > Add devices** screen. Search and select the name of the registered Nebula Device that is to be added to this site. See [Section 7.2.5 on page 288](#) for information on adding Nebula Devices.

### 6.3.3 License & Inventory

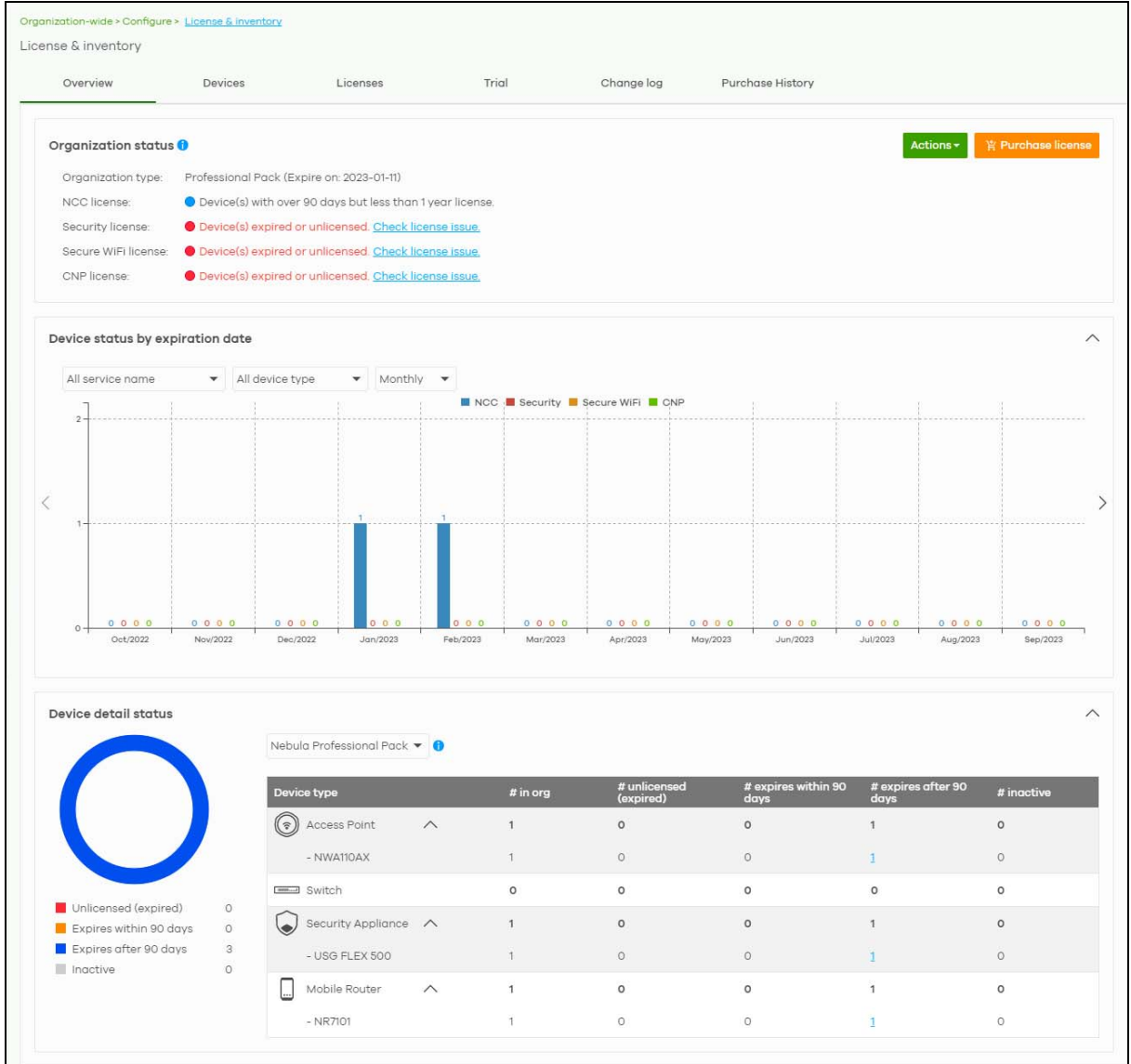
The following section describes license management screens in NCC.

Unused licenses can be transferred from a Nebula Device in an Organization to another Nebula Device in an Organization.

#### 6.3.3.1 License & Inventory Overview Screen

Use these screens to view licenses and Nebula Devices in the organization. Click **Organization-wide > Configure > License & Inventory > Overview** to access this screen.

Figure 52 Organization-wide > Configure > License & Inventory > Overview



The following table describes the labels in this screen.

Table 38 Organization-wide > Configure > License & inventory > Overview

LABEL	DESCRIPTION
Organization Status	
Actions	<p>Click this button to add licenses and/or Nebula Devices to the organization. Choose one of the following actions:</p> <ul style="list-style-type: none"> <li><b>Add more devices:</b> Add new Nebula Devices to the organization, by serial number and MAC address. For details, see <a href="#">Section 6.3.3.2 on page 198</a>.</li> <li><b>Add more licenses:</b> Add new licenses to the organization, by license key. For details, see <a href="#">Section 6.3.3.4 on page 199</a>.</li> <li><b>Install wizard:</b> 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 <a href="#">Section 6.3.3.5 on page 200</a>.</li> </ul>

Table 38 Organization-wide &gt; Configure &gt; License &amp; inventory &gt; Overview (continued)

LABEL	DESCRIPTION
Purchase License	<p>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).</p> <p>If you do not have a Circle account, you can do the following:</p> <ol style="list-style-type: none"> <li>1. Select what license to purchase and set the target expiration date to keep the Pro/Plus tier features/services running.</li> <li>2. You may export the list of required licenses to your computer.</li> <li>3. After calculating the license to purchase, click the <b>Zyxel license marketplace (Check out)</b> button to complete your purchase. Purchased licenses are directly assigned to Nebula Device(s).</li> </ol> <p><b>Unused</b> licenses assigned to your organization will not be counted as it is not yet assigned to a Nebula Device.</p> <p>This button is available only for the Full (Delegated) administrator privilege or Owner administrator account with a registered Nebula Device(s).</p>
Upgrade Now	<p>Click this button to upgrade the organization to Plus or Pro tier.</p> <p>The button is only available if you have a Plus or Pro license for every Nebula Device in the organization.</p>
Downgrade Now	<p>Click this button to downgrade the organization from Plus or Pro to Base tier, or from Pro to Plus tier.</p> <p>All active NCC licenses in the organization will stay active and continue to count down to their expiry time.</p>
Organization type	<p>This shows the licensing tier of the organization. Possible values are: <b>Base, Plus Pack, Professional Pack, and Trial.</b></p>
NCC license	<p>This shows whether there are any Nebula Devices with near expiring licenses.</p>
NSS/UTM license	<p>This shows whether the current site has an active NSS or UTM license.</p>
Secure WiFi license	<p>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.</p>
Device status by expiration date	<p>Click this button to select the data to be shown in the graph. Choose one from each of the following criteria:</p> <ul style="list-style-type: none"> <li>• <b>All service name, Nebula Professional Pack, Nebula Plus Pack, Nebula Security Pack, UTM Security Pack, or Secure WiFi:</b> select the category of licenses to display.</li> <li>• <b>All device type, Access Point, Switch, or Security Gateway:</b> select the category of Nebula Device to display.</li> <li>• <b>Monthly, Quarterly, or Yearly:</b> select the period of time to display.</li> </ul>
Device detail status	
License type	<p>Select the license type to filter your selection (<b>Nebula Professional Pack, Nebula Plus Pack, Gold Security Pack, Nebula Security Pack, UTM Security Pack, Content Filter Pack, Secure WiFi, Connect &amp; Protect</b>).</p>
Device type	<p>This shows the category of Nebula Device (<b>Access Point, Switch, Security Appliance, Mobile Router</b>) and Nebula Device model.</p>
# in org	<p>This shows the total number of Nebula Devices of the specified category and model that are in the organization.</p>
# unlicensed (expired)	<p>This shows the total number of Nebula Devices of the specified category and model that have:</p> <ul style="list-style-type: none"> <li>• No NCC Pro or Plus license.</li> <li>• An expired NCC Pro or Plus license.</li> </ul>
# near expiration in 90 days	<p>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.</p>

Table 38 Organization-wide &gt; Configure &gt; License &amp; inventory &gt; 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.

### 6.3.3.2 Add Devices Screen

Use this screen to add Nebula Devices to an organization. Click **Organization-wide > Configure > License & Inventory > Overview > Actions > Add more devices** to access this screen.

Figure 53 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Overview: Add devices: Add devices

The following table describes the labels in this screen.

Table 39 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; 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.
Acknowledge	Select this to confirm that your NCC account will be the owner of the new Nebula Devices.

Table 39 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Overview: Add devices: Add devices

LABEL	DESCRIPTION
Finish	Click this to add the Nebula Devices to the organization.
Cancel	Click this to close the screen without saving.

### 6.3.3.3 Firmware Upgrade Screen

If a newer Nebula Device firmware is available, use this screen to upgrade it. Click **Organization-wide > Configure > License & Inventory > Overview > Actions > Add more devices > Firmware upgrade** to access this screen.

**Figure 54** Organization-wide > Configure > License & Inventory > Overview: Add devices: Firmware upgrade

The screenshot shows a modal window titled "Add devices" with a close button (X) in the top right. On the left, there is a sidebar with "Add devices" and a link for "Firmware upgrade". The main content area is titled "Firmware upgrade" and contains the following text: "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)." Below this text are two radio buttons: "Yes" (which is selected) and "No". At the bottom right of the modal, there are three buttons: "Previous" (disabled), "Cancel" (disabled), and "Finish" (active).

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.

### 6.3.3.4 Add Licenses Screen


Use this screen to add licenses to an organization. Click **Organization-wide > Configure > License & Inventory > Overview > Actions > Add more licenses** to access this screen.

**Figure 55** Organization-wide > Configure > License & Inventory > Overview: Add licenses

The screenshot shows a modal window titled "Add licenses" with a close button (X) in the top right. On the left, there is a sidebar with "Add licenses" and a link for "Add licenses". The main content area is titled "Add licenses" and contains the following text: "Enter one more license keys. Or You can download the [template](#) here and [import](#) multiple license keys for faster registration." Below this text is a table with two columns: "License key" and "License information". The table has one row with an empty input field under "License key" and a trash icon under "License information". Below the table is a green "+ Add" button. At the bottom right of the modal, there are two buttons: "Cancel" (disabled) and "Finish" (disabled).

The following table describes the labels in this screen.

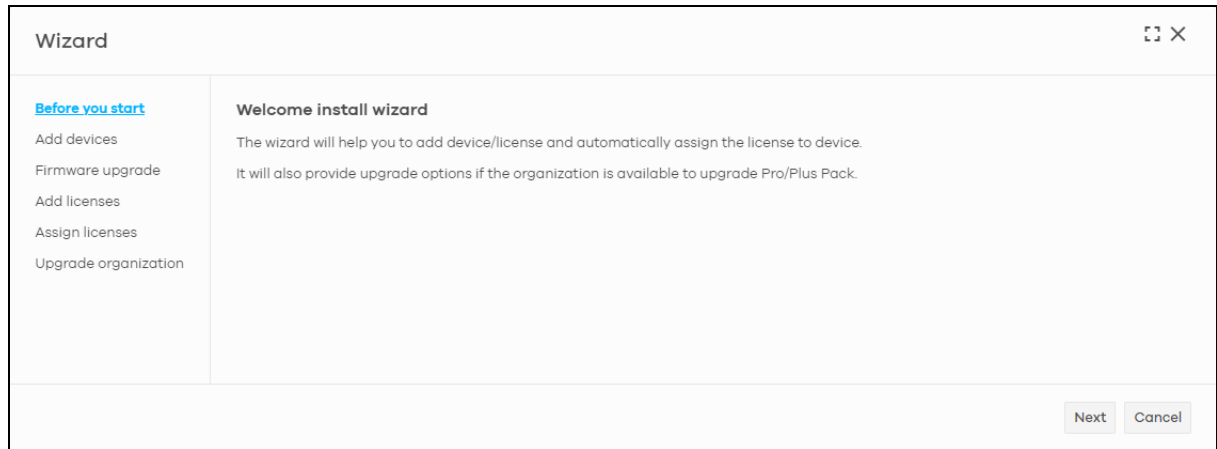
Table 40 Organization-wide > Configure > License & Inventory > Overview: Add licenses

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.

### 6.3.3.5 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 > Configure > License & Inventory > Overview > Actions > Install wizard**. After the wizard window opens, click **Next**.



- 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 6.3.3.2 on page 198](#).



**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
<input type="text"/>	<input type="text"/>	<input type="text"/>			

[+ Add another device](#)

Previous Next Cancel

- 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

Previous Next Cancel

- 4 Add the license keys of one or more licenses, and then click **Next**. For more information on this page, see [Section 6.3.3.4 on page 199](#).

**Wizard**

Before you start  
 Add devices  
 Firmware upgrade  
[Add licenses](#)  
 Assign licenses  
 Upgrade organization

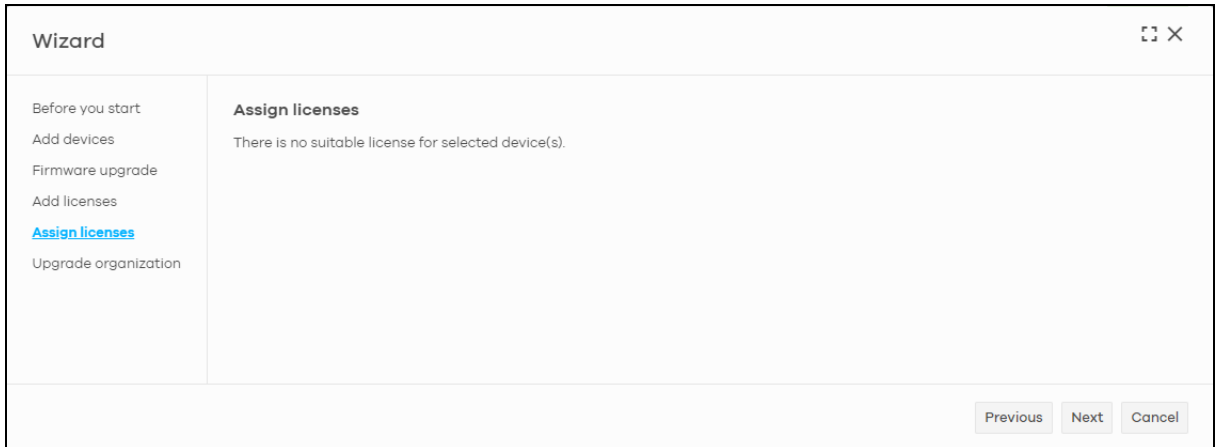
**Add licenses**  
 Enter one more license keys. Or You can download the [template](#) here and [import](#) multiple license keys for faster registration.

License key	License information
<input type="text"/>	

[+Add](#)

Previous Next Cancel

- 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**.



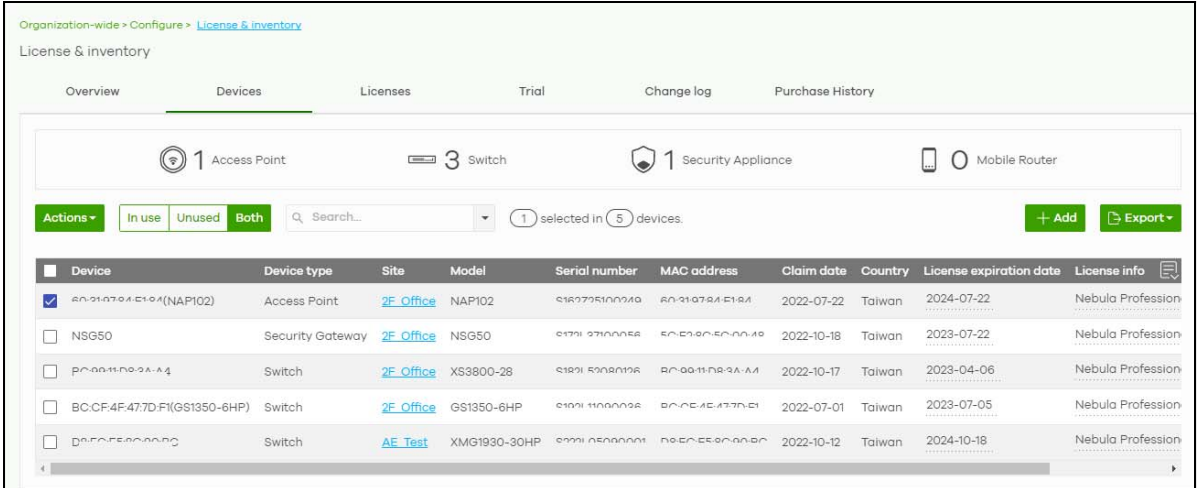
- 6 If the organization is on the base tier and you have added sufficient licenses for all Nebula Devices, you are given the option to upgrade to the Pro or Plus tier. Select **Yes** or **No**, and then click **Finish**.



### 6.3.3.6 License & Inventory Devices Screen

Use these screen to view and manage Nebula Devices in the organization. Click **Organization-wide > Configure > License & Inventory > Devices** to access this screen.

**Figure 56** Organization-wide > Configure > License & Inventory > Devices



The following table describes the labels in this screen.

**Table 41** Organization-wide > Configure > 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 41 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Devices (continued)

LABEL	DESCRIPTION
Actions	<p>Select one or more Nebula Devices and then click this button to perform one of the following actions:</p> <p><b>Change organization:</b> Moves the Nebula Device to an organization. The organizations must have the same owners.</p> <p><b>Change site assignment:</b> Moves the selected Nebula Devices to a site, or remove them from their current site while leaving them in the organization.</p> <p>Note: When you change the site for a Security Firewall (see <a href="#">Table 1 on page 12</a> for information on the supported Security Firewall devices), select the deployment method for management by Nebula (see <a href="#">Step 7: Set up the Deployment Method on page 50</a> for more information), configure the WAN settings and choose the installation method.</p> <p><b>Remove from organization:</b> Remove the Nebula Devices from NCC. You can manage the Nebula Devices in standalone mode, or re-add them to NCC later.</p> <p><b>Assign license:</b> Assign licenses to the selected Nebula Devices.</p> <p><b>Undo assign:</b> Unlink the inactive licenses from the associated Nebula Devices. After unlinking, the license will be categorized as unused in <b>Inventory</b>. An inactive license is a license that has been assigned to a Nebula Device but is not yet in use or queued.</p> <p><b>Transfer license:</b> 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.</p> <p><b>Purchase license:</b> 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 <b>Zyxel license marketplace (Check out)</b> button to complete your purchase.</p> <p><b>Unused</b> licenses assigned to your organization will not count as it is not yet assigned to a Nebula Device.</p> <p>This button is available only for the Organization (Delegated) or Owner administrator account with a registered Nebula Device(s).</p>
In use / Unused / Both	Select to display the Nebula Device currently in a site ( <b>In use</b> ), not current ( <b>Unused</b> ), or show all ( <b>Both</b> ).
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 <a href="#">Section 6.3.3.2 on page 198</a> .
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 ( <b>Access Point, Switch, Security Appliance, Firewall, Mobile Router</b> ) 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.

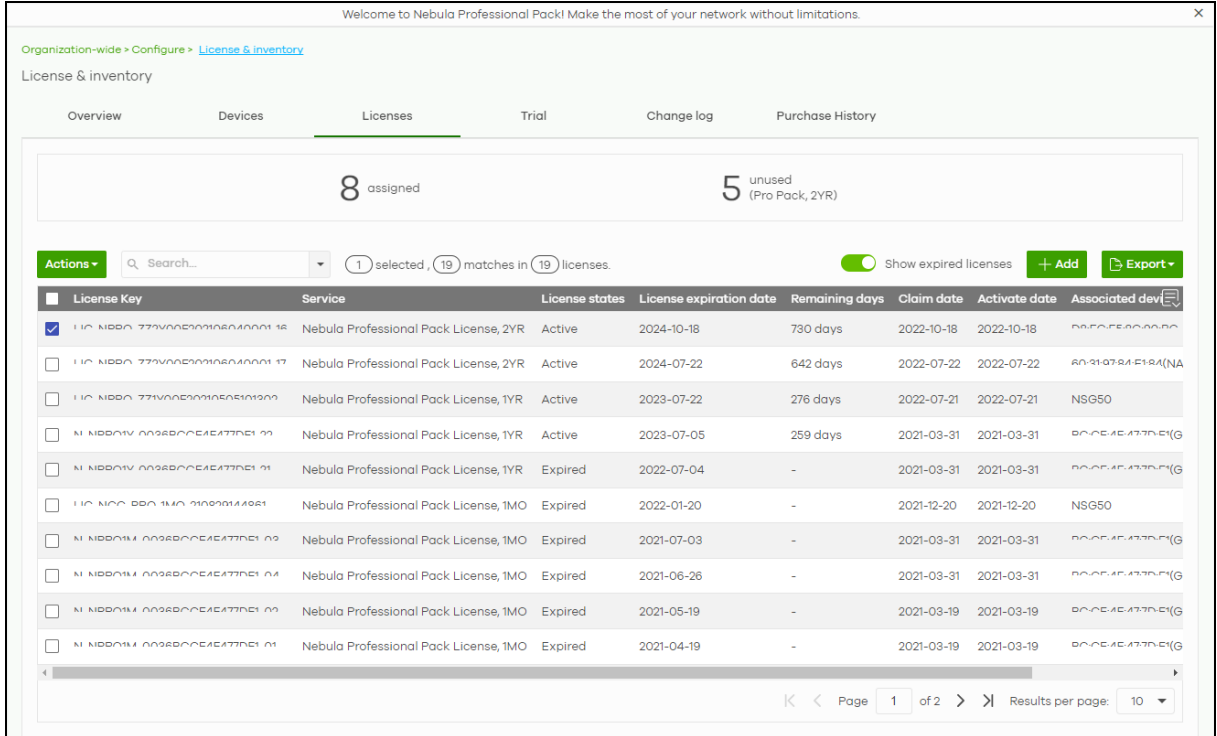
Table 41 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Devices (continued)

LABEL	DESCRIPTION
Claim date	<p>This shows the date on which the Nebula Device was added to NCC. If the Security Firewall has NOT yet connected to NCC (see <a href="#">Table 1 on page 12</a> for the list of Security Firewalls):</p> <ul style="list-style-type: none"> <li>• <b>Native mode.</b> Click this button and select <b>Nebula Native mode</b> in the <b>Deployment Method</b>. Follow the instructions to connect the Security Firewall to NCC.</li> <li>• <b>Waiting ZTP</b> will be shown if <b>Native mode</b> is not available. Click the <b>Waiting ZTP</b> button and select <b>Zero Touch Provisioning</b> in <b>Deployment Method</b> to configure the ZTP settings.</li> </ul>
Unused / In use	<p>This shows <b>Unused</b> if the Nebula Device is not assigned to a site, or <b>In use</b> if the Nebula Device is currently in a site.</p>
Country	<p>This shows the country in which the Nebula Device is located.</p>
License expiration date	<p>This shows the date on which the Nebula Device's NCC license will expire.</p>
License info	<p>This shows the type of NCC license assigned to the Nebula Device.</p> <p>Note: Move the pointer over this field to see information about all licenses associated with this Nebula Device.</p>
Action	<p>Select one or more Nebula Devices and then click this button to perform one of the following actions:</p> <p><b>Change organization:</b> Moves the Nebula Device to an organization. The organizations must have the same owners.</p> <p><b>Change site assignment:</b> Moves the selected Nebula Devices to a selected site, or removes them from their current site while leaving them in the organization.</p> <p>Note: When you change the site for a Security Firewall (see <a href="#">Table 1 on page 12</a> for information on the supported Security Firewall devices), select the deployment method for management by Nebula (see <a href="#">Step 7: Set up the Deployment Method on page 50</a> for more information), configure the WAN settings and choose the installation method.</p> <p><b>Remove from organization:</b> Remove the Nebula Devices from NCC. You can manage the Nebula Devices in standalone mode, or re-add them to NCC later.</p> <p><b>Assign license:</b> Assign unassigned licenses to the selected Nebula Devices.</p> <p><b>Undo assign:</b> Unlink the inactive licenses from the associated Nebula Devices. After unlinking, the license will be categorized as unused in <b>Inventory</b>. An inactive license is a license that has been assigned to a Nebula Device but is not yet in use or queued.</p> <p><b>Transfer license:</b> 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.</p>

### 6.3.3.7 License & Inventory Licenses Screen

Use these screen to view and manage licenses in the organization. Click **Organization-wide > Configure > License & Inventory > Licenses** to access this screen.

**Figure 57** Organization-wide > Configure > License & Inventory > Licenses



The following table describes the labels in this screen.

**Table 42** Organization-wide > Configure > 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.

Table 42 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Licenses (continued)

LABEL	DESCRIPTION
Actions	<p>Select one or more Nebula Devices and then click this button to perform one of the following actions:</p> <p><b>Change organization:</b> Moves the selected licenses to an organization. The organizations must have the same owners.</p> <p><b>Assign License:</b> Assign the selected licenses to one or more Nebula Devices. Only the licenses applicable for the Nebula Device can be selected.</p> <p><b>Undo assign:</b> Unlink the inactive licenses from the associated Nebula Devices. After unlinking, the license will be categorized as unused in <b>Inventory</b>. An inactive license is a license that has been assigned to a Nebula Device but is not yet in use or queued.</p> <p><b>Transfer license:</b> 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.</p>
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 <a href="#">Section 6.3.3.4 on page 199</a> .
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	<p>This shows the current status of the license:</p> <ul style="list-style-type: none"> <li>• <b>Active:</b> The license is assigned to a specific Nebula Device and activated.</li> <li>• <b>Inactive:</b> The license is assigned to a specific Nebula Device but not activated.</li> <li>• <b>Expired:</b> The license is past its validity.</li> <li>• <b>Queued:</b> The license is assigned to a specific Nebula Device, and the license is waiting for the currently active license to expire.</li> <li>• <b>Unused:</b> The license is not assigned to a specific Nebula Device.</li> </ul>
License expiration date	<p>This shows the date on which the license will expire.</p> <p><b>Queued</b> means there are multiple licenses assigned to the Nebula Device, and the license is waiting for the currently active license to expire.</p>
Remaining days	This shows how days remain until the license expires.
Claim date	<p>This shows the date on which the license was added to NCC. If the Security Firewall has NOT yet connected to NCC:</p> <ul style="list-style-type: none"> <li>• <b>Native mode.</b> Click this button and select <b>Nebula Native mode</b> in <b>Deployment Method</b>. Follow the instructions to connect the Security Firewall to NCC.</li> <li>• <b>Waiting ZTP</b> will be shown if <b>Native mode</b> is not available. Click the <b>Waiting ZTP</b> button and select <b>Zero Touch Provisioning</b> in <b>Deployment Method</b> to configure the ZTP settings.</li> </ul>
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.

Table 42 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Licenses (continued)

LABEL	DESCRIPTION
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	<p>Click this button to perform the following actions:</p> <p><b>Change organization:</b> Moves the selected licenses to an organization. The organizations must have the same owners.</p> <p><b>Assign License:</b> Assign the selected licenses to one or more Nebula Devices. Only the licenses applicable for the Nebula Device can be selected.</p> <p><b>Undo assign:</b> Unlink the inactive licenses from the associated Nebula Devices. After unlinking, the license will be categorized as unused in <b>Inventory</b>. An inactive license is a license that has been assigned to a Nebula Device but is not yet in use or queued.</p> <p><b>Transfer license:</b> 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.</p>

### 6.3.3.8 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 43 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 <a href="#">Section 7.2.1 on page 277</a> 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.



Table 43 Trial Licenses Summary (continued)

TRIAL LICENSE	ASSOCIATED FEATURES OR NEBULA DEVICES
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 15](#) 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 > Configure > License & Inventory > Trial** to access this screen.

Figure 58 Organization-wide > Configure > License & Inventory > Trial

The following table describes the labels in this screen.

Table 44 Organization-wide > Configure > License & Inventory > Trial

LABEL	DESCRIPTION
Actions	<p>Click this to perform one of the following actions:</p> <ul style="list-style-type: none"> <li><b>Activate trial for all:</b> select this to start using all trial licenses available for your organization. Then click <b>Confirm</b> to continue.</li> <li><b>Deactivate trial for all:</b> select this to cancel all trial licenses currently in use in your organization. Then click <b>Confirm</b> to continue.</li> </ul> <p>Note: When you cancel any trial license, you cannot re-activate the unused portion of the trial license.</p>
(Status)	<p>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 <b>Activate</b> to start using the services of the trial license.</p> <p>Note: You can activate each type of 30-day trial license on each organization only once.</p>
IN PROGRESS	<p>The 30-day countdown for the trial license has begun. Click <b>Deactivate</b> if you want to cancel the trial license.</p> <p>Note: You can cancel the trial license anytime during the 30-day trial period, but you cannot re-activate it.</p>
TRIAL EXPIRED	You have previously activated a trial or standard license and the license period has ended.
CANCELED	You have deactivated the trial license during the 30-day trial period.
Activate	Click this to start using the 30-day trial license. Then click <b>Confirm</b> to continue.
Deactivate	Click this to cancel the 30-day trial license anytime before it expires. Then click <b>Confirm</b> to continue.

### 6.3.3.9 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 > Configure > License & Inventory > Change log** to access this screen.

Figure 59 Organization-wide > Configure > License & Inventory > Change log

Date and time	Action	Before	After	Admin
2022-10-12 07:15:25	Claimed device: 00000000000000000000000000000000		Added to Inventory	W Huang
2022-10-12 07:15:25	Moved device: 00000000000000000000000000000000	Inventory	added to Site: [AE_Test]	W Huang
2022-10-12 02:15:54	Removed device: 00000000000000000000000000000000	Inventory		W Huang
2022-10-12 02:15:53	Moved device: 00000000000000000000000000000000	Site: [2F_Office]	Inventory	W Huang

The following table describes the labels in this screen.

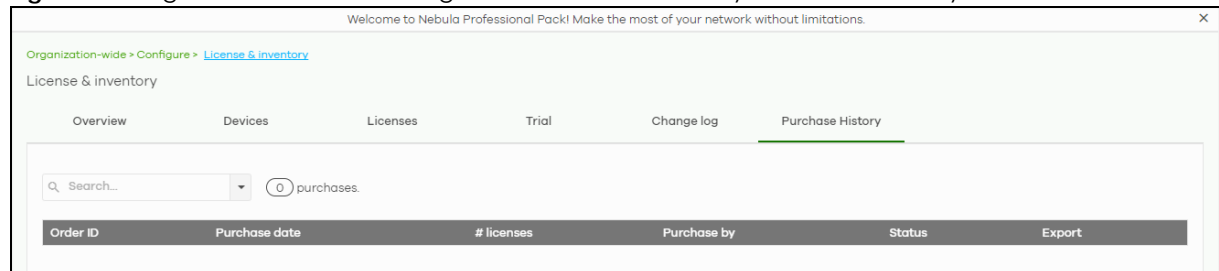
Table 45 Organization-wide > Configure > License & Inventory > Change Log

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 <b>Search</b> to filter log entries by date. <b>Range:</b> Display log entries from the first specified date to the second specified date. <b>Before:</b> 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.
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.

### 6.3.3.10 License & Inventory Purchase History Screen

Use this screen to view a record of Nebula Device license purchased within the organization. Click **Organization-wide > Configure > License & Inventory > Purchase History** to access this screen.

Figure 60 Organization-wide > Configure > License & Inventory > Purchase History



The following table describes the labels in this screen.

Table 46 Organization-wide > Configure > 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 <b>Marketplace &gt; Order History</b> screen.

Table 46 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Purchase History (continued)

LABEL	DESCRIPTION
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. <ul style="list-style-type: none"> <li><b>Done:</b> The order has been paid for and the license was successfully activated on the target Nebula Device.</li> <li><b>Processing:</b> The license activation on the target Nebula Device is still under process.</li> <li><b>Failed:</b> The license was not successfully activated on the target Nebula Device.</li> </ul>
Export	Click this to download the order details as a CSV or XML file to your computer. This includes the <b>Order ID</b> and each license's assigned device information.

### 6.3.4 Administrators

Use this screen to view, manage and create administrator accounts for the specified organization. Click **Organization-wide > Configure > Administrators** to access this screen.

Figure 61 Organization-wide &gt; Configure &gt; Administrators

The following table describes the labels in this screen.


Table 47 Organization-wide &gt; Configure &gt; Administrators

LABEL	DESCRIPTION
Activation	Click this button to <b>Activate/Deactivate</b> the selected accounts. Then click <b>Update</b> .
Force logout	Click this button to force the selected accounts to log out of the NCC.
Delete	Click this button to remove the selected accounts.
Search	Specify your desired filter criteria to filter the list of administrator accounts.
administrators	This shows the number of administrator accounts in the list.

Table 47 Organization-wide &gt; Configure &gt; Administrators (continued)

LABEL	DESCRIPTION
Change owner	<p>This button is only available if you are the organization owner.</p> <p>Click this button to transfer ownership of the organization to another user account. The new owner account must be an organization full administrator.</p> <div data-bbox="495 394 1175 758" style="border: 1px solid black; padding: 10px;"> <p><b>Change organization owner</b> <span style="float: right;">✕</span></p> <hr/> <p>Please select current organization admin to become new owner.</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;"> <span style="font-size: 0.8em;">Tom - Thomas.Hanning@cytel.com.br</span> <span style="float: right;">▼</span> </div> <p><input type="checkbox"/> This action will cause you lose ownership rights include Nebula devices under this organization. Do you want to continue?</p> <div style="text-align: right; margin-top: 10px;"> <span style="border: 1px solid #ccc; padding: 2px 10px;">No</span> <span style="border: 1px solid #ccc; padding: 2px 10px;">Yes</span> </div> </div> <p>After transferring ownership, NCC performs the following actions:</p> <ul style="list-style-type: none"> <li>Changes your account from organization owner to organization full administrator.</li> <li>Transfers all Nebula Devices and licenses in the organization to the new owner.</li> <li>Sends the new owner an email, notifying them of the change.</li> </ul>
Import	<p>Click this button to create administrator accounts in bulk by importing a complete list of all new administrators in an Excel file.</p> <div data-bbox="495 1003 1240 1352" style="border: 1px solid black; padding: 10px;"> <p><b>Bulk Import</b> <span style="float: right;">✕</span></p> <hr/> <p>"Bulk Import" supports for faster inputting. Please follow <a href="#">this template</a> to import</p> <div style="border: 1px dashed #ccc; padding: 10px; text-align: center; margin: 10px 0;"> <div style="background-color: #00a0e3; color: white; padding: 5px 15px; display: inline-block; margin-bottom: 5px;">Browse</div> <p>Or drag file here...</p> </div> <div style="text-align: right; margin-top: 10px;"> <span style="border: 1px solid #ccc; padding: 2px 10px;">Close</span> </div> </div>
Add	Click this button to create a new administrator account. See <a href="#">Section 6.3.4.1 on page 214</a> .
Name	This shows the name of the administrator account.
Email address	This shows the email address of the administrator account.
Merged privilege	<p>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:</p> <ul style="list-style-type: none"> <li><b>MSP &gt; Configure &gt; Admins &amp; teams &gt; Admins</b></li> <li><b>MSP &gt; Configure &gt; Admins &amp; teams &gt; Teams</b></li> <li><b>Group-wide &gt; Configure &gt; Administrators</b></li> <li><b>Organization-wide &gt; Configure &gt; Administrators</b></li> </ul> <p>For more information, see <a href="#">Section 4.6.0.1 on page 160</a>.</p>

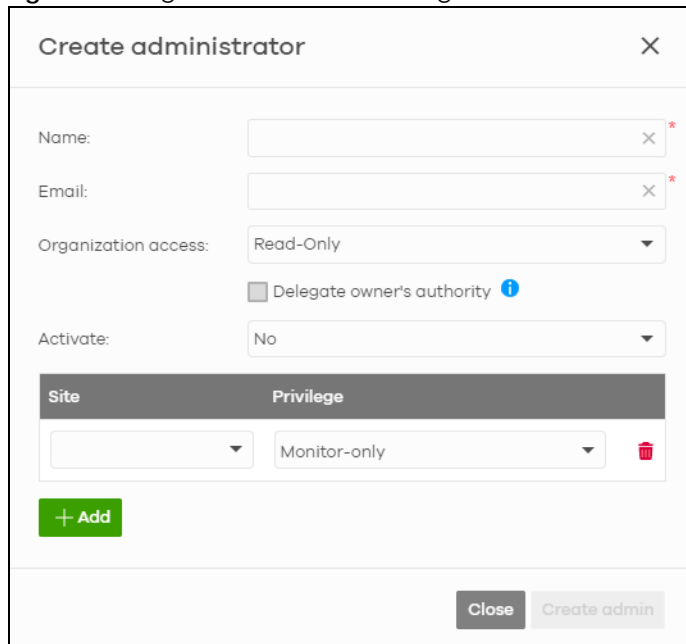
Table 47 Organization-wide &gt; Configure &gt; Administrators (continued)

LABEL	DESCRIPTION
Privilege	<p>This shows whether the administrator account has read-only, monitor-only, guest ambassador, or read and write (full) access to the organization and sites.</p> <p><b>Installer</b> indicates that the administrator account can register Nebula Devices at a site.</p> <p><b>Owner</b> 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.</p> <p><b>Organization (Delegated)</b> 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:</p> <ul style="list-style-type: none"> <li>• Delete organization</li> <li>• Transfer organization ownership</li> <li>• Assign delegate owner privileges to an administrator account.</li> </ul>
Account status	This shows whether the administrator account has been validated ( <b>OK</b> ). It shows <b>Deactivated</b> 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.

### 6.3.4.1 Create/Update Administrator

In the **Organization-wide > Configure > 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 62 Organization-wide &gt; Configure &gt; Administrator: Create/Update administrator



**Create administrator**
✕

---

Name:  ✕ \*

Email:  ✕ \*

Organization access: Read-Only ▼

Delegate owner's authority ⓘ

Activate: No ▼

Site	Privilege
▼	Monitor-only <span style="float: right;">✕</span>

+ Add

Close
Create admin

The following table describes the labels in this screen.

Table 48 Organization-wide > Configure > 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 ( <b>Full</b> ) 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 <b>Read-only</b> , 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 <b>None</b> , the administrator account can only be a site administrator.
Delegate owner's authority	This setting is only available when <b>Organization access</b> is set to <b>Full</b> .  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: <ul style="list-style-type: none"> <li>• Delete organization</li> <li>• Transfer organization ownership</li> <li>• Assign delegate owner privileges to an administrator account.</li> </ul>
Activate	Select <b>Yes</b> to enable the account or <b>No</b> to temporarily disable the account.
YES, I want to do it.	The check box displays only when an administrator that has full access to the organization selects <b>No</b> in the <b>Activate</b> field to disable his/her own account.  Note: After you select the check box and click <b>Update admin</b> , 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 <b>MSP Portal</b> screen.
Site	This field is available only when you set the account's organization access to <b>Read-only</b> or <b>None</b> .  Select the site to which you want to set the account's access. You can also select the site tag created using the <b>Organization-wide &gt; Monitor &gt; Overview: Sites</b> screen.
Privilege	This field is available only when you set the account's organization access to <b>Read-only</b> or <b>None</b> .  Set the administrator account's access to the site.  You can select from <b>Read-only</b> , <b>Monitor-only</b> , <b>Guest Ambassador</b> , <b>Installer</b> and <b>Full</b> (read and write).  An administrator account that has <b>Guest Ambassador</b> access can create, remove or manage guest accounts using the <b>Cloud Authentication</b> screen (see <a href="#">Section 6.3.5 on page 216</a> ).  <b>Installer</b> 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.

Table 48 Organization-wide &gt; Configure &gt; Administrator: Create/Update administrator (continued)

LABEL	DESCRIPTION
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.

## 6.3.5 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 > Configure > 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 7.2.7 on page 296](#)).

### 6.3.5.1 User Account Types

NCC has the following types of user accounts. For details on using these accounts for WiFi and network authentication, see [Section 12.3.2 on page 540](#).

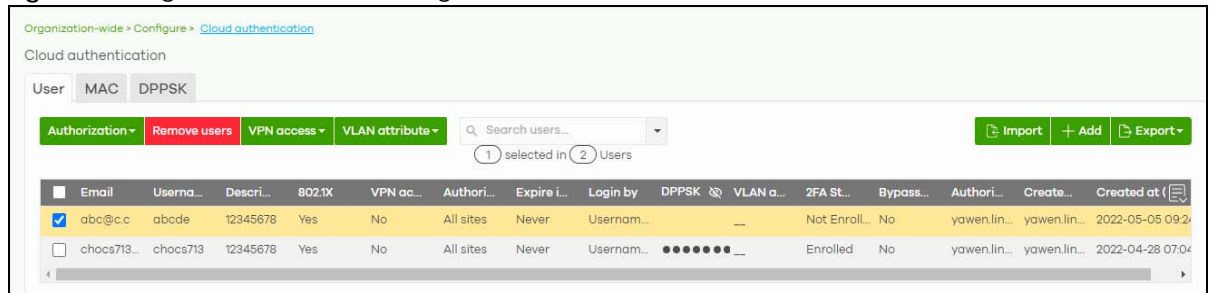
Table 49 Cloud Authentication: User Account Types

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.	<ul style="list-style-type: none"> <li>WiFi authentication (WPA-Enterprise)</li> <li>Network access through captive portal</li> <li>VPN Access</li> <li>WiFi authentication + network authentication through DPPSK</li> </ul>
MAC	The Nebula Device account that can gain access to the networks by authenticating using its MAC address.	<ul style="list-style-type: none"> <li>MAC-based Nebula Device authentication (combined with DPPSK)</li> </ul>
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.	<ul style="list-style-type: none"> <li>WiFi authentication + network authentication through DPPSK</li> </ul>

### 6.3.5.2 Cloud Authentication User Screen

Use this screen to view and manage regular NCC network user accounts. Click **Organization-wide > Configure > Cloud Authentication > User** to access this screen.

Figure 63 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; User



The screenshot shows the 'Cloud authentication' user management interface. It includes a breadcrumb trail 'Organization-wide > Configure > Cloud authentication', a sub-header 'Cloud authentication', and tabs for 'User', 'MAC', and 'DPPSK'. The 'User' tab is active. Below the tabs are action buttons: 'Authorization', 'Remove users', 'VPN access', and 'VLAN attribute'. A search bar 'Search users...' and a 'selected in 2 Users' indicator are present. On the right, there are 'Import', '+ Add', and 'Export' buttons. The main area contains a table with columns: Email, Username, Description, 802.1X, VPN access, Authorization, Expiration, Login by, DPPSK, VLAN access, 2FA Status, Bypass, Authorization, Create, and Created at. Two rows are visible: one for 'abc@c.c' and one for 'chocs713...'.

Email	Username	Description	802.1X	VPN access	Authori...	Expire i...	Login by	DPPSK	VLAN a...	2FA St...	Bypass...	Authori...	Create...	Created at
<input checked="" type="checkbox"/>	abc@c.c	abcde	12345678	Yes	No	All sites	Never	Usernam...	--	Not Enroll...	No	yawen.lin...	yawen.lin...	2022-05-05 09:2
<input type="checkbox"/>	chocs713...	chocs713	12345678	Yes	No	All sites	Never	Usernam...	.....	Enrolled	No	yawen.lin...	yawen.lin...	2022-04-28 07:04



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 50 Organization-wide > Configure > Cloud Authentication > User

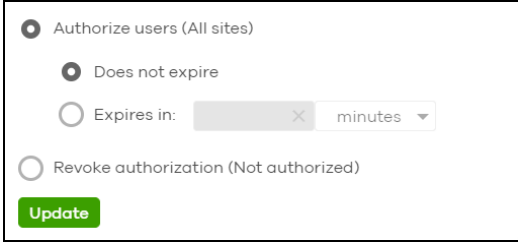
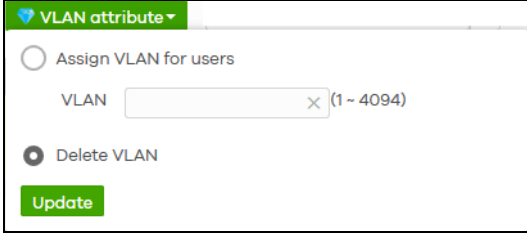

LABEL	DESCRIPTION
Authorization	<p>Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.</p> 
Remove users	<p>Select one or more than one user account and click this button to remove the selected user accounts.</p>
VPN access	<p>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.</p>
VLAN attribute	<p>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 <b>Update</b>.</p> 
Print	<p>Click this button to print information about each selected user account, such as their user name and password.</p>
Search users	<p>Enter a key word as the filter criteria to filter the list of user accounts.</p>
N User	<p>This shows how many user accounts (N) match the filter criteria and how many user accounts of the selected type are created in total.</p>
Import	<p>Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.</p> this template to import'. Below is a dashed box containing a 'Browse' button and the text 'Or drag file here...'. There is a 'Close' button at the bottom right." data-bbox="306 721 761 888"/>

Table 50 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; User (continued)

LABEL	DESCRIPTION
Add	Click this button to create a new user account. See <a href="#">Section 6.3.5.3 on page 218</a> .
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 ( <b>No</b> ). If the user is authorized, it shows <b>All sites</b> 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 <b>Never</b> if the account never expires.  This shows <b>Multiple value</b> if the account has different <b>Expire in</b> 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 <b>User</b> .  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 <b>Multiple value</b> .
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.

### 6.3.5.3 Create/Update User Account

In the **Site-wide** or **Organization-wide > Configure > 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 64** Organization-wide > Configure > Cloud Authentication > User: Create/Update user

**Create user** [X]

Account type: USER

Email: test@zyxel.com.tw [X] \*

Username: [X]

Description: [X]

Password: IAN6xmw1 [X] \* Generate

DPPSK: [X] Generate

802.1X:  Allow to use WPA-Enterprise to access network

VPN Access:  Allow to use Remote VPN access

Authorized: Not authorized [v]

Login by: Email [v]

VLAN assignment: Beta [X]

Two-Factor Auth.:  Bypass two-factor authentication.

Email to user:  Email account information to user.

[Close] [Print] Create user

The following table describes the labels in this screen.

Table 51 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; 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 <b>Login by</b> is set to <b>Email</b> .
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 <b>Generate</b> to have NCC create a password for the account automatically.
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 <b>Generate</b> 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.

Table 51 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; User: Create/Update user

LABEL	DESCRIPTION
Authorized	Set whether you want to authorize the user of this account.  You can select to authorize the user's access to <b>All Sites</b> or <b>Specified Sites</b> in the organization. If you select <b>Specified Sites</b> , 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 <b>Change</b> 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 <b>Expire in</b> values across different sites, it will show <b>Multiple value</b> and the <b>Change</b> link.  Otherwise, select <b>Never</b> 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.

### 6.3.5.4 Cloud Authentication MAC Screen

Use this screen to view and manage NCC Nebula Device user accounts, used for MAC-based authorization. Click **Organization-wide > Configure > Cloud Authentication > MAC** to access this screen.

Figure 65 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; MAC

The screenshot shows the 'Cloud authentication' interface with the 'MAC' tab selected. At the top, there are buttons for 'Authorization', 'Remove users', and 'Import', '+ Add', 'Export'. A search bar contains 'Search users...' and shows '1 selected in 4 Users'. Below is a table with the following data:

MAC address	Description	Account type	Authorized	Authorized by	Expire in (UTC)	Created at (UTC)
<input checked="" type="checkbox"/> 11:11:11:11:11:11	11	MAC	All sites	y@zyxel.com.tw	Never	2021-10-21 05:09:01
<input type="checkbox"/> 22:22:22:22:22:22	22	MAC	All sites	y@zyxel.com.tw	Never	2022-03-31 15:52:09
<input type="checkbox"/> 40:08:00:14:6FFF	IPHONE135	MAC	All sites	y@zyxel.com.tw	Never	2022-04-07 08:28:08
<input type="checkbox"/> 00:66:0A:87:03:75	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 52 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; MAC

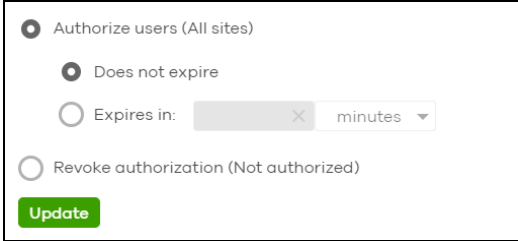
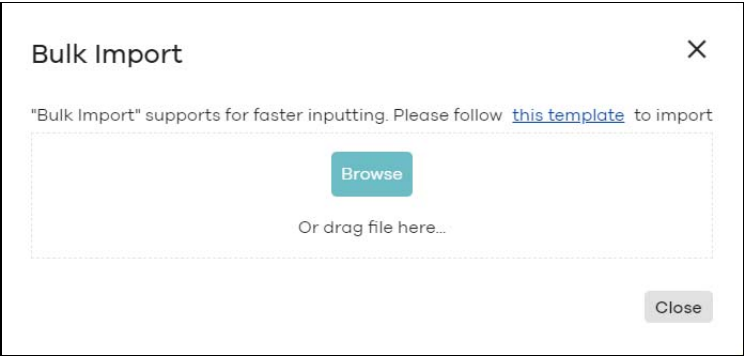

LABEL	DESCRIPTION
Authorization	<p>Select one or more than one account and click this button to configure the authorization settings for the selected user accounts.</p> 
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
Search users	Enter 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	<p>Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.</p> 
Add	Click this button to create a new user account. See <a href="#">Section 6.3.5.5 on page 222</a> .
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.
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 ( <b>No</b> ). If the user is authorized, it shows <b>All sites</b> or the name of the site to which the user is allowed access.
Authorized by	<p>This shows the email address of the administrator account that authorized the user.</p> <p>If the account has been authorized by different admins across different sites, it shows <b>Multiple value</b>.</p>

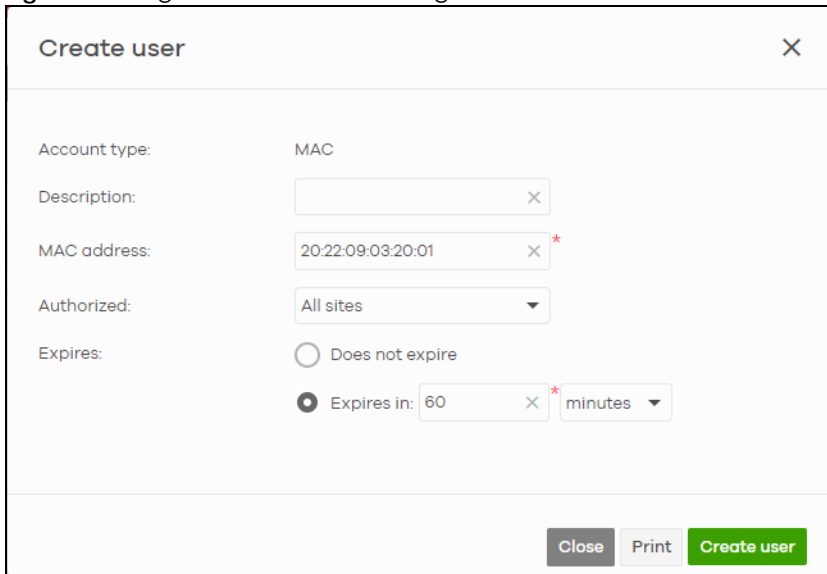
Table 52 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; MAC (continued)

LABEL	DESCRIPTION
Expire in (UTC)	This shows the date and time that the account expires. This shows -- if authentication is disabled for this account. This shows <b>Never</b> if the account never expires. This shows <b>Multiple value</b> if the account has different <b>Expire in</b> 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.

### 6.3.5.5 Create/Update MAC Account

In the **Site-wide** or **Organization-wide > Configure > 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 66 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; MAC: Create/Update user



The following table describes the labels in this screen.

Table 53 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; 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 <b>All Sites</b> or <b>Specified sites</b> to allow the user access to all or some sites in the organization. If you select <b>Specified sites</b> , a field displays allowing you to specify the sites to which the user access is authorized. Select <b>Not authorized</b> to prevent the user access to all the sites in the organization.
Expires	Specify the number of <b>minutes/hours/days/weeks</b> the user has access to site(s) in the organization.
Close	Click this button to exit this screen without saving.

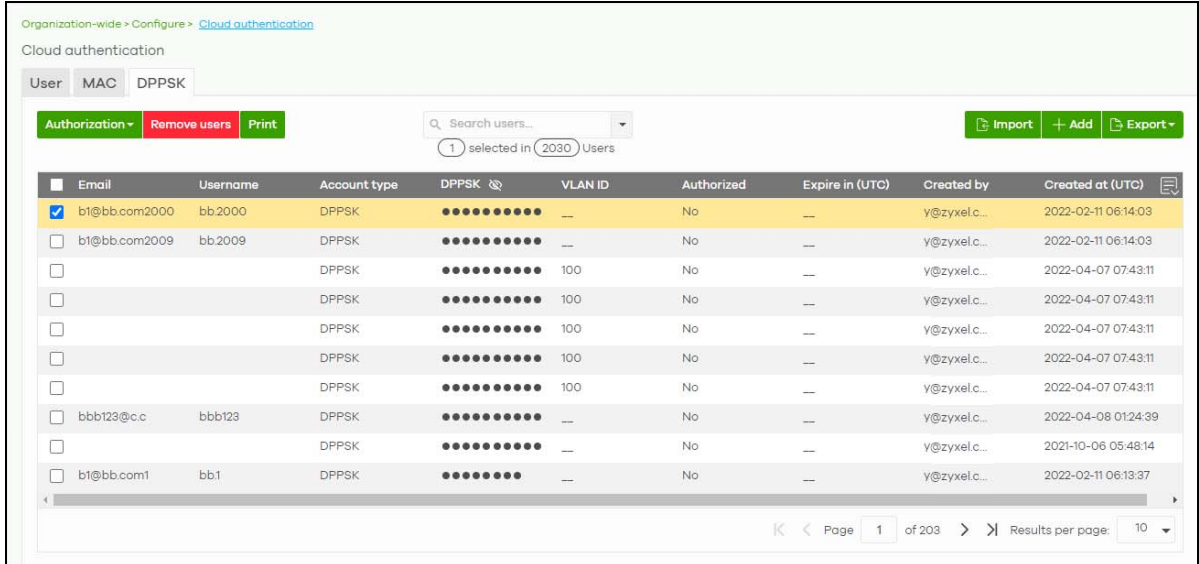
Table 53 Organization-wide > Configure > Cloud Authentication > MAC: Create/Update user

LABEL	DESCRIPTION
Print	Click this button to print the account information.
Create user	Click this button to save your changes and close the screen.

### 6.3.5.6 Cloud Authentication DPPSK Screen

Use this screen to view and manage DPPSK network user accounts. Click **Organization-wide > Configure > Cloud Authentication > DPPSK** to access this screen.

Figure 67 Organization-wide > Configure > Cloud Authentication > DPPSK



The following table describes the labels in this screen.

Table 54 Organization-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. <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <input checked="" type="radio"/> Authorize users (All sites)                         <ul style="list-style-type: none"> <li><input checked="" type="radio"/> Does not expire</li> <li><input type="radio"/> Expires in: <input type="text" value="x"/> minutes</li> <li><input type="radio"/> Revoke authorization (Not authorized)</li> </ul> <input type="button" value="Update"/> </div>
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.

Table 54 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; DPPSK (continued)



LABEL	DESCRIPTION
Print	<p>Click this button to print the unique dynamic personal pre-shared key (DPPSK) and expiry time of each selected user account.</p> <p>The account details can be cut into cards, and then given to users in order to grant them WiFi network access.</p> <div style="text-align: center; border: 1px solid black; padding: 10px;"> <p><b>DPPSK</b></p>  </div>
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	<p>Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><b>Bulk Import</b> <span style="float: right;">✕</span></p> <p>"Bulk Import" supports for faster inputting. Please follow <a href="#">this template</a> to import</p> <div style="border: 1px dashed gray; padding: 5px; text-align: center; margin: 5px 0;"> <p><span style="background-color: #00a651; color: white; padding: 5px 15px; border-radius: 3px;">Browse</span></p> <p>Or drag file here...</p> </div> <p style="text-align: right;"><span style="background-color: #ccc; padding: 2px 10px; border-radius: 3px;">Close</span></p> </div>
Add	<p>Click this button to create a single new account, or a batch of accounts.</p> <ul style="list-style-type: none"> <li>Single DPPSK: See <a href="#">Section 6.3.5.7 on page 225</a>.</li> <li>Batch create DPPSK: See <a href="#">Section 6.3.5.8 on page 226</a>.</li> </ul>
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 or not ( <b>No</b> ). If the user is authorized, it shows <b>All sites</b> or the name of the site to which the user is allowed access.
Expire in (UTC)	<p>This shows the date and time that the account expires.</p> <p>This shows -- if authentication is disabled for this account.</p> <p>This shows <b>Never</b> if the account never expires.</p> <p>This shows <b>Multiple value</b> if the account has different <b>Expire in</b> values across different sites.</p>
Created by	This shows the email address of the administrator account that created the user.



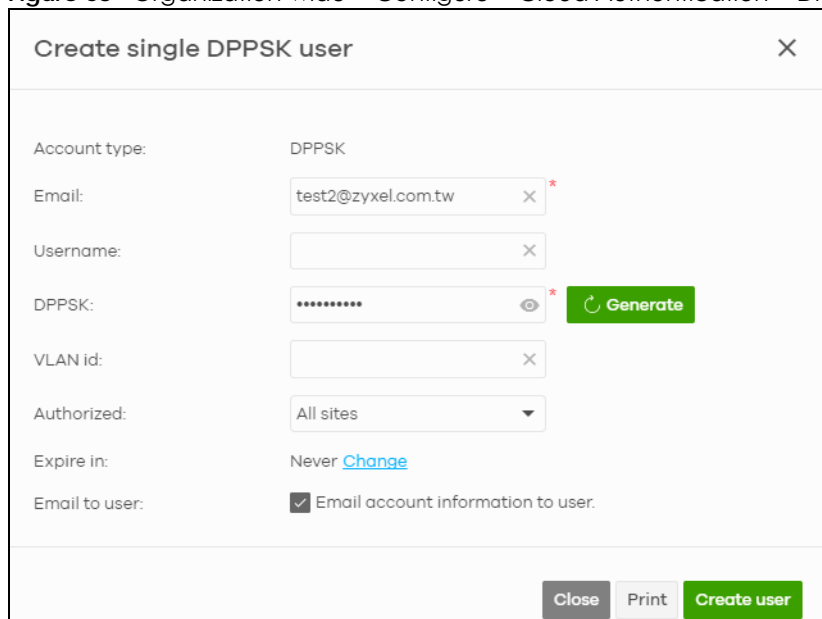
Table 54 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; DPPSK (continued)

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.

### 6.3.5.7 Add/Edit DPPSK Account

In the **Site-wide** or **Organization-wide > Configure > 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 68 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; DPPSK: Create/Update DPPSK user



**Create single DPPSK user** [X]

Account type: DPPSK

Email: test2@zyxel.com.tw [X]

Username: [X]

DPPSK: [Masked] [Generate]

VLAN id: [X]

Authorized: All sites [v]

Expire in: Never [Change](#)

Email to user:  Email account information to user.

[Close] [Print] [Create user]

The following table describes the labels in this screen.

Table 55 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; 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 <b>Generate</b> 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 <b>All Sites</b> or <b>Specified Sites</b> in the organization. If you select <b>Specified Sites</b> , a field displays allowing you to specify the sites to which the user access is authorized.

Table 55 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; DPPSK: Create/Update DPPSK user

LABEL	DESCRIPTION
Expire in	This field is available only when the user is authorized.  Click <b>Change</b> 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 <b>Expire in</b> values across different sites, it will show <b>Multiple value</b> and the <b>Change</b> link.  Otherwise, select <b>Never</b> 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.

### 6.3.5.8 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** > **Configure** > **Cloud Authentication** > **DPPSK** screen, click **Add**, and then select **Batch Create DPPSK**.

Figure 69 Organization-wide &gt; Configure &gt; Cloud Authentication: Batch Create DPPSK

The screenshot shows a dialog box titled "Batch create DPPSK user" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Account type: DPPSK
- Number of accounts: 20 (with a red asterisk and "(1-20)" next to the input field)
- VLAN id: (empty input field)
- E-mail account info to: (empty input field)
- Authorized: All sites (dropdown menu)
- Expire in: Never [Change](#) (link)

At the bottom right of the dialog, there are two buttons: "Close" (grey) and "Create user" (green).

The following table describes the labels in this screen.

Table 56 Organization-wide &gt; Configure &gt; 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).

Table 56 Organization-wide &gt; Configure &gt; Cloud Authentication: Batch Create DPPSK (continued)

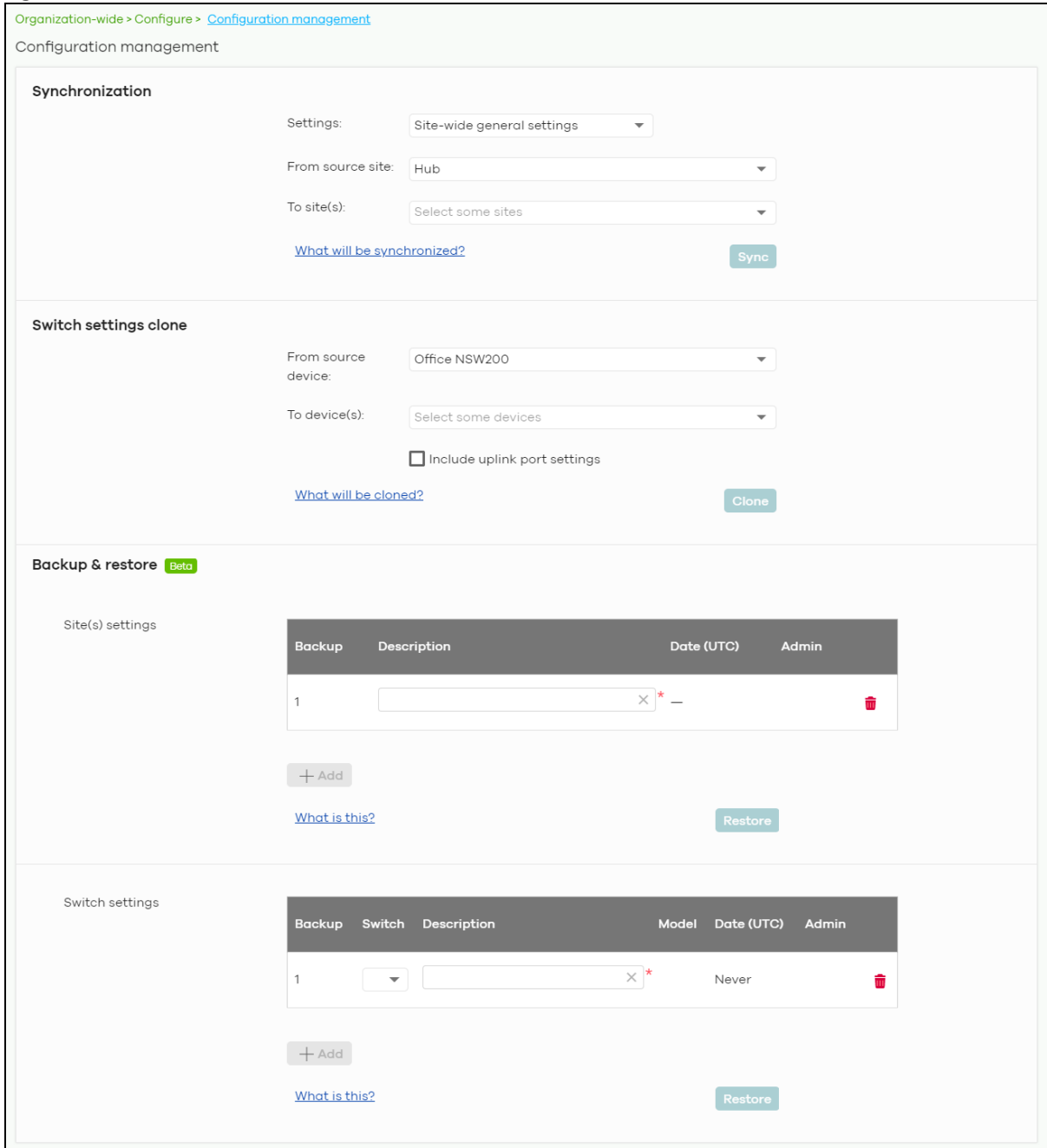
LABEL	DESCRIPTION
E-mail account info to	Send a copy of each user account's dynamic personal pre-shared key (DPPSK) and expiry date to the specified email address. This information is in a printable format.  The expiry date includes a time and date in UTC format.
Authorized	Set whether you want to authorize the user of this account.  You can select to authorize the user's access to <b>All Sites</b> or <b>Specified Sites</b> in the organization. If you select <b>Specified Sites</b> , 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 <b>Change</b> 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 <b>Expire in</b> values across different sites, it will show <b>Multiple value</b> and the <b>Change</b> link.  Otherwise, select <b>Never</b> 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.

### 6.3.6 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 > Configure > Configuration Management** to access this screen.

**Figure 70** Organization-wide > Configure > Configuration Management



The following table describes the labels in this screen.

**Table 57** Organization-wide > Configure > 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 <b>What will be synchronized?</b> 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 <b>Organization &gt; Monitor &gt; Overview: Sites</b> screen.

Table 57 Organization-wide &gt; Configure &gt; 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 <b>Add</b> 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 <b>Add</b> 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 57 Organization-wide &gt; Configure &gt; 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.

### 6.3.7 Configuration Template

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 6.3.7.3 on page 232](#)).

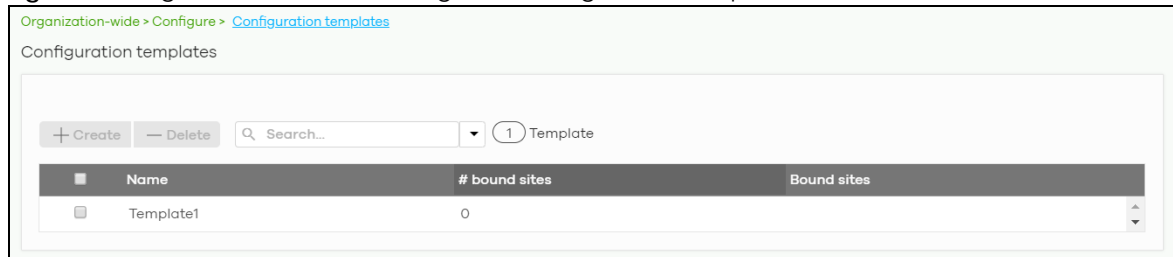
Use this screen to create and manage configuration templates. You can then bind or unbind a site from the template (see [Section 6.3.7.1 on page 231](#)).

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.

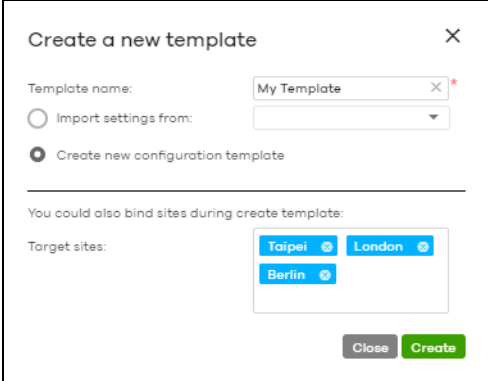
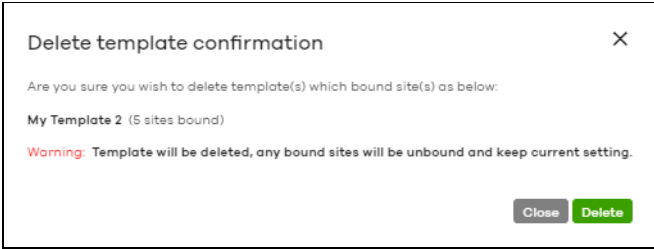
Click **Organization-wide > Configure > Configuration templates** to access this screen.

**Figure 71** Organization-wide > Configure > Configuration templates



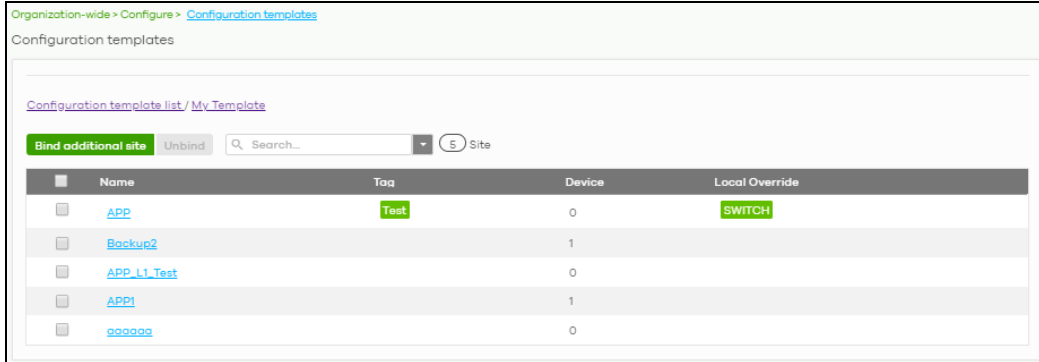
The following table describes the labels in this screen.

Table 58 Organization-wide > Configure > Configuration templates

LABEL	DESCRIPTION
Create	<p>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.</p> 
Delete	<p>Click this button to remove the selected templates. A window pops up asking you to confirm that you want to delete the templates.</p> <p>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.</p> 
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.


### 6.3.7.1 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 > Configure > Configuration Template** screen to access this screen. To go back to the previous screen, click the **Configuration template list** link.

**Figure 72** Organization-wide > Configure > Configuration Template: Template

The following table describes the labels in this screen.

**Table 59** Organization-wide > Configure > Configuration Template: 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 <b>Target sites</b> field and click <b>Bind</b> . 
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.

### 6.3.7.2 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, Switch, and access point settings.

### 6.3.7.3 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 **Switch**) 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.

### 6.3.7.4 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 11.3.1.1 on page 485](#) for details.) after the Switch is bound to a profile, turn on the local override function (see [Section 6.3.7.3 on page 232](#)).

## 6.3.8 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 **Firewall > Configure > Security Service**.

### 6.3.8.1 Configuring Security Profile Sync

Follow the steps below to enable security profile sync in an organization.

- 1 Go to **Organization-wide > Configure > 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 **Firewall > Configure > Security service** and select **Override security profile sync**.

### 6.3.8.2 Security Profile Sync Screen

Use this screen to enable and configure security profile sync. Click **Organization-Wide > Configure > Security profile sync** to access this screen.

Figure 73 Organization-wide > Configure > Security Profile Sync

Organization-wide > Configure > Security profile sync

Security profile sync

**Security profile sync**

Enabled

Sync sites

---

**Content filtering** [Model list](#)

Drop connection when there is an HTTPS connection with SSL v3(or previous version)

Denied Access Message

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

DNS Threat Filter Redirect IP

URL Threat Filter

URL Threat Filter policy

URL Threat Filter Denied Access Message

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

Allow list

URL Threat Filter external block list

Enabled	Name	External DB	Description
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

[+ 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  Test

Category list 0

Anonymous Proxies  
 Negative Reputation  
 Tor Proxies  
 BotNets

Denial of Service  
 Scanners  
 Web Attacks

Exploits  
 Spam Sources  
 Phishing

Block list  ×

Allow list  ×

External block list

Enabled	Name	External DB	Description
<input type="checkbox"/>	<input type="text" value=""/> <span>×</span>	<input type="text" value=""/> <span>×</span>	<input type="text" value=""/> <span>×</span>

+ Add

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

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 60 Organization-wide &gt; Configure &gt; 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 <b>All sites</b> 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 <b>On</b> 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 <a href="#">Section 9.3.8.1 on page 378</a> 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 <a href="#">Section 9.3.8.2 on page 381</a> 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 <b>On</b> to turn on the rule. Otherwise, select <b>Off</b> to turn off the rule.
DNS Threat Filter policy	Select <b>Pass</b> 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 <b>Redirect</b> to have the Nebula Device reply with a DNS reply packet containing a default or custom-defined IP address.

Table 60 Organization-wide &gt; Configure &gt; 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 <b>On</b> to turn on the rule. Otherwise, select <b>Off</b> to turn off the rule.
URL Threat Filter Policy	<p>Select <b>Pass</b> to allow users to access web pages that the external web filtering service has not categorized.</p> <p>Select <b>Block</b> 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.</p> <p>Select <b>Warn</b> to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.</p>
URL Threat Filter Denied Access Message	<p>Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0–9a–zA–Z;/?:@&amp;=+\$\._!~*()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator".</p> <p>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.</p>
URL Threat Filter Redirect URL	<p>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.</p> <p>Use "http://" or "https://" followed by up to 262 characters (0–9a–zA–Z;/?:@&amp;=+\$\._!~*()%,"). For example, http://192.168.1.17/blocked access.</p>
Test Threat Category	Enter a URL using http://domain or https://domain and click the <b>Test</b> 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	<p>Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0–9 a–z). The casing does not matter.</p>
Allow list	<p>Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0–9 a–z). The casing does not matter.</p>
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 60 Organization-wide &gt; Configure &gt; 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 <b>Daily</b> to set the time of the day, or <b>Weekly</b> 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 <b>Pass</b> to have the Nebula Device allow the packet to go through.  Select <b>Block</b> 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 ( <b>High, Medium and above, Low and above</b> ).  The threat level is determined by the IP reputation engine. It grades IPv4 addresses. <ul style="list-style-type: none"> <li>• <b>High</b>: an IPv4 address that scores 0 to 20 points.</li> <li>• <b>Medium and above</b>: an IPv4 address that scores 0 to 60 points.</li> <li>• <b>Low and above</b>: an IPv4 address that scores 0 to 80 points.</li> </ul> For example, a score of "10" will cause the Nebula Device to take action whether you set the <b>Threat level threshold</b> at <b>High, Medium and above</b> , or <b>Low and above</b> .  But a score of "61" will not cause the Nebula Device to take any action if you set the <b>Threat level threshold</b> at <b>Medium and above</b> .
Test Category	Enter an IPv4 address of a website, and click the <b>Test</b> 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 60 Organization-wide &gt; Configure &gt; 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-ubl.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 <b>Daily</b> to set the time of the day, or <b>Weekly</b> 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 <b>On</b> to turn on the rule. Otherwise, select <b>Off</b> 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 patterns. 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 <b>Express Mode</b> and <b>Stream Mode</b> 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 60 Organization-wide &gt; Configure &gt; Security Profile Sync (continued)

LABEL	DESCRIPTION
Block list	<p>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.</p> <ul style="list-style-type: none"> <li>• Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• The whole file name has to match if you do not use a question mark or asterisk.</li> <li>• If you do not use a wildcard, the Nebula Device checks up to the first 80 characters of a file name.</li> </ul>
Allow list	<p>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.</p> <ul style="list-style-type: none"> <li>• Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• The whole file name has to match if you do not use a question mark or asterisk.</li> <li>• If you do not use a wildcard, the Nebula Device checks up to the first 80 characters of a file name.</li> </ul>
Sandboxing	<p>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.</p>
Enabled	<p>Select this option to turn on sandboxing on the Nebula Device</p>
Log	<p>Enable this option to allow the Security Firewall to create a log when a suspicious file is detected.</p>
Policy	<p>Specify whether the Nebula Device deletes (<b>Destroy</b>) or forwards (<b>Allow</b>) malicious files. Malicious files are files given a high score for malware characteristics by the Defend Center.</p>



Table 60 Organization-wide &gt; Configure &gt; 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 <b>On</b> to enable Detection.
Prevention	Select <b>On</b> to enable Prevention.

### 6.3.9 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.

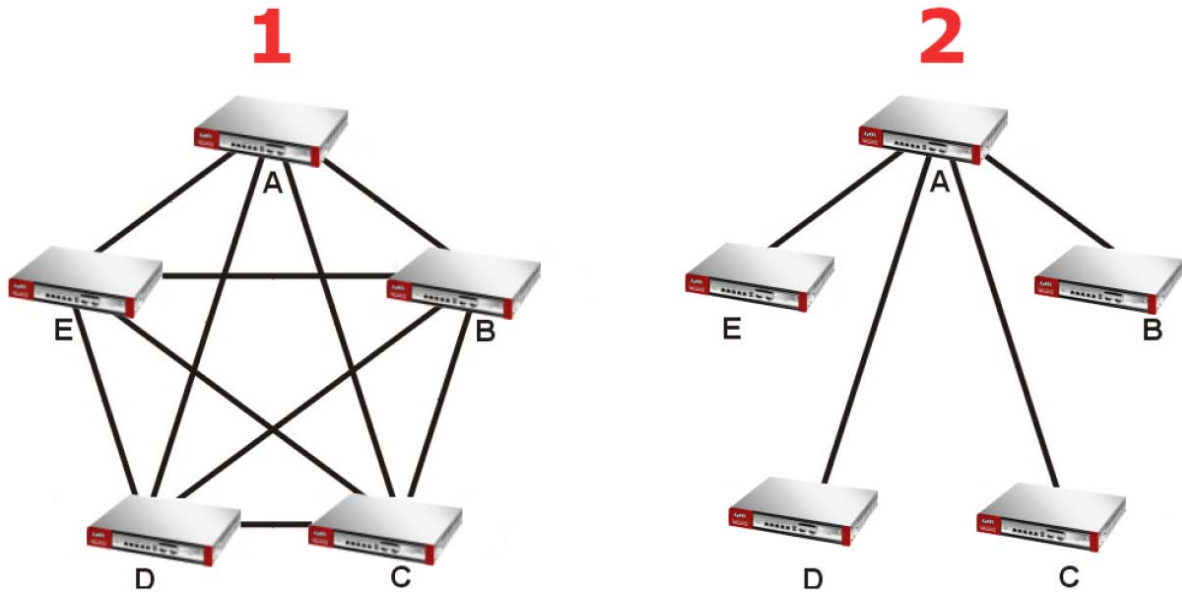
Note: You can manually create VPN connections between sites at **Gateway > Configure > Site-to-Site VPN** or **Firewall > Configure > Site-to-Site VPN**.

#### 6.3.9.1 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 74 VPN Topologies (Fully Meshed and Hub-and-Spoke)



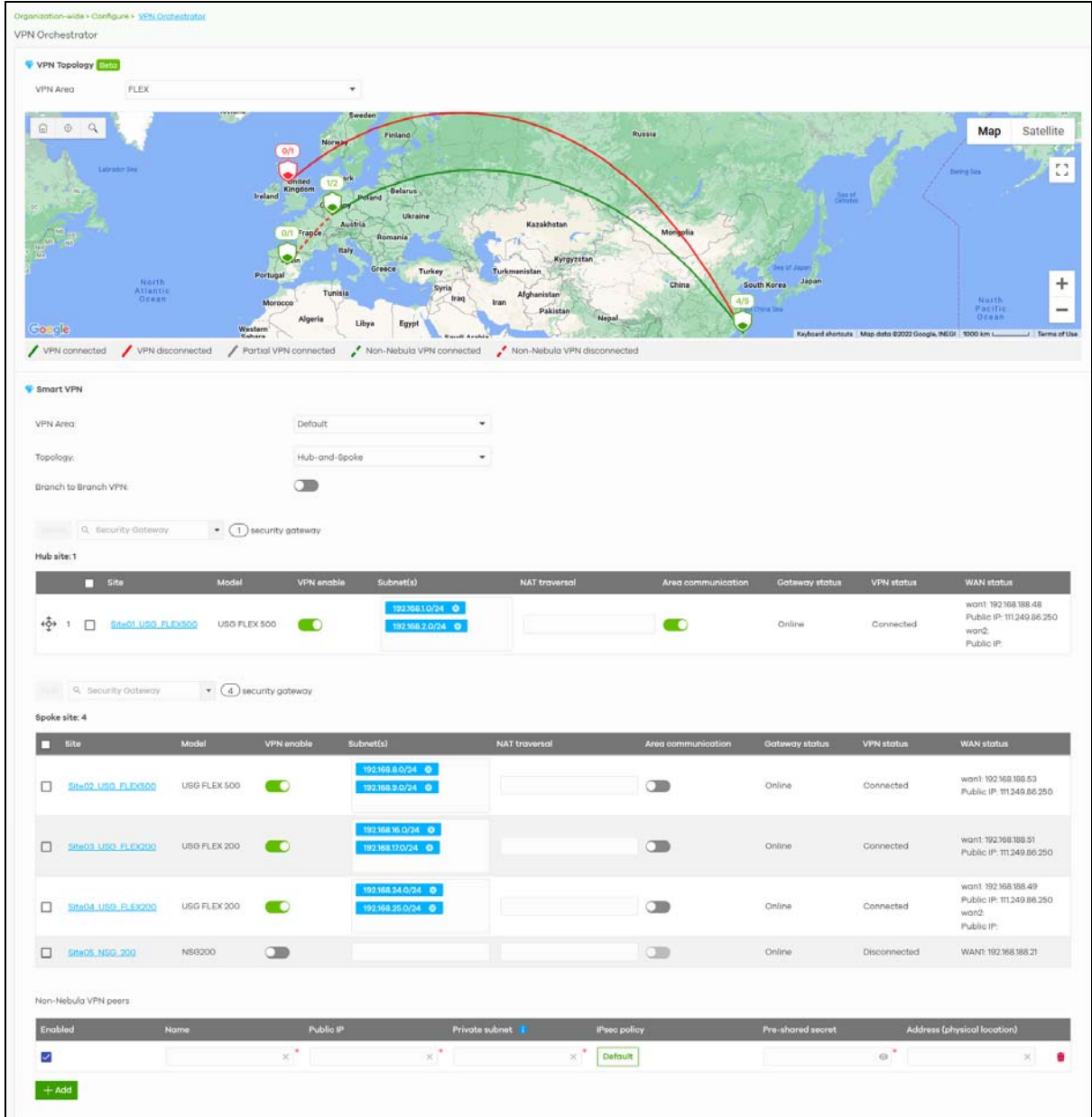
### 6.3.9.2 VPN Areas

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.

### 6.3.9.3 VPN Orchestrator Screen

Use this screen to manage and create site-to-site VPNs within the current organization. Click **Organization-Wide > Configure > VPN Orchestrator** to access this screen.

Figure 75 Organization-wide > Configure > VPN Orchestrator



The following table describes the labels in this screen.

Table 61 Organization-Wide > Configure > VPN Orchestrator


LABEL	DESCRIPTION
VPN Topology	
VPN Area	Select the name of a VPN area to view on the map. Select <b>Overview</b> to view all VPN areas in this organization on the map.
Smart VPN	
VPN Area	Select the name of a VPN to configure. Select <b>+ Create VPN area</b> to create a new VPN within the organization.
	Click the remove icon to delete the VPN area.

Table 61 Organization-Wide &gt; Configure &gt; VPN Orchestrator (continued)



LABEL	DESCRIPTION
Topology	Click this to select a topology for the VPN area. For details on topologies, see <a href="#">Section 6.3.9.1 on page 241</a> .  Select <b>Disable</b> to disable VPN connections for all sites in the VPN area.
The following settings are shown when <b>Topology</b> is set to <b>Hub-and-Spoke</b> .	
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 <b>Topology</b> is set to <b>Site-to-Site</b> , then you must assign at least one site in each VPN area as the <b>Area Leader</b> . 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 <a href="#">Section 10.3.6.1 on page 439</a> for detailed information.

Table 61 Organization-Wide &gt; Configure &gt; 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.

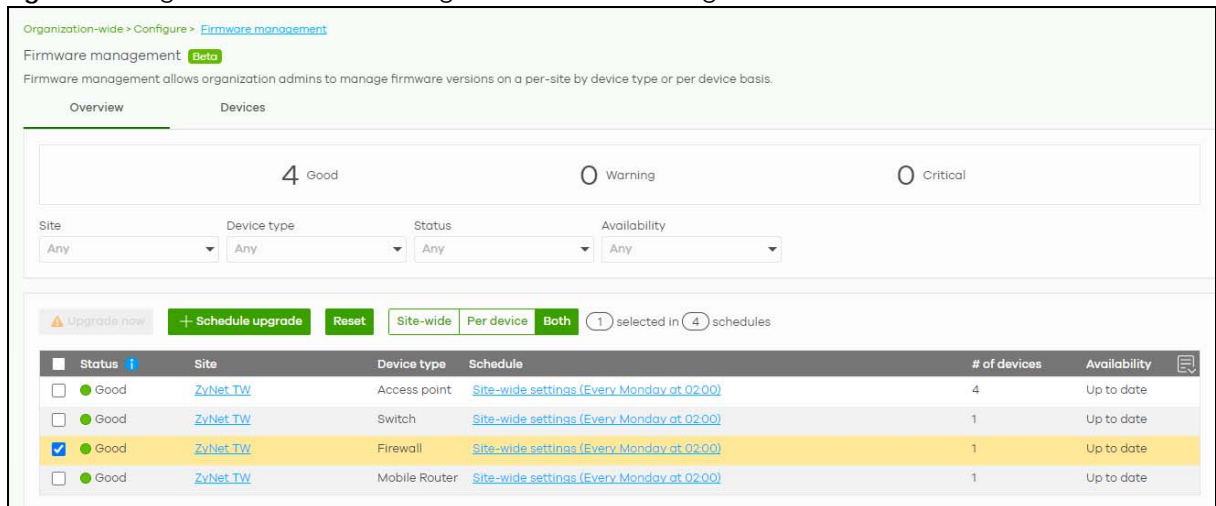
## 6.3.10 Firmware Management

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 > Configure > Firmware management** to access this screen.

### 6.3.10.1 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 > Configure > Firmware management > Overview** to access this screen.

Figure 76 Organization-Wide &gt; Configure &gt; Firmware management &gt; Overview



The screenshot displays the 'Firmware management' overview screen. At the top, it shows the breadcrumb 'Organization-wide > Configure > Firmware management' and a 'Beta' label. Below this, a summary bar indicates '4 Good', '0 Warning', and '0 Critical' devices. There are four filter dropdowns: Site (Any), Device type (Any), Status (Any), and Availability (Any). Below the filters, there are buttons for 'Upgrade now', '+ Schedule upgrade', and 'Reset'. A summary bar shows '1 selected in 4 schedules' with tabs for 'Site-wide', 'Per device', and 'Both'. A table lists devices with columns for Status, Site, Device type, Schedule, # of devices, and Availability.

Status	Site	Device type	Schedule	# of devices	Availability
<input type="checkbox"/> Good	ZyNet TW	Access point	Site-wide settings (Every Monday at 02:00)	4	Up to date
<input type="checkbox"/> Good	ZyNet TW	Switch	Site-wide settings (Every Monday at 02:00)	1	Up to date
<input checked="" type="checkbox"/> Good	ZyNet TW	Firewall	Site-wide settings (Every Monday at 02:00)	1	Up to date
<input type="checkbox"/> 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 > Configure > 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.

### 6.3.10.2 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 > Configure > 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).

### 6.3.10.3 Firmware Management Overview Screen

The following table describes the labels in this screen.


Table 62 Organization-Wide > Configure > Firmware management > Overview

LABEL	DESCRIPTION
Site	Select a site in your organization. By default, all the sites are displayed <b>(Any)</b> .
Device type	Select the type of Nebula Device. By default, all the Nebula Devices are displayed <b>(Any)</b> .
Status	<p>Select the status of the Nebula Device's firmware. By default, all the status are displayed <b>(Any)</b>.</p> <p>Select <b>Good</b> to display the Nebula Devices running a stable firmware with no immediate action is required.</p> <p>Select <b>Warning</b> 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.</p> <p>Select <b>Critical</b> 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.</p> <p>Select <b>N/A</b> to display the Nebula Devices that are offline and its firmware status is not available.</p>
Availability	Select to show the Nebula Devices with <b>Up to date</b> firmware, there is firmware update available for the Nebula Device ( <b>Upgrade available</b> ), or a specific version of firmware has been installed by Zyxel customer support ( <b>Locked</b> ). By default, all the available firmware are displayed <b>(Any)</b> .
Upgrade Now	<p>Click this to immediately upgrade the firmware on all selected sites.</p> <p>This button is selectable only when there is firmware update available for the Nebula Devices for the selected sites.</p>

Table 62 Organization-Wide &gt; Configure &gt; Firmware management &gt; Overview (continued)

LABEL	DESCRIPTION
Schedule Upgrade	<p>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.</p> <div data-bbox="534 348 1291 951" style="border: 1px solid black; padding: 10px;"> <p style="text-align: right;"><b>Schedule upgrade</b> <span style="float: right;">✕</span></p> <p style="background-color: #fff9c4; padding: 5px; border: 1px solid #ccc;">Note: Schedule upgrade will follow each site's time zone.</p> <p>Upgrade policy</p> <p><input checked="" type="radio"/> Auto upgrade at <span style="margin-left: 10px;">Monday ▼</span> <span style="margin-left: 10px;">02:00 ▼</span></p> <p><input type="radio"/> Upgrade at <span style="margin-left: 10px;">2023-01-04  12:00 ▼</span></p> <p><input type="radio"/> Upgrade now</p> <p><input type="radio"/> Ignore upgrade</p> <p>Firmware type <span style="margin-left: 10px;">Stable ▼</span></p> <p style="text-align: right;"><span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;">Cancel</span> <span style="background-color: #4caf50; color: white; padding: 2px 10px;">Update</span></p> </div> <p>Note: Nebula Devices are upgraded according to the time zone of the site they are in.</p>
Reset	<p>Select one or more <b>Site-wide</b> firmware upgrade <b>Schedules</b>, and then click <b>Reset</b> to restore the default site-wide settings (<b>Every Monday at 02:00</b>).</p> <p>Select one or more <b>Per device</b> firmware upgrade <b>Schedules</b>, and then click <b>Reset</b> to allow the Nebula Devices to follow the site-wide firmware management settings.</p>
Site-wide/Per device	Select your desired filter criteria to filter the list of firmware upgrade schedules.
<p>Note: Drag the following column headings to change the order. Click the column heading to change the sorting, ascending or descending order.</p>	
Status	<p>This shows the status of the Nebula Device's firmware.</p> <ul style="list-style-type: none"> <li>Green: All Nebula Devices are running <b>Stable</b> or above firmware.</li> <li>Amber: One or more Nebula Devices is not running the <b>Latest</b> firmware.</li> <li>Red: One or more Nebula Devices is running firmware that may have security vulnerabilities and/or lack key performance improvements.</li> <li>Gray: No schedule is set for upgrading the Nebula Device's firmware.</li> </ul>
Site	<p>This shows which site the Nebula Device is in.</p> <p>Click the site name to go to the site's Dashboard.</p>
Device type	This shows the type of Nebula Device.
Schedule	<p>This shows the day and time when a new firmware upgrade is scheduled to occur. <b>Site-wide settings</b> means the Nebula Device is following the site-wide firmware schedule. <b>Per device settings</b> means a firmware schedule is set for the Nebula Device and it will not follow the site-wide firmware schedule.</p>
# of devices	<p>This shows the number of Nebula Devices in the site for a particular <b>Schedule status</b>. Click this to change the schedule (see the <b>Schedule upgrade</b> field in <a href="#">Table 63 on page 248</a> for more information).</p>

Table 62 Organization-Wide > Configure > Firmware management > Overview (continued)

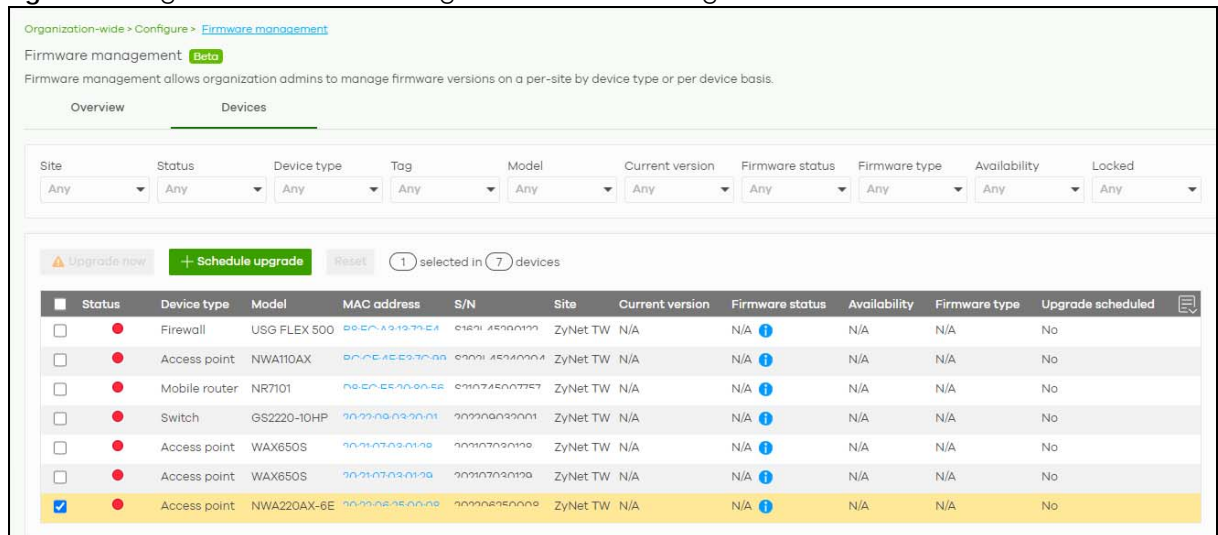
LABEL	DESCRIPTION
Availability	This shows whether the firmware on the Nebula Device is <b>Up to date</b> , there is firmware update available for the Nebula Device ( <b>Upgrade available</b> ), or a specific version of firmware has been installed by Zyxel customer support ( <b>Locked</b> ).
	Click this icon to show and hide columns in the table.

### 6.3.10.4 Firmware Management Devices Screen

Use this screen to make different firmware upgrade schedules for the Nebula Devices in the organization. Click **Organization-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 77 Organization-Wide > Configure > Firmware management > Devices



The following table describes the labels in this screen.

Table 63 Organization-Wide > Configure > 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 63 Organization-Wide > Configure > Firmware management > Devices (continued)

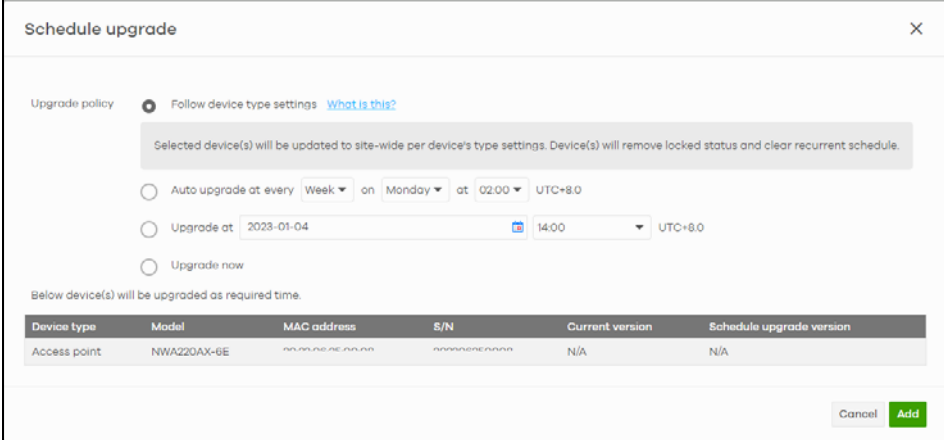

LABEL	DESCRIPTION
Schedule upgrade	<p>Click this to pop up a window where you can create a new schedule for the selected Nebula Devices.</p> <p>You can select to upgrade firmware according to the organization-wide schedule configured for the Nebula Device type in the site, create a recurring schedule, 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.</p> <p>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.</p> 
Reset	<p>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.</p>
Status	<p>This shows the status of the Nebula Device.</p> <ul style="list-style-type: none"> <li>Green: The Nebula Device is online and has no alerts.</li> <li>Amber: The Nebula Device has alerts.</li> <li>Red: The Nebula Device is offline.</li> <li>Gray: The Nebula Device has been offline for 7 days or more.</li> </ul>
Device type	<p>This shows the type of the Nebula Device.</p>
Model	<p>This shows the model number of the Nebula Device.</p>
Tag	<p>This shows the tag created and added to the Nebula Device.</p>
Name	<p>This shows the descriptive name of the Nebula Device.</p>
MAC address	<p>This shows the MAC address of the Nebula Device.</p>
S/N	<p>This shows the serial number of the Nebula Device.</p>
Site	<p>This shows the descriptive name of the site.</p>
Current version	<p>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.</p>

Table 63 Organization-Wide &gt; Configure &gt; Firmware management &gt; Devices (continued)

LABEL	DESCRIPTION
Firmware status	<p>The status shows <b>Good</b> 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 <b>Firmware type</b>.</p> <p>The status shows <b>Warning</b> if a newer firmware is available and immediate action is recommended. The newer firmware may contain security enhancements, new features, and performance improvements.</p> <p>The status shows <b>Critical</b> if a newer firmware is available and immediate action is required. The firmware may have security vulnerabilities and/or lack key performance improvements.</p> <p>The status shows <b>Custom</b> if the Nebula Device is running a firmware with specialized features that is not available to the general public.</p> <p>The status changes to <b>Upgrading...</b> after you click <b>Upgrade Now</b> to install the firmware immediately.</p>
Firmware type	<p>This shows <b>Stable</b> when the installed firmware may not have the latest features but has passed Zyxel internal and external testing.</p> <p>This shows <b>Latest</b> when the installed firmware is the most recent release with the latest features, improvements, and bug fixes.</p> <p>This shows <b>General Availability</b> when the installed firmware is a release before <b>Latest</b>, but is still undergoing Zyxel external testing.</p> <p>This shows <b>Dedicated</b> 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.</p> <p>This shows <b>Beta</b> when the installed firmware is a release version for testing the latest features and is still undergoing Zyxel internal and external testing.</p> <p>This shows <b>N/A</b> when the Nebula Device is offline and its firmware status is not available.</p> <p>Note: See <a href="#">Table 64 on page 251</a> for an example <b>Firmware type</b> version progression example scenario.</p>
Availability	<p>This shows whether the firmware on the Nebula Device is <b>Up to date</b>, there is firmware update available for the Nebula Device (<b>Upgrade available</b>), or a specific version of firmware has been installed by Zyxel customer support (<b>Locked</b>).</p>
Upgrade scheduled	<p>This shows the date and time when a new firmware upgrade is scheduled to occur. Otherwise, it shows <b>Follow upgrade time</b> and the Nebula Device sticks to the site-wide schedule or <b>No</b> when the firmware on the Nebula Device is up-to-date or the Nebula Device goes offline and its firmware status is not available.</p> <p>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.</p>
Last upgrade time	<p>This shows the last date and time the firmware was upgraded on the Nebula Device.</p>
Schedule upgrade version	<p>This shows the version number of the firmware which is scheduled to be installed.</p>
	<p>Click this icon to display a greater or lesser number of configuration fields.</p>

## Firmware Type / Version Progression

The following table shows an example firmware version progression scenario.

Table 64 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.

# CHAPTER 7

## Site-wide

### 7.1 Monitor

Use the **Monitor** menus to check the dashboard, summary report, map and floor plan, network topology and client list of the Nebula Devices for the selected site.

#### 7.1.1 Dashboard

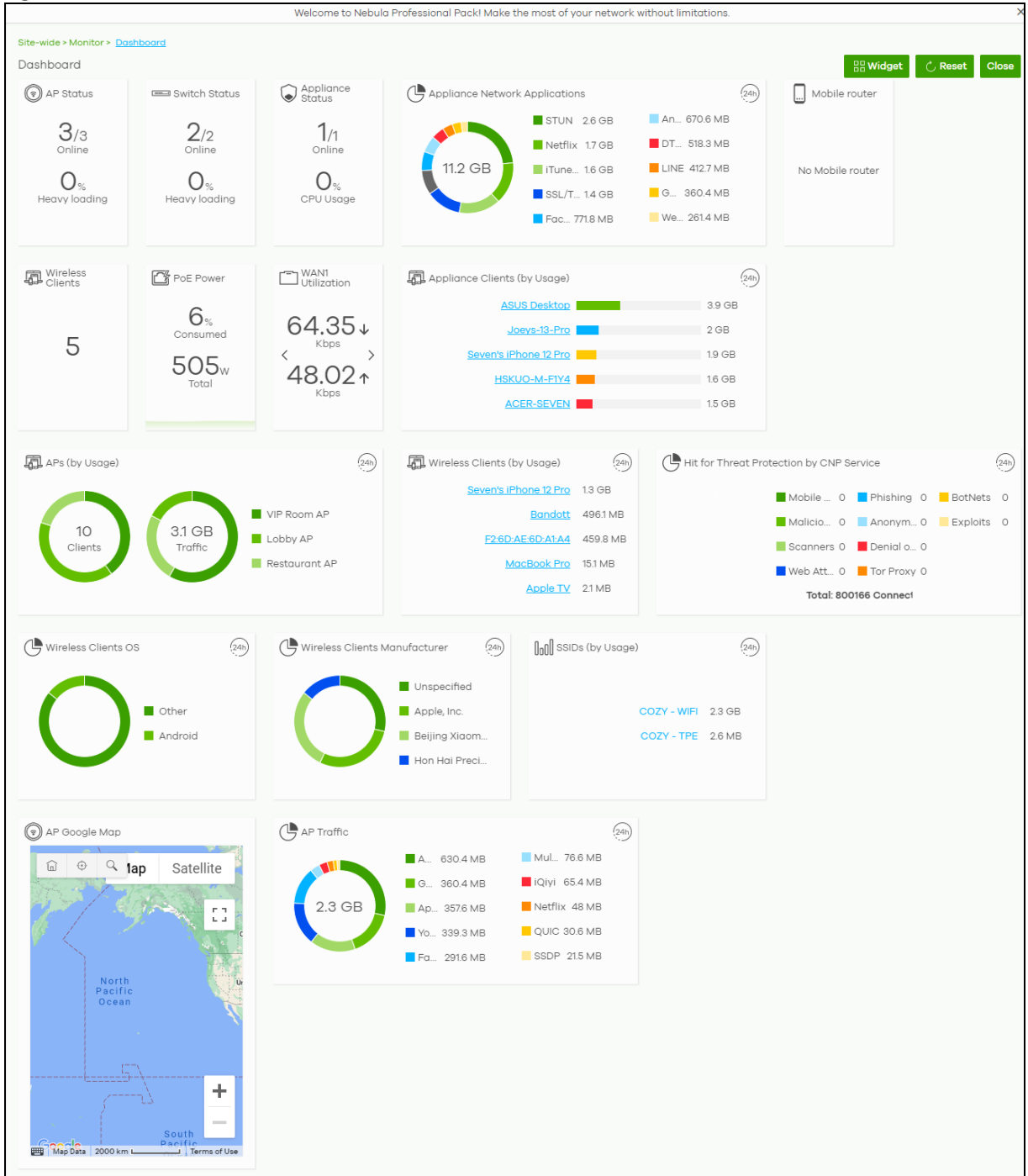
If a site is created and selected, the **Dashboard** is always the first menu you see when you log into the NCC. You can also click **Site-wide > Monitor > Dashboard** to access this screen.

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 **Switch > 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 78 Site-Wide > Monitor > Dashboard



The following table describes the labels in this screen.

Table 65 Site-Wide &gt; Monitor &gt; Dashboard

LABEL	DESCRIPTION
AP 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 <b>Access Point &gt; Configure &gt; Traffic shaping</b> ) 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.
PoE Power	This shows the total PoE power budget on the Switch and the current amount of power consumed by the powered devices.
Appliance 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.
Appliance Network Applications	This shows the top ten applications used by the Nebula Security Appliance in the past 24 hours.
Appliance 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 <b>Access Point &gt; Monitor &gt; Summary report</b> 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 <b>Access Point &gt; Monitor &gt; Clients: Client list</b> screen.
Wireless Clients Manufacturer	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 <b>Access Point &gt; Monitor &gt; Clients</b> screen and view the client devices which are made by the manufacturer.
Hit for Collaborative Detect & Response	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 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 <b>Access Point &gt; Monitor &gt; Clients</b> 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 <b>Access Point &gt; Monitor &gt; Access Points: AP Details</b> screen.
AP Traffic	This shows the usage statistic of the top ten applications used in the site in the past 24 hours.

Table 65 Site-Wide &gt; Monitor &gt; Dashboard (continued)

LABEL	DESCRIPTION
AP Google Map	This shows the locations of access points on the Google map.
Hit for Threat Protection by CNP Service	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.

## 7.1.2 Clients

This screen shows a list of all wired and WiFi clients connected to Nebula Devices (access points, Switches, Security Appliances, Security Firewalls, mobile routers) in the site. You can also block or allow clients. Click **Site-Wide > Monitor > Clients** to access this screen.

Figure 79 Site-Wide &gt; Monitor &gt; Clients &gt; Client list


Status	Description	Connected to	MAC address	IPv4 address	First seen	Last seen	Manufacturer	Policy	Note
<input type="checkbox"/>	MRG2-NSBU	Shawn_NSW100...	00:18:0A:2F:0A:C0		2023-01-10 11:09...	2023-01-10 13:04...	Cisco Meraki	Normal	
<input type="checkbox"/>	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	
<input type="checkbox"/>	22:10:A8:0B:86:C8	BC:CF:4F:56:BD:6D	22:10:A8:0B:86:C8		2023-01-10 11:59:05	2023-01-10 13:05:10	Unspecified	Normal	
<input type="checkbox"/>	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	
<input type="checkbox"/>	TWNNT03196-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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	TWNNT03245-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	

The following table describes the labels in this screen.

Table 66 Site-Wide &gt; Monitor &gt; Clients &gt; 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, Security Firewall, 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.
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.

Table 66 Site-Wide &gt; Monitor &gt; Clients &gt; Client list (continued)

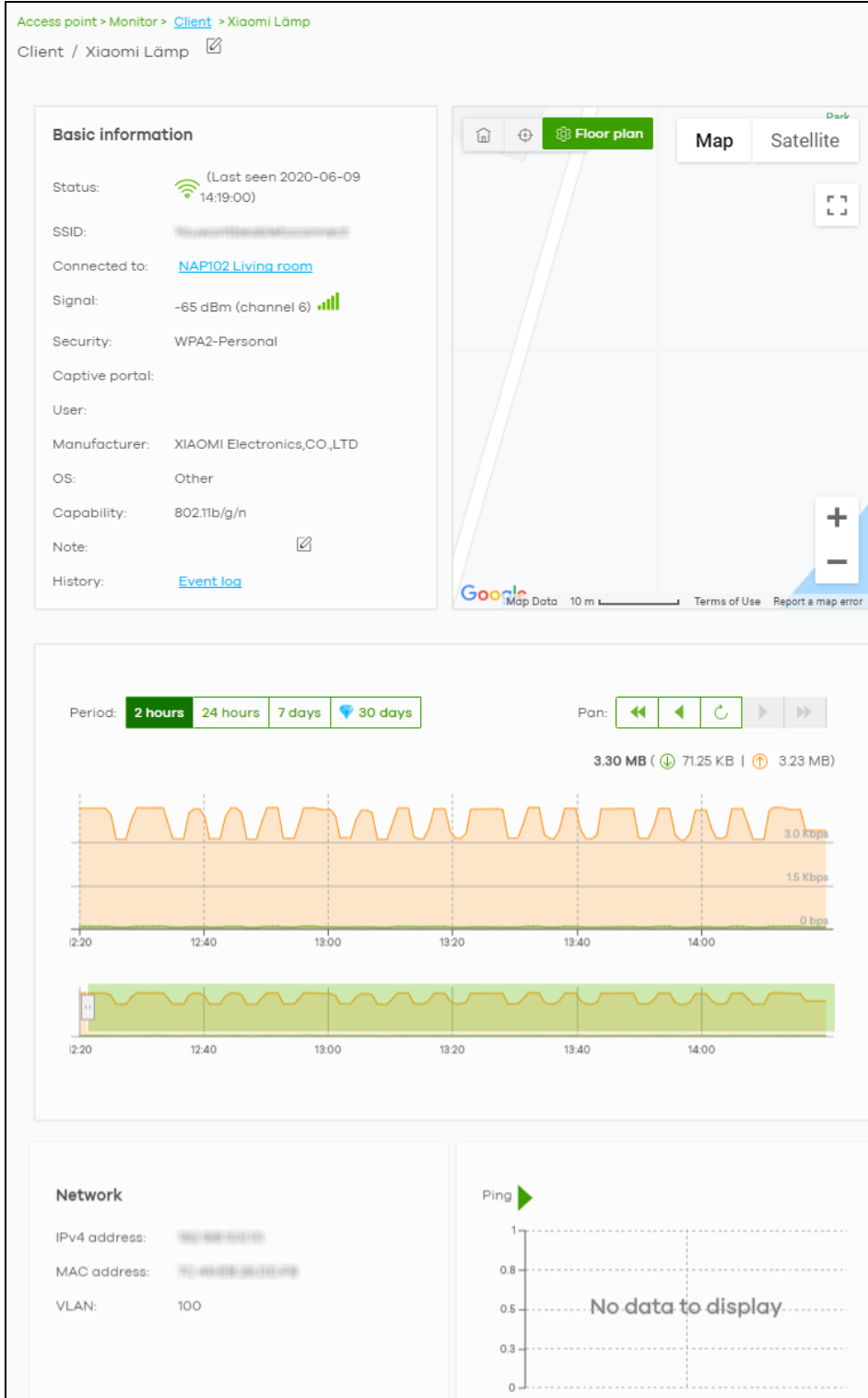
LABEL	DESCRIPTION
Policy	<p>Select the clients from the table below, and then choose the security policy that you want to apply to the selected clients. Choose one of the following policies, then click <b>Apply policy</b>.</p> <ul style="list-style-type: none"> <li>• <b>Allow list:</b> The selected clients to bypass captive portal authentication.</li> <li>• <b>Block list:</b> The selected clients cannot connect to the site. How a client is blocked depends on the connected Nebula Device type selected under <b>Client list</b>. <ul style="list-style-type: none"> <li><b>AP:</b> The client is blocked by MAC address from connecting to any AP in the site.</li> <li><b>Switch:</b> The client is blocked by MAC address from sending or receiving network traffic.</li> <li><b>Gateway:</b> The Security Appliance will not route traffic for the client's IP address.</li> </ul> </li> <li>• <b>To specific SSID:</b> Selectively apply captive portal authentication to specific SSIDs on an AP.</li> <li>• <b>Normal:</b> The selected clients have no policies applied to them.</li> </ul>
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	<p>This shows whether the client is online (green) or offline (red), and whether the client is wired or wireless.</p> <ul style="list-style-type: none"> <li>• Clients connected to an Access Point are reported as wireless.</li> <li>• Clients connected to a Switch or Security Appliance are reported as wired.</li> </ul>
Description	<p>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:</p> <ul style="list-style-type: none"> <li>• User customized description</li> <li>• Hostname detected from client's LLDP (Link Layer Discovery Protocol) System Name</li> <li>• Hostname detected from the Nebula-managed access point</li> <li>• Hostname detected from the Nebula-managed Security Appliance.</li> </ul> <p>Click the name to display the individual client statistics. See wireless: <a href="#">Section 7.1.2.1 on page 257</a> and wired: <a href="#">Section 7.1.2.2 on page 259</a>.</p>
Connected to	<p>This shows the name of the Nebula Device to which the client is connected in this site.</p> <p>Click the Nebula Device name to display the screen where you can view detailed information about the Nebula Device.</p>
MAC address	<p>This shows the MAC address of the client.</p> <p>Click the MAC address to display the individual client statistics. See wireless: <a href="#">Section 7.1.2.1 on page 257</a> and wired: <a href="#">Section 7.1.2.2 on page 259</a>.</p>
IPv4 address	<p>This shows the IPv4 address of the client. By default, the field is blank. The client IPv4 address can be obtained through the following:</p> <ul style="list-style-type: none"> <li>• IPv4 address detected from client's LLDP (Link Layer Discovery Protocol) Management Address</li> <li>• IPv4 address detected from the Nebula-managed access point</li> <li>• IPv4 address detected from the Nebula-managed Security Appliance.</li> </ul>
First seen	This shows the first date and time the client was discovered over the specified period of time.
Last seen	This shows the last date and time the client was discovered over the specified period of time.
Manufacturer	This shows the manufacturer of the client hardware.
Policy	This shows the security policy applied to the client.
Note	This shows additional information about the client.
	Click this icon to display a greater or lesser number of configuration fields.



### 7.1.2.1 WiFi Client Details

Click a WiFi client entry in the **Site-Wide > Monitor > Clients > Clients list** screen to display individual client statistics.

**Figure 80** Site-Wide > Monitor > Clients > Clients list: WiFi Client Details



The following table describes the labels in this screen.

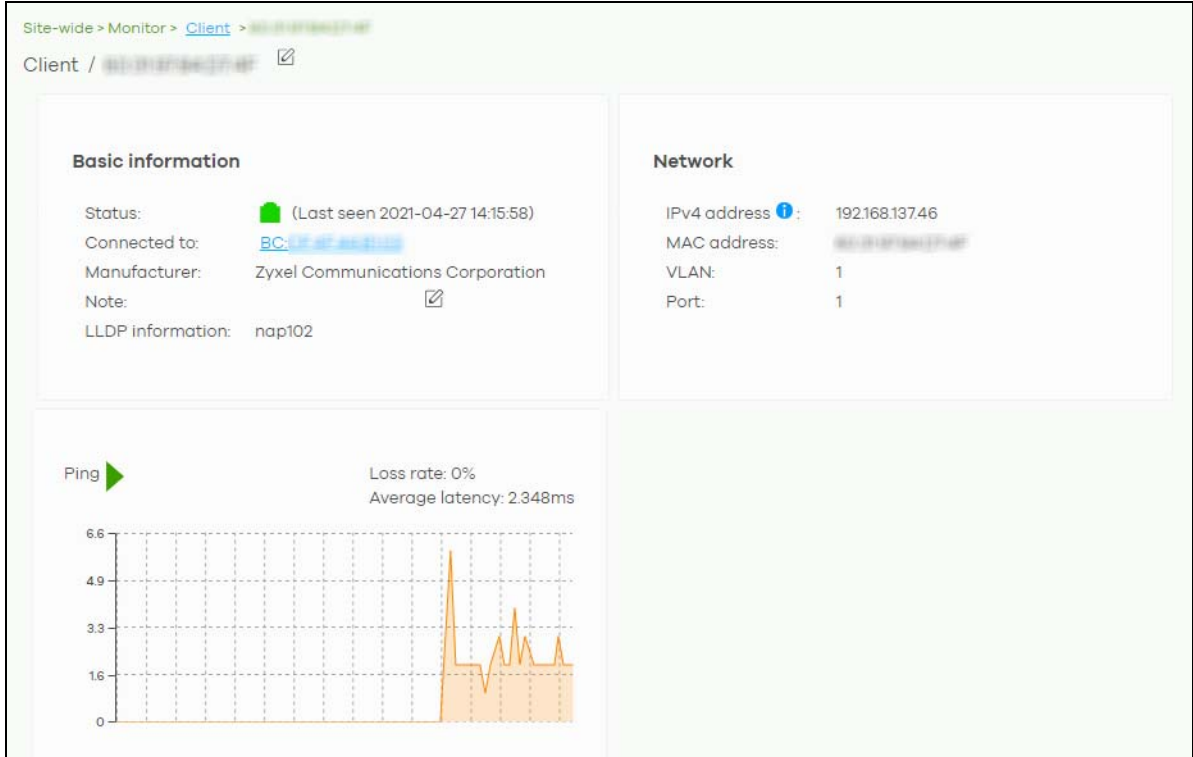
Table 67 Site-Wide > Monitor > Clients > Clients list: WiFi Client Details

LABEL	DESCRIPTION
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 <a href="#">Section 12.2.1.1 on page 516</a> .
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: <ul style="list-style-type: none"> <li>• Green/5 blocks: signal is greater than -67 dBm, strong signal</li> <li>• Amber/4 blocks: signal -67 to -73 dBm, average signal</li> <li>• Amber/3 blocks: signal -74 to -80 dBm, below average signal</li> <li>• Red/2 blocks: signal is less than -80 dBm, weak signal</li> </ul>
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 <b>Event log</b> to go to the <b>Access Point &gt; Monitor &gt; Event log</b> 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.  If you applied a security policy to a client using the <b>Add client</b> button in the <b>Access Point &gt; Monitor &gt; Clients</b> screen, and the client has never been connected to the Access Point's network, an edit icon appears allowing you to modify the client's MAC address,
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.

## 7.1.2.2 Wired Client Details

Click a wired client's descriptive name in the **Site-Wide > Monitor > Clients > Clients list** screen to display individual client statistics.

**Figure 81** Site-Wide > Monitor > Clients > Clients list: Wired Client Details



The following table describes the labels in this screen.

**Table 68** Site-Wide > Monitor > 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.

## 7.1.3 WiFi Aid

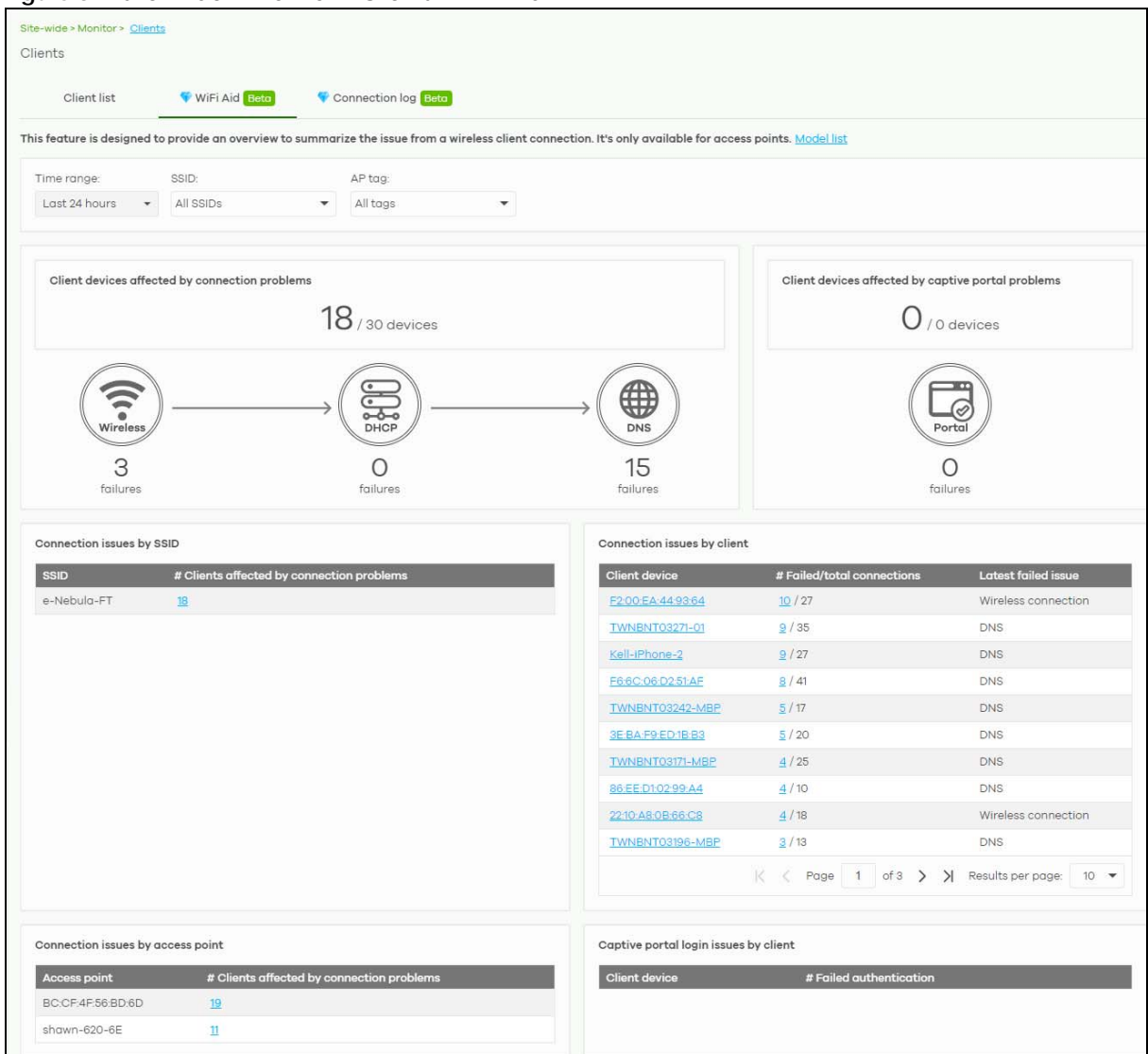
The **WiFi Aid** screen displays the number of WiFi clients that cannot connect to an AP(s) in a site. It also displays the number of WiFi clients who cannot authenticate in a hotspot (captive portal) or who have timed out.

Use this screen to identify connection problems between WiFi clients and supported AP(s). Click **Site-Wide > Monitor > 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 82** Site-Wide > Monitor > Clients > WiFi Aid



The following table describes the labels in this screen.

Table 69 Site-Wide > Monitor > Clients > WiFi Aid

LABEL	DESCRIPTION
WiFi Aid	<p>Select a <b>Time range</b>. The overview will show all WiFi clients' connection issues in the <b>Last hour</b>, <b>Last 12 hours</b>, <b>Last 24 hours</b>, or <b>Custom range</b> (from 15 minutes to one day).</p> <p>Select to filter the overview of the client's WiFi connection issues based on one AP WiFi network (<b>SSID</b>), or all WiFi networks (<b>All SSIDs</b>, default).</p> <p>Select to filter the overview of all WiFi clients' connection issues based on one <b>AP tag</b>, or <b>All tags</b> (default). This is the tag you create in <b>Access point &gt; Monitor &gt; Access points</b>.</p>
Client devices affected by connection problems	<p>This chart displays the number of WiFi clients with the following connection problems.</p> <ul style="list-style-type: none"> <li>• <b>Wireless</b> failures. This displays the number of WiFi clients that failed association to an AP or failed authentication.</li> <li>• <b>DHCP</b> failures. This displays the number of WiFi clients that failed to receive an IP address due to DHCP failure/timeout with the DHCP server.</li> <li>• <b>DNS</b> failures. This displays the number of WiFi clients that failed DNS query due to DNS timeout from a DNS server.</li> </ul>
Client devices affected by captive portal problems	<p>This chart displays the number of WiFi clients that failed hotspot authentication. This includes entering the wrong user credentials or an authentication timeout.</p>
Connection issues by SSID	<p>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.</p> <p>Clicking the hyperlink in the <b># Clients affected by connection problems</b> column will direct you to the <b>Site-wide &gt; Monitor &gt; Connection log</b> screen. See <a href="#">Section 7.1.4 on page 262</a> for more information on this screen.</p>
Connection issues by client	<p>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.</p> <p>Clicking the hyperlink in the <b>Client device</b> column will direct you to the <b>Site-wide &gt; Monitor &gt; Client: Client device</b> screen. See <a href="#">Section 7.1.2 on page 255</a> for more information on this screen.</p> <p>Clicking the numerator hyperlink in the <b># Failed/total connections</b> column will direct you to the <b>Site-wide &gt; Monitor &gt; Connection log</b> screen. See <a href="#">Section 7.1.4 on page 262</a> for more information on this screen.</p>
Connection issues by access point	<p>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.</p> <p>Clicking the hyperlink in the <b># Clients affected by connection problems</b> column will direct you to the <b>Site-wide &gt; Monitor &gt; Connection log</b> screen. See <a href="#">Section 7.1.4 on page 262</a> for more information on this screen.</p>
Captive portal login issues by client	<p>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.</p> <p>Clicking the hyperlink in the <b>Client device</b> column will direct you to the <b>Site-wide &gt; Monitor &gt; Client: Client device</b> screen. See <a href="#">Section 7.1.2 on page 255</a> for more information on this screen.</p> <p>Clicking the hyperlink in the <b># Failed authentication</b> column will direct you to the <b>Site-wide &gt; Monitor &gt; Connection log</b> screen. See <a href="#">Section 7.1.4 on page 262</a> for more information on this screen.</p>

## 7.1.4 Connection Log

Use this screen 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. Click **Site-Wide > Monitor > Clients > Connection log** to access this screen.

Note: This feature is available for Nebula Pro Pack license only.

**Figure 83** Site-Wide > Monitor > Clients > Connection log

Connection time	Connected to	Event type	Detail Issue
2023-01-05 14:22:27	<a href="#">BC:CF:4F:56:8D:6D</a>	DNS failure [WiFi Aid]	A4:5E:60:C4:7B:C7 DNS query failed due to DNS timeout from DNS server 173.16.2.1, SSID: e-Nebula-FT.
2023-01-05 14:22:27	<a href="#">BC:CF:4F:56:8D:6D</a>	DHCP client [WiFi Aid]	A4:5E:60:C4:7B:C7/TWNBNT03171-MBP succeeded to receive IP address 173.16.2.51, SSID: e-Nebula-FT.
2023-01-05 14:22:27	<a href="#">BC:CF:4F:56:8D:6D</a>	Association	Station: a4:5e:60:c4:7b:c7 connected on Channel: 149, SSID: e-Nebula-FT, 5GHz, Signal: -60dBm, Interface: wlan-2-1
2023-01-05 14:22:27	<a href="#">BC:CF:4F:56:8D:6D</a>	Association	STA roamed, MAC:A4:5E:60:C4:7B:C7, From:Marketing2, To:BC:CF:4F:56:8D:6D, SSID:e-Nebula-FT.
2023-01-05 14:19:52	<a href="#">shawn-620-6E</a>	DHCP client [WiFi Aid]	22:10:A8:0B:66:C8 succeeded to receive IP address 173.16.2.89, SSID: e-Nebula-FT.
2023-01-05 14:19:52	<a href="#">shawn-620-6E</a>	Association	Station: 22:10:a8:0b:66:c8 connected on Channel: 149, SSID: e-Nebula-FT, 5GHz, Signal: -50dBm, Interface: wlan-2-1
2023-01-05 14:15:44	<a href="#">Marketing2</a>	Association	Station: 1a:9f:c2:cf:ed:f5 connected on Channel: 161, SSID: e-Nebula-FT, 5GHz, Signal: -58dBm, Interface: wlan-2-1
2023-01-05 14:04:49	<a href="#">Marketing2</a>	Association	STA fast roamed, MAC:F6:6C:06:D2:51:AF, From:shawn-620-6E, To:Marketing2, SSID:e-Nebula-FT.
2023-01-05 14:04:49	<a href="#">Marketing2</a>	Association	Station: f6:6c:06:d2:51:af connected on Channel: 161, SSID: e-Nebula-FT, 5GHz, Signal: -57dBm, Interface: wlan-2-1
2023-01-05 14:03:16	<a href="#">shawn seat2</a>	Association	STA fast roamed, MAC:F6:6C:06:D2:51:AF, From:Marketing2, To:shawn seat2, SSID:e-Nebula-FT.

The following table describes the labels in this screen.

**Table 70** Site-Wide > Monitor > Clients > Connection log

LABEL	DESCRIPTION
Clients list	<p>Select a time; the list shows each client's event logs in the past hour, last 12 hours, last day, or custom range (from 15 minutes to one day within the last month).</p> <p>Select to filter the list of client's event logs based on the SSID, or <b>All SSIDs</b> (default).</p> <p>Select to filter the list of client's event logs based on the AP, or <b>All APs</b> (default).</p> <p>Select to filter the list of client's event logs, based on the event type (<b>Association, Disconnection, DHCP server, Wireless failed connection, DHCP client, DNS failure, Captive portal</b>) that occurred, or <b>All event types</b> (default).</p> <p>Select the client, or <b>All clients</b> (default).</p>
Connection time	This shows the starting time period from which the event log is recorded.
Connected to	This shows the name (if available) or MAC address of the connected client.
Event type	This shows the event type ( <b>Association, Authentication, Disconnection, DHCP server, Wireless failed connection, DHCP client, DNS failure, Captive portal</b> ) that occurred.
Detail issue	This shows a summary of the Access Points and Security Appliances (NSG, USG FLEX, ATP, and USG20(W)-VPN) event logs in chronological order.

## 7.1.5 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 84** Site-Wide > Monitor > Containment list

The following table describes the labels in this screen.

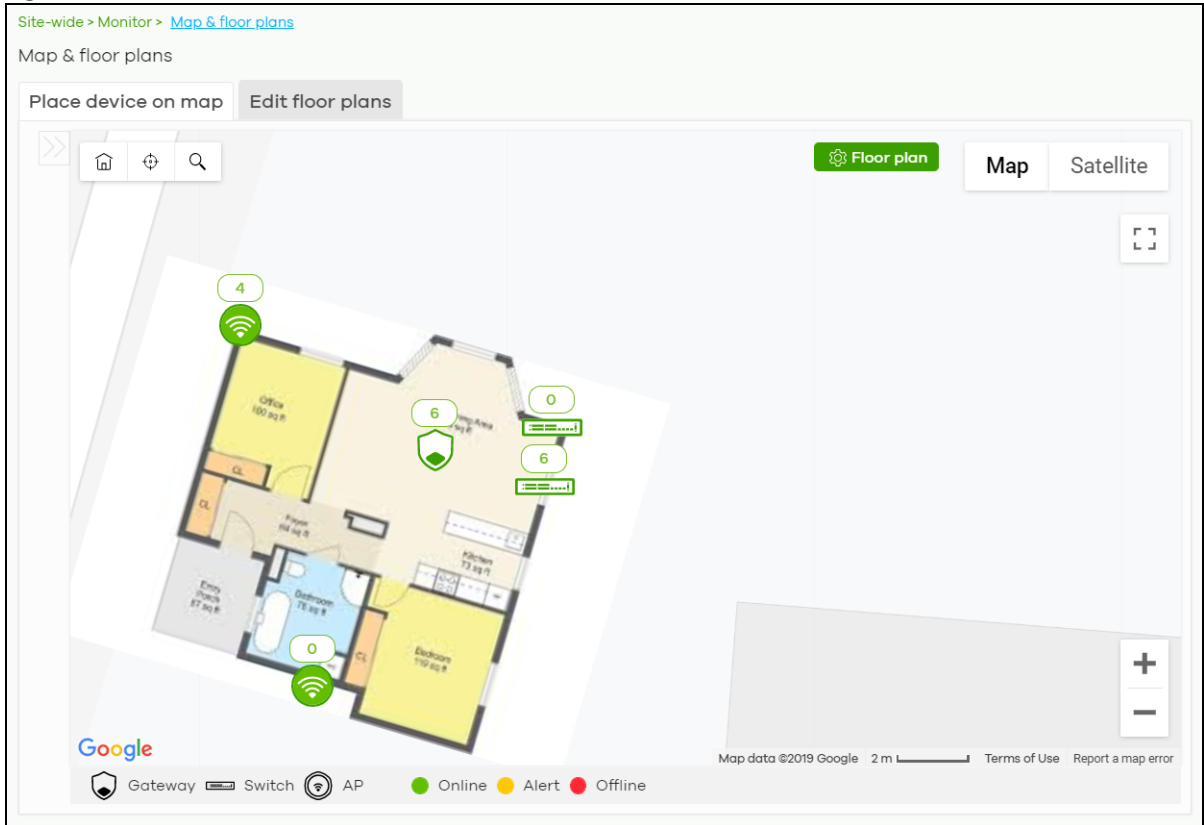
**Table 71** Site-Wide > Monitor > Containment list

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 <b>OK</b> to release this client device from CDR containment. This client device's IP or MAC address is exempt from future CDR checking.

## 7.1.6 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 > Monitor > Map & floor plans** to access this screen.

**Figure 85** Site-Wide > Monitor > Map & floor plans



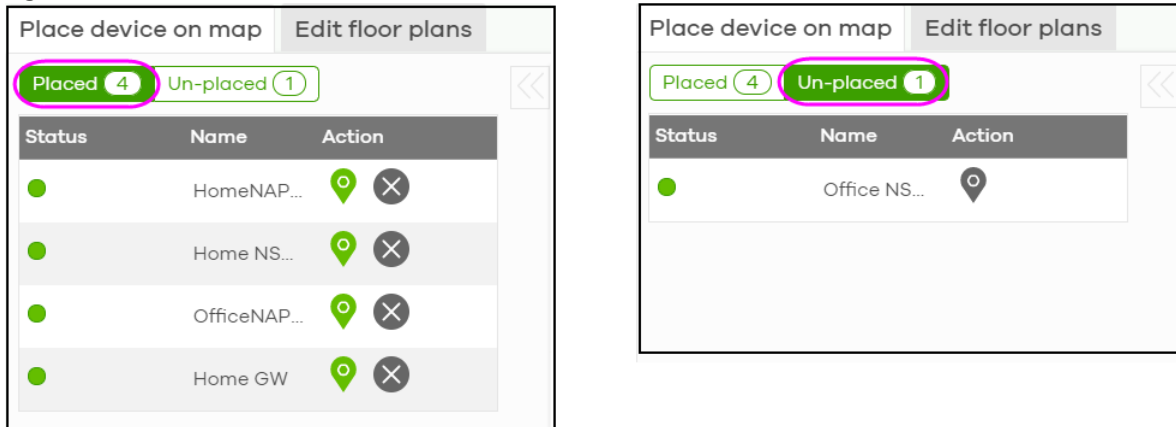
### Place devices on map

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.

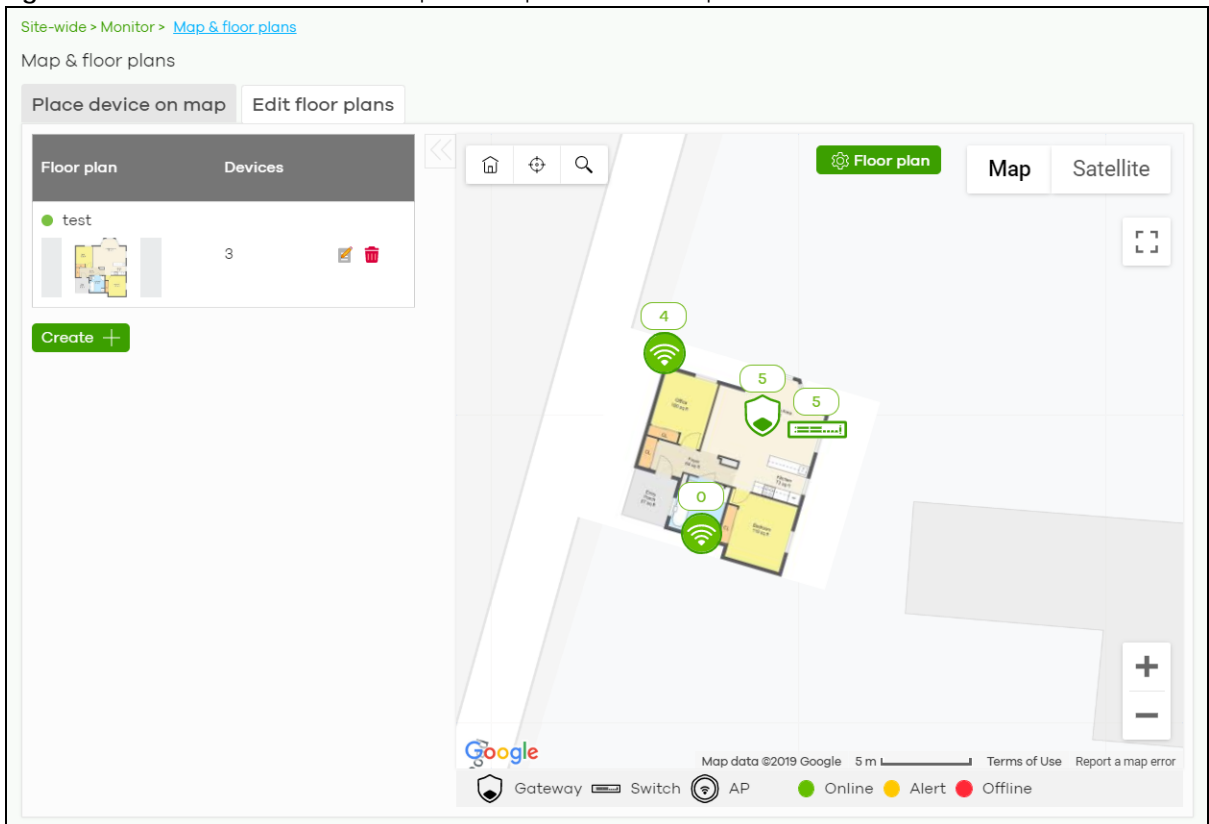


**Figure 86** Site-Wide > Monitor > Map & floor plans: Place device on map

## 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 87** Site-Wide > Monitor > Map & floor plans: Edit floor plans

The following table describes the labels in this screen.

Table 72 Site-Wide > Monitor > 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.

## 7.1.7 Topology

Use this screen to view the links between Nebula Devices in the site. Click **Site-Wide > Monitor > 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.

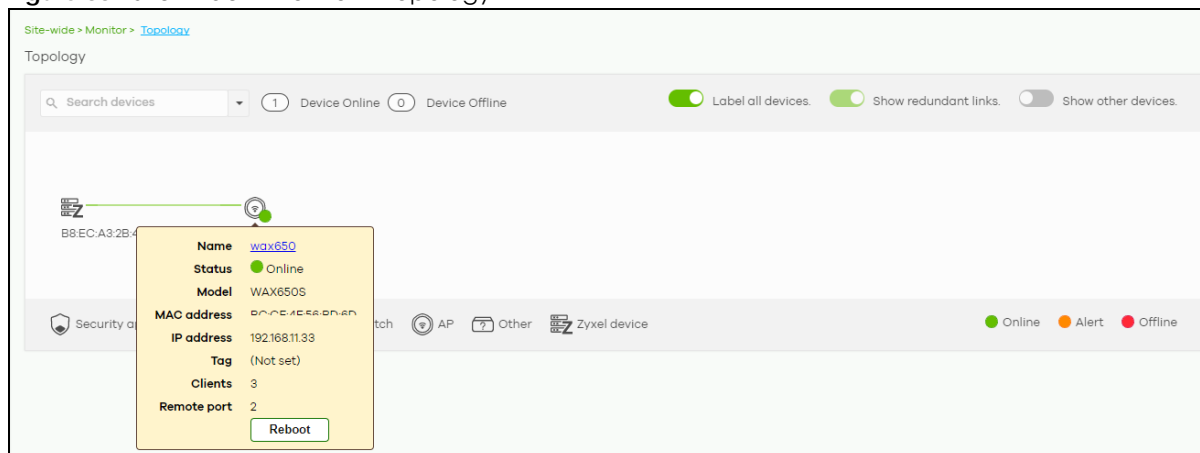
Enable **Label all devices** to show Nebula Device information, such as MAC address in the network topology diagram.

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 88 Site-Wide &gt; Monitor &gt; Topology



## 7.1.8 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.

### 7.1.8.1 Using Vouchers

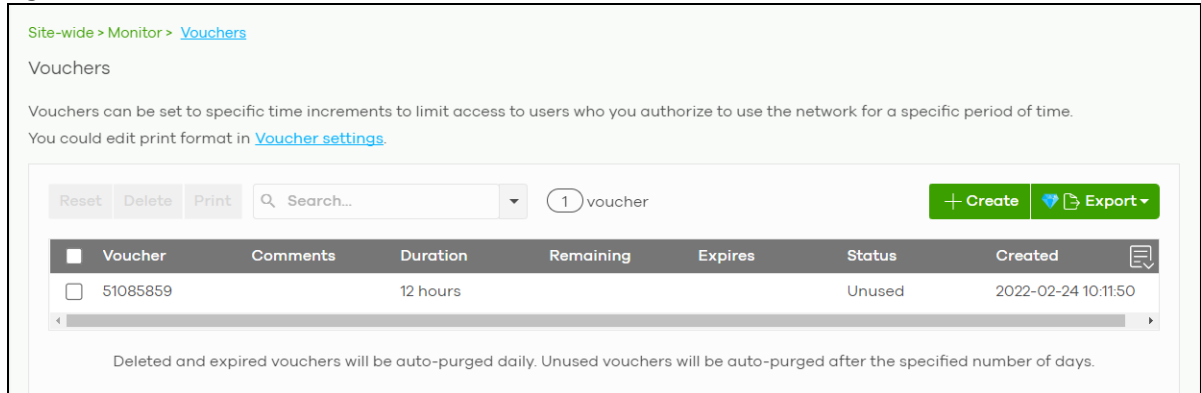
- 1 Go to **Access Point > Configure > SSID settings**, and create a dedicated SSID for voucher-based WiFi access. For example, "Hotel\_Guest\_Network".  
For details on configuring SSIDs, see [Section 12.3.1 on page 538](#).
- 2 Go to **Access Point > Configure > Authentication**, select the SSID, and then under **Sign-in method** select **Voucher**.  
For details, see [Section 12.3.2 on page 540](#).
- 3 Go to **Site-wide > Configure > General settings > Voucher settings** to configure how the vouchers will look when printed.  
For details, see [Section 7.2.1 on page 277](#).
- 4 Go to **Site-Wide > Monitor > Vouchers**, and then click **Create** to create one or more vouchers.

### 7.1.8.2 Vouchers Screen

This screen allows you to create and manage vouchers for WiFi network authentication.

Click **Site-Wide > Monitor > Vouchers** to access this screen.

Figure 89 Site-Wide &gt; Monitor &gt; Vouchers



The following table describes the labels in this screen.

Table 73 Site-Wide &gt; Monitor &gt; 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 <b>Unused</b> and time remaining is reset to the time configured in <b>Duration</b> .
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 <b>Site-wide &gt; Configure &gt; General settings</b> .
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 <a href="#">Section 7.1.8.3 on page 269</a> .
Export	Click this button to export the voucher table and all information in it to a CSV or XML file.
Voucher	This displays the voucher's unique authentication code.
Comments	This displays information about the voucher.
Duration	This displays how long the voucher is valid from when it is activated, in hours.
Remaining	This displays how much time is left before the voucher expires. NCC only starts counting this time after the voucher has been activated.
Expire in	This displays the date and time that the voucher will expire.
Status	This displays the current status of the voucher: <b>Unused:</b> The voucher has not yet been used for authentication. <b>Active:</b> A user has used the voucher for authentication. NCC has started counting down the duration. <b>Expire:</b> The voucher has reached the end of its duration period and can no longer be used. <b>Delete:</b> The voucher is unused and has reached the time set under <b>Purge after (days)</b> . Note: NCC automatically deletes vouchers with the status <b>Expire</b> or <b>Delete</b> 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.

### 7.1.8.3 Create Vouchers Screen

Use this screen to create one or more new vouchers.

**Figure 90** Site-Wide > Monitor > Vouchers > Create

The following table describes the labels in this screen.

**Table 74** 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.
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.
Print after created	Select this to print the vouchers immediately after clicking <b>Create</b> .
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](#).

### 7.1.9 Cloud Intelligence 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 > Cloud intelligence logs** to access this screen.

**Figure 91** Site-Wide > Monitor > Cloud intelligence logs

Site-wide > Monitor > [Cloud intelligent logs](#)

Cloud intelligent logs

Feature:  Keyword:  Category:

From:  14:16 To:  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 75** Site-Wide > Monitor > Cloud intelligent 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 <b>Feature</b> .
Range/Before	Select filtering options, set a date, and then click <b>Search</b> to filter log entries by date. <b>Range:</b> Display log entries from the first specified date to the second specified date. <b>Before:</b> Display log entries from the beginning of the log to the selected date.
Reset filters <input type="button" value="X"/>	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 <b>Site-wide &gt; Configure &gt; General settings</b> .
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 75 Site-Wide &gt; Monitor &gt; Cloud intelligent logs (continued)

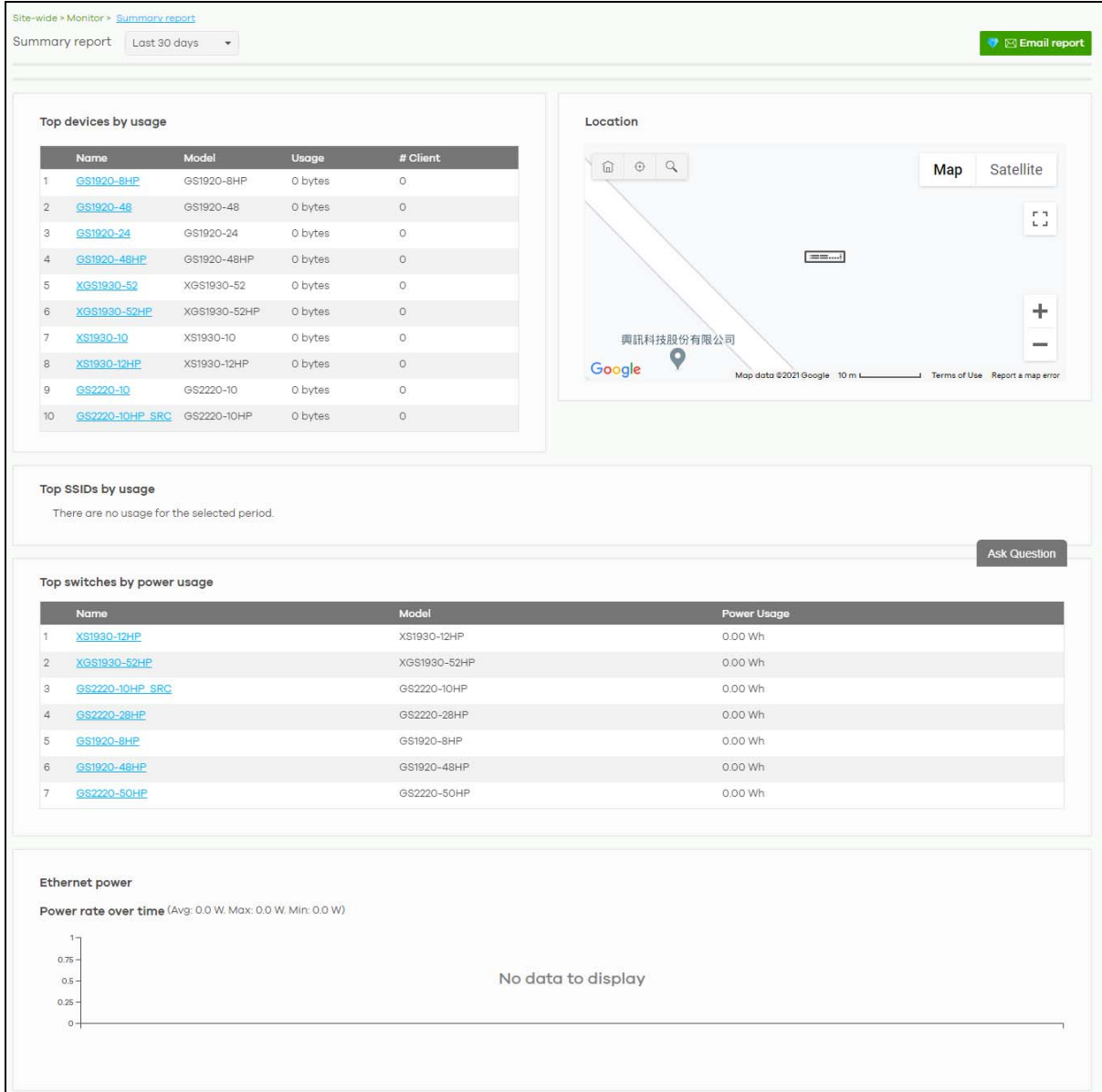
LABEL	DESCRIPTION
Detail	This shows the details of the event.  Note: Click the Nebula Device name link for an Auto configuration recovery alert to go to <b>Switch &gt; Monitor &gt; Switches: Switch Details</b> screen for more information.
	Click this icon to display a greater or lesser number of configuration fields.

## 7.1.10 Summary Report

Use this screen to view statistics for the Nebula Devices and networks in the selected site.

Click **Site-wide > Monitor > Summary report** to access this screen.

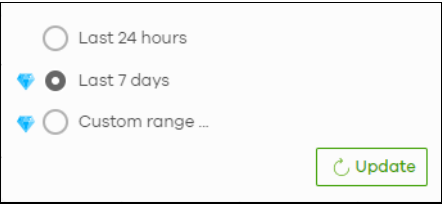
Figure 92 Site-wide > Monitor > Summary report





The following table describes the labels in this screen.

Table 76 Site-wide> Monitor > Summary Report

LABEL	DESCRIPTION
Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
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.
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.

## 7.1.11 Applications

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 > Monitor > Applications** to access this screen.

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

**Figure 93** Site-Wide > Monitor > Applications: Application View

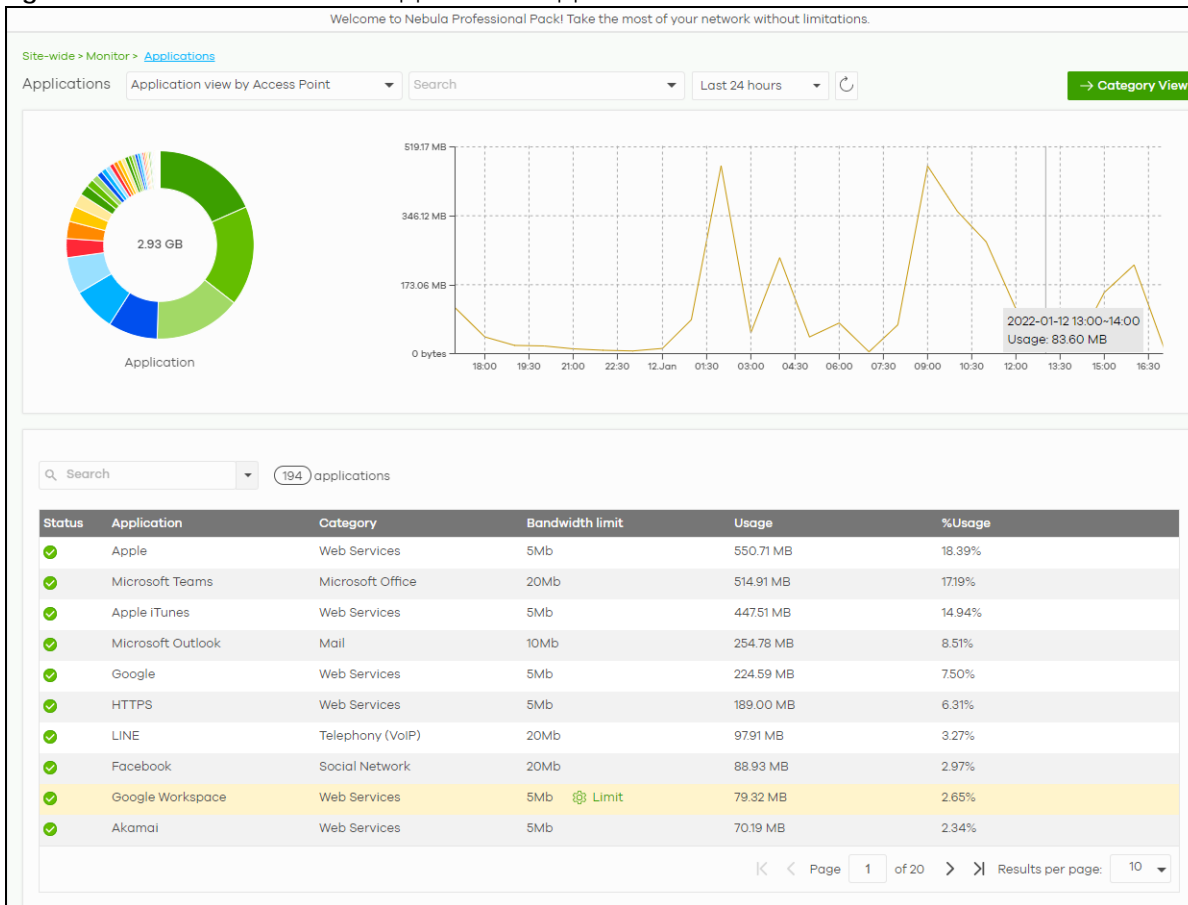
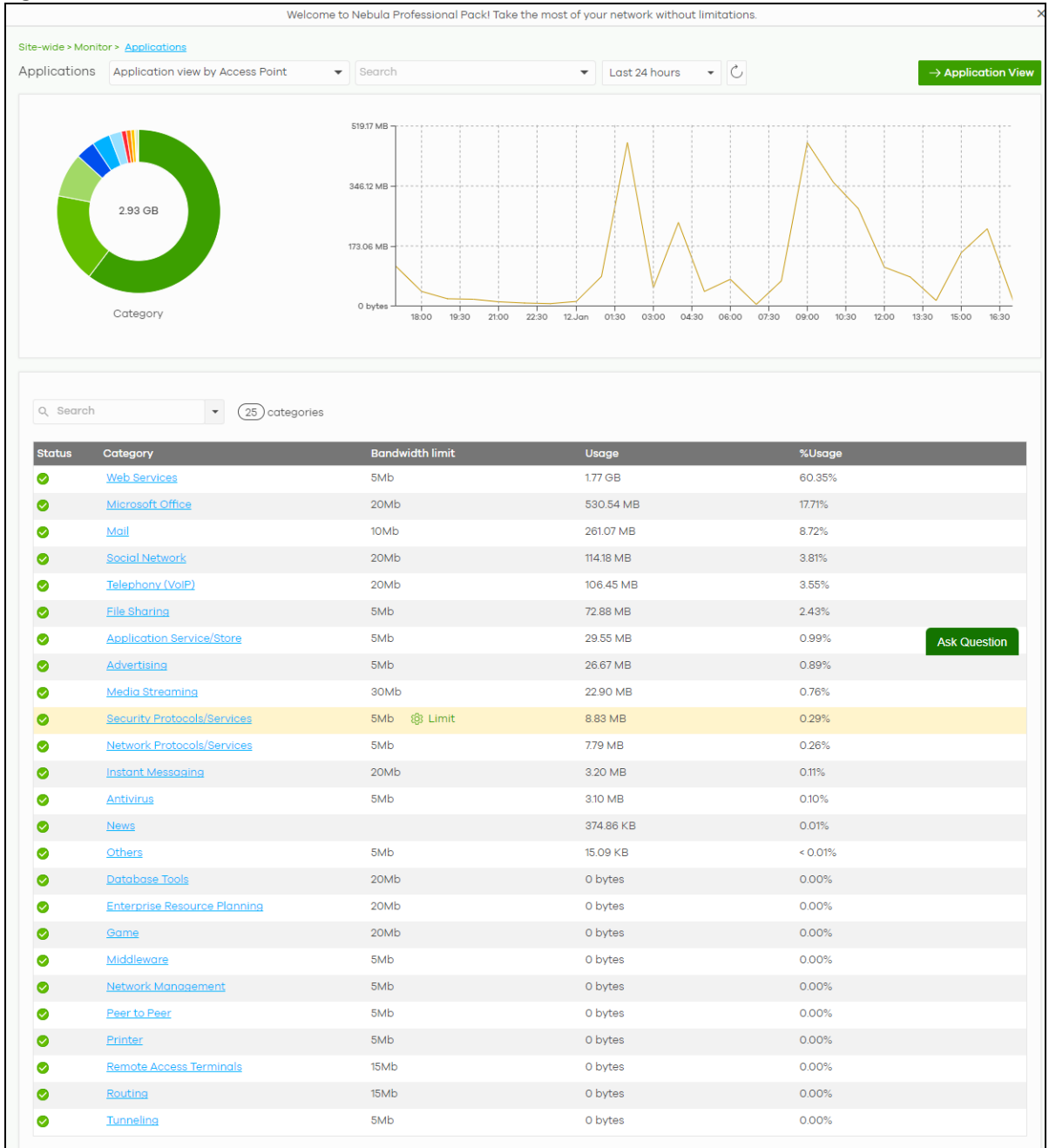
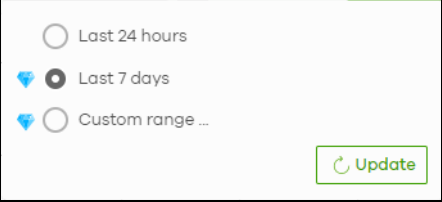



Figure 94 Site-Wide > Monitor > Applications: Category View



The following table describes the labels in this screen.

Table 77 Site-Wide &gt; Monitor &gt; Applications

LABEL	DESCRIPTION
Applications	<p>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.</p> <p>In Category view, select to view all applications of Nebula Security Appliances / Nebula Access Points only.</p> <p>Select to view the report for the past day or week. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
	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	<p>This shows the name of the category to which the application belongs.</p> <p>Note: Click this field in Category view to see all applications in the category.</p>
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	<p>Click this to limit the bandwidth for the application on the site's gateway.</p> <p>You can apply the restrictions per gateway interface, or for all interfaces.</p>

## 7.2 Configure

Use the **Configure** menus to set the general and email alert settings for the selected site, or register a new Nebula Device and assign it to the site.

## 7.2.1 General 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, WiFi network authentication voucher settings, and API access for DPPSK third-party integration. Click **Site-Wide > Configure > General settings** to access this screen.

**Figure 95** Site-Wide > Configure > General settings

This site is bound to template [SSID\\_Template2](#)

Site-wide > Configure > [General settings](#)

General settings  Override site-wide configuration

---

**Site information**

Site name:  ✕ \*

Local time zone:   ✕

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

---

**Device configuration**

Local credentials

Username:  (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?](#)

---

**Captive portal reauthentication**

For my AD server users:  ▼

For my RADIUS server users:  ▼

For click-to-continue users:  ▼

For cloud authentication users ?:  ▼

---

**SNMP**

SNMP access:  ▼

SNMP community string:  ✕

### Reporting

Syslog server

Server IP	Types	Action
<input type="text"/>	AP traffic log	

[+ Add](#)

AP traffic log

SecuReporter  Sending Security Appliance traffic logs to SecuReporter.

---

### Voucher settings

See [Using Vouchers](#) for more information

Duration text:  This text will precede the duration on the printed voucher

Date Text:  This text will precede the voucher expiration date on the printed voucher

Access text:  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: [Upload an image](#)

---

### API access

API token:  [Delete](#)

The following table describes the labels in this screen.


Table 78 Site-Wide > Configure > General 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.
Configuration template	The name of the template that the site is bound to is shown here. Click <b>Unbind</b> to release the site from using the configuration template. The site which is unbound from the template still retains the settings applied from the template.
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.

Table 78 Site-Wide &gt; Configure &gt; General settings (continued)

LABEL	DESCRIPTION
Smart guest/ VLAN network	<p>Click <b>On</b> 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.</p> <p>The guest settings you configure for a gateway interface (in <b>Security Gateway &gt; Configure &gt; Interface addressing</b>) will also apply to the WiFi networks (SSIDs) associated with the same VLAN ID (in <b>Access Point &gt; Configure &gt; SSID settings</b>). 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.</p>
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 <b>V1/V2c</b> to allow SNMP managers using SNMP to access the Nebula Devices in this site. Otherwise, select <b>Disable</b> .
SNMP community string	<p>This field is available when you select <b>V1/V2c</b>.</p> <p>Enter the password for the incoming SNMP requests from the management station.</p>
Reporting	
Syslog server	Click <b>Add</b> to create a new entry.
Server IP	Enter the IP address of the server.
Types	<p>Select the type of logs the server is for.</p> <p>Note: Besides sending <b>Gateway traffic log</b> 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. <b>Gateway traffic log</b> includes the traffic information (such as its source, destination or usage) of the Security Appliance clients.</p>
Action	Click the <b>Delete</b> icon to remove the entry.
AP traffic log	<p>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 <b>AP traffic log</b> under <b>Syslog server &gt; Types</b>.</p> <p>For details on configuring <b>NAT mode</b>, see <a href="#">Section 12.3.2 on page 540</a>.</p>
SecuReporter	<p>Click <b>On</b> to enable this feature. This allows the NCC to send traffic logs to SecuReporter.</p> <p>Note: Disable this option if you have configured sending of traffic logs to an external syslog server.</p>

Table 78 Site-Wide &gt; Configure &gt; General settings (continued)

LABEL	DESCRIPTION
Voucher settings	<p>Use these settings to configure how WiFi network authentication vouchers for this site look when printed.</p>  <p>For more information on vouchers, see <a href="#">Section 7.1.8 on page 267</a>.</p>
Duration Text	Sets the text that proceeds the duration on the voucher. The text must consist of 1 – 16 characters.
Access Text	Sets the text that proceeds the access 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 <b>Choose File</b> 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.
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.
Generate	Click this button to create a new API key.
Copy	Click this button to copy the API key to the system's clipboard.
Delete	Click this button to delete the API key.

## 7.2.2 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 79 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. <ul style="list-style-type: none"> <li>CDR fields in an "Enabled/Disabled" state will show "Enabled/Disabled" but grayed-out.</li> <li>The <b>Policy</b> rule settings, <b>Quarantine VLAN</b>, and <b>Exempt list</b> will be kept in <b>Site-wide &gt; Configure &gt; Collaborative detection &amp; response</b>.</li> <li>Previously quarantined clients will be released.</li> </ul>
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. <ul style="list-style-type: none"> <li>CDR event detection is available</li> <li>CDR triggered events are logged in the <b>Site-wide &gt; Monitor &gt; Cloud intelligent logs</b></li> <li><b>Containment</b> actions (<b>Alert/Block/Quarantine</b>) is not available</li> <li>Previously blocked/quarantined clients will be released in <b>Site-wide &gt; Monitor &gt; CDR &gt; Containment list</b>.</li> </ul>	CDR will disable its full functionality. <ul style="list-style-type: none"> <li>CDR fields in an "Enabled/Disabled" state will show "Enabled/Disabled" but grayed-out.</li> <li>The <b>Policy</b> rule settings, <b>Quarantine VLAN</b>, and <b>Exempt list</b> will be kept in <b>Site-wide &gt; Configure &gt; Collaborative detection &amp; response</b>.</li> <li>Previously quarantined clients will be released.</li> </ul>

Figure 96 Site-Wide > Configure > Collaborative Detection & Response

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 <input type="text"/> × *	60 <input type="text"/> × *	Alert
IDP	Vulnerability exploit detected	2 <input type="text"/> × *	10 <input type="text"/> × *	Alert
Web Threats	Connections to malicious web sites detected	3 <input type="text"/> × *	30 <input type="text"/> × *	Alert

**Containment**

**General**

Theme



Default
  Modern
 Ask Question

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

The following table describes the labels in this screen.

Table 80 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	
Category	Category refers to the signature type that identified the malicious traffic: <b>Malware</b> (Anti-Malware, Anti-Virus), <b>IDP</b> (IPS), and <b>Web Threat</b> (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 <b>Duration</b> to trigger a CDR <b>Containment</b> action.
Duration (1–1440)	Enter the length of time in minutes the event should occur from a client the <b>Occurrence</b> number of times to trigger a CDR <b>Containment</b> action.  For example, <b>Occurrence</b> is set to 10, and <b>Duration</b> is set to 100. If the NCC detects 10 or more occurrences of malicious traffic in less than 100 minutes, then <b>CDR Containment</b> is triggered.
Containment	Select the action to be taken when the number of security events exceed the threshold within the defined duration.  <b>Alert:</b> Select this if you just want to issue a notification in NCC.  <b>Block:</b> 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.  <b>Quarantine:</b> 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.  <ul style="list-style-type: none"> <li>Click the <b>Preview</b> icon at the upper right corner of a theme image to display the block page in a new frame.</li> <li>Click the <b>Copy</b> icon to create a new custom theme (block page).</li> </ul>
Logo	This shows the logo image that you uploaded for the customized block page.  Click <b>Choose File</b> and specify the location and file name of the logo graphic or click <b>Browse</b> 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 <b>Block</b> or <b>Quarantine</b> action is triggered. For example, "Malicious traffic is coming from your device so traffic is temporarily stopped. Please contact the network administrator."  <b>Redirect external URL:</b> Enter a URL in "http://domain" or "https://domain" format to an external notification page. The client is redirected here when a <b>Block</b> or <b>Quarantine</b> 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 <b>Block</b> or <b>Quarantine</b> action is triggered. You can download a sample block page by clicking <b>Download</b> .  Note: The external notification page must be accessible from NCC.

Table 80 Site-Wide &gt; Configure &gt; Collaborative Detection &amp; Response (continued)

LABEL	DESCRIPTION
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 <b>Monitor &gt; CDR &gt; Containment List</b> .
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.
Quarantine	
Quarantine VLAN	Click <b>Set</b> 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.

## 7.2.3 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 97** Site-Wide > Configure > Collaborative detection & response > Containment > Quarantine

The screenshot shows a configuration window titled "Quarantine interface configuration". It is organized into three main sections:

- Interface Properties:**
  - Interface name: Quarantine
  - Port group: LAN Group 1
  - VLAN ID: 44 (range 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

At the bottom right, there are "Cancel" and "Ok" buttons.

Each field is explained in the following table.

Table 81 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)
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 <b>OK</b> to save your changes back to the NCC.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 7.2.4 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 avoid 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 98 Site-Wide &gt; Configure &gt; Alert settings

Site-wide > Configure > [Alert settings](#)

### Alert settings

**Recipient**

All site administrators  Email to all site administrators

Custom email recipient

---

**System alerts** ⓘ

Wireless   minutes after AP goes offline

Switches   minutes after Switches goes offline

minutes  goes down

Security gateway   minutes after the gateway goes offline

Any DHCP lease pool is exhausted

A VPN connection is established or disconnected

WAN connectivity status changed

Other  Configuration settings are changed

**Security alerts**

CDR containment ⓘ  Email to receive containment alerts

---

Security Report

Notification mode  Email to receive security alerts by SecuReport

Email subject  (Optional, maximum character is 64.)

Email description  (Optional, maximum character is 255.)

Notification interval  Select notification interval if events were triggered

Event severity  Select severity level for email information

Event threshold

Category	Event Type	Severity	Alert criteria
Network Security	Attack counts	High	Highest severity attacks within 5 minutes.
Network Security	Attack counts	High	<input type="text" value="10"/> times attacks within 5 minutes.
Network Security	Malware/virus detection	High	<input type="text" value="10"/> count(s) of malware/virus attack within 5 minutes.
Network Security	Malware/virus detection	Medium	The same malware/virus is detected over 2 times within 15 minutes.
Network Security	Alert counts	High	<input type="text" value="10"/> count(s) of Malware/IP(highest severity)/ADP(protocol anomaly) hits count exceed 10 within 1 mins.
Anomaly	Login failure	Medium	Number of login failures is over 10 times within 1 minutes.
Anomaly	Traffic anomaly	High	<input type="text" value="1"/> times of traffic anomaly scans/floods detected within 5 minutes.
Anomaly	Protocol anomaly	High	<input type="text" value="1"/> times of protocol anomaly TCP/UDP/CMP/IP decoders within 5 minutes.
Network Security	URL Threat Filter	High	<input type="text" value="5"/> times of connection to threat websites within 60 minutes.

The following table describes the labels in this screen.

Table 82 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 addresses	Enter the email addresses to which you want to send alerts.
Notification Type	For each alert, you can set how to receive alert notifications: <ul style="list-style-type: none"> <li>• <b>Email:</b> Alert notifications are sent by email to configured administrators, custom email recipients, and additional recipients.</li> <li>• <b>In-app Push:</b> 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.</li> <li>• <b>Both:</b> Alert notifications are sent by email and app notification.</li> <li>• <b>Disabled:</b> No alerts are sent.</li> </ul>
Show additional recipients	Add additional user accounts who will receive email and in-app notifications for the alert.
System Alerts	

Table 82 Site-Wide &gt; Configure &gt; Alert settings (continued)

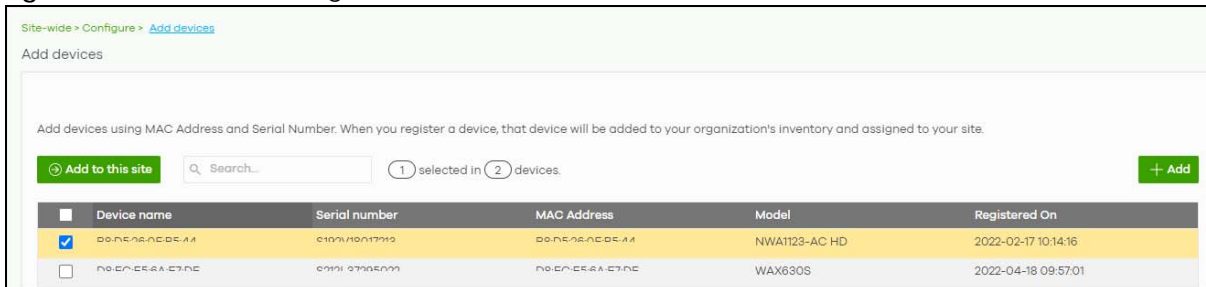
LABEL	DESCRIPTION
Wireless	Specify how long in minutes the NCC waits before generating and sending an alert when an AP becomes offline.
Switches	Specify how long in minutes the NCC waits before generating and sending an alert when a port or a Switch goes offline.
Security Appliance	Select the check box to have the NCC generate and send an alert by email when the following events occur: <ul style="list-style-type: none"> <li>A Security Appliance goes offline.</li> <li>Any DHCP pool on the Security Appliance runs out of IP addresses.</li> <li>A VPN connection to or from the Security Appliance is established or disconnected.</li> <li>The WAN connectivity status changed.</li> </ul>
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.
Security alerts	
CDR containment	Specify whether to send an alert each time a CDR block or containment action is triggered.
Security Report	
Notification mode	Select whether to receive email security reports from SecuReporter.
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.  For some events, you can set the alert threshold. For example, <b>X count(s) of malware/virus attack within 5 minutes</b> 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.

## 7.2.5 Add Devices

Use this screen to register a Nebula Device and add it to the site. Click **Site-Wide > Configure > Add devices** to access this screen.

Note: You have to contact Zyxel customer support if you need to change the Nebula Device owner at myZyxel or remove an Organization from the NCC. Please configure your Nebula Device owners and organizations carefully. See also [Section 6.3.3 on page 195](#).



**Figure 99** Site-Wide > Configure > Add devices

The following table describes the labels in this screen.

**Table 83** Site-Wide > Configure > Add devices

LABEL	DESCRIPTION
Add to this site	Click this button to assign the selected Nebula Devices to the site. If you have selected a Security Firewall (see <a href="#">Table 1 on page 12</a> for a list of Security Firewalls), a pop-up window for you to select the deployment method appears. See <a href="#">Step 7: Set up the Deployment Method on page 50</a> for more information.
Search	Enter a keyword to filter the list of Nebula Devices by device name, serial number, MAC address, or model.
N devices	This shows the number of registered Nebula Devices (N) which have not been assigned to a site.
+ Add	This button is available only for an organization administrator or site administrator that has full access.  Click this button to pop up a window where you can enter a Nebula Device's serial number, MAC address, and name to register it at the NCC. For details, see <a href="#">Section 6.3.3.2 on page 198</a> .  You can also schedule the firmware upgrade for the Nebula Device during registration. For details, see <a href="#">Section 6.3.3.3 on page 199</a> .
Device name	This shows the descriptive name of the Nebula Device.
Serial number	This shows the serial number of the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
Model	This shows the model name of the Nebula Device.
Registered On	This shows the time and date that the Nebula Device was added to NCC.

## 7.2.6 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.

### 7.2.6.1 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 100 Site-Wide > Configure > Firmware management > Overview

Site-wide > Configure > [Firmware management](#)

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 latest firmware version.

[What is this?](#)

**Settings**

Upgrade policy

Auto upgrade at Monday 02:00 UTC+8.0

Upgrade at 2022-10-11 15:30 UTC+8.0

Upgrade now

Ignore upgrade

Firmware type Stable

---

Switch

**Upgrade available**

[What is this?](#)

**Settings**

Upgrade policy

Auto upgrade at Monday 02:00 UTC+8.0

Upgrade at 2022-10-11 15:30 UTC+8.0

Upgrade now

Ignore upgrade

Firmware type Stable

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.

---

Security Gateway

No devices

[What is this?](#)

---

Mobile Router

No devices

[What is this?](#)

The following table describes the labels in this screen.

Table 84 Site-Wide > Configure > Firmware management > Overview

LABEL	DESCRIPTION																		
Access Point / Switch / Firewall or Security Gateway / Mobile Router																			
Upgrade available	<p>This shows the status of the Nebula Device's firmware in your site.</p> <ul style="list-style-type: none"> <li>• <b>Up to date</b> 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.</li> <li>• <b>Upgrade available</b> is displayed if there is firmware update available for any of the Nebula Device(s) of a particular type in your site. Click <b>Applicable devices</b> to see a table list of your Nebula Device(s) that can receive this upgrade.</li> </ul> <div data-bbox="534 537 1481 884" style="border: 1px solid black; padding: 5px;"> <p><b>Applicable devices</b> <span style="float: right;">X</span></p> <p>Firmware Type: Stable</p> <table border="1" data-bbox="565 680 1450 779"> <thead> <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> </thead> <tbody> <tr> <td>Access point</td> <td>NWA1123-AC HD</td> <td>5C-6A-80-ED-4A-82</td> <td>S172V37001024</td> <td>V6.25(ABIN.4)</td> <td>V6.25(ABIN.6)</td> </tr> <tr> <td>Access point</td> <td>WAX610D</td> <td>B0-CE-1E-D0-FC-CE</td> <td>S2021-36210587</td> <td>V6.30(ABTE.0)</td> <td>V6.30(ABTE.4)</td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Close"/></p> </div> <ul style="list-style-type: none"> <li>• <b>Locked</b> 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.</li> <li>• <b>No devices</b> is displayed if there is no Nebula Device of a particular type (for example, Mobile Router) registered in your site.</li> </ul>	Device type	Model	MAC address	S/N	Current version	Schedule upgrade version	Access point	NWA1123-AC HD	5C-6A-80-ED-4A-82	S172V37001024	V6.25(ABIN.4)	V6.25(ABIN.6)	Access point	WAX610D	B0-CE-1E-D0-FC-CE	S2021-36210587	V6.30(ABTE.0)	V6.30(ABTE.4)
Device type	Model	MAC address	S/N	Current version	Schedule upgrade version														
Access point	NWA1123-AC HD	5C-6A-80-ED-4A-82	S172V37001024	V6.25(ABIN.4)	V6.25(ABIN.6)														
Access point	WAX610D	B0-CE-1E-D0-FC-CE	S2021-36210587	V6.30(ABTE.0)	V6.30(ABTE.4)														

Table 84 Site-Wide &gt; Configure &gt; Firmware management &gt; Overview (continued)

LABEL	DESCRIPTION
Settings	<p>Create a schedule for each Nebula Device type. The following <b>Upgrade policy</b> are available:</p> <ul style="list-style-type: none"> <li>• Select <b>Auto upgrade at</b> 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.</li> <li>• Select <b>Upgrade at</b> 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.</li> </ul> <p>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 <b>Auto upgrade at</b> schedule after performing the firmware update.</p> <ul style="list-style-type: none"> <li>• Select <b>Upgrade now</b> to immediately install the firmware for each Nebula Device type. Then select the <b>Firmware type</b> (<b>Stable</b> or <b>Latest</b> (default)).</li> </ul> <p>Note: This button is selectable only when there is firmware update available. This field's setting will return to its previous setting (<b>Auto upgrade at</b> or <b>Ignore upgrade</b>) after performing the firmware update.</p> <ul style="list-style-type: none"> <li>• Select <b>Ignore upgrade</b> if you choose not to install the firmware.</li> </ul> <p>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 <b>Auto upgrade at</b> is earlier than the mandatory upgrade schedule, then the <b>Auto upgrade at</b> schedule has priority.</p>
Firmware type	<p>Set the type of firmware to be installed for each Nebula Device type.</p> <ul style="list-style-type: none"> <li>• Select <b>Stable</b> to install a firmware that may not have the latest features but has passed Zyxel internal and external testing.</li> <li>• Select <b>Latest</b> to install the most recently release firmware with the latest features, improvements, and bug fixes.</li> <li>• Select <b>General Availability</b> to install a firmware release before <b>Latest</b>, but is still undergoing Zyxel external testing.</li> <li>• Select <b>Dedicated</b> to install the firmware version for Nebula Device issue monitoring by Zyxel support.</li> <li>• Select <b>Beta</b> to install a release version for testing the latest features and is still undergoing Zyxel internal and external testing.</li> </ul> <p>Note: This field is hidden when <b>Ignore upgrade</b> is selected in <b>Settings</b>. We generally recommend updating to the <b>Latest</b> 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 <b>Stable</b> firmware type.</p>

### 7.2.6.2 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 101 Site-Wide > Configure > Firmware management > Devices

Site-wide > Configure > [Firmware management](#)

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

<input type="checkbox"/>	Status	Device type	Model	MAC address	S/N	Current version	Firmware status	Availability	Firmware type	Upgrade sch
<input type="checkbox"/>	<span style="color: green;">●</span>	Switch	NSW100-10P	88EFA37B4C5A	8172112000001	V2.00(ABGO.2)   11/19/2019	Good <span style="color: blue;">i</span>	Upgrade available	Stable	No
<input type="checkbox"/>	<span style="color: red;">●</span>	Access point	WAX510D	095CE579E09E	8192140100451	V6.00(ABTF.0)IT_20221019121600	Custom <span style="color: blue;">i</span>	Upgrade available	General Availability	No
<input type="checkbox"/>	<span style="color: red;">●</span>	Access point	NWA50AX	88EFA37B4C5A	8118120000001	V1.00(ABYW.0)	Warning <span style="color: blue;">i</span>	Upgrade available	General Availability	No
<input type="checkbox"/>	<span style="color: green;">●</span>	Access point	WAX650S	88EFA37B4C5A	8192120000005	V6.50(ABRM.0)b5	Custom <span style="color: blue;">i</span>	Upgrade available	Beta	No
<input type="checkbox"/>	<span style="color: green;">●</span>	Access point	NWA50AX PRO	88EFA37B4C5A	8192151000001	V6.50(ACGE.0)b6	Custom <span style="color: blue;">i</span>	Upgrade available	General Availability	No
<input type="checkbox"/>	<span style="color: red;">●</span>	Access point	NWA90AX PRO	88EFA37B4C5A	8192151000001	V6.50(ACGF.0)b6	Custom <span style="color: blue;">i</span>	Upgrade available	General Availability	No
<input checked="" type="checkbox"/>	<span style="color: green;">●</span>	Access point	WAX620D-6E	1071B31B781C	8192165011741	V6.50(ACCN.0)b5	Custom <span style="color: blue;">i</span>	Upgrade available	General Availability	<span style="color: blue;">📅</span> Every Monday

The following table describes the labels in this screen.

Table 85 Site-Wide > Configure > Firmware management > Devices

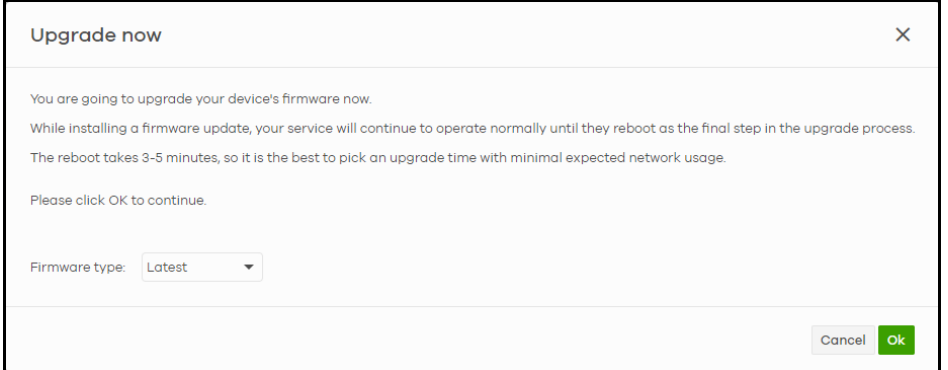
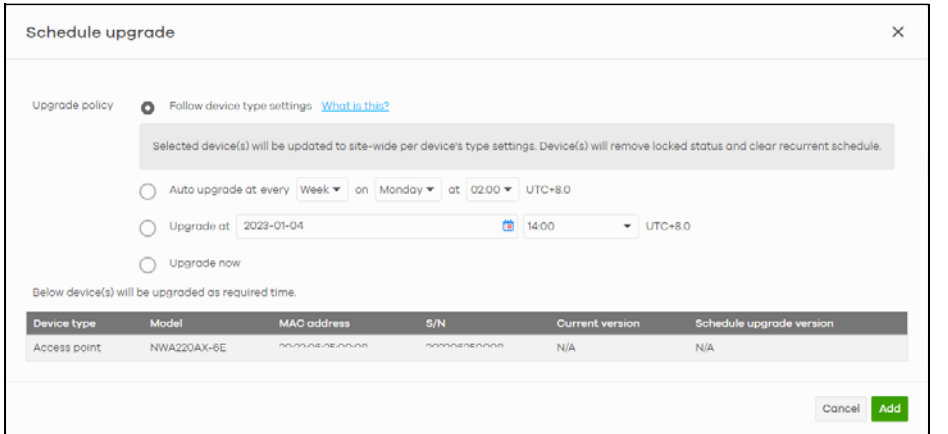

LABEL	DESCRIPTION												
Upgrade Now	<p>Click this to immediately install the firmware on the selected Nebula Devices.</p> <p>This button is selectable only when there is firmware update available for all the selected Nebula Devices.</p> <p>Then, select the <b>Firmware type</b> to be installed.</p> <ul style="list-style-type: none"> <li>• Select <b>Stable</b> to install a firmware that may not have the latest features but has passed Zyxel internal and external testing.</li> <li>• Select <b>Latest</b> to install the most recently release firmware with the latest features, improvements, and bug fixes.</li> </ul> 												
Schedule Upgrade	<p>Click this to pop up a window where you can create a new schedule for the selected Nebula Devices.</p> <p>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.</p> <p>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.</p>  <table border="1" data-bbox="557 1619 1433 1665"> <thead> <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> </thead> <tbody> <tr> <td>Access point</td> <td>NWA220AX-6E</td> <td>XXXXXXXXXX</td> <td>XXXXXXXXXX</td> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Device type	Model	MAC address	S/N	Current version	Schedule upgrade version	Access point	NWA220AX-6E	XXXXXXXXXX	XXXXXXXXXX	N/A	N/A
Device type	Model	MAC address	S/N	Current version	Schedule upgrade version								
Access point	NWA220AX-6E	XXXXXXXXXX	XXXXXXXXXX	N/A	N/A								
Reset	<p>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.</p>												

Table 85 Site-Wide &gt; Configure &gt; Firmware management &gt; Devices (continued)

LABEL	DESCRIPTION
Status	<p>This shows the status of the Nebula Device.</p> <ul style="list-style-type: none"> <li>• Green: The Nebula Device is online and has no alerts.</li> <li>• Amber: The Nebula Device has alerts.</li> <li>• Red: The Nebula Device is offline.</li> <li>• Gray: The Nebula Device has been offline for 7 days or more.</li> </ul>
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 <b>N/A</b> when the Nebula Device goes offline and its firmware version is not available.
Firmware status	<p>The status shows <b>Good</b> 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.</p> <p>The status shows <b>Warning</b> if a newer firmware is available and immediate action is recommended. The newer firmware may contain security enhancements, new features, and performance improvements.</p> <p>The status shows <b>Critical</b> if a newer firmware is available and immediate action is required. The firmware may have security vulnerabilities and/or lack key performance improvements.</p> <p>The status shows <b>Custom</b> if the Nebula Device is running a firmware with specialized features that is not available to the general public.</p> <p>The status changes to <b>Upgrading...</b> after you click <b>Upgrade Now</b> to install the firmware immediately.</p>
Firmware type	<p>This shows <b>Stable</b> when the installed firmware may not have the latest features but has passed Zyxel internal and external testing.</p> <p>This shows <b>Latest</b> when the installed firmware is the most recent release with the latest features, improvements, and bug fixes.</p> <p>This shows <b>General Availability</b> when the installed firmware is a release before <b>Latest</b>, but is still undergoing Zyxel external testing.</p> <p>This shows <b>Dedicated</b> 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.</p> <p>This shows <b>Beta</b> when the installed firmware is a release version for testing the latest features and is still undergoing Zyxel internal and external testing.</p> <p>This shows <b>N/A</b> when the Nebula Device is offline and its firmware status is not available.</p>
Availability	This shows whether the firmware on the Nebula Device is <b>Up to date</b> , there is firmware update available for the Nebula Device ( <b>Upgrade available</b> ), or a specific version of firmware has been installed by Zyxel customer support ( <b>Locked</b> ). Contact Zyxel customer support if you want to unlock the firmware in order to upgrade to a later one.
Upgrade scheduled	<p>This shows the date and time when a new firmware upgrade is scheduled to occur. Otherwise, it shows <b>Follow upgrade time</b> and the Nebula Device sticks to the site-wide schedule or <b>No</b> when the firmware on the Nebula Device is up-to-date or the Nebula Device goes offline and its firmware status is not available.</p> <p>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.</p>

Table 85 Site-Wide &gt; Configure &gt; Firmware management &gt; Devices (continued)

LABEL	DESCRIPTION
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.

## 7.2.7 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 **Site-wide > Configure > Cloud authentication** to access these screen.

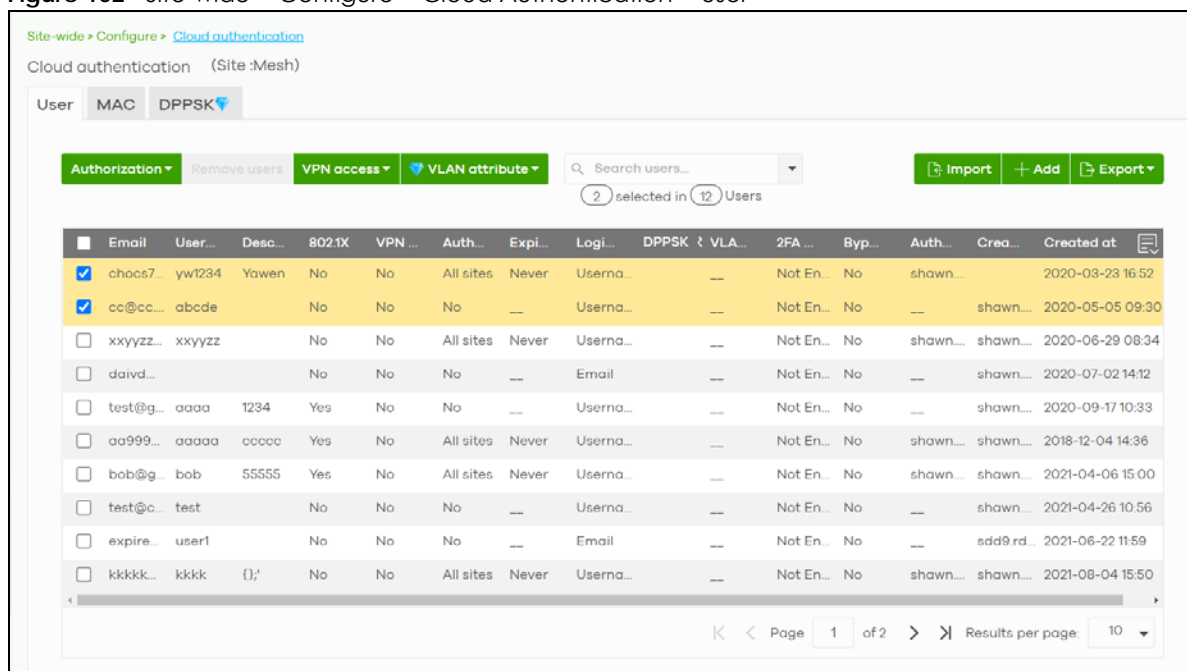
Note: The changes you made in this screen apply only to the current site. To change the cloud authentication settings for all sites in the organization, go to **Organization-wide > Configure > Cloud Authentication** (see [Section 7.2.7 on page 296](#)).

Note: For more information on user account types, see [Section 6.3.5.1 on page 216](#).

### 7.2.7.1 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 102 Site-wide &gt; Configure &gt; Cloud Authentication &gt; User



The screenshot shows the 'User' screen under 'Cloud authentication (Site:Mesh)'. It features a table with columns: Email, User..., Desc..., 802.1X, VPN..., Auth..., Expi..., Logi..., DPPSK, VLA..., 2FA..., Byp..., Auth..., Crea..., and Created at. There are 10 rows of user data, with the first two rows selected. The table is filtered to show 2 users out of 12 total.

<input type="checkbox"/>	Email	User...	Desc...	802.1X	VPN...	Auth...	Expi...	Logi...	DPPSK	VLA...	2FA...	Byp...	Auth...	Crea...	Created at
<input checked="" type="checkbox"/>	chocs7...	yw1234	Yawen	No	No	All sites	Never	Userna...	---	Not En...	No	shawn...	shawn...	2020-03-23 16:52	
<input checked="" type="checkbox"/>	cc@cc...	abcde		No	No	No	---	Userna...	---	Not En...	No	---	shawn...	2020-05-05 09:30	
<input type="checkbox"/>	xyyyzz...	xyyyzz		No	No	All sites	Never	Userna...	---	Not En...	No	shawn...	shawn...	2020-06-29 08:34	
<input type="checkbox"/>	daivd...			No	No	No	---	Email	---	Not En...	No	---	shawn...	2020-07-02 14:12	
<input type="checkbox"/>	test@g...	aaaa	1234	Yes	No	No	---	Userna...	---	Not En...	No	---	shawn...	2020-09-17 10:33	
<input type="checkbox"/>	aa999...	aaaaa	cccc	Yes	No	All sites	Never	Userna...	---	Not En...	No	shawn...	shawn...	2018-12-04 14:36	
<input type="checkbox"/>	bob@g...	bob	55555	Yes	No	All sites	Never	Userna...	---	Not En...	No	shawn...	shawn...	2021-04-06 15:00	
<input type="checkbox"/>	test@c...	test		No	No	No	---	Userna...	---	Not En...	No	---	shawn...	2021-04-26 10:56	
<input type="checkbox"/>	expire...	user1		No	No	No	---	Email	---	Not En...	No	---	sdd9 rd...	2021-06-22 11:59	
<input type="checkbox"/>	kkkkk...	kkkk	{},'	No	No	All sites	Never	Userna...	---	Not En...	No	shawn...	shawn...	2021-08-04 15:50	

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 86 Site-wide &gt; Configure &gt; Cloud Authentication &gt; User

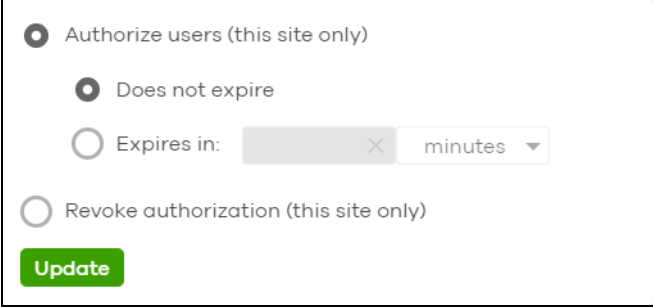
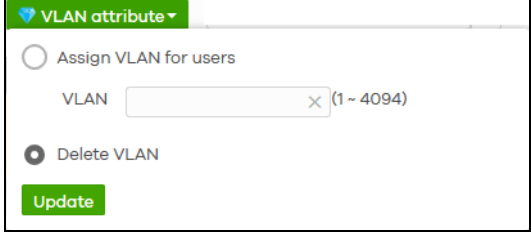

LABEL	DESCRIPTION
Authorization	<p>Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.</p> 
Remove users	<p>Select one or more than one user account and click this button to remove the selected user accounts.</p>
VPN access	<p>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.</p>
VLAN attribute	<p>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 <b>Update</b>.</p> 
Print	<p>Click this button to print information about each selected user account, such as their user name and password.</p>
Search users	<p>Enter a key word as the filter criteria to filter the list of user accounts.</p>
N User	<p>This shows how many user accounts (N) match the filter criteria and how many user accounts of the selected type are created in total.</p>
Import	<p>Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.</p> this template to import'. There is a 'Browse' button and a dashed box for 'Or drag file here...'. There is a 'Close' button at the bottom right." data-bbox="305 705 760 870"/>
Add	<p>Click this button to create a new user account. See <a href="#">Section 7.2.7.2 on page 298</a>.</p>

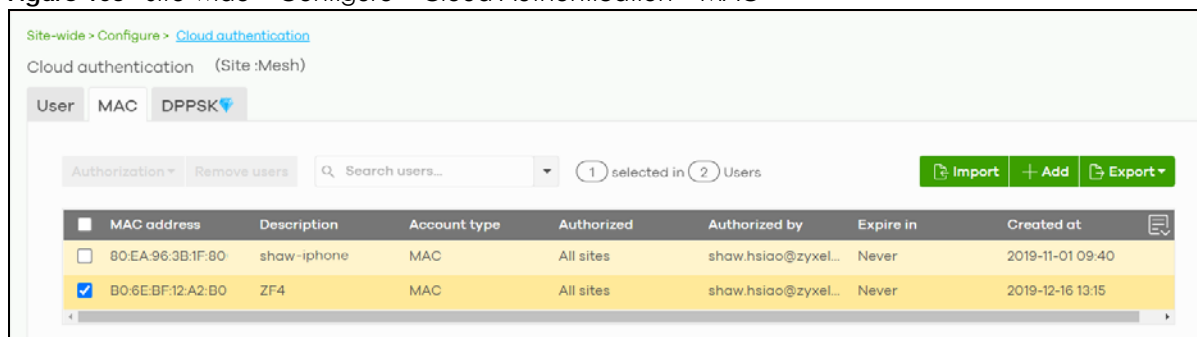
Table 86 Site-wide &gt; Configure &gt; Cloud Authentication &gt; User (continued)

LABEL	DESCRIPTION
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 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 <b>Never</b> if the account never expires. This shows <b>Multiple value</b> if the account has different <b>Expire in</b> 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 <b>User</b> . 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 <b>Multiple value</b> .
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.

### 7.2.7.2 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 103 Site-wide &gt; Configure &gt; Cloud Authentication &gt; MAC



MAC address	Description	Account type	Authorized	Authorized by	Expire in	Created at
<input type="checkbox"/> 80:EA:96:3B:1F:80	shaw-iphone	MAC	All sites	shaw.hsiao@zyxel...	Never	2019-11-01 09:40
<input checked="" type="checkbox"/> 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 87 Site-wide &gt; Configure &gt; Cloud Authentication &gt; MAC


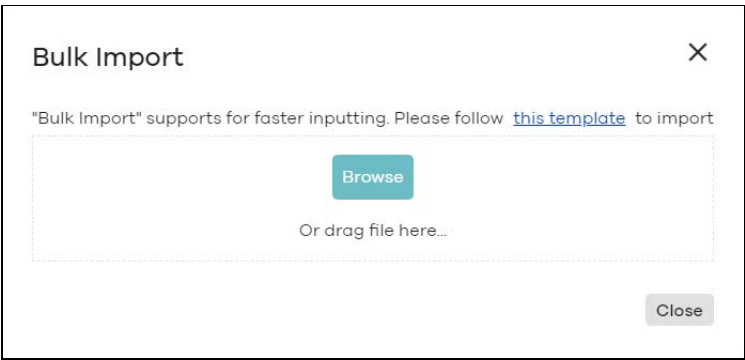

LABEL	DESCRIPTION
Authorization	<p>Select one or more than one account and click this button to configure the authorization settings for the selected user accounts.</p> 
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
Search users	Enter 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	<p>Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.</p> 
Add	Click this button to create a new user account. See <a href="#">Section 7.2.7.3 on page 300</a> .
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.
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	<p>This shows the email address of the administrator account that authorized the user.</p> <p>If the account has been authorized by different administrators across different sites, it shows <b>Multiple value</b>.</p>
Expire in (UTC)	<p>This shows the date and time that the account expires.</p> <p>This shows -- if authentication is disabled for this account.</p> <p>This shows <b>Never</b> if the account never expires.</p> <p>This shows <b>Multiple value</b> if the account has different <b>Expire in</b> values across different sites.</p>

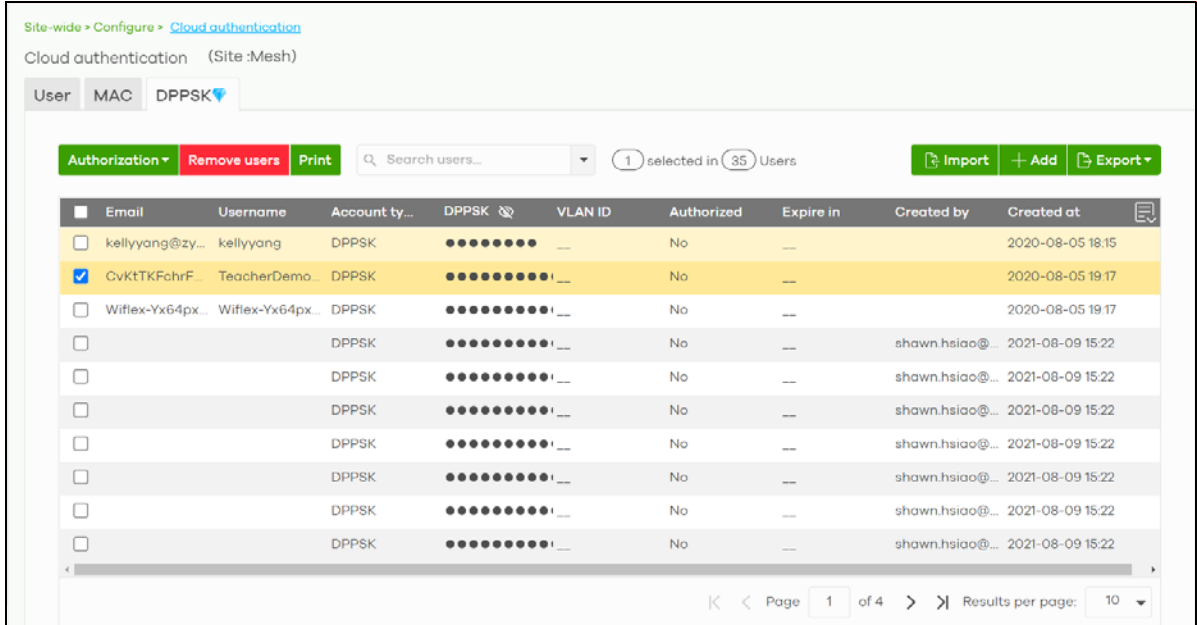
Table 87 Site-wide > Configure > Cloud Authentication > MAC (continued)

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.

### 7.2.7.3 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 104 Site-wide > Configure > Cloud Authentication > DPPSK



The following table describes the labels in this screen.

Table 88 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. <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <input checked="" type="radio"/> Authorize users (this site only)                     <ul style="list-style-type: none"> <li><input checked="" type="radio"/> Does not expire</li> <li><input type="radio"/> Expires in: <input type="text" value=""/> minutes</li> </ul> <input type="radio"/> Revoke authorization (this site only)                     <div style="text-align: right; margin-top: 10px;"><b>Update</b></div> </div>
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.

Table 88 Site-wide &gt; Configure &gt; Cloud Authentication &gt; DPPSK (continued)

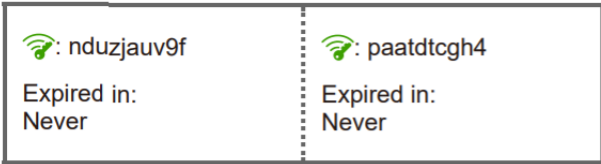

LABEL	DESCRIPTION
Print	<p>Click this button to print the unique dynamic personal pre-shared key (DPPSK) and expiry time of each selected user account.</p> <p>The account details can be cut into cards, and then given to users in order to grant them WiFi network access.</p> <div data-bbox="521 436 1118 653" style="text-align: center; border: 1px solid black; padding: 10px;"> <p>DPPSK</p>  </div>
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	<p>Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.</p> <div data-bbox="495 856 1235 1205" style="border: 1px solid black; padding: 10px;"> <p><b>Bulk Import</b> <span style="float: right;">✕</span></p> <p>"Bulk Import" supports for faster inputting. Please follow <a href="#">this template</a> to import</p> <div style="text-align: center; border: 1px dashed gray; padding: 10px; margin: 10px 0;"> <p><span style="background-color: #00a651; color: white; padding: 5px 15px; border-radius: 3px;">Browse</span></p> <p>Or drag file here...</p> </div> <p style="text-align: right;"><span style="background-color: #ccc; padding: 2px 10px; border-radius: 3px;">Close</span></p> </div>
Add	<p>Click this button to create a single new account, or a batch of accounts.</p> <ul style="list-style-type: none"> <li>• Single DPPSK: See <a href="#">Section 6.3.5.7 on page 225</a>.</li> <li>• Batch create DPPSK: See <a href="#">Section 6.3.5.8 on page 226</a>.</li> </ul>
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 (UTC)	<p>This shows the date and time that the account expires.</p> <p>This shows -- if authentication is disabled for this account.</p> <p>This shows <b>Never</b> if the account never expires.</p> <p>This shows <b>Multiple value</b> if the account has different <b>Expire in</b> values across different sites.</p>
Created by	This shows the email address of the administrator account that created the user.

Table 88 Site-wide &gt; Configure &gt; Cloud Authentication &gt; 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.

---

# PART IV

## Manage by Device Type

---

# CHAPTER 8

## Mobile Router

### 8.1 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**.

### 8.2 Configuration

From the navigation panel, click **Mobile router** and the following screen appears. The **Mobile router > 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 105 Mobile Router > Configuration (Indoor)

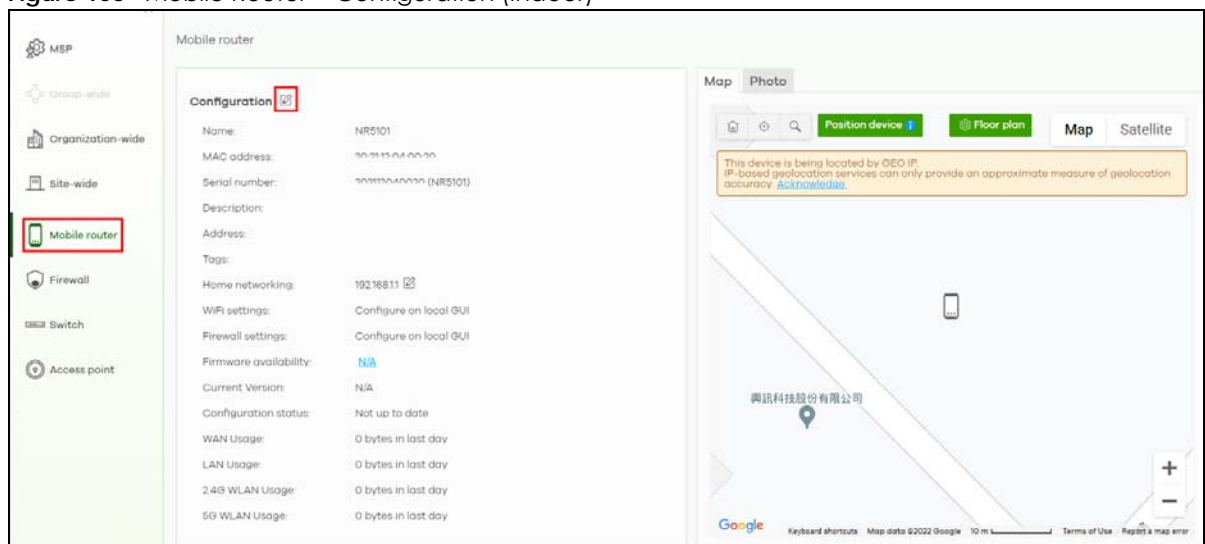




Figure 106 Mobile Router &gt; Configuration (Outdoor)



## 8.2.1 Configuration: Edit

The following screen displays after you click the edit icon. Use the **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 107 Mobile Router &gt; Configuration: Edit

The following table describes the labels in this screen.

Table 89 Mobile Router > Configuration: Edit

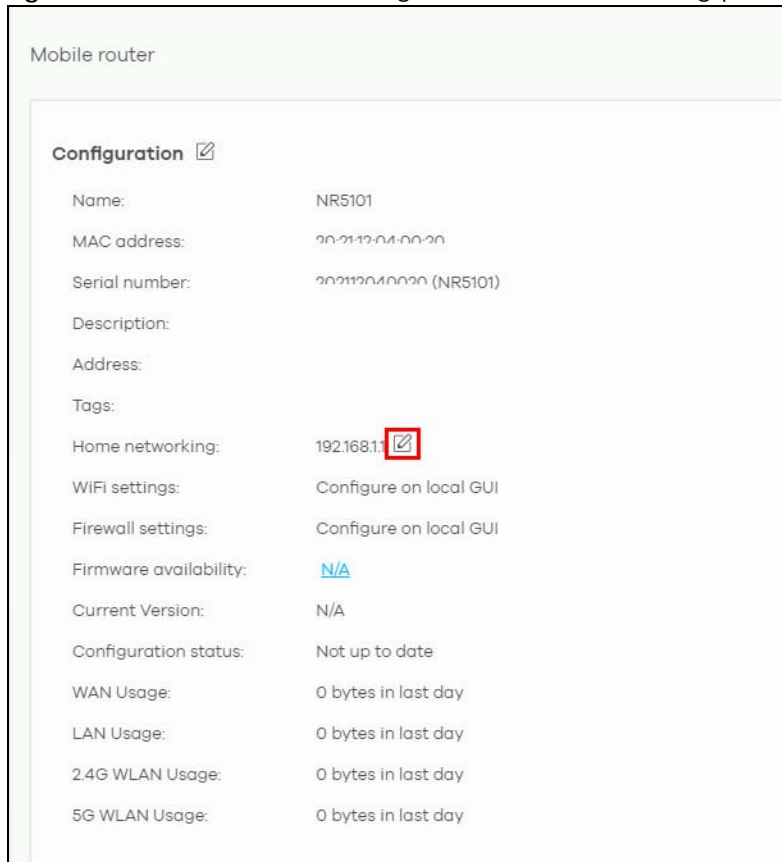
LABEL	DESCRIPTION
Configuration	
Name	Enter a descriptive name for the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
Serial number	This shows the serial number of the Nebula Device.
Description	Enter a user-specified description for the Nebula Device.
Tags	Enter a user-specified tag for the Nebula Device.
Address	Enter a user-specified address for the Nebula Device.
Save	Click <b>Save</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 8.2.2 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 108 Mobile Router > Configuration: Home networking (Indoor)



The following **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 109 Mobile Router &gt; Configuration &gt; Home networking: Edit

The following table describes the labels in this screen.

Table 90 Mobile Router &gt; Configuration &gt; 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 <b>Subnet mask</b> . 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: <b>Infinite</b> – select this if IP addresses never expire; <b>days, hours, minutes</b> – select this to enter how long IP addresses are valid.
Close	Click <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.

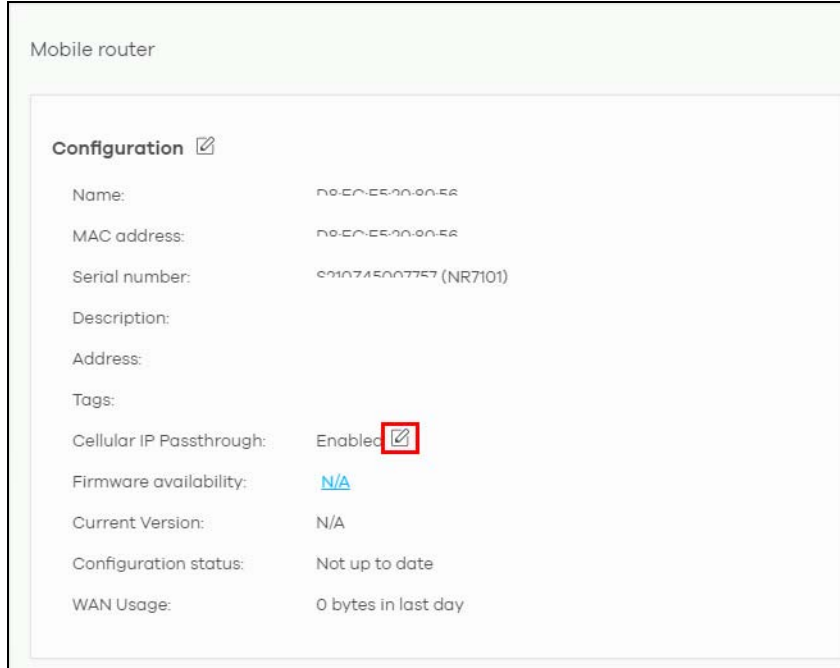
### 8.2.3 Cellular IP Passthrough

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.

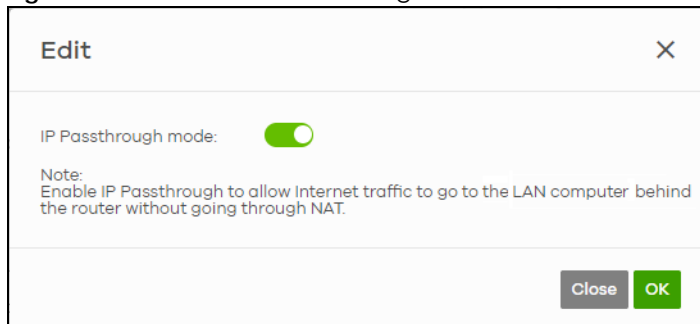
Note: As of this writing, cellular IP passthrough is for NR7101 and LTE7461 only.

**Figure 110** Mobile Router > Configuration: Cellular IP Passthrough (Outdoor)



The following **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 111** Mobile Router > Configuration > Cellular IP Passthrough: Edit



The following table describes the labels in this screen.

Table 91 Mobile Router > Configuration > Cellular IP Passthrough: Edit

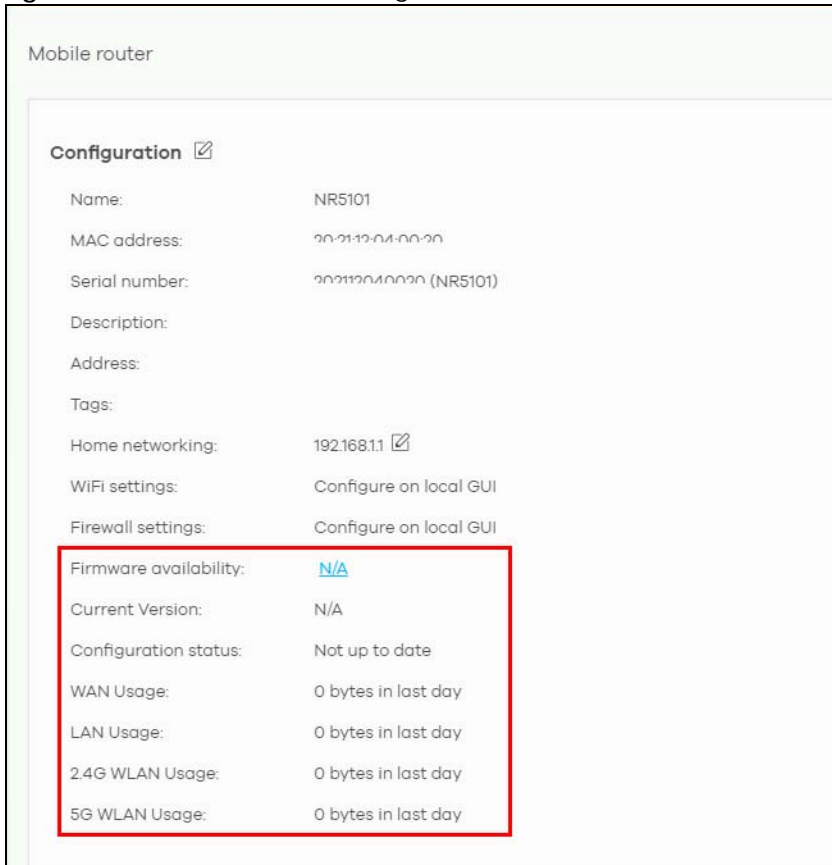
LABEL	DESCRIPTION
IP Passthrough mode	This displays if IP passthrough is enabled on the Nebula Device.
Close	Click <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.

## 8.2.4 Firmware Status

Go back to the **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 112** Mobile Router > Configuration > Firmware status



The following table describes the labels in this screen.

Table 92 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 <b>Firmware availability</b> field to go to the <b>Site-wide &gt; Configure &gt; Firmware management</b> screen and configure your Firmware management settings.
Current Version	This shows the firmware version currently installed on the Nebula Device.

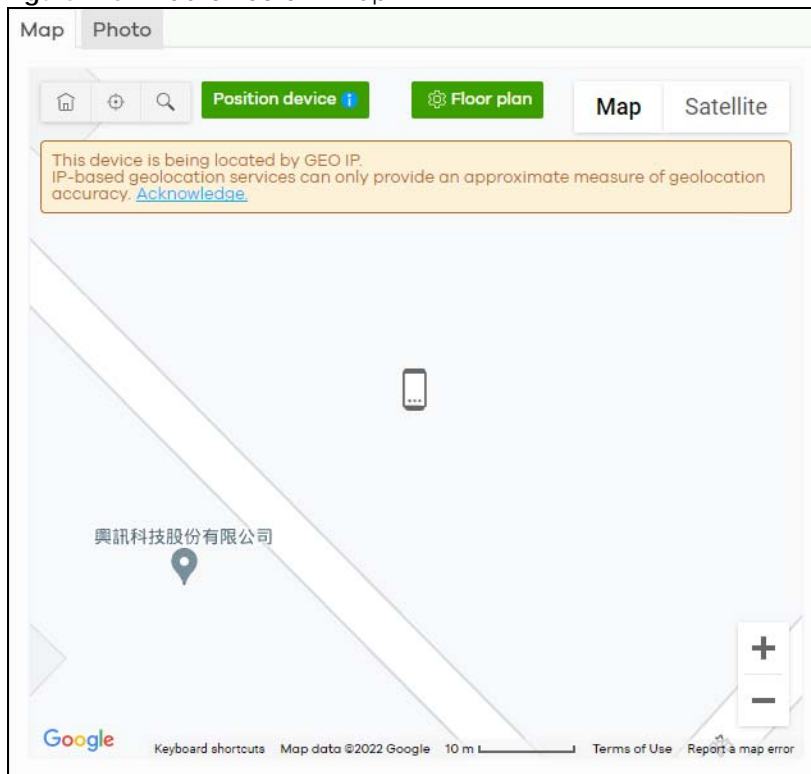
Table 92 Mobile Router &gt; Configuration &gt; Firmware status (continued)

LABEL	DESCRIPTION
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 (uplink/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.

## 8.3 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 113 Mobile Router &gt; Map



The following table describes the labels in this screen.

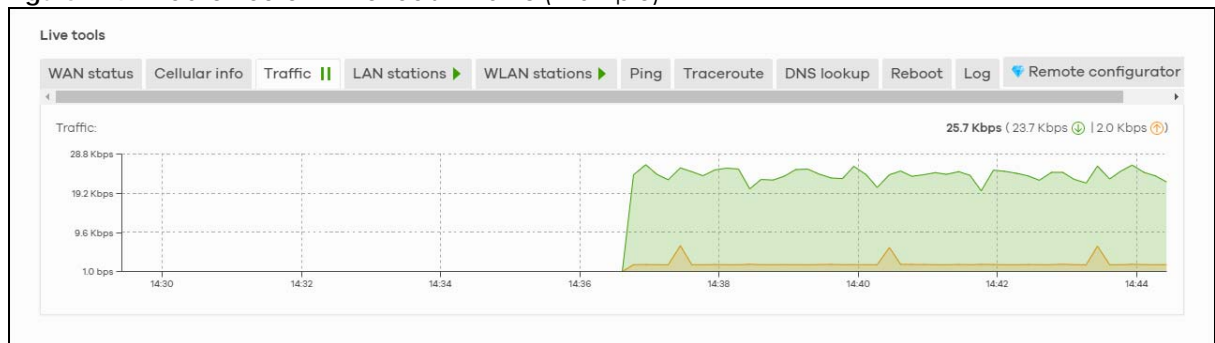
Table 93 Mobile Router > Map/Photo



LABEL	DESCRIPTION
Map	<p>This shows the location of the Nebula Device on Google Maps (<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).</p> <div data-bbox="537 485 1216 919" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><b>Position device</b> <span style="float: right;">✕</span></p> <p>Update my device's location. <a href="#">What is this?</a></p> <p><input checked="" type="radio"/> Use the device's IP address (GEO IP).</p> <p><input type="radio"/> Get my location from web browser.</p> <p><input type="radio"/> Use the following address or coordinates.</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <input type="text"/> <span style="float: right;">✕</span> </div> <p style="text-align: right;"> <input type="button" value="Cancel"/> <input type="button" value="Update"/> </p> </div> <ul style="list-style-type: none"> <li>Select <b>GEO IP</b> to use the public IP address of the Nebula Device.</li> <li>Select <b>Get my location from web browser</b> to use the public IP address of the computer accessing the NCC portal.</li> <li>Select <b>Use the following address or coordinates</b> to enter the complete address or coordinates of the Nebula Device.</li> </ul> <p>Note: Nebula Devices that are offline cannot use GEO IP.</p>
Photo	<p>This shows the photo of the Nebula Device. Click <b>Add</b> to upload up to five photos of your Nebula Device. Click the remove icon (🗑️) to delete a photo.</p>

## 8.4 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 114 Mobile Router > Live tools > Traffic (Example)



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.

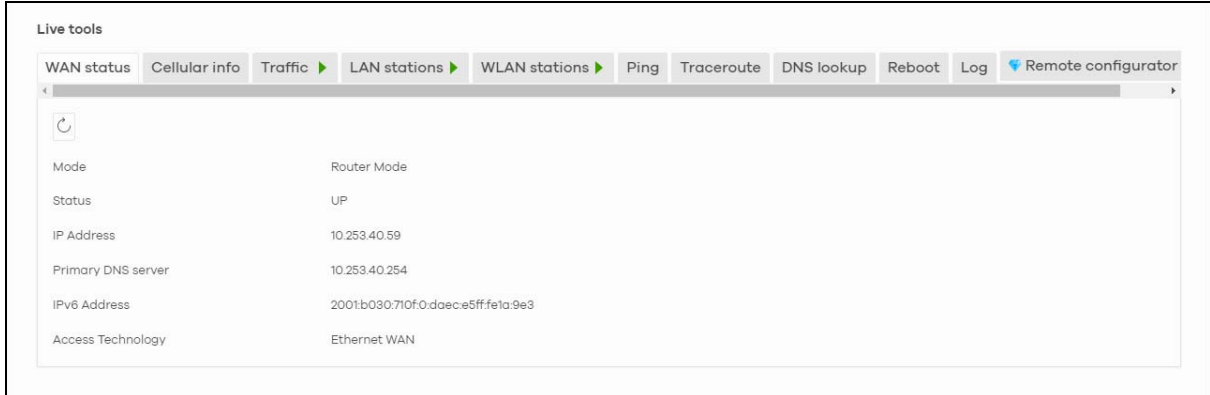
Table 94 Mobile Router > Live tools

LABEL	DESCRIPTION
WAN Status	This shows the connection status of the Ethernet WAN interface. See <a href="#">Section 8.4.1 on page 312</a> for more information.
Cellular info	This shows the connection status of the cellular WAN interface. See <a href="#">Section 8.4.2 on page 313</a> 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' <b>MAC address</b> and <b>IPv4 Address</b> .
WLAN stations (indoor NCCs only)	This shows the Nebula Device's connected WiFi clients' <b>MAC address</b> , <b>SSID name</b> , <b>IPv4 address</b> , <b>Signal strength</b> , <b>Security</b> , <b>Channel</b> , <b>Tx rate</b> , <b>Rx rate</b> , <b>Tx/Rx</b> , and <b>Capability</b> . See <a href="#">Section 8.4.4 on page 320</a> 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 <b>Ping</b> .  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 <b>Run</b> . This determines the path a packet takes to the specified computer.
DNS lookup	Enter a host domain name and click <b>Run</b> to resolve the IP address for the specified domain name.
Reboot	Click this button to restart the Nebula Device.
Log	Select this to display <b>System log</b> and <b>Security log</b> entries in the past 24 hours.
Remote configurator	Click <b>Establish</b> 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 <b>Ok</b> , NCC will provide a remote connection IPv4 address and service port number. For example, <a href="https://63.35.218.205:31479">https://63.35.218.205:31479</a> . 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 <b>Port 443</b> .  Note: <b>Remote configuration</b> is only available if the Nebula Device is running the latest firmware. Otherwise, <b>Device firmware is not up to date, please update it.</b> will appear when you click <b>Establish</b> .

## 8.4.1 WAN Status


Go to the **Mobile router > Live tools > WAN status** screen to view the Ethernet WAN status of the Nebula Device.



**Figure 115** Mobile Router > Live tools > WAN status

The following table describes the labels in this screen.

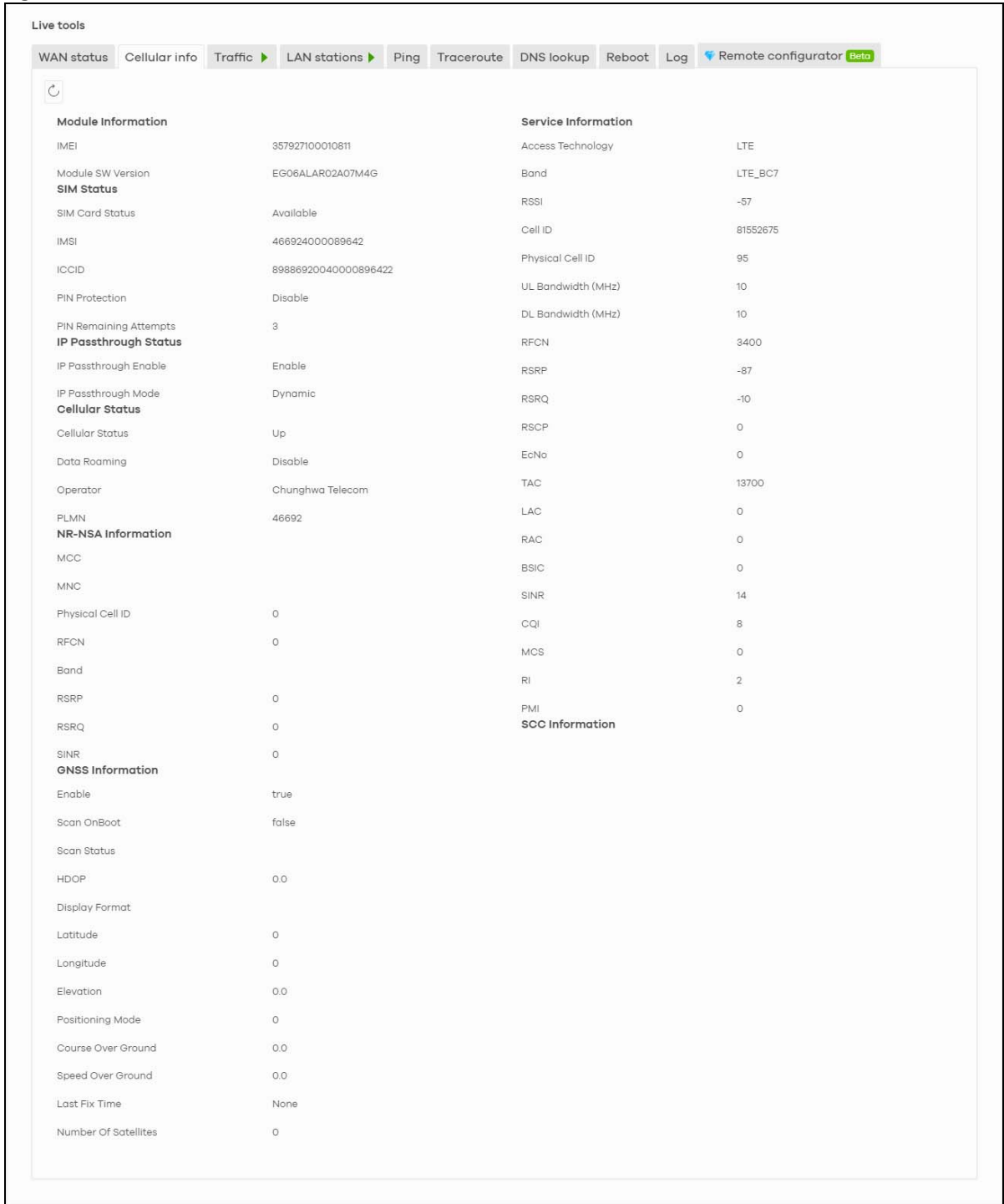
**Table 95** Mobile Router > Live tools > WAN status

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.

## 8.4.2 Cellular Info

Go to the **Mobile router > Live tools > Cellular Info** screen to view the cellular WAN status of the Nebula Device.

Figure 116 Mobile Router > Live tools > Cellular Info



The following table describes the labels in this screen.

Table 96 Mobile Router > Live tools > Cellular Info

LABEL	DESCRIPTION
Module Information	
IMEI	This shows the International Mobile Equipment Identity of the Nebula Device.

Table 96 Mobile Router &gt; Live tools &gt; 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:  <b>None</b> – the Nebula Device does not detect that there is a SIM card inserted. <b>Available</b> – the SIM card could either have or does not have PIN code security. <b>Locked</b> – the SIM card has PIN code security, but you did not enter the PIN code yet. <b>Blocked</b> – 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. <b>Error</b> – 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 <b>Enable</b> if <b>PIN Protection</b> is enabled. Otherwise, this field shows <b>Disable</b> .
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 <b>Dynamic</b> 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 <b>Fixed</b> 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 96 Mobile Router &gt; Live tools &gt; Cellular Info (continued)

LABEL	DESCRIPTION
RFCN	<p>This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Nebula Device is connecting.</p> <p>The value depends on the type of the mobile network (such as LTE, UMTS, GSM) to which the Nebula Device is connecting:</p> <ul style="list-style-type: none"> <li>• For UMTS (3G), it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101.</li> <li>• 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.</li> </ul>
Band	This displays the current cellular band of your Nebula Device.
RSRP	<p>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.</p> <p>The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214.</p> <p>The reporting range is specified in 3GPP-TS.36.133.</p> <p>An undetectable signal is indicated by the lower limit, example -140 dBm.</p> <p>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.</p>
RSRQ	<p>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.</p> <p>The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214.</p> <p>An undetectable signal is indicated by the lower limit, example -240.</p> <p>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.</p>
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	<p>This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Nebula Device is connecting.</p> <p>The value depends on the Current Access Technology:</p> <ul style="list-style-type: none"> <li>• For GPRS, it is the Cell Identity as specified in 3GPP-TS.25.331.</li> <li>• For UMTS, it is the Cell Identity as defined in SIB3 3GPP-TS.25.331, 3GPP-TS.24.008.</li> <li>• For LTE/5G, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331.</li> </ul> <p>The value is '0' (zero) or 'N/A' if there is no network connection.</p>
Physical Cell ID	This displays the Physical Cell ID (PCI) of the SCC.

Table 96 Mobile Router &gt; Live tools &gt; Cellular Info (continued)

LABEL	DESCRIPTION
UL Bandwidth (MHz)	<p>This shows the uplink cellular channel bandwidth from the Nebula Device to the base station.</p> <p>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.</p>
DL Bandwidth (MHz)	<p>This shows the downlink cellular channel bandwidth from the base station to the Nebula Device.</p> <p>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.</p>
RFCN	<p>This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Nebula Device is connecting.</p> <p>The value depends on the type of the mobile network (such as LTE, UMTS, GSM) to which the Nebula Device is connecting:</p> <ul style="list-style-type: none"> <li>• For UMTS (3G), it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101.</li> <li>• For LTE/5G, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101.</li> </ul> <p>The value is '0' (zero) or 'N/A' if there is no network connection.</p>
RSRP	<p>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.</p> <p>The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214.</p> <p>The reporting range is specified in 3GPP-TS.36.133.</p> <p>An undetectable signal is indicated by the lower limit, example -140 dBm.</p> <p>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.</p>
RSRQ	<p>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.</p> <p>The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214.</p> <p>An undetectable signal is indicated by the lower limit, example -240.</p> <p>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.</p>
RSCP	<p>This displays the Received Signal Code Power, which measures the power of channel used by the Nebula Device.</p> <p>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.</p> <p>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.</p>
EcNo	<p>This displays the ratio (in dB) of the received energy per chip and the interference level.</p> <p>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.</p> <p>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.</p>



Table 96 Mobile Router &gt; Live tools &gt; Cellular Info (continued)

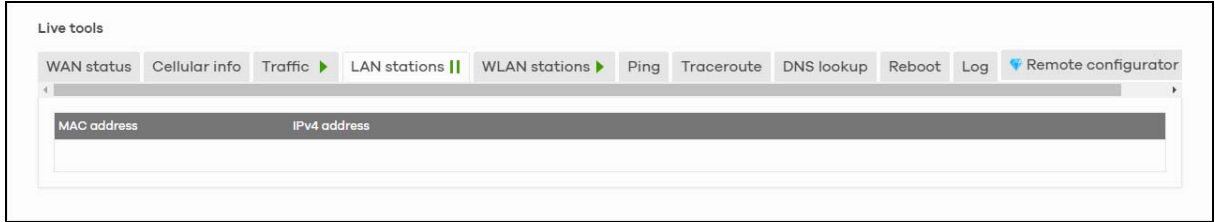
LABEL	DESCRIPTION
TAC	<p>This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber.</p> <p>The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101.</p> <p>This parameter is for LTE only. The value is '0' (zero) or 'N/A' if the Current Access Technology is not LTE or there is no network connection.</p>
LAC	<p>This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN.</p> <p>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].</p> <p>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.</p>
RAC	<p>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.</p> <p>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.</p> <p>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].</p> <p>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.</p>
BSIC	<p>The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station.</p> <p>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.</p>
SINR	<p>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.</p>
CQI	<p>This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good or bad the communication channel quality is.</p>
MCS	<p>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.</p>
RI	<p>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.</p>
PMI	<p>This displays the Precoding Matrix Indicator (PMI).</p> <p>PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer).</p> <p>PMI determines how cellular data are encoded for the antennas to improve downlink rate.</p>
SCC Information	<p>If the cellular service provider supports carrier aggregation (CA), then this section displays statistics for the connection's secondary component carriers (SCCs).</p>
GNSS Information	<p>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, you can easily locate the Nebula Device with accurate information.</p>

Table 96 Mobile Router &gt; Live tools &gt; Cellular Info (continued)

LABEL	DESCRIPTION
Enable	This shows if GNSS is enabled.  Note: This can only be configured by a qualified service technician.
Scan OnBoot	This shows Enable if Scan OnBoot is enabled, so that GNSS runs automatically after the Nebula Device is turned on.  Note: This can only be configured by a qualified service technician.
Scan Status	This shows GNSS error codes for debugging by a qualified service technician.
HDOP	Horizontal Dilution of Precision (HDOP) shows how accurate data collected by the Nebula Device is according to the current satellite configuration. A smaller value of HDOP means a higher precision.
Display Format	This shows the latitude and longitude display modes. There are three modes: 0, 1, and 2. Below are examples for these modes shown in latitude/longitude.  0 – ddmm.mmmmN/S, dddmm.mmmmE/W 1 – ddmm.mmmmmm, N/S, dddmm.mmmmmm, E/W 2 – (-)dd.ddddd, (-)ddd.ddddd N/S/E/W: North/South/East/West “-” : Negative values refer to South latitude/West longitude respectively. Positive values refer to North latitude/East longitude respectively.
Latitude	This shows the latitude coordinate of the Nebula Device. These positioning values (latitude, longitude, and altitude) help you locate the Nebula Device accurately.
Longitude	This shows the longitude coordinate of the Nebula Device.
Elevation	This shows the altitude of the Nebula Device above sea level in meters.
Positioning Mode	This shows the GNSS positioning mode. 2D ("2") GNSS positioning mode displays latitude and longitude coordinates; 3D ("3") 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.

### 8.4.3 LAN Stations

Go to the **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 117** Mobile Router > Live tools > LAN stations

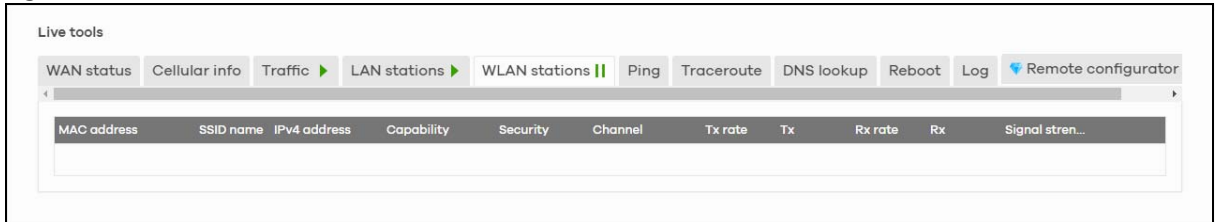
The following table describes the labels in this screen.

**Table 97** 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.

## 8.4.4 WLAN Stations

Go to the **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 118** Mobile Router > Live tools > WLAN stations

The following table describes the labels in this screen.

**Table 98** Mobile Router > Live tools > WLAN stations

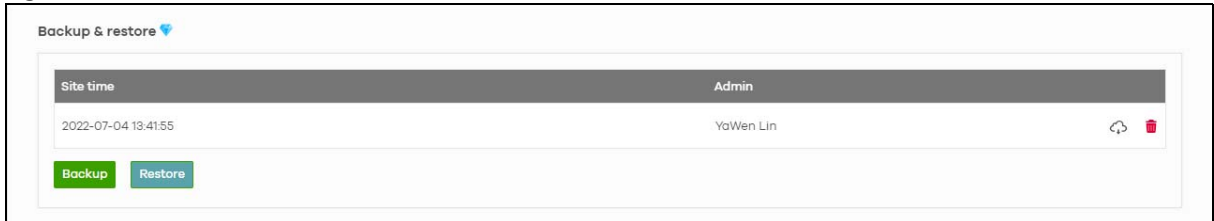
LABEL	DESCRIPTION
MAC address	This field displays the MAC address of an associated WiFi station.
SSID name	This is the descriptive name used to identify the Nebula Device in a WiFi network.
IPv4 address	This indicate the IPv4 address of the gateway that helps forward this route's traffic.
Capability	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.



## 8.5 Backup & Restore

Use the **Mobile router > Backup & restore** screen to back up your configuration settings to the cloud or restore your current setting to the backup configuration.

**Figure 119** Mobile Router > Backup & restore



The following table describes the labels in this screen.

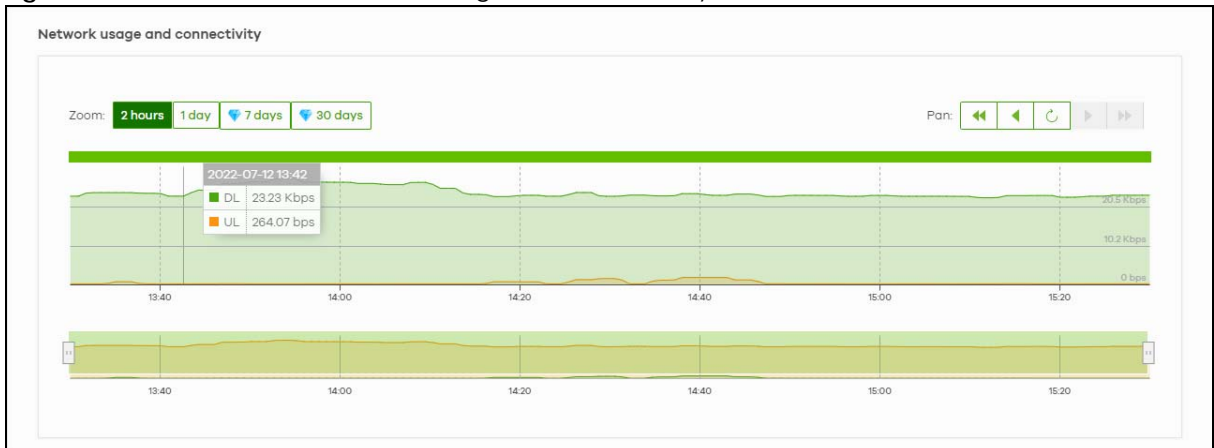
**Table 99** Mobile Router > Backup & restore

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.

## 8.6 Network Usage and Connectivity

Go to the **Mobile router > Network usage and connectivity** screen and then move the cursor to see the transmission rate (uplink/downlink) of a specific time.

**Figure 120** Mobile Router > Network usage and connectivity



The following table describes the labels in this screen.

Table 100 Mobile Router > Network usage and connectivity

LABEL	DESCRIPTION
Network usage and connectivity	Move the cursor over the chart to see the transmission rate at a specific time.
Zoom	Select a time period to view the statistics in the past 2 hours, day, week, or month.
Pan	Use this to move backward or forward by one day or a week.

# CHAPTER 9

## Firewall

### 9.1 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.

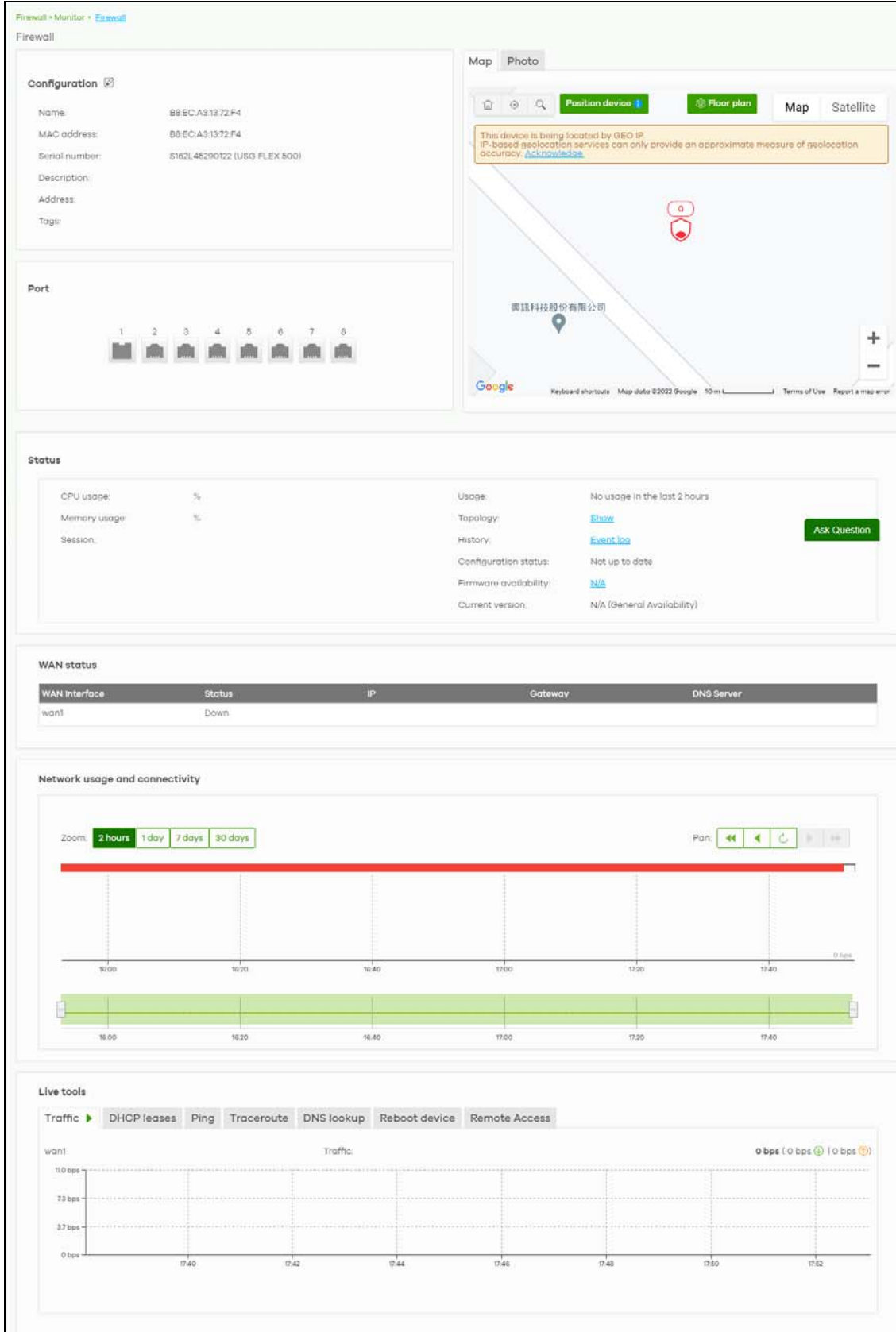
### 9.2 Monitor

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 Firewall

This screen allows you to view the detailed information about the Nebula Device in the selected site. Click **Firewall > Monitor > Firewall** to access this screen.

Figure 121 Firewall > Monitor > Firewall



The following table describes the labels in this screen.

Table 101 Firewall &gt; Monitor &gt; 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	<p>This shows the ports on the Nebula Device.</p> <p>The port is highlighted in green color when it is connected and the link is up.</p> <p>Move the pointer over a port to see additional port information, such as its name, connection status, MAC address, and connection speed.</p>
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	<p>This shows the location of the Nebula Device on Google Maps (<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).</p> <div data-bbox="537 1104 1214 1545" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: right;"><b>Position device</b> <span style="float: right;">✕</span></p> <hr/> <p>Update my device's location. <a href="#">What is this?</a></p> <p><input checked="" type="radio"/> Use the device's IP address (GEO IP).</p> <p><input type="radio"/> Get my location from web browser.</p> <p><input type="radio"/> Use the following address or coordinates.</p> <div style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <input style="width: 90%; border: none;" type="text"/> <span style="float: right; font-size: 0.8em;">✕</span> </div> <p style="text-align: right;"> <input type="button" value="Cancel"/> <input style="background-color: #28a745; color: white; padding: 2px 10px;" type="button" value="Update"/> </p> </div> <ul style="list-style-type: none"> <li>Select <b>GEO IP</b> to use the public IP address of the Nebula Device.</li> <li>Select <b>Get my location from web browser</b> to use the public IP address of the computer accessing the NCC portal.</li> <li>Select <b>Use the following address or coordinates</b> to enter the complete address or coordinates of the Nebula Device.</li> </ul> <p>Note: Nebula Devices that are offline cannot use GEO IP.</p>
Photo	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.
Status	

Table 101 Firewall &gt; Monitor &gt; 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 <b>Show</b> to go to the <b>Site-Wide &gt; Monitor &gt; Topology</b> screen. See <a href="#">Section 7.1.7 on page 266</a> .
History	Click <b>Event log</b> to go to the <b>Firewall &gt; Monitor &gt; Event log</b> screen.
Configuration status	This shows whether the configuration on the Nebula Device is <b>Up-to-date</b> .
Firmware availability	This shows whether the firmware installed on the Nebula Device is <b>Up-to-date</b> .
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 <b>Ping</b> . You can select the interface (WAN, LAN, or VLAN) through which the Security Firewall sends queries for ping.  Note: <ul style="list-style-type: none"> <li>To ping for VPN/routing issues, it is not necessary to connect an end-device on the LAN interface of the Nebula Device.</li> <li>A routing problem is possible if the WAN interface can reach the Internet but not the LAN interface.</li> </ul>
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 <b>Run</b> to resolve the IP address for the specified domain name.

Table 101 Firewall &gt; Monitor &gt; Firewall (continued)

LABEL	DESCRIPTION
Reboot device	Click the <b>Reboot</b> 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 <b>Port</b> number and clicking <b>Establish</b> .

## 9.2.2 Clients

This menu item redirects to **Site-Wide > Monitor > Clients**, with type set to **Security gateway clients**. For details, see [Section 7.1.2 on page 255](#).

## 9.2.3 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 **Firewall > Monitor > Event log** to access this screen.

Figure 122 Firewall &gt; Monitor &gt; Event log

The screenshot displays the 'Event log' interface. At the top, there are search filters: 'Keyword: Any', 'Category: Any', and a time range set to 'Before 2022-08-29 11:50 UTC+8'. A green 'Search' button is on the right. Below the filters, there are navigation buttons for 'Newer', 'Older', and 'Export'. The main area contains a table of event logs with the following columns: Time, Category, Source IP, Source port, Destination IP, Destination port, and Detail. The table lists several events, including Myzyxel Dot Com uploads, System Monitoring, and DHCP operations. The bottom of the interface shows pagination: 'Page 1 of 2' and 'Results per page: 10'.

Time	Category	Source IP	Source port	Destination IP	Destination port	Detail
2022-08-29 11:36:52	Myzyxel Dot Com					[SecuReporter] Upload fail when https post. Server response:401/40101/The r
2022-08-29 11:16:52	Myzyxel Dot Com					[SecuReporter] Upload fail when https post. Server response:401/40101/The r
2022-08-29 11:07:28	System Monitoring					hostname=usgflex100,modelname=USG FLEX 100,firmwareversion=V5.30(AB
2022-08-29 11:06:52	Myzyxel Dot Com					[SecuReporter] Upload fail when https post. Server response:401/40101/The r
2022-08-29 11:02:24	DHCP					Requested 192.168.3.47 from NSW100(B8:EC:A3:10:45:A6)
2022-08-29 11:02:24	DHCP					DHCP server assigned 192.168.3.47 to NSW100(B8:EC:A3:10:45:A6)
2022-08-29 11:02:21	DHCP					DHCP server offered 192.168.3.47 to NSW100(B8:EC:A3:10:45:A6)
2022-08-29 11:02:17	DHCP					DHCP released 192.168.3.47 with NSW100(B8:EC:A3:10:45:A6)
2022-08-29 10:59:41	Myzyxel Dot Com					[SecuReporter] Upload fail when https post. Server response:401/40101/The r
2022-08-29 10:57:30	Myzyxel Dot Com					[SecuReporter] An SSL error has occurred and a secure connection to the se

## 9.2.4 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 9.3.5 on page 350](#) for more information.

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

**Figure 123** Firewall > Monitor > VPN connections

The screenshot shows the 'VPN connections' page. At the top, there is a breadcrumb 'Firewall > Monitor > VPN connections' and a refresh button. Below this is a 'Connection status' section with a 'Configuration' field showing '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'. The 'Site connectivity' section contains a table with columns: Location, Subnet, Status, Inbound, Outbound, Tunnel Up Time, and Last Heartbeat. Below this is the 'Non-Nebula VPN peers connectivity' section with a similar table. The 'Remote AP VPN' section has a table with columns: Name, Status, Inbound, Outbound, Tunnel Up Time, and Last Heartbeat. Finally, the 'Client to site VPN login account' section has a table with columns: User Name, Hostname, Assigned IP, and Public IP.

The following table describes the labels in this screen.

Table 102 Firewall > Monitor > 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 <b>VPN usage and connectivity</b> 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 <b>Firewall &gt; Configure &gt; Site-to-Site VPN</b> screen, where you can modify the VPN settings.
Subnet	This shows the address of the local networks behind the Non-Nebula peer gateway.



Table 102 Firewall &gt; Monitor &gt; VPN connections (continued)

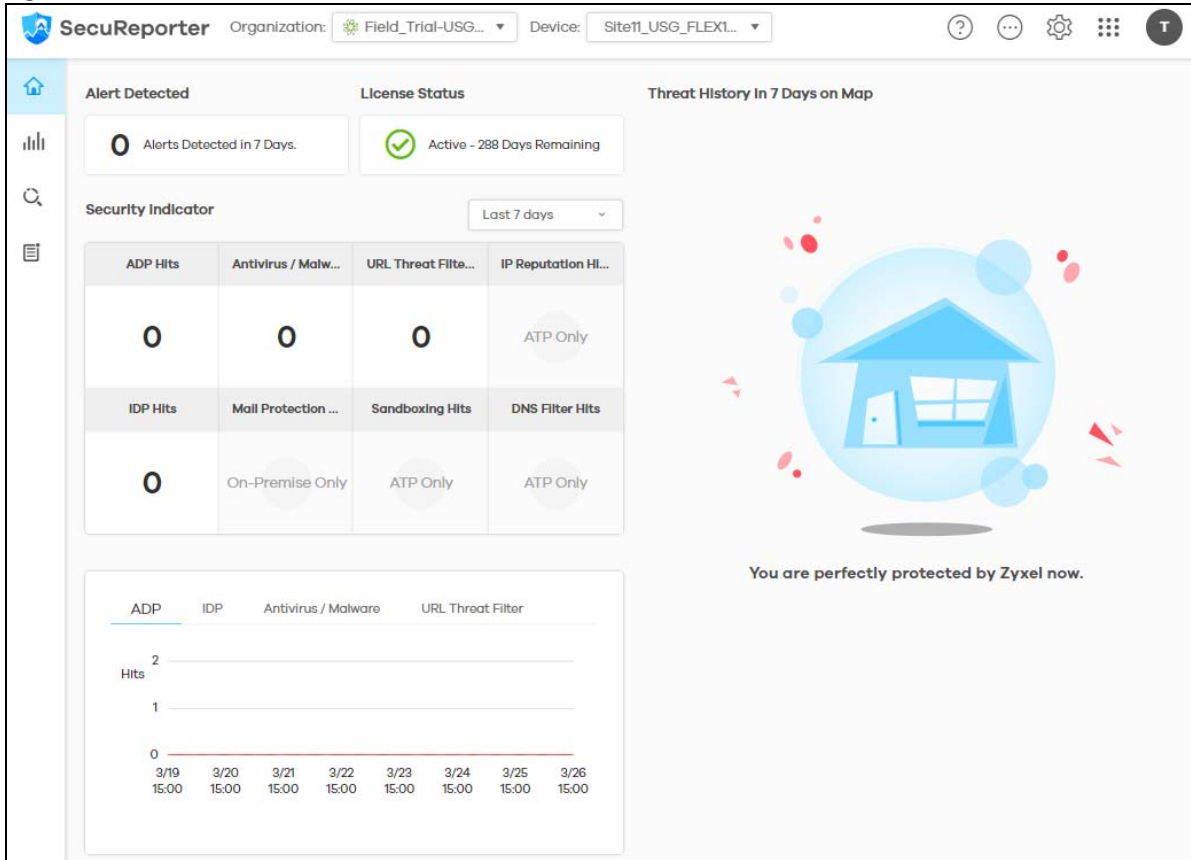
LABEL	DESCRIPTION
Status	This shows whether the VPN tunnel is connected or disconnected.
Inbound	This shows the amount of traffic that has gone through the VPN tunnel from the Non-Nebula peer gateway to the Nebula Device since the VPN tunnel was established.
Outbound	This shows the amount of traffic 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.

## 9.2.5 SecuReporter

Click **Firewall > Monitor > 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 124 Firewall > Monitor > SecuReporter

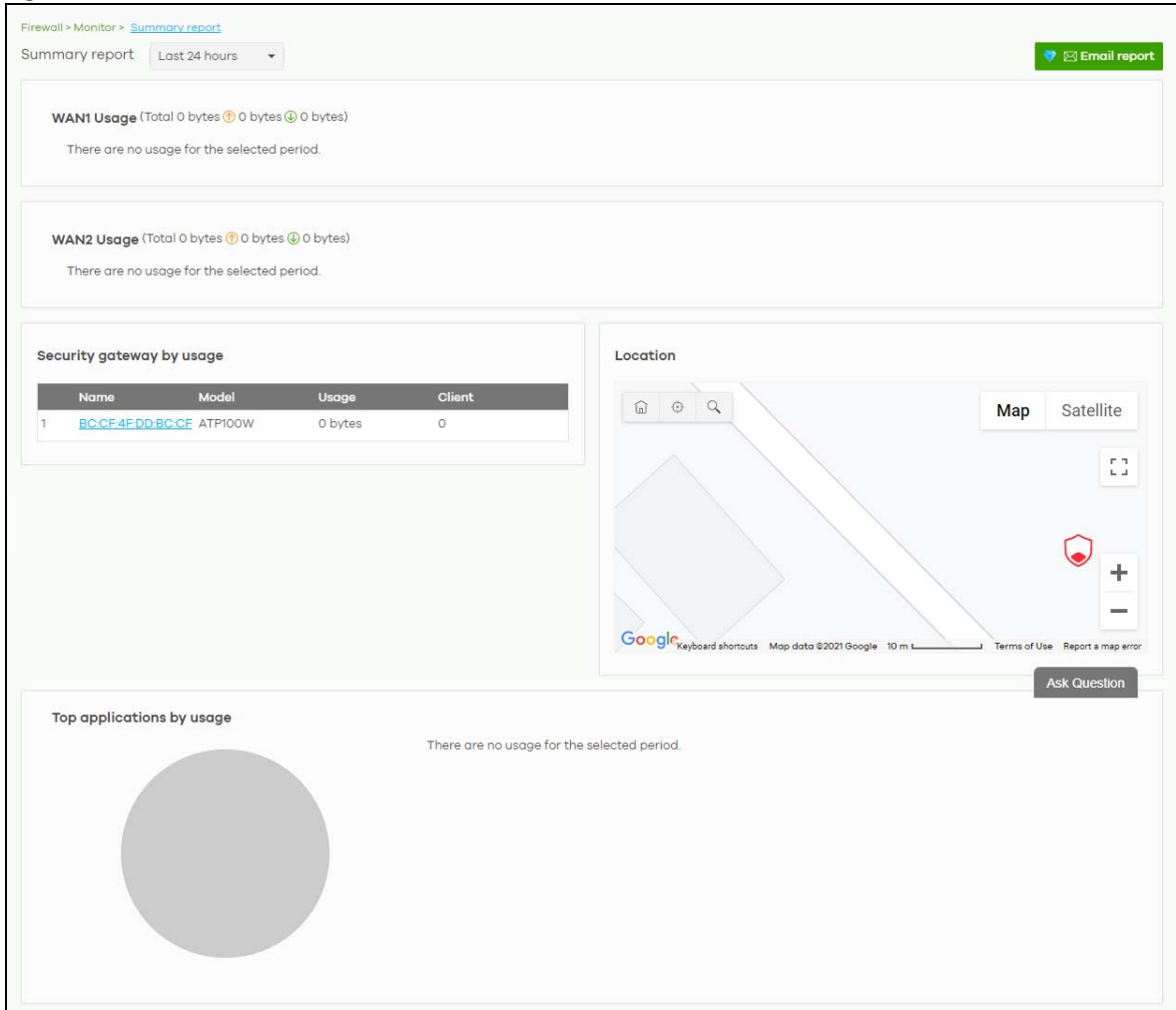


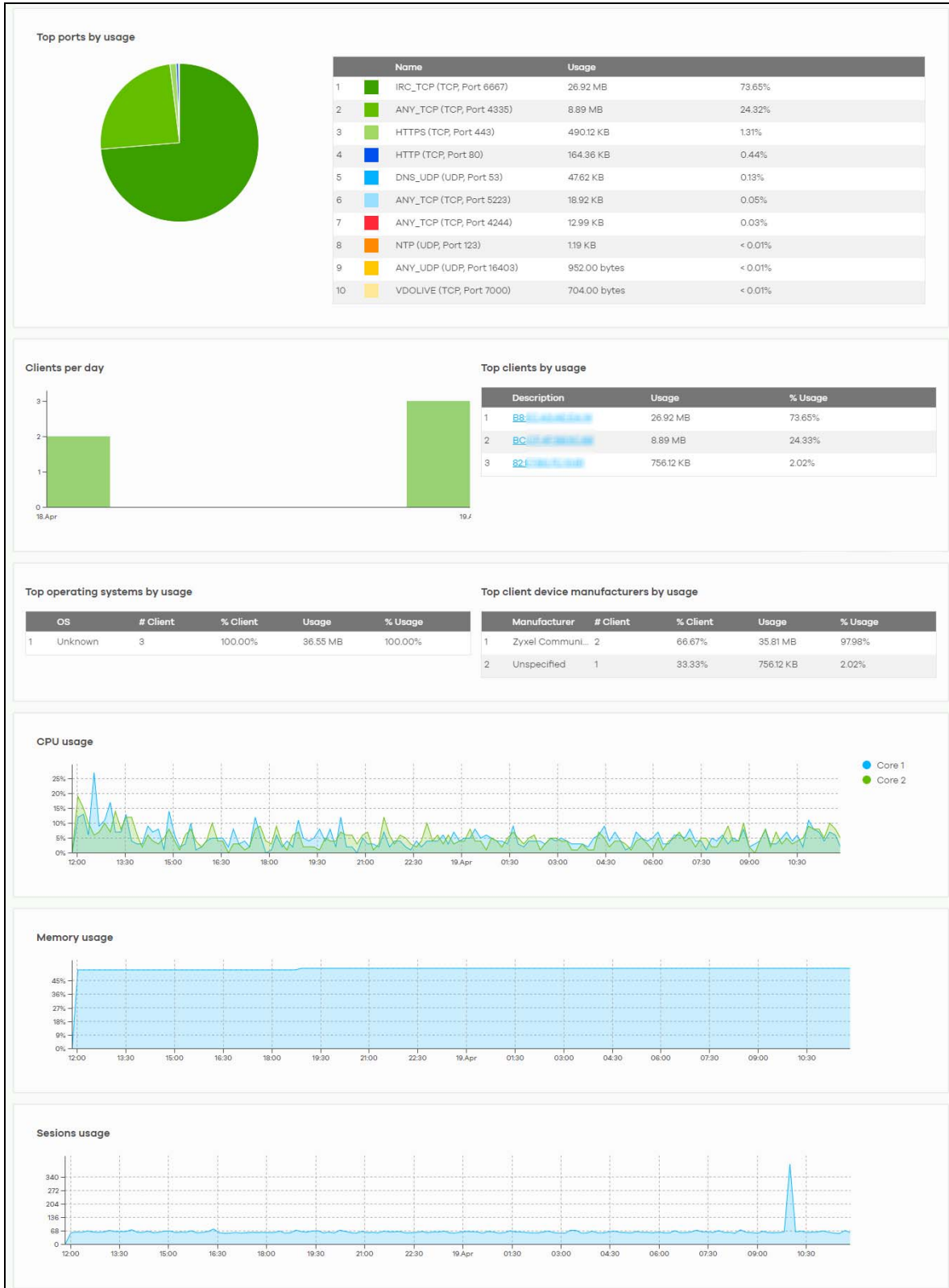
### 9.2.6 Summary Report

This screen displays network statistics for the Nebula Device of the selected site, such as WAN usage, top applications and/or top clients.

Click **Firewall > Monitor > Summary report** to access this screen.

Figure 125 Firewall > Monitor > Summary report





The following table describes the labels in this screen.

Table 103 Firewall &gt; Monitor &gt; Summary report

LABEL	DESCRIPTION
Security gateway – Summary report	Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table. <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <input type="radio"/> Last 24 hours  <input checked="" type="radio"/> Last 7 days  <input type="radio"/> Custom range ...           </div> <div style="text-align: right; margin-top: 5px;"> <input type="button" value="Update"/> </div>
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 103 Firewall &gt; Monitor &gt; 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.

## 9.3 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.

### 9.3.1 Port

Use this screen to configure port groups on the Nebula Device. To access this screen, click **Firewall > Configure > Port**.

**Figure 126** Firewall > Configure > Port



The screenshot shows the 'Port' configuration interface. At the top, it says 'Welcome to Nebula Professional Pack! Take the most of your network without limitations.' Below that, the breadcrumb 'Firewall > Configure > Port' is visible. The main area is titled 'Port' and contains a table for configuring port groups. The table has columns for ports P1 through P8. Each port has a 'Port Type' label: P1, P4, P5, P6, P7, and P8 are 'Optional' (yellow); P2 and P3 are 'WAN' (blue). Below this, there are two sections: 'WAN Port Group' and 'LAN Port Group'. Each section has two rows of radio buttons for 'WAN Group 1', 'WAN Group 2', 'LAN Group 1', and 'LAN Group 2'. In the WAN section, P2 and P3 are selected for WAN Group 2. In the LAN section, P3, P7, and P8 are selected for LAN Group 1, while P4 and P5 are selected for LAN Group 2. There are '+ Add' buttons for both sections.

The following table describes the labels in this screen.

**Table 104** Firewall > Configure > Port

LABEL	DESCRIPTION
Port Group	<p>Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.</p> <p>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.</p> <p>For example, to add port <b>P3</b> to <b>LAN Group 1</b>, select P3's radio button in the LAN Group 1 row.</p> <p>Note: See <a href="#">Table 1 on page 12</a> for the list of Nebula Device that do NOT have a P1 port.</p>
Port Type	This shows whether the port is a <b>WAN</b> port or a <b>LAN</b> port. <b>Optional</b> means the port can be assigned as either WAN or LAN, by adding it to a WAN or LAN group.
WAN Port Group	

Table 104 Firewall &gt; Configure &gt; Port (continued)

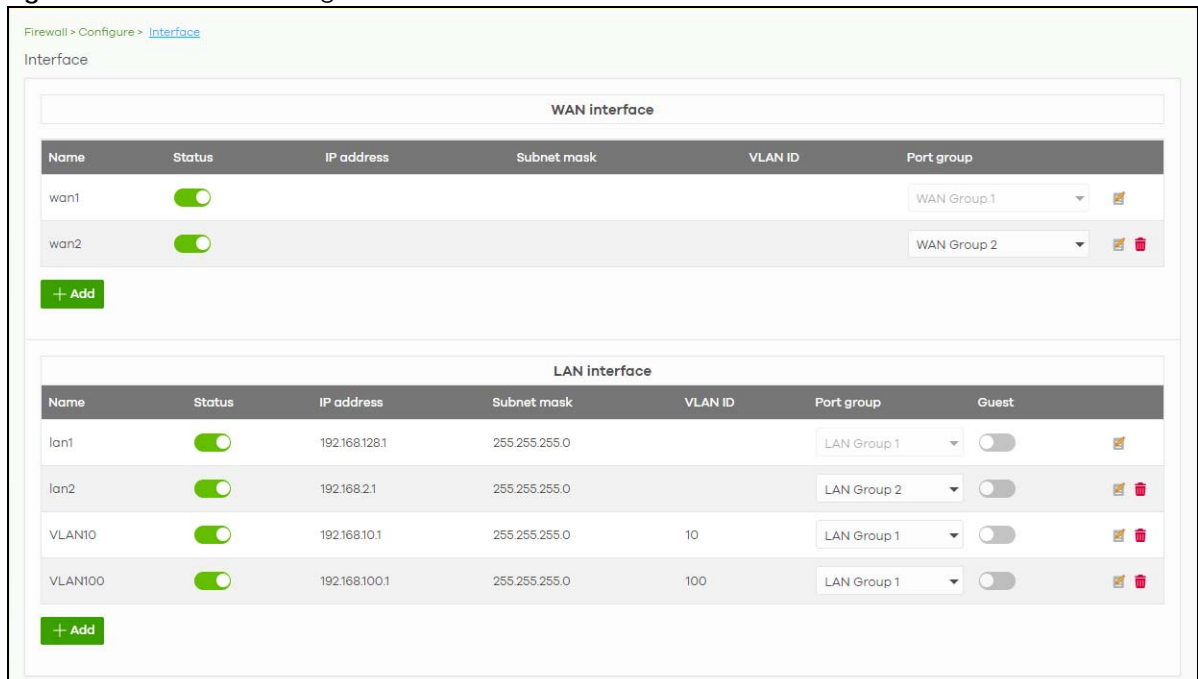
LABEL	DESCRIPTION
WAN Group 1	This shows the name of the WAN port group.  Note: Each WAN port group can only contain one port.
	Click this icon to remove a WAN port group.
Add	Click this button to create a new WAN port group.
LAN Port Group	
LAN Group 1	This shows the name of the LAN port group.
	Click this icon to remove a LAN port group.
Add	Click this button to create a new LAN port group.
Close	Click <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.

### 9.3.2 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 **Firewall > Configure > Interface**.

Figure 127 Firewall &gt; Configure &gt; Interface



Firewall > Configure > Interface

Interface

WAN interface

Name	Status	IP address	Subnet mask	VLAN ID	Port group
wan1	<input checked="" type="checkbox"/>				WAN Group 1
wan2	<input checked="" type="checkbox"/>				WAN Group 2

+ Add

LAN interface





Name	Status	IP address	Subnet mask	VLAN ID	Port group	Guest
lan1	<input checked="" type="checkbox"/>	192.168.128.1	255.255.255.0		LAN Group 1	<input type="checkbox"/>
lan2	<input checked="" type="checkbox"/>	192.168.2.1	255.255.255.0		LAN Group 2	<input type="checkbox"/>
VLAN10	<input checked="" type="checkbox"/>	192.168.10.1	255.255.255.0	10	LAN Group 1	<input type="checkbox"/>
VLAN100	<input checked="" type="checkbox"/>	192.168.100.1	255.255.255.0	100	LAN Group 1	<input type="checkbox"/>

+ Add



The following table describes the labels in this screen.

Table 105 Firewall &gt; Configure &gt; Interface

LABEL	DESCRIPTION
WAN Interface	
Name	<p>This field is read-only if you are editing an existing WAN interface.</p> <p>Specify a name for the interface.</p> <p>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.</p>
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	<p>This shows the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.)</p> <p>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.</p>
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	<p>This field is read-only if you are editing an existing LAN interface.</p> <p>Specify a name for the interface.</p> <p>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.</p>
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	<p>This is the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.)</p> <p>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.</p>
Port group	Select the name of the port group to which you want the interface to (network) belong.
Guest	Select <b>On</b> 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.

### 9.3.2.1 WAN Interface Configuration

Click the **Add** button or click the **Edit** button in the **WAN Interface** section to open the **Firewall > Configure > Interface > WAN interface configuration** screen.

**Figure 128** Firewall > Configure > Interface > WAN interface configuration

The following table describes the labels in this screen.


Table 106 Firewall > Configure > 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 106 Firewall &gt; Configure &gt; Interface &gt; WAN interface configuration (continued)

LABEL	DESCRIPTION
Type	<p>Select the type of interface to create.</p> <p><b>DHCP:</b> The interface will automatically get an IP address and other network settings from a DHCP server.</p> <p><b>Static:</b> You must manually configure an IP address and other network settings for the interface.</p> <p><b>PPPoE:</b> 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.</p> <p><b>PPPoE with static IP:</b> Assign a static IP address to the WAN interface and your WAN interface is getting an Internet connection from a PPPoE server.</p>
IP address assignment	These fields are displayed if you select <b>Static</b> .
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	<p>Enter a DNS server's IP address.</p> <p>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.</p>
Second DNS server	Enter the IP address of another DNS server. This field is optional.
These fields are displayed if you selected <b>PPPoE</b> or <b>PPPoE with static IP</b> .	
Authentication Type	<p>Select an authentication protocol for outgoing connection requests. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Chap/PAP</b> – The Nebula Device accepts either CHAP or PAP when requested by the remote node.</li> <li>• <b>Chap</b> – The Nebula Device accepts CHAP only.</li> <li>• <b>PAP</b> – The Nebula Device accepts PAP only.</li> <li>• <b>MSCHAP</b> – The Nebula Device accepts MSCHAP only.</li> <li>• <b>MSCHAP-V2</b> – The Nebula Device accepts MSCHAP-V2 only.</li> </ul>
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.
<b>ADVANCED OPTIONS</b>	
Connectivity check	<p>The interface can periodically check whether it can connect to its default gateway (<b>Default gateway</b>), or to two user-specified servers (<b>Check the two addresses below</b>). If the check fails, the interface's status changes to <b>Down</b>.</p> <p>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.</p>

Table 106 Firewall &gt; Configure &gt; Interface &gt; WAN interface configuration (continued)

LABEL	DESCRIPTION
Probe Succeeds When	<p>This field applies when you select <b>Check the two addresses</b> and specify two domain names or IP addresses for the connectivity check.</p> <p>Select <b>any one</b> if you want the check to pass if at least one of the domain names or IP addresses responds.</p> <p>Select <b>all</b> if you want the check to pass only if both domain names or IP addresses respond.</p>
Proxy ARP	<p>Proxy ARP (RFC 1027) allows the Nebula Device to answer external interface ARP requests on behalf of a device on its internal interface.</p> <p>Click <b>Add new</b> to add the IP address or IP range of devices that the interface will answer proxy ARP requests for.</p>
IP Address	<p>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).</p> <p>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.</p>
	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 <b>Auto</b> , <b>Unicast</b> and <b>Broadcast</b> .
DHCP option 60	<p>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.</p> <p>Enter a string using up to 63 of these characters [a-z A-Z 0-9 !"#%&amp;'()*+,-./ :;&lt;=&gt;?@\[\]\^_`{}] to identify this Nebula Device to the DHCP server. For example, Zyxel-TW.</p>
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 <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.

### 9.3.2.2 LAN Interface Configuration

Click the **Add** button or click the **Edit** button in the **LAN interface** section to open the **Firewall > Configure > Interface > LAN interface configuration** screen.

**Figure 129** Firewall > Configure > Interface > LAN interface configuration

The following table describes the labels in this screen.

**Table 107** Firewall > Configure > 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 107 Firewall &gt; Configure &gt; Interface &gt; LAN interface configuration (continued)


LABEL	DESCRIPTION
DHCP setting	<p>Select what type of DHCP service the Nebula Device provides to the network. Choices are:</p> <p><b>None</b> – the Nebula Device does not provide any DHCP services. There is already a DHCP server on the network.</p> <p><b>DHCP Relay</b> – the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network.</p> <p><b>DHCP Server</b> – 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.</p>
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	<p>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 <b>Static DHCP Table</b>.</p> <p>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.</p>
First DNS Server, Second DNS Server, Third DNS Server	<p>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.</p> <p><b>Custom Defined</b> – enter a static IP address.</p> <p><b>From ISP</b> – select the DNS server that another interface received from its DHCP server.</p> <p><b>This Gateway</b> – the DHCP clients use the IP address of this interface and the Nebula Device works as a DNS relay.</p>
Lease Time	<p>Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are:</p> <p><b>infinite</b> – select this if IP addresses never expire.</p> <p><b>days, hours, and minutes (Optional)</b> – select this to enter how long IP addresses are valid.</p>
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 107 Firewall &gt; Configure &gt; Interface &gt; LAN interface configuration (continued)

LABEL	DESCRIPTION
DHCP extended options	<p>This table is available if you select <b>ADVANCED OPTIONS</b>.</p> <p>Configure this table if you want to send more information to DHCP clients through DHCP packets.</p> <p>Click <b>Add new</b> to create an entry in this table. See <a href="#">Section 7.3.2.3 on page 189</a> for detailed information.</p>
First WINS server Second WINS server	<p>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.</p>
PXE server	<p>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).</p> <p>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.</p> <p>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.</p>
PXE Boot loader file	<p>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.</p>
Default gateway	<p>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.</p>
IGMP proxy	<p>Select this to allow the Nebula Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.</p>
IGMP Upstream	<p>Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.</p>
IGMP Downstream	<p>Enable IGMP Downstream on the interface which connects to the multicast hosts.</p>
Close	<p>Click <b>Close</b> to exit this screen without saving.</p>
OK	<p>Click <b>OK</b> to save your changes.</p>

### 9.3.2.3 DHCP Option

Click the **Add new** button in the **DHCP extended options** section to open the **Firewall > Configure > Interface > LAN interface configuration: DHCP option** screen.

**Figure 130** Firewall > Configure > Interface: LAN interface configuration: DHCP option

The following table describes the labels in this screen.

**Table 108** Firewall > Configure > 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 <b>User defined</b> in the <b>Option</b> 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 <b>User defined</b> in the <b>Option</b> field, enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. If you selected <b>User defined</b> in the <b>Option</b> 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 <b>TFTP Server Name (66)</b> and the type is <b>TEXT</b> , enter the DNS domain name of a TFTP server here. This field is mandatory.
First/Second/Third IP address	If you selected <b>User defined / Time/NTP/SIP/TFTP server / CAPWAP AC</b> in the <b>Option</b> field, enter up to three IP addresses.
Close	Click <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.

### 9.3.3 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 **Firewall > Configure > Routing: Policy Route/Traffic Shaping** to access this screen.

**Figure 131** Firewall > Configure > Routing: Policy Route/Traffic Shaping

Enabled	Source	Destination	Service	Next-Hop	Traffic Shaping	Description
<input checked="" type="checkbox"/>	Any	Any	Any	Internet: wan1	Download Limit: unlimited Upload Limit: unlimited Priority: Medium(4)	PR-1

The following table describes the labels in this screen.

Table 109 Firewall > Configure > 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. <b>Any</b> means all services. Select <b>Protocol</b> 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 <a href="#">Section 9.3.7.1 on page 364</a> for more information.

### 9.3.3.1 Add/Edit Policy Route / Traffic Shaping Rule

Click the **Add** button or an edit icon in the **Firewall > Configure > Routing: Policy Route/Traffic Shaping: Add/Edit** screen to access this screen.

**Figure 132** Firewall > Configure > Routing: Policy Route/Traffic Shaping: Add/Edit

The following table describes the labels in this screen.

Table 110 Firewall &gt; Configure &gt; 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 <b>Add</b> . Select <b>Any</b> 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 <b>Add</b> . Select <b>Any</b> 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 110 Firewall &gt; Configure &gt; Routing: Policy Route/Traffic Shaping: Add/Edit (continued)

LABEL	DESCRIPTION
Service	Select a protocol to apply the policy route to.  <b>TCP, UDP, TCP &amp; UDP, ICMP</b> – Match packets from the specified network protocol, going to the optional destination port.  <b>Protocol</b> – Match packets for the specified custom protocol. Enter the <b>Protocol ID</b> , 1 – 143 (1 for <b>ICMP</b> , 6 for <b>TCP</b> , 17 for <b>UDP</b> ; the <b>Service</b> will automatically select <b>ICMP / TCP / UDP</b> respectively).  <b>Application</b> – Match packets from the application.  Otherwise, select <b>Any</b> .
Policy Route	Select this to enable policy route.
Type	Select <b>Internet Traffic</b> to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).  Select <b>Intranet Traffic</b> to route the matched packets to the next-hop router or Switch you specified in the <b>Next-Hop</b> field.  Select <b>VPN Traffic</b> to route the matched packets through the VPN tunnel you specified in the <b>Next-Hop</b> field.
Next-Hop	If you select <b>Internet Traffic</b> in the <b>Type</b> 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 <b>Intranet Traffic</b> in the <b>Type</b> field, enter the IP address of the next-hop router or Switch.  If you select <b>VPN Traffic</b> in the <b>Type</b> field, select the remote VPN gateway's site name.  <ul style="list-style-type: none"> <li>Only the VPN gateway sites belonging to the same <b>VPN Area</b> that you set in <b>Organization-wide &gt; Configure &gt; VPN Orchestrator</b> will be available. See <a href="#">Section 6.3.9.3 on page 242</a> for more information).</li> <li>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.</li> </ul>
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.

### 9.3.3.2 Static Route

Click the **Add** button in the **Static Route** section of the **Firewall > Configure > Routing: Static Route** screen to open the following screen.

Figure 133 Firewall &gt; Configure &gt; Routing: Static Route


Static Route

Subnet	Next Hop Type	Next Hop	Metric(0-127)	Description
<input type="text"/>	IP Address	<input type="text"/>	1	<input type="text"/>

+ Add

The following table describes the labels in this screen.

Table 111 Firewall > Configure > 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 <b>IP Address</b> or <b>Interface</b> 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.

### 9.3.3.3 WAN Load Balancing

Go to **Firewall > Configure > 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 134 Firewall > Configure > Routing: WAN Load Balancing



The following table describes the labels in this section.

Table 112 Firewall > Configure > 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.

## 9.3.4 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 **Firewall > Configure > NAT**. The following screen appears, providing a summary of the existing NAT rules.




**Figure 135** Firewall > Configure > NAT

The following table describes the labels in this screen.

**Table 113** Firewall > Configure > 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: <b>TCP</b> , <b>UDP</b> , and <b>Both</b> .
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 <b>Any</b> 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 113 Firewall &gt; Configure &gt; 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 <b>Any</b> 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: <b>TCP</b> , <b>UDP</b> , and <b>Both</b> .
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 <b>Any</b> 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.

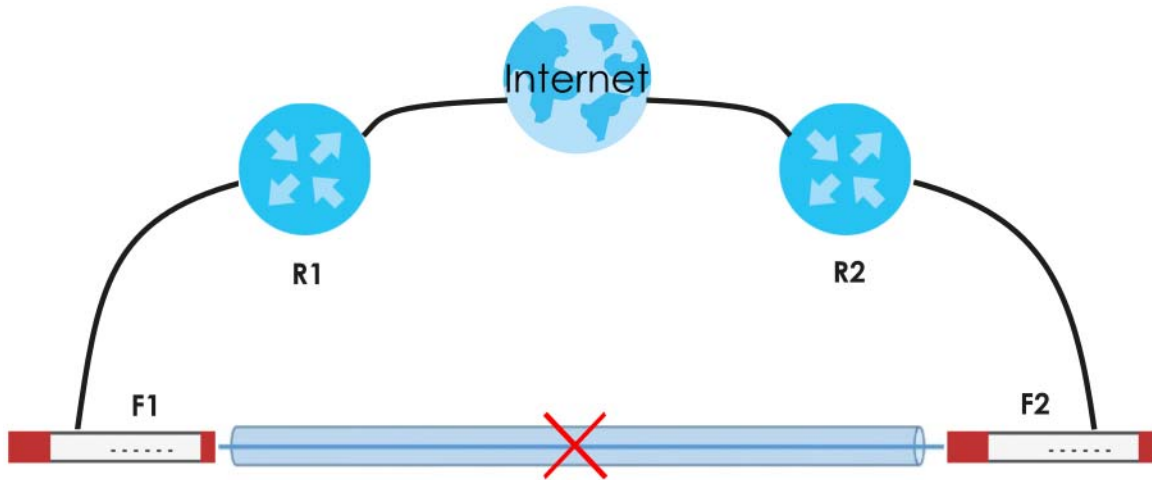
### 9.3.5 Site-to-Site VPN

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 136 Two VPN Sites Behind NAT Example



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

Figure 137 Firewall > Configure > Site-to-Site VPN

Firewall > Configure > [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	<input checked="" type="checkbox"/>
lan2	192.168.2.0/24	<input checked="" type="checkbox"/>
VLAN10	192.168.10.0/24	<input checked="" type="checkbox"/>
VLAN100	192.168.100.0/24	<input checked="" type="checkbox"/>
IPSec remote client VPN	192.168.200.0/24	<input checked="" type="checkbox"/>

VPN Area: Default

Nebula VPN enable:

Nebula VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

Hub-and-Spoke: 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

Save or Cancel

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

**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	Availability
<input checked="" type="checkbox"/>				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 114 Firewall &gt; Configure &gt; Site-to-Site VPN

LABEL	DESCRIPTION
Outgoing Interface	Select the WAN interface to which the VPN connection is going. Select <b>AUTO</b> 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 <b>Outgoing Interface</b> to <b>AUTO</b> .
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 <b>ON</b> to allow the computers on the network to use the VPN tunnel. Otherwise, select <b>OFF</b> .
VPN Area	Select the VPN area of the site. For details, see <a href="#">Section 6.3.9.2 on page 242</a> .
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 <a href="#">Section 6.3.9.1 on page 241</a> . 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 <b>Topology</b> is set to <b>Hub-and-Spoke</b> . You can configure hub sites at <b>Organization-wide &gt; Configure &gt; VPN Orchestrator</b> .
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 <b>Custom</b> 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 <a href="#">Section 9.3.8.1 on page 378</a> for detailed information.

Table 114 Firewall &gt; Configure &gt; 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 <b>All sites</b> to allow the non-Nebula gateway to connect to any site in the VPN area. Select <b>This site</b> and the non-Nebula gateway can only connect to the Nebula Device in this site.
Address	Enter the address (physical location) of the device.

### 9.3.5.1 IPsec Policy

Click the **Default** button in the **Non-Nebula VPN peers** section of the **Firewall > Configure > Site-to-Site VPN** screen to access this screen.

Figure 138 Firewall &gt; Configure &gt; Site-to-Site VPN: IPsec Policy

The screenshot shows the IPsec Policy configuration window. It is titled "Custom" and has a close button (X) in the top right corner. The configuration is organized into sections:

- Preset:** A dropdown menu set to "Default".
- Phase 1:**
  - IKE version:** A dropdown menu set to "IKEv1".
  - Encryption:** A dropdown menu set to "AES128".
  - Authentication:** A dropdown menu set to "SHA128".
  - Diffie-Hellman group:** A dropdown menu set to "DH2".
  - Lifetime (seconds):** A text input field containing "86400" with a clear (X) button.
- Advanced:** A blue link to expand advanced options.
- Phase 2:** A table with three columns: "Set", "Encryption", and "Authentication".
 

Set	Encryption	Authentication
Set 1	AES128	SHA128
Set 2	None	None
Set 3	None	None
- PFS group:** A dropdown menu set to "DH2".
- Lifetime (seconds):** A text input field containing "28800" with a clear (X) button.
- Connectivity check:** A text input field with a clear (X) button.

At the bottom right of the window, there are "Close" and "OK" buttons.

The following table describes the labels in this screen.

Table 115 Firewall > Configure > Site-to-Site VPN: IPsec Policy

LABEL	DESCRIPTION
Preset	Select a pre-defined IPsec policy, or select <b>Custom</b> 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).
IKE version	Select <b>IKEv1</b> or <b>IKEv2</b> .  <b>IKEv1</b> and <b>IKEv2</b> 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:  <b>DES</b> – a 56-bit key with the DES encryption algorithm <b>3DES</b> – a 168-bit key with the DES encryption algorithm <b>AES128</b> – a 128-bit key with the AES encryption algorithm <b>AES192</b> – a 192-bit key with the AES encryption algorithm <b>AES256</b> – 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 <b>SHA128</b> , <b>SHA256</b> , <b>SHA512</b> and <b>MD5</b> . 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:  <b>DH1</b> – use a 768-bit random number <b>DH2</b> – use a 1024-bit random number <b>DH5</b> – use a 1536-bit random number <b>DH14</b> – 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.  <b>Main</b> encrypts the Nebula Device's and remote IPsec router's identities but takes more time to establish the IKE SA.  <b>Aggressive</b> 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 115 Firewall &gt; Configure &gt; 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	<p>Select which key size and encryption algorithm to use in the IPsec SA. Choices are:</p> <p><b>(None)</b> – no encryption key or algorithm</p> <p><b>DES</b> – a 56-bit key with the DES encryption algorithm</p> <p><b>3DES</b> – a 168-bit key with the DES encryption algorithm</p> <p><b>AES128</b> – a 128-bit key with the AES encryption algorithm</p> <p><b>AES192</b> – a 192-bit key with the AES encryption algorithm</p> <p><b>AES256</b> – a 256-bit key with the AES encryption algorithm</p> <p>The Nebula Device and the remote IPsec router must both have at least one proposal that uses the same encryption and the same key.</p> <p>Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.</p>
PFS group	<p>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:</p> <p><b>None</b> – disable PFS</p> <p><b>DH1</b> – enable PFS and use a 768-bit random number</p> <p><b>DH2</b> – enable PFS and use a 1024-bit random number</p> <p><b>DH5</b> – enable PFS and use a 1536-bit random number</p> <p><b>DH14</b> – enable PFS and use a 2048-bit random number</p> <p>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.</p> <p>PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.</p>
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	<p>Enter an IP address that the Nebula Device can ping, to check whether the non-Nebula VPN peer gateway is available.</p> <p>Note: By default, NCC will use the private subnet IP address to do connectivity check.</p>
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

### 9.3.6 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 **Firewall > Configure > Remote access VPN** to access this screen.

Figure 139 Firewall > Configure > Remote access VPN

Firewall > Configure > 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:  [Send Email](#)

---

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:  [Send Email](#)

The following table describes the labels in this screen.

Table 116 Firewall > Configure > 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 <b>AUTO</b> in the <b>WAN interface</b> 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 <b>IKEv1</b> or <b>IKEv2</b> .  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 <b>Specify nameserver</b> to enter a static IP address.
Custom nameservers	If you select <b>Specify nameserver</b> in the <b>DNS name servers</b> field, manually enter the DNS server IP addresses.
Upload Bandwidth Limit	This field is available only if you select <b>IKEv2</b> in <b>IKE version</b> . 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 <a href="#">Section 9.3.6.1 on page 359</a> .
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 <b>Send Email</b> . 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 <b>Specify nameserver</b> to enter a static IP address.
Custom nameservers	If you select <b>Specify nameserver</b> in the <b>DNS name servers</b> field, manually enter the DNS server IP addresses.
Secret	This field is available only if you select <b>IKEv1</b> in <b>IKE version</b> . 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 116 Firewall &gt; Configure &gt; Remote access VPN (continued)

LABEL	DESCRIPTION
Policy	Configure custom VPN tunnel settings. For details, see <a href="#">Section 9.3.6.1 on page 359</a> .
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. <ul style="list-style-type: none"> <li>If <b>Authentication</b> is set to <b>Nebula Cloud Authentication</b>, the default email address list contains all authorized VPN user email addresses and your email address.</li> <li>If <b>Authentication</b> is set to <b>AD and RADIUS Authentication</b>, the default email address list contains your user email address.</li> </ul> This field is available only when you select <b>L2TP over IPSec client</b> in the <b>Client VPN server</b> field.

### 9.3.6.1 Remote Access VPN > Custom VPN Policy

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

Figure 140 Firewall &gt; Configure &gt; Remote access VPN: Default

**Custom** [X]

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

[Close] [OK]

The following table describes the labels in this screen.

Table 117 Firewall > Configure > Remote access VPN: Default

LABEL	DESCRIPTION
Custom	
Preset	Select a pre-defined IPSec policy, or select <b>Custom</b> to configure the policy settings yourself.
Phase 1	
Encryption	<p>Select which key size and encryption algorithm to use in the IPSec SA. Choices are:</p> <p><b>(None)</b> – no encryption key or algorithm</p> <p><b>DES</b> – a 56-bit key with the DES encryption algorithm</p> <p><b>3DES</b> – a 168-bit key with the DES encryption algorithm</p> <p><b>AES128</b> – a 128-bit key with the AES encryption algorithm</p> <p><b>AES192</b> – a 192-bit key with the AES encryption algorithm</p> <p><b>AES256</b> – a 256-bit key with the AES encryption algorithm</p> <p>The Nebula Device and the remote IPSec router must both have at least one proposal that use the same encryption and the same key.</p> <p>Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IKE SA.</p> <p>Choices are <b>SHA128</b>, <b>SHA256</b>, <b>SHA512</b> and <b>MD5</b>. SHA is generally considered stronger than MD5, but it is also slower.</p> <p>The remote IPSec router must use the same authentication algorithm.</p>
Diffie-Hellman group	<p>Select the Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are:</p> <p><b>DH1</b> – use a 768-bit random number</p> <p><b>DH2</b> – use a 1024-bit random number</p> <p><b>DH5</b> – use a 1536-bit random number</p> <p><b>DH14</b> – use a 2048-bit random number</p> <p>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.</p>
Lifetime (seconds)	<p>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.</p>
Phase 2	
Set	This shows the index number of the IPSec policy.



Table 117 Firewall &gt; Configure &gt; Remote access VPN: Default (continued)

LABEL	DESCRIPTION
Encryption	<p>Select which key size and encryption algorithm to use in the IPsec SA. Choices are:</p> <p><b>(None)</b> – no encryption key or algorithm</p> <p><b>DES</b> – a 56-bit key with the DES encryption algorithm</p> <p><b>3DES</b> – a 168-bit key with the DES encryption algorithm</p> <p><b>AES128</b> – a 128-bit key with the AES encryption algorithm</p> <p><b>AES192</b> – a 192-bit key with the AES encryption algorithm</p> <p><b>AES256</b> – a 256-bit key with the AES encryption algorithm</p> <p>The Nebula Device and the remote IPsec router must both have at least one proposal that use the same encryption and the same key.</p> <p>Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IKE SA.</p> <p>Choices are <b>None</b>, <b>SHA128</b>, <b>SHA256</b>, <b>SHA512</b> and <b>MD5</b>. SHA is generally considered stronger than MD5, but it is also slower.</p> <p>The remote IPsec router must use the same authentication algorithm.</p>
PFS group	<p>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:</p> <p><b>None</b> – disable PFS</p> <p><b>DH1</b> – enable PFS and use a 768-bit random number</p> <p><b>DH2</b> – enable PFS and use a 1024-bit random number</p> <p><b>DH5</b> – enable PFS and use a 1536-bit random number</p> <p><b>DH14</b> – enable PFS and use a 2048 bit random number</p> <p>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.</p> <p>PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.</p>
Lifetime (seconds)	<p>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.</p>
Close	<p>Click this button to exit this screen without saving.</p>
OK	<p>Click this button to save your changes and close the screen.</p>

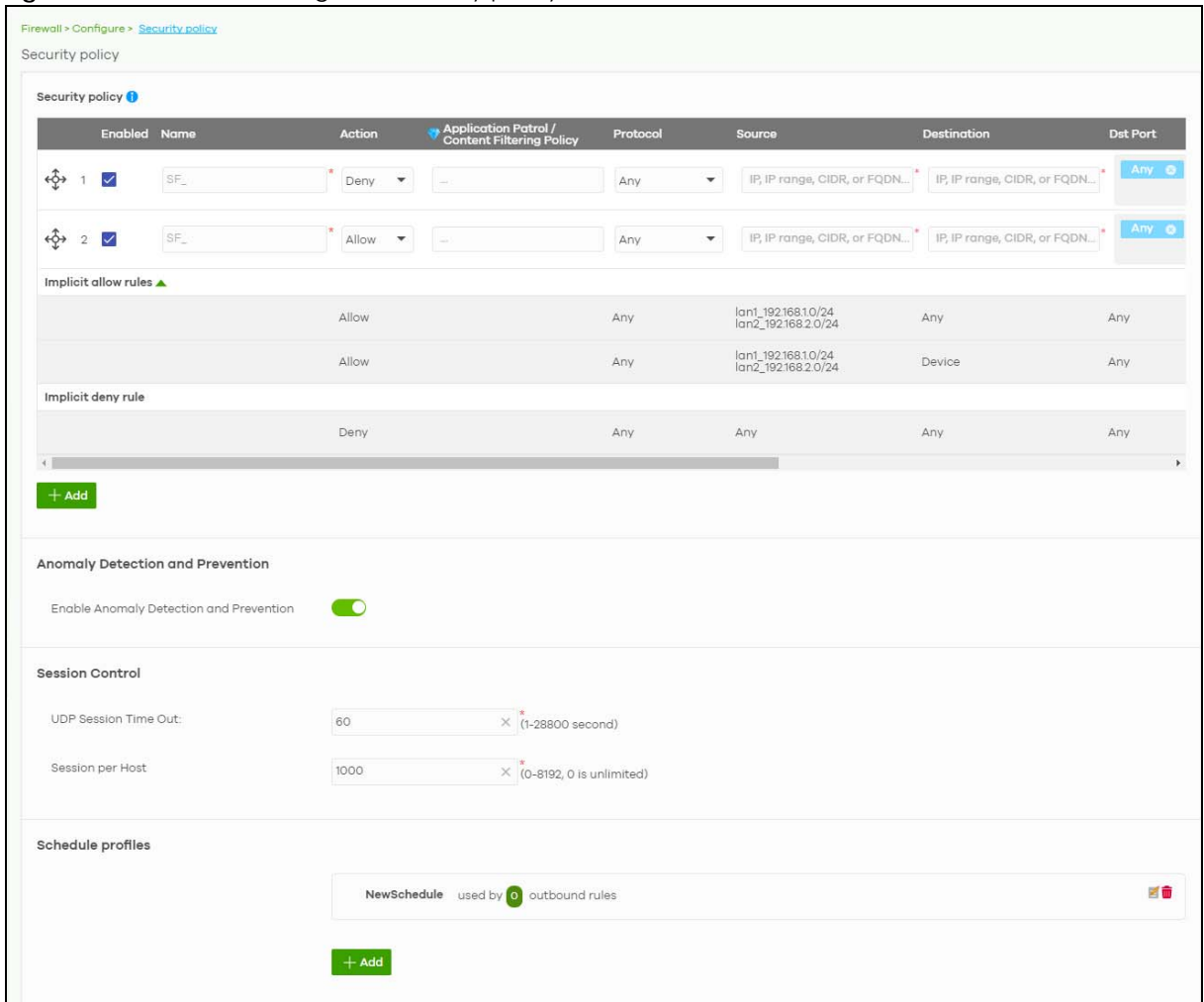
### 9.3.7 Security Policy

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 **Firewall > Configure > 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 141 Firewall > Configure > Security policy



The following table describes the labels in this screen.

Table 118 Firewall > Configure > 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 <b>Deny</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.  Select <b>Allow</b> to permit the passage of the packets.

Table 118 Firewall &gt; Configure &gt; Security policy (continued)




LABEL	DESCRIPTION
Application Patrol/ Content Filtering Policy	<p>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.</p> <p>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 <a href="#">Section 9.3.7.1 on page 364</a> for how to create an Application Patrol profile.</p> <p>Content Filtering controls access to specific web sites or web content. See <a href="#">Section 9.3.7.2 on page 365</a> for how to create a Content Filtering profile.</p>
Protocol	Select the IP protocol to which this rule applies. Choices are: <b>ICMP, TCP, UDP, TCP and UDP</b> and <b>Any</b> .
Source	<p>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 <b>Add</b>. Enter <b>any</b> to apply the rule to all IP addresses.</p> <p>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.</p>
Destination	<p>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 <b>Add</b>. Enter <b>any</b> to apply the rule to all IP addresses.</p> <p>Note: IP/CIDR, FQDN, and GEO IP objects cannot be use at the same time. Multiple FQDNs are not supported.</p>
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 <b>Add</b> . Enter <b>any</b> to apply the rule to all ports.
User	Select the <b>External User Group</b> name configured in <b>Firewall &gt; Configure &gt; Firewall settings</b> .
Schedule	Select the name of the schedule profile that the rule uses. <b>Always</b> 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	<p>Select whether to have the Nebula Device generate a log (<b>ON</b>) or not (<b>OFF</b>) when traffic matches the profile's policy.</p> <p>Note: By default, <b>Log</b> is <b>ON</b> when the <b>Action</b> field is <b>Deny</b>. <b>Log</b> is <b>OFF</b> when the <b>Action</b> field is <b>Allow</b>.</p>
	Click this icon to remove the rule.
Implicit allow rules	<p>This shows the system generated <b>Allow</b> rules.</p> <ul style="list-style-type: none"> <li>• LAN interface / remote access VPN to <b>Any</b></li> <li>• Guest interface to WAN interface</li> <li>• LAN interface / remote access VPN to Nebula Device</li> <li>• Guest interface to Nebula Device TCP (TCP:443, 80, 53)</li> <li>• Guest interface to Nebula Device UDP (UDP:53)</li> </ul>
Implicit deny rule	<p>This shows the system generated <b>Deny</b> rule.</p> <ul style="list-style-type: none"> <li>• <b>Any to Any</b></li> </ul>
Add	Click this button to create a new rule.
Anomaly Detection and Prevention	

Table 118 Firewall &gt; Configure &gt; 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 <a href="#">Section 9.3.7.3 on page 368</a> for more information.

### 9.3.7.1 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 **Firewall > Configure > 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 142** Firewall > Configure > Firewall: Add an Application Profile

The screenshot shows the 'Add profile' configuration window. It has a title bar with a close button. The main area contains:
 

- Name:** A text input field with a clear button (x).
- Description (Optional):** A text input field with a clear button (x).
- Log:** A green toggle switch that is currently turned on.
- Application Management:** A table with columns: Enabled, Category, Application, and Action.
 

Enabled	Category	Application	Action
1 <input checked="" type="checkbox"/>	Antivirus	All	Reject
- + Add:** A green button to add a new application category.
- Search Application:** A text input field to search for applications.
- Close:** A grey button to exit the screen.
- Create:** A grey button to save changes and close the screen.

The following table describes the labels in this screen.

**Table 119** Firewall > Configure > Firewall: 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 ( <b>ON</b> ) or not ( <b>OFF</b> ) 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 <b>All</b> or select an application within the category to apply the policy.
Action	Select the default action for the applications selected in this category. <b>Reject</b> – 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 <b>Add</b> 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.

### 9.3.7.2 Add a Content Filtering Profile

Click “+” in the **Application Patrol/Content Filtering Policy** section of the **Firewall > Configure > Firewall** screen to access this screen.

Figure 143 Firewall &gt; Configure &gt; Firewall: Add a Content Filtering Profile

The following table describes the labels in this screen.

Table 120 Firewall &gt; Configure &gt; Firewall: Add a 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 ( <b>ON</b> ) or not ( <b>OFF</b> ) 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	
Action for Unrated Web Pages	Select <b>Pass</b> to allow users to access web pages that the external web filtering service has not categorized.  Select <b>Block</b> 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 <b>Warn</b> to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.

Table 120 Firewall &gt; Configure &gt; Firewall: Add a Content Filtering Profile (continued)



LABEL	DESCRIPTION
Action When Service is Unavailable	<p>Select <b>Pass</b> to allow users to access any requested web page if the external content filtering database is unavailable.</p> <p>Select <b>Block</b> to block access to any requested web page if the external content filtering database is unavailable.</p> <p>Select <b>Warn</b> to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable.</p> <p>The following are possible causes for the external content filtering server not being available:</p> <ul style="list-style-type: none"> <li>• There is no response from the external content filtering server within the time period specified in the Content Filter Server Unavailable Timeout field.</li> <li>• The Nebula Device is not able to resolve the domain name of the external content filtering database.</li> <li>• 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").</li> </ul>
Block Category	
Templates	Select the block category. Choices are <b>Parental control</b> , <b>Productivity</b> and <b>Custom</b> .
Test URL	<p>You can check which category a web page belongs to. Enter a web site URL in the text box.</p> <p>When the content filter is active, you should see the web page's category. The query fails if the content filter is not active.</p> <p>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.</p>
Search category	<p>Click to display or hide the category list.</p> <p>These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.</p>
Custom block web site	<p>Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0 – 9 a – z). The casing does not matter.</p>
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.
Custom allow web site	<p>Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0 – 9 a – z). The casing does not matter.</p>
Add	Click this button to create a new application category and set actions for specific applications within the category.

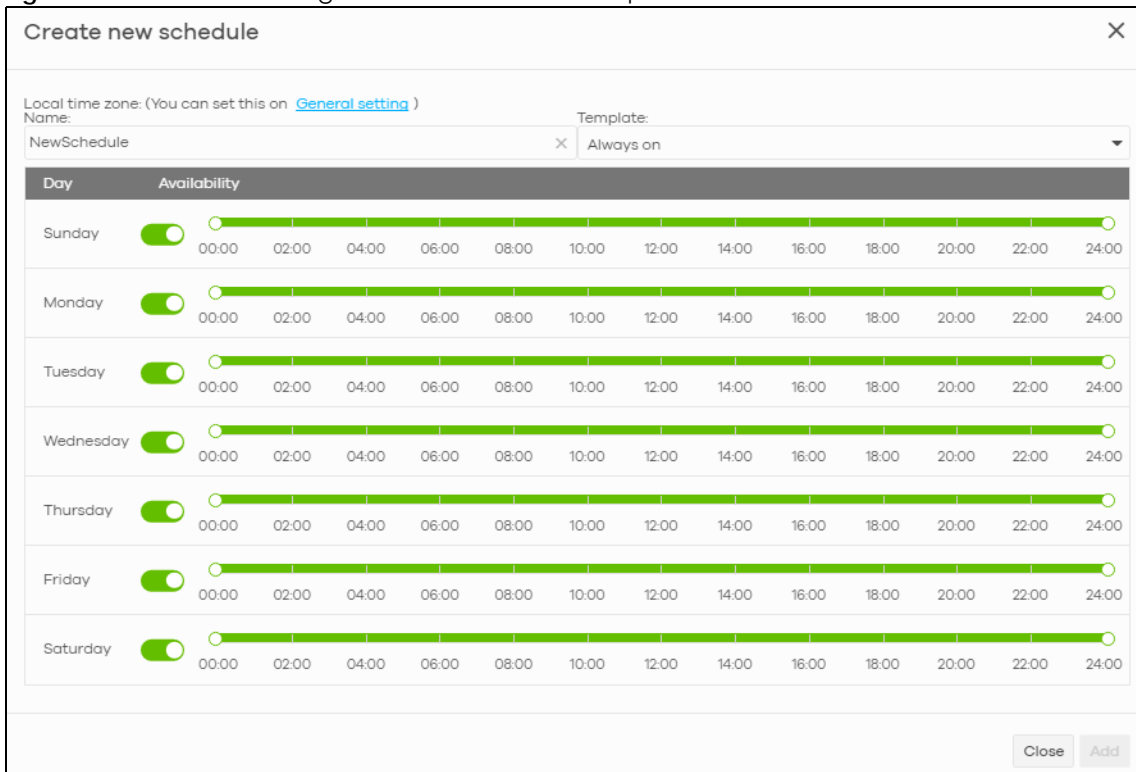
Table 120 Firewall &gt; Configure &gt; Firewall: Add a Content Filtering Profile (continued)

LABEL	DESCRIPTION
	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.

### 9.3.7.3 Create a New Schedule

Click the **Add** button in the **Schedule Profiles** section of the **Firewall > Configure > Firewall > Schedule profiles** screen to access this screen.

Figure 144 Firewall &gt; Configure &gt; Firewall &gt; Schedule profiles: Create a new schedule



The following table describes the labels in this screen.

Table 121 Firewall &gt; Configure &gt; Firewall &gt; Schedule profiles: Create a new schedule

LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identification purposes.
Templates	Select a pre-defined schedule template or select <b>Custom schedule</b> 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 <b>On</b> to enable the associated rule at the specified time on this day. Otherwise, select <b>Off</b> 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.



### 9.3.8 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 **Firewall > Configure > 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 6.3.8 on page 233](#).

Figure 145 Firewall > Configure > Security service

Firewall > Configure > Security service

### Security service

**Content filtering** [Model list](#)

Drop connection when there is an HTTP 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](#)

---

**IP Exception** [Model list](#)

Enabled	Source IP	Destination IP	Description
<input checked="" type="checkbox"/>	-	-	-

[+ Add](#)

---

**DNS/URL Threat Filter** [Model list](#)

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

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:  [Ask Question](#)

Allow list:

URL Threat Filter external block list:

Enabled	Name	External DB	Description
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

[+ Add](#)

Schedule update:  External DB schedule update

Daily

03:00

### IP Reputation [Model list](#)

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

Enabled:

Log:

Policy: Block

Threat level threshold: Medium and above

Test Category:

Category list:
 

- Anonymous Proxies
- Denial of Service
- Exploits
- Negative Reputation
- Scanners
- Spam Sources
- Tor Proxies
- Web Attacks
- Phishing
- BotNets

Black list:

Allow list:

External block list:
 

Enabled	Name	External DB	Description
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Schedule update:  External DB schedule update  
Daily  
03:00

### Anti-Malware [Model list](#)

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

Enabled:

Log:

Scan mode: Stream mode Express mode

Cloud Query:

Block list:

File Types:

File Pattern:

Allow list:

File Pattern:

### Sandboxing [Model list](#)

Enabled:

Log:

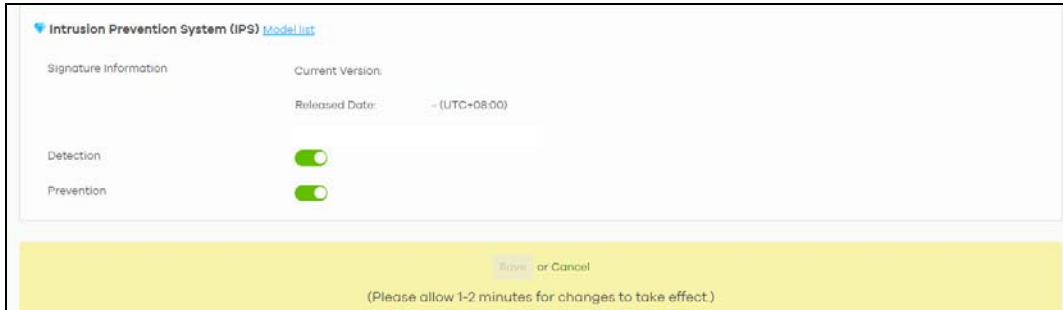
Policy: Allow

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:



The following table describes the labels in this screen.

Table 122 Firewall > Configure > Security service





LABEL	DESCRIPTION
Content Filtering	
Drop connection when HTTPS connection with SSL V3 or previous version	Select <b>On</b> 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 <b>Redirect URL</b> 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 <a href="#">Section 9.3.7.2 on page 365</a> 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 <a href="#">Section 9.3.8.2 on page 381</a> 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 122 Firewall &gt; Configure &gt; 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	<p>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.</p> <p>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.</p>
Signature information	This shows the <b>Current Version</b> of the DNS/URL threat definition and the <b>Released Date</b> .
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 <b>On</b> to turn on the rule. Otherwise, select <b>Off</b> to turn off the rule.
DNS Threat Filter Policy	<p>Select <b>Pass</b> 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.</p> <p>Select <b>Redirect</b> to have the Nebula Device reply with a DNS reply packet containing a default or custom-defined IP address.</p>
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 <b>On</b> to turn on the rule. Otherwise, select <b>Off</b> to turn off the rule.
URL Threat Filter Policy	<p>Select <b>Pass</b> to allow users to access web pages that the external web filtering service has not categorized.</p> <p>Select <b>Block</b> 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.</p> <p>Select <b>Warn</b> to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.</p>
URL Threat Filter Denied Access Message	<p>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;/?:@&amp;=+\$\._!~*()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator".</p> <p>It is also possible to leave this field blank if you have a URL specified in the <b>Redirect URL</b> 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.</p>
URL Threat Filter Redirect URL	<p>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.</p> <p>Use "http:///" or "https:///" followed by up to 262 characters (0–9 a–z A–Z;/?:@&amp;=+\$\._!~*()%,). For example, http://192.168.1.17/blocked access.</p>

Table 122 Firewall &gt; Configure &gt; Security service (continued)


LABEL	DESCRIPTION
Test Threat Category	Enter a URL using http://domain or https://domain and click the <b>Test</b> 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	<p>Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0–9 a–z). The casing does not matter.</p>
Allow list	<p>Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0–9 a–z). The casing does not matter.</p>
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	<p>Enter the exact file name, path and IP address of the server containing the block list file. The file type must be 'txt'.</p> <p>For example, http://172.16.107.20/blacklist-files/myip-ubl.txt</p> <p>The server must be reachable from the Nebula Device.</p>
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	<p>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.</p> <p>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.</p> <p>Select <b>Daily</b> to set the time of the day, or <b>Weekly</b> to set the day of the week and the time of the day.</p> <p>Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.</p>
IP Reputation	

Table 122 Firewall &gt; Configure &gt; Security service (continued)


LABEL	DESCRIPTION
Signature information	This shows the <b>Current Version</b> of the signature set the Nebula Device is using and the <b>Released Date</b> .
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 <b>Pass</b> to have the Nebula Device allow the packet to go through.  Select <b>Block</b> 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 ( <b>High, Medium and above, Low and above</b> ).  The threat level is determined by the IP reputation engine. It grades IPv4 addresses. <ul style="list-style-type: none"> <li>• <b>High</b>: an IPv4 address that scores 0 to 20 points.</li> <li>• <b>Medium and above</b>: an IPv4 address that scores 0 to 60 points.</li> <li>• <b>Low and above</b>: an IPv4 address that scores 0 to 80 points.</li> </ul> For example, a score of "10" will cause the Nebula Device to take action whether you set the <b>Threat level threshold</b> at <b>High, Medium and above</b> , or <b>Low and above</b> .  But a score of "61" will not cause the Nebula Device to take any action if you set the <b>Threat level threshold</b> at <b>Medium and above</b> .
Test Category	Enter an IPv4 address of a website, and click the <b>Test</b> 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-eb1.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 122 Firewall &gt; Configure &gt; Security service (continued)

LABEL	DESCRIPTION
Schedule update	<p>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.</p> <p>Select <b>Daily</b> to set the time of the day, or <b>Weekly</b> to set the day of the week and the time of the day.</p> <p>Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.</p>
Anti-Malware	
Signature information	This shows the <b>Current Version</b> of the signature set the Nebula Device is using and the <b>Released Date</b> .
Enabled	Select <b>On</b> to turn on the rule. Otherwise, select <b>Off</b> 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 patterns. 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)	<p>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.</p> <p>Note: The Nebula Device decompresses a compressed file once. The Nebula Device does NOT decompress any files within a compressed file.</p>
Destroy compressed files that could not be decompressed	<p>When you select this check box, the Nebula Device deletes compressed files that use password encryption.</p> <p>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.</p> <p>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.</p>
Cloud Query	Select the Cloud Query supported file types for the Nebula Device to scan for viruses.



Table 122 Firewall &gt; Configure &gt; Security service (continued)

LABEL	DESCRIPTION
Block list	<p>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.</p> <p>File patterns:</p> <ul style="list-style-type: none"> <li>• Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• The whole file name has to match if you do not use a question mark or asterisk.</li> <li>• If you do not use a wildcard, the Security Firewall checks up to the first 80 characters of a file name.</li> </ul>
Allow list	<p>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.</p> <p>File patterns:</p> <ul style="list-style-type: none"> <li>• Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• The whole file name has to match if you do not use a question mark or asterisk.</li> <li>• If you do not use a wildcard, the Nebula Device checks up to the first 80 characters of a file name.</li> </ul>
Sandboxing	<p>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.</p>
Enabled	<p>Select this option to turn on sandboxing on the Nebula Device</p>
Log	<p>Enable this option to allow the Security Firewall to create a log when a suspicious file is detected.</p>
Policy	<p>Specify whether the Nebula Device deletes (<b>Destroy</b>) or forwards (<b>Allow</b>) malicious files. Malicious files are files given a high score for malware characteristics by the Defend Center.</p>

Table 122 Firewall &gt; Configure &gt; Security service (continued)

LABEL	DESCRIPTION
Inspect selected downloaded files	<p>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.</p> <p>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.</p>
File submission options	Specify the type of files to be sent for sandbox inspection.
Intrusion Detection/Prevention	
Signature information	This shows the <b>Current Version</b> of the signature set the Nebula Device is using and the <b>Released Date</b> .
Detection	Select <b>On</b> to enable Detection.
Prevention	Select <b>On</b> to enable Prevention.

### 9.3.8.1 Create a Content Filtering Profile

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

Figure 146 Firewall > Configure > 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

Action When Service is Unavailable

**Block Category**

Templates

Test URL

• Enter a url to know website category

^ Category list

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

**Block web site**

Web Site	
1	<input style="width: 95%;" type="text"/>
<input type="button" value="Delete"/>	
<input type="button" value="+ Add"/>	

**Allow web site**


Web Site	
1	<input style="width: 95%;" type="text"/>
<input type="button" value="Delete"/>	
<input type="button" value="+ Add"/>	

The following table describes the labels in this screen.

Table 123 Firewall > Configure > 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	<p>Select this option to turn on DNS filtering on the Nebula Device.</p> <p>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.</p>
Block Web Pages	
Action for Unrated Web Pages	<p>Select <b>Pass</b> to allow users to access web pages that the external web filtering service has not categorized.</p> <p>Select <b>Block</b> 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.</p> <p>Select <b>Warn</b> to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.</p>
Action when service is Unavailable	<p>Select <b>Pass</b> to allow users to access any requested web page if the external content filtering database is unavailable.</p> <p>Select <b>Block</b> to block access to any requested web page if the external content filtering database is unavailable.</p> <p>Select <b>Warn</b> to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable.</p> <p>The following are possible causes for the external content filtering server not being available:</p> <ul style="list-style-type: none"> <li>• There is no response from the external content filtering server within the time period specified in the Content Filter Server Unavailable Timeout field.</li> <li>• The Nebula Device is not able to resolve the domain name of the external content filtering database.</li> <li>• 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").</li> </ul>
Block Category	
<p>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 <b>Denied access message</b> field along with the category of the blocked web page.</p>	
Templates	<p>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 <b>Custom</b> and manually select categories in this section to control access to specific types of Internet content.</p>

Table 123 Firewall &gt; Configure &gt; Security service &gt; Content Filtering: Add/Edit (continued)

LABEL	DESCRIPTION
Test URL	<p>You can check which category a web page belongs to. Enter a web site URL in the text box.</p> <p>When the content filter is active, you should see the web page's category. The query fails if the content filter is not active.</p> <p>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. <b>Test URL</b> displays both results in the test.</p>
Search Category	Specify your desired filter criteria to filter the list of categories.
Category List	<p>Click to display or hide the category list.</p> <p>These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.</p>
Block web site	<p>Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0–9 a–z). The casing does not matter.</p>
Add	Click this button to add a new entry.
Allow web site	<p>Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0–9 a–z). The casing does not matter.</p>
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.

### 9.3.8.2 Add Application Patrol Profile

Click the **Add** button in the **Application Patrol** section of the **Firewall > Configure > Security service** screen to access this screen.

**Figure 147** Firewall > Configure > Security service > Application Patrol: Add/Edit

**Add profile** [X]

Name [ ] [X]

Description (Optional) [ ] [X]

Log

Application Management

Enabled	Category	Application	Action
1 <input checked="" type="checkbox"/>	Anti-...	All [ ]	Reject [ ]

+ Add Search Application [ ]

Close Create

The following table describes the labels in this screen.

Table 124 Firewall &gt; Configure &gt; Security service &gt; 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 <b>All</b> or select an application within the category to apply the policy.
Action	Displays the default action for the applications selected in this category. <b>Reject</b> – 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 <b>Add</b> 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.

### 9.3.9 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 **Firewall > Configure > Captive portal** to access this screen.

**Figure 148** Firewall > Configure > Captive portal

The screenshot shows the 'Captive portal' configuration page. At the top, the breadcrumb 'Firewall > Configure > Captive portal' is visible. The page title is 'Captive portal'. Below this, the 'Interface' is set to 'VLAN100'. A note states: 'Captive portal on this interface is direct access. You can change this setting [here](#).' The 'Themes' section shows a preview of a theme with a 'BUTTON' and options for 'Default' and 'Modern'. The 'Click-to-continue/Voucher/Sign-on page' section includes a 'Logo' field with a 'No logo' placeholder and an 'Upload a logo' button, and a 'Message' text area. The 'Success page' section has a 'Message' field containing the text 'Success!'. The 'External captive portal URL' section has a 'Use URL:' toggle (which is turned on), a 'URL:' text box, and a note: 'To use custom captive portal page, please download the zip file and edit them. [Download](#) the customized captive portal page example.' The 'Captive portal behavior' section has a question: 'After the captive portal page where the user should go?' with two radio button options: 'Stay on Captive portal authenticated successfully page' (which is unselected) and 'To promotion URL:' (which is selected), followed by a 'URL:' text box.

The following table describes the labels in this screen.

Table 125 Firewall > Configure > Captive portal

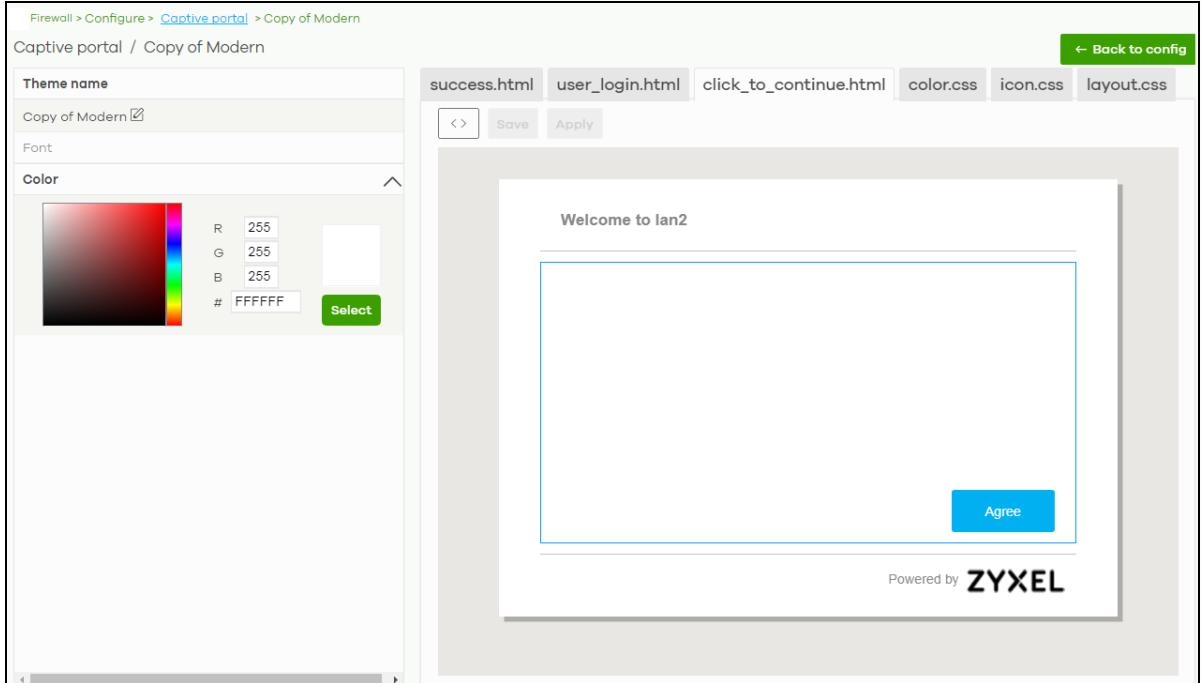
LABEL	DESCRIPTION
Interface	Select the Nebula Device's interface (network) to which the settings you configure here is applied.
Themes	<p>This section is not configurable when <b>External captive portal URL</b> is set to <b>ON</b>.</p> <ul style="list-style-type: none"> <li>Click the <b>Preview</b> icon at the upper right of a theme image to display the portal page in a new frame.</li> <li>Click the <b>Copy</b> icon to create a new custom theme (portal page).</li> <li>Click the <b>Edit</b> icon of a custom theme to go to a screen, where you can view and configure the details of the custom portal pages. See <a href="#">Section 9.3.9.1 on page 384</a>.</li> <li>Click the <b>Remove</b> icon to delete a custom theme.</li> </ul> <p>Select the theme you want to use on the specified interface.</p>
Click-to-continue/Sign-on page	
This section is not configurable when <b>External captive portal URL</b> is set to <b>ON</b> .	
Logo	<p>This shows the logo image that you uploaded for the customized login page.</p> <p>Click <b>Upload a logo</b> and specify the location and file name of the logo graphic or click <b>Browse</b> to locate it. You can use the following image file formats: GIF, PNG, or JPG.</p>
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	<p>Select <b>On</b> 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.</p> <p>Specify the login page's URL; for example, <code>http://IIS server IP Address/login.asp</code>. The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>
Captive portal behavior	
After the captive portal page where the user should go?	Select <b>To promotion URL</b> and specify the URL of the web site/page to which the user is redirected after a successful login. Otherwise, select <b>Stay on Captive portal authenticated successfully page</b> .

### 9.3.9.1 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 **Firewall > Configure > Captive portal** screen to access this screen.



Figure 149 Firewall &gt; Configure &gt; Captive portal: Edit



The following table describes the labels in this screen.

Table 126 Firewall &gt; Configure &gt; Captive portal: Edit

LABEL	DESCRIPTION
Back to config	Click this button to return to the <b>Captive portal</b> 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 <b>Select</b> 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.

### 9.3.10 Authentication Method

Use this screen to enable or disable web authentication on an interface.

Click **Firewall > Configure > Authentication Method** to access this screen.

**Figure 150** Firewall > Configure > Authentication Method

The screenshot shows the 'Authentication Method' configuration page. At the top, there is a breadcrumb trail: 'Firewall > Configure > Authentication Method'. Below this, the page title is 'Authentication Method'. There is a dropdown menu for 'Interfaces:' with 'lan1' selected. The main configuration area is divided into several sections:

- Network Access:** Contains four radio button options: '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' (set to 'Nebula Cloud Authentication'), and 'Two-factor authentication' (which is currently checked).
- Walled garden:** A toggle switch is turned on. Below it is a text input field for 'Walled garden ranges' which is currently empty, with a 'What do I enter here?' link below it.
- Captive portal access attribute:** Contains two dropdown menus: 'Self-registration' (set to 'Don't allow users to create accounts') and 'Login on multiple client devices' (set to 'Multiple devices access simultaneously').
- NCAS disconnection behavior:** Contains two radio button options: 'Allowed' (Client devices can access the network without signing in, except they are explicitly blocked) and '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 127 Firewall > Configure > Authentication method

LABEL	DESCRIPTION
Interfaces	Select the Nebula Device's interface (network) to which the settings you configure here is applied.
Network Access	<p>Select <b>Disable</b> to turn off web authentication.</p> <p>Select <b>Click-to-continue</b> to block network traffic until a client agrees to the policy of user agreement.</p> <p>Select <b>Sign-on with</b> to block network traffic until a client authenticates with an external RADIUS or AD server through the specifically designated web portal page. Select <b>Nebula Cloud Authentication</b> or an authentication server that you have configured in the <b>Firewall &gt; Configure &gt; Firewall settings</b> screen (see <a href="#">Section 9.3.12 on page 389</a>).</p> <p>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.</p>
Walled garden	<p>This field is not configurable if you set <b>Network Access</b> to <b>Disable</b>.</p> <p>Select to turn on or off the walled garden feature.</p> <p>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.</p>
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	<p>This field is available only when you select <b>Sign-on with Nebula Cloud authentication</b> in the <b>Network Access</b> field.</p> <p>Select <b>Allow users to create accounts with auto authorized</b> or <b>Allow users to create accounts with manual authorized</b> 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 <b>Allow users to create accounts with manual authorized</b>, users cannot log in with the account until the account is authorized and granted access. For <b>Allow users to create accounts with auto authorized</b>, users can just use the registered account to log in without administrator approval.</p> <p>Select <b>Don't allow users to create accounts</b> to not display a link for account creation in the captive portal login page.</p>
Login on multiple client devices	<p>This field is available only when you select <b>Sign-on with</b> in the <b>Network Access</b> field.</p> <p>Select <b>Multiple devices access simultaneously</b> if you allow users to log in as many times as they want as long as they use different IP addresses.</p> <p>Select <b>One device at a time</b> if you do not allow users to have simultaneous logins.</p>
NCAS disconnection behavior	<p>This field is available only when you select <b>Sign-on with Nebula Cloud Authentication</b> in the <b>Network Access</b> field.</p> <p>Select <b>Allowed</b> to allow any users to access the network without authentication when the NCAS (Nebula Cloud Authentication Server) is not reachable.</p> <p>Select <b>Limited</b> to allow only the currently connected users or the users in the white list to access the network.</p>

## 9.3.11 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 **Firewall > Configure > Wireless** to access this screen.

**Figure 151** Firewall > Configure > Wireless

The screenshot shows the 'Wireless' configuration page. It is divided into two main sections: 'SSID Settings' and 'Radio Settings'.

**SSID Settings:** A table with 4 columns representing different SSIDs. The first two are enabled, the last two are disabled.

No.	1	2	3	4																				
Name	Private Network (Zycamp) ✕*	Guest Network (Zycamp) ✕*	SSID3 ✕*	SSID4 ✕*																				
Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																				
Authentication	<table border="1"> <tr> <td>WLAN Security</td> <td>WPA2-PSK</td> <td>Open</td> <td>Open</td> <td>Open</td> </tr> <tr> <td>Associate Key</td> <td>***** ✕*</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Band</td> <td>Concurrent operation(2.4G..</td> <td>Concurrent operation(2.4G..</td> <td>Concurrent operation(2.4G..</td> <td>Concurrent operation(2.4G..</td> </tr> <tr> <td>Outgoing interface</td> <td>VLAN10</td> <td>lan1</td> <td>lan1</td> <td>lan1</td> </tr> </table>				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
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 128** Firewall > Configure > 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 <b>Open</b> to allow any WiFi client to associate with this network without any data encryption nor authentication. Select <b>WPA2-PSK</b> 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 <b>2.4 GHz band only</b> or the <b>5 GHz band only</b> . If you select <b>Concurrent operation (2.4 GHz and 5 GHz)</b> , the SSID uses both frequency bands.

Table 128 Firewall &gt; Configure &gt; Wireless (continued)

LABEL	DESCRIPTION
Outgoing Interface	Select the interface for outgoing traffic from the Nebula Device to the Internet.
Radio Settings	
Maximum output power	Enter the maximum output power of the radio (in dBm).
Channel width	<p>Select the WiFi channel bandwidth you want the Nebula Device to use.</p> <p>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.</p> <p>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.</p> <p>Note: It is suggested that you select 20 MHz when there is more than one 2.4 GHz Nebula Device in the network.</p>
2.4 GHz channel deployment	<p>Select <b>Three-Channel Deployment</b> 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.</p> <p>Select <b>Four-Channel Deployment</b> 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. <b>Four-Channel Deployment</b> expands your pool of possible channels while keeping the channel interference to a minimum.</p> <p>Select <b>Manual</b> to choose the allowable channels 1 – 11.</p>
5 GHz channel deployment	<p>Select how you want to specify the channels the Nebula Device switches between for 5 GHz operation.</p> <p>Select <b>Auto</b> to have the Nebula Device automatically select the best channel.</p> <p>Select <b>Manual</b> to choose from the allowable channels.</p>

### 9.3.12 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 **Firewall > Configure > Firewall settings** to access this screen.

Figure 152 Firewall > Configure > Firewall settings

Firewall > Configure > [Firewall settings](#)

Firewall settings

### DNS

Address Record

FQDN	IP Address
<input type="text"/>	<input type="text"/>

[+ Add](#)

Domain Zone Forwarder

Domain Zone	IP Address	Interface
<input type="text"/>	<input type="text"/>	auto

[+ Add](#)

### 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
<input type="text"/>	<input type="text"/>	<input type="text"/>	389	<input type="text"/>	<input type="text"/>

[+ Add](#)

My LDAP Server

Name	Server address	Backup server address	Port	Base DN	Bind
<input type="text"/>	<input type="text"/>	<input type="text"/>	389	<input type="text"/>	<input type="text"/>

[+ Add](#)

My RADIUS Server

Name	Server address	Backup server address	Port	Secret	Adv
<input type="text"/>	<input type="text"/>	<input type="text"/>	1812	<input type="text"/>	<input type="text"/>

[+ Add](#)

### External User Group

[+ Add](#) Please create authentication server before add external user group

### Walled garden

Global walled garden

This is global walled garden configuration. All web authentication interface will match this policy first and the second priority is the interface walled garden policy. If needed only allow specify interface, please go to Network access method configure

[What do I enter here?](#)

### SIP ALG

SIP ALG

SIP Signaling Port

[ADVANCED OPTIONS](#)

### Advanced Options

Isolate unwanted traffic between tunnel mode APs

The following table describes the labels in this screen.

Table 129 Firewall > Configure > 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 <b>Default</b> or <b>Custom</b> advanced settings. See <a href="#">Section 9.3.12.3 on page 396</a> .
	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 129 Firewall &gt; Configure &gt; 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 alphanumeric 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 alphanumeric characters.  For example, cn=zywallAdmin specifies zywallAdmin as the user name.
Password	If required, enter the password (up to 15 alphanumeric characters) required to bind or log in to the LDAP server.
Advanced	Click to open a screen where you can select to use <b>Default</b> or <b>Custom</b> advanced settings. See <a href="#">Section 9.3.12.3 on page 396</a> .
	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 <b>Default</b> or <b>Custom</b> advanced settings. See <a href="#">Section 9.3.12.3 on page 396</a> .
	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 <b>Name</b> of the <b>Authentication Server</b> you added in <b>My AD Server</b> , <b>My LDAP Server</b> , or <b>My RADIUS Server</b> .
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 <b>On</b> to block broadcast and multicast traffic coming from Remote APs (RAPs).



### 9.3.12.1 Dynamic DNS

Enable **Dynamic DNS** to open the **Firewall > Configure > Firewall settings: Dynamic DNS** screen.

**Figure 153** Firewall > Configure > Firewall settings: Dynamic DNS

The following table describes the labels in this screen.

Table 130 Firewall > Configure > Firewall settings: Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	
Automatic registration	Click <b>On</b> to use dynamic DNS. Otherwise, select <b>Off</b> to disable it.
General Settings	
DDNS provider	Select your Dynamic DNS service provider from the drop-down list box. If you select <b>User customize</b> , create your own DDNS service.
DDNS type	Select the type of DDNS service you are using. Select <b>DynDNS custom</b> to create your own DDNS service and configure the <b>DynDNS</b> and <b>DDNS static</b> fields below. If the DDNS provider is <b>Dynu</b> , you can select the account type of <b>DynuBasic</b> or <b>DynuPremium</b> .

Table 130 Firewall &gt; Configure &gt; Firewall settings: Dynamic DNS (continued)

LABEL	DESCRIPTION
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 <b>Backup binding address</b> 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	<p>Select <b>Auto</b> 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.</p> <p>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.</p> <p>Select <b>Custom</b> if you have a static IP address. Enter the IP address to use it for the domain name.</p> <p>Select <b>Interface</b> to have the Nebula Device use the IP address of the specified interface.</p>
Backup binding address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the <b>Primary binding address</b> settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name.
IP address	<p>Select <b>Auto</b> 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.</p> <p>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.</p> <p>Select <b>Custom</b> if you have a static IP address. Enter the IP address to use it for the domain name.</p> <p>Select <b>Interface</b> to have the Security Firewall use the IP address of the specified interface.</p>
Enable wildcard	<p>This option is only available with a DynDNS account.</p> <p>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.</p>
Mail exchanger	<p>This option is only available with a DynDNS account.</p> <p>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.</p> <p>If you are using this service, type the host record of your mail server here. Otherwise, leave the field blank.</p>

Table 130 Firewall &gt; Configure &gt; Firewall settings: Dynamic DNS (continued)

LABEL	DESCRIPTION
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 <a href="http://www.dyndns.org">www.dyndns.org</a> for more information about this service.
DYNDNS Server	This field displays when you select <b>User customize</b> from the <b>DDNS provider</b> field above. Enter the IP address of the server that will host the DDNS service.
URL	This field displays when you select <b>User customize</b> from the <b>DDNS provider</b> 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 <b>User customize</b> from the <b>DDNS provider</b> field above. These are the options supported at the time of writing: <ul style="list-style-type: none"> <li>• <code>dyndns_system</code> to specify the DYNDNS Server type – for example, <code>dyndns@dyndns.org</code></li> <li>• <code>ip_server_name</code> which should be the URL to get the server's public IP address – for example, <code>http://myip.easylife.tw/</code></li> </ul>

### 9.3.12.2 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 **Firewall > Configure > 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 154 Firewall &gt; Configure &gt; Firewall settings: SIP ALG

**SIP ALG**

SIP ALG

SIP Signaling Port

**ADVANCED OPTIONS**

SIP Inactivity Timeout

SIP Media Inactivity Timeout  seconds

SIP Signaling Inactivity Timeout  seconds

Restrict Peer to Peer Signaling Connection

Restrict Peer to Peer Media Connection

The following table describes the labels in this screen.

Table 131 Firewall > Configure > 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 <b>Add</b> 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.

### 9.3.12.3 Advanced Settings

Click the **Advanced** column in the **Firewall > Configure > Firewall settings** screen to access this screen.

Figure 155 Firewall > Configure > Firewall settings: Advanced

**Advanced** ✕

Preset:

Timeout:  ✕ (1-300 seconds)

Case-Sensitive User Name:  off

NAS IP Address:  ✕

Close OK

The following table describes the labels in this screen.

Table 132 Firewall > Configure > Firewall settings: Advanced

LABEL	DESCRIPTION
Preset	Select <b>Default</b> to use the pre-defined settings, or select <b>Custom</b> 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 <b>ON</b> if the server checks the case of the user name. Otherwise, click <b>OFF</b> 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 10

# Security Gateway

## 10.1 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.

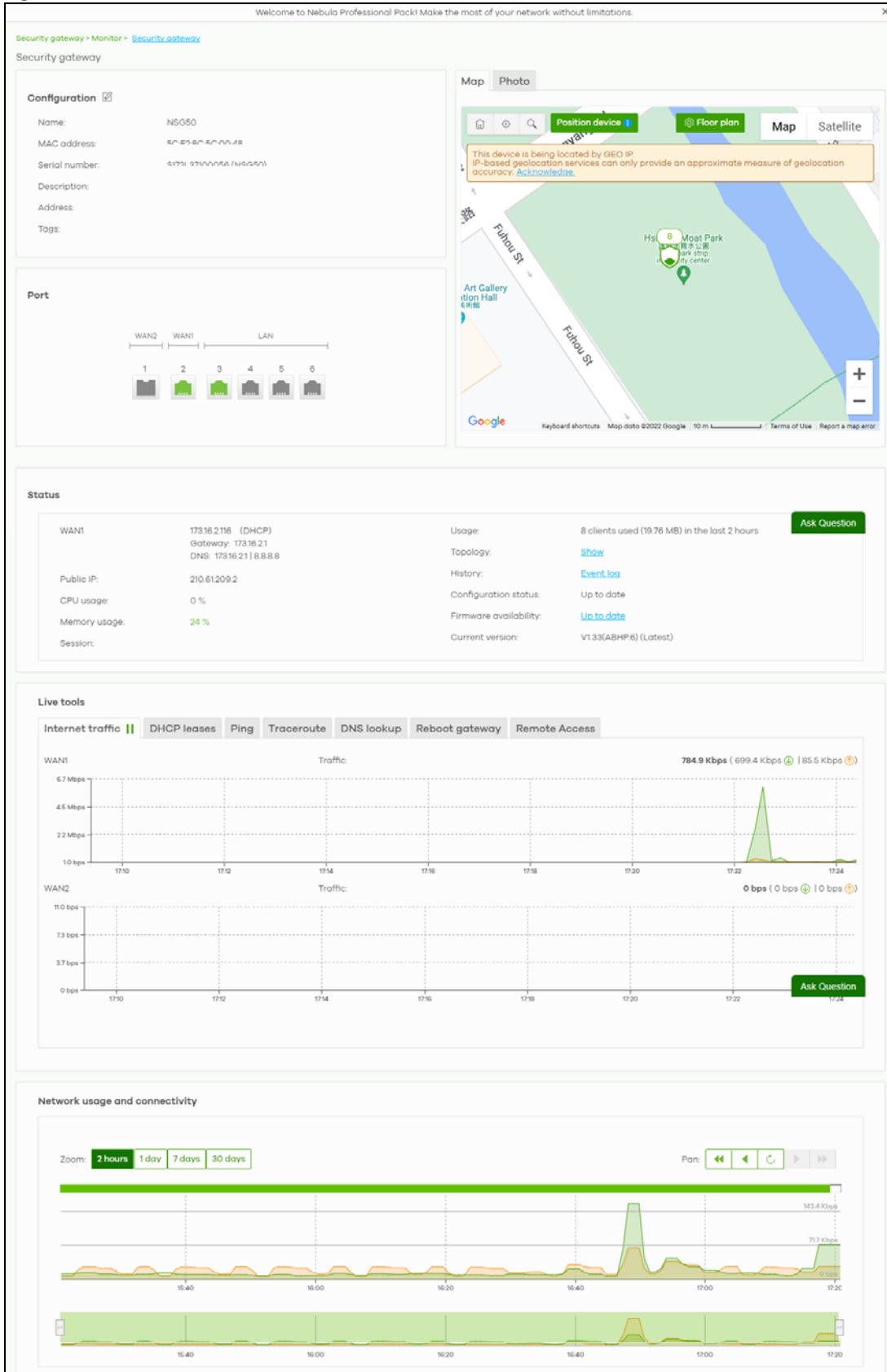
## 10.2 Monitor

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.

### 10.2.1 Security Appliance

This screen allows you to view the detailed information about a Nebula Device in the selected site. Click **Security gateway > Monitor > Security gateway** to access this screen.

Figure 156 Security gateway > Monitor > Security gateway



The following table describes the labels in this screen.

Table 133 Security gateway > Monitor > 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	<p>This shows the ports on the Nebula Device.</p> <p>The port is highlighted in green color when it is connected and the link is up.</p> <p>Move the pointer over a port to see additional port information, such as its name, connection status, MAC address, and connection speed.</p>
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	<p>This shows the location of the Nebula Device on the 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).</p> <div data-bbox="537 1213 1216 1654" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><b>Position device</b> <span style="float: right;">✕</span></p> <hr/> <p>Update my device's location. <a href="#">What is this?</a></p> <p><input checked="" type="radio"/> Use the device's IP address (GEO IP).</p> <p><input type="radio"/> Get my location from web browser.</p> <p><input type="radio"/> Use the following address or coordinates.</p> <div style="border: 1px solid #ccc; padding: 2px; margin: 5px 0; width: 100%;"> <input type="text"/> <span style="float: right;">✕</span> </div> <p style="text-align: right;"> <input type="button" value="Cancel"/> <input type="button" value="Update"/> </p> </div> <ul style="list-style-type: none"> <li>Select <b>GEO IP</b> to use the public IP address of the Nebula Device.</li> <li>Select <b>Get my location from web browser</b> to use the public IP address of the computer accessing the NCC portal.</li> <li>Select <b>Use the following address or coordinates</b> to enter the complete address or coordinates of the Nebula Device.</li> </ul> <p>Note: Nebula Devices that are offline cannot use GEO IP.</p>



Table 133 Security gateway &gt; Monitor &gt; Security gateway (continued)

LABEL	DESCRIPTION
Photo	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.
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 <b>What is this?</b> 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 <b>Show</b> to go to the <b>Site-Wide &gt; Monitor &gt; Topology</b> screen. See <a href="#">Section 7.1.7 on page 266</a> .
History	Click <b>Event log</b> to go to the <b>Security gateway &gt; Monitor &gt; Event log</b> 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 <b>Ping</b> . 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 <b>Run</b> to resolve the IP address for the specified domain name.
Reboot gateway	Click the <b>Reboot</b> 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 <b>Port</b> number and clicking <b>Establish</b> .
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.

## 10.2.2 Clients

This menu item redirects to **Site-Wide > Monitor > Clients**, with type set to **Security gateway clients**. For details, see [Section 7.1.2 on page 255](#).

## 10.2.3 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 **Security gateway > Monitor > Event Log** to access this screen.

**Figure 157** Security gateway > Monitor > Event log

Security gateway > Monitor > [Event log](#)

Event log

Keyword:  Category:

Before  10:56 1h UTC+8

338 Event log

Time	Category	Source	Destination	Detail
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	ISAKMP SA [S201711070315] is disconnected
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	The cookie pair is : 0xa8c4726c50064617 / 0x6f8f4...
2019-10-29 09:56:53	VPN	61.216.142.42	192.168.11.74	Recv.[NOTIFY:NO_PROPOSAL_CHOSEN]
2019-10-29 09:56:53	VPN	61.216.142.42	192.168.11.74	The cookie pair is : 0x6f8f47eb7aac5173 / 0xa8c472...
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	Send:[SA][VID][VID][VID][VID][VID][VID][VID][...
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

## 10.2.4 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 **Security gateway > Configure > Site-to-Site VPN** screen to view and configure a VPN rule. See [Section 10.3.6 on page 436](#) for more information.

Click **Security gateway > Monitor > VPN Connections** to access this screen.

**Figure 158** Security gateway > Monitor > VPN Connections

Security gateway > Monitor > [VPN connections](#)

VPN connections

**Connection status**

Configuration: This security gateway is exporting 1 subnet over the VPN: 100.251.0/24

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
<a href="#">Hub</a>	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	-	-
<a href="#">Site25_NCC_AE_B...</a>	-	-	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 134** Security gateway > Monitor > 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 <b>Security gateway &gt; Configure &gt; Site-to-Site VPN</b> screen, where you can modify the VPN settings.
Subnet(s)	This shows the address of the local networks behind the Nebula Device.
Status	This shows whether the VPN tunnel is connected or disconnected.
Inbound (Bytes)	This shows the amount of traffic that has gone through the VPN tunnel from the remote IPSec router to the Nebula Device since the VPN tunnel was established.
Outbound (Bytes)	This shows the amount of traffic that has gone through the VPN tunnel from the Nebula Device to the remote IPSec router since the VPN tunnel was established.
Tunnel up time	This shows how many seconds the VPN tunnel has been active.
Last heartbeat	This shows the last date and time a heartbeat packet is sent to determine if the VPN tunnel is up or down.
Client to site VPN login account	
User Name	This shows the remote user's login account name.
Hostname	This shows the name of the computer that has this L2TP VPN connection with the Nebula Device.

Table 134 Security gateway &gt; Monitor &gt; VPN Connections (continued)

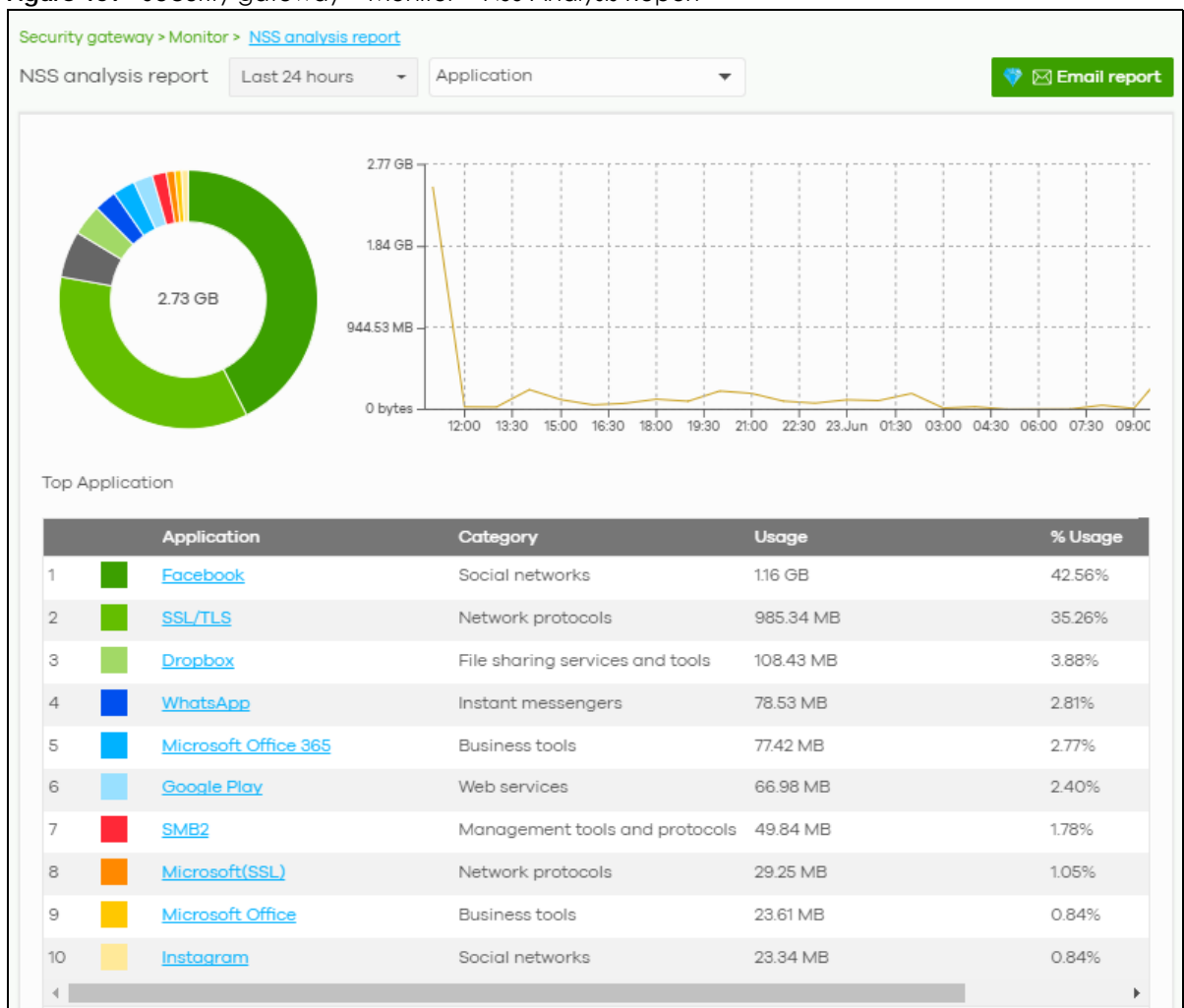
LABEL	DESCRIPTION
Assigned IP	This shows the IP address that the Nebula Device assigned for the remote user's computer to use within the L2TP VPN tunnel.
Public IP	This shows the public IP address that the remote user is using to connect to the Internet.

## 10.2.5 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 **Security gateway > Monitor > NSS Analysis Report** to access this screen.

Figure 159 Security gateway &gt; Monitor &gt; NSS Analysis Report



The following table describes the labels in this screen.

Table 135 Security gateway &gt; Monitor &gt; NSS Analysis Report

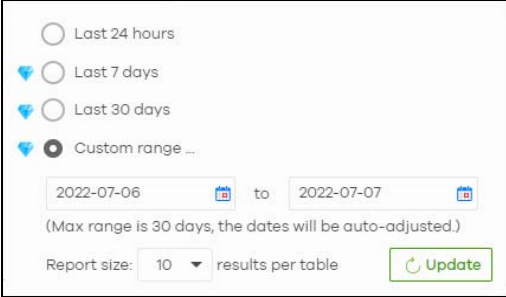
LABEL	DESCRIPTION
Security Appliance – NSS Analysis	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
	Select the type of service for which you want to view the statistics report.
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
Application	<p>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 <b>Top Application</b> under the chart to switch back to the previous screen.</p>
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	<p>This shows the name of the client who used the application.</p> <p>This field is available when you click the application name. Click the name to display the individual client statistics. See <a href="#">Section 10.2.3 on page 402</a>.</p>
IPv4 Address	<p>This shows the IPv4 address of the client who used the application.</p> <p>This field is available when you click the application name.</p>
MAC Address	<p>This shows the MAC address of the client who used the application.</p> <p>This field is available when you click the application name.</p>
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	<p>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 <b>Content Filtering</b> under the chart to switch back to the previous screen.</p>
y-axis	The y-axis shows the number of hits on web pages that the Nebula Device's content filter service has blocked.
x-axis	The x-axis shows the time period over which the web page is checked.
Website	This shows the URL of the web page to which the Nebula Device blocked access. Click a website URL to view the IPv4 addresses of the clients who tried to access the web page.

Table 135 Security gateway &gt; Monitor &gt; NSS Analysis Report (continued)

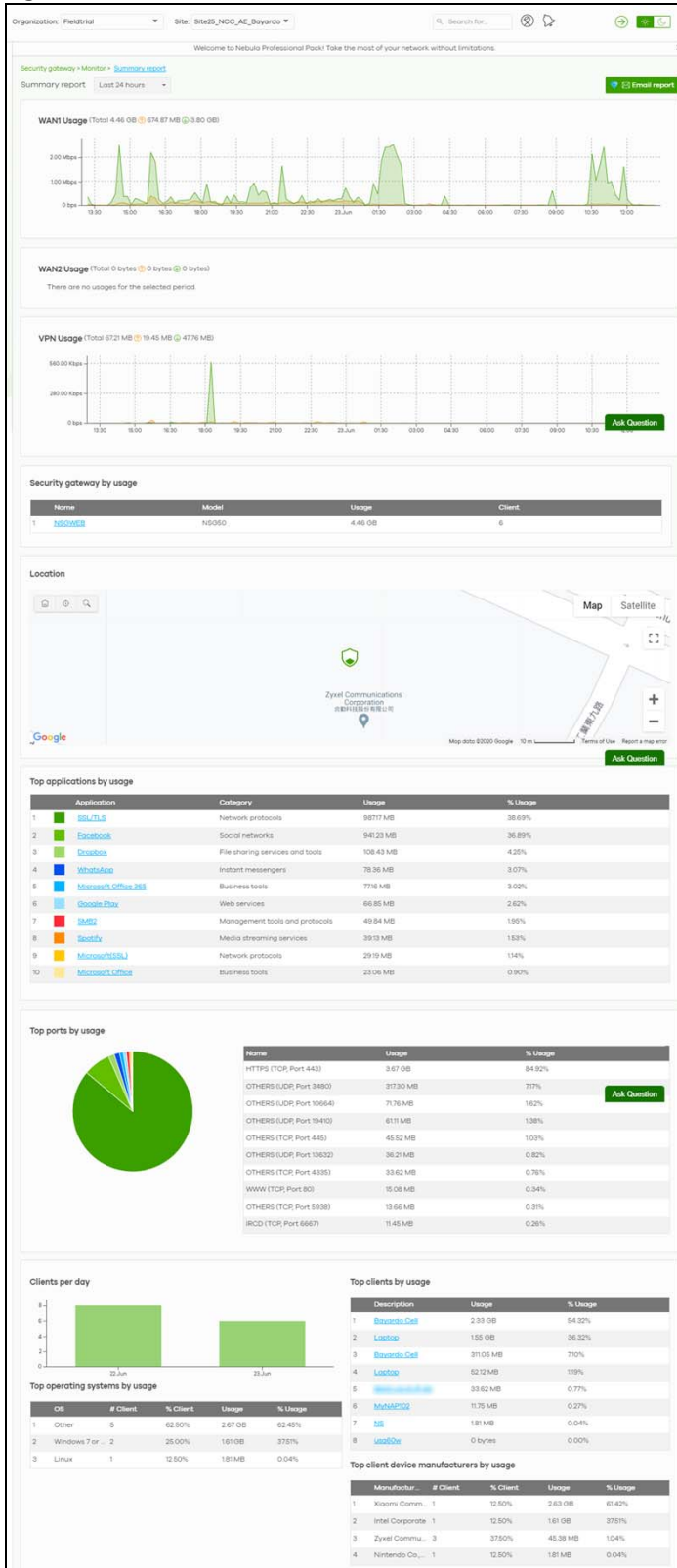
LABEL	DESCRIPTION
Description	This shows the name of the client who tried to access the web page. This field is available when you click the website URL. Click the name to display the individual client statistics. See <a href="#">Section 10.2.3 on page 402</a> .
IPv4 Address	This shows the IPv4 address 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.
<b>Anti-Virus</b> The following fields are displayed when you select <b>Anti-Virus</b> . 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 <b>Anti-Virus</b> under the chart to switch back to the previous screen.	
y-axis	The y-axis shows the total number of viruses that the gateway has detected.
x-axis	The x-axis shows the time period over which the virus is detected.
Virus Name	This shows the name of the virus that the Nebula Device has detected and blocked. Click a virus name to view the IPv4 addresses of the clients who sent the virus.
Description	This shows the name of the client who sent the virus. This field is available when you click the virus name. Click the name to display the individual client statistics. See <a href="#">Section 10.2.3 on page 402</a> .
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.
<b>Intrusion Detection / Prevention</b> The following fields are displayed when you select <b>Intrusion Detection / Prevention</b> . 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.

## 10.2.6 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 **Security gateway > Monitor > Summary Report** to access this screen.

**Figure 160** Security gateway > Monitor > Summary Report



The following table describes the labels in this screen.

Table 136 Security gateway &gt; Monitor &gt; Summary Report

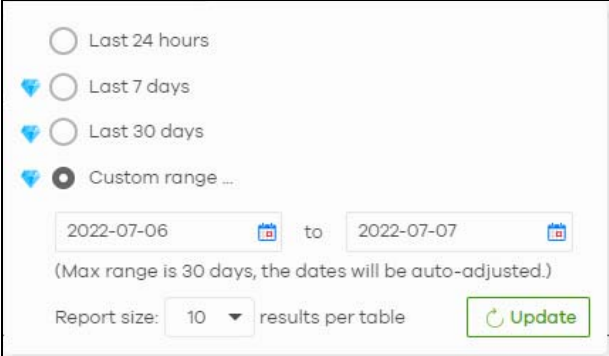
LABEL	DESCRIPTION
Security gateway – Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click 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 136 Security gateway &gt; Monitor &gt; 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.

## 10.3 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.

### 10.3.1 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 **Security gateway > Configure > 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 10.3.5 on page 433](#).

Figure 161 Security gateway > Configure > Interface addressing

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

Security gateway > Configure > 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.
- Route  
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:	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Port Group 2:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Interface**

Name	IP address	Subnet mask	VLAN ID	Port Group	Guest
LAN1	100.25.11	255.255.255.0		Port Group 1	<input type="checkbox"/>
LAN2	173.16.25.1	255.255.255.0		Port Group 2	<input checked="" type="checkbox"/>
VLAN100	192.168.100.1	255.255.255.0	100	Port Group 1	<input checked="" type="checkbox"/>
VLAN10	192.168.10.1	255.255.255.0	10	Port Group 1	<input checked="" type="checkbox"/>
VLAN250	192.168.250.1	255.255.255.0	250	Port Group 1	<input checked="" type="checkbox"/>

[Add](#)

**Static Route**

Name	Destination	Subnet mask	Next hop IP
s5	192.168.10.0	255.255.255.0	192.168.10.1

[Add](#)

**Dynamic DNS**

Automatic registration:

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: WAN1

IP address: Custom

Backup binding address

Interface: WAN1

IP address: Custom

Enable wildcard:

Mail exchanger:  (Optional)

Backup mail exchanger:

The following table describes the labels in this screen.

Table 137 Security gateway &gt; Configure &gt; Interface addressing

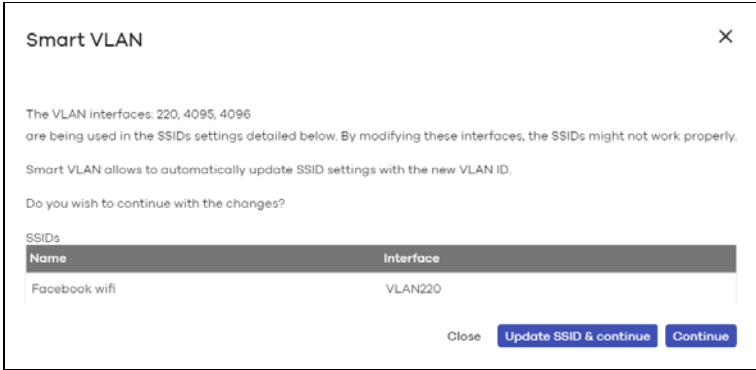
LABEL	DESCRIPTION
Network wide	
Mode	<p>Select <b>Network address translation (NAT)</b> to have the Nebula Device automatically use SNAT for traffic it routes from internal interfaces to external interfaces.</p> <p>Select <b>Router</b> to have the Nebula Device forward packets according to the routing policies. The Nebula Device does not automatically convert a packet's source IP address.</p>
Port Group Setting	<p>Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.</p> <p>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.</p> <p>For example, select a port's <b>Port Group 1</b> radio button to use the port as part of the first port group. The port will use the first group's IP address.</p> <p>Note: You cannot select ports 1 and 2, as these ports are reserved for WAN usage.</p>
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	<p>This shows the ID number of the VLAN with which the interface (network) is associated.</p> <p>If you have associated an SSID with the VLAN ID, the <b>Smart VLAN</b> screen displays after you change or delete the VLAN ID and click <b>Save</b>. You can exit the screen without saving, or apply your changes directly. If the <b>Smart guest/VLAN network</b> feature is enabled in the <b>Site-Wide &gt; Configure &gt; General settings</b> screen, you can select to apply the changes and update the SSID's VLAN setting as well.</p> 
Port group	This shows the name of the port group to which the interface (network) belongs.

Table 137 Security gateway &gt; Configure &gt; Interface addressing (continued)





LABEL	DESCRIPTION
Guest	Select <b>On</b> 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 <b>Off</b> to not use the interface as a Guest interface.  Note: If the <b>Smart guest/VLAN network</b> feature is enabled in the <b>Site-Wide &gt; Configure &gt; General settings</b> 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 <a href="#">Section 10.3.1.1 on page 414</a> 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 <a href="#">Section 10.3.1.1 on page 414</a> 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 <a href="#">Section 10.3.2.4 on page 424</a> for detailed information.
	Click this icon to remove a static route.
Add	Click this button to create a new static route. See <a href="#">Section 10.3.2.4 on page 424</a> for detailed information.
Dynamic DNS	
Automatic registration	Click <b>On</b> to use dynamic DNS. Otherwise, select <b>Off</b> to disable it.
General Settings	
DDNS provider	Select your Dynamic DNS service provider from the drop-down list box.  If you select <b>User custom</b> , create your own DDNS service.
DDNS type	Select the type of DDNS service you are using.  Select <b>User custom</b> to create your own DDNS service and configure the <b>DYNDNS Server</b> , <b>URL</b> , and <b>Additional DDNS Options</b> 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 <b>Backup binding address</b> if the interface specified by these settings is not available.

Table 137 Security gateway &gt; Configure &gt; Interface addressing (continued)

LABEL	DESCRIPTION
Interface	Select the interface to use for updating the IP address mapped to the domain name.
IP address	<p>Select <b>Auto</b> 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.</p> <p>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.</p> <p>Select <b>Custom</b> if you have a static IP address. Enter the IP address to use it for the domain name.</p> <p>Select <b>Interface</b> to have the Nebula Device use the IP address of the specified interface.</p>
Backup binding address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the <b>Primary binding address</b> settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name.
IP address	<p>Select <b>Auto</b> 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.</p> <p>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.</p> <p>Select <b>Custom</b> if you have a static IP address. Enter the IP address to use it for the domain name.</p> <p>Select <b>Interface</b> to have the Nebula Device use the IP address of the specified interface.</p>
Enable wildcard	<p>This option is only available with a DynDNS account.</p> <p>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, <code>www.yourhost.dyndns.org</code> and still reach your hostname.</p>
Mail exchanger	<p>This option is only available with a DynDNS account.</p> <p>DynDNS can route email for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes email for <code>john-doe@yourhost.dyndns.org</code> to the host record specified as the mail exchanger.</p> <p>If you are using this service, type the host record of your mail server here. Otherwise, leave the field blank.</p>
Backup mail exchanger	<p>This option is only available with a DynDNS account.</p> <p>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 <a href="http://www.dyndns.org">www.dyndns.org</a> for more information about this service.</p>
DYNDNS Server	<p>This field displays when you select <b>User custom</b> from the <b>DDNS provider</b> field above.</p> <p>Enter the IP address of the server that will host the DDNS service.</p>

Table 137 Security gateway &gt; Configure &gt; Interface addressing (continued)

LABEL	DESCRIPTION
URL	This field displays when you select <b>User custom</b> from the <b>DDNS provider</b> 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 <b>User custom</b> from the <b>DDNS provider</b> field above. These are the options supported at the time of writing: <ul style="list-style-type: none"><li>• dyndns_system to specify the DYNDNS Server type – for example, dyndns@dyndns.org</li><li>• ip_server_name which should be the URL to get the server's public IP address – for example, http://myip.easylife.tw/</li></ul>

### 10.3.1.1 Local LAN (Add VLAN)

Click the **Add** button or click the **Edit** button in the **Interface** section of the **Security gateway > Configure > Interface addressing** screen.

**Figure 162** Security gateway > Configure > Interface addressing: Local LAN (VLAN)

The following table describes the labels in this screen.

**Table 138** Security gateway > Configure > 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 138 Security gateway &gt; Configure &gt; Interface addressing: Local LAN (VLAN) (continued)

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:  <b>None</b> – the Nebula Device does not provide any DHCP service. There is already a DHCP server on the network.  <b>DHCP Relay</b> – the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network.  <b>DHCP Server</b> – 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 <b>DHCP Relay</b> .	
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 <b>DHCP Server</b> .	
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 <b>Add new</b> under <b>Static DHCP Table</b> .
Pool size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's <b>Subnet mask</b> . For example, if the <b>Subnet mask</b> is 255.255.255.0 and <b>IP pool start address</b> 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.  <b>Custom Defined</b> – enter a static IP address.  <b>From ISP</b> – select the DNS server that another interface received from its DHCP server.  <b>NSG</b> – 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 138 Security gateway &gt; Configure &gt; Interface addressing: Local LAN (VLAN) (continued)

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:  <b>infinite</b> – select this if IP addresses never expire. <b>days, hours, minutes</b> – select this to enter how long IP addresses are valid.
Extended options	This table is available if you selected <b>DHCP server</b> .  Configure this table if you want to send more information to DHCP clients through DHCP packets.  Click <b>Add new</b> to create an entry in this table. See <a href="#">Section 10.3.2.3 on page 422</a> 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 <b>IP pool start address</b> and <b>Pool size</b> .  Click <b>Add new</b> 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 <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.

## 10.3.2 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.

### 10.3.2.1 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 163** Security gateway > Configure > Interface addressing (LAG Interface Type)

Security gateway > Configure > [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	P7	P8
LAN1-6	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
LAG1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
LAG2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

**Interface**

Name	IP address	Subnet mask	VLAN ID	Port Group	Guest
LAN1	0.0.0.0	0.0.0.0		LAN1	<input type="checkbox"/>
LAN2	0.0.0.0	0.0.0.0		LAN2	<input type="checkbox"/>
LAN3	0.0.0.0	0.0.0.0		LAN3	<input type="checkbox"/>
LAN4	0.0.0.0	0.0.0.0		LAN4	<input type="checkbox"/>
LAN5	0.0.0.0	0.0.0.0		LAN5	<input type="checkbox"/>
LAN6	0.0.0.0	0.0.0.0		LAN6	<input type="checkbox"/>
LAG1	192.168.1.0	255.255.255.0		LAG1	<input type="checkbox"/>
LAG2	192.168.2.0	255.255.255.0		LAG2	<input type="checkbox"/>

[+ Add](#)



**Static Route**

The following table describes the labels in this screen.

**Table 139** Security gateway > Configure > 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 139 Security gateway &gt; Configure &gt; Interface addressing (LAG Interface Type) (continued)

LABEL	DESCRIPTION						
VLAN ID	<p>This shows the ID number of the VLAN with which the interface (network) is associated.</p> <p>Note: If you have associated an SSID with the VLAN ID, the <b>Smart VLAN</b> screen displays after you change or delete the VLAN ID and click <b>Save</b>. You can exit the screen without saving, or apply your changes directly. If the <b>Smart guest/VLAN network</b> feature is enabled in the <b>Site-Wide &gt; Configure &gt; General settings</b> screen, you can select to apply the changes and update the SSID's VLAN setting as well.</p> <div data-bbox="496 537 1248 903" style="border: 1px solid black; padding: 5px;"> <p><b>Smart VLAN</b> <span style="float: right;">✕</span></p> <p>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.</p> <p>Smart VLAN allows to automatically update SSID settings with the new VLAN ID.</p> <p>Do you wish to continue with the changes?</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">SSIDs</th> <th style="text-align: left;">Interface</th> </tr> <tr> <th style="text-align: left;">Name</th> <th style="text-align: left;">Interface</th> </tr> </thead> <tbody> <tr> <td>Facebook wifi</td> <td>VLAN220</td> </tr> </tbody> </table> <p style="text-align: right;">Close <span style="margin-left: 10px;">Update SSID &amp; continue</span> <span style="margin-left: 10px;">Continue</span></p> </div>	SSIDs	Interface	Name	Interface	Facebook wifi	VLAN220
SSIDs	Interface						
Name	Interface						
Facebook wifi	VLAN220						
Port group	<p>For an Ethernet port, this shows the name of the port group to which the port belongs.</p> <p>For a link aggregation group, this shows its member port groups.</p>						
Guest	<p>Select <b>On</b> 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.</p> <p>Otherwise, select <b>Off</b> to not use the interface as a Guest interface.</p> <p>Note: If the <b>Smart guest/VLAN network</b> feature is enabled in the <b>Site-Wide &gt; Configure &gt; General settings</b> 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.</p>						
	<p>Click this button to modify the network settings. See <a href="#">Section 10.3.1.1 on page 414</a> for detailed information.</p> <p>If the interface is a member of a link aggregation group, you cannot edit the interface's network settings.</p>						
	<p>Click this icon to delete a VLAN entry or link aggregation group.</p>						
Add	<p>Click this button to create a VLAN or link aggregation group.</p> <ul style="list-style-type: none"> <li>• For details on creating a VLAN, see <a href="#">Section 10.3.1.1 on page 414</a>.</li> <li>• For details on creating a link aggregation group, see <a href="#">Section 10.3.2.2 on page 419</a>.</li> </ul>						

### 10.3.2.2 Local LAN (LAG Interface Type)

Click the **Add** button or click the **Edit** button in the **Interface** section of the **Security gateway > Configure > Interface addressing** screen.

**Figure 164** Security gateway > Configure > Interface addressing: Local LAN (LAG Interface Type)

The following table describes the labels in this screen.

**Table 140** Security gateway > Configure > 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".
LAG Configuration	

Table 140 Security gateway &gt; Configure &gt; Interface addressing: Local LAN (LAG Interface Type)

LABEL	DESCRIPTION
Mode	Select a mode for this Link Aggregation Group (LAG) interface. Choices are as follows: <ul style="list-style-type: none"> <li>• <b>active-backup</b>: Only one port in the LAG interface is active and another port becomes active only if the active port fails.</li> <li>• <b>802.3ad</b> (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.</li> <li>• <b>balance-alb</b> (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.</li> </ul>
Link Monitoring	Select how each link is monitored. <p><b>mii</b> (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.</p> <p><b>arp</b> – 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.</p>
Miimom	This field displays for <b>mii</b> 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 <b>mii</b> Link Monitoring. Set the waiting time in milliseconds to confirm that a member interface link is up.
Downdelay	This field displays for <b>mii</b> 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.) <p>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.</p>
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: <p><b>None</b> – the Nebula Device does not provide any DHCP services. There is already a DHCP server on the network.</p> <p><b>DHCP Relay</b> – the Nebula Device routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network.</p> <p><b>DHCP Server</b> – 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.</p>
These fields appear if the Nebula Device is a <b>DHCP Relay</b> .	
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 <b>DHCP Server</b> .	
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 <b>Add new</b> under <b>Static DHCP Table</b> .

Table 140 Security gateway &gt; Configure &gt; Interface addressing: Local LAN (LAG Interface Type)

LABEL	DESCRIPTION
Pool size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's <b>Subnet mask</b> . For example, if the <b>Subnet mask</b> is 255.255.255.0 and <b>IP pool start address</b> 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.  <b>Custom Defined</b> – enter a static IP address.  <b>From ISP</b> – select the DNS server that another interface received from its DHCP server.  <b>NSG</b> – 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:  <b>infinite</b> – select this if IP addresses never expire <b>days, hours, minutes</b> – select this to enter how long IP addresses are valid.
Extended options	This table is available if you selected <b>DHCP server</b> .  Configure this table if you want to send more information to DHCP clients through DHCP packets.  Click <b>Add new</b> to create an entry in this table. See <a href="#">Section 10.3.2.3 on page 422</a> 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 <b>IP pool start address</b> and <b>Pool size</b> .  Click <b>Add new</b> 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 <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.

### 10.3.2.3 DHCP Option

Click the **Add new** button under **Extended options** in the **Security gateway > Configure > Interfaces addressing: Local LAN** screen.

**Figure 165** Security gateway > Configure > Interfaces addressing: Local LAN: DHCP Option

The following table describes the labels in this screen.

**Table 141** Security gateway > Configure > Interfaces 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 <b>User_Defined</b> in the <b>Option</b> 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 <b>User_Defined</b> in the <b>Option</b> field, enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. If you selected <b>User_Defined</b> in the <b>Option</b> 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 <b>TFTP Server Name (66)</b> and the type is <b>TEXT</b> , 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 <b>Time Server (4)</b> , <b>NTP Server (41)</b> , <b>SIP Server (120)</b> , <b>CAPWAP AC (138)</b> , or <b>TFTP Server (150)</b> , 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 <b>VIVC (124)</b> or <b>VIVS (125)</b> , 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 141 Security gateway &gt; Configure &gt; Interfaces addressing: Local LAN: DHCP Option (continued)

LABEL	DESCRIPTION
First class Second class	If you selected <b>VIVC (124)</b> , 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 <b>VIVS (125)</b> , enter additional information for the corresponding enterprise number in these fields.
First FQDN Second FQDN Third FQDN	If the <b>Type</b> is <b>FQDN</b> , 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 <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.

### 10.3.2.4 Static Route

Click the **Add** button in the **Static Route** section of the **Security gateway > Configure > Interfaces addressing** screen.

Figure 166 Security gateway &gt; Configure &gt; Interfaces addressing: Static Route

The following table describes the labels in this screen.

Table 142 Security gateway &gt; Configure &gt; Interfaces 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 <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.



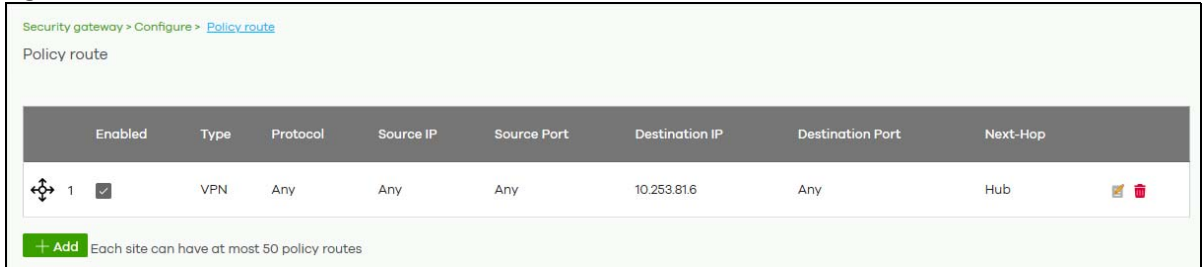
## 10.3.3 Policy Route

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 **Security gateway > Configure > Policy Route** to access this screen.

**Figure 167** Security gateway > Configure > Policy Route



The following table describes the labels in this screen.

**Table 143** Security gateway > Configure > 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 ( <b>INTRANET</b> ), VPN tunnel ( <b>VPN</b> ) or outgoing interface ( <b>INTERNET</b> ).
Protocol	This displays the IP protocol that defines the service used by the packets. <b>Any</b> 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. <b>Any</b> 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. <b>Any</b> 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 <a href="#">Section 10.3.4.1 on page 431</a> for more information.

### 10.3.3.1 Add/Edit policy route

Click the **Add** button or an edit icon in the **Security gateway > Configure > Policy Route** screen to access this screen.

**Figure 168** Security gateway > Configure > Policy Route: Add/Edit

The following table describes the labels in this screen.

Table 144 Security gateway &gt; Configure &gt; Policy Route: Add/Edit

LABEL	DESCRIPTION
Type	Select <b>Internet Traffic</b> to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).  Select <b>Intranet Traffic</b> to route the matched packets to the next-hop router or switch you specified in the <b>Next-Hop</b> field.  Select <b>VPN Traffic</b> to route the matched packets through the VPN tunnel you specified in the <b>Next-Hop</b> field.
Protocol	Select <b>TCP</b> or <b>UDP</b> if you want to specify a protocol for the policy route. Otherwise, select <b>Any</b> .
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. <b>Any</b> 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. <b>Any</b> means all service ports.
Next-Hop	If you select <b>Internet Traffic</b> in the <b>Type</b> 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 <b>Intranet Traffic</b> in the <b>Type</b> field, enter the IP address of the next-hop router or switch.  If you select <b>VPN Traffic</b> in the <b>Type</b> 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.

### 10.3.4 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 **Security gateway > Configure > 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 169 Security gateway > Configure > Firewall

Security gateway > Configure > Firewall

Firewall

**Security policy**

Policy rules

Destination	Dest port	Schedule	Description
10.253.615	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
<input checked="" type="checkbox"/>	WAN1			any	

+ Add

Virtual Server

Enabled	Uplink	Protocol	Public IP	Public port	LAN IP
<input checked="" type="checkbox"/>	WAN1	Any	any		

+ Add

The following table describes the labels in this screen.

Table 145 Security gateway &gt; Configure &gt; 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 <b>Deny</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.  Select <b>Allow</b> 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 <a href="#">Section 10.3.4.1 on page 431</a> for how to create an application patrol profile.
Protocol	Select the IP protocol to which this rule applies. Choices are: <b>TCP</b> , <b>UDP</b> , and <b>Any</b> .
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 <b>any</b> 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 <b>any</b> 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 <b>any</b> to apply the rule to all ports.
Schedule	Select the name of the schedule profile that the rule uses. <b>Always</b> 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.  <b>Any</b> allows all IP addresses.
Application Patrol	
Application monitor	Click <b>On</b> to enable traffic analysis for all applications and display information about the top 10 applications in the <b>Site-wide &gt; Monitor &gt; Dashboard: Traffic Summary</b> screen. Otherwise, select <b>Off</b> 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 <a href="#">Section 10.3.4.1 on page 431</a> 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 145 Security gateway &gt; Configure &gt; 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 <a href="#">Section 10.3.4.2 on page 432</a> for more information.
SIP ALG	
SIP ALG	<p>Session Initiation Protocol (SIP) is an application-layer protocol that can be used to create voice and multimedia sessions over the Internet.</p> <p>Application Layer Gateway (ALG) allows the following applications to operate properly through the Nebula Device's NAT.</p> <p>Turn <b>on</b> 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.</p>
SIP Signaling Port	If you are using a custom UDP port number (not <b>5060</b> ) 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	<p>Use this field to set how many <b>seconds (1 – 86400)</b> the Nebula Device will allow a SIP session to remain idle (without voice traffic) before dropping it.</p> <p>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.</p>
SIP Signaling Inactivity Timeout	<p>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.</p> <p>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 (<b>1 – 86400</b>).</p>
NAT	
1:1 NAT	
<p>A 1:1 NAT rule maps a public IP address to the private IP address of a LAN server to give WAN users access.</p> <p>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.</p>	
	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	<p>Enter the destination IP address of the packets received by the interface specified in this NAT rule.</p> <p>Note: To enable NAT loop-back, enter a specific IP address instead of <b>any</b> in this field. NAT loop-back allows communications between two hosts on the LAN behind the Nebula Device through an external IP address.</p>
LAN IP	Specify to which translated destination IP address this NAT rule forwards packets.
Allowed Remote IP	<p>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.</p> <p><b>any</b> allows all IP addresses.</p>

Table 145 Security gateway &gt; Configure &gt; 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 ( <b>TCP</b> , <b>UDP</b> , or <b>Any</b> ) 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 <b>any</b> 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.  <b>any</b> 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.

### 10.3.4.1 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 **Security gateway > Configure > 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 170** Security gateway > Configure > Firewall: Add an application profile

The following table describes the labels in this screen.

**Table 146** Security gateway > Configure > 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 ( <b>ON</b> ) or not ( <b>OFF</b> ) 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 <b>All</b> or select an application within the category to apply the policy.
Policy	Select the default action for the applications selected in this category. <b>Forward</b> – the Nebula Device routes packets that matches these application signatures. <b>Drop</b> – the Nebula Device silently drops packets that matches these application signatures without notification. <b>Reject</b> – 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 <b>Add</b> 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.

### 10.3.4.2 Create new schedule

Click the **Add** button in the **Schedule Profiles** section of the **Security gateway > Configure > Firewall** screen to access this screen.



**Figure 171** Security gateway > Configure > Firewall: Add a schedule profile

**Create new schedule** ✕

Local time zone: (You can set this on [General setting](#))

Name:  ✕ Template: Always on ▼

Day	Availability
Sunday	<input checked="" type="radio"/> on <input type="radio"/> off 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Monday	<input checked="" type="radio"/> on <input type="radio"/> off 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Tuesday	<input checked="" type="radio"/> on <input type="radio"/> off 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Wednesday	<input checked="" type="radio"/> on <input type="radio"/> off 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Thursday	<input checked="" type="radio"/> on <input type="radio"/> off 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Friday	<input checked="" type="radio"/> on <input type="radio"/> off 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00

Close Add

The following table describes the labels in this screen.

**Table 147** Security gateway > Configure > 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 <b>Custom schedule</b> 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 <b>On</b> to enable the associated rule at the specified time on this day. Otherwise, select <b>Off</b> 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.

### 10.3.5 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/spyware infection.

Click **Security gateway > Configure > 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 172 Security gateway > Configure > Security service

Security gateway > Configure > Security service

Security service

**Content filtering**

Enabled

Interface	Enabled
LAN1	<input checked="" type="checkbox"/>
LAN2	<input checked="" type="checkbox"/>
VLAN100	<input checked="" type="checkbox"/>
VLAN10	<input checked="" type="checkbox"/>
VLAN250	<input checked="" type="checkbox"/>

Denied access message: This category has been blocked. Please contact the network admin.

Redirect URL:

Block list:

White list:

**Block Category**

Templates: Security

Test URL:

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

Block list:

White list:

**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

Prevention

The following table describes the labels in this screen.

Table 148 Security gateway &gt; Configure &gt; Security service

LABEL	DESCRIPTION
Content Filtering	
Enabled	Click <b>ON</b> to enable the content filtering feature on the Nebula Device. Otherwise, click <b>OFF</b> to disable it.
Interface	This shows the name of the interfaces created on the Nebula Device. Click <b>ON</b> to enable content filtering on the interfaces.
Denied access message	<p>Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0–9a–zA–Z;/?:@&amp;=+\$\._!~*()%). For example, "Access to this web page is not allowed. Please contact the network administrator".</p> <p>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.</p>
Redirect URL	<p>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.</p> <p>Use "http://" or "https://" followed by up to 262 characters (0–9a–zA–Z;/?:@&amp;=+\$\._!~*()%). For example, http://192.168.1.17/blocked access.</p>
Black list	<p>Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0–9a–z–). The casing does not matter.</p>
White list	<p>Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.</p> <p>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.</p> <p>Use up to 127 characters (0–9a–z–). The casing does not matter.</p>
<p><b>Block Category</b></p> <p>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 <b>Denied access message</b> field along with the category of the blocked web page.</p>	
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 <b>Custom</b> and manually select categories in this section to control access to specific types of Internet content.
Test URL	<p>You can check which category a web page belongs to. Enter a web site URL in the text box.</p> <p>When the content filter is active, you should see the web page's category. The query fails if the content filter is not active.</p> <p>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. <b>Test URL</b> displays both results in the test.</p>

Table 148 Security gateway &gt; Configure &gt; 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 <b>Current Version</b> of the anti-virus definition, its <b>Signature Number</b> and the <b>Released Date</b> .
Enabled	Click <b>On</b> to enable anti-virus on the Nebula Device. Otherwise, select <b>Off</b> 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. <ul style="list-style-type: none"> <li>Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed.</li> <li>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.</li> <li>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.</li> <li>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.</li> <li>The whole file name has to match if you do not use a question mark or asterisk.</li> <li>If you do not use a wildcard, the Nebula Device checks up to the first 80 characters of a file name.</li> </ul>
Intrusion Detection / Prevention System	
Signature Information	This shows the <b>Current Version</b> of the anti-intrusion definition, its <b>Signature Number</b> and the <b>Released Date</b> .
Detection	Click <b>On</b> to detect malicious or suspicious packets. Otherwise, select <b>Off</b> to disable it.
Prevention	Click <b>On</b> to identify and respond to intrusions. Otherwise, select <b>Off</b> to disable it.

### 10.3.6 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 **Security gateway > Configure > Site-to-Site VPN** to access this screen.

Figure 173 Security gateway &gt; Configure &gt; Site-to-Site VPN

Security gateway > Configure > [Site-to-Site VPN](#)

Site-to-Site VPN

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

Outgoing interface: WANI

Local networks

Name	Subnet	Use VPN
LAN1	192.168.1.0/24	<input checked="" type="checkbox"/>
LAN2	192.168.2.0/24	<input checked="" type="checkbox"/>

VPN Area: Default

Nebula VPN enable:

Nebula VPN topology: Split tunnel (send only site-to-site traffic over the VPN)  
Hub-and-Spoke

Branch to branch VPN:

Hubs (peers connect to):

Area communication:

NAT traversal: IP or FQDN

Remote VPN 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	Ipssec policy	Preshared secret	Availability
<input checked="" type="checkbox"/>				Default		This site

+ Add

The following table describes the labels in this screen.

Table 149 Security gateway &gt; Configure &gt; Site-to-Site VPN

LABEL	DESCRIPTION
Outgoing Interface	Select the WAN interface to which the VPN connection is going. Select <b>AUTO</b> 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 <b>Outgoing Interface</b> to <b>AUTO</b> .
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 <a href="#">Section 6.3.9.2 on page 242</a> .

Table 149 Security gateway &gt; Configure &gt; 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 <b>Disable</b> to not set a VPN connection. In the <b>Site-to-Site</b> 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 <b>Hub-and-Spoke</b> 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 <b>Server-and-Client</b> 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 <b>Topology</b> to <b>Hub-and-Spoke</b> . 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 <b>Hub-and-Spoke</b> 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 <b>Topology</b> to <b>Server-and-Client</b> . 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 <b>On</b> 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 <a href="#">Section 10.3.6.1 on page 439</a> 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 149 Security gateway &gt; Configure &gt; Site-to-Site VPN (continued)

LABEL	DESCRIPTION
Availability	Select <b>All sites</b> to allow the peer gateway to connect to any Nebula Device in the organization through a VPN tunnel.  Select <b>This site</b> 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.

### 10.3.6.1 Custom IPSec Policy

Click an existing **IPSec Policy** button in the **Non-Nebula VPN peers** section of the **Security gateway > Configure > Site-to-Site VPN** screen to access this screen.

**Figure 174** Security gateway > Configure > Site-to-Site VPN: Custom IPsec Policy

**Custom** X

Preset

**Phase 1**

IKE version

Encryption

Authentication

Diffie-Hellman group

Lifetime (seconds)

**Advanced**

**Phase 2**

Set	Encryption	Authentication
Set 1	<input type="text" value="3DES"/>	<input type="text" value="SHA128"/>
Set 2	<input type="text" value="None"/>	<input type="text" value="None"/>
Set 3	<input type="text" value="None"/>	<input type="text" value="None"/>

PFS group

Lifetime (seconds)

Close

The following table describes the labels in this screen.

**Table 150** Security gateway > Configure > Site-to-Site VPN: Custom IPsec Policy

LABEL	DESCRIPTION
Preset	Select a pre-defined IPsec policy, or select <b>Custom</b> 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 150 Security gateway &gt; Configure &gt; Site-to-Site VPN: Custom IPSec Policy (continued)

LABEL	DESCRIPTION
IKE version	<p>Select <b>IKEv1</b> or <b>IKEv2</b>.</p> <p><b>IKEv1</b> applies to IPv4 traffic only. <b>IKEv2</b> 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.</p>
Encryption	<p>Select which key size and encryption algorithm to use in the IKE SA. Choices are:</p> <p><b>DES</b> – a 56-bit key with the DES encryption algorithm</p> <p><b>3DES</b> – a 168-bit key with the DES encryption algorithm</p> <p><b>AES128</b> – a 128-bit key with the AES encryption algorithm</p> <p><b>AES192</b> – a 192-bit key with the AES encryption algorithm</p> <p><b>AES256</b> – a 256-bit key with the AES encryption algorithm</p> <p>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.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IKE SA.</p> <p>Choices are <b>SHA128</b>, <b>SHA256</b>, <b>SHA512</b> and <b>MD5</b>. SHA is generally considered stronger than MD5, but it is also slower.</p> <p>The remote IPSec router must use the same authentication algorithm.</p>
Diffie-Hellman group	<p>Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are:</p> <p><b>DH1</b> – use a 768-bit random number</p> <p><b>DH2</b> – use a 1024-bit random number</p> <p><b>DH5</b> – use a 1536-bit random number</p> <p><b>DH14</b> – use a 2048-bit random number</p> <p>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.</p>
Lifetime (seconds)	<p>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.</p>
Advanced	<p>Click this to display a greater or lesser number of configuration fields.</p>
Mode	<p>Select the negotiation mode to use to negotiate the IKE SA. Choices are:</p> <p><b>Main</b> – this encrypts the Nebula Device's and remote IPSec router's identities but takes more time to establish the IKE SA</p> <p><b>Aggressive</b> – this is faster but does not encrypt the identities</p> <p>The Nebula Device and the remote IPSec router must use the same negotiation mode.</p>
Local ID	<p>Enter the identity of the Nebula Device during authentication. <b>Any</b> indicates that the remote IPSec router does not check the identity of the Nebula Device.</p>
Peer ID	<p>Enter the identity of the remote IPSec router during authentication. <b>Any</b> indicates that the Nebula Device does not check the identity of the remote IPSec router.</p>
Phase 2	<p>Phase 2 uses the SA that was established in phase 1 to negotiate SAs for IPSec.</p>

Table 150 Security gateway &gt; Configure &gt; Site-to-Site VPN: Custom IPSec Policy (continued)

LABEL	DESCRIPTION
Encryption	<p>Select which key size and encryption algorithm to use in the IPSec SA. Choices are:</p> <p><b>(none)</b> – no encryption key or algorithm</p> <p><b>DES</b> – a 56-bit key with the DES encryption algorithm</p> <p><b>3DES</b> – a 168-bit key with the DES encryption algorithm</p> <p><b>AES128</b> – a 128-bit key with the AES encryption algorithm</p> <p><b>AES192</b> – a 192-bit key with the AES encryption algorithm</p> <p><b>AES256</b> – a 256-bit key with the AES encryption algorithm</p> <p>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.</p> <p>Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IPSec SA.</p> <p>Choices are <b>None</b>, <b>MD5</b>, <b>SHA128</b>, <b>SHA256</b>, and <b>SHA512</b>. SHA is generally considered stronger than MD5, but it is also slower.</p> <p>The Nebula Device and the remote IPSec router must both have a proposal that uses the same authentication algorithm.</p>
PFS group	<p>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:</p> <p><b>None</b> – disable PFS</p> <p><b>DH1</b> – enable PFS and use a 768-bit random number</p> <p><b>DH2</b> – enable PFS and use a 1024-bit random number</p> <p><b>DH5</b> – enable PFS and use a 1536-bit random number</p> <p><b>DH14</b> – enable PFS and use a 2048-bit random number</p> <p>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.</p> <p>PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.</p>
Lifetime (seconds)	<p>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.</p>
<p>VPN tunnel interface (optional)</p> <p>IPSec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.</p> <p>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.</p> <p>This section is available when you select <b>IKEv2</b> in the <b>IKE Version</b> field.</p>	
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.

## 10.3.7 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 **Security gateway > Configure > Remote access VPN** to access this screen.

**Figure 175** Security gateway > Configure > Remote access VPN

Security gateway > Configure > Remote access VPN

Remote access VPN

IPSec VPN server  [Download VPN Client](#)

Outgoing interface: WANI

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 [Send Email](#)

The following table describes the labels in this screen.

Table 151 Security gateway > Configure > Remote access VPN


LABEL	DESCRIPTION
	Click this icon to download VPN client software.
IPSec VPN server	Select to enable the <b>IPSec client</b> feature on the Nebula Device. Otherwise, select <b>Disable</b> 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 <b>Use Google Public DNS</b> to use the DNS service offered by Google. Otherwise, select <b>Specify nameserver</b> to enter a static IP address.
Custom nameservers	If you select <b>Specify nameserver</b> in the <b>DNS name servers</b> 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 <b>No WINS Servers</b> to not send WINS server addresses to the users. Otherwise, select <b>Specify nameserver</b> to enter the IP addresses of WINS servers to assign to the remote users.
Custom nameservers	If you select <b>Specify nameserver</b> in the <b>WINS</b> field, manually enter the WINS server IP addresses.
Secret	Enter the pre-shared key (password) which is used to set up the <b>IPSec</b> 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 <b>Disable</b> 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 <b>Use Google Public DNS</b> to use the DNS service offered by Google. Otherwise, select <b>Specify nameserver</b> to enter a static IP address.
Custom nameservers	If you select <b>Specify nameserver</b> in the <b>DNS name servers</b> 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 <b>No WINS Servers</b> to not send WINS server addresses to the users. Otherwise, select <b>Specify nameserver</b> to enter the IP addresses of WINS servers to assign to the remote users.
Custom nameservers	If you select <b>Specify nameserver</b> in the <b>WINS</b> 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 151 Security gateway &gt; Configure &gt; 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	<p>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.</p> <p>You can send the email to one or more email addresses.</p> <ul style="list-style-type: none"> <li>• If <b>Authentication</b> is set to <b>Nebula Cloud Authentication</b>, the default email address list contains all authorized VPN user email addresses and your email address.</li> <li>• If <b>Authentication</b> is set to <b>AD and RADIUS Authentication</b>, the default email address list contains your user email address.</li> </ul>

### 10.3.8 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 **Security gateway > Configure > Captive portal** to access this screen.

Figure 176 Security gateway &gt; Configure &gt; Captive portal


Security gateway > Configure > Captive portal

Captive portal


Interface:  ▼

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:  [Upload a logo](#)

Message:

**Success page**

Message:

**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:

or Cancel

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

The following table describes the labels in this screen.

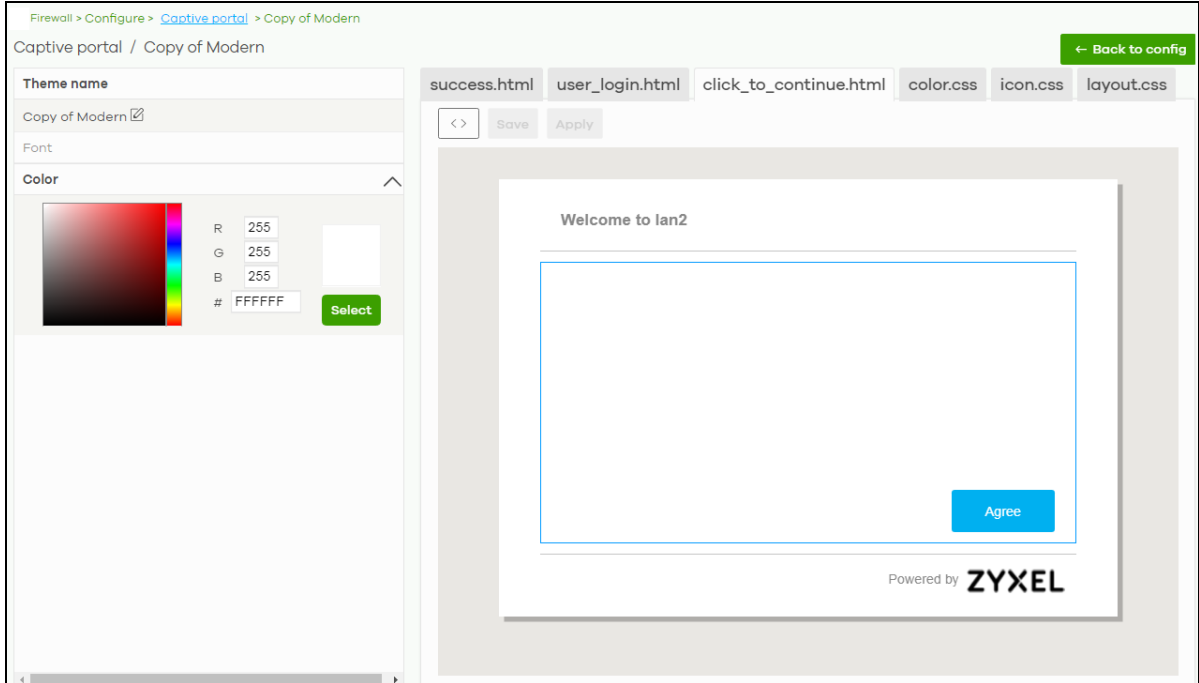
Table 152 Security gateway > Configure > Captive portal

LABEL	DESCRIPTION
Interface	Select the Nebula Device's interface (network) to which the settings you configure here is applied.
Themes	<p>This section is not configurable when <b>External captive portal URL</b> is set to <b>ON</b>.</p> <ul style="list-style-type: none"> <li>Click the <b>Preview</b> icon at the upper right of a theme image to display the portal page in a new frame.</li> <li>Click the <b>Copy</b> icon to create a new custom theme (portal page).</li> <li>Click the <b>Edit</b> icon of a custom theme to go to a screen, where you can view and configure the details of the custom portal pages. See <a href="#">Section 10.3.8.1 on page 447</a>.</li> <li>Click the <b>Remove</b> icon to delete a custom theme.</li> </ul> <p>Select the theme you want to use on the specified interface.</p>
Click-to-continue/Sign-on page	
This section is not configurable when <b>External captive portal URL</b> is set to <b>ON</b> .	
Logo	<p>This shows the logo image that you uploaded for the customized login page.</p> <p>Click <b>Upload a logo</b> and specify the location and file name of the logo graphic or click <b>Browse</b> to locate it. You can use the following image file formats: GIF, PNG, or JPG.</p>
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	<p>Select <b>On</b> 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.</p> <p>Specify the login page's URL; for example, <code>http://IIS server IP Address/login.asp</code>. The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>
Captive portal behavior	
After the captive portal page where the user should go?	Select <b>To promotion URL</b> and specify the URL of the web site/page to which the user is redirected after a successful login. Otherwise, select <b>Stay on Captive portal authenticated successfully page</b> .

### 10.3.8.1 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 **Security gateway > Configure > Captive portal** screen to access this screen.

Figure 177 Security gateway &gt; Configure &gt; Captive portal: Edit



The following table describes the labels in this screen.

Table 153 Security gateway &gt; Configure &gt; Captive portal: Edit

LABEL	DESCRIPTION
Back to config	Click this button to return to the <b>Captive portal</b> 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 <b>Select</b> 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.



## 10.3.9 Network Access Method

Use this screen to enable or disable web authentication on an interface.

Click **Security gateway > Configure > Network access method** to access this screen.

**Figure 178** Security gateway > Configure > Network access method

Security gateway > Configure > Network access method

Network access method

Interfaces: LAN1

---

**Network Access**

Disable  
 Users can access the network directly

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

Sign-on-with Nebula Cloud Authentication

---

**Walled garden** on

Walled garden ranges

[What do I enter here?](#)

One IP address/domain in one line to specify your walled garden.  
 Example:  
 \*.zyxel.com  
 www.zyxel.com  
 192.168.1.0/24

---

**Captive portal access attribute**

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

Login on multiple client devices: Multiple devices access simultaneously

---

**NCAS disconnection behavior** ⓘ

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

Limited:  
 Only currently authorized clients and whitelisted client devices will be able to access the network

The following table describes the labels in this screen.

Table 154 Security gateway > Configure > 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 <b>Disable</b> to turn off web authentication.  Select <b>Click-to-continue</b> to block network traffic until a client agrees to the policy of user agreement.  Select <b>Sign-on with</b> to block network traffic until a client authenticates with an external RADIUS or AD server through the specifically designated web portal page. Select <b>Nebula Cloud Authentication</b> or an authentication server that you have configured in the <b>Security gateway &gt; Configure &gt; Gateway settings</b> screen (see <a href="#">Section 10.3.11 on page 453</a> ).  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 <b>Network Access</b> to <b>Disable</b> .  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 <b>Sign-on with Nebula Cloud authentication</b> in the <b>Network Access</b> field.  Select <b>Allow users to create accounts with auto authorized</b> or <b>Allow users to create accounts with manual authorized</b> 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 <b>Allow users to create accounts with manual authorized</b> , users cannot log in with the account until the account is authorized and granted access. For <b>Allow users to create accounts with auto authorized</b> , users can just use the registered account to log in without administrator approval.  Select <b>Don't allow users to create accounts</b> 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 <b>Sign-on with</b> in the <b>Network Access</b> field.  Select <b>Multiple devices access simultaneously</b> if you allow users to log in as many times as they want as long as they use different IP addresses.  Select <b>One device at a time</b> if you do NOT allow users to have simultaneous logins.
NCAS disconnection behavior	This field is available only when you select <b>Sign-on with Nebula Cloud Authentication</b> in the <b>Network Access</b> field.  Select <b>Allowed</b> to allow any users to access the network without authentication when the NCAS (Nebula Cloud Authentication Server) is not reachable.  Select <b>Limited</b> to allow only the currently connected users or the users in the white list to access the network.

### 10.3.10 Traffic Shaping

Use this screen to configure maximum bandwidth and load balancing on the Nebula Device.

Click **Security gateway > Configure > Traffic shaping** to access this screen.

**Figure 179** Security gateway > Configure > Traffic shaping

Security gateway > Configure > [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 155 Security gateway > Configure > Traffic shaping

LABEL	DESCRIPTION
Uplink configuration	
WAN 1	Set the amount of upstream/downstream bandwidth for the WAN interface.
WAN 2	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	<p>Select a load balancing method to use from the drop-down list box.</p> <ul style="list-style-type: none"> <li>• Select <b>Least Load First</b> to send new session traffic through the least utilized WAN interface.</li> <li>• Select <b>Round Robin</b> 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.</li> <li>• Select <b>Failover</b> to send traffic through a second WAN interface when the primary WAN interface is down or disabled.</li> </ul>
Prefer WAN	<p>Specify the primary WAN interface through which the Nebula Device forwards traffic.</p> <p>This field is available when you set <b>WAN load balancing algorithm</b> to <b>Failover</b>.</p>
WAN Connectivity check	<p>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.</p> <p>If the WAN connection is down (the check fails), the Nebula Device will switch (failover) to use a redundant WAN connection.</p> <ul style="list-style-type: none"> <li>• Select <b>Check Default Gateway</b> to use the default gateway for the connectivity check.</li> <li>• Select <b>Check this address</b> to specify a domain name or IP address for the connectivity check.</li> </ul> <p>Note: If you select <b>Check this address</b> 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 <b>Check this address</b>.</p> <p>This field is available when you set <b>WAN load balancing algorithm</b> to <b>Failover</b>.</p>
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	<p>Enter the destination IP addresses for which the Nebula Device applies the rule.</p> <p>Enter <b>any</b> if the rule is effective for every destination.</p>
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. <b>any</b> means all service ports.
Protocol	<p>Select <b>TCP</b> or <b>UDP</b> if you want to specify a protocol for the rule. Otherwise select <b>Any</b>.</p> <p><b>Any</b> means the rule is applicable to all services.</p>

Table 155 Security gateway &gt; Configure &gt; 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.

### 10.3.11 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 **Security gateway > Configure > Gateway settings** to access this screen.

Figure 180 Security gateway &gt; Configure &gt; Gateway settings

Security gateway > Configure > [Gateway settings](#)

Gateway settings

### DNS

Address Record

FQDN	IP Address
d.nebula.zyxel.com	52.19.85.221
www.nebula.zyxel.com	52.84.248.13
s.nebula.zyxel.com	18.202.42.142

[+ Add](#)

Domain Zone Forwarder

Domain Zone	IP Address	Interface
		LAN1

[+ Add](#)

### Authentication Server

My AD Server

Name	Server address	Backup server address	Port	AD domain
ADTest	192.168.8.1		389	zyxel.com

[+ Add](#)

My RADIUS Server

Name	Server address	Backup server address	Port	Secret
			1812	

[+ Add](#)

### Walled garden

Global walled garden

This is global walled garden configuration. All web authentication interface will match this policy first and the second priority is the interface walled garden policy. If needed only allow specify interface, please go to Network access method configure

[What do I enter here?](#)

The following table describes the labels in this screen.

Table 156 Security gateway > Configure > 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 <b>Default</b> or <b>Custom</b> advanced settings. See <a href="#">Section 10.3.11.1 on page 456</a> .
	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 156 Security gateway &gt; Configure &gt; 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 <b>Default</b> or <b>Custom</b> advanced settings. See <a href="#">Section 10.3.11.1 on page 456</a> .
	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.

### 10.3.11.1 Advanced Settings

Click the **Advanced** column in the **Security gateway > Configure > Gateway settings** screen to access this screen.

Figure 181 Security gateway &gt; Configure &gt; Gateway settings: Advanced



The following table describes the labels in this screen.

Table 157 Security gateway &gt; Configure &gt; Gateway settings: Advanced

LABEL	DESCRIPTION
Preset	Select <b>Default</b> to use the pre-defined settings, or select <b>Custom</b> 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 <b>ON</b> if the server checks the case of the user name. Otherwise, click <b>OFF</b> 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 157 Security gateway > Configure > 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 11

## Switch

### 11.1 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**.

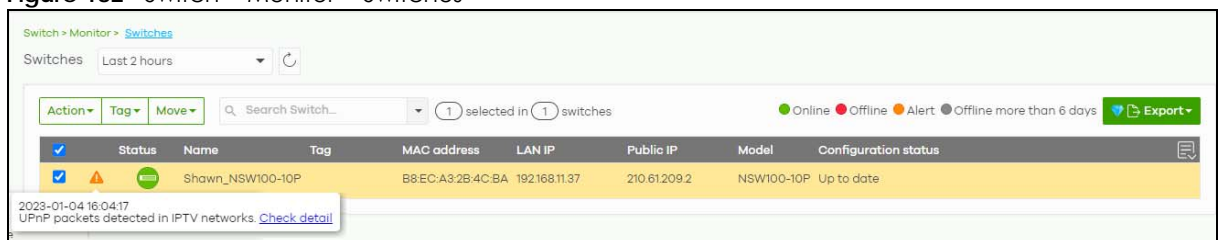
### 11.2 Monitor

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.

#### 11.2.1 Switches

This screen allows you to view the detailed information about a Nebula Device in the selected site. Click **Switch > Monitor > Switches** to access this screen.

Figure 182 Switch > Monitor > Switches



The following table describes the labels in this screen.


Table 158 Switch > Monitor > Switches

LABEL	DESCRIPTION
Switch	Select to view the Nebula Device information and connection status in the past two hours, day, week or month.
	Click this button to reload the data-related frames on this page.
Action	Perform an action on the selected Nebula Devices.
Reboot	Restart the Nebula Device.
Upgrade	Upgrade the firmware on the Nebula Device.
Tag	Select one or multiple Nebula Devices and click this button to create a new tag for the Nebula Devices or delete an existing tag.

Table 158 Switch &gt; Monitor &gt; Switches (continued)

LABEL	DESCRIPTION
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	<p>This shows the status of the Nebula Device. Hover the mouse over the icon for a brief description.</p> <ul style="list-style-type: none"> <li>• Green: The Nebula Device is online and has no alerts.</li> <li>• Amber: The Nebula Device has alerts.</li> <li>• Red: The Nebula Device is offline.</li> <li>• Gray: The Nebula Device has been offline for 7 days or more.</li> <li>• With lock: The Nebula Device is locked by Auto Configuration Recovery. See <a href="#">Table 180 on page 506</a> for more information.</li> </ul> <p>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.</p>
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	<p>This shows the Nebula Device connection status. Nothing displays if the Nebula Device is offline.</p> <p>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.</p>
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 158 Switch &gt; Monitor &gt; Switches (continued)

LABEL	DESCRIPTION
Firmware type	<p>This shows <b>Stable</b> when the installed firmware may not have the latest features but has passed Zyxel internal and external testing.</p> <p>This shows <b>Latest</b> when the installed firmware is the most recent release with the latest features, improvements, and bug fixes.</p> <p>This shows <b>General Availability</b> when the installed firmware is a release before <b>Latest</b>, but is still undergoing Zyxel external testing.</p> <p>This shows <b>Dedicated</b> 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.</p> <p>This shows <b>Beta</b> when the installed firmware is a release version for testing the latest features and is still undergoing Zyxel internal and external testing.</p> <p>This shows <b>N/A</b> when the Nebula Device is offline and its firmware status is not available.</p>
Firmware availability	This shows whether the firmware on the Nebula Device is <b>Up to date</b> , there is firmware update available for the Nebula Device ( <b>Upgrade available</b> ), or a specific version of firmware has been installed by Zyxel customer support ( <b>Locked</b> ).
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 ( <b>DHCP</b> ), or manually ( <b>Static IP</b> ).
	Click this icon to display a greater or lesser number of configuration fields. For faster loading of data, select only the configuration fields listed that do NOT take a long time to fetch data.

### 11.2.1.1 Switch Details

Click a Nebula Device entry in the **Switch > Monitor > Switches** screen to display individual Nebula Device statistics.

Figure 183 Switch > Monitor > Switches: Switch Details

Switch > Monitor > [Switch](#) > Shawn\_NSW100-10P

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:

Map Photo

### 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)

### Ports [Configure ports](#)

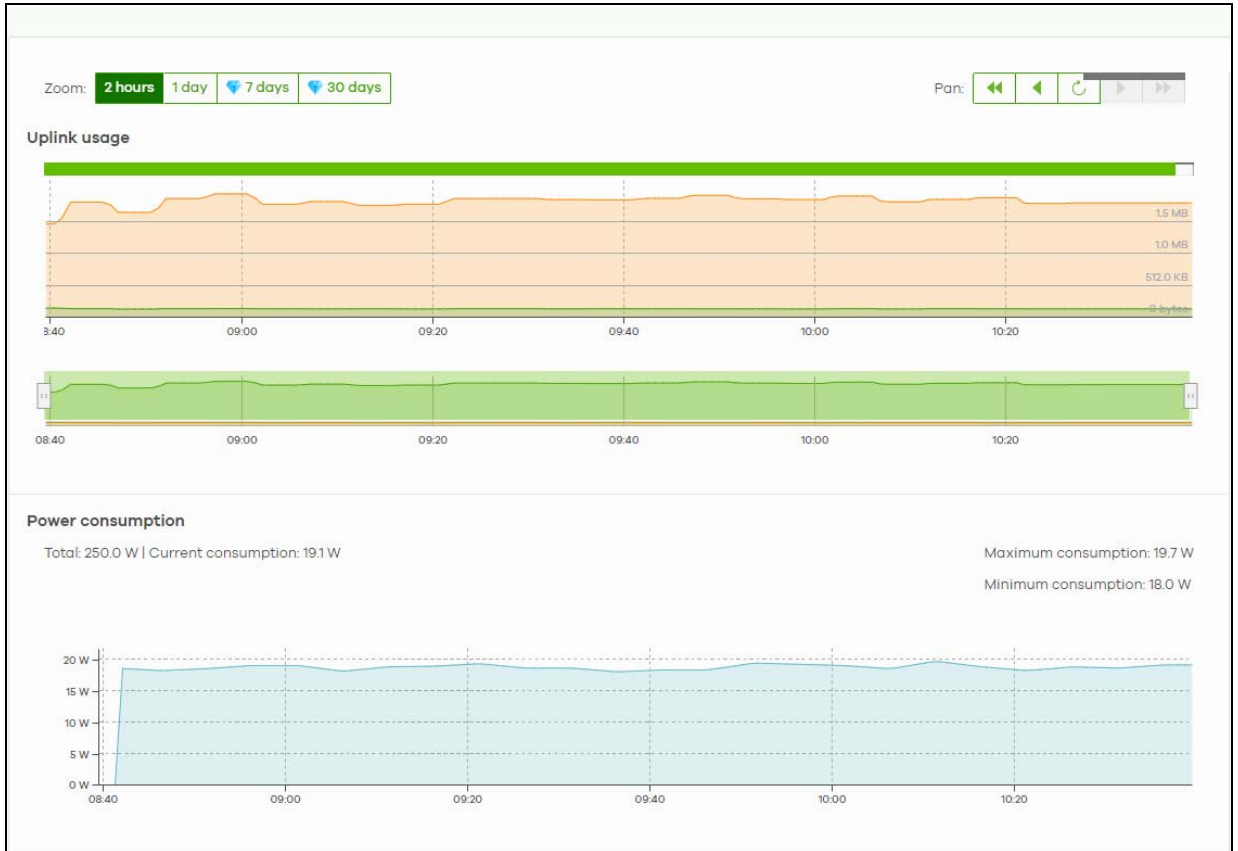
2	4	6	8	10	10	<ul style="list-style-type: none"> <li><span style="color: orange;">■</span> 10/100Mbps</li> <li><span style="color: green;">■</span> 1Gbps</li> <li><span style="color: blue;">■</span> 2.5Gbps</li> <li><span style="color: purple;">■</span> 5Gbps</li> <li><span style="color: darkblue;">■</span> 10Gbps</li> <li><span style="color: red;">⊘</span> STP blocking</li> <li><span style="color: blue;">↑</span> Uplink</li> <li><span style="color: green;">P</span> PoE</li> </ul>
1	3	5	7	9	9	

### Live tools

[Ping](#)
[Port power cycle](#)
[MAC table](#)
[Reboot switch](#)
[Locator LED](#)

Enter a hostname or IP address.

× [Ping](#)



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 159 Switch > Monitor > 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 159 Switch &gt; Monitor &gt; Switches: Switch Details (continued)

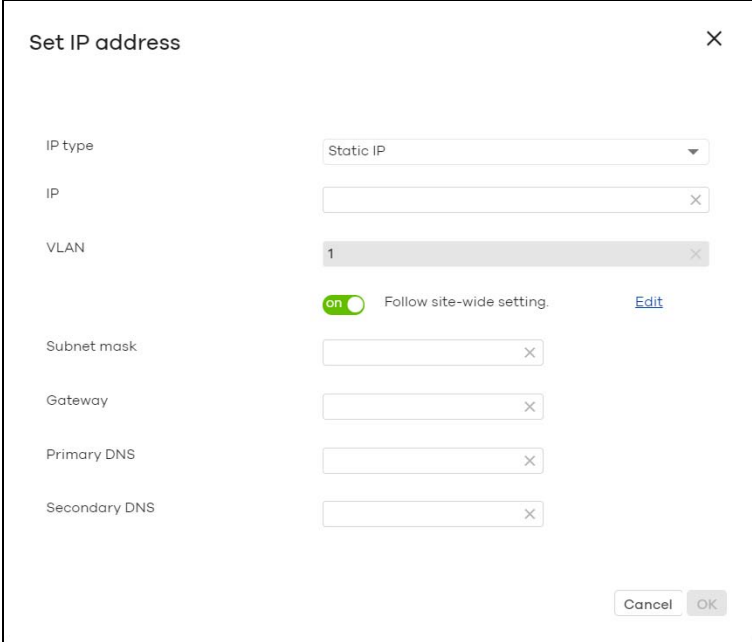
LABEL	DESCRIPTION
LAN IP	<p>This shows the local (LAN) IP address of the Nebula Device. It also shows the IP addresses of the gateway and DNS servers.</p> <p>Click the edit icon to open a screen where you can change the IP address, VLAN ID number and DNS server settings.</p> 
DHCP server	This shows the IP address of the DHCP server.
Public IP	This shows the global (WAN) IP address of the Nebula Device.
Topology	Click <b>Show</b> to go to the <b>Site-wide &gt; Monitor &gt; Topology</b> screen. See <a href="#">Section 7.1.7 on page 266</a> .
RSTP status	This shows <b>Disabled</b> 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	<p>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. <b>N/A</b> displays if the Nebula Device does not support PoE.</p> <p>Click the edit icon to open the <b>PoE Configuration</b> screen. See <a href="#">Section 11.2.1.2 on page 466</a>.</p>
History	Click <b>Event log</b> to go to the <b>Switch &gt; Monitor &gt; Event log</b> 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 159 Switch &gt; Monitor &gt; Switches: Switch Details (continued)


LABEL	DESCRIPTION
Map	<p>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).</p> <div data-bbox="537 428 1216 869" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: right;"><b>Position device</b> <span style="float: right;">✕</span></p> <hr/> <p>Update my device's location. <a href="#">What is this?</a></p> <p><input checked="" type="radio"/> Use the device's IP address (GEO IP).</p> <p><input type="radio"/> Get my location from web browser.</p> <p><input type="radio"/> Use the following address or coordinates.</p> <div style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <input type="text"/> <span style="float: right;">✕</span> </div> <p style="text-align: right;"> <input type="button" value="Cancel"/> <input type="button" value="Update"/> </p> </div> <ul style="list-style-type: none"> <li>Select <b>GEO IP</b> to use the public IP address of the Nebula Device.</li> <li>Select <b>Get my location from web browser</b> to use the public IP address of the computer accessing the NCC portal.</li> <li>Select <b>Use the following address or coordinates</b> to enter the complete address or coordinates of the Nebula Device.</li> </ul> <p>Note: Nebula Devices that are offline cannot use GEO IP.</p>
Photo	<p>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.</p>
Ports	<p>This shows the ports on the Nebula Device. You can click a port to see the individual port statistics. See <a href="#">Section 11.2.1.3 on page 466</a>. Move the pointer over a port to see additional port information. The port color indicates the connection status of the port.</p> <ul style="list-style-type: none"> <li>Gray (#888888): The port is disconnected.</li> <li>Orange (#FF8900): The port is connected and is transmitting data at 10 or 100 Mbps.</li> <li>Green (#64BE00): The port is connected and is transmitting data at 1000 Mbps (1 Gbps).</li> <li>Azure (#0079FF): The port is connected and is transmitting data at 2.5 Gbps.</li> <li>Violet (#8800FF): The port is connected and is transmitting data at 5 Gbps.</li> <li>Blue (#004FEE): The port is connected and is transmitting data at 10000 Mbps (10 Gbps).</li> </ul> <p>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.</p>
Name	This shows the Nebula Device name configured in NCC.
Status	This shows the connection status of the port.
Type	This shows the port type ( <b>Trunk</b> or <b>Access</b> ), 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.
Reset	<p>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.</p> <p>Note: This button is not available for an uplink port.</p>



Table 159 Switch &gt; Monitor &gt; Switches: Switch Details (continued)


LABEL	DESCRIPTION
Configure ports	Click this button to go to the <b>Switch &gt; Configure &gt; Switch ports</b> screen, where you can view port summary. See <a href="#">Section 11.3.1 on page 482</a> .
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 <b>Ping</b> .
Port Power Cycle	Enter the number of the ports and click the <b>Reset</b> button to disable and enable the ports again.
MAC table	<p>This shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which ports.</p> <p>You can define how it displays and arrange the data in the summary table below.</p> <p>Note: This tab will appear for NSW100 and NSW200 Series only.</p>
Switch tables	<p>Import the following data into NCC:</p> <ul style="list-style-type: none"> <li>• <b>MAC table.</b> Click <b>Run</b> 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.</li> <li>• <b>Routing table.</b> Click <b>Run</b> to show the routing destination, gateway, interface IP addresses, hop count, and routing methods. The routing table is only displayed for L3 Nebula Devices.</li> <li>• <b>ARP table.</b> Click <b>Run</b> to show the IP-to-MAC address mappings. The ARP table is only displayed for L3 Nebula Devices.</li> <li>• <b>IP source guard.</b> Click <b>Run</b> to show the static, DHCP snooping, blocked client entries, and expiration time of DHCP snooping and blocked entries on the Nebula Device.</li> </ul> <p>After clicking <b>Run</b> in <b>IP source guard</b>, the IPSG (IP source guard) table could be empty if:</p> <ul style="list-style-type: none"> <li>• It takes about 5 minutes to refresh the address table after you apply the Nebula Device settings</li> <li>• Protected port is not specified</li> <li>• NCC may not get completed data from Nebula Device due to unstable network. Please retry.</li> </ul>
Reboot switch	Click the <b>Reboot</b> button to restart the Nebula Device.
Locator LED	<p>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.</p> <p>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.</p>
Remote Access	<p>Select to use TCP (Transmission Control Protocol) <b>Port 22</b> or <b>443</b> to establish a remote connection to this Nebula Device. The Nebula Device will create a reverse SSH (Secure SHell) connection. Then click <b>Establish</b>.</p> <p>After clicking <b>Ok</b>, 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.</p> <p>In case the connection cannot be established, confirm that the network allows <b>Port 22</b> or <b>443</b>.</p> <p>Note: Use <b>Remote Access</b> for troubleshooting only.</p>
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 159 Switch &gt; Monitor &gt; Switches: Switch Details (continued)

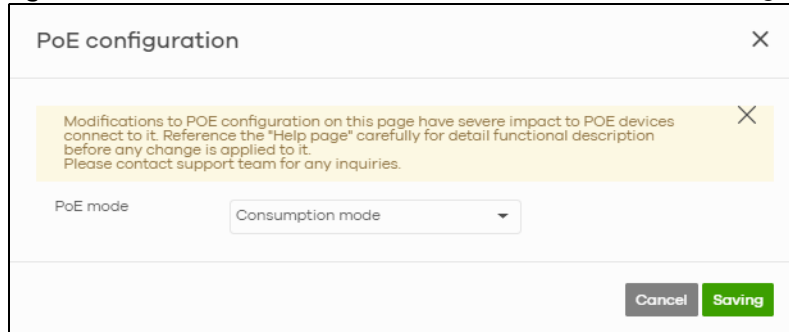
LABEL	DESCRIPTION
	Select to view the Nebula Device power consumption in the past two hours, day, week or month.
	This shows the current, total, maximum and minimum power consumption of the Nebula Device.
y-axis	The y-axis shows how much power is used in Watts.
x-axis	The x-axis shows the time period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

### 11.2.1.2 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 **Switch > Monitor > 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 11.3.1 on page 482](#).

Figure 184 Switch &gt; Monitor &gt; Switches: Switch Details: PoE Configuration



The following table describes the labels in this screen.

Table 160 Switch &gt; Monitor &gt; Switches: Switch Details: PoE Configuration

LABEL	DESCRIPTION
PoE Mode	Select the power management mode you want the Nebula Device to use.  <b>Classification mode</b> – 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.  <b>Consumption mode</b> – 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.

### 11.2.1.3 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 **Switch > Monitor > Switches: Switch Details** screen or click the **details** link next to a port in the **Switch > Configure > Switch ports** screen.

Figure 185 Switch > Monitor > Switches: Switch Details: Port Details

Switch > Monitor > Switch > Shawn\_NSW100-10P > Port 4

Switch / Shawn\_NSW100-10P / Port 4 Last 24 hours

2

4

6

8

10

10

10/100Mbps

1Gbps

2.5Gbps

5Gbps

10Gbps

STP blocking

Uplink

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
	00:10:AA:25:0A:CA	1
	48:4B:AA:77:00:59	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 161 Switch &gt; Monitor &gt; 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	<p>This figure shows the ports on the Nebula Device.</p> <p>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.</p> <p>The port color indicates the connection status of the port.</p> <ul style="list-style-type: none"> <li>• Gray (#888888): The port is disconnected.</li> <li>• Orange (#FF8900): The port is connected and is transmitting data at 10 or 100 Mbps.</li> <li>• Green (#64BE00): The port is connected and is transmitting data at 1000 Mbps (1 Gbps).</li> <li>• Azure (#0079FF): The port is connected and is transmitting data at 2.5 Gbps.</li> <li>• Violet (#8800FF): The port is connected and is transmitting data at 5 Gbps.</li> <li>• Blue (#004FEE): The port is connected and is transmitting data at 10000 Mbps (10 Gbps).</li> </ul> <p>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.</p>
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 ( <b>Trunk</b> or <b>Access</b> ), 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 <b>Switch ports</b> screen and show the ports that match the filter criteria (the selected port number). See <a href="#">Section 11.3.1 on page 482</a> .	
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 <b>Event log</b> to go to the <b>Switch &gt; Monitor &gt; Event log</b> 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 161 Switch &gt; Monitor &gt; 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: <ul style="list-style-type: none"> <li>• LLDP remote information</li> <li>• Information collected by the Nebula Security Gateway (NSG) in this site</li> <li>• Information collected by NCC when the client connected to Nebula</li> </ul>
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 <b>Diagnose</b> 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 161 Switch &gt; Monitor &gt; Switches: Switch Details: Port Details (continued)

LABEL	DESCRIPTION
Pair Status	<p><b>OK:</b> The physical connection between the wire-pair is okay.</p> <p><b>Open:</b> There is no physical connection (an open circuit detected) between the wire-pair.</p> <p><b>Short:</b> There is a short circuit detected between the wire-pair.</p> <p><b>Unknown:</b> The Nebula Device failed to run cable diagnostics on the cable connected to this port.</p> <p><b>Unsupported:</b> The port is a fiber port or it is not active.</p>
Cable Length	<p>This displays the total length of the Ethernet cable that is connected to the port when the <b>Pair Status</b> is <b>OK</b> and the Nebula Device chipset supports this feature.</p> <p>This shows <b>N/A</b> if the <b>Pair Status</b> is <b>Open</b> or <b>Short</b>. Check the <b>Distance to fault</b>.</p> <p>This shows <b>Unsupported</b> if the Nebula Device chipset does not support to show the cable length.</p>
Distance to fault (m)	<p>This displays the distance between the port and the location where the cable is open or shorted.</p> <p>This shows <b>N/A</b> if the <b>Pair Status</b> is <b>OK</b>.</p> <p>This shows <b>Unsupported</b> if the Nebula Device chipset does not support to show the distance.</p>
DDMI	This section is available only on an SFP (Small Form Factor Pluggable) port.
DDMI	Click <b>DDMI</b> (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.

## 11.2.2 Clients

This menu item redirects to **Site-Wide > Monitor > Clients**, with type set to **Switches clients**. For details, see [Section 7.1.2 on page 255](#).

## 11.2.3 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 **Switch > Monitor > Event Log** to access this screen.

**Figure 186** Switch > Monitor > Event log

The screenshot displays the 'Event log' interface. At the top, there are search filters for Switch, Keyword, Priority, Category, and Tag, all set to 'Any'. Below these are date and time filters: 'From: 2022-07-07 10:05' and 'To: 2022-07-07 11:05' in UTC+8. A 'Search' button is on the right. Below the filters, there are navigation buttons for 'Newer', 'Older', and 'Export'. The main area is a table with the following data:

Time	Priority	Switch	Tag	Category	Detail
2022-07-07 11:03:01	Information	<a href="#">XS3800-1-1</a>	system	System	Auto restore back up configuration
2022-07-07 11:02:56	Information	<a href="#">XS3800-1-1</a>	system	System	Save system configuration
2022-07-07 10:57:39	Information	<a href="#">XS3800-1-1</a>	system	System	Save system configuration
2022-07-07 10:57:01	Notice	<a href="#">XS3800-1-1</a>	system	System	Gets the time and date from a time server successfully
2022-07-07 10:56:54	Information	<a href="#">XS3800-1-1</a>	system	System	Save system configuration
2022-07-07 10:56:46	Information	<a href="#">XS3800-1-1</a>	switch	System	Cloud: Device is online, VLAN 1, DHCP IP 10.214.48.34
2022-07-07 10:56:45	Information	<a href="#">XS3800-1-1</a>	switch	System	Cloud: Set IP 10.214.48.34 on VLAN 1 by Local
2022-07-07 10:56:25	Information	<a href="#">XS3800-1-1</a>	switch	Switch	Cloud Netconf connection has been terminated
2022-07-07 10:53:43	Information	<a href="#">XS3800-1-1</a>	system	System	Save system configuration
2022-07-07 10:52:08	Notice	<a href="#">XS3800-1-1</a>	system	System	Gets the time and date from a time server successfully

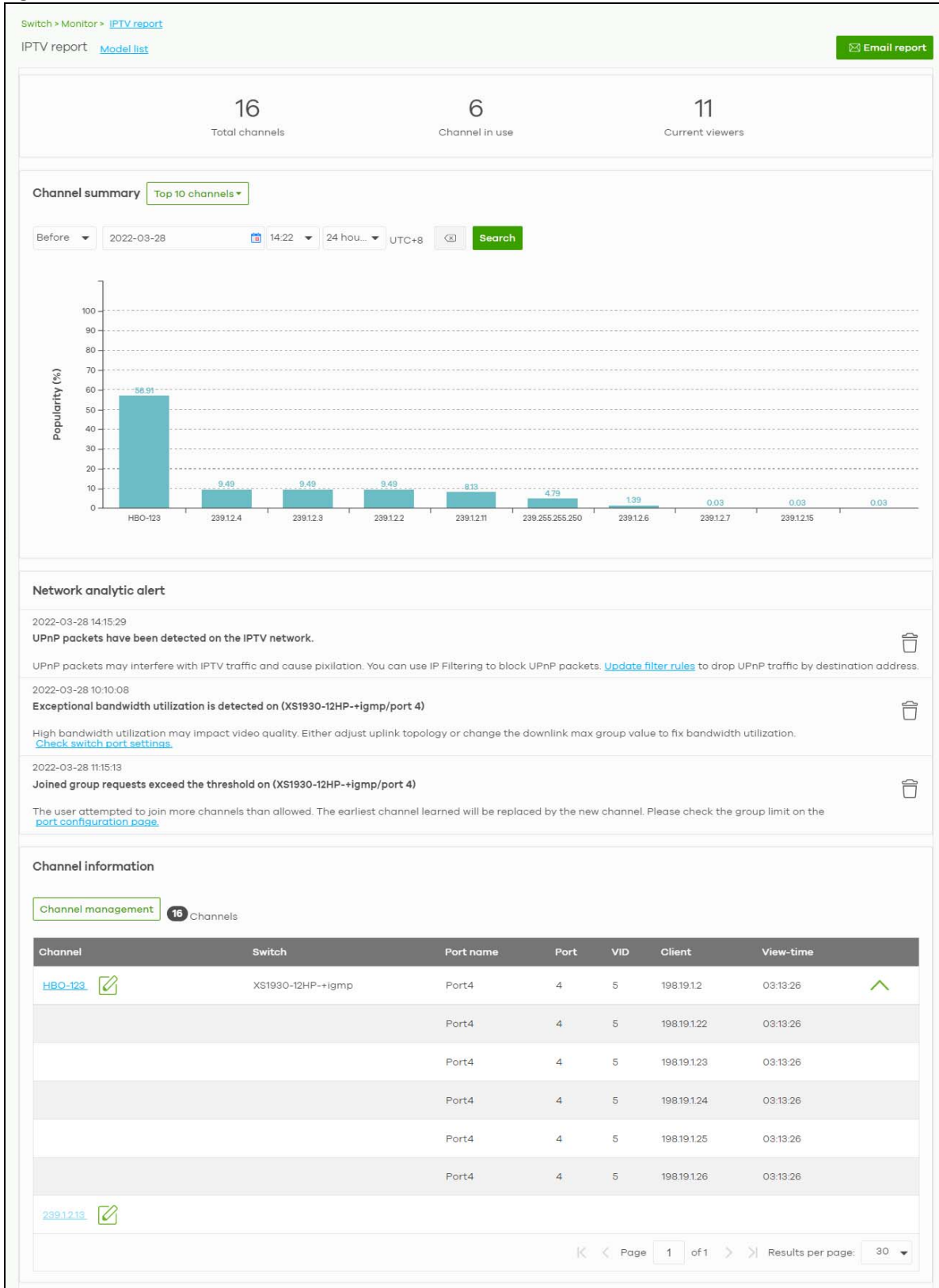
At the bottom right, there are navigation controls: 'Page 1 of 56' and 'Results per page: 10'.

## 11.2.4 IPTV Report

Use this screen to view available IPTV channels and client information.

Click **Switch > Monitor > IPTV report** to access this screen.

Figure 187 Switch > Monitor > IPTV Report



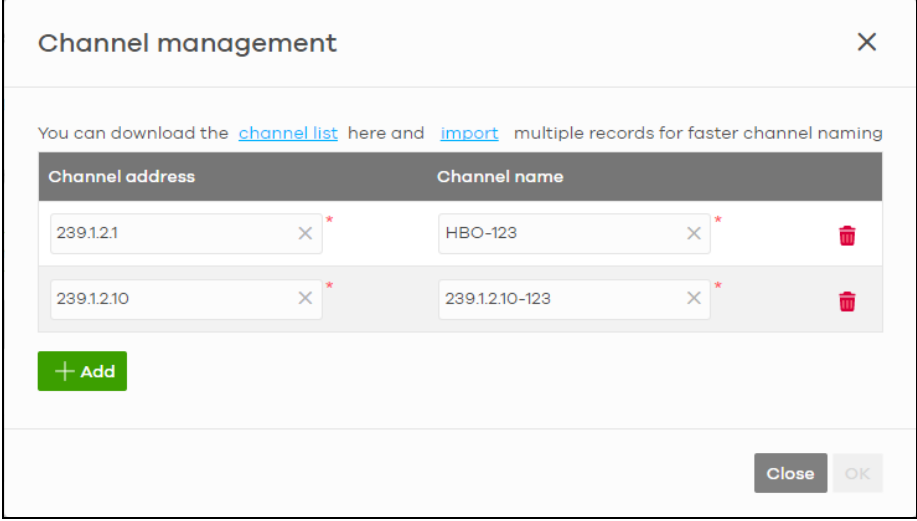


The following table describes the labels in this screen.

Table 162 Switch > Monitor > IPTV Report

LABEL	DESCRIPTION
IPTV report	Click <b>Model list</b> to show the <b>Non-supported model list</b> . Click <b>See more</b> to go to the <b>Help &gt; Support tools &gt; Device function table</b> 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	
	<p>Select to view the channels according to the ranking. Alternatively, select <b>Select channels</b> to choose specific channels and click <b>Apply</b>.</p> <div data-bbox="537 695 899 1052" style="border: 1px solid black; padding: 5px;"> <p><input checked="" type="radio"/> Top 10 channels</p> <p><input type="radio"/> Top 11 to 20 channels</p> <p><input type="radio"/> Bottom 11 to 20 channels</p> <p><input type="radio"/> Bottom 10 channels</p> <p><input type="radio"/> Select channels (10 channels max)</p> </div>
Search	<p>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 <b>Search</b>.</p> <p>You can also select <b>Range</b> in the second field, set a time range and click <b>Search</b> to display only the channels available within the specified period of time.</p>
y-axis	The y-axis represents the <b>Popularity (%)</b> 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	<p>This shows the alerts the NCC generates when an error or something abnormal is detected on the IPTV network.</p> <p>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.</p>
Channel Information	

Table 162 Switch &gt; Monitor &gt; IPTV Report (continued)

LABEL	DESCRIPTION
Channel Management	<p>Download the channel list and import multiple records for faster channel naming. Click <b>Add</b> to add new channels.</p> 
Channel	<p>This shows the name of the channel. Click the edit icon to change the channel name.</p> <p>Click the channel name to display the channel's client statistics. See <a href="#">Section 11.2.4.2 on page 476</a>.</p>
Switch	<p>This shows the name of the Nebula Device to which the client is connected.</p>
Port Name	<p>This shows the name of the Nebula Device port to which the client is connected.</p>
Port	<p>This shows the number of the Nebula Device port to which the client is connected.</p>
VID	<p>This shows the ID number of the VLAN to which the Nebula Device port belongs.</p>
Client	<p>This shows the IP address of the client who is watching the TV program on the channel.</p>
View-time	<p>This shows the amount of time the client has spent watching the IPTV channel.</p>

### 11.2.4.1 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 **Switch > Monitor > IPTV Report** screen.

Figure 188 Switch &gt; Monitor &gt; IPTV Report: Email report

**Email report**

Email Channel Summary report - 2022-03-31 to 2022-04-01

Address:

Format:

**Schedule reports**

Current logo

Upload new logo:

No logo

Email address	Subject	Frequency	Type	Channel summary
<input type="text" value="y@zyxel.com.tw"/>	<input type="text" value="HTML-test"/>	<input type="text" value="Weekly"/>	<input type="text" value="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
<input type="text" value="y@zyxel.com.tw"/>	<input type="text" value="plain-test"/>	<input type="text" value="Weekly"/>	<input type="text" value="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 163 Switch &gt; Monitor &gt; IPTV Report: Email report

LABEL	DESCRIPTION
Email Channel Summary report	This shows the range of the date/time you specified in the <b>Switch &gt; Monitor &gt; IPTV Report</b> screen.
Address	Enter the recipient's email address of the IPTV channel summary report.
Format	Select to send the IPTV channel summary report in <b>HTML</b> or <b>Plain text</b> 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 <b>Current logo</b> to continue using the present logo.  Select <b>Upload new logo</b> and click <b>Choose File</b> 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 <b>No logo</b> if you do not want a logo to appear on the IPTV channel summary report.

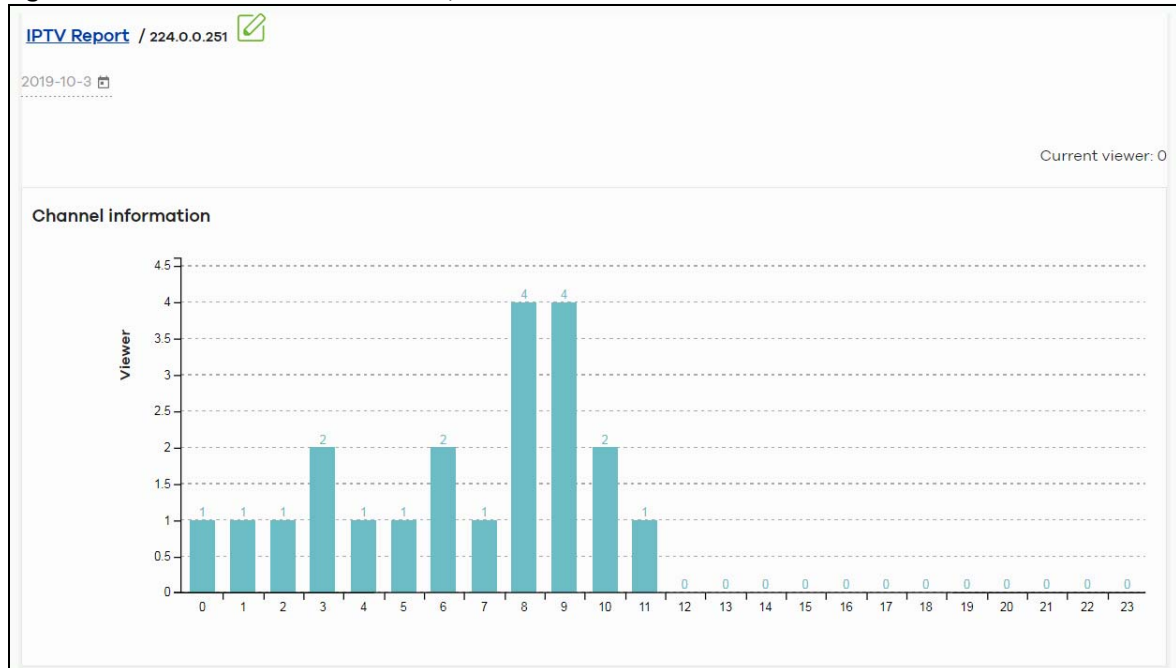
Table 163 Switch &gt; Monitor &gt; IPTV Report: Email report (continued)

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 <b>Monthly</b> , <b>Weekly</b> , or <b>Daily</b> .
Type	Select to send the IPTV channel summary report in <b>HTML</b> or <b>Plain text</b> format.
Channel summary	
	<p>Select to view the channels report according to the ranking. Alternatively, select <b>Select channels</b> to choose specific channels and click <b>Update</b>.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content;"> <p><input checked="" type="checkbox"/> Top 10 channels</p> <p><input type="checkbox"/> Top 11 to 20 channels</p> <p><input type="checkbox"/> Bottom 11 to 20 channels</p> <p><input type="checkbox"/> Bottom 10 channels</p> <p><input type="checkbox"/> Select channels (10 channels max) <span style="color: blue;">i</span></p> <p style="text-align: center; background-color: #4CAF50; color: white; padding: 2px 10px; border-radius: 3px;">Update</p> </div>
Remove	Click this to delete a scheduled profile.
Save	Click <b>Save</b> to save the new scheduled profile.

### 11.2.4.2 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 **Switch > Monitor > IPTV Report** screen.

Figure 189 Switch &gt; Monitor &gt; IPTV Report: Channel Information



The following table describes the labels in this screen.

Table 164 Switch > Monitor > 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.

## 11.2.5 Surveillance

Use this screen to view information about Powered Devices (PDs) connected to ports on the Nebula Device.

Click **Switch > Monitor > Surveillance** to access this screen.

Figure 190 Switch > Monitor > Surveillance



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	Auto-1000M	0.0W	Tx: 10.68 Rx: 2.23	0	Disable		
BC:CF-4F-47:7D:F1(...)	Port2	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable		
BC:CF-4F-47:7D:F1(...)	Port3	Auto-1000M	Auto-1000M	0.0W	Tx: 2.60 Rx: 9.06	0	Disable	Others	XGS4600
BC:CF-4F-47:7D:F1(...)	Port4	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable		
BC:CF-4F-47:7D:F1(...)	Port5	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable		
BC:CF-4F-47:7D:F1(...)	Port6	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable		

The following table describes the labels in this screen.

Table 165 Switch > Monitor > Surveillance

LABEL	DESCRIPTION
Search ports	Enter a keyword to filter the list of ports or devices.
N switch ports	This shows the number of Nebula Device ports (N) in the list.
	This shows the number of connected PDs that did not respond to an automatic PD alive check.
	This shows the number of ONVIF-compatible IP camera devices connected to Nebula Devices in the site.

Table 165 Switch &gt; Monitor &gt; Surveillance (continued)

LABEL	DESCRIPTION
	This shows the number of ONVIF-compatible NVR devices connected to Nebula Devices in the site.
	This shows the number of connected devices that did not respond to an ONVIF discovery query, or are of an unknown type.
Switch/Port	This shows the port number of the Nebula Device.
Port name	This shows the port description on the Nebula Device.
PD health	<p>This shows the status of auto PD recovery on this port.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Yellow: The Nebula Device is restarting the connected PD by turning the power off and turning it on again.</li> <li>• Green: The Nebula Device successfully discovered the connected PD using LLDP or ping.</li> <li>• --: 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.</li> </ul> <p>Note: For details on configuring auto PD recovery on a port, see <a href="#">Section 11.3.1 on page 482</a>.</p>
Link speed	This shows the speed (either <b>10M</b> for 10 Mbps, <b>100M</b> for 100 Mbps, or <b>1G</b> for 1 Gbps) and the duplex ( <b>F</b> for full duplex or <b>H</b> for half). This field displays <b>Down</b> if the port is not connected to any device.
PoE draw(W)	This shows the total power that the connected PD draws from the port, in watts. This allows you to plan and use within the power budget of the Nebula Device.
Bandwidth (Kbps)	Tx shows the number of kilobytes per second transmitted on this port. Rx shows the number of kilobytes per second received on this port.
CRC	This shows the number of packets received with CRC (Cyclic Redundant Check) errors.
Extended range	This shows whether extended range is enabled on the port.
Device type	This shows the device type of the PD, as reported by ONVIF discovery.
System name	This shows the name of the connected PD, as reported by ONVIF or LLDP.
IP	This shows the IP address of the connected PD, as reported by ONVIF or LLDP.
Discovered devices	<p>This shows how many devices are connected to the port.</p> <p>Click the number to go to the <b>Surveillance Port Details</b> screen.</p>

## 11.2.6 Surveillance Port Details

Use this screen to view detailed information about a port on the **Surveillance** screen.

Go to **Switch > Monitor > Surveillance** and click on a value in the **Discovered Devices** column to access this screen.

Figure 191 Switch &gt; Monitor &gt; Surveillance &gt; Port Details

Switch > Monitor > Surveillance > BC:CF:4F:47:7D:F1(GS1350-6HP) > Port 3  
 Surveillance / BC:CF:4F:47:7D:F1(GS1350-6HP) / Port 3 Last 2 hours

**Status**

Link speed:	Auto-1000M	Bandwidth Tx/Rx(Kbps):	2.46/8.97
PoE draw:	0.0 W	CRC:	0
PD health:		Power cycle:	<input type="button" value="Reset"/>
Extended range:	Disable		

**Neighbor detail**

Search clients  1 clients

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 166 Switch &gt; Monitor &gt; Surveillance &gt; Port Details

LABEL	DESCRIPTION
Status	
Link speed	This shows the speed (either <b>10M</b> for 10 Mbps, <b>100M</b> for 100 Mbps, or <b>1G</b> for 1 Gbps) and the duplex ( <b>F</b> for full duplex or <b>H</b> for half). This field displays <b>Down</b> if the port is not connected to any device.
PoE draw	This shows the total power that the connected PD draws from the port, in watts. This allows you to plan and use within the power budget of the Nebula Device.
PD health	This shows the status of auto PD recovery on this port. <ul style="list-style-type: none"> <li>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.</li> <li>Yellow: The Nebula Device is restarting the connected PD by turning the power off and turning it on again.</li> <li>Green: The Nebula Device successfully discovered the connected PD using LLDP or ping.</li> <li>--: 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.</li> </ul> For details on configuring auto PD recovery on a port, see <a href="#">Section 11.3.1 on page 482</a> .
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 <b>Reset</b> 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.

Table 166 Switch > Monitor > Surveillance > Port Details (continued)

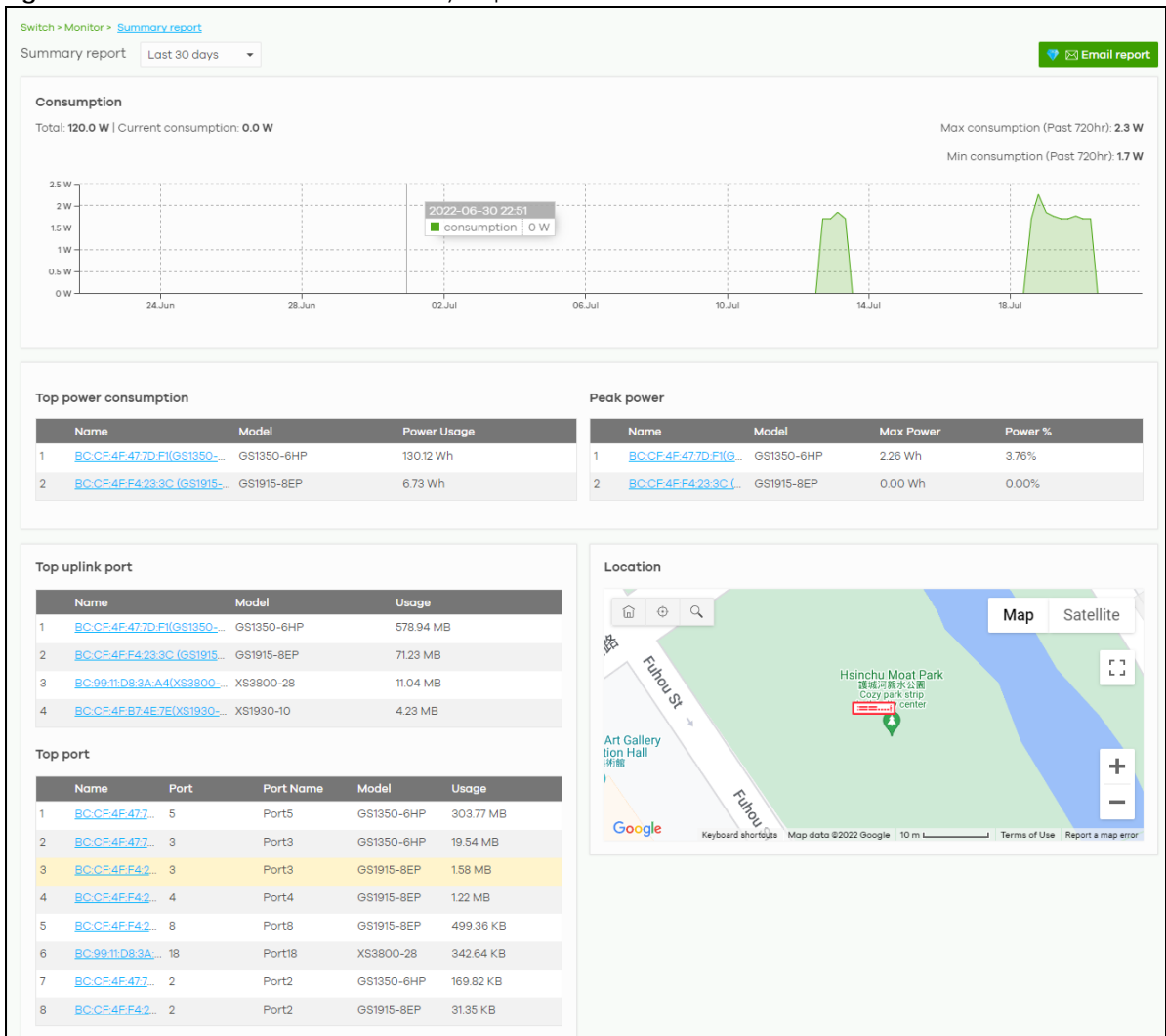
LABEL	DESCRIPTION
Port	This displays the number of the Nebula Device port that is connected to the Nebula Device.
IP	This shows the IP address of the Nebula Device.
Firmware	This shows the firmware version currently installed on the Nebula Device.
Description	This shows the descriptive name of the Nebula Device.

## 11.2.7 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 **Switch > Monitor > Summary Report** to access this screen.

Figure 192 Switch > Monitor > Summary Report





The following table describes the labels in this screen.

Table 167 Switch &gt; Monitor &gt; Summary Report

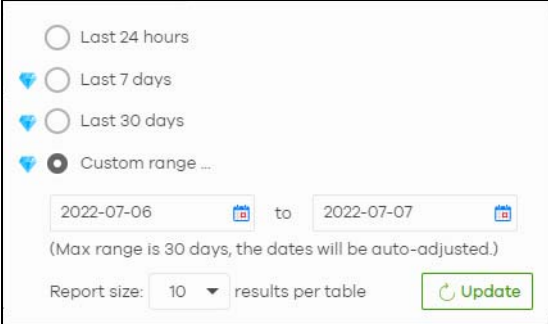
LABEL	DESCRIPTION
Switch – Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click this button 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 167 Switch &gt; Monitor &gt; 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.

## 11.3 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.

### 11.3.1 Switch Ports

Use this screen to view port summary and configure Nebula Device settings for the ports. To access this screen, click **Switch > Configure > Switch ports** or click the **Configure ports** button in the **Switch > Monitor > Switch: Switch Details** screen.

Figure 193 Switch &gt; Configure &gt; Switch ports

Switch / Port	Port name	# Port	LLDP	Received bytes	Sent bytes	Connection	PoE	Tag	IPSP protected	Management
<input checked="" type="checkbox"/> BC.CF.4F.47.7D.F1(GS1350-6HP)/1 Uplink <a href="#">details</a>	Port1	1	nsg50	128 MB	313 MB		Enabled	N/A	N/A	Enabled
<input checked="" type="checkbox"/> BC.CF.4F.47.7D.F1(GS1350-6HP)/2 <a href="#">details</a>	Port2	2	XGS4600	773.77 KB	664.21 KB		Enabled	N/A	N/A	Enabled
<input type="checkbox"/> BC.CF.4F.47.7D.F1(GS1350-6HP)/3 <a href="#">details</a>	Port3	3	NAP102	733.08 KB	125 MB		3.20	N/A	N/A	Enabled
<input type="checkbox"/> BC.CF.4F.47.7D.F1(GS1350-6HP)/4 <a href="#">details</a>	Port4	4	Enabled	0 bytes	0 bytes		Enabled	N/A	N/A	Enabled
<input type="checkbox"/> BC.CF.4F.47.7D.F1(GS1350-6HP)/5 <a href="#">details</a>	Port5	5	Enabled	0 bytes	0 bytes		Enabled	N/A	N/A	Enabled
<input type="checkbox"/> BC.CF.4F.47.7D.F1(GS1350-6HP)/6 <a href="#">details</a>	Port6	6	Enabled	0 bytes	0 bytes		N/A	N/A	N/A	Enabled
<input type="checkbox"/> D8.EC.E5.60.99.8A/1 <a href="#">details</a>	Port1	1	Enabled	0 bytes	0 bytes		N/A	N/A	N/A	Enabled
<input type="checkbox"/> D8.EC.E5.60.99.8A/2 <a href="#">details</a>	Port2	2	Enabled	0 bytes	0 bytes		N/A	N/A	N/A	Enabled
<input type="checkbox"/> D8.EC.E5.60.99.8A/3 <a href="#">details</a>	Port3	3	Enabled	0 bytes	0 bytes		N/A	N/A	N/A	Enabled
<input type="checkbox"/> D8.EC.E5.60.99.8A/4 <a href="#">details</a>	Port4	4	Enabled	0 bytes	0 bytes		N/A	N/A	N/A	Enabled

The following table describes the labels in this screen.


Table 168 Switch &gt; Configure &gt; 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.

Table 168 Switch &gt; Configure &gt; Switch ports (continued)

LABEL	DESCRIPTION
Edit	Select the ports you want to configure and click this button to configure Nebula Device settings on the ports, such as link aggregation, PoE schedule, LLDP and STP.
Aggregate	Select more than one port and click this button to group the physical ports into one logical higher-capacity link.
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 <b>Confirm</b> 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 <b>Switch &gt; Monitor &gt; Switches: Switch Details: Port Details</b> for the details. See <a href="#">Section 11.2.1.3 on page 466</a> 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 ( <b>Static</b> ) or configured to join the trunk group through LACP ( <b>LACP</b> ). If the port is connected to an uplink gateway, it shows <b>Uplink</b> .  Click <b>details</b> to display the port details screen. See <a href="#">Section 11.2.1.3 on page 466</a> .
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.

Table 168 Switch &gt; Configure &gt; Switch ports (continued)

LABEL	DESCRIPTION
Link	<p>This shows the speed of the Ethernet connection on this port.</p> <p><b>Auto</b> (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support.</p>
Connection	<p>This shows the connection status of the port.</p> <ul style="list-style-type: none"> <li>• Gray (#888888): The port is disconnected.</li> <li>• Orange (#FF8900): The port is connected and is transmitting data at 10 or 100 Mbps.</li> <li>• Green (#64BE00): The port is connected and is transmitting data at 1000 Mbps (1 Gbps).</li> <li>• Azure (#0079FF): The port is connected and is transmitting data at 2.5 Gbps.</li> <li>• Violet (#8800FF): The port is connected and is transmitting data at 5 Gbps.</li> <li>• Blue (#004FEE): The port is connected and is transmitting data at 10000 Mbps (10 Gbps).</li> </ul> <p>When the port is in the STP blocking state, failed LACP negotiation state, or failed port authentication state, a blocked icon displays.</p> <p>Move the cursor over a time slot to see the actual date and time when a port is connected or disconnected.</p>
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	<p>If STP/RSTP is enabled, this field displays the STP state of the port.</p> <p>If STP/RSTP is disabled, this field displays <b>FORWARDING</b> if the link is up, otherwise, it displays <b>Disabled</b>.</p>
Schedule	This shows the name of the PoE schedule applied to the port.
Type	This shows the port type ( <b>Trunk</b> or <b>Access</b> ).
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 <a href="#">Table 169 on page 486</a> for more information.
	Click this icon to display a greater or lesser number of configuration fields.

### 11.3.1.1 Update ports

Click to select the port you want to configure in the **Switch > Configure > Switch ports** screen.

**Figure 194** Switch > Configure > Switch ports: Edit

Update 1 port
✕

---

**General settings**
▼

Switch ports

Name  ✕

Tags

Port enabled  ▼

RSTP  ▼

STP guard  ▼

LLDP  ▼

Link  ▼

Port isolation  ▼

Auth. policy  ▼

Bandwidth control  ▼

Ingress  Kbps ✕

Egress  Kbps ✕

Loop guard  ▼

Storm control  ▼

Broadcast Limit (pps)  ✕

Multicast Limit (pps)  ✕

DLF Limit (pps)  ✕

Type  ▼

Management control  ▼

VLAN type  ▼

PVID  ✕

---

**PoE settings**
▼

---

**IPTV setting**
Override advanced IGMP setting 
▼

Leave mode  ▼  ms ✕

Maximum Group  ▼  ✕

IGMP filtering profile  ▼

Fixed router port  ▼

Close Update

The following table describes the labels in this screen.

Table 169 Switch > Configure > 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	<p>This field is available only when RSTP is enabled on the ports.</p> <p>Select <b>Root guard</b> to prevent the Nebula Devices attached to the ports from becoming the root bridge.</p> <p>Select <b>BPDU guard</b> to have the Nebula Device shut down the ports if there is any BPDU received on the ports.</p> <p>Otherwise, select <b>None</b>.</p>
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 <b>10M/Half Duplex</b> , <b>10M/Full Duplex</b> , <b>100M/Half Duplex</b> , <b>100M/Full Duplex</b> , <b>1000M/Full Duplex</b> , <b>Auto</b> , <b>10M/AN</b> , and <b>100M/AN</b> (Gigabit connections only).
Extended range	<p>Select to enable or disable extended range.</p> <p>Extended range allows the port to transmit power and data at a distance of 250 meters.</p> <p>Note: When enabled, the port's PoE <b>Power up mode</b> is locked to 802.3at, and the port's link speed is limited to 10M/Full Duplex.</p>
Media type	<p>You can insert either an SFP+ transceiver or an SFP+ Direct Attach Copper (DAC) cable into the 10 Gigabit interface of the Nebula Device.</p> <p>Select the media type (<b>SFP+</b> or <b>DAC 10G</b>) of the SFP+ module that is attached to the 10 Gigabit interface.</p>
Port Isolation	<p>Select to enable or disable port isolation on the ports.</p> <p>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.</p>
IPSG protected	Select to enable or disable IP source guard protection on the port.
Auth. policy	<p>This field is available only when you select <b>Access</b> in the <b>Type</b> field.</p> <p>Select the authentication policy type and name of the pre-configured authentication policy that you want to apply to the ports. See <a href="#">Table 178 on page 502</a> for more information on authentication policy type. See <a href="#">Section 11.3.6 on page 500</a> for more information on configuring authentication policy.</p> <p>Select <b>Open</b> if you do NOT want to enable port authentication on the ports.</p>
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 169 Switch &gt; Configure &gt; Switch ports: Edit (continued)

LABEL	DESCRIPTION
Loop guard	<p>Select to enable or disable loop guard on the ports.</p> <p>Note: The loop guard feature cannot be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.</p>
Storm Control	<p>Select to enable or disable broadcast storm control on the ports.</p>
Broadcast Limit (pps)	<p>Specifies the maximum number of broadcast packets the Nebula Device accepts per second on the ports.</p>
Multicast Limit (pps)	<p>Specifies the maximum number of multicast packets the Nebula Device accepts per second on the ports.</p>
DLF Limit (pps)	<p>Specifies the maximum number of DLF packets the Nebula Device accepts per second on the ports.</p>
Type	<p>Set the type of the port.</p> <p>Select <b>Access</b> 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.</p> <p>Select <b>Trunk</b> 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.</p>
Management control	<p>Select <b>Enabled</b> to configure the port as a management port. The default is <b>Enabled</b>. This allows the administrator to set the Nebula Device ports through which the device management VLAN traffic is allowed.</p> <p>Note: Make sure to enable this for an uplink port to maintain connection with Nebula.</p>
VLAN type	<p>This field is available only when you select <b>Access</b> in the <b>Type</b> field.</p> <p><b>None:</b> This port is a regular access port and follows the device's access port rules.</p> <p><b>Vendor ID based VLAN:</b> Apply the Vendor ID based VLAN settings from <b>Switch &gt; Configure &gt; Switch settings</b> to this port.</p> <p><b>Voice VLAN:</b> Apply the Voice VLAN settings from <b>Switch &gt; Configure &gt; Switch settings</b> to this port.</p> <p>Note: For details on configuring Vendor ID based VLAN and Voice VLAN settings, see <a href="#">Section 11.3.8 on page 504</a>.</p>
PVID	<p>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.</p> <p>Enter a number between 1 and 4094 as the port VLAN ID.</p>
Allowed VLANs	<p>This field is available only when you select <b>Trunk</b> in the <b>Type</b> field.</p> <p>Specify the VLANs from which the traffic comes. You can then transmit or receive traffic on the ports. See <a href="#">Section 3.24 on page 137</a> for the steps in setting up dynamic VLAN with RADIUS. See <a href="#">Section 3.25 on page 139</a> for more information on monitoring dynamic VLANs using event logs.</p>
PoE Settings	
PoE	<p>Select <b>Enabled</b> to provide power to a PD connected to the ports.</p>

Table 169 Switch &gt; Configure &gt; Switch ports: Edit (continued)

LABEL	DESCRIPTION
PoE schedule	<p>This field is available only when you enable PoE.</p> <p>Select a pre-defined schedule (created using the <b>Switch &gt; Configure &gt; PoE schedule</b> screen) to control when the Nebula Device enables PoE to provide power on the ports.</p> <p>Note: You must select <b>Unschedule</b> in the <b>PoE schedule</b> field before you can disable PoE on the ports.</p> <p>If you enable PoE and select <b>Unschedule</b>, PoE is always enabled on the ports.</p> <p>Note: The Nebula Device will follow the PoE schedule even when the Nebula Device is not connected to NCC.</p> <p>Click <b>Edit</b> to go to <b>Switch &gt; Configure &gt; PoE schedule</b> screen to create a new PoE schedule.</p>
PoE priority	<p>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.</p> <p>Select <b>Low</b> to set the Nebula Device to assign the remaining power to the port after all critical and medium priority ports are served.</p> <p>Select <b>Medium</b> to set the Nebula Device to assign the remaining power to the port after all critical priority ports are served.</p> <p>Select <b>Critical</b> to give the highest PD priority on the port.</p>
Power up mode	<p>Set how the Nebula Device provides power to a connected PD at power-up.</p> <p><b>802.3at</b> – 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.</p> <p><b>802.3af</b> – the Nebula Device follows the IEEE 802.3af Power over Ethernet standard to supply power to the connected PDs during power-up.</p> <p><b>Legacy</b> – 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.</p> <p><b>Pre-802.3at</b> – 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).</p> <p><b>Force 802.3at</b> – 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.</p> <p><b>802.3bt</b> – 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.</p> <p><b>Pre-802.3bt</b> – 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.</p>
Auto PD recovery	<p>Select to enable or disable automatic PD recovery on the port.</p> <p>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.</p>



Table 169 Switch &gt; Configure &gt; Switch ports: Edit (continued)

LABEL	DESCRIPTION
Detecting mode	<p>Select <b>LLDP</b> 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.</p> <p>Select <b>Ping</b> 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.</p>
Action	<p>Set the action to take when the connected Powered Device (PD) has stopped responding.</p> <p>Select <b>Reboot-Alarm</b> 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.</p> <p>Select <b>Alarm</b> to have the Nebula Device send an SNMP trap and generate a log message.</p>
Neighbor IP	<p>Set the IPv4 address of the Powered Device (PD) connected to this port.</p> <p>Note: If <b>Detecting Mode</b> is set to <b>Ping</b> and the PD supports LLDP, the connected PD's IPv4 address to which the Nebula Device sends ping requests is displayed automatically.</p>
Polling Interval	<p>Specify the number of seconds the Nebula Device waits for a response before sending another ping request.</p> <p>For example, the Nebula Device will try to detect the PD status by performing ping requests every 20 seconds.</p>
Polling Count	<p>Specify how many times the Nebula Device resends a ping request before considering the PD unreachable.</p>
Resume Polling interval (sec)	<p>Specify the number of seconds the Nebula Device waits before monitoring the PD status again after it restarts the PD on the port.</p>
PD Reboot Count	<p>Specify how many times the Nebula Device attempts to restart the PD on the port.</p> <p>The <b>PD Reboot Count</b> resets if any of the following conditions are true:</p> <ul style="list-style-type: none"> <li>• The Nebula Device successfully pings the PD.</li> <li>• You modify any <b>Auto PD Recovery</b> settings and apply them.</li> <li>• The Nebula Device restarts.</li> </ul>
Resume Power Interval (sec)	<p>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.</p>
IPTV Setting	
Overwrite advanced IGMP setting	<p>Select <b>ON</b> to overwrite the port's advanced IGMP settings (configured in the <b>Configure &gt; Advanced IGMP</b> screen) with the settings you configure in the fields below. Otherwise, select <b>OFF</b>.</p>

Table 169 Switch &gt; Configure &gt; Switch ports: Edit (continued)

LABEL	DESCRIPTION
Leave Mode	<p>Select <b>Immediate Leave</b> 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.</p> <p>Select <b>Normal Leave</b> or <b>Fast Leave</b> 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.</p> <p>In <b>Normal Leave</b> 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.</p> <p>In <b>Fast Leave</b> 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.</p>
Maximum Group	<p>Select <b>Enable</b> 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.</p> <p>Otherwise, select <b>Disable</b> to turn off multicast group limits.</p>
IGMP filtering profile	<p>An IGMP filtering profile specifies a range of multicast groups that clients connected to the Nebula Device are able to join.</p> <p>Select the name of the IGMP filtering profile to use for this port. Otherwise, select <b>No Select</b> to remove restrictions and allow the port to join any multicast group.</p>
Fixed router port	<p>Select <b>Auto</b> 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.</p> <p>Select <b>Fixed</b> 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.</p>

## 11.3.2 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 **Switch > Configure > ACL** to access this screen.

Figure 195 Switch &gt; Configure &gt; ACL

Switch > Configure > 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
<input checked="" type="checkbox"/>	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.192.168.1.0/24
	Allow	Any	Any	Any	Any	Any	Any

+ Add

The following table describes the labels in this screen.

Table 170 Switch &gt; Configure &gt; 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.

### 11.3.3 IP & Routing

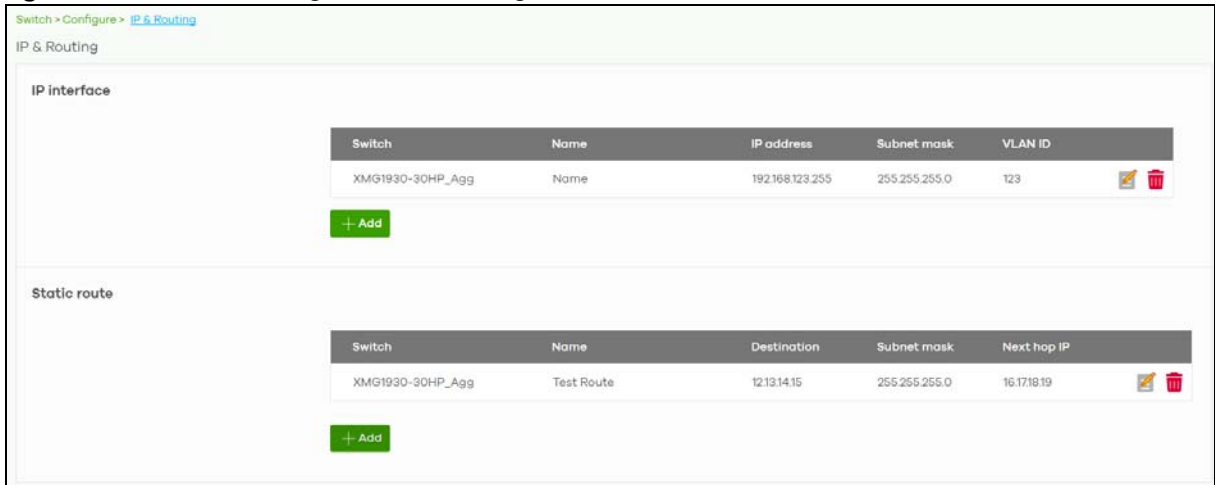
This screen enables you to create IP interfaces and static routes on Nebula Devices in the site. This allows you to do the following:

- 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 **Switch > Configure > IP & Routing** to access this screen.

**Figure 196** Switch > Configure > IP & Routing



The following table describes the labels in this screen.

Table 171 Switch > Configure > 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.

### 11.3.3.1 Add IP Interface

Click the + **Add** button on the **Switch > Configure > IP & Routing > IP Interface** screen to access this screen.

**Figure 197** Switch > Configure > IP & Routing > IP Interface > Add

The following table describes the labels in this screen.

**Table 172** Switch > Configure > 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	Enter 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 <b>Close</b> to exit this screen without saving.
Create	Click <b>Create</b> to save your changes and create the interface.

### 11.3.3.2 Add Static Route

Click the + **Add** button on the **Switch > Configure > IP & Routing > Static Route** screen to access this screen.

**Figure 198** Switch > Configure > IP & Routing > Static Route > Add

The following table describes the labels in this screen.

Table 173 Switch &gt; Configure &gt; IP &amp; Routing &gt; Static Route &gt; 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 <b>Close</b> to exit this screen without saving.
Create	Click <b>Create</b> to save your changes and create the static route.

### 11.3.4 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.

### 11.3.4.1 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 **Switch > Configure > 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 **Switch > Configure > 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.


### 11.3.4.2 ONVIF Discovery Screen

Click **Switch > Configure > ONVIF discovery** to access this screen.

**Figure 199** Switch > Configure > ONVIF discovery

The following table describes the labels in this screen.

**Table 174** Switch > Configure > 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.

## 11.3.5 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 **Switch > Configure > Advanced IGMP** to access this screen. You can make adjustments on a per-port basis using the **Switch > Configure > Switch ports** screen.

**Figure 200** Switch > Configure > Advanced IGMP

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

Switch > Configure > [Advanced IGMP](#)

Advanced IGMP

IGMP snooping

IGMP-snooping VLAN [Model list](#)

Auto-detect

x

User Assign VLANs.

Unknown multicast drop [Model list](#)

Drop on VLAN  x

IGMP filtering profiles [?](#) **0** IGMP filtering profiles

(There are no IGMP filtering profiles for this site)

[+ Add](#)

IPTV topology setup [IGMP snooping](#) [Role](#) [Port settings](#) [IGMP topology tips](#)

<input type="checkbox"/>	Switch name	IGMP snooping	IGMP report proxy	Role	Port settings
<input checked="" type="checkbox"/>	XMG1930-30HP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Querier	<a href="#">Advanced setup</a>
<input type="checkbox"/>	XGS220-30HP_Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Access	<a href="#">Advanced setup</a>



The following table describes the labels in this screen.

Table 175 Switch &gt; Configure &gt; Advanced IGMP




LABEL	DESCRIPTION
IGMP snooping	Select <b>ON</b> to enable and configure IGMP snooping settings on all Nebula Devices in the site. Select <b>OFF</b> to disable it.
IGMP-snooping VLAN	<p>Select <b>Auto-detect</b> to have the Nebula Device learn multicast group membership information of any VLANs automatically.</p> <p>Select <b>User Assigned VLANs</b> and enter the VLAN IDs to have the Nebula Device only learn multicast group membership information of the VLANs that you specify.</p> <p>Click <b>Model List</b> to view a list of Zyxel Nebula Device models that do not support this feature.</p> <p>Note: The Nebula Device can perform IGMP snooping on up to 16 VLANs.</p>
Unknown multicast drop	<p>Specify the action to perform when the Nebula Device receives an unknown multicast frame. Select <b>ON</b> to discard the frames. Select <b>OFF</b> to send the frames to all ports.</p> <p>Click <b>Model List</b> to view a list of Zyxel Nebula Device models that do and do not support this feature.</p>
Drop on VLAN	<p>This allows you to define the VLANs in which unknown multicast packets can be dropped.</p> <p>Note: The Nebula Device can drop unknown multicast packets on up to 8 VLANs.</p>
IGMP filtering profiles	<p>An IGMP filtering profile specifies a range of multicast groups that clients connected to the Nebula Device are able to join.</p> <p>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.</p>
	Click the edit icon to change the profile settings. See <a href="#">Section 11.3.5.1 on page 498</a> .
	Click the remove icon to delete the profile.
+Add	Click this button to create a new profile. See <a href="#">Section 11.3.5.1 on page 498</a> .
<p>IPTV topology setup</p> <p>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.</p>	
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 <b>Port Settings</b> screen, where you can change IGMP leave mode and IGMP filtering profile for the ports on the selected Nebula Devices. See <a href="#">Section 11.3.5.2 on page 499</a> .
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 <a href="#">Section 11.3.5 on page 496</a> for more information on IGMP snooping.

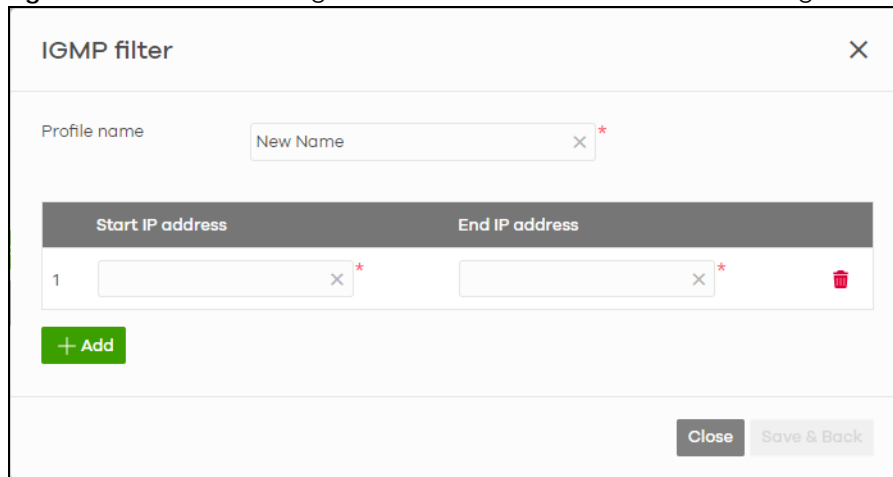
Table 175 Switch &gt; Configure &gt; Advanced IGMP (continued)

LABEL	DESCRIPTION
IGMP report proxy	<p>Click this to enable IGMP report proxy on the Nebula Device. An IGMP report is generated when monitoring multicast address or membership query.</p> <p>It is highly recommended to disable this in the following conditions:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>
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 <b>Advanced Setup</b> to open the <b>Port Settings</b> screen, where you can change IGMP leave mode and IGMP filtering profile for the ports on the Nebula Device. See <a href="#">Section 11.3.5.2 on page 499</a> .
The following fields display when the IGMP role of a Nebula Device is set to <b>Querier</b> .	
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.

### 11.3.5.1 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 **Switch > Configure > Advanced IGMP** screen.


Figure 201 Switch &gt; Configure &gt; Advanced IGMP: Add IGMP Filtering Profile



The screenshot shows the 'IGMP filter' configuration window. At the top, there's a title bar with 'IGMP filter' and a close button (X). Below the title bar, there's a 'Profile name' field containing 'New Name' with a delete icon (X) and an asterisk (\*). Underneath, there's a table with two columns: 'Start IP address' and 'End IP address'. The first row has '1' in the 'Start IP address' column and a delete icon (X) in the 'End IP address' column. Below the table is a green '+ Add' button. At the bottom right, there are 'Close' and 'Save & Back' buttons.

The following table describes the labels in this screen.

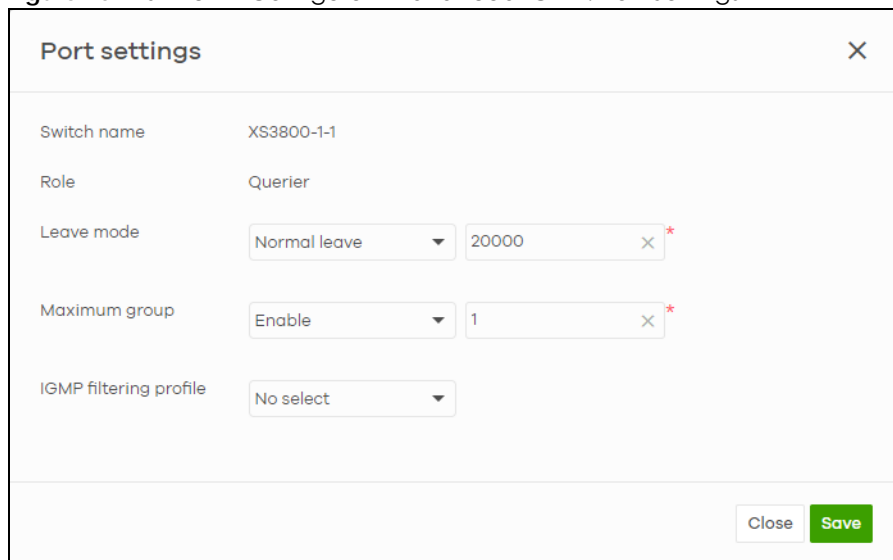
Table 176 Switch > Configure > Advanced IGMP: Add/Edit IGMP Filtering Profile

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 <b>Start IP Address</b> and <b>End IP Address</b> 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.

### 11.3.5.2 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 Setting** button or click a Nebula Device's **Advanced Setup** button in the **IPTV Topology Setup** section of the **Switch > Configure > Advanced IGMP** screen.

Figure 202 Switch > Configure > Advanced IGMP: Port Settings



The following table describes the labels in this screen.

Table 177 Switch > Configure > 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 177 Switch &gt; Configure &gt; Advanced IGMP: Port Settings (continued)

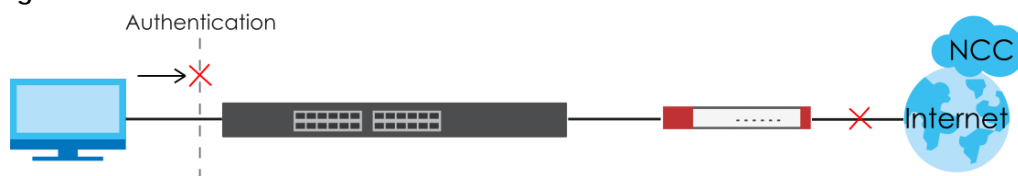
LABEL	DESCRIPTION
Leave mode	<p>Select <b>Immediate Leave</b> to set the Nebula Device to remove this port from the multicast tree immediately when an IGMP leave message is received on this port. Select this option if there is only one host connected to this port.</p> <p>Select <b>Normal Leave</b> or <b>Fast Leave</b> 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.</p> <p>In <b>Normal Leave</b> 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.</p> <p>In <b>Fast Leave</b> 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.</p>
Maximum group	<p>Select <b>Enable</b> 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.</p> <p>Otherwise, select <b>Disable</b> to turn off multicast group limits.</p>
IGMP filtering profile	<p>An IGMP filtering profile specifies a range of multicast groups that clients connected to the Nebula Device are able to join.</p> <p>Select the name of the IGMP filtering profile to use for this port. Otherwise, select <b>No Select</b> to remove restrictions and allow the port to join any multicast group.</p>
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.

### 11.3.6 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.

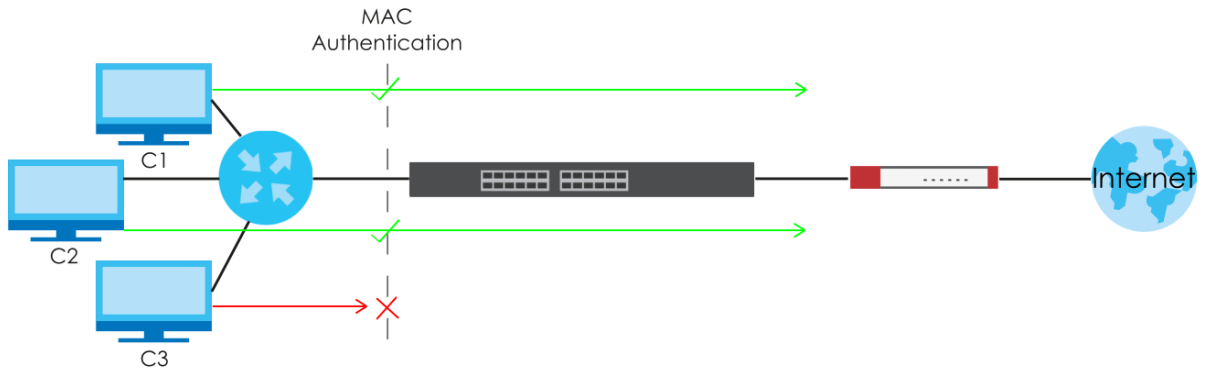
Note: Network traffic from clients will be denied when the Nebula cloud authentication server (NCAS) cannot be reached.

**Figure 203** 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 204** MAC Authentication Application



Click **Switch > Configure > Authentication** to access this screen.

**Figure 205** Switch > Configure > Authentication

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

Switch > Configure > [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	x*	x*

+ Add

**Authentication policy**

Password for MAC-Base Auth: \*\*\*\*\*

Name	Auth. type	Guest VLAN	Port security	MAC limitation	Auth. ports
1 Test	MAC-Base		<input checked="" type="checkbox"/>	0	<a href="#">g</a>

+ Add

The following table describes the labels in this screen.

Table 178 Switch &gt; Configure &gt; Authentication




LABEL	DESCRIPTION
Authentication Server	
Server type	<p>Select <b>External radius server</b> 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.</p> <p>Note: Make sure to configure VLAN for the Nebula Device before enabling VLAN assignment in the external RADIUS server.</p> <p>Select <b>Nebula cloud authentication</b> 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 <a href="#">Section 3.23 on page 136</a> for the steps in setting up MAC authentication with NCAS.</p> <p>Blocked clients do not appear in the Nebula Device MAC address table. The Nebula Device re-authenticates blocked clients when:</p> <ul style="list-style-type: none"> <li>• 5 minutes after blocked client failed authentication</li> <li>• Blocked client disconnects and reconnects to the Nebula Device port.</li> </ul> <p>Note: The <b>Blocked</b> client in the <b>Site-wide &gt; Monitor &gt; Clients &gt; Client list</b> screen has a higher priority than MAC-based authentication. All network traffic from clients will be denied when the NCAS cannot be reached.</p>
The following fields appear when you select <b>External radius server</b> as the <b>Server type</b> .	
	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 <b>Switch &gt; Configure &gt; Switch ports: Edit</b> (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	<p>Select <b>MAC-Base</b> if you want to validate access to the ports based on the MAC address and password of the client.</p> <p>Select <b>802.1X</b> if you want to validate access to the ports based on the user name and password provided by the client.</p> <p>Note: 802.1X is not supported when you select <b>Nebula cloud authentication</b> in <b>Server type</b>.</p>
Guest VLAN	<p>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.</p> <p>Enter the number that identifies the guest VLAN.</p>
Port security	Click <b>On</b> to enable port security on the ports. Otherwise, select <b>Off</b> to disable port security on the ports.

Table 178 Switch &gt; Configure &gt; 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.

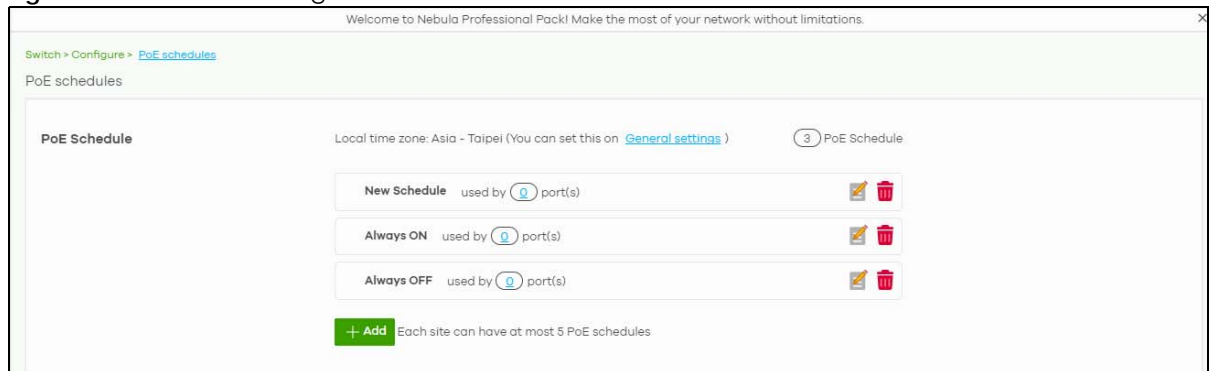
## 11.3.7 PoE Schedules

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 **Switch > Configure > 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 11.3.7.1 on page 503](#).

Figure 206 Switch &gt; Configure &gt; PoE schedules



### 11.3.7.1 Create new schedule

Click the **Add** button in the **Switch > Configure > PoE schedule** screen to access this screen.

Figure 207 Switch &gt; Configure &gt; PoE schedule: Add

The following table describes the labels in this screen.

Table 179 Switch &gt; Configure &gt; PoE schedule: Add

LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identification purposes.
Schedule templates	Select a pre-defined schedule template or select <b>Custom schedule</b> and manually configure the day and time at which PoE is enabled.
Day	This shows the day of the week.
Availability	Click <b>On</b> to enable PoE at the specified time on this day. Otherwise, select <b>Off</b> 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.

### 11.3.8 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 **Switch > Configure > Switch settings** to access this screen.



Figure 208 Switch > Configure > Switch settings

Switch > Configure > [Switch settings](#)

Switch settings

**Auto configuration recovery** [Model list](#) Beta

Auto configuration recovery ?

---

**VLAN configuration**

Management VLAN  x \*

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
<input type="text" value=""/> <span style="color: #dc3545;">x</span> <span style="color: #dc3545;">*</span>	1	<input type="text" value=""/> <span style="color: #dc3545;">x</span> <span style="color: #dc3545;">*</span> <span style="color: #dc3545;">🗑️</span>

+ Add

[What is this?](#)

QoS allows network traffic prioritization based on application and service demands. IEEE802.1P defines eight priority levels to be mapped to different class of service (CoS) queue upon traffic prioritization. For each VLAN, a traffic priority class value from 1 (low) through 6 (high) can be set. Priority 7 is reserved for system packets, while 0 is not recommended to use.

---

**Port mirroring**

Port mirroring:

Switch	Destination Port	Source Port
1 XMG1930-30HP <span style="color: #dc3545;">v</span>	<input type="text" value=""/> <span style="color: #dc3545;">x</span> <span style="color: #dc3545;">*</span>	<input type="text" value=""/> <span style="color: #dc3545;">x</span> <span style="color: #dc3545;">*</span> <span style="color: #dc3545;">🗑️</span>

+ Add

---

**Err-disable recovery**

Err-disable recovery

Cause reason	Expiration time (second)
Loop guard	<input type="text" value="300"/> <span style="color: #dc3545;">x</span> <span style="color: #dc3545;">*</span>

---

**Voice VLAN**

Voice VLAN ?

Voice VLAN ID:  x

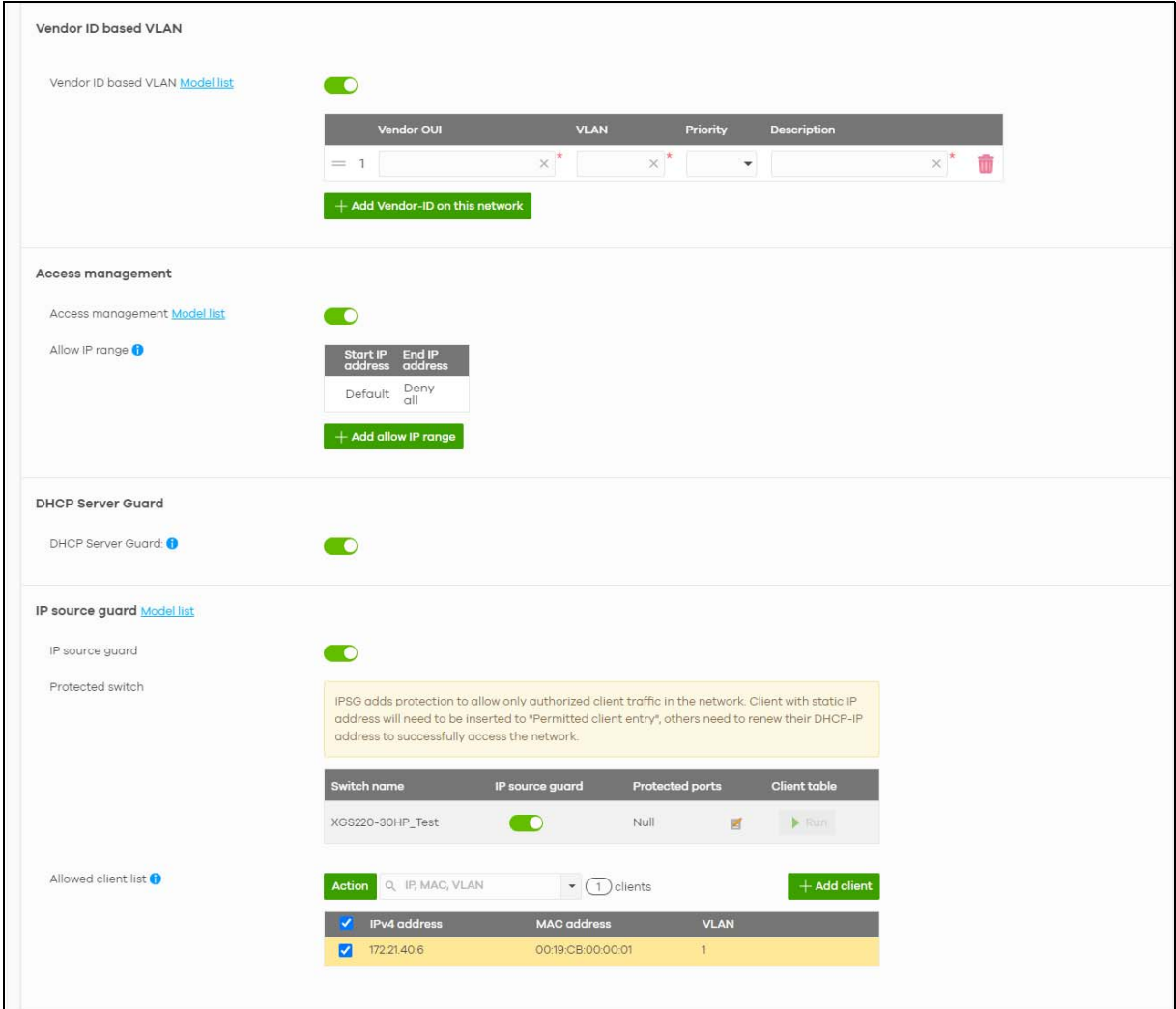
Priority:  v

Assign VLAN by:  v

OUI:

OUI	Description
1 <input type="text" value=""/> <span style="color: #dc3545;">x</span> <span style="color: #dc3545;">*</span>	<input type="text" value=""/> <span style="color: #dc3545;">x</span> <span style="color: #dc3545;">*</span> <span style="color: #dc3545;">🗑️</span>

+ Add OUI on this network



The following table describes the labels in this screen.

Table 180 Switch > Configure > Switch settings

LABEL	DESCRIPTION
Auto configuration recovery	
Auto configuration recovery	<p>When <b>On</b>, 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 <b>N Switches are currently protected by Auto Configuration Recovery</b> will be displayed.</p> <p>Otherwise, the latest configuration will be saved as the new custom default configuration.</p> <p>Note: If the NCC connectivity error occur 5 minutes after a configuration change, the Nebula Device will not return to its last saved configuration.</p> <p>Note: When <b>Auto configuration recovery</b> is turned <b>Off</b>, a pop-up message appears informing you that the locked Nebula Device(s) will be unlocked. Click <b>Confirm</b> if you wish to continue.</p>
VLAN configuration	

Table 180 Switch &gt; Configure &gt; Switch settings (continued)

LABEL	DESCRIPTION
Management VLAN	<p>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.</p> <p>Before changing the management VLAN for an uplink port, check the following to avoid disconnection with NCC:</p> <ul style="list-style-type: none"> <li>• <b>Management Control</b> is enabled in <b>Switch &gt; Configure &gt; Switch ports</b></li> <li>• The uplink port belongs to the management VLAN in <b>Switch &gt; Configure &gt; Switch ports: PVID</b>.</li> </ul>
STP configuration	
Rapid spanning tree protocol (RSTP)	Select <b>On</b> to enable RSTP on the Nebula Device. Otherwise, select <b>Off</b> .
STP bridge priority	<p>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.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge.</p> <p>Click <b>Set the bridge priority for another switch</b> 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.</p>
Quality of service	
Quality of service	<p>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).</p> <p>Click <b>Add</b> to create a new entry.</p>
Port mirroring	
Port mirroring	<p>Click <b>Add</b> to create a new entry.</p> <p>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.</p>
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 error was gone.
Voice VLAN	
Voice VLAN	<p>Select <b>On</b> to enable the Voice VLAN feature on the Nebula Device. Otherwise, select <b>Off</b>.</p> <p>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.</p>
Voice VLAN ID	Enter a VLAN ID number.
Priority	Select the priority level of the Voice VLAN from 1 to 6.

Table 180 Switch &gt; Configure &gt; Switch settings (continued)

LABEL	DESCRIPTION
Assign VLAN by	<p>Select how the Nebula Device assigns ports connected to VoIP devices to the Voice VLAN.</p> <p><b>OUI</b> (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.</p> <p><b>LLDP-MED</b>: 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.</p> <p>Note: The connected device must support LLDP-MED and have LLDP-MED enabled.</p>
OUI	<p>This field appears when you select <b>OUI</b> in the <b>Assign VLAN by</b> field.</p> <p>Click <b>Add OUI on this network</b> to add an OUI and a description for the OUI.</p> <p>An Organizationally Unique Identifier identifies a manufacturer. Typically, a device's OUI is the first three octets of the device's MAC address.</p> <p>For example, if you have an IP phone from Company A with MAC address 00:0a:95:9d:68:16, you can enter OUI <i>00:0a:95</i> to match all devices from Company A.</p>
DSCP	<p>This field appears when you select <b>LLDP-MED</b> in the <b>Assign VLAN by</b> field.</p> <p>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.</p>
Vendor ID based VLAN	
Vendor ID based VLAN	<p>Select <b>On</b> to enable the Vendor ID based VLAN feature on the Nebula Device. Otherwise, select <b>Off</b>.</p> <p>Click the <b>Add Vendor-ID on this network</b> 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 [~!@#\$%^&amp;*()_+{} :"&lt;&gt;-=[]\;',./].</p>
Access management	
Access management	<p>Select <b>On</b> to enable the access management feature on the Nebula Device. Otherwise, select <b>Off</b>.</p>
Allow IP range	<p>Click the <b>Add allow IP range</b> 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.</p>
DHCP Server Guard	
DHCP Server Guard	<p>Select <b>On</b> 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.</p> <p>Otherwise, select <b>Off</b> to disable it.</p>
IP source guard	
IP source guard	<p>Select <b>On</b> 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.</p> <p>To successfully access the network:</p> <ul style="list-style-type: none"> <li>• Client with static IP address will need to be added to the <b>Allowed client list</b></li> <li>• Client with dynamic IP address will need to get their IP address from an authorized DHCP server.</li> </ul>

Table 180 Switch &gt; Configure &gt; Switch settings (continued)

LABEL	DESCRIPTION
Protected switch	<p>This shows the Nebula Device(s).</p> <ul style="list-style-type: none"> <li>• Select <b>On</b> to enable IP source guard protection on the Nebula Device. Then click <b>Save</b>.</li> <li>• Click the edit icon to go to <b>Switch &gt; Configure &gt; Switch ports</b> to configure <b>Protected ports</b> (see <a href="#">Section 11.3.1 on page 482</a> for more information).</li> <li>• Click <b>Run</b> to display a pop-up window showing the current client table.</li> <li>• Select the DHCP-snooping or Block entries and click <b>Transfer</b> to add these to the allowed client list. Then click <b>Save</b>.</li> </ul>
Allowed client list	<p>This allows the administrator to define a set of clients. Click <b>Add client</b> to define the <b>IPv4 address</b>, <b>MAC address</b>, and <b>VLAN</b> of the static client. A previous entry will be overwritten when you enter a duplicate MAC address and VLAN ID.</p> <p>Click <b>Actions &gt; Edit</b> to modify the static client entry. Then click <b>Update</b>. The <b>MAC address</b> and <b>VLAN ID</b> will appear in red when you enter a duplicate entry.</p> <p>Click <b>Actions &gt; Delete</b> to remove the static client entry.</p> <p>Click <b>Save</b> to activate the settings.</p> <p>Note: Maximum of 128 static entries is allowed per site.</p>

# CHAPTER 12

## Access Point

### 12.1 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.

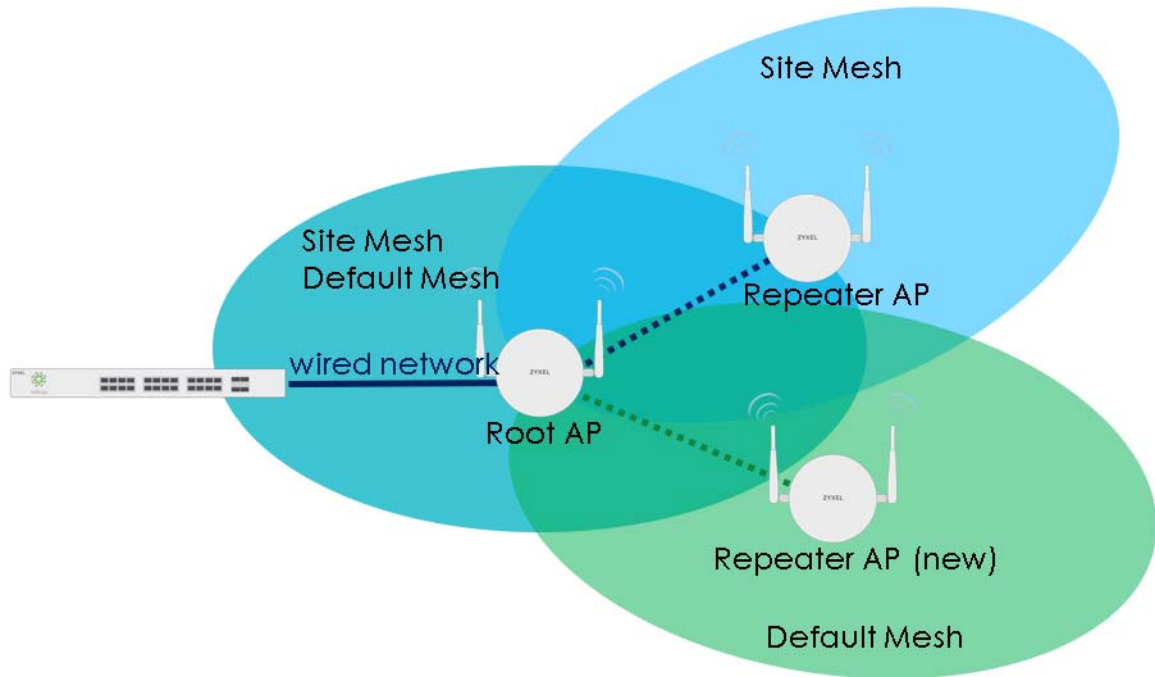
Table 181 Features/Fields Supported on Specific Nebula Devices Only

FEATURES/FIELDS	INCLUDED NEBULA DEVICES	LOCATION
Ethernet Secure Tunnel Setting in Remote AP Setting	WAC500H	Click a Nebula Device entry in the <b>Access Point &gt; Monitor &gt; Access Points</b> screen to display individual Nebula Device statistics. See <a href="#">Section 12.2.1 on page 512</a> for more information.
Wired stations		
WPA3 in Security options	NWA110AX, WAX510D, WAX650S	Click <b>Access Point &gt; Configure &gt; SSID advanced settings</b> . See <a href="#">Section 12.3.2 on page 540</a> for more information.
Ethernet Traffic options Forwarding Mode	WAC500H	Click an entry in the <b>Port setting</b> table of the <b>Access Point &gt; Configure &gt; AP &amp; port settings</b> screen to access the <b>Edit – AP &amp; port settings</b> screen. See <a href="#">Section 12.3.8.1 on page 567</a> for more information.

#### 12.1.1 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 209 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.

## 12.1.2 Smart Mesh Network Topology

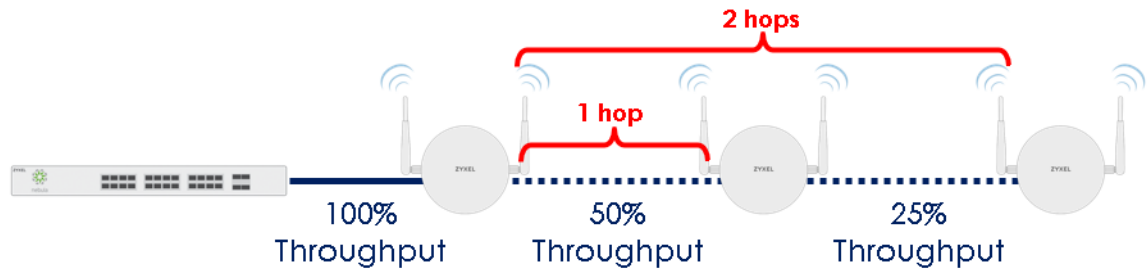
After you add a Nebula Device to an NCC site and then turn it on, the new Nebula Device automatically connects to a mesh network called the **default mesh**. The Nebula Device then tries to connect to a mesh controller and contact NCC. After the Nebula Device successfully contacts NCC and joins the site,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

### 12.1.2.1 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 210** Nebula Smart Mesh Wireless Hops

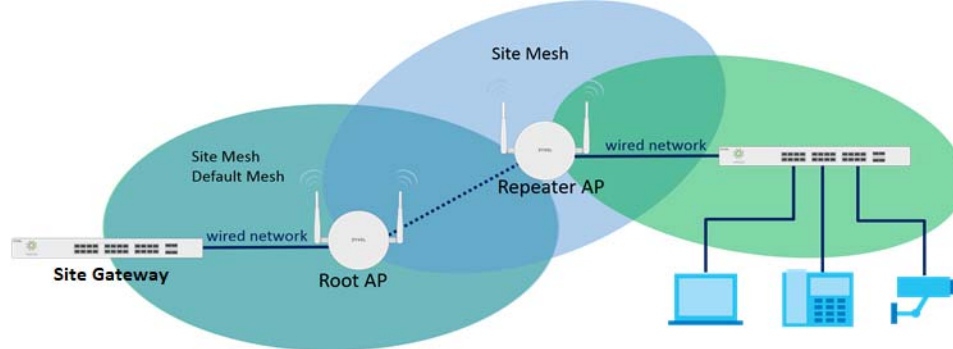


### 12.1.2.2 Wireless Bridge

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 211** Nebula Smart Mesh Wireless Bridge



## 12.2 Monitor

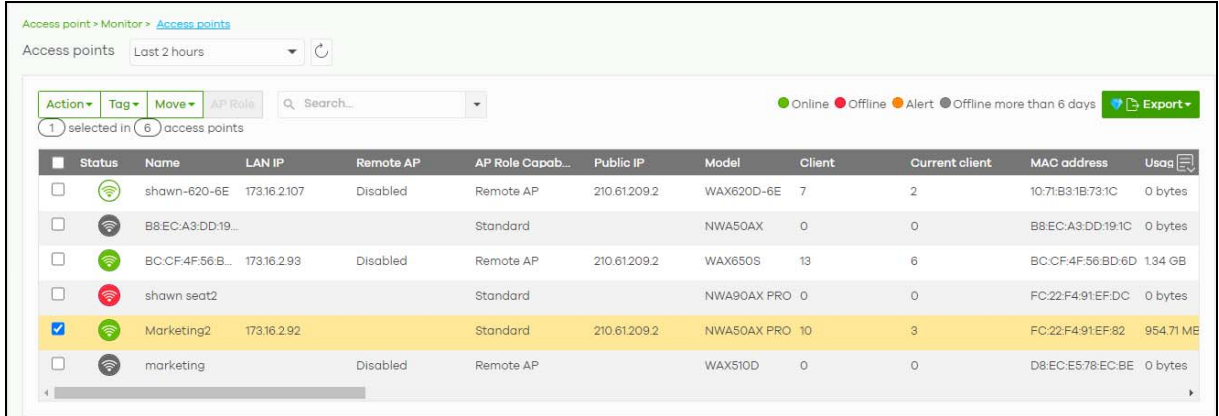
Use the **Monitor** menus to check Nebula Device information, client information, event log messages and summary report for Nebula Devices in the selected site.

### 12.2.1 Access Points

This screen allows you to view the detailed information about an Nebula Device in the selected site. Click **Access point > Monitor > Access points** to access this screen.



Figure 212 Access point > Monitor > Access points



The following table describes the labels in this screen.

Table 182 Access point > Monitor > Access points

LABEL	DESCRIPTION
Access point	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. <div data-bbox="495 1102 1198 1428" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"><b>Update programmable pre-shared key</b> <span style="float: right;">✕</span></p> <p><input type="radio"/> Re-generate a random pre-shared key</p> <p><input checked="" type="radio"/> Custom pre-shared key <input style="margin-left: 5px;" type="text" value="*****"/></p> <p style="text-align: center; color: red; font-size: small;">WPA2 pre-shared-key supports 8-63 characters</p> <p style="text-align: right;"><input type="button" value="Cancel"/> <input type="button" value="OK"/></p> </div> <p>Note: <b>Programmable SSID</b> must be enabled in <b>Access Point &gt; Configure &gt; SSID settings</b>.</p>
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.  At the time of writing, there are two pre-defined tags. The LED tags have priority over the LED setting in the <b>Site-Wide &gt; General Setting</b> screen. <ul style="list-style-type: none"> <li>LED_Off: this tag allows you to turn off the LEDs (except the locator LED) on the selected Nebula Devices.</li> <li>LED_On: this tag allows you to have the LEDs stay lit after the selected Nebula Devices are ready.</li> </ul>
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.

Table 182 Access point &gt; Monitor &gt; Access points (continued)



LABEL	DESCRIPTION
AP Role	<p>Select one or multiple Nebula Devices and click this button to enable or disable the <b>Remote AP</b> feature.</p> <p>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.</p> <p>Note: Enabling Remote Nebula Device automatically enables Ethernet and wireless storm control on the Nebula Device.</p>
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	<p>This shows the status of the Nebula Device.</p> <ul style="list-style-type: none"> <li>• Green: The Nebula Device is online and has no alerts.</li> <li>• Amber: The Nebula Device has alerts.</li> <li>• Red: The Nebula Device is offline.</li> <li>• Gray: The Nebula Device has been offline for 7 days or more.</li> <li>• : The Nebula Device is acting as a repeater.</li> </ul> <p>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 <b>Limited Power mode</b>.</p>
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 <b>Enabled</b> or <b>Disabled</b> .
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 ( <b>Remote AP</b> ) or not ( <b>Standard AP</b> ).
Public IP	This shows the global (WAN) IP address of the Nebula Device.
Model	This shows the model number of the Nebula Device.
Client	This shows how many clients are connected to the Nebula Device within the specified time period.
Current client	This shows how many clients are currently connecting to the Nebula Device.
MAC address	This shows the MAC address of the Nebula Device.
Channel	This shows the channel ID the Nebula Device is using.
Channel Utilization 2.4GHz	This shows the percentage of the 2.4 GHz channel ID usage.
Channel Utilization 5GHz	This shows the percentage of the 5 GHz channel ID usage.
Channel Utilization 6GHz	This shows the percentage of the 6 GHz channel ID usage.
Usage	This shows the amount of data consumed by the Nebula Device's clients.
% Usage	This shows the percentage of the Nebula Device's data usage.
Description	This shows the user-specified description for the Nebula Device.

Table 182 Access point &gt; Monitor &gt; Access points (continued)

LABEL	DESCRIPTION
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	<p>This shows the access point connection status.</p> <p>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.</p>
Ethernet 1	This shows the speed and duplex mode of the Ethernet connection on the Nebula Device's up-link port. It shows <b>Down</b> 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 ( <b>DHCP</b> ), or manually ( <b>Static IP</b> ).
Uplink AP	<p>This shows the role and descriptive name of the Nebula Device to which this Nebula Device is connected wirelessly.</p> <p>When Smart Mesh is enabled and the mesh extender loses connection to the mesh controller, click <b>Reconnect</b> to re-establish connection.</p> <p>Note: Make sure to enable <b>Manual uplink</b> in <b>Access point &gt; Monitor &gt; Access point: Details &gt; Status &gt; Smart mesh &gt; Edit</b>. You also need to specify the mesh controller in <b>select an AP</b>. See <a href="#">Table 183 on page 518</a> for more information.</p>
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	<p>This shows whether wireless bridge is enabled on the Nebula Device.</p> <p>For more information about wireless bridge, see <a href="#">Section 12.1.2.2 on page 512</a>.</p>
Uplink	This shows whether the Nebula Device is connected to the gateway through a wired Ethernet connection or WiFi connection.
Power mode	<p>This shows the Nebula Device's power status.</p> <p><b>Full</b> – 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.</p> <p><b>Limited</b> – 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.</p> <p>When the Nebula Device's power mode is <b>Limited</b>, the Nebula Device throughput decreases and has just one transmitting radio chain.</p> <p>It always shows <b>Full</b> if the Nebula Device does not support power detection.</p>
Firmware availability	This shows whether the firmware on the Nebula Device is <b>Up to date</b> , there is firmware update available for the Nebula Device ( <b>Upgrade available</b> ), or a specific version of firmware has been installed by Zyxel customer support ( <b>Locked</b> ).

Table 182 Access point &gt; Monitor &gt; Access points (continued)

LABEL	DESCRIPTION
Firmware status	This shows whether the firmware installed on the Nebula Device is up-to-date.
Firmware type	<p>This shows <b>Stable</b> when the installed firmware may not have the latest features but has passed Zyxel internal and external testing.</p> <p>This shows <b>Latest</b> when the installed firmware is the most recent release with the latest features, improvements, and bug fixes.</p> <p>This shows <b>General Availability</b> when the installed firmware is a release before <b>Latest</b>, but is still undergoing Zyxel external testing.</p> <p>This shows <b>Dedicated</b> 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.</p> <p>This shows <b>Beta</b> when the installed firmware is a release version for testing the latest features and is still undergoing Zyxel internal and external testing.</p> <p>This shows <b>N/A</b> when the Nebula Device is offline and its firmware status is not available.</p>
Current version	This shows the firmware version currently installed on the Nebula Device.
Remote AP VPN	<p>This shows which VPN the Remote Nebula Device tunnel is configured to use.</p> <p>If Remote Nebula Device is disabled, this field shows <b>Disconnected</b>.</p>
	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.

### 12.2.1.1 Access Point Details

Click a Nebula Device entry in the **Access point > Monitor > Access points** screen to display individual Nebula Device statistics.

Figure 213 Access point > Monitor > Access points: Details Part 1

Access point > Monitor > [Access point](#) > wax650

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

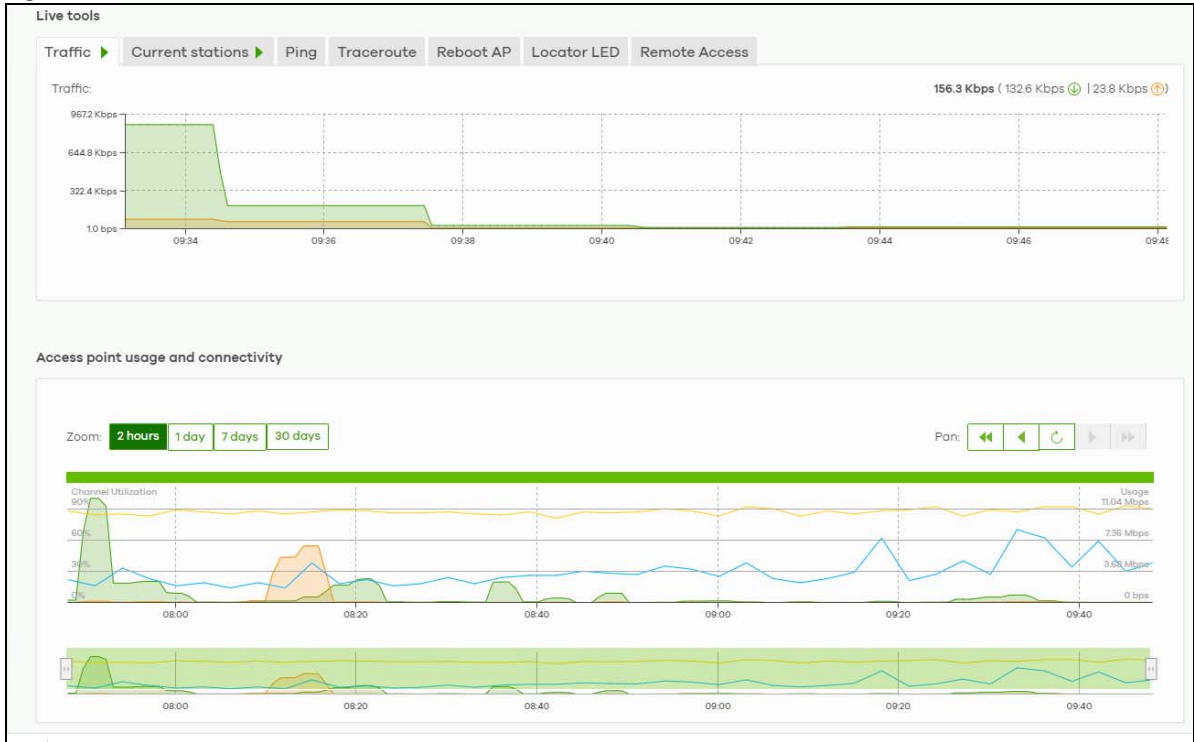
- LAN IP: 192.168.11.33   
Gateway: 192.168.11.1 | DNS: 8.8.8.8
- Public IP: 210.61.209.2
- Usage: 1.37 GB used in the last 24 hours.
- Current clients: [3 client\(s\)](#)
- Topology: [Show](#)
- Neighbor info: B8:EC:A3:2B:4C:BA(NSW100)/2/Uplink
- Link: Uplink: 1000M/Full  
LAN 1: Down
- Ports: LAN 1  
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. i
- Firmware availability: [Upgrade available](#)
- Current version: V6.40(ABRM.6)-DF-2022-08-25 (General Availability)

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](#)

Figure 214 Access point > Monitor > Access points: Details Part 2



The following table describes the labels in this screen.

Table 183 Access point > Monitor > 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 183 Access point > Monitor > Access points: Details (continued)

LABEL	DESCRIPTION																			
Remote AP	<p>Click this to enable or disable the <b>Remote AP</b> feature.</p> <p><b>Remote AP</b> 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.</p> <p>With the <b>Remote AP</b> 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.</p> <p>Note: Enabling <b>Remote AP</b> automatically enables Ethernet and wireless storm control on the Nebula Device. At the time of writing, <b>Ethernet Secure Tunnel Setting</b> for <b>Remote AP Setting</b> is available for WAC500H only.</p> <div data-bbox="537 753 1471 1323" style="border: 1px solid black; padding: 10px;"> <p><b>Remote AP Setting</b> <span style="float: right;">X</span></p> <p><b>Local SSID Setting</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Enabled</th> <th>SSID</th> <th>Security Mode</th> <th>Key</th> <th>Band</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td></td> <td style="text-align: center;">X *</td> <td>WPA2-Perso...</td> <td style="text-align: center;">*</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td></td> <td style="text-align: center;">X *</td> <td>WPA2-Perso...</td> <td style="text-align: center;">*</td> </tr> </tbody> </table> <p><b>Ethernet Secure Tunnel Setting</b> <span style="color: green; font-weight: bold;">Beta</span></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Enabled</th> <th>Tunnel to gateway interface</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>VLAN520</td> </tr> </tbody> </table> <p style="text-align: right;"><span>Cancel</span> <span style="background-color: green; color: white; padding: 2px 5px;">Save</span></p> </div> <p>Configure and enable up to two <b>SSID(s)</b> in <b>Local SSID Setting</b>. WiFi clients connected to these SSIDs are forwarded to the local network of the remote site. The <b>Local SSID Setting</b> are different from the SSIDs you configured in <b>Access Point &gt; Configure &gt; SSID advanced settings</b>. See <a href="#">Section 12.3.2 on page 540</a> for the description of the fields.</p> <p>Select from the available LAN or VLAN interface in <b>Tunnel to gateway interface</b> to enable it, and click <b>Save</b>.</p>	Enabled	SSID	Security Mode	Key	Band	<input type="checkbox"/>		X *	WPA2-Perso...	*	<input type="checkbox"/>		X *	WPA2-Perso...	*	Enabled	Tunnel to gateway interface	<input checked="" type="checkbox"/>	VLAN520
Enabled	SSID	Security Mode	Key	Band																
<input type="checkbox"/>		X *	WPA2-Perso...	*																
<input type="checkbox"/>		X *	WPA2-Perso...	*																
Enabled	Tunnel to gateway interface																			
<input checked="" type="checkbox"/>	VLAN520																			
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 183 Access point &gt; Monitor &gt; Access points: Details (continued)

LABEL	DESCRIPTION
LAN IP	<p>This shows the local (LAN) IP address of the Nebula Device. It also shows the IP addresses of the gateway and DNS server.</p> <p>Click the edit icon to open a screen where you can change the IP addresses, VLAN ID number and tagging setting.</p> <div data-bbox="537 422 1403 1010" style="border: 1px solid black; padding: 10px;"> <p style="text-align: right;"><b>Set IP Address</b> <span style="float: right;">✕</span></p> <p>IP type <span style="float: right;">Static IP ▾</span></p> <p>IP <span style="float: right;">✕</span></p> <p>Management VLAN ID <span style="float: right;">1 ✕ (1-4094)</span></p> <p><input checked="" type="radio"/> Untagged <input type="radio"/> Tagged</p> <p>Subnet mask <span style="float: right;">✕</span></p> <p>Gateway <span style="float: right;">✕</span></p> <p>Primary DNS <span style="float: right;">✕</span></p> <p style="text-align: right;"><span>Close</span> <span style="background-color: #28a745; color: white; padding: 2px 5px;">OK</span></p> </div>
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 <b>Show</b> to go to the <b>Site-Wide &gt; Monitor &gt; Topology</b> screen. See <a href="#">Section 7.1.7 on page 266</a> .
Neighbor info	This shows the LLDP information received on the up-link port.
Link	<p>This shows the speed and duplex mode of the Ethernet connection on the Nebula Device's ports.</p> <p>It shows <b>Uplink: Wireless</b> if the access point is a mesh extender and connected to a mesh controller wirelessly.</p> <p>A warning icon displays when the Nebula Device is running at 100 Mbps or a lower speed.</p>
Ports	<p>This is available only for the Nebula Device that has one or more than one Ethernet LAN port (except the uplink port).</p> <p>This shows the PVID of the LAN port and the ID number of VLANs to which the LAN port belongs. See <a href="#">Section 12.3.8 on page 564</a> for how to change the port's VLAN settings.</p>
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 183 Access point &gt; Monitor &gt; Access points: Details (continued)

LABEL	DESCRIPTION
Power mode	<p>This shows <b>Full</b> when the Nebula Device receives power directly through a power outlet.</p> <p>This shows <b>Full (Power by DC)</b> when the Nebula Device receives power using a power adapter.</p> <p>This shows <b>Full (Power by PoE)</b> 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.</p> <p>This shows <b>Limited (Require 802.3bt power)</b> 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.</p> <p>This shows <b>Limited (Require 802.3at power)</b> 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.</p> <p>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.</p> <p>Click the edit icon to open a screen where you can enable full power mode.</p> <div data-bbox="537 856 1360 1119" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><b>Power Setting</b> <span style="float: right;">✕</span></p> <p><input checked="" type="checkbox"/> Force override the power mode to full power</p> <p><b>Note:</b> Please make sure the power source can provide full power to avoid the system interrupt issue.</p> <p style="text-align: right;"><span>Close</span> <span>Update</span></p> </div> <p>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.</p>
Antenna	This displays the antenna orientation settings for the Nebula Device that comes with internal antennas and also has an antenna switch.
Smart mesh	<p>This shows whether Nebula Smart Mesh is enabled on the Nebula Device.</p> <p>For more information about Smart Mesh, see <a href="#">Section 12.1.1 on page 510</a>.</p> <p>To view the list of Nebula Devices that support smart mesh, go to <b>Help &gt; Device function table</b>.</p>

Table 183 Access point &gt; Monitor &gt; Access points: Details (continued)

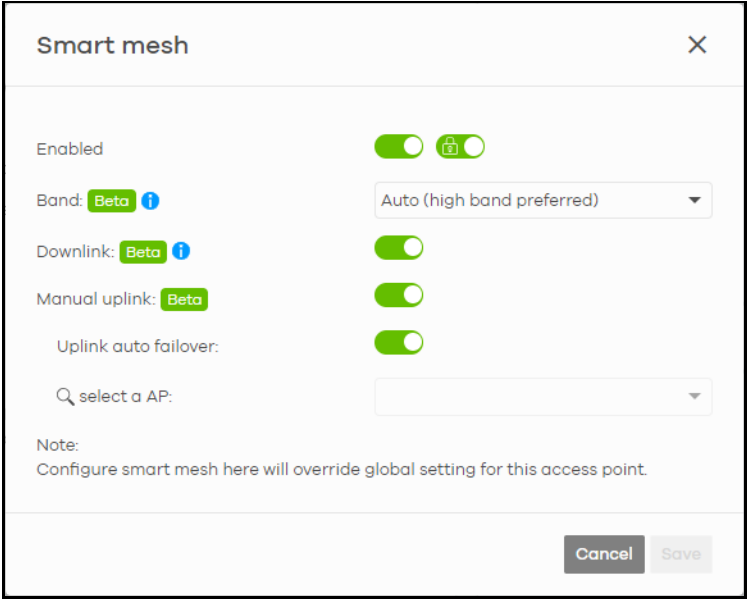

LABEL	DESCRIPTION
Edit	Edit the Nebula Device's Smart Mesh settings. 
Enabled	Enable or disable Smart Mesh on the Nebula Device. This setting overrides the Smart Mesh settings configured for the Nebula Device's site in NCC.
Lock	When enabled, the Nebula Device's local Smart Mesh settings overrides the 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 <b>Lock</b> to on and <b>Enabled</b> 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 <b>Lock</b> to on and <b>Enabled</b> to on.
Band	This setting will apply to mesh extender. <ul style="list-style-type: none"> <li>• Select <b>Auto (high band preferred)</b> to allow the mesh extender to select a higher radio band mesh controller.</li> <li>• Select <b>2.4 GHz</b> to use the 2.4 GHz band for regular Internet surfing and downloading.</li> <li>• Select <b>5 GHz</b> or <b>6 GHz</b> to use the 5 or 6 GHz band for time sensitive traffic like high-definition video, music, and gaming.</li> </ul> Note: <b>6 GHz</b> 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 <a href="#">Section 12.1.2.2 on page 512</a> . Note: Wireless bridge can only work when smart mesh is enabled in this screen.
Edit	Edit the Nebula Device's wireless bridge settings.

Table 183 Access point &gt; Monitor &gt; Access points: Details (continued)

LABEL	DESCRIPTION
Enabled	<p>Enable or disable wireless bridge on the Nebula Device.</p> <p>Note: If Smart Mesh is disabled for the site in NCC, then enabling wireless bridge automatically enables Smart Mesh on the Nebula Device.</p>
Allowed VLANs	<p>Enter the IDs of the VLANs that the Nebula Device will forward over the wireless bridge.</p> <p>By default, this field uses the VLANs allowed for LAN1 at <b>Access point &gt; Configure &gt; AP &amp; port settings</b>. For details, see <a href="#">Section 12.3.8 on page 564</a>.</p>
History	Click <b>Event log</b> to go to the <b>Access point &gt; Monitor &gt; Event log</b> 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	<p>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).</p> <div data-bbox="537 852 1216 1293" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: right;"><b>Position device</b> <span style="float: right;">✕</span></p> <hr/> <p>Update my device's location. <a href="#">What is this?</a></p> <p><input checked="" type="radio"/> Use the device's IP address (GEO IP).</p> <p><input type="radio"/> Get my location from web browser.</p> <p><input type="radio"/> Use the following address or coordinates.</p> <div style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <input style="width: 100%;" type="text"/> <span style="float: right;">✕</span> </div> <p style="text-align: right;"> <input type="button" value="Cancel"/> <input type="button" value="Update"/> </p> </div> <ul style="list-style-type: none"> <li>Select <b>GEO IP</b> to use the public IP address of the Nebula Device.</li> <li>Select <b>Get my location from web browser</b> to use the public IP address of the computer accessing the NCC portal.</li> <li>Select <b>Use the following address or coordinates</b> to enter the complete address or coordinates of the Nebula Device.</li> </ul> <p>Note: Nebula Devices that are offline cannot use GEO IP.</p>
Photo	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.
Live tools	
Traffic	This shows the Nebula Device traffic statistics.
Current stations	This shows the Nebula Device's connected WiFi clients' <b>MAC address, SSID name, IPv4 Address, Signal strength, Security, Channel, Tx rate, Rx rate, Association time, and Capability</b> .
Ping	<p>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 <b>Ping</b>.</p> <p>This can be used to determine if the Nebula Device and the computer are able to communicate with each other.</p>

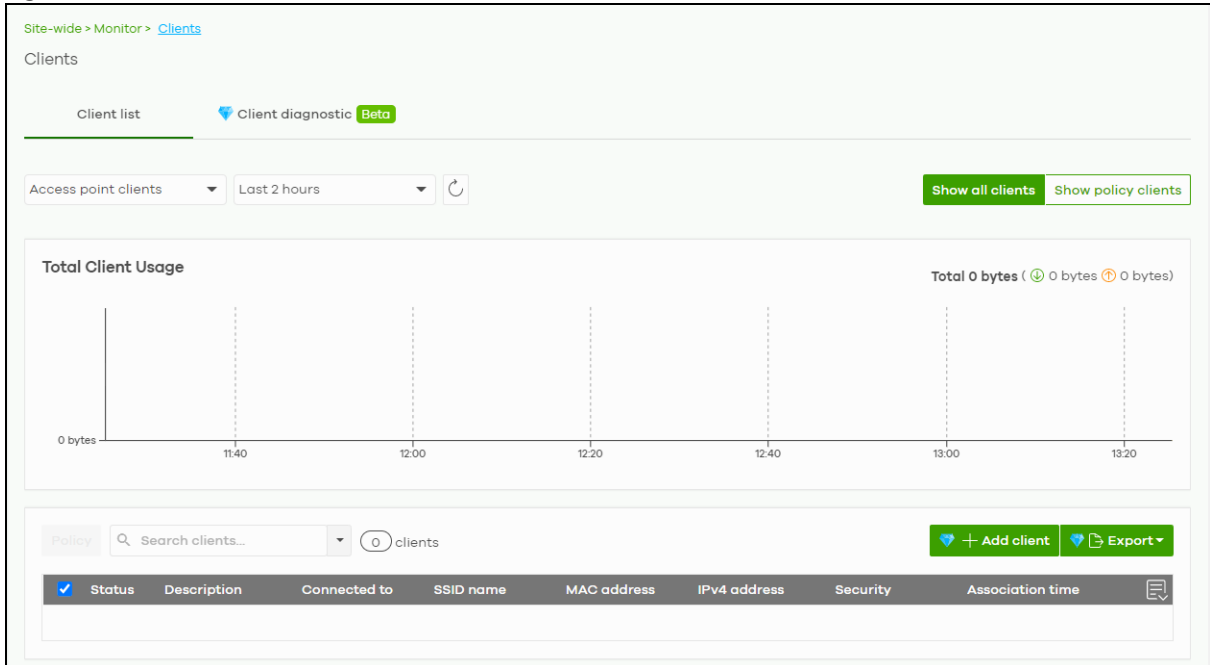
Table 183 Access point &gt; Monitor &gt; Access points: Details (continued)

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 <b>Run</b> . This determines the path a packet takes to the specified computer.
Reboot AP	Click the <b>Reboot</b> 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 <b>Establish</b> .  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' <b>MAC address</b> , <b>IPv4 Address</b> , <b>Port number</b> , and the <b>VLAN ID</b> assigned to the wired station.  Note: At the time of writing <b>Wired stations</b> 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.

## 12.2.2 Clients

This screen allows you to view the connection status and detailed information about clients connected to an Nebula Device in the selected site. Click **Access Point > Monitor > Clients** to access this screen.

Figure 215 Access Point &gt; Monitor &gt; Clients



The following table describes the labels in this screen.

Table 184 Access Point &gt; Monitor &gt; Clients

LABEL	DESCRIPTION
Clients	Select to view the connected device information and connection status in the past two hours, day, week or month. <ul style="list-style-type: none"> <li>Select <b>Show all clients</b> to show clients that have been online during the selected time period.</li> <li>Select <b>Show policy clients</b> 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.</li> </ul>
	Click this button to reload the data-related frames on this page.
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.

Table 184 Access Point &gt; Monitor &gt; Clients (continued)

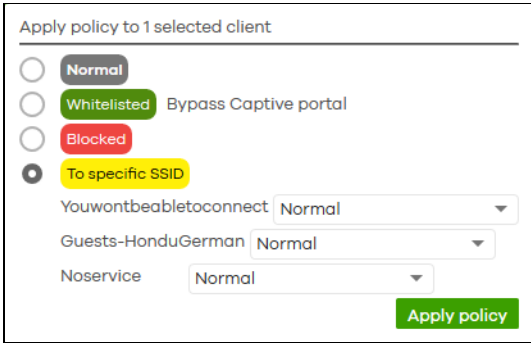

LABEL	DESCRIPTION
Policy	<p>Select the clients from the table below, and then choose the security policy that you want to apply to the selected clients. Choose <b>Normal</b> to apply the captive portal authentication to the selected clients. To allow the selected clients to bypass captive portal authentication, choose <b>Whitelisted</b>. Choose <b>Blocked</b> when the selected clients fails the captive portal authentication. Choose <b>To specific SSID</b> to selectively apply captive portal authentication to specific_SSID. Then, click <b>Apply policy</b>.</p> 
Search	Specify your desired filter criteria to filter the list of clients.
Clients	This shows the number of clients connected to an Nebula Device in the site network.
Add client	Click this button to open a window where you can specify a client's name and MAC address to apply a policy before it is connected to the Nebula Device's network.
Export	Click this button to save the client list as a CSV or XML file to your computer.
Status	This shows whether the client is online (green) or offline (red), and whether the client is wired or WiFi.
Description	<p>This shows the descriptive name of the client.</p> <p>Click the name to display the individual client statistics. See <a href="#">Section 12.2.2.1 on page 527</a>.</p>
Connected to	<p>This shows the name of the Nebula Device to which the client is connected.</p> <p>Click the name to display the individual Nebula Device statistics. See <a href="#">Section 12.2.1.1 on page 516</a>.</p>
SSID name	This shows the name of the Nebula Device's WiFi network to which the client is connected.
MAC address	This shows the MAC address of the client.
IPv4 address	This shows the IP address of the client.
Channel	This shows the channel ID the client is using.
Band	This shows the WiFi frequency band currently being used by the client.
Signal strength	<p>This shows the RSSI (Received Signal Strength Indicator) of the client's WiFi connection, and an icon showing the signal strength.</p> <p>Icon default thresholds:</p> <ul style="list-style-type: none"> <li>Green/5 blocks: signal is greater than <math>-67</math> dBm, strong signal</li> <li>Amber/4 blocks: signal <math>-67</math> to <math>-73</math> dBm, average signal</li> <li>Amber/3 blocks: signal <math>-74</math> to <math>-80</math> dBm, below average signal</li> <li>Red/2 blocks: signal is less than <math>-80</math> dBm, weak signal</li> </ul>
Security	This shows which secure encryption method is being used by the client to connect to the Nebula Device.
Tx Rate	This shows maximum transmission rate of the client.
Rx Rate	This shows maximum reception rate of the client.
Download	This shows the amount of data received by the client since it last connected.

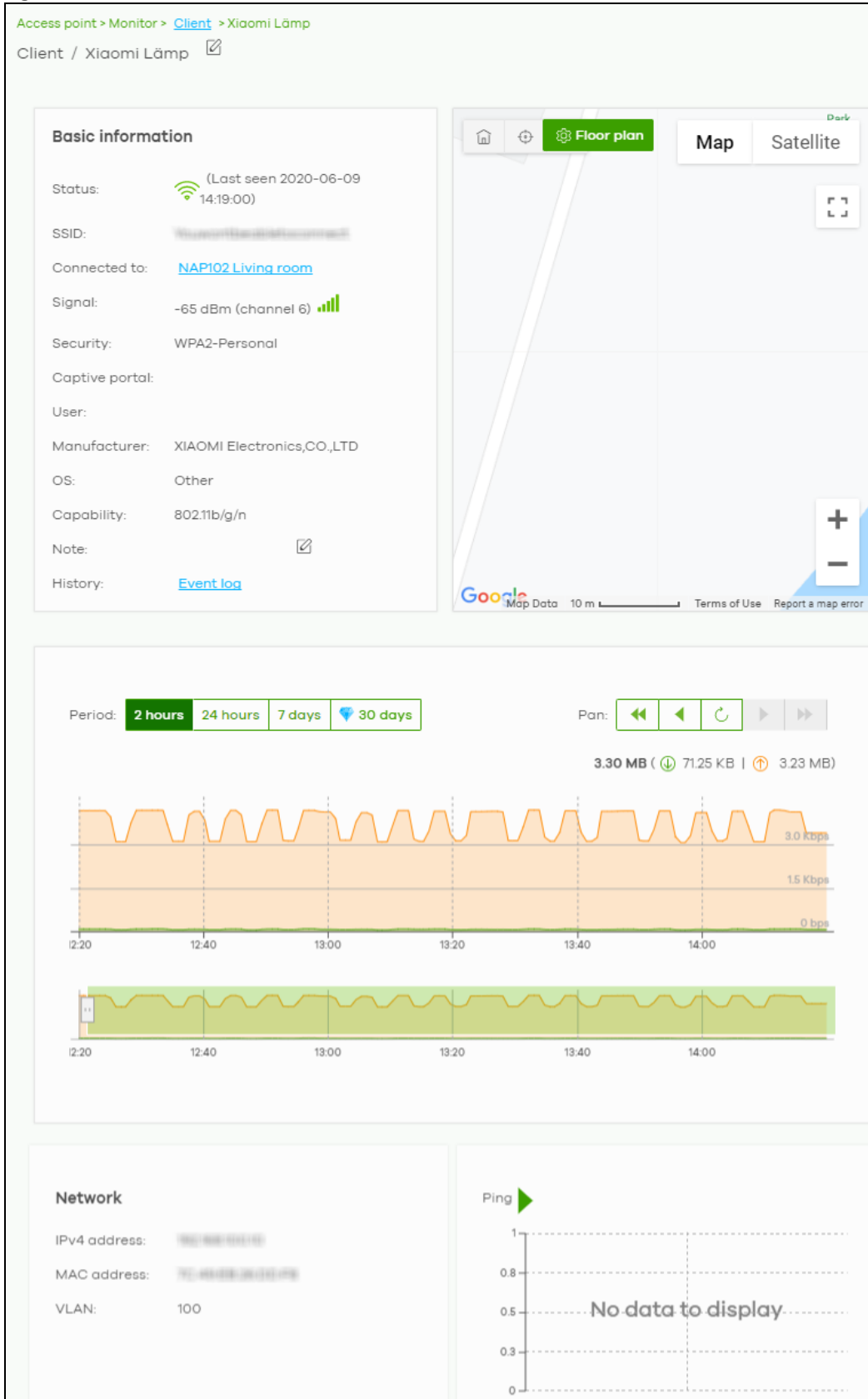
Table 184 Access Point &gt; Monitor &gt; Clients (continued)

LABEL	DESCRIPTION
Upload	This shows the amount of data transmitted from the client since it last connected.
Usage	This shows the amount of data consumed by the access point (upload + download) since it last connected.
Association time	This shows the date and time the client associated with the Nebula Device.
First seen	This shows the first date and time the client was discovered.
Last seen	This shows the last date and time the client was discovered.
Capability	This shows the WiFi standards supported by the client or the supported standards currently being used by the client.
Manufacturer	This shows the manufacturer of the client device.
Authentication	This shows the authentication method used by the client to access the network. This shows <b>Unauthorized</b> if the captive portal page displays but the client has not proceeded with the authentication process. The field is blank if web authentication is disabled.
User	This shows the user account information used to log into the NCC through captive portal, using Facebook login or 802.1x with Nebula cloud authentication or a RADIUS server. This field is blank if the user logs in through Facebook WiFi or web authentication is disabled.
OS	This shows the operating system running on the client device.
Policy	This shows the security policy applied to the client.
VLAN	This shows the ID number of the VLAN to which the client belongs.
Note	This shows additional information for the client.
	Click this icon to display a greater or lesser number of configuration fields.

### 12.2.2.1 Client Details

Click a client entry in the **Access Point > Monitor > Clients** screen to display individual client statistics.

Figure 216 Access Point > Monitor > Clients: Client Details





The following table describes the labels in this screen.

Table 185 Access Point &gt; Monitor &gt; Clients: Client Details

LABEL	DESCRIPTION
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 Nebula Device's WiFi network to which the client is connected.
Connected to	This shows the name of the Nebula Device to which the client is connected. Click the name to display the individual Nebula Device statistics. See <a href="#">Section 12.2.1.1 on page 516</a> .
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: <ul style="list-style-type: none"> <li>Green/5 blocks: signal is greater than -67 dBm, strong signal</li> <li>Amber/4 blocks: signal -67 to -73 dBm, average signal</li> <li>Amber/3 blocks: signal -74 to -80 dBm, below average signal</li> </ul> Red/2 blocks: signal is less than -80 dBm, weak signal
Security	This shows the encryption method used to connect to the Nebula Device.
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 client device connected to the Nebula Device.
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 <b>Event log</b> to go to the <b>Access Point &gt; Monitor &gt; Event log</b> 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. If you applied a security policy to a client using the <b>Add client</b> button in the <b>Access Point &gt; Monitor &gt; Clients</b> screen, and the client has never been connected to the Nebula Device's network, an edit icon appears allowing you to modify the client's MAC address,
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 Device 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.

## 12.2.3 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 **Access Point > Monitor > Event Log** to access this screen.

**Figure 217** Access Point > Monitor > Event log

The screenshot shows the 'Event log' interface. At the top, there are search filters for 'Access Point', 'Keyword', and 'Category', all set to 'Any'. Below these are date and time filters: 'Before' (2019-10-30), '17:12', '1h', and 'UTC+8'. A 'Search' button is present. Below the filters, there are navigation buttons for 'Newer' and 'Older', a count of '135' events, and an 'Export' button. The main part of the screen is a table with the following columns: 'Time', 'Access point', 'Category', and 'Detail'. The table contains several entries, all with the category 'Wireless LAN'. The details include messages about station association, blocking, and WPA authenticator disconnect requests.

Time	Access point	Category	Detail
2019-10-30 16:14:23	[Link]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has associated on Channel: 6, SS...
2019-10-30 16:14:27	[Link]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by Hostapd3 on Ch...
2019-10-30 16:14:27	[Link]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by prev-Auth Failed ...
2019-10-30 16:14:27	[Link]	Wireless LAN	WPA authenticator requests disconnect: reason 1. Interf...
2019-10-30 16:14:27	[Link]	Wireless LAN	WPA authenticator requests disconnect: reason 2. Interf...
2019-10-30 16:19:26	[Link]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has associated on Channel: 6, SS...
2019-10-30 16:19:30	[Link]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by Hostapd3 on Ch...
2019-10-30 16:19:30	[Link]	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by prev-Auth Failed ...
2019-10-30 16:19:30	[Link]	Wireless LAN	WPA authenticator requests disconnect: reason 1. Interf...
2019-10-30 16:19:30	[Link]	Wireless LAN	WPA authenticator requests disconnect: reason 2. Interf...

At the bottom of the table, there is a pagination control showing 'Page 1 of 14' and 'Results per page: 10'.

## 12.2.4 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 **Access Point > Monitor > Wireless Health** to access this screen.

Figure 218 Access Point > Monitor > Wireless Health

Access point > Monitor > [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

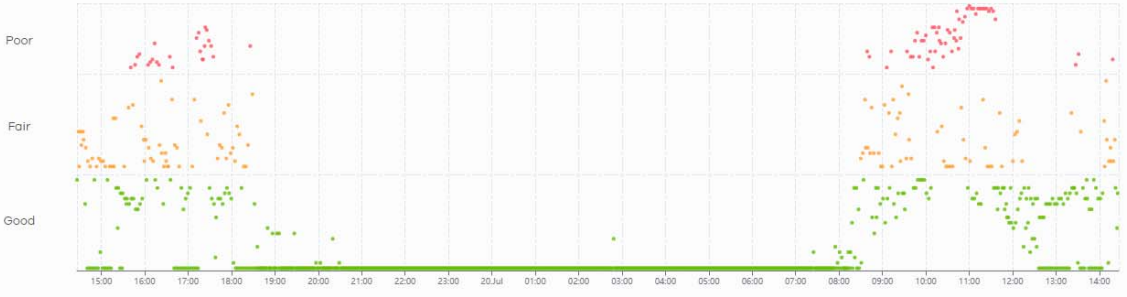
 2  
Good
 

 0  
Fair
 

 0  
Poor

---

Last 24 hours Last 7 days Last 30 days  ▾




---

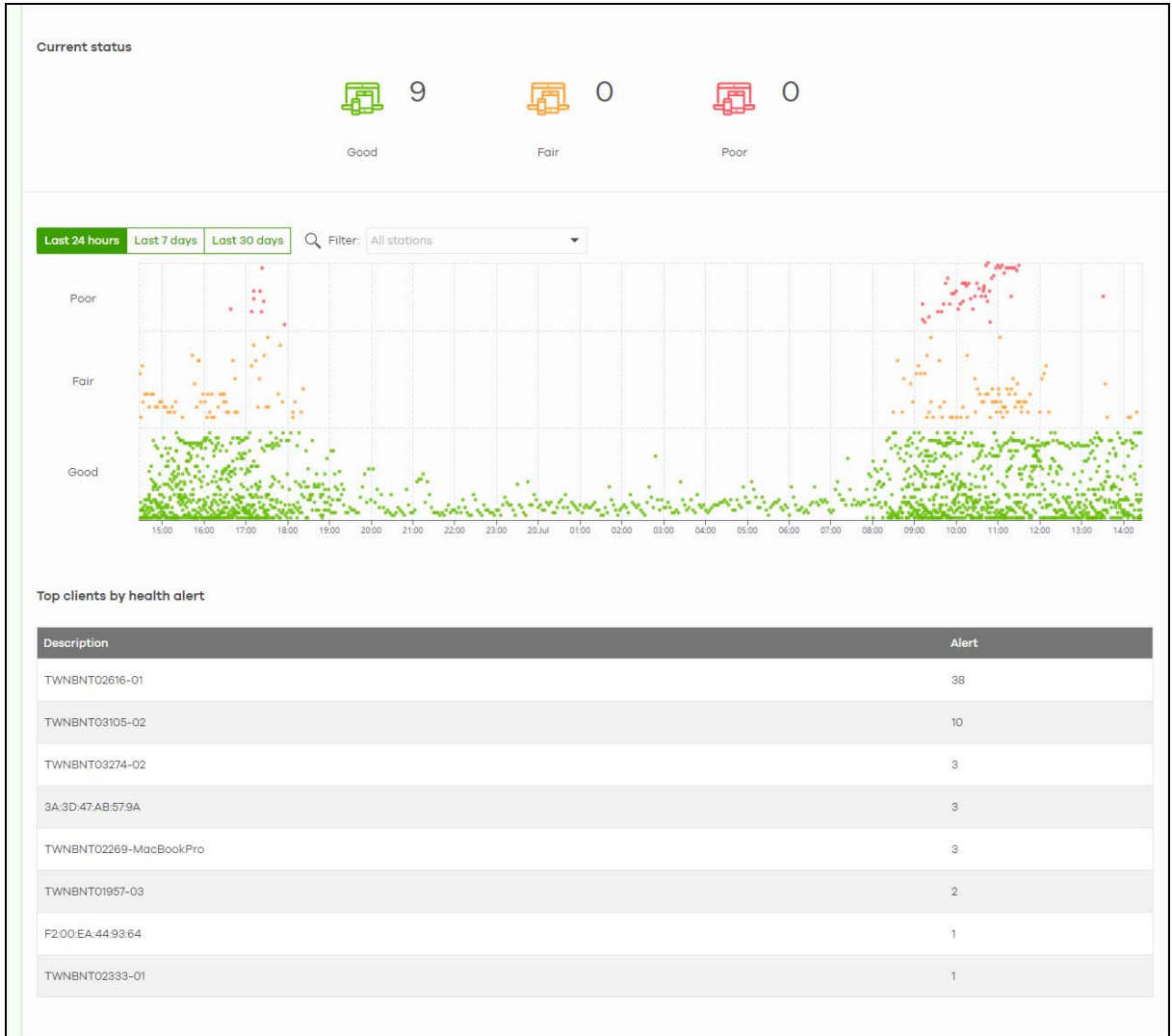
Top APs by health alert

Name	Model	Alert
marketing	WAX510D	65
Shawn seat	WAX510D	13

---

Clients wireless health overview

6 GHz 5 GHz 2.4 GHz All



The following table describes the labels in this screen.

Table 186 Access Point > Monitor > Wireless Health

LABEL	DESCRIPTION
Auto optimization action	
6G radio	<p>Select <b>ON</b> to enable and specify how the Nebula Device improves the WiFi network performance. Otherwise, select <b>OFF</b> to disable it.</p> <ul style="list-style-type: none"> <li>• <b>Adaptive channel width</b> – 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).</li> <li>• <b>DCS (Dynamic Channel Selection)</b> – select this option to have the Nebula Device scan and choose a radio channel that has least interference.</li> </ul>

Table 186 Access Point &gt; Monitor &gt; Wireless Health (continued)

LABEL	DESCRIPTION
5G radio	<p>Select <b>ON</b> to enable and specify how the Nebula Device improves the WiFi network performance. Otherwise, select <b>OFF</b> to disable it.</p> <ul style="list-style-type: none"> <li>• <b>Adaptive channel width</b> – 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).</li> <li>• <b>DCS (Dynamic Channel Selection)</b> – select this option to have the Nebula Device scan and choose a radio channel that has least interference.</li> </ul>
2.4G radio	<p>Select <b>ON</b> to enable and specify how the Nebula Device improves the WiFi network performance. Otherwise, select <b>OFF</b> to disable it.</p> <ul style="list-style-type: none"> <li>• <b>DCS (Dynamic Channel Selection)</b> – select this option to have the Nebula Device scan and choose a radio channel that has least interference.</li> </ul>
Client	<p>Select <b>ON</b> 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 <b>OFF</b> to disable steering.</p>
Optimization aggressiveness	<p><b>High, Standard and Low</b> 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.</p> <p>Select a suitable traffic rate threshold level for your network.</p> <p><b>High:</b> Select this if you want the Nebula Device to postpone the action set when the access point network traffic is heavy.</p> <p><b>Standard:</b> Select this if you want the Nebula Device to postpone the action set when the access point network traffic is medium.</p> <p><b>Low:</b> Select this if you want the Nebula Device to postpone the action set when the access point network traffic is low.</p>
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 <b>Good, Fair</b> or <b>Poor</b> 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	<p>This shows how many times the Nebula Device is in a poor state of wireless health.</p> <p>The NCC generates a log when the Nebula Device is in poor wireless health. You can view the log messages in the <b>Access Point &gt; Monitor &gt; Event Log</b> screen.</p>
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 <b>Good, Fair</b> or <b>Poor</b> wireless health threshold as detected by Nebula.
Client health	<p>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.</p> <p>You can select to view the health report for the past day, week or month, as well as filter the WiFi station to view.</p>
y-axis	The y-axis represents the state of wireless health.

Table 186 Access Point &gt; Monitor &gt; Wireless Health (continued)

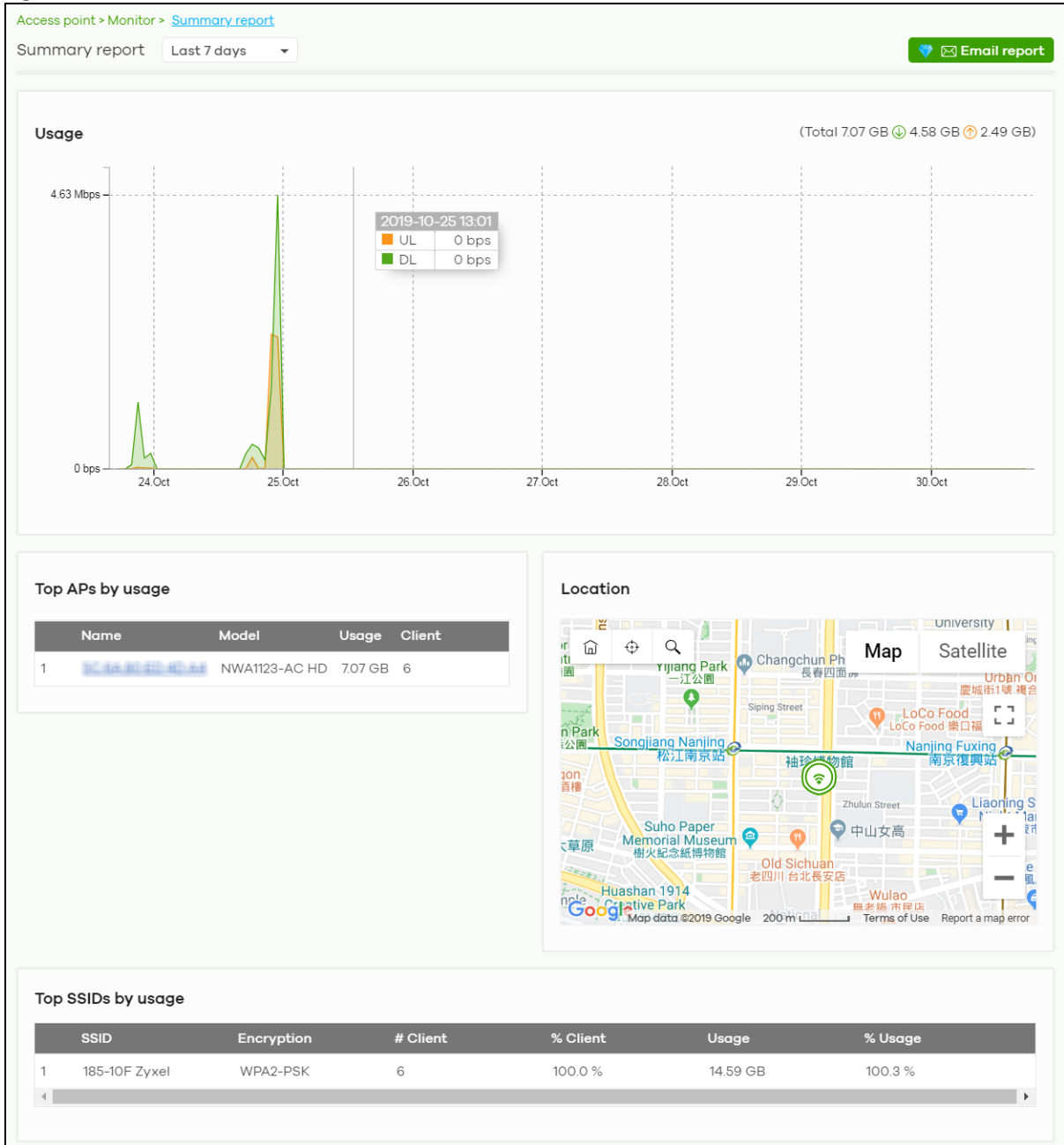
LABEL	DESCRIPTION
x-axis	The x-axis shows the time period over which the client health state is recorded.
Top clients by health alert	
Description	This shows the descriptive name of the client.
Alert	This shows how many times the client is in a poor state of wireless health.  The NCC generates a log when the client is in poor wireless health. You can view the log messages in the <b>Access Point &gt; Monitor &gt; Event Log</b> screen.

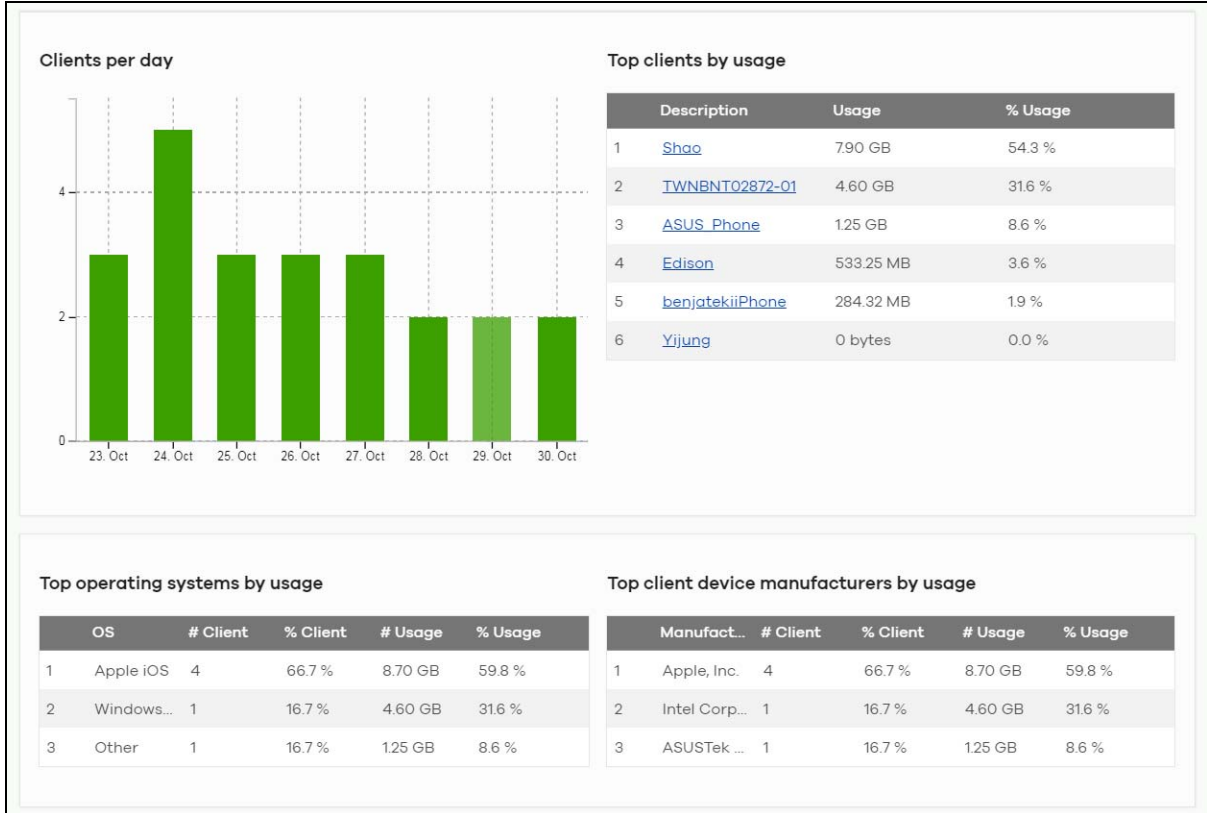
## 12.2.5 Summary Report

This screen displays network statistics for Nebula Devices of the selected site, such as bandwidth usage, top clients and/or top SSIDs.

Click **Access Point > Monitor > Summary Report** to access this screen.

Figure 219 Access Point > Monitor > Summary Report





The following table describes the labels in this screen.

Table 187 Access Point > Monitor > Summary Report

LABEL	DESCRIPTION
Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p> <input checked="" type="radio"/> Last 24 hours  <input type="radio"/> Last 7 days  <input type="radio"/> Last 30 days  <input type="radio"/> Custom range ...                 </p> <p>Report size: <input type="text" value="10"/> results per table <input type="button" value="Update"/></p> </div>
Email report	Click this button to send summary reports by email, change the report logo and set email schedules.
<b>Usage</b>	
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.
<b>Top APs by usage</b>	
#	This shows the ranking of the Nebula Device.
Name	This shows the descriptive name of the Nebula Device.



Table 187 Access Point &gt; Monitor &gt; Summary Report (continued)

LABEL	DESCRIPTION
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 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.
% 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.

## 12.3 Configure

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

### 12.3.1 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 **Access Point > Configure > SSID settings** to access this screen.

**Figure 220** Access Point > Configure > SSID settings

Access point > Configure > SSID settings

SSID settings

Simple mode: **Beta**  [What is this?](#)

Enable simple mode to provide an instant wireless setting for service. Admin can disable this function to configure full features.

[+ Add SSID network](#) [Export](#)

No.	1	2	3
Name	e-Nebula-MAC	e-Nebula-Login	e-Nebula-purplewifi
Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Programmable SSID <b>Beta</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Name	DPPSK-\$AP(\$)		
PSK			
Tagging	Tag	Tag	Tag
Guest Network	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SSID advanced settings	<a href="#">Edit</a>	<a href="#">Edit</a>	<a href="#">Edit</a>
WLAN security	DPPSK	Open	Open
Sign-in method	Disable	Sign-on with My RADIUS server	Sign-on with My RADIUS server
Band mode	2.4 GHz 5 GHz 6 GHz	5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
VLAN ID	1	1	101
Rate limiting	Unlimited Kb/s Unlimited Kb/s	Unlimited Kb/s Unlimited Kb/s	Unlimited Kb/s Unlimited Kb/s
Captive portal customization	<a href="#">Edit</a>	<a href="#">Edit</a>	<a href="#">Edit</a>
Theme	Modern	Modern	Modern

The following table describes the labels in this screen.

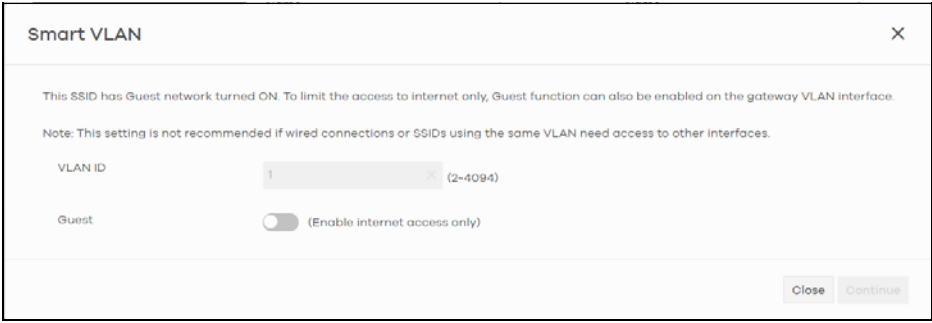
**Table 188** Access Point > Configure > SSID settings

LABEL	DESCRIPTION
Simple Mode	Select <b>On</b> to enable <b>Simple Mode</b> .  Simple Mode 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 Devices
No.	This shows the index number of this profile.
delete	Click this icon to remove the SSID profile.

Table 188 Access Point &gt; Configure &gt; SSID settings (continued)

LABEL	DESCRIPTION
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	<p>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.</p> <p>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.</p>
Name	<p><b>Name:</b> Enter a programmable SSID name in the format PREFIX+VALUE(X). This name overrides the original SSID name.</p> <ul style="list-style-type: none"> <li>• PREFIX: Optional prefix to add to the SSID, for example "FreeWiFi_". To use "\$" in the SSID name, enter "\$\$"</li> <li>• VALUE: Specify a Nebula Device value to use to generate the SSID name. Use one of the following: <ul style="list-style-type: none"> <li>\$AP = Nebula Device device name.</li> <li>\$MAC = Nebula Device MAC address.</li> <li>\$SN = Nebula Device serial number.</li> </ul> </li> <li>• 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.</li> </ul> <p>Example: <i>FreeWiFi_Room\$AP(-3)</i> generates an SSID called "FreeWiFi_Room" + the last three characters of the access point device name.</p>
PSK	<p><b>PSK:</b> Enter an optional programmable PSK in the format GENTYPE(Y).</p> <ul style="list-style-type: none"> <li>• GENTYPE: Specify how the Nebula Device will generate a random PSK. <ul style="list-style-type: none"> <li>\$GENMIX = The Nebula Device generates a mix of random letters and numbers.</li> <li>\$GENNUM = The Nebula Device generates a mix of random numbers only.</li> <li>\$AP = Nebula Device device name.</li> <li>\$MAC = Nebula Device MAC address.</li> <li>\$SN = Nebula Device serial number.</li> <li>Y = Specify the length of the PSD. The minimum length is 8.</li> </ul> </li> </ul> <p>Example 1: <i>\$GENNUM(10)</i> generates a unique 10-character PSK for this SSID, consisting only of numbers.</p> <p>Example 2: <i>\$MAC(-5)\$SN(-5)</i> uses the MAC address's last 5 characters and the serial number's last 5 characters (for example, 8E3AE02451).</p> <p>Example 3: <i>ZYXEL-\$GENMIX(4)</i> appends the fixed characters 'ZYXEL' and generates a unique 4-character mix of random letters and numbers (for example, ZYXEL-3c4d).</p> <p>Note: You can specify a fixed PSK for this SSID at <b>Access point &gt; Configure &gt; SSID advanced settings</b>.</p>
Tagging	<p>Enter or select the tags you created for Nebula Devices in the <b>Access Point &gt; Monitor &gt; Access Points</b> screen. The SSID profile will only be applied to Nebula Devices with the specified tag.</p> <p>If you leave this field blank, this SSID profile will be applied to all Nebula Devices in the site.</p>

Table 188 Access Point &gt; Configure &gt; SSID settings (continued)

LABEL	DESCRIPTION
Guest Network	<p>Select <b>On</b> 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.</p> <p>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 <a href="#">Section 12.3.2 on page 540</a>.</p> <p>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, <b>Smart Guest/VLAN network tip, click here</b>, displays after you select <b>On</b>. Click <b>here</b> to open a screen where you can directly select to use the interface as a Guest interface.</p> 
SSID advanced settings	
Edit	Click this button to go to the <b>Authentication</b> screen and configure the advanced settings, such as SSID availability, WiFi security, L2 isolation, intra-BSS traffic blocking and walled garden settings. See <a href="#">Section 12.3.2 on page 540</a> .
WLAN security	This shows the encryption method used in this profile.
Sign-in method	This shows the authentication method used in this profile.
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 <b>Captive Portal</b> screen and configure the captive portal settings. See <a href="#">Section 12.3.3 on page 549</a> .
Theme	If captive portal is enabled, this shows the name of the captive portal page used in this profile.

## 12.3.2 SSID Advanced Settings

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

Click **Access Point > Configure > SSID advanced settings** to access this screen.

Figure 221 Access Point &gt; Configure &gt; SSID advanced settings Part 1

Access point > Configure > [SSID advanced settings](#)

SSID advanced settings

SSID:

---

**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 ⓘ [Model list](#)

MAC-based Authentication with Nebula cloud authentication ⓘ [Model list](#)  
Use MAC address as a username and password

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

Sign-in method

Disabled  
Users can access the network without any web authentication

Click-to-continue  
Users must view and agree the captive portal page in order to access the network

Voucher  
Users must enter a voucher code in order to access the network  
Create and manage voucher passcode on the [Vouchers](#) page.

Sign-on with 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:

[What do I enter here?](#)

Self-registration:

Simultaneous login limit:  ⓘ [Model list](#)

Strict Policy:

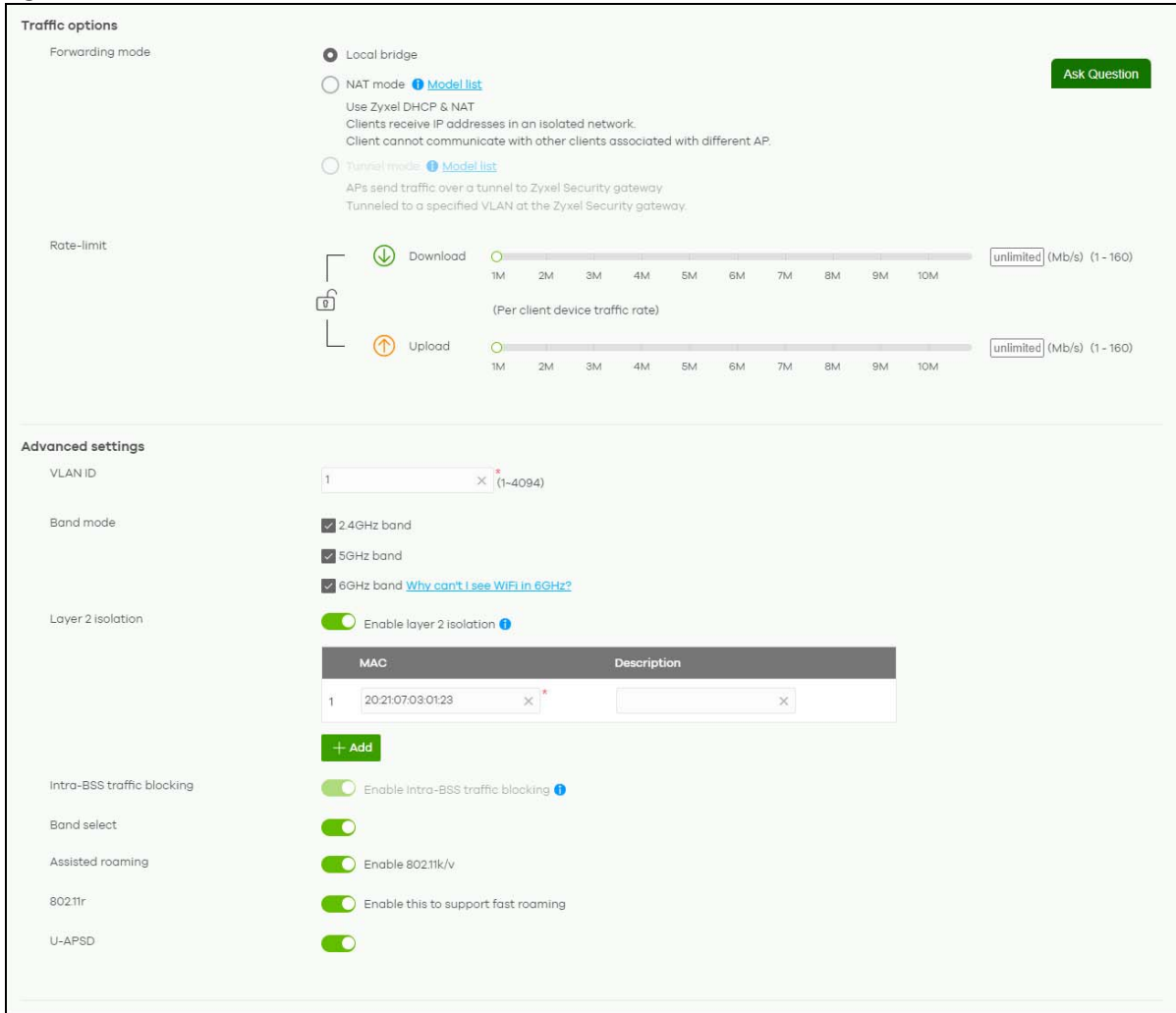
Reauth time:

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 222 Access Point > Configure > SSID advanced settings Part 2



The following table describes the labels in this screen.

Table 189 Access Point > Configure > 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 <a href="#">Section 6.3.5 on page 216</a> .

Table 189 Access Point &gt; Configure &gt; SSID advanced settings (continued)

LABEL	DESCRIPTION
Security options	<p>Select <b>Open</b> to allow any client to associate this network without any data encryption or authentication.</p> <p>Select <b>Enhanced-open</b> to allow any client to associate this network without any password but with improved data encryption.</p> <p>Upon selecting <b>Enhanced-open</b> or <b>WPA Personal With WPA3, transition mode</b> generates two VAP so devices that do not support <b>Enhanced-Open/WPA Personal With WPA3</b> can connect using <b>Open/WPA Personal With WPA2</b> network. This is always <b>on</b> at the time of writing.</p> <p>Select <b>WPA Personal With (WPA1/WPA2/WPA3)</b> and enter a pre-shared key from 8 to 64 case-sensitive keyboard characters to enable WPA1/2/3-PSK data encryption. Upon selecting <b>WPA Personal With WPA3</b>, Nebula Devices that do not support it will revert to WPA2.</p> <ul style="list-style-type: none"> <li>• Turn on <b>802.11r</b> 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.</li> </ul> <p>Click <b>Print</b> to display the QR code that includes the password for quick access. You can save the QR code as PDF.</p> <p>Select <b>Dynamic personal psk</b> 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.</p> <p>After enabling this option, you must create one or more DPPSK users in the site or organization at <b>Configure &gt; Cloud authentication &gt; Account Type &gt; DPPSK</b>.</p> <ul style="list-style-type: none"> <li>• For details on creating a site DPPSK user, see <a href="#">Section 6.3.5.3 on page 218</a>.</li> <li>• For details on creating organization DPPSK users, see <a href="#">Section 7.2.7 on page 296</a>.</li> </ul> <p>Turn on <b>MAC-based Authentication with</b> to authenticate WiFi clients by their MAC addresses together with <b>My RADIUS server</b> to use an external RADIUS server. Or select <b>Nebula cloud authentication</b> to use the NCC for MAC authentication.</p> <p>Select <b>WPA-Enterprise with</b> to enable 802.1X secure authentication. You can select <b>My RADIUS server</b> to use an external RADIUS server or select <b>Nebula cloud authentication</b> to use the NCC for 802.1X authentication.</p> <ul style="list-style-type: none"> <li>• Turn on <b>802.11r</b> 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.</li> <li>• Select <b>Two-Factor Authentication</b> 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 <b>Enable on RAP only</b> to only require Two-Factor Authentication when accessing the network through a remote access point (RAP).</li> </ul>

Table 189 Access Point &gt; Configure &gt; SSID advanced settings (continued)

LABEL	DESCRIPTION
Sign-in method	<p>Select <b>Disabled</b> to turn off web authentication.</p> <p>Select <b>Click-to-continue</b> to block network traffic until a client agrees to the policy of user agreement.</p> <p>Note: After enabling <b>Click-to-continue</b>, 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.</p> <p>Select <b>Voucher</b> to require that a user logs in with a voucher code. For details on vouchers, see <a href="#">Section 7.1.8 on page 267</a>.</p> <p>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.</p> <p>Select <b>Sign-on with</b> and:</p> <ul style="list-style-type: none"> <li>select <b>Nebula cloud authentication</b> to block network traffic until a client authenticates with the NCC through the specifically designated web portal page.</li> <li>select <b>My RADIUS server</b> to block network traffic until a client authenticates with an external RADIUS server through the specifically designated web portal page. Enable <b>MAC authentication fallback</b> when both RADIUS-based MAC authentication and web authentication are implemented.</li> </ul> <p><b>Scenario 1:</b> 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.</p> <p><b>Scenario 2:</b> When MAC authentication is successful. A WiFi client tries to connect to the WiFi network and passes MAC authentication. Web authentication is then skipped.</p> <p>Note: When <b>MAC authentication fallback</b> is enabled, the WiFi client can avoid network disassociations due to MAC authentication failure.</p> <ul style="list-style-type: none"> <li>select <b>Facebook</b> to block network traffic until a client authenticates with the NCC using Facebook Login.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>select <b>Facebook Wi-Fi</b> 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.</li> </ul> <p>Click <b>here</b> 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.</p>



Table 189 Access Point &gt; Configure &gt; SSID advanced settings (continued)

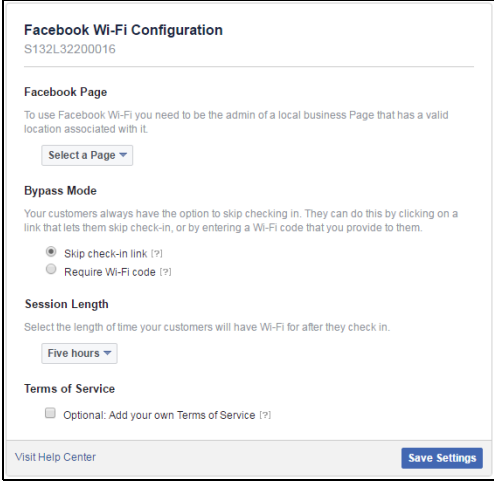
LABEL	DESCRIPTION
Sign-in method (continued)	 <p>Note: When the NCC license of the organization expires, the SSID configured with Facebook WiFi will be disabled automatically. To enable the SSID again, change its authentication method or register with a new license key.</p>
RADIUS server	<p>This field is available only when you select to use the following:</p> <ul style="list-style-type: none"> <li>• <b>MAC-based Authentication with My RADIUS server</b> or <b>WPA2-Enterprise with My RADIUS server</b> in the <b>WLAN security</b> field, or</li> <li>• when you select <b>Sign-on with My RADIUS server</b> in the <b>Sign-in method</b> field.</li> </ul> <p>Click <b>Add</b> to specify the IP address/domain name, port number, and shared secret password of the RADIUS server to be used for authentication.</p> <p>Note: User must enter the <b>Account Format</b> and <b>Calling Station ID</b> when <b>MAC authentication fallback</b> field is enabled.</p> <p>Note: Nebula Devices with firmware version 5.50 or older will turn OFF this SSID when the <b>Host</b> field is configured with a domain name.</p>
NAS Identifier	<p>If the RADIUS server requires the Nebula Device to provide the Network Access Server identifier attribute with a specific value, enter it here.</p>
RADIUS accounting	<p>This field is available only when you select to use <b>WPA2-Enterprise with My RADIUS server</b> in the <b>WLAN security</b> field, or when you select <b>Sign-on with My RADIUS server</b> in the <b>Sign-in method</b> field.</p> <p>Select <b>RADIUS accounting enabled</b> to enable user accounting through an external RADIUS server.</p> <p>Select <b>RADIUS accounting disabled</b> to disable user accounting through an external RADIUS server.</p>
RADIUS accounting servers	<p>If you select <b>RADIUS accounting enabled</b>, click <b>Add</b> to specify the IP address, port number and shared secret password of the RADIUS server to be used for accounting.</p>
Captive portal advance setting	
Walled garden	<p>Select <b>On</b> to enable Walled garden.</p>

Table 189 Access Point &gt; Configure &gt; SSID advanced settings (continued)

LABEL	DESCRIPTION
Walled garden ranges	<p>This field is not configurable if you set <b>Sign-in method</b> to <b>Disable</b>. 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.</p> <p>Select to turn on or off the walled garden feature.</p> <p>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.</p>
Self-registration	<p>This field is available only when you set <b>Sign-in method</b> to <b>Sign-on with Nebula Cloud authentication</b>.</p> <p>Select <b>Allow users to create accounts with auto authorized</b> or <b>Allow users to create accounts with manual authorized</b> 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 <b>Allow users to create accounts with manual authorized</b>, users cannot log in with the account until the account is authorized and granted access. For <b>Allow users to create accounts with auto authorized</b>, users can just use the registered account to log in without administrator approval.</p> <p>Select <b>Don't allow users to create accounts</b> to not display a link for account creation in the captive portal login page.</p>
Simultaneous login limit	<p>This field is available only when you set <b>Sign-in method</b> to <b>Sign-on with My RADIUS server</b> or <b>Sign-on with Nebula Cloud authentication</b>.</p> <p>Select <b>Unlimited</b> if you allow users to log in as many times as they want as long as they use different IP addresses.</p> <p>Select <b>1 to 10</b> if you do NOT allow users to have simultaneous logins.</p>
Strict Policy	<p>Select <b>Allow HTTPS traffic without sign-on</b> to let users use HTTPS to access a web site without authentication.</p> <p>Select <b>Block all access until sign-on</b> 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.</p>
Reauth time	<p>Select <b>Follow site-wide setting</b> or select a specific time the user can be logged in through the captive portal in one session before having to log in again.</p>
NCAS disconnect behavior	<p>This field is available only when:</p> <ul style="list-style-type: none"> <li>• you set <b>Sign-in method</b> to <b>Sign-on with Nebula Cloud authentication</b></li> <li>• you enable <b>MAC-based Authentication with</b> and you select <b>Nebula cloud authentication</b></li> </ul> <p>Select <b>Allowed</b> to allow any users to access the network without authentication when the NCAS (Nebula Cloud Authentication Server) is not reachable.</p> <p>Select <b>Limited</b> to allow only the currently connected users or the users in the white list to access the network.</p>
Traffic options	

Table 189 Access Point &gt; Configure &gt; SSID advanced settings (continued)

LABEL	DESCRIPTION
Forwarding mode	<p>Select <b>Local bridge</b> 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.</p> <p>Select <b>NAT mode</b> 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.</p> <p>The following Nebula Device features do not work when <b>NAT mode</b> is enabled:</p> <ul style="list-style-type: none"> <li>• 802.11r</li> <li>• Layer2 isolation</li> <li>• Dynamic VLAN (cloud authentication, RADIUS server)</li> </ul> <p>Note: In NAT mode, clients cannot communicate with clients connected to a different Nebula Device.</p> <p>Select <b>Tunnel mode</b> 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 <b>Security gateway &gt; Configure &gt; Interface addressing</b>.</p> <p>Note: Tunnel mode is available for Nebula Device (Security Firewall device) only. In Tunnel mode, make sure the ICMP protocol is enabled. See <b>Firewall &gt; Configure &gt; Routing: Policy Routes/Traffic Shaping</b> and <b>Firewall &gt; Configure &gt; Security Policy: Action</b> for information.</p> <p>Select <b>Tunnel mode</b> for clients that want to access the network behind the Nebula Device. Select <b>Local bridge</b> for clients that want to access the Internet, but you do not want them to access the network behind the Nebula Device.</p>
Rate-limit	<p>Set the maximum data download and upload rates in Kbps, on a per-station basis.</p> <p>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.</p>
Advanced settings	

Table 189 Access Point &gt; Configure &gt; SSID advanced settings (continued)

LABEL	DESCRIPTION
VLAN ID	<p>Enter the ID number of the VLAN to which the SSID belongs.</p> <p>Note: If you have a Nebula Security Appliance installed in the site but did not configure an identical VLAN interface on the gateway, <b>Smart Guest/VLAN network tip, click here</b>. displays. Click <b>here</b> to open a screen where you can create a gateway interface with the specified VLAN ID.</p> <div data-bbox="537 478 1459 940" style="border: 1px solid black; padding: 10px;"> <p><b>Smart VLAN</b> <span style="float: right;">✕</span></p> <p>Nebula detected that VLAN1000 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.</p> <p>VLAN ID: <input type="text" value="1000"/> (1-4094)</p> <p>IP address: <input type="text" value=""/> ✕</p> <p>Subnet mask: <input type="text" value=""/> ✕</p> <p>Port group: <input type="text" value="Port Group 1"/> ▾</p> <p>DHCP: <input type="text" value="None"/> ▾</p> <p>Guest: <input checked="" type="checkbox"/> (Enable internet access only)</p> <p style="text-align: right;">Close <input type="button" value="Continue"/></p> </div> <p>Note: If you select <b>Tunnel mode</b> in <b>Forwarding mode</b>, the <b>Tunnel to gateway interface</b> field appears. Select <b>LAN1</b> as the default.</p>
Band mode	Select to have the SSID use either <b>2.4GHz band</b> , <b>5GHz band</b> , or <b>6GHz band</b> only.
Layer 2 isolation	<p>This field is not configurable if you select NAT mode.</p> <p>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.</p> <p>Click <b>Add</b> 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.</p>
Intra-BSS traffic blocking	Select <b>on</b> to prevent crossover traffic from within the same SSID. Select <b>off</b> to allow intra-BSS traffic.
Band select	<p>Select to enable band steering. When enabled, the Nebula Device steers WiFi clients to the 5 GHz band.</p> <p>Note: Band mode must be set to Concurrent operation (2.4 GHz and 5 GHz).</p>
Assisted roaming	<p>Select to turn on or off IEEE 802.11k/v assisted roaming on the Nebula Device.</p> <p>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.</p>
802.11r	<p>Select to turn on or off IEEE 802.11r fast roaming on the Nebula Device.</p> <p>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.</p>
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.

### 12.3.3 Captive Portal Customization

Use this screen to configure captive portal settings for SSID profiles. A captive portal intercepts network traffic until the user authenticates his or her connection, usually through a specifically designated login web page.

Click **Access Point > Configure > Captive portal customization** to access this screen.

**Figure 223** Access Point > Configure > Captive portal customization

The screenshot shows the 'Captive portal customization' configuration page. At the top, the breadcrumb 'Access point > Configure > Captive portal customization' is visible. The main heading is 'Captive portal customization'. Below this, the 'SSID' is set to 'RAP\_Field\_Trial\_Stress (Disabled)', and a note states 'Captive portal on this SSID is disabled. You can change this setting [here](#).' The 'Themes' section displays a preview of a captive portal theme with a blue 'BUTTON' and options for 'Default' and 'Modern'. The 'Click-to-continue/Voucher/Sign-on page' section includes a 'Logo' field with a 'No logo' placeholder and an 'Upload a logo' link, a 'Message' text area, and a 'Success page' section with a 'Message' field containing the text 'Success!'. The 'External captive portal URL' section has a 'Use URL:' toggle (currently off) and a 'URL:' text field. Below this, a note says 'To use custom captive portal page, please download the zip file and edit them.' and a link to 'Download the customized captive portal page example.' The 'Captive portal behavior' section asks 'After the captive portal page where the user should go?' and offers two options: 'Stay on Captive portal authenticated successfully page' (selected) and 'To promotion URL:' with an associated text field.

The following table describes the labels in this screen.

Table 190 Access Point > Configure > Captive portal customization

LABEL	DESCRIPTION
SSID	Select the SSID profile to which the settings you configure here is applied.
Themes	<p>This section is not configurable when <b>External captive portal URL</b> is set to <b>ON</b>.</p> <ul style="list-style-type: none"> <li>• Click the <b>Preview</b> icon at the upper right of a theme image to display the portal page in a new frame.</li> <li>• Click the <b>Copy</b> icon to create a new custom theme (login page).</li> <li>• Click the <b>Edit</b> icon of a custom theme to go to a screen where you can view and configure the details of the custom theme pages. See <a href="#">Section 12.3.3.1 on page 551</a>.</li> <li>• Click the <b>Remove</b> icon to delete a custom theme page.</li> </ul> <p>Select the theme you want to use on the specified SSID.</p>
<p>Click-to-continue/Voucher/Sign-on page</p> <p>This section is not configurable when <b>External captive portal URL</b> is set to <b>ON</b>.</p>	
Logo	<p>This shows the logo image that you uploaded for the customized login page.</p> <p>Click <b>Upload a logo</b> and specify the location and file name of the logo graphic or click <b>Browse</b> to locate it. You can use the following image file formats: GIF, PNG, or JPG.</p>
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	

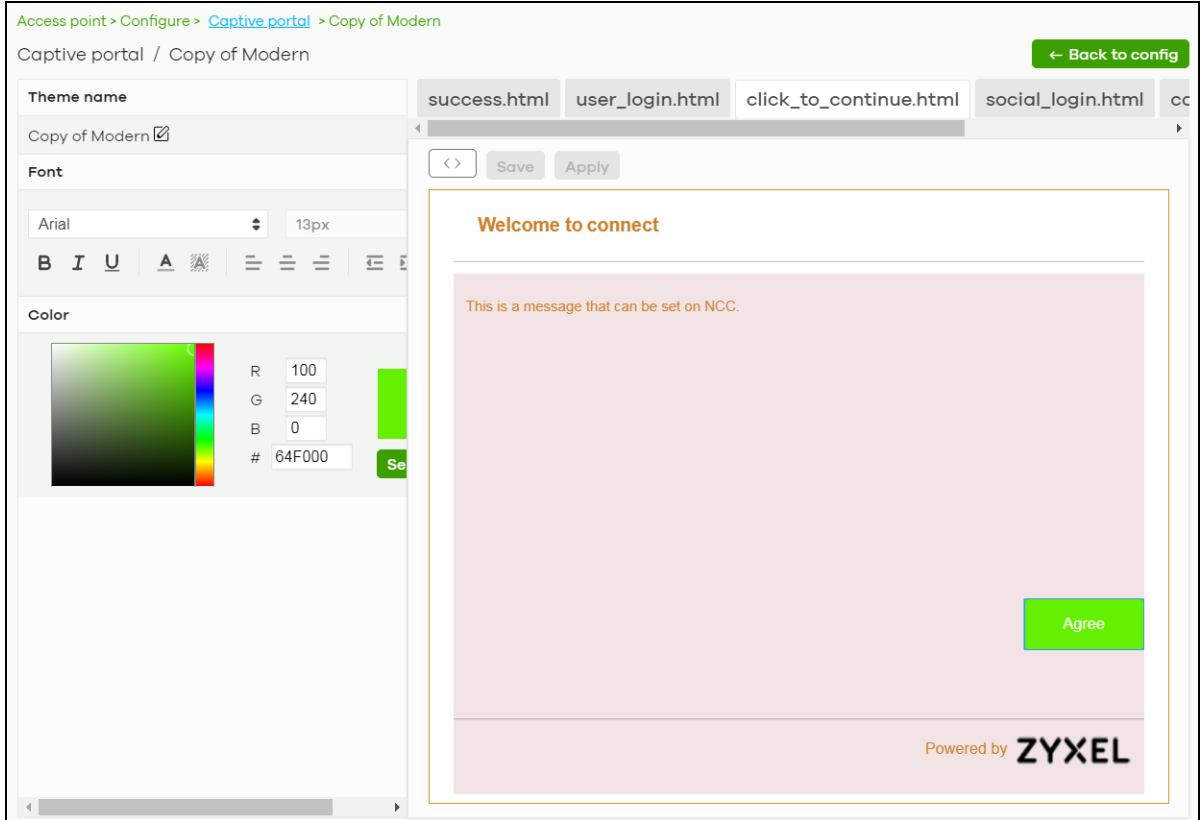
Table 190 Access Point &gt; Configure &gt; Captive portal customization (continued)

LABEL	DESCRIPTION														
Use URL	<p>Select <b>On</b> 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.</p> <p>Specify the login page's URL; for example, <code>http://IIS server IP Address/login.asp</code>. The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p> <p>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.</p> <div data-bbox="537 491 1451 1266" style="border: 1px solid black; padding: 10px;"> <p><b>Edit</b> <span style="float: right;">✕</span></p> <p>URL format:  <code>http(s)://external_html?gw_addr=http(s)://192.168.1.35&amp;apmac=aa:bb:cc:ee:ff:gg&amp;usermac=aa:11:bb:22:cc:33&amp;apip=192.168.1.35&amp;userip=192.168.1.37&amp;ssid_name=MySSID&amp;auth_path=/login.cgi&amp;apurl=http(s)://192.168.1.35</code></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Attribute Name</th> <th style="width: 70%;">Customized Name</th> </tr> </thead> <tbody> <tr> <td>gw_addr</td> <td><input type="text" value="gw_addr"/> ✕*</td> </tr> <tr> <td>apmac</td> <td><input type="text" value="apmac"/> ✕*</td> </tr> <tr> <td>usermac</td> <td><input type="text" value="usermac"/> ✕*</td> </tr> <tr> <td>apip</td> <td><input type="text" value="apip"/> ✕*</td> </tr> <tr> <td>userip</td> <td><input type="text" value="userip"/> ✕*</td> </tr> <tr> <td>ssid_name</td> <td><input type="text" value="ssid_name"/> ✕*</td> </tr> </tbody> </table> <p style="text-align: right;">Close <span style="background-color: #4CAF50; color: white; padding: 2px 5px;">OK</span></p> </div>	Attribute Name	Customized Name	gw_addr	<input type="text" value="gw_addr"/> ✕*	apmac	<input type="text" value="apmac"/> ✕*	usermac	<input type="text" value="usermac"/> ✕*	apip	<input type="text" value="apip"/> ✕*	userip	<input type="text" value="userip"/> ✕*	ssid_name	<input type="text" value="ssid_name"/> ✕*
Attribute Name	Customized Name														
gw_addr	<input type="text" value="gw_addr"/> ✕*														
apmac	<input type="text" value="apmac"/> ✕*														
usermac	<input type="text" value="usermac"/> ✕*														
apip	<input type="text" value="apip"/> ✕*														
userip	<input type="text" value="userip"/> ✕*														
ssid_name	<input type="text" value="ssid_name"/> ✕*														
Captive portal behavior															
After the captive portal page where the user should go?	Select <b>To promotion URL</b> and specify the URL of the web site or page to which the user is redirected after a successful login. Otherwise, select <b>Stay on Captive portal authenticated successfully page</b> .														

### 12.3.3.1 Custom Theme Edit

Use this screen to check what the custom portal pages look like. You can also view and modify the CSS values of the selected HTML file. Click a custom login page's **Edit** button in the **Access Point > Configure > Captive portal** screen to access this screen.

Figure 224 Access Point &gt; Configure &gt; Captive portal: Edit



The following table describes the labels in this screen.

Table 191 Access Point &gt; Configure &gt; Captive portal: Edit

LABEL	DESCRIPTION
Back to config	Click this button to return to the <b>Captive portal</b> 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 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 <b>Select</b> 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).



Table 191 Access Point &gt; Configure &gt; Captive portal: Edit (continued)

LABEL	DESCRIPTION
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.

## 12.3.4 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 **Access Point > Configure > SSID availability** to access this screen.

Figure 225 Access Point &gt; Configure &gt; SSID availability

Access point > Configure > [SSID availability](#)

SSID availability

SSID:

---

**SSID availability**

Visibility:

Tagging:

Enable SSID on APs with any of the specified tags.

---

**SSID schedule**

Enabled:

Schedule:

Schedule template:

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

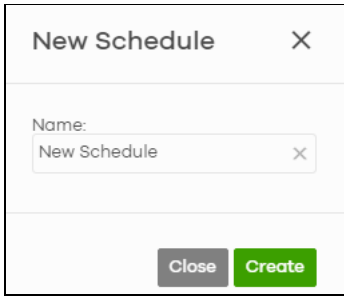
Day	Availability
Sunday	<input checked="" type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Monday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Tuesday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Wednesday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Thursday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Friday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Saturday	<input checked="" type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00

Each site can have at most 5 SSID schedules.

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

The following table describes the labels in this screen.

Table 192 Access Point > Configure > SSID availability

LABEL	DESCRIPTION
SSID	Select the SSID profile to which the settings you configure here is applied.
SSID availability	
Visibility	<p>Select <b>Hide this SSID</b> 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 <b>Broadcast this SSID</b>.</p> <p>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).</p>
Tagging	<p>Enter the tags you created for Nebula Devices in the <b>Access Point &gt; Monitor &gt; Access Points</b> screen. The SSID profile will only be applied to Nebula Devices with the specified tag.</p> <p>If you leave this field blank, this SSID profile will be applied to all Nebula Devices in the site.</p>
SSID schedule	
Enabled	Click <b>On</b> 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 <b>Custom schedule</b> and manually configure the day and time at which the SSID is enabled or disabled.
Day	This shows the day of the week.
Availability	<p>Click <b>On</b> to enable the SSID at the specified time on this day. Otherwise, select <b>Off</b> to disable the SSID on the day and at the specified time.</p> <p>Specify the hour and minute when the schedule begins and ends each day.</p>
Add	<p>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.</p> 
Delete	Click this button to remove a schedule which is not used in any SSID profile.

### 12.3.5 Radio Settings

Use this screen to configure global radio settings for all Nebula Devices in the site. Click **Access Point > Configure > Radio settings** to access this screen.

Figure 226 Access Point > Configure > Radio settings

Group: TW Test Organization: Test\_July Site: ZyNet TW

This site is bound to template: [SSID\\_Template2](#)

Access point > Configure > [Radio settings](#)  Override access point configuration

Radio settings

Country: Taiwan [The 6GHz supported country list can be found Here](#)

Deployment selection: Custom [i](#)

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
  - 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](#)

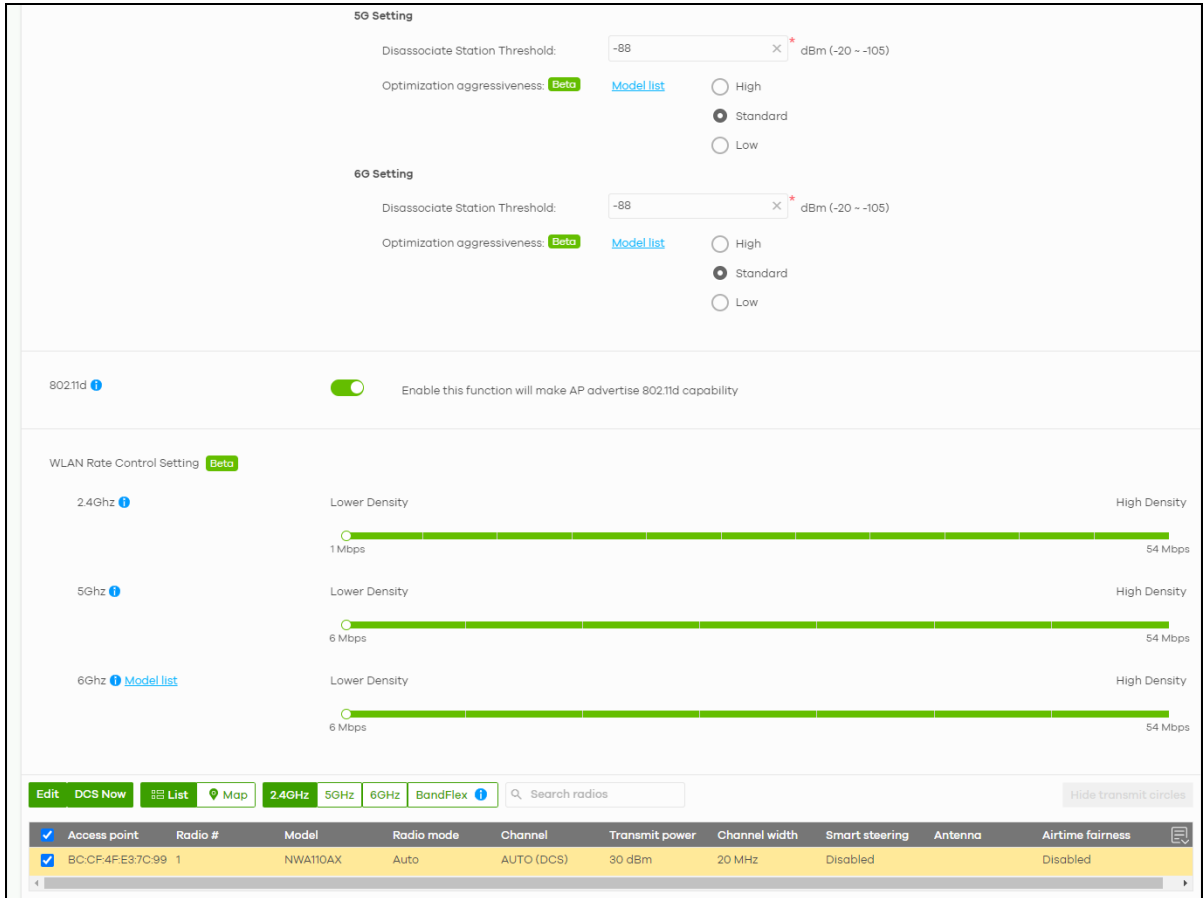
Allow 802.11ax/ac/n stations only:   
If turned ON, legacy clients including 802.11a/b/g will not be allowed to associate.

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



The following table describes the labels in this screen.

Table 193 Access Point > Configure > 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 <b>High-density (More than 10 APs)</b> for the lowest output power for 10 or more Access Points.  Select <b>Moderate-density (6-9 APs)</b> for moderate output power for 5 to 9 Access Points.  Select <b>Low-density (2-5 APs)</b> for higher concentration of output power for less than 5 Access Points.  Select <b>Single AP</b> for highest concentration of output power for a single Access Point.
Maximum output power	Selecting any of the options in the <b>Deployment selection</b> field will automatically set the maximum output power for 2.4 / 5 / 6 GHz. But you can change the setting (1 – 30 dBm).

Table 193 Access Point &gt; Configure &gt; Radio settings (continued)

LABEL	DESCRIPTION
Channel width	<p>Select the wireless channel bandwidth you want the access point to use.</p> <p>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.</p> <p>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.</p> <p>Note: It is suggested that you select <b>20 MHz</b> when there is more than one 2.4 GHz Nebula Device in the network.</p> <p>Note: It is not possible to set channel bandwidth to 160 MHz for the whole site. To configure an Nebula Device to use 160 MHz, select a supported Nebula Device in the table at the bottom of the screen, click <b>Edit</b>, and then select <b>160 MHz</b> under <b>Channel width</b>.</p>
DCS setting	
DCS time interval	<p>Select <b>ON</b> 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.</p>
DCS schedule	<p>Select <b>ON</b> 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.</p> <p>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.</p>
DCS client aware	<p>Select <b>ON</b> to have the Nebula Device wait until all connected clients have disconnected before switching channels.</p>
Avoid 5G DFS channel	<p>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.</p>
Blacklist DFS channels in the presence of radar	<p>Select <b>ON</b> 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.</p>
2.4 GHz channel deployment	<p>Select <b>Three-Channel Deployment</b> 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.</p> <p>Select <b>Four-Channel Deployment</b> 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.</p> <p>Select <b>All available channels</b> to allow channel-hopping to have the Nebula Device automatically select the best channel.</p> <p>Select <b>Manual</b> to select the individual channels the Nebula Device switches between.</p>


Table 193 Access Point &gt; Configure &gt; Radio settings (continued)

LABEL	DESCRIPTION
5 GHz channel deployment	<p>Select how you want to specify the channels the Nebula Device switches between for 5 GHz operation.</p> <p>Select <b>All available channels</b> to have the Nebula Device automatically select the best channel.</p> <p>Select <b>Manual</b> to select the individual channels the Nebula Device switches between.</p> <p>Note: The method is automatically set to <b>All available channels</b> when no channel is selected or any one of the previously selected channels is not supported.</p>
6 GHz channel deployment	<p>Select how you want to specify the channels the Nebula Device switches between for 6 GHz operation.</p> <p>Select <b>All available channels</b> to have the Nebula Device automatically select the best channel.</p> <p>Select <b>Manual</b> to select the individual channels the Nebula Device switches between.</p> <p>Note: The method is automatically set to <b>All available channels</b> when no channel is selected or any one of the previously selected channels is not supported.</p>
Allow 802.11ax/ac/n stations only	Select <b>ON</b> 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	<p>Select <b>ON</b> 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.</p> <p>Select <b>OFF</b> to disable this feature on the Nebula Device.</p>
ADVANCED OPTIONS	Click this to display a greater or lesser number of configuration fields.
2.4G/5G/6G Setting	
Disassociate Station Threshold	<p>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.</p> <p>–20 dBm is the strongest signal you can require and –105 dBm is the weakest.</p>
Optimization aggressiveness	<p><b>High, Standard and Low</b> 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.</p> <p>Select a suitable traffic rate threshold level for your network.</p> <p><b>High:</b> Select this if you want the Nebula Device to postpone the action set when the access point network traffic is heavy.</p> <p><b>Standard:</b> Select this if you want the Nebula Device to postpone the action set when the access point network traffic is medium.</p> <p><b>Low:</b> Select this if you want the Nebula Device to postpone the action set when the access point network traffic is low.</p>
802.11d	<p>Click this to enable 802.11d on the access point.</p> <p>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.</p>
WLAN Rate Control Setting	

Table 193 Access Point &gt; Configure &gt; Radio settings (continued)

LABEL	DESCRIPTION
2.4Ghz/5Ghz/ 6Ghz	<p>Sets the minimum data rate that 2.4 GHz, 5 GHz, and 6 GHz WiFi clients can connect to the Nebula Device, in Mbps.</p> <p>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.</p>
Edit	<p>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.</p> <p>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 <b>Wall</b> if you mount the Nebula Device to a wall. Select <b>Ceiling</b> if the Nebula Device is mounted on a ceiling. You can switch from <b>Wall</b> to <b>Ceiling</b> if there are still WiFi dead zones, and so on. If you select <b>Hardware Switch</b>, you use the physical antenna switch to adjust coverage and apply the same antenna orientation settings to both radios.</p> <div data-bbox="537 716 1468 1383" style="border: 1px solid black; padding: 10px;"> <p><b>Edit</b> <span style="float: right;">✕</span></p> <p>Access Point: <b>BC:CF:4F:E3:7C:99</b></p> <p>Radio #: 1</p> <p>Model: NWA110AX</p> <p>Band: 2.4 GHz</p> <p>Radio mode: 802.11ax <input checked="" type="checkbox"/></p> <p>Channel: 1 <input checked="" type="checkbox"/></p> <p>Channel width: 40 MHz <input checked="" type="checkbox"/></p> <p>Maximum output power: 29 dBm <input checked="" type="checkbox"/></p> <p>Airtime Fairness: <b>Beta</b> <input checked="" type="checkbox"/></p> <p>Smart steering: <input checked="" type="checkbox"/> <input checked="" type="checkbox"/></p> <p>Enable this function will steer the client to the better signal AP.</p> <p><b>▲ ADVANCED OPTIONS</b></p> <p>Disassociate Station Threshold: <input type="text" value="-88"/> dBm (-20 - -105)</p> <p>Optimization aggressiveness: <b>Beta</b></p> <p><input checked="" type="radio"/> High</p> <p><input type="radio"/> Standard</p> <p><input type="radio"/> Low</p> <p style="text-align: right;"><input type="button" value="Close"/> <input type="button" value="Update"/></p> </div> <p>Note: On this screen, you can set channel width to 160 MHz for the 5/6 GHz channel, if the Nebula Device supports it.</p>
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 193 Access Point &gt; Configure &gt; 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 194 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

### 12.3.6 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 **Access Point > Configure > SSID advanced settings**, which is applied on a per station basis. Use this screen to configure maximum bandwidth on the Nebula Device.

Click **Access point > Configure > Traffic shaping** to access this screen.



Figure 227 Access point &gt; Configure &gt; Traffic shaping

The following table describes the labels in this screen.

Table 195 Access point &gt; Configure &gt; Traffic shaping

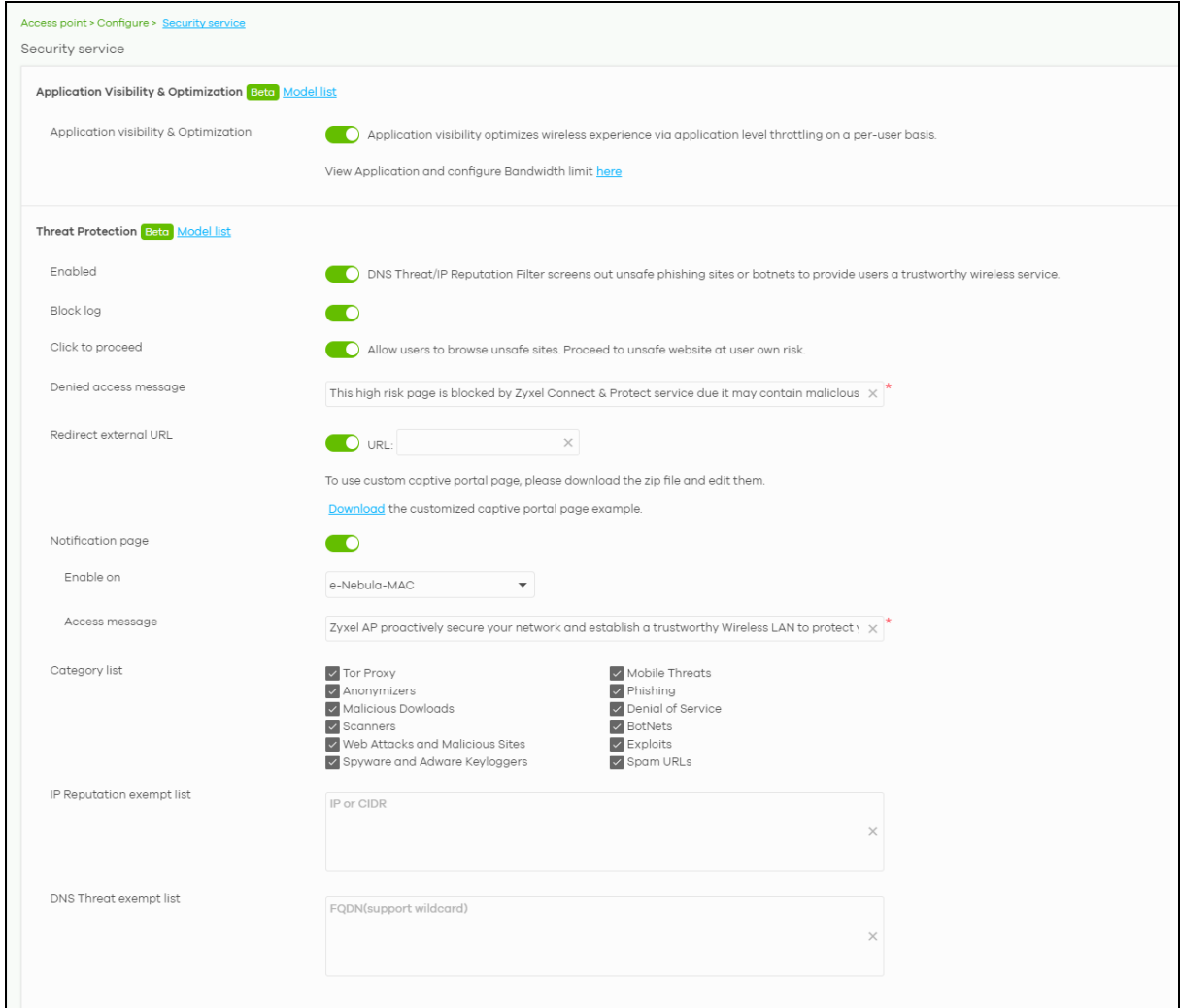
LABEL	DESCRIPTION
WLAN traffic shaping	
Rule Name	Enter the name of the traffic shaping rule. The name is used to refer to the traffic shaping rule. You may use 1 – 31 alphanumeric characters, underscores(_), or dashes (-). This value is case-sensitive.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely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

## 12.3.7 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 **Access Point > Configure > Security service** to access this screen.

Figure 228 Access Point > Configure > Security service



The following table describes the labels in this screen.

Table 196 Access Point > Configure > Security service

LABEL	DESCRIPTION
Application Visibility & Optimization	
Application visibility & Optimization	<p>Select this option to turn on application visibility and optimization. Application visibility and optimization does the following:</p> <ul style="list-style-type: none"> <li>• Detects the type of applications used by WiFi clients,</li> <li>• Throttles specific applications to save WiFi bandwidth.</li> </ul> <p>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.</p> <p>Application optimization limits the applications bandwidth usage by their categories. You can manage and view the applications and their categories in <b>Site-wide &gt; Monitor &gt; Applications &gt; Application view by Access Point.</b></p>
Threat Protection	

Table 196 Access Point &gt; Configure &gt; Security service (continued)

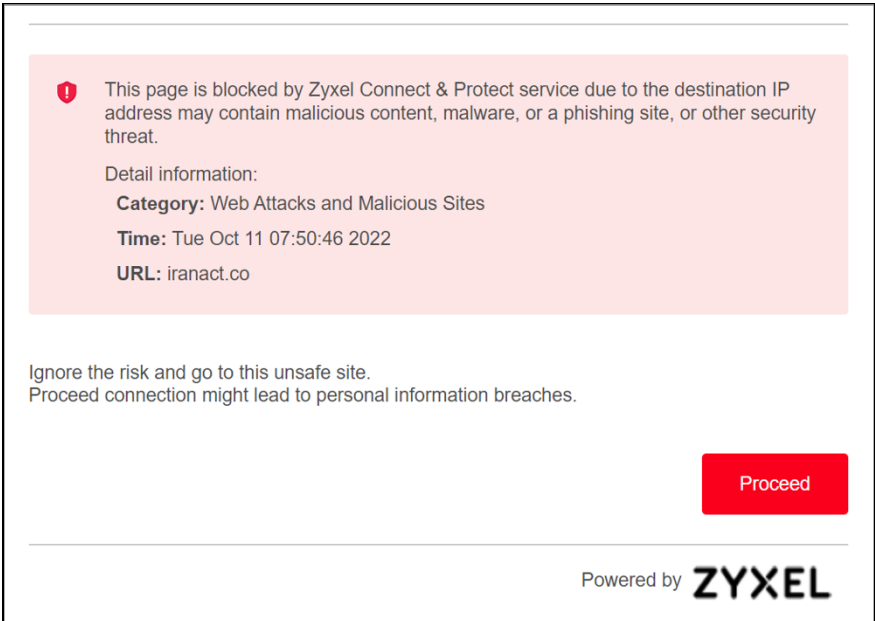
LABEL	DESCRIPTION
Enabled	<p>Select this option to allow inspection of DNS queries made by clients on your network and turn on IP blocking on the Nebula Device.</p> <p>When you enable the DNS threat service, your Nebula Device inspects the DNS queries against a database of blocked or allowed Fully Qualified 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).</p> <p>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.</p>
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	<p>Select this option to allow clients to browse unsafe websites. When enabled, the denied access message window includes the <b>Proceed</b> button. To continue, you must close and restart your web browser to visit the unsafe website.</p> <div data-bbox="534 730 1403 1346" style="border: 1px solid black; padding: 10px;">  </div>
Denied access message	<p>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;/?:@&amp;=+\$\._!~*()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator".</p> <p>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.</p>
Redirect external URL	<p>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.</p> <p>Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&amp;=+\$\._!~*()%,"). For example, http://192.168.1.17/blocked access.</p>
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 196 Access Point &gt; Configure &gt; Security service (continued)

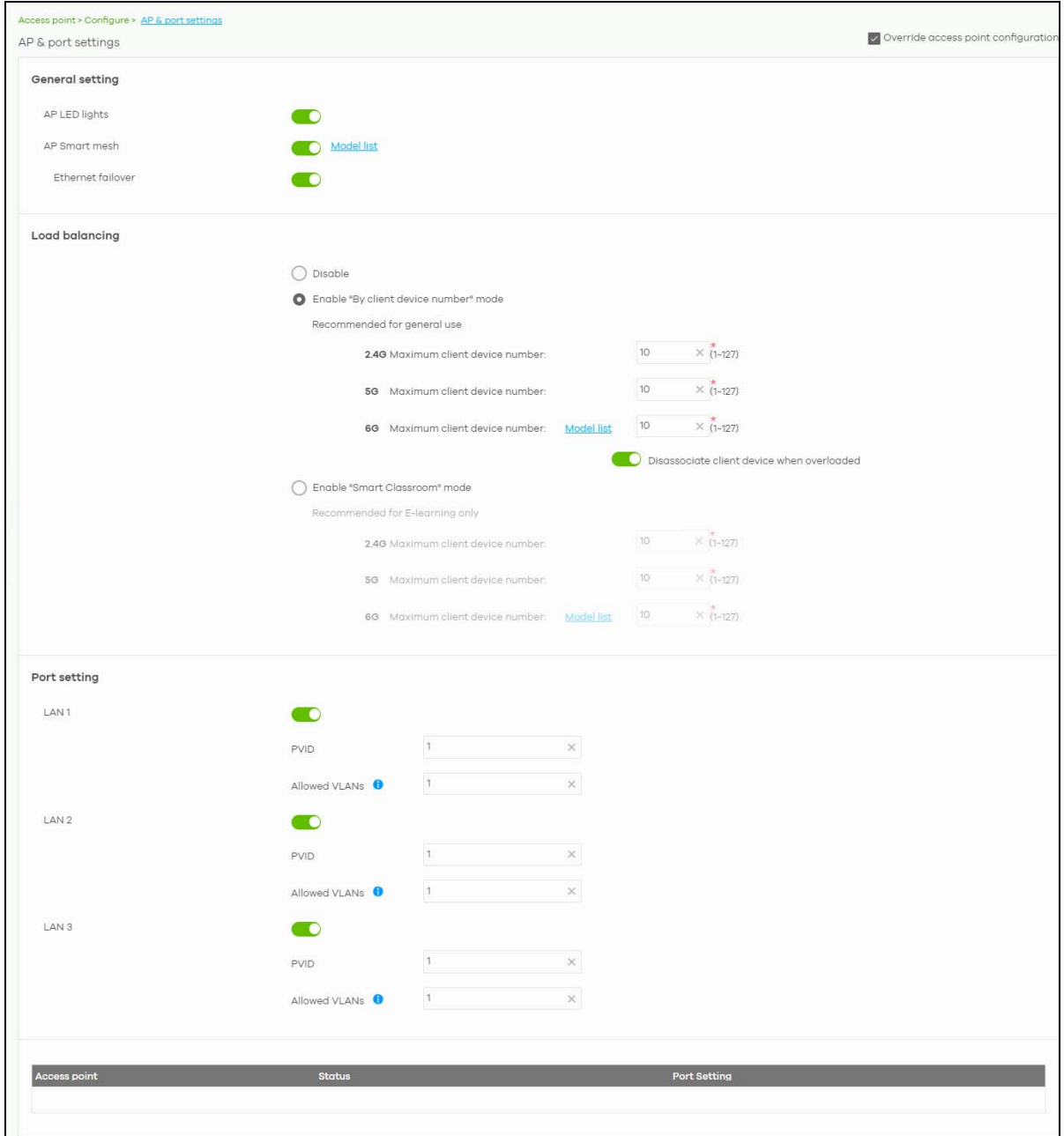
LABEL	DESCRIPTION
Category list	Select the categories of packets that come from the Internet and are known to pose a security threat to users or their computers.
IP Reputation exempt list	<p>Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.</p> <p>Add the IPv4 addresses that the Nebula Device will allow the incoming and outgoing packets.</p>
DNS Threat exempt list	<p>Domain names that you want to allow access to, regardless of their reputation, can be allowed by adding them to this list.</p> <p>Add the Fully Qualified Domain Names (FQDNs) that the Nebula Device will allow the DNS query packets.</p>

### 12.3.8 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 **Access Point > Configure > AP & port settings** to access this screen.

**Figure 229** Access Point > Configure > AP & port settings



The following table describes the labels in this screen.

**Table 197** Access Point > Configure > AP & port settings

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

Table 197 Access Point &gt; Configure &gt; AP &amp; port settings (continued)

LABEL	DESCRIPTION
AP Smart Mesh	<p>Click to enable or disable the Nebula Smart Mesh feature on all Nebula Devices in the site.</p> <p>Click <b>Model list</b> to see whether your Nebula Device supports Nebula Smart Mesh.</p> <p>Note: Nebula Smart Mesh is a WiFi mesh solution for Nebula Devices. For details, see <a href="#">Section 12.1.1 on page 510</a>.</p> <p>Note: You can override NCC settings and enable or disable Smart Mesh on individual Nebula Devices. For details, see <a href="#">Section 12.2.1.1 on page 516</a>.</p> <p>Note: Disabling Nebula Device Smart Mesh automatically disables wireless bridge on all Nebula Devices in the site. For details on wireless bridge, see <a href="#">Section 12.2.1.1 on page 516</a>.</p>
Ethernet failover	<p>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.</p> <p>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.</p> <p>Note: For details on mesh controller and mesh extender, see <a href="#">Section 12.1.1 on page 510</a>.</p>
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	<p>Select <b>ON</b> to disassociate WiFi clients connected to the Nebula Device when it becomes overloaded.</p> <p>Select <b>OFF</b> 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.</p> <p>The disassociation priority is determined automatically by the Nebula Device and is as follows:</p> <ul style="list-style-type: none"> <li>• <b>Idle Time</b> – Devices that have been idle the longest will be disassociated first. If none of the connected devices are idle, then the priority shifts to <b>Signal Strength</b>.</li> <li>• <b>Signal Strength</b> – Devices with the weakest signal strength will be disassociated first.</li> </ul>
Enable "Smart Classroom" mode	<p>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.</p> <p>The <b>Disassociate client device when overloaded</b> function is enabled by default and the disassociation priority is always Signal Strength when you select this option.</p>
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	<p>This is the name of the physical Ethernet port on the Nebula Device.</p> <p>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 <b>Edit</b> button in the table below.</p>
ON/OFF	Select <b>ON</b> to turn on the LAN port of the Nebula Device. Select <b>OFF</b> to disable the port.

Table 197 Access Point &gt; Configure &gt; AP &amp; 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.

### 12.3.8.1 Edit Port Settings

Click an entry in the **Port setting** table of the **Access Point > Configure > 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 189 on page 542](#) 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 230 Access Point > Configure > AP & port settings: Edit

### Edit

Ethernet Traffic options  
Forwarding Mode

Local bridge

NAT mode

Use Zyxel DHCP & NAT Beta [Model list](#)

Clients receive IP addresses in an isolated network.

Client cannot communicate with other clients associated with different AP.

---

#### LAN 1

Enabled

PVID

Allowed VLANs



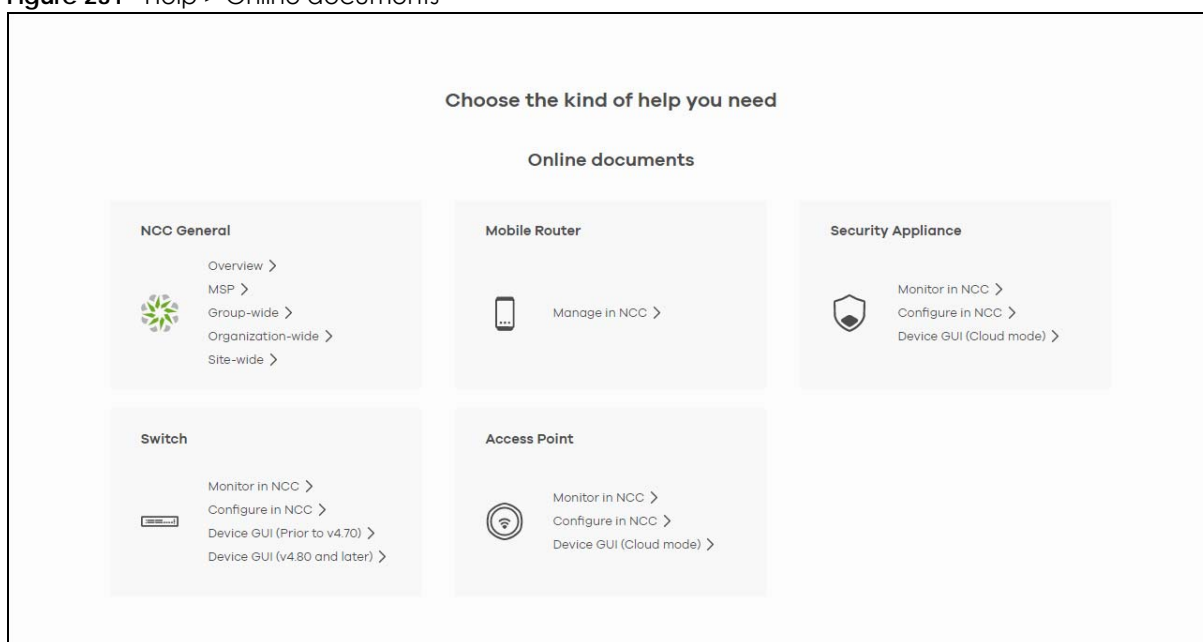
# CHAPTER 13

## Help

### 13.1 Online documents

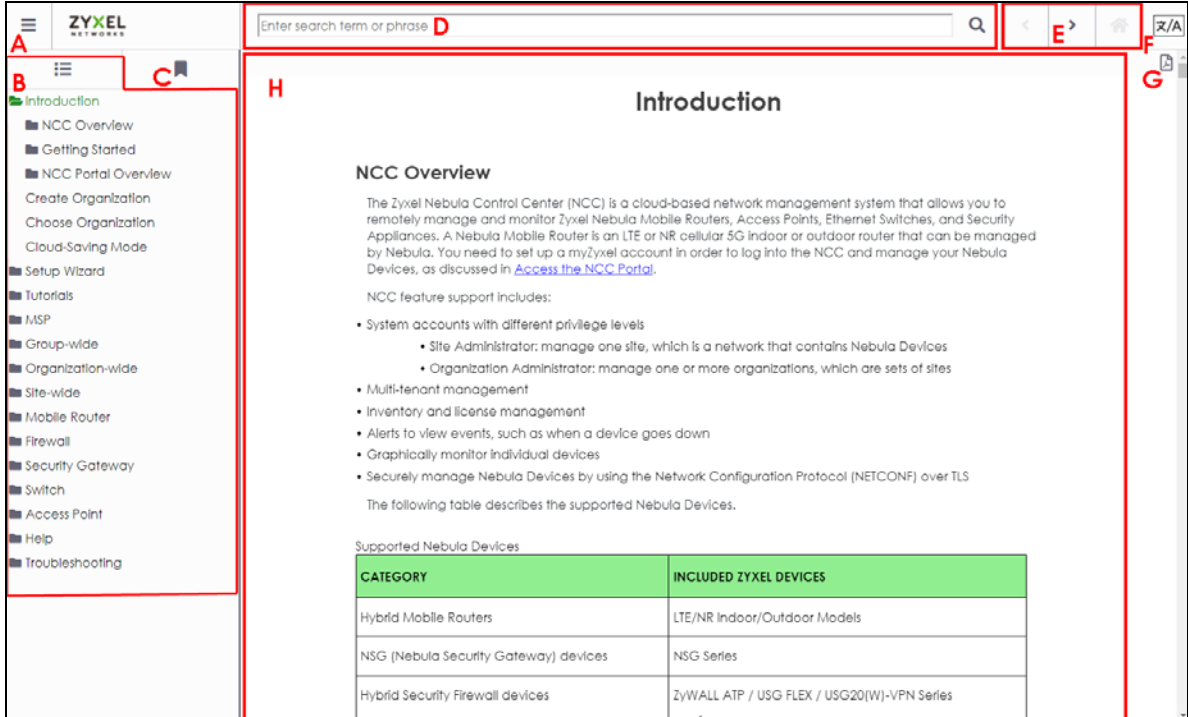
Click **Help > Online documents** to view the documentation for NCC and NCC-compatible devices. For example, to view the Security Firewall Series configuration and hardware information, locate the documents under **Security Appliance**.

**Figure 231** Help > Online documents



The following summarizes how to navigate the online document screen. The online document screen is divided into these parts:

Figure 232 Online Document Overview



- 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 198 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. <ul style="list-style-type: none"> <li>• Click the Previous button to display the previous chapter in the online document.</li> <li>• Click the Next button to display the next chapter in the online document.</li> <li>• Click the Home button to display the first chapter in the online document.</li> </ul>
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 198 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.

## 13.2 Troubleshooting Tips

To find suggestions to solve problems you might encounter with NCC and Nebula Devices, go to [Chapter 14 on page 577](#) for more information.

### 13.2.1 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.

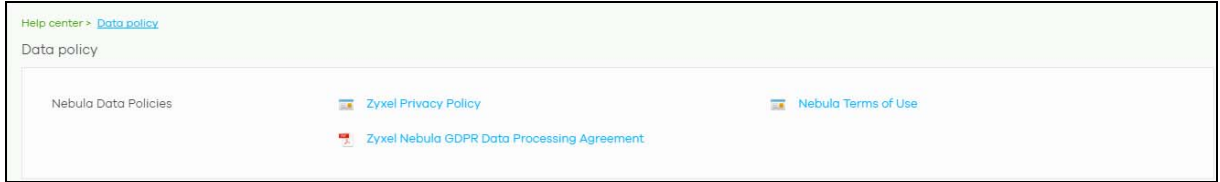
The following table shows the sample information required for firewall rules at the time of writing.

Table 199 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

### 13.2.2 Data Policy

Click **Help > Support tools > Data Policy** to view and download NCC GDPR data policy, privacy policy, and terms of use.

**Figure 233** Help > Support tools > Data Policy

## 13.3 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 234** 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								

## 13.4 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.

## 13.5 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 235** 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 assistance 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:  [Definition of priority](#)

Upload site's topology to speed up the process:

No file chosen

Total File Upload Limit 7MB!(The maximum length of a filename is 60 characters)

The following table describes the labels in this screen.

Table 200 Help > Still need help?: Support Request


LABEL	DESCRIPTION				
Zyxel Support Access  Invite Zyxel support as administrator	<p>Select <b>ON</b> 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 <b>Never</b>.</p> <p>If you select <b>ON</b>, you can click <a href="#">here</a> to change the support account's name and access right to the organization and sites.</p> <div data-bbox="496 527 1042 1192" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"><b>Update administrator</b> <span style="float: right;">✕</span></p> <hr/> <p>Name: <input type="text" value="Zyxel Support"/> ✕ *</p> <p>Email: <input type="text" value="nebula.cso@zyxel.com.tw"/> ✕</p> <p>Organization access: <input type="text" value="Read-only"/> ▼</p> <p>Activated: <input type="text" value="Yes"/> ▼</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Site</th> <th style="width: 70%;">Privilege</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">▼</td> <td style="text-align: center;"><input type="text" value="Monitor-only"/> ▼ <span style="float: right;">🗑️</span></td> </tr> </tbody> </table> <p style="text-align: center; margin-top: 5px;"><span style="background-color: #4CAF50; color: white; padding: 5px 10px; border-radius: 3px;">+ Add</span></p> <hr/> <p style="text-align: right; margin-top: 10px;"> <span style="border: 1px solid #ccc; padding: 2px 10px;">Close</span> <span style="background-color: #4CAF50; color: white; padding: 5px 15px; border-radius: 3px; margin-left: 10px;">Update admin</span> </p> </div>	Site	Privilege	▼	<input type="text" value="Monitor-only"/> ▼ <span style="float: right;">🗑️</span>
Site	Privilege				
▼	<input type="text" value="Monitor-only"/> ▼ <span style="float: right;">🗑️</span>				
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 200 Help &gt; Still need help?: Support Request (continued)

LABEL	DESCRIPTION
Priority	Select the severity level of the ticket. Click the <b>Definition of priority</b> 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 <b>New Case</b> section without saving.
Submit	Click this button to send your ticket to the Zyxel customer support.

---

# PART V

## Troubleshooting and Appendices

---



# CHAPTER 14

## 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 8.2 on page 304](#) for more information.
- To know how to monitor Security Appliances in NCC, go to [Section 9.2 on page 323](#) (Security Firewalls) or [Section 10.2 on page 398](#) (Security Gateways) for more information.
- To know how to configure Security Appliances in NCC, go to [Section 9.3 on page 335](#) (Security Firewalls) or [Section 10.3 on page 409](#) (Security Gateways) for more information.
- To know how to monitor Switches in NCC, go to [Section 11.2 on page 458](#) for more information.
- To know how to configure Switches in NCC, go to [Section 11.3 on page 482](#) for more information.
- To know how to monitor Access Points in NCC, go to [Section 12.2 on page 512](#) for more information.
- To know how to configure Access Points in NCC, go to [Section 12.3 on page 538](#) 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 50](#) 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 50](#) 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 > General 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.
  - **Firewall > Monitor > Firewall**
  - **Security gateway > Monitor > Security gateway**
  - **Access Point > Monitor > Access Point**

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 6.3.3 on page 195](#).
- Make sure that you have created an organization and site and add the Nebula Devices to the site. See [Create Organization on page 42](#) and [Section 6.3.2 on page 194](#).

---

### [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 approximately 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 **Firewall / Security gateway / Switches / Access points > Monitor > Firewall: 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 Point 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 183 on page 518](#).
- The maximum number of Remote Access Points depends on the Nebula Security Firewall.

Table 201 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 Access point > Monitor > Access points](#).

---

- Click **Reconnect** in [Access point > Monitor > 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 [Access Point > Configure > AP & port settings](#). See [Section 12.3.8 on page 564](#) for more information.

Note: For more information about smart mesh, see [Section 12.1.1 on page 510](#).

---

The mesh extender does not broadcast the mesh controller SSID.

---

- Make sure you enable **Downlink** in [Access point > Monitor > Access points: Details](#). See [Section 12.2.1.1 on page 516](#) 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.

---

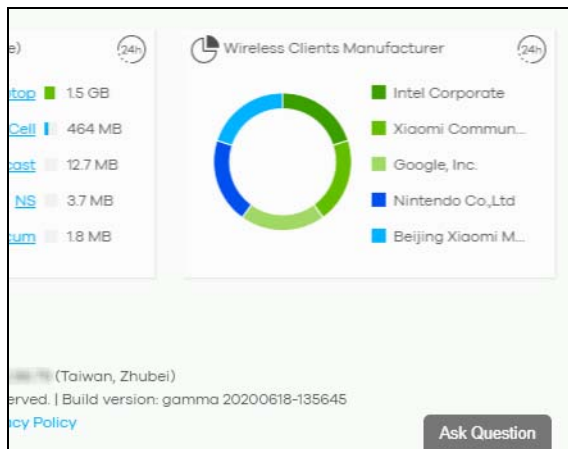
- The Nebula Device has a power-related error. Disconnect and reconnect the power cord. Make sure that you are using the included power cord for the Nebula Device and it is plugged into an appropriate power source. See the related Quick Start Guide.
- If the LED is still red, you may have a hardware problem. In this case, you should contact your local customer support.

## 14.1 Getting More Troubleshooting Help

Go to [support.zyxel.com](https://support.zyxel.com) at the Zyxel website for other technical information on the NCC.

## 14.2 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 Corporation
- <https://www.zyxel.com>

### Asia

#### China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <https://www.zyxel.com/cn/zh/>

#### India

- Zyxel Technology India Pvt Ltd.
- <https://www.zyxel.com/in/en/>

#### Kazakhstan

- Zyxel Kazakhstan
- <https://www.zyxel.kz>

## **Korea**

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

## **Malaysia**

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

## **Pakistan**

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

## **Philippines**

- Zyxel Philippines
- <http://www.zyxel.com.ph>

## **Singapore**

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

## **Taiwan**

- Zyxel Communications Corporation
- <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 BY
- <https://www.zyxel.by>

### **Bulgaria**

- Zyxel България
- <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.fr>

## Germany

- Zyxel Deutschland GmbH
- <https://www.zyxel.com/de/de/>

## Hungary

- Zyxel Hungary & SEE
- <https://www.zyxel.com/hu/hu/>

## Italy

- Zyxel Communications Ital
- <https://www.zyxel.com/it/it/>

## Netherlands

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl/>

## Norway

- Zyxel Communications
- <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>

## **Russia**

- Zyxel Russia
- <https://www.zyxel.com/ru/ru/>

## **Slovakia**

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <https://www.zyxel.com/sk/sk/>

## **Spain**

- Zyxel Communications ES Ltd.
- <https://www.zyxel.com/es/es/>

## **Sweden**

- Zyxel Communications
- <https://www.zyxel.com/se/sv/>

## **Switzerland**

- Studerus AG
- <https://www.zyxel.ch/de>
- <https://www.zyxel.ch/fr>

## **Turkey**

- Zyxel Turkey A.S.
- <https://www.zyxel.com/tr/tr/>

## **UK**

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en/>

## **Ukraine**

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

## **South America**

### **Argentina**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

## **Brazil**

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

## **Colombia**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

## **Ecuador**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

## **South America**

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

## **Middle East**

### **Israel**

- Zyxel Communications Corporation
- <http://il.zyxel.com/>

## **North America**

### **USA**

- Zyxel Communications, Inc. – North America Headquarters
- <https://www.zyxel.com/us/en/>

# APPENDIX B

## Legal Information

### Copyright

Copyright © 2023 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

### Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

### Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

### Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

### Registration

Register your product online at [www.zyxel.com](http://www.zyxel.com) to receive email notices of firmware upgrades and related information.

## Symbols

- +Hub button [182](#)
- +Org-to-Org Service [183](#)

## Numbers

- 2FA [25](#)
  - enable [104](#)
  - set up [110](#)
- 3GPP specifications [317](#)
- 802.11k neighbor lists [548](#)
- 802.11r fast roaming [543](#)
- 802.11v capable client [548](#)
- 802.1X (WPA-Enterprise) authentication [218, 298](#)
- 802.1X authentication [543](#)

## A

- access point
  - connection status [515](#)
- access point list
  - export [514](#)
- Access points screen [512](#)
- access port [487](#)
- account
  - disable [163, 186](#)
  - expire [222, 224](#)
- account list
  - export [218, 221, 224, 298, 299, 301](#)
- account status [162, 185, 214](#)
- ACL rule
  - configure [490](#)
- ACL screen [490](#)
- Active
  - license state [207](#)
- Active Directory [389, 453](#)
- AD server [389, 453](#)
- add a device
  - tutorial [57](#)
- Add devices screen [198, 199, 288](#)
- Add licenses screen [199](#)
- Add more devices
  - action [196](#)
- Add more licenses
  - action [196](#)
- address
  - gateway [400](#)
- administrator
  - create [162](#)
  - delete [99](#)
  - privilege [160](#)
  - update [162](#)
- administrator account password [144](#)
- administrator accounts [212](#)
- Administrator screen [185, 214](#)
- Administrators screen [212](#)
- Admins & teams [160](#)
- Admins screen [160](#)
- advanced [240](#)
- AES encryption algorithm [360](#)
- Alert Settings screen [285](#)
- ALG [395](#)
- allow list [237, 240, 377](#)
- antenna orientation [521](#)
- antenna switch [521](#)
- anti-malware [239](#)
- Anti-Malware signature [280](#)
- AP [560](#)
- AP & Port Settings screen [564](#)
- AP Google Map
  - Dashboard [255](#)
- AP photo [523](#)
- AP Smart Mesh [510](#)
- AP Status
  - Dashboard [254](#)
- AP Traffic

Dashboard [254](#)  
AP/switch setting  
  overwrite [91](#)  
API token  
  generate [280](#)  
App ID [544](#)  
Appliance Clients (by Usage)  
  Dashboard [254](#)  
Appliance Network Applications  
  Dashboard [254](#)  
Appliance Status  
  Dashboard [254](#)  
Application Layer Gateway, see ALG  
application patrol [236](#), [363](#)  
application patrol profile [431](#)  
  add [364](#)  
Applications screen [274](#)  
APs (by Usage)  
  Dashboard [254](#)  
ARP packet [131](#)  
Ask Question  
  button [581](#)  
assign administrator  
  tutorial [76](#)  
Assign License  
  action [204](#), [205](#), [207](#), [208](#)  
assisted roaming [548](#)  
ATP device  
  license [16](#)  
  trial license [209](#)  
Authentication Method screen [386](#)  
Authentication screen [501](#)  
Automatic Power Save Delivery [548](#)  
auto-negotiation [484](#)

## B

Backup & restore screen [321](#)  
backup code [28](#)  
  download [28](#)  
  inactive [28](#)  
bandwidth utilization [468](#)  
Base Station Identity Code (BSIC) [318](#)  
Base tier [16](#)

base transceiver station [316](#)  
Batch Create DPPSK [226](#)  
battery life [548](#)  
Beta  
  firmware type [250](#), [295](#), [460](#), [516](#)  
binding table [132](#)  
block list [237](#), [240](#), [377](#)  
blocked client  
  release [263](#)  
Branch to Branch VPN  
  enable [180](#)  
bridge priority [507](#)  
  set [507](#)  
browser  
  supported [577](#)  
browser support [22](#)  
BSIC [318](#)  
bundled license [22](#)  
bypass mode [544](#)

## C

captive portal [383](#), [445](#)  
Captive portal customization screen [549](#)  
Captive portal screen [383](#), [445](#)  
captive portal setting  
  SSID profile [549](#)  
carrier aggregation (CA) [316](#), [318](#)  
CDR  
  configure [141](#)  
  tutorial [141](#)  
CDR (Collaborative Detection & Response) [16](#)  
CDR containment [143](#)  
CDR security service [263](#)  
cell ID [316](#)  
Cell Identity [316](#)  
cellular band [316](#)  
Cellular Info screen [313](#)  
cellular IP passthrough  
  setting [307](#)  
  supported model [308](#)  
certificate  
  import [194](#)  
  update [194](#)

- certifications
  - viewing **587**
- Change log screen **157, 177, 191, 210**
- Change organization
  - action **204, 205, 207, 208**
- change owner **213**
- Change site assignment
  - action **204, 205**
- channel bandwidth **532, 533**
- channel ID **326**
- channel list **129**
- channel profile and naming
  - configure **128**
- Channel Quality Indicator (CQI) **318**
- channel width **557**
- Classification mode **466**
- client IP traffic
  - block **141**
- client list
  - export **526**
- client statistics
  - display **257**
- client steering **558**
- clients list **262**
- Clients list screen **257**
- Clients screen **255, 524**
- Cloud Authentication account
  - privilege **166**
- Cloud Authentication screen **216, 296**
- Cloud authentication screen **102**
- Cloud Intelligence Logs screen **269**
- cloud mode **144**
- cloud sandboxing **240**
- Cloud-Saving mode **44**
- CNP security service
  - enable **93**
- Collaborative Detection & Response (CDR) **21, 280**
- Collaborative detection & response screen **142**
- configuration backup **227**
- configuration management **227**
- configuration synchronization **227**
- configuration template **230, 278**
  - tutorial **79**
- Configuration templates screen **230**
- Configure menu **179, 192, 276, 538**
- Connect & Protect (CNP) license **16**
- Connect & Protect (CNP) trial license **209**
- Connect & Protect Plus (CNP+) **16**
- connected device
  - summary **187**
- Connection log screen **262**
- connection speed
  - port **400**
- connection status
  - port **400**
- Connection Test button **145**
- connectivity **191**
- Consumption mode **466**
- contact information **582**
- containment action **283**
- Containment List screen **263**
- Content Filter Pack license **16**
- Content Filter Pack trial license **209**
- content filtering **236, 363, 369, 433**
- content filtering profile
  - add **365**
- controller mesh **511**
- Coordinated Universal Time (UTC) **47**
- copyright **587**
- CPU usage **326, 401**
- CQI **318**
- CRC (Cyclic Redundant Check) error **478, 479**
- CRC error **469**
- create
  - user account **222, 225**
- Create Group window **174**
- Create organization screen **43, 158**
- Create site **194**
- create user account **218**
- Critical
  - firmware status **246, 250, 295**
- cross-org site clone **166**
- cross-org sync **166**
- Cross-org synchronization screen **167**
- CSS value **384, 447**
- Custom
  - firmware status **250, 295**
- custom portal page **447, 551**

custom theme [447, 550](#)  
customer support [574, 582](#)  
Cyclic Redundant Check [469](#)

## D

dark mode [34](#)  
Dashboard logo [159](#)  
    specs [159](#)  
dashboard logo  
    upload/replace/remove [13](#)  
Dashboard screen [29, 252](#)  
    change default view [61](#)  
Data Policy screen [571](#)  
data roaming [315](#)  
DCS  
    time interval [557](#)  
DCS (Dynamic Channel Selection) [532, 533](#)  
DDMI [470](#)  
Dedicated  
    firmware type [250, 295, 460, 516](#)  
Defend Center [240](#)  
Delegate owner's authority  
    privilege [185](#)  
delete icon [321](#)  
Deployment Method  
    Setup Wizard [147](#)  
deployment method [204, 205, 207, 289](#)  
    set up [50](#)  
DES encryption algorithm [360](#)  
description  
    gateway [400](#)  
destination lookup failure (DLF) [520](#)  
device  
    add to site [47](#)  
    view [32](#)  
Device function table [12, 304, 458, 510](#)  
Device function table screen [572](#)  
device list  
    export [177, 190, 204](#)  
Device screen [202](#)  
Devices screen [248, 292](#)  
Devices tab [190](#)  
DH key [441](#)

DHCP relay [416, 421](#)  
DHCP server [416, 421](#)  
DHCP server guard [508](#)  
DHCP service [416, 421](#)  
Differentiated Services Code Point (DSCP) value [508](#)  
Diffie-Hellman key group [441](#)  
Diffie-Hellman key group (DHx) [355, 360](#)  
Digital Diagnostics Monitoring Interface [470](#)  
disable account [163, 186, 215](#)  
disclaimer [587](#)  
DNS content filtering  
    enable [366](#)  
DNS lookup [312](#)  
DNS setting [389, 453](#)  
DNS/URL threat filter [236](#)  
domain name [312](#)  
domain zone [391, 455](#)  
download icon [321](#)  
DPPSK account  
    add/edit [225](#)  
    batch creation [226](#)  
DPPSK screen [223, 300](#)  
DPPSK third-party integration [280](#)  
Dynamic Personal Pre-Shared Key (DPPSK) [19, 218, 219, 224, 225, 227, 269, 298, 301, 544](#)  
    print [224, 301](#)  
DynDNS account [413](#)

## E

EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) [316, 317](#)  
EcNo [317](#)  
Edit floor plans tab [265](#)  
eITS ticket [574](#)  
email  
    alert notification [287](#)  
email address  
    user account [299, 301](#)  
email recipient  
    MSP alerts [171](#)  
email report [333, 405, 408, 473, 481, 536](#)  
Email Verification [27](#)  
encryption algorithm [356, 360](#)

encryption method  
  SSID network [273](#)  
eNodeB (Evolved Node-B) [318](#)  
Ethernet WAN status [312](#)  
E-UTRA Absolute Radio-Frequency Channel  
  Number [316](#), [317](#)  
event log [327](#), [402](#), [471](#), [530](#)  
Event Log screen [327](#), [402](#), [471](#), [530](#)  
event type  
  client diagnostic [262](#)  
Expired  
  license state [207](#)  
expired license  
  renew [62](#)  
extender mesh [511](#)

## F

Facebook app ID [544](#)  
Facebook fan page [544](#)  
Facebook login [527](#), [544](#)  
Facebook WiFi [527](#), [544](#)  
factory-default setting  
  reset to [144](#)  
fan page  
  Facebook [544](#)  
fast roaming [543](#)  
firewall information  
  export [571](#)  
  port information [579](#)  
Firewall information screen [571](#)  
firewall rule [427](#)  
  default [361](#)  
Firewall screen [361](#), [431](#)  
Firewall settings  
  Dynamic DNS screen [393](#)  
Firewall settings screen [389](#)  
firmware  
  maintain [74](#)  
  upgrade [48](#)  
Firmware management screen [245](#), [289](#)  
firmware upgrade  
  priority [245](#)  
  schedule [245](#), [247](#), [289](#)

Firmware upgrade screen [199](#)  
firmware version  
  view [309](#)  
floor plan [264](#)  
force logout [184](#), [212](#)  
FQDN [182](#), [391](#), [455](#)  
FQDN (Fully-Qualified Domain Name) [571](#)  
Full (read and write)  
  access [215](#)  
full access [214](#)  
Full privilege [185](#), [186](#)  
Fully-Qualified Domain Name [391](#), [455](#)  
Fully-Qualified Domain Name (FQDN) [180](#)

## G

gateway  
  log message [402](#)  
Gateway settings screen [453](#), [456](#)  
General Availability  
  firmware type [250](#), [295](#), [460](#), [516](#)  
General settings screen [277](#)  
get started [22](#)  
Gold Security Pack license [16](#)  
Gold Security Pack trial license [209](#)  
Good  
  firmware status [246](#), [250](#), [295](#)  
Google Authenticator app [27](#)  
  install [111](#)  
Google authenticator passcode [104](#)  
Google map [310](#), [400](#), [529](#)  
  client location [258](#)  
  site location [187](#)  
grace period  
  organization license [22](#)  
group  
  create [174](#)  
  definition [174](#)  
Group Administrator account [183](#)  
Group list [175](#)  
Group-wide  
  overview [175](#)  
Group-wide menu [175](#)  
guest ambassador



access [214, 215](#)  
Guest interface [412, 419](#)  
guest VLAN [502](#)  
guest WiFi network [49](#)

## H

hash algorithm [361](#)  
Hit for AP Network IP Reputation Filter  
  Dashboard [255](#)  
Hit for Collaborative Detect & Response  
  Dashboard [254](#)  
Home networking  
  setting [306](#)  
hub [241](#)  
  add [182](#)  
hub to hub VPN [180, 182](#)  
hub-and-spoke topology [180, 241](#)  
Hub-and-Spoke VPN [438](#)

## I

ICCID [315](#)  
icon  
  delete [321](#)  
  download [321](#)  
  More [32](#)  
  pause [312](#)  
  photo remove [311](#)  
  play [312](#)  
idle timeout [193](#)  
IDP [369, 433](#)  
IEEE 802.11k/v [548](#)  
IEEE 802.11r [543](#)  
IEEE 802.3af Power over Ethernet standard [488](#)  
IEEE 802.3at High Power over Ethernet standard [488](#)  
IGMP filtering profile [490](#)  
IGMP Group-Specific Query (GSQ) message [490, 500](#)  
IGMP multicast groups [473](#)  
IGMP query port [490](#)  
IGMP snooping [496](#)  
IGMP status [463](#)  
IKE (Internet Key Exchange) [358, 441](#)  
IKE SA [354](#)  
IKE SA (Security Association) [440](#)  
IKE version [103, 355](#)  
image  
  maximum file size [280](#)  
  upload/replace/remove [280](#)  
IMEI [314](#)  
import certificate [194](#)  
IMSI [315](#)  
Inactive  
  license state [207](#)  
in-app push  
  alert notification [287](#)  
Install wizard  
  action [196](#)  
installation wizard [200](#)  
Installer  
  access [215](#)  
installer privilege [214](#)  
instant messenger (IM) [364, 431](#)  
Insufficient Licenses status [22](#)  
Integrated Circuit Card Identifier (ICCID) [315](#)  
Interface addressing screen [409](#)  
Interface screen [336](#)  
Interfaces addressing  
  Local LAN screen [422](#)  
Interfaces addressing screen [424](#)  
internal antenna [521](#)  
International Mobile Equipment Identity (IMEI) [314](#)  
International Mobile Subscriber Identity (IMSI) [315](#)  
Internet access  
  voucher [267](#)  
Internet Information Server (IIS) [551](#)  
Internet Protocol Security [443](#)  
Internet Service Provider [315](#)  
intra-BSS traffic blocking [540, 548](#)  
Intrusion Detection and Prevention [369, 433](#)  
Intrusion Detection and Prevention (IDP) [329, 404, 406](#)  
intrusion detection/prevention [241](#)  
Inventory screen [176](#)  
IP & Routing screen [492](#)  
IP address  
  add [180](#)

- client [259](#)
  - IP passthrough [315](#)
  - IP source guard
    - setup [131](#)
  - IPS (IDP) signature [280](#)
  - IPS (Intrusion Prevention System) [16](#)
  - IPSec [443](#)
  - IPSec SA [356, 360](#)
  - IPSec tunnel
    - maximum [580](#)
  - IPSec VPN [440](#)
  - IPSec VPN client
    - enable remote access VPN rule [103](#)
  - IPSec VPN tunnel [197](#)
  - IPTV
    - manage [125](#)
    - set up VLAN [125](#)
  - IPTV channel [41, 128, 473](#)
  - IPTV client [473](#)
  - IPTV report [41](#)
  - IPTV report screen [471](#)
  - IPTV topology setup [126](#)
  - IPTV traffic [473](#)
  - IPv4 address
    - gateway [320](#)
    - LAN station [320](#)
  - ISP (Internet Service Provider) [315](#)
- K**
- key size [360](#)
- L**
- L2 isolation [540](#)
  - L2TP [443](#)
  - L2TP VPN [443](#)
  - LAC [318](#)
  - LAI (Location Area ID) [318](#)
  - LAN interface configuration
    - DHCP option screen [343](#)
  - LAN interface configuration screen [340](#)
  - LAN stations screen [319](#)
  - LAN usage
    - view [309](#)
  - language
    - select [34](#)
  - Latest
    - firmware type [250, 295, 460, 516](#)
  - Layer 2 Tunneling Protocol [443](#)
  - layer-2 isolation [548](#)
  - leave mode
    - fast [490](#)
    - normal [490](#)
  - LED tags [513](#)
  - license
    - activate/assign [57](#)
    - activation [58](#)
    - assign to Nebula Device in new organization [66](#)
    - Circle [197](#)
    - feature difference [17](#)
    - general information [22](#)
    - monitor expiration [61](#)
    - payment method [176](#)
    - purchase [197](#)
    - states [58](#)
    - transfer [63, 98](#)
    - transfer to a different organization [65](#)
    - transfer to a Nebula Device in same/new organization [68](#)
    - undo assign [64](#)
    - validity [22](#)
  - license concept [14](#)
  - License Expired status [22](#)
  - license list
    - export [207](#)
  - license management [195](#)
  - License screen [22, 205](#)
  - license summary table [15](#)
  - license tier
    - organization [16](#)
  - License transfer
    - action [205, 207, 208](#)
  - license types [58](#)
  - licenses purchase
    - export [197, 204](#)
  - Link Aggregation Control Protocol (LACP) [421](#)
  - Link Aggregation Group (LAG) [417](#)
  - Link Layer Discovery Protocol [468](#)

- Link Layer Discovery Protocol (LLDP) [483](#)
  - live tools [311](#)
  - LLDP [468](#)
  - LLDP (Link Layer Discovery Protocol) [259](#)
  - LLDP-MED protocol [508](#)
  - load balancing [519, 566](#)
  - load balancing method [452](#)
  - Local credentials password [141](#)
  - local override [230, 232](#)
    - enable [89](#)
    - switch [233](#)
  - Location Area Code (LAC) [318](#)
  - Location Area ID [318](#)
  - locator LED [465](#)
  - log
    - full [157, 177](#)
  - log list
    - export [157, 178, 192, 211, 270](#)
  - log message [471, 530](#)
  - login account
    - menu [32](#)
  - login information [105](#)
  - login page [550](#)
  - login password [141](#)
  - logo
    - remove [159](#)
    - replace [159](#)
    - upload [159](#)
  - loop guard [484](#)
- ## M
- MAC account
    - create/update [222](#)
  - MAC address
    - client [259](#)
    - gateway [400](#)
    - LAN station [320](#)
    - Nebula Device [289](#)
    - port [400](#)
    - user account [299](#)
    - WiFi station [320](#)
  - MAC authentication [543](#)
  - MAC screen [220, 222, 298](#)
  - Managed Service Provider (MSP) [13, 153](#)
    - management control
      - enable [484](#)
    - management port [487](#)
    - management VLAN [507](#)
    - map
      - pin a device [264](#)
    - Map & floor plans screen [264](#)
    - Max Power (mW) [466](#)
    - MCC [315](#)
    - MCS [318](#)
    - Media Independent Interface (MII) [421](#)
    - Memory usage [326, 401](#)
    - merged privilege [213](#)
    - mii (Media Independent Interface) [421](#)
    - MNC [315](#)
    - Mobile Country Code (MCC) [315](#)
    - Mobile Network Code (MNC) [315](#)
    - Mobile router
      - Dashboard [254](#)
    - mobile router
      - restart [312](#)
    - model name
      - Nebula Device [289](#)
    - modulation coding scheme [318](#)
    - monitor a site [79](#)
    - Monitor menu [187, 252, 323, 398, 458, 512](#)
    - Monitor-only
      - access [214, 215](#)
    - More icon [32](#)
    - MSP
      - create organization [158](#)
      - introduction [13](#)
    - MSP administrator [168](#)
    - MSP alerts
      - create [170](#)
      - email recipient [171](#)
      - notification type [172](#)
      - update [170](#)
    - MSP alerts screen [168](#)
    - MSP branding [159](#)
    - MSP license [15, 153](#)
      - activate [93](#)
    - MSP Pack trial license [208](#)
    - MSP portal [153](#)

- MSP Trial license [15](#)
  - My RADIUS server [544](#)
  - myZyxel account [12, 14, 23](#)
    - email address [27, 70](#)
  - myZyxel portal [72](#)
- N**
- N/A
    - firmware type [246, 250, 295, 460, 516](#)
  - name
    - Nebula Device [289](#)
    - port [400](#)
    - user account [299, 301](#)
  - NAS [397, 456](#)
  - NAS identifier [545](#)
  - NAS IP address [397, 456](#)
  - NAT rule [348](#)
  - NAT screen [349](#)
  - Native mode [205, 207](#)
  - NCAS [546](#)
  - NCAS (Nebula Cloud Authentication Server) [387](#)
  - NCC
    - access [23](#)
    - account settings [35](#)
    - alert [33](#)
    - change device owner [42](#)
    - create organization [42](#)
    - dark mode [34](#)
    - Dashboard [252](#)
    - display language [34](#)
    - example network [14](#)
    - features [12](#)
    - license expiration [156, 176](#)
    - license status [176](#)
    - live chat [581](#)
    - log message view [33](#)
    - login [23](#)
    - menu [35](#)
    - notification [34](#)
    - organization [13](#)
    - overview [12, 56](#)
    - portal website [23](#)
    - sample network topology [14](#)
    - settings icon [34](#)
    - site [13](#)
    - two-factor authentication [25](#)
  - NCC license [197](#)
    - category [15](#)
    - status [155](#)
  - NCC logo
    - replace [159](#)
  - NCC menu summary [36](#)
  - NCC portal
    - access [23](#)
    - no access [577](#)
    - overview [29](#)
    - parts [29](#)
    - title bar [30](#)
  - NCC, Nebula Control Center [12, 56](#)
  - Near Expiring status [22](#)
  - Nebula account
    - login [28](#)
  - Nebula cloud authentication
    - select [544](#)
  - Nebula Cloud Authentication Server [546](#)
  - Nebula configuration [146](#)
  - Nebula Device
    - location [310](#)
    - power consumption [466](#)
    - remove [97](#)
    - status [62](#)
  - Nebula Device list
    - export [459](#)
  - Nebula Device port list
    - export [483](#)
  - Nebula managed device
    - connect [23](#)
  - Nebula management mode
    - select [144](#)
  - Nebula Mode
    - select [144](#)
  - Nebula native mode [147](#)
    - deploy [143](#)
    - deployment method [50](#)
  - Nebula portal [146](#)
  - Nebula SD-WAN [24](#)
  - Nebula Security Service [39, 40, 329, 404](#)
  - Nebula Security Service (NSS) license [15](#)
  - Nebula Smart Mesh [510, 566](#)
  - NETCONF [12](#)
  - NETCONF over TLS [12](#)

- Network Access Server [397, 456](#)
  - Network Access Server identifier [545](#)
  - Network address translation (NAT) [411](#)
  - Network Configuration Protocol (NETCONF) [12](#)
  - network connection
    - check [141](#)
  - Network Interface Card (NIC)
    - PXE-capable [343](#)
  - network topology [266](#)
    - fully-meshed [241](#)
  - Network usage and connectivity screen [321](#)
  - next hop [345, 425](#)
  - NSG device
    - license [15](#)
  - NSS [39, 40, 329, 404](#)
  - NSS Analysis Report screen [404](#)
  - NSS/UTM license [197](#)
- O**
- online document
    - parts [569](#)
  - Online documents screen [569](#)
  - ONVIF (Open Network Video Interface Forum) [494](#)
  - ONVIF discovery
    - configure [495](#)
  - ONVIF discovery screen [495](#)
  - operating system
    - show [527](#)
  - Orchestrator [24](#)
  - Orchestrator Management [24](#)
  - organization
    - choose [43](#)
    - copy settings [158](#)
    - create [42, 46, 146, 158](#)
    - create new [25](#)
    - delete [97, 100](#)
    - overview [187](#)
    - privilege [164](#)
    - summary view [31](#)
  - organization (delegated) privilege [214](#)
  - organization access [186, 215](#)
  - organization administrator [12, 14](#)
  - organization license [15](#)
    - grace period [22](#)
  - organization name
    - change [73](#)
  - Organization Trial license [15](#)
  - organization-wide schedule
    - firmware upgrade [249](#)
  - Org-to-Org Service [180](#)
  - Org-to-Org VPN [180, 182](#)
    - configure [180](#)
    - example [180](#)
  - Org-to-Org VPN screen [181](#)
  - OSI (Open System Interconnection) [369, 434](#)
  - OUI (Organizationally Unique Identifier) [508](#)
  - output power
    - radio [556](#)
  - override site-wide configuration
    - enable [89](#)
  - Overview screen [187, 195, 245, 289](#)
  - owner
    - change [213](#)
  - owner privilege [214](#)
- P**
- passcode
    - 2FA [112](#)
  - password
    - administration account [144](#)
    - login [277](#)
    - reset [69](#)
  - pause icon [312](#)
  - payment method
    - license [176](#)
  - PCC [316](#)
  - PCI [315, 316](#)
  - PD priority [488](#)
  - peer-to-peer (P2P) [364, 431](#)
  - Perfect Forward Secrecy [442](#)
  - Perfect Forward Secrecy (PFS) [356, 361](#)
  - Personal Identification Number [315](#)
  - PFS [442](#)
  - photo
    - upload [310](#)
  - photo remove icon [311](#)

- Physical Cell ID (PCI) [315, 316](#)
  - PIN (Personal Identification Number) [315](#)
  - PIN code [315](#)
  - Pin Unlock Key [315](#)
  - ping
    - perform [312](#)
  - play icon [312](#)
  - PLMN (Public Land Mobile Network) [315](#)
  - Plus Pack license [15](#)
  - Plus tier [16](#)
  - PMI [318](#)
  - PoE [503](#)
  - PoE mode [466](#)
  - PoE Power
    - Dashboard [254](#)
  - PoE schedule [488](#)
  - PoE schedules screen [503](#)
  - PoE status [463](#)
  - policy route [344, 425](#)
  - Policy Route screen [425](#)
  - port
    - disabled [507](#)
    - gateway [400](#)
  - port group [335, 411](#)
  - port isolation [486](#)
  - port mirroring [468, 507](#)
  - Port screen [335](#)
  - port security [502](#)
  - port setting
    - Nebula AP [564](#)
  - port VLAN ID [484, 487](#)
  - power consumption
    - Nebula Device [466](#)
    - port [469, 481](#)
  - power management mode [463, 466](#)
  - Power over Ethernet [503](#)
  - Power over Ethernet (PoE) [266](#)
  - power-up mode [488](#)
  - Precoding Matrix Indicator (PMI) [318](#)
  - pre-shared key [245, 354, 438](#)
  - pre-shared key (PSK) [539, 543](#)
  - primary component carrier (PCC) [316](#)
  - privilege [214](#)
    - admin in organization [185](#)
    - administrator [160](#)
    - assign [165](#)
    - merged [213](#)
    - organization [162, 164](#)
  - privilege priority [160](#)
  - Pro Pack license [15](#)
  - Pro Pack trial license [208](#)
  - Pro tier [16](#)
  - problems [577](#)
  - product registration [587](#)
  - profile
    - switch [233](#)
  - protocol ID [347](#)
  - Public Land Mobile Network [315](#)
  - PUCCH (Physical Uplink Control Channel) [318](#)
  - PUK (Pin Unlock Key) [315](#)
  - purchase history
    - export [212](#)
  - Purchase History screen [211](#)
  - Purchase license
    - action [204](#)
  - PUSCH (Physical Uplink Shared Channel) [318](#)
  - PVID [487, 520](#)
  - PXE (Preboot eXecution Environment) [343](#)
- ## Q
- QR code [27, 111](#)
  - QSG (Quick Start Guide)
    - Nebula Device [141](#)
  - Quality of Service (QoS) [507](#)
  - Quarantine screen [284](#)
  - quarantine VLAN [284](#)
  - Queued
    - license state [207](#)
- ## R
- RAC (Routing Area Code) [318](#)
  - radio
    - output power [556](#)
  - Radio Frequency Channel Number [316, 317](#)

- radio setting
    - AP [554](#)
  - Radio settings screen [554](#)
  - RADIUS accounting [545](#)
  - RADIUS server [453](#), [545](#)
  - RAI (Routing Area ID) [318](#)
  - Rank Indication [318](#)
  - rate limiting [540](#)
  - read and write (Full)
    - access [215](#)
  - read and write access [214](#)
  - read-only access [214](#), [215](#)
  - Read-only privilege [185](#), [186](#)
  - reboot
    - mobile router [312](#)
  - Received Signal Code Power [317](#)
  - recurring schedule
    - firmware upgrade [249](#), [294](#)
  - Reference Signal Receive Power (RSRP) [316](#), [317](#)
  - Reference Signal Receive Quality (RSRQ) [316](#), [317](#)
  - Reference Signals (RS) [316](#), [317](#)
  - register
    - device [288](#)
  - register a device [38](#)
  - registration
    - product [587](#)
  - remote access VPN
    - setup [101](#)
  - Remote access VPN screen [103](#), [356](#)
  - remote AP
    - maximum number of [580](#)
  - Remote AP (RAP) [392](#)
  - remote AP feature
    - enable [519](#)
  - remote configurator
    - mobile router [312](#)
  - Remove from organization
    - action [204](#), [205](#)
  - renewal license [22](#)
  - repeater AP [511](#)
  - RESET button [144](#)
  - Resource Element (RE) [316](#), [317](#)
  - restore configuration [230](#)
  - RFCN [316](#), [317](#)
  - roaming
    - mobile router [315](#)
  - root AP [511](#)
  - root bridge [463](#)
  - Routing
    - Policy Routes/Traffic Shaping screen [345](#)
    - Static Route screen [347](#)
  - Routing Area Code [318](#)
  - Routing Area ID [318](#)
  - RSCP [317](#)
  - RSRP [316](#), [317](#)
  - RSRQ [316](#), [317](#)
  - RSSI [316](#)
  - RSSI (Received Signal Strength Indicator) [320](#), [526](#)
  - RSTP status [463](#)
- ## S
- sandboxing [240](#)
  - schedule firmware upgrade [37](#), [38](#), [245](#), [289](#)
  - schedule profile
    - add [433](#)
  - schedule template [504](#), [554](#)
  - SD-WAN license [24](#)
  - search
    - for NCC-managed device [32](#)
  - SecuExtender license key
    - activate [105](#)
  - SecuExtender software
    - install [105](#)
  - Secure WiFi license [16](#), [197](#)
  - Secure WiFi trial license [209](#)
  - SecuReporter screen [329](#)
  - Security Alert
    - Dashboard [254](#)
  - Security Gateway screen [398](#)
  - security log
    - display [312](#)
  - security policy [362](#)
  - security profile sync [236](#)
    - configure [233](#)
  - Security Profile Sync (SPS) [369](#)
  - Security profile sync screen [233](#)
  - Security Service license [15](#)

- Security service screen [369, 561](#)
- security services [401](#)
- serial number [459](#)
  - gateway [400](#)
  - Nebula Device [289](#)
- Server-and-Client VPN [438](#)
- service provider [315](#)
- Service Set Identifier [538](#)
- Settings screen [179, 192](#)
- Setup Wizard [140, 146](#)
- setup wizard [29, 45](#)
  - steps [45](#)
- Setup Wizard screen [144](#)
- severity level [575](#)
- SFP (Small Form Factor Pluggable) port [470](#)
- signal strength
  - mobile router [313](#)
- Signal to Interference plus Noise Ratio (SINR) [316, 318](#)
- SIM card
  - install [141](#)
  - status [315](#)
- single sign-on (SSO) [219](#)
- SINR [316, 318](#)
- SIP
  - ALG [395](#)
- site [241](#)
  - create [46, 146, 194](#)
  - delete [98](#)
  - summary [187](#)
- site (network)
  - add [194](#)
- site administrator [12, 14](#)
- site binding [231](#)
- site list
  - export [188](#)
- site name
  - change [73](#)
- site tag
  - summary [187](#)
- Site tags tab [189](#)
- Sites tab [188](#)
- Site-to-Site VPN screen [351, 436, 439](#)
- site-wide schedule
  - firmware upgrade [294](#)
- Smart Alert Engine [169, 285](#)
- smart client steering [560](#)
- Smart Mesh [510, 521](#)
  - network topology [511](#)
  - wireless hops [511](#)
- Smart VPN [180](#)
- spanning tree [463](#)
- SSID [48, 538](#)
  - mobile router [320](#)
- SSID availability screen [553](#)
- SSID network
  - encryption method [273](#)
- SSID overview screen [538](#)
- SSID profile [538](#)
  - settings [540](#)
- SSID schedule [553](#)
- SSID settings screen [540](#)
- SSIDs (by Usage)
  - Dashboard [254](#)
- Stable
  - firmware type [250, 295, 460, 516](#)
- static route [344, 425](#)
- status
  - voucher [268](#)
- submit ticket [572](#)
- summary report [264](#)
- Summary Report screen [271, 330, 407, 480, 534](#)
- support
  - contact detail [13](#)
- support account [574](#)
- Support contact [159](#)
- Support forum [572](#)
- Support Request screen [573](#)
- supported browsers [577](#)
- supported Nebula Devices [12, 304, 458, 510](#)
- Surveillance screen [477](#)
- switch
  - define role [126](#)
- switch connection status [459](#)
- Switch ports screen [485](#)
- Switch settings screen [504](#)
- Switch Status
  - Dashboard [254](#)
- Switches screen [458](#)
- Syslog server [279](#)
- system log



display [312](#)

## T

TAC [318](#)

tag

gateway [400](#)

tag list

export [189](#)

team

create [164](#)

name [164](#)

update [164](#)

Teams screen [163](#)

template

configuration [230, 278](#)

setting [232](#)

template setting

duplicate/import to a site [83](#)

template site/setting

create/bind [79](#)

ticket

support request [572](#)

ticket details [573](#)

time zone

set [47](#)

site location [278](#)

topology overview [241](#)

Topology screen [266](#)

traceroute

perform [312, 524](#)

traceroute function [326](#)

Tracking Area Code (TAC) [318](#)

traffic log

AP [279](#)

traffic shaping [450, 560](#)

Traffic shaping screen [450, 560](#)

transfer license

action [204](#)

tutorial [63](#)

transfer license to another organization

tutorial [65](#)

transferable license

select [63](#)

transmitting power [560](#)

trial license

activate [54](#)

expiration date [42](#)

trial license summary table [208](#)

Trial screen [209](#)

troubleshooting [577](#)

more help [581](#)

trunk group [483](#)

trunk port [487](#)

TV pixelation [473](#)

Two factor authentication screen [110](#)

two-factor authentication

bypass [218, 298](#)

enable [25, 104](#)

type

user account [301](#)

## U

U/TM Security Pack license [16](#)

U-APSD [548](#)

UARFCN (UTRA Absolute Radio-Frequency Channel Number) [316, 317](#)

UE (User Equipment) [318](#)

Undo assign

action [204, 205, 207, 208](#)

Unused

license state [207](#)

Upgrading

firmware status [250, 295](#)

uplink AP [515](#)

uplink port [134, 487, 507](#)

UPnP

conflict with ONVIF [494](#)

user

remove [100](#)

user account

bind [110](#)

create [218](#)

remove [217, 221](#)

type [216](#)

User screen [216, 218, 296](#)

USG FLEX device

license **16**  
trial license **209**  
USG FLEX screen **323**  
USG VPN device  
license **16**  
trial license **209**  
UTRA Absolute Radio-Frequency Channel Number **316, 317**

## V

virtual machine (VM) **240**  
virtual private network **350, 436**  
Virtual Private Network (VPN)  
create automatically **241**  
VLAN attribute **217, 297**  
VLAN for IPTV **125**  
VLAN ID **48**  
client **259**  
VLAN settings  
guest **49**  
Voice over IP (VoIP) **364, 431**  
voice VLAN **507**  
configure **122**  
voucher **267**  
create **269**  
status **268**  
voucher code  
login **544**  
voucher table  
export **268**  
voucher-based WiFi access **267**  
Vouchers screen **267**  
VPN **350, 436**  
VPN access **217, 297**  
VPN area **242, 353**  
VPN client  
setup **105**  
VPN client setting **356**  
VPN client software  
download **444**  
VPN configuration file **105**  
import steps **105**  
VPN Connections screen **328, 402**

VPN connections screen **112**  
VPN gateway site **347**  
VPN Orchestrator screen **180, 242**  
VPN rule  
enable **103**  
VPN setup  
by user **105**  
VPN tunnel **403**  
open steps **108**  
VPN Tunnel Interface (VTI) **442**  
VPN user  
create **102**

## W

walled garden **387, 389, 392, 453, 540, 546**  
WAN interface configuration screen **338**  
WAN load balancing  
configure **348**  
WAN settings **144**  
configure **144**  
WAN status screen **312**  
WAN Throughput  
Dashboard **254**  
WAN usage  
view **309**  
Warning  
firmware status **246, 250, 295**  
warranty **587**  
note **587**  
web authentication **386, 449**  
Web Filtering signature **280**  
widget  
rearrange **252**  
WiFi  
guest **49**  
WiFi aid **261**  
WiFi Aid screen **260**  
WiFi frequency band **326**  
WiFi mesh solution **510**  
WiFi network name  
enter **48**  
WiFi password  
enter **48**

WiFi settings [48](#)  
WiFi status  
    mobile router [320](#)  
wildcard domain name [546](#)  
WINS (Windows Internet Naming Service) server [416](#),  
[422](#)  
wired clients [255](#)  
wireless bridge  
    use [512](#)  
wireless channel bandwidth [557](#)  
Wireless Clients [255](#)  
    Dashboard [254](#)  
Wireless Clients (by Usage)  
    Dashboard [254](#)  
Wireless Clients Manufacturer  
    Dashboard [254](#)  
Wireless Clients OS  
    Dashboard [254](#)  
Wireless Health screen [530](#)  
Wireless screen [388](#)  
wizard  
    installation [200](#)  
WLAN stations screen [320](#)  
WLAN usage  
    view [309](#)  
world map [264](#)  
WPA Enterprise [544](#)  
WPA2-PSK data encryption [388](#)

## Z

Zero Touch Provision [143](#)  
Zero Touch Provision mode [147](#)  
Zero Touch Provisioning [50](#)  
ZTP (Zero Touch Provision) [143](#)  
ZTP (Zero Touch Provisioning) [50](#)  
ZTP deployment method [147](#)  
ZyWALL VPN device  
    configure [24](#)  
Zyxel Device [266](#)  
Zyxel license marketplace [197](#), [204](#)  
Zyxel webstore [176](#)