

# User's Guide

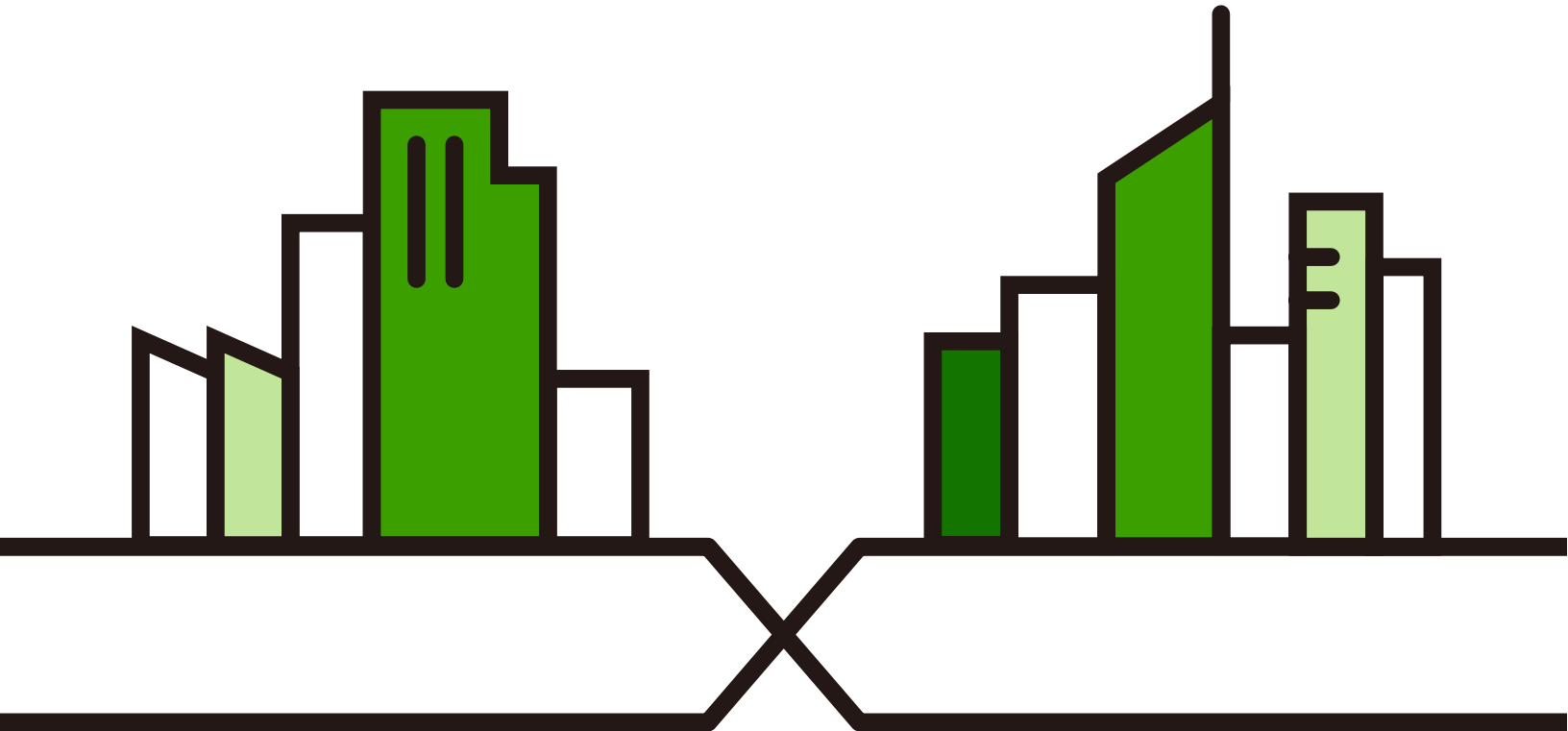
## NCC

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 11 Edition 2, 07/2021



---

## **IMPORTANT!**

### **READ CAREFULLY BEFORE USE.**

### **KEEP THIS GUIDE FOR FUTURE REFERENCE.**

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

Note: This User's Guide is intended for people who want to manage their networks using the Nebula 2.0 user interface with new feature enhancements.

### **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 gateway.

- 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 [support.zyxel.com](http://support.zyxel.com) to find other information on the NCC.



# Table of Contents

<b>Table of Contents</b> .....	<b>3</b>
<b>Part I: User's Guide</b> .....	<b>9</b>
<b>Chapter 1</b>	
<b>Introduction</b> .....	<b>10</b>
1.1 NCC Overview .....	10
1.1.1 Organizations, Sites and Accounts .....	11
1.2 Getting Started .....	13
1.2.1 Connect Nebula Managed Devices .....	13
1.2.2 Access the NCC Portal .....	13
1.3 NCC Portal Overview .....	19
1.3.1 Title Bar .....	19
1.3.2 Navigation Panel .....	25
1.4 Create Organization .....	32
1.5 Choose Organization .....	33
1.6 Cloud-Saving Mode .....	33
<b>Chapter 2</b>	
<b>Setup Wizard</b> .....	<b>35</b>
2.1 Setup Wizard .....	35
2.1.1 Step1: Run the Wizard .....	35
2.1.2 Step 2: Create an Organization and Site .....	36
2.1.3 Step 3: Add Your Devices .....	37
2.1.4 Step 4: Set up your WiFi Network .....	38
2.1.5 Step 5: Set up a Guest WiFi Network .....	39
2.1.6 Step 6: Set up the ZTP (Zero Touch Provisioning) .....	40
2.1.7 Step 7: View the Summary .....	41
2.1.8 Step 8: Activate NCC Pro Pack and Security Services Trial Period .....	42
<b>Chapter 3</b>	
<b>Tutorial</b> .....	<b>43</b>
3.1 Overview .....	43
3.1.1 Adding a Device .....	43
3.1.2 Monitoring a Site .....	44
3.1.3 Managing a Configuration Template .....	45

<b>Part II: Technical Reference</b> .....	<b>63</b>
<b>Chapter 4</b>	
<b>MSP</b> .....	<b>64</b>
4.1 Overview .....	64
4.2 MSP Portal .....	64
4.3 MSP Branding .....	66
4.4 Admins & Teams .....	68
4.4.1 Admins Screen .....	68
4.4.2 Teams Screen .....	71
4.4.3 Cross-org synchronization .....	73
4.5 MSP Alerts .....	75
4.5.1 Alert Settings .....	76
<b>Chapter 5</b>	
<b>Group-wide</b> .....	<b>79</b>
5.1 Introduction .....	79
5.1.1 Creating a Group .....	79
5.1.2 Group-Wide Menu .....	80
5.2 Monitor .....	80
5.2.1 Overview .....	80
5.2.2 Inventory .....	81
5.2.3 Change Log .....	82
5.3 Configure .....	84
5.3.1 Group Settings .....	84
5.3.2 Org-To-Org VPN .....	85
5.3.3 Administrators .....	88
<b>Chapter 6</b>	
<b>Organization-wide</b> .....	<b>92</b>
6.1 Overview .....	92
6.2 Monitor .....	92
6.2.1 Organization Overview .....	92
6.2.2 Change Log .....	96
6.3 Configure .....	97
6.3.1 Create Site .....	97
6.3.2 License & Inventory .....	98
6.3.3 Organization Settings .....	114
6.3.4 Administrators .....	116
6.3.5 Cloud Authentication .....	120
6.3.6 Configuration Management .....	131
6.3.7 Configuration Template .....	134
6.3.8 Security Profile Sync .....	137



---

6.3.9 VPN Orchestrator .....	143
6.3.10 Firmware Management .....	146
<b>Chapter 7</b>	
<b>Site-wide .....</b>	<b>148</b>
7.1 Monitor .....	148
7.1.1 Dashboard .....	148
7.1.2 Clients .....	150
7.1.3 Containment List .....	157
7.1.4 Map & Floor Plans .....	158
7.1.5 Topology .....	160
7.1.6 Vouchers .....	161
7.1.7 Cloud Intelligence Logs .....	164
7.1.8 Summary Report .....	165
7.1.9 Applications .....	168
7.2 Configure .....	171
7.2.1 General Settings .....	172
7.2.2 Collaborative Detection & Response .....	175
7.2.3 Quarantine Interface Configuration .....	178
7.2.4 Alert Settings .....	179
7.2.5 Add Devices .....	182
7.2.6 Firmware Management .....	183
7.2.7 Cloud Authentication .....	186
<b>Chapter 8</b>	
<b>Security Gateway .....</b>	<b>192</b>
8.1 Overview .....	192
8.2 Monitor .....	192
8.2.1 Security Gateway .....	192
8.2.2 Clients .....	195
8.2.3 Event Log .....	195
8.2.4 VPN Connections .....	196
8.2.5 NSS Analysis Report .....	198
8.2.6 Summary Report .....	200
8.3 Configure .....	203
8.3.1 Interface Addressing .....	203
8.3.2 Link Aggregation Groups .....	211
8.3.3 Policy Route .....	219
8.3.4 Firewall .....	220
8.3.5 Security Service .....	227
8.3.6 Site-to-Site VPN .....	230
8.3.7 Remote Access VPN .....	236
8.3.8 Captive Portal .....	238

---

8.3.9 Network Access Method .....	241
8.3.10 Traffic Shaping .....	243
8.3.11 Gateway Settings .....	246
<b>Chapter 9</b>	
<b>USG FLEX .....</b>	<b>251</b>
9.1 Overview .....	251
9.2 Monitor .....	251
9.2.1 USG FLEX .....	251
9.2.2 Clients .....	255
9.2.3 Event Log .....	255
9.2.4 VPN Connections .....	255
9.2.5 SecuReporter .....	257
9.2.6 Summary Report .....	258
9.3 Configure .....	263
9.3.1 Port .....	263
9.3.2 Interface .....	264
9.3.3 Routing .....	272
9.3.4 NAT .....	277
9.3.5 Site-to-Site VPN .....	278
9.3.6 Remote Access VPN .....	283
9.3.7 Firewall .....	288
9.3.8 Security Service .....	295
9.3.9 Captive Portal .....	303
9.3.10 Authentication Method .....	306
9.3.11 Authentication Method .....	308
9.3.12 Wireless .....	310
9.3.13 Gateway Settings .....	312
<b>Chapter 10</b>	
<b>Switch .....</b>	<b>321</b>
10.1 Overview .....	321
10.2 Monitor .....	321
10.2.1 Switches .....	321
10.2.2 Clients .....	332
10.2.3 Event Log .....	332
10.2.4 IPTV Report .....	332
10.2.5 Surveillance .....	336
10.2.6 Surveillance Port Details .....	337
10.2.7 Summary Report .....	338
10.3 Configure .....	341
10.3.1 Switch Ports .....	341
10.3.2 ACL .....	348

10.3.3 IP & Routing .....	349
10.3.4 ONVIF Discovery .....	352
10.3.5 Advanced IGMP .....	354
10.3.6 RADIUS Policies .....	358
10.3.7 PoE Schedules .....	360
10.3.8 Switch Settings .....	361
<b>Chapter 11</b>	
<b>Access Point .....</b>	<b>365</b>
11.1 Overview .....	365
11.1.1 Nebula Smart Mesh .....	365
11.1.2 Smart Mesh Network Topology .....	366
11.2 Monitor .....	367
11.2.1 Access Points .....	367
11.2.2 Clients .....	375
11.2.3 Event Log .....	380
11.2.4 Wireless Health .....	380
11.2.5 Summary Report .....	383
11.3 Configure .....	386
11.3.1 SSID Overview .....	386
11.3.2 SSID Settings .....	389
11.3.3 Captive Portal Customization .....	396
11.3.4 SSID Availability .....	400
11.3.5 Radio Settings .....	401
11.3.6 AP & Port Settings .....	406
<b>Chapter 12</b>	
<b>Help .....</b>	<b>410</b>
12.1 Support Forum .....	410
12.2 Support Request .....	410
12.3 Online documents .....	412
12.4 Firewall Information .....	412
12.5 Data Policy .....	413
12.6 Device Function Table .....	413
<b>Chapter 13</b>	
<b>Troubleshooting .....</b>	<b>415</b>
13.1 Getting More Troubleshooting Help .....	416
Appendix A Customer Support .....	417
13.2 Zyxel Support .....	417
13.3 NCC Live Chat .....	422
Appendix B Legal Information .....	424

[Index .....](#)425

---

# PART I

## User's Guide

---

# 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 APs, Ethernet switches, and security gateways. 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 13](#).

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

At the time of writing, the devices that can be managed through the NCC are:

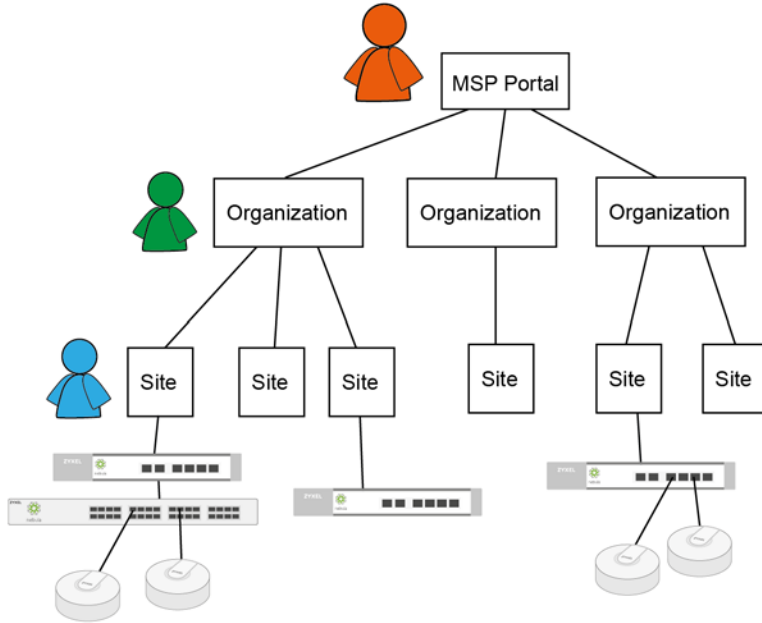
Table 1 Supported Nebula Devices

SECURITY GATEWAY	ETHERNET SWITCH	ACCESS POINT (AP)
<ul style="list-style-type: none"> <li>• NSG50</li> <li>• NSG100</li> <li>• NSG200</li> <li>• NSG300</li> <li>• USG FLEX 100</li> <li>• USG FLEX 100W</li> <li>• USG FLEX 200</li> <li>• USG FLEX 500</li> <li>• USG FLEX 700</li> </ul>	<ul style="list-style-type: none"> <li>• NSW100 series</li> <li>• NSW200-28P</li> <li>• GS1350 series</li> <li>• GS1920v2 series</li> <li>• GS2220 series</li> <li>• XGS1930 series</li> <li>• XS3800-28</li> <li>• XS1930 series</li> </ul>	<ul style="list-style-type: none"> <li>• NAP102</li> <li>• NAP203</li> <li>• NAP303</li> <li>• NAP353</li> <li>• NWA110AX</li> <li>• NWA210AX</li> <li>• NWA1123-ACv2</li> <li>• NWA1123-ACv3</li> <li>• NWA1123-AC HD</li> <li>• NWA1123-AC PRO</li> <li>• NWA1302-AC</li> <li>• NWA50AX</li> <li>• NWA5123-AC HD</li> <li>• WAC500</li> <li>• WAC500H</li> <li>• WAC5302D-Sv2</li> <li>• WAC6103D-I</li> <li>• WAC6303D-S</li> <li>• WAC6502D-S</li> <li>• WAC6502D-E</li> <li>• WAC6503D-S</li> <li>• WAC6552D-S</li> <li>• WAC6553D-E</li> <li>• WAX510D</li> <li>• WAX610D</li> <li>• WAX650S</li> </ul>

## 1.1.1 Organizations, Sites and Accounts

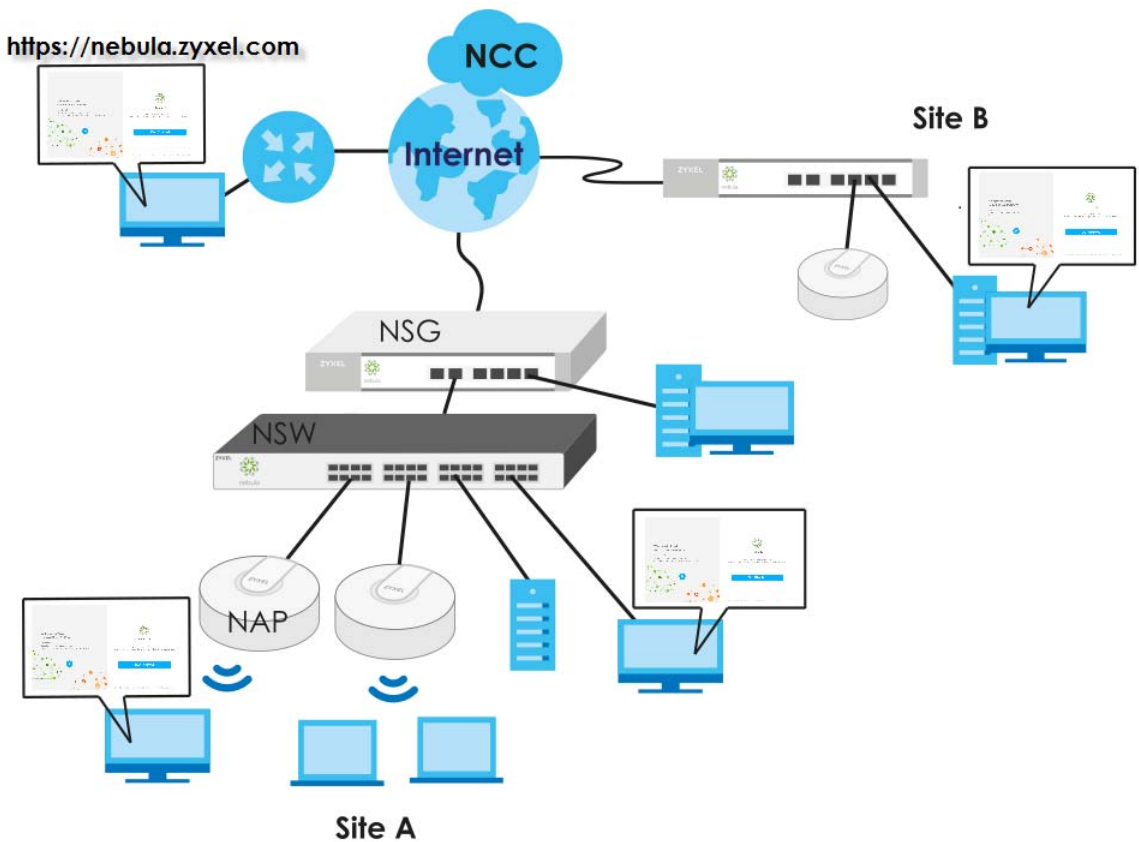
In the NCC, a site is a group of Nebula-managed devices in the same network. An organization is a group of sites. To use the NCC to manage your Nebula devices, each device should be assigned to a site and the site must belong to an organization.

- A site can have multiple Nebula devices, but can only belong to one organization.
- A site can be managed by more than one site/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 116](#)).
- A Managed Service Provider (MSP) network is a group of organizations that belong to the same organization administrator. The organization administrator can use the MSP portal page to view the organization summary and transfer licenses (see [Section 4.2 on page 64](#)).
- To see the MSP menus, you need an MSP license assigned to your NCC login account, as discussed in [Section 4.1 on page 64](#).
- A site administrator can manage more than one site.



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 devices even when they are located at different places.

Figure 1 NCC Example Network Topology





## 1.2 Getting Started

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

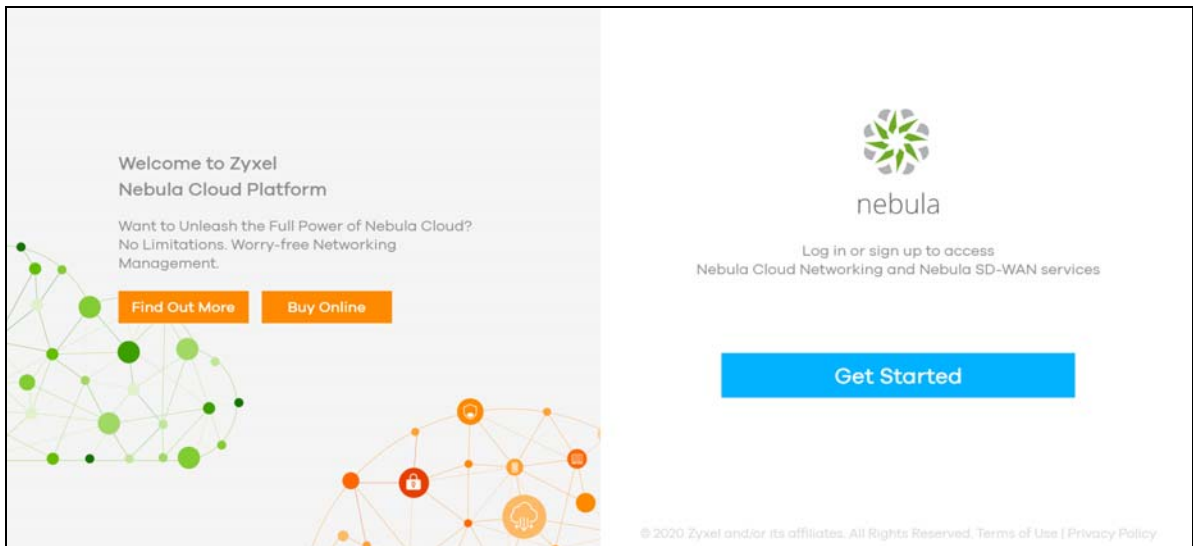
### 1.2.1 Connect Nebula Managed Devices

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 Type <http://nebula.zyxel.com> in a supported web browser. Click **Get Started**.

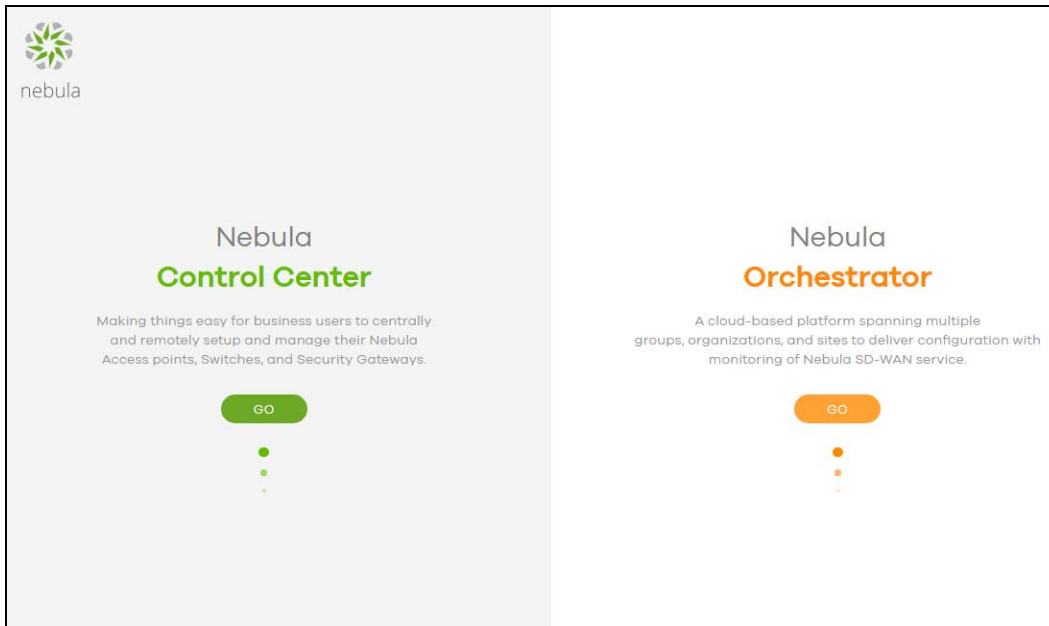


Note: The NCC requires a myZyxel account before you can register and manage Nebula devices. Log into the NCC with your myZyxel account. Click **Create Account** if you do not have a myZyxel account and create an account with your existing email address.

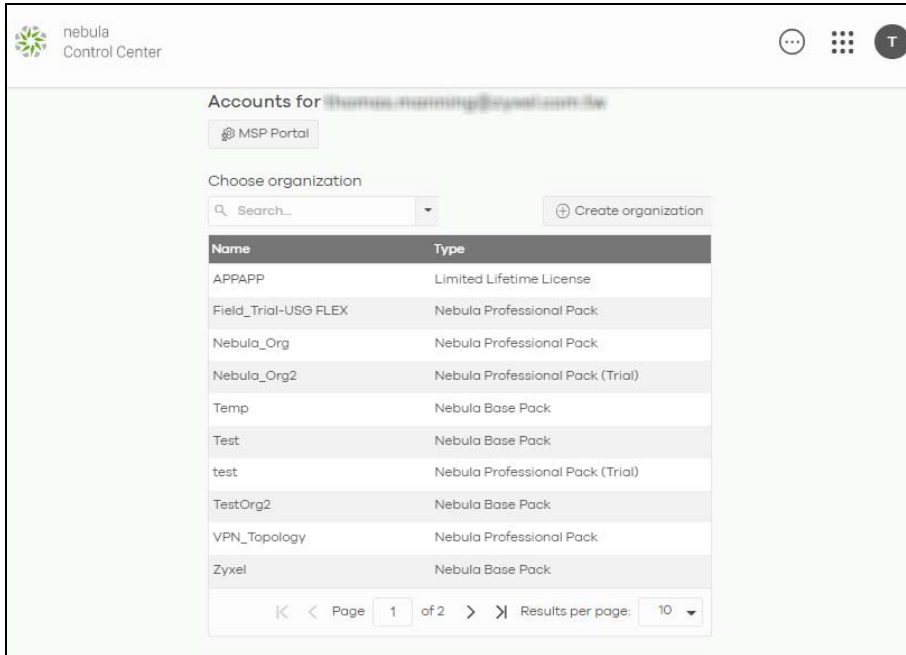
- 2 Enter the **Email Address** and **Password**, and then click **Sign In**.

The image shows a 'Sign In' form. At the top is the title 'Sign In'. Below it is an 'Email Address' field with a placeholder 'businessname@business.com'. A checkbox labeled 'Remember my email.' is checked. Below that is a 'Password' field with a placeholder '\*\*\*\*\*' and a 'Forgot Password' link. A large green 'Sign In' button is centered. Below the button, there is a link for users who haven't activated their account: 'I have signed up but haven't activated my account. Resend Activation Email'. At the bottom, there is a link for new users: 'Don't have an account? Create account'. At the very bottom, there are links for 'Legal Notice', 'Terms of Use', 'Privacy', and 'Cookie Settings', and a copyright notice: '249.7 Copyright © 2021 Zyxel and/or its affiliates. All Rights Reserved.'

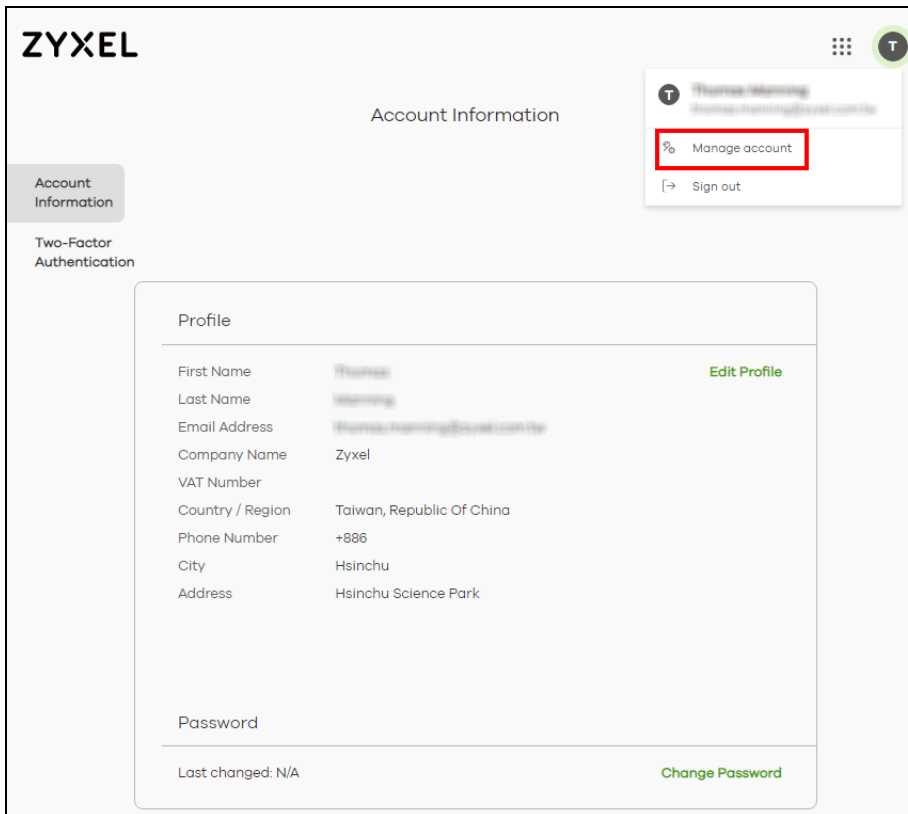
- 3 Click **Go** under Nebula Control Center to log in NCC.



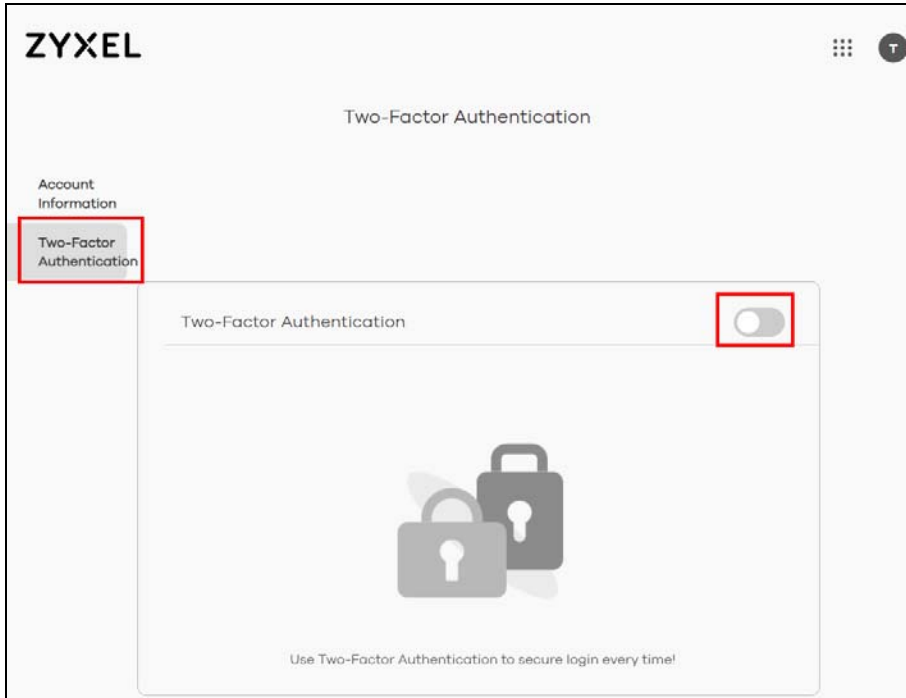
- 4 Click **Create organization** to create a new organization. If this is the first time you have logged into NCC, proceed to step 10. If you have more than one organization, click a row to select the organization you want to manage.



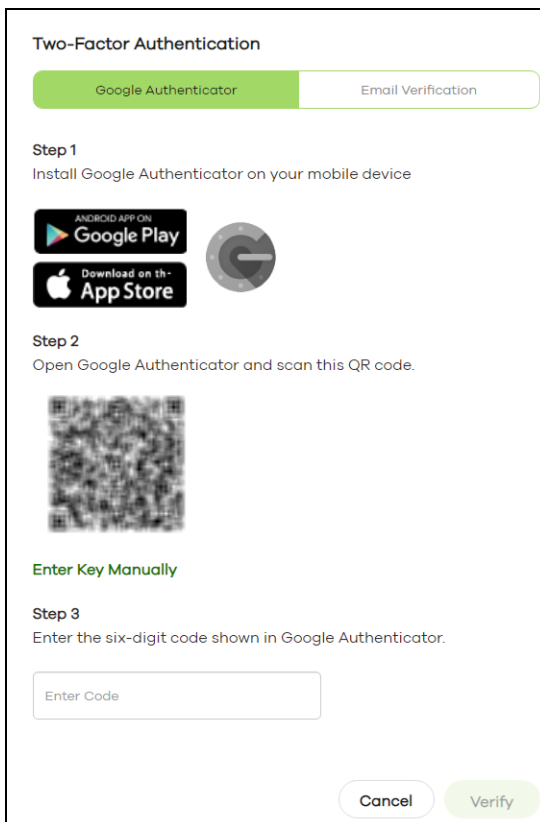
- The NCC supports two-factor authentication (2FA) to add a second layer of security to your account. Click **Manage account** to enable Two-factor authentication on the following page. Otherwise, you can skip 2FA and go to step 10 directly.



- 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 mobile phone 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.



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

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

The screenshot shows a 'Two-Factor Authentication' setup screen. At the top, there are two tabs: 'Google Authenticator' and 'Email Verification', with the latter being selected and highlighted in green. Below the tabs, a message states: 'We have send a verification email to [redacted]@\*\*\*el.com.tw. Please enter the six-digit code in the email.' There is a text input field labeled 'Enter Code'. Below the input field is a green 'Resend' link. At the bottom, there are two buttons: 'Cancel' and 'Verify'.

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

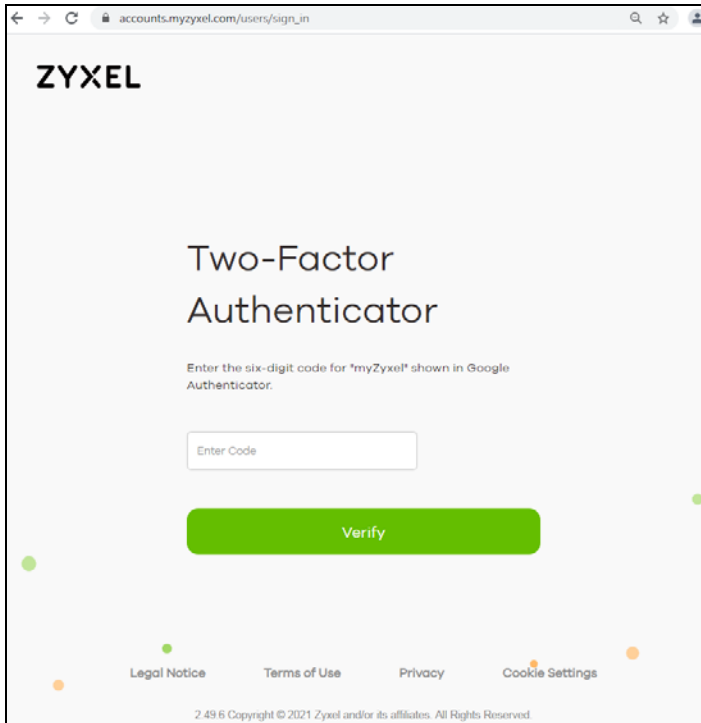
Note: If you generate a new set of backup codes, the old set will become inactive.

The screenshot shows the 'Two-Factor Authentication' setup screen with the 'Email Verification' option selected. A toggle switch for 'Two-Factor Authentication' is turned on. Below this, there are two main sections. The first section is for 'Google Authenticator', which is marked with a green checkmark and includes a link to 'Get code on Google Authenticator app'. The second section is for 'Backup Code', which includes a description: 'These one-off-passcodes allow you to sign in when you use Google Authenticator away from your mobile phone. Each backup code can only be used once. You may generate more codes as you need.' Below this description is a grid of 10 backup codes arranged in two rows of five. At the bottom of the backup code section are two links: 'Download' and 'Generate New Code'. The 'Email Verification' option is shown at the bottom with an unselected radio button.

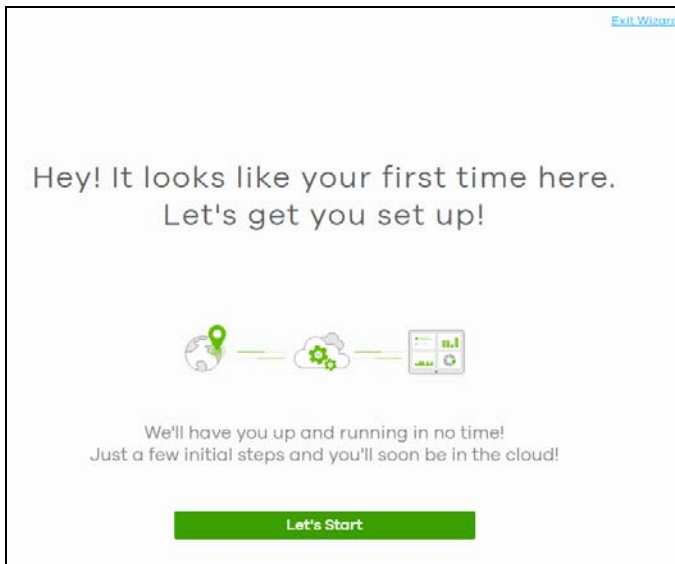
122220	482019	064804	716777	867627
485769	496888	306540	556545	164640

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.

- 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.



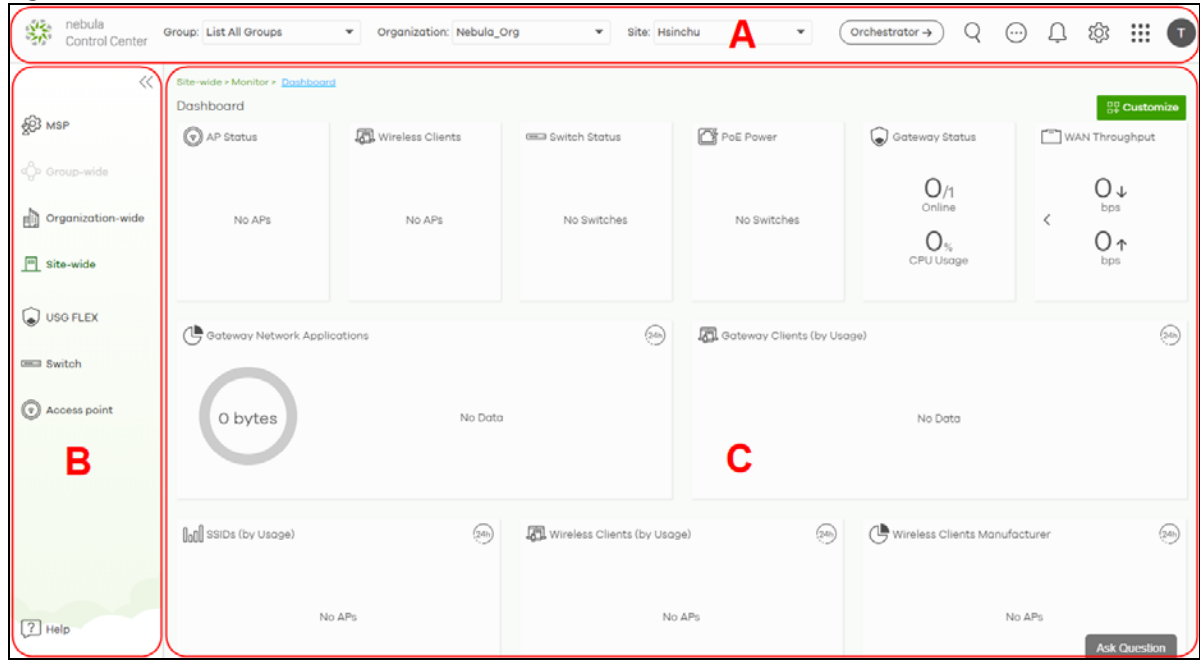
- If this is the first time you have logged into NCC, the setup wizard welcome screen displays. You need to create your organization and sites, register Nebula devices and associate them with a site. See [Chapter 2 on page 34](#) for how to use the wizard and [Chapter 5 on page 69](#) for detailed information about organization and sites.



## 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 2** 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 3** NCC Title Bar



The icons provide the following functions.

**Table 2** NCC Title Bar

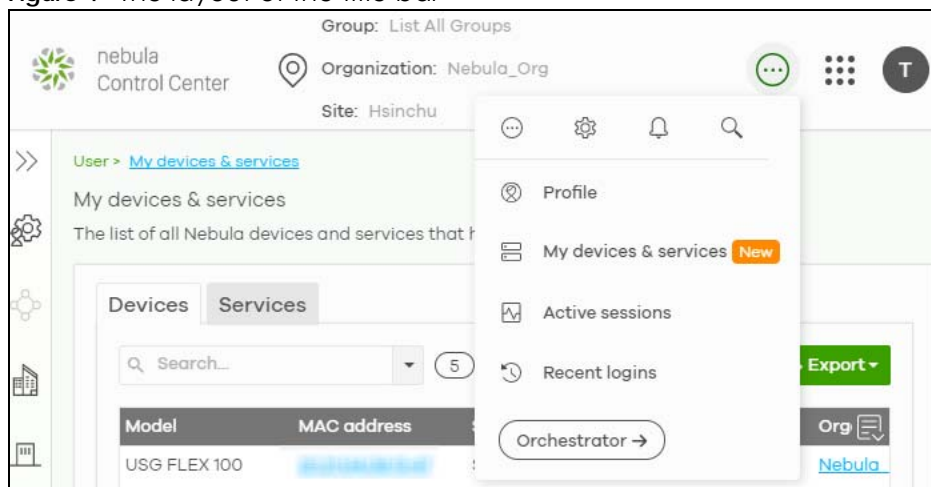
LABEL	DESCRIPTION
Group	This shows the name of the groups you are managing, if your NCC account has an MSP license. Click to choose another group if you have multiple groups.  Note: To create a group, you must be the owner of two or more Pro pack organizations that are not currently assigned to a group, as discussed in <a href="#">Section 5.1.1 on page 79</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.

Table 2 NCC Title Bar (continued)

LABEL	DESCRIPTION
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.
Orchestrator	Click this to go to the Nebula Orchestrator portal to manage your SD-WAN devices. See the SD-WAN user's guide.
Search	Use this to search for managed devices by model, description or MAC address.
More	Click this to view your account information, login history and active sessions. You can also view your 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, Circle, SecuReporter, CNC, 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 4 The layout of the title bar



### 1.3.1.1 Group/Organization/Site

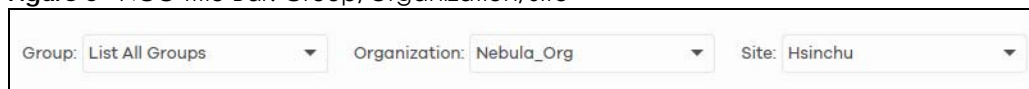
Select the group, organization and site that you want to manage.

- 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 64](#)).

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 32](#)).

Figure 5 NCC Title Bar: Group/Organization/Site

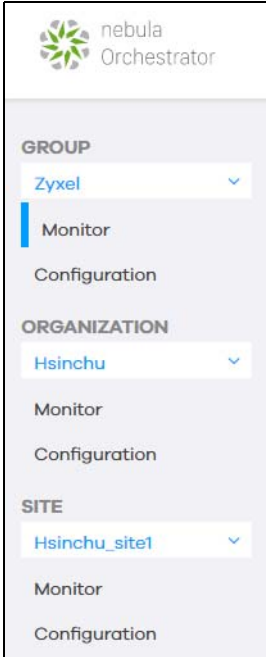




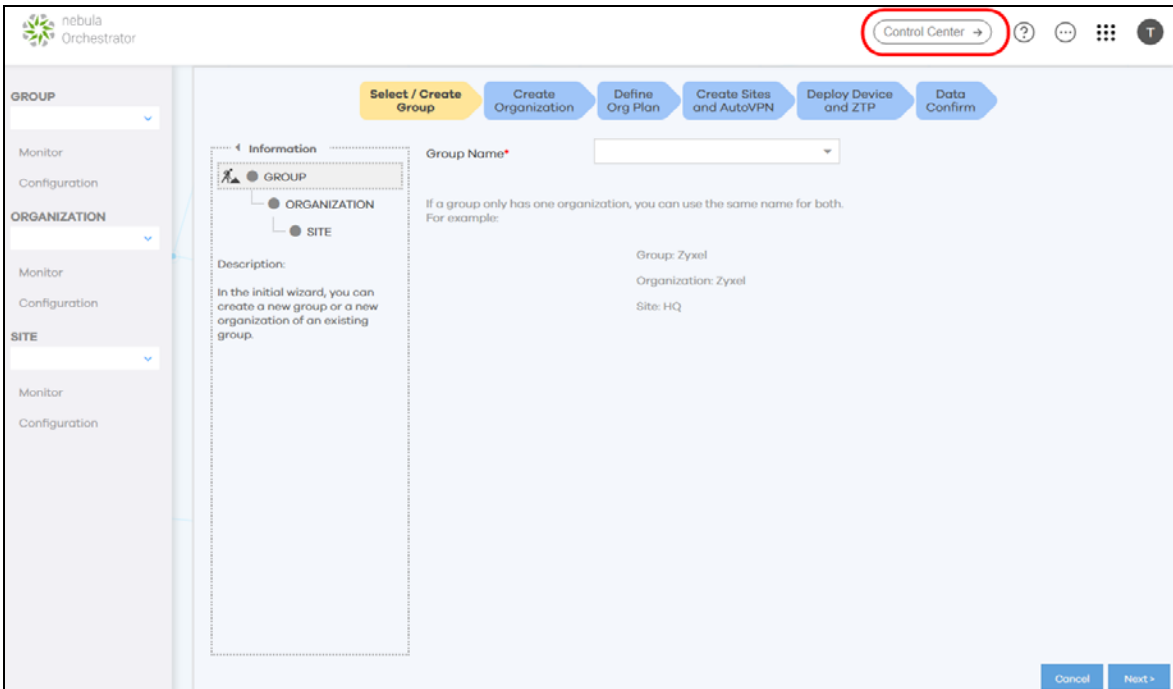
### 1.3.1.2 Orchestrator

Click this 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 6 Nebula SD-WAN (Orchestrator)



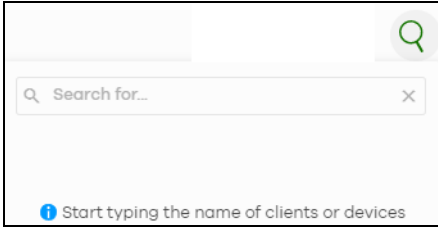
You can click **Control Center** to go back to the NCC platform.



### 1.3.1.3 Search

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

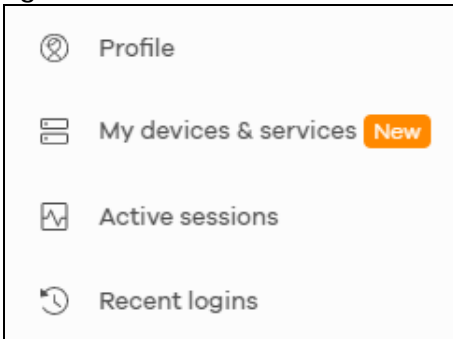
**Figure 7** Search



### 1.3.1.4 More

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

**Figure 8** More



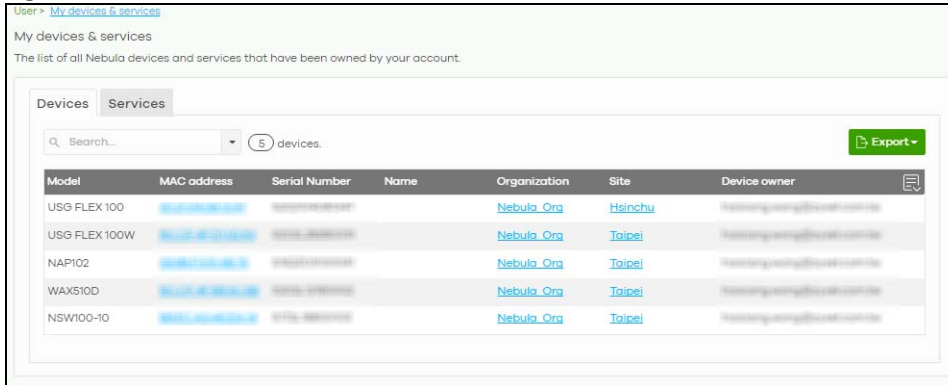
The following table describes this menu.

Table 3 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 devices in NCC that have your login account as the owner. You can filter the list of 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 IP address, location, and time.

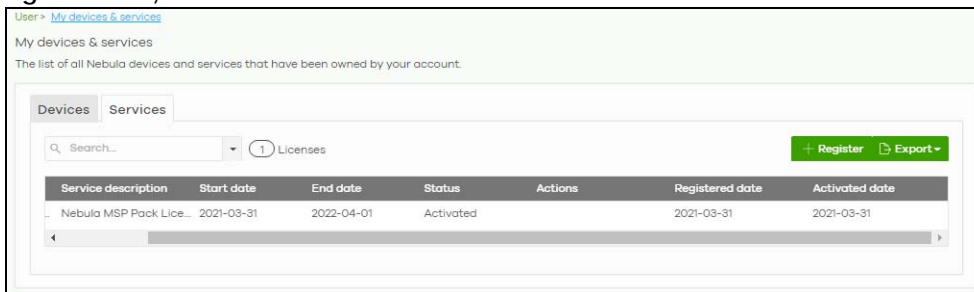
Click **My devices & services** and the following screen appears. Click **Devices** to view all devices of the user account which can be managed by NCC, and/or all devices not registered to this user account but with a Full (Delegated) administrator privilege. See the table on [MSP > Configure > Admins & teams > Admins](#) in [Section 4.4.1 on page 68](#) for details on the organization privileges.

Figure 9 My devices



Click **Services** to view and configure the start dates, end dates, registered dates, activated dates and statuses of an MSP license.

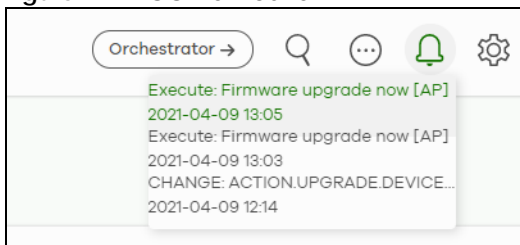
Figure 10 My services



### 1.3.1.5 Notification

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

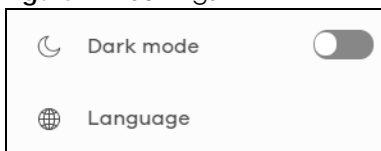
Figure 11 NCC Notification



### 1.3.1.6 Settings

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

Figure 12 Settings

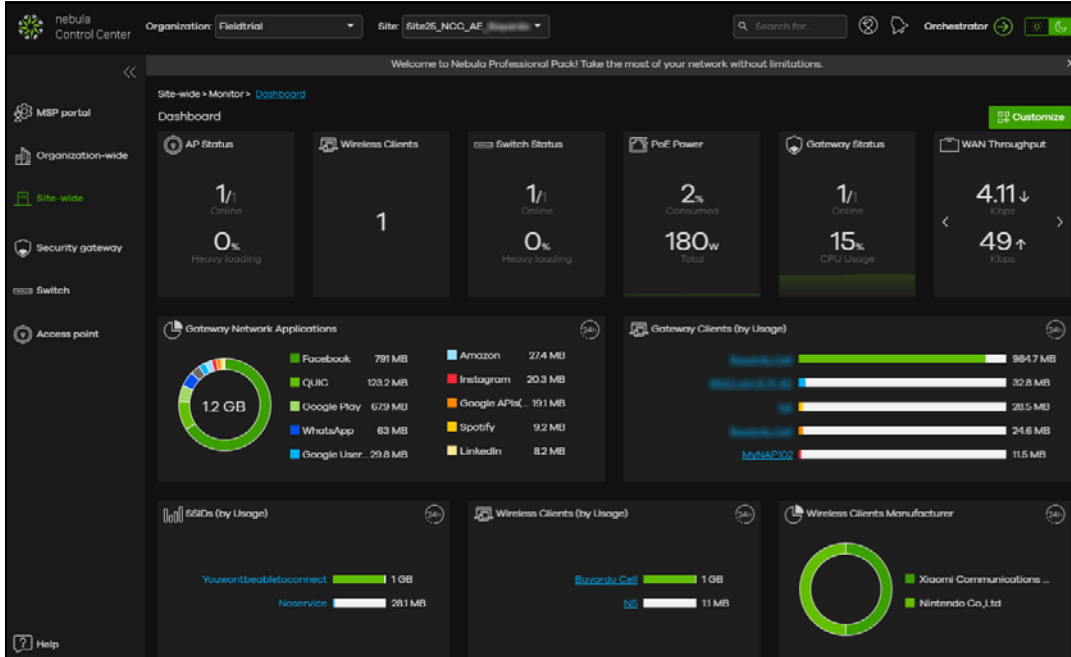


The following table describes this menu.

Table 4 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.

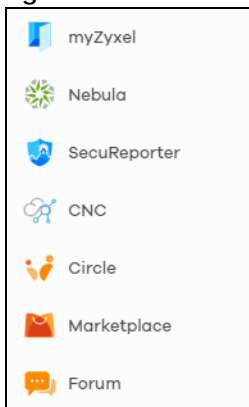
Figure 13 Dark Mode



### 1.3.1.7 Applications

Click this to display a list of related NCC links.

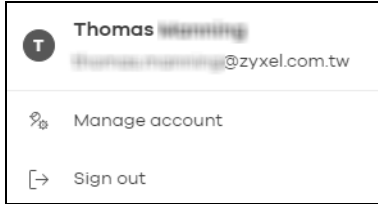
Figure 14 Related NCC Links



### 1.3.1.8 Account

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

**Figure 15** Account



The following table describes this menu.

**Table 5** 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 6** 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.
Organization-wide	Manage multiple network sites within an organization.
Site-wide	Manage devices in a site.
Use these menus to set up customer devices.	
Security gateway	Manage Zyxel security gateways (firewalls).
USG FLEX	Manage Zyxel security gateways (firewalls).
Switch	Manage Zyxel switches.
Access point	Manage Zyxel switches APs.
Help	Access the Zyxel community forum, submit a support ticket, view User Guides for Nebula and 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 7 NCC Menu Summary

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
MSP	Monitor	
	MSP portal	Use this menu to create multiple organizations and change the branding and assign administrators to multiple organizations.
	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 alerts	Use this menu to configure <b>MSP alerts</b> to monitor devices for unexpected events (for example, online/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 devices belonging to organizations. You may also export the list of 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 7 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
Organization-wide	Monitor	
	Overview	Use this menu to view a list of sites belonging to the selected organization and detailed information about the 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 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 devices in the organization.

Table 7 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
Site-wide	Monitor	
	Dashboard	Use this menu to view device connection status and traffic summary.
	Clients	Use this menu to view the connection status and detailed information about a client of the site.
	Containment list	Use this menu to view and manage devices contained by CDR (Collaborative Detection & Response).
	Map & Floor plans	Use this menu to locate devices on a world map or on a floor plan.
	Topology	Use this menu to view 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 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, device login password and firmware upgrade schedule.
	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 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 device and add it to the site.
	Firmware management	Use this menu to upgrade firmware or schedule firmware upgrades for 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.



Table 7 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
Security gateway		Use these menus to monitor and configure the security gateways, not including USG Flex series, managed by the NCC. The settings are applied when a Nebula gateway is registered and attached to the selected site.
	Monitor	
	Security gateway	Use this menu to view the detailed information about the security gateway 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 gateway. An event is something that has happened to a 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 gateway in the site.
	Configure	
	Interface addressing	Use this menu to configure network mode, port grouping, interface address, static route and DDNS settings on the gateway.
	Policy route	Use this menu to view and configure policy routes.
	Firewall	Use this menu to configure firewall rules for outbound traffic, application patrol, schedule profiles and port forwarding rules for inbound traffic.
	Security service	Use this menu to enable content filtering and block access to specific web sites. You can also enable Anti-virus and Intrusion Detection and Prevention (IDP) on the security gateway.
	Site-to-Site VPN	Use this menu to configure VPN rules.
	Remote access VPN	Use this menu to enable and configure IPsec VPN or L2TP VPN settings.
	Captive portal	Use this menu to configure captive portal settings for each gateway interface.
	Network access method	Use this menu to enable or disable web authentication on an interface.
	Traffic shaping	Use this menu to configure the maximum bandwidth and load balancing.
	Gateway settings	Use this menu to configure the DNS server and address records and also set the external AD (Active Directory) server or RADIUS server that the security gateway can use in authenticating users. You can also specify walled garden web site links for all interfaces on the gateway.

Table 7 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
USG FLEX		Use these menus to monitor and configure the USG FLEX devices, not including NSG devices, managed by the NCC. The settings are applied when a Nebula gateway is registered and attached to the selected site.
	Monitor	
	USG FLEX	Use this menu to view the detailed information about the security gateway 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 gateway. An event is something that has happened to a 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 gateway in the site.
	Configure	
	Port	Use this menu to configure network mode and port grouping on the gateway.
	Interface	Use this menu to configure interface address, subnet mask and VLAN ID settings on the gateway.
	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 gateways.
	Remote access VPN	Use this menu to enable and configure IPsec VPN or L2TP VPN rules from off-site clients to an on-site gateway.
	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 gateway.
	Captive portal	Use this menu to configure captive portal settings for each gateway 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 USG FLEX 100(W).  Note: This menu only appears for the USG FLEX 100(W).
	Gateway settings	Use this menu to configure the DNS server and address records and also set the external AD (Active Directory) server or RADIUS server that the security gateway can use in authenticating users. You can also specify walled garden web site links for all interfaces on the gateway.

Table 7 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	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 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.
	RADIUS policies	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 7 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
Access Point		Use these menus to monitor and configure the APs managed by the NCC. The settings are applied when a Nebula AP is registered and attached to the selected site.
	Monitor	
	Access points	Use this menu to view the list of APs added to the site.
	Clients	Use this menu to view WiFi clients which are connected to the APs in the site.
	Event log	Use this menu to view all events on the AP. An event is something that has happened to a managed device.
	Wireless health	Use this menu to view health of the wireless networks for the supported APs and connected clients.
	Summary report	Use this menu to view network statistics specific to APs in the site.
	Configure	
	SSID overview	Use this menu to view and configure SSID settings and authentication methods.
	SSID 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 clients steering for all APs in the site.
	AP & port settings	Use this menu to configure load balancing settings and enable or disable a port on the managed AP 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 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. Please configure your device owners and organizations carefully. See also [Section 6.3.2 on page 98](#).

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.

- 1 Click **Create Organization** from the **Organization** drop-down list box in the title bar. The Wizard starts. See [Chapter 2 on page 35](#) 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 before clicking the **Create organization** button.
- 4 Click the **Create organization** button to add a new organization.

**Figure 16** Create Organization

- 5 Choose whether to activate a one-month trial of Nebula Pro Pack and Nebula Security Services for the organization.

## 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 buy a MSP license to see the MSP Portal menu.

**Figure 17** Choose Organization

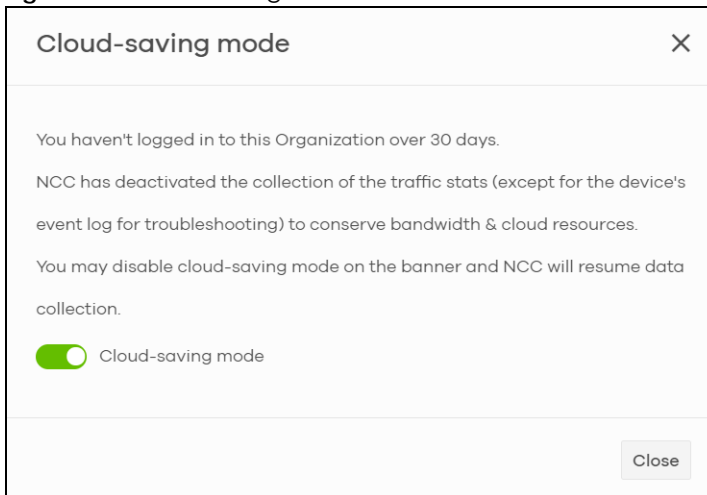
Name	Type
Org1	Nebula
Org2	Nebula

## 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. When Cloud-saving is enabled, NCC does not record any

data traffic statistics, except for event logs. To disable Cloud-saving mode, click the link in the NCC banner when notified.

**Figure 18** Cloud-saving mode

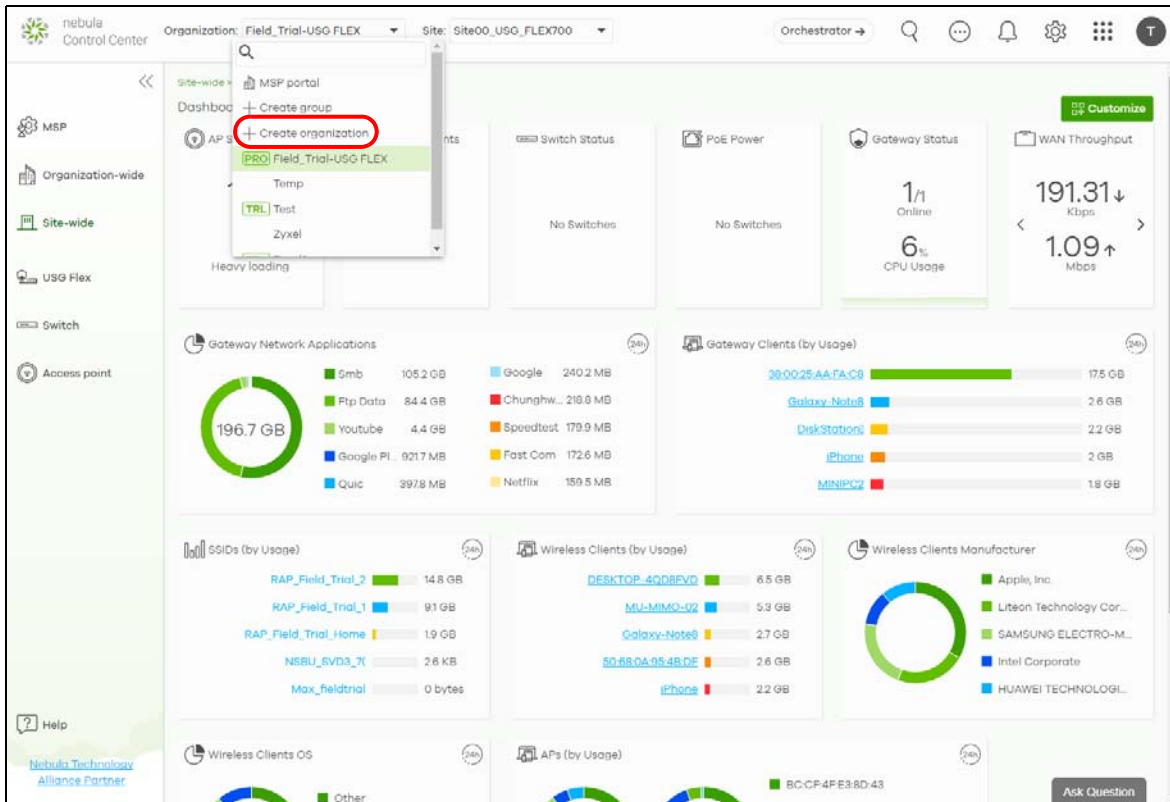


# CHAPTER 2

# Setup Wizard

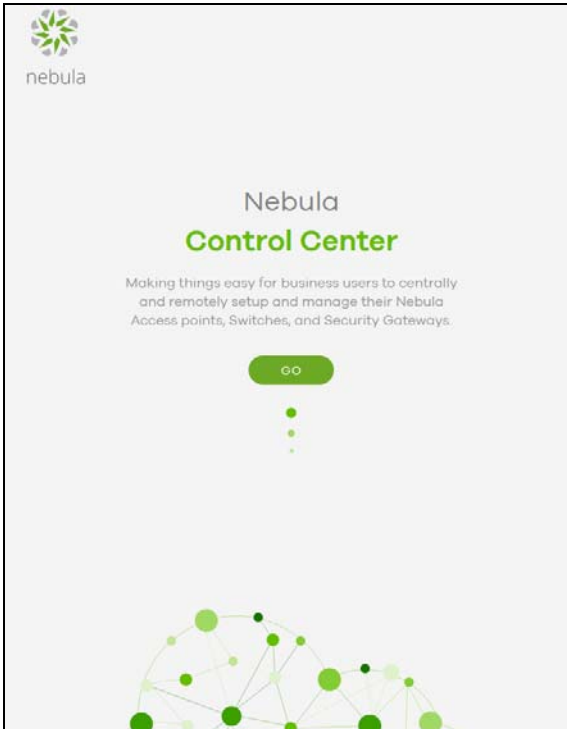
## 2.1 Setup Wizard

- The setup wizard helps you create an organization and site, add devices 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.

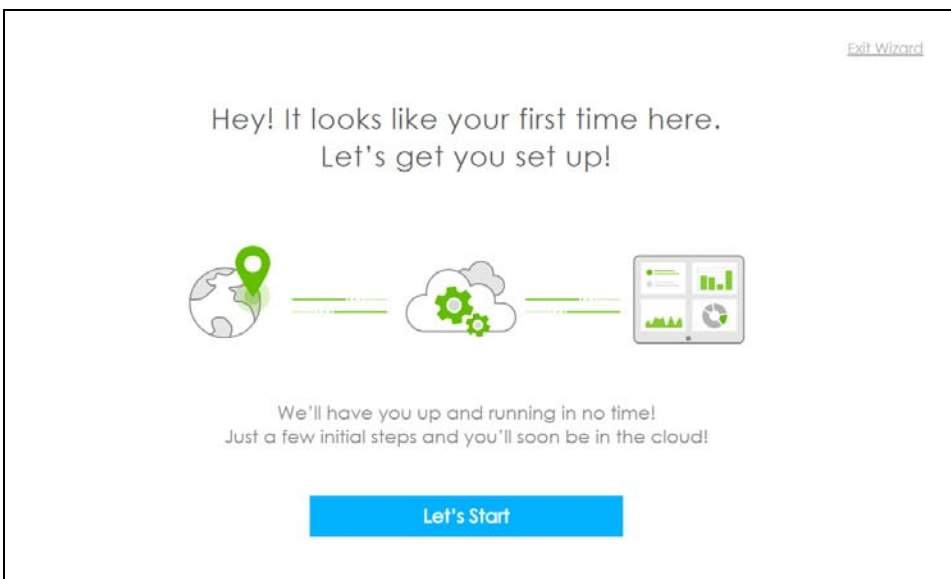


### 2.1.1 Step1: Run the Wizard

- 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 a web-based setup wizard. On the left, a sidebar contains a progress indicator '01' and explanatory text: 'Nebula is organized into Organizations, for example, "YourCompany" or "YourClient", and Sites, for example, "London Branch" or "Factory". You can create as many Organizations and Sites as you need once you're up and running. The country allows us to set the correct time zone for your site and the legal requirements for settings like radio power on access points. Please enter your Organization and Site names and select the correct Country and Time Zone.' The main content area is titled 'First step is to create your Organization and Site' and features a form with the following fields: 'Organization' (text input with a clear 'x' button), 'Site' (text input with a clear 'x' button), 'Country' (dropdown menu showing 'Taiwan'), and 'Timezone' (dropdown menu showing 'Asia - Taipei (UTC +8.0)'). A 'Next' button is located at the bottom center of the form area. An 'Exit Wizard' link is visible in the top right corner.

### 2.1.3 Step 3: Add Your 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 device.

- 2 Click the + **Add** button to register and add the device to the site. You can register multiple devices at a time.
- 3 Click **Next** to proceed.

[Exit Wizard](#)

**02**

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

Serial Number

MAC address

You might just click Next to skip this step.

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

X  
 X

+ Add

Name	MAC	Serial Number
Please click Add button after filling in the MAC address and Serial Number		

Back
Next

## 2.1.4 Step 4: 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 IP address and subnet mask and enable the DHCP server function for this interface.

- 3 Click **Next** to proceed.

[Exit Wizard](#)

**03**

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

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

You might just click Next to skip this step.

### Let's get your WiFi set up

WiFi Name (SSID)

Password (Pre-Shared Key)

VLAN

▲ Set up VLAN interface **Gateway**

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

[Skip WiFi settings](#)

## 2.1.5 Step 5: 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 wireless security, your network is accessible to any wireless 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 IP 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](#)

**04**

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

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

You might just click Next to skip this step.

### Need to set up a Guest WiFi?

WiFi Name (SSID)

Password (Pre-Shared Key)

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

▲ Set up VLAN interface **Gateway**

## 2.1.6 Step 6: Set up the ZTP (Zero Touch Provisioning)

Configure the Zero Touch Provisioning (ZTP) settings to send an activation link to the admin who is in charge of the device management.

Note: This step is necessary only when you have added a USG FLEX device in step 3.

- 1 Enable **VLAN Tag** and configure the **VLAN ID** (1 – 4094) for the WAN port.
- 2 Select **DHCP**, **Static**, or **PPPoE** for the WAN port of the gateway device based on your ISP service.
- 3 Select **I will install USG Flex by myself** to receive an activation email and activation file. If you want another admin to activate the gateway device, enter and select the recipient's **Email Address**.

[Exit Wizard](#)

### WAN Configuration and Zero Touch Provisioning(ZTP)

----- **05**

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.

Model Name: USG FLEX 500 [Show device information](#)

VLAN Tag:

VLAN ID:  (1 - 4094)

WAN Type: DHCP Port: P2

Send ZTP installation file to installer:

I will install USG FLEX by myself.

Email Address

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

## 2.1.7 Step 7: View the Summary

- 1 A summary of the wizard configuration will display after you complete the ZTP registration.
- 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.

[Exit Wizard](#)

Well that's the basics sorted...You're ready to go!

**Organization**  
Zyxel2

Site  
Hsinchu

---

**Nebula Devices**  
1 Device >

**WiFi Name (SSID)**  
SSID1

WiFi Password  
12345678

**Guest WiFi Name (SSID)**  
SSID2

Guest WiFi Password  
12345678

Authentication  
Sign-On with Facebook

**Model Name**  
USG FLEX 500

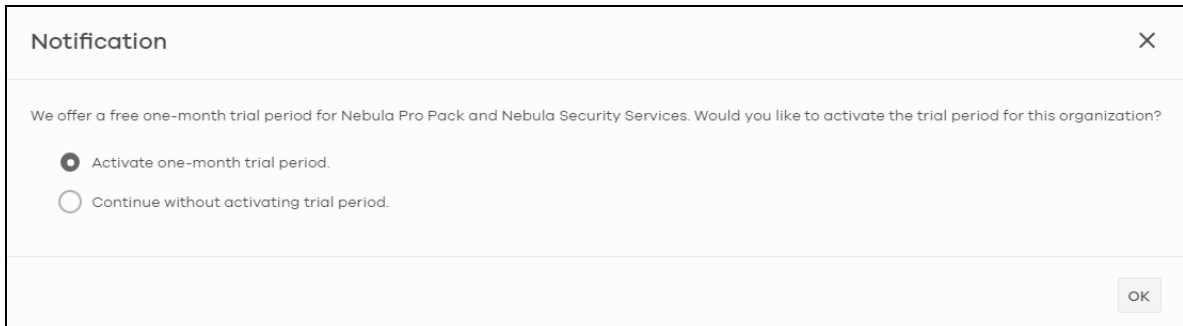
WAN Setting  
WAN Port: P2  
WAN Type: DHCP

Recipient  
thomas.hernandez@zyxel.com.tw

[Go to Nebula Dashboard](#)

## 2.1.8 Step 8: Activate NCC Pro Pack and Security Services Trial Period

- 1 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.
- 2 If you choose to activate the trial period, click **Activate one-month trial period**. NCC will send you an email reminding you to purchase the full license when the trial is close to expiring.



The image shows a notification dialog box with a title bar that says "Notification" and a close button (X) in the top right corner. The main text of the dialog reads: "We offer a free one-month trial period for Nebula Pro Pack and Nebula Security Services. Would you like to activate the trial period for this organization?". Below this text are two radio button options: "Activate one-month trial period." (which is selected) and "Continue without activating trial period.". In the bottom right corner of the dialog, there is an "OK" button.

# CHAPTER 3

## Tutorial

### 3.1 Overview

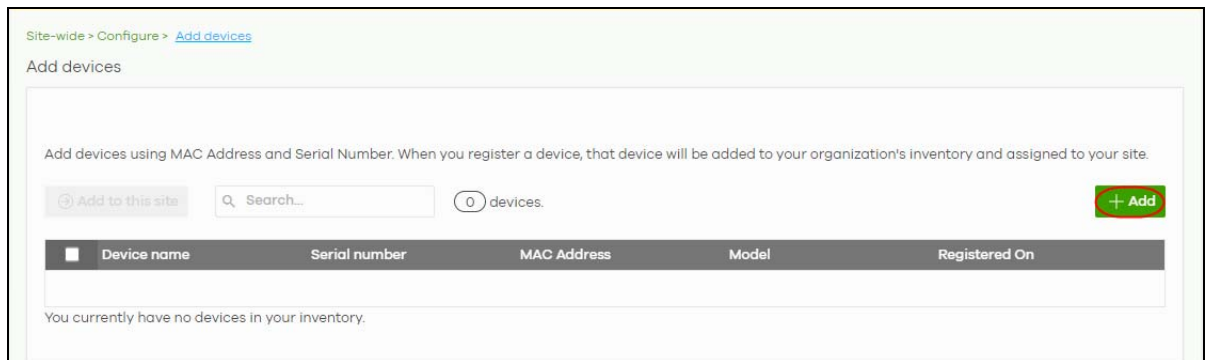
This chapter shows you how to use the NCC's various features.

- [Adding a Device](#)
- [Monitoring a Site](#)
- [Managing a Configuration Template](#)

#### 3.1.1 Adding a Device

This section shows you how to add a security gateway, AP or switch to a selected organization and site on NCC for management.

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



Site-wide > Configure > [Add devices](#)

Add devices

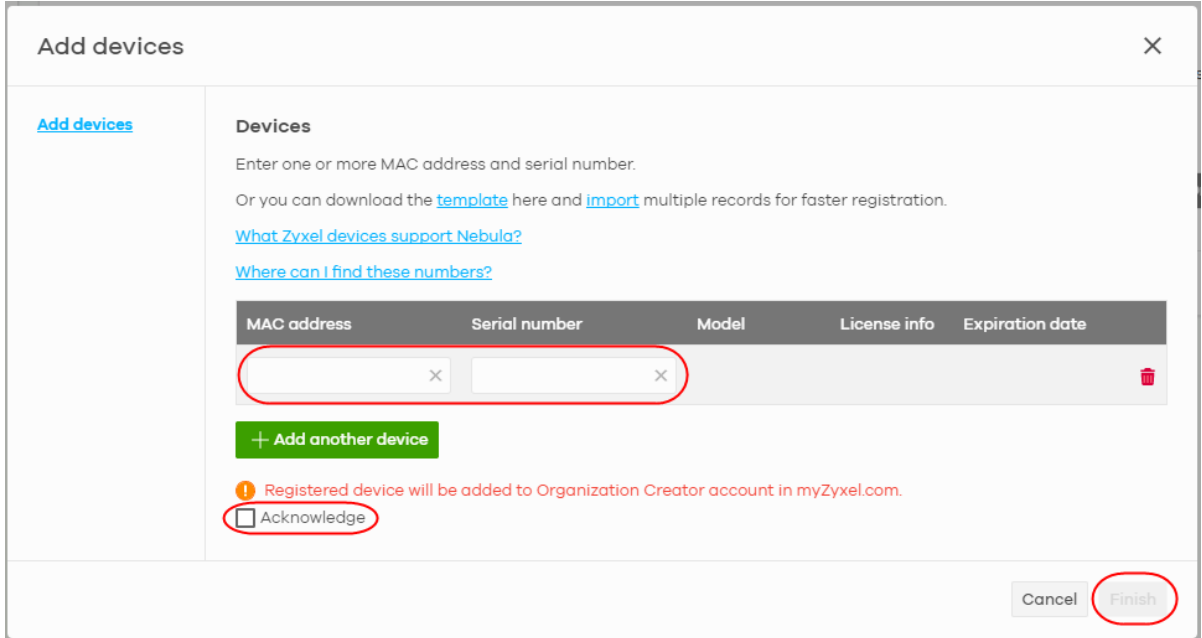
Add devices using MAC Address and Serial Number. When you register a device, that device will be added to your organization's inventory and assigned to your site.

0 devices.

Device name	Serial number	MAC Address	Model	Registered On
-------------	---------------	-------------	-------	---------------

You currently have no devices in your inventory.

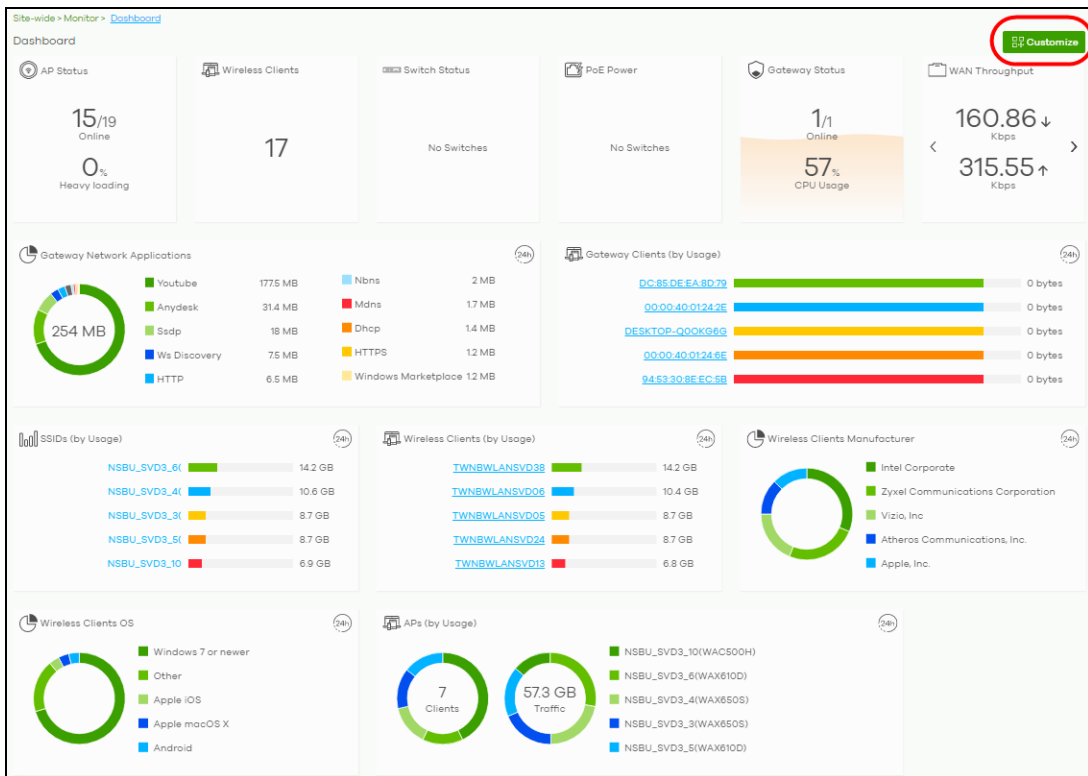
- 2 Enter the **Serial number** and **MAC address** of the device you want to add. Select **Acknowledge** to add the device to the Organization creator's account in myZyvel.com. Then click **Finish** to save the changes.



### 3.1.2 Monitoring a Site

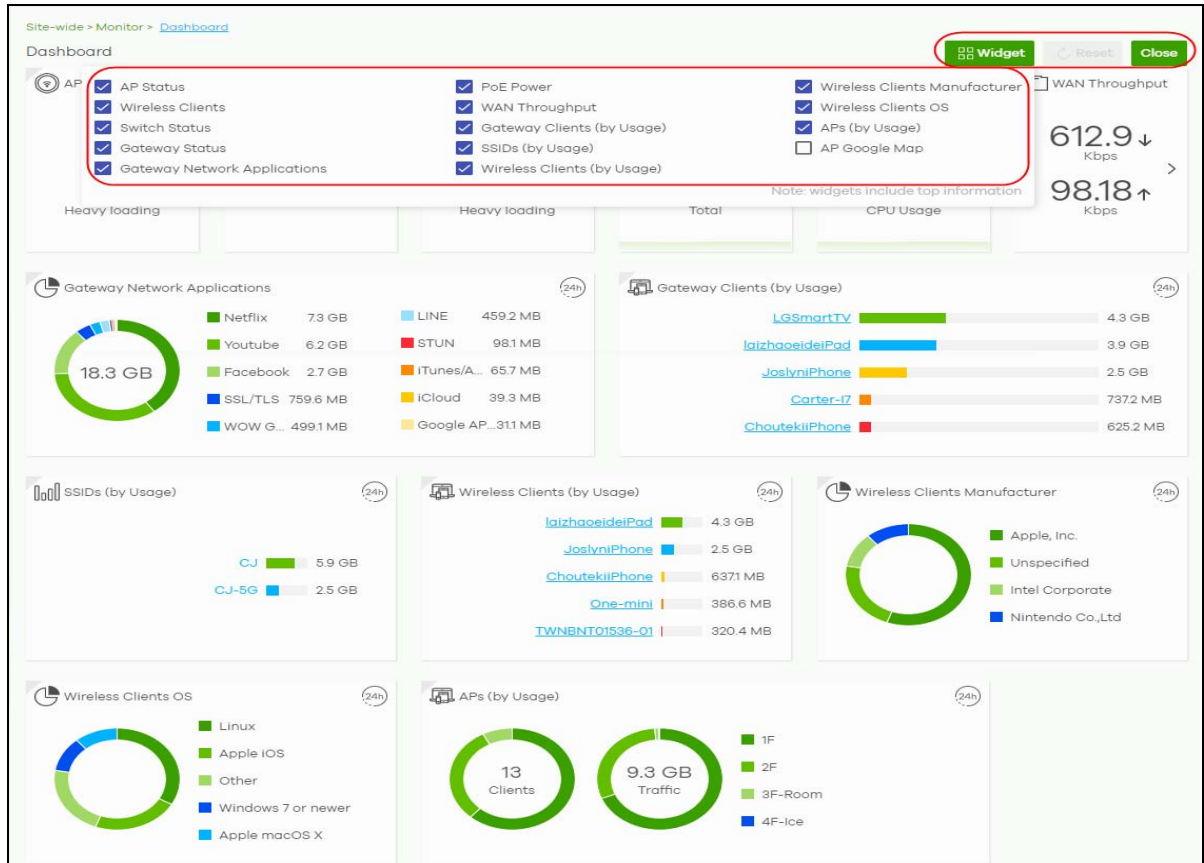
This section shows you how to view and monitor your devices and WiFi/wired networks within a site.

- 1 Go to the **Site-wide > Monitor > Dashboard** screen. Click **Customize** to show the **Widget**, **Reset**, and **Close** buttons.





- Click **Widget** to select which widgets are displayed. Click **Reset** to restore the dashboard back to the default setting. Click **Close** to return to the **Customize** button.



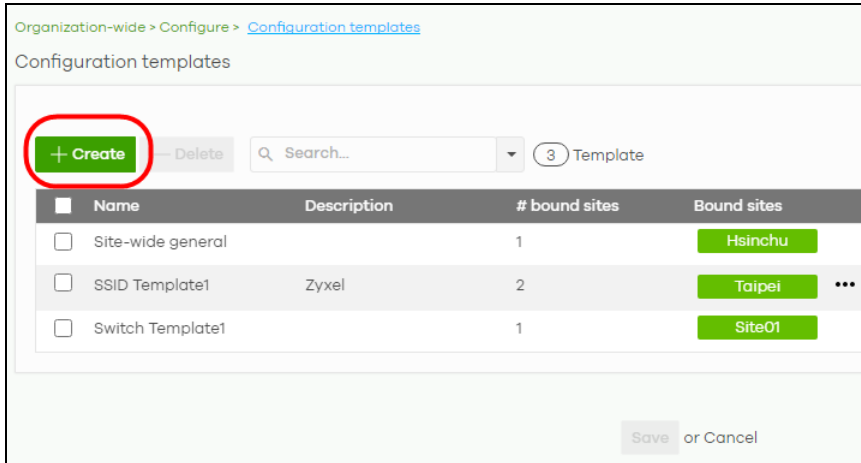
### 3.1.3 Managing a Configuration Template

This section shows you how to use configuration templates to create and manage sites for your organization. Use a configuration template to create a site and then modify the details of the site using a template or enabling the local override configuration.

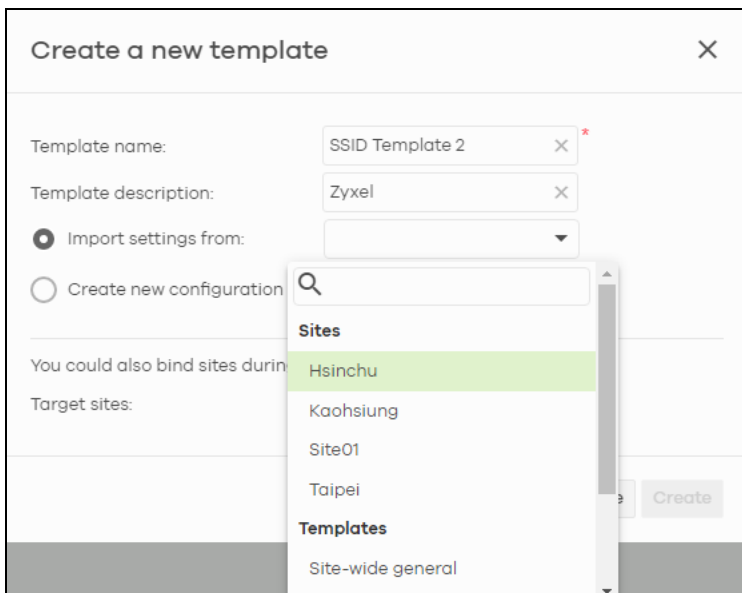
- 1 [Create a Template Site/Setting](#)
- 2 [Apply a Template Setting to a Site](#)
- 3 [Enable the Override site-wide configuration \(Local Override\) Feature](#)

#### 3.1.3.1 Create a Template Site/Setting

- 1 Go to the **Organization-wide > Configure > Configuration Templates** screen. Click **+Create**.



- 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**.



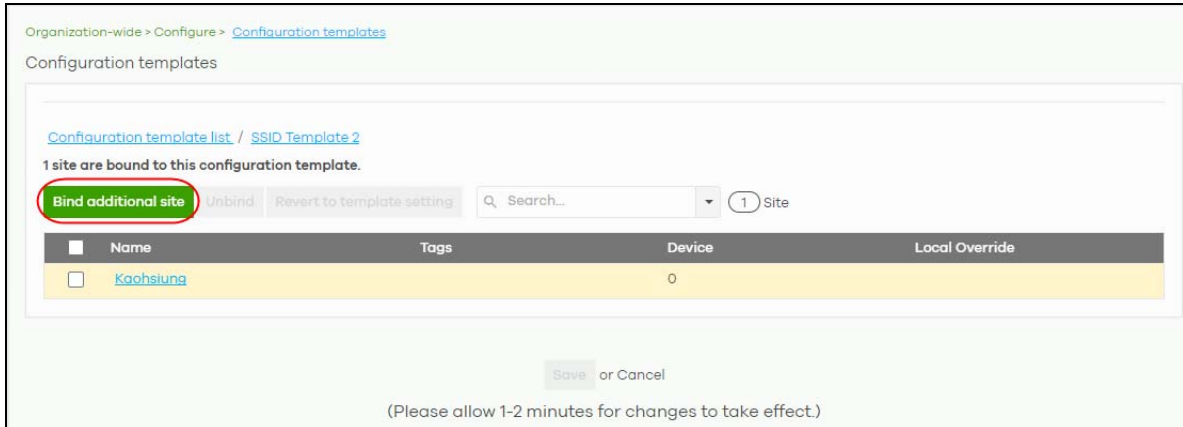
Note: Under **Import settings from**, select a site from **Sites** to copy a site's settings. Under **Import setting from**, select a template from **Templates** to copy a site's site-wide general setting, an AP's SSIDs setting or a switch's port setting.

- Select a site from the **Target sites** drop down list box to apply the template to a site.  
Or, just click **Create** to save the changes.  
If you skip this step, you can apply 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.

If you skip this step, you can apply 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.

<input type="checkbox"/>	Name	Description	# bound sites	Bound sites
<input type="checkbox"/>	Site-wide general		1	Hsinchu
<input checked="" type="checkbox"/>	SSID Template 2	Zyxel	0	
<input type="checkbox"/>	SSID Template1	Zyxel	2	Taipei
<input type="checkbox"/>	SSID Template3		0	
<input type="checkbox"/>	Switch Template1		1	Site01

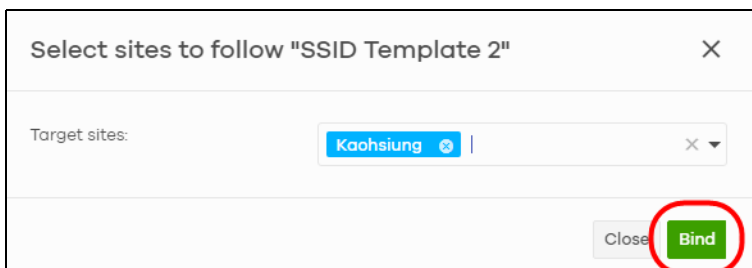
- 4 The following screen appears. Click **Bind additional site** to select the site you want to apply the template to.



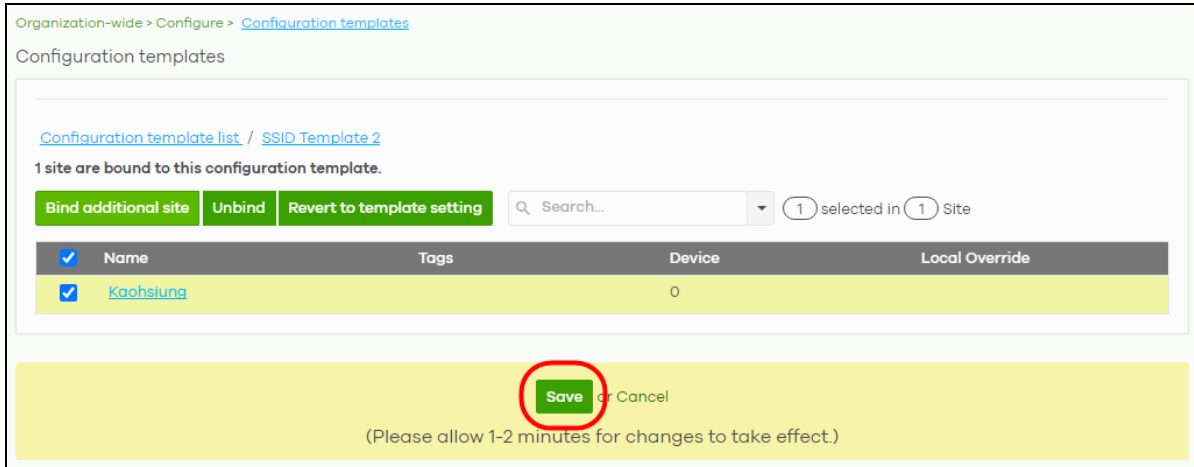
- 5 The following screen appears. Click the **Target sites** drop down list box.



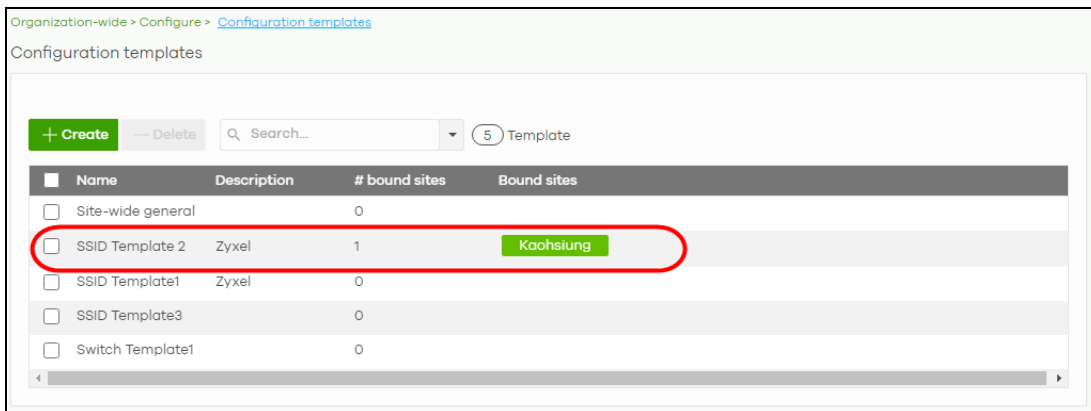
- 6 Select a site from the **Target sites** drop down box list and then click **Bind**.



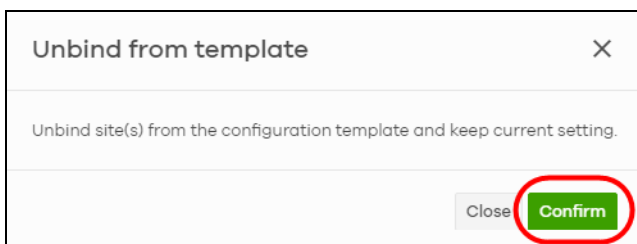
- 7 Click **Save** to save the changes.



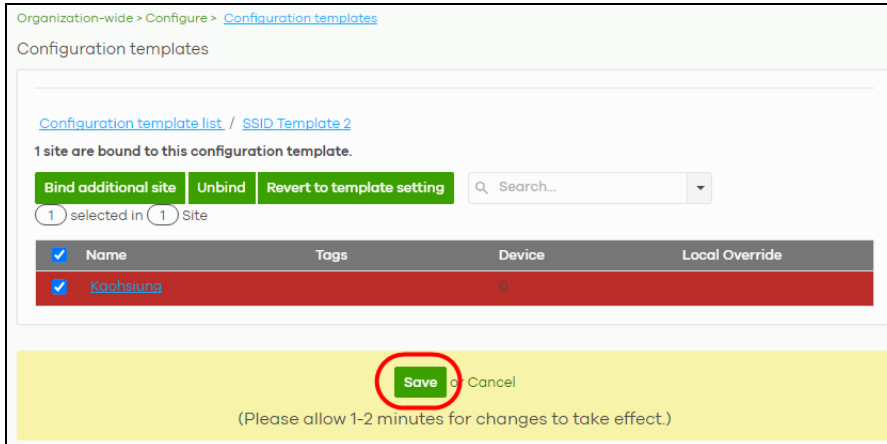
- 8 A configuration template is created as shown on the **Organization-wide > Configure > Configuration template** screen.



- 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.



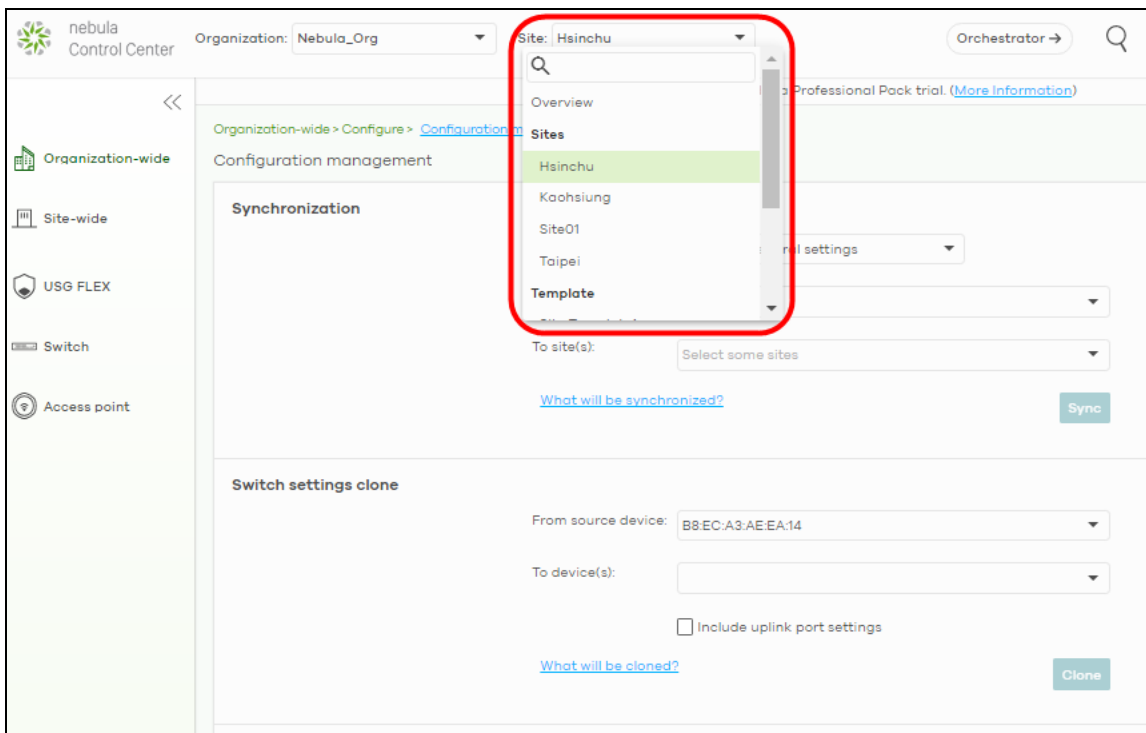
### 3.1.3.2 Apply a Template Setting to a Site

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

- The site-wide general setting includes the device configuration, SNMP and captive portal re-authentication.
- An AP'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: Site-wide general settings

From source site: Site-wide general settings

To site(s): Kaohsiung

[What will be synchronized?](#)

**Switch settings clone**

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

To device(s):

Include uplink port settings

[What will be cloned?](#)

- 3 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: Site-wide general settings

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?](#)

- 4 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: Site-wide general settings

From source site: Hsinchu

To site(s): Kaohsiung

[What will be cloned?](#)

**Switch settings clone**

From source device:

To device(s):

Include uplink port settings

[What will be cloned?](#)

Q

**Sites**

- Kaohsiung
- Site01
- Taipei

## An AP'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:

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 SSIDs 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 SSIDs to. Click **Sync** to save the changes.

Organization-wide > Configure > Configuration management

Configuration management

**Synchronization**

Settings: SSIDs

From source site: Hsinchu

To site(s): Kaohsiung

[What will be](#)

**Switch settings clone**

From source device:

To device(s):

Include uplink port settings

[What will be cloned?](#)

Clone

## A switch's port setting

- 1 Go to the **Organization-wide > Configure > Configuration Management** screen. Under **Switch settings clone**, select the 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: SSIDs

From source site: Hsinchu

To site(s): Kaohsiung

[What will be synchronized?](#)

Sync

**Switch settings clone**

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

To device(s):

Include uplink port settings

[What will be cloned?](#)

Clone

- From the **To device(s)** drop down list box, select the 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: SSIDs

From source site: Hsinchu

To site(s): Kaohsiung

[What will be synchronized?](#) **Sync**

**Switch settings clone**

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

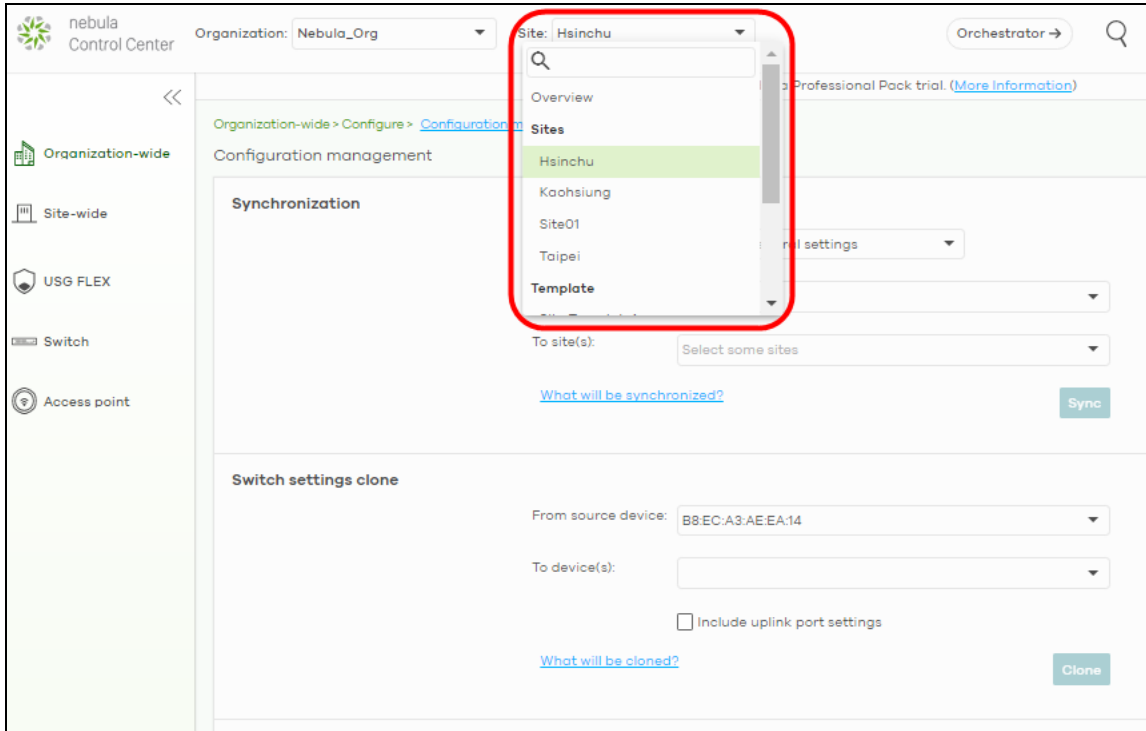
To device(s): [Empty dropdown menu]

Include uplink port settings

[What will be cloned?](#) **Clone**

### 3.1.3.3 Enable the Override site-wide configuration (Local Override) Feature

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. 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 [q](#) page under **Site-wide > Configure** and then select the **Override site-wide configuration** box. The **Configuration** page of a bound site contains a **Override site-wide configuration** box.

Note: If **Override site-wide configuration** is enabled on any of the **Site-wide > Configure > General settings / Alert settings / Firmware management** pages, the **Override site-wide configuration** option in the **Switch** and **Access point** configuration pages will be enabled.

This site is bound to template [Site Template1](#)

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

General settings  Override site-wide configuration

### Site information

Site name: Hsinchu

Gateway type: USG FLEX

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

Configuration template: This site uses the configuration of the template [Site Template1](#) [Unbind](#)

### Device configuration

Local credentials: Username: admin Password: \*\*\*\*\*

Smart guest/VLAN network [Beta](#)  [What is this?](#)

### Captive portal reauthentication

For my AD server users: Every day

For my RADIUS server users: Every day

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

**Override template** [X]

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

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

3 If you go to 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 [Site Template1](#)

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

General settings  Override site-wide configuration

**Site information**

Site name: Hsinchu

Gateway type: USG FLEX

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

Configuration template: This site uses the configuration of the template [Site Template1](#). [Unbind](#)

**Device configuration**

Local credentials: Username: admin, Password: [REDACTED]

Smart guest/VLAN network: [Beta](#)  [What is this?](#)

**Captive portal reauthentication**

For my AD server users: Every day

For my RADIUS server users: Every day

- 4 To verify the local override setting of a site, go to **Organization-wide > Configuration > Configuration template**. The **Local Override** field shows which settings in the template do not apply 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	<input checked="" type="checkbox"/> AP

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

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

- 5 If you decide to use the template setting instead, de-select the **Override site-wide configuration** box on any page under **Site-wide > Configuration**. The following screen appears. Click **Confirm** to continue.

**Revert override** X

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

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

## Overwriting the AP Setting

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

Note: If the local override configuration is enabled on one page, all configuration pages of the device type will be enabled.

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

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

This site is bound to template [Site Template1](#)

Access point > Configure > [SSID overview](#)

SSID overview

Simple mode: **Beta**  [What is this?](#)

**Show All** **Hide disable SSIDs**

No.	1	
<b>Name</b>	SSID1 <input type="text"/>	
<b>Enabled</b>	<input checked="" type="checkbox"/>	
<b>Programmable SSID</b> <b>Beta</b>	<input type="checkbox"/>	
<b>Tagging</b>	<input type="text" value="Tag"/> Enable SSID on APs with any of the specified tags	
<b>Guest Network</b>	<input type="checkbox"/>	
<b>Authentication</b>	<a href="#">Edit</a> WLAN security: Open Sign-in method: Disable Band: Concurrent operation(2.4GHz and 5GHz) VLAN ID: 1 Rate limiting: Unlimited Kb/s/Unlimited Kb/s	
<b>Captive Portal</b>	<a href="#">Edit</a> Theme: Modern	

- 4 If you decide to use the template's setting instead, de-select the **Override switch configuration** box on any page under **Access Point > Configuration**. The following screen appears. Click **Confirm** to continue.

**Revert override**

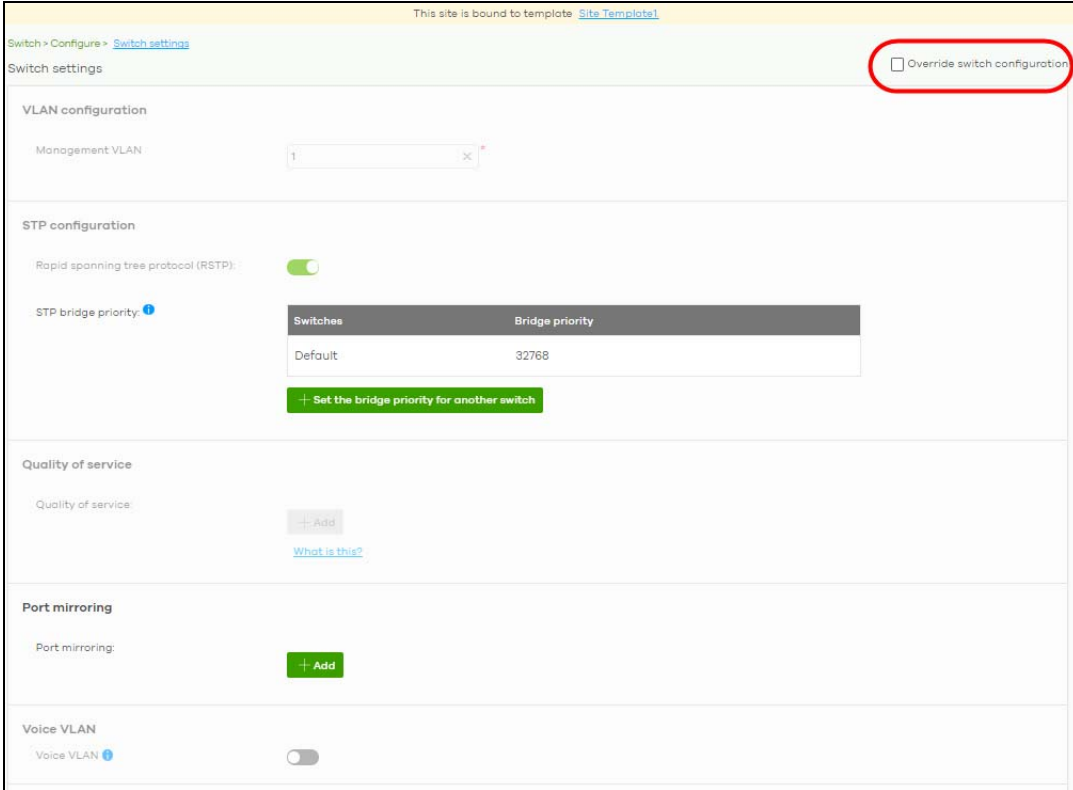
Configuration in this page will follow template Site Template1.  
Please click confirm to continue...

## Overwriting the Switch Setting

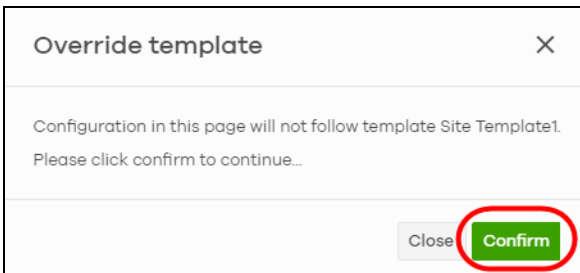
- 1 Go to any page under **Switch > Configure** and then select the **Override switch configuration** box. Every **Configuration** page of a bound site contains a **Override site-wide configuration** box.

Note: If the local override configuration is enabled on one page, all configuration pages of the device type will be enabled.

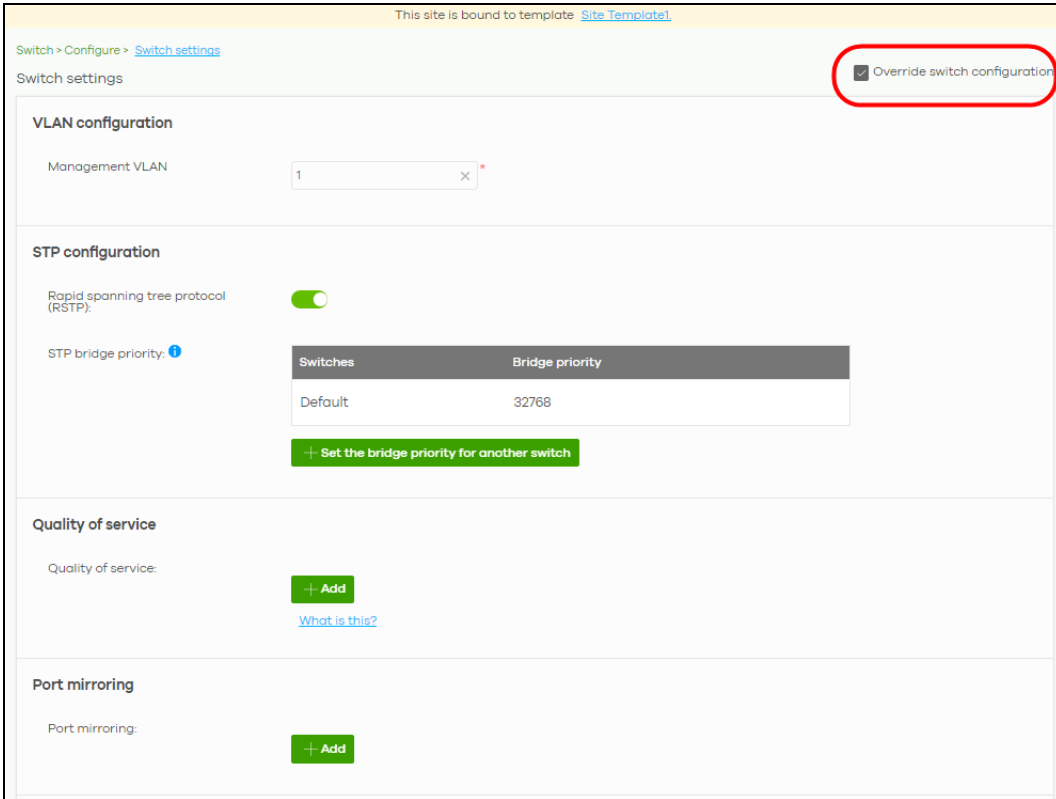




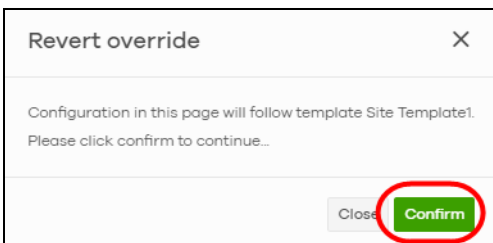
2 The following screen appears. Click **Confirm** to continue.



3 If you go to the **Switch > Configuration > Switch setting** screen, edit **VLAN configuration**, **STP configuration**, **Quality of service**, or **Port mirroring** settings on the following page. Click **Save** to save the changes.



- 4 If you decide to use the template's setting instead, de-select the **Override switch configuration** box on any page under **Switch > Configuration**. The following screen appears. Click **Confirm** to continue.



---

# PART II

## Technical Reference

---

# CHAPTER 4

## MSP

### 4.1 Overview

The **MSP** (Managed Services Provider) menus allow you to view the summary of organizations, transfer licenses between organizations, and change the branding on NCC.

An MSP license that has expired will keep the previous settings in MSP but disable the MSP features.

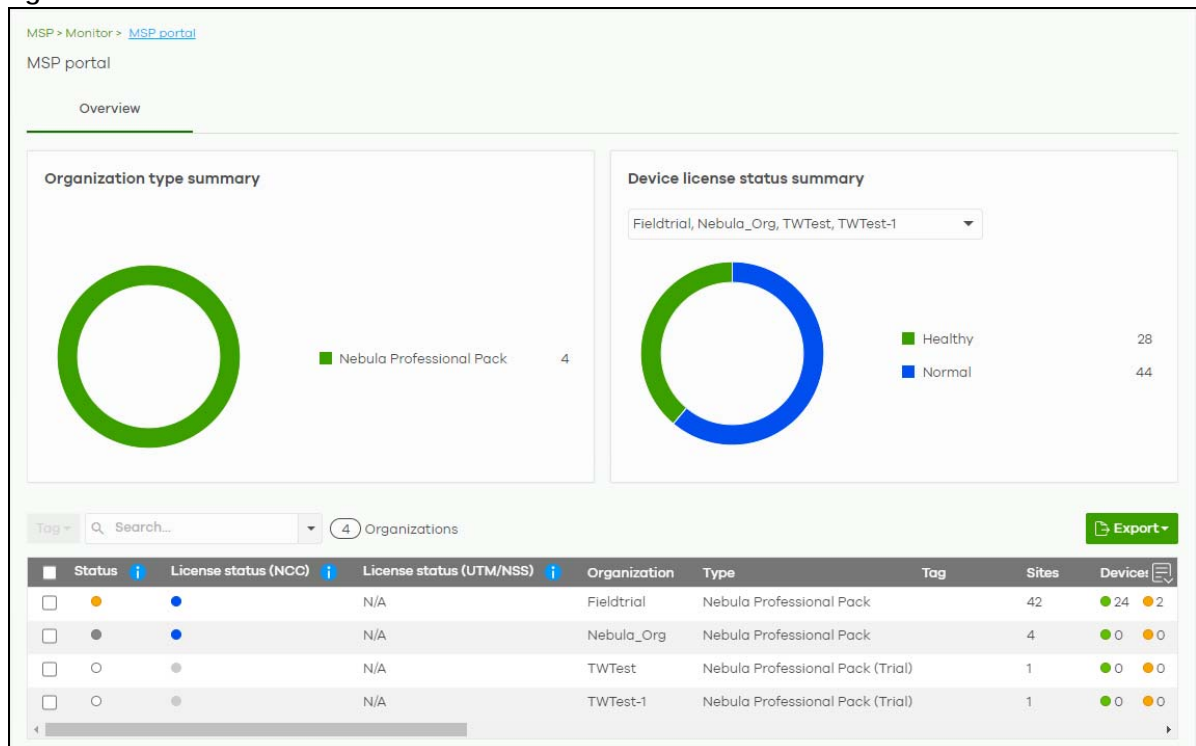
Note: To see these menus, you need an MSP license assigned to your NCC login account.

### 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 19 MSP > Monitor > MSP Portal Screen



The following table describes the labels in this screen.

Table 8 MSP &gt; Monitor &gt; 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 managed devices with NCC 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.
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 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.
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.
Status	<p>This shows the status of devices in the organization.</p> <ul style="list-style-type: none"> <li>• Green: All devices are online and have no alerts.</li> <li>• Orange: Some devices have alerts.</li> <li>• Red: Some devices are offline.</li> <li>• Gray: All devices have been offline for 7 days or more.</li> <li>• White: No devices in this organization.</li> </ul>
License status (NCC)	<p>This shows the license status of devices in the organization.</p> <ul style="list-style-type: none"> <li>• Green: All devices with over 1 year licenses.</li> <li>• Blue: Any device with over 90 days but less than 1 year license together with another device with over 1 year license.</li> <li>• Orange: Any device with license that will expire in 90 days together with another device with over 90 days license.</li> <li>• Red: Any device with an expired license or is unlicensed.</li> <li>• Gray: No devices in this organization.</li> </ul>
License status (UTM/NSS)	<p>This shows the license status of security gateways in the organization.</p> <ul style="list-style-type: none"> <li>• Green: All security gateways with over 1 year licenses.</li> <li>• Blue: Any security gateway with over 90 days but less than 1 year license together with another device with over 1 year license.</li> <li>• Orange: Any security gateway license that will expire in 90 days together with another device with over 90 days license.</li> <li>• Red: Any security gateway with an expired license or is unlicensed.</li> <li>• Gray: No security gateways in this organization.</li> </ul>

Table 8 MSP &gt; Monitor &gt; MSP Portal (continued)

LABEL	DESCRIPTION
Organization	This shows the descriptive name of the organization.
Type	This shows your NCC version type.
Tag	This shows the tag name assigned to this organization. Otherwise, the organization does not have a tag.
Sites	This shows the number of sites belonging to this organization.
Devices online	This shows the number of Nebula devices in this organization which are online (green), have recently had alerts (orange), recently went offline (red), or have been offline for more than 6 days (gray).
AP	This shows the number of Nebula APs connected to the sites in this organization.
SW	This shows the number of Nebula switches connected to the sites in this organization.
GW	This shows the number of Nebula security gateways 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, 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.
Next NSS/UTM license expiration date	For example, if you have two devices in the organization: <ul style="list-style-type: none"> <li>• Device 1 is with NCC license expiration date on 2021/10/1</li> <li>• Device 2 is with NCC license expiration date on 2021/11/1</li> </ul> This field will show the nearest expiration date '2021/10/1'.
# 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/NSS/UTM/RAP license	This shows the number of unused NCC (Nebula Control Center) / NSS (Nebula Security Service) / UTM (Unified Threat Management) / RAP (Remote Access Point) licenses in this organization.
Export	Click this button to save the MSP Portal list as a CSV or XML file to your computer.

## 4.3 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 20** MSP > Configure > MSP branding

The following table describes the labels in this screen.

**Table 9** NCC MSP Portal > 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.
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	

Table 9 NCC MSP Portal &gt; MSP Branding (continued)

LABEL	DESCRIPTION
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 privileges will still see the hidden default screen section.
Customized MSP support contact information	Create your own support contact information. Up to 1000 characters are allowed for this field including special characters inside the square quotes [~!@#\$\$%^&*()_+{} :"<>?-=[\];',./].
Apply to	<p>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.</p> <p>Select <b>Custom</b> to choose which Nebula Professional Pack organization to apply the support contact information.</p> <p>Select <b>None</b> if you only wish to save the settings but will not apply it yet.</p>

## 4.4 Admins & Teams

The Admins & Groups 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.

### 4.4.0.1 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.

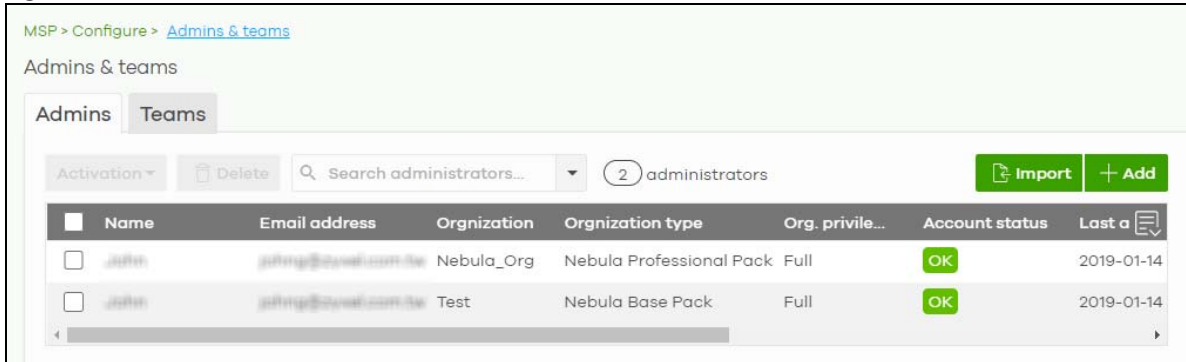
Example, account User1 has four different privilege levels configured for organization Org1 on the four screens above: None, Read-Only, Full, Full (Delegate). User1's final privilege level for Org1 is Full (Delegate).

### 4.4.1 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 21 MSP &gt; Configure &gt; Admins &amp; teams &gt; Admins




The following table describes the labels in this screen.

Table 10 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="495 949 1125 1272" style="border: 1px solid black; padding: 5px; margin: 5px 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: 10px; 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.
Org. privilege	This shows the privileges the administrator has within the specified organization. <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 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>

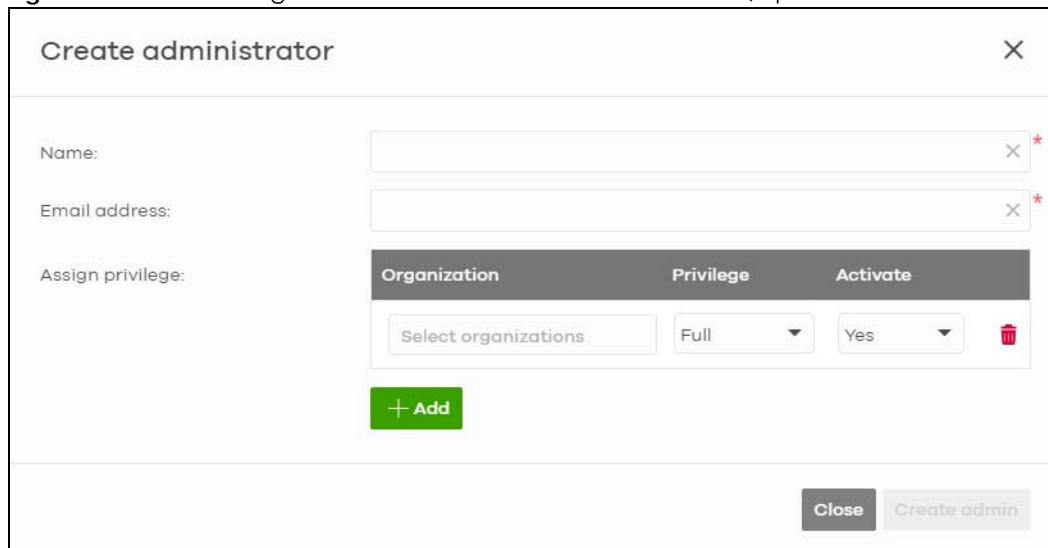
Table 10 MSP &gt; Configure &gt; Admins &amp; teams &gt; Admins (continued)

LABEL	DESCRIPTION
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.

#### 4.4.1.1 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 22 MSP &gt; Configure &gt; Admins &amp; teams &gt; Admins: Create/Update administrator




The following table describes the labels in this screen.

Table 11 MSP &gt; Configure &gt; Administrator: Create/Update administrator

LABEL	DESCRIPTION
Name	Enter a descriptive name for the administrator account.
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.

Table 11 MSP &gt; Configure &gt; Administrator: Create/Update administrator (continued)

LABEL	DESCRIPTION
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 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 organizations.
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.

## 4.4.2 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 23 MSP &gt; Configure &gt; Admins &amp; teams &gt; Teams




The following table describes the labels in this screen.

Table 12 MSP &gt; Configure &gt; Admins &amp; teams &gt; Teams

LABEL	DESCRIPTION
Delete	Click this button to remove the selected teams.
Search	Specify your desired filter criteria to filter the list of teams.
N teams	This shows the number of teams (N) in the list.
Add	Click this button to create a new administrator team.
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 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.

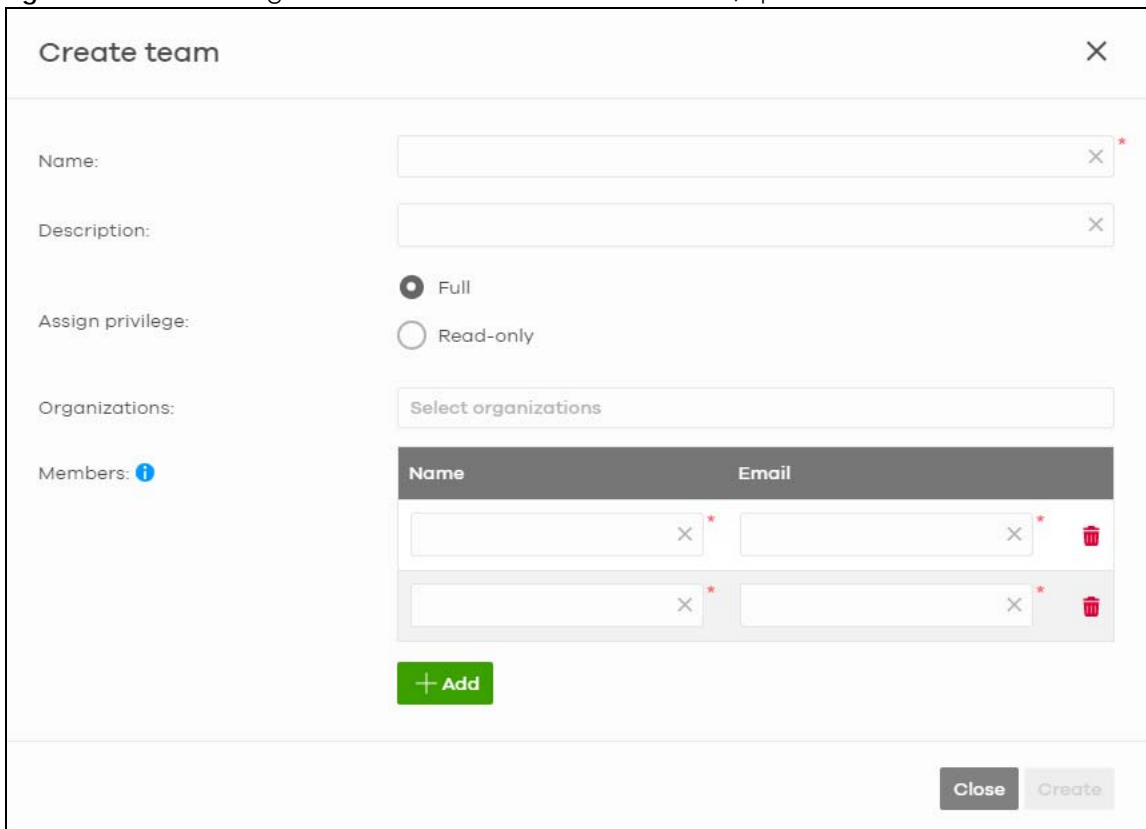
Table 12 MSP &gt; Configure &gt; Admins &amp; teams &gt; Teams (continued)

LABEL	DESCRIPTION
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.

#### 4.4.2.1 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 24 MSP &gt; Configure &gt; Admins &amp; teams &gt; Teams: Create/Update Team



**Create team**
✕

---

Name:  ✕ \*

Description:  ✕

Assign privilege:

Full

Read-only

Organizations:

Members: i

Name	Email
<input style="width: 90%;" type="text"/> ✕ *	<input style="width: 90%;" type="text"/> ✕ * <span style="color: red;">✖</span>
<input style="width: 90%;" type="text"/> ✕ *	<input style="width: 90%;" type="text"/> ✕ * <span style="color: red;">✖</span>

+ Add


Close
Create

The following table describes the labels in this screen.

Table 13 Group-wide &gt; Configure &gt; Administrator: Create/Update Team

LABEL	DESCRIPTION
Name	Enter a descriptive name for the team.
Email address	Enter a description of the team, for example their role or membership.

Table 13 Group-wide &gt; Configure &gt; Administrator: Create/Update Team (continued)

LABEL	DESCRIPTION
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 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.
Members	
Name	Enter a descriptive name for the administrator account.
Email address	Enter the email address of the administrator account, which is used to log into the NCC.
	Click the remove icon to delete the current set of admin privileges.
Add	Add another NCC account to this team.
Close	Click this button to exit this screen without saving.
Create/Update	Click this button to save your changes and close the screen.

### 4.4.3 Cross-org synchronization

The Cross-org synchronization screen allows you to copy settings or a site from one organization to another.

#### 4.4.3.1 Cross-Org setting sync

Cross-org sync copies the following items from one organization to another organization:

- Organization-wide settings
- Administrators
- Cloud Authentication accounts (Users and MAC)
- Configuration templates

Your account must have **owner** or **organization-full** privileges in both source and destination organizations. When copying organization-wide settings, the following settings will not be overwritten if they are already configured in the destination organization:

- **Organization-wide > 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.

### 4.4.3.2 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.

### 4.4.3.3 Cross-org synchronization Screen

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

**Figure 25** MSP > Configure > Cross-org synchronization

The following table describes the labels in this screen.

Table 14 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 setting sync	
From source organization	Select the organization to copy settings from.

Table 14 MSP &gt; Configure &gt; Cross-org synchronization (continued)

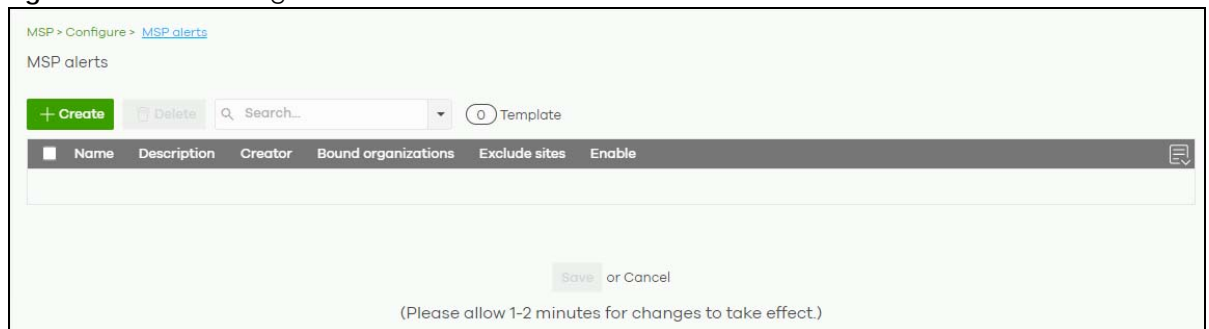
LABEL	DESCRIPTION
Org. setting	Select the settings that you want to copy from the source to the destination organization. Select <b>All org-wide settings</b> to copy everything.
To dest. organization	Select the organization to copy settings to.
Sync	Click this to copy the selected settings from the source to the destination organization.
Cross-Org site clone	
From source organization	Select the organization to copy sites from, and then select one or more sites. Select <b>All sites</b> to copy all sites from the source to the destination organization.
To dest. organization	Select the organization to copy the selected sites to.
Clone	Click this to copy the selected sites from the source to the destination organization.

## 4.5 MSP Alerts

The MSP administrator can configure **MSP alerts** to monitor devices for unexpected events (for example, online/offline events). This screen will list the alert templates you have created. See [Section 4.5.1 on page 76](#) for details on creating an alert template.

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

Figure 26 MSP &gt; Configure &gt; MSP alerts



The following table describes the labels in this screen.

Table 15 MSP &gt; Configure &gt; MSP alerts

LABEL	DESCRIPTION
+ Create	Click this button to add a new alert template (see <a href="#">Section 4.5.1 on page 76</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.

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

LABEL	DESCRIPTION
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.	

## 4.5.1 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 alerts > 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 27 MSP > Configure > MSP alerts > Create/Update alert

**Create alert**
✕

---

**General**

Template name

Description

Email recipient ?

Apply to   
 All organizations   
 Select organizations

Exclude sites   
  + Add to exclude list

Enable

---

**System alerts** ?

Wireless   
  minutes after AP goes offline   
+ Show additional recipients

Switches   
  minutes after Switches goes offline   
+ Show additional recipients

minutes  goes down   
+ Show additional recipients

Security gateway   
  minutes after the gateway goes offline   
+ Show additional recipients

Any DHCP lease pool is exhausted   
+ Show additional recipients

A VPN connection is established or disconnected   
+ Show additional recipients

WAN connectivity status changed   
+ Show additional recipients

Other   
 Configuration settings are changed   
+ Show additional recipients

---

**Security alerts**

CDR containment ?   
 Email to receive containment alerts   
+ Show additional recipients

Close
Create

The following table describes the labels in this screen.

Table 16 MSP > Configure > MSP alerts > Create/Update alert

LABEL	DESCRIPTION
General	
Template name	Enter a descriptive name for the alert template (up to 64 alphanumeric characters including spaces).

Table 16 MSP &gt; Configure &gt; MSP alerts &gt; Create/Update alert (continued)

LABEL	DESCRIPTION
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 3 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.
Enable	Click this to activate the alert template.
System alerts	
Notification Type	<p>For each alert, you can set how to receive alert notifications:</p> <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 NCC 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 AP 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	<p>Specify how long in minutes the NCC waits before generating and sending an alert when the following events occur:</p> <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>
Other alerts	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.

# CHAPTER 5

## Group-wide

### 5.1 Introduction

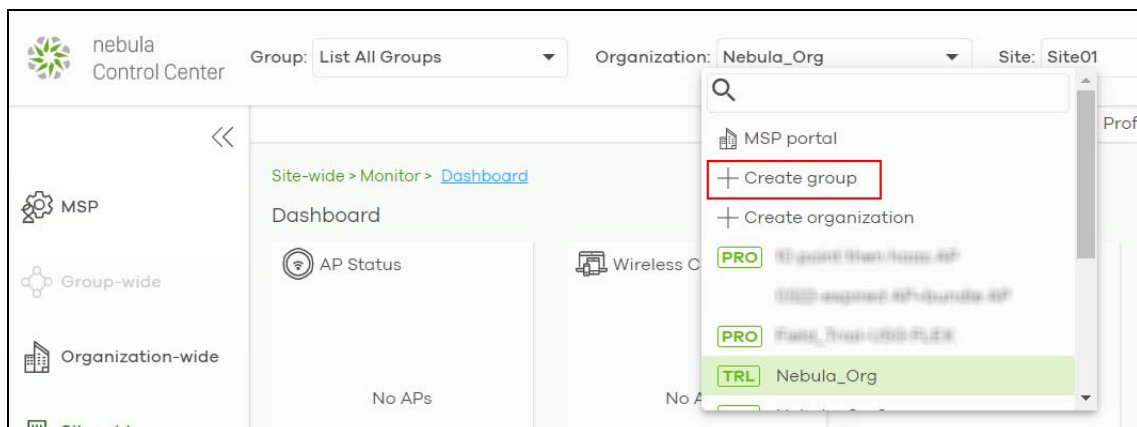
This chapter discusses the menus that you can use to monitor and manage your groups settings.

A group is a collection of one or more organizations. Groups allow you to view and management 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 on 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 license. Then click **OK**.

**Create group** [X]

Group name: Test Group [X]

Group member: test TestOrg2

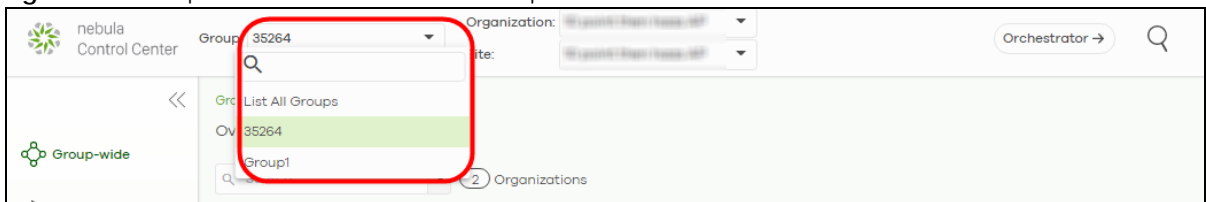
Note: You could select organizations own by you to join Group.

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 28** Group > Monitor > Overview: Group



## 5.2 Monitor

The **Group** menus allow you to monitor and configure groups 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 29** 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

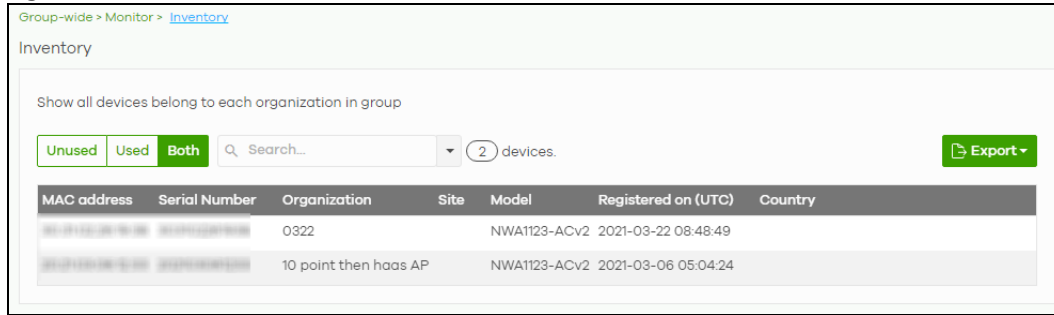
The following table describes the labels in this screen.

Table 17 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 devices in the organization. <ul style="list-style-type: none"> <li>• Green: All devices are online and have no alerts.</li> <li>• Amber: One or more devices have alerts.</li> <li>• Red: One or more devices are offline.</li> <li>• Gray: All devices have been offline for 7 days or more.</li> <li>• White: No 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 webstore or a third-party, 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 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 devices in the organization that have one of the following statuses: <ul style="list-style-type: none"> <li>• Green: The device is online and has no alerts.</li> <li>• Amber: The device has alerts.</li> <li>• Red: The device has been offline for less than 7 days.</li> <li>• Gray: The device has been offline for 7 days or more.</li> </ul>
NAP	This shows the number of NAP series APs in the organization.
NSW	This shows the number of NSW series switches in the organization.
NSG	This shows the number of NSG and USG FLEX series security gateways connected to the sites in this organization.

## 5.2.2 Inventory

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

**Figure 30** Group-wide > Monitor > Inventory

The following table describes the labels in this screen.

**Table 18** Group-wide > Monitor > Inventory

LABEL	DESCRIPTION
Unused	Click this button to show the devices which are not assigned to a site yet.
Used	Click this button to show the devices which are assigned to a site.
Both	Click this button to show all 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 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 devices in the list.
Export	Click this button to save the device list as a CSV or XML file to your computer.
MAC address	This shows the MAC address of the device. Click on the MAC address to view the device details page.
Serial number	This shows the serial number of the device.
Organization	This shows the organization of the device.
Site	This shows the name of the site to which the device is connected.
Model	This shows the model number of the device.
Registered on (UTC)	This shows the date and time that the device was registered at the NCC.
Country	This shows the country where the 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 new ones.

Figure 31 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</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</del> ...		Added, Organizati...
2021-03-23 03:28:51	svd nsbu	Administrator	Added <del>Admin</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</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 19 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 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.
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 32** 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 20** Group-wide > Configure > Settings

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



Table 20 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 Configuring Org-to-Org VPN

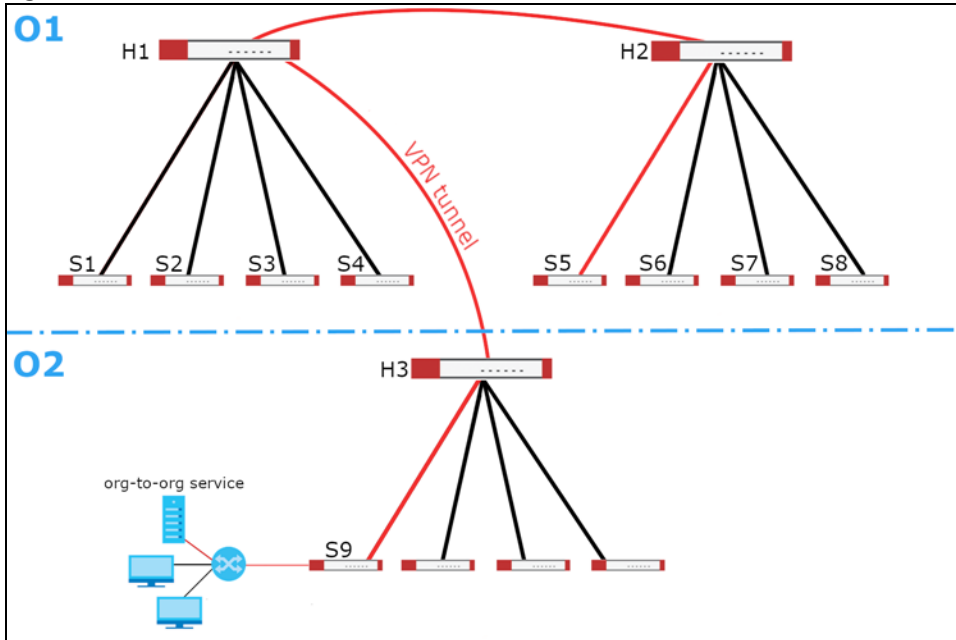
Follow the steps below to configure Org-to-Org VPN in the group.

- 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 33](#) shows organization **O1** with 2 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 device behind **S5** wants to access the server behind **S9**, traffic will pass through its hub **H2** and then to **H1** and **H3**.

Figure 33 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 34 Group-wide > Configure > Org-to-Org VPN

The screenshot shows the 'Org-to-Org VPN' configuration page. At the top, there is a breadcrumb: 'Group-wide > Configure > Org-to-Org VPN'. Below it, the page title is 'Org-to-Org VPN'. The configuration includes:

- Reserved IP Address Pool:** A dropdown menu showing '10.255.255.0/24'.
- AutoVPN:** A section with a toggle for 'Hub to Hub VPN' which is turned on (green).
- Organization:** A table with one entry: 'Hub'.
- Service:** A table with columns for 'Organization', 'FQDN', and 'IP Address'. There is a '+ Org-to-Org Service' button below it.

At the bottom, there is a yellow bar with a 'Save or Cancel' button and a note: '(Please allow 1-2 minutes for changes to take effect.)'

The following table describes the labels in this screen.

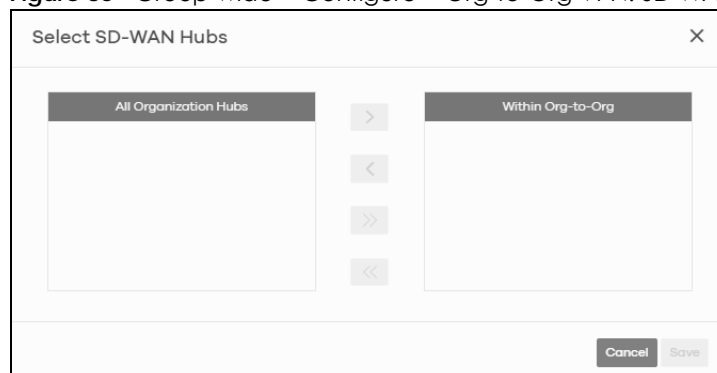
Table 21 Group-wide > Configure > Org-to-Org VPN

LABEL	DESCRIPTION
Reserved IP Address Pool	Specify the IP addresses that devices uses 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 devices behind them are given access.
IP Address	This displays the IP address of the network service which security gateway devices and 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 35 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 22 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 36 Group-wide > Configure > Org-to-Org VPN: Service

The following table describes the labels in this screen.

Table 23 Group-wide > Configure > Org-to-Org VPN: Service

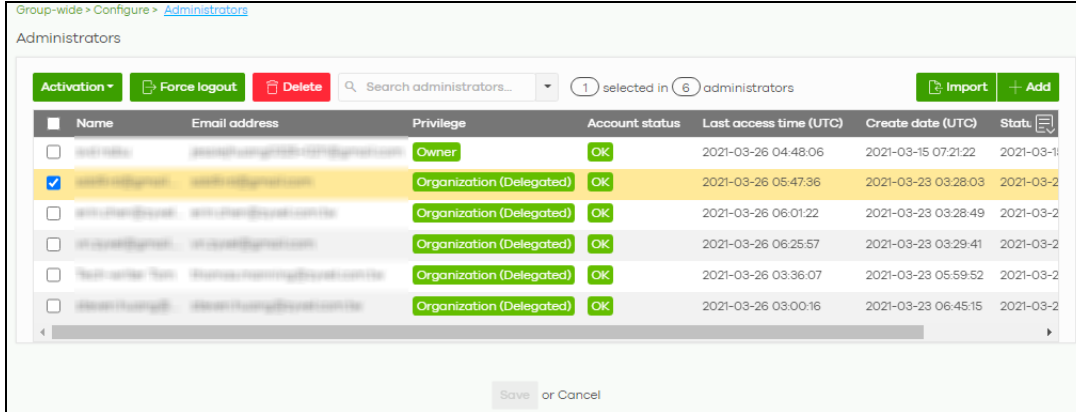
LABEL	DESCRIPTION
Organization	Select the organization which the service you want to add is linked to.
FQDN	Type the Fully-Qualified Domain Name (FQDN) associated with the service.  An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw 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 37 Group-wide > Configure > Administrators




The following table describes the labels in this screen.

Table 24 Group-wide > Configure > Administrator

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="495 1039 1128 1365" style="border: 1px solid black; padding: 5px; margin: 5px 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. See <a href="#">Section 5.3.3.1 on page 90</a> .
Name	This shows the name of the administrator account.
Email address	This shows the email address of the administrator account.
Privilege	This shows the privileges the administrator has within all organizations in the group.  <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 devices in the organization.  <b>Read-only:</b> the administrator account has no write access to the organization, but can be a site administrator.  <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: <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>

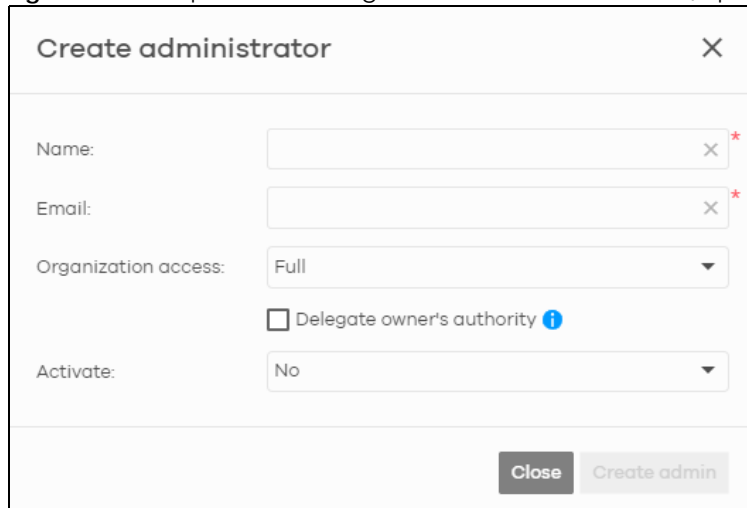
Table 24 Group-wide &gt; Configure &gt; Administrator (continued)

LABEL	DESCRIPTION
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 in 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 > Administrator** 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 38 Group-wide &gt; Configure &gt; Administrator: Create/Update administrator



The following table describes the labels in this screen.

Table 25 Group-wide &gt; Configure &gt; 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 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 devices in the organization. <b>Read-only:</b> the administrator account has no write access to the organization, but can be a site administrator.

Table 25 Group-wide &gt; Configure &gt; Administrator: Create/Update administrator (continued)

LABEL	DESCRIPTION
Delegate owner's authority	<p>This setting is only available when <b>Organization access</b> is set to <b>Full</b>.</p> <p>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:</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>
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, devices, accounts, licenses, and VPN members for the organization.

### 6.2 Monitor

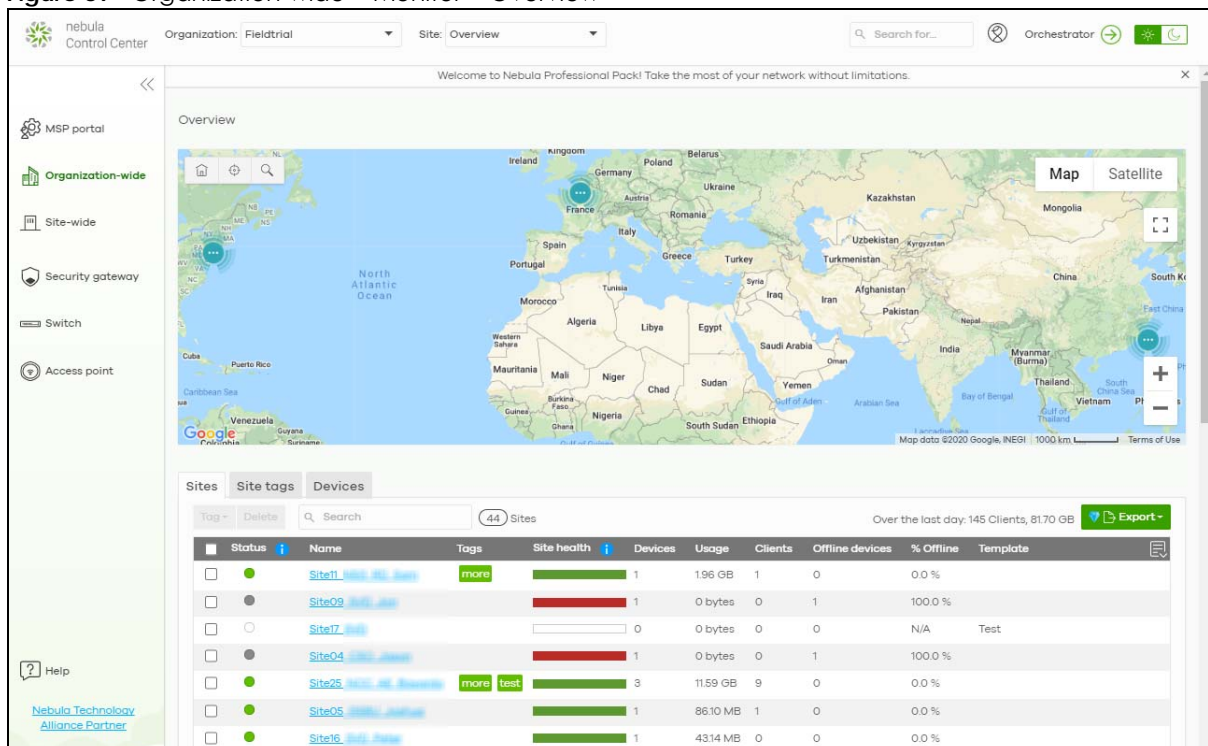
Use the **Monitor** menus to check the site and device information and change logs for the selected organization.

#### 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 devices for the selected organization.

Click **Organization-wide > Monitor > Overview** to access this screen.

**Figure 39** 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 40** 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 26** 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 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 devices in the site. <ul style="list-style-type: none"> <li>Green: All devices are online and have no alerts.</li> <li>Amber: Some devices have alerts.</li> <li>Red: Some devices are offline.</li> <li>Gray: All devices have been offline for 7 days or more.</li> <li>White: No 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 26 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 off-line.
	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 41 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	●	more	7.93 GB
10	5	0.0 %	0	0	1	●	test	7.93 GB

The following table describes the labels in this screen.

Table 27 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 devices in sites with the specified tag. <ul style="list-style-type: none"> <li>Green: All devices are online and have no alerts.</li> <li>Amber: Some devices have alerts.</li> <li>Red: Some devices are offline.</li> <li>Gray: All devices have been offline for 7 days or more.</li> <li>White: No 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 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 devices which are connected to the sites in the selected organization.

**Figure 42** 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	Green		0 bytes
0	B8EC:A3:B4:CC:67	NSG50	B8.EC:A3.B4:CC:67	Site09	Red		0 bytes
0	B8EC:A3:B4:CF:B5	NSG50	B8.EC:A3.B4:CF:B5	Site04	Red		0 bytes
9	8CE2B05C01FE	NSG50	Home GW	Site25	Green		0 bytes
0	B8EC:A3:B4:CD:34	NSW200-28P	Office NSW200	Site25	Green		0 bytes
3	B8B8F31A4675	NAP102	OfficeNAP102-MESH	Site25	Green		0 bytes
5	40219784D713	NAP102	HomeNAP102	Site25	Green	Home	2.61 GB
9	B8EC:A3:B4:7F:4D	NSW100-10P	Home NSW100	Site25	Green		2.69 GB
1	B8EC:A3:B4:CD:87	NSG50	B8.EC:A3.B4:CD:87	Site05	Green		0 bytes
0	B8EC:A3:B4:CC:43	NSG50	B8.EC:A3.B4:CC:43	Site16	Red		0 bytes

The following table describes the labels in this screen.

**Table 28** Organization-wide > Monitor > Overview: Devices

LABEL	DESCRIPTION
Search	Enter a key word as the filter criteria to filter the list of connected 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 device list as a CSV or XML file to your computer.
Status	This shows the status of the device. <ul style="list-style-type: none"> <li>Green: The device is online.</li> <li>Amber: The device recently had alerts.</li> <li>Red: The device was recently offline.</li> <li>Gray: The device has been offline line for more than 6 days.</li> </ul>
Model	This shows the model number of the device.
Name	This shows the descriptive name of the device.
Site	This shows the name of the site to which the device is connected.
MAC address	This shows the MAC address of the device.
Tag	This shows the user-specified tag for the device.
Client	This shows the number of the clients which are currently connected to the device.
Usage	This shows the amount of data consumed by the device.
Serial number	This shows the serial number of the device.

Table 28 Organization-wide > Monitor > Overview: Devices (continued)

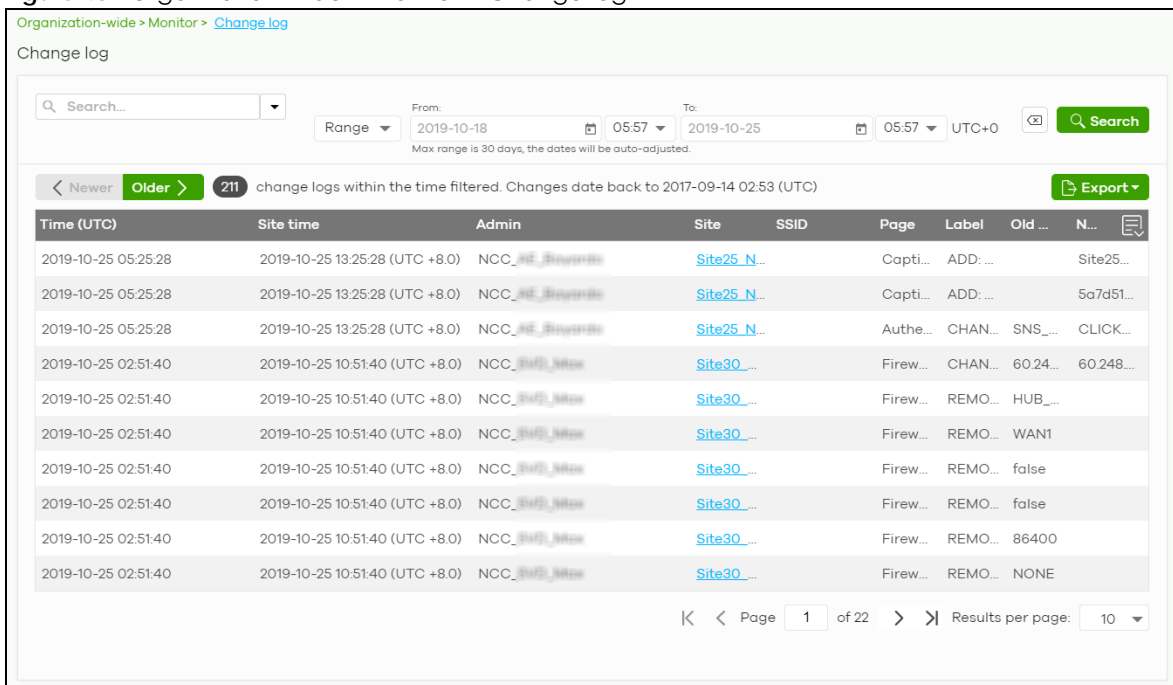
LABEL	DESCRIPTION
Configuration status	This shows whether the configuration on the device is up-to-date.
Connectivity	This shows the device connection status.  The red time slot indicates the connection to the NCC is down, and the green time slot indicates the connection is up. Move the cursor over a time slot to see the actual date and time when a device is connected or disconnected.
Public IP	This shows the global (WAN) IP address of the 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 43 Organization-wide > Monitor > Change log



The following table describes the labels in this screen.

Table 29 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 29 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 device, change organization general settings, and manage licenses, user accounts, administrator accounts or VPN members in the organization.

### 6.3.1 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 134](#)), you can select to bind the new site to the specified template.

- 3 Choose the time zone of the site's location.
- 4 Search and select the name of the registered device that is to be added to this site. If there is no registered Nebula device in the organization, you can click **Register** to claim one.
- 5 Click **Create site** to add the new site to your organization.

**Figure 44** Organization-wide > Configure > Create Site

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

Create site

Site name:

Configuration:

Default configuration

Clone from

Bind to template

You can create and manage templates from [here](#)

Local time zone:

Devices:

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

1 selected in 2 devices.

<input type="checkbox"/>	Device name	Serial Number	MAC address	Model
<input checked="" type="checkbox"/>	NSG50	1778-27000001	9C:43:8C:9C:02:76	NSG50
<input type="checkbox"/>	NSG50	1778-27000002	9C:43:8C:9C:02:76	NSG50

## 6.3.2 License & Inventory

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

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

Note: In NCC version 11, Nebula changed from a points-based licensing model to a device-based licensing model.

### 6.3.2.1 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 gateway device.
- MSP: This license unlocks the MSP menu for an NCC user account.

The following table gives a summary of all licenses in NCC.

Table 30 Licenses Summary

LICENSE	CATEGORY	ASSIGN TO	DESCRIPTION
Pro Pack	Organization	Any NCC-managed device	<p>Unlocks all advanced features within the device's organization.</p> <p>For details on Pro features, see <a href="#">Section 6.3.2.2 on page 100</a>.</p>
Plus Pack	Organization	Any NCC-managed device	<p>Unlocks certain advanced features within the device's organization.</p> <p>For details on Plus features, see <a href="#">Section 6.3.2.2 on page 100</a>.</p>
Organization Trial	Organization	Organization	<p>Available when creating a new organization. Unlocks all <b>Pro Pack</b> and <b>Nebula Security Service (NSS)</b> features in the organization for 30 days. There are no restrictions on the allowed number of devices or sites.</p> <p>Note: Each Nebula user account can create 10 new organizations with trial licenses every 90 days.</p>
Nebula Security Service (NSS)	Security Service	Nebula Security Gateway (NSG) device	<p>Unlocks security services, such as anti-virus and anti-malware, on a Nebula Security Gateway (NSG) device.</p> <p>You can use these security services within the NSG's site.</p>
U/TM Security Pack	Security Service	USG FLEX device	<p>Unlocks security services, such as anti-spam and anti-malware, on a USG FLEX device.</p> <p>You can then use these security services within the USG FLEX's site.</p>
Secure WiFi	Security Service	USG FLEX device	Unlocks the Remote AP feature on a USG FLEX device.
MSP	MSP	NCC user account	Unlocks the MSP menu and MSP features for the assigned user account.

### 6.3.2.2 Organization License Tiers

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

- The **Base** tier is free and included with every organization.
- The **Plus** and **Pro** licenses unlock additional features within the organization. These features are marked in the user interface with a diamond icon (💎).

The feature differences between the license tiers are listed below:

Table 31 NCC License Tier Differences

FEATURE	BASE	PLUS	PRO	LOCATION	NOTES
Groups-wide menu (create organization groups, admins & teams, org-to-org VPN)	No	No	Yes	Groups-wide	To create a group, you must be an NCC admin and the owner of two or more Pro organizations.
Organization change logs	No	No	Yes	Organization-wide > Monitor > Change log	
Login IP address ranges for an organization	No	No	Yes	Organization-wide > Configure > Setting	
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: Users)	
Cloud Authentication DPPSK account type	No	No	Yes	Organization-wide > Configure > Cloud authentication (Account type: DPPSK)	
Vouchers as general authentication credentials	No	Yes	Yes	Site-wide > Monitor > Vouchers Site-wide > Configure > General Settings	
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	



Table 31 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PRO	LOCATION	NOTES
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 configuration templates are not available
Add client to block list/allow list	No	No	Yes	Site-wide > 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 > Monitor > Summary report	
Time period for summary reports	24 hours	7 days	365 days	Site-wide / Access point / Switch / Security gateway > Monitor > Summary report	
Time period for device monitoring statistics	24 hours	7 days	365 days	Access point / Switch / Security gateway > Monitor > AP / SW / SG > [Select AP / SW]	
Time period for client monitoring statistics	24 hours	7 days	365 days	Access point / Switch / Security gateway > Monitor > Clients > [Select client]	
Export data to CSV/XML file	No	Yes	Yes	All monitoring pages with tables	
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	
Nebula mobile app push notifications for VPN	No	Yes	Yes	App > Notification Center	
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	
Priority support requests from NCC UI or Nebula app	No	No	Yes	Help > Support request	

Table 31 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PRO	LOCATION	NOTES
Web chat with tech support directly from NCC UI	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 > Monitor > AP / SG [Select AP] Live tools	
Wireless health monitor and report	No	No	Yes	Access point > Monitor > Wireless health	
Programmable SSID	No	No	Yes	Access point > Configure > SSID overview	
Dynamic Personal Pre-Shared Key (DPPSK)	No	No	Yes	Access point > Configure > SSID settings	
Vouchers as WiFi authentication credentials	No	Yes	Yes	Site-wide > Monitor > Vouchers  Site-wide > Configure > General Settings  Access point > Configure > SSID settings  Access point > Configure > Captive portal customization > [Portal Theme]	
Facebook WiFi	No	No	Yes	Access point > Configure > SSID settings	
RADIUS accounting for captive portal	No	No	Yes	Access point > Configure > SSID settings	
Customize RADIUS NAS ID	No	No	Yes	Access point > Configure > SSID settings	
Customize portal redirect URL parameter	No	No	Yes	Access point > Configure > Captive portal customization	
Smart steering per AP	No	No	Yes	Access point > Configure > Radio settings > [Edit the Selected AP]	

Table 31 NCC License Tier Differences (continued)

FEATURE	BASE	PLUS	PRO	LOCATION	NOTES
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 devices
Extended PoE range	No	No	Yes	Switch > Configure > Switch ports > [Select Port]	Currently only supported on GS1350 series devices
Automatic PoE device recovery	No	No	Yes	Switch > Configure > Switch ports > [Select Port]	Currently supported on GS1350 and GS2220 series devices
Port bandwidth control	No	No	Yes	Switch > Configure > Switch ports > [Edit the Selected port]	
Vendor ID-based VLAN	No	No	Yes	Switch > Configure > Switch settings	
IP interface & static route	No	No	Yes	Switch > Configure > IP & Routing	
Packet capture	No	No	Yes	USG Flex > Monitor > Security gateway	Only supported on USG FLEX devices
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 NSG NSS-SP license
VPN topology with traffic usage	No	No	Yes	Organization-wide > Configure > VPN Orchestrator	
Smart VPN	No	No	Yes	Organization-wide > Configure > VPN Orchestrator	Free beta feature until the end of 2021
VPN provision script email	No	No	Yes	Security gateway > Configure > Remote access VPN (L2TP/IPSec)	
Collaborative Detection & Response (CDR) with automatically respond action	No	No	Yes	Site-wide > Configure > Collaborative detection & response	Require USG Flex UTM Security Pack license

## Organization License Grace Period

If a Pro or Plus license expires while assigned to a device or you add an unlicensed 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 Pro license to the unlicensed device.
- Remove the unlicensed device from the organization.

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

### 6.3.2.3 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, a 1-year license is activated on January 1st 2021, then its expiry date is January 1st 2022.

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

#### Bundled and Renewal Licenses

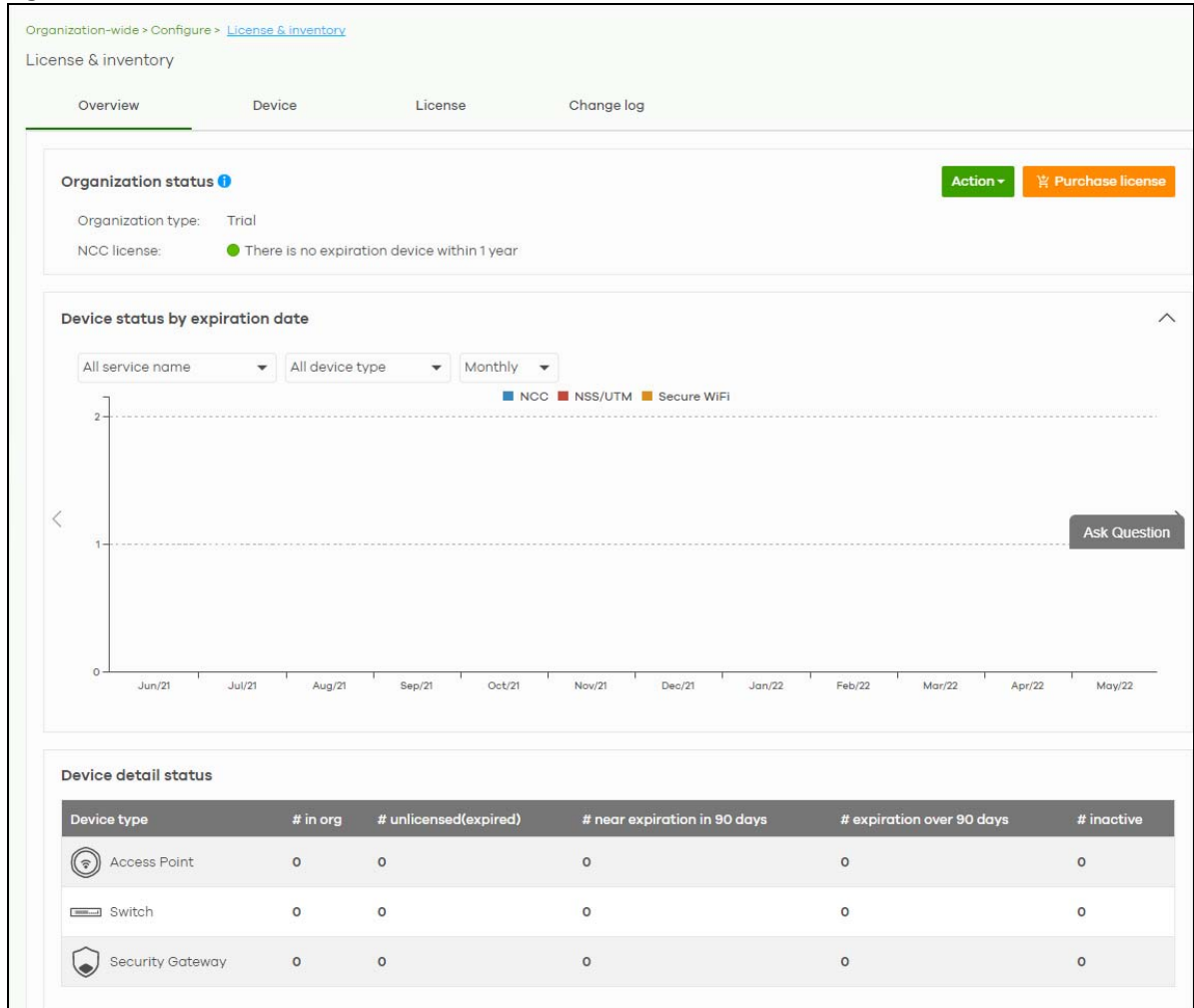
A **bundled license** is a license that is included when you purchase a device. The bundled license is automatically assigned to the purchased device when you add the device to NCC.

An **renewal license** is a license purchased separately from a device as a license key, from Zyxel or a 3rd-party reseller. To assign a renewal license to a device, go to **Organization-wide > Configure > License & inventory > License** and then click **+Add**.

### 6.3.2.4 License & Inventory Overview Screen

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

Figure 45 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Overview



The following table describes the labels in this screen.

Table 32 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Overview

LABEL	DESCRIPTION
Organization Status	
Action	<p>Click this button to add licenses and/or 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 devices to the organization, by serial number and MAC address. For details, see <a href="#">Section 6.3.2.5 on page 106</a>.</li> <li><b>Add more licenses:</b> Add new license to the organization, by license key. For details, see <a href="#">Section 6.3.2.6 on page 107</a>.</li> <li><b>Install wizard:</b> Add devices and licenses to the organization, assign the licenses to the devices, and then upgrade the organization if required. For details, see <a href="#">Section 6.3.2.7 on page 108</a>.</li> </ul>
Purchase License	Click this button to open the Zyxel license marketplace in a new window.
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 device in the organization.</p>

Table 32 Organization-wide &gt; Configure &gt; License &amp; inventory &gt; Overview (continued)

LABEL	DESCRIPTION
Downgrade Now	Click this button to downgrade the organization from Plus or Pro to Base tier, or from Pro to Plus tier.  All active NCC licenses in the organization will stay active and continue to count down to their expiry time.
Organization type	This shows the licensing tier of the organization. Possible values are: <b>Base, Plus Pack, Professional Pack, and Trial.</b>
NCC license	This shows whether there are any devices with near expiring licenses.
NSS/UTM license	This shows whether the current site has an active NSS or UTM license.
Device status by expiration date	Click this button to select the data to be shown in the graph. Choose one from each of the following criteria: <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 device to display.</li> <li>• <b>Monthly, Quarterly, or Yearly:</b> select the period of time to display.</li> </ul>
Device detail status	
Device type	This shows the category of device ( <b>Access Point, Switch, Security Gateway</b> ) and device model.
# in org	This shows the total number of devices of the specified category and model that are in the organization.
# unlicensed (expired)	This shows the total number of devices of the specified category and model that have: <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	This shows the total number of devices of the specified category and model that have an NCC Pro or Plus license that will expire within 90 days.
# expiration over 90 days	This shows the total number of devices of the specified category and model that have an NCC Pro or Plus license that more than 90 days before expiration.
# inactive	This shows the total number of devices of the specified category and model that have an NCC Pro or Plus license that has not been activated.

### 6.3.2.5 Add Devices Screen

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

**Figure 46** Organization-wide > Configure > License & Inventory > Overview: Add devices

The following table describes the labels in this screen.

**Table 33** Organization-wide > Configure > License & Inventory > Overview: 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 devices at once. Follow the instructions and formatting in the template to add the device's serial numbers and MAC addresses.
import	Click this to upload a completed template XLSX file and import all devices in the file.
MAC address	Enter the MAC address of the new device
Serial Number	Enter the serial number of the new device.
Model	This shows the model number of the device being added.
License info	This shows the type of NCC license activated on the device, if there is one.
Expiration date	This shows the expiration date of the NCC license activated on the device, if there is one.
Assign licenses from inventory	Click here to assign unassigned licenses already in the organization to the device.  Note: If the organization is a Pro or Plus tier, you must assign a Pro or Plus license to the device within 15 days.
	Click the remove icon to delete the entry.
Add another device	Click this to add another device to the organization.
Acknowledge	Select this to confirm that your NCC account will be the owner of the new devices.
Finish	Click this to add the devices to the organization.
Cancel	Click this to close the screen without saving.

### 6.3.2.6 Add Licenses Screen

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

**Figure 47** Organization-wide > Configure > License & Inventory > Overview: Add licenses

The following table describes the labels in this screen.

**Table 34** 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.

### 6.3.2.7 Install Wizard

Use this wizard to add licenses and devices to an organization, assign licenses to the new devices, and the upgrade the organization if required. Follow the steps below to use the wizard.

- 1 Click **Organization-wide > Configure > License & Inventory > Overview > Action > Install wizard**. After the wizard window opens, click **Next**.

- 2 Add the MAC address and serial number of one or more devices, select **Acknowledge**, and then click **Next**. For more information on this page, see [Section 6.3.2.5 on page 106](#).

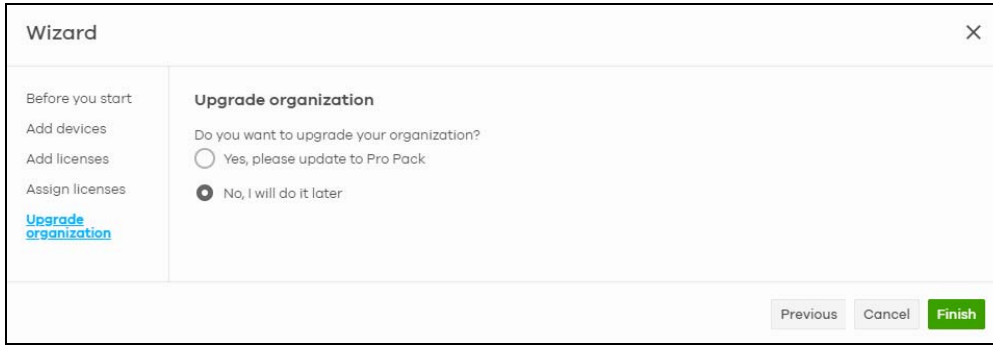


- 3 Add the license keys of one or more licenses, and then click **Next**. For more information on this page, see [Section 6.3.2.6 on page 107](#).

- 4 NCC automatically tries to assign an unused license to each matching device. Reassign unused licenses for each device manually by clicking **Select # of license**. Then click **Next**.

Devices	Sites	Model	Serial number	MAC address	Expiration date	Selected licenses	Select # of license
58 BB... ..	Taipei	NAP102	S16...	58 BB...	2022-04-10	Nebula Professional Pack License, 1YR *1	Select # of license
88 BC...	Taipei	NSW100-10	S17...	88 BC...	2024-04-11		Select # of license
20 B...	Hsinchu	USG FLEX 100	S20...	20 21...	2022-04-21		Select # of license
BC CF...	Taipei	WAX510D	S20...	BC CF...	2024-04-11		Select # of license
BC CF...	Taipei	USG FLEX 100W	S20...	BC CF...	2023-04-22		Select # of license

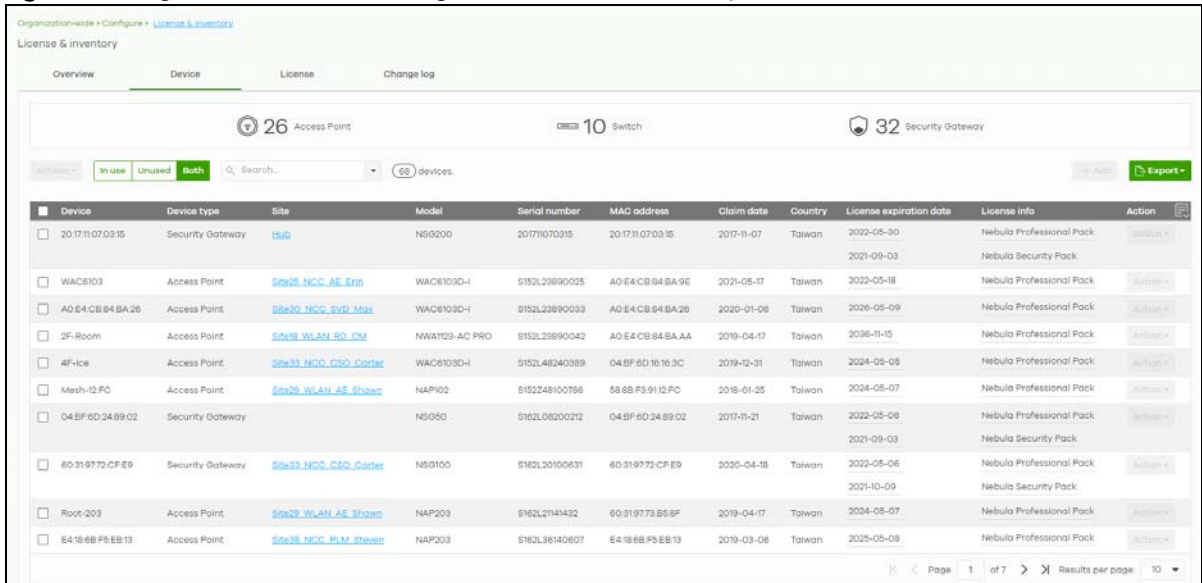
- 5 If the organization is on the base tier and you have added sufficient licenses for all devices, you are given the option to upgrade to the Pro or Plus tier. Select **Yes** or **No**, and then click **Finish**.



### 6.3.2.8 License & Inventory Device Screen

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

**Figure 48** Organization-wide > Configure > License & Inventory > Device



The following table describes the labels in this screen.

**Table 35** Organization-wide > Configure > License & Inventory > Device

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 Gateway	This shows the total number of security gateways devices (N) in the organization.

Table 35 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Device

LABEL	DESCRIPTION
Actions	<p>Select one or more devices and then click this button to perform one of the following actions:</p> <p><b>Change organization:</b> Moves the device to an organization. The organizations must have the same owners.</p> <p><b>Change site assignment:</b> Moves the selected devices to a site, or remove them from their current site while leaving them in the organization.</p> <p><b>Remove from organization:</b> Remove the devices from NCC. You can manage the devices in standalone mode, or re-add them to NCC later.</p> <p><b>Assign license:</b> Assign licenses to the selected devices.</p> <p><b>Undo assign:</b> Unlink the inactive licenses from the associated 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 device but is not yet in use or queued.</p> <p><b>License transfer:</b> Moves the unused licenses linked to a device to another device. The devices can be in the same organization or in a different organization. The devices must have the same owner. Bundled, Trial, and Promotion licenses cannot be transferred.</p>
In use / Unused / Both	Select to display the Nebula Device current 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 devices.
+ Add	Add one or more new devices to the organization, by entering the device's MAC address and serial number. For details, see <a href="#">Section 6.3.2.5 on page 106</a> .
Export	Click this button to save the device list as a CSV or XML file to your computer.
Device	This shows the hostname of the device.
Device type	This shows the category of device ( <b>Access Point, Switch, Security Gateway</b> ) and device model.
Site	This shows the site that the device is currently. If the device is not in any site, the value is blank.
Model	This shows the device's model.
Serial Number	This shows the device's serial number.
MAC address	This shows the MAC address of the device's first Ethernet port.
Claim date	This shows the date on which the device was added to NCC.
Country	This shows the country in which the device is located.
License expiration date	This shows the date on which the device's NCC license will expire.
License info	<p>This shows the type of NCC license assigned to the device.</p> <p>Note: Move the pointer over this field to see information about all licenses associated with this device.</p>
Action	<p>Select one or more devices and then click this button to perform one of the following actions:</p> <p><b>Change site assignment:</b> Moves the selected devices to a selected site, or removes them from their current site while leaving them in the organization.</p> <p><b>Remove from organization:</b> Remove the devices from NCC. You can manage the devices in standalone mode, or re-add them to NCC later.</p> <p><b>Assign license:</b> Assign unassigned licenses to the selected devices.</p>

### 6.3.2.9 License & Inventory License Screen

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

**Figure 49** Organization-wide > Configure > License & Inventory > License

Organization-wide > Configure > License & Inventory

License & inventory

Overview Device License Change log

361 assigned      20 unused (Pro Pack, 1YR)      1 unused (UTM Pack, 2YR)

Actions Search... (552) licenses + Add Export

License Key	Service	License status	License expiration date	Remaining days	Claim date	Activate date
UO-NBPO-774U-005000M050014000	Nebula Professional Pack License, 1YR	Active	2022-05-30	336 days	2021-05-10	2021-05-10
UO-NBPO-774U-005000M050014007	Nebula Professional Pack License, 1YR	Active	2022-05-06	312 days	2021-05-03	2021-05-05
UO-NBPO-774U-005000M050014008	Nebula Professional Pack License, 1YR	Active	2022-05-06	312 days	2021-05-03	2021-05-05
UO-NBPO-774U-005000M050014009	Nebula Professional Pack License, 1YR	Active	2022-05-06	312 days	2021-05-03	2021-05-05
UO-NBPO-774U-005000M050014004	Nebula Professional Pack License, 1YR	Active	2022-05-06	312 days	2021-05-05	2021-05-05
UO-NBPO-774U-005000M050014007	Nebula Professional Pack License, 1YR	Active	2022-05-06	312 days	2021-05-03	2021-05-05
UO-NBPO-774U-005000M050014008	Nebula Professional Pack License, 1YR	Active	2022-05-06	312 days	2021-05-03	2021-05-05
UO-NBPO-774U-005000M050014009	Nebula Professional Pack License, 1YR	Active	2022-05-06	312 days	2021-05-03	2021-05-05
UO-NBPO-774U-005000M050014007	Nebula Professional Pack License, 1YR	Active	2022-05-06	312 days	2021-05-03	2021-05-05
UO-NBPO-774U-005000M050014008	Nebula Professional Pack License, 1YR	Active	2022-05-06	312 days	2021-05-03	2021-05-05

Page 1 of 56 Results per page: 10

The following table describes the labels in this screen.

**Table 36** Organization-wide > Configure > License & Inventory > License

LABEL	DESCRIPTION
N assigned	This shows the total number of licenses (N) in the organization that are assigned to a device and activate.
N unused (Pro Pack, 1MO/1YR/2YR/4YR/7YR) or N unused (Plus Pack, 1MO/1YR/2YR)	This shows the total number of Pro/Plus Pack licenses (N) in the organization that are not assigned to a 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 device.
Actions	Select one or more devices and then click this button to perform one of the following actions: <b>Assign License:</b> Assign the selected licenses to one or more devices.
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.
+ Add	Add one or more new licenses to the organization, by entering their license keys. For details, see <a href="#">Section 6.3.2.6 on page 107</a> .
Export	Click this button to save the license list as a CSV or XML file to your computer.
License Key	This shows the key of license.
Service	This shows the service that license is for, for example "Nebula Professional Pack".

Table 36 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; License (continued)

LABEL	DESCRIPTION
License states	This shows the current status of the license: <ul style="list-style-type: none"> <li><b>Active:</b> The license is assigned to a specific device and activated.</li> <li><b>Inactive:</b> The license is assigned to a specific 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 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 device.</li> </ul>
License expiration date	This shows the date on which the license will expire. <b>Queued</b> means there are multiple licenses assigned to the device, and the license is waiting for the currently active license to expire.
Remaining days	This shows how days remain until the license expires.
Claim date	This shows the date on which the license was added to NCC.
Activate date	This shows the date on which the license was activated.
Associated device	This shows the name and model of the device that the license is assigned to.
Associated site	This shows the name of the site that the license is being used in. Click on the site to go to its dashboard.
Action	Click this button to perform the following actions: <b>Assign License:</b> Assign the selected license to a device.

### 6.3.2.10 License & Inventory Change Log Screen

Use this screen to view a record of 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 50 Organization-wide &gt; Configure &gt; License &amp; Inventory &gt; Change Log

Organization-wide > Configure > License & Inventory

License & inventory

Overview Device License Change log

Keyword:  Search... Range:  From: 2021-03-30 08:32 To: 2021-03-31 08:32 UTC+0



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

< Newer Older > 33 matches in 33 change logs within the time filtered. Changes date back to 2021-03-09 00:41 (UTC)

Date and time	Action	Before	After	Admin
2021-03-31 08:30:52	Downgraded license(s)DOWNGRADED	NCC Pro	NCC Base	
2021-03-31 08:00:55	Removed device(s) <input type="text"/>	# removed from ORG-Nebula_Org		
2021-03-31 08:00:54	Removed device(s) <input type="text"/>	# removed from SITE-Site01		
2021-03-31 08:00:53	Upgraded license(s)UPGRADED	NCC Base	NCC Pro	
2021-03-31 07:34:05	Added device(s) <input type="text"/>		# added to SITE-Site01	<input type="button" value="Add"/>
2021-03-31 07:33:17	Added device(s) <input type="text"/>		# added to ORG-Nebula_Org	<input type="button" value="Add"/>
2021-03-31 07:33:17	Downgraded license(s)DOWNGRADED	NCC Pro	NCC Base	
2021-03-31 07:30:56	Removed device(s) <input type="text"/>	# removed from ORG-Nebula_Org		
2021-03-31 07:30:55	Removed device(s) <input type="text"/>	# removed from SITE-Site01		
2021-03-31 07:30:53	Upgraded license(s)UPGRADED	NCC Base	NCC Pro	

The following table describes the labels in this screen.

Table 37 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 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.
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 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 51 Organization-wide &gt; Configure &gt; Settings

Organization-wide > Configure > Settings

Settings

**Organization information**

Name: Temp

Country: Taiwan

**Security**

Idle Timeout  0 minutes of inactivity will logout users.

Login IP ranges  Only allow access to Dashboard from IP addresses in the specified ranges.

This computer is using IP address : 61.222.86.79

Import certificate  Use my certificate

Name: (64 letters)

File Path:

Upload a PKCS#12 file that bundles a private key with its X.509 certificate.

Password: (PKCS#12 only)

Delete this organization **Beta**

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](#), [inventory](#) of devices.

The following table describes the labels in this screen.

Table 38 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.
Security	
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.
Login IP ranges	Select <b>ON</b> and specify the IP address range of the computers from which an administrator is allowed to log into the NCC.  Select <b>OFF</b> to allow any IP address of the computer from which an administrator can log into the NCC.

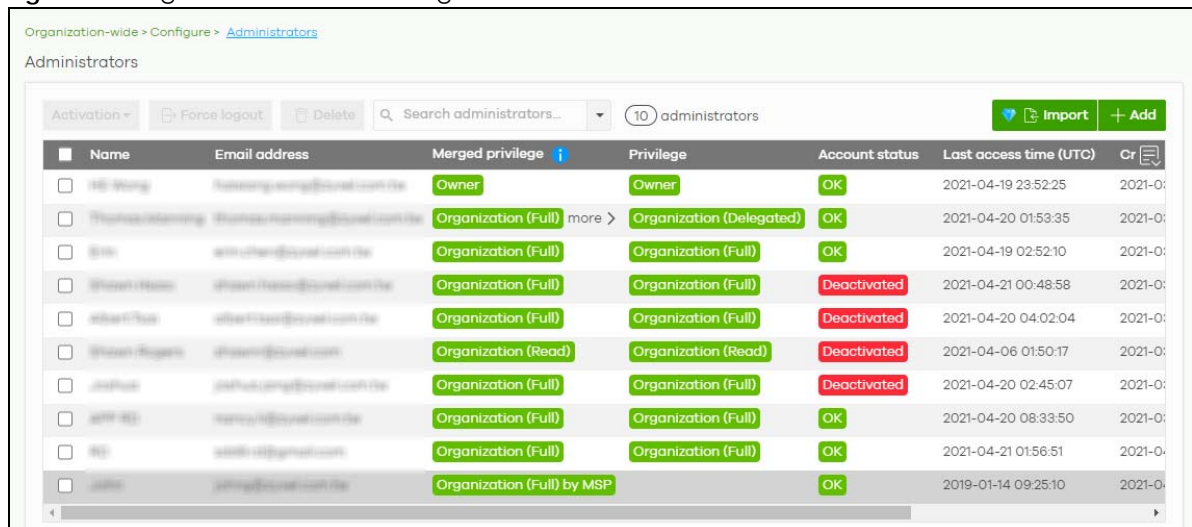
Table 38 Organization-wide > Configure > Settings (continued)

LABEL	DESCRIPTION
Import certificate	Select <b>ON</b> to import a certificate that can be used by connected Nebula APs in WPA2 authentication.
Certificate	This shows the name used to identify the certificate.
Status	This shows whether the certificate is active.
Actions	Click <b>Edit</b> to change the certificate name or password or replace the certificate.
Update certificate	Click this button to save a new certificate to the NCC.
Name	Enter a name for the certificate.
File Path	Click to find the certificate file you want to upload.
Password	Enter the certificate file's password.
Delete this organization	Click the <b>Delete organization</b> button to remove the organization when it does not have any sites, devices or users.  Note: You will be redirected to the <b>Choose organization</b> page after this organization is deleted.

### 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 52 Organization-wide > Configure > Administrators



The following table describes the labels in this screen.

Table 39 Organization-wide > Configure > Administrator


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 39 Organization-wide &gt; Configure &gt; Administrator (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="496 411 1175 774" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <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: 5px;"> <span style="font-size: 0.8em;">Tom - Thomas.Turning@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; margin-right: 5px;">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 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="496 991 1240 1346" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <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: #00a651; color: white; padding: 5px 15px; display: inline-block; margin-bottom: 5px;">Browse</div> <p style="margin: 0;">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 118</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 4.4.0.1 on page 68</a>.</p>

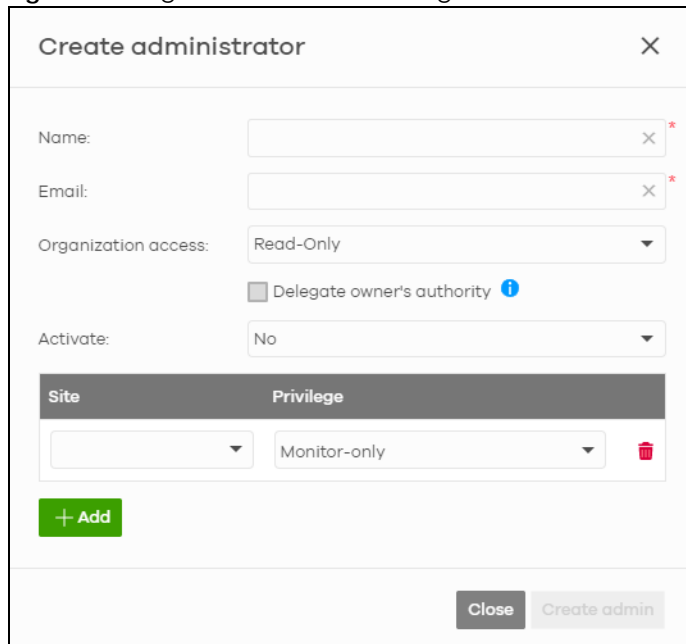
Table 39 Organization-wide &gt; Configure &gt; Administrator (continued)

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 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 53** Organization-wide > Configure > 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 40 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 the 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 120</a> ).  <b>Installer</b> access allows an administrator to register 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 40 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 these 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 186](#)).

### 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 11.3.2 on page 389](#).

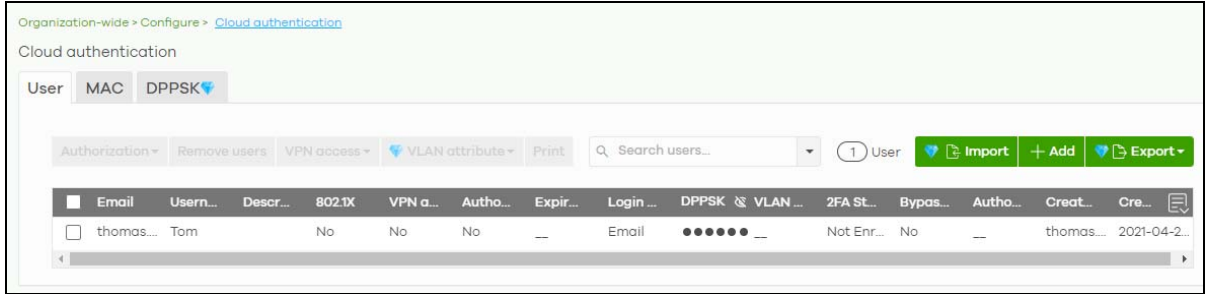
Table 41 Cloud Authentication: User Account Types

ACCOUNT TYPE	DESCRIPTION	AUTHENTICATION METHODS
User	The user account can gain access to the networks by authenticating using a pre-created username 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 device account that can gain access to the networks by authenticating using its MAC address.	<ul style="list-style-type: none"> <li>Mac-based 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 these screen.

**Figure 54** Organization-wide > Configure > Cloud Authentication > User



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 42** Organization-wide > Configure > Cloud Authentication > User

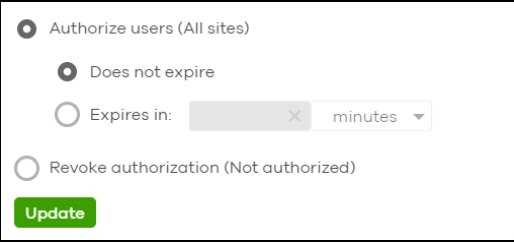
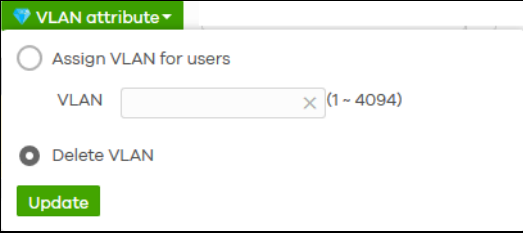
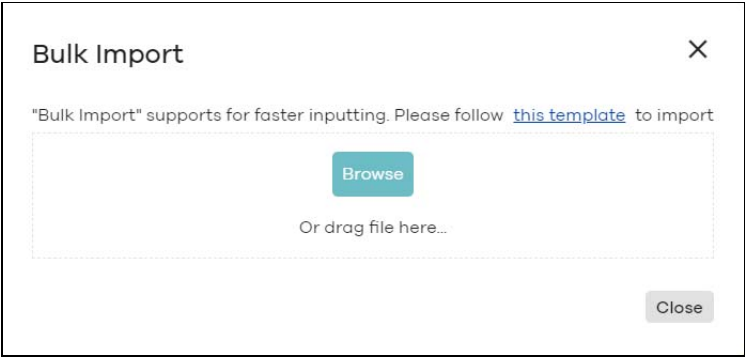

LABEL	DESCRIPTION
Authorization	<p>Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.</p> 
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
VPN access	Select one or more than one user account and click this button to configure whether the accounts can be used to connect to the organization's networks through VPN.
VLAN attribute	<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	Click this button to print information about each selected user account, such as their username and password.
Search users	Enter a key word as the filter criteria to filter the list of user accounts.
N User	This shows how many user accounts (N) match the filter criteria and how many user accounts of the selected type are created in total.

Table 42 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; User (continued)

LABEL	DESCRIPTION
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 6.3.5.3 on page 123</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)	<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>
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	<p>This field is available only when the account type is set to <b>User</b>.</p> <p>This shows the VLAN assigned to the user.</p>
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	<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>
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 **Side-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 55** Organization-wide > Configure > Cloud Authentication > User: Create/Update user

The following table describes the labels in this screen.

**Table 43** Organization-wide > Configure > Cloud Authentication > User: Create/Update user

LABEL	DESCRIPTION
Account type	This shows the type of the user account.
Email	Enter the email address of the user account, which is used to log into the networks.
Username	Enter a user name for this account.  Note: This field is optional if <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 username 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.

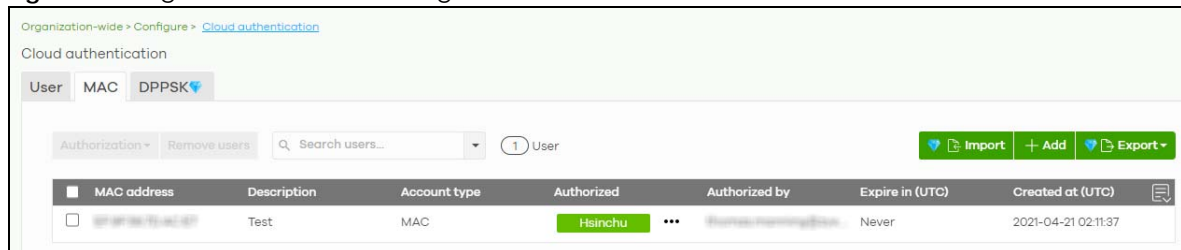
Table 43 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; User: Create/Update user

LABEL	DESCRIPTION
802.1X	Select this to allow the account to be used for single sign-on (SSO) network and WiFi authentication using 802.1X (WPA-Enterprise).
VPN Access	Select this to allow the account to be used to connect to the organization's networks through VPN.
Authorized	Set whether you want to authorize the user of this account.  You can select to authorize the user's access to <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 device user accounts, used for MAC-based authorization. Click **Organization-wide > Configure > Cloud Authentication > MAC** to access this screen.

Figure 56 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; MAC



The screenshot shows the 'Cloud authentication' interface with tabs for 'User', 'MAC', and 'DPPSK'. The 'MAC' tab is active, displaying a table of user accounts. The table has columns for MAC address, Description, Account type, Authorized, Authorized by, Expire in (UTC), and Created at (UTC). A single user account is listed with a MAC address of 08:00:20:08:00:20, Description of 'Test', Account type of 'MAC', Authorized status of 'Hsinchu', Authorized by of 'Hsinchu@ncc.gov.tw', Expire in (UTC) of 'Never', and Created at (UTC) of '2021-04-21 02:11:37'.

MAC address	Description	Account type	Authorized	Authorized by	Expire in (UTC)	Created at (UTC)
08:00:20:08:00:20	Test	MAC	Hsinchu	Hsinchu@ncc.gov.tw	Never	2021-04-21 02:11:37

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 44 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; MAC

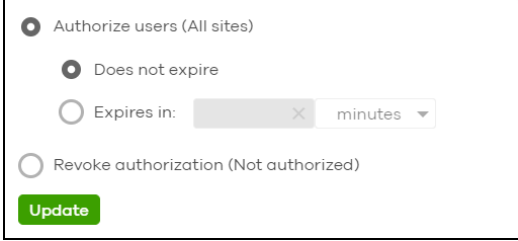
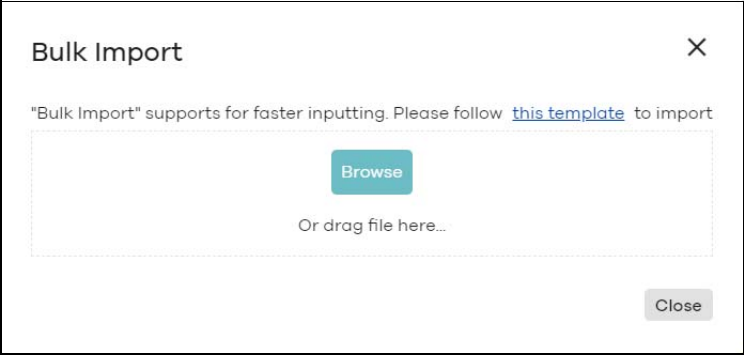

LABEL	DESCRIPTION
Authorization	<p>Select one or more than one account and click this button to configure the authorization settings for the selected user accounts.</p> 
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
Search users	Enter 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 126</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 this 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>
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>

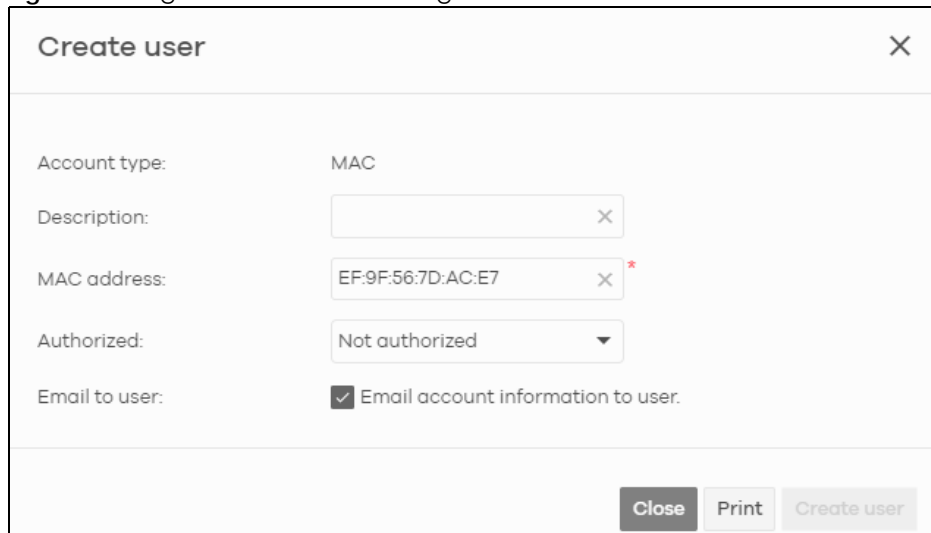
Table 44 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; MAC (continued)

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.

### 6.3.5.5 Create/Update MAC Account

In the **Side-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 57 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; MAC: Create/Update MAC user



The following table describes the labels in this screen.

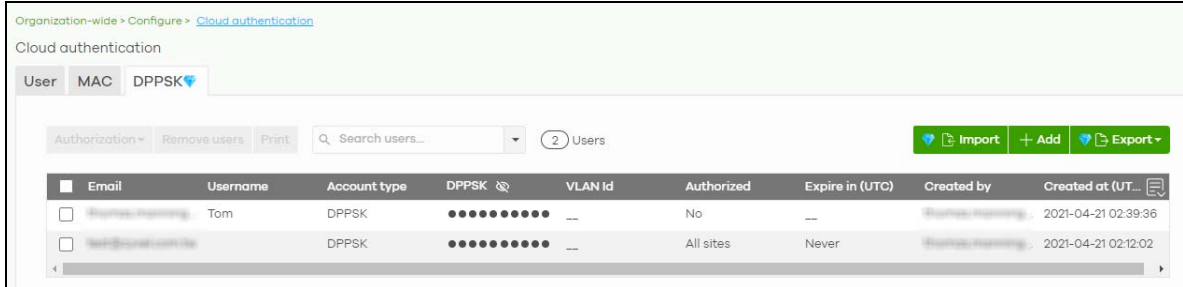
Table 45 Organization-wide &gt; Configure &gt; Cloud Authentication: Create/Update user

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 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.
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.

### 6.3.5.6 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 58** Organization-wide > Configure > Cloud Authentication > DPPSK

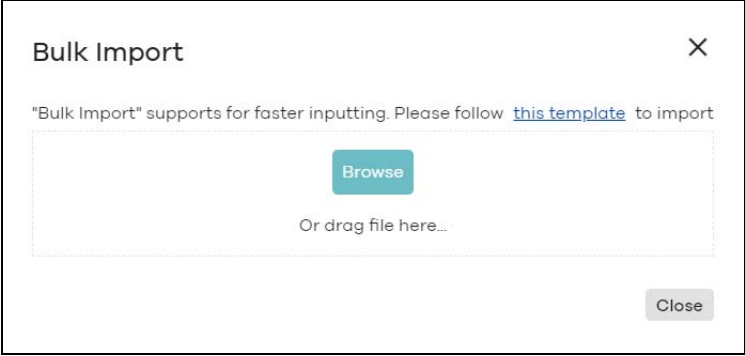



The following table describes the labels in this screen.

**Table 46** Organization-wide > Configure > Cloud Authentication > DPPSK

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> <div style="border: 1px solid black; padding: 5px; width: fit-content;"> <p><input checked="" type="radio"/> Authorize users (All sites)</p> <p><input checked="" type="radio"/> Does not expire</p> <p><input type="radio"/> Expires in: <input type="text" value=""/> minutes</p> <p><input type="radio"/> Revoke authorization (Not authorized)</p> <p><input type="button" value="Update"/></p> </div>
Remove users	<p>Select one or more than one user account and click this button to remove the selected user accounts.</p>
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 wireless network access.</p> <div style="text-align: center; margin: 10px 0;">DPPSK</div> <div style="border: 1px solid black; padding: 10px; display: flex; justify-content: space-around;"> <div style="text-align: center;">  nduzjauv9f              Expired in: Never         </div> <div style="text-align: center;">  paatdtcgh4              Expired in: Never         </div> </div>
Search users	<p>Enter a key word as the filter criteria to filter the list of user accounts.</p>
N Users	<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>

Table 46 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; DPPSK (continued)

LABEL	DESCRIPTION
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	<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 128</a>.</li> <li>• Batch create DPPSK: See <a href="#">Section 6.3.5.8 on page 130</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 this 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.
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 **Side-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 59** Organization-wide > Configure > Cloud Authentication > DPPSK: Create/Update DPPSK user

**Create single DPPSK user** [X]

Account type: DPPSK

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

Username: [X]

DPPSK: [DPPSK] [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 47** Organization-wide > Configure > Cloud Authentication > DPPSK: Create/Update DPPSK user

LABEL	DESCRIPTION
Account type	This shows the type of the user account.
Email	Enter the email address of the user account, which is used to log into the networks.
Username	Enter a user name for this account.
Description	Enter a descriptive name for the account.
DPPSK	Enter a dynamic personal pre-shared key (DPPSK) for this DPPSK user account, It can consist of 8- 31 alphanumeric characters. You can click <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.
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.

Table 47 Organization-wide &gt; Configure &gt; Cloud Authentication &gt; DPPSK: Create/Update DPPSK user

LABEL	DESCRIPTION
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 **Side-wide** or **Organization-wide > Configure > Cloud Authentication > DPPSK** screen, click **Add**, and then select **Batch Create DPPSK**.

Figure 60 Organization-wide &gt; Configure &gt; Cloud Authentication: Batch Create DPPSK

The screenshot shows a web form titled "Batch create DPPSK user" with a close button (X) in the top right corner. The form 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](#)

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

The following table describes the labels in this screen.

Table 48 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).
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.

Table 48 Organization-wide &gt; Configure &gt; Cloud Authentication: Batch Create DPPSK

LABEL	DESCRIPTION
Expire in	<p>This field is available only when the user is authorized.</p> <p>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.</p> <p>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.</p> <p>Otherwise, select <b>Never</b> and the user of this account will never be logged out.</p>
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/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 61** Organization-wide > Configure > Configuration Management

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?](#)

---

### Backup & restore Beta

Site(s) settings

Backup	Description	Date (UTC)	Admin
1	<input type="text" value=""/>		<input type="button" value="x"/> <input type="button" value="−"/>

[What is this?](#)

---

Switch settings

Backup	Switch	Description	Model	Date (UTC)	Admin
1	<input type="text" value=""/>	<input type="text" value=""/>		Never	<input type="button" value="x"/> <input type="button" value="−"/>

[What is this?](#)

The following table describes the labels in this screen.

**Table 49** 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.
Sync	Click this button to start synchronizing configuration settings between the selected sites.
Switch settings clone	



Table 49 Organization-wide &gt; Configure &gt; Configuration Management (continued)

LABEL	DESCRIPTION
From source device	Select the Nebula switch from which you want to copy its switch port settings to other 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 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 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 49 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 136](#)).

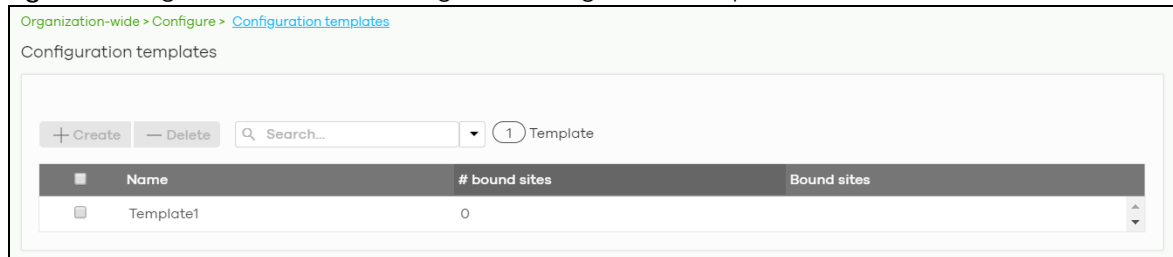
Use this screen to create and manage configuration templates. You then can bind or unbind a site from the template (see [Section 6.3.7.1 on page 135](#)).

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 Basic, all the sites will be unbound from the templates but retain the settings already applied from the template.

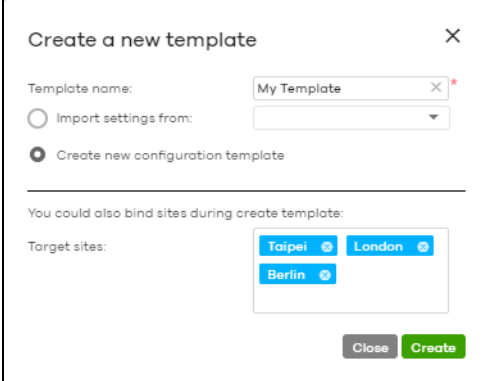
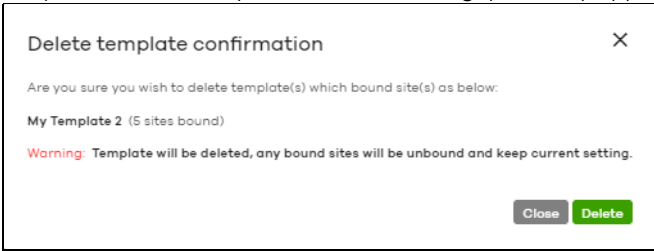
Click **Organization-wide > Configure > Configuration Template** to access this screen.

Figure 62 Organization-wide &gt; Configure &gt; Configuration Template



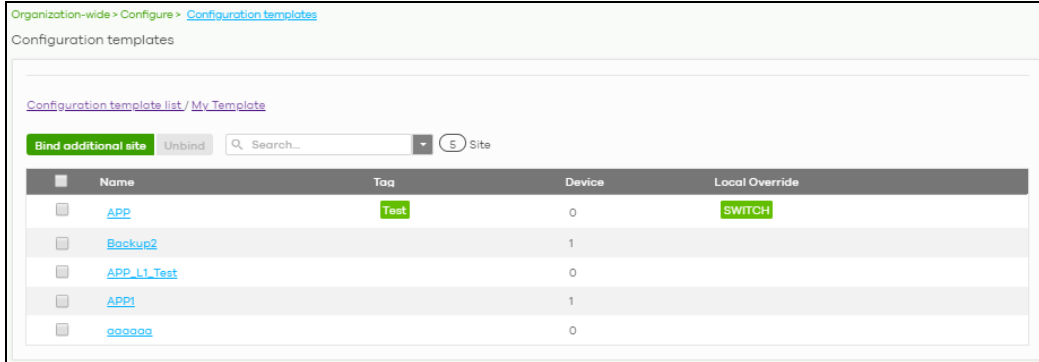
The following table describes the labels in this screen.

Table 50 Organization-wide > Configure > Configuration Template

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.

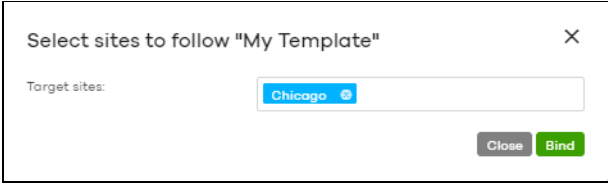
### 6.3.7.1 Site Binding

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 63** Organization-wide > Configure > Configuration Template: Template

The following table describes the labels in this screen.

**Table 51** 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 10.3.1.1 on page 343](#) for details.) after the switch is bound to a profile, turn on the local override function (see [Section 6.3.7.3 on page 136](#)).

## 6.3.8 Security Profile Sync

Security profile sync allows you to share the same USG FLEX security service settings with multiple sites in an organization. This replaces the Unified Threat Management (UTM) settings configured for each site at **USG FLEX > 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 USG FLEX 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 on 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 **USG FLEX > 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 64 Organization-wide > Configure > Security Profile Sync

Organization-wide > Configure > [Security profile sync](#)

Security profile sync

**Security profile sync** Beta

Enabled

Sync sites

**Content filtering**

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.

**Application Patrol**

Application profiles

There are no profiles defined for this site.

**URL Threat Filter**

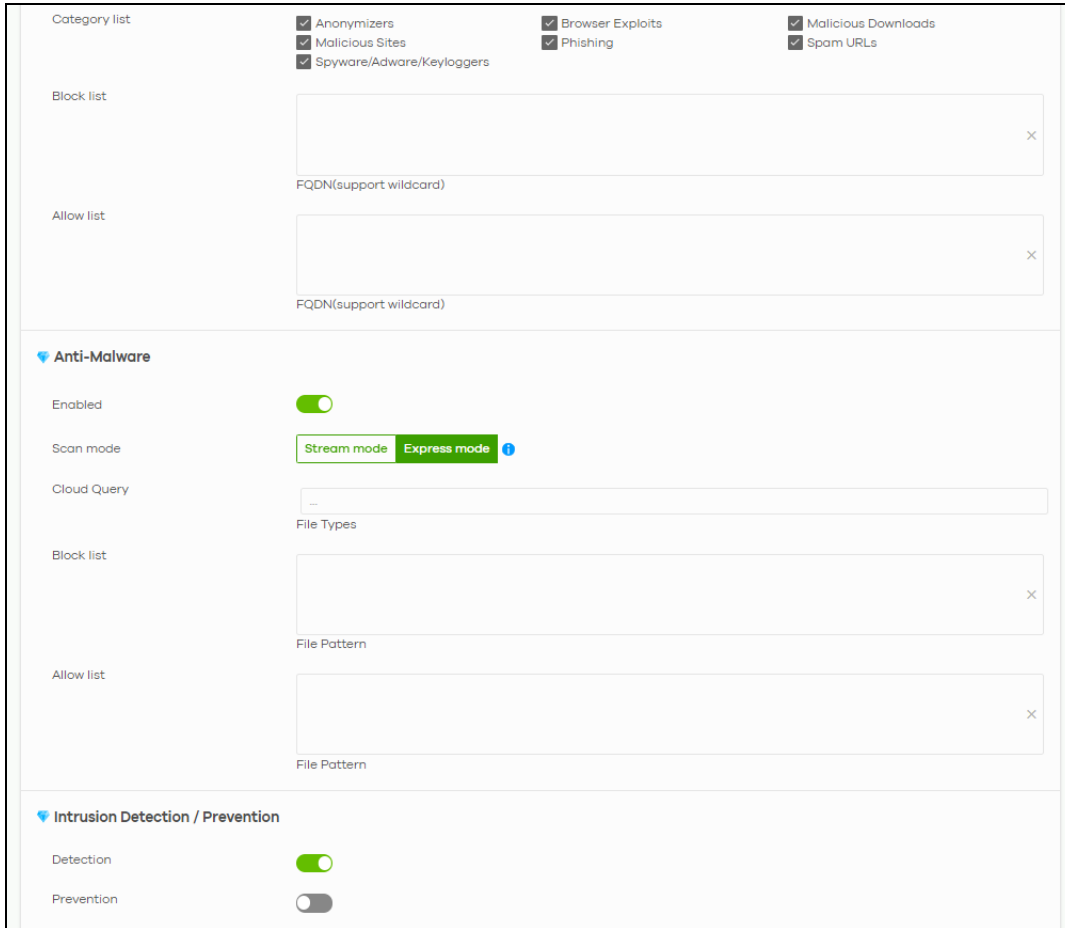
Enabled

Log

Policy

Denied Access Message

Redirect URL



The following table describes the labels in this screen.

Table 52 Organization-wide > Configure > 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 USG FLEX gateway device.
Content Filtering	
Drop connection when 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.

Table 52 Organization-wide &gt; Configure &gt; Security Profile Sync (continued)





LABEL	DESCRIPTION
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message.  Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+\$\._!~*()%). For example, http://192.168.1.17/blocked access.
Enabled	Select the 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 300</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 302</a> for more information.
URL Threat Filter	
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 Security Gateway generate a log (log), log and alert (log alert) or not (no) when the policy is matched to the criteria listed above.
Policy	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.
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.
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.



Table 52 Organization-wide &gt; Configure &gt; Security Profile Sync (continued)

LABEL	DESCRIPTION
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 do 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>
Anti-Malware	
Enabled	Select <b>On</b> to turn on the rule. Otherwise, select <b>Off</b> to turn off the rule.
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.
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’s OK 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 Security Gateway to scan for viruses.

Table 52 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>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's OK to upload a firmware package to the Nebula Device with the check box. This field displays the file or encryption pattern of the entry.</p> <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>
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 devices behind it to communicate securely.

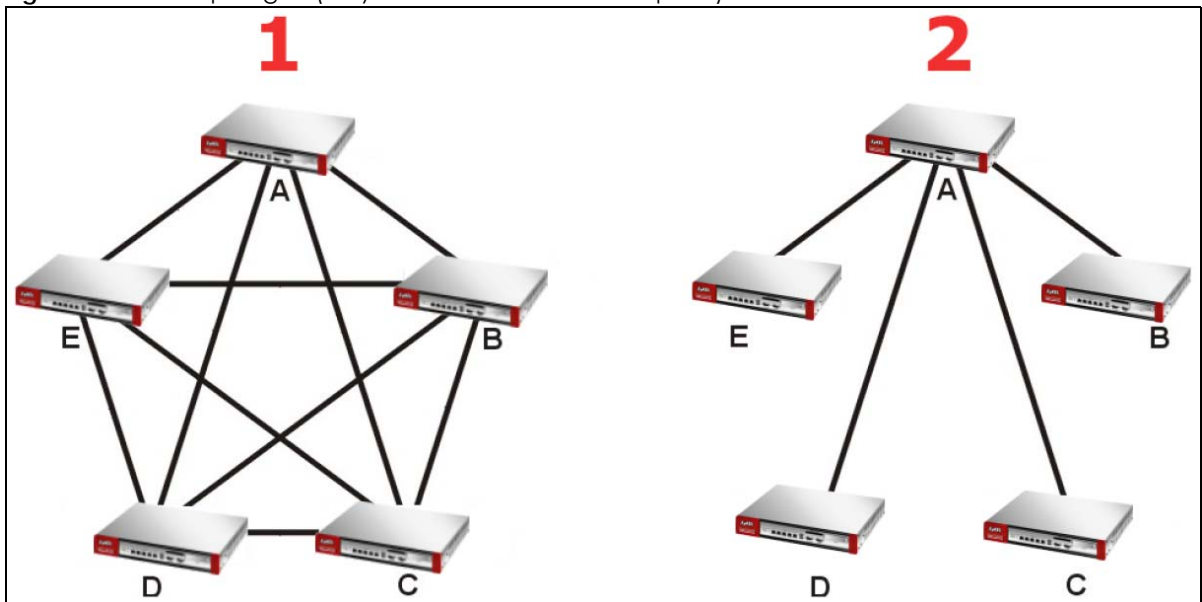
Note: You can manually create VPN connections between sites at **Gateway > Configure > Site-to-Site VPN** or **USG FLEX > Configure > Site-to-Site VPN**.

#### 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 2 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 65 VPN Topologies (Fully Meshed and Hub-and-Spoke)



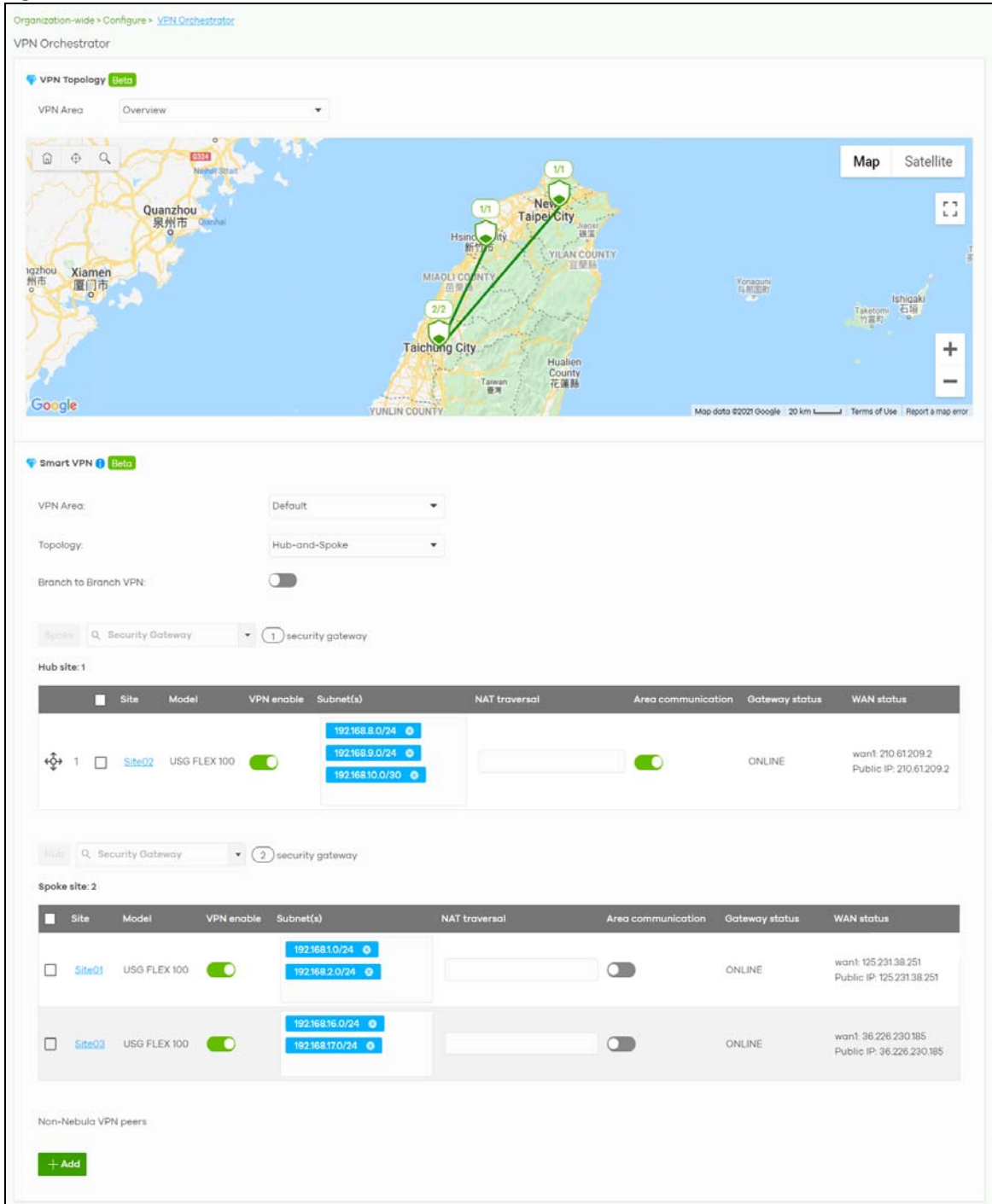
#### 6.3.9.2 VPN Areas

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 66 Organization-wide > Configure > VPN Orchestrator



The following table describes the labels in this screen.

Table 53 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.

Table 53 Organization-Wide &gt; Configure &gt; VPN Orchestrator (continued)




LABEL	DESCRIPTION
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.
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 143</a> . Select disable 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 device to filter the list of sites.
Hub site: N	This shows the number of hub sites (N) in the hub list.  Note: The maximum number of hub sites is 5.
Spoke site: N	This shows the number of spoke sites (N) in the spoke list.
#	This shows the priority of the hub site. If VPN area contains multiple hub sites, then 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.
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 a ZyWALL ATP device, 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.

Table 53 Organization-Wide &gt; Configure &gt; VPN Orchestrator (continued)

LABEL	DESCRIPTION
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 8.3.6.1 on page 232</a> for detailed information.
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 device.
	Click the remove icon to delete the entry.

## 6.3.10 Firmware Management

Use this screen to upgrade device firmware, or schedule a firmware upgrade for devices within the organization. Click **Organization-Wide > Configure > Firmware management** to access this screen.


Figure 67 Organization-Wide &gt; Configure &gt; Firmware management

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

Firmware management

The Firmware Upgrades allows organization admins to manage firmware versions on a per-site and per-device type basis.

Site: Any | Device type: Any | Firmware status: Any

 Upgrade Now | + Schedule Upgrade | Reset | 2 sites

Site	Device type	Firmware status	Upgrade scheduled	Time zone
<input type="checkbox"/> <a href="#">GS1350</a>	Access point	Upgrade available	Follow upgrade time	Asia/Taipei
<input type="checkbox"/> <a href="#">GS1350</a>	Switch	Up to date	No	Asia/Taipei

You can select devices by device type and by site, but you cannot select individual devices. For example, you can upgrade all switches in Site A and all APs in site B. To upgrade individual devices, go to **Organization-Wide > Configure > Firmware management**.

Note: This is a Nebula Professional Pack feature. If your Nebula Professional Pack license expires, existing firmware upgrades will still run as scheduled.

### 6.3.10.1 Firmware Upgrade Priority



NCC prioritizes the different device firmware upgrade schedules as follows, from highest to lowest:

1. Individual device upgrade schedule (set at **Organization-Wide > Configure > Firmware management**).
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 (90 days after new firmware is released).

### 6.3.10.2 Firmware Management Screen

The following table describes the labels in this screen.

Table 54 Organization-Wide > Configure > Firmware management

LABEL	DESCRIPTION
Site/Device Type/ Firmware Status	Specify your desired filter criteria to filter the list of devices.
Upgrade Now	Click this to immediately upgrade the firmware on all selected device types.  This button is selectable only when there is firmware update available for the selected devices.
Schedule Upgrade	<p>Click this to pop up a window where you can set a specific date and time to upgrade the firmware on the selected devices.</p>  <p>Note: Devices are upgraded according to the time zone of the site they are in, rather than the time zone of NCC (UTC).</p>
Reset	Click this button to clear the individual upgrade schedules of each selected device. The devices will go back to following the upgrade schedule of their site.
Site	This shows which site the device is in.  Click on the site name to go to the site's Dashboard.
Device Type	This shows the type of the device.
Firmware status	This shows whether the firmware on the device is <b>Up to date</b> , there is firmware update available for the device ( <b>Upgrade available</b> ), custom firmware was installed manually ( <b>Custom</b> ), a specific version of firmware has been installed by Zyxel customer support ( <b>Dedicated</b> ) or the device goes off-line and its firmware status is not available ( <b>N/A</b> ).  The status changes to <b>Upgrading...</b> after you click <b>Upgrade Now</b> to install the firmware immediately.
Upgrade scheduled	This shows the date and time when a new firmware upgrade is scheduled to occur. <b>Follow upgrade time</b> means the device is following the site-wide or organization-wide firmware schedule. <b>No</b> means the firmware on the device is up-to-date, or the device is offline and its firmware status is not available.  A lock icon means a specific firmware schedule has been created for the device. This means the device firmware will not be upgraded according to the schedule configured for the site or organization.
Time zone	This shows the time zone settings of the device's site.
	Click this icon to show and hide columns in the table.

# CHAPTER 7

## Site-wide

### 7.1 Monitor

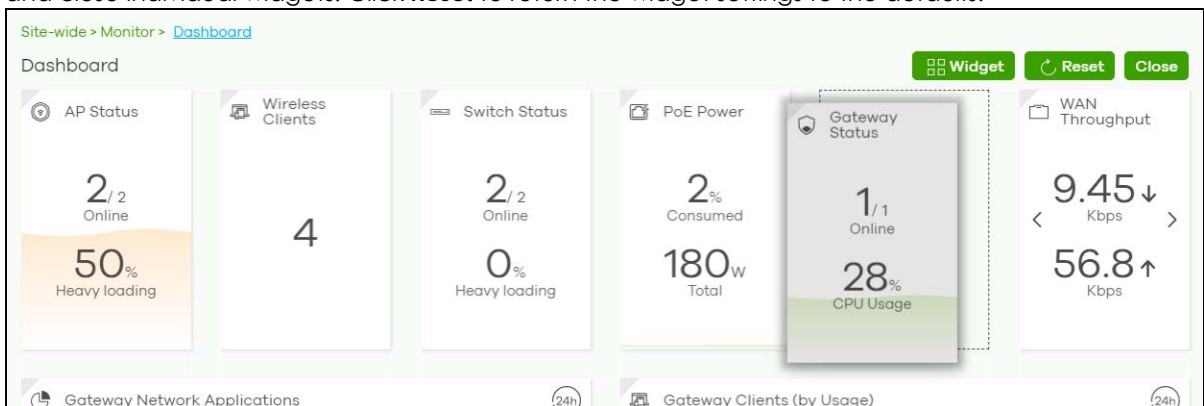
Use the **Monitor** menus to check the dashboard, summary report, map and floor plan, network topology and client list of the Nebula devices for the selected site.

#### 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.

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.



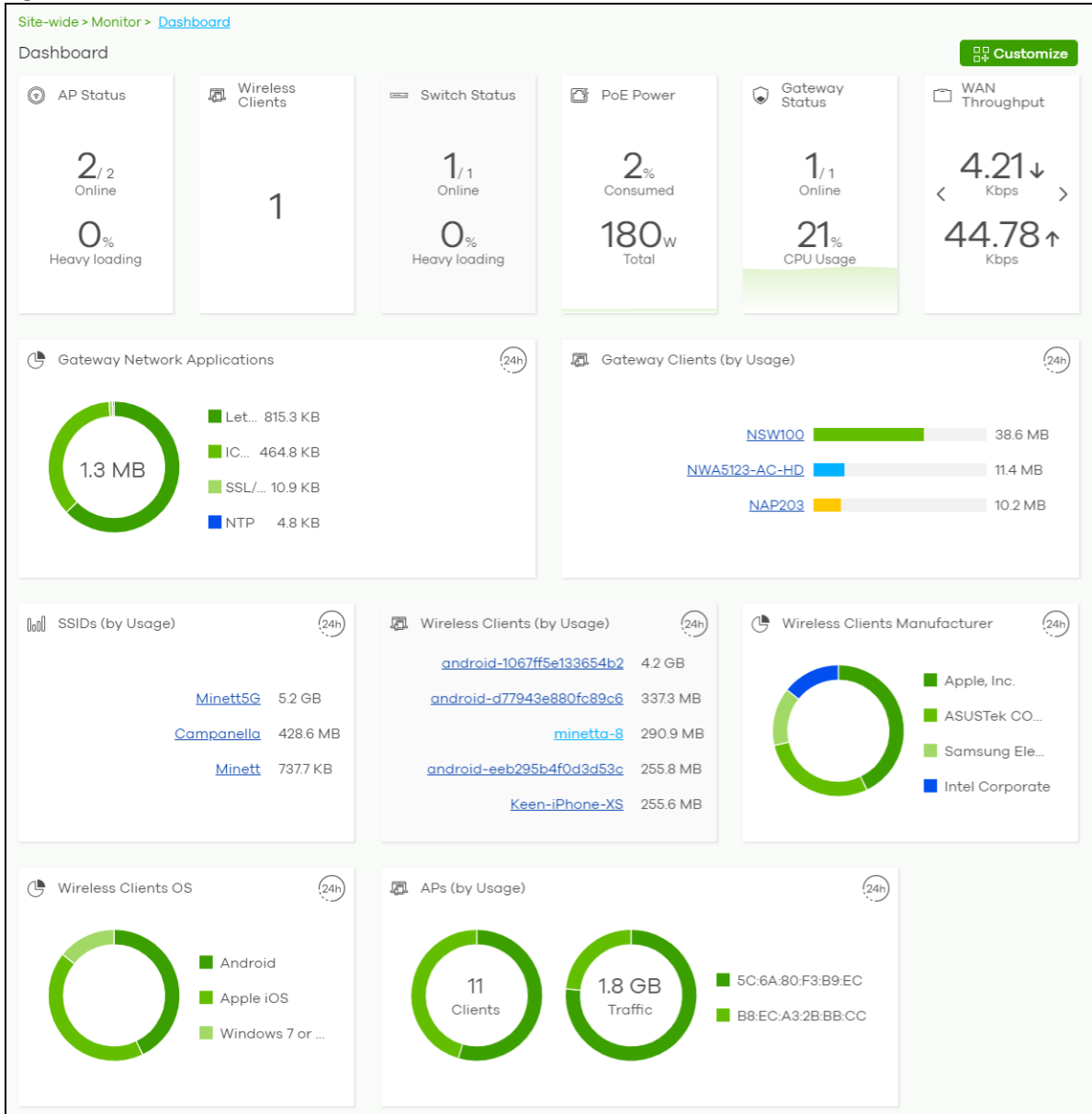
The **Dashboard** screen allows you to view:

- **AP Status:** how many Nebula APs are assigned and connected, and what percentage of the APs become overloaded, that is, the number of online APs that exceed the maximum client device number (in **AP > Configure > Load Balancing**) by total number of online APs in the site.
- **Wireless Clients:** how many WiFi clients are currently connected to the managed APs.
- **Switch Status:** how many Nebula switches are 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:** the total PoE power budget on the switch and the current amount of power consumed by the powered devices.
- **Gateway Status:** how many Nebula security gateways are assigned and connected, and what percentage of the gateway's processing capability is currently being used if the CPU goes over 93% usage.



- **WAN Throughput:** 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 gateway supports multiple WAN interfaces and more than one are active, use the arrow to switch and view the throughput of each WAN interface.
- **Gateway Network Applications:** the top ten applications in the past 24 hours.
- **Gateway Clients (by Usage):** the top five clients of the Nebula security gateway with the highest percentage of bandwidth usage in the past 24 hours.
- **SSIDs (by Usage):** the top three SSIDs with the highest percentage of bandwidth usage in the past 24 hours. You can click a WiFi network name to go to the **Access Point > Monitor > Summary Report** screen.
- **Wireless Clients (by Usage):** the top five WiFi clients (clients of the APs only) with the highest percentage of bandwidth usage in the past 24 hours. You can click a client's name to go to the **Access Point > Monitor > Clients: Client Details** screen.
- **Wireless Clients Manufacturer:** the top five manufacturers of WiFi client devices in the past 24 hours. You can click a manufacturer name to go to the **Access Point > Monitor > Client** screen and view the client devices which are made by the manufacturer.
- **Wireless Clients OS:** 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 **Access Point > Monitor > Client** screen and view the client devices which use this operating system.
- **APs (by Usage):** the top five managed APs with the highest percentage of bandwidth usage in the past 24 hours. This also shows the number of WiFi clients associated with the APs. You can click an AP's name to go to the **Access Point > Monitor > Access Points: AP Details** screen.
- **AP Google Map:** the locations of APs on the Google map.

Figure 68 Site-Wide > Monitor > Dashboard



### 7.1.2 Clients

This screen shows a list of all wired and wireless clients connected to devices (APs, switches, gateway) in the site. You can also block or allow clients. Click **Site-Wide > Monitor > Clients** to access this screen.

Figure 69 Site-Wide &gt; Monitor &gt; Clients

The screenshot shows the 'Site-wide > Monitor > Clients' interface. At the top, there are filters for 'Clients' (set to 'All'), 'Last 2 hours', and a refresh button. There are two buttons: 'Show all clients' and 'Show policy clients'. Below the filters is a search bar labeled 'Search clients...' and a count of '1822 clients' with an 'Export' button. The main area is a table with the following columns: Status, Description, Connected to, MAC address, IPv4 address, and First seen. The table lists several clients with their respective details.

Status	Description	Connected to	MAC address	IPv4 address	First seen
<input type="checkbox"/>	GSBU SVD RAP...	GSBU SVD RAP...	...	192.168.188.98	2021-04-14 15:23:...
<input type="checkbox"/>	GSBU AE Joshua	GSBU AE Joshua	...	192.168.2.35	2021-04-14 15:23:...
<input type="checkbox"/>	NSBU SVD3 5(W...	NSBU SVD3 5(W...	...	192.168.1.34	2021-04-14 15:23:...
<input type="checkbox"/>	NSBU SVD3 10(...	NSBU SVD3 10(...	...	192.168.1.39	2021-04-14 15:23:...
<input type="checkbox"/>	NSBU SVD3 10(...	NSBU SVD3 10(...	...	192.168.1.43	2021-04-14 15:23:...
<input type="checkbox"/>	NSBU SVD3 10(...	NSBU SVD3 10(...	...	192.168.1.33	2021-04-14 15:23:...

The following table describes the labels in this screen.

Table 55 Site-Wide &gt; Monitor &gt; Clients

LABEL	DESCRIPTION
Clients	Select to filter the list of clients, based on what type of device (access point, switch, security gateway) the client is connected to.  You can also set a time; the list shows each client's connection status in the past two hours, day, week or month.
	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 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.
Usage	Move the cursor over the chart to see the transmission rate at a specific time.
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.
Policy	Select the clients from the table below, and then choose the security policy that you want to apply to the selected clients. Choose one of the following policies: <ul style="list-style-type: none"> <li><b>Allowed:</b> The selected clients to bypass captive portal authentication.</li> <li><b>Blocked:</b> The selected clients cannot connect to the site. How a client is blocked depends on the connected device type selected under <b>Clients</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 gateway 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.
Add client	Click this button to open a window where you can specify a client's name and IP address to apply a policy before it is connected to the gateway's network.

Table 55 Site-Wide &gt; Monitor &gt; Clients (continued)


LABEL	DESCRIPTION
Export	Click this button to save the client list as a CSV or XML file to your computer.
General fields	
Status	This shows whether the client is online (green) or offline (red), and whether the client is wired or wireless. <ul style="list-style-type: none"> <li>• Clients connected to an AP appear are reported as wireless.</li> <li>• Clients connected to a switch or gateway are reported as wired.</li> </ul>
Description	This shows the descriptive name of the client. By default, this is the client's MAC address. Click the name to display the individual client statistics. See wireless: <a href="#">Section 7.1.2.1 on page 153</a> and wired: <a href="#">Section 7.1.2.2 on page 155</a> .
Connected to	This shows the name of the Nebula device to which the client is connected in this site. Click the device name to display the screen where you can view detailed information about the Nebula device.
MAC address	This shows the MAC address of the client. Click the MAC address to display the individual client statistics. See wireless: <a href="#">Section 7.1.2.1 on page 153</a> and wired: <a href="#">Section 7.1.2.2 on page 155</a> .
IPv4 address	This shows the IP address of the client.
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.
LLDP	This shows the LLDP (Link Layer Discovery Protocol) information received from the client.
Usage	This shows the amount of data consumed by the AP (upload + download) since it was last connected.
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.
	Click this icon to display a greater or lesser number of configuration fields.
AP-related fields	
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	This shows the RSSI (Received Signal Strength Indicator) of the client's wireless 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 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 was last connected.

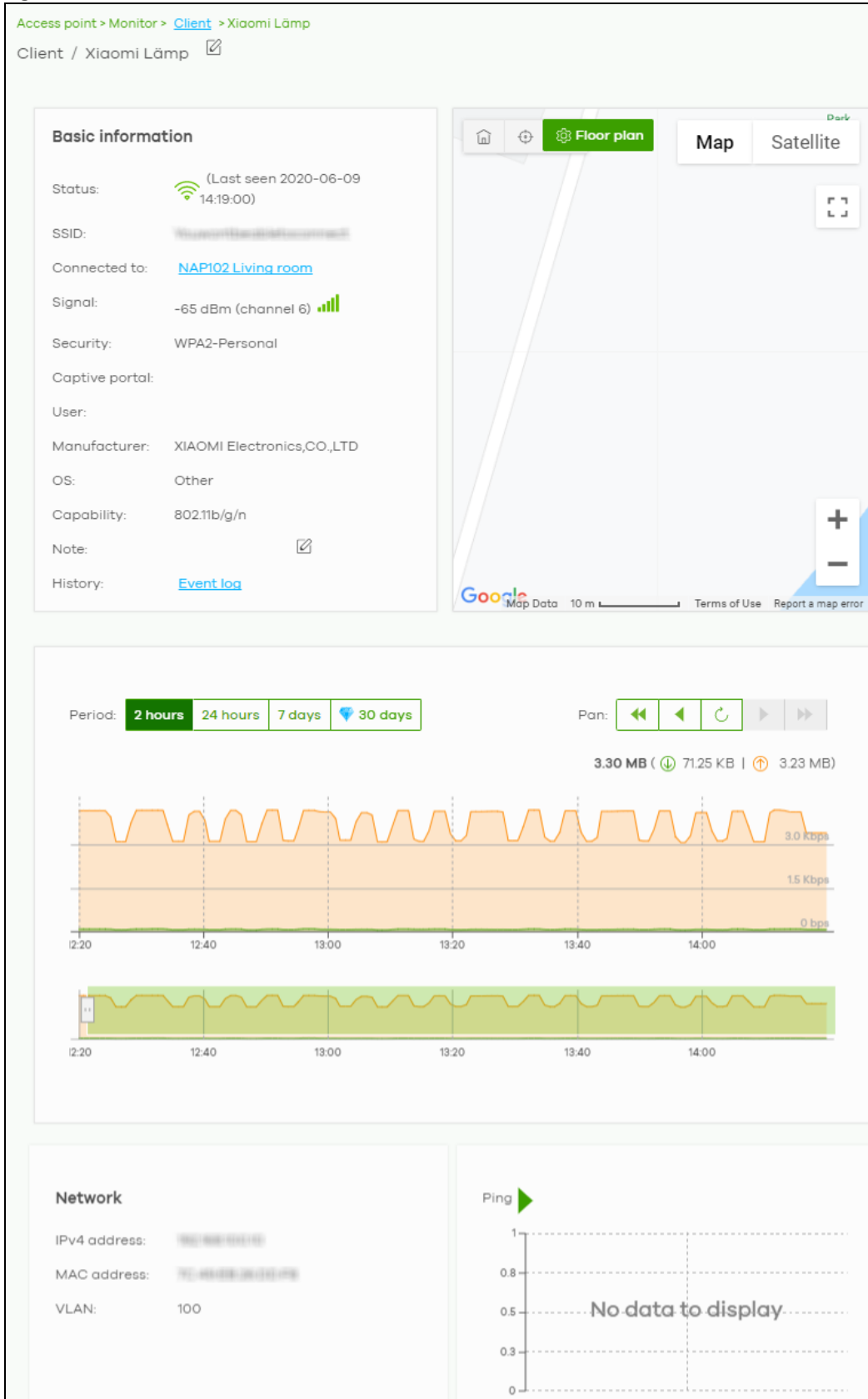
Table 55 Site-Wide &gt; Monitor &gt; Clients (continued)

LABEL	DESCRIPTION
Upload	This shows the amount of data transmitted from the client since it was last connected.
Association time	This shows the date and time the client associated with the Nebula device.
Capability	This shows the WiFi standards supported by the client or the supported standards currently being used by the client.
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.
VLAN	This shows the ID number of the VLAN to which the client belongs.

### 7.1.2.1 Wireless Client Details

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

Figure 70 Site-Wide > Monitor > Clients: Wireless Client Details



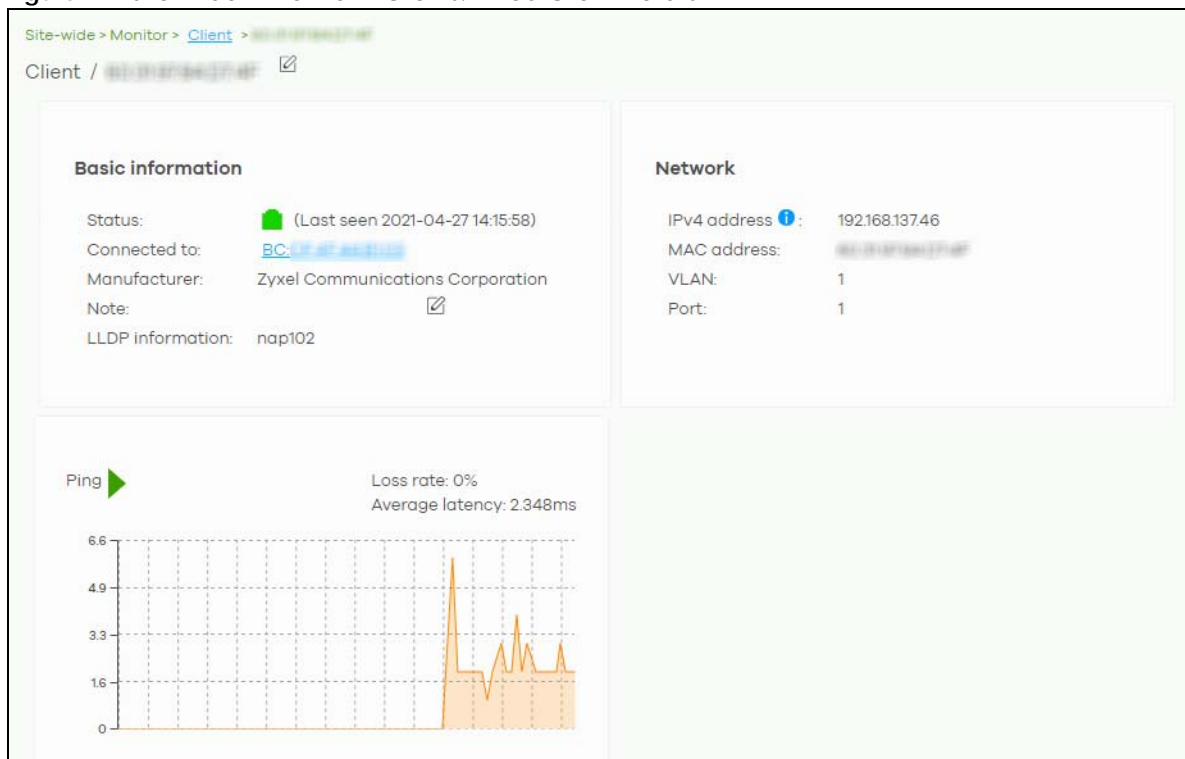
The following table describes the labels in this screen.

Table 56 Site-Wide > Monitor > Clients: Wireless Client Details

LABEL	DESCRIPTION
Status	This shows whether the client is online (green), or goes off-line (red). It also shows the last date and time the client was discovered.
SSID	This shows the name of the AP's wireless network to which the client is connected.
Connected to	This shows the name of the Nebula managed AP to which the client is connected. Click the name to display the individual AP statistics. See <a href="#">Section 11.2.1.1 on page 369</a> .
Signal	This shows the RSSI (Received Signal Strength Indicator) of the client's wireless 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 AP.
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 AP.
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 AP'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** screen to display individual client statistics.

**Figure 71** Site-Wide > Monitor > Clients: Wired Client Details

The following table describes the labels in this screen.

**Table 57** Site-Wide > Monitor > Clients: 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 gateway to which the client is connected.
User	This shows the number of users currently connected to the network through the client device.
Manufacturer	This shows the manufacturer of the client device.
OS	This shows the operating system running on the client device, if known.
Note	Enter information about this device, for yourself or for other administrators.
History	Click <b>Event log</b> to go to the <b>USG FLEX &gt; Monitor &gt; Event log</b> screen.
LLDP information	This shows the LLDP (Link Layer Discovery Protocol) information received from the remote device.
Network	
IPv4 address	This shows the IP address of the client.
Interface	This shows the interface on the Security Gateway to which the client belongs.
Port forwarding	This shows the port forwarding rules set for this client.
Public IP	This shows the port forwarding and 1:1 NAT IP addresses for each 1:1 NAT rule configured for this client.
Period	Select to view the client connection status in the past two hours, day, week or month.
Pan	Click to move backward or forward by two hours or one day.



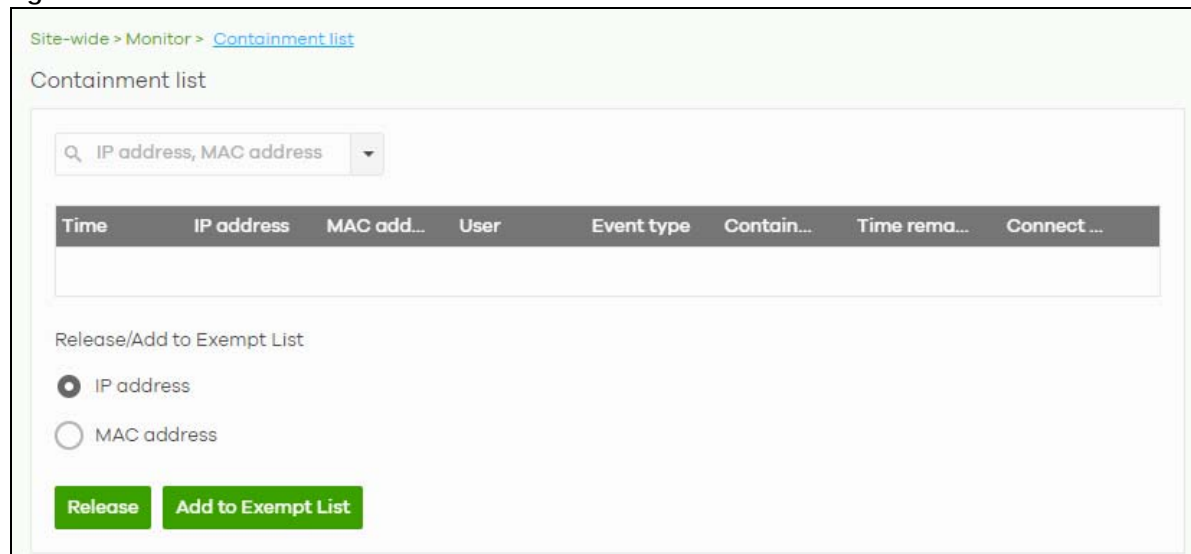
Table 57 Site-Wide &gt; Monitor &gt; Clients: Wired Client Details (continued)

LABEL	DESCRIPTION
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.
Top Application	A donut chart shows the percentage of usage for each application used by the client, if any. The number in the center of the donut chart indicates the amount of the application's traffic which has been transmitted or received by the client. Click <b>View More</b> to display the application statistics. Click <b>Hide Info</b> to hide them.
Application	This shows the name of the application. Click an application name to view information about the clients who used the application. For details, see <a href="#">Section 7.1.9 on page 168</a> .
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 the client.
% Usage	This shows the percentage of usage for the application used by the client.
Ping	Click the button to ping the client's IP address from the gateway to test connectivity.

### 7.1.3 Containment List

This screen shows a list of clients 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 72 Site-Wide &gt; Monitor &gt; Containment List



The following table describes the labels in this screen.

Table 58 Site-Wide &gt; Monitor &gt; 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.

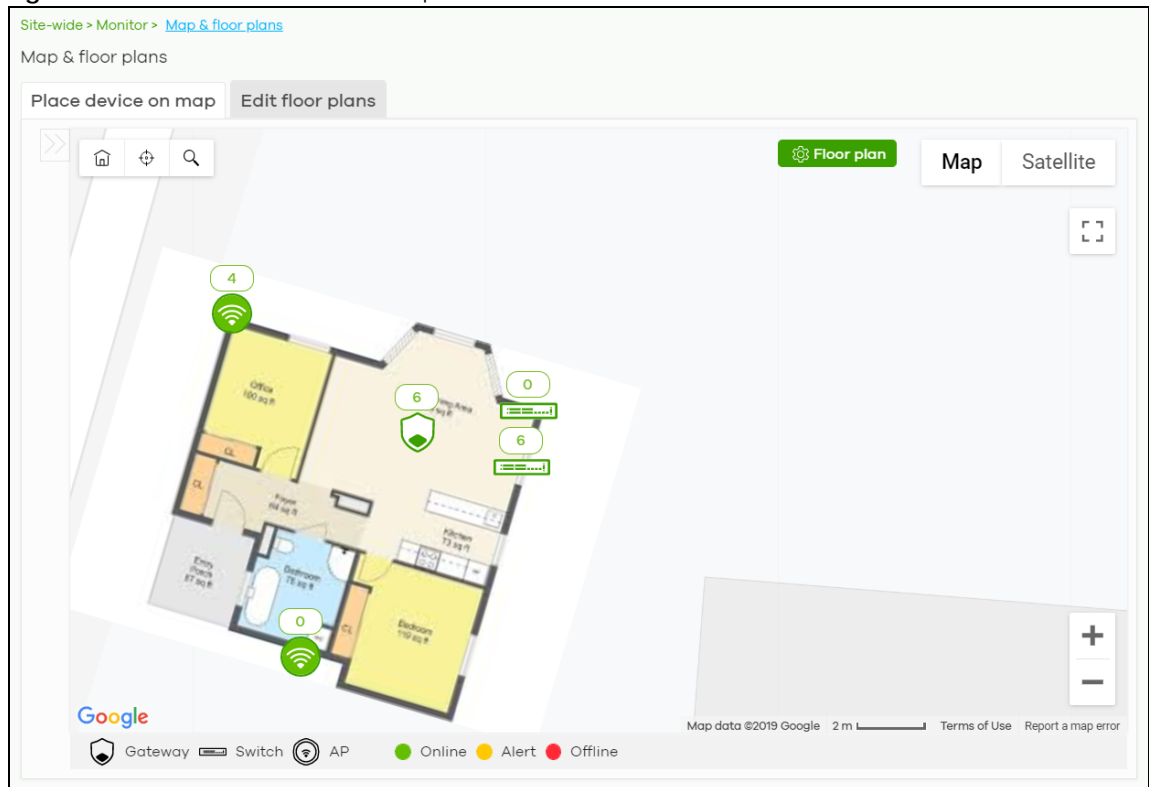
Table 58 Site-Wide > Monitor > Containment List (continued)

LABEL	DESCRIPTION
User	The 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 AP 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 device from CDR containment.
Add to Exempt List	Select a client, select IP address or MAC address, and then click this to release this device from CDR containment. This device's IP or MAC address is except from future CDR checking

### 7.1.4 Map & Floor Plans

This screen allows you to locate a 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 73 Site-Wide > Monitor > Map & Floor Plans



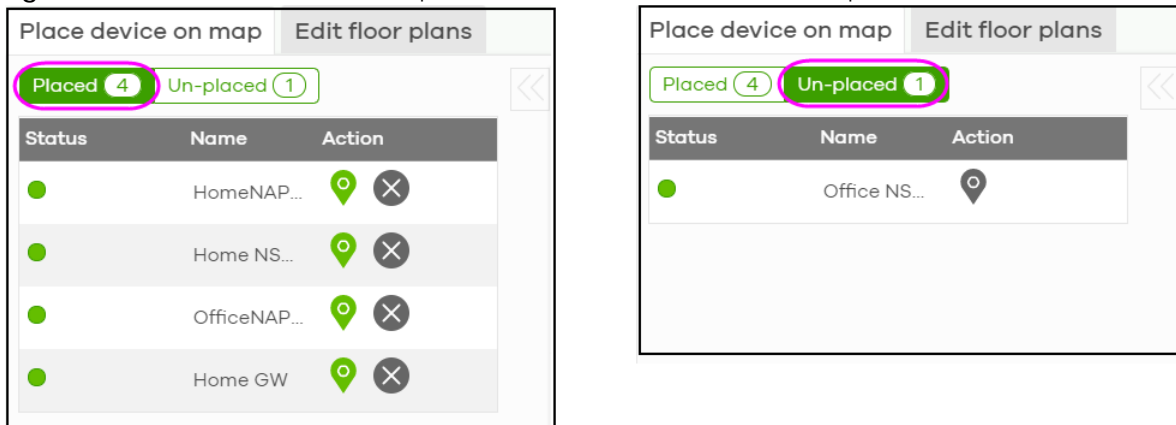
## Place devices on map

You can mark on the map the places where the devices are located. Click the **Place device on map** tab to display the 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 devices that you have pinned on the map and/or the floor plan. Click the **Un-placed** button to show the devices that remain to be pinned on the map. To pin a device, select the device from the **Un-placed** list, then drag and drop it on to the map.

The pin icon next to a device name is green (📍) if you have marked the device on the map. Otherwise, the pin icon is gray (📍). Click the ✕ icon to remove a device from the map.

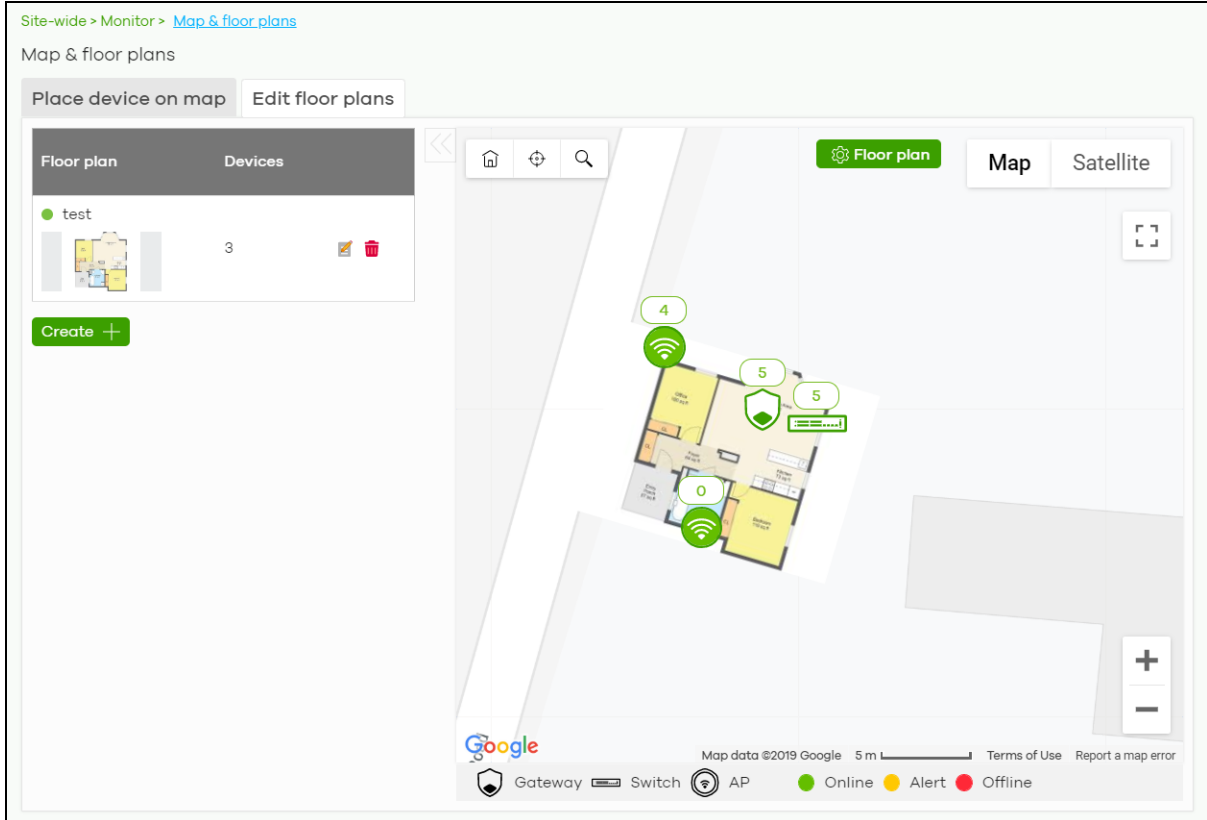
**Figure 74** Site-Wide > Monitor > Map & Floor Plans: Place devices on map



## 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 75** Site-Wide > Monitor > Map & Floor Plans: Edit floor plans

The following table describes the labels in this screen.

Table 59 Site-Wide &gt; Monitor &gt; Map &amp; Floor Plans: Edit floor plans

LABEL	DESCRIPTION
Floor plan	This shows the descriptive name of the floor plan.
Devices	This shows the number of the 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.

## 7.1.5 Topology

Use this screen to view the links between devices in the site. Click **Site-Wide > Monitor > Topology** to access this screen.

The icon of a node in the network topology indicates its device type and the color shows whether the device is online (green), has alerts (amber), or is off-line (red).

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

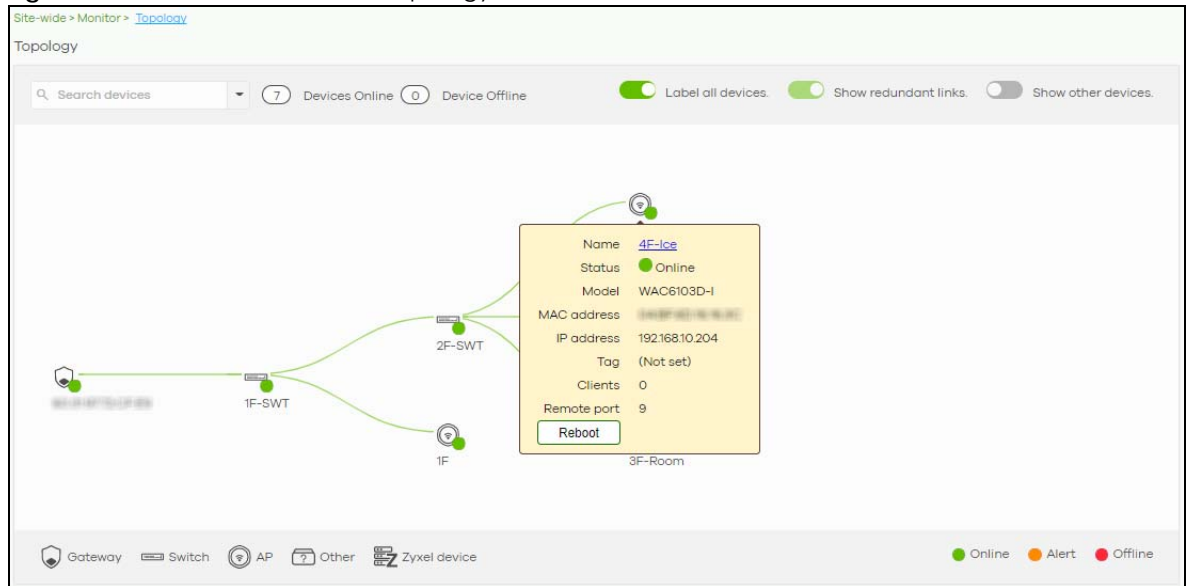
Enable **Label all devices** to show device information, such as MAC address in the network topology diagram.

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

Enable **Show other devices** to also display the devices that are connected to your network but cannot be identified by the NCC. This on/off switch button 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 76** Site-Wide > Monitor > Topology



## 7.1.6 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 buy a voucher for two hours of Internet access in a hotel or coffee shop.

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

### 7.1.6.1 Using Vouchers

- 1 Go to **Access Point > Configure > SSID Overview**, and create a dedicated SSID for voucher-based WiFi access. For example, "Hotel\_Guest\_Network".  
For details on configuring SSIDs, see [Section 11.3.1 on page 386](#).
- 2 Go to **Access Point > Configure > Authentication**, select the SSID, and then under **Sign-in method** select **Voucher**.  
For details, see [Section 11.3.2 on page 389](#).

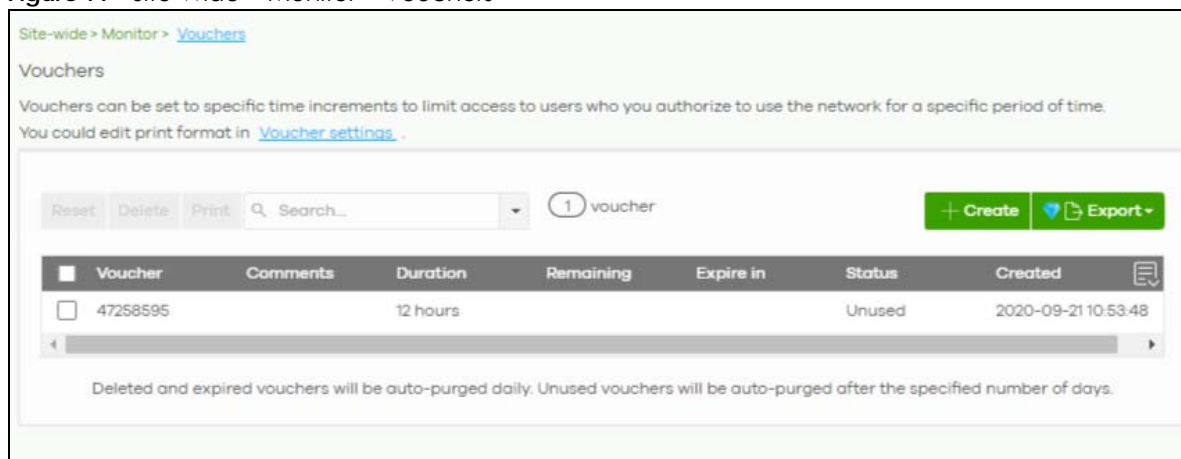
- 3 Go to **Site-wide > Configure > General settings > Voucher Settings** to configure how the vouchers will look when printed.  
For details, see [Section 7.2.1 on page 172](#).
- 4 Go to **Site-Wide > Monitor > Vouchers**, and then click **Create** to create one or more vouchers.

### 7.1.6.2 Voucher Screen

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

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

**Figure 77** Site-Wide > Monitor > Vouchers



The following table describes the labels in this screen.

**Table 60** Site-Wide > Monitor > Vouchers

LABEL	DESCRIPTION
Reset	Select one or more vouchers and then click this button to reset the vouchers back to their original states. Each voucher's status is set to <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 new vouchers. For details, see <a href="#">Section 7.1.6.3 on page 163</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.

Table 60 Site-Wide &gt; Monitor &gt; Vouchers (continued)

LABEL	DESCRIPTION
Status	<p>This displays the current status of the voucher:</p> <p><b>Unused:</b> The voucher has not yet been used for authentication.</p> <p><b>Active:</b> A user has used the voucher for authentication. NCC has started counting down the duration.</p> <p><b>Expire:</b> The voucher has reached then end of its duration period and can no longer be used.</p> <p><b>Delete:</b> The voucher is unused and has reached the time set under <b>Purge after (days)</b>.</p> <p>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.</p>
Created	This displays the date and time that the voucher was created.

### 7.1.6.3 Create Vouchers Screen

Use this screen to create one or more new vouchers.

Figure 78 Site-Wide &gt; Monitor &gt; Vouchers &gt; Create

The screenshot shows a 'Create vouchers' dialog box with the following fields and values:

- Quantity: 1
- Code length: 8
- Comment: (empty)
- Duration (hours): 12
- Purge after (days): 30
- Print after created:
- Save as default:

Buttons at the bottom right: Cancel, Create

The following table describes the labels in this screen.

Table 61 Site-Wide &gt; Monitor &gt; Vouchers &gt; Create

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

Table 61 Site-Wide &gt; Monitor &gt; Vouchers &gt; Create (continued)

LABEL	DESCRIPTION
Duration (hours)	Sets how long the voucher is valid for 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 11.3.2 on page 389](#).

## 7.1.7 Cloud Intelligence Logs

This screen displays events from the gateway device 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 79 Site-Wide &gt; Monitor &gt; Cloud Intelligence Logs



The following table describes the labels in this screen.

Table 62 Site-Wide &gt; Monitor &gt; 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.



Table 62 Site-Wide &gt; Monitor &gt; Cloud intelligent logs

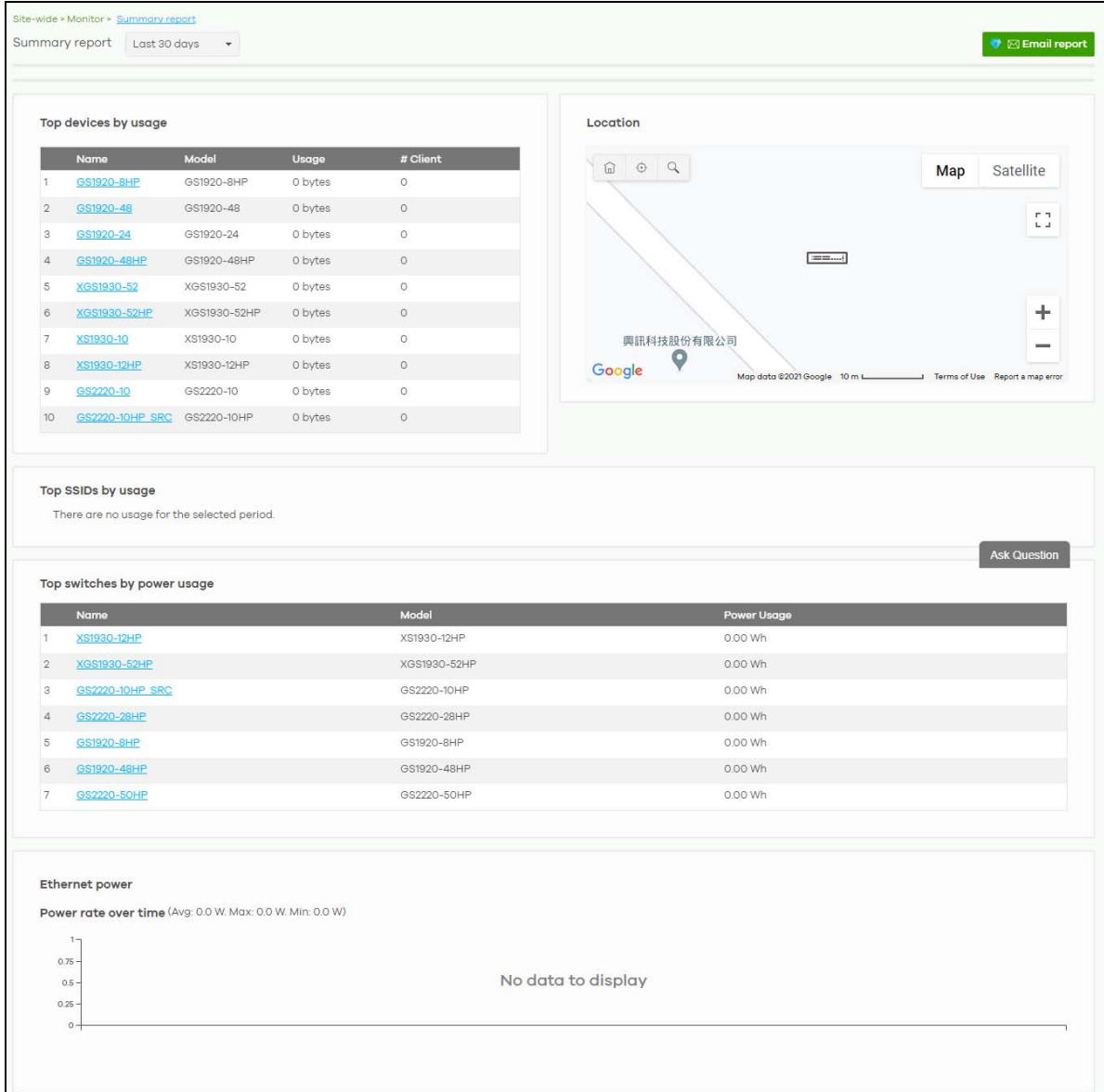
LABEL	DESCRIPTION
Category	Select the type of log messages you want to view. The available categories will depend on the features you have selected under <b>Feature</b> .
Range/Before	Select a filtering options, set a date, and then click <b>Search</b> to filter log entries by date. <b>Range:</b> Display 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 	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 in 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.
Detail	This shows detail of the event.
	Click this icon to display a greater or lesser number of configuration fields.

## 7.1.8 Summary Report

This screen statistics for the devices and networks in the selected site.

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

Figure 80 Site-wide > Monitor > Summary Report



The following table describes the labels in this screen.

Table 63 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 device.
Name	This shows the descriptive name of the device. You can click on the name to view device details.
Model	This shows the model number of the device.
Usage	This shows the amount of data that has been transmitted by or through the device.
Client	This shows the number of clients currently connected to the 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.

Table 63 Site-wide&gt; Monitor &gt; Summary Report (continued)

LABEL	DESCRIPTION
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 the power consumption is recorded.

## 7.1.9 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 81 Site-Wide > Monitor > Applications: Application View

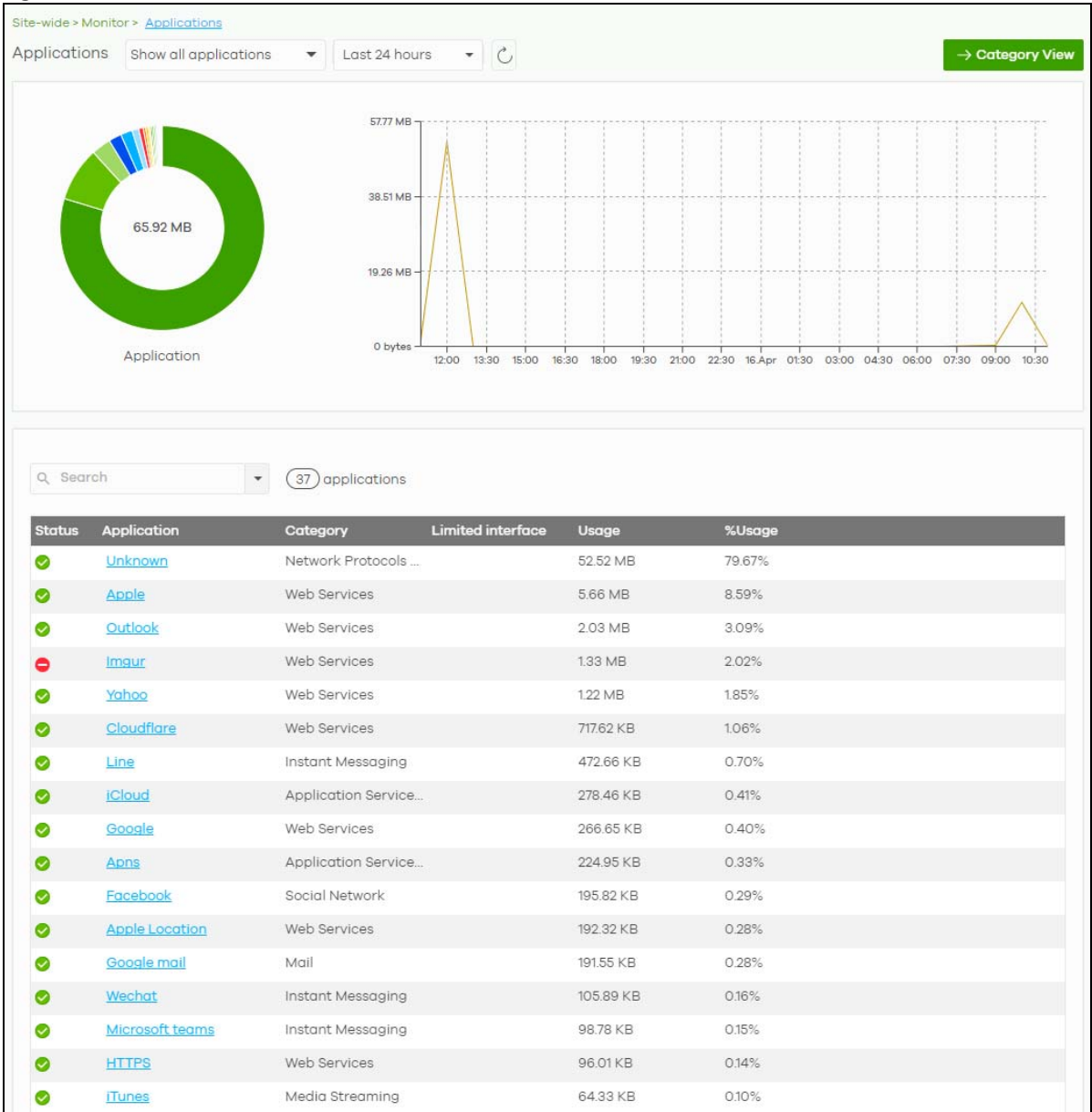
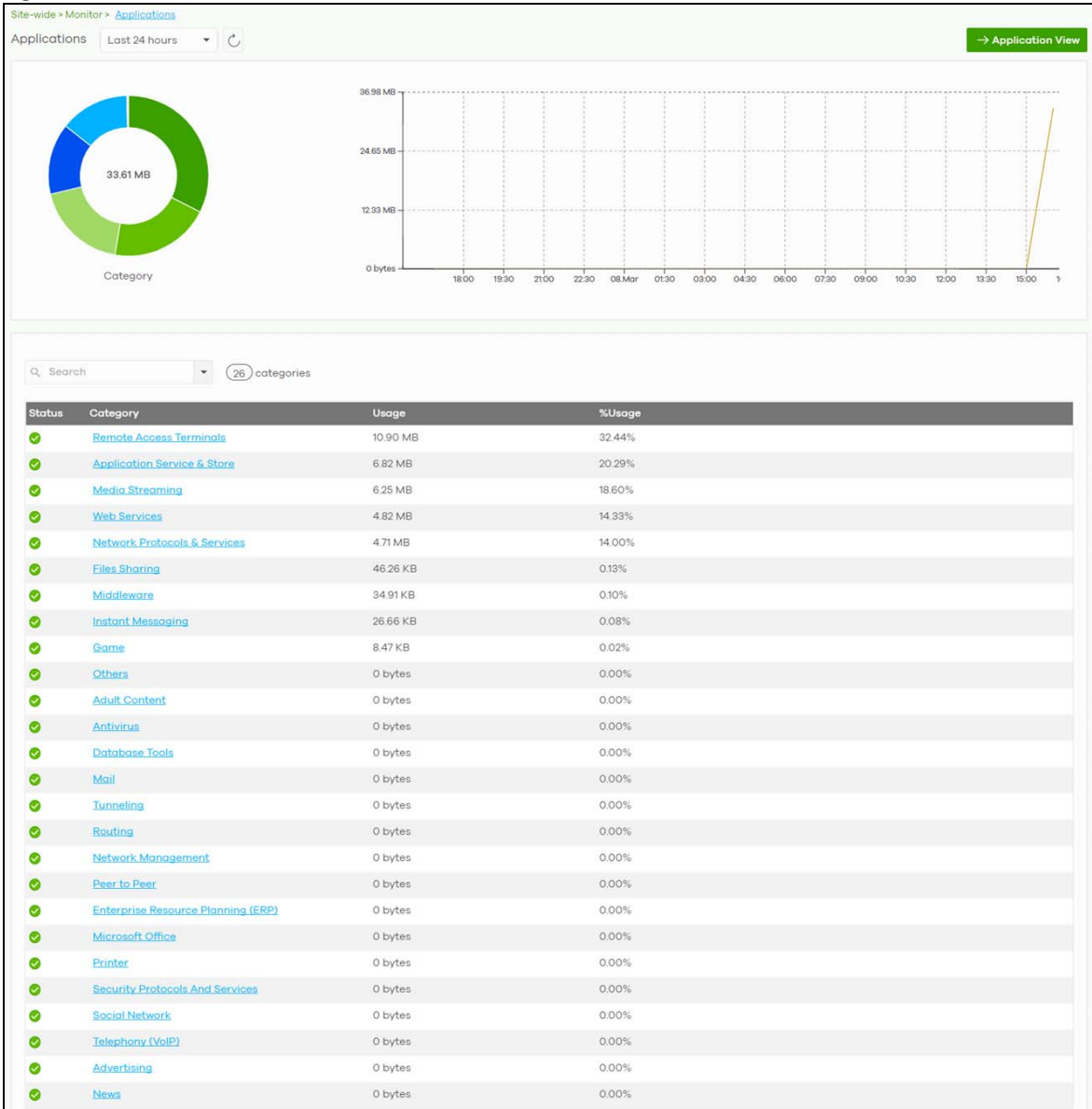




Figure 82 Site-Wide > Monitor > Applications: Category View



The following table describes the labels in this screen.

Table 64 Site-Wide > Monitor > Applications

LABEL	DESCRIPTION
Applications	<p>In Application view, select to view all applications, or only applications with bandwidth or block policies applied.</p> <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> 
	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.
Status	This shows whether the application or category is blocked or allowed within the current site.
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>
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.
Block / Unblock	Blocks or unblocks the application or application category on the site's gateway.
Application-View Fields	
Application	This shows the application name.
Limited interface	This shows the site gateway's interfaces that have bandwidth restriction policies on the for the application.
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, device login password and firmware upgrade schedule. Click **Site-Wide > Configure > General Settings** to access this screen.

**Figure 83** Site-Wide > Configure > General settings

The screenshot shows the 'General settings' page for a site-wide configuration. The page is divided into several sections:

- Site information:** Includes fields for 'Site name' (Taipei), 'Gateway type' (USG FLEX), and 'Local time zone' (Taiwan, Asia - Taipei (UTC +...)).
- Device configuration:** Includes 'Local credentials' with 'Username: admin (USG FLEX username is "support")' and a 'Password' field (masked with asterisks). A note below the password field states: '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: ~ ! @ # \$ % ^ & \* ( ) \_ + ' - = { } ; : < > .'. There is also a 'Smart guest/VLAN network' toggle (Beta) which is turned on, with a 'What is this?' link.
- Captive portal reauthentication:** Includes four dropdown menus for reauthentication frequency: 'For my AD server users', 'For my RADIUS server users', 'For click-to-continue users', and 'For cloud authentication users', all set to 'Every day'.
- SNMP:** Includes an 'SNMP access' dropdown menu set to 'Disable'.



**Reporting**

Syslog server  [+ Add](#)

**AP traffic log** Beta

**Voucher settings**

See [Using Vouchers](#) for more information

Duration text:   This text will precede the duration 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** i

API token:

The following table describes the labels in this screen.

Table 65 Site-Wide > Configure > General settings

LABEL	DESCRIPTION
Site Information	
Site name	Enter a descriptive name for the site.
Gateway	Click this to select whether the sites will contain a USG FLEX or NSG device as its security gateway. This choice changes which settings are available within the site, and changes the gateway menu between <b>Security Gateway</b> and <b>USG FLEX</b> .  Note: If you have added a security gateway device to the site, then this field is set automatically and cannot be edited.
Local time zone	Choose the time zone of the site's location.
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 device's built-in web-based configurator. The settings here apply to all Nebula devices in this site.
Smart guest/ VLAN network	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 gateway in the same site to ensure guest network connectivity.  The guest settings you configure for a gateway interface (in <b>Security Gateway &gt; Configure &gt; Interfaces addressing</b> ) will also apply to the wireless networks (SSIDs) associated with the same VLAN ID (in <b>AP &gt; Configure &gt; SSID overview</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.
Captive portal reauthentication	

Table 65 Site-Wide &gt; Configure &gt; General settings (continued)







LABEL	DESCRIPTION								
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 an 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 devices in this site. Otherwise, select <b>Disable</b> .								
SNMP community string	This field is available when you select <b>V1/V2c</b> . Enter the password for the incoming SNMP requests from the management station.								
Reporting									
Syslog server	Click <b>Add</b> to create a new entry.								
Server IP	Enter the IP address of the server.								
Types	Select the type of logs the server is for.  Note: Besides sending <b>Gateway traffic log</b> to a Syslog server, you can also set the security gateway (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 gateway clients.								
Action	Click the <b>Delete</b> icon to remove the entry.								
AP traffic log	Log traffic for APs in the site that have NAT Mode set to <b>Use Zyxel DHCP &amp; NAT</b> . You can also send the logs to a Syslog server, by selecting <b>AP traffic log</b> under <b>Syslog server &gt; Types</b> .  For details on configuring <b>NAT Mode</b> , see <a href="#">Section 11.3.2 on page 389</a> .								
Voucher settings	Use these settings to configure how WiFi network authentication vouchers for this site look when printed.  <table border="1" data-bbox="532 1262 1005 1612"> <tr> <td rowspan="2"></td> <td colspan="2"><b>SSID: SSID1</b></td> </tr> <tr> <td><b>Duration Text</b> 12</td> <td><b>Access Text</b> 47258595</td> </tr> <tr> <td><b>Promotion Text</b></td> <td colspan="2"></td> </tr> </table> For more information on vouchers, see <a href="#">Section 7.1.6 on page 161</a> .		<b>SSID: SSID1</b>		<b>Duration Text</b> 12	<b>Access Text</b> 47258595	<b>Promotion Text</b>		
	<b>SSID: SSID1</b>								
	<b>Duration Text</b> 12	<b>Access Text</b> 47258595							
<b>Promotion Text</b>									
Duration test	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.								

Table 65 Site-Wide &gt; Configure &gt; General settings (continued)

LABEL	DESCRIPTION
Promotion text	Sets the promotional text on the voucher. This text is optional. The text must consist of 1 – 16 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 a logo	Click this button to upload an image from your local computer.
Replace this logo	Click this button to change the uploaded image.
Remove this logo	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.
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.

Figure 84 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 Upload a logo

No 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

**Block**

Block wireless client

**Quarantine**

Quarantine VLAN Set

**Exempt list**

IP or MAC

The following table describes the labels in this screen.

Table 66 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 an 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 200KB, and images larger than 244x190 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> Type 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 66 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	Type how long a suspect client should be blocked or quarantined. You can type 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 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 85 Site-Wide &gt; Configure &gt; Collaborative Detection &amp; Response &gt; Quarantine

Each field is explained in the following table.

Table 67 Site-Wide &gt; Configure &gt; Collaborative Detection &amp; Response &gt; 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.

Table 67 Site-Wide &gt; Configure &gt; Collaborative Detection &amp; Response &gt; Quarantine (continued)

LABEL	DESCRIPTION
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's 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 gateway 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 gateway begins allocating IP addresses for this VLAN.
Pool size	
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 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 86** Site-Wide > Configure > 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 68 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 NCC 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	

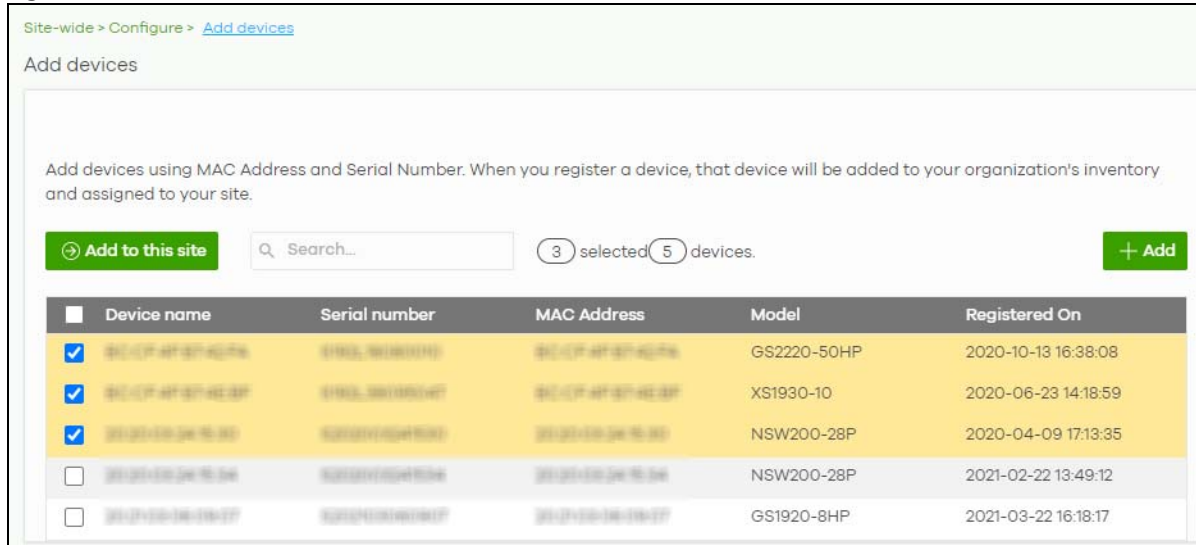
Table 68 Site-Wide &gt; Configure &gt; Alert settings (continued)

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 gateway	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 gateway device goes offline.</li> <li>• Any DHCP pool on the gateway device runs out of IP addresses.</li> <li>• A VPN connection to or from the gateway device is established or disconnected.</li> <li>• The WAN connectivity status changed</li> </ul>
Other alerts	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.
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 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 device owner at myZyxel or remove an Organization from the NCC. Please configure your device owners and organizations carefully. See also [Section 6.3.2 on page 98](#).

**Figure 87** Site-Wide > Configure > Add devices

The following table describes the labels in this screen.

**Table 69** Site-Wide > Configure > Add devices

LABEL	DESCRIPTION
Add to this site	Click this button to assign the selected devices to the site.
Search	Enter a keyword to filter the list of devices by device name, serial number, MAC address, or model.
N devices	This shows the number of registered 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 device's serial number and MAC address to register it at the NCC. For details, see <a href="#">Section 6.3.2.5 on page 106</a> .
Device name	This shows the descriptive name of the device.
Serial number	This shows the serial number of the device.
MAC address	This shows the MAC address of the device.
Model	This shows the model name of the device.
Registered On	This shows the time and date that the 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 device. Click **Site-Wide > Configure > Firmware management** to access this screen.

**Figure 88** Site-Wide > Configure > Firmware management

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

Firmware management

Upgrade time   [What is this?](#)

---

All APs New firmware is available for APs in this site.  
You can reschedule upgrade time as you wish or upgrade now.

2020-06-09  UTC+8.0

Upgrade now

All Switches New firmware is available for Switches in this site.  
You can reschedule upgrade time as you wish or upgrade now.

2020-06-09  UTC+8.0

Upgrade now

Security Gateway The gateway in this site is using the latest available firmware.

---

Status  Device type  Tag  Model  Current version  Firmware status  Locked

[Upgrade Now](#) [+ Schedule Upgrade](#) 3 devices

<input type="checkbox"/>	Status	Device t...	Model	MAC	S/N	Current...	Firmwa...	Upgrade sc...
<input type="checkbox"/>	<span style="color: green;">●</span>	Security g...	NSG200	38-7F-14D7...	2017061708...	V1.33(ABL...	Up to date	No
<input type="checkbox"/>	<span style="color: green;">●</span>	Switch	NSW100-10	8C-8B-71A...	2018.1200...	V3.00(AB...	Upgrade a...	Follow upgrade
<input type="checkbox"/>	<span style="color: green;">●</span>	Access poi...	NAP102	88E0-43F...	20180208...	V6.00(AB...	Custom	Follow upgrade

The following table describes the labels in this screen.


**Table 70** Site-Wide > Configure > Firmware management

LABEL	DESCRIPTION
Upgrade time	Select the day of the week and time of the day to install the firmware. The changes you make here also apply to the <b>Site-Wide &gt; Configure &gt; General setting</b> screen after you click <b>Save</b> .
All APs	This section is grayed out if there is no AP in this site. Set a new schedule for the firmware upgrade and select <b>On</b> to enable the schedule. The changes you make here also apply to the <b>Site-Wide &gt; Configure &gt; General setting</b> screen after you click <b>Save</b> .
All Switches	This section is grayed out if there is no switch in this site. Set a new schedule for the firmware upgrade and select <b>On</b> to enable the schedule. The changes you make here also apply to the <b>Site-Wide &gt; Configure &gt; General setting</b> screen after you click <b>Save</b> .

Table 70 Site-Wide &gt; Configure &gt; Firmware management (continued)

LABEL	DESCRIPTION				
Security Gateway	<p>This section is grayed out if there is no gateway in this site.</p> <p>Set a new schedule for the firmware upgrade and select <b>On</b> to enable the schedule.</p> <p>The changes you make here also apply to the <b>Site-Wide &gt; Configure &gt; General setting</b> screen after you click <b>Save</b>.</p>				
Status/Device Type/ Tag/Model/Current Version/Firmware Status/Locked	Specify your desired filter criteria to filter the list of devices.				
Upgrade Now	<p>Click this to immediately install the firmware on the selected devices.</p> <p>This button is selectable only when there is firmware update available for all the selected devices.</p>				
Schedule Upgrade	<p>Click this to pop up a window where you can create a new schedule for the selected devices.</p> <p>You can select to upgrade firmware according to the side-wide schedule configured for all devices in the site, create a recurring schedule, or edit the schedule with a specific date and time when firmware update is available for all the selected devices.</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 devices. If the NCC service is downgraded from Nebula Professional Pack to Nebula, the devices automatically changes to adhere to the side-wide schedule.</p> <div data-bbox="537 932 1295 1423" style="border: 1px solid black; padding: 10px;"> <p><b>Schedule firmware</b> <span style="float: right;">✕</span></p> <p>Site timezone: UTC +8.0</p> <p><input checked="" type="radio"/> Follow global setting. <a href="#">What is this?</a></p> <p><input type="radio"/> Every <span>Week</span> on <span>Monday</span> at <span>02:00</span></p> <p><input type="radio"/> Schedule the upgrade for: <span>2019-10-25</span> at <span>00:00</span> <a href="#">What is this?</a></p> <p>Below devices will be upgrade as required time.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Device type</th> <th style="text-align: right;"># of devices</th> </tr> </thead> <tbody> <tr> <td>Switch</td> <td style="text-align: right;">1</td> </tr> </tbody> </table> <p style="text-align: right;">Cancel <span style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">Add</span></p> </div>	Device type	# of devices	Switch	1
Device type	# of devices				
Switch	1				
Status	<p>This shows the status of the device.</p> <ul style="list-style-type: none"> <li>Green: The device is online and has no alerts.</li> <li>Amber: The device has alerts.</li> <li>Red: The device is offline.</li> <li>Gray: The device has been offline for 7 days or more.</li> </ul>				
Device Type	This shows the type of the device.				
Model	This shows the model number of the device.				
Tag	This shows the tag created and added to the device.				
Name	This shows the descriptive name of the device.				
MAC	This shows the MAC address of the device.				
S/N	This shows the serial number of the device.				

Table 70 Site-Wide &gt; Configure &gt; Firmware management (continued)

LABEL	DESCRIPTION
Current version	This shows the version number of the firmware the device is currently running. It shows <b>N/A</b> when the device goes off-line and its firmware version is not available.
Firmware status	This shows whether the firmware on the device is <b>Up to date</b> , there is firmware update available for the device ( <b>Upgrade available</b> ), custom firmware was installed manually ( <b>Custom</b> ), a specific version of firmware has been installed by Zyxel customer support ( <b>Dedicated</b> ) or the device goes off-line and its firmware status is not available ( <b>N/A</b> ).  The status changes to <b>Upgrading...</b> after you click <b>Upgrade Now</b> to install the firmware immediately.
Upgrade scheduled	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 device sticks to the site-wide schedule or <b>No</b> when the firmware on the device is up-to-date or the device goes off-line and its firmware status is not available.  A lock icon displays if a specific schedule is created for the device, which means the device firmware will not be upgraded according to the schedule configured for all devices in the site.
Last upgrade time	This shows the last date and time the firmware was upgraded on the 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.

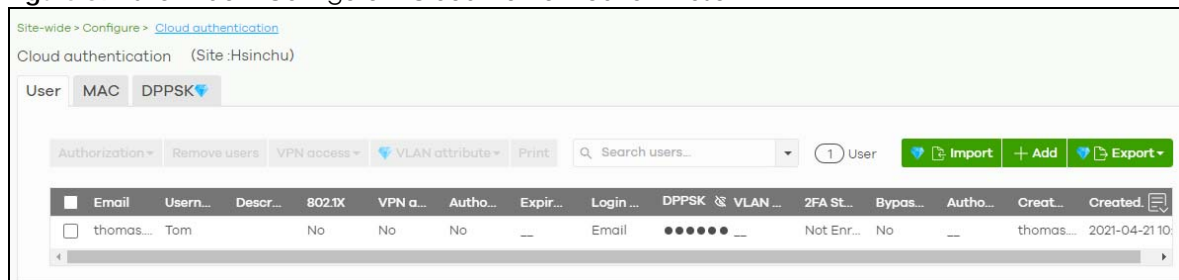
Note: The changes you made in this screen apply only to the current site. To change the cloud authentication settings for all sites in the organization, go to **Organization-wide > Configure > Cloud Authentication** (see [Section 7.2.7 on page 186](#)).

Note: For more information on user account types, see [Section 6.3.5.1 on page 120](#).

### 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 these screen.

**Figure 89** Site-wide > Configure > Cloud Authentication > User



Email	User...	Descr...	802.1X	VPN a...	Autho...	Expir...	Login ...	DPPSK	VLAN ...	2FA St...	Bypas...	Autho...	Creat...	Created
<input type="checkbox"/>	thomas...	Tom	No	No	No	--	Email	●●●●●●	--	Not Enr...	No	--	thomas...	2021-04-21 10:...

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

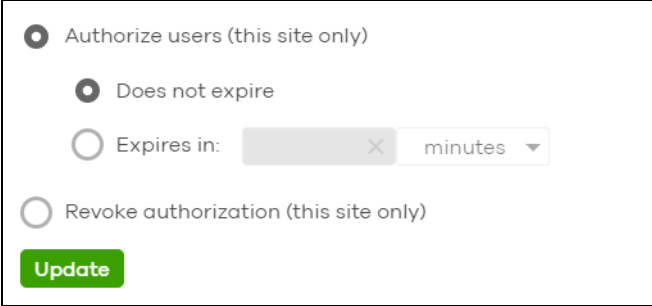
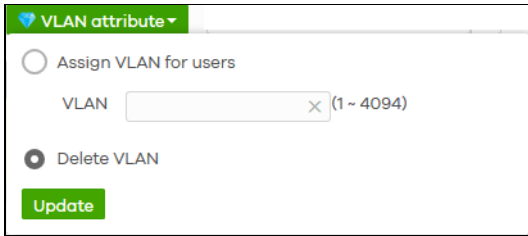
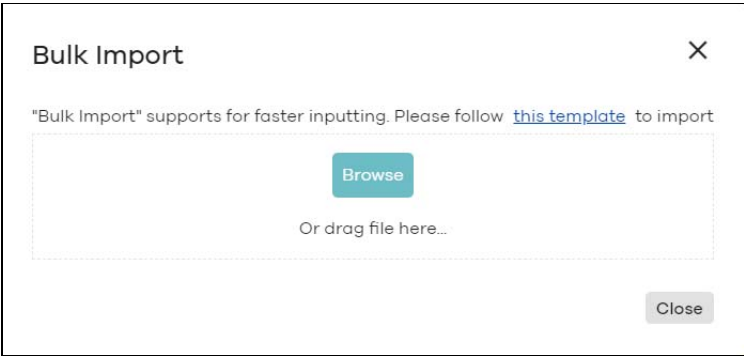

LABEL	DESCRIPTION
Authorization	<p>Select one or more than one user account and click this button to configure the authorization settings for the selected user accounts.</p> 
Remove users	<p>Select one or more than one user account and click this button to remove the selected user accounts.</p>
VPN access	<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 username 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> 
Add	<p>Click this button to create a new user account. See <a href="#">Section 7.2.7.2 on page 188</a>.</p>
Export	<p>Click this button to save the account list as a CSV or XML file to your computer.</p>

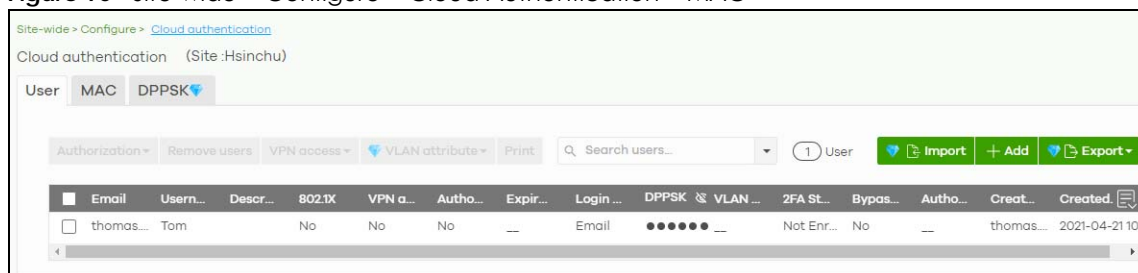
Table 71 Site-wide &gt; Configure &gt; Cloud Authentication &gt; User (continued)

LABEL	DESCRIPTION
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 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.

### 7.2.7.2 Cloud Authentication MAC Screen

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

Figure 90 Site-wide &gt; Configure &gt; Cloud Authentication &gt; MAC



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 72 Site-wide &gt; Configure &gt; Cloud Authentication &gt; MAC

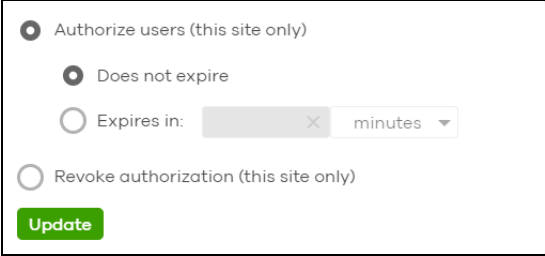
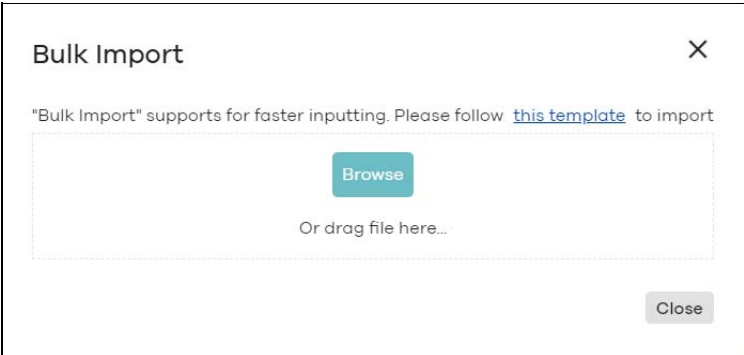

LABEL	DESCRIPTION
Authorization	<p>Select one or more than one account and click this button to configure the authorization settings for the selected user accounts.</p> 
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
Search users	Enter 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 190</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 this 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 admins 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>

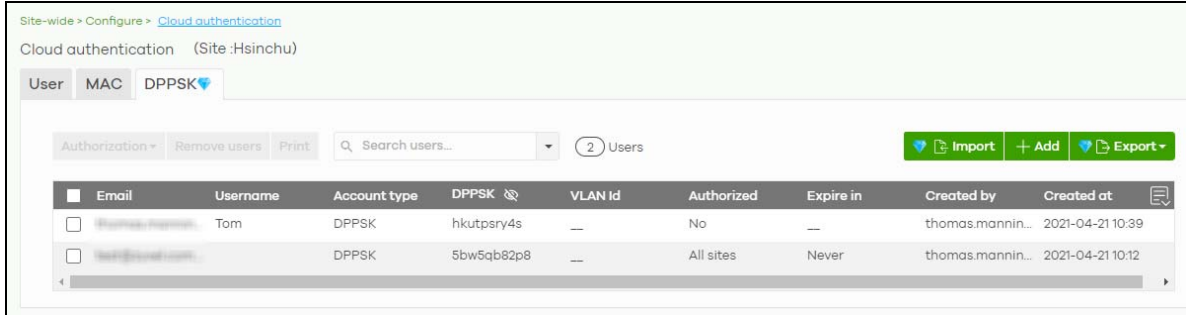
Table 72 Site-wide > Configure > Cloud Authentication > MAC (continued)

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 91 Site-wide > Configure > Cloud Authentication > DPPSK



The following table describes the labels in this screen.

Table 73 Side-wide > Configure > Cloud Authentication > DPPSK




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> <div style="border: 1px solid black; padding: 5px;"> <p><input checked="" type="radio"/> Authorize users (this site only)</p> <p style="margin-left: 20px;"><input checked="" type="radio"/> Does not expire</p> <p style="margin-left: 20px;"><input type="radio"/> Expires in: <input type="text"/> minutes</p> <p><input type="radio"/> Revoke authorization (this site only)</p> <p><input type="button" value="Update"/></p> </div>
Remove users	Select one or more than one user account and click this button to remove the selected user accounts.
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 wireless network access.</p> <div style="text-align: center; margin-top: 10px;"> <p>DPPSK</p> <div style="border: 1px solid black; padding: 10px; display: flex; justify-content: space-around;"> <div style="text-align: center;">  nduzjauv9f Expired in: Never                     </div> <div style="text-align: center;">  paatdtcgh4 Expired in: Never                     </div> </div> </div>
Search users	Enter a key word as the filter criteria to filter the list of user accounts.

Table 73 Side-wide &gt; Configure &gt; Cloud Authentication &gt; DPPSK (continued)

LABEL	DESCRIPTION
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="493 386 1235 737" 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="border: 1px dashed gray; padding: 5px; text-align: center;"> <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 128</a>.</li> <li>• Batch create DPPSK: See <a href="#">Section 6.3.5.8 on page 130</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 this 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.
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.

# CHAPTER 8

# Security Gateway

## 8.1 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.

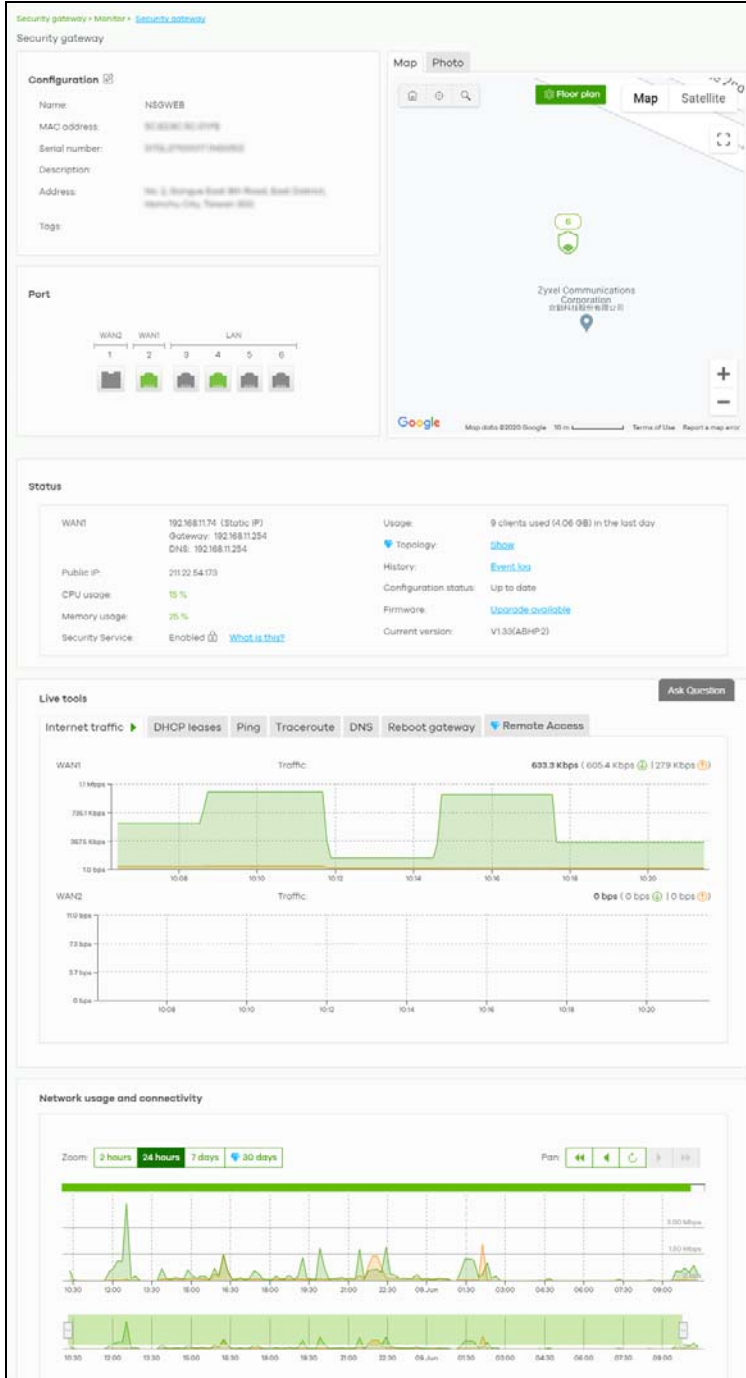
## 8.2 Monitor

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

### 8.2.1 Security Gateway

This screen allows you to view the detailed information about a security gateway in the selected site. Click **Security Gateway > Monitor > Security Gateway** to access this screen.

Figure 92 Security Gateway > Monitor > Security Gateway



The following table describes the labels in this screen.

Table 74 Security Gateway > Monitor > Security Gateway

LABEL	DESCRIPTION
Configuration	Click the edit icon to change the device name, description, tags and address. You can also move the device to another site.
Name	This shows the descriptive name of the gateway.

Table 74 Security Gateway &gt; Monitor &gt; Security Gateway (continued)

LABEL	DESCRIPTION
MAC address	This shows the MAC address of the gateway.
Serial number	This shows the serial number of the gateway.
Description	This shows the user-specified description for the gateway.
Address	This shows the user-specified address for the gateway.
Tags	This shows the user-specified tag for the gateway.
Port	This shows the ports on the gateway. The port is highlighted in green color when it is connected and the link is up. Move the pointer over a port to see additional port information, such as its name, MAC address, type, and connection speed.
Name	This shows the descriptive name of the port.
Status	This shows the connection status of the port.
MAC address	This shows the MAC address of the port.
Speed	This shows the current connection speed of the port. If the speed is unavailable, this displays "Ethernet".
LLDP	This shows the LLDP information received on the port.
Map	This shows the location of the gateway on the Google map.
Photo	This shows the photo of the gateway. 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 gateway.
CPU usage	This shows what percentage of the gateway's processing capability is currently being used.
Memory usage	This shows what percentage of the gateway's RAM is currently being used.
Security Service:	This shows whether Nebula Security Services (NSS) are enabled on the gateway. 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 gateway's clients.
Topology	Click <b>Show</b> to go to the <b>Site-Wide &gt; Monitor &gt; Topology</b> screen. See <a href="#">Section 7.1.5 on page 160</a> .
History	Click <b>Event log</b> to go to the <b>Gateway &gt; Monitor &gt; Event log</b> screen.
Configuration status	This shows whether the configuration on the gateway is up-to-date.
Firmware	This shows whether the firmware installed on the gateway is up-to-date.
Current version	This shows the firmware version currently installed on the 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 gateway sends queries for ping.

Table 74 Security Gateway &gt; Monitor &gt; Security Gateway (continued)

LABEL	DESCRIPTION
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	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 gateway.
Remote Access	This option is available only for the 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.

## 8.2.2 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 150](#).

## 8.2.3 Event Log

Use this screen to view gateway 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 93 Gateway &gt; Monitor &gt; Event log

Security gateway > Monitor > [Event log](#)

Event log

Keyword:  Category:

Before 2019-10-29 10:56 1h UTC+8

338 Event log

Time	Category	Source	Destination	Detail
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	ISAKMP SA [S201711070315] is disconnected
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	The cookie pair is : 0xa8c4726c50064617 / 0x6f8f4...
2019-10-29 09:56:53	VPN	61.216.142.42	192.168.11.74	Recv:[NOTIFY:NO_PROPOSAL_CHOSEN]
2019-10-29 09:56:53	VPN	61.216.142.42	192.168.11.74	The cookie pair is : 0xa8c4726c50064617 / 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

## 8.2.4 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 8.3.6 on page 230](#) for more information.

Click **Security Gateway > Monitor > VPN Connections** to access this screen.



**Figure 94** 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	disconnected	0 bytes	0 bytes	-	-
	172.16.0.0/12					
	10.251.0.0/16					
<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 75** 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 security gateway, 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 security gateway 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 gateway.
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 security gateway since the VPN tunnel was established.
Outbound (Bytes)	This shows the amount of traffic that has gone through the VPN tunnel from the Nebula security gateway 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 gateway.

Table 75 Security Gateway &gt; Monitor &gt; VPN Connections (continued)

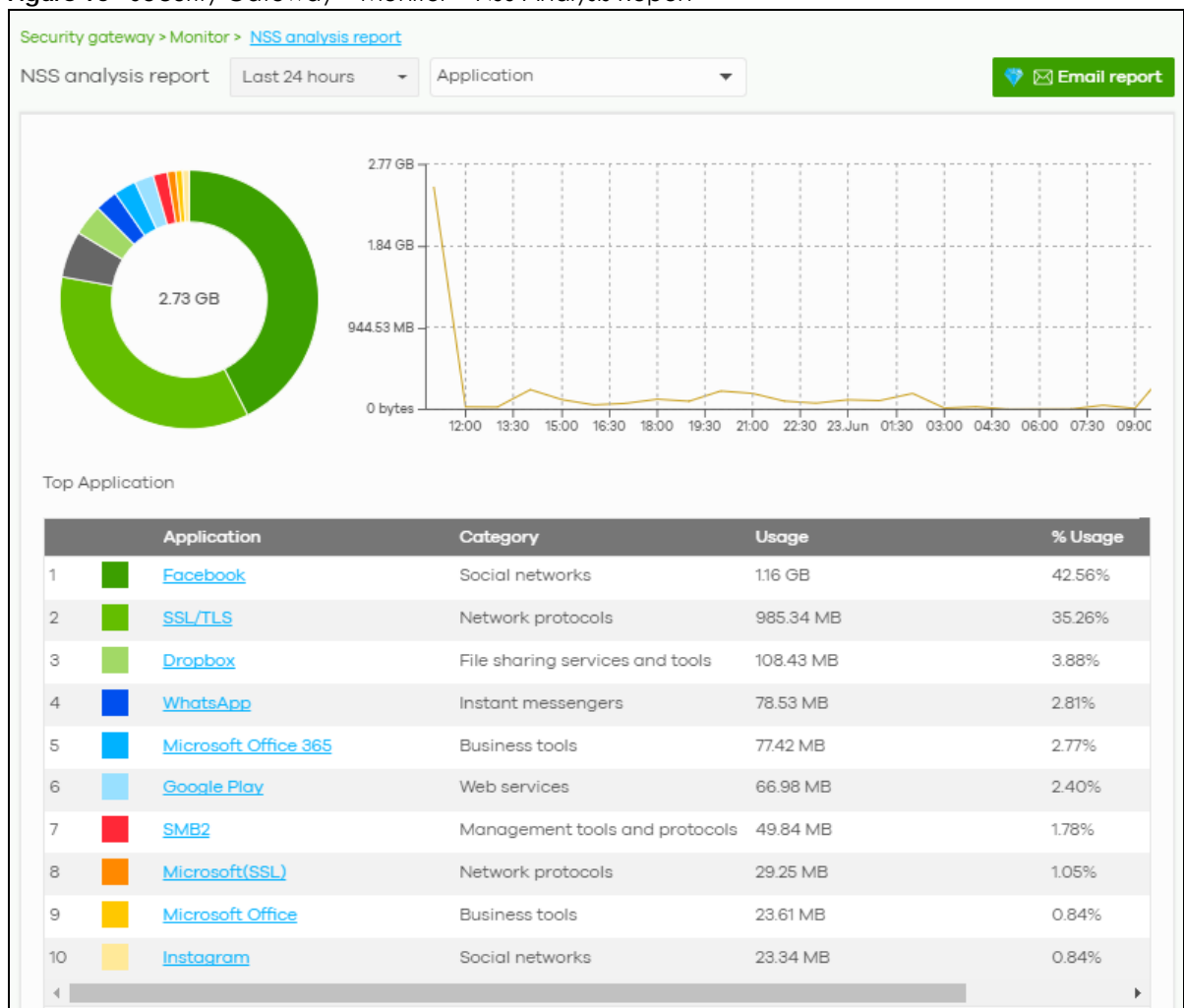
LABEL	DESCRIPTION
Assigned IP	This shows the IP address that the gateway assigned for the remote user's computer to use within the L2TP VPN tunnel.
Public IP	This shows the public IP address that the remote user is using to connect to the Internet.

## 8.2.5 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 95 Security Gateway &gt; Monitor &gt; NSS Analysis Report



The following table describes the labels in this screen.

Table 76 Security Gateway &gt; Monitor &gt; NSS Analysis Report

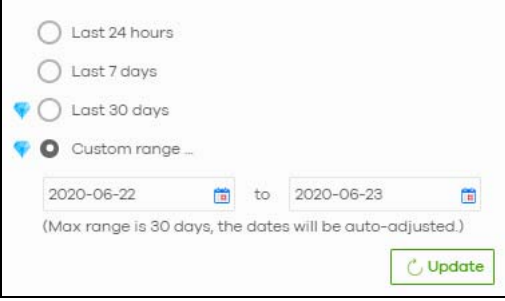
LABEL	DESCRIPTION
Security Gateway - NSS Analysis	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
	Select the type of service 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 8.2.3 on page 195</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 displays 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 gateway'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 gateway blocked access. Click a website URL to view the IPv4 addresses of the clients who tried to access the web page.

Table 76 Security Gateway &gt; Monitor &gt; NSS Analysis Report (continued)

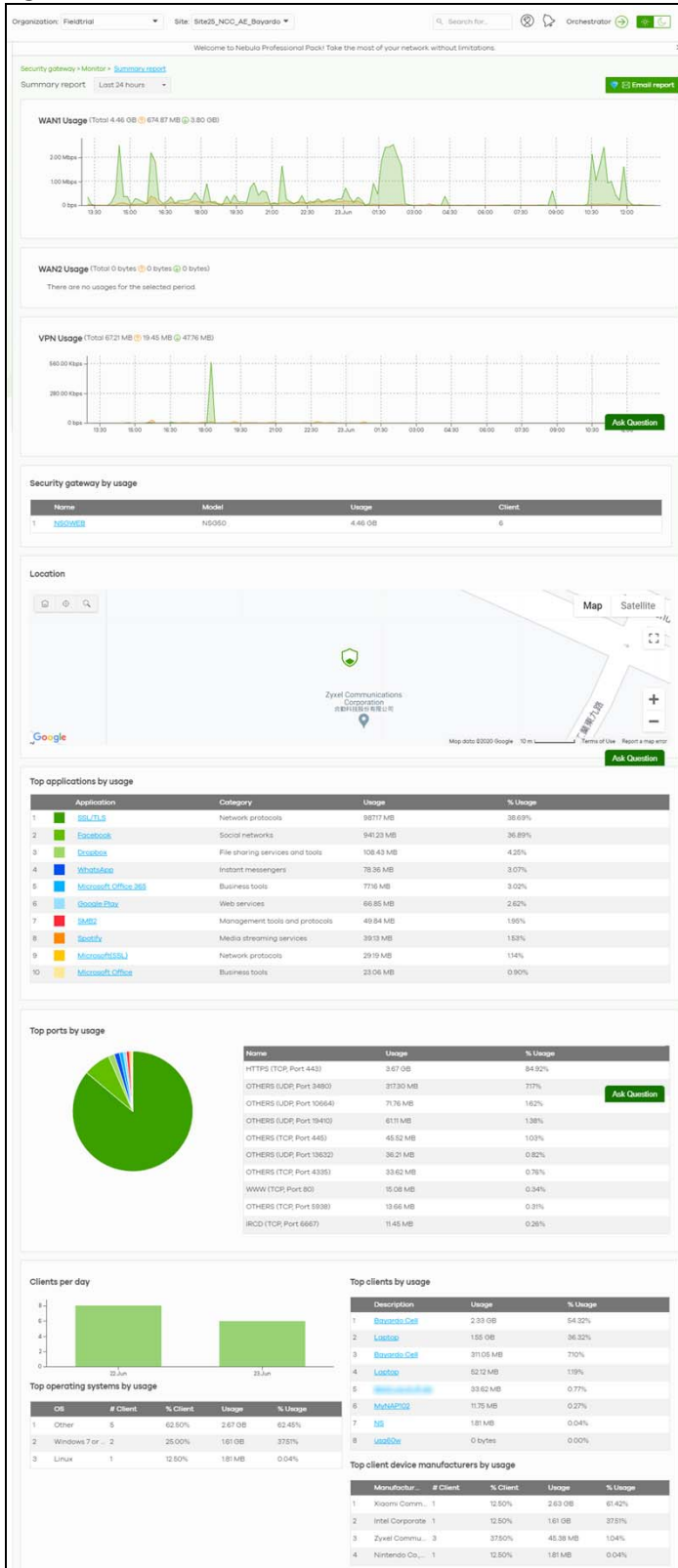
LABEL	DESCRIPTION
Description	This shows the name of the client who tried to access the web page. This field is available when you click the website URL. Click the name to display the individual client statistics. See <a href="#">Section 8.2.3 on page 195</a> .
IPv4 Address	This shows the IPv4 address 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 gateway 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 8.2.3 on page 195</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.

## 8.2.6 Summary Report

This screen displays network statistics for the gateway 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 96** Security Gateway > Monitor > Summary Report



The following table describes the labels in this screen.

Table 77 Security Gateway &gt; Monitor &gt; Summary Report

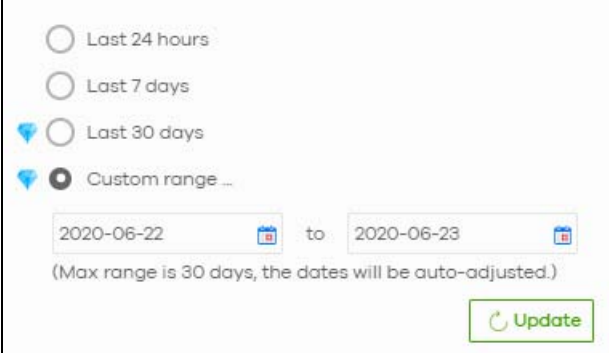
LABEL	DESCRIPTION
Security gateway - Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click 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 gateway.
Name	This shows the descriptive name of the Nebula gateway.
Model	This shows the model number of the Nebula gateway.
Usage	This shows the amount of data that has been transmitted through the gateway's WAN port.
Client	This shows the number of clients currently connected to the gateway.
Location	
	This shows the location of the Nebula gateways 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	
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	

Table 77 Security Gateway &gt; Monitor &gt; Summary Report (continued)

LABEL	DESCRIPTION
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.

## 8.3 Configure

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

### 8.3.1 Interface Addressing

Use this screen to configure network mode, port grouping, interface address, static route and DDNS settings on the gateway. 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 8.3.5 on page 227](#).

Figure 97 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 checked="" 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 78 Security Gateway > Configure > Interface addressing

LABEL	DESCRIPTION				
Network wide					
Mode	<p>Select <b>Network address translation (NAT)</b> to have the gateway automatically use SNAT for traffic it routes from internal interfaces to external interfaces.</p> <p>Select <b>Router</b> to have the gateway forward packets according to the routing policies. The gateway 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 gateway.				
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>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 1226 1247 1591" 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> </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	Facebook wifi	VLAN220
SSIDs	Interface				
Facebook wifi	VLAN220				
Port group	This shows the name of the port group to which the interface (network) belongs.				

Table 78 Security Gateway &gt; Configure &gt; Interface addressing (continued)





LABEL	DESCRIPTION
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 gateway.</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 wireless 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>
	Click this button to modify the network settings. See <a href="#">Section 8.3.1.1 on page 208</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 8.3.1.1 on page 208</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 security gateway's interfaces. It helps forward packets to their destinations.
	Click this button to modify the static route settings. See <a href="#">Section 8.3.2.4 on page 218</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 8.3.2.4 on page 218</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	<p>Select your Dynamic DNS service provider from the drop-down list box.</p> <p>If you select <b>User custom</b>, create your own DDNS service.</p>
DDNS type	<p>Select the type of DDNS service you are using.</p> <p>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.</p>
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 security gateway determines the IP address that is mapped to your domain name in the DDNS server. The security gateway uses the <b>Backup binding address</b> if the interface specified by these settings is not available.

Table 78 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 gateway 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 gateway and the DDNS server.</p> <p>Note: The gateway 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 gateway 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 gateway 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 gateway and the DDNS server.</p> <p>Note: The gateway 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 gateway 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, <a href="http://www.yourhost.dyndns.org">www.yourhost.dyndns.org</a> and still reach your hostname.</p>
Mail exchanger	<p>This option is only available with a DynDNS account.</p> <p>DynDNS can route e-mail for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes e-mail for <a href="mailto:john-doe@yourhost.dyndns.org">john-doe@yourhost.dyndns.org</a> 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 e-mail. With this service, DynDNS holds onto your e-mail 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>Type the IP address of the server that will host the DDSN service.</p>

Table 78 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. Type 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>

### 8.3.1.1 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 98** Security Gateway > Configure > Interface addressing: Local LAN

The following table describes the labels in this screen.

**Table 79** 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 gateway supports Link Aggregation Groups (LAGs). If the gateway does not support LAGs, then VLAN is the default interface type.

Table 79 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 security gateway provides to the network. Choices are:  <b>None</b> - the security gateway does not provide any DHCP services. There is already a DHCP server on the network.  <b>DHCP Relay</b> - the security gateway routes DHCP requests to one or more DHCP servers you specify. The DHCP servers may be on another network.  <b>DHCP Server</b> - the security gateway assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The security gateway is the DHCP server for the network.
These fields appear if the security gateway 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 security gateway is a <b>DHCP Server</b> .	
IP pool start address	Enter the IP address from which the security gateway 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 security gateway 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 security gateway 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 79 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 8.3.2.3 on page 216</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 security gateway assigns to computers connected to the interface. Otherwise, the security gateway 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.

## 8.3.2 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.

### 8.3.2.1 Interface Addressing with Link Aggregation Groups

If the gateway 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 99** 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	192.168.1.10	255.255.255.0		LAN1	<input type="checkbox"/>
LAG2	192.168.20.1	255.255.255.0		LAN5 LAN6	<input type="checkbox"/>

[+ Add](#)

---



**Static Route**

**Table 80** 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 gateway.
IP address	This shows the IP address of the interface (network).
Subnet mask	This shows the subnet mask of the interface (network).



Table 80 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="496 499 1248 863" 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> <p>SSIDs</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 70%;">Name</th> <th style="width: 30%;">Interface</th> </tr> </thead> <tbody> <tr> <td>Facebook wifi</td> <td>VLAN220</td> </tr> </tbody> </table> <p style="text-align: right;"> <span>Close</span> <span style="margin-left: 10px;">Update SSID &amp; continue</span> <span style="margin-left: 10px;">Continue</span> </p> </div>	Name	Interface	Facebook wifi	VLAN220
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 gateway.</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 wireless 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 8.3.1.1 on page 208</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 8.3.1.1 on page 208</a>.</li> <li>• For details on creating a link aggregation group, see <a href="#">Section 8.3.2.2 on page 213</a>.</li> </ul>				

### 8.3.2.2 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 100** Security Gateway > Configure > Interface addressing: Local LAN (LAG Interface Type)

The following table describes the labels in this screen.

**Table 81** 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 gateway supports Link Aggregation Groups (LAGs). If the gateway 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 81 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 gateway monitors the state of the local interface only. The gateway can't tell if the link can transmit or receive packets.</p> <p><b>arp</b> - The gateway monitors the link by sending ARP queries. The gateway 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 security gateway provides to the network. Choices are: <p><b>None</b> - the security gateway does not provide any DHCP services. There is already a DHCP server on the network.</p> <p><b>DHCP Relay</b> - the security gateway 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 security gateway assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The security gateway is the DHCP server for the network.</p>
These fields appear if the security gateway 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 security gateway is a <b>DHCP Server</b> .	
IP pool start address	Enter the IP address from which the security gateway 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 81 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 security gateway 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 security gateway works as a DNS relay.
First WINS server Second WINS server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: <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 8.3.2.3 on page 216</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 security gateway assigns to computers connected to the interface. Otherwise, the security gateway 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.

### 8.3.2.3 DHCP Option

Click the **Add new** button under **Extended options** in the **Security Gateway > Configure > Interfaces addressing: Local LAN** screen.

**Figure 101** Security Gateway > Configure > Interfaces addressing: Local LAN: DHCP Option

The following table describes the labels in this screen.

**Table 82** 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 82 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.

### 8.3.2.4 Static Route

Click the **Add** button in the **Static Route** section of the **Security Gateway > Configure > Interfaces addressing** screen.

Figure 102 Security Gateway &gt; Configure &gt; Interfaces addressing: Static Route

The following table describes the labels in this screen.

Table 83 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.

### 8.3.3 Policy Route

Use policy routes and static routes to override the security gateway'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 103** Security Gateway > Configure > Policy Route

Enabled	Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	Next-Hop
<input checked="" type="checkbox"/>	VPN	Any	Any	Any	10.253.81.6	Any	Hub

+ Add Each site can have at most 50 policy routes

The following table describes the labels in this screen.

**Table 84** 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 8.3.4.1 on page 225</a> for more information.

#### 8.3.3.1 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 104** Security Gateway > Configure > Policy Route: Add/Edit

The following table describes the labels in this screen.

**Table 85** Security Gateway > Configure > 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 gateway 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 gateway 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 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.
Close	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

### 8.3.4 Firewall

By default, a LAN user can initiate a session from within the LAN and the security gateway allows the response. However, the security gateway 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 security gateway has the following hidden default firewall rules: LAN to WAN is allowed, WAN to LAN is blocked.

Figure 105 Security Gateway > Configure > Firewall

Security gateway > Configure > [Firewall](#)

### Firewall

**Security policy**

Inbound rules: Inbound traffic will be restricted to this service in NAT settings.

Outbound rules:

Source	Destination	Dst port	Schedule	Description
any	10.253.61.5	any	Always	REDMINE ACCESS
192.168.250.1/24	any	any	Always	
Any	Any	Any	Always	Default rule

[+ Add](#)

Security gateway services:

Service	Allowed remote IPs
Ping	any
Web (local status & configuration)	none

---

**Application Patrol**

Application monitor:  on

Enable this option to allow traffic analysis with application patrol.

Application profiles:

Name	Description
1 applications	

[+ Add](#)

---

**Schedule profiles**

There are no **schedule profiles** defined for this site.

[+ Add](#)

---

**SIP ALG**

SIP ALG:  on

SIP Signaling Port: 5060

ADVANCED OPTIONS

SIP Inactivity Timeout:  on

SIP Media Inactivity Timeout: 120 seconds

SIP Signaling Inactivity Timeout: 1800 seconds

---

**NAT**

1:1 NAT: There are no 1:1 NAT mappings. [+ Add](#)

Virtual Server: There are no virtual server mappings. [+ Add](#)

The following table describes the labels in this screen.

Table 86 Security Gateway &gt; Configure &gt; Firewall





LABEL	DESCRIPTION
Security Policy	
Outbound 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 firewall 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 firewall takes the action set in the profile when traffic matches the application patrol signatures. See <a href="#">Section 8.3.4.1 on page 225</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 with which the computer is allowed to access the security gateway using the service. You can specify a range of IP addresses.  <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 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 8.3.4.1 on page 225</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 86 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 8.3.4.2 on page 226</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 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	
<p>1:1 NAT</p> <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 security gateway 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 security gateway 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 security gateway 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 86 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	
This makes computers on a private network behind the security gateway available to a public network outside the security gateway (like the Internet).	
	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 security gateway 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 security gateway 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.

### 8.3.4.1 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 security gateway 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 106** Security Gateway > Configure > Firewall: Add an application profile

The following table describes the labels in this screen.

**Table 87** 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 security gateway 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 security gateway routes packets that matches these application signatures. <b>Drop</b> - the security gateway silently drops packets that matches these application signatures without notification. <b>Reject</b> - the security gateway 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.

### 8.3.4.2 Create new schedule

Click the **Add** button in the **Schedule Profiles** section of the **Security Gateway > Configure > Firewall** screen to access this screen.

**Figure 107** 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"/>
Monday	<input checked="" type="radio"/>
Tuesday	<input checked="" type="radio"/>
Wednesday	<input checked="" type="radio"/>
Thursday	<input checked="" type="radio"/>
Friday	<input checked="" type="radio"/>

Close

The following table describes the labels in this screen.

**Table 88** 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.

### 8.3.5 Security Service

Use this screen to enable or disable the features available in the security pack for your security gateway, 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 108 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 89 Security Gateway &gt; Configure &gt; Security Service

LABEL	DESCRIPTION
Content Filtering	
Enabled	Click <b>ON</b> to enable the content filtering feature on the security gateway. Otherwise, click <b>OFF</b> to disable it.
Interface	This shows the name of the interfaces created on the security gateway. 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 security gateway 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 do 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 security gateway 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 89 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 security gateway. 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	<p>For a black list entry, specify a pattern to identify the names of files that the security gateway should log and delete.</p> <p>For a white list entry, specify a pattern to identify the names of files that the security gateway 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 security gateway 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 gateway checks up to the first 80 characters of a file name.</li> </ul>
Intrusion Detection / Prevention	
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.

### 8.3.6 Site-to-Site VPN

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

Click **Security Gateway > Configure > Site-to-Site VPN** to access this screen.

**Figure 109** Security Gateway > Configure > Site-to-Site VPN

Security gateway > Configure > Site-to-Site VPN

Site-to-Site VPN

Outgoing interface: WAN1

Local networks:

Name	Subnet	Use VPN
LAN1	192.168.16.0/24	<input type="checkbox"/>
LAN2	192.168.17.0/24	<input type="checkbox"/>

VPN Area: Default

Nebula VPN enable:

**Site-wide settings**

Options in this section apply to this Nebula gateway only.

**Non-Nebula VPN peers**

[+ Add](#)

The following table describes the labels in this screen.

Table 90 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.
Prefer uplink	Specify the primary WAN interface through which the security gateway forwards VPN traffic when you set <b>Outgoing Interface</b> to <b>AUTO</b> .
Local networks	This shows the local networks behind the security gateway.
Name	This shows the network name.
Subnet	This shows the IP address and subnet mask of the computer on the network.
VPN Area	Select the VPN area of the site. For details, see <a href="#">Section 6.3.9.2 on page 143</a> .
Nebula 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.

Table 90 Security Gateway &gt; Configure &gt; Site-to-Site VPN (continued)

LABEL	DESCRIPTION
Nebula VPN Topology	<p>This shows the VPN mode supported by the security gateway.</p> <p>Select a VPN topology.</p> <p>Select <b>Disable</b> to not set a VPN connection.</p> <p>In the <b>Site-to-Site</b> VPN topology, the remote IPSec device has a static IP address or a domain name. This security gateway can initiate the VPN tunnel.</p> <p>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.</p> <p>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.</p>
Hubs (peers to connect to)	<p>This field is available when you set <b>Topology</b> to <b>Hub-and-Spoke</b>. The field is configurable only when the security gateway of the selected site is the hub router.</p> <p>You can select another site's name to have the gateway of that site act as the hub router in the <b>Hub-and-Spoke</b> VPN topology.</p>
NAT traversal	<p>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.</p>
Server (client to connect to)	<p>This field is available when you set <b>Topology</b> to <b>Server-and-Client</b>. The field is configurable only when the security gateway of the selected site is the VPN server.</p> <p>You can select another site's name to have the gateway of that site act as the VPN server.</p>
Client-to-Client communication	<p>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 security gateway of the selected site is the VPN server.</p>
Remote VPN participants	<p>This shows the remote (peer) Nebula gateway's network name and address.</p>
Non-Nebula VPN peers	<p>If the remote VPN gateway is not a Nebula device, use this section to set up a VPN connection between it and the Nebula security gateway.</p>
Enabled	<p>Select the check box to turn on the rule. Otherwise, clear the check box to turn off the rule.</p>
Name	<p>Enter the name of the peer gateway.</p>
Public IP	<p>Enter the public IP address of the peer gateway.</p>
Private Subnet	<p>Enter the local network address or subnet behind the peer gateway.</p>
IPSec policy	<p>Click to select a pre-defined policy or have a custom one. See <a href="#">Section 8.3.6.1 on page 232</a> for detailed information.</p>
Preshared secret	<p>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.</p>
Availability	<p>Select <b>All sites</b> to allow the peer gateway to connect to any Nebula security gateway in the organization through a VPN tunnel.</p> <p>Select <b>This site</b> and the peer gateway can only connect to the Nebula security gateway in this site through a VPN tunnel.</p> <p>You can also configure any specific sites in the organization,</p>
Action	<p>Click the remove icon to delete the entry.</p>
Add	<p>Click this button to add a peer VPN gateway to the list.</p>

### 8.3.6.1 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 110** 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 91** 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 91 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 security gateway 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 security gateway 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 security gateway'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 security gateway and the remote IPSec router must use the same negotiation mode.</p>
Local ID	<p>Type the identity of the security gateway during authentication. <b>Any</b> indicates that the remote IPSec router does not check the identity of the security gateway.</p>
Peer ID	<p>Type the identity of the remote IPSec router during authentication. <b>Any</b> indicates that the security gateway 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 91 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 security gateway 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 security gateway 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>Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The security gateway 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.

## 8.3.7 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 111** Security Gateway > Configure > Remote access VPN

The screenshot shows the 'Remote access VPN' configuration page. At the top, there is a breadcrumb trail: 'Security gateway > Configure > Remote access VPN'. Below this, the page title 'Remote access VPN' is displayed. The configuration is divided into two main sections, each with a toggle switch and several input fields.

**IPSec VPN server section:**

- IPSec VPN server:** A green toggle switch is turned on. A 'Download VPN Client' link is visible in the top right corner.
- Outgoing interface:** A dropdown menu set to 'WAN1'.
- NAT traversal:** An empty text input field with an 'X' icon and '(IP or FQDN)' label.
- Client VPN subnet:** An empty text input field with an 'X' icon and a red asterisk.
- DNS name servers:** A dropdown menu set to 'Use Google Public DNS'.
- WINS:** A dropdown menu set to 'No WINS servers'.
- Secret:** An empty text input field with an eye icon and a red asterisk.
- Authentication:** A dropdown menu set to 'Nebula Cloud Authentication'.

**L2TP over IPSec VPN server section:**

- L2TP over IPSec VPN server:** A green toggle switch is turned on.
- Client VPN subnet:** An empty text input field with an 'X' icon and a red asterisk.
- DNS name servers:** A dropdown menu set to 'Use Google Public DNS'.
- WINS:** A dropdown menu set to 'No WINS servers'.
- Secret:** An empty text input field with an eye icon and a red asterisk.
- Authentication:** A dropdown menu set to 'Nebula Cloud Authentication'.

**VPN provision script:**

- VPN provision script:** A text input field containing 'E.g. nebula@zyxel.com' and a 'Send Email' button.



The following table describes the labels in this screen.

Table 92 Security Gateway &gt; Configure &gt; 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 security gateway. 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 security gateway 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 type 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 security gateway 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 security gateway. Otherwise, select <b>Disable</b> to turn it off.
Client VPN subnet	Specify the IP addresses that the security gateway 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 type 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 92 Security Gateway &gt; Configure &gt; Remote access VPN (continued)

LABEL	DESCRIPTION
Authentication	Select how the security gateway 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 gateway. The email contains two scripts; one for macOS 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>

### 8.3.8 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 112 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.

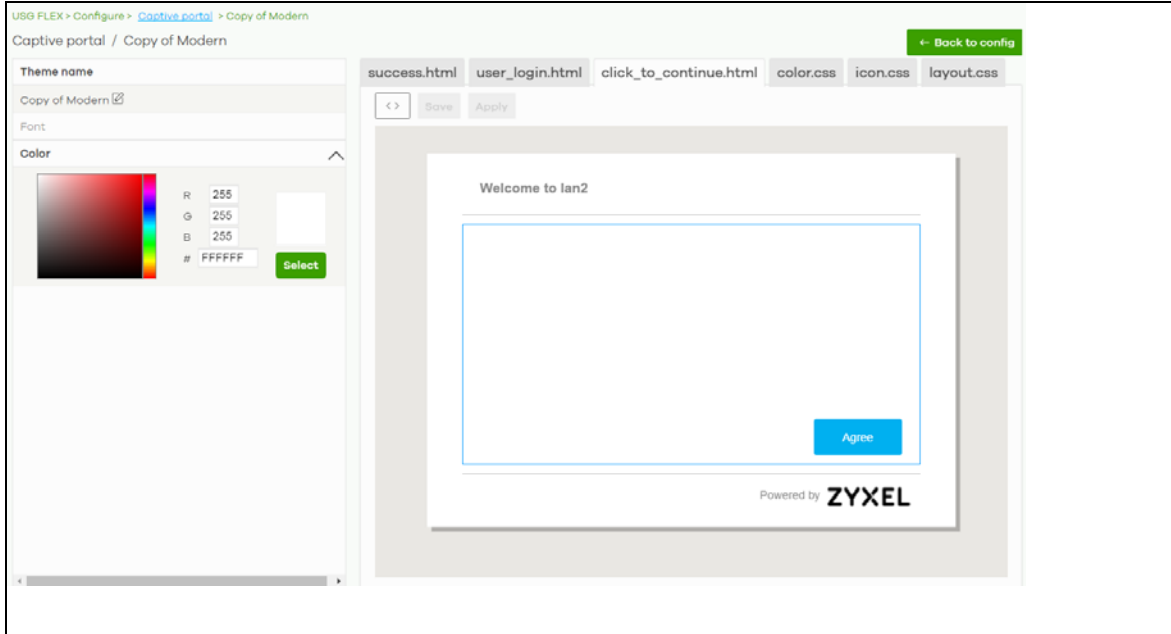
Table 93 Security Gateway > Configure > Captive portal

LABEL	DESCRIPTION
Interface	Select the gateway'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 corner 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 8.3.8.1 on page 240</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> .

### 8.3.8.1 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 113 Security Gateway &gt; Configure &gt; Captive portal: Edit



The following table describes the labels in this screen.

Table 94 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 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 on 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 a HTML file to display the portal page. You can also change colors and modify the CSS values of the selected HTML file.
<>	Click this button to view and modify the CSS values of the selected HTML file. It is recommended that you do NOT change the script code to ensure proper operation of the portal page.
⦿	Click this button to preview the portal page (the selected HTML file).
Save	Click this button to save your settings for the selected HTML file to the NCC.
Apply	Click this button to save your settings for the selected HTML file to the NCC and apply them to the security gateway in the site.

### 8.3.9 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 114** 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**

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 95 Gateway > Configure > Network access method

LABEL	DESCRIPTION
Interfaces	Select the gateway'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 8.3.11 on page 246</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 don't 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.

## 8.3.10 Traffic Shaping

Use this screen to configure maximum bandwidth and load balancing on the security gateway.

Click **Security Gateway > Configure > Traffic shaping** to access this screen.

**Figure 115** 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 96 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 security gateway chooses WAN 1 for 2 sessions' traffic and WAN 2 for 1 session's traffic in each round of 3 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 security gateway 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 security gateway 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 security gateway 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 security gateway will switch to the other one even if the primary WAN connection is still up. Make sure your security gateway 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 security gateway applies the rule.
Source Last IP	Enter the last IP address in a range of source IP addresses for which the security gateway applies the rule.
Destination IPs	<p>Enter the destination IP addresses for which the security gateway 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 security gateway 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 96 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 security gateway 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.

### 8.3.11 Gateway Settings

Use this screen to configure DNS settings and external AD (Active Directory) server or RADIUS server that the security gateway 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 gateway. The settings in this screen apply to all networks (interfaces) on the security gateway. 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 116 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 97 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 security gateway can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the security gateway 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 security gateway 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 security gateway 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 security gateway 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 8.3.11.1 on page 249</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 97 Security Gateway &gt; Configure &gt; Gateway settings (continued)

LABEL	DESCRIPTION
Port	Specify the port number on the RADIUS server to which the security gateway 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 security gateway.  The key is not sent over the network. This key must be the same on the external authentication server and the security gateway.
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 8.3.11.1 on page 249</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.

### 8.3.11.1 Advanced Settings

Click the **Advanced** column in the **Security Gateway > Configure > Gateway settings** screen to access this screen.

Figure 117 Security Gateway &gt; Configure &gt; Gateway settings: Advanced



The screenshot shows a dialog box titled "Advanced" with a close button (X) in the top right corner. It contains the following fields:

- Preset:** A dropdown menu with "Default" selected.
- Timeout:** A text input field containing "5", with a clear button (X) and "(1-300 seconds)" to its right.
- Case-Sensitive User Name:** A radio button labeled "off" is selected.
- NAS IP Address:** A text input field containing "1270.0.1", with a clear button (X) to its right.

At the bottom right, there are two buttons: "Close" (in a blue box) and "OK".

The following table describes the labels in this screen.

Table 98 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 security gateway 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 servers 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.  Type the IP address of the NAS (Network Access Server).

Table 98 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 9

## USG FLEX

### 9.1 Overview

This chapter describes the menus used to monitor and configure the USG FLEX device that is acting as a security gateway in the current organization.

Note: In this chapter, the Security Gateway is used to refer to the USG FLEX device.

### 9.2 Monitor

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

#### 9.2.1 USG FLEX

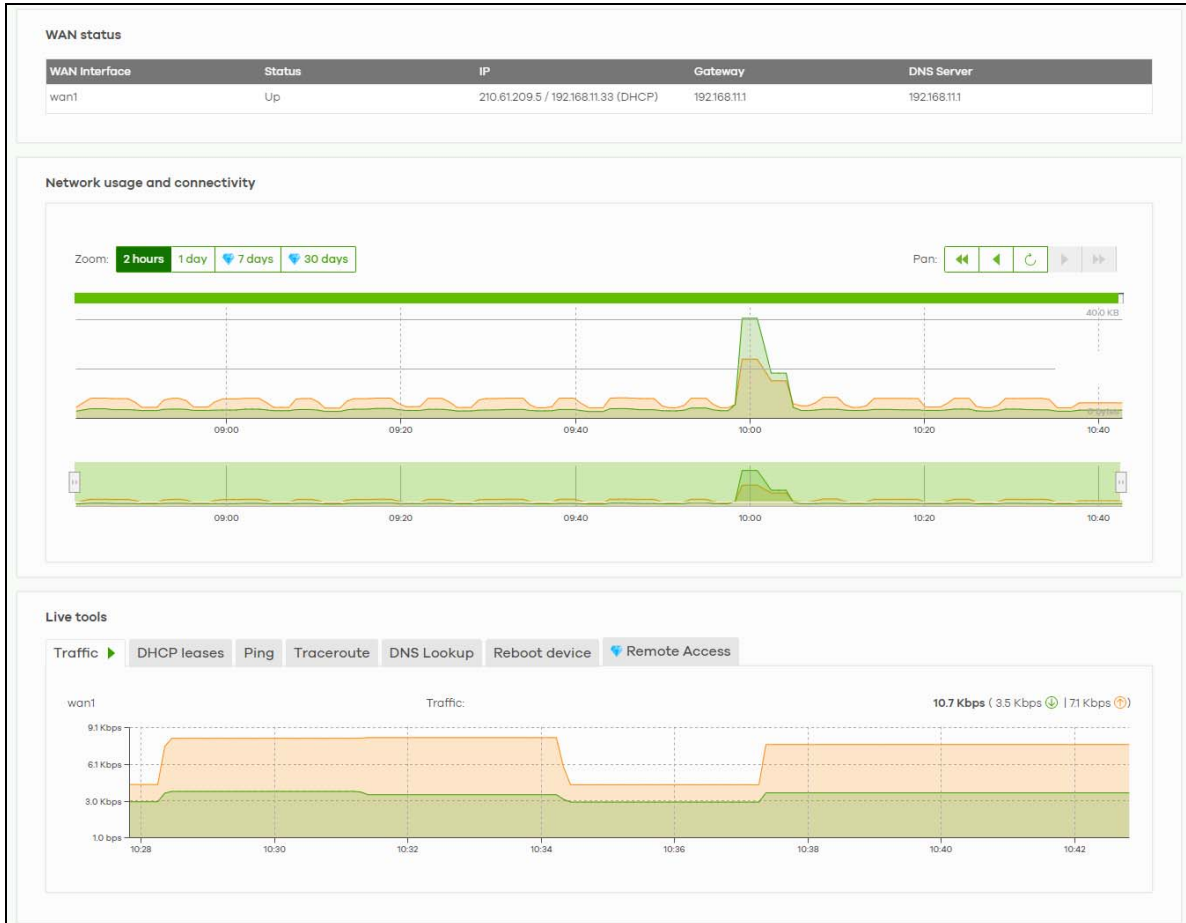
This screen allows you to view the detailed information about the Security Gateway in the selected site. Click **USG FLEX > Monitor > USG FLEX** to access this screen.

Figure 118 USG FLEX > Monitor > USG FLEX

The screenshot displays the 'USG FLEX' monitor page. It is divided into several sections:

- Configuration:** A table with fields for Name, MAC address, Serial number, Description, Address, and Tags. The serial number is 'S2:...' and includes '(USG FLEX 100W)'.
- Port:** A row of six port status icons labeled 1 through 6. Port 2 is highlighted in green, indicating it is active.
- Map:** A map interface with 'Map' and 'Photo' tabs. A 'Floor plan' button is active. A location marker with the number '2' is visible on the map.
- Status:** A summary of system metrics:
  - CPU usage: 3%
  - Memory usage: 53%
  - Session: 63
  - Usage: 3 clients used (3.67 MB) in the last day
  - Topology: [Show](#)
  - History: [Event Log](#)
  - Configuration status: Up to date
  - Firmware: [Upgrade available](#)
  - Current version: V5.00(ABWC.0)





The following table describes the labels in this screen.

Table 99 USG FLEX > Monitor > USG FLEX

LABEL	DESCRIPTION
Configuration	Click the edit icon to change the Security Gateway name, description, tags and address (physical location). You can also move the device to another site.
Name	This shows the descriptive name of the gateway.
MAC address	This shows the MAC address of the gateway's WAN port.
Serial number	This shows the serial number of the gateway.
Description	This shows the user-specified description for the gateway.
Address	This shows the user-specified address (physical location) for the gateway.
Tags	This shows the user-specified tags for the gateway.
Port	This shows the ports on the gateway. The port is highlighted in green color when it is connected and the link is up. Move the pointer over a port to see additional port information, such as its name, MAC address, type, and connection speed.
Port	This shows the identity number of the selected port.
Port Group	This shows the name of the port group that the port belongs to.
Status	This shows the connection status of the port.

Table 99 USG FLEX &gt; Monitor &gt; USG FLEX (continued)

LABEL	DESCRIPTION
Map	This shows the location of the gateway on Google Maps.
Photo	This shows the photo of the gateway. Click <b>Add</b> to upload one or more photos. Click <b>x</b> to remove a photo.
Status	
CPU usage	This shows what percentage of the gateway's processing capability is currently being used.
Memory usage	This shows what percentage of the gateway's RAM is currently being used.
Session	This shows how many sessions the gateway currently has. A session is a unique established connection that passes through, from, to, or within the gateway.
Usage	This shows the amount of data that has been transmitted or received by the gateway's clients.
Topology	Click <b>Show</b> to go to the <b>Site-Wide &gt; Monitor &gt; Topology</b> screen. See <a href="#">Section 7.1.5 on page 160</a> .
History	Click <b>Event log</b> to go to the <b>USG FLEX &gt; Monitor &gt; Event log</b> screen.
Configuration status	This shows whether the configuration on the gateway is <b>Up-to-date</b> .
Firmware	This shows whether the firmware installed on the gateway is <b>Up-to-date</b> .
Current version	This shows the firmware version currently installed on the 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 gateway 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 through which the gateway 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 device	Click the <b>Reboot</b> button to restart the Security Gateway.
Remote Access	This option is available only for the device owner. Establish a remote command line interface (CLI) connection to the 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 150](#).

## 9.2.3 Event Log

Use this screen to view gateway 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 **USG FLEX > Monitor > Event Log** to access this screen.

**Figure 119** USG FLEX > Monitor > Event log

Time	Category	Source	Destination	Detail
2021-01-11 16:21:00	VPN	61.216.142.39	111.249.71.200	IKE SA [SA_202009041737_22] is disconnected
2021-01-11 16:21:00	VPN	61.216.142.39	111.249.71.200	[INIT] Send:[SA][IKE][NONCE][NOTIFY][NOTIFY][NOTIFY][CERTREQ][VID][VID][VID][VID]
2021-01-11 16:21:00	VPN	111.249.71.200	61.216.142.39	Recv IKE sa: SA[0] protocol = IKE (1), AES CBC key len = 128, HMAC-SHA1 PRF, HMAC-SHA1-96, 1024 bit MODP, .)
2021-01-11 16:21:00	VPN	111.249.71.200	61.216.142.39	[INIT] Recv. [SA][IKE][NONCE][NOTIFY][NOTIFY][VID][VID][VID]
2021-01-11 16:21:00	VPN	111.249.71.200	61.216.142.39	Receiving IKEv2 request
2021-01-11 16:21:01	VPN	61.216.142.39	111.249.71.200	[SA] : No proposal chosen
2021-01-11 16:21:01	VPN	111.249.71.200	61.216.142.39	[AUTH] Recv.:[ID][CERT][CERTREQ][IDr][AUTH][SA][TSr][NOTIFY][NOTIFY][NOTIFY][NOTIFY]
2021-01-11 16:21:01	VPN	61.216.142.39	111.249.71.200	IKE SA [SA_202009041737_22] is disconnected
2021-01-11 16:21:01	VPN	61.216.142.39	111.249.71.200	IKE SA [SA_202009041737_22] is disconnected
2021-01-11 16:21:01	VPN	61.216.142.39	111.249.71.200	IPsec SA negotiation failed
2021-01-11 16:21:01	VPN	61.216.142.39	111.249.71.200	[ID] : Tunnel [SA_BB8CA3E60F0_11] Phase 2 Local policy mismatch
2021-01-11 16:21:01	VPN	61.216.142.39	111.249.71.200	IKE SA [SA_202009041737_22] is disconnected
2021-01-11 16:21:01	Myzyxel Dot Com			[SecuReporter] Parameter required. arg_cnt=8
2021-01-11 16:21:01	VPN	61.216.142.39	111.249.71.200	IKE SA [SA_202009041737_22] is disconnected
2021-01-11 16:21:03	VPN	61.216.142.39	192.168.188.19	The cookie pair is : 0xc88f69bfa8cd2d2e / 0x0000000000000000
2021-01-11 16:21:03	VPN	61.216.142.39	192.168.188.68	The cookie pair is : 0xc17b8f327435fd56 / 0x0000000000000000
2021-01-11 16:21:03	VPN	61.216.142.39	192.168.188.19	[INIT] Send:[SA][IKE][NONCE][NOTIFY][NOTIFY][VID][VID][VID]
2021-01-11 16:21:03	VPN	61.216.142.39	192.168.188.19	The cookie pair is : 0xc88f69bfa8cd2d2e / 0x0000000000000000
2021-01-11 16:21:03	VPN	61.216.142.39	192.168.188.19	Tunnel[SA_BB8CA3B4CC5B_21SA_BB8CA3B4CC5B_21] Send IKEv2 request
2021-01-11 16:21:03	VPN	61.216.142.39	192.168.188.68	The cookie pair is : 0xc17b8f327435fd56 / 0x0000000000000000
2021-01-11 16:21:03	VPN	61.216.142.39	192.168.188.68	[INIT] Send:[SA][IKE][NONCE][NOTIFY][NOTIFY][VID][VID][VID]

## 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 USG FLEX, go to the **USG FLEX > Configure > Site-to-Site VPN** screen to view and configure a VPN rule. See [Section 9.3.5 on page 278](#) for more information.

Click **USG FLEX > Monitor > VPN Connections** to access this screen.

Figure 120 USG FLEX &gt; Monitor &gt; VPN Connections

USG FLEX > Monitor > VPN Connections

VPN connections

**Connection status**

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

**Site connectivity**

Location	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
<a href="#">Site01_NSG50_Vulliam</a>	192.168.11/24	connected	25.83 KB	874.00 bytes	1768	2021-01-11 16:53:57
<a href="#">Site01_USG_FLEX500</a>	192.168.11/24	connected	81.01 KB	1.09 KB	1626	2021-01-11 16:54:16
<a href="#">Site02_NSG50_Early</a>	192.168.12/24	connected	25.83 KB	874.00 bytes	1738	2021-01-11 16:54:16
<a href="#">Site03_NSG50_Dam</a>	192.168.13/24	disconnected	0 bytes	0 bytes	-	-
<a href="#">Site04_NSG50_Dorman</a>	192.168.14/24	connected	21.90 KB	483.00 bytes	103	2021-01-11 16:54:12
<a href="#">Site05_NSG50_Jess</a>	192.168.15/24	disconnected	0 bytes	0 bytes	-	-
<a href="#">Site06_NSG50_Dani</a>	192.168.16/24	connected	25.83 KB	874.00 bytes	1343	2021-01-11 16:53:57
<a href="#">Site07_NSG50_Shawn</a>	192.168.17/24	connected	25.83 KB	874.00 bytes	1610	2021-01-11 16:54:16
<a href="#">Site08_USG_FLEX500</a>	192.168.11/24	disconnected	0 bytes	0 bytes	-	-
<a href="#">Site09_USG_FLEX200</a>	192.168.16/24	connected	50.88 KB	1.08 KB	1686	2021-01-11 16:54:16

Page 1 of 2 Results per page: 10

**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
B0CF4F-0376F96	disconnected	0 bytes	0 bytes	-	-

**Client to site VPN login account**

User Name	Host Name	Inbound	Outbound	Tunnel Up Time	Assigned IP	Public IP

The following table describes the labels in this screen.

Table 100 USG FLEX &gt; Monitor &gt; VPN Connections

LABEL	DESCRIPTION
	Click this button to reload the data on this page.
<b>Connection Status</b>	
Configuration	This shows the number and address of the local networks behind the Security Gateway, on which the computers are allowed to use the VPN tunnel.
<b>Site Connectivity</b>	
Location	This shows the name of the site to which the Nebula peer gateway is assigned. Click the name to go to the <b>USG FLEX &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 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.
<b>Non-Nebula VPN peers connectivity</b>	
Location	This shows the name of the site to which the Non-Nebula peer gateway is assigned. Click the name to go to the <b>USG FLEX &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.
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 Security Gateway since the VPN tunnel was established.
Outbound	This shows the amount of traffic that has gone through the VPN tunnel from the Security Gateway to the Non-Nebula peer gateway since the VPN tunnel was established.

Table 100 USG FLEX &gt; Monitor &gt; VPN Connections (continued)

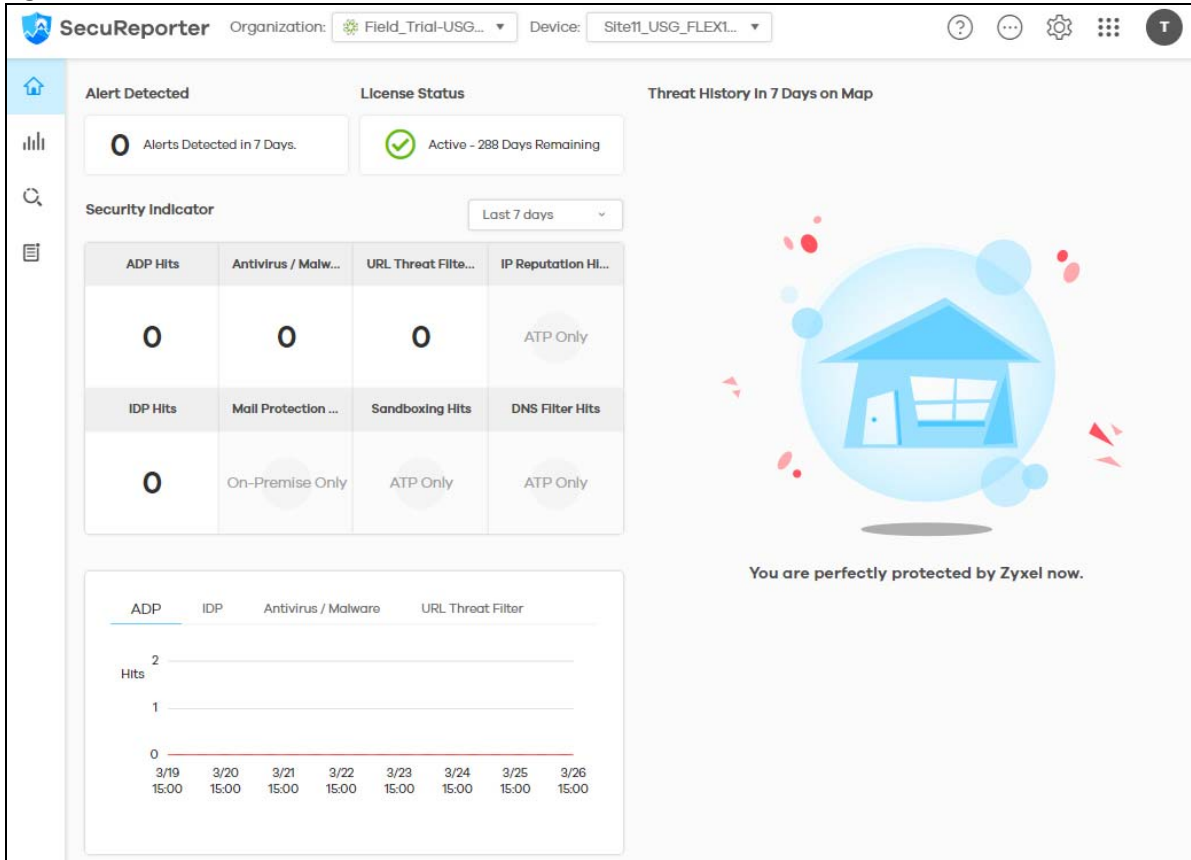
LABEL	DESCRIPTION
Tunnel up time	This shows how many seconds the VPN tunnel has been active.
Last heartbeat	This shows the last date and time a heartbeat packet was sent to determine if the VPN tunnel is up or down.
Remote AP VPN	
Name	This shows the name of the remote access point (AP).
Status	This 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 Security Gateway since the VPN tunnel was established.
Outbound	This shows the amount of traffic that has gone through the VPN tunnel from the Security Gateway 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 Security Gateway.
Inbound	This shows the amount of traffic that has gone through the VPN tunnel from the remote user's computer to the Security Gateway since the VPN tunnel was established.
Outbound	This shows the amount of traffic that has gone through the VPN tunnel from the Security Gateway to the remote user's computer since the VPN tunnel was established.
Tunnel up time	This shows how many seconds the VPN tunnel has been active.
Assigned IP	This shows the IP address that the Security Gateway 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 **USG FLEX > 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 121 USG FLEX > Monitor > SecuReporter

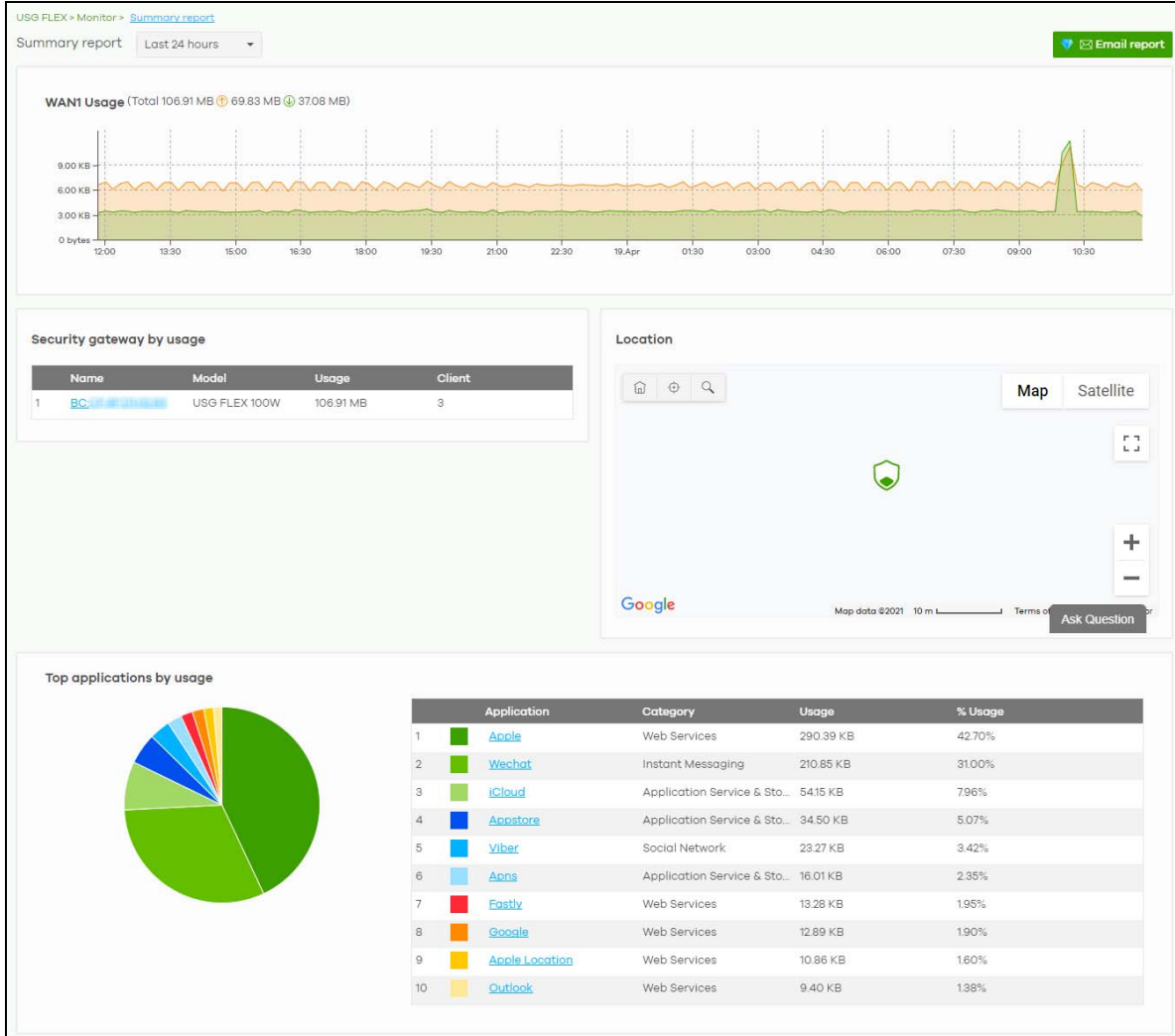


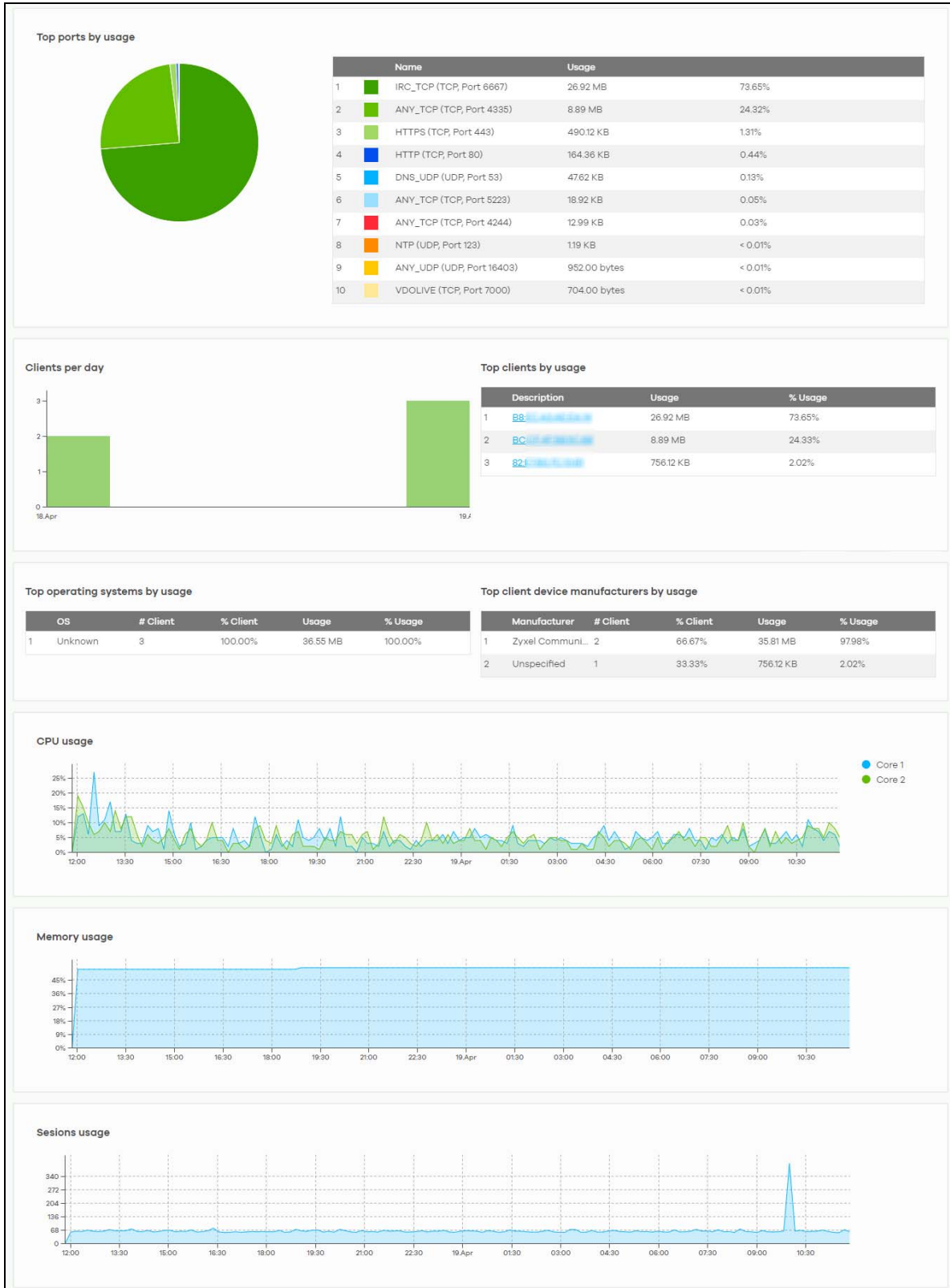
## 9.2.6 Summary Report

This screen displays network statistics for the Security Gateway of the selected site, such as WAN usage, top applications and/or top clients.

Click **USG FLEX > Monitor > Summary Report** to access this screen.

Figure 122 USG FLEX > Monitor > Summary Report







The following table describes the labels in this screen.

Table 101 USG FLEX > Monitor > Summary Report

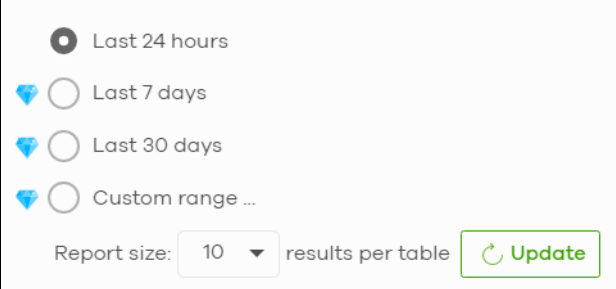
LABEL	DESCRIPTION
Security gateway – Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
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 between the Security Gateway and USG FLEX's, 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 between the Security Gateway and non-USG FLEX's, 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 VPN tunnel between the Security Gateway 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 gateway.
Name	This shows the descriptive name of the Nebula gateway.
Model	This shows the model number of the Nebula gateway.
Usage	This shows the amount of data that has been transmitted through the gateway's WAN port.
Client	This shows the number of clients currently connected to the gateway.
Location	
This shows the location of the Nebula gateways on the map.	
Top applications by usage	
	This shows the index number of the application.

Table 101 USG FLEX &gt; Monitor &gt; Summary Report (continued)

LABEL	DESCRIPTION
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 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 Security Gateway'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 Security Gateway'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 Security Gateway, or passed through the Security Gateway.
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 Security Gateway of the selected site.

### 9.3.1 Port

Use this screen to configure port groups on the Security Gateway. To access this screen, click **USG FLEX > Configure > Port**.


**Figure 123** USG FLEX > Configure > Port

The following table describes the labels in this screen.

**Table 102** USG FLEX > Configure > Port

LABEL	DESCRIPTION
Port Group	Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.  The physical LAN Ethernet ports, for example P1, P2, P3, are shown at the top of the screen. The port groups are shown at the left of the screen. Use the radio buttons to select which ports are in each port group.  For example, to add port P3 to <b>LAN Group 1</b> , select P3's radio button in the LAN Group 1 row.
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	
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.

Table 102 USG FLEX &gt; Configure &gt; Port (continued)

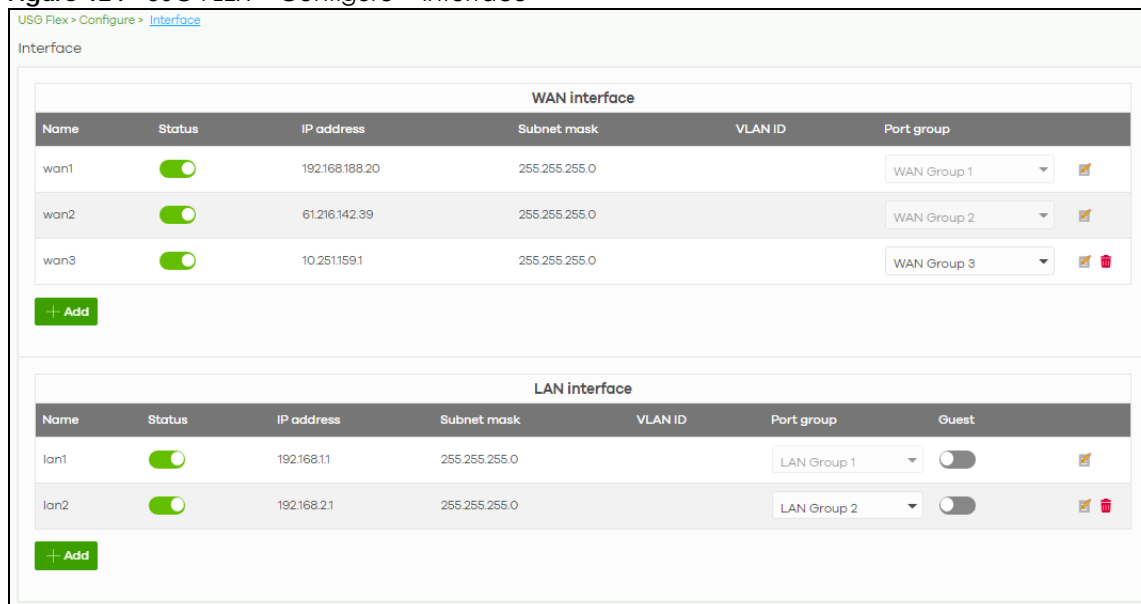
LABEL	DESCRIPTION
	Click this icon to remove a LAN port group.
Add	Click this button to create a new LAN port group.
Close	Click <b>Close</b> to exit this screen without saving.
OK	Click <b>OK</b> to save your changes.

## 9.3.2 Interface

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

To access this screen, click **USG FLEX > Configure > Interface**.

Figure 124 USG FLEX &gt; Configure &gt; Interface



The screenshot shows the 'Interface' configuration page. It is divided into two main sections: 'WAN interface' and 'LAN interface'. Each section contains a table of existing interfaces and an '+ Add' button.

**WAN interface table:**

Name	Status	IP address	Subnet mask	VLAN ID	Port group
wan1	<input checked="" type="checkbox"/>	192.168.188.20	255.255.255.0		WAN Group 1
wan2	<input checked="" type="checkbox"/>	61.216.142.39	255.255.255.0		WAN Group 2
wan3	<input checked="" type="checkbox"/>	10.251.159.1	255.255.255.0		WAN Group 3

**LAN interface table:**





Name	Status	IP address	Subnet mask	VLAN ID	Port group	Guest
lan1	<input checked="" type="checkbox"/>	192.168.1.1	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"/>

The following table describes the labels in this screen.

Table 103 USG FLEX &gt; Configure &gt; Interface

LABEL	DESCRIPTION
WAN Interface	
Name	This field is read-only if you are editing an existing WAN interface.  Specify a name for the interface.  The format of interface names is strict. Each name consists of 2 – 4 letters (interface type), followed by a number (x). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, VLAN interfaces are vlan0, vlan1, vlan2, and so on.
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.

Table 103 USG FLEX &gt; Configure &gt; Interface (continued)

LABEL	DESCRIPTION
VLAN ID	This shows the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.)  Note: NCC will show an error message when the VLAN ID in the interface is configured to be the same as the WAN port's VLAN ID.
Port group	Select the name of the port group to which you want the interface to (network) belong.
	Click the edit icon to modify the interface.
	Click the remove icon to delete the interface.
Add	Click this button to create a virtual WAN interface, which associates a VLAN with a WAN port group.
LAN Interface	
Name	This field is read-only if you are editing an existing LAN interface.  Specify a name for the interface.  The format of interface names is strict. Each name consists of 2 – 4 letters (interface type), followed by a number (x). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, VLAN interfaces are vlan0, vlan1, vlan2, and so on.
Status	Select this to activate the LAN interface.
IP address	This is the IP address for this interface.
Subnet mask	This is the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	This is the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 – 4094. (0 and 4095 are reserved.)  Note: NCC will show an error message when the VLAN ID in the 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.
Guest	Select On to configure the interface as a Guest interface. Devices connected to a Guest interface have Internet access but cannot communicate with each other directly or access networks behind the gateway.
	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 **USG FLEX > Configure > Interface > WAN interface configuration** screen.

Figure 125 USG FLEX &gt; Configure &gt; Interface &gt; WAN interface configuration

The following table describes the labels in this screen.

Table 104 USG FLEX &gt; Configure &gt; Interface &gt; 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.)
Type	Select the type of interface to create.  <b>DHCP:</b> The interface will be automatically get an IP address and other network settings from a DHCP server.  <b>Static:</b> You must manually configure an IP address and other network settings for the interface.  <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.

Table 104 USG FLEX &gt; Configure &gt; Interface &gt; WAN interface configuration (continued)


LABEL	DESCRIPTION
IP address assignment	These fields are displayed if you selected <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 gateway through which this interface sends traffic.
First DNS server	Enter a DNS server's IP address.  The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Nebula Device uses the first and second DNS servers, in that order to resolve domain names for VPN, DDNS and the time server. Leave the field blank if you do not want to configure DNS servers.
Second DNS server	Enter the IP address of another DNS server. This field is optional.
These fields are displayed if you selected <b>PPPoE</b> .	
Username	Type the user name provided by your ISP. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed.
Password	Type the password provided by your ISP. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
Retype password	Type 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. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Nebula Device divides it into smaller fragments. Allowed values are 576 – 1500.
ADVANCED OPTIONS	
Connectivity check	The interface can periodically check whether it can connect to its default gateway ( <b>Default gateway</b> ), or to 2 user-specified servers ( <b>Check the two addresses below</b> ). If the check fails, the interface's status changes to <b>Down</b> .  You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Nebula Device stops routing to the gateway.
Probe Succeeds When	This field applies when you select <b>Check the two addresses</b> and specify 2 domain names or IP addresses for the connectivity check.  Select <b>any one</b> if you want the check to pass if at least one of the domain names or IP addresses responds.  Select <b>all</b> if you want the check to pass only if both domain names or IP addresses respond.
Proxy ARP	Proxy ARP (RFC 1027) allows the Security Gateway to answer external interface ARP requests on behalf of a device on its internal interface.  Click <b>Add new</b> to add the IP address or IP range of devices that the interface will answer proxy ARP requests for.
IP Address	Enter a single IPv4 address, an IPv4 CIDR (for example, 192.168.1.1/24) or an IPv4 Range (for example, 192.168.1.2-192.168.1.100).  The Nebula Device answers external ARP requests if they match one of these target IP addresses. For example, if the IPv4 Address is 192.168.1.5, then the Nebula Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address.
	Click the remove icon to delete the proxy ARP IP address.

Table 104 USG FLEX &gt; Configure &gt; Interface &gt; WAN interface configuration (continued)

LABEL	DESCRIPTION
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 Gateway 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 **USG FLEX > Configure > Interface > LAN interface configuration** screen.



**Figure 126** USG FLEX > Configure > Interface > LAN interface configuration

The following table describes the labels in this screen.

**Table 105** USG FLEX > 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 105 USG FLEX &gt; Configure &gt; Interface &gt; LAN interface configuration (continued)


LABEL	DESCRIPTION
DHCP setting	<p>Select what type of DHCP service the Security Gateway provides to the network. Choices are:</p> <p><b>None</b> – the Security Gateway does not provide any DHCP services. There is already a DHCP server on the network.</p> <p><b>DHCP Relay</b> – the Security Gateway 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 Security Gateway assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Security Gateway is the DHCP server for the network.</p>
These fields appear if the Security Gateway 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 Security Gateway is a DHCP Server.	
IP pool start address	<p>Enter the IP address from which the Security Gateway 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 Security Gateway 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 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 Security Gateway 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 Security Gateway assigns to computers connected to the interface. Otherwise, the Security Gateway 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. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG FLEX divides it into smaller fragments. Allowed values are 576 – 1500. Usually, this value is 1500.
ADVANCED OPTIONS	

Table 105 USG FLEX &gt; Configure &gt; Interface &gt; LAN interface configuration (continued)

LABEL	DESCRIPTION
DHCP extended options	This table is available if you select <b>ADVANCED OPTIONS</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 7.3.2.3 on page 189</a> for detailed information
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.
PXE server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system through a PXE-capable Network Interface Card (NIC).  PXE is available for computers on internal interfaces to allow them to boot up using boot software on a PXE server. The USG FLEX acts as an intermediary between the PXE server and the computers that need boot software.  The PXE server must have a public IPv4 address. You must enable DHCP Server on the USG FLEX so that it can receive information from the PXE server.
PXE Boot loader file	A boot loader is a computer program that loads the operating system for the computer. Type the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is typed, then the client computers cannot boot.
Default gateway	If you set this interface to DHCP Server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway.
IGMP proxy	Select this to allow the USG FLEX 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.

### 9.3.2.3 DHCP Option

Click the **Add new** button in the **DHCP extended options** section to open the **USG FLEX > Configure > Interface > LAN interface configuration: DHCP option** screen.

**Figure 127** USG FLEX > Configure > Interface: LAN interface configuration: DHCP option

The following table describes the labels in this screen.

Table 106 USG FLEX &gt; Configure &gt; Interface: LAN interface configuration: DHCP option

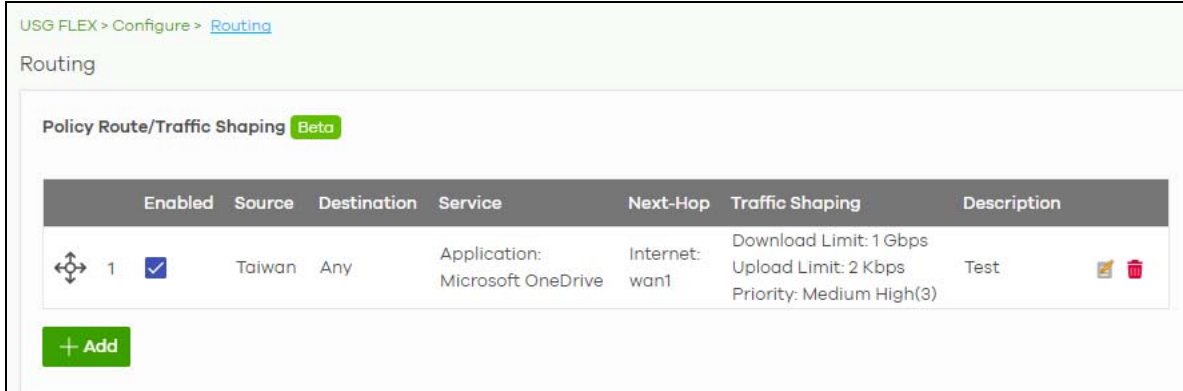
LABEL	DESCRIPTION
Option	Select which DHCP option that you want to add in the DHCP packets sent through the interface.
Name	This field displays the name of the selected DHCP option. If you selected <b>User_Defined</b> in the <b>Option</b> field, enter a descriptive name to identify the DHCP option.
Code	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.
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 Security Gateway'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 **USG FLEX > Configure > Routing: Policy Routes/Traffic Shaping** to access this screen.

**Figure 128** USG FLEX > Configure > Routing: Policy Routes/Traffic Shaping

The following table describes the labels in this screen.

Table 107 USG FLEX &gt; Configure &gt; Routing: Policy Routes/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 290</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 **USG FLEX > Configure > Routing: Policy Routes/Traffic Shaping: Add/Edit** screen to access this screen.

**Figure 129** USG FLEX > Configure > Routing: Policy Routes/Traffic Shaping: Add/Edit

The following table describes the labels in this screen.

Table 108 USG FLEX &gt; Configure &gt; Routing: Policy Routes/Traffic Shaping: Add/Edit

LABEL	DESCRIPTION
Matching Criteria	
Description	Enter a descriptive name for the rule.
Source	Specify the source IP addresses to which this rule applies. You can add multiple IP, CIDR, FQDN, or GEO IP (country) objects 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.  Note: IP/CIDR, FQND, and GEO IP objects cannot be use at the same time.
Destination	Specify the destination IP addresses or subnet to which this rule applies. You can add multiple IP, CIDR, FQDN, or GEO IP (country) objects 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.  Note: IP/CIDR, FQND, and GEO IP objects cannot be use at the same time.

Table 108 USG FLEX &gt; Configure &gt; Routing: Policy Routes/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.  <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.
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 **USG FLEX > Configure > Routing: Static Route** screen to open the following screen.

Figure 130 USG FLEX &gt; Configure &gt; Routing: Static Route

The screenshot shows the 'Static Route' configuration interface. At the top, there's a title 'Static Route'. Below it is a table with the following columns: 'Subnet', 'Next Hop Type', 'Next Hop', 'Metric(0-127)', and 'Description'. The 'Subnet' field is empty with a close button (x) and a plus sign (+). The 'Next Hop Type' is a dropdown menu currently showing 'IP Address'. The 'Next Hop' field is empty with a close button (x) and a plus sign (+). The 'Metric(0-127)' field contains the value '1' with a close button (x) and a plus sign (+). The 'Description' field is empty with a close button (x) and a plus sign (+). At the bottom left, there is a green '+ Add' button.

The following table describes the labels in this screen.

Table 109 USG FLEX > 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.

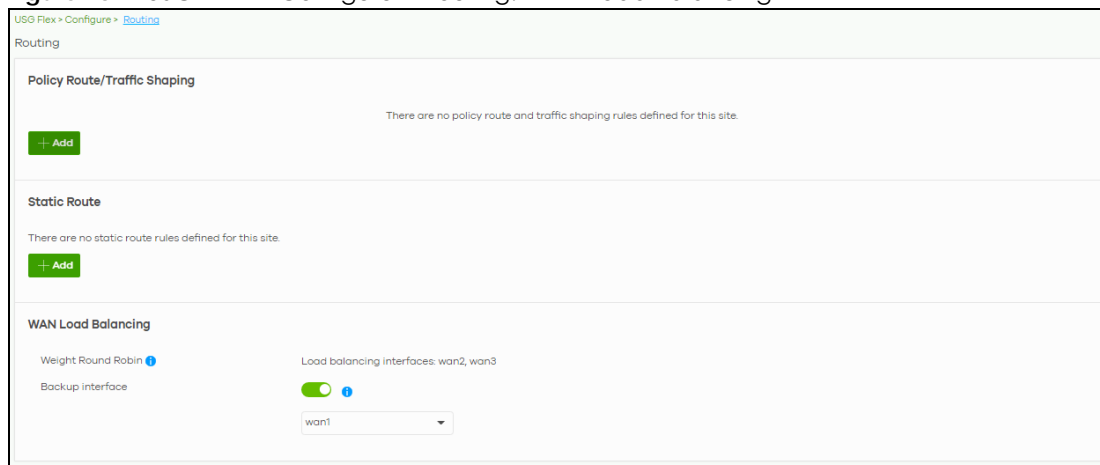
### 9.3.3.3 WAN Load Balancing

Go to **USG FLEX > Configure > Routing: WAN Load Balancing** to configure WAN load balancing.

By default, the Security Gateway 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 security gateway chooses WAN 1 for two sessions' traffic and WAN 2 for one session's traffic in each round of three new sessions.

Figure 131 USG FLEX > Configure > Routing: WAN Load Balancing



The following table describes the labels in this section.

Table 110 USG FLEX > 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. To access this screen, click **USG FLEX > Configure > NAT**. The following screen appears, providing a summary of the existing NAT rules.

**Figure 132** USG FLEX > Configure > NAT



The screenshot shows the NAT configuration interface. At the top, there's a breadcrumb 'USG Flex > Configure > NAT'. Below that, the 'Virtual Server' section contains a table with columns: Public IP, Public Port, LAN IP, Local Port, Allow Remote IPs, and Description. There are input fields for each column and an '+ Add' button. Below this is the '1:1 NAT' section. It has a toggle for 'Enable' (currently on), a 'Name' field (containing 'SN\_'), 'Public IP' and 'LAN IP' fields, and an 'Uplink' dropdown (set to 'wan1'). Underneath is the 'Allowed inbound connections' table with columns: Enable, Protocol, Local Port, and Remote IPs. There is one row with '1' in the 'Enable' column, 'Any' in 'Protocol', and 'any' in 'Remote IPs'. There are '+ Add' buttons at the bottom of both sections.

The following table describes the labels in this screen.

**Table 111** USG FLEX > 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 Security Gateway on which packets for the NAT rule must be received.
Protocol	Select the IP protocol to which this rule applies. Choices are: TCP, UDP, and Any.
Public Port	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.
Local Port	Enter the original destination port or range of destination ports this NAT rule supports.
Allowed Remote IPs	Specify the remote IP addresses that are allowed to access the public IP address. You can specify a range of IP addresses. <b>Any</b> allows all IP addresses.
Description	This is the descriptive name of the policy.
	Click the remove icon to delete it.

Table 111 USG FLEX &gt; Configure &gt; NAT (continued)

LABEL	DESCRIPTION
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	Type in 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 Gateway 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 specify a range of IP addresses. <b>Any</b> allows all IP addresses.
	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.

Click **USG FLEX > Configure > Site-to-Site VPN** to access this screen.

**Figure 133** USG FLEX > Configure > Site-to-Site VPN

USG Flex > Configure > Site-to-Site VPN

Site-to-Site VPN

Outgoing interface: AUTO

Preferred uplink: wan1

Local networks:

Name	Subnet	Use VPN
Ian1	192.168.1.0/24	<input checked="" type="checkbox"/>
Ian2	192.168.2.0/24	<input checked="" type="checkbox"/>

VPN Area: Field\_Trial\_VPN

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):

SiteName
1 Site00_USG_FLEX700

Area communication:

NAT traversal:  Auto  Custom NAT traversal IP

---

Remote VPN participants:

Network	Subnet
Site01_NSG50_Yullian	192.168.51.0/24
Site02_NSG50_Eddy	192.168.52.0/24
Site03_NSG50_Dan	192.168.53.0/24
Site04_NSG50_Darren	192.168.54.0/24
Site05_NSG50_Jess	192.168.55.0/24
Site06_NSG50_Demi	192.168.56.0/24
Site07_NSG50_Shawn	192.168.57.0/24
Site08_USG_FLEX500	192.168.8.0/24 192.168.9.0/24
Site09_USG_FLEX200	192.168.16.0/24 192.168.17.0/24
Site10_USG_FLEX200	192.168.24.0/24 192.168.25.0/24

Site-wide settings

Options in this section apply to this Nebula gateway only.

Non-Nebula VPN peers

Enabled	Name	Public IP	Private subnet	IPsec policy	Preshared secret	Availability	Address
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Default	<input type="text"/>	This site	<input type="text"/>

The following table describes the labels in this screen.

Table 112 USG FLEX &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.
Prefer uplink	Specify the preferred uplink to which non-Nebula VPN peers should connect to the Security Gateway.
Local networks	This shows the local networks behind the Security Gateway. Note: Non-Nebula VPN peers use the first interface with a local policy.
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 143</a> .
Nebula 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.
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 143</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 Security Gateway 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 security gateway 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, such as a ZyWALL ATP device, 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.
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 300</a> for detailed information.
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.

Table 112 USG FLEX &gt; Configure &gt; Site-to-Site VPN (continued)

LABEL	DESCRIPTION
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 security gateway 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 **USG FLEX > Configure > Site-to-Site VPN** screen to access this screen.

Figure 134 USG FLEX &gt; Configure &gt; Site-to-Site VPN: IPsec Policy

The screenshot shows the 'Custom' IPsec Policy configuration window. It is divided into 'Phase 1' and 'Phase 2' sections. Phase 1 settings are: Preset (Default), IKE version (IKEv1), Encryption (AES128), Authentication (SHA128), Diffie-Hellman group (DH2), and Lifetime (seconds) (86400). Phase 2 settings include a table for three sets of Encryption and Authentication, PFS group (DH2), Lifetime (seconds) (28800), and Connectivity check. The 'OK' button is highlighted in green.

Set	Encryption	Authentication
Set 1	AES128	SHA128
Set 2	None	None
Set 3	None	None

The following table describes the labels in this screen.

Table 113 USG FLEX &gt; Configure &gt; 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 2 phases: Phase 1 (Authentication) and Phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

Table 113 USG FLEX &gt; Configure &gt; Site-to-Site VPN: 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 IPv4 traffic only. 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 security gateway 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 security gateway 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>Set the negotiation mode.</p> <p><b>Main</b> encrypts the USG FLEX's and remote IPSec router's identities but takes more time to establish the IKE SA.</p> <p><b>Aggressive</b> is faster but does not encrypt the identities.</p>
Local ID	<p>Enter an identifier used to identify the Security Gateway during authentication.</p> <p>This can be an IP address or hostname.</p>
Peer ID	<p>Enter an identifier used to identify the remote IPSec router during authentication.</p> <p>This can be an IP address or hostname.</p>
Phase2	<p>Phase 2 uses the SA that was established in phase 1 to negotiate SAs for IPSec.</p>

Table 113 USG FLEX &gt; Configure &gt; Site-to-Site VPN: 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 security gateway 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>
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>Type the maximum number of seconds the IPsec SA can last. Shorter life times provide better security. The security gateway automatically negotiates a new IPsec SA before the current one expires, if there are users who are accessing remote resources.</p>
Connectivity check	<p>Enter an IP address that the Security Gateway can ping, to check whether the non-Nebula VPN peer gateway is available.</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>

### 9.3.6 Remote Access VPN

Use this screen to configure the VPN client settings on the Security Gateway. This allows incoming VPN clients to connect to the Security Gateway 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 **USG FLEX > Configure > Remote access VPN** to access this screen.

Figure 135 USG FLEX &gt; Configure &gt; Remote access VPN

USG FLEX > Configure > [Remote access VPN](#)

Remote access VPN

WAN interface: Auto

Domain name: alpha-5fb36a3d.d2ns-nbl.com

---

IPSec VPN server:

Client VPN subnet: 192.168.177.0/24

DNS name servers: Specify nameserver ...

Custom nameservers: 8.8.8.8, 8.8.4.4

One IP address in one line to specify your nameserver. Maximum number of nameservers is two.  
Example:  
192.168.11  
192.168.3710

Secret: \*\*\*\*\*

Policy: Default

Authentication: Nebula Cloud Authentication

Two-factor authentication with Captive Portal

---

L2TP over IPSec VPN server:

Client VPN subnet: 192.168.166.0/24

DNS name servers: Specify nameserver ...

Custom nameservers: 8.8.8.8, 8.8.4.4

One IP address in one line to specify your nameserver. Maximum number of nameservers is two.  
Example:  
192.168.11  
192.168.3710

Secret: \*\*\*\*\*

Authentication: Nebula Cloud Authentication

Policy: Default

VPN provision script: E.g. nebula@zyxel.com [Send Email](#)



The following table describes the labels in this screen.

Table 114 USG FLEX &gt; Configure &gt; Remote access VPN

LABEL	DESCRIPTION
WAN interface	Select the WAN interface which VPN users connect to.
Domain name	This displays the domain name of the NAT router if the VPN tunnel must pass through NAT (there is a NAT router between the IPsec devices).  This field is available only when you select <b>AUTO</b> in the <b>WAN interface</b> field.  Note: To allow an IPsec connection, the NAT router must have the following ports open: UDP 500, 4500.
IPsec VPN server	Select this to enable the IPsec VPN server.
Client VPN subnet	Specify the IP addresses that the Security Gateway 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	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="#">Appendix on page 286</a> .
Authentication	Select how the Security Gateway 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 Security Gateway through VPN.  Note: Two-factor authentication is only supported with Zyxel SecuExtender IPsec client.
L2TP over IPsec VPN server	Select this to enable the L2TP over IPsec VPN server.
Client VPN subnet	Specify the IP addresses that the Security Gateway 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.
Secret	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 Security Gateway authenticates a remote user before allowing access to the VPN tunnel.
Policy	Configure custom VPN tunnel settings.  For details, see <a href="#">Appendix on page 286</a> .
VPN provision script	Send an email to help automatically configure VPN settings on client devices so that the devices can remotely access this gateway. The email contains 2 scripts; one for macOS 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> <p>This field is available only when you select <b>L2TP over IPsec client</b> in the <b>Client VPN server</b> field.</p>

### 9.3.6.1 Remote Access VPN > Custom VPN Policy

Click **Default** in **USG FLEX > Configure > Remote access VPN > Policy** to open the following screen.

**Figure 136** USG FLEX > Configure > Remote access VPN: Default

The screenshot shows the 'Custom' configuration window for a VPN policy. It features a 'Preset' dropdown set to 'Custom'. Under 'Phase 1', there are dropdown menus for 'IKE version', 'Encryption' (3DES), 'Authentication' (SHA128), and 'Diffie-Hellman group' (DH2), along with a text input for 'Lifetime (seconds)' (86400). An 'Advanced' link is visible. The 'Phase 2' section contains a table with three rows: 'Set 1' (3DES, SHA128), 'Set 2' (None, None), and 'Set 3' (None, None). 'Close' and 'OK' buttons are at the bottom right.

The following table describes the labels in this screen.

Table 115 USG FLEX > 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	
IKE version	Select <b>IKEv1</b> or <b>IKEv2</b> .  <b>IKEv1</b> applies to IPv4 traffic only. <b>IKEv2</b> applies to IPv4 traffic only. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows 2 parties to send data securely

Table 115 USG FLEX &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>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 security gateway 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 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 IPSec SA can last. Shorter life times provide better security. The security gateway automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.</p>
Advanced	
Mode	<p>Set the negotiation mode.</p> <p><b>Main</b> encrypts the USG FLEX's and remote IPSec router's identities but takes more time to establish the IKE SA.</p> <p><b>Aggressive</b> is faster but does not encrypt the identities.</p>
Local ID	<p>Enter an identifier used to identify the Security Gateway during authentication.</p> <p>This can be an IP address or hostname.</p>
Peer ID	<p>Enter an identifier used to identify the remote IPSec router during authentication.</p> <p>This can be an IP address or hostname.</p>
Phase2	
Set	<p>This shows the index number of the IPSec policy.</p>

Table 115 USG FLEX &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 security gateway 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 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>Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The security gateway 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>

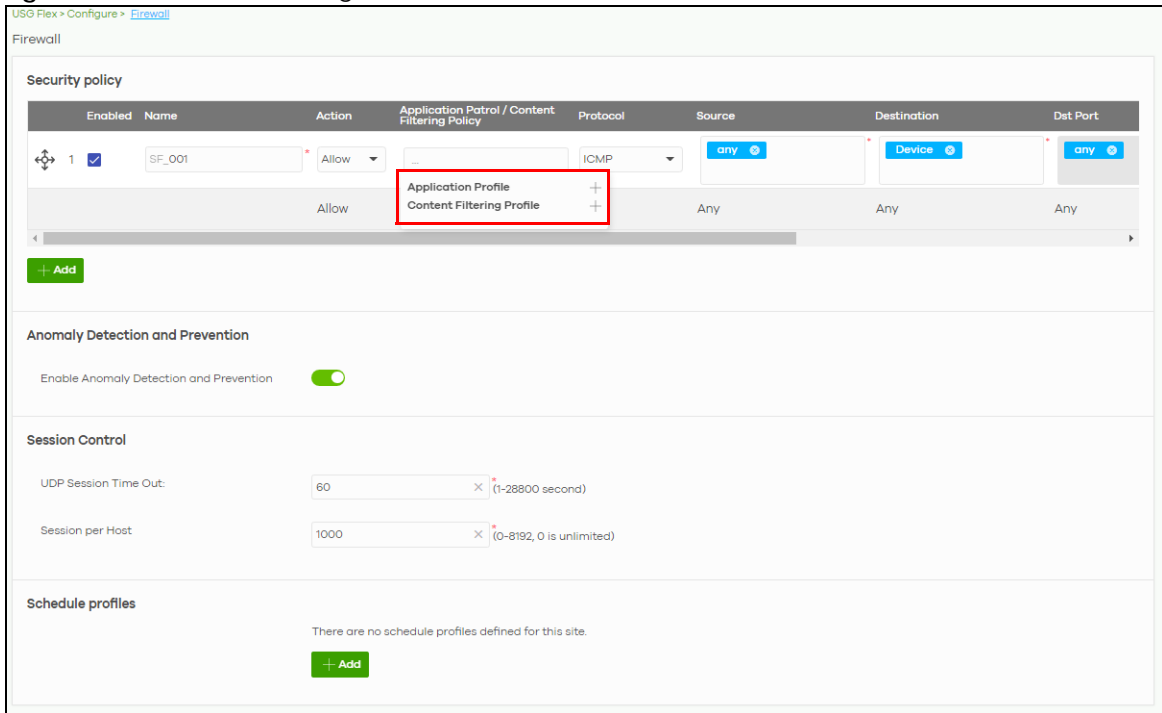
### 9.3.7 Firewall

By default, a LAN user can initiate a session from within the LAN and the Security Gateway allows the response. However, the Security Gateway 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 **USG FLEX > Configure > Firewall** to access this screen.

Note: The security gateway has the following hidden default firewall rules: LAN to WAN is allowed, WAN to LAN is blocked.

Figure 137 USG FLEX > Configure > Firewall






The following table describes the labels in this screen.

Table 116 USG FLEX > Configure > Firewall

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	Type in the name of the security policy.
Action	Select what the firewall 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.
Application Patrol/Content Filtering Policy	Click the "+" to add an Application Patrol or Content Filtering profile. The firewall takes the action set in the profile when traffic matches the profile's policy.  See <a href="#">Section 9.3.7.1 on page 290</a> for how to create an application patrol profile.
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	Specify the source IP addresses to which this rule applies. You can add multiple IP, CIDR, FQDN, or GEO IP (country) objects 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.  Note: IP/CIDR, FQND, and GEO IP objects cannot be use at the same time.

Table 116 USG FLEX &gt; Configure &gt; Firewall (continued)

LABEL	DESCRIPTION
Destination	Specify the destination IP addresses or subnet to which this rule applies. You can add multiple IP, CIDR, FQDN, or GEO IP (country) objects 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.  Note: IP/CIDR, FQND, and GEO IP objects cannot be use at the same time.
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.
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.
Anomaly Detection and Prevention	
Enable Anomaly Detection and Prevention	Select this to enable traffic anomaly and protocol anomaly detection and prevention.
Session Control	
UDP Session Time out	Set how many seconds the Security Gateway 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 294</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 Security Gateway 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 **USG FLEX > 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 138** USG FLEX > Configure > Firewall: Add an Application Profile

The following table describes the labels in this screen.

**Table 117** USG FLEX > 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 Security Gateway 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 Security Gateway 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 **USG FLEX > Configure > Firewall** screen to access this screen.

Figure 139 USG FLEX &gt; Configure &gt; Firewall: Add a Content Filtering Profile

The screenshot shows a configuration window titled "Create content filtering profile". It contains the following sections and controls:

- Add profile:**
  - Name: Text input field with a clear button (x) and a red asterisk (\*).
  - Description (Optional): Text input field with a clear button (x).
- Log:** Toggle switch, currently turned ON.
- DNS content filtering:**
  - Enabled: Toggle switch, currently turned ON.
- Block Web Pages:**
  - Action for Unrated Web Pages: Dropdown menu set to "Warn".
  - Action When Service is Unavailable: Dropdown menu set to "Warn".
- Block Category:**
  - Templates: Dropdown menu set to "Parental control".
  - Test URL: Text input field with a clear button (x) and a "Test" button. Below the field is the text "Enter a url to know website category".
  - Search category: Text input field with a clear button (x) and a "Category list" dropdown arrow.
- Block web site:** Text "There are no block web site rules defined for this site." with a "+ Add" button.
- Allow web site:** Text "There are no allow web site rules defined for this site." with a "+ Add" button.

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

The following table describes the labels in this screen.

Table 118 USG FLEX &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 Security Gateway 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 USG FLEX 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 118 USG FLEX &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 USG FLEX 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 do 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

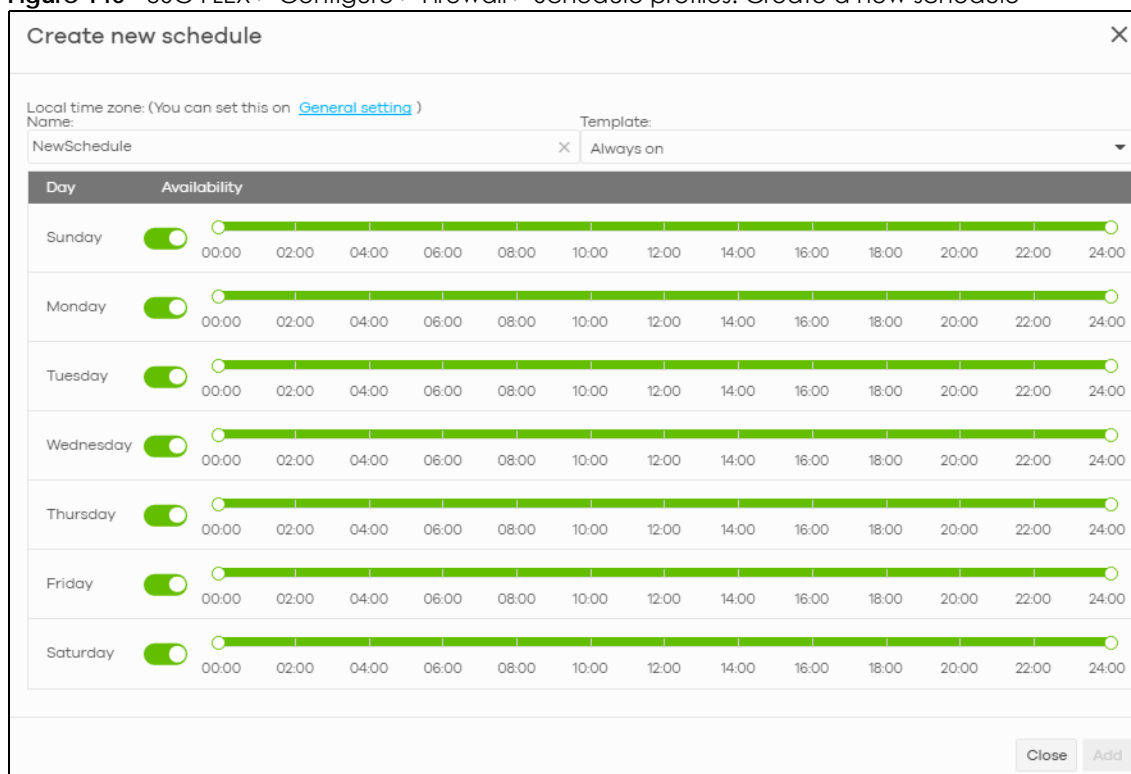
Table 118 USG FLEX &gt; Configure &gt; Firewall: Add a Content Filtering Profile (continued)

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 **USG FLEX > Configure > Firewall > Schedule profiles** screen to access this screen.

Figure 140 USG FLEX &gt; Configure &gt; Firewall &gt; Schedule profiles: Create a new schedule



The following table describes the labels in this screen.

Table 119 USG FLEX &gt; Configure &gt; 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.

## 9.3.8 Security Service

Use this screen to enable or disable the features available in the security pack for your Security Gateway, 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 **USG FLEX > Configure > Security Service** to access this screen.

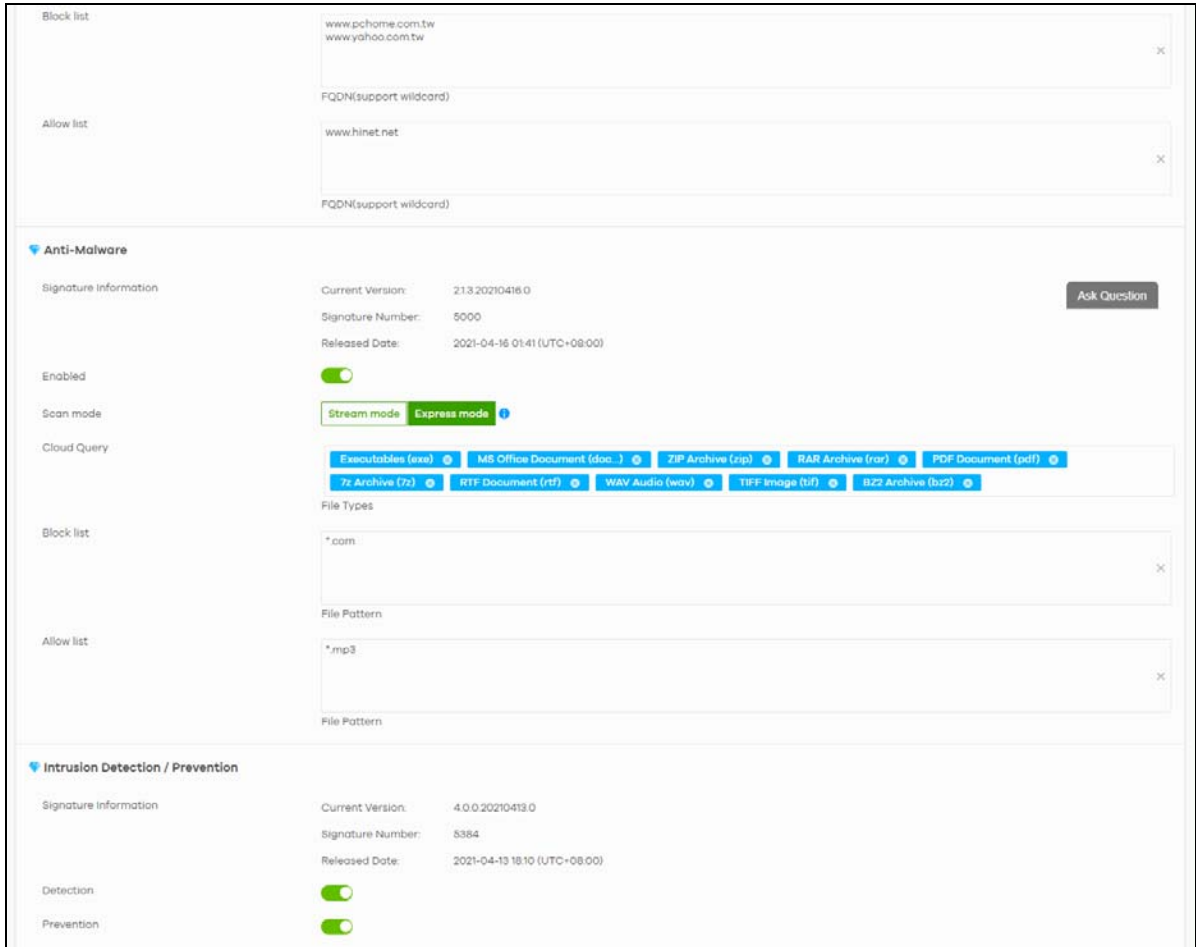
Note: Packet inspection signatures examine packet content for malicious data. Packet inspection applies to OSI (Open System Interconnection) layer-4 to layer-7 contents. You need to subscribe for IDP service in order to be able to download new signatures.

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 137](#).

**Figure 141** USG FLEX > Configure > Security Service

The screenshot shows the 'Security service' configuration page in USG FLEX. The page is divided into four main sections:

- IP Exception:** A table with columns 'Enabled', 'Source IP', 'Destination IP', and 'Description'. One entry is visible with 'Enabled' checked. A '+ Add' button is below the table.
- Content filtering:** A toggle switch for 'Drop connection when there is an HTTPS connection with SSL v3(or previous version)' is turned on. Below are input fields for 'Denied Access Message' (containing 'Web access is restricted. Please contact the administrator(SPS\_CF)') and 'Redirect URL' (containing 'https://192.168.188.40'). A table below lists one profile: 'SPS\_CF test' with description 'SPS\_CF test'. A '+ Add' button is below the table.
- Application Patrol:** A section for 'Application profiles' with a table listing one profile: 'SPS\_YT\_netflix\_FB'. A '+ Add' button and an 'Ask Question' button are also present.
- URL Threat Filter:** A section with several options: 'Enabled' (toggle on), 'Log' (toggle on), 'Policy' (dropdown set to 'Block'), 'Denied Access Message' (input field with 'Web access is restricted. Please contact the administrator(sps\_URL)'), and 'Redirect URL' (input field). At the bottom, there is a 'Category list' with checkboxes for: Anonymizers, Phishing, Browser Exploits, Spam URLs, Malicious Downloads, Spyware/Adware/Keyloggers, and Malicious Sites. All these checkboxes are checked.



The following table describes the labels in this screen.

Table 120 USG FLEX > Configure > Security Service


LABEL	DESCRIPTION
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.
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.
Content Filtering	
Drop connection when 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.

Table 120 USG FLEX &gt; Configure &gt; Security Service (continued)





LABEL	DESCRIPTION
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 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.</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 (0–9 a–z A–Z;/?:@&amp;=+\$\._!~*()%,"). For example, http://192.168.1.17/blocked access.</p>
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 291</a> for more information.
Application Patrol	
Application profiles	
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 application patrol profile. See <a href="#">Section 9.3.8.2 on page 302</a> for more information.
URL Threat Filter	
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 Security Gateway generate a log when the policy is matched to the criteria listed above.
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>
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 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.</p>

Table 120 USG FLEX &gt; Configure &gt; Security Service (continued)

LABEL	DESCRIPTION
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>
Category List	<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 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 do 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>
Anti-Malware	
Enabled	<p>Select <b>On</b> to turn on the rule. Otherwise, select <b>Off</b> to turn off the rule.</p>
Scan Mode	
Express Mode	<p>In this mode you can define which types of files are scanned using the File Type For Scan fields. The USG FLEX then scans files by sending each file's hash value to a cloud database using cloud query. This is the fastest scan mode.</p>
Stream Mode	<p>In this mode the USG FLEX scans all files for viruses using its anti-malware signatures to detect known virus patterns. This is the deepest scan mode.</p>
File decompression (ZIP and RAR)	<p>Select this check box to have the USG FLEX scan a compressed file (the file does not need to have a "zip" or "rar" file extension). The USG FLEX first decompresses the file and then scans the contents for malware.</p> <p>Note: The USG FLEX decompresses a compressed file once. The USG FLEX 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 USG FLEX deletes compressed files that use password encryption.</p> <p>Select this check box to have the USG FLEX delete any compressed files that it cannot decompress. The USG FLEX cannot decompress password protected files or a file within another compressed file. There are also limits to the number of compressed files that the USG FLEX can concurrently decompress.</p> <p>Note: The USG FLEX's firmware package cannot go through the USG FLEX with this check box enabled. The USG FLEX 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 OK to upload a firmware package to the USG FLEX with the check box selected.</p>
Cloud Query	<p>Select the Cloud Query supported file types for the Security Gateway to scan for viruses.</p>

Table 120 USG FLEX &gt; Configure &gt; Security Service (continued)

LABEL	DESCRIPTION
Block list	<p>This field displays the file or encryption pattern of the entry. Enter a MD5 hash or file pattern that would cause the USG FLEX 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 USG FLEX 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 USG FLEX checks up to the first 80 characters of a file name.</li> </ul>
Allow list	<p>When you select this check box, the USG FLEX deletes compressed files that use password encryption.</p> <p>Select this check box to have the USG FLEX delete any compressed files that it cannot decompress. The USG FLEX cannot decompress password protected files or a file within another compressed file. There are also limits to the number of compressed files that the USG FLEX can concurrently decompress.</p> <p>Note: The USG FLEX's firmware package cannot go through the USG FLEX with this check box enabled. The USG FLEX 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's OK to upload a firmware package to the USG FLEX with the check box. This field displays the file or encryption pattern of the entry.</p> <p>Enter the file or encryption pattern for this entry. Enter a MD5 hash or file pattern to identify the names of files that the USG FLEX 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 USG FLEX 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 USG FLEX checks up to the first 80 characters of a file name.</li> </ul>
Intrusion Detection/Prevention	

Table 120 USG FLEX > Configure > Security Service (continued)

LABEL	DESCRIPTION
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 **USG FLEX > Configure > Security service** screen to access this screen.

Figure 142 USG FLEX > Configure > Security Service > Content Filtering: Add/Edit

The following table describes the labels in this screen.

Table 121 USG FLEX > 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 Security Gateway generate a log when the policy is matched to the criteria listed above.
Block Web Pages	



Table 121 USG FLEX &gt; Configure &gt; Security Service &gt; Content Filtering: Add/Edit (continued)

LABEL	DESCRIPTION
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 USG FLEX 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>
<p><b>Block Category</b></p> <p>The security gateway 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>
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	<p>Specify your desired filter criteria to filter the list of categories.</p>
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>

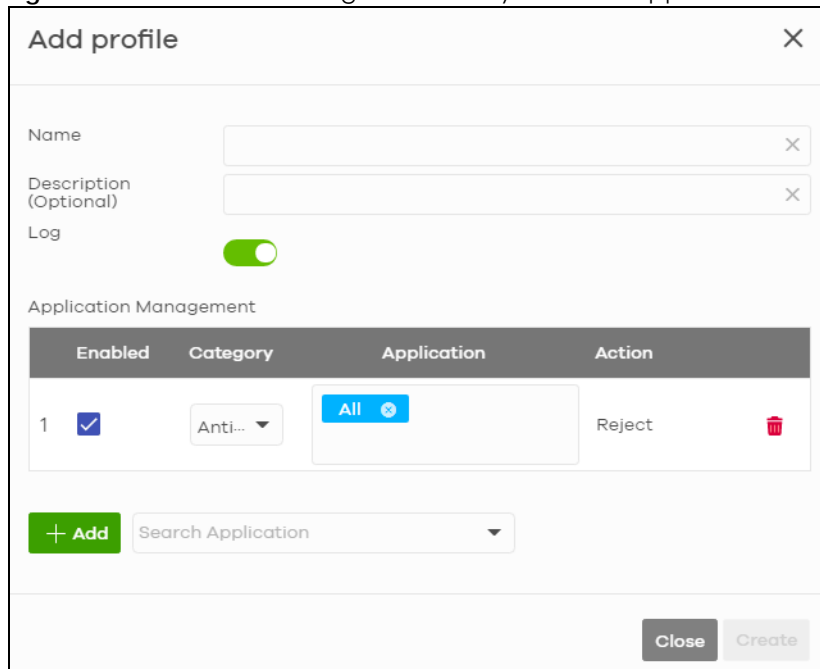
Table 121 USG FLEX &gt; Configure &gt; Security Service &gt; Content Filtering: Add/Edit (continued)

LABEL	DESCRIPTION
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 do 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.
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 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 **USG FLEX > Configure > Security service** screen to access this screen.

Figure 143 USG FLEX &gt; Configure &gt; Security Service &gt; 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 122 USG FLEX > Configure > Security Service > Application Patrol: Add/Edit

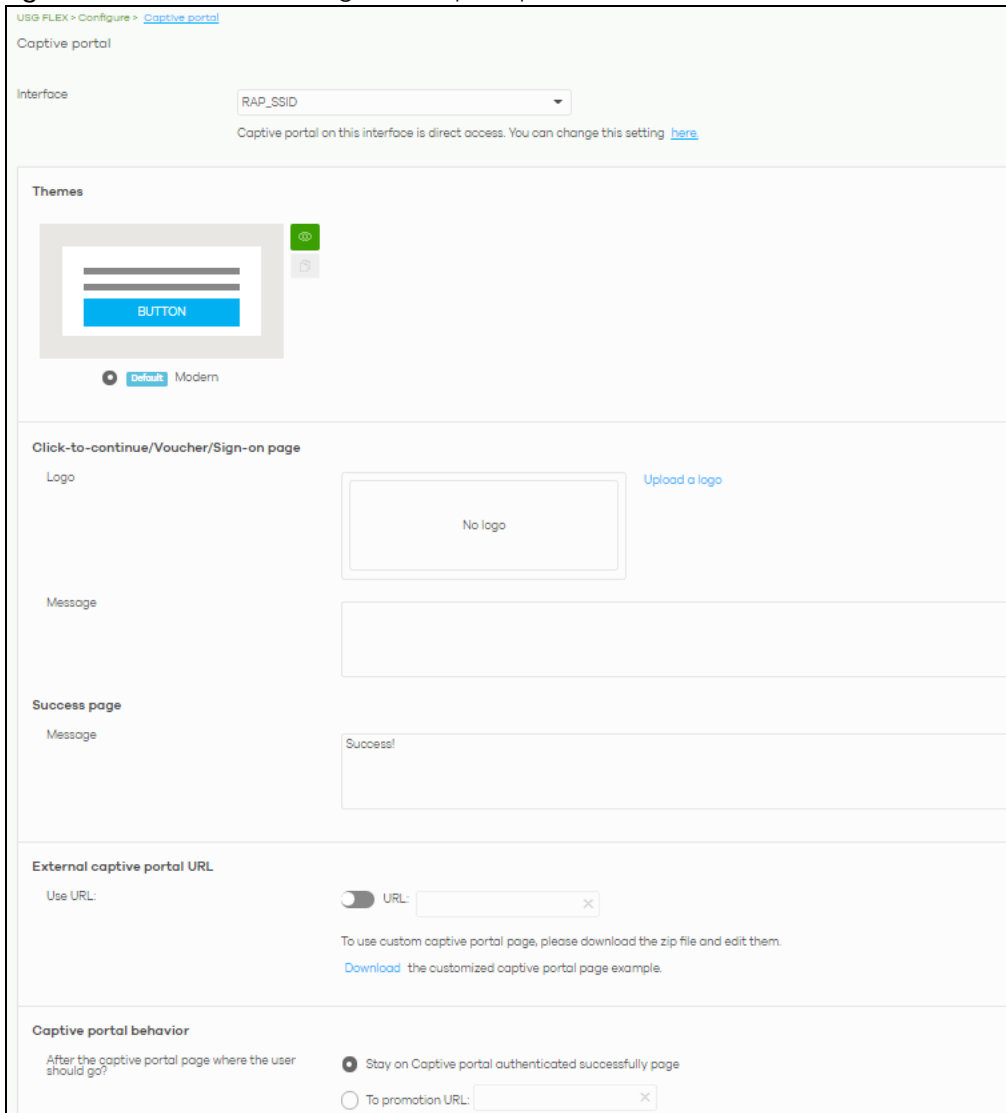
LABEL	DESCRIPTION
Add profile	
Name	This column lists the names of the application patrol profile rule.
Description (Optional)	This column lists the description of the application patrol profile rule.
Log	Select whether to have the Security Gateway generate a log when the policy is matched to the criteria 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 Security Gateway 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 **USG FLEX > Configure > Captive portal** to access this screen.

Figure 144 USG FLEX > Configure > Captive portal



The following table describes the labels in this screen.

Table 123 USG FLEX > Configure > Captive portal

LABEL	DESCRIPTION
Interface	Select the gateway'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 corner 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 305</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> .

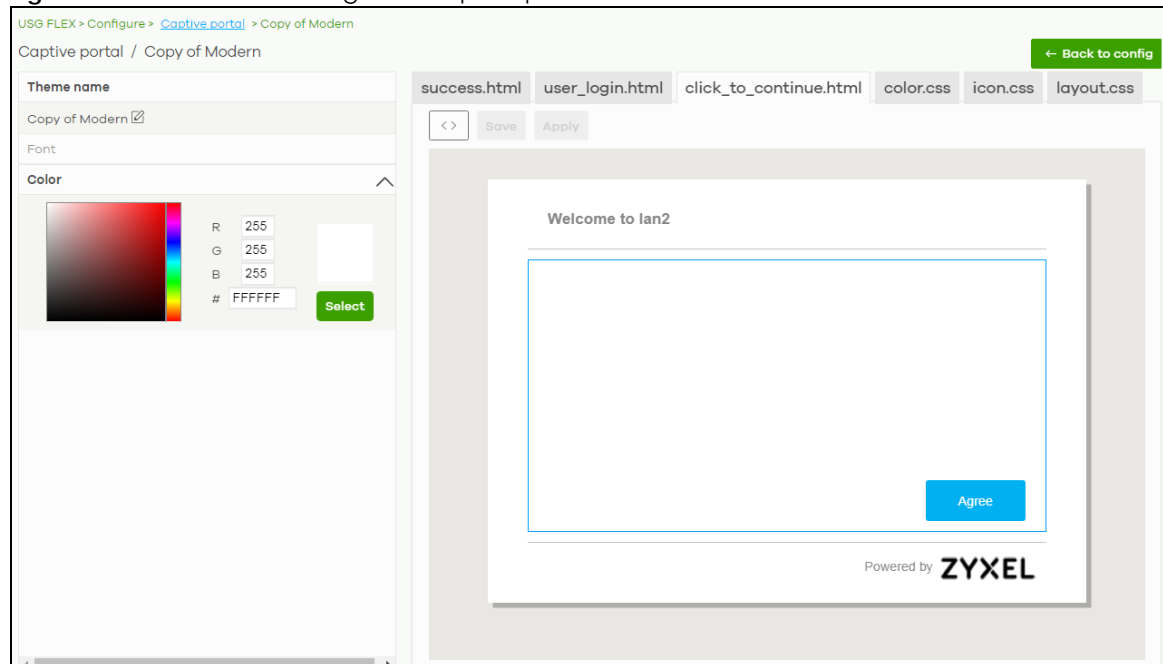
Table 123 USG FLEX &gt; Configure &gt; Captive portal (continued)

LABEL	DESCRIPTION
Logo	This shows the logo image that you uploaded for the customized login page. 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.
Message	Enter a note to display below the title. Use up to 1024 printable ASCII characters. Spaces are allowed.
Success page	
Message	Enter a note to display on the page that displays when a user logs in successfully. Use up to 1024 printable ASCII characters. Spaces are allowed.
External captive portal URL	
Use URL	Select <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. Specify the login page's URL; for example, http://IIS server IP Address/login.asp. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Captive portal behavior	
After the captive portal page where the user should go?	Select <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 **USG FLEX > Configure > Captive portal** screen to access this screen.

Figure 145 USG FLEX &gt; Configure &gt; Captive portal: Edit



The following table describes the labels in this screen.

Table 124 USG FLEX > Configure > 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 on 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 a HTML file to display the portal page. You can also change colors and modify the CSS values of the selected HTML file.
	Click this button to view and modify the CSS values of the selected HTML file. It is recommended that you do NOT change the script code to ensure proper operation of the portal page.
	Click this button to preview the portal page (the selected HTML file).
Save	Click this button to save your settings for the selected HTML file to the NCC.
Apply	Click this button to save your settings for the selected HTML file to the NCC and apply them to the security gateway in the site.

### 9.3.10 Authentication Method

Use this screen to enable or disable web authentication on an interface.

Click **USG FLEX > Configure > Authentication Method** to access this screen.

**Figure 146** USG FLEX > Configure > Authentication Method

The screenshot shows the 'Authentication Method' configuration page in USG FLEX. At the top, the breadcrumb is 'USG FLEX > Configure > Authentication Method'. Below the breadcrumb, 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 turned on).
- Walled garden:** Contains a toggle switch that is turned on, and a text input field for 'Walled garden ranges' with a link 'What do I enter here?' 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 125 USG FLEX &gt; Configure &gt; Authentication method

LABEL	DESCRIPTION
Interfaces	Select the gateway'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>USG FLEX &gt; Configure &gt; Gateway Settings</b> screen (see <a href="#">Section 9.3.13 on page 312</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>

Table 125 USG FLEX &gt; Configure &gt; Authentication method (continued)

LABEL	DESCRIPTION
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 Authentication Method

Use this screen to enable or disable web authentication on an interface.

Click **USG FLEX > Configure > Authentication Method** to access this screen.



**Figure 147** USG FLEX > Configure > Authentication Method

USG FLEX > Configure > Authentication Method

Authentication Method

Interfaces:

---

**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

Two-factor authentication [?](#)

---

**Walled garden**

Walled garden ranges

[What do I enter here?](#)

---

**Captive portal access attribute**

Self-registration

Login on multiple client devices

---

**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 126 USG FLEX &gt; Configure &gt; Authentication method

LABEL	DESCRIPTION
Interfaces	Select the gateway'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>USG FLEX &gt; Configure &gt; Gateway Settings</b> screen (see <a href="#">Section 9.3.13 on page 312</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>

Table 126 USG FLEX &gt; Configure &gt; Authentication method (continued)

LABEL	DESCRIPTION
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>

### 9.3.12 Wireless

This screen allows you to configure different SSID profiles for your USG FLEX. 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 **USG FLEX > Configure > Wireless** to access this screen.

Figure 148 USG FLEX &gt; Configure &gt; Wireless

USG FLEX > Configure > Wireless

Wireless

**SSID Settings**

No.	1	2	3	4
Name	aaaaaaaaaaaaaaaa	bbbbbb	vvvv	ccccccc
Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WLAN Security	WPA2-PSK	Open	WPA2-PSK	Open
Associate Key	*****		*****	
Band	Concurrent operation(2.4G...)	2.4GHz band only	5GHz band only	Concurrent operation(2.4G...)
Outgoing Interface	lan1	lan1	lan2	VLAN1

**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

Current channel: 1 [2.4GHz]

Current channel: 153\*/149/157/161 [5GHz]

The following table describes the labels in this screen.

Table 127 USG FLEX &gt; Configure &gt; 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.
Outgoing Interface	Select the interface for outgoing traffic from the security gateway to the Internet.
Radio Settings	
Maximum output power	Enter the maximum output power of the radio (in dBm).

Table 127 USG FLEX &gt; Configure &gt; Wireless (continued)

LABEL	DESCRIPTION
Channel width	<p>Select the WiFi channel bandwidth you want the USG FLEX 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. A 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 wireless signal.</p> <p>Note: It is suggested that you select 20 MHz when there is more than one 2.4 GHz USG FLEX 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 3 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 3 "safe" channels.</p> <p>Select <b>Four-Channel Deployment</b> to limit channel switching to 4 channels. Depending on the country domain, if the only allowable channels are 1 – 11 then the USG FLEX uses channels 1, 4, 7, 11 in this configuration; otherwise, the USG FLEX 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 USG FLEX switches between for 5 GHz operation.</p> <p>Select <b>Auto</b> to have the USG FLEX automatically select the best channel.</p> <p>Select <b>Manual</b> to choose from the allowable channels.</p>

### 9.3.13 Gateway Settings

Use this screen to configure DNS settings and external AD (Active Directory), RADIUS, or LDAP server that the Security Gateway 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 gateway. The settings in this screen apply to all networks (interfaces) on the Security Gateway. If you want to configure walled garden web site links for a specific interface, use the **Authentication method** screen.

Click **USG FLEX > Configure > Gateway settings** to access this screen.

**Figure 149** USG FLEX > Configure > Gateway settings

USG FLEX > Configure > [Gateway settings](#)

Gateway settings

**DNS**

Address Record

[+ Add](#)

Domain Zone Forwarder

[+ 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

[+ Add](#)

My LDAP Server

[+ Add](#)

My RADIUS Server

[+ 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 128 USG FLEX &gt; Configure &gt; 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.

Table 128 USG FLEX &gt; Configure &gt; Gateway settings (continued)





LABEL	DESCRIPTION
Domain Zone Forwarder	This specifies a DNS server's IP address. The security gateway can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the security gateway 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 security gateway 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 security gateway 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 security gateway 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 9.3.13.3 on page 319</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.
Port	Specify the port number on the LDAP server to which the USG FLEX 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 9.3.13.3 on page 319</a> .
	Click this icon to remove the entry.
My RADIUS server	

Table 128 USG FLEX &gt; Configure &gt; Gateway settings (continued)

LABEL	DESCRIPTION
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 security gateway 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 security gateway.  The key is not sent over the network. This key must be the same on the external authentication server and the security gateway.
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 9.3.13.3 on page 319</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.
Isolate unwanted traffic between tunnel mode APs	Select <b>On</b> to block broadcast and multicast traffic coming from Remote APs (RAPs).

### 9.3.13.1 Dynamic DNS

Enable **Dynamic DNS** to open the **USG FLEX > Configure > Gateway settings: Dynamic DNS** screen.

**Figure 150** USG FLEX > Configure > Gateway settings: Dynamic DNS

**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

DDNS type

**DDNS account**

Username

Password

Confirm password

**DDNS settings**

Domain name

**Primary binding address**

Interface

IP address

**Backup binding address**

Interface

IP address

Enable wildcard

Mail exchanger  (Optional)

Backup mail exchanger

The following table describes the labels in this screen.

**Table 129** USG FLEX > Configure > Gateway 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> .
DDNS account	
Username	Enter the user name used when you registered your domain name.
Password	Enter the password provided by the DDNS provider.



Table 129 USG FLEX &gt; Configure &gt; Gateway settings: Dynamic DNS (continued)

LABEL	DESCRIPTION
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 security gateway determines the IP address that is mapped to your domain name in the DDNS server. The security gateway 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 gateway 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 gateway and the DDNS server.</p> <p>Note: The gateway 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 gateway 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 gateway 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 gateway and the DDNS server.</p> <p>Note: The gateway 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 gateway 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, <a href="http://www.yourhost.dyndns.org">www.yourhost.dyndns.org</a> 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 <a href="mailto:john-doe@yourhost.dyndns.org">john-doe@yourhost.dyndns.org</a> 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 e-mail. 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>

Table 129 USG FLEX &gt; Configure &gt; Gateway settings: Dynamic DNS (continued)

LABEL	DESCRIPTION
DYNDNS Server	This field displays when you select <b>User customize</b> from the <b>DDNS provider</b> field above. Type the IP address of the server that will host the DDSN service.
URL	This field displays when you select <b>User customize</b> from the <b>DDNS provider</b> field above. Type the URL that can be used to access the server that will host the DDSN 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>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>

### 9.3.13.2 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 **USG FLEX > Configure > Gateway 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 151 USG FLEX &gt; Configure &gt; Gateway 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 130 USG FLEX > Configure > Gateway settings: SIP ALG

LABEL	DESCRIPTION
SIP ALG	Turn on SIP ALG to detect SIP traffic and help build SIP sessions through the USG FLEX'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 USG FLEX 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 USG FLEX 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 USG FLEX 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 USG FLEX.  If the SIP client does not have this mechanism and makes no calls during the USG FLEX SIP timeout, the USG FLEX 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.

### 9.3.13.3 Advanced Settings

Click the **Advanced** column in the **USG FLEX > Configure > Gateway settings** screen to access this screen.

Figure 152 USG FLEX > Configure > Gateway settings: Advanced

Advanced
✕

Preset:

Timeout:  ✕ (1-300 seconds)

Case-Sensitive User Name:  off

NAS IP Address:  ✕

The following table describes the labels in this screen.

Table 131 USG FLEX > Configure > 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 security gateway 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 servers 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 USG FLEX 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

## Switch

### 10.1 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.

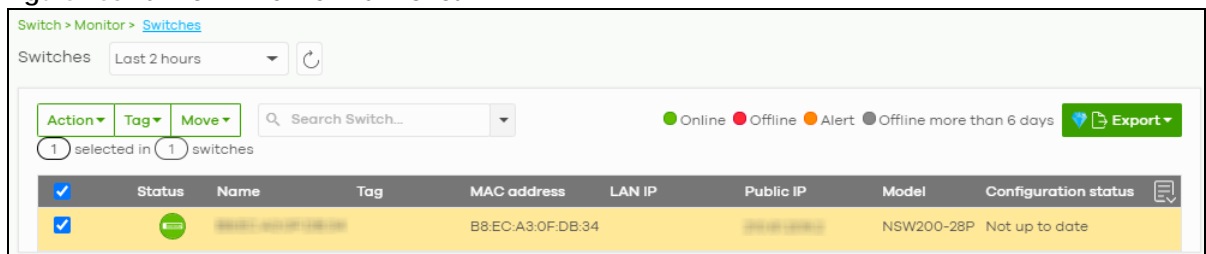
### 10.2 Monitor

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.

#### 10.2.1 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 153 Switch > Monitor > Switches




The following table describes the labels in this screen.

Table 132 Switch > Monitor > Switches

LABEL	DESCRIPTION
Switch	Select to view the device information and connection status in the past two hours, day, week or month.
	Click this button to reload the data-related frames on this page.
Action	Perform an action on the selected Nebula Devices.
Reboot	Restart the Nebula Device.
Upgrade	Upgrade the firmware on the Nebula Device.
Tag	Select one or multiple Nebula Devices and click this button to create a new tag for the Nebula Devices or delete an existing tag.
Move	Select one or multiple Nebula Devices and click this button to move the Nebula Device to another site or remove the Nebula Device from the current site.
Search	Specify your desired filter criteria to filter the list of Nebula Devices.

Table 132 Switch &gt; Monitor &gt; Switches (continued)

LABEL	DESCRIPTION
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.</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> <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	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 off-line.</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.
Current version	This shows the firmware version currently installed on the device.
Usage	This shows the amount of data that has been transmitted or received by the Nebula Device's clients.
	Click this icon to display a greater or lesser number of configuration fields.

### 10.2.1.1 Switch Details

Click a Nebula Device entry in the **Switch > Monitor > Switches** screen to display individual Nebula Device statistics.

Figure 154 Switch > Monitor > Switches: Switch Details

Switch > Monitor > [Switch](#) > 2F-SWT

Switch / 2F-SWT

### Configuration

Name: 2F-SWT  
 MAC address: B0-0E-4E-53-DE-00  
 Serial number: 6100125000049 (GS1350-18HP)  
 Description:  
 Address:  
 Tag:

### Status

LAN IP: 192.168.10.219 (via DHCP)   
 Gateway: 192.168.10.254  
 DNS: 192.168.10.254,8.8.8.8  
 VLAN: 1  
 DHCP server: 192.168.10.254   
 Public IP: 207.171.27.149  
 Topology: [Show](#)  
 RSTP status: root is [1F-SWT](#) / root bridge priority: 4096  
 IGMP status: Enabled  
 PoE status: Consumption 19.1 / 250 W   
 History: [Event log](#)  
 Configuration status: Up to date  
 Firmware: [Custom](#)  
 Current version: V4.70(ABPK1)b1 | 03/02/2021

Map Photo

Floor plan

Map Satellite

Zhongyang Road

Fuhou Street

Fuhou Street

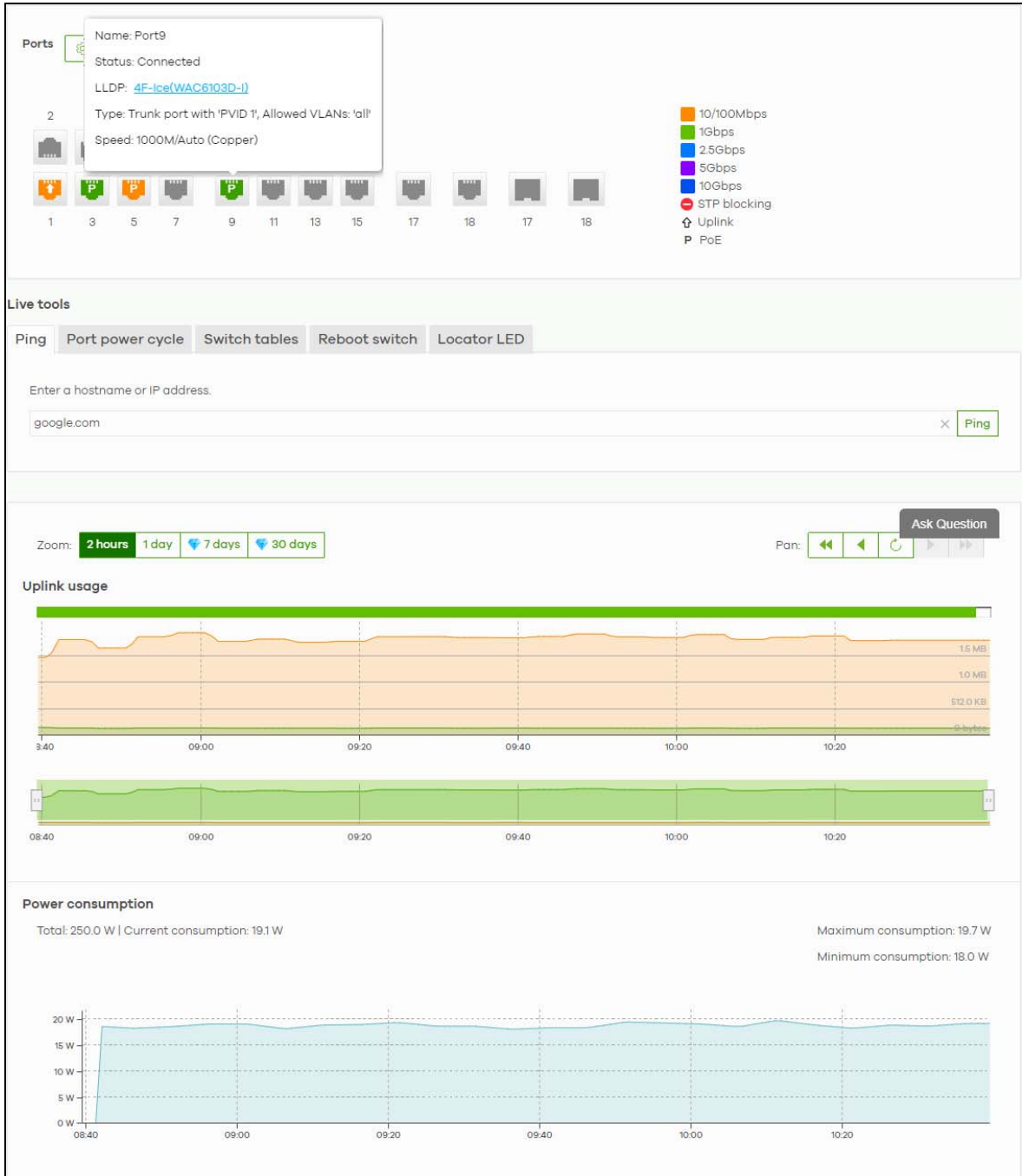
Wenhua Street

Hsinchu Moat Park

20 湖濱公園  
Ark strip  
Community Center

Ask Question

Google Keyboard shortcuts Map data ©2021 Google 10 m L Terms of Use Report a map error



The following table describes the labels in this screen.

Table 133 Switch > Monitor > Switches: Switch Details


LABEL	DESCRIPTION
	Click this button to reload the data-related frames on this page.
Configuration	
Click the edit icon to change the device name, description, tags and address. You can also move the device to another site. After modifying a device name, the new name will be synchronized to the device and can be seen by protocols such as SNMP and LLDP.	



Table 133 Switch &gt; Monitor &gt; Switches: Switch Details (continued)

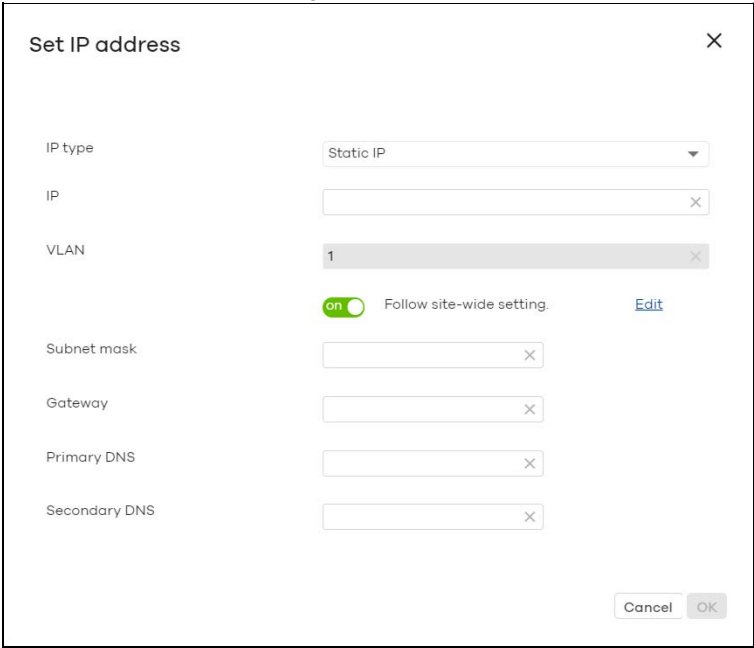
LABEL	DESCRIPTION
Name	This shows the descriptive name of the Nebula Device.
MAC Address	This shows the MAC address of the Nebula Device.
Serial Number	This shows the serial number of the Nebula Device.
Description	This shows the user-specified description for the Nebula Device.
Address	This shows the user-specified address for the Nebula Device.
Tags	This shows the user-specified tag for the Nebula Device.
Status	
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 7.1.5 on page 160</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 10.2.1.2 on page 327</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.

Table 133 Switch &gt; Monitor &gt; Switches: Switch Details (continued)



LABEL	DESCRIPTION
Firmware	This shows whether the firmware on the Nebula Device is up-to-date or there is firmware update available for the Nebula Device.
Current version	This shows the firmware version currently installed on the Nebula Device.
Map	This shows the location of the Nebula Device on the Google map.
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.
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 10.2.1.3 on page 327</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, 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.
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 10.3.1 on page 341</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 arranges the data in the summary table below.</p>
Switch tables	<p>This shows the MAC address, routing, and ARP tables on the Nebula Device. To import the data into NCC, click <b>Run</b>.</p> <p>Note: The ARP table and routing table are only displayed for L3 Nebula Devices</p>
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>
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.

Table 133 Switch &gt; Monitor &gt; Switches: Switch Details (continued)

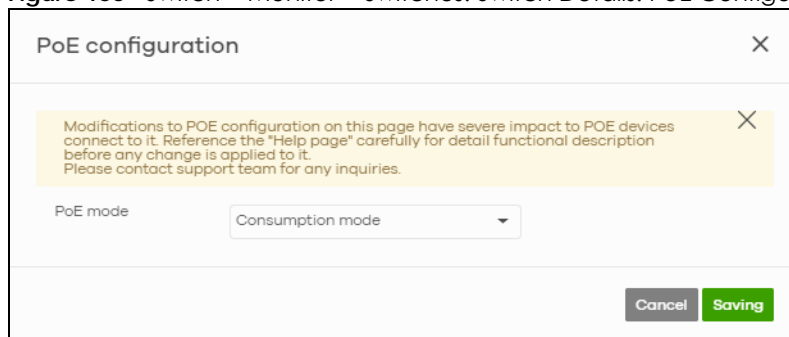
LABEL	DESCRIPTION
Pan	Click to move backward or forward by one day or week.
Power Consumption	
	Select to view the Nebula Device power consumption in the past two hours, day, week or month.
	This shows the current, total, maximum and minimum power consumption of the Nebula Device.
y-axis	The y-axis shows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

### 10.2.1.2 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 10.3.1 on page 341](#).

Figure 155 Switch &gt; Monitor &gt; Switches: Switch Details: PoE Configuration



The following table describes the labels in this screen.

Table 134 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.

### 10.2.1.3 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 156 Switch > Monitor > Switches: Switch Details: Port Details



The following table describes the labels in this screen.

Table 135 Switch > Monitor > 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 drawing 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, 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 10.3.1 on page 341</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	
Total	This shows the total power consumption of the port.

Table 135 Switch &gt; Monitor &gt; Switches: Switch Details: Port Details (continued)

LABEL	DESCRIPTION
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.
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 3 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 135 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 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.

## 10.2.2 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 150](#).

## 10.2.3 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 157** Switch > Monitor > Event log

The screenshot shows the 'Event log' interface. At the top, there are search filters for Switch (Any), Keyword (Any), Priority (Any), and Category (Any). Below these is a Tag field (Any) and a date/time range selector. The range is set from 2019-10-29 10:20 to 2019-10-30 11:20 UTC+8. A 'Search' button is visible. Below the filters, there are navigation buttons for 'Newer' and 'Older', a count of '8 Event log' items, and an 'Export' button. The main part of the screen is a table with the following columns: Time, Priority, Switch, Tag, Category, and Detail. The table contains eight entries, all with 'Information' priority and 'Broadcast storm detected on port 4 - P...' in the detail column. The Switch column for all entries is 'Home NSW100' and the Tag column is 'interface'.

Time	Priority	Switch	Tag	Category	Detail
2019-10-29 20:26:11	Information	<a href="#">Home NSW100</a>	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-29 20:45:...	Information	<a href="#">Home NSW100</a>	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-29 22:17:50	Information	<a href="#">Home NSW100</a>	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 06:13:...	Information	<a href="#">Home NSW100</a>	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 07:04:...	Information	<a href="#">Home NSW100</a>	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 08:31:52	Information	<a href="#">Home NSW100</a>	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 08:44:...	Information	<a href="#">Home NSW100</a>	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 09:04:...	Information	<a href="#">Home NSW100</a>	interface	Interface	Broadcast storm detected on port 4 - P...

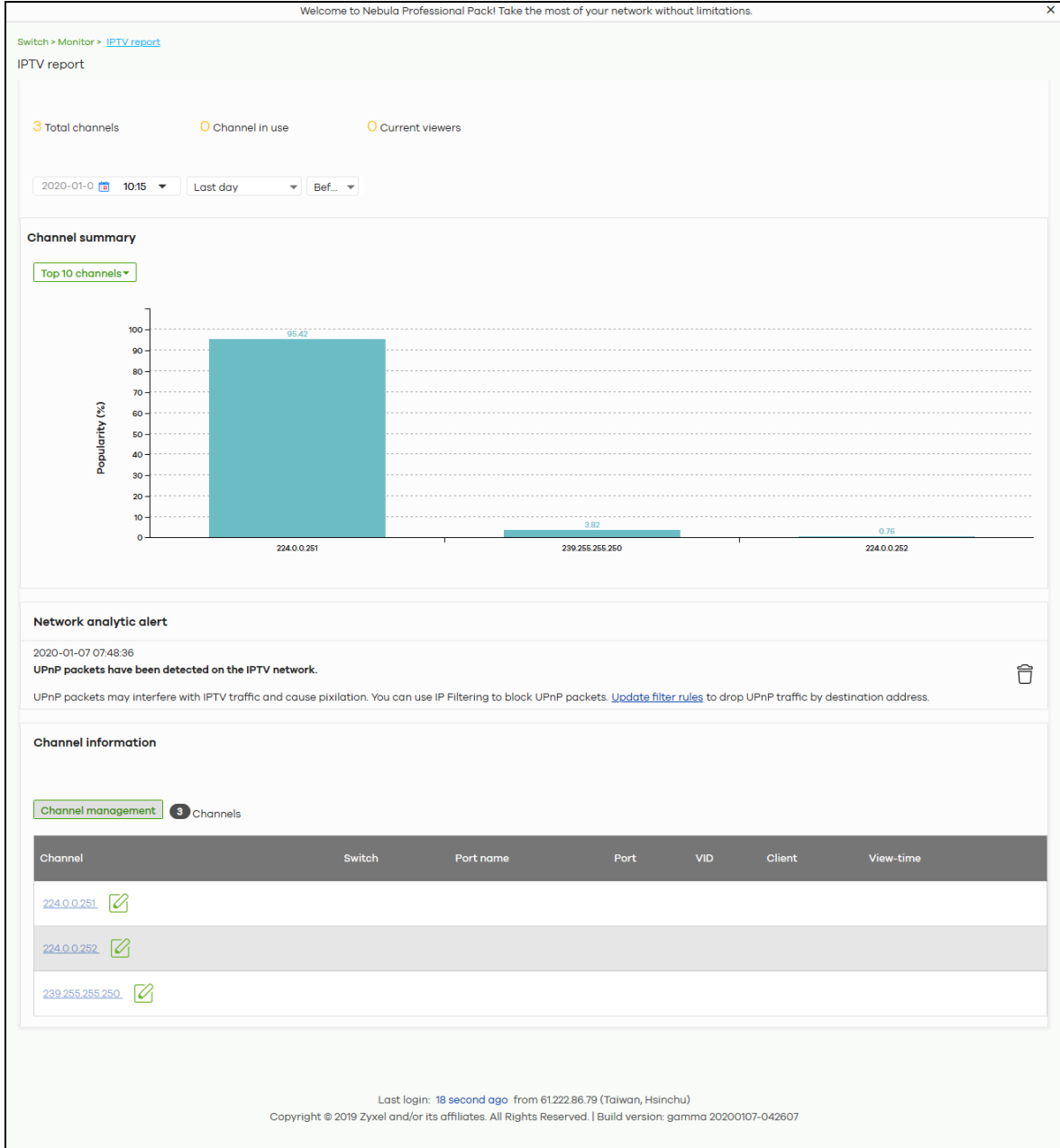
## 10.2.4 IPTV Report

Use this screen to view available IPTV channels and client information.

Click **Switch > Monitor > IPTV Report** to access this screen.



Figure 158 Switch &gt; Monitor &gt; IPTV Report



The following table describes the labels in this screen.

Table 136 Switch &gt; Monitor &gt; IPTV Report

LABEL	DESCRIPTION
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.
Search	Specify a date/time and select to view the channels available in the past day, week or month before the specified date/time after you click <b>Search</b> .  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.

Table 136 Switch &gt; Monitor &gt; IPTV Report (continued)

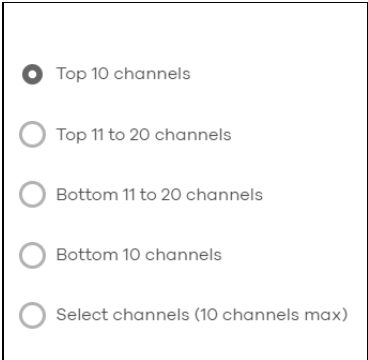
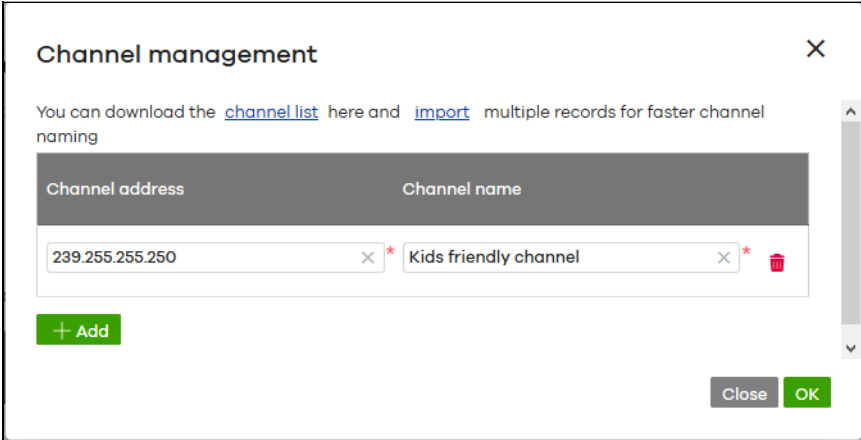
LABEL	DESCRIPTION
Channel Summary	
	<p>Select to view the channels according to the ranking. Alternatively, select <b>Select channels</b> to choose specific channels and click <b>Apply</b>.</p> 
y-axis	The y-axis represents the popularity of IPTV channels.
x-axis	The x-axis shows the name of the IPTV channel. It shows the channel's multicast group address by default.
Network Analytic Alert	<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	
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 10.2.4.1 on page 335</a>.</p>
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.

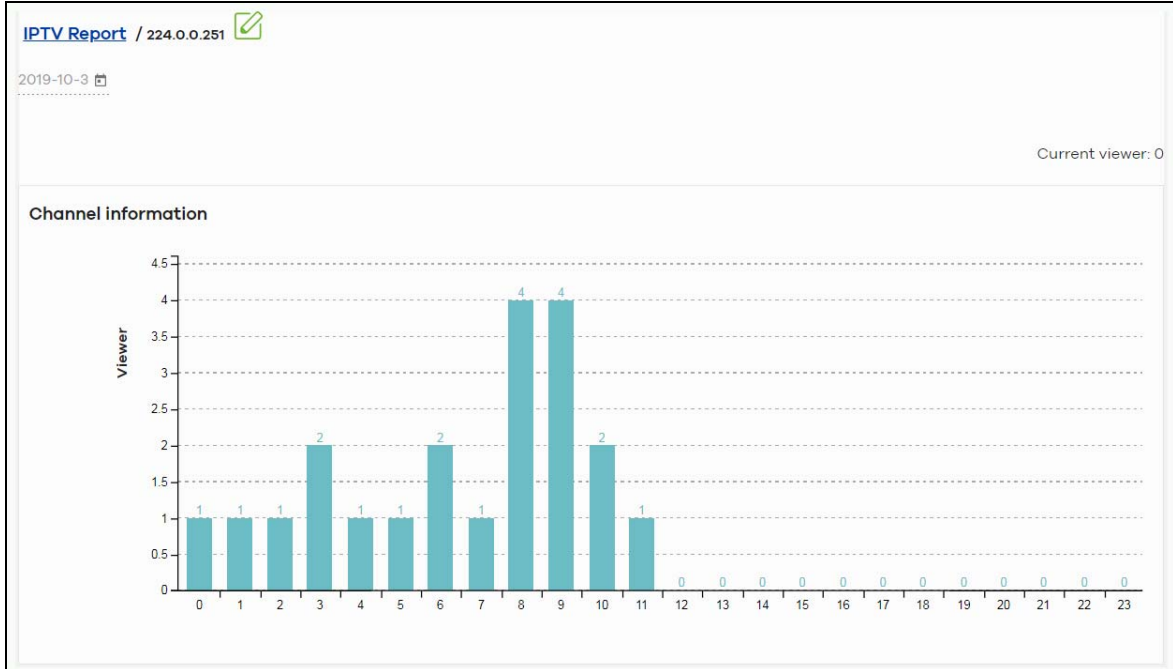
Table 136 Switch &gt; Monitor &gt; IPTV Report (continued)

LABEL	DESCRIPTION
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.

### 10.2.4.1 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 159 Switch &gt; Monitor &gt; IPTV Report: Channel Information



The following table describes the labels in this screen.

Table 137 Switch &gt; Monitor &gt; IPTV Report: Channel Information

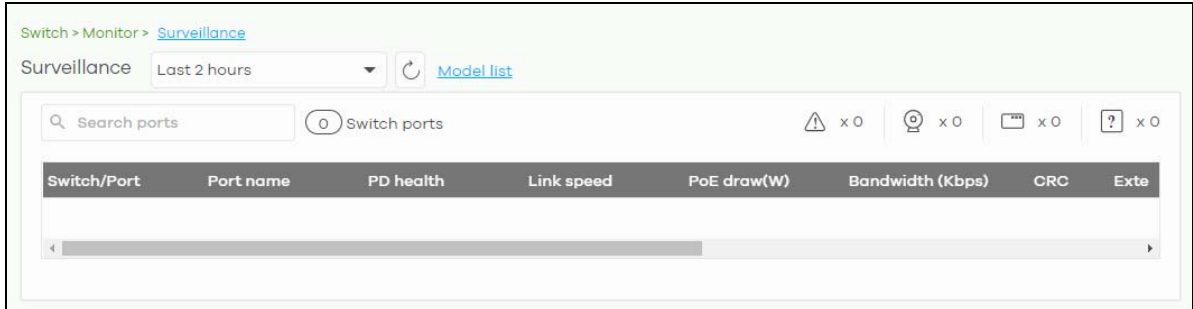
LABEL	DESCRIPTION
	Select a specific date to display only the clients who watch the IPTV channel on that day.
Current Viewer	This shows the number of clients who are currently watching the IPTV channel.
y-axis	The y-axis shows the number of clients watching the IPTV channel.
x-axis	The x-axis shows the 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.

## 10.2.5 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 160** Switch > Monitor > Surveillance



The following table describes the labels in this screen.

**Table 138** 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 a automatic PD alive check.
	This shows the number of ONVIF-compatible IP camera devices connected to Nebula Devices in the site.
	This shows the number of ONVIF-compatible NVR devices connected to Nebula Devices in the site.
	This shows the number of connected devices that did not respond to an ONVIF discovery query, or are of an unknown type.
Switch/Port	This shows the port number of the Nebula Device.
Port Name	This shows the port description on the Nebula Device.
PD Health	<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 10.3.1 on page 341</a>.</p>
Link Speed	This shows the speed (either <b>10M</b> for 10Mbps, <b>100M</b> for 100Mbps, 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.

Table 138 Switch &gt; Monitor &gt; Surveillance (continued)

LABEL	DESCRIPTION
CRC	This shows the number of packets received with CRC (Cyclic Redundant Check) errors.
Extended Range	This shows whether extended range is enabled on the port.
Device type	This shows the device type of the PD, as reported by ONVIF discovery.
System name	This shows the name of the connected PD, as reported by ONVIF or LLDP.
IP	This shows the IP address of the connected PD, as reported by ONVIF or LLDP.
Discovered Devices	This shows how many devices are connected to the port. Click the number to go to the <b>Surveillance Port Details</b> screen.

## 10.2.6 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 161 Switch &gt; Monitor &gt; Surveillance &gt; Port Details

The following table describes the labels in this screen.

Table 139 Switch &gt; Monitor &gt; Surveillance &gt; Port Details

LABEL	DESCRIPTION
Status	
Link speed	This shows the speed (either <b>10M</b> for 10Mbps, <b>100M</b> for 100Mbps, 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.

Table 139 Switch &gt; Monitor &gt; Surveillance &gt; Port Details (continued)

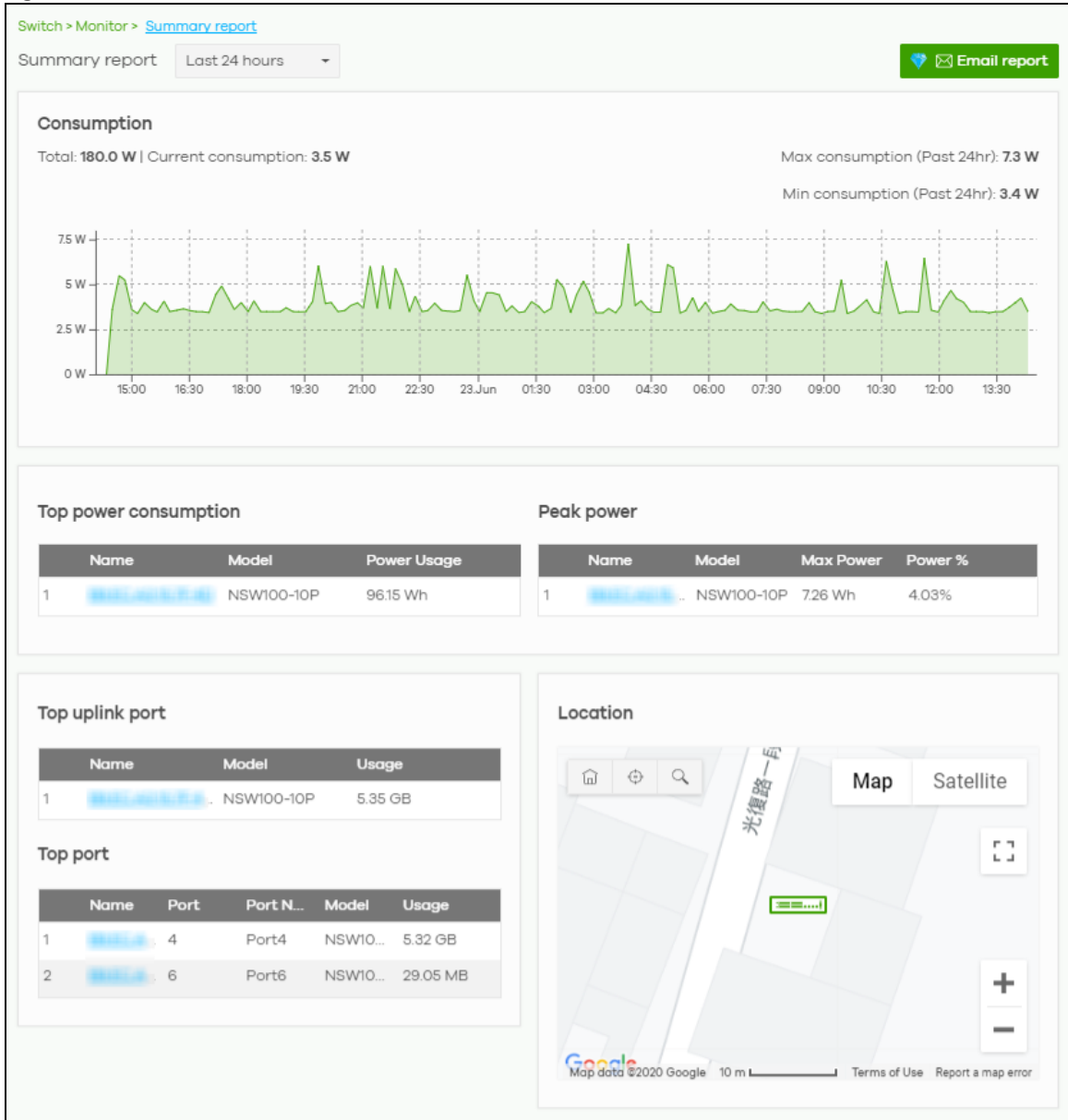
LABEL	DESCRIPTION
PoE draw	This shows the total power that the connected PD draws from the port, in watts. This allows you to plan and use within the power budget of the Nebula Device.
PD health	<p>This shows the status of auto PD recovery on this port.</p> <ul style="list-style-type: none"> <li>• Red: 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 Nebula Device is not supplying power to the connected PD.</li> </ul> <p>For details on configuring auto PD recovery on a port, see <a href="#">Section 10.3.1 on page 341</a>.</p>
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.
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 device.

## 10.2.7 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 162 Switch > Monitor > Summary Report



The following table describes the labels in this screen.

Table 140 Switch &gt; Monitor &gt; Summary Report

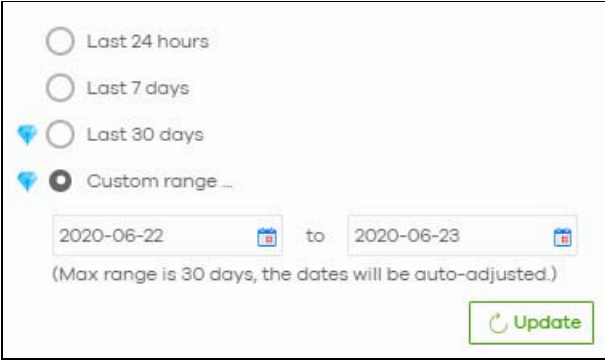
LABEL	DESCRIPTION
Switch – Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Custom range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click this button 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 140 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.

## 10.3 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.

### 10.3.1 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 163 Switch &gt; Configure &gt; Switch ports

Switch > Configure > Switch ports

Switch ports Last 2 hours

Edit Aggregate Split Tag Search ports... 2 selected in 38 Switch ports Export

Switch / Port	# Port	Port name	Allowed VLAN	Broadcast (pps)	Connection	DLF (pps)	Enabled	LLDP
<input checked="" type="checkbox"/> Office NSW200/1 <a href="#">details</a>	1	Port1	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled
<input checked="" type="checkbox"/> Office NSW200/2 <a href="#">details</a>	2	Port2	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled
<input type="checkbox"/> Office NSW200/3 <a href="#">details</a>	3	Port3	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled
<input type="checkbox"/> Office NSW200/4 <a href="#">details</a>	4	Port4	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled
<input type="checkbox"/> Office NSW200/5 <a href="#">details</a>	5	Port5	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled
<input type="checkbox"/> Office NSW200/6 <a href="#">details</a>	6	Port6	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled
<input type="checkbox"/> Office NSW200/7 <a href="#">details</a>	7	Port7	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled
<input type="checkbox"/> Office NSW200/8 <a href="#">details</a>	8	Port8	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled
<input type="checkbox"/> Office NSW200/9 <a href="#">details</a>	9	Port9	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled
<input type="checkbox"/> Office NSW200/10 <a href="#">details</a>	10	Port10	all	100	<div style="width: 100%;"></div>	100	Enabled	Enabled

Page 1 of 4 Results per page: 10

The following table describes the labels in this screen.

Table 141 Switch > Configure > Switch ports



LABEL	DESCRIPTION
Switch ports	Select to view the detailed information and connection status of the Nebula Device port in the past two hours, day, week or month.
	Click this button to reload the data-related frames on this page.
Edit	Select the ports you want to configure and click this button to configure Nebula Device settings on the ports, such as link aggregation, PoE schedule, LLDP and STP.
Aggregate	Select more than one port and click this button to group the physical ports into one logical higher-capacity link.
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.
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.
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 10.2.1.3 on page 327</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.
Link	This shows the speed of the Ethernet connection on this port.  <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.

Table 141 Switch &gt; Configure &gt; Switch ports (continued)

LABEL	DESCRIPTION
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, 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>
RADIUS policy	This shows the name of RADIUS 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 (pps)	This shows the maximum number of broadcast packets the Nebula Device accepts per second on this port.
Multicast (pps)	This shows the maximum number of multicast packets the Nebula Device accepts per second on this port.
DLF (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.
Number of IGMP Group	This shows the number of IGMP groups the port has joined.
	Click this icon to display a greater or lesser number of configuration fields.

### 10.3.1.1 Update ports

Select the ports you want to configure and click the **Edit** button in the **Switch > Configure > Switch ports** screen.

Figure 164 Switch &gt; Configure &gt; Switch ports: Edit

The following table describes the labels in this screen.

Table 142 Switch &gt; Configure &gt; 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.
Enabled	Select to enable or disable the ports. A port must be enabled for data transmission to occur.
RSTP	Select to enable or disable RSTP on the ports.
STP guard	This field is available only when RSTP is enabled on the ports. Select <b>Root guard</b> to prevent the Nebula Devices attached to the ports from becoming the root bridge. Select <b>BPDU guard</b> to have the Nebula Device shut down the ports if there is any BPDU received on the ports. Otherwise, select <b>Disable</b> .
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>Auto-1000M</b> , <b>10M/Half Duplex</b> , <b>10M/Full Duplex</b> , <b>100M/Half Duplex</b> , <b>100M/Full Duplex</b> and <b>1000M/Full Duplex</b> (Gigabit connections only).

Table 142 Switch &gt; Configure &gt; Switch ports: Edit (continued)

LABEL	DESCRIPTION
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>
RADIUS policy	<p>This field is available only when you select <b>Access</b> in the <b>Type</b> field.</p> <p>Select the name of the pre-configured RADIUS policy that you want to apply to the ports. Select <b>Open</b> if you do not want to enable port authentication on the ports.</p>
Bandwidth Control	<p>Select to enable or disable bandwidth control on the port.</p>
Ingress	<p>Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on the ports.</p>
Egress	<p>Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on the ports.</p>
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 (pps)	<p>Specifies the maximum number of broadcast packets the Nebula Device accepts per second on the ports.</p>
Multicast (pps)	<p>Specifies the maximum number of multicast packets the Nebula Device accepts per second on the ports.</p>
DLF (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>
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 10.3.8 on page 361</a>.</p>

Table 142 Switch &gt; Configure &gt; Switch ports: Edit (continued)

LABEL	DESCRIPTION
PVID	<p>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.</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 is allowed to be transmitted or received on the ports.</p>
PoE Settings	
PoE	Select <b>Enable</b> to provide power to a PD connected to the ports.
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>
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>
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>
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>

Table 142 Switch &gt; Configure &gt; Switch ports: Edit (continued)

LABEL	DESCRIPTION
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>
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>

Table 142 Switch &gt; Configure &gt; Switch ports: Edit (continued)

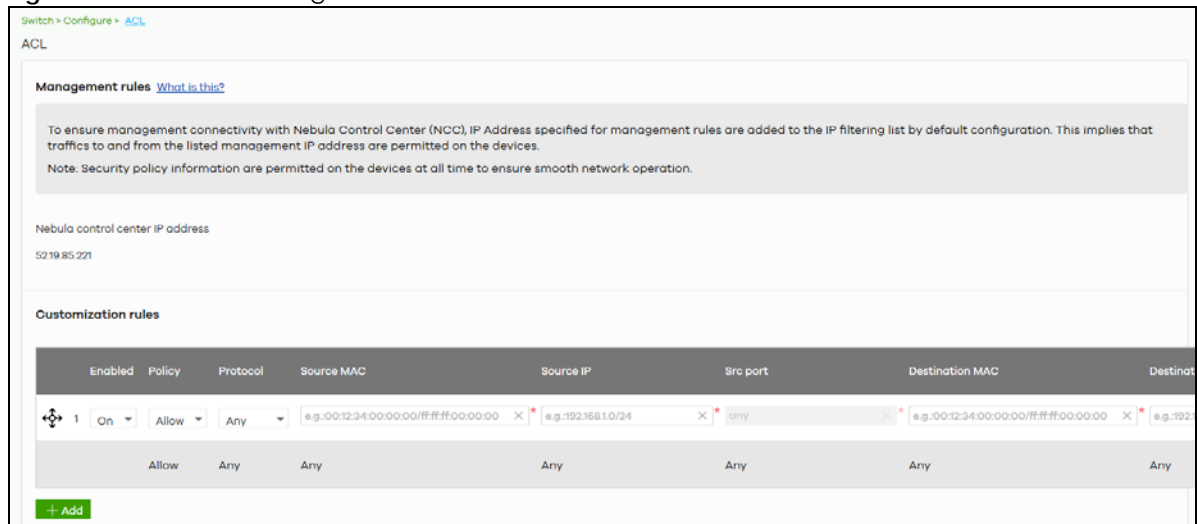
LABEL	DESCRIPTION
Maximum Group	Select <b>Enable</b> and enter the maximum number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report received on this port will replace the earliest group entry in the multicast forwarding table.  Otherwise, select <b>Disable</b> to turn off multicast group limits.
IGMP Filtering Profile	An IGMP filtering profile specifies a range of multicast groups that clients connected to the Nebula Device are able to join.  Select the name of the IGMP filtering profile to use for this port. Otherwise, select <b>No Select</b> to remove restrictions and allow the port to join any multicast group.
Fixed Router Port	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.  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.

## 10.3.2 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 165 Switch &gt; Configure &gt; ACL



The following table describes the labels in this screen.

Table 143 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.



Table 143 Switch &gt; Configure &gt; ACL (continued)

LABEL	DESCRIPTION
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.

### 10.3.3 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 166 Switch &gt; Configure &gt; IP &amp; Routing

Switch > Configure > [IP & Routing](#)

IP & Routing

**IP interface**

Switch	Name	IP address	Subnet mask	VLAN ID	
XS1930-12HP		192.168.123.255	255.255.255.0	123	

[+ Add](#)

**Static route**

Switch	Name	Destination	Subnet mask	Next hop IP address	
XGS1930-52HP	Test Route	12.13.14.15	255.255.255.0	16.17.18.19	

[+ Add](#)

The following table describes the labels in this screen.

Table 144 Switch &gt; Configure &gt; IP &amp; 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 gateway'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.

### 10.3.3.1 Add IP Interface

Click the + **Add** button on the **Switch > Configure > IP & Routing > IP Interface** screen to access this screen.

**Figure 167** Switch > Configure > IP & Routing > IP Interface > Add

The following table describes the labels in this screen.

Table 145 Switch > Configure > IP & Routing

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.

### 10.3.3.2 Add Static Route

Click the + **Add** button on the **Switch > Configure > IP & Routing > Static Route** screen to access this screen.

**Figure 168** Switch > Configure > IP & Routing > Static Route > Add

The following table describes the labels in this screen.

Table 146 Switch &gt; Configure &gt; IP &amp; Routing

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 address	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.

### 10.3.4 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.

### 10.3.4.1 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.

### 10.3.4.2 ONVIF Discovery Screen

Click **Switch > Configure > ONVIF discovery** to access this screen.

**Figure 169** Switch > Configure > ONVIF discovery

Switch > Configure > ONVIF discovery

ONVIF discovery

ONVIF configuration [Model list](#)

ONVIF discovery

ONVIF VLAN ID

Surveillance switch

	Switch name	Port list	Description	Model
1	2F-SWT	1-18		GS1350-18HP

+ Add

The following table describes the labels in this screen.

**Table 147** 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.

## 10.3.5 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 170** Switch > Configure > Advanced IGMP

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 [?](#) 1 IGMP filtering profiles

Test used by 0 ports 🗑️

[+ Add](#)

IPTV topology setup

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

Switch name	IGMP snooping	Role	Port settings
<input checked="" type="checkbox"/> B8:EC:A3:AE:EA:14	<input checked="" type="checkbox"/>	-Select role-	<a href="#">Advanced setup</a>

The following table describes the labels in this screen.

Table 148 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	Select <b>Auto-detect</b> to have the Nebula Device learn multicast group membership information of any VLANs automatically.  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.  Click <b>Model List</b> to view a list of Zyxel Nebula Device models that do not support this feature.  Note: The Nebula Device can perform IGMP snooping on up to 16 VLANs.
Unknown multicast drop	Specify the action to perform when the Nebula Device receives an unknown multicast frame. Select <b>ON</b> to discard the frames. Select <b>OFF</b> to send the frames to all ports.  Click <b>Model List</b> to view a list of Zyxel Nebula Device models that support this feature.
Drop on VLAN	This allows you to define the VLANs in which unknown multicast packets can be dropped.
IGMP filtering profiles	An IGMP filtering profile specifies a range of multicast groups that clients connected to the Nebula Device are able to join.  You can set the Nebula Device to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating a port to the profile.
	Click the edit icon to change the profile settings. See <a href="#">Section 10.3.5.1 on page 356</a> .
	Click the remove icon to delete the profile.
Add	Click this button to create a new profile. See <a href="#">Section 10.3.5.1 on page 356</a> .
IPTV Topology Setup	
The following three buttons are available only when there are multiple Nebula Devices in the site and your administrator account has full access to this screen.	
IGMP Snooping	Select the Nebula Devices you want to configure and click this button to turn on or off IGMP snooping on the selected Nebula Devices.
Role	Select the Nebula Devices you want to configure and click this button to change the IGMP role of the selected Nebula Devices.
Port Setting	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 10.3.5.2 on page 357</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	This shows whether IGMP snooping is enabled or not on the Nebula Device.
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. Click the question mark to view more information about IGMP roles.
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 10.3.5.2 on page 357</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.

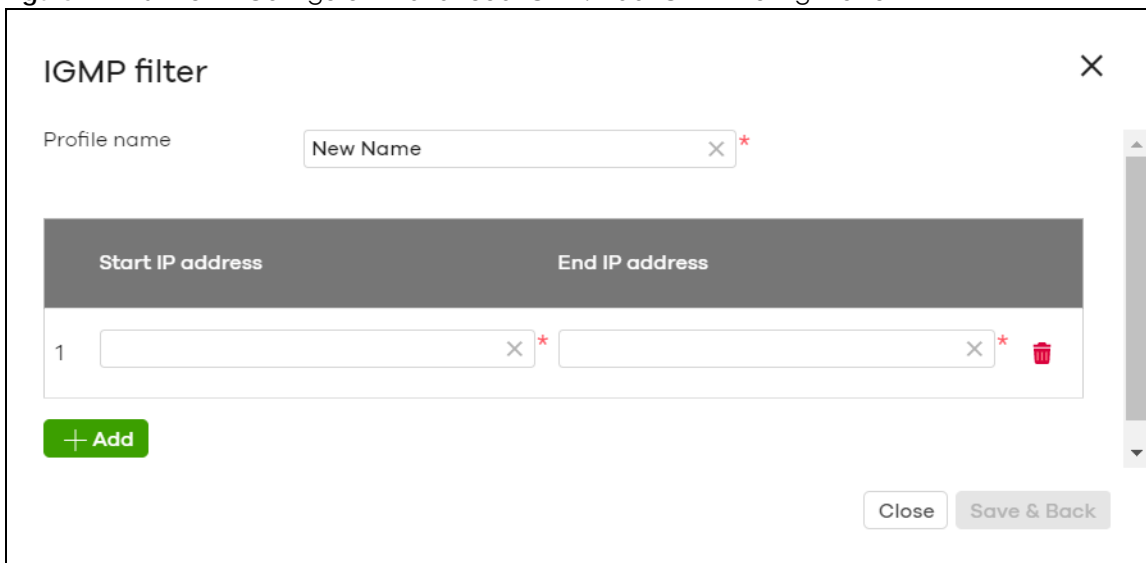
Table 148 Switch &gt; Configure &gt; Advanced IGMP (continued)

LABEL	DESCRIPTION
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.

### 10.3.5.1 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 171 Switch &gt; Configure &gt; Advanced IGMP: Add IGMP Filtering Profile



The following table describes the labels in this screen.

Table 149 Switch &gt; Configure &gt; Advanced IGMP: Add/Edit IGMP Filtering Profile


LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for this profile for identification purposes.
Rule	This shows the index number of the rule.
Start IP Address	Type 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	Type 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.



Table 149 Switch &gt; Configure &gt; Advanced IGMP: Add/Edit IGMP Filtering Profile (continued)

LABEL	DESCRIPTION
Close	Click this button to exit this screen without saving.
Save & Back	Click this button to save your changes and close the screen.

### 10.3.5.2 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 172 Switch &gt; Configure &gt; Advanced IGMP: Port Settings

The screenshot shows a 'Port settings' dialog box with the following fields and values:

- Switch name: Office NSW200
- Role: Aggregator
- Leave mode: Normal leave (dropdown), 4000 (text input with a red asterisk)
- Maximum group: Disable (dropdown)
- IGMP filtering profile: No select (dropdown)

Buttons for 'Close' and 'Save' are located at the bottom right of the dialog.

The following table describes the labels in this screen.

Table 150 Switch &gt; Configure &gt; 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 150 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.

### 10.3.6 RADIUS Policies

Use this screen to configure authentication servers and policies to validate access to ports on the Nebula Device using an external RADIUS server.

Click **Switch > Configure > RADIUS policies** to access this screen.

**Figure 173** Switch > Configure > RADIUS policies

Switch > Configure > [RADIUS policies](#)

RADIUS policies

**RADIUS server**

	Host	Port	Secret
1	192.168.8.1	1812	XXXXXXXXXX

+ Add

**RADIUS policy**

Password for MAC-Base Auth:

	RADIUS policy type	Guest VLAN	Port security	Limited numbers of MAC address	Switch ports (currently using this policy)
	802.1X	250	on	2	
	802.1X	100	off	0	

+ Add

The following table describes the labels in this screen.

Table 151 Switch &gt; Configure &gt; RADIUS policies




LABEL	DESCRIPTION
RADIUS server	
	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.
RADIUS policy	
Password for MAC-Base Auth	Type 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.
RADIUS policy type	Select <b>MAC-Base</b> if you want to validate access to the ports based on the MAC address and password of the client. 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.

Table 151 Switch &gt; Configure &gt; RADIUS policies (continued)

LABEL	DESCRIPTION
Guest VLAN	A guest VLAN is a pre-configured VLAN on the Nebula Device that allows non-authenticated users to access limited network resources through the Nebula Device. Enter the number that identifies the guest VLAN.
Port security	Click <b>On</b> to enable port security on the ports. Otherwise, select <b>Off</b> to disable port security on the ports.
Limited numbers of MAC address	This field is configurable only when you enable port security. Specify the maximum number of MAC addresses that may be learned on a port.
Switch 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.

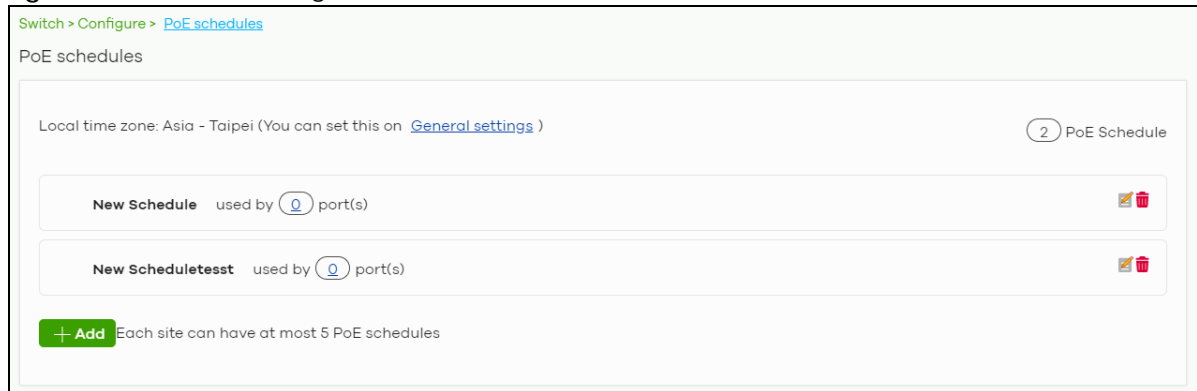
### 10.3.7 PoE Schedules

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 off-line 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 10.3.7.1 on page 360](#).

**Figure 174** Switch > Configure > PoE schedules



#### 10.3.7.1 Create new schedule

Click the **Add** button in the **Switch > Configure > PoE schedule** screen to access this screen.

Figure 175 Switch &gt; Configure &gt; PoE schedule: Add

The following table describes the labels in this screen.

Table 152 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.

### 10.3.8 Switch Settings

Use this screen to configure global Nebula Device settings, such as (R)STP, QoS, port mirroring, voice VLAN and DHCP server guard.

Click **Switch > Configure > Switch settings** to access this screen.

Figure 176 Switch > Configure > Switch settings

Switch > Configure > [Switch settings](#)

Switch settings

---

**VLAN configuration**

Management VLAN:

---

**STP configuration**

Rapid spanning tree protocol (RSTP):

STP bridge priority: [?](#)

Switches	Bridge priority
Stack 1	32768 - default
Default:	32768

[+ Set the bridge priority for another switch](#)

---

**Quality of service**

Quality of service:

VLAN	Priority	Description
<input type="text"/>	1	<input type="text"/>

[+ Add](#)  
[What's this?](#)

---

**Port mirroring**

Port mirroring:

Switch	Destination Port	Source Port
1 Stack 1	<input type="text"/>	<input type="text"/>

[+ Add](#)

---

**Voice VLAN**

Voice VLAN:

Voice VLAN ID:

Priority:

Assign VLAN by:

OUI:

OUI	Description
1 <input type="text"/>	<input type="text"/>

[+ Add OUI on this network](#)

---

**Vendor ID based VLAN**

Vendor ID based VLAN: [Model list](#)

VLAN	Priority	Description
<input type="text"/>	<input type="text"/>	<input type="text"/>

[+ Add Vendor-ID on this network](#)

---

**Access management**

Access management: [Model list](#)

Allow IP range: [?](#)

Start IP address	End IP address
Default	Deny all

[+ Add allow IP range](#)

---

**Management VLAN control**

Switch name	Model	Control ports
1 Stack 1	NSW100-10	All
Default:		All

---

**DHCP Server Guard**

DHCP Server Guard:

The following table describes the labels in this screen.

Table 153 Switch &gt; Configure &gt; Switch settings

LABEL	DESCRIPTION
VLAN configuration	
Management VLAN	Enter the VLAN identification number associated with the Nebula Device IP address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the Nebula Device make sure the port that you are connected to is a member of Management VLAN.
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 the button 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.</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>
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 onto 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.
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 device must support LLDP-MED and have LLDP-MED enabled.</p>
OUI	<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>

Table 153 Switch &gt; Configure &gt; Switch settings (continued)

LABEL	DESCRIPTION
DSCP	Enter the Differentiated Services Code Point (DSCP) value for traffic on the voice VLAN. The value is defined from 0 through 63, and 0 is the default.
Vendor ID based VLAN	
Vendor ID based VLAN	<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 button to define the vendor MAC address OUI, assign to which VLAN, and set the priority.</p>
Access management	
Access management	Select <b>On</b> to enable the access management feature on the Nebula Device. Otherwise, select <b>Off</b> .
Allow IP range	Click the button to set the devices' starting and ending IP addresses that will be allowed to access the Nebula Devices through telnet, SSH, HTTP, HTTPS, and FTP.
Management VLAN control	<p>This allows the administrator to set the Nebula Device ports through which device management VLAN traffic is allowed. For example, 1, 10-15, or ALL.</p> <p>By default, Nebula allows the device management VLAN traffic through all ports (even if <b>Allowed VLAN</b> in the <b>Switch &gt; Configure &gt; Switch port settings</b> is restricted). This avoids the device disconnecting from NCC during configuration.</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>



# CHAPTER 11

## Access Point

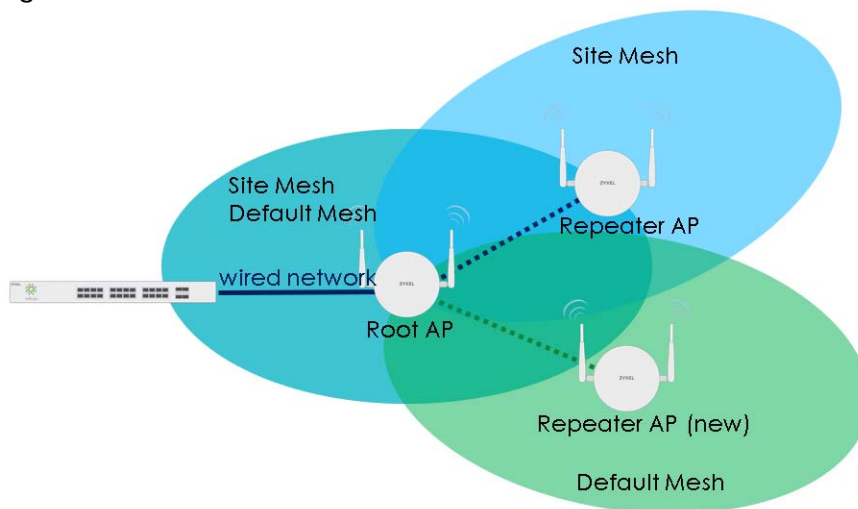
### 11.1 Overview

This chapter discusses the menus that you can use to monitor the Nebula-managed APs in your network and configure settings even before an AP is deployed and added to the site.

#### 11.1.1 Nebula Smart Mesh

Nebula Smart Mesh, also called Smart Mesh or AP Smart Mesh, is a WiFi mesh solution for Nebula APs. With Smart Mesh, you can have two or more Nebula APs automatically create a mesh network within your home or office, ensuring there are no areas with a weak wireless signal.

**Figure 177** Nebula Smart Mesh



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

- **Root AP:** An AP that is connected to the network by Ethernet and can reach the gateway device.
- **Repeater AP:** An AP that is connected to the network wirelessly, or that is connected to the network by Ethernet but cannot reach the gateway device.

The Repeater APs rebroadcast the root AP's SSID, and then relay wireless traffic back to the gateway.

To create a Smart Mesh network, add two or more APs to the same Nebula-managed site and ensure that each AP has Smart Mesh enabled. Then connect one or more Nebula APs to your network's gateway using an Ethernet cable, so that you have at least one root AP. Finally, place one or more non-wired Nebula APs in areas where you want to extend wireless coverage.

## 11.1.2 Smart Mesh Network Topology

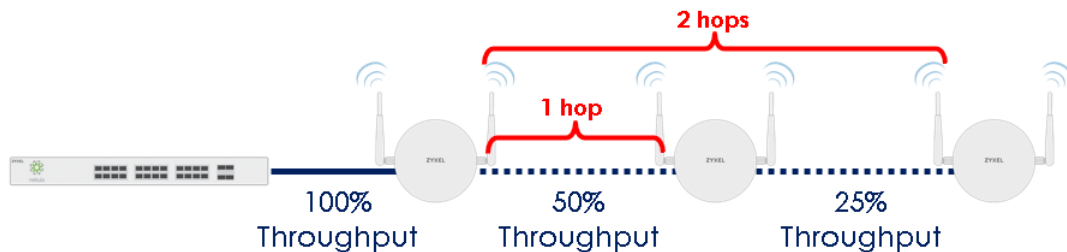
After you add a Nebula AP to an NCC site and then turn it on, the new AP automatically connects to a mesh network called the **default mesh**. The AP then tries to connect to a root AP and contact NCC. After the AP successfully contacts NCC and joins the site, the AP stops using the default mesh and instead connects to other APs in the site using a dedicated network called the **site mesh**.

### 11.1.2.1 Smart Mesh Wireless Hops

Each repeater AP tries to connect to the site gateway through a root AP. If a repeater AP cannot connect directly to a root AP, then the repeater AP relays its wireless traffic through another repeater AP. Each time traffic passes through a wireless 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 178** Nebula Smart Mesh Wireless Hops

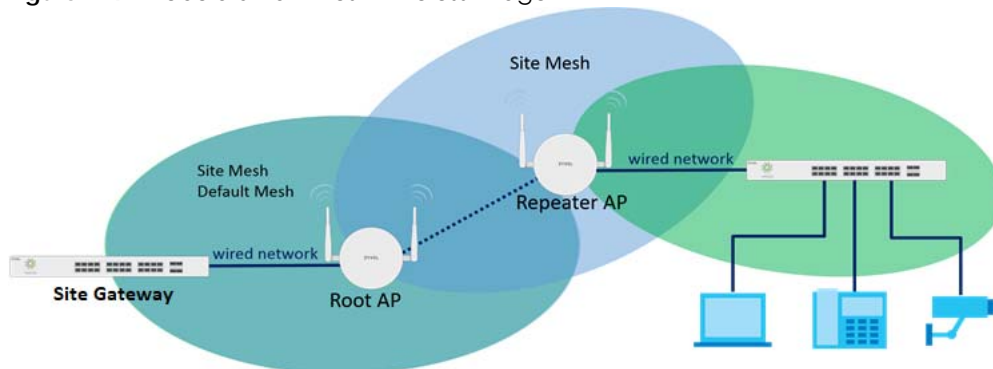


### 11.1.2.2 Wireless Bridge

Wireless bridge is a Smart Mesh feature that allows two Nebula APs to automatically connect 2 network segments together over a wireless 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 APs in NCC. Then connect wired clients to one of the AP's LAN port. These wired clients form a new network segment and are able to reach the site gateway through the AP's wireless connection.

**Figure 179** Nebula Smart Mesh Wireless Bridge



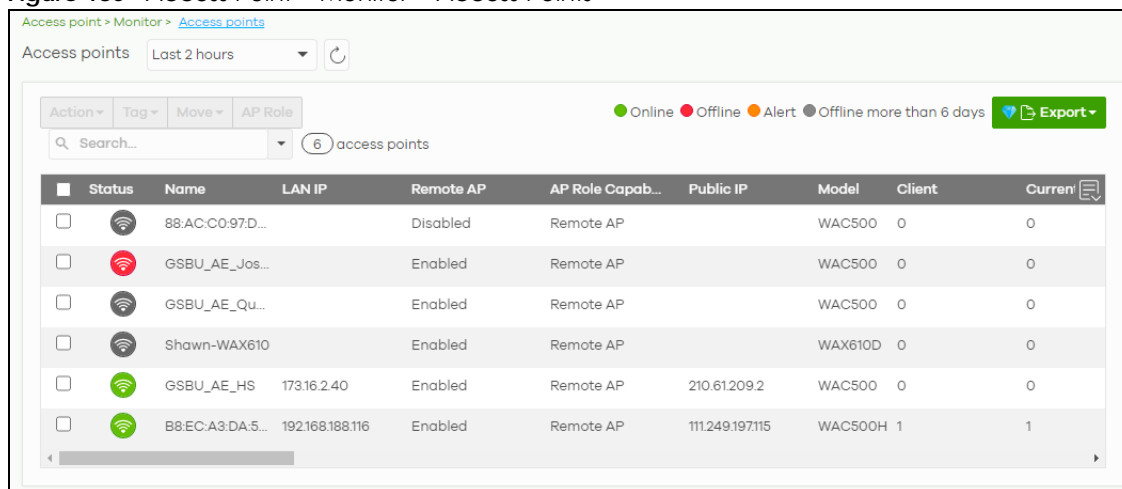
## 11.2 Monitor

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

### 11.2.1 Access Points

This screen allows you to view the detailed information about an AP in the selected site. Click **Access Point > Monitor > Access Points** to access this screen.

**Figure 180** Access Point > Monitor > Access Points



The following table describes the labels in this screen.

**Table 154** 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 APs.
Reboot	Select this to restart the AP.
Upgrade	Select this to upgrade the firmware on the AP.
Tag	Select one or multiple APs and click this button to create a new tag for the APs 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 APs.</li> <li>LED_On: this tag allows you to have the LEDs stay lit after the selected APs are ready.</li> </ul>
Move	Select one or multiple APs and click this button to move the APs to another site or remove the APs from the current site.

Table 154 Access Point &gt; Monitor &gt; Access Points (continued)



LABEL	DESCRIPTION
AP Role	<p>Select one or multiple APs and click this button to enable or disable the <b>Remote AP</b> feature.</p> <p>Remote AP enables the site's Security Gateway to connect to the Access Point (AP) through a secure VPN tunnel. This allows you to set up VPN-enabled WiFi APs in remote locations, such as in a branch office or at home. Clients connected to these APs can securely access your network through the VPN tunnel.</p> <p>Note: Enabling Remote AP automatically enables Ethernet and wireless storm control on the AP.</p>
Search	Specify your desired filter criteria to filter the list of APs.
access points	This shows the number of APs connected to the site network.
Export	Click this button to save the AP list as a CSV or XML file to your computer.
Status	<p>This shows the status of the AP.</p> <ul style="list-style-type: none"> <li>• Green: The AP is online and has no alerts.</li> <li>• Amber: The AP has alerts.</li> <li>• Red: The AP is offline.</li> <li>• Gray: The AP has been offline for 7 days or more.</li> <li>• : The AP is acting as a repeater.</li> </ul> <p>For example, an alert is created and the status color is amber when the AP is transmitting data at 100 Mbps in full duplex mode or when the AP is in a <b>Limited Power mode</b>.</p>
Name	This shows the descriptive name of the AP.
LAN IP	This shows the local (LAN) IP address of the AP.
Remote AP	This shows whether the Remote AP function is <b>Enabled</b> or <b>Disabled</b> .
AP Role Capability	This displays whether the AP can act as a remote AP ( <b>Remote AP</b> ) or not ( <b>Standard AP</b> ).
Public IP	This shows the global (WAN) IP address of the AP.
Model	This shows the model number of the AP.
Client	This shows how many clients connected to the AP within the specified time period.
Current Client	This shows how many clients are currently connecting to the AP.
MAC Address	This shows the MAC address of the AP.
Channel	This shows the channel ID the AP is using.
Channel Utilization	This shows the percentage of the channel ID usage.
Usage	This shows the amount of data consumed by the AP's clients.
% Usage	This shows the percentage of the AP's data usage.
Description	This shows the user-specified description for the AP.
Tag	This shows the user-specified tag for the AP.
Serial Number	This shows the serial number of the AP.
Configuration Status	This shows whether the configuration on the AP is up-to-date.
Connectivity	<p>This shows the AP 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 AP is connected or disconnected.</p>
Ethernet 1	This shows the speed and duplex mode of the Ethernet connection on the AP's up-link port. It shows <b>Down</b> if the AP is connected to a root AP wirelessly.
Neighbor Info	This shows the LLDP information received on the up-link port.

Table 154 Access Point &gt; Monitor &gt; Access Points (continued)

LABEL	DESCRIPTION
Production Information	This shows the production information of the AP.
Hop	This shows the hop count of the AP. For example, "1" means the AP is connected to a root AP directly. "2" means there is another repeater AP between this AP and the root AP.
Uplink AP	This shows the role and descriptive name of the AP to which this AP is connected wirelessly.
Uplink Signal	Before the slash, this shows the signal strength the uplink AP (a root AP or a repeater) receives from this AP (in repeater mode). After the slash, this shows the signal strength this AP (in repeater mode) receives from the uplink AP.
Uplink Tx/Rx Rate	This is the maximum transmission/reception rate of the root AP or repeater to which the AP is connected.
Wireless bridge	This shows whether wireless bridge is enabled on the AP.  For more information about wireless bridge, see <a href="#">Section 11.1.2.2 on page 366</a> .
Uplink	This shows whether the AP is connected to the gateway through a wired Ethernet connection or wireless connection.
Power mode	This shows the AP's power status.  <b>Full</b> – the AP 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.  <b>Limited</b> – the AP receives power through a PoE switch/injector using IEEE 802.3af PoE even when it is also connected to a power source using a power adapter. The PoE device that supports IEEE 802.3af PoE can supply power of up to 15.4W per Ethernet port.  When the AP's power mode is <b>Limited</b> , the AP throughput decreases and has just one transmitting radio chain.  It always shows <b>Full</b> if the AP does not support power detection.
Firmware status	This shows whether the firmware installed on the AP is up-to-date.
Current version	This shows the firmware version currently installed on the AP.
Remote AP VPN	This shows which VPN the Remote AP tunnel is configured to use.  If Remote AP is disabled, this field shows <b>Disconnected</b> .
	Click this icon to display a greater or lesser number of configuration fields.

### 11.2.1.1 AP Details

Click an AP entry in the **Access Point > Monitor > Access Points** screen to display individual AP statistics.

Figure 181 Access Point > Monitor > Access Points: AP Details Part 1

Access point > Monitor > [Access point](#) > 4F-Ice

Access point / 4F-Ice

### Configuration

Name:	4F-Ice
MAC address:	04:BF:6D:16:16:3C
Serial number:	S152L48240389 (WAC6103D-I)
Description:	
Address:	新竹市香山區大庄路64巷21號
Tag:	
Load balancing:	

### Status

LAN IP:	192.168.10.204
Gateway:	192.168.10.254   DNS: 192.168.10.254
Public IP:	220.132.37148
Usage:	29.31 MB used in the last 24 hours.
Current clients:	No client.
Topology:	<a href="#">Show</a>
Neighbor info:	<a href="#">2F-SWT(GS1350-18HP)/9/Uplink</a>
Link:	Uplink: 1000M/Full LAN 1: Down
Ports:	LAN 1 PVID: 1 Allowed VLANs: 1
Channel (Band):	6 (DCS) [2.4GHz] 157*/161 (DCS) [5GHz]
Channel utilization:	4% [2.4GHz] 1% [5GHz]
Power mode:	Full
Antenna:	Ceiling
Smart mesh:	Disabled
Wireless bridge:	Disabled
History:	<a href="#">Event log</a>
Configuration status:	Up to date
Firmware status:	<a href="#">Custom</a>
Current version:	V6.20(AAXH.0)b8

Map Photo

Floor plan Map Satellite

Ask Question

Google Keyboard shortcuts Map data ©2021 Google 10 m Terms of Use Report a map error

Figure 182 Access Point > Monitor > Access Points: AP Details Part 2



The following table describes the labels in this screen.

Table 155 Access Point > Monitor > Access Points: AP Details

LABEL	DESCRIPTION
	Click this button to reload the data-related frames on this page.
Configuration	Click the edit configuration icon to change the device name, description, tags and address. You can also move the device to another site.
Remote AP	Click this to enable or disable the <b>Remote AP</b> feature.  Remote AP enables the site's Security Gateway to connect to the Access Point (AP) through a secure VPN tunnel. This allows you to set up VPN-enabled WiFi APs in remote locations, such as in a branch office or at home. Clients connected to these APs can securely access your network through the VPN tunnel.  Note: Enabling Remote AP automatically enables Ethernet and wireless storm control on the AP.
Name	This shows the descriptive name of the AP.
MAC Address	This shows the MAC address of the AP.
Serial number	This shows the serial number of the AP.
Description	This shows the user-specified description for the AP.
Address	This shows the user-specified address for the AP.
Tag	This shows the user-specified tag for the AP.

Table 155 Access Point > Monitor > Access Points: AP Details (continued)

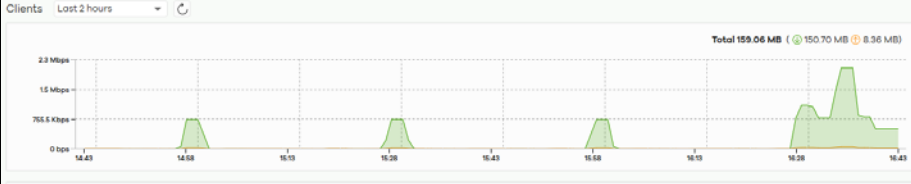
LABEL	DESCRIPTION																																			
Load balancing	This shows the load balancing group name that the AP belongs (up to two groups per AP). APs in the same group should be within the proximity. This allows them to share the load.																																			
Status																																				
LAN IP	<p>This shows the local (LAN) IP address of the AP. 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="537 499 1401 1083" 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 AP.																																			
Usage	This shows the amount of data consumed by the clients.																																			
Current clients	<p>This shows the number of clients which are currently connecting to the AP and its details.</p> <div data-bbox="532 1236 1446 1612" style="border: 1px solid #ccc; padding: 5px;"> <p style="font-size: small;">Access point &gt; Monitor &gt; Clients</p> <p style="font-size: x-small;">Clients Last 2 hours <span style="float: right;">🔄</span></p> <p style="text-align: right; font-size: x-small;">Total 159.06 MB (📶 150.70 MB 📶 8.36 MB)</p>  <p style="font-size: x-small;">Policy (status=online) AND (conn=) 1 selected, 4 matches in 5 clients <span style="float: right;">+ Add client Export</span></p> <table border="1" style="width: 100%; border-collapse: collapse; font-size: x-small;"> <thead> <tr> <th>Policy</th> <th>Status</th> <th>Description</th> <th>Connected to</th> <th>SSID name</th> <th>Security</th> <th>MAC address</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>📶</td> <td>T.Landoo</td> <td>HomeNAP02</td> <td>Youwontbeabiet...</td> <td>WPA2-Personal</td> <td>08:00:27:00:00:10</td> </tr> <tr> <td><input type="checkbox"/></td> <td>📶</td> <td>Vaccum</td> <td>HomeNAP02</td> <td>Youwontbeabiet...</td> <td>WPA2-Personal</td> <td>8C:8E:28:28:28:28</td> </tr> <tr> <td><input type="checkbox"/></td> <td>📶</td> <td>Xiaomi Lamp</td> <td>HomeNAP02</td> <td>Youwontbeabiet...</td> <td>WPA2-Personal</td> <td>9C:8E:28:28:28:28</td> </tr> <tr> <td><input type="checkbox"/></td> <td>📶</td> <td>NS</td> <td>HomeNAP02</td> <td>Youwontbeabiet...</td> <td>WPA2-Personal</td> <td>9C:8E:28:28:28:28</td> </tr> </tbody> </table> </div>	Policy	Status	Description	Connected to	SSID name	Security	MAC address	<input checked="" type="checkbox"/>	📶	T.Landoo	HomeNAP02	Youwontbeabiet...	WPA2-Personal	08:00:27:00:00:10	<input type="checkbox"/>	📶	Vaccum	HomeNAP02	Youwontbeabiet...	WPA2-Personal	8C:8E:28:28:28:28	<input type="checkbox"/>	📶	Xiaomi Lamp	HomeNAP02	Youwontbeabiet...	WPA2-Personal	9C:8E:28:28:28:28	<input type="checkbox"/>	📶	NS	HomeNAP02	Youwontbeabiet...	WPA2-Personal	9C:8E:28:28:28:28
Policy	Status	Description	Connected to	SSID name	Security	MAC address																														
<input checked="" type="checkbox"/>	📶	T.Landoo	HomeNAP02	Youwontbeabiet...	WPA2-Personal	08:00:27:00:00:10																														
<input type="checkbox"/>	📶	Vaccum	HomeNAP02	Youwontbeabiet...	WPA2-Personal	8C:8E:28:28:28:28																														
<input type="checkbox"/>	📶	Xiaomi Lamp	HomeNAP02	Youwontbeabiet...	WPA2-Personal	9C:8E:28:28:28:28																														
<input type="checkbox"/>	📶	NS	HomeNAP02	Youwontbeabiet...	WPA2-Personal	9C:8E:28:28:28:28																														
Topology	Click <b>Show</b> to go to the <b>Site-Wide &gt; Monitor &gt; Topology</b> screen. See <a href="#">Section 7.1.5 on page 160</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 AP's ports.</p> <p>It shows <b>Uplink: Wireless</b> if the AP is a repeater and connected to a root AP wirelessly.</p> <p>A warning icon displays when the AP is running at 100 Mbps or a lower speed.</p>																																			



Table 155 Access Point &gt; Monitor &gt; Access Points: AP Details (continued)

LABEL	DESCRIPTION
Ports	<p>This is available only for the Nebula AP 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 11.3.6 on page 406</a> for how to change the port's VLAN settings.</p>
Storm control	<p>Storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets received per second on the AP'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.</p>
Channel (Band)	<p>This shows the channel ID and WiFi frequency band currently being used by the AP.</p>
Channel utilization	<p>This shows the percentage of the channel ID usage.</p>
Power mode	<p>This shows <b>Full</b> when the AP receives power directly through a power outlet.</p> <p>This shows <b>Full (Power by DC)</b> when the AP receives power using a power adapter.</p> <p>This shows <b>Full (Power by PoE)</b> when the AP 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 AP 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 AP 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 AP's firmware is older than version 5.50 or (WAX650S or WAX510D firmware is older than version 6.00P4C0). Or when the AP is offline.</p> <p>Click the edit icon to open a screen where you can enable full power mode.</p> <div data-bbox="537 1192 1360 1457" 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	<p>This displays the antenna orientation settings for the AP that comes with internal antennas and also has an antenna switch.</p>
Smart mesh	<p>This shows whether Nebula Smart Mesh is enabled on the AP.</p> <p>For more information about Smart Mesh, see <a href="#">Section 11.1.1 on page 365</a>.</p>
Edit	<p>Edit the AP's Smart Mesh settings.</p>

Table 155 Access Point &gt; Monitor &gt; Access Points: AP Details (continued)


LABEL	DESCRIPTION
Enabled	Enable or disable Smart Mesh on the AP. This setting overrides the Smart Mesh settings configured for the AP's site in NCC.
Lock	When enabled, the AP's local Smart Mesh settings overrides the Smart Mesh settings configured for the AP's site in NCC.  Example 1: If Smart Mesh is enabled for the site in NCC, you can disable Smart Mesh on the AP by setting Lock to on and Enabled to off.  Example 2: If Smart Mesh is disabled for the site in NCC, you can enable Smart Mesh on the AP by setting Lock to on and Enabled to on.
Wireless bridge	This shows whether wireless bridge is enabled on the AP. For more information about wireless bridge, see <a href="#">Section 11.1.2.2 on page 366</a> .
Edit	Edit the AP's wireless bridge settings.
Enabled	Enable or disable wireless bridge on the AP.  Note: If Smart Mesh is disabled for the site in NCC, then enabling wireless bridge automatically enables Smart Mesh on the AP.
Allowed VLANs	Enter the IDs of the VLANs that the AP will forward over the wireless bridge.  By default, this field uses the VLANs allowed for LAN1 at <b>AP &gt; Configure &gt; AP &amp; Port Settings</b> . For details, see <a href="#">Section 11.3.6 on page 406</a> .
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 AP is up-to-date.
Firmware status	This shows whether the firmware on the AP is up-to-date or there is firmware update available for the AP.
Current version	This shows the firmware version currently installed on the device.
Map	This shows the location of the AP on Google map.
Photo	This shows the photo of the AP. Click <b>Add</b> to upload one or more photos. Click <b>x</b> to remove a photo.
Live tools	
Traffic	This shows the AP traffic statistics.
Current stations	This shows the AP's connected wireless clients' <b>MAC address, SSID name, IPv4 Address, Signal strength, Security, Channel, Tx rate, Rx rate, Association time, and Capability</b> .
Ping	Enter the domain name or IP address of a computer that you want to perform ping from the AP in order to test a connection and click <b>Ping</b> .  This can be used to determine if the AP 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 AP 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 AP.
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 AP between several devices in the network.
Remote Access	This allows you to establish a remote connection to this AP 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.

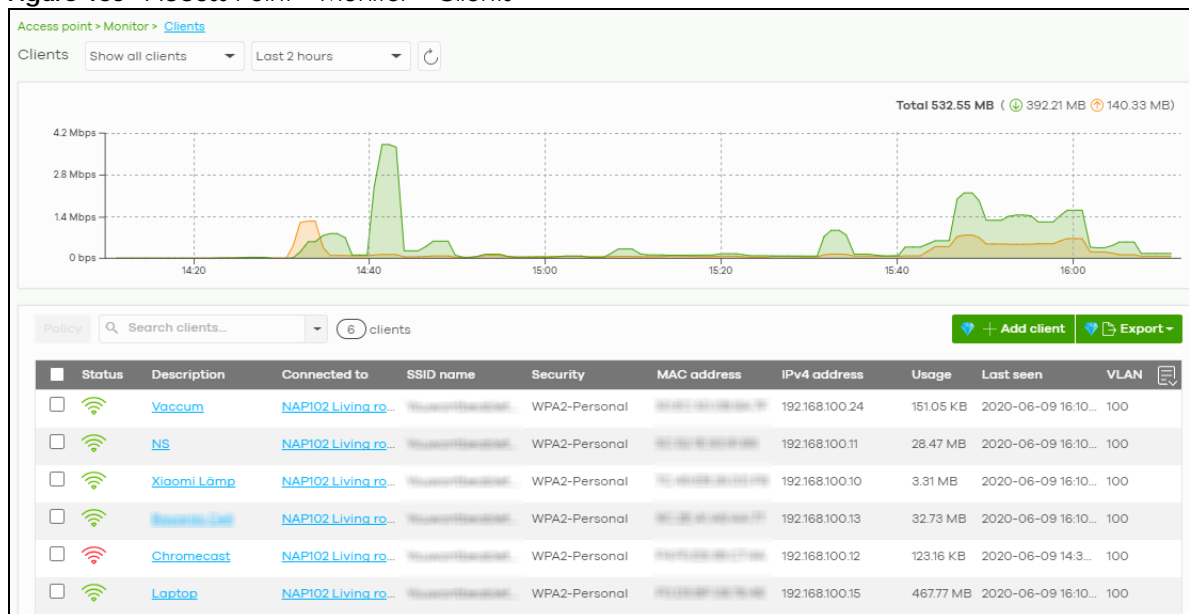
Table 155 Access Point &gt; Monitor &gt; Access Points: AP Details (continued)

LABEL	DESCRIPTION
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.

## 11.2.2 Clients

This screen allows you to view the connection status and detailed information about clients connected to an AP in the selected site. Click **Access Point > Monitor > Clients** to access this screen.

Figure 183 Access Point &gt; Monitor &gt; Clients



The following table describes the labels in this screen.

Table 156 Access Point &gt; Monitor &gt; Clients

LABEL	DESCRIPTION
Clients	Select to view the 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 156 Access Point &gt; Monitor &gt; Clients (continued)

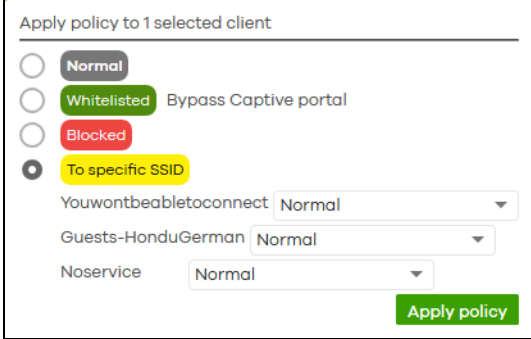

LABEL	DESCRIPTION
Policy	<p>Select the clients from the table below, and then choose the security policy that you want to apply to the selected clients. Choose <b>Normal</b> to apply the captive portal authentication to the selected clients. To allow the selected clients to bypass captive portal authentication, 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_SSIDs. 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 AP 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 AP'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 wireless.
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 11.2.2.1 on page 377</a>.</p>
Connected to	<p>This shows the name of the Nebula managed AP to which the client is connected.</p> <p>Click the name to display the individual AP statistics. See <a href="#">Section 11.2.1.1 on page 369</a>.</p>
SSID Name	This shows the name of the AP's wireless 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 wireless 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 was last connected.
Upload	This shows the amount of data transmitted from the client since it was last connected.

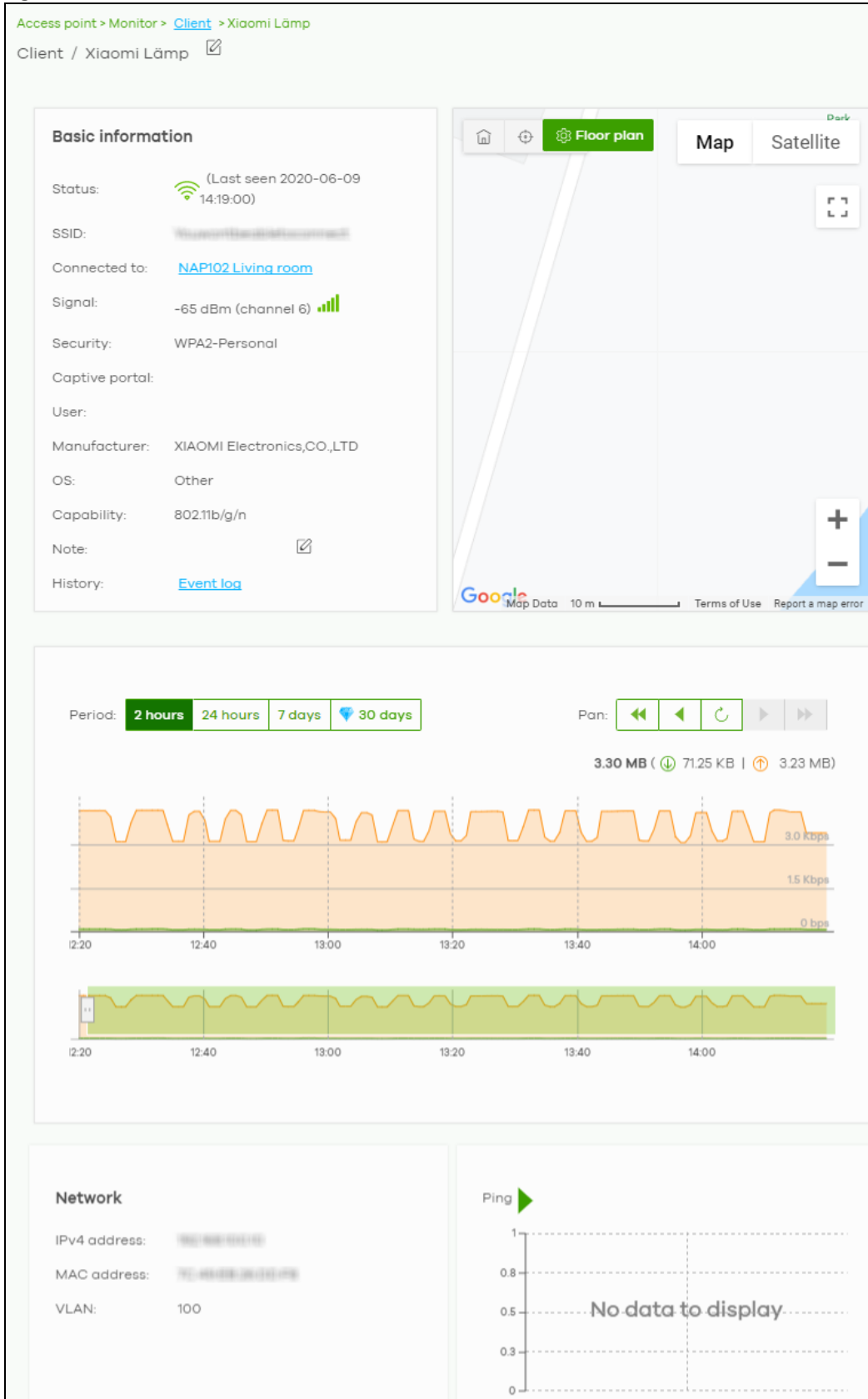
Table 156 Access Point &gt; Monitor &gt; Clients (continued)

LABEL	DESCRIPTION
Usage	This shows the amount of data consumed by the AP (upload + download) since it was 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.

### 11.2.2.1 Client Details

Click a client entry in the **Access Point > Monitor > Clients** screen to display individual client statistics.

Figure 184 Access Point > Monitor > Clients: Client Details



The following table describes the labels in this screen.

Table 157 Access Point > Monitor > Clients: Client Details

LABEL	DESCRIPTION
Status	This shows whether the client is online (green), or goes off-line (red). It also shows the last date and time the client was discovered.
SSID	This shows the name of the AP's wireless network to which the client is connected.
Connected to	This shows the name of the Nebula managed AP to which the client is connected. Click the name to display the individual AP statistics. See <a href="#">Section 11.2.1.1 on page 369</a> .
Signal	This shows the RSSI (Received Signal Strength Indicator) of the client's wireless 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 <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> </ul> Red/2 blocks: signal is less than $-80$ dBm, weak signal
Security	This shows the encryption method used to connect to the AP.
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 AP.
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 AP'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.

## 11.2.3 Event Log

Use this screen to view wireless AP log messages. You can enter the AP 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 185** Access Point > Monitor > Event log

Access point > Monitor > [Event log](#)

Event log

Access Point:  Keyword:  Category:

Before  17:12  UTC+8

135 Event log

Time	Access point	Category	Detail
2019-10-30 16:14:23	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has associated on Channel: 6, SS...
2019-10-30 16:14:27	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by Hostapd3 on Ch...
2019-10-30 16:14:27	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by prev-Auth Failed ...
2019-10-30 16:14:27	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	WPA authenticator requests disconnect: reason 1. Interf...
2019-10-30 16:14:27	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	WPA authenticator requests disconnect: reason 2. Interf...
2019-10-30 16:19:26	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has associated on Channel: 6, SS...
2019-10-30 16:19:30	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by Hostapd3 on Ch...
2019-10-30 16:19:30	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by prev-Auth Failed ...
2019-10-30 16:19:30	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	WPA authenticator requests disconnect: reason 1. Interf...
2019-10-30 16:19:30	<a href="#">9c:5c:f9:61:f6:c1</a>	Wireless LAN	WPA authenticator requests disconnect: reason 2. Interf...

Page 1 of 14 Results per page: 10

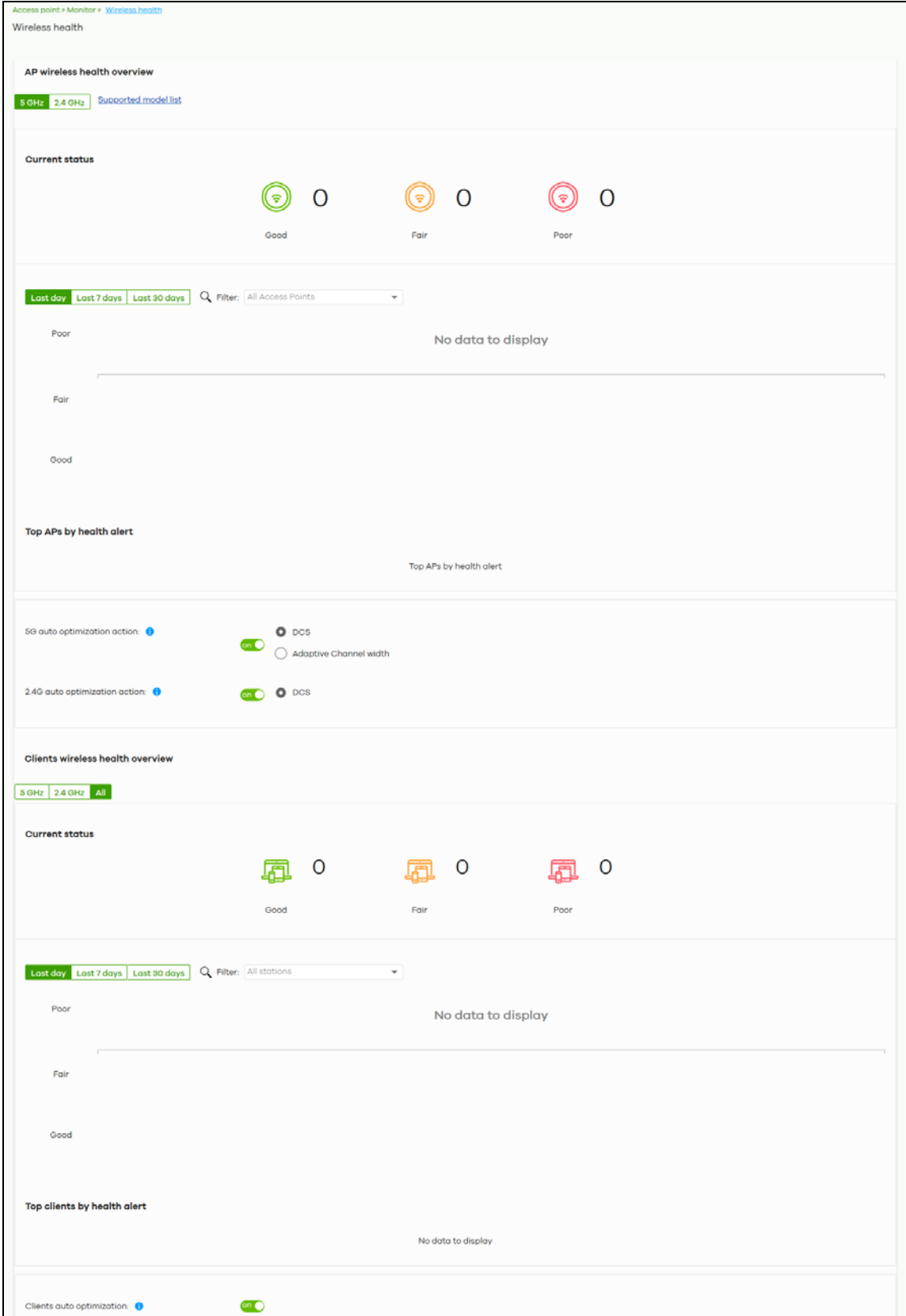
## 11.2.4 Wireless Health

This screen lets you know health of wireless networks for your APs and connected wireless clients. You can take actions by enabling DCS, changing channel bandwidth and/or client steering to reduce interference and improve wireless network performance.

Click **Access Point > Monitor > Wireless Health** to access this screen.



Figure 186 Access Point > Monitor > Wireless Health



The following table describes the labels in this screen.

Table 158 Access Point > Monitor > Wireless Health

LABEL	DESCRIPTION
AP wireless health overview	
Move the cursor over the information icon to view the supported AP model list.	
Good/Fair/Poor	This shows the number of supported APs that are currently online, using the specified frequency band and in good, fair or poor wireless health.
AP radio health	Select to view the health of all supported AP wireless networks using the 5 GHz or 2.4 GHz band.  You can select to view the health report for the past day, week or month, as well as filter the AP to view.
y-axis	The y-axis represents the state of wireless health.
x-axis	The x-axis shows the time period over which the AP health state is recorded.
Top APs by health alert	
Name	This shows the descriptive name of the AP.
Model	This shows the model number of the AP.
Alert	This shows how many times the AP is in a poor state of wireless health.  The NCC generates a log when the AP is in poor wireless health. You can view the log messages in the <b>Access Point &gt; Monitor &gt; Event Log</b> screen.
5G auto optimization action	Select <b>ON</b> to enable and specify how the AP improves the wireless network performance. Otherwise, select <b>OFF</b> to disable it.  <ul style="list-style-type: none"> <li><b>Adaptive channel width</b> – select this option to have the AP change the channel bandwidth from 80 MHz to 20 MHz to reduce the radio interference with other APs.</li> </ul> <p>Note: In AP firmware version 6.10 and later, if adaptive channel width does not improve wireless performance then the AP also performs Dynamic Channel Selection (DCS).</p> <ul style="list-style-type: none"> <li><b>DCS (Dynamic Channel Selection)</b> – select this option to have the AP scan and choose a radio channel that has least interference.</li> </ul>
2.4G auto optimization action	Select <b>ON</b> to enable and specify how the AP improves the wireless network performance. Otherwise, select <b>OFF</b> to disable it.  <ul style="list-style-type: none"> <li><b>DCS (Dynamic Channel Selection)</b> – select this option to have the AP scan and choose a radio channel that has least interference.</li> </ul>
Client wireless health overview	
Good/Fair/Poor	This shows the number of connected wireless clients that are currently online, using the specified frequency band and in good, fair or poor wireless health.
Client health	Select to view the health of all wireless clients which are connected to the supported APs using the 5 GHz or 2.4 GHz band.  You can select to view the health report for the past day, week or month, as well as filter the wireless station to view.
y-axis	The y-axis represents the state of wireless health.
x-axis	The x-axis shows the time period over which the client health state is recorded.
Top clients by health alert	
Description	This shows the descriptive name of the client.

Table 158 Access Point &gt; Monitor &gt; Wireless Health (continued)

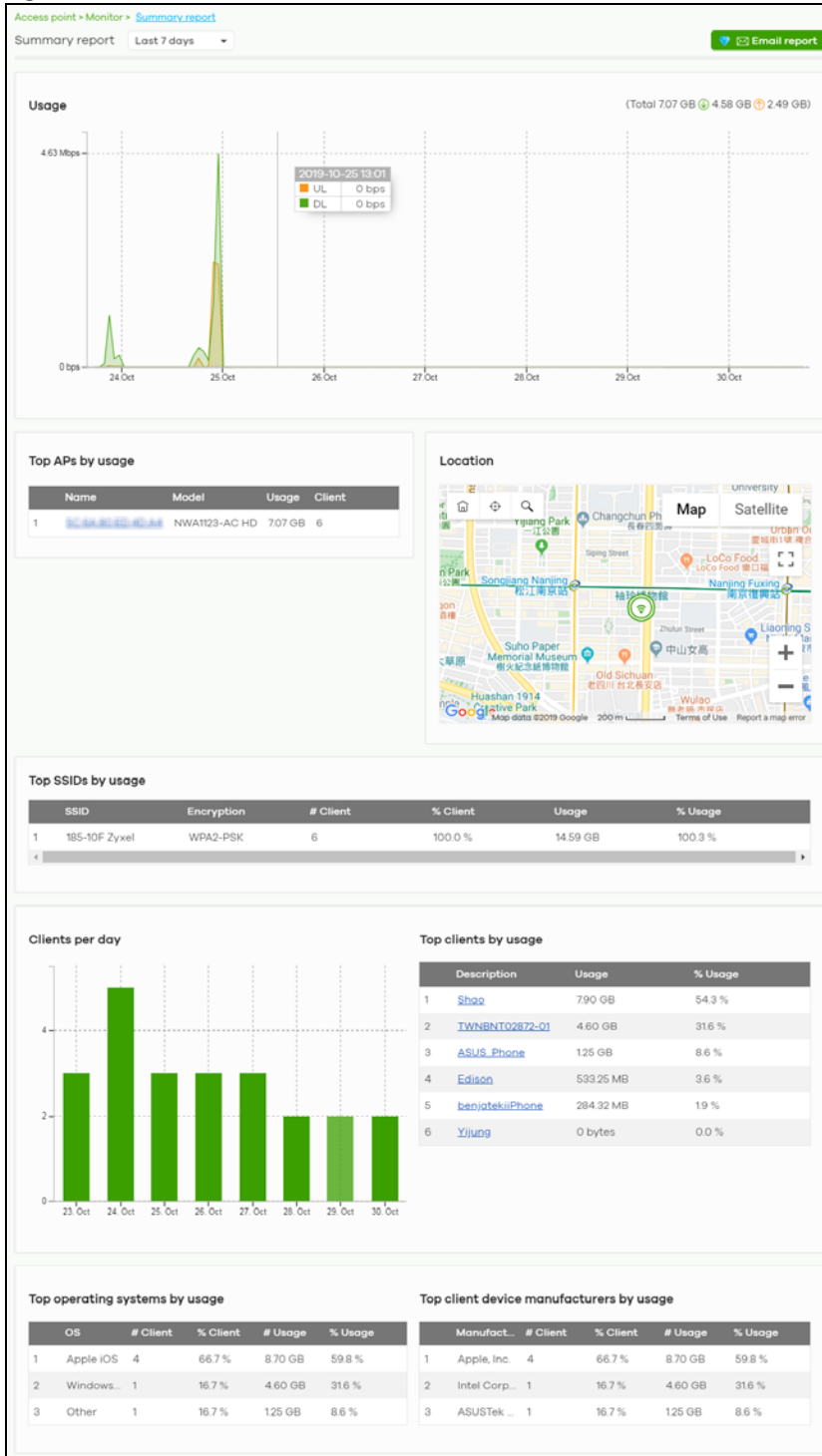
LABEL	DESCRIPTION
Alert	This shows how many times the client is in a poor state of wireless health. The NCC generates a log when the client is in poor wireless health. You can view the log messages in the <b>Access Point &gt; Monitor &gt; Event Log</b> screen.
Clients auto optimization	Select <b>ON</b> to have the AP try to steer the wireless clients in poor health to an AP or SSID with a strong signal every 30 minutes. Otherwise, select <b>OFF</b> to disable steering.

## 11.2.5 Summary Report

This screen displays network statistics for APs 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 187 Access Point > Monitor > Summary Report



The following table describes the labels in this screen.

Table 159 Access Point &gt; Monitor &gt; Summary Report

LABEL	DESCRIPTION
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: 5px; margin-top: 10px;"> <input checked="" type="radio"/> Last 24 hours  <input type="radio"/> Last 7 days  <input type="radio"/> Last 30 days  <input type="radio"/> Custom range ...            Report size: <input type="text" value="10"/> results per table <input type="button" value="Update"/> </div>
Email report	Click this button to send summary reports by email, change the report logo and set email schedules.
Usage	
y-axis	The y-axis shows the transmission speed of data sent on this port in megabits per second (Mbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Top APs by usage	
#	This shows the ranking of the Nebula AP.
Name	This shows the descriptive name of the Nebula AP.
Model	This shows the model number of the Nebula AP.
Usage	This shows the amount of data transmitted or received by the Nebula AP.
Client	This shows how many clients are currently connecting to the Nebula AP.
Location	
This shows the location of the Nebula APs 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.
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.

Table 159 Access Point &gt; Monitor &gt; Summary Report (continued)

LABEL	DESCRIPTION
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.

## 11.3 Configure

Use the **Configure** menus to set the wireless and WiFi security settings for APs of the selected site.

### 11.3.1 SSID Overview

This screen allows you to configure up to eight different SSID profiles for your APs. An SSID, or Service Set Identifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the wireless network name when a person makes a connection to it.

Click **Access Point > Configure > SSID overview** to access this screen.

Figure 188 Access Point &gt; Configure &gt; SSID overview

No.	1	2	3
Name	RAP_Field_Trial_Stress	!!!@Field_Trial_RAP	RAP_Field_Trial_Home
Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Programmable SSID Beta	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Name:	<input type="text"/>	<input type="text"/>	<input type="text"/>
PSK:	<input type="text"/> (optional)	<input type="text"/> (optional)	<input type="text"/>
Tagging	<input type="text"/> Tag Enable SSID on APs with any of the specified tags	<input type="text"/> Tag Enable SSID on APs with any of the specified tags	<input type="text"/> Tag Enable SSID on APs with any of the specified tags
Guest Network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication	Open	Open	WPA2 Pre-shared key
WLAN security	Open	Open	WPA2 Pre-shared key
Sign-in method	Disable	Disable	Disable
Band	5GHz band only	Concurrent operation(2.4GHz and 5GHz)	Concurrent operation(2.4GHz and 5GHz)
VLAN ID	1	1	1
Rate limiting	Unlimited Kb/s	Unlimited Kb/s	Unlimited Kb/s
Captive Portal	Modern	Modern	Modern
Theme	Modern	Modern	Modern

The following table describes the labels in this screen.

Table 160 Access Point &gt; Configure &gt; SSID overview

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 wireless settings to default.
Show All/Hide disabled SSIDs	Select to display all SSID profiles or the active SSID profiles only.
No.	This shows the index number of this profile.
Name	This shows the SSID name for this profile. Click the text box and enter a new SSID if you want to change it.
Enabled	Click to turn on or off this profile.
Programmable SSID	Select On to have each AP that uses this SSID generate a unique SSID name and pre-shared key (PSK) based on the AP's model name, serial number, or MAC address. For example, a hotel can install an AP in each room and then have each AP broadcast a unique SSID based on the room number: FreeWiFi_Room1, FreeWiFi_Room2, FreeWiFi_Room3, and so on.

Table 160 Access Point &gt; Configure &gt; SSID overview (continued)

LABEL	DESCRIPTION
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 an AP value to use to generate the SSID name. Use one of the following: \$AP = AP device name. \$MAC = AP MAC address. \$SN = AP serial number.</li> <li>• X: Specify how many characters of the AP 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 AP 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 AP will generate a random PSK. \$GENMIX = The AP generates a mix of random letters and numbers. \$GENNUM = The AP generates a mix of random numbers only. Y = Specify the length of the PSD. The minimum length is 8.</li> </ul> <p>Example: \$GENNUM(10) generates a unique 10-character PSK for this SSID, consisting only of numbers.</p> <p>Note: You can specify a fixed PSK for this SSID at <b>Access point &gt; Configure &gt; SSID settings</b>.</p>
Tagging	<p>Enter or select the tags you created for APs in the <b>Access Point &gt; Monitor &gt; Access Points</b> screen. The SSID profile will only be applied to APs with the specified tag.</p> <p>If you leave this field blank, this SSID profile will be applied to all APs in the site.</p>
Guest Network	<p>Select <b>On</b> to set this wireless network as a guest network. Layer 2 isolation and intra-BSS blocking are automatically enabled on the SSID. Wireless clients connecting to this SSID can access the Internet through the AP but cannot directly connect to the LAN or the wireless 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 AP'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 11.3.2 on page 389</a>.</p> <p>Note: If you have a Nebula security gateway installed in the site but the gateway interface with the same VLAN ID is not configured as a guest interface, <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> <div data-bbox="537 1446 1325 1755" style="border: 1px solid black; padding: 5px;"> <p><b>Smart VLAN</b> <span style="float: right;">✕</span></p> <p>This SSID has Guest network turned ON. To limit the access to internet only, Guest function can also be enabled on the gateway VLAN interface.</p> <p>Note: This setting is not recommended if wired connections or SSIDs using the same VLAN need access to other interfaces.</p> <p>VLAN ID: <input type="text" value="100"/> (1-4094)</p> <p>Guest: <input checked="" type="checkbox"/> (Enable internet access only)</p> <p style="text-align: right;"><input type="button" value="Close"/> <input type="button" value="Continue"/></p> </div>
Authentication	
Edit	<p>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 11.3.2 on page 389</a>.</p>



Table 160 Access Point &gt; Configure &gt; SSID overview (continued)

LABEL	DESCRIPTION
WLAN security	This shows the encryption method used in this profile.
Sign-in method	This shows the authentication method used in this profile.
Band	This shows whether the SSID use either 2.4 GHz band or the 5 GHz band. If it shows <b>Concurrent operation</b> , the SSID uses both frequency bands.
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	
Edit	Click this button to go to the <b>Captive Portal</b> screen and configure the captive portal settings. See <a href="#">Section 11.3.3 on page 396</a> .
Theme	If captive portal is enabled, this shows the name of the captive portal page used in this profile.

## 11.3.2 SSID 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 settings** to access this screen.

Figure 189 Access Point &gt; Configure &gt; SSID settings Part 1

Access point > Configure > [SSID settings](#)

SSID settings

**Network access**

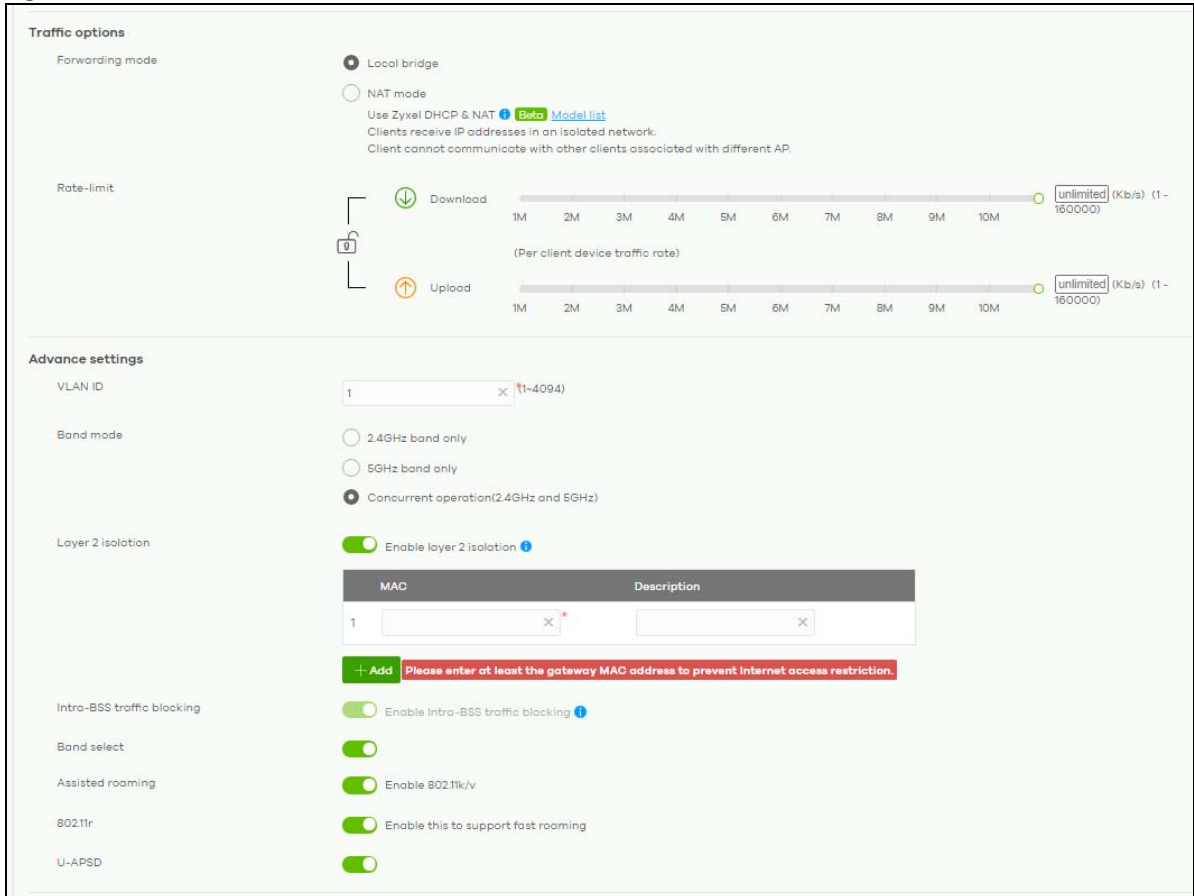
Security options:

- 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:  ⓘ\*
- Dynamic personal psk ⓘ Beta [Model list](#)
- MAC-based Authentication with Nebula cloud authentication ▾  
Use MAC address as a username and password
- WPA Enterprise with WPA2 ▾  
Use 802.1X authentication that requires a unique username and password  
WPA Enterprise with Nebula cloud authentication ▾

Sign-in method:

- Disabled  
Users can access the network without any web authentication
- Click-to-continue  
Users must view and agree the captive portal page then can access the network
- Voucher Beta ⓘ  
Users must enter a voucher code then can access the network  
Create and manage voucher passcode on the [Vouchers](#) page.
- Sign-on with Nebula cloud authentication ▾  
Users must enter a username and password then can access the network

Figure 190 Access Point > Configure > SSID settings Part 2



The following table describes the labels in this screen.

Table 161 Access Point > Configure > SSID settings

LABEL	DESCRIPTION
SSID settings	Select the SSID profile to which the settings you configure here is applied.
Network access	<p>Note: You cannot enable MAC authentication, 802.1X authentication and web authentication at the same time.</p> <p>Note: User accounts can be created and authenticated using the NCC user database. See <a href="#">Section 6.3.5 on page 120</a>.</p>

Table 161 Access Point &gt; Configure &gt; SSID 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 2 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>, APs that do not support it will revert to WPA2.</p> <p>Note: Only the NWA110AX, WAX510D, WAX650S supports WPA3 as of this writing.</p> <ul style="list-style-type: none"> <li>• Turn on <b>802.11r</b> to enable IEEE 802.11r fast roaming on the AP. 802.11r fast roaming reduces the delay when the clients switch from one AP to another by allowing security keys to be stored on all APs in a network. Information from the original association is passed to the new AP when the client roams. The client does not need to perform the whole 802.1x authentication process.</li> </ul> <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 wireless 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 123</a>.</li> <li>• For details on creating organization DPPSK users, see <a href="#">Section 7.2.7 on page 186</a>.</li> </ul> <p>Turn on <b>MAC-based Authentication with</b> to authenticate wireless clients by their MAC addresses. 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 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 AP. 802.11r fast roaming reduces the delay when the clients switch from one AP to another by allowing security keys to be stored on all APs in a network. Information from the original association is passed to the new AP 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 161 Access Point &gt; Configure &gt; SSID settings (continued)

LABEL	DESCRIPTION
Sign-in method	<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>Note: After enabling <b>Click-to-continue</b>, the AP creates a user account with username "clicktocontinue_X_Y", where X is the radio type (1 = 2.4GHz, 2 = 5GHz) and Y is the SSID number (1–8) of the SSID profile. The AP 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 7.1.6 on page 161</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.</li> <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 AP's wireless 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 <a href="#">here</a> to open the Facebook Wi-Fi 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> <div data-bbox="537 1270 1076 1797" style="border: 1px solid black; padding: 5px;"> <p><b>Facebook Wi-Fi Configuration</b> S132L32200016</p> <hr/> <p><b>Facebook Page</b> To use Facebook Wi-Fi you need to be the admin of a local business Page that has a valid location associated with it.</p> <p>Select a Page ▾</p> <p><b>Bypass Mode</b> Your customers always have the option to skip checking in. They can do this by clicking on a link that lets them skip check-in, or by entering a Wi-Fi code that you provide to them.</p> <p><input checked="" type="radio"/> Skip check-in link [?] <input type="radio"/> Require Wi-Fi code [?]</p> <p><b>Session Length</b> Select the length of time your customers will have Wi-Fi for after they check in.</p> <p>Five hours ▾</p> <p><b>Terms of Service</b> <input type="checkbox"/> Optional: Add your own Terms of Service [?]</p> <p>Visit Help Center <span style="float: right;">Save Settings</span></p> </div> <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>

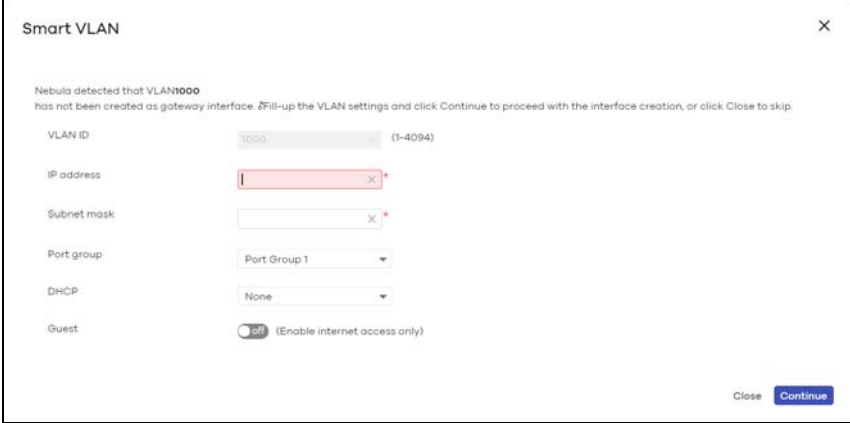
Table 161 Access Point &gt; Configure &gt; SSID settings (continued)

LABEL	DESCRIPTION
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: APs 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 AP 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 settings	
Walled garden	<p>Select <b>On</b> to enable Walled garden.</p>
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>
Login on multiple client devices	<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>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>

Table 161 Access Point &gt; Configure &gt; SSID settings (continued)

LABEL	DESCRIPTION
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	
Forwarding mode	<p>Select <b>NAT mode</b> to have the AP create a DHCP subnet with its own NAT for the SSID. This simplifies wireless network management, as you do not need to configure a separate DHCP server.</p> <p>The following AP 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 AP.</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>
Advance settings	

Table 161 Access Point &gt; Configure &gt; SSID 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 gateway 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> 
Band mode	<p>Select to have the SSID use either <b>2.4 GHz band only</b> or the <b>5 GHz band only</b>.</p> <p>If you select <b>Concurrent operation (2.4 GHz and 5 GHz)</b>, the SSID uses both frequency bands. You can then turn on <b>Band Select</b> to have the dual-band AP steer the wireless clients to the 5 GHz band.</p>
Layer 2 isolation	<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	<p>This field is not configurable if you enable Layer 2 isolation.</p> <p>Select <b>on</b> to prevent crossover traffic from within the same SSID. Select <b>off</b> to allow intra-BSS traffic.</p>
Band select	<p>Select to enable band steering. When enabled, the AP 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 AP.</p> <p>When the connected clients request 802.11k neighbor lists, the AP will response with a list of neighbor APs that can be candidates for roaming. When the 802.11v capable clients are using the 2.4 GHz band, the AP 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 AP.</p> <p>802.11r fast roaming reduces the delay when the clients switch from one AP to another, by allowing security keys to be stored on all APs in a network. Information from the original association is passed to the new AP when the client roams. The client does not need to perform the whole 802.1x authentication process.</p>
U-APSD	<p>Select to turn on or off Automatic Power Save Delivery. This helps increase battery life for battery-powered wireless clients connected to the AP.</p>

### 11.3.3 Captive Portal Customization

Use this screen to configure captive portal settings for SSID profiles. A captive portal can 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 191** Access Point > Configure > Captive portal customization

Access point > Configure > [captive portal customization](#)

Captive portal customization

SSID:    
 Captive portal on this SSID is disabled. You can change this setting [here](#).

**Themes**

   
 **Default** Modern

**Click-to-continue/Voucher/Sign-on page**

Logo:  [Upload a logo](#)

Message:  [×](#)

**Success page**

Message:  [×](#)

**External captive portal URL**

Use URL:  URL:  [×](#)

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

**Captive portal behavior**

After the captive portal page where the user should go?

Stay on Captive portal authenticated successfully page

To promotion URL:  [×](#)



The following table describes the labels in this screen.

Table 162 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 corner 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 11.3.3.1 on page 398</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>
Click-to-continue/Voucher/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	

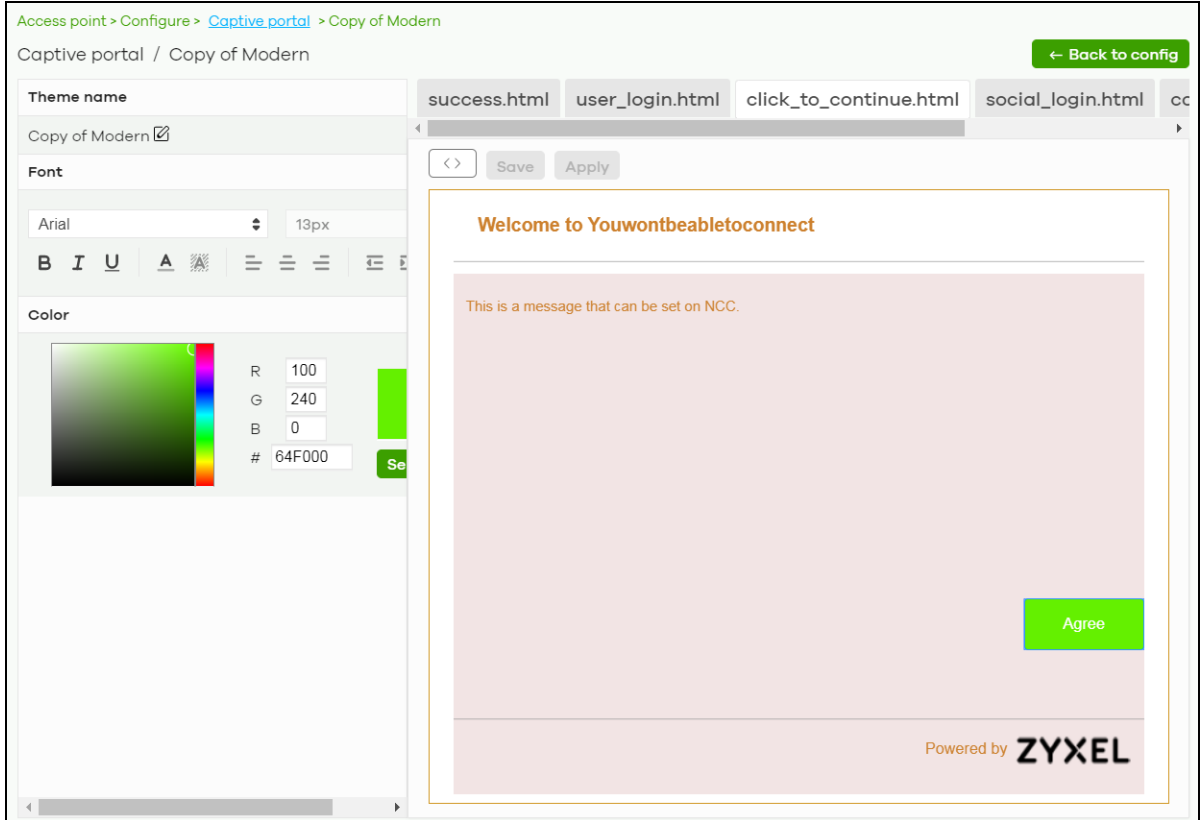
Table 162 Access Point &gt; Configure &gt; Captive portal customization (continued)

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="537 464 1346 1150" style="border: 1px solid black; padding: 5px;"> <p><b>Edit</b> <span style="float: right;">X</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;apuri=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"/> X*</td> </tr> <tr> <td>apmac</td> <td><input type="text" value="apmac"/> X*</td> </tr> <tr> <td>usermac</td> <td><input type="text" value="usermac"/> X*</td> </tr> <tr> <td>apip</td> <td><input type="text" value="apip"/> X*</td> </tr> <tr> <td>userip</td> <td><input type="text" value="userip"/> X*</td> </tr> <tr> <td>ssid_name</td> <td><input type="text" value="ssid_name"/> X*</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"/> X*	apmac	<input type="text" value="apmac"/> X*	usermac	<input type="text" value="usermac"/> X*	apip	<input type="text" value="apip"/> X*	userip	<input type="text" value="userip"/> X*	ssid_name	<input type="text" value="ssid_name"/> X*
Attribute Name	Customized Name														
gw_addr	<input type="text" value="gw_addr"/> X*														
apmac	<input type="text" value="apmac"/> X*														
usermac	<input type="text" value="usermac"/> X*														
apip	<input type="text" value="apip"/> X*														
userip	<input type="text" value="userip"/> X*														
ssid_name	<input type="text" value="ssid_name"/> X*														
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> .														

### 11.3.3.1 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 192 Access Point &gt; Configure &gt; Captive portal: Edit



The following table describes the labels in this screen.

Table 163 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 on 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 163 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 APs in the site.

### 11.3.4 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 193 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](#))

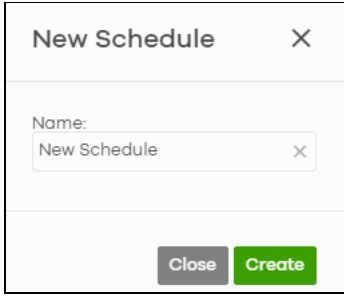
Day	Availability
Sunday	<input checked="" type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Monday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Tuesday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 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 164 Access Point > Configure > SSID availability

LABEL	DESCRIPTION
SSID	Select the SSID profile to which the settings you configure here is applied.
SSID availability	
Visibility	Select <b>Hide this SSID</b> if you want to hide your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway. Otherwise, select <b>Broadcast this SSID</b> .  When an SSID is "hidden" and a wireless client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wireless connection setup screens (these vary by client, client connectivity software, and operating system).
Tagging	Enter the tags you created for APs in the <b>Access Point &gt; Monitor &gt; Access Points</b> screen. The SSID profile will only be applied to APs with the specified tag.  If you leave this field blank, this SSID profile will be applied to all APs in the site.
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	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.  Specify the hour and minute when the schedule begins and ends each day.
Add	Click this button to create a new schedule. A window pops up asking you to enter a descriptive name for the schedule for identification purposes.  
Delete	Click this button to remove a schedule which is not used in any SSID profile.

### 11.3.5 Radio Settings

Use this screen to configure global radio settings for all APs in the site. Click **Access Point > Configure > Radio settings** to access this screen.

Figure 194 Access Point &gt; Configure &gt; Radio settings

The following table describes the labels in this screen.

Table 165 Access Point &gt; Configure &gt; Radio settings

LABEL	DESCRIPTION
Country	Select the country where the AP is located/installed.  The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs in order to prevent roaming failure and interference with other systems.
Maximum output power	Set the maximum target output power of the radio (in dBm).

Table 165 Access Point &gt; Configure &gt; Radio settings (continued)

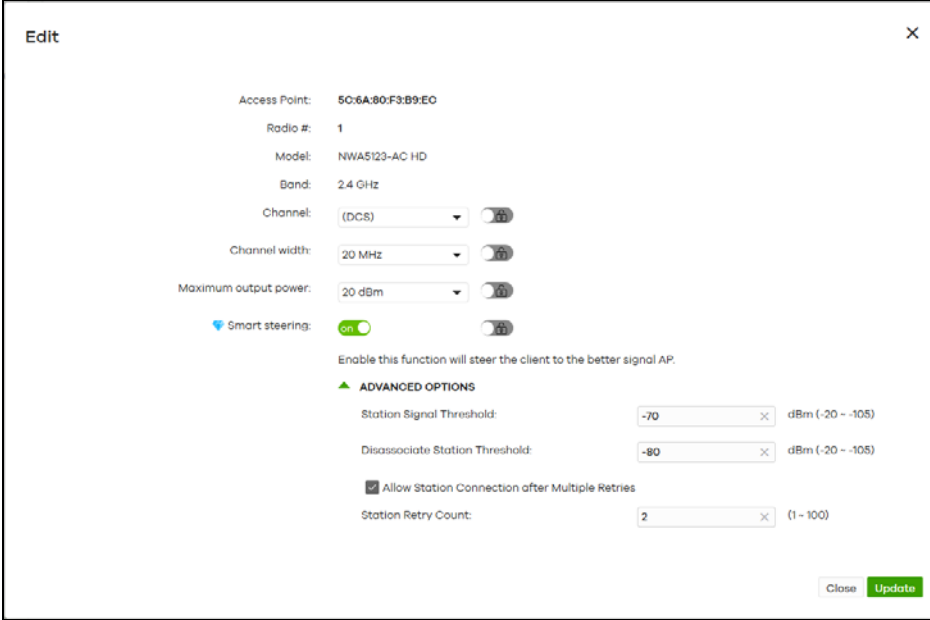
LABEL	DESCRIPTION
Channel width	<p>Select the wireless channel bandwidth you want the AP to use.</p> <p>A standard 20 MHz channel offers transfer speeds of up to 144 Mbps (2.4 GHz) or 217 Mbps (5 GHz) whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps (2.4 GHz) or 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. A 80 MHz channel consists of two adjacent 40 MHz channels. The wireless 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 wireless signal.</p> <p>Note: It is suggested that you select <b>20 MHz</b> when there is more than one 2.4 GHz AP in the network.</p> <p>Note: It is not possible to set channel bandwidth to 160 MHz for the whole site. To configure an AP to use 160 MHz, select a supported AP 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 AP surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the AP 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 AP 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 AP use DCS to automatically scan and find a less-used channel.</p>
DCS client aware	<p>Select <b>ON</b> to have the AP wait until all connected clients have disconnected before switching channels.</p>
Avoid 5G DFS channel	<p>If your APs are operating in an area known to have RADAR devices, the AP will choose non-DFS channels to provide a stable wireless service.</p>
Blacklist DFS channels in the presence of radar	<p>Select <b>ON</b> to blacklist a channels if RADAR is detected. After being blacklisted, the AP will not use the channel again until the AP is rebooted. However, the AP 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 AP uses channels 1, 4, 7, 11 in this configuration; otherwise, the AP 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>Manual</b> to select the individual channels the AP switches between.</p>
5 GHz channel deployment	<p>Select how you want to specify the channels the AP switches between for 5 GHz operation.</p> <p>Select <b>Auto</b> to have the AP automatically select the best channel.</p> <p>Select <b>Manual</b> to select the individual channels the AP switches between.</p> <p>Note: The method is automatically set to <b>Auto</b> when no channel is selected or any one of the previously selected channels is not supported.</p>

Table 165 Access Point &gt; Configure &gt; Radio settings (continued)

LABEL	DESCRIPTION
Allow 802.11ax/ac/n stations only	Select <b>ON</b> to have the AP 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 AP. Client steering helps monitor wireless clients and drop their connections to optimize the bandwidth when the clients are idle or have a low signal. When a wireless client is dropped they have the opportunity to steer to an AP with a strong signal. Additionally, dual band wireless clients can also steer from one band to another.</p> <p>Select <b>OFF</b> to disable this feature on the AP.</p>
ADVANCED OPTIONS	Click this to display a greater or lesser number of configuration fields.
2.4G/5G Setting	
Station Signal Threshold	<p>Set a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold.</p> <p>-20 dBm is the strongest signal you can require and -105 is the weakest.</p>
Disassociate Station Threshold	<p>Set a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the AP disconnects the wireless client.</p> <p>-20 dBm is the strongest signal you can require and -105 is the weakest.</p>
Allow Station Connection after Multiple Retries	Select the check box to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.
Station Retry Count	Set the maximum number of times a wireless client can attempt to re-connect to the AP.
802.11d	<p>Click this to enable 802.11d on the AP.</p> <p>802.11d is a wireless network specification, for use in countries where 802.11 WiFi is restricted. Enabling 802.11d causes the AP to broadcast the country where it is located, which is determined by the Country setting.</p>
WLAN Rate Control Setting	
2.4Ghz/5Ghz	<p>Sets the minimum data rate that 2.4 GHz and 5 GHz WiFi clients can connect to the AP, 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 AP.</p>



Table 165 Access Point &gt; Configure &gt; Radio settings (continued)

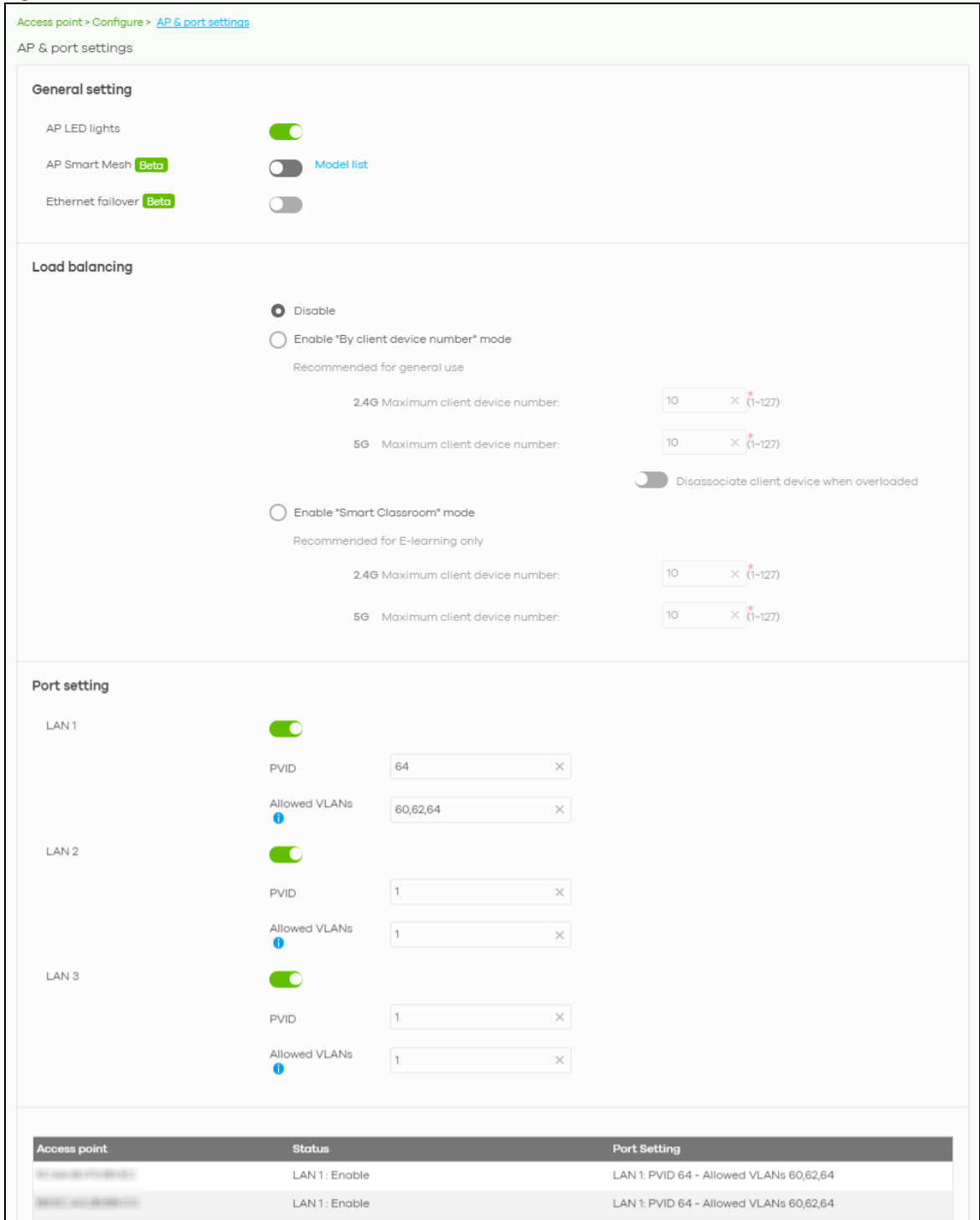
LABEL	DESCRIPTION
Edit	<p>Click this button to modify the channel, output power, channel width and smart steering settings for the selected APs.</p> <p>On the AP that comes with internal antennas and also has an antenna switch, you can adjust coverage depending on the orientation of the antenna for the AP radios. Select <b>Wall</b> if you mount the AP to a wall. Select <b>Ceiling</b> if the AP is mounted on a ceiling. You can switch from <b>Wall</b> to <b>Ceiling</b> if there are still wireless dead zones, and vice versa. 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>  <p>Note: On this screen, you can set channel width to 160 Mhz for the 5Ghz channel, if the AP supports it.</p>
DCS Now	Click this button to have the selected APs immediately scan for and select a channel that has least interference.
List	Click this to display a list of all connected APs.
Map	Click this to display the locations of all connected APs on the Google map.
2.4 GHz	Click this to display the connected APs using the 2.4 GHz frequency band.
5 GHz	Click this to display the connected APs using the 5 GHz frequency band.
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 AP.
Radio #	This displays the number of the connected AP's radio.
Model	This displays the model name of the connected AP.
Radio mode	This displays the type of Wi-Fi radio the AP is currently using, for example 802.11b/g/n.
Channel	This displays the channel ID currently being used by the connected AP's radio.
Transmit power	This displays the current transmitting power of the connected AP's radio. If the AP is off-line, this shows the maximum output power you configured for the AP.
Channel width	This displays the wireless channel bandwidth the connected AP's radio is set to use.
Smart steering	This displays whether smart client steering is enabled or disabled on the connected APs.
Antenna	This displays the antenna orientation settings for the AP that comes with internal antennas and also has an antenna switch.

## 11.3.6 AP & Port Settings

Use this screen to configure general AP settings and network traffic load balancing between the APs in the site. This screen also allows you to enable or disable a port on the managed AP and configure the port's VLAN settings. The port settings apply to all Nebula APs 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 195 AP > Configure > AP & Port Settings



The following table describes the labels in this screen.

Table 166 AP > Configure > AP & Port Settings

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

Table 166 AP &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 APs in the site.</p> <p>Click <b>Model list</b> to see whether your AP supports Nebula Smart Mesh.</p> <p>Note: Nebula Smart Mesh is a WiFi mesh solution for Nebula APs. For details, see <a href="#">Section 11.1.1 on page 365</a>.</p> <p>Note: You can override NCC settings and enable and disable Smart Mesh on individual APs. For details, see <a href="#">Section 11.2.1.1 on page 369</a>.</p> <p>Note: Disabling AP Smart Mesh automatically disables wireless bridge on all APs in the site. For details on wireless bridge, see <a href="#">Section 11.2.1.1 on page 369</a>.</p>
Ethernet failover	<p>When enabled, a wired AP in the site automatically changes its role from root AP to repeater AP if the AP is unable to reach the site's gateway.</p> <p>When disabled, a wired AP in the site automatically changes its role from root AP to repeater AP only if the AP's uplink Ethernet cable is unplugged.</p> <p>Note: For details on root and repeater APs, see <a href="#">Section 11.1.1 on page 365</a>.</p>
Load balancing	
Disable	Select this option to disable load balancing on the AP.
Enable "By client device number" mode	Select this option to balance network traffic based on the number of specified client devices connected to the AP.
Maximum client device number	Enter the threshold number of client devices at which the AP begins load balancing its connections.
Disassociate client device when overloaded	<p>Select <b>ON</b> to disassociate wireless clients connected to the AP when it becomes overloaded.</p> <p>Select <b>OFF</b> to disable this option, then the AP simply delays the connection until it can afford the bandwidth it requires, or it transfers the connection to another AP within its broadcast radius.</p> <p>The disassociation priority is determined automatically by the AP 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 kicked 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 kicked 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 AP. The AP 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 AP begins load balancing its connections.
Port setting	
LAN x	<p>This is the name of the physical Ethernet port on the AP.</p> <p>This section lets you configure global port VLAN settings for all APs in the site. To modify port settings for a specific AP, 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 AP. Select <b>OFF</b> to disable the port.
PVID	<p>Enter the port's PVID.</p> <p>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.</p>

Table 166 AP &gt; Configure &gt; AP &amp; Port Settings (continued)

LABEL	DESCRIPTION
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 AP. Only the AP that has an extra Ethernet LAN port will be listed, such as NAP203 or NAP303.
Status	This shows whether the AP's Ethernet LAN port is enabled or disabled.
Port Setting	This displays the port's VLAN settings for the managed AP.

### 11.3.6.1 Edit Port Settings

Click an entry in the **Port setting** table of the **AP > Configure > AP & Port Settings** screen to access this screen.

By default, all APs 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 196** AP > Configure > AP & Port Settings: Edit

The screenshot shows a configuration window titled "Edit" for "LAN 1". The settings are as follows:

- Enabled:** A toggle switch is turned on (green) and is locked (lock icon).
- PVID:** A text input field contains the value "64".
- Allowed VLANs:** A text input field contains the value "60,62,64".

At the bottom right, there are two buttons: "Close" (grey) and "OK" (green).

# CHAPTER 12

## Help

### 12.1 Support Forum

Click **Help > Support forum** to go to Zyxel Nebula Forum, where you can get the latest Nebula information and have conversations with other people by posting your messages.

### 12.2 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 Zyxel Nebula Forum before you use this screen to send a ticket.

Click **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.

**Figure 197** Help > Support Request: My Cases

Help > [Support request](#)

Support request

Zyxel Support  Invite Zyxel support as administrator

By enabling this, you are granting temporary access (21 days) to Zyxel support as administrator of your Organization. So they can help check your configuration & logs. This will automatically be switched off after 21 days, or you could turn it off right after your issue is solved. You might also edit the access privileges here.

**My Cases**

Open

4 items found, displaying all items. Page: 1

Case Number	Created	Last Updated	Creator	Subject	Priority	Status	Support Engineer
<a href="#">190600137</a>	2019-09-04 15:59:25	2019-09-10 14:11:51	bayardo.salgado@zy...	Device online	Low	Open	
<a href="#">190600103</a>	2019-08-14 14:04:15	2019-10-18 10:37:40	bayardo.salgado@zy...	Hello Support	Low	Open	
<a href="#">190600068</a>	2019-06-19 10:40:32	2019-10-15 11:20:16	bayardo.salgado@zy...	Nebula Support requ...	Medium	Open	
<a href="#">180300006</a>	2018-03-30 09:58:58	2019-10-09 17:35:20	bayardo.salgado@zy...	Nebula is great!	Low	Open	

The following table describes the labels in this screen.

Table 167 Help &gt; Support Request


LABEL	DESCRIPTION
Zyxel Support	<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. The support account will be deactivated automatically after 21 days. You can also select <b>OFF</b> to immediately disable the support account's access to the organization after finding a solution to the problem.</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="500 527 967 936" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;"><b>Update administrator</b> <span style="float: right;">✕</span></p> <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="Full"/> ▼</p> <p>Activated: <input type="text" value="Yes"/> ▼</p> <p style="text-align: center;"><span style="background-color: #28a745; color: white; padding: 2px 5px; border-radius: 3px;">+ Add</span></p> <p style="text-align: right;"><span style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">Close</span> <span style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">Update admin</span></p> </div> <p>A <b>Reset expire day</b> button displays and becomes active when you select <b>ON</b> and the number of days remaining before the support account is deactivated is less than or equal to 14.</p>
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.
Device	Select the NCC or the name of the device that cannot work properly.
Issue Description	Enter a complete and detailed description of your issue.
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.

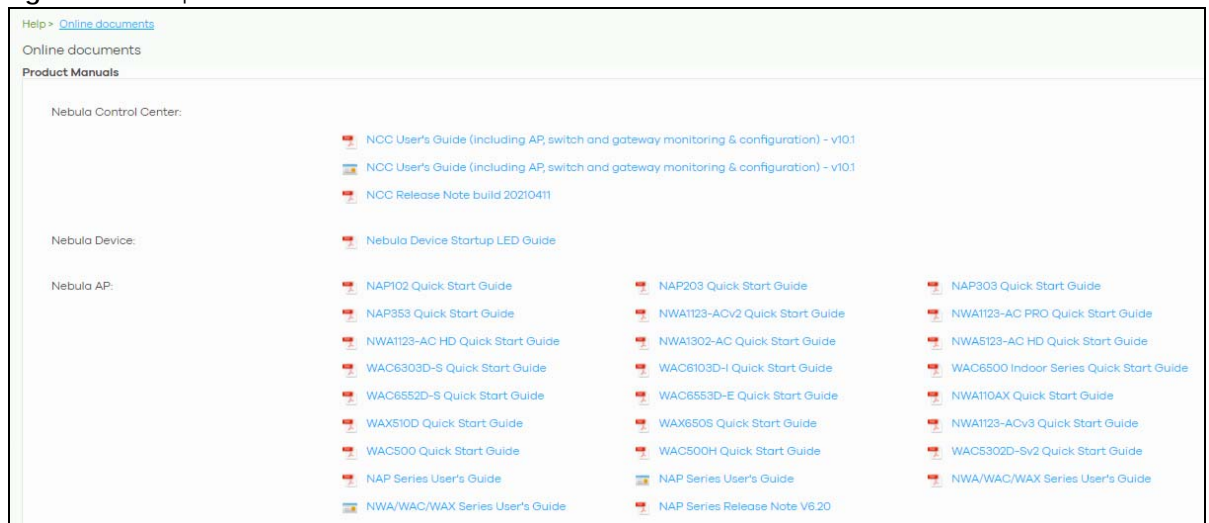
Table 167 Help &gt; Support Request (continued)

LABEL	DESCRIPTION
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.

## 12.3 Online documents

Click **Help** > **Online documents** to view the documentation for NCC and NCC-compatible devices.

Figure 198 Help &gt; Online documents



## 12.4 Firewall Information

Click **Help** > **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.



Figure 199 Help &gt; Firewall information

Help > [Firewall information](#)

Firewall information

This list is intended to help guide you in creating firewall rules for the Zyxel Nebula Control Center. [Export](#)

Service	FQDN	IP address	Port
Nebula Cloud Management (NETCONF)	d.nebula.zyxel.com	34.247.112.130, 52.210.12.1, 52.48.11...	4335 / 6667
Nebula Cloud Management	s.nebula.zyxel.com	Dynamic	443
Network Time Protocol	*.pool.ntp.org	Dynamic	123
Nebula Cloud Management (Zero Touch Provisioning)	d-a.nebula.zyxel.com	Dynamic	443
Nebula Cloud Management (Configure related service for USG FLEX series)	d-cp.nebula.zyxel.com	34.245.7199, 54.194.231.70	4335
Nebula Cloud Management (Monitor related service for USG FLEX series)	d-mp.nebula.zyxel.com	34.244.187.223, 54.217.13.185	443

## 12.5 Data Policy

Click **Help** > **Data Policy** to view and download NCC data policy, privacy policy, and terms of use.

Figure 200 Help &gt; Firewall information

Help > [Data policy](#)

Data policy

<a href="#">Nebula Data Policies</a>	<a href="#">Zyxel Privacy Policy</a>	<a href="#">Nebula Terms of Use</a>
<a href="#">Nebula Data Policies</a>	<a href="#">Data Processing Addendum (DPA)</a>	

## 12.6 Device Function Table

Click **Help** > **Device Function Table** to view a list of NCC-compatible APs, switches, and gateway devices. The table also includes which features each device supports.

Figure 201 Help > Device Function Table

[Help > Device function table](#)

Device function table

Access point Switch Gateway

Model Name	ACL	Radius Policy	Advanced IGMP	LLDP-MED	Switch name provisioning	Create IP Interface	IPv4 static route	Surveillance Monitoring	ONVIF discovery	Block Client	Port features			
											Auto PD Recovery	Extended Range	SFP+ Media Type Assignment	Spanning tree (STP) guard
NSW100-28P	*	*	*			*								*
NSW100-10P	*	*	*			*								*
NSW100-10	*	*	*			*								*
NSW100-28	*	*	*			*								*
NSW200-28P	*	*	*			*								*
XGS1930-28	*	*	*	*	*	*	*			*			*	*
XGS1930-28HP	*	*	*	*	*	*	*			*			*	*

# CHAPTER 13

## Troubleshooting

This chapter offers some suggestions to solve problems you might encounter with NCC and Nebula devices.

---

### None of the Nebula device LEDs turn on.

---

- Make sure that you have the power cord connected to the Nebula device and plugged in to an appropriate power source. Make sure you have the Nebula device turned on.
- Check all cable connections. See the related Quick Start Guide.
- If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local customer support.

---

### The Nebula device PWR LED is red.

---

- The Nebula device has a power-related error. Disconnect and reconnect the power cord. Make sure that you are using the included power cord for the Nebula device and it is plugged into an appropriate power source. See the related Quick Start Guide.
- If the LED is still red, you may have a hardware problem. In this case, you should contact your local customer support.

---

### I 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. Browsers supported are:
  - Firefox 36.0.1 or later
  - Chrome 41.0 or later
  - IE 10 or later

---

### 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 don't have a myZyxel account and create an account.

---

### I cannot see my devices in the NCC Dashboard or the corresponding device monitor page.

---

- At the time of writing, you can only manage Zyxel Nebula APs, switches or security gateways through the NCC. See [Section 1.1 on page 10](#).
- If your device supports NebulaFlex or NebulaFlex Pro, make sure that the device is working in Nebula cloud manage mode with NCC Discovery enabled.
- Make sure that your device can connect to the NCC by checking your network's firewall/security settings. The following ports must be allowed:
  - TCP: 443, 4335 and 6667
  - UDP: 123

Note: Go to **Help > Firewall Information** to find the latest port information.

- Make sure that you have registered your Nebula devices with the NCC. See [Section 6.3.2 on page 98](#).
- Make sure that you have created an organization and site and add the devices to the site. See [Create Organization on page 32](#) and [Section 6.3.1 on page 97](#).

## 13.1 Getting More Troubleshooting Help

Go to [support.zyxel.com](https://support.zyxel.com) at the Zyxel website for other technical information on the NCC.

# APPENDIX A

## Customer Support

### 13.2 Zyxel 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.

See <https://www.zyxel.com/homepage.shtml> and also [https://www.zyxel.com/about\\_zyxel/zyxel\\_worldwide.shtml](https://www.zyxel.com/about_zyxel/zyxel_worldwide.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>

### **Belgium**

- Zyxel Communications B.V.

- <https://www.zyxel.com/be/nl/>
- <https://www.zyxel.com/be/fr/>

## **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/>

## **Estonia**

- Zyxel Estonia
- <https://www.zyxel.com/ee/et/>

## **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/>

## **Latvia**

- Zyxel Latvia
- <https://www.zyxel.com/lv/lv/>

## **Lithuania**

- Zyxel Lithuania
- <https://www.zyxel.com/lt/lt/>

## **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/>

## Middle East

- Zyxel Communications Corporation
- <https://www.zyxel.com/me/en/>

## North America

### USA

- Zyxel Communications, Inc. - North America Headquarters
- <https://www.zyxel.com/us/en/>

## Oceania

### Australia

- Zyxel Communications Corporation
- <https://www.zyxel.com/au/en/>

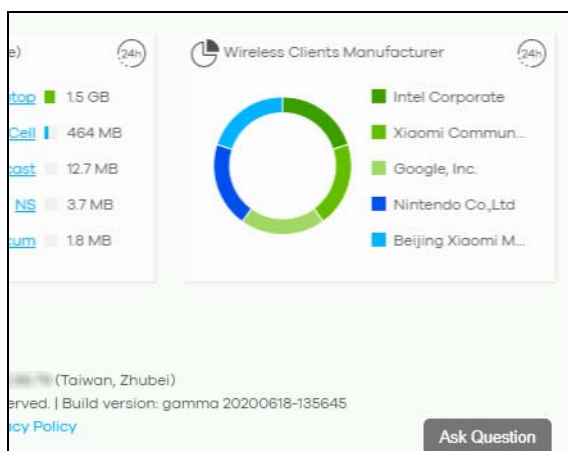
## Africa

### South Africa

- Nology (Pty) Ltd.
- <https://www.zyxel.com/za/en/>

## 13.3 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 Pro-pack feature.

Note: 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 B

## Legal Information

### Copyright

Copyright © 2021 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 Communications Corporation.

Published by Zyxel Communications Corporation. 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.

## Numbers

2FA [15](#)  
802.11k neighbor lists [395](#)  
802.11r fast roaming [391](#)  
802.1X authentication [391](#)

## A

access port [345](#)  
account  
  disable [71](#)  
account status [70, 90, 118](#)  
ACL [348, 349](#)  
Active Directory [246, 312](#)  
AD server [246, 312](#)  
administrator  
  create [70](#)  
  privilege [68](#)  
  update [70](#)  
administrator accounts [116](#)  
Admins & teams [68](#)  
Admins screen [68](#)  
ALG [318](#)  
antenna orientation [373](#)  
antenna switch [373](#)  
AP connection status [368](#)  
AP photo [374](#)  
App ID [392](#)  
Application Layer Gateway, see ALG  
application patrol profile [225, 290](#)  
assisted roaming [395](#)  
Automatic Power Save Delivery [395](#)  
auto-negotiation [342](#)

## B

backup code [17](#)  
  download [17](#)  
  inactive [17](#)  
bandwidth utilization [329](#)  
battery life [395](#)  
bridge priority [363](#)  
browser support [13](#)  
bypass mode [392](#)

## C

captive portal [238, 303, 396](#)  
certifications  
  viewing [424](#)  
channel bandwidth [382](#)  
channel width [403](#)  
Classification mode [327](#)  
client steering [404](#)  
cloud authentication [120](#)  
Cloud Authentication account  
  privilege [73](#)  
Cloud-Saving mode [33](#)  
configuration backup [131](#)  
configuration management [131](#)  
configuration synchronization [131](#)  
configuration template [134](#)  
connectivity [96](#)  
Consumption mode [327](#)  
contact information [417](#)  
content filtering [227, 295](#)  
Coordinated Universal Time (UTC) [37](#)  
copyright [424](#)  
CPU usage [194, 254](#)  
CRC error [330](#)  
Create Organization screen [32](#)  
create user account [123, 126, 128](#)

cross-org site clone [74](#)  
cross-org sync [73](#)  
Cross-org synchronization screen [74](#)  
CSS values [240](#), [305](#)  
custom portal pages [398](#)  
custom theme [397](#)  
customer support [411](#), [417](#)  
Cyclic Redundant Check [330](#)

## D

dark mode [24](#)  
Dashboard logo [66](#)  
dashboard logo  
  specs [67](#)  
Dashboard screen [19](#)  
DCS [382](#)  
  time interval [403](#)  
DDMI [331](#)  
device  
  add to site [37](#)  
  view [22](#)  
DH key [234](#)  
DHCP relay [210](#), [215](#)  
DHCP server [210](#), [215](#)  
DHCP server guard [364](#)  
DHCP service [210](#), [215](#)  
Diffie-Hellman key group [234](#)  
Digital Diagnostics Monitoring Interface [331](#)  
disable account [71](#), [91](#), [119](#)  
disclaimer [424](#)  
DNS settings [246](#), [312](#)  
domain zone [248](#), [314](#)

## E

eITS ticket [411](#)  
email recipient  
  MSP alerts [78](#)  
email report [385](#)  
Email Verification [17](#)  
event log [195](#), [255](#), [332](#), [380](#)

## F

Facebook App ID [392](#)  
Facebook fan page [392](#)  
Facebook login [152](#), [377](#), [392](#)  
Facebook Wi-Fi [152](#), [377](#), [392](#)  
fan page [392](#)  
fast roaming [391](#)  
firewall [221](#), [288](#)  
floor plan [158](#)  
force logout [89](#), [116](#)  
FQDN [248](#), [313](#)  
full access [118](#)  
Fully-Qualified Domain Name [248](#), [313](#)

## G

get started [13](#)  
Google Authenticator app [16](#)  
guest ambassador [118](#)  
  access [119](#)  
Guest interface [206](#), [213](#)  
guest VLAN [360](#)  
guest WiFi network [39](#)

## H

Hub-and-Spoke VPN [232](#)

## I

idle timeout [115](#)  
IDP [227](#), [295](#)  
IEEE 802.11k/v [395](#)  
IEEE 802.11r [391](#)  
IGMP filtering profile [348](#)  
IGMP multicast groups [334](#)  
IGMP query port [348](#)  
IGMP snooping [354](#)  
import certificate [116](#)

installer [118](#)  
Installer access [119](#)  
internal antennas [373](#)  
Internet Protocol Security [236](#)  
Intra-BSS traffic blocking [395](#)  
intra-BSS traffic blocking [389](#)  
Intrusion Detection and Prevention [227, 295](#)  
IPSec [236](#)  
IPSec VPN [233](#)  
IPTV channels [31, 333](#)  
IPTV report [31, 332](#)

## L

L2 isolation [389](#)  
L2TP [236](#)  
L2TP VPN [236](#)  
language  
  select [24](#)  
Layer 2 Tunneling Protocol [236](#)  
layer-2 isolation [395](#)  
leave mode  
  fast [347](#)  
  normal [347](#)  
LED tags [367](#)  
license management [85, 98](#)  
Link Layer Discovery Protocol [329](#)  
LLDP [329](#)  
load balancing [408](#)  
load balancing method [245](#)  
Local Override [136, 137](#)  
local override [134](#)  
  switch [137](#)  
locator LED [326](#)  
log message [332](#)  
log messages [380](#)  
login account  
  menu [22](#)  
login page [397](#)  
logo  
  remove [67](#)  
  replace [67](#)  
  upload [67](#)

loop guard [343](#)

## M

MAC authentication [391](#)  
Managed Service Provider (MSP) [11](#)  
Managed Services Provider [64](#)  
management VLAN [363](#)  
map  
  pin a device [159](#)  
Memory usage [194, 254](#)  
MSP administrator [75](#)  
MSP alerts  
  create [77](#)  
  email recipient [78](#)  
  notification type [78](#)  
  update [77](#)  
MSP alerts screen [75](#)  
MSP branding [66](#)  
MSP license [64](#)  
MSP portal [64](#)  
myZyxel account [10, 13](#)  
  email address [17](#)  
myZyxel.com account [11](#)

## N

NAS [249, 320](#)  
NAS Identifier [393](#)  
NAS IP Address [249, 320](#)  
NCAS [394](#)  
NCC  
  access [13](#)  
  account settings [25](#)  
  alert [23](#)  
  change device owner [32](#)  
  create organization [32](#)  
  dark mode [24](#)  
  Dashboard [148](#)  
  display language [24](#)  
  example network [12](#)  
  features [10](#)  
  license expiration [66, 81](#)

- license status [81](#)
- log message view [23](#)
- login [13](#)
- menu [25](#)
- notification [23](#)
- organization [11](#)
- overview [10, 43](#)
- portal [415](#)
- portal website [13](#)
- sample network topology [12](#)
- settings icon [23](#)
- site [11](#)
- two-factor authentication [15](#)
- version differences [100](#)
- NCC logo
  - replace [66](#)
- NCC Menu Summary [26](#)
- NCC portal
  - access [13](#)
  - overview [19](#)
  - parts [19](#)
  - title bar [19](#)
- NCC Pro Pack
  - activate [42](#)
- NCC, Nebula Control Center [10, 43](#)
- Nebula account
  - login [18](#)
- Nebula Cloud Authentication Server [394](#)
- Nebula managed device
  - connect [13](#)
- Nebula SD-WAN [21](#)
- Nebula Security Service [29, 30, 198, 257](#)
- Nebula Smart Mesh [408](#)
- NETCONF [10](#)
- NETCONF over TLS [10](#)
- Network Access Server [249, 320](#)
- Network Access Server identifier [393](#)
- Network Configuration Protocol (NETCONF) [10](#)
- network topology [160](#)
  - fully-meshed [143](#)
- network, org-to-org
  - service [85](#)
- next hop [219, 273](#)
- NSS [29, 30, 198, 257](#)
- NSS/UTM
  - license expiration [66](#)

## O

- operating system [152, 377](#)
- Orchestrator [21](#)
- Orchestrator Management [21](#)
- organization
  - choose [33](#)
  - create [32, 36](#)
  - create new [14](#)
  - privilege [71](#)
  - summary view [20](#)
- organization access [90, 119](#)
- organization administrator [10, 12](#)
- output power [402](#)
- owner [118](#)

## P

- PD priority [346](#)
- Perfect Forward Secrecy [235](#)
- PFS [235](#)
- PoE [360](#)
- PoE mode [327](#)
- PoE schedule [346, 360](#)
- policy route [219, 272](#)
- port groups [205, 263](#)
- port isolation [345](#)
- port mirroring [329, 363](#)
- port security [360](#)
- port settings [406](#)
- port VLAN ID [343, 346](#)
- power consumption [329](#)
- power management mode [325, 327](#)
- Power over Ethernet [360](#)
- power-up [346](#)
- pre-shared key [146, 232, 280](#)
- privilege [89, 118](#)
  - administrator [68](#)
  - assign [73](#)
  - organization [69, 71](#)
- privilege priority [68](#)
- problems [415](#)
- product registration [424](#)



profile  
  switch [137](#)  
PVID [346, 373](#)

## Q

QR code [16](#)

## R

radio settings [401](#)  
RADIUS accounting [393](#)  
RADIUS server [393](#)  
rate limiting [389](#)  
read and write access [118](#)  
read-only [118](#)  
recurring schedule [185](#)  
register a device [28, 182](#)  
registration  
  product [424](#)  
restore configuration [134](#)  
root bridge [325](#)  
RSTP Status [325](#)

## S

schedule firmware upgrade [27, 28, 146, 183](#)  
schedule template [361, 401](#)  
SD-WAN license [21](#)  
search  
  for NCC-managed device [22](#)  
security services [194](#)  
Security Services Trial  
  activate [42](#)  
serial number [322](#)  
Server-and-Client VPN [232](#)  
Service Set Identifier [386](#)  
setup wizard [18, 35](#)  
  steps [35](#)  
severity level [411](#)  
side-wide schedule [185](#)

SIP  
  ALG [318](#)  
site  
  create [36](#)  
site administrator [10, 11](#)  
site binding [135](#)  
site, hub [143](#)  
Site-to-Site VPN [232](#)  
Smart Alert Engine [76](#)  
spanning tree [325](#)  
SSID [38, 386](#)  
SSID profiles [386](#)  
SSID schedule [400](#)  
submit ticket [410](#)  
summary report [158](#)  
support account [411](#)  
Support contact [66](#)  
support request [410](#)  
supported  
  access point [11](#)  
  Ethernet switch [11](#)  
  security gateway [11](#)  
supported browsers [415](#)  
supported Nebula devices [11](#)  
switch connection status [322](#)

## T

team  
  create [72](#)  
  update [72](#)  
Teams screen [71](#)  
ticket details [410](#)  
time zone  
  set [37](#)  
traffic shaping [243](#)  
transmitting power [405](#)  
troubleshooting [415](#)  
trunk group [342](#)  
trunk port [345](#)  
Two-factor authentication  
  enable [15](#)

## U

U-APSD [395](#)  
uplink AP [369](#)

## V

virtual private network [230, 278](#)  
VLAN ID [38](#)  
VLAN settings  
    guest [39](#)  
Voice VLAN [363](#)  
VPN [230, 278](#)  
VPN (Virtual Private Network) [143](#)

## W

walled garden [246, 312, 389, 393](#)  
WAN throughput [149](#)  
warranty [424](#)  
    note [424](#)  
web authentication [241, 306, 308](#)  
WiFi  
    guest [39](#)  
WiFi network name  
    enter [38](#)  
WiFi password  
    enter [38](#)  
WiFi settings [38](#)  
WINS server [210, 216](#)  
wireless channel bandwidth [403](#)  
wireless health [380](#)  
world map [158](#)

## Z

Zero Touch Provisioning [40](#)  
ZTP (Zero Touch Provisioning) [40](#)  
ZyWALL VPN device  
    configure [21](#)