

# User's Guide

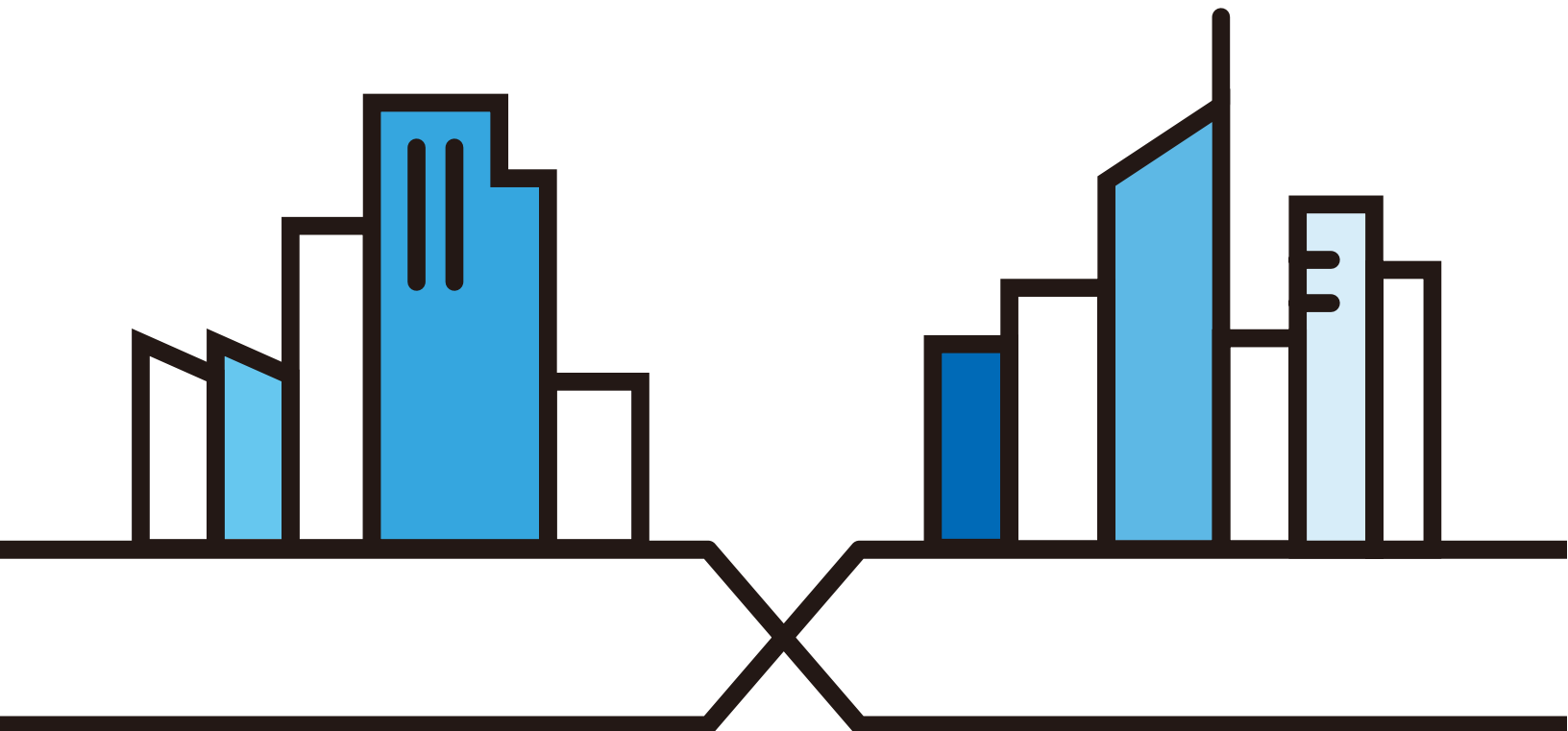
## NCC

Nebula Control Center

### Default Login Details

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

Version 6.1.0 Edition 1, 01/2019



---

**IMPORTANT!**

**READ CAREFULLY BEFORE USE.**

**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

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

### **Related Documentation**

- Quick Start Guide

The Quick Start Guide shows how to connect the managed device, such as the Nebula AP, switch or security gateway.

- 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>6</b>
<b>Chapter 1</b>	
<b>Introduction .....</b>	<b>7</b>
1.1 NCC Overview .....	7
1.1.1 NCC Versions .....	7
1.1.2 NCC Version Differences .....	8
1.1.3 Relationship between Organizations, Sites and Accounts .....	9
1.2 Getting Started .....	11
1.2.1 Connect Nebula Managed Devices .....	11
1.2.2 Access the NCC Portal .....	11
1.3 NCC Portal Overview .....	17
1.3.1 Title Bar .....	18
1.3.2 Navigation Panel .....	23
<b>Chapter 2</b>	
<b>Setup Wizard.....</b>	<b>27</b>
2.1 Accessing the Wizard .....	27
2.2 Using the Wizard .....	27
2.2.1 Step 1 Create an organization and site .....	27
2.2.2 Step 2 Add your devices .....	28
2.2.3 Step 3 Set up your WiFi network .....	29
2.2.4 Step 4 Set up a Guest WiFi network .....	29
2.2.5 Summary .....	30
<b>Part II: Technical Reference.....</b>	<b>31</b>
<b>Chapter 3</b>	
<b>Site-Wide.....</b>	<b>32</b>
3.1 Monitor .....	32
3.1.1 Dashboard .....	32
3.1.2 Summary Report .....	34
3.1.3 Map & Floor Plan .....	36
3.1.4 Topology .....	38

3.2 Configure .....	39
3.2.1 General Setting .....	39
3.2.2 Alert Setting .....	42
3.2.3 Add Device .....	43
3.2.4 Firmware Management .....	45
<b>Chapter 4</b>	
<b>AP .....</b>	<b>48</b>
4.1 Overview .....	48
4.2 Monitor .....	48
4.2.1 Access Point .....	48
4.2.2 Client .....	53
4.2.3 Event Log .....	57
4.2.4 Summary Report .....	58
4.3 Configure .....	61
4.3.1 SSIDs .....	61
4.3.2 SSID Schedule .....	63
4.3.3 Authentication .....	65
4.3.4 Captive Portal .....	69
4.3.5 Radio Setting .....	73
4.3.6 Client Steering .....	76
4.3.7 Port Setting .....	77
<b>Chapter 5</b>	
<b>Switch .....</b>	<b>80</b>
5.1 Overview .....	80
5.2 Monitor .....	80
5.2.1 Switch .....	80
5.2.2 Client .....	90
5.2.3 Event Log .....	92
5.2.4 IPTV Report .....	92
5.2.5 Summary Report .....	95
5.3 Configure .....	97
5.3.1 Switch Ports .....	98
5.3.2 IP Filtering .....	103
5.3.3 Advanced IGMP .....	104
5.3.4 RADIUS Policy .....	109
5.3.5 PoE Schedule .....	110
5.3.6 Switch Configuration .....	111
<b>Chapter 6</b>	
<b>Gateway .....</b>	<b>115</b>
6.1 Overview .....	115

6.2 Monitor .....	115
6.2.1 Security Gateway .....	115
6.2.2 Client .....	118
6.2.3 Event Log .....	121
6.2.4 VPN Connection .....	121
6.2.5 NSS Analysis Report .....	123
6.2.6 Summary Report .....	125
6.3 Configure .....	128
6.3.1 Interfaces Addressing .....	128
6.3.2 Firewall .....	136
6.3.3 Policy Route .....	142
6.3.4 Content Filtering .....	143
6.3.5 Site-to-Site VPN .....	146
6.3.6 L2TP over IPSec Client .....	150
6.3.7 Network Access Method .....	151
6.3.8 Walled Garden .....	153
6.3.9 Captive Portal .....	154
6.3.10 Traffic Shaping .....	158
6.3.11 Security Filtering .....	161
6.3.12 Network Servers .....	162
<b>Chapter 7</b>	
<b>Organization.....</b>	<b>166</b>
7.1 Overview .....	166
7.2 Monitor .....	166
7.2.1 Organization Overview .....	166
7.2.2 Change Log .....	169
7.3 Configure .....	171
7.3.1 Create Site .....	171
7.3.2 Inventory .....	171
7.3.3 License Management .....	173
7.3.4 Organization Setting .....	176
7.3.5 Administrator .....	178
7.3.6 Cloud Authentication .....	181
7.3.7 VPN Members .....	184
7.3.8 Configuration Management .....	188
<b>Chapter 8</b>	
<b>Troubleshooting.....</b>	<b>191</b>
8.1 Getting More Troubleshooting Help .....	192
Appendix A Customer Support.....	193
Appendix B Legal Information.....	199

---

# 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. Being a SaaS (Software as a Service) solution, it provides access to the licensed software and applications on a subscription basis over the Internet.

Feature support includes:

- System accounts with different privilege levels
  - Site Administrator: manage one site
  - Organization Administrator: manage one or more organizations
- Multi-tenant management
- Inventory and license management
- Alerts to view events, such as when a device goes down
- Graphically monitoring individual devices
- Securely managing Nebula devices by using the Network Configuration Protocol (NETCONF) over TLS

At the time of writing, the supported Nebula devices are NAP102, NAP203, NAP303, NAP353, NWA1123-ACv2, NWA1123-AC HD, NWA1123-AC PRO, NWA1302-AC, NSW100-10P, NSW100-28P, NSW200-28P, GS1920v2 series, XGS1930 series, NSG50, NSG100, NSG200 and NSG300.

### 1.1.1 NCC Versions

Zyxel offers two versions of the NCC: Nebula Professional Pack and Nebula. The professional pack requires NCC licenses and provides the whole set of features you would need or expect to manage your network. Nebula is the free version of NCC, that has limited features.

The two NCC versions are organization-based. You can create and manage either one or both Nebula Professional Pack organization(s) and Nebula free organization(s) on one account.

#### Nebula Professional Pack

To set up an organization with Nebula Professional Pack, you should at least have a 90-day NCC service license to manage all Nebula devices registered to the organization. To extend the license before it expires, you can register a new Nebula device that comes with a NCC service license or enter a license key and activate it in the **Organization > License Management** screen.

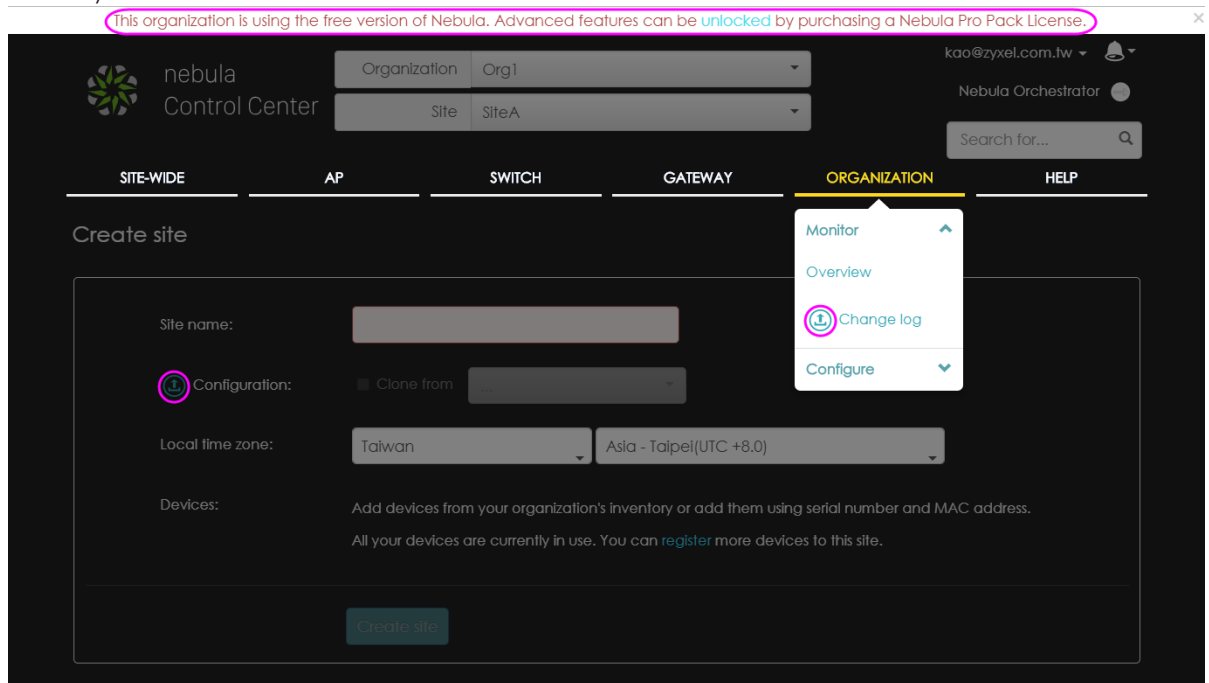
Note: If the NCC license of an organization expires, the NCC service will be automatically downgraded from Nebula Professional Pack to Nebula.

## Nebula

With a Nebula free organization, you can manage supported devices without any NCC license. Even though you add a Nebula device that comes with a license, its license credit will not be consumed in the Nebula organization.

Note: The NCC service will be automatically upgraded from Nebula to Nebula Professional Pack when an license is activated and the number of days remaining before the license expires is greater than 90.

After logging into the NCC and selecting to manage a Nebula free organization, you will see a warning banner about feature limitations. Besides, you also see the upgrade (📌) icon next to a feature, which indicates the feature is available only for Nebula Professional Pack organizations. When you click the icon, a window then displays asking you to upgrade to Nebula Professional Pack with a license key before you can use this advanced feature.



### 1.1.2 NCC Version Differences

The differences of Nebula from Nebula Professional Pack are listed below.

- Maximum limits
  - Number of administrator accounts: 5
  - Number of cloud authentication entries: 100
  - Number of AP photos: 1 for Nebula (5 for Nebula Professional Pack)
  - Statistics or monitoring information for up to 7 days
- Service limitations
  - No email summary reports
  - No email alerts
  - No in-app push notifications

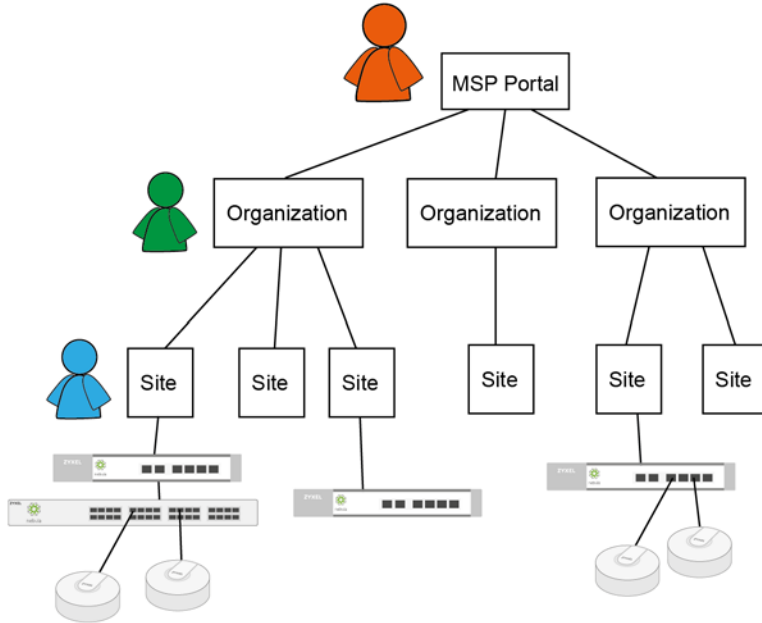


- No organization change logs
- No support tickets (forum and regional support still available)
- Features disabled
  - Viewing the site-wide network topology
  - Viewing the organization VPN topology
  - Viewing IPTV report and channel information
  - Adding clients for a managed AP
  - Cloning site settings when creating a site
  - Specifying login IP address ranges for an organization
  - Exporting data to a CSV or XML file
  - Creating firmware upgrade schedules on a per-device basis
  - Enabling RADIUS accounting with captive portal for an SSID profile
  - Setting NAS ID for web authentication (captive portal) via RADIUS
  - Sending gateway traffic log to a syslog server
  - Configuring IGMP snooping, IGMP filtering profiles and IGMP-related port settings
  - Configuration management including site settings synchronizing, switch settings cloning and configuration backup/restoration
  - Specifying destination IPs, port numbers, protocol type and priority for bandwidth limits in traffic shaping
  - Setting which alerts to be created and sending notifications within the Nebula mobile app

### 1.1.3 Relationship between Organizations, Sites and Accounts

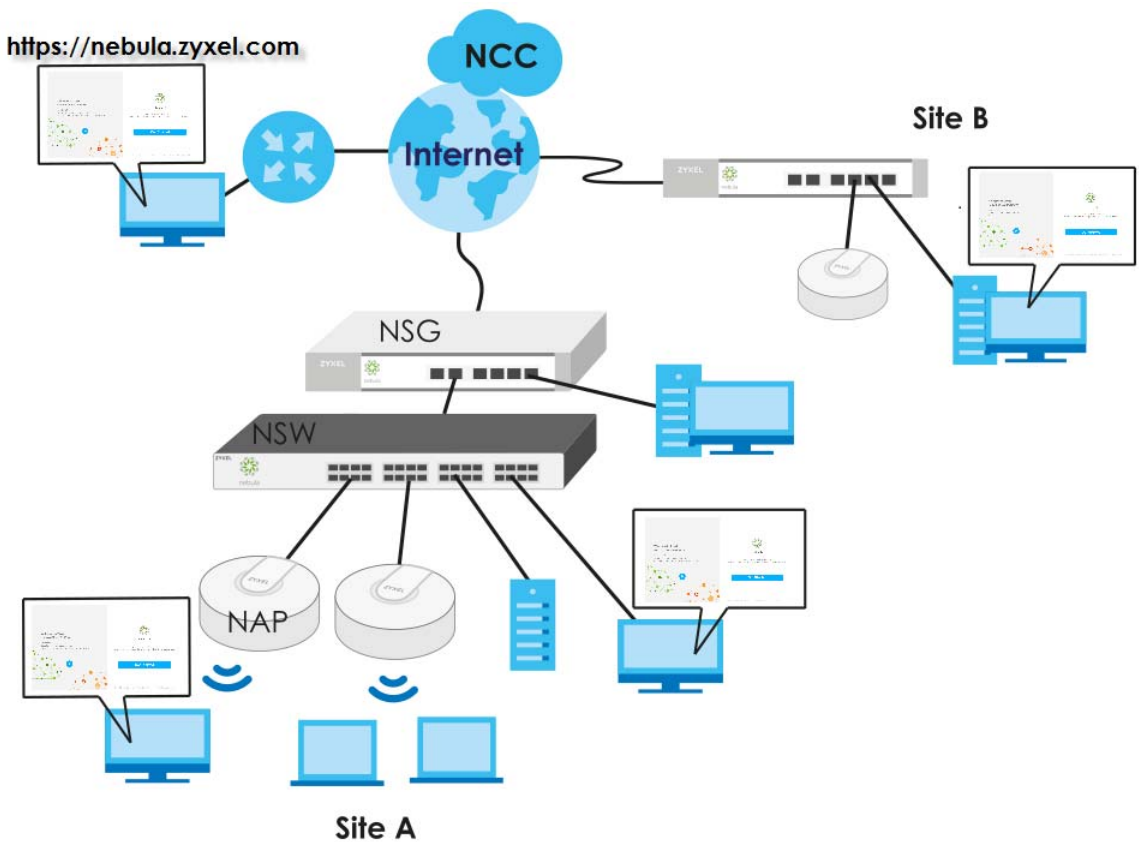
In the NCC, a site is a group of devices. An organization is a group of sites. To use the NCC to manage your Nebula devices, each device should be assigned to a site and the site must belong to an organization.

- 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 7.3.5 on page 178](#)).
- An organization administrator can manage more than one organization and use the MSP portal page to view the organization summary (see [MSP Portal on page 18](#)).
- 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 by the NCC using an Internet browser. Browsers supported are:

- Firefox 36.0.1 or later
- Chrome 41.0 or later
- IE 10 or later

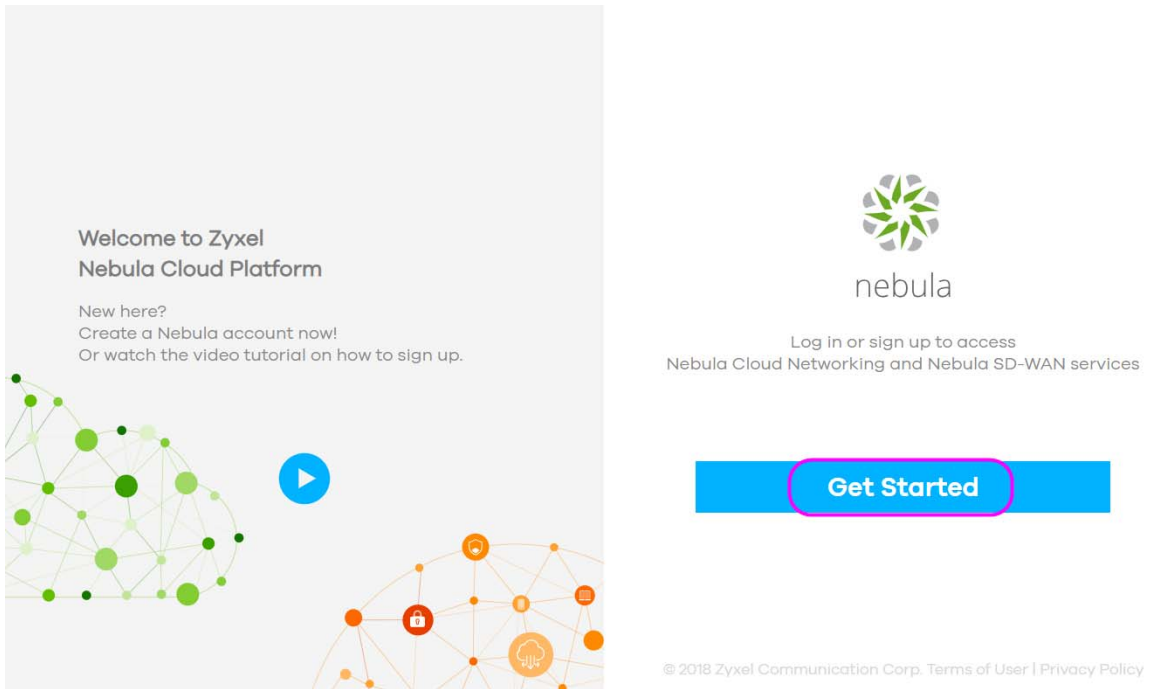
### 1.2.1 Connect Nebula Managed Devices

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.

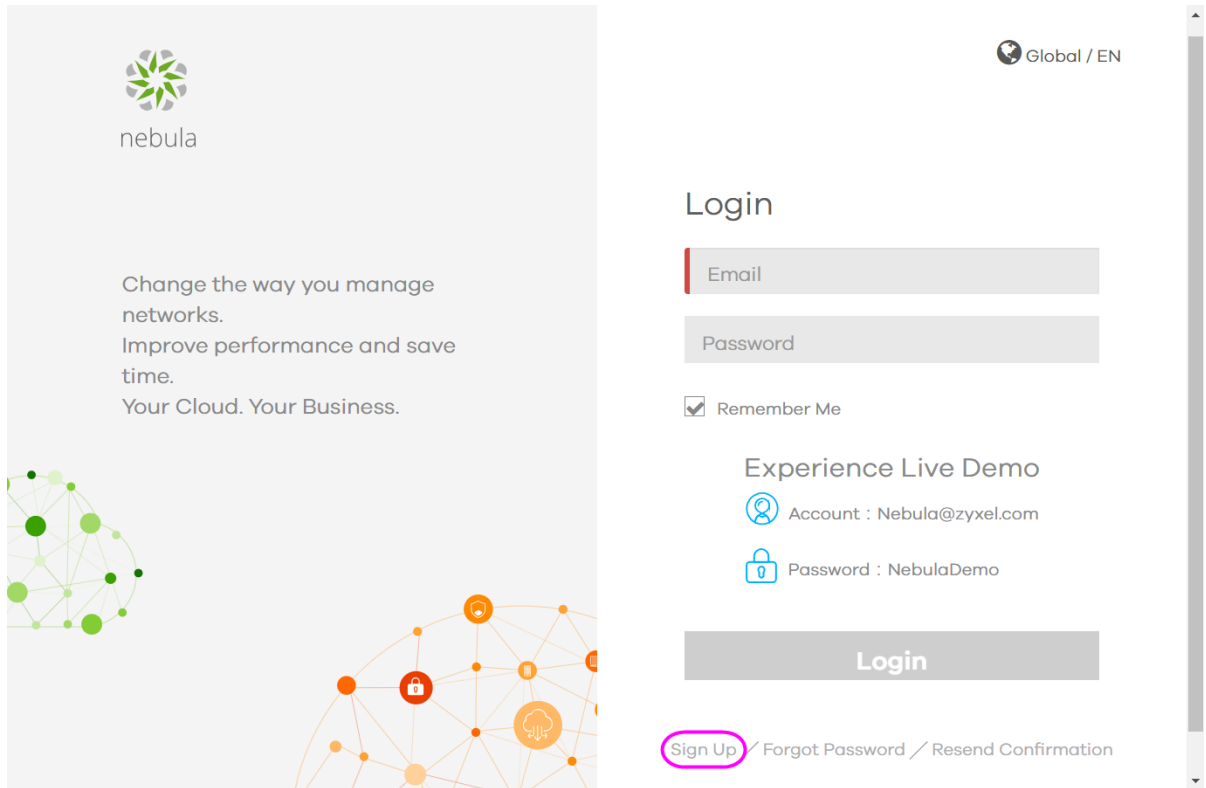
### 1.2.2 Access the NCC Portal

Go to the NCC portal website.

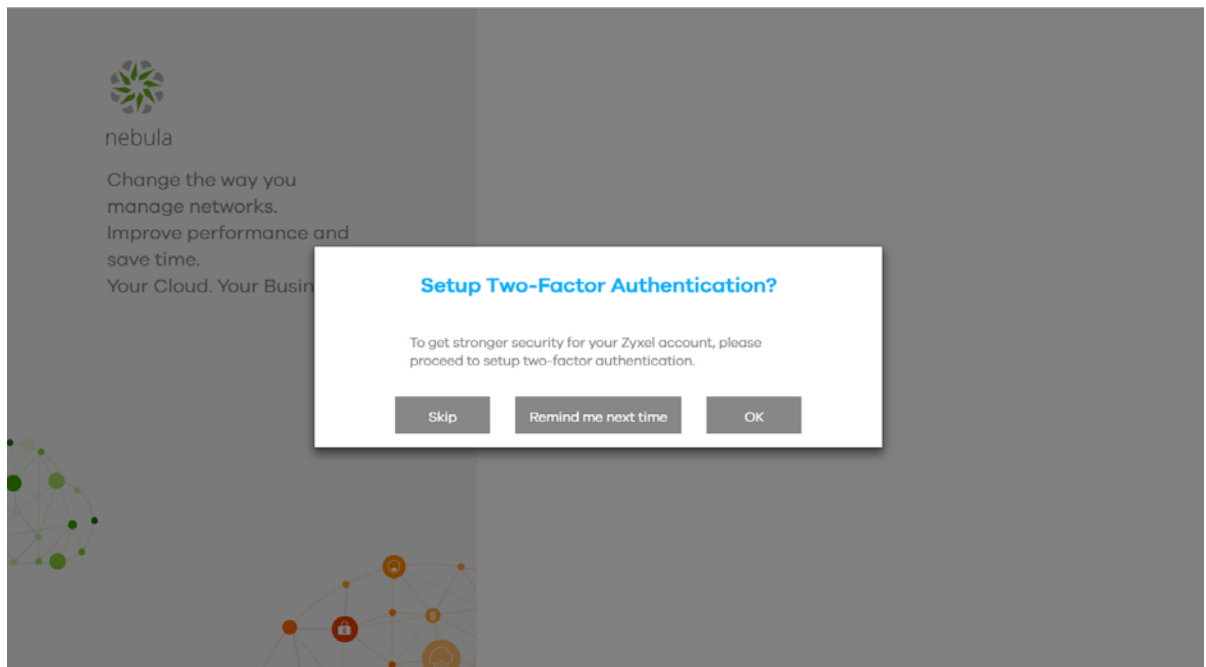
- 1 Type <http://nebula.zyxel.com> in a supported web browser. Click **Get Started**.



- 2 The NCC requires a myZyxel account before you can register and manage Nebula devices. Log into the NCC with your myZyxel account. Click **Sign Up** if you don't have a myZyxel account and quickly create an account with your existing email address.



- 3 The NCC supports two-factor authentication (2FA) to add a second layer of security to your account. After providing your account name and password, you can click **OK** to activate the two-step verification service using the Google Authenticator app or your email address. Alternatively, click **Skip** to disable 2FA or **Remind me next time** to use 2FA the next time you log in and go to step 4 directly.



Select **Google Authenticator** or **Email Verification** to get a code and click **Next**.



### Google Authenticator

Google Authenticator generates a two-step verification code on your phone.

The two-factor verification mechanism will require a second-step verification when you sign in to your account, thereby further ensuring your account is safe. When this feature is enabled, in addition to entering your password when logging into your account, you must also enter the verification code generated by your Google Authenticator app on your

**Google Authenticator**  
Use "Authenticator" app to generate login codes.

**Email Verification**  
Verification instructions is sent by email.

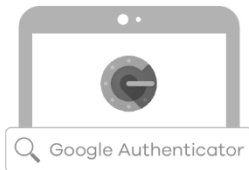
**Next**

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 six-digit one-time code. Then enter the code and click **Verify** to authenticate your identity.

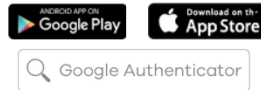


### Setup Google Authenticator

Use "Authenticator" app to generate login codes.



**1** Get the Authenticator App from the Google Play Store (Android) or iTunes App Store (iOS).



**2** Choose Scan a barcode.



[Can't scan it?](#)

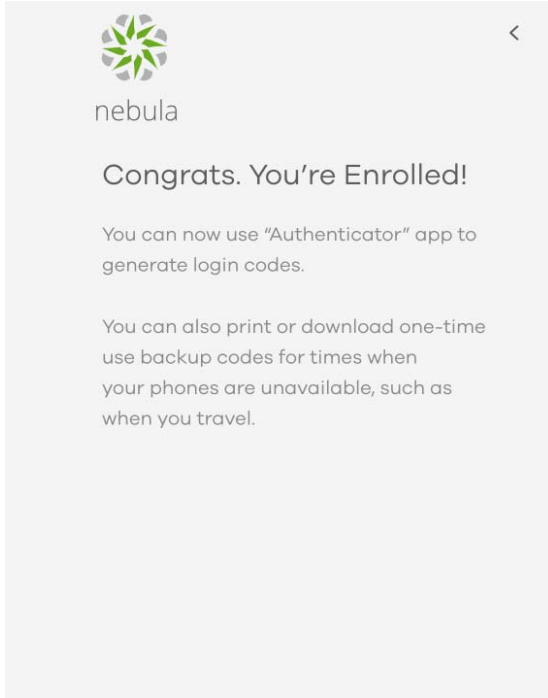
**3** Set up Authenticator. Enter the six-digit code that you see in the app.

Enter Code

**Verify**

Click **Generate Backup Codes** to get 10 backup codes, which help regain access to your account in

case you lose your phone.



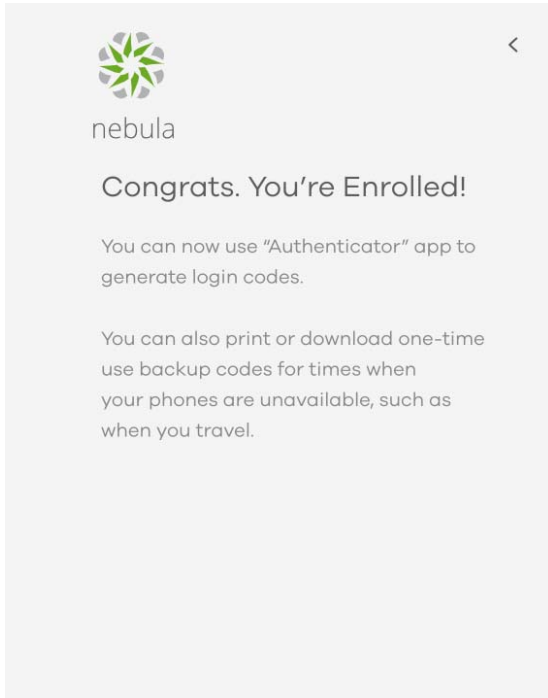
If you ever lose access to your smart phone, you can always use backup code.

Generate Backup Codes

Done

Write down or print out the backup codes for your account. Each code can only work once. Click **Done** to finish two-factor authentication.

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



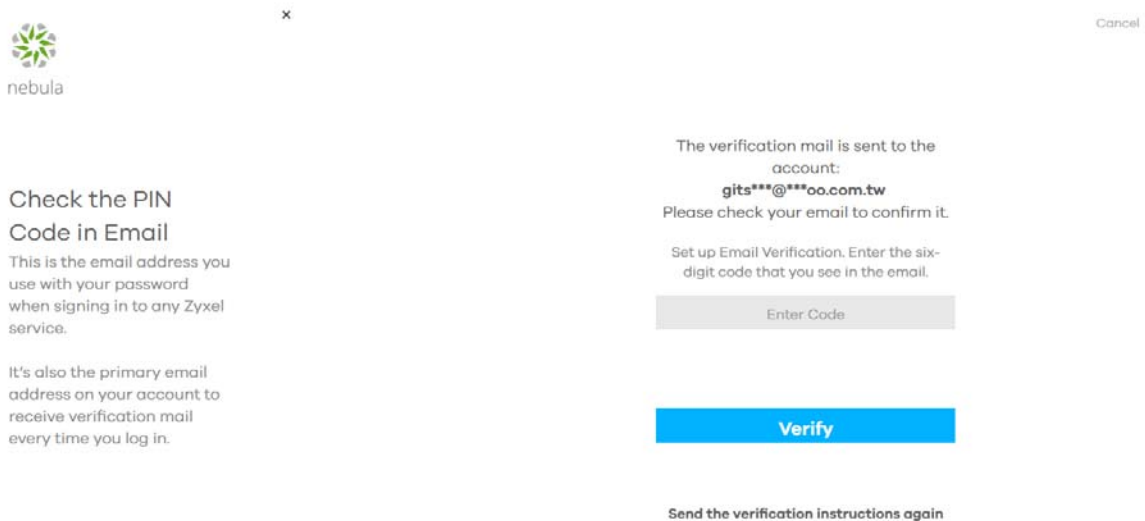
If you ever lose access to your smart phone, you can always use backup code.

Your Backup Codes	
1. 976 653	6. 284 958
2. 900 972	7. 622 057
3. 785 750	8. 152 774
4. 472 935	9. 975 861
5. 116 997	10. 869 882

**Save your backup codes**

**Done**

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



Enter a backup email address and click **Next**.



Click **Done** to finish two-factor authentication and log into NCC.



- 4 If this is the first time you have logged into NCC, the setup wizard welcome screen displays. You need to create your organization and site(s), register Nebula devices and associate them with a site. See [Chapter 2 on page 27](#) for how to use the wizard and [Chapter 7 on page 166](#) for detailed information about organization and sites.



[Exit Wizard](#)

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



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

[Let's Start](#)

## 1.3 NCC Portal Overview

The NCC portal screen is divided into these parts:

Figure 2 NCC Overview

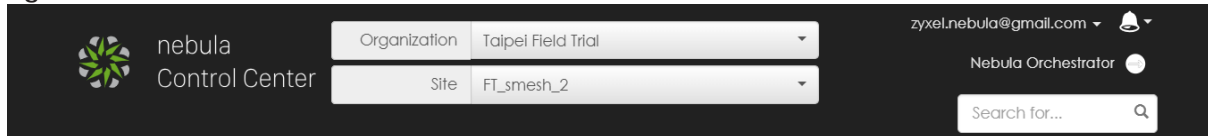


- A - Title Bar
- B - Navigation Panel
- C - Main Screen

### 1.3.1 Title Bar

Select the organization and site you want to manage. If you create multiple organizations, select **MSP Portal** from the **Organization** drop-down list box to view your organization summary. If you need to have another organization, select **Create Organization** from the **Organization** drop-down list box to create a new organization.

Figure 3 NCC Title Bar



### MSP Portal

The MSP (Managed Services Provider) Portal option allows you to view the summary of organizations when you are managing more than one organization. Click the organization entry you want to manage and go to its **SITE WIDE > Dashboard** screen.

Figure 4 NCC MSP Portal

The screenshot shows the NCC MSP Portal interface. At the top, there is a navigation bar with tabs for SITE-WIDE, AP, SWITCH, GATEWAY, ORGANIZATION (selected), and HELP. The main content area is titled 'MSP portal' and contains a search bar, a dropdown menu for '5 organizations', and a table of organizations. The table has the following columns: Status, Organization, Type, NCC License status, NCC License expiration (UTC), Sites, Devices, NAP, and NSV. The data rows are as follows:

Status	Organization	Type	NCC License status	NCC License expiration (UTC)	Sites	Devices	NAP	NSV
●	Irene	Nebula Professional Pack	ok	N/A	1	0 0 0 0 0 0 0 0	0	0
●	Pan	Nebula	expired	2018-09-27	1	0 0 0 0 2 2 0 0	0	0
●	shawn	Nebula Professional Pack	ok	2019-10-28	2	5 1 0 0 0 5 1 0	1	0
●	Taipei Field Trial	Nebula Professional Pack	ok	N/A	1	0 0 0 0 0 0 0 0	0	0
●	tpe	Nebula Professional Pack	ok	2019-02-17	4	3 2 0 0 4 9 0 0	0	0

The following table describes the labels in this screen.

Table 1 NCC MSP Portal &gt; Organization

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.
organizations	This shows the number of organizations that you can manage.
Status	This shows whether all the Nebula devices registered to a site in the organization are online (green) or have been off-line for at least six days (gray), or some of them have recently generated alerts (amber) or go off-line (red). The color is white when there is no Nebula device in the organization.
Organization	This shows the descriptive name of the organization.
Type	This shows your NCC version type.
NCC License Status	This shows whether the license is valid ( <b>ok</b> ), the license has expired and the organization downgraded from Nebula Professional Pack to Nebula ( <b>expired</b> ), or this is a Nebula free organization and NCC license is not required ( <b>N/A</b> ).
NCC License expiration (UTC)	This shows the date when the license will expire, or <b>N/A</b> when there is no Nebula device in the organization or this is a Nebula free organization and NCC license is not required.
Sites	This shows the number of sites belonging to this organization.
Devices	This shows the number of Nebula devices in this organization which are online (green), have generated alerts (amber), go off-line (red) or have been off-line for at least six days (gray).
NAP	This shows the number of Nebula APs connecting to the sites in this organization.
NSW	This shows the number of Nebula switches connecting to the sites in this organization.
NSG	This shows the number of Nebula security gateways connecting to the sites in this organization.

## License Transfer

You can transfer the license credit between organizations, which belong to the same organization creator/owner.

**Figure 5** NCC MSP Portal > License Transfer

The following table describes the labels in this screen.

**Table 2** NCC MSP Portal > License Transfer

LABEL	DESCRIPTION
From organization	Select the organization from which the license credit will be transferred.
Nebula Points	This shows the number of the selected organization's current device points for the NCC service.
Nebula Security Points	This shows the number of the selected organization's current device points for the NSS-SP service.
License Type	Select the type of the license and specify the number of points to transfer.
Add	Click this button to create a new entry for another license type.
Remove	Click this button to delete the entry for the type of license and points that you no longer want to transfer.
To organization	Select the organization to which the license credit will be transferred.
Reset	Click this button to return the screen to its last-saved settings.
OK	Click this button to save your changes.

## Create Organization

Use this screen to create an organization before you can create a site (network) in the organization and add devices to the network in order to manage them via the NCC.

**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 7.3.3 on page 173](#).

- 1 Click **Create Organization** from the **Organization** drop-down list box in the title bar. The Wizard starts. See [Chapter 2 on page 27](#) 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 organizations 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.

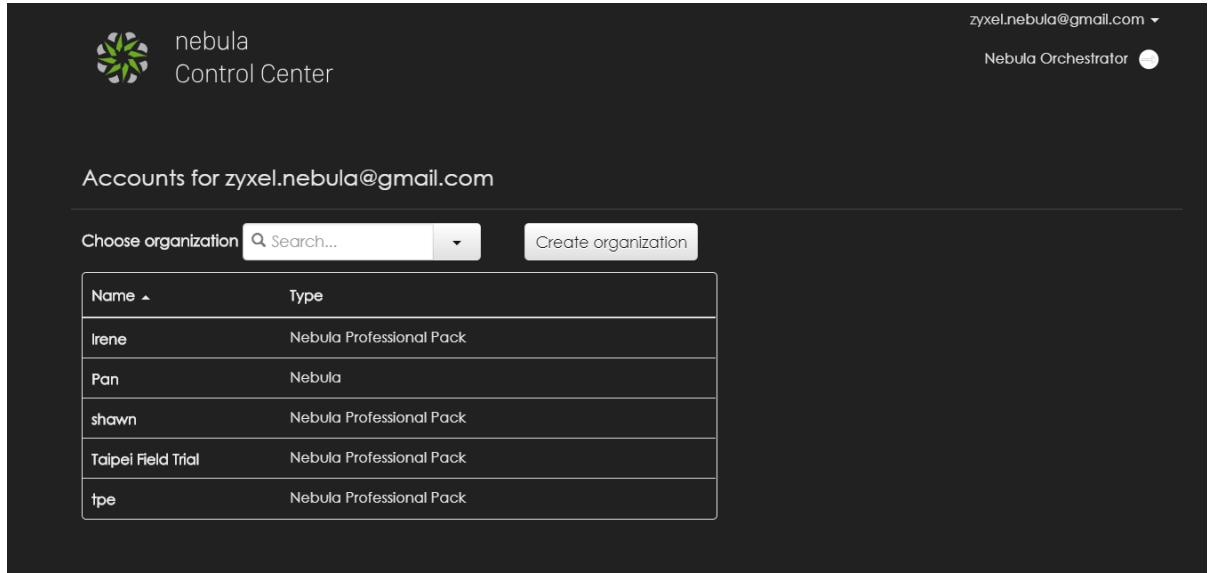
**Figure 6** Create Organization

The screenshot displays the Nebula Control Center interface. At the top left is the nebula logo and 'Control Center' text. To the right are dropdown menus for 'Organization' (set to 'Choose an Organization') and 'Site'. Further right is the user email 'zyxel.nebula@gmail.com' and 'Nebula Orchestrator' status. A search bar is also present. Below the navigation bar, the 'ORGANIZATION' tab is active. The 'Create Organization' wizard is shown with two input fields: 'Organization name:' and 'Copy setting from:' (set to '(None)'). A warning message is displayed: 'Clone a new organization from one of your existing organization. Organization-wide settings for your new organization will be copied from the one you specify. ⚠ This operation cannot be undone.' A 'Create organization' button is located at the bottom of the form.

## Choose Organization

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

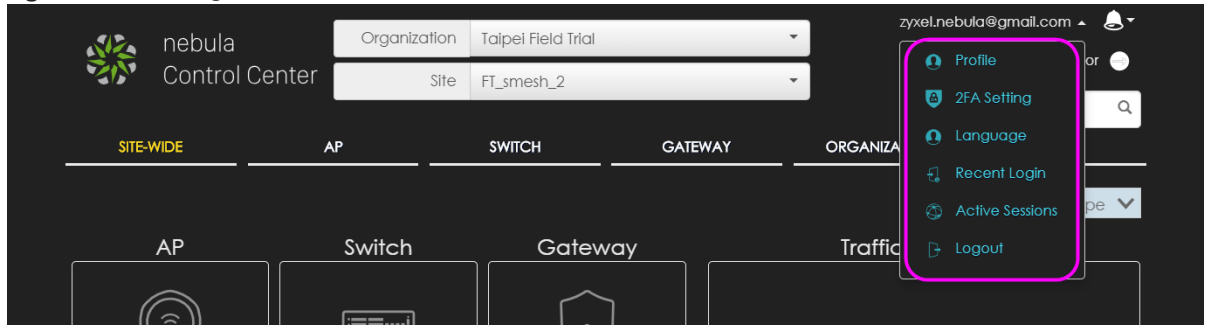
Figure 7 Choose Organization



## Login Account

Click your login account at the top right hand corner of the screen to display a menu, where you can click a link to view your account profile settings, open a screen which shows how to change your two-factor authentication settings, login history and active sessions, select the language you prefer, or log out of the NCC portal.

Figure 8 NCC Login Account



## Alert

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

Figure 9 NCC Alert



## 1.3.2 Navigation Panel

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

Table 3 NCC Menu Summary

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
SITE-WIDE		Use these menus to view information on all Nebula managed devices that are deployed in the selected site.
	Monitor	
	Dashboard	Use this menu to view device connection status and traffic summary.
	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.
	Map & Floor Plan	Use this menu to locate devices on the world map and even on a floor plan.
	Topology	Use this menu to view the site's network topology.
	Configure	
	General Setting	Use this menu to change the general settings for the site, such as the site name, device login password and firmware upgrade schedule.
	Alert Setting	Use this menu to set which alerts are created and emailed or sent by the Zyxel Nebula Mobile app. You can also set the email address(es) to which an alert is sent.
	Add Device	Use this menu to register a device and add it to the site.
	Firmware Management	Use this menu to schedule firmware upgrades.
	AP	
Monitor		
Access Point		Use this menu to view the list of APs added to the site.
Client		Use this menu to view WiFi clients which are connecting to the APs in the site.
Event Log		Use this menu to view all events on the AP. An event is a log of something that has happened to a managed device.
Summary Report		Use this menu to view network statistics specific to APs in the site.
Configure		
SSIDs		Use this menu to enable and configure basic settings for SSID profiles.
SSID Schedule		Use this menu to set whether the SSID is enabled or disabled on each day of the week.
Authentication		Use this menu to configure WiFi security, L2 isolation, intra-BSS and walled garden settings for SSID profiles.
Captive Portal		Use this menu to configure captive portal settings for SSID profiles.
Radio Setting		Use this menu to configure global radio settings for all APs in the site.
Client Steering		Use this menu to configure load balancing settings and enable smart clients steering for all APs in the site.
Port Setting		Use this menu to enable or disable a port on the managed AP and configure the port's VLAN settings.

Table 3 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
SWITCH		Use these menus to monitor and configure the managed switch(es) by the NCC.  The settings are applied when a Nebula switch is registered and attached to the selected site.
	Monitor	
	Switch	Use this menu to view the list of switches added to the site.
	Client	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 a log of something that has happened to a managed device.
	IPTV Report	Use this menu to view available IPTV channels and client information.
	Summary Report	Use this menu to view network statistics specific to switches in the site.
	Configure	
	Switch Ports	Use this menu to view the switch port statistics and configure switch settings for the ports.
	IP filtering	Use this menu to configure the access control list in order to control access to the switches.
	Advanced IGMP	Use this menu to enable and configure IGMP snooping and create IGMP filtering profiles.
	RADIUS Policy	Use this menu to configure port authentication.
	PoE Schedule	Use this menu to set the schedule for switches in distributing power to powered devices.
Switch Configuration	Use this menu to configure global switch settings, such as (R)STP, QoS, port mirroring, authentication servers, voice VLAN and DHCP white list.	



Table 3 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
GATEWAY		Use these menus to monitor and configure the managed security gateway(s) 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 a security gateway in the selected site.
	Client	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 a log of something that has happened to a managed device.
	VPN Connection	Use this menu to view status of the site-to-site VPN connections.
	NSS Analysis	Use this menu to view the statistics report for NSS (Nebula Security Service).
	Summary Report	Use this menu to view network statistics specific to the gateway in the site.
	Configure	
	Interfaces Addressing	Use this menu to configure network mode, port grouping, interface address, static route and DDNS settings on the gateway.
	Firewall	Use this menu to configure firewall rules for outbound traffic, application patrol, schedule profiles and port forwarding rules for inbound traffic.
	Policy Route	Use this menu to view and configure policy routes.
	Content Filtering	Use this menu to enable content filtering and block access to specific web sites.
	Site-to-Site VPN	Use this menu to configure VPN rules.
	L2TP over IPSec Client	Use this menu to enable and configure L2TP VPN settings.
	Network Access Method	Use this menu to enable or disable web authentication on an interface.
	Walled Garden	Use this menu to configure walled garden web site links,
	Captive Portal	Use this menu to configure captive portal settings for each gateway interface.
	Traffic Shaping	Use this menu to configure the maximum bandwidth and load balancing.
	Security Filtering	Use this menu to enable or disable Intrusion Detection and Prevention (IDP) on the security gateway.
	Network Servers	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.

Table 3 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
ORGANIZATION	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	
	Create Site	Use this menu to create a new site.
	Inventory	Use this menu to view the summary of devices which have been registered and assigned to the sites in the selected organization.
	License Management	Use this menu to view and manage your licenses.
	Setting	Use this menu to configure the security settings or delete the organization.
	Administrator	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 which are allowed access to the Nebula devices via different authentication methods, such as the MAC-based authentication, captive portal or the IEEE 802.1x authentication method.
	VPN Members	Use this menu to view and manage the VPN members in the organization.
	Configuration Management	Use this menu to synchronize the configuration between sites or switch ports and back up or restore a configuration file.
HELP	Support Forum	Use this menu to go to Zyxel Nebula Forum, where you can get the latest Nebula information and have conversations with other people by posting your messages.
	Support Request	Use this menu to view or submit a new eITS ticket.
	Online Documentation	Use this menu to view the documentation for the NCC and Nebula devices.
	Firewall Info	Use this menu to view information required for firewall rules to allow management traffic between the NCC and Nebula devices, such as the port number and protocol type.
	Data Policy	Use this menu to view NCC legal documents, such as the privacy policy, terms of use and data processing agreement.
	License Calculator	Use this menu to specify the number of Nebula devices and a time period to determine the license credit (device points) you should get for the NCC service within a specific time frame.

# CHAPTER 2

## Setup Wizard

### 2.1 Accessing the 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.

### 2.2 Using the Wizard

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

[Exit Wizard](#)

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



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

**Let's Start**

#### 2.2.1 Step 1 Create an organization and site

Enter a descriptive name for your organization and site. Select the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). Click **Next** to continue the wizard.

**01** \_\_\_\_\_

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.

[Exit Wizard](#)

### First step is to create your Organization and Site

Organization

Site

Country  
Taiwan

Timezone  
Asia - Taipei(UTC +8.0)


Next

## 2.2.2 Step 2 Add your devices

Enter a device's MAC address and serial number, then click the + **Add** button to register and add it to the site. You can register multiple devices at a time. Click **Next** to proceed. You can also leave the fields blank and click **Next** to move on to the next step without adding a device.

\_\_\_\_\_ **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 → [XXXXXXXXXXXXXX]  
MAC address → [XXXXXXXXXXXXXX]

[Exit Wizard](#)

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

MAC Address

Serial Number

+ Add

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

Back

Next

## 2.2.3 Step 3 Set up your WiFi network

Configure the WiFi settings for the managed APs. Enter the WiFi network name (SSID) and the WiFi password. Configure the ID number of the VLAN to which the SSID belongs. Click **Next** to proceed. You can also leave the fields blank and click **Next** to move on to the next step without setting up the main WiFi network.

[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.

You might just click Next to skip this step.

### Let's get your WiFi set up

WiFi Name (SSID)

Password (Pre-Shared Key)

VLAN

1

Back Next

## 2.2.4 Step 4 Set up a Guest WiFi network

Configure WiFi and VLAN settings for guest users. 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. Click **Next** to proceed. You can also leave the fields blank and click **Next** to move on to the next step without setting up the guest WiFi network.

**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.

You might just click Next to skip this step.

### Need to set up a Guest WiFi? [Exit Wizard](#)

How do you prefer guests 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


Back
Next

## 2.2.5 Summary

A summary of the wizard configuration will display. You can click a section's gray edit icon (✎) to modify its setting. If you want to save your changes click **Go to Nebula Dashboard**; 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 ✎


**Org123**

Site **SiteA**

---


Nebula Devices ✎

**0 Devices** >



WiFi Name (SSID) ✎

WiFi Password



Guest WiFi Name (SSID) ✎

Guest WiFi Password

Authentication

Go to Nebula Dashboard

---

# PART II

## Technical Reference

---

# CHAPTER 3

## Site-Wide

### 3.1 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.

#### 3.1.1 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.

The screen varies depending on what you select in the **Display** field. It shows the status and information for all types of Nebula devices connected to the selected site by default. You can also select to only show information for APs in the site.

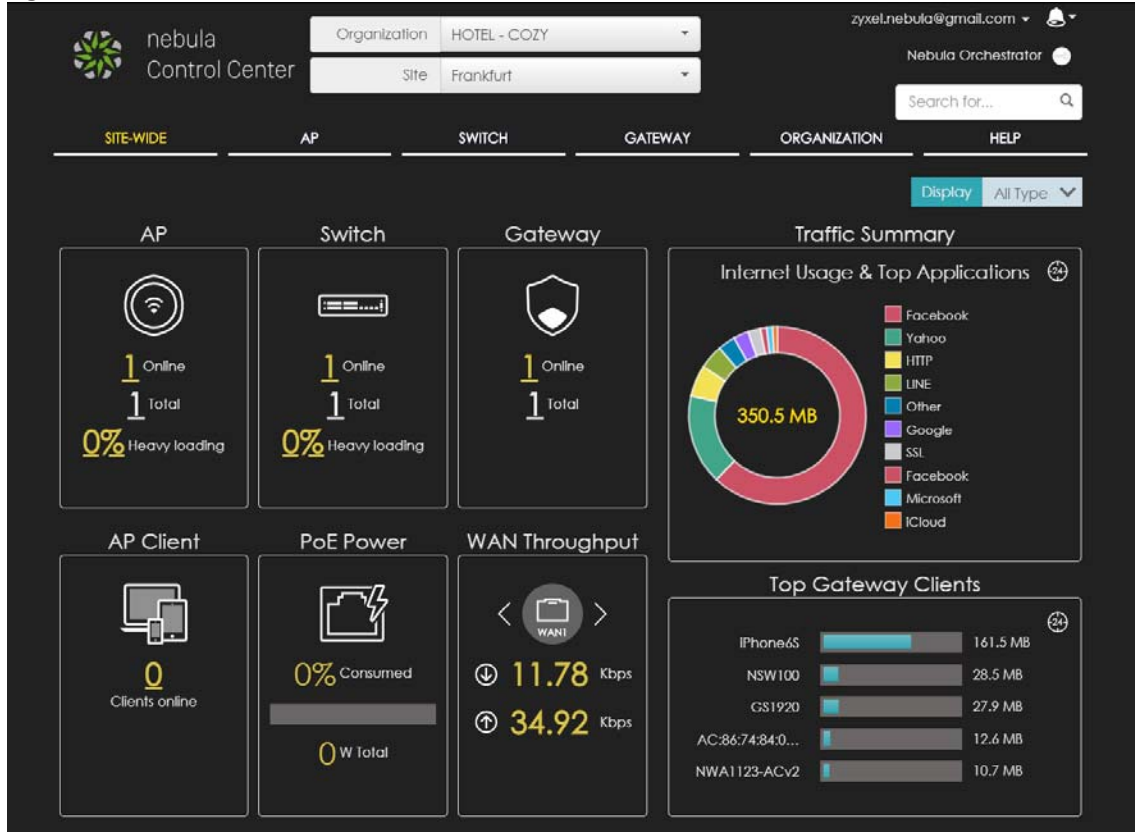
#### Display: All Type

The screen allows you to view:

- **AP:** 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,
- **AP Client:** how many WiFi clients are currently connecting to the managed AP(s),
- **Switch:** 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:** 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 both of them are active, use the arrow to switch and view the throughput of each WAN interface.
- **Traffic Summary:** the Internet usage and top ten applications in the past 24 hours,
- **Top Gateway Clients:** the top five clients of the Nebula security gateway with the highest percentage of bandwidth usage in the past 24 hours.



Figure 10 Site-Wide &gt; Monitor &gt; Dashboard: All Type

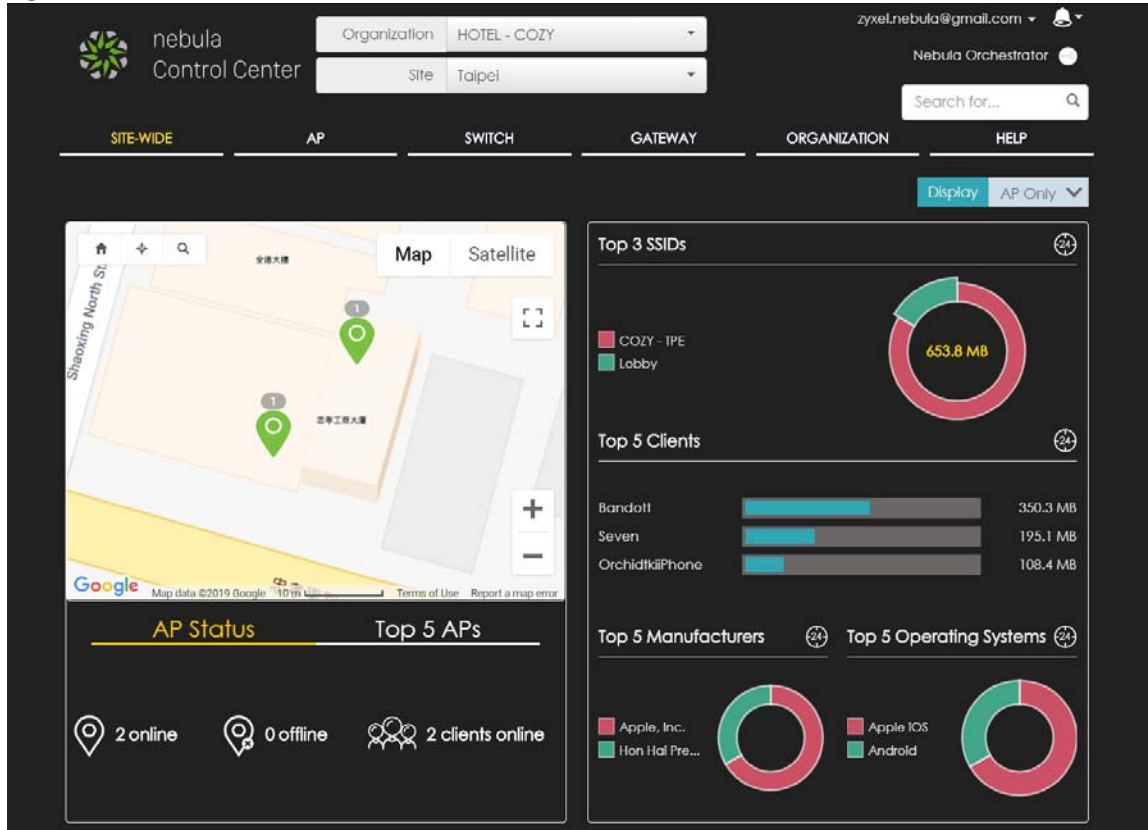


## Display: AP Only

The screen allows you to view:

- **AP Status:** the total number of online/offline APs in the site, and how many WiFi clients are currently connecting to the managed AP(s).
- **Top 5 APs:** the top five managed AP(s) with the highest number of WiFi clients or the highest percentage of bandwidth usage in the past 24 hours. You can click an AP's name to go to the **AP > Monitor > Access Point: AP Details** screen.
- **Top 3 SSIDs:** the top three SSIDs with the highest percentage of bandwidth usage in the past 24 hours. You can click a client's name to go to the **AP > Monitor > Summary Report** screen.
- **Top 5 Clients:** 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 **AP > Monitor > Client: Client Details** screen.
- **Top 5 Manufacturers:** the top five manufacturers of WiFi client devices in the past 24 hours. You can click a manufacturer name to go to the **AP > Monitor > Client** screen and view the client devices which are made by the manufacturer.
- **Top 5 Operating Systems:** 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 **AP > Monitor > Client** screen and view the client devices which use this operating system.

Figure 11 Site-Wide &gt; Monitor &gt; Dashboard: AP Only

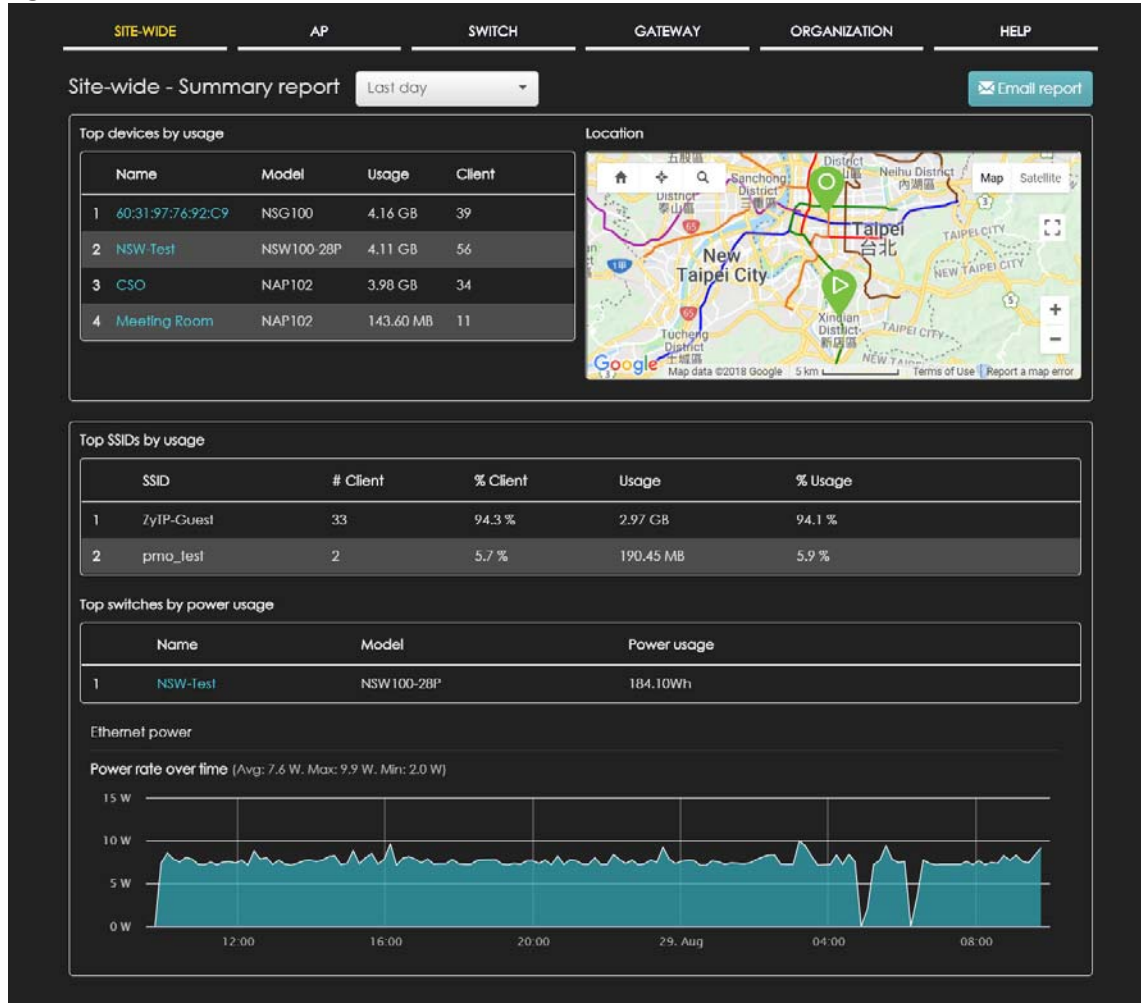


### 3.1.2 Summary Report

This screen displays network statistics for the selected site, such as bandwidth usage, power usage, top devices, top clients and/or top SSIDs.

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

Figure 12 Site-Wide > Monitor > Summary Report



The following table describes the labels in this screen.

Table 4 Site-Wide > Monitor > Summary Report

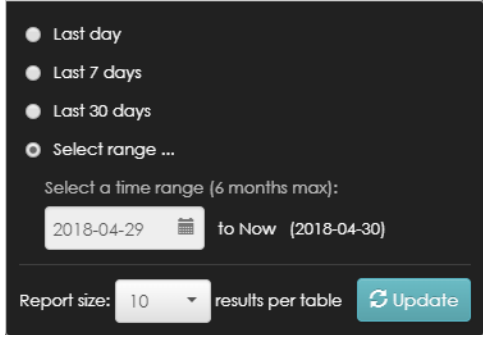
LABEL	DESCRIPTION
Summary Report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Select range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
Top devices by usage	

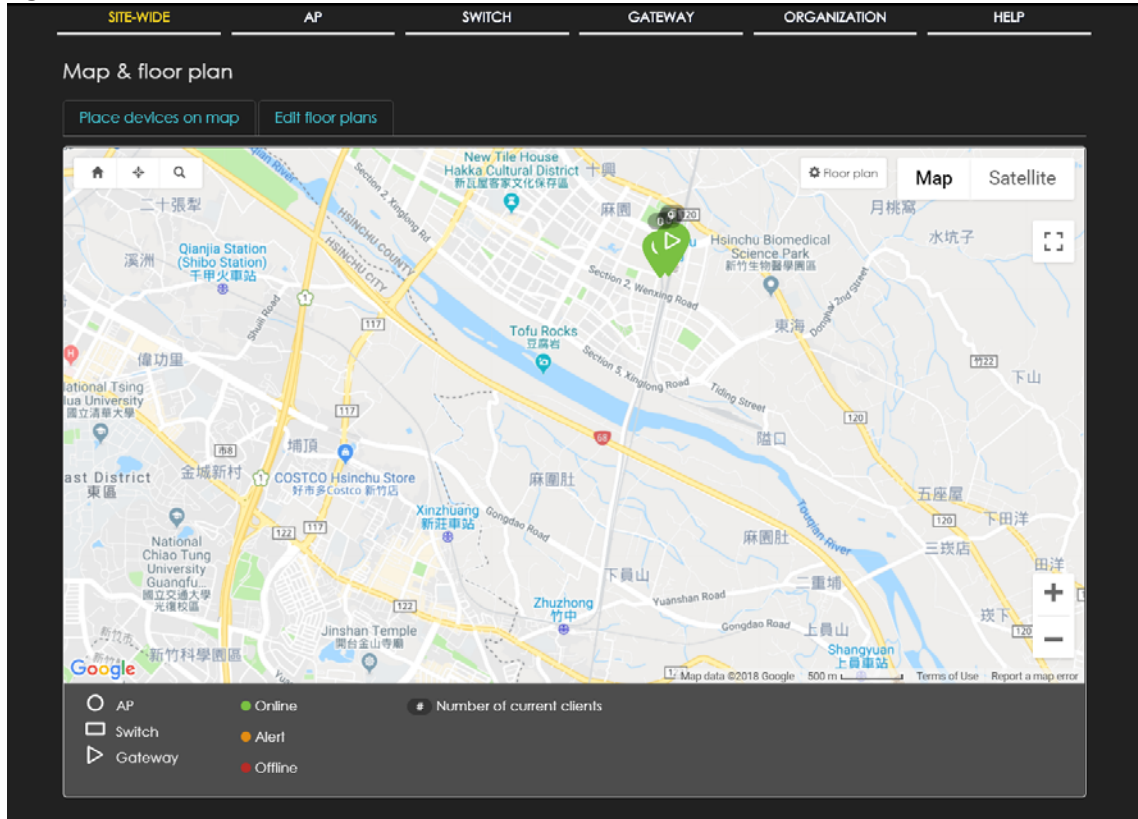
Table 4 Site-Wide &gt; Monitor &gt; Summary Report (continued)

LABEL	DESCRIPTION
#	This shows the index number of the Nebula device.
Name	This shows the descriptive name of the Nebula device.
Model	This shows the model number of the Nebula device.
Usage	This shows the amount of data transmitted or received by the Nebula device.
Client	This shows how many clients are currently connecting to the Nebula device.
Location	This shows the location of the top Nebula devices on the map.
Top SSIDs by usage	
#	This shows the index number of the SSID.
SSID	This shows the SSID network name.
# Clients	This shows how many WiFi clients are connecting to this SSID.
% Clients	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 what percentage of the transmitted data is for this SSID.
Top switches by power usage	
#	This shows the index number of the switch.
Name	This shows the descriptive name of the switch.
Model	This shows the model number of the switch.
Power usage	This shows the switch's energy consumption in watt-hour (Wh).
Ethernet power	
Power rate over time	This shows the average, maximum and minimum power consumption of the switches.
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.

### 3.1.3 Map & Floor Plan

This screen allows you to locate a device on the world map and use a floor plan to show the space and relationship between the Nebula devices. Click **Site-Wide > Monitor > Map & floor plan** to access this screen.

Figure 13 Site-Wide &gt; Monitor &gt; Map &amp; Floor Plan



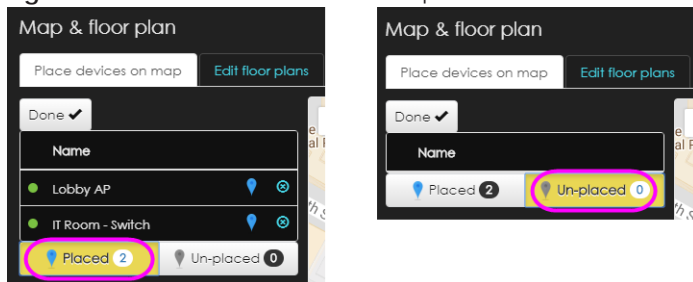
## Place devices on map

You can mark spots on the map, that is, the places where the devices are located. Click the **Place devices on map** tab to display the device list for the selected site. Click **Done** to hide the device 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 blue (📍) 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 14 Site-Wide &gt; Monitor &gt; Map &amp; Floor Plan: Place devices on map

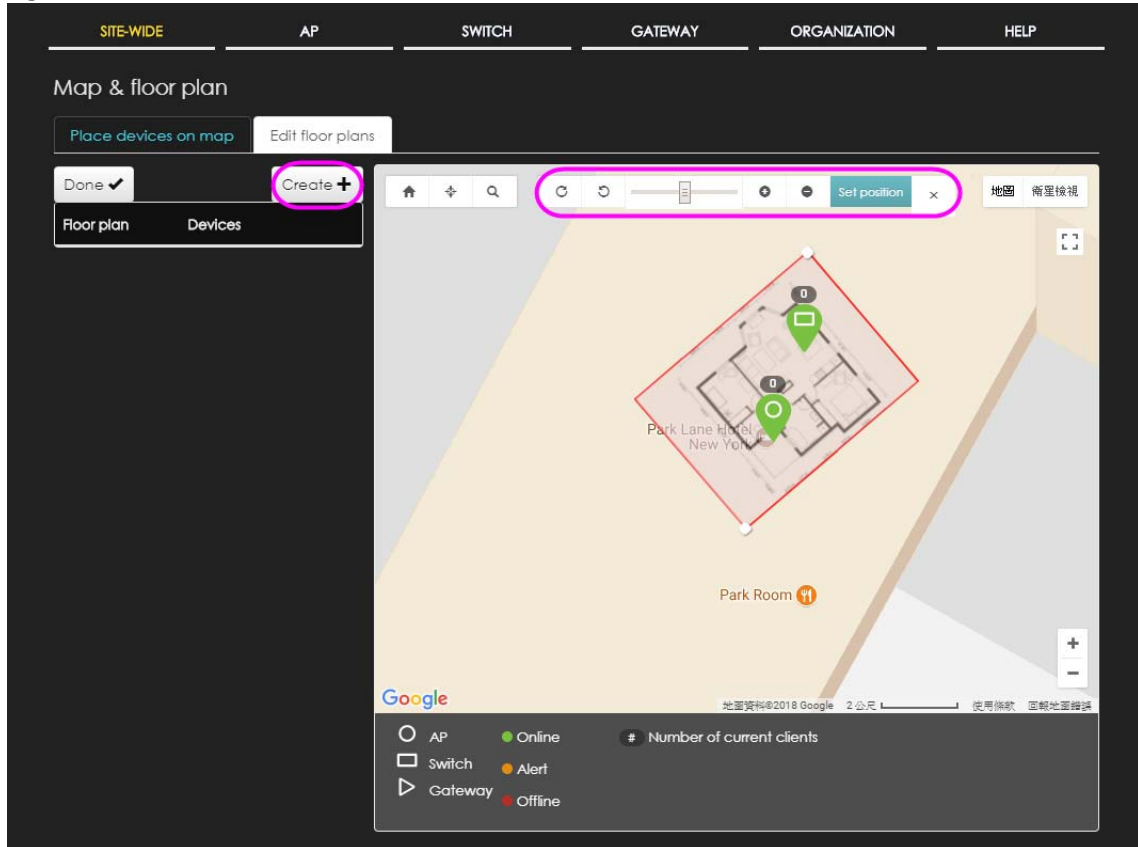


## Edit floor plans

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 **Done** to hide the list. Use the **Create+** button to upload new floor plans.

Select a floor plan from the list. 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.

**Figure 15** Site-Wide > Monitor > Map & Floor Plan: Edit floor plans



The following table describes the labels in this screen.

**Table 5** Site-Wide > Monitor > Map & Floor Plan: Edit floor plans

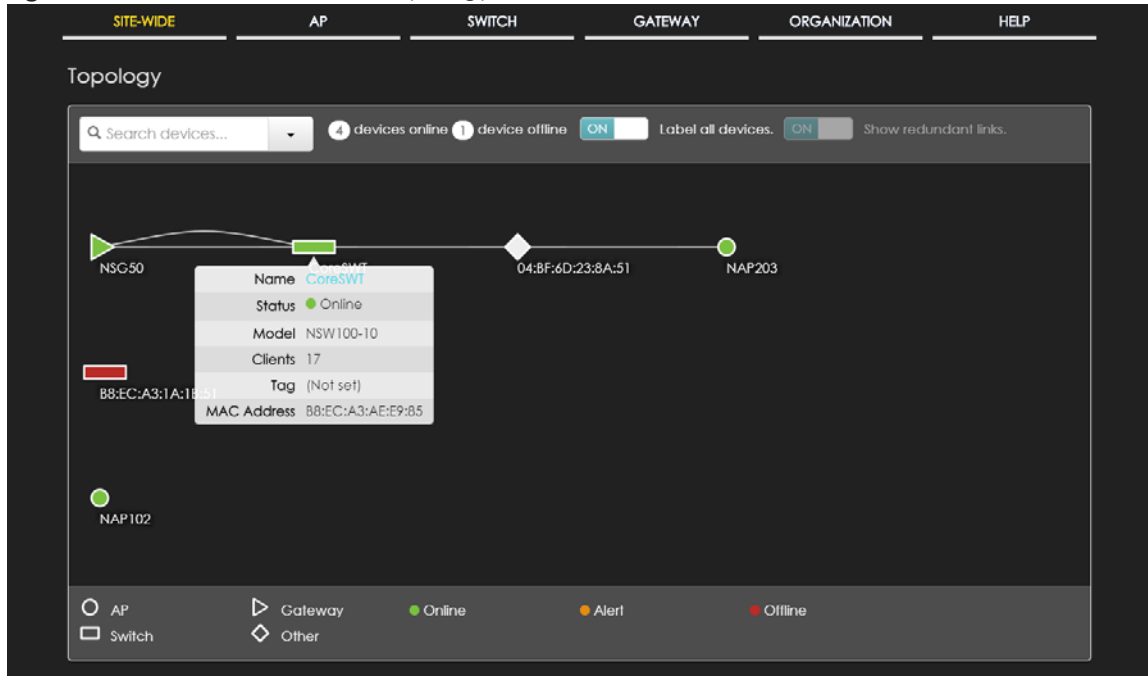
LABEL	DESCRIPTION
Floor plan	This shows the descriptive name of the floor plan.
Devices	This shows the number of the device(s) marked on this floor plan.
Edit	Click this icon to open a screen, where you can modify the name, address and/or dimension of the floor plan.
Remove	Click this icon to delete the floor plan.

### 3.1.4 Topology

Use this screen to view the network topology of the site. Click **Site-Wide > Monitor > Topology** to access this screen.

The shape of a node in the network topology indicates its device type and the color shows whether the device is online (green), has generated alerts (amber), or goes offline (red). Click a node to view detailed device information, such as its name, model number, number of connected clients, and MAC address.

Figure 16 Site-Wide > Monitor > Topology



## 3.2 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.

### 3.2.1 General Setting

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 Setting** to access this screen.

Figure 17 Site-Wide &gt; Configure &gt; General setting

SITE-WIDE
AP
SWITCH
GATEWAY
ORGANIZATION
HELP

### General setting

#### Site information

Site name

Local time zone

#### Device configuration

Local credentials

Username:

Password:  [Show password](#)

Password must be at least 8 characters in length and consists of letters and numerals. The valid characters are letters, numerals and symbols as follow: ! @ # \$ % ^ & \* ( ) \_ + ' - = { } ; : < > . /

AP LED lights

AP Smart Mesh BETA  [Model list](#)

#### Captive portal reauthentication

For my AD server users

For my RADIUS server users

For click-to-continue users

For cloud authentication users

#### SNMP

SNMP access

#### Reporting

Syslog server

Server IP	Types	Action
<input type="text" value="10.1.7.123"/>	<input type="text" value="Gateway log"/> <a href="#">+</a>	<a href="#">-</a>
<input type="text" value="10.0.1.2"/>	<input type="text" value="Gateway log"/> <a href="#">+</a>	<a href="#">-</a>

[+ Add](#)
Items have reached the maximum number (2)

#### Firmware upgrades

NEW New way to manage your device(s) firmware. Check [here](#) to try it.

Upgrade time   [What is this?](#)

Access point upgrade

New firmware is available for this site.  
The upgrade is scheduled for 2018-12-31 00:00 UTC +8.0.  
Last upgraded on 2018-11-16 14:47 UTC +8.0.

- Upgrade as scheduled
- Reschedule the upgrade to   UTC +8.0
- Perform the upgrade now

Switch upgrade

The switches in this site are configured to run the latest available firmware.

- Follow upgrade time
- Schedule the upgrade to   UTC +8.0
- Perform the upgrade now

Gateway upgrade

Last upgraded on 2018-12-11 10:51 UTC +8.0.  
The gateways in this site are configured to run the latest available firmware.

- Follow upgrade time
- Schedule the upgrade to   UTC +8.0
- Perform the upgrade now



The following table describes the labels in this screen.

Table 6 Site-Wide > Configure > General setting

LABEL	DESCRIPTION
Site Information	
Site name	Enter a descriptive name for the site.
Local time zone	Choose the time zone of the site's location.
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.
AP LED lights	Click to turn on or off the LED(s) on the APs.
AP Smart Mesh	Click to turn on or off the Nebula Smart Mesh feature on the APs.  When Nebula Mesh is enabled, wireless mesh links between managed APs are created automatically. When an AP fails to connect to the gateway in the site through a wired Ethernet connection, it acts as a repeater and wirelessly connects to an available root AP to get configuration updates. The root AP is an AP that can transmit and receive data from the gateway via a wired Ethernet connection.  Click <b>Model list</b> to see whether your AP supports the Nebula Smart Mesh feature at the time of writing.
Captive portal reauthentication	
For my AD server users	Select how often the user (authenticated by an AD server) has to log in again.
For my RADIUS server users	Select how often the user (authenticated by an RADIUS server) has to log in again.
For click-to-continue users	Select how often the user (authenticated via 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.
Action	Click the <b>Delete</b> icon to remove the entry.
Firmware upgrades	
Upgrade time	Select the day of the week and time of the day to install the firmware.
Access point upgrade	This section is grayed out if there is no AP in this site. It shows if there is a new version of the firmware available for the APs, and the date and time of the last firmware upgrade.  Select <b>Follow upgrade time</b> to install the firmware at the time you choose in the <b>Upgrade time</b> field.  Select <b>Schedule the upgrade to xx</b> to set a new schedule for the firmware upgrade.  Select <b>Perform the upgrade now</b> to install the firmware immediately.

Table 6 Site-Wide &gt; Configure &gt; General setting (continued)

LABEL	DESCRIPTION
Switch upgrade	<p>This section is grayed out if there is no switch in this site. It shows if there is a new version of the firmware available for the switches, and the date and time of the last firmware upgrade.</p> <p>Select <b>Follow upgrade time</b> to install the firmware at the time you choose in the <b>Upgrade time</b> field.</p> <p>Select <b>Schedule the upgrade to xx</b> to set a new schedule for the firmware upgrade.</p> <p>Select <b>Perform the upgrade now</b> to install the firmware immediately.</p>
Gateway upgrade	<p>This section is grayed out if there is no gateway in this site. It shows if there is a new version of the firmware available for the gateways, and the date and time of the last firmware upgrade.</p> <p>Select <b>Follow upgrade time</b> to install the firmware at the time you choose in the <b>Upgrade time</b> field.</p> <p>Select <b>Schedule the upgrade to xx</b> to set a new schedule for the firmware upgrade.</p> <p>Select <b>Perform the upgrade now</b> to install the firmware immediately.</p>

### 3.2.2 Alert Setting

Use this screen to set which alerts are created and emailed. You can also set the email address(es) to which an alert is sent. Click **Site-Wide > Configure > Alert Setting** to access this screen.

Figure 18 Site-Wide &gt; Configure &gt; Alert setting

The screenshot shows the 'Alert setting' configuration page. At the top, there are navigation tabs: SITE-WIDE (selected), AP, SWITCH, GATEWAY, ORGANIZATION, and HELP. The main content area is titled 'Alert setting' and contains the following sections:

- Send alerts via email to:**
  - All site administrators:** A toggle switch is set to 'ON'.
  - Custom email addresses:** A text input field containing 'E.g. nebula@zyxel.com'.
- Alert types:** A table with columns for the alert type, a time delay (in minutes), and checkboxes for 'Email' and 'In-app push notifications'.
 

Alert types	Time	Event	Email	In-app push notifications
Wireless alerts	60 minutes	after AP goes offline	<input type="checkbox"/>	<input type="checkbox"/>
Switch alerts	60 minutes	after switch goes offline	<input type="checkbox"/>	<input type="checkbox"/>
	60 minutes	Any switch port goes down	<input type="checkbox"/>	<input type="checkbox"/>
Security gateway alerts	60 minutes	after the gateway goes offline	<input type="checkbox"/>	<input type="checkbox"/>
		Any DHCP lease pool is exhausted	<input type="checkbox"/>	
		A VPN connection is established or disconnected	<input type="checkbox"/>	
		WAN connectivity status changed	<input type="checkbox"/>	
Other alerts		Configuration settings are changed	<input type="checkbox"/>	

The following table describes the labels in this screen.

Table 7 Site-Wide > Configure > Alert setting

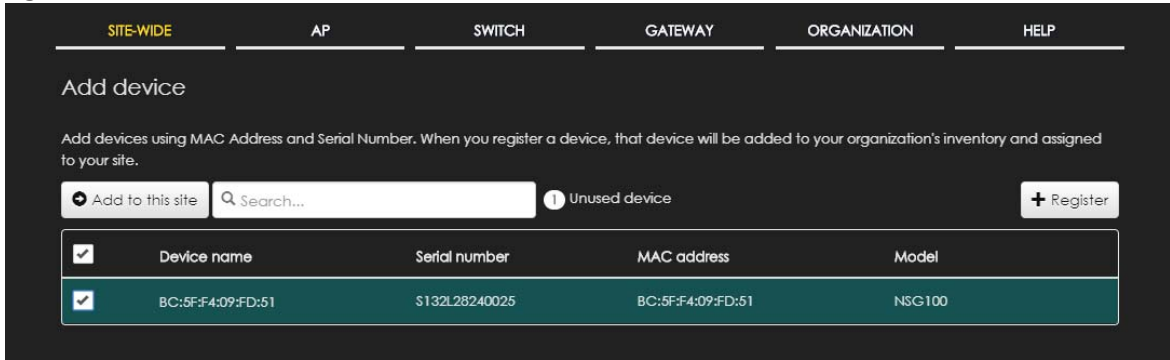
LABEL	DESCRIPTION
Send alerts via email to	
All site administrators	Click <b>On</b> to send alerts to all site administrators in the selected site.
Custom email addresses	Enter the email address(es) to which you want to send alerts.
Alert types	
Wireless alerts	<p>Select the check box to have the NCC generate and send an alert by email (<b>Email</b>) and/or have the Zyxel Nebula Mobile app send notifications (<b>In-app push notifications</b>) when the event occurs.</p> <p>If you select <b>In-app push notifications</b>, you can use the Zyxel Nebula Mobile app to decide whether the smart phone should receive or ignore notifications.</p> <p>You can also specify how long in minutes the NCC waits before generating and sending an alert when an AP becomes off-line.</p>
Switch alerts	<p>Select the check box to have the NCC generate and send an alert by email (<b>Email</b>) and/or have the Zyxel Nebula Mobile app send notifications (<b>In-app push notifications</b>) when the event occurs.</p> <p>If you select <b>In-app push notifications</b>, you can use the Zyxel Nebula Mobile app to decide whether the smart phone should receive or ignore notifications.</p> <p>You can also specify how long in minutes the NCC waits before generating and sending an alert when a port or a switch goes down.</p>
Security gateway alerts	<p>Select the check box to have the NCC generate and send an alert by email (<b>Email</b>) and/or have the Zyxel Nebula Mobile app send notifications (<b>In-app push notifications</b>) when the event occurs.</p> <p>If you select <b>In-app push notifications</b>, you can use the Zyxel Nebula Mobile app to decide whether the smart phone should receive or ignore notifications.</p> <p>You can also specify how long in minutes the NCC waits before generating and sending an alert when a gateway becomes off-line.</p>
Other alerts	Select the check box to have the NCC generate and send an alert by email when the event occurs.

### 3.2.3 Add Device

Use this screen to register a device and add it to the site. Click **Site-Wide > Configure > Add device** 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 7.3.3 on page 173](#).

Figure 19 Site-Wide > Configure > Add device



The following table describes the labels in this screen.

Table 8 Site-Wide > Configure > Add device

LABEL	DESCRIPTION								
Add to this site	Click this button to assign the selected device(s) to the site.								
Unused device	This shows the number of registered devices which have not been assigned to a site.								
+ Register	<p>This button is available only for an organization administrator or site administrator that has full access.</p> <p>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.</p> <p>You can click <b>template</b> in the pop-up window to download the template (an example Excel file), add device information in the Excel file, and then click <b>import</b> to register multiple devices quickly by importing the Excel file.</p> <div data-bbox="537 1039 1393 1583" style="border: 1px solid black; padding: 5px;"> <p>Register by MAC address and serial number <span style="float: right;">×</span></p> <p>Enter one or more MAC address and serial number. Or you can download the <a href="#">template</a> here and <a href="#">import</a> multiple records for faster registration.</p> <p><a href="#">Where can I find these numbers?</a> <a href="#">What do I enter here?</a></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 25%;">MAC address</th> <th style="width: 25%;">Serial Number</th> <th style="width: 25%;">Model</th> <th style="width: 25%;">License</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td></td> <td style="text-align: right;"></td> </tr> </tbody> </table> <p><a href="#">+ Register another device</a></p> <p style="color: red; font-size: small;">Registered device will be added to Organization Creator account in myZyxel.com.</p> <p><input type="checkbox"/> Acknowledge</p> <p style="text-align: right;"><a href="#">Close</a> <a href="#">OK</a></p> </div>	MAC address	Serial Number	Model	License	<input type="text"/>	<input type="text"/>		
MAC address	Serial Number	Model	License						
<input type="text"/>	<input type="text"/>								
	Select the check box of the device that you want to add to the selected site.								
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.								

## 3.2.4 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 even create a schedule for a specific device. Click **Site-Wide > Configure > Firmware management** to access this screen.

**Figure 20** Site-Wide > Configure > Firmware management

The screenshot displays the 'Firmware management' configuration page. At the top, there are navigation tabs: SITE-WIDE (selected), AP, SWITCH, GATEWAY, ORGANIZATION, and HELP. The main content area is titled 'Firmware management' and contains the following sections:

- Upgrade time:** A dropdown menu set to 'Sunday' and a time selector set to '12am'. A link 'What is this?' is present.
- All APs:** A toggle switch is turned 'ON'. The upgrade date is '2019-03-31' and the time is '00:00'. The time zone is 'UTC +8.0'. Below this, it says 'You can reschedule upgrade time as you wish.'
- All Switches:** A toggle switch is turned 'OFF'. The upgrade date is '2018-12-17' and the time is '00:00'. The time zone is 'UTC +8.0'. Below this, it says 'You can reschedule upgrade time as you wish.'
- Security Gateway:** A toggle switch is turned 'OFF'. The upgrade date is '2018-12-17' and the time is '00:00'. The time zone is 'UTC +8.0'. Below this, it says 'The gateway in this site are using the latest available firmware.'

Below these settings, there is a section titled 'Manage firmware by site? Please go to [General setting.](#)' with a table of filters:

Status	Device Type	Tag	Model	Current Version	Firmware Status	Locked
Any	Any	Any	Any	Any	Any	Any

Below the filters, there are two buttons: 'Upgrade Now' and '+ Schedule upgrade'. To the right of the buttons, it says '0 of devices selected'.

The main table below has the following columns: Status, Device type, Model, MAC, S/N, Current version, Firmware status, and a date. The table contains four rows of device information:

Status	Device type	Model	MAC	S/N	Current version	Firmware status	Date
Green dot	Access point	NAP102	58:8B:F3:90:F6:3E	S152Z36000075	V4.30(ABDF.0)IT_20181212140919	Custom	2019-03-31
Green dot	Access point	NWA1123-AC PRO	60:31:97:73:BB:07	S162L21141437	V4.30(ABHD.0)IT_20181212140409	Custom	2019-03-31
Red dot	Access point	NWA1123-AC HD	5C:E2:8C:7D:9D:AE	S172V43004112	V5.46(ABIN.0)b5-2018-12-06	Custom	2019-03-31
Green dot	Switch	NSW100-28P	60:31:97:77:82:66	S162L23002094	V2.00(ABBT.3)   09/28/2017	Upgrade available	Follow upg

At the bottom of the page, there are 'Save' and 'Cancel' buttons. Below the buttons, it says '(Please allow 1-2 minutes for changes to take effect.)'

The following table describes the labels in this screen.

Table 9 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> .
Security Gateway	This section is grayed out if there is no gateway 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> .
Status/Device Type/ Tag/Model/Current Version/Firmware Status/Locked	Specify your desired filter criteria to filter the list of devices.
Upgrade Now	Click this to immediately install the firmware on the selected device(s).
Schedule Upgrade	Click this to create a new schedule for the selected device(s).
Status	This shows whether the device is online (green), has generated alerts (amber), or goes off-line during the past day (red) or has been off-line for at least one week (gray).
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.
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> to follow the site-wide schedule or <b>No</b> when the firmware on the device is up-to-date.  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.

Table 9 Site-Wide > Configure > Firmware management (continued)

LABEL	DESCRIPTION
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.

# CHAPTER 4

## AP

### 4.1 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.

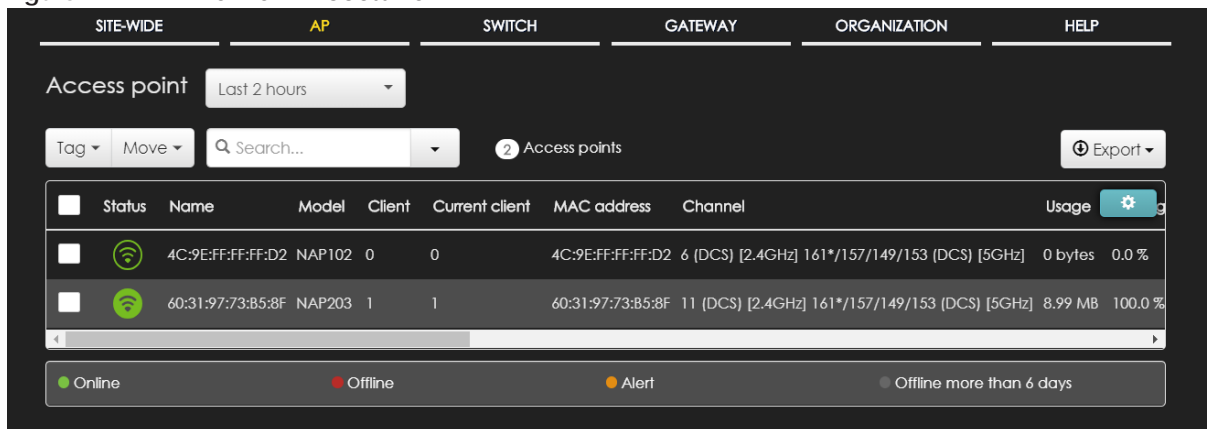
### 4.2 Monitor

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

#### 4.2.1 Access Point

This screen allows you to view the detailed information about an AP in the selected site. Click **AP > Monitor > Access Point** to access this screen.

Figure 21 AP > Monitor > Access Point



Status	Name	Model	Client	Current client	MAC address	Channel	Usage
Online	4C:9E:FF:FF:D2	NAP102	0	0	4C:9E:FF:FF:D2	6 (DCS) [2.4GHz] 161*/157/149/153 (DCS) [5GHz]	0 bytes 0.0 %
Online	60:31:97:73:B5:8F	NAP203	1	1	60:31:97:73:B5:8F	11 (DCS) [2.4GHz] 161*/157/149/153 (DCS) [5GHz]	8.99 MB 100.0 %

Legend: Online (green dot), Offline (red dot), Alert (orange dot), Offline more than 4 days (grey dot)



The following table describes the labels in this screen.

Table 10 AP &gt; Monitor &gt; Access Point



LABEL	DESCRIPTION
Access point	Select to view device information and connection status in the past two hours, day, week or month.
Tag	Select one or multiple APs and click this button to create a new tag for the AP(s) 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 LED(s) (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 AP(s) to another site or remove the AP(s) from the current site.
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	This shows whether the AP is online (green), acts as a repeater (  ) , has generated alerts (amber), goes off-line (red), or has been off-line for at least six days (gray). 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.
Name	This shows the descriptive name of the AP.
LAN IP	This shows the local (LAN) IP address of the AP.
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.
Usage	This shows the amount of data consumed by the AP's clients.
% Usage	This shows the percentage of the AP's data usage.
Tag	This shows the user-specified tag for the AP.
Serial Number	This shows the serial number of the AP.
Production Information	This shows the production information of the AP.
Description	This shows the user-specified description for the AP.
Configuration Status	This shows whether the configuration on the AP is up-to-date.
Connectivity	This shows the AP connection status.  The gray or 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.
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.
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.

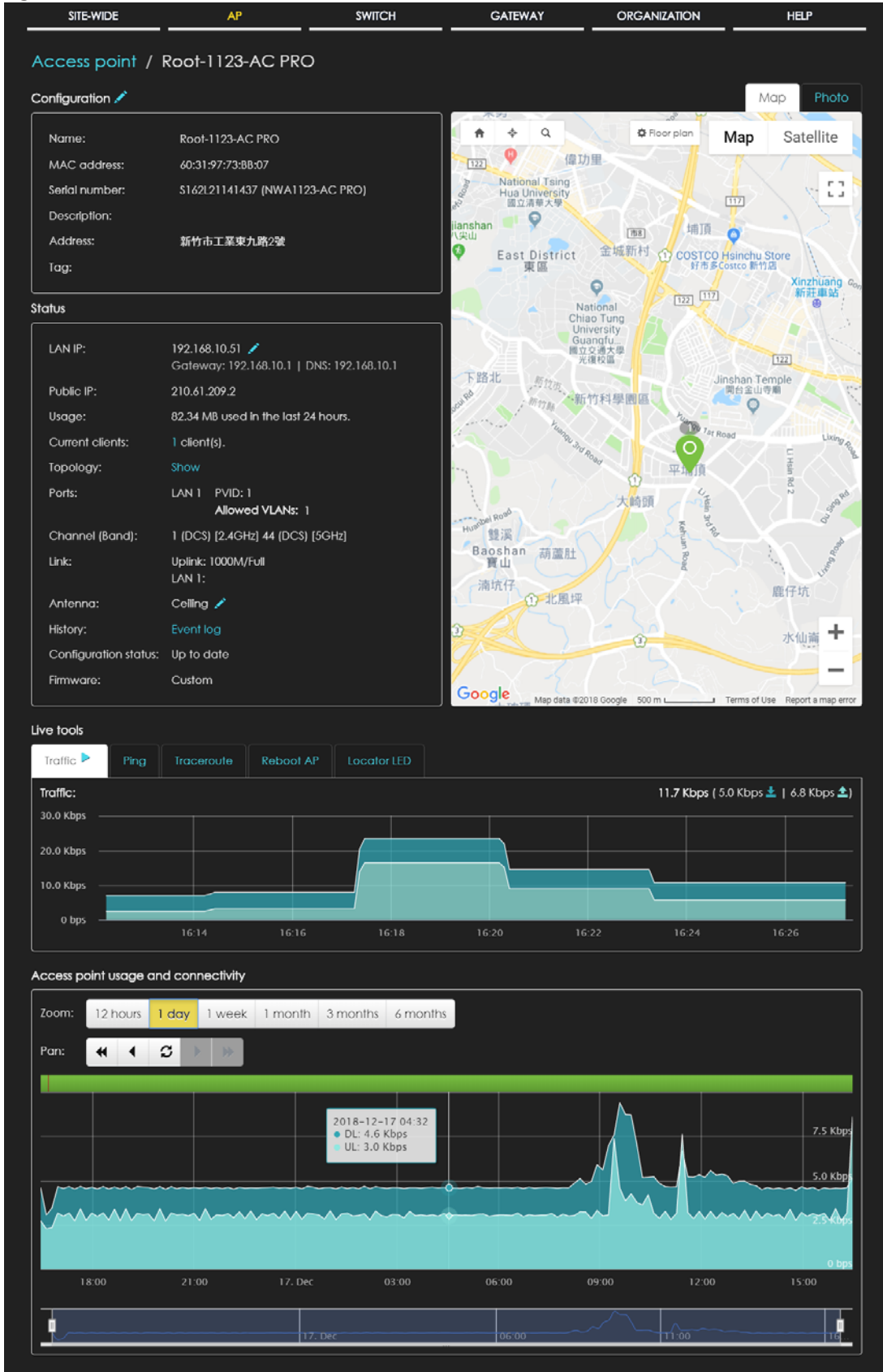
Table 10 AP &gt; Monitor &gt; Access Point (continued)

LABEL	DESCRIPTION
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.
Uplink	This shows whether the AP is connected to the gateway via a wired Ethernet connection or wireless connection.
	Click this icon to display a greater or lesser number of configuration fields.

#### 4.2.1.1 AP Details

Click an AP entry in the **AP > Monitor > Access Point** screen to display individual AP statistics.

Figure 22 AP > Monitor > Access Point: AP Details



The following table describes the labels in this screen.

Table 11 AP &gt; Monitor &gt; Access Point: AP Details

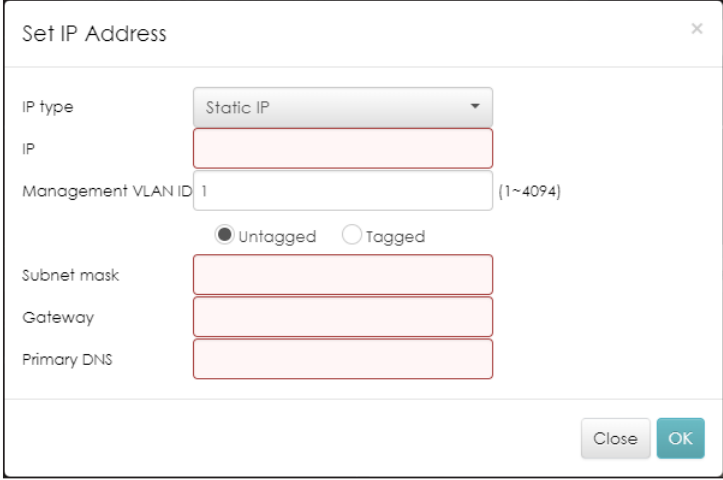

LABEL	DESCRIPTION
Configuration	
Click the edit icon to change the device name, description, tags and address. You can also move the device to another site.	
Name	This shows the descriptive name of the AP.
MAC Address	This shows the MAC address of the AP.
Serial Number	This shows the serial number of 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.
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> 
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	This shows the number of clients which are currently connecting to the AP.
Topology	Click <b>Show</b> to go to the <b>Site-Wide &gt; Monitor &gt; Topology</b> screen. See <a href="#">Section 3.1.4 on page 38</a> .
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 VLAN(s) to which the LAN port belongs. See <a href="#">Section 4.3.7 on page 77</a> for how to change the port's VLAN settings.</p>
Channel (Band)	This shows the channel ID and WiFi frequency band currently being used by the AP.
Link	<p>This shows the speed and duplex mode of the Ethernet connection on the AP's port(s).</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>
Antenna	This displays the antenna orientation settings for the AP that comes with internal antennas and also has an antenna switch.

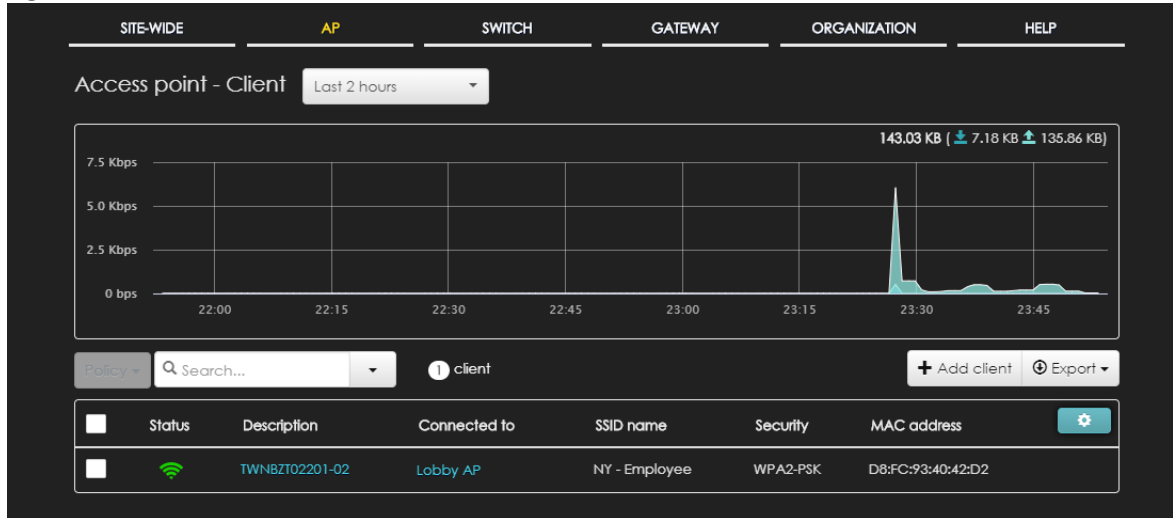
Table 11 AP &gt; Monitor &gt; Access Point: AP Details (continued)

LABEL	DESCRIPTION
History	Click <b>Event log</b> to go to the <b>AP &gt; Monitor &gt; Event log</b> screen.
Configuration status	This shows whether the configuration on the AP is up-to-date.
Firmware	This shows whether the firmware on the AP is up-to-date or there is firmware update available for the AP.
Map	This shows the location of the AP on the 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.
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 to stop the locator LED from blinking. The locator LED will start to blink for the number of minutes set here  Click the  button to turn on the locator feature, which shows the actual location of the AP between several devices in the network.
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 twelve hours, day, week, month, three months or six months.
Pan	Click to move backward or forward by one day or week.

## 4.2.2 Client

This screen allows you to view the connection status and detailed information about a client in the selected site. Click **AP > Monitor > Client** to access this screen.

Figure 23 AP &gt; Monitor &gt; Client




The following table describes the labels in this screen.

Table 12 AP &gt; Monitor &gt; Client

LABEL	DESCRIPTION
Access point - Client	Select to view the device information and connection status in the past two hours, day, week or month.
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 client(s) from the table below, and then choose the security policy that you want to apply to the selected client(s).
Search	Specify your desired filter criteria to filter the list of clients.
Clients	This shows the number of clients connected to 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 goes off-line (red).
Description	This shows the descriptive name of the client. Click the name to display the individual client statistics. See <a href="#">Section 4.2.2.1 on page 55</a> .
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 4.2.1.1 on page 50</a> .
SSID Name	This shows the name of the AP's wireless network to which the client is connected.
Security	This shows which secure encryption method is being used by the client to connect to the Nebula device.
MAC address	This shows the MAC 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	This shows the RSSI (Received Signal Strength Indicator) of the client's wireless connection.
IPv4 address	This shows the IP address of the client.
Tx Rate	This shows maximum transmission rate of the client.
Rx Rate	This shows maximum reception rate of the client.

Table 12 AP &gt; Monitor &gt; Client (continued)

LABEL	DESCRIPTION
Tx	This shows the amount of data (in bytes) received by the client since it was last connected.
Rx	This shows the amount of data (in bytes) transmitted from the client 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.
User	This shows the user's account information used to log into the NCC via captive portal, using Facebook login or 802.1x with Nebula cloud authentication or an RADIUS server.
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.

#### 4.2.2.1 Client Details

Click a client entry in the **AP > Monitor > Client** screen to display individual client statistics.

Figure 24 AP &gt; Monitor &gt; Client: Client Details



The following table describes the labels in this screen.

Table 13 AP &gt; Monitor &gt; Client: 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.
Access point	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 4.2.1.1 on page 50</a> .
Captive portal	This shows the web authentication method used by the client to access the network.
Signal	This shows the RSSI (Received Signal Strength Indicator) of the client's wireless connection.
User	This shows the number of users currently connected to the network through the client device.
Device type	This shows the manufacturer of the client device and the operating system running on it.



Table 13 AP &gt; Monitor &gt; Client: Client Details (continued)

LABEL	DESCRIPTION
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>AP &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>AP &gt; Monitor &gt; Client</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.
Ping	Click the button to ping the client's IP address from the Nebula AP to test connectivity.
Loss rate	This shows the rate of packet loss when you perform ping.
Average latency	This shows the average latency in ms when you perform ping.

### 4.2.3 Event Log

Use this screen to view wireless AP log messages. You can enter the AP name, 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 **AP > Monitor > Event Log** to access this screen.

Figure 25 AP &gt; Monitor &gt; Event log

Access point - Event log

Access point: Any Keyword: Any Category: Any

Range: 2018-08-29 12:45 - 2018-08-29 14:45 Range Search

< Newer Older > 343 Event logs Export

Time	Access point	Category	Detail
2018-08-29 12:45:43	CSO	wlan	Station: 5c:c5:d4:23:65:8b has deauth by STA Leave(L2UPFrame) on Channel: 6, SSID: ZyTP-Guest, ...
2018-08-29 12:45:43	Meeting Room	wlan	Station: 5c:c5:d4:23:65:8b has authorized on Channel: 11, SSID: ZyTP-Guest, 2.4GHz. Interface:wla...
2018-08-29 12:45:43	Meeting Room	wlan	Station: 5c:c5:d4:23:65:8b has associated on Channel: 11, SSID: ZyTP-Guest, 2.4GHz, Signal: -56dB...
2018-08-29 12:45:43	Meeting Room	wlan	Station: 5c:c5:d4:23:65:8b has disassoc by STA Logout on Channel: 11, SSID: ZyTP-Guest, 2.4GHz, Tx...
2018-08-29 12:46:22	CSO	wlan	Station: 00:b3:62:0b:5e:46 has authorized on Channel: 6, SSID: ZyTP-Guest, 2.4GHz. Interface:wlan...
2018-08-29 12:46:22	CSO	wlan	Station: 00:b3:62:0b:5e:46 has associated on Channel: 6, SSID: ZyTP-Guest, 2.4GHz, Signal: -68dBm...
2018-08-29 12:46:26	CSO	wlan	Station: 00:b3:62:0b:5e:46 has disassoc by Wpriv(kickmac) on Channel: 6, SSID: ZyTP-Guest, 2.4GH...
2018-08-29 12:46:26	CSO	wlan	Station: 00:b3:62:0b:5e:46 has authorized on Channel: 149, SSID: ZyTP-Guest, 5GHz. Interface:wlan...
2018-08-29 12:46:26	CSO	wlan	Station: 00:b3:62:0b:5e:46 has associated on Channel: 149, SSID: ZyTP-Guest, 5GHz, Signal: -57dBm...
2018-08-29 12:47:26	Meeting Room	wlan	Station: 5c:c5:d4:23:65:8b has authorized on Channel: 11, SSID: ZyTP-Guest, 2.4GHz. Interface:wla...

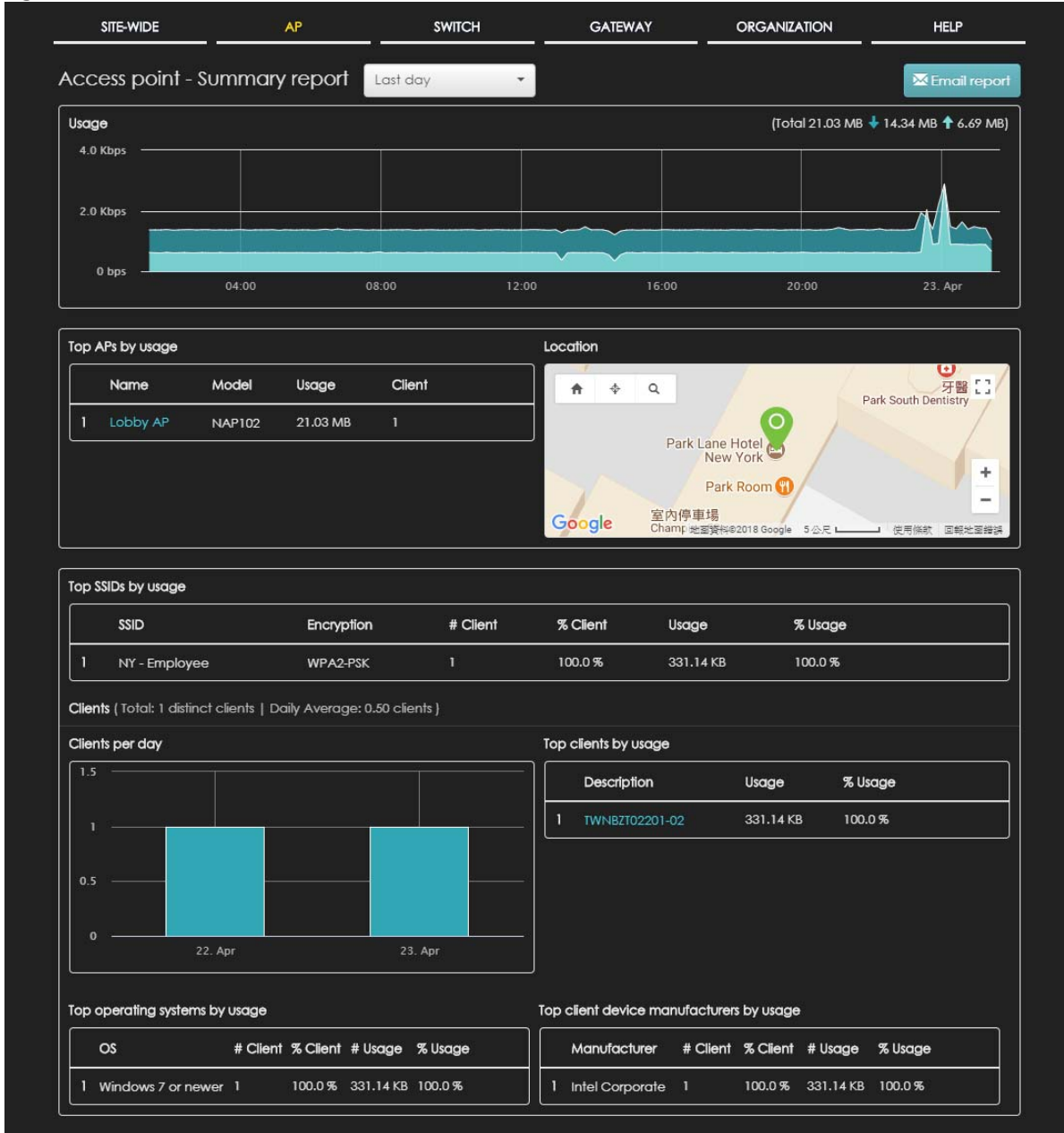
1 2 3 4 5 ... 34 35 Go to 1 Results per page 10

## 4.2.4 Summary Report

This screen displays network statistics for APs of the selected site, such as bandwidth usage, top clients and/or top SSIDs.

Click **AP > Monitor > Summary Report** to access this screen.

Figure 26 AP > Monitor > Summary Report



The following table describes the labels in this screen.

Table 14 AP &gt; Monitor &gt; Summary Report

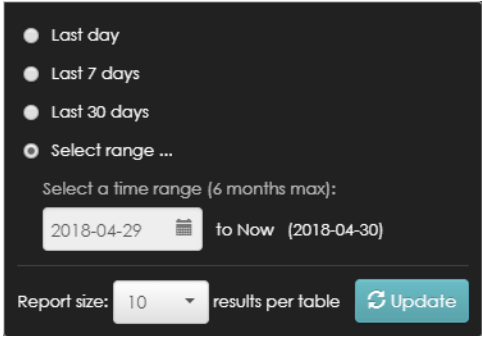
LABEL	DESCRIPTION
Access Point - Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Select range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
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 index number 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 index number 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	
Total	This shows the total number of clients connected to the Nebula device within the specified period of time.
Daily Average	This shows the average daily number of clients within the specified period of time.
Clients per day	
y-axis	The y-axis represents the number of clients.
x-axis	The x-axis represents the date.

Table 14 AP &gt; Monitor &gt; Summary Report (continued)

LABEL	DESCRIPTION
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.
Usage details	
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 client device manufacturers by usage	
	This shows the index number 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.

## 4.3 Configure

Use the **Configure** menus to set the wireless and WiFi security settings for APs of the selected site.

### 4.3.1 SSIDs

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 **AP > Configure > SSIDs** to access this screen.

Figure 27 AP &gt; Configure &gt; SSIDs

The screenshot displays the SSIDs configuration page with the following details:

- Navigation:** SITE-WIDE, AP (selected), SWITCH, GATEWAY, ORGANIZATION, HELP.
- SSIDs Section:**
  - Buttons: Show all, Hide disabled SSIDs (highlighted), 1, 2, 3.
  - Status: Showing 3 of 8 SSIDs.
- Profile 1: Testingbeta5**
  - Name: Testingbeta5 (with Edit button)
  - Enabled: ON
  - Tagging: (empty text box)
  - Guest Network: ON
  - Authentication: WPA2 Pre-shared key
  - Captive portal method: Disable
  - Captive portal: Enabled (No), Theme (Copy of Modem)
  - Band: 2.4GHz band only (selected), 5GHz band only, Concurrent operation (2.4GHz and 5GHz), OFF Band select
  - VLAN ID: 100 (range 1 - 4094)
  - Rate limiting: unlimited Down (Kb/s), unlimited Up (Kb/s)
- Profile 2: HS\_Unifi\_Test**
  - Name: HS\_Unifi\_Test (with Edit button)
  - Enabled: ON
  - Tagging: (empty text box)
  - Guest Network: OFF
  - Authentication: WPA2 Pre-shared key
  - Captive portal method: Disable
  - Captive portal: Enabled (No), Theme (Modem)
  - Band: 2.4GHz band only (selected), 5GHz band only, Concurrent operation (2.4GHz and 5GHz), OFF Band select
  - VLAN ID: 200 (range 1 - 4094)
  - Rate limiting: unlimited Down (Kb/s), unlimited Up (Kb/s)
- Footer:** Save or Cancel button, note: (Please allow 1-2 minutes for changes to take effect.)

The following table describes the labels in this screen.

Table 15 AP &gt; Configure &gt; SSIDs

LABEL	DESCRIPTION
Show all/Hide disabled SSIDs	Select to display all SSID profiles or the active SSID profiles only.
Name	This shows the SSID name for this profile. Click the text box and enter a new SSID if you want to change it.
Edit	Click this button to go to the <b>Authentication</b> screen and configure the advanced settings, such as SSID availability, WiFi security, L2 isolation, intra-BSS traffic blocking and walled garden settings. See Section 4.3.3 on page 65.
Enabled	Click to turn on or off this profile.

Table 15 AP &gt; Configure &gt; SSIDs (continued)

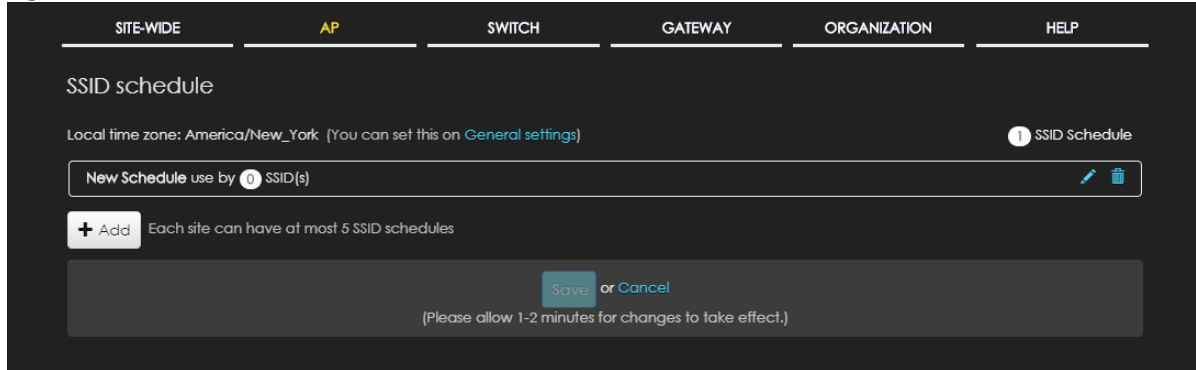
LABEL	DESCRIPTION
Tagging	<p>Enter a tag and click <b>Add new</b> to create a new tag. Alternatively, enter the tag(s) you created for APs in the <b>AP &gt; Monitor &gt; Access Point</b> screen. The SSID profile will only be applied to APs with the specified tag.</p> <p>If you leave this field blank, 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 can not 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 4.3.3 on page 65</a>.</p>
Authentication	
WLAN security	This shows the encryption method used in this profile.
Captive portal method	This shows the authentication method used in this profile.
Captive portal	
Enabled	This shows whether captive portal is enabled for the SSID profile.
Theme	If captive portal is enabled, this shows the name of the captive portal page used in this profile.
Band	<p>Select to have the SSID use either 2.4 GHz band or the 5 GHz band.</p> <p>If you select <b>Concurrent operation</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>
VLAN ID	Enter the ID number of the VLAN to which the SSID belongs.
Rate limiting	<p>Set the maximum incoming/outgoing transmission data rate (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 inbound and outbound traffic. If the lock is unlocked, you can set inbound and outbound traffic to have different transmission speeds.</p>

### 4.3.2 SSID Schedule

Use this screen to view and configure the schedules which can be applied to the SSIDs. The SSID is enabled or disabled at the specified time. Click **AP > Configure > SSID schedule** to access this screen.

The table shows the name of the existing schedules and the number of SSIDs 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 4.3.2.1 on page 64](#).

Figure 28 AP &gt; Configure &gt; SSID schedule



### 4.3.2.1 Create new schedule

Click the **Add** button in the **AP > Configure > SSID schedule** screen to access this screen.

Figure 29 AP &gt; Configure &gt; SSID schedule: Add

The following table describes the labels in this screen.

Table 16 AP &gt; Configure &gt; SSID schedule: Add

LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identifying purposes.
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 on this day. Otherwise, select <b>Off</b> to disable the SSID.



Table 16 AP &gt; Configure &gt; SSID schedule: Add (continued)

LABEL	DESCRIPTION
From - To	Specify the hour and minute when the schedule begins and ends each day
Time display	Select the time format in which the time is displayed.
Close	Click this button to exit this screen without saving.
Add	Click this button to save your changes and close the screen.

### 4.3.3 Authentication

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

Click **AP > Configure > Authentication** to access this screen.

Figure 30 AP > Configure > Authentication

SITE-WIDE
AP
SWITCH
GATEWAY
ORGANIZATION
HELP

### Authentication

SSID: Testingbeta5

**SSID availability**

Visibility Broadcast this SSID

Schedule Always on [Edit setting](#)

**Network access**

**WLAN security**

Open  
Users can connect without entering a password

WPA2 Pre-shared key  
Users must enter this key to associate: \*\*\*\*\* [Show key](#)

ON 802.11r  
Users enable this to support fast roaming

MAC-based Authentication with XXXXXXXXXXXXXXXXXXXX  
Uses MAC address as a username and password

WPA2-Enterprise with XXXXXXXXXXXXXXXXXXXX  
Uses 802.1X authentication that requires a unique username and password

**Captive portal**

Disable  
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

Sign-on with My RADIUS server  
Users must enter a username and password then can access the network

**RADIUS server**

Host	Port	Secret	Action
1	<span style="border: 1px solid #ccc; padding: 2px;"></span>	<span style="border: 1px solid #ccc; padding: 2px;"></span>	<span style="border: 1px solid #ccc; padding: 2px;"></span>

NAS Identifier

[+ Add a server](#)

**RADIUS accounting**

RADIUS accounting disabled

**Assisted roaming**

Enable 802.11k/v

**U-APSD**

**Walled garden**

Walled garden ranges

[What do I enter here?](#)

**Captive portal access attribute**

Login on multiple client devices Multiple devices access simultaneously

Strict Policy Allow HTTPS traffic without sign-on

**Layer 2 isolation**

Enable layer 2 isolation

This allows you to create and manage Layer 2 isolation list that can be used by your SSIDs. If a client device's MAC addresses is NOT listed in a layer 2 isolation list, it is blocked from communicating with other client devices in an SSID on which Layer 2 isolation is enabled.

MAC	Description	Action
1	<span style="border: 1px solid #ccc; padding: 2px;"></span>	<span style="border: 1px solid #ccc; padding: 2px;"></span>

[+ Add](#)

**Intra-BSS traffic blocking**

Enable Intra-BSS traffic blocking

Enable this option to prevent crossover traffic from within the same SSID.

[Apply](#) or [Cancel](#)

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

The following table describes the labels in this screen.

Table 17 AP > Configure > Authentication

LABEL	DESCRIPTION
SSID	Select the SSID profile to which the settings you configure here is applied.
SSID availability	
Visibility	<p>Select <b>Hide this SSID</b> if you want to hide your SSID from 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>.</p> <p>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 screen(s) (these vary by client, client connectivity software, and operating system).</p>
Schedule	Select a schedule to control when the SSID is enabled or disabled.
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 7.3.6 on page 181</a>.</p>
WLAN security	<p>Select <b>Open</b> to allow any client to associate this network without any data encryption or authentication.</p> <p>Select <b>WPA2 Pre-shared key</b> and enter a pre-shared key from 8 to 64 case-sensitive keyboard characters to enable WPA2-PSK data encryption.</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 doesn't need to perform the whole 802.1x authentication process.</li> <li>• 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.</li> </ul> <p>Select <b>WPA2-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 doesn't need to perform the whole 802.1x authentication process.</li> </ul>
Captive portal	<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 the NCC (<b>Nebula cloud authentication</b>) or an external RADIUS server (<b>My RADIUS server</b>) through the specifically designated web portal page.</p> <p>Select <b>Facebook</b> to block network traffic until a client authenticates with the NCC using Facebook Login. Facebook Login is a secure and quick way for users to log into your app or website using their existing Facebook accounts.</p> <p>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>

Table 17 AP &gt; Configure &gt; Authentication (continued)

LABEL	DESCRIPTION
RADIUS server	<p>This field is available only when you select to use <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 when you select <b>Sign-on with My RADIUS server</b> in the <b>Captive portal</b> field.</p> <p>Click <b>Add a server</b> to specify the IP address, port number and shared secret password of the RADIUS server to be used for authentication.</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>Captive portal</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 a server</b> to specify the IP address, port number and shared secret password of the RADIUS server to be used for accounting.</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>
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>
Walled garden	<p>Select to turn on or off the walled garden feature. This field is not configurable if you set <b>Captive portal</b> to <b>Disable</b>.</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	<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>
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>Captive portal</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 My RADIUS server</b> or <b>Sign-on with Nebula Cloud authentication</b> in the <b>Captive portal</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 don't allow users to have simultaneous logins.</p>

Table 17 AP &gt; Configure &gt; Authentication (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>
NCAS disconnection behavior	<p>This field is available only when you select <b>Click-to-continue</b> or <b>Sign-on with</b> in the <b>Captive portal</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>
Layer 2 isolation	
Enable 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	
Enable 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>

### 4.3.4 Captive Portal

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 **AP > Configure > Captive portal** to access this screen.

Figure 31 AP &gt; Configure &gt; Captive portal

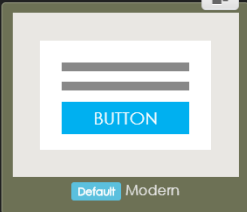
SITE-WIDE    **AP**    SWITCH    GATEWAY    ORGANIZATION    HELP

### Captive portal

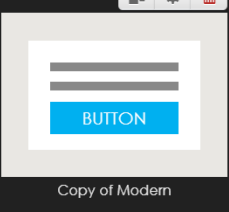
SSID: Youwontbeabletoconnect

Captive portal on this SSID is disabled. You can change this setting [here](#).


**Themes**



Default Modern



Copy of Modern



Copy of 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

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

The following table describes the labels in this screen.

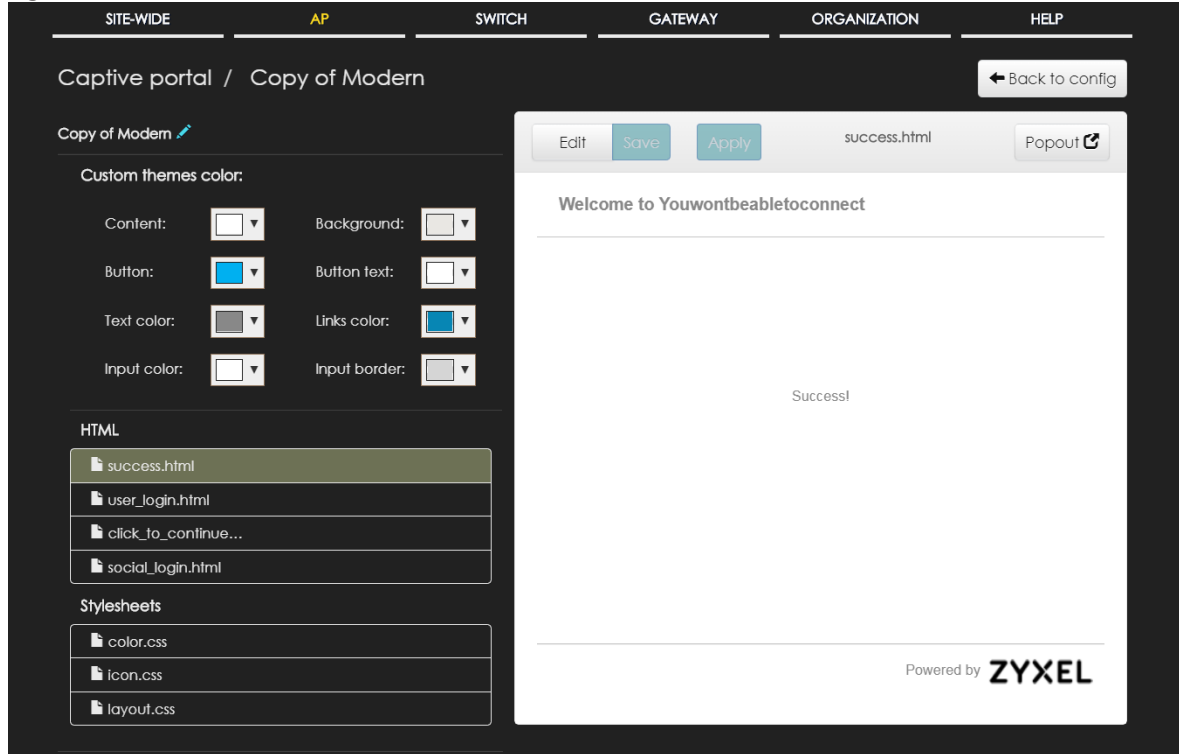
Table 18 AP > Configure > Captive portal

LABEL	DESCRIPTION
SSID	Select the SSID profile to which the settings you configure here is applied.
Themes	Click the <b>Copy</b> icon at the upper right corner of the default theme image to create a new custom theme (login page).  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 page(s). See <a href="#">Section 4.3.4.1 on page 71</a> .  Click the <b>Remove</b> icon to delete a custom theme page.
Click-to-continue/ Sign-on page	
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> .

#### 4.3.4.1 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 **AP > Configure > Captive portal** screen to access this screen.

Figure 32 AP &gt; Configure &gt; Captive portal: Edit



The following table describes the labels in this screen.

Table 19 AP &gt; Configure &gt; Captive portal: Edit

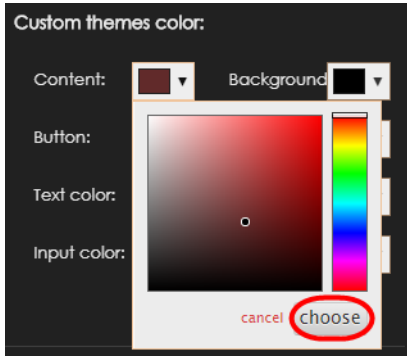
LABEL	DESCRIPTION
Back to config	Click this button to return to the <b>Captive portal</b> screen.
Copy of Modern	This shows the name of the theme. Click the edit icon the change it.
Custom themes color	<p>Customize the colors on the selected custom portal page (HTML file), such as the color of the button, text, window's background, links, borders, and etc.</p> <p>Select a color that you want to use and click the <b>Choose</b> button.</p> 
HTML	<p>This shows the HTML file name of the portal page created for the selected custom theme.</p> <p>Click an HTML file to display the portal page on the right side of the screen. You can also change colors and modify the CSS values of the selected HTML file.</p>
Stylesheets	This shows the name of the main CSS file created for the selected custom theme.



Table 19 AP &gt; Configure &gt; Captive portal: Edit (continued)

LABEL	DESCRIPTION
Edit/Preview	Click <b>Edit</b> 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 <b>Preview</b> to display the corresponding portal page.
Save	Click this button to save your color settings for the selected HTML file.
Apply	Click this button to apply your color settings to the selected HTML file.
Popout	Click this button to display the corresponding portal page in a pop-up window.

### 4.3.5 Radio Setting

Use this screen to configure global radio settings for all APs in the site. Click **AP > Configure > Radio setting** to access this screen.

Figure 33 AP &gt; Configure &gt; Radio setting

The screenshot displays the 'Radio setting' configuration page. At the top, there is a navigation bar with tabs: SITE-WIDE, AP (selected), SWITCH, GATEWAY, ORGANIZATION, and HELP. The main content area is titled 'Radio setting' and contains several configuration sections:

- Country:** Taiwan
- Maximum output power:** 2.4 GHz: 30 dBm, 5 GHz: 30 dBm
- Channel width:** 2.4 GHz: 20 MHz, 5 GHz: 80 MHz
- DCS setting:**
  - DCS time interval: 720 (10~1440 minutes)
  - DCS schedule: ON
  - DCS client aware: ON
  - Avoid 5G DFS channel: OFF
  - 2.4 GHz channel deployment: Three-Channel Deployment
  - 5 GHz channel deployment: Auto
- Allow 802.11ac/n stations only:** ON

At the bottom, there is a table of radio settings:

Access point	Radio #	Model	Band	Channel	Transmit power	Channel width	Antenna
HomeNAP	1	NAP102	2.4 GHz	11 (DCS)	20 dBm	20 MHz	<a href="#">Edit</a>

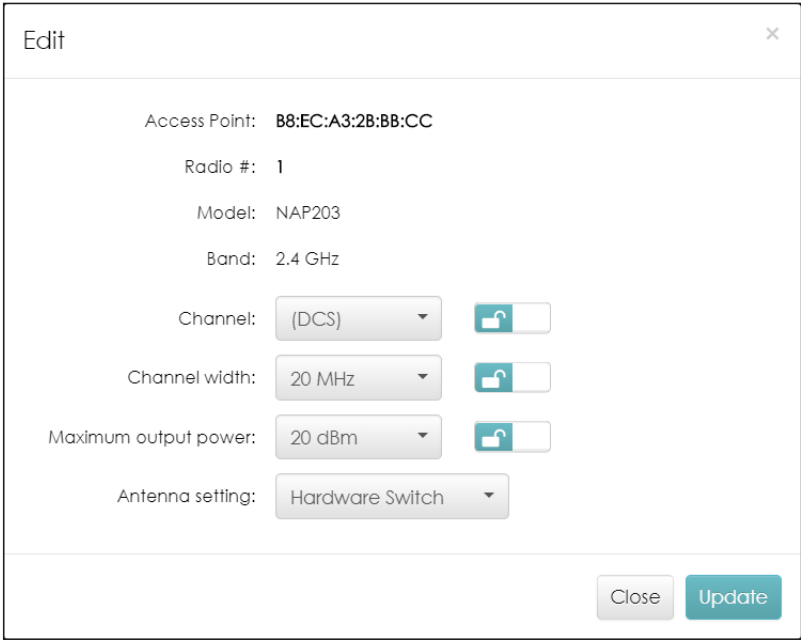
Below the table, there are 'Save' and 'Cancel' buttons, and a note: '(Please allow 1-2 minutes for changes to take effect.)'

The following table describes the labels in this screen.

Table 20 AP > Configure > Radio setting

LABEL	DESCRIPTION
Country	<p>Select the country where the AP is located/installed.</p> <p>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 to other systems.</p>
Maximum output power	<p>Set the maximum target output power of the radio (in dBm).</p>
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 144Mbps (2.4GHz) or 217Mbps (5GHz) whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps (2.4GHz) or 450Mbps (5GHz). An IEEE 802.11ac-specific 80MHz channel offers speeds of up to 1.3Gbps.</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 2.4GHz AP in the network.</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>Select <b>ON</b> to force the AP to select a non-DFS channel if your APs are operating in an area known to have RADAR devices.</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 20 AP &gt; Configure &gt; Radio setting (continued)

LABEL	DESCRIPTION
Allow 802.11ac/n stations only	Select <b>ON</b> to have the AP allow only IEEE 802.11n/ac clients to connect, and reject IEEE 802.11a/b/g clients.
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.
DCS Now	Click this button to have the APs immediately scan for and select a channel that has least interference.
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.
Band	This displays the frequency band used by the connected AP's radio.
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.
Antenna	This displays the antenna orientation settings for the AP that comes with internal antennas and also has an antenna switch.
Edit	<p>Click this button to modify the AP's channel, output power and channel width settings.</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> 

## 4.3.6 Client Steering

Use this screen to configure network traffic load balancing between the APs and enable smart client steering.

Click **AP > Configure > Client Steering** to access this screen.

**Figure 34** AP > Configure > Client Steering

The following table describes the labels in this screen.

**Table 21** AP > Configure > Load balancing

LABEL	DESCRIPTION
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.

Table 21 AP &gt; Configure &gt; Load balancing (continued)

LABEL	DESCRIPTION
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.
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.
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 -76 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.

### 4.3.7 Port Setting

Use this screen 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 **AP > Configure > Port Setting** to access this screen.



Figure 35 AP &gt; Configure &gt; Port Setting

The following table describes the labels in this screen.

Table 22 AP &gt; Configure &gt; Port Setting

LABEL	DESCRIPTION
LAN x	This is the name of the physical Ethernet port on the AP.  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.
ON/OFF	Select <b>ON</b> to turn on the LAN port of the AP. Select <b>OFF</b> to disable the port.
PVID	Enter the port's PVID.  A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
Allowed VLANs	Enter the VLAN ID number(s) 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.

Table 22 AP &gt; Configure &gt; Port Setting (continued)

LABEL	DESCRIPTION
Port Setting	This displays the port's VLAN settings for the managed AP.
Edit	<p>By default, all APs in the site use the global port settings. Click this button 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 VLAN(s) to which the port belongs.</p> <div data-bbox="540 394 1334 800"><p>Edit <span>×</span></p><p>LAN 1</p><p>Enabled <input checked="" type="checkbox"/> ON <input type="checkbox"/> </p><p>PVID <input type="text" value="64"/> </p><p>Allowed VLANs <input type="text" value="60,62,64"/></p><p><input type="button" value="Close"/> <input checked="" type="button" value="OK"/></p></div>

# CHAPTER 5

## Switch

### 5.1 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 switch is deployed and added to the site.

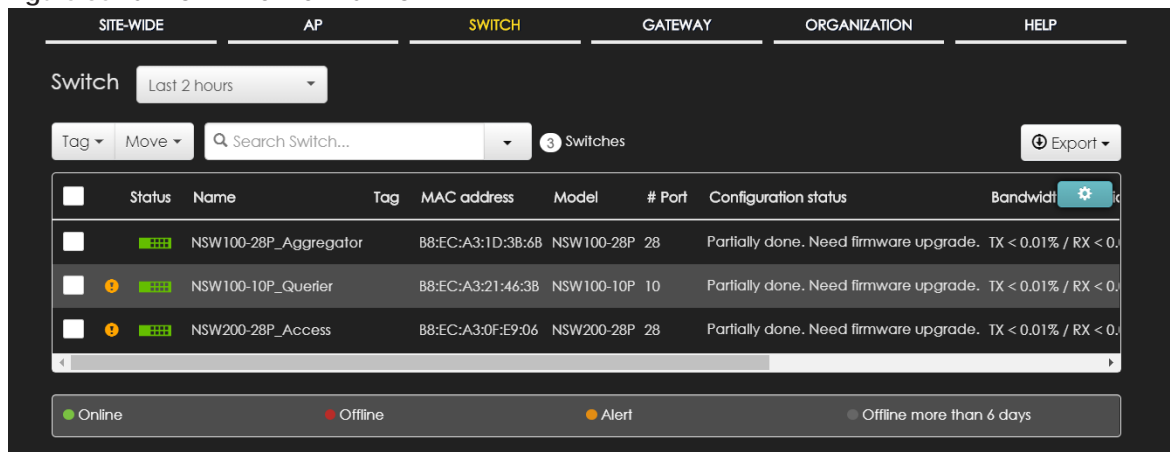
### 5.2 Monitor

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

#### 5.2.1 Switch

This screen allows you to view the detailed information about a switch in the selected site. Click **Switch > Monitor > Switch** to access this screen.

Figure 36 Switch > Monitor > Switch




The following table describes the labels in this screen.

Table 23 Switch > Monitor > Switch

LABEL	DESCRIPTION
	Select to view the device information and connection status in the past two hours, day, week or month.
Tag	Select one or multiple switches and click this button to create a new tag for the switch(es) or delete an existing tag.
Move	Select one or multiple switches and click this button to move the switch(es) to another site or remove the switch(es) from the current site.



Table 23 Switch &gt; Monitor &gt; Switch (continued)

LABEL	DESCRIPTION
Search	Specify your desired filter criteria to filter the list of switches.
Switch	This shows the number of switches connected to the site network.
Export	Click this button to save the switch list as a CSV or XML file to your computer.
Status	This shows whether the switch is online (green), has generated alerts (amber), goes off-line (red) or has been off-line for at least six days (gray).  Move the cursor over an amber alert icon to view the alerts the NCC generates when an error or something abnormal is detected on the IPTV network.
Name	This shows the descriptive name of the switch.
Tag	This shows the user-specified tag for the switch.
MAC address	This shows the MAC address of the switch.
LAN IP	This shows the local (LAN) IP address of the switch.
Public IP	This shows the global (WAN) IP address of the switch.
Model	This shows the model number of the switch.
# Port	This shows the number of the switch port which is connected to the NCC.
Configuration status	This shows whether the configuration on the switch is up-to-date.
Bandwidth Utilization	This shows what percentage of the upstream/downstream bandwidth is currently being used by the switch's uplink port.
Production information	This shows the production information of the switch.
Connectivity	This shows the switch connection status. Nothing displays if the switch is off-line.  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 switch is connected or disconnected.
Description	This shows the user-specified description for the switch.
Serial number	This shows the serial number of the switch.
Usage	This shows the amount of data that has been transmitted or received by the switch's clients.
	Click this icon to display a greater or lesser number of configuration fields.

### 5.2.1.1 Switch Details

Click a switch entry in the **Switch > Monitor > Switch** screen to display individual switch statistics.

Figure 37 Switch > Monitor > Switch: Switch Details

The screenshot displays the 'Switch Details' page for a switch with MAC address B8:EC:A3:28:4B:91. The interface is divided into several sections:

- Configuration:**
  - Name: B8:EC:A3:28:4B:91
  - MAC address: B8:EC:A3:28:4B:91
  - Serial number: S172L13000023 (NSW100-10P)
  - Description:
  - Address:
  - Tags:
- Status:**
  - LAN IP: 192.168.173.51 (via DHCP)
  - Gateway: 192.168.173.1
  - DNS: 192.168.64.171, | 192.168.64.170
  - VLAN: 173
  - DHCP Server: 192.168.173.1
  - Public IP: 60.248.159.196
  - Topology: [Show](#)
  - RSTP Status: root is B8:EC:A3:28:4B:91 / root bridge priority: 32768
  - IGMP Status: Disabled
  - PoE Status: Classification 4.2 / 180 W
  - History: [Event log](#)
  - Configuration status: Up to date
  - Firmware: Up to date
- Ports:** A grid of 10 port status icons, with a 'Configure ports' button.
- Live tools:** Includes buttons for Ping, Port Power Cycle, MAC table, Reboot switch, and Locator LED. A text input field contains 'google.com' and a 'Ping' button.
- Uplink usage:** A line graph showing network usage over time. The x-axis shows dates from 18 Dec to 15 Dec. The y-axis shows usage in Mbps, with markers at 20.0 and 40.0. A 'Zoom' dropdown is set to '1 day'.
- Power Consumption:** A line graph showing power usage over the last 2 hours. The x-axis shows times from 15:00 to 16:45. The y-axis shows power in Watts (W), with markers at 0 W, 2.5 W, 5 W, and 7.5 W. Summary statistics: Total: 180.0 W, Current Consumption: 4.2 W, Maximum Consumption: 6.4 W, Minimum Consumption: 4.1 W.

The following table describes the labels in this screen.

Table 24 Switch > Monitor > Switch: Switch Details

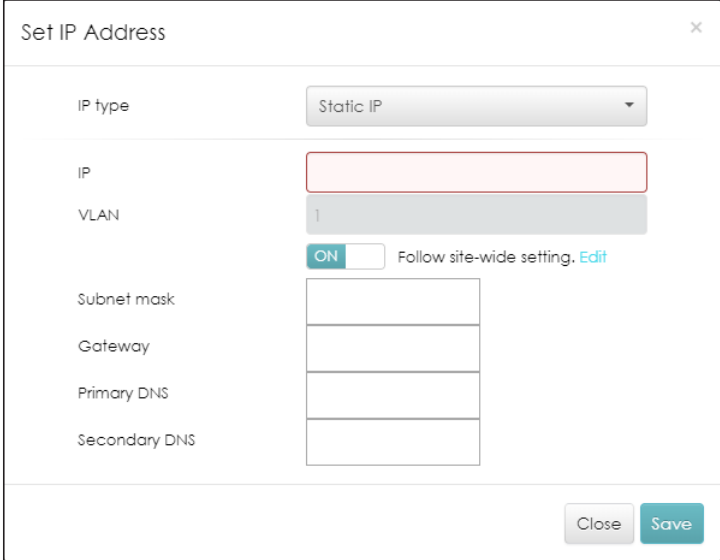

LABEL	DESCRIPTION
Configuration	
Click the edit icon to change the device name, description, tags and address. You can also move the device to another site.	
Name	This shows the descriptive name of the switch.
MAC Address	This shows the MAC address of the switch.
Serial Number	This shows the serial number of the switch.
Description	This shows the user-specified description for the switch.
Address	This shows the user-specified address for the switch.
Tags	This shows the user-specified tag for the switch.
Status	
LAN IP	<p>This shows the local (LAN) IP address of the switch. 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 switch.
Topology	Click <b>Show</b> to go to the <b>SITE-WIDE &gt; Monitor &gt; Topology</b> screen. See <a href="#">Section 3.1.4 on page 38</a> .
RSTP Status	This shows <b>Disabled</b> when RSTP is disabled on the switch. Otherwise, it shows the name or MAC address of the switch that is the root bridge of the spanning tree, and the bridge priority.
IGMP Status	This shows whether IGMP is enabled on the switch. If IGMP is enabled, it also shows the ID number of the VLAN on which the switch learns the multicast group membership and the IP address of the switch interface in IGMP querier mode.
PoE Status	<p>This shows the power management mode, the amount of power the switch is currently supplying to the connected PoE-enabled devices and the total power the switch can provide to the connected PoE-enabled devices on the PoE ports. <b>N/A</b> displays if the switch doesn't support PoE.</p> <p>Click the edit icon to open the <b>PoE Configuration</b> screen. See <a href="#">Section 5.2.1.2 on page 84</a>.</p>

Table 24 Switch &gt; Monitor &gt; Switch: Switch Details (continued)

LABEL	DESCRIPTION
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 switch is up-to-date.
Firmware	This shows whether the firmware on the switch is up-to-date or there is firmware update available for the switch.
Map	This shows the location of the switch on the Google map.
Photo	This shows the photo of the switch. 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 switch. You can click a port to see the individual port statistics. See <a href="#">Section 5.2.1.3 on page 86</a>. The port colors indicate the status of the ports.</p> <ul style="list-style-type: none"> <li>• Gray: The port is disconnected.</li> <li>• Light blue: The port is blocked.</li> <li>• Orange: The port is connected and transmitting data at 10 or 100 Mbps.</li> <li>• Green: The port is connected and transmitting data at 1000 Mbps (1 Gbps).</li> <li>• Blue: The port is connected and transmitting data at 10000 Mbps (10 Gbps).</li> </ul>
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 5.3.1 on page 98</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 port(s) and click the <b>Reset</b> button to disable and enable the port(s) again.
MAC table	<p>This shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s).</p> <p>You can define how it displays and arranges the data in the summary table below.</p>
Reboot switch	Click the <b>Reboot</b> button to restart the switch.
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 switch between several devices in the network.</p>
Uplink usage	<p>Move the cursor over the chart to see the transmission rate at a specific time.</p>
Zoom	Select to view the statistics in the past twelve hours, day, week, month, three months or six months.
Pan	Click to move backward or forward by one day or week.
Power Consumption	
	Select to view the switch power consumption in the past two hours, day, week or month.
	This shows the current, total, maximum and minimum power consumption of the switch.
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.

### 5.2.1.2 PoE Configuration

Use this screen to set the PoE mode, priority levels and power-up mode for the switch in distributing power to PDs. To access this screen, click the edit icon next to **PoE Status** in the **Switch > Monitor > Switch: Switch Details** screen.

**Figure 38** Switch > Monitor > Switch: Switch Details: PoE Configuration

PoE Configuration

Modifications to POE configuration on this page have severe impact to POE devices connect to it. Reference the "Help page" carefully for detail functional description before any change is applied to it. Please contact support team for any inquiries.

PoE Mode: Classification mode

Port	Priority	Power-up
1	Low	802.3at
2	Low	802.3at
3	Low	802.3at
4	Low	802.3at
5	Low	802.3at
6	Low	802.3at
7	Low	802.3at
8	Low	802.3at
...	...	...
24	Low	802.3at

Close Saving

The following table describes the labels in this screen.

**Table 25** Switch > Monitor > Switch: Switch Details: PoE Configuration

LABEL	DESCRIPTION
PoE Mode	Select the power management mode you want the switch to use.  <b>Classification mode</b> - Select this if you want the switch 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 switch to manage the total power supply so that each connected PD gets a resource. However, the power allocated by the switch 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.
Port	This is the port index number.

Table 25 Switch &gt; Monitor &gt; Switch: Switch Details: PoE Configuration (continued)

LABEL	DESCRIPTION
Priority	<p>When the total power requested by the PDs exceeds the total PoE power budget on the switch, you can set the PD priority to allow the switch to provide power to ports with higher priority.</p> <p>Select <b>Critical</b> to give the highest PD priority on the port.</p> <p>Select <b>Medium</b> to set the switch to assign the remaining power to the port after all critical priority ports are served.</p> <p>Select <b>Low</b> to set the switch to assign the remaining power to the port after all critical and medium priority ports are served.</p>
Power-up	<p>Set how the switch provides power to a connected PD at power-up.</p> <p><b>802.3af</b> - the switch 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 switch 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 switch 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 switch is performing 2-event Layer-1 classification (PoE+ hardware classification) or the connected PD is NOT performing Layer 2 power classification using Link Layer Discovery Protocol (LLDP).</p> <p><b>802.3at</b> - the switch 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>
Close	Click this button to exit this screen without saving.
Saving	Click this button to save your changes and close the screen.

### 5.2.1.3 Switch Port Details

Use this to view individual switch port statistics. To access this screen, click a port in the **Ports** section of the **Switch > Monitor > Switch: Switch Details** screen or click the **details** link next to a port in the **Switch > Configure > Switch ports** screen.

Figure 39 Switch > Monitor > Switch: Switch Details: Port Details

SITE-WIDE
AP
SWITCH
GATEWAY
ORGANIZATION
HELP

Switch / Mesh-NSW100-28HP / Port 4
Last 2 hours

2 4 6 8 10 12 14 16 18 20 22 24 26 28

1 3 5 7 9 11 13 15 17 19 21 23 25 27 25 27

**Configuration**

Summary: Trunk port with PVID 1, Allowed VLANs: 'all'

RSTP: Enable

Port mirroring: Not mirroring traffic

**Status**

Name: Port4

Status: 1000M/Auto (Copper)

LLDP: N/A/203

History: [Event log](#)

**Bandwidth Utilization**

Current Utilization: < 0.01% | < 0.01%

Maximum Utilization: < 0.01% | 0.10%

Minimum Utilization: < 0.01% | < 0.01%

**Power Consumption**

Total: 30.0 W | Current Consumption: 4.8 W

Maximum Consumption: 10.3 W

Minimum Consumption: 4.6 W

**Packets Counters**

TX / RX Unicast: 317,393 pkts / 168,198 pkts

TX / RX Multicast: 4,177 pkts / 6,261 pkts

TX / RX Broadcast: 4,737 pkts / 4,982 pkts

TX / RX Pause: 0 pkt / 0 pkt

**IGMP V2**

Query Rcv: 0

Report Rcv: 0

Report Tc: 0

Report Drops: 0

Leave Rcv: 0

Leave Tc: 0

Leave Drops: 0

**IGMP V3**

Query Rcv: 0

Report Rcv: 0

Report Tc: 0

Report Drops: 0

**Error Packets**

RX CRC: 0 pkt

Length: 0 pkt

Runt: 0 pkt

IPv4 Address	MAC Address	VLAN
	4E:D4:FF:FF:D7	1
	B8:81:98:6D:06:A5	1
	AC:78:A1:80:73:9F	1
	EC:43:F6:73:45:34	1
	60:31:97:73:85:8F	1
	40:98:AD:02:8F:42	1
	80:6E:8F:12:A2:C8	1
	00:CD:FE:24:94:59	1
	00:18:0A:2F:0A:C0	1
	A0:A8:CD:DF:9E:1D	1

1
2
Go to 
Results per page

**Cable Diagnostic**

Cable diagnostics will cause temporary network disconnection on the selected port as well as all devices connected to it

Channel	Pair Status	Cable Length	Distance to fault (m)
Pair-A	OK	11.00	N/A
Pair-B	OK	11.00	N/A
Pair-C	OK	11.00	N/A
Pair-D	OK	11.00	N/A

The following table describes the labels in this screen.

Table 26 Switch > Monitor > Switch: Switch Details: Port Details

LABEL	DESCRIPTION
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 switch.</p> <p>Click a port to go to the corresponding port details screen. The selected port is highlighted in color. The port colors indicate the status of the ports.</p> <ul style="list-style-type: none"> <li>• Gray: The port is disconnected.</li> <li>• Light blue: The port is blocked.</li> <li>• Orange: The port is connected and transmitting data at 10 or 100 Mbps.</li> <li>• Green: The port is connected and transmitting data at 1000 Mbps (1 Gbps).</li> <li>• Blue: The port is connected and transmitting data at 10000 Mbps (10 Gbps).</li> </ul>
Configuration	
Click the edit icon to open the <b>Switch ports</b> screen and show the port(s) that match the filter criteria (the selected port number). See <a href="#">Section 5.3.1 on page 98</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.
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.



Table 26 Switch &gt; Monitor &gt; Switch: Switch Details: Port Details (continued)

LABEL	DESCRIPTION
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) error(s).
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.
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.
Pair Status	<b>OK:</b> The physical connection between the wire-pair is okay. <b>Open:</b> There is no physical connection (an open circuit detected) between the wire-pair. <b>Short:</b> There is an short circuit detected between the wire-pair. <b>Unknown:</b> The Switch failed to run cable diagnostics on the cable connected this port. <b>Unsupported:</b> The port is a fiber port or it is not active.
Cable Length	This displays the total length of the Ethernet cable that is connected to the port when the <b>Pair Status</b> is <b>OK</b> and the switch chipset supports this feature.  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> .  This shows <b>Unsupported</b> if the switch chipset does not support to show the cable length.
Distance to fault (m)	This displays the distance between the port and the location where the cable is open or shorted.  This shows <b>N/A</b> if the <b>Pair Status</b> is <b>OK</b> .  This shows <b>Unsupported</b> if the switch chipset does not support to show the distance.
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 switch.
Vendor	This shows the vendor name of the transceiver installed in the port.

Table 26 Switch &gt; Monitor &gt; Switch: Switch Details: Port Details (continued)

LABEL	DESCRIPTION
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.

## 5.2.2 Client

This screen allows you to view the connection status and detailed information about a client in the selected site. Click **Switch > Monitor > Client** to access this screen.


Figure 40 Switch &gt; Monitor &gt; Client

The screenshot shows the 'Switch - Client' interface with a navigation bar at the top containing 'SITE-WIDE', 'AP', 'SWITCH' (highlighted), 'GATEWAY', 'ORGANIZATION', and 'HELP'. Below the navigation bar, there is a search bar labeled 'Search clients...' and a dropdown menu set to 'Last 2 hours'. A notification bubble indicates '10 Clients' and an 'Export' button is visible. The main content is a table with the following columns: Status, Description, MAC address, Connected to, Port, and VLAN. A settings gear icon is located at the top right of the table.

Status	Description	MAC address	Connected to	Port	VLAN
🟢	00:18:0A:7C:C4:3D	00:18:0A:7C:C4:3D	IT Room - Switch	28	1
🟢	00:18:0A:7C:C4:45	00:18:0A:7C:C4:45	IT Room - Switch	28	1
🟢	1C:74:0D:F9:9C:A0	1C:74:0D:F9:9C:A0	IT Room - Switch	24	1
🟢	60:31:97:84:D7:3A	60:31:97:84:D7:3A	IT Room - Switch	2	1
🟢	70:81:EB:76:FB:95	70:81:EB:76:FB:95	IT Room - Switch	2	1
🟢	88:58:DD:85:70:80	88:58:DD:85:70:80	IT Room - Switch	10	1
🟢	B8:EC:A3:0F:DA:4C	B8:EC:A3:0F:DA:4C	IT Room - Switch	24	1
🔴	B8:EC:A3:0F:E9:97	B8:EC:A3:0F:E9:97	IT Room - Switch	24	1
🔴	B8:EC:A3:A6:90:6C	B8:EC:A3:A6:90:6C	IT Room - Switch	24	1
🟢	F0:76:1C:73:98:30	F0:76:1C:73:98:30	IT Room - Switch	24	1

The following table describes the labels in this screen.

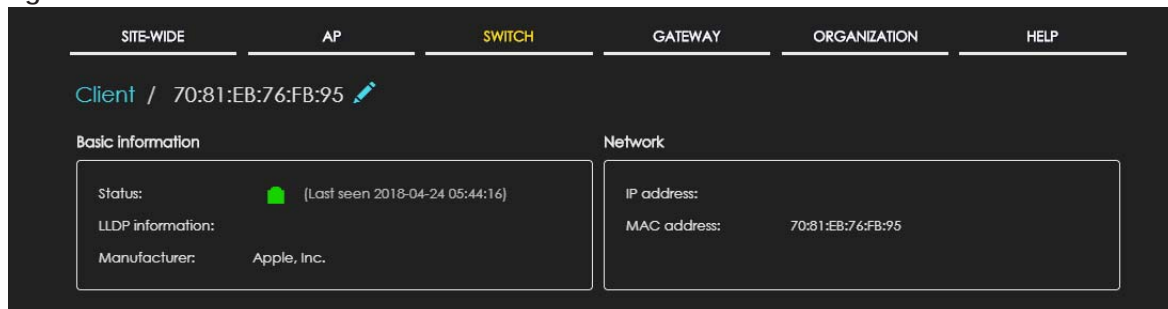
Table 27 Switch > Monitor > Client

LABEL	DESCRIPTION
Switch - Client	Select to view the device information and connection status in the past two hours, day, week or month.
Search	Specify your desired filter criteria to filter the list of clients.
Clients	This shows the number of clients connected to the site 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 goes off-line (red).
Description	This shows the descriptive name of the client. Click the name to display the individual client statistics. See <a href="#">Section 5.2.2.1 on page 91</a> .
MAC Address	This shows the MAC address of the client.
Connected to	This shows the name of the Nebula managed switch to which the client is connected. Click the name to display the individual switch statistics. See <a href="#">Section 5.2.1.1 on page 81</a> .
Port	This shows the number of the switch port to which the client is connected.
VLAN	This shows the ID number of the VLAN to which the client belongs.
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.
LLDP	This shows the LLDP (Link Layer Discovery Protocol) information received from the remote device.
IPv4 address	This shows the IP address of the client.
	Click this icon to display a greater or lesser number of configuration fields.

### 5.2.2.1 Client Details

Click a client entry in the **Switch > Monitor > Client** screen to display individual client statistics.

Figure 41 Switch > Monitor > Client: Client Details



The following table describes the labels in this screen.

Table 28 Switch > Monitor > Client: Client Details

LABEL	DESCRIPTION
Basic Information	
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.
LLDP information	This shows the LLDP (Link Layer Discovery Protocol) information received from the remote device.

Table 28 Switch &gt; Monitor &gt; Client: Client Details (continued)

LABEL	DESCRIPTION
Manufacturer	This shows the manufacturer of the client device.
Network	
IP address	This shows the IP address of the client.
MAC address	This shows the MAC address of the client.

## 5.2.3 Event Log

Use this screen to view switch log messages. You can enter the switch name, 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 42 Switch &gt; Monitor &gt; Event log

The screenshot shows the 'Switch - Event log' interface. At the top, there are navigation tabs: SITE-WIDE, AP, SWITCH (selected), GATEWAY, ORGANIZATION, and HELP. Below the tabs, there are search filters for Switch, Keyword, Priority, Category, and Tag, each with a dropdown menu set to 'Any'. A 'Before' filter is set to '2018-08-30 15:15' with a time range of '8h' and a 'Before' dropdown. A 'Search' button is visible. Below the filters, there are navigation buttons for 'Newer', 'Older', and 'Export'. The main content is a table with the following columns: Time, Priority, Switch, Tag, Category, and Detail. The table contains 10 rows of log entries. At the bottom, there are pagination controls showing '1' of 4 pages, a 'Go to' field with '1', and 'Results per page' set to '10'.

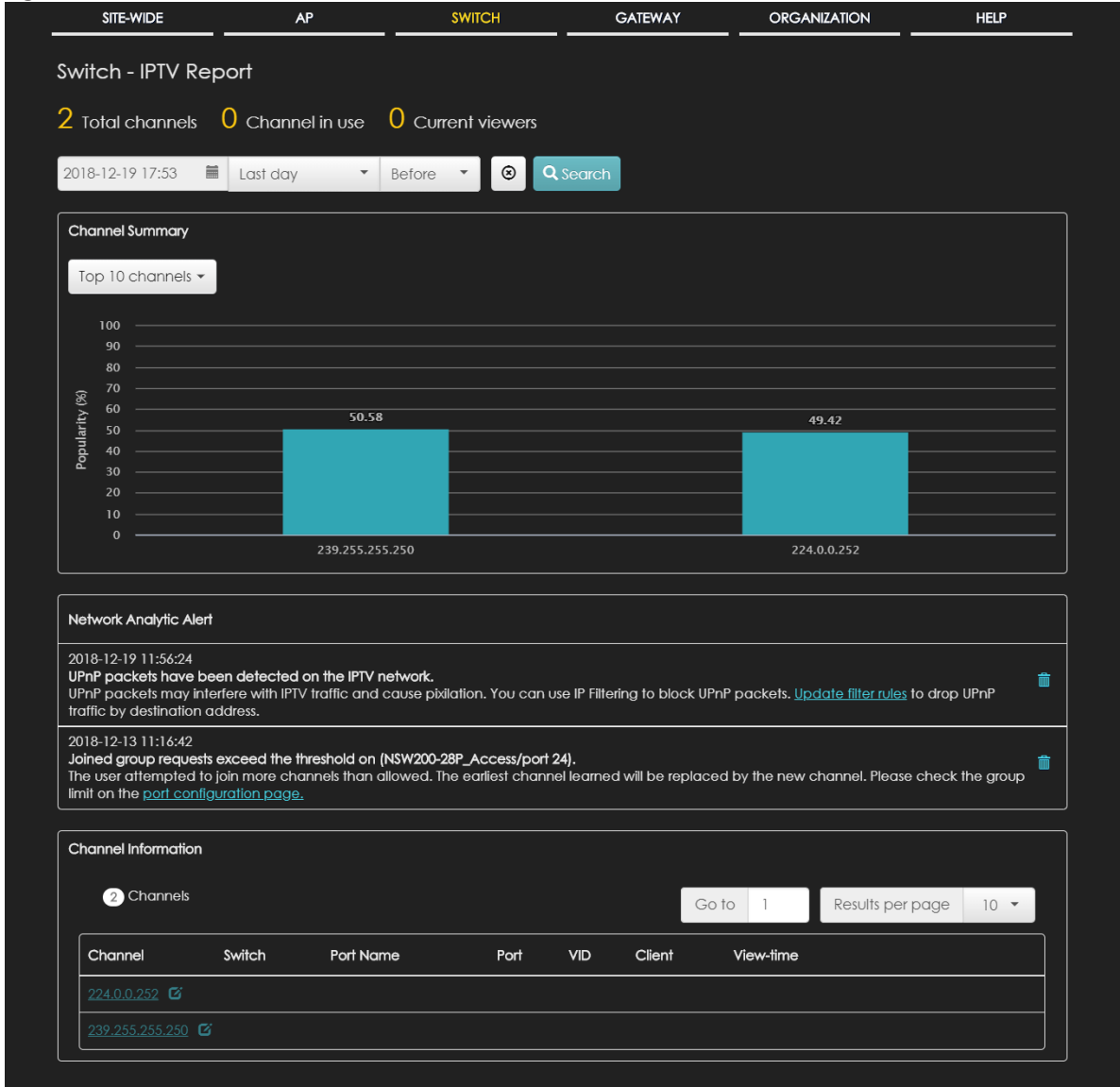
Time	Priority	Switch	Tag	Category	Detail
2018-08-30 08:22:59	INFO	NSW-Test	switch	SWITCH	Netconf client destroy, type = CLOUD
2018-08-30 08:22:59	INFO	NSW-Test	switch	SYSTEM	Cloud: close socket 8210, src_port 14939, dst 6667
2018-08-30 08:22:59	INFO	NSW-Test	switch	SYSTEM	Cloud: DNS query for d.nebula.zyxel.com
2018-08-30 08:23:01	INFO	NSW-Test	switch	SYSTEM	Cloud: Start TLS Handshake
2018-08-30 08:23:35	INFO	NSW-Test	switch	SWITCH	Netconf client destroy, type = CLOUD
2018-08-30 08:23:35	INFO	NSW-Test	switch	SYSTEM	Cloud: close socket 8210, src_port 15506, dst 6667
2018-08-30 08:23:35	INFO	NSW-Test	switch	SYSTEM	Cloud: DNS query for d.nebula.zyxel.com
2018-08-30 08:23:58	INFO	NSW-Test	switch	SYSTEM	Cloud: Start TLS Handshake
2018-08-30 08:24:31	INFO	NSW-Test	switch	SWITCH	Netconf client destroy, type = CLOUD
2018-08-30 08:24:31	INFO	NSW-Test	switch	SYSTEM	Cloud: close socket 8210, src_port 15512, dst 6667

## 5.2.4 IPTV Report

Use this screen to view available IPTV channels and client information.

Click **Switch > Monitor > IPTV Report** to access this screen.

Figure 43 Switch &gt; Monitor &gt; IPTV Report

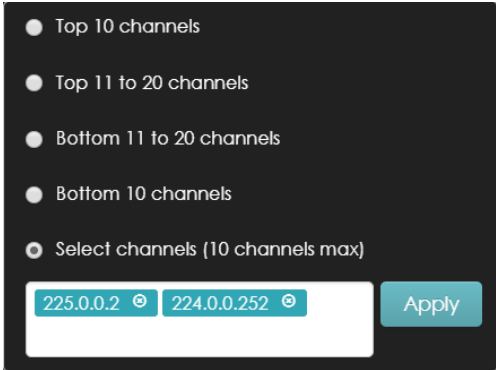


The following table describes the labels in this screen.

Table 29 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.
Channel Summary	

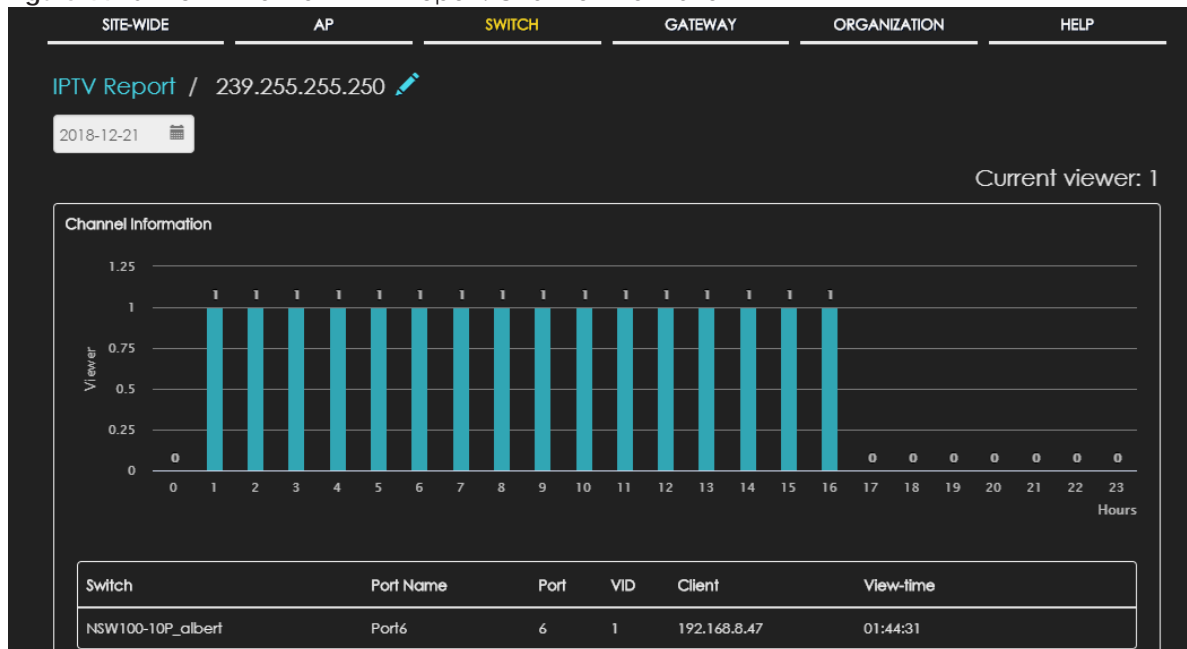
Table 29 Switch &gt; Monitor &gt; IPTV Report (continued)

LABEL	DESCRIPTION
	<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 switch 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 switch port results in loss of video quality.</p>
Channel Information	
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 5.2.4.1 on page 94</a>.</p>
Switch	This shows the name of the switch to which the client is connected.
Port Name	This shows the name of the switch port to which the client is connected.
Port	This shows the number of the switch port to which the client is connected.
VID	This shows the ID number of the VLAN to which the switch 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.

### 5.2.4.1 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 44 Switch &gt; Monitor &gt; IPTV Report: Channel Information



The following table describes the labels in this screen.

Table 30 Switch &gt; Monitor &gt; IPTV Report: Channel Information

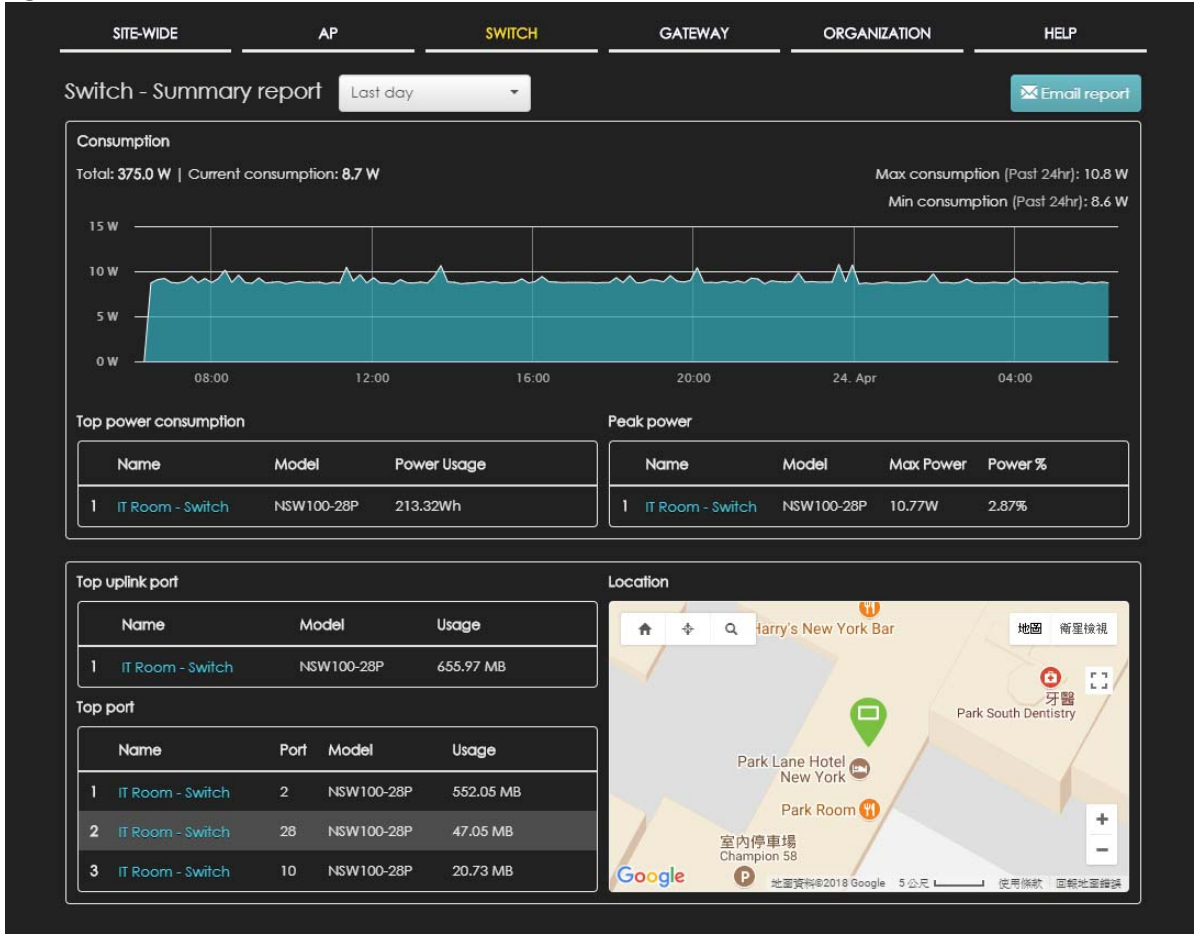
LABEL	DESCRIPTION
	Select a specific date to display only the clients who watch the IPTV channel on that day.
Current Viewer	This shows the number of clients who are currently watching the IPTV channel.
y-axis	The y-axis shows the number of clients watching the IPTV channel.
x-axis	The x-axis shows the hour of the day in 24-hour format.
Switch	This shows the name of the switch to which the client is connected.
Port Name	This shows the name of the switch port to which the client is connected.
Port	This shows the number of the switch port to which the client is connected.
VID	This shows the ID number of the VLAN to which the switch 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.

## 5.2.5 Summary Report

This screen displays network statistics for switches of the selected site, such as bandwidth usage, top ports and/or top switches.

Click **Switch > Monitor > Summary Report** to access this screen.

Figure 45 Switch > Monitor > Summary Report



The following table describes the labels in this screen.

Table 31 Switch > Monitor > Summary Report

LABEL	DESCRIPTION
Switch - Summary report	Select to view the report for the past day, week or month. Alternatively, select <b>Select 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;"> <ul style="list-style-type: none"> <li><input type="radio"/> Last day</li> <li><input type="radio"/> Last 7 days</li> <li><input type="radio"/> Last 30 days</li> <li><input checked="" type="radio"/> Select range ...</li> </ul> <p>Select a time range (6 months max):</p> <p>2018-04-29 <input type="text"/> to Now (2018-04-30)</p> <p>Report size: 10 results per table <input type="button" value="Update"/></p> </div>
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 switch ports.



Table 31 Switch &gt; Monitor &gt; Summary Report (continued)

LABEL	DESCRIPTION
Current Consumption	This shows the current power consumption of the switch ports.
Max Consumption	This shows the maximum power consumption of the switch ports.
Min Consumption	This shows the minimum power consumption of the switch 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 index number 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 device(s) during the specified period of time.
Peak Power	
	This shows the index number of the Nebula switch.
Name	This shows the descriptive name of the Nebula switch.
Model	This shows the model number of the Nebula switch.
Max Power	This shows the maximum power consumption for the Nebula switch's connected PoE device(s) during the specified period of time.
Power %	This shows what percentage of the Nebula switch's total power budget has been consumed.
Top uplink port	
	This shows the index number of the Nebula switch.
Name	This shows the descriptive name of the Nebula switch.
Model	This shows the model number of the Nebula switch.
Usage	This shows the amount of data that has been transmitted through the switch's uplink port.
Top port	
	This shows the index number of the Nebula switch port.
Name	This shows the descriptive name of the Nebula switch.
Port	This shows the port number on the Nebula switch.
Model	This shows the model number of the Nebula switch.
Usage	This shows the amount of data that has been transmitted through the switch's port.
Location	
This shows the location of the Nebula switches on the map.	

## 5.3 Configure

Use the **Configure** menus to configure port setting, IP filtering, RADIUS policies, PoE schedules, and other switch settings for switches of the selected site.

## 5.3.1 Switch Ports

Use this screen to view port summary and configure switch 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 46** Switch > Configure > Switch ports

Switch / Port	Port name	# Port	LLDP	Received bytes	Sent bytes	Connection	
IT Room Switch/1 Uplink <a href="#">details</a>	Uplink	1	nsg100	83.62 MB	42.95 MB	<div style="width: 100%; height: 10px; background-color: green;"></div>	Enabled
IT Room Switch/2 <a href="#">details</a>	Port2	2	Enabled	0 bytes	0 bytes	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Enabled
IT Room Switch/3, 5, 7 Static <a href="#">details</a>	Port3	3, 5, 7	Enabled	0 bytes	0 bytes	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Enabled
IT Room Switch/4 <a href="#">details</a>	Port4	4	NAP303	14.77 MB	54.31 MB	<div style="width: 100%; height: 10px; background-color: green;"></div>	4.80
IT Room Switch/6 <a href="#">details</a>	Port6	6	NAP203	25.46 MB	30.98 MB	<div style="width: 100%; height: 10px; background-color: green;"></div>	4.50
IT Room Switch/8 <a href="#">details</a>	Port8	8	Enabled	0 bytes	0 bytes	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Enabled
IT Room Switch/9 <a href="#">details</a>	Port9	9	Enabled	0 bytes	0 bytes	<div style="width: 0%; height: 10px; background-color: gray;"></div>	N/A
IT Room Switch/10 <a href="#">details</a>	Port10	10	Enabled	0 bytes	0 bytes	<div style="width: 0%; height: 10px; background-color: gray;"></div>	N/A

The following table describes the labels in this screen.


**Table 32** Switch > Configure > Switch ports

LABEL	DESCRIPTION
Switch ports	Select to view the detailed information and connection status of the switch port in the past two hours, day, week or month.
Edit	Select the port(s) you want to configure and click this button to configure switch settings on the port(s), 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 switch ports.
Switch ports	This shows the number of ports on the switch.
Export	Click this button to save the switch port list as a CSV or XML file to your computer.

Table 32 Switch &gt; Configure &gt; Switch ports (continued)

LABEL	DESCRIPTION
Switch/Port	<p>This shows the switch name and port number.</p> <p>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 via LACP (<b>LACP</b>). If the port is connected to a uplink gateway, it shows <b>Uplink</b>.</p> <p>Click <b>details</b> to display the port details screen. See <a href="#">Section 5.2.1.3 on page 86</a>.</p> <p>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.</p>
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.
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	<p>This shows the speed of the Ethernet connection on this port.</p> <p><b>Auto</b> (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support.</p>
Connection	<p>This shows the connection status of the port.</p> <ul style="list-style-type: none"> <li>• Gray: The port is disconnected.</li> <li>• Light blue: The port is blocked.</li> <li>• Orange: The port is connected and transmitting data at 10 or 100 Mbps.</li> <li>• Green: The port is connected and transmitting data at 1000 Mbps (1 Gbps).</li> <li>• Blue: The port is connected and transmitting data at 10000 Mbps (10 Gbps).</li> </ul> <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> ).

Table 32 Switch &gt; Configure &gt; Switch ports (continued)

LABEL	DESCRIPTION
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 switch 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 switch accepts per second on this port.
Multicast (pps)	This shows the maximum number of multicast packets the switch accepts per second on this port.
DLF (pps)	This shows the maximum number of DLF packets the switch accepts per second on this port.
Loop Guard	This shows whether loop guard is enabled or disabled on the port.
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.

### 5.3.1.1 Update ports

Select the port(s) you want to configure and click the **Edit** button in the **Switch > Configure > Switch ports** screen.

**Figure 47** Switch > Configure > Switch ports: Edit

The following table describes the labels in this screen.

**Table 33** Switch > Configure > Switch ports: Edit

LABEL	DESCRIPTION
Switch ports	This shows the switch name and port number for the port(s) you are configuring in this screen.
Name	Enter a descriptive name for the port(s).
Tags	Select or create a new tag for outgoing traffic on the port(s).
Enabled	Select to enable or disable the port(s). A port must be enabled for data transmission to occur.
RSTP	Select to enable or disable RSTP on the port(s).

Table 33 Switch &gt; Configure &gt; Switch ports: Edit (continued)

LABEL	DESCRIPTION
STP guard	<p>This field is available only when RSTP is enabled on the port(s).</p> <p>Select <b>Root guard</b> to prevent the switch(es) attached to the port(s) from becoming the root bridge.</p> <p>Select <b>BPDU guard</b> to have the switch shut down the port(s) if there is any BPDU received on the port(s).</p> <p>Otherwise, select <b>Disable</b>.</p>
LLDP	Select to enable or disable LLDP on the port(s).
PoE	Select <b>Enable</b> to provide power to a PD connected to the port(s).
Link	Select the speed and the duplex mode of the Ethernet connection on the port(s). 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).
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 switch enables PoE to provide power on the port(s).</p> <p>Note: You must select <b>Unschedule</b> in the <b>PoE schedule</b> field before you can disable PoE on the port(s).</p> <p>If you enable PoE and select <b>Unschedule</b>, PoE is always enabled on the port(s).</p>
Port Isolation	<p>Select to enable or disable port isolation on the port(s).</p> <p>The port(s) with port isolation enabled cannot communicate with each other. They can communicate only with the CPU management port of the same switch and the switch's other ports on which the isolation feature is not enabled.</p>
Bandwidth Control	Select to enable or disable bandwidth control on the port(s).
Ingress	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on the port(s).
Egress	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on the port(s).
Loop guard	<p>Select to enable or disable loop guard on the port(s).</p> <p>Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.</p>
Storm Control	Select to enable or disable broadcast storm control on the port(s).
Broadcast (pps)	Specifies the maximum number of broadcast packets the switch accepts per second on the port(s).
Multicast (pps)	Specifies the maximum number of multicast packets the switch accepts per second on the port(s).
DLF (pps)	Specifies the maximum number of DLF packets the switch accepts per second on the port(s).
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 single 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 switch or router.</p>
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>

Table 33 Switch &gt; Configure &gt; Switch ports: Edit (continued)

LABEL	DESCRIPTION
RADIUS policy	This field is available only when you select <b>Access</b> in the <b>Type</b> field.  Select the name of the pre-configured RADIUS policy that you want to apply to the port(s). Select <b>Open</b> if you don't want to enable port authentication on the port(s).
Allowed VLANs	This field is available only when you select <b>Trunk</b> in the <b>Type</b> field.  Specify the VLANs from which the traffic comes is allowed to be transmitted or received on the port(s).
IPTV Setting	
Overwrite advanced IGMP setting	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> .
Leave Mode	Select <b>Immediate Leave</b> to set the switch to remove this port from the multicast tree immediately when an IGMP leave message is received on this port. Select this option if there is only one host connected to this port.  Select <b>Normal Leave</b> or <b>Fast Leave</b> and enter an IGMP normal/fast leave timeout value to have the switch 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 switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.  In normal leave mode, when the Switch 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 Switch forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table.  In fast leave mode, right after receiving an IGMP leave message from a host on a port, the switch itself sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process.
Maximum Group	Select <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 switch are able to join.  Select the name of the IGMP filtering profile to use for this port. Otherwise, select <b>No Select</b> to have no restriction and allow the port to join any multicast group.
Fixed Router Port	Select <b>Auto</b> to have the switch use the port as an IGMP query port if the port receives IGMP query packets. The switch forwards IGMP join or leave packets to an IGMP query port.  Select <b>Fixed</b> to have the switch always use the port as an IGMP query port. This helps prevent IGMP network topology changes when query packet losses occur in the network.

### 5.3.2 IP Filtering

IP filtering lets you allow or block traffic according to the rule settings. Use this screen to configure IP filtering rules on the switches.

Click **Switch > Configure > IP filtering** to access this screen.

Figure 48 Switch &gt; Configure &gt; IP filtering

The following table describes the labels in this screen.

Table 34 Switch &gt; Configure &gt; IP filtering

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.
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	Enter the source IP address of the packets that you want to filter.
Src port	Enter the source port number(s) that defines the traffic type.
Destination	Enter the destination IP address of the packets that you want to filter
Dst port	Enter the destination port number(s) 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.

### 5.3.3 Advanced IGMP

A switch can passively snoop on IGMP packets transferred between IP multicast routers/switches 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 multicasting accordingly. IGMP snooping allows the switch to learn multicast groups without you having to manually configure them.

The switch 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 Switch.

Use this screen to enable IGMP snooping on the switches in the site, create IGMP filtering profiles and configure advanced IGMP snooping settings that apply to all ports on the switch 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 49** Switch > Configure > Advanced IGMP

The screenshot displays the 'Advanced IGMP' configuration page. At the top, there is a navigation bar with tabs for 'SITE-WIDE', 'AP', 'SWITCH' (highlighted), 'GATEWAY', 'ORGANIZATION', and 'HELP'. The main content area is titled 'Advanced IGMP' and contains several sections:

- IGMP snooping:** A toggle switch is set to 'ON'.
- IGMP-snooping VLAN:** Two radio buttons are present. 'Auto-detect' is selected. Below it is a text input field for 'User Assign VLANs'.
- Unknown multicast drop:** A toggle switch is set to 'ON'.
- IGMP filtering profiles:** A section with a header 'IGMP filtering profiles' and a sub-header 'IGMP filtering profiles'. Below this is a list of profiles, currently showing 'Block windows default used by 1 port'. There is an '+ Add' button.
- IPTV Topology Setup:** A section with tabs for 'IGMP Snooping', 'Role', and 'Port Setting'. Below these tabs is a table with columns: 'Switch Name', 'IGMP Snooping', 'Role', and 'Port Setting'. The table contains three rows: 'NSW100-28P\_Aggregator' (ON, Aggregator), 'NSW200-28P\_Access' (ON, Access), and 'NSW100-10P\_Querier' (ON, Querier). Each row has an 'Advanced Setup' button. Below the table is a sub-table for 'Querier' settings with columns: 'VLAN', 'Querier Ip Interface', and 'Mask'. It shows one entry with VLAN '2', Querier Ip Interface '2.2.2.2', and Mask '255.255.255.0'. There is an '+Add' button.

At the bottom of the page, there are 'Save' and 'Cancel' buttons, and a note: '(Please allow 1-2 minutes for changes to take effect.)'

The following table describes the labels in this screen.

Table 35 Switch > Configure > Advanced IGMP


LABEL	DESCRIPTION
IGMP snooping	Select <b>ON</b> to enable and configure IGMP snooping settings on all switches in the site. Select <b>OFF</b> to disable it.
IGMP-snooping VLAN	Select <b>Auto-detect</b> to have the switch learn multicast group membership information of any VLANs automatically.  Select <b>User Assigned VLANs</b> and enter the VLAN ID(s) to have the switch only learn multicast group membership information of the VLAN(s) that you specify.  Note: The switch can perform IGMP snooping on up to 16 VLANs.
Unknown multicast drop	Specify the action to perform when the switch receives an unknown multicast frame. Select <b>ON</b> to discard the frame(s). Select <b>OFF</b> to send the frame(s) to all ports.
IGMP filtering profiles	An IGMP filtering profile specifies a range of multicast groups that clients connected to the switch are able to join.  You can set the switch 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.
Edit	Click the edit icon to change the profile settings. See <a href="#">Section 5.3.3.1 on page 107</a> .
Remove	Click the remove icon to delete the profile.
Add	Click this button to create a new profile. See <a href="#">Section 5.3.3.1 on page 107</a> .
IPTV Topology Setup	
The following three buttons are available only when there are multiple switches in the site and your administrator account has full access to this screen.	
IGMP Snooping	Select the switch(es) you want to configure and click this button to turn on or off IGMP snooping on the selected switch(es).
Role	Select the switch(es) you want to configure and click this button to change the IGMP role of the selected switch(es).
Port Setting	Select the switch(es) 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 switch(es). See <a href="#">Section 5.3.3.2 on page 107</a> .
The following list shows you the IGMP settings for each switch in the site.	
Switch Name	This shows the name of the switch in the site.
IGMP Snooping	This shows whether IGMP snooping is enabled or not on the switch.
Role	This shows whether the switch is acting as an IGMP snooping querier, aggregation switch or access switch in the IPTV network. Click the question mark to view more information about IGMP roles.
Port Setting	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 switch. See <a href="#">Section 5.3.3.2 on page 107</a> .
	Click this icon to display a greater or lesser number of configuration fields.
The following fields display when the IGMP role of a switch is set to <b>Querier</b> .	
VLAN	Enter the ID number of the VLAN on which the switch learns the multicast group membership.
Querier IP Interface	Enter the IP address of the switch interface in IGMP querier mode.  The switch 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 switch interface in IGMP querier mode.

Table 35 Switch &gt; Configure &gt; Advanced IGMP (continued)

LABEL	DESCRIPTION
Remove	Click the remove icon to delete the rule.
Add	Click this button to create a new rule.

### 5.3.3.1 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 50 Switch &gt; Configure &gt; Advanced IGMP: Add IGMP Filtering Profile

The following table describes the labels in this screen.

Table 36 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.
Add Rule	Click this button to create a new rule in this profile.
Close	Click this button to exit this screen without saving.
Save & Back	Click this button to save your changes and close the screen.

### 5.3.3.2 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 switch. To access this screen, select one or more switches and click the **Port Setting** button or click a switch's **Advanced Setup** button in the **IPTV Topology Setup** section of the **Switch > Configure > Advanced IGMP** screen.

**Figure 51** Switch > Configure > Advanced IGMP: Port Settings

The following table describes the labels in this screen.

**Table 37** Switch > Configure > Advanced IGMP: Port Settings

LABEL	DESCRIPTION
Switch name	This shows the name of the switch(es) that you select to configure.
Role	This shows whether the switch(es) you selected is an IGMP snooping querier, aggregation switch or access switch in the IPTV network.
Leave Mode	<p>Select <b>Immediate Leave</b> to set the switch 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 switch 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 switch 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 normal leave mode, when the Switch 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 Switch 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 fast leave mode, right after receiving an IGMP leave message from a host on a port, the switch 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 switch 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 have no restriction 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.

## 5.3.4 RADIUS Policy

Use this screen to configure port authentication to validate access to ports on the switch using an external RADIUS server.

Click **Switch > Configure > RADIUS policy** to access this screen.

**Figure 52** Switch > Configure > RADIUS policy

The following table describes the labels in this screen.

**Table 38** Switch > Configure > RADIUS policy

LABEL	DESCRIPTION
Password for MAC-Base Auth	Type the password the switch 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 port(s) based on the MAC address and password of the client. Select <b>802.1x</b> if you want to validate access to the port(s) based on the user name and password provided by the client.
Guest VLAN	A guest VLAN is a pre-configured VLAN on the switch that allows non-authenticated users to access limited network resources through the switch. Enter the number that identifies the guest VLAN.
Port security	Click <b>On</b> to enable port security on the port(s). Otherwise, select <b>Off</b> to disable port security on the port(s).

Table 38 Switch &gt; Configure &gt; RADIUS policy (continued)

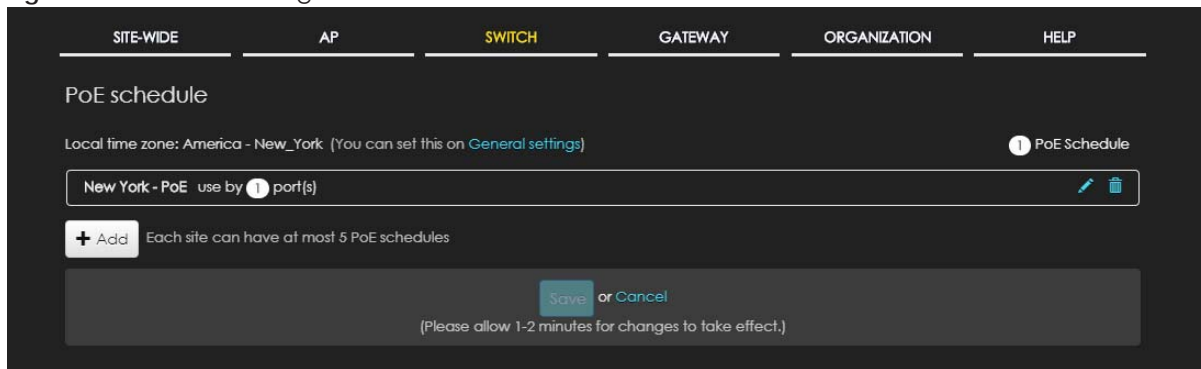
LABEL	DESCRIPTION
Limited numbers of MAC address	This field is configurable only when you enable port security. Specify the maximum number of MAC addresses that may be learned on a port.
Switch ports	This shows the number of the switch ports to which this policy is applied.
Add	Click this button to create a new policy.

### 5.3.5 PoE Schedule

Use this screen to view and configure the schedules which can be applied to the ports. PoE is enabled at the specified time/date. Click **Switch > Configure > PoE schedule** to access this screen.

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 5.3.5.1 on page 110](#).

Figure 53 Switch &gt; Configure &gt; PoE schedule



#### 5.3.5.1 Create new schedule

Click the **Add** button in the **Switch > Configure > PoE schedule** screen to access this screen.

**Figure 54** Switch > Configure > PoE schedule: Add

The following table describes the labels in this screen.

**Table 39** Switch > Configure > PoE schedule: Add

LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identifying 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 on this day. Otherwise, select <b>Off</b> to turn PoE off.
From - To	Specify the hour and minute when the schedule begins and ends each day
Time display	Select the time format in which the time is displayed.
Close	Click this button to exit this screen without saving.
Add	Click this button to save your changes and close the screen.

### 5.3.6 Switch Configuration

Use this screen to configure global switch settings, such as (R)STP, QoS, port mirroring, authentication servers, voice VLAN and DHCP server guard.

Click **Switch > Configure > Switch configuration** to access this screen.

Figure 55 Switch > Configure > Switch configuration

SITE-WIDE
AP
SWITCH
GATEWAY
ORGANIZATION
HELP

### Switch configuration

**VLAN configuration**

Management VLAN

**STP configuration**

Rapid spanning tree protocol (RSTP)

STP bridge priority

Switches	Bridge priority
Default	32768

[+ Set the bridge priority for another switch](#)

STP ensures a loop-free network topology for Ethernet networks. Ethernet switch determines the root bridge based on the switch with the lowest bridge ID, which comprises of STP bridge priority and its MAC address. The default bridge priority is 32768 and can be configurable in multiple of 4096.

**Quality of service**

Quality of service (No traffic will be prioritized)

QoS allows network traffic prioritization based on application and service demands. IEEE802.1P defines eight priority levels to be mapped to different class of service (CoS) queue upon traffic prioritization.

[+ Add](#)

**Port mirroring**

Port mirroring (No traffic will be mirrored)

[+ Add](#)

**Authentication servers**

RADIUS server (No RADIUS server)

[+ Add](#)

**Voice VLAN**

Voice VLAN  OFF

**DHCP Server Guard**

DHCP Server Guard  OFF

Save
or Cancel

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



The following table describes the labels in this screen.

Table 40 Switch > Configure > Switch configuration

LABEL	DESCRIPTION
VLAN configuration	
Management VLAN	Enter the VLAN identification number associated with the switch 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 switch 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 switch. Otherwise, select <b>Off</b> .
STP bridge priority	<p>Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.</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 switch(es) 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 switch 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 switch 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 port(s), and also enter the source port on which you mirror the traffic.</p>
Authentication servers	
RADIUS server	<p>Click <b>Add</b> to create a new RADIUS server entry.</p> <p>Enter the IP address of an external RADIUS server, the port of the RADIUS server for authentication (default 1812), and a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch.</p>
Voice VLAN	
Voice VLAN	<p>Select <b>On</b> to enable the Voice VLAN feature on the switch. 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 switch port.</p>
Voice VLAN ID	Enter a VLAN ID number.
Priority	Select the priority level of the Voice VLAN from 1 to 6.
OUI	<p>Click the button to add MAC address of IP phones from specific manufacturers by using its ID from the Organizationally Unique Identifiers (OUI). You also need to type the mask for the specified MAC address to determine which bits a packet's MAC address should match.</p> <p>Enter "f" for each bit of the specified MAC address that the IP phone's MAC address should match. Enter "0" for the bit(s) of the IP phone's MAC address, which can be of any hexadecimal character(s).</p>

Table 40 Switch &gt; Configure &gt; Switch configuration (continued)

LABEL	DESCRIPTION
DHCP Server Guard	
DHCP Server Guard	Select <b>On</b> to enable the DHCP server guard feature on the switch in order to prevent illegal DHCP servers. Only the first DHCP server that assigned the switch IP address is allowed to assign IP addresses to devices in this management VLAN.  Otherwise, select <b>Off</b> to disable it.

# CHAPTER 6

## Gateway

### 6.1 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.

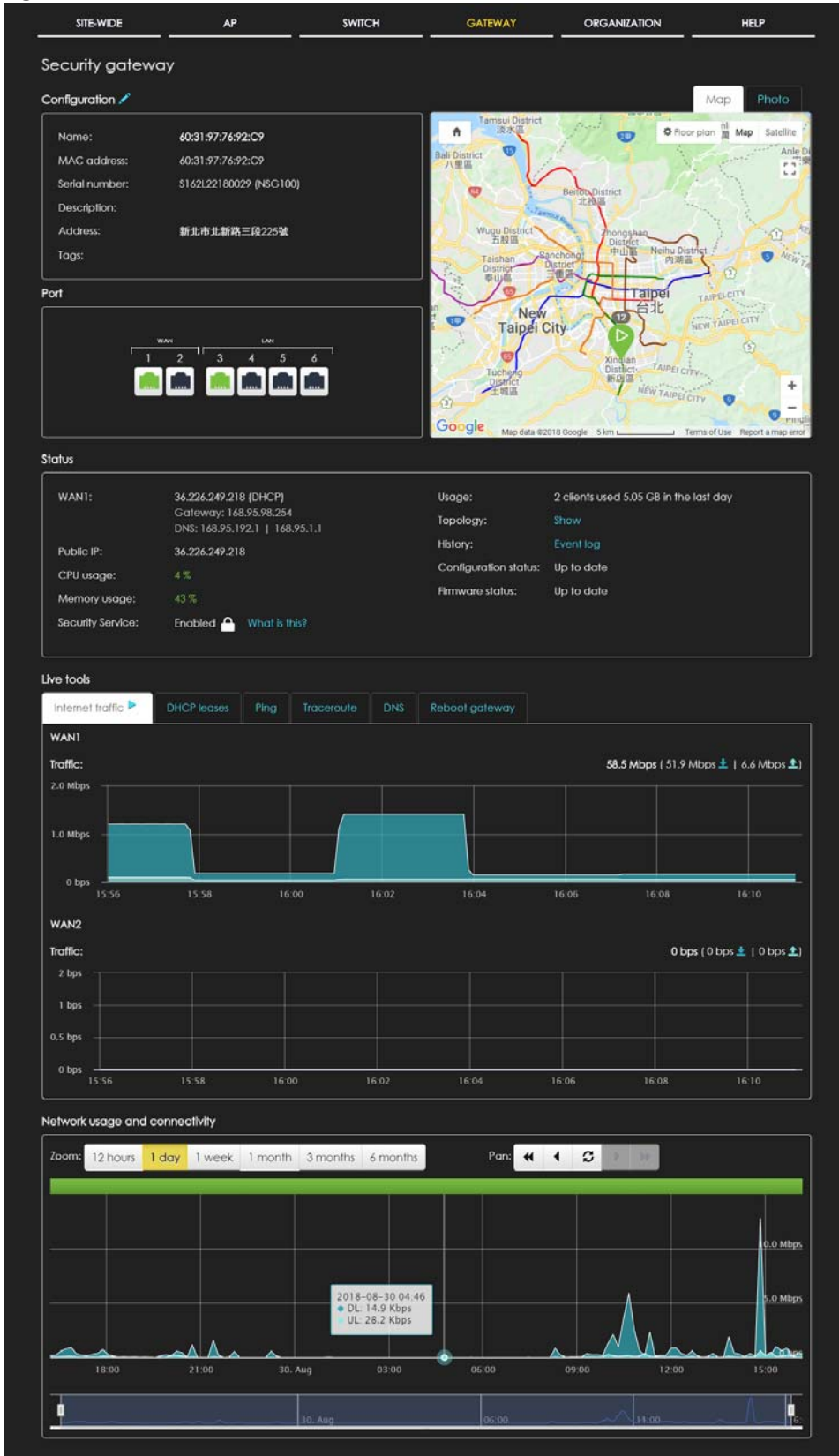
### 6.2 Monitor

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.

#### 6.2.1 Security Gateway

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

Figure 56 Gateway > Monitor > Security Gateway



The following table describes the labels in this screen.

Table 41 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.
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.
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 and DNS 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 security services are enabled on the gateway. Click <b>What is this?</b> to view the type of enabled security services.
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 3.1.4 on page 38</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 status	This shows whether the firmware installed on the gateway is up-to-date.
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.
Trace route	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.
Network usage and connectivity	
Move the cursor over the chart to see the transmission rate at a specific time.	

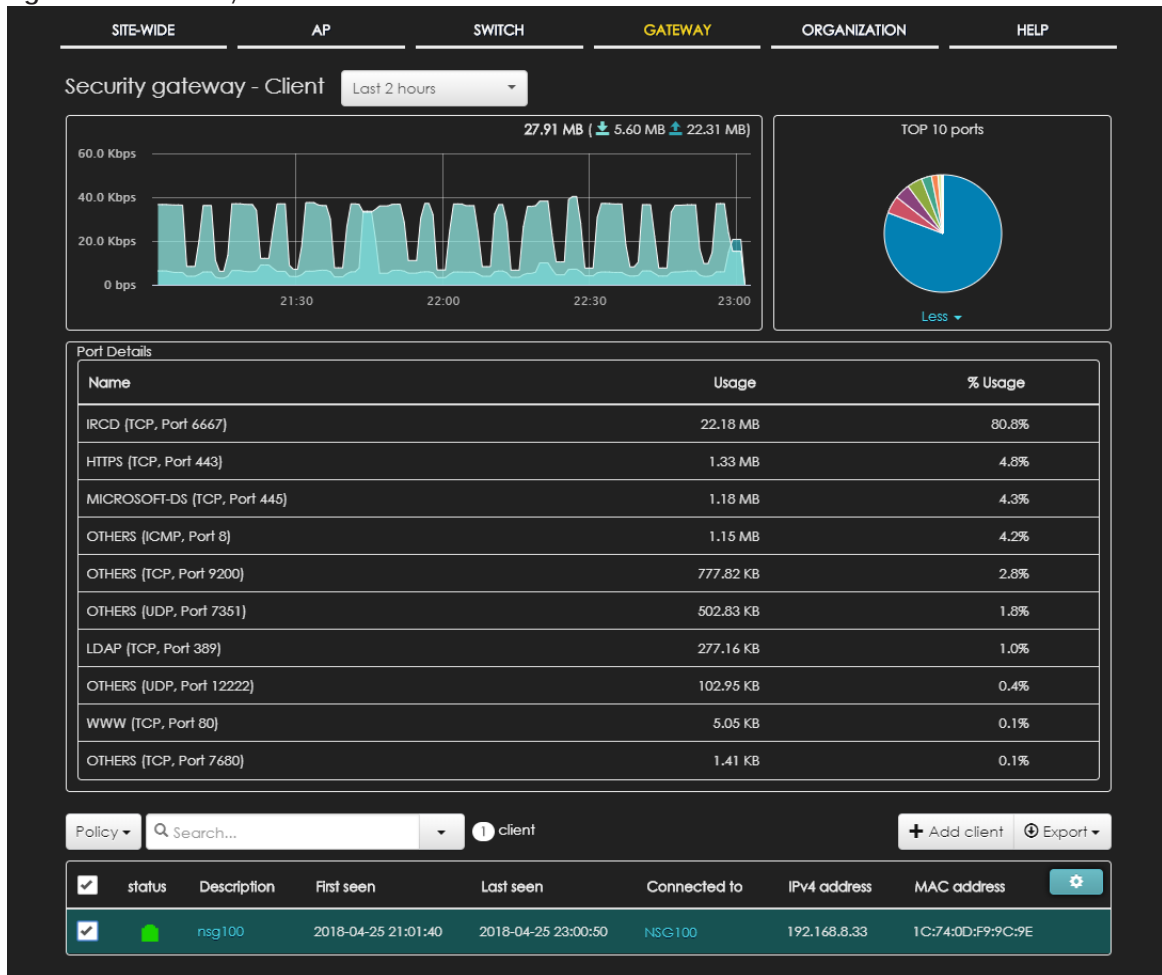
Table 41 Gateway &gt; Monitor &gt; Security Gateway (continued)

LABEL	DESCRIPTION
Zoom	Select to view the statistics in the past twelve hours, day, week, month, three months or six months.
Pan	Click to move backward or forward by one day or week.

## 6.2.2 Client

This screen allows you to view the connection status and detailed information about a client in the selected site. Click **Gateway > Monitor > Client** to access this screen.

Figure 57 Gateway &gt; Monitor &gt; Client

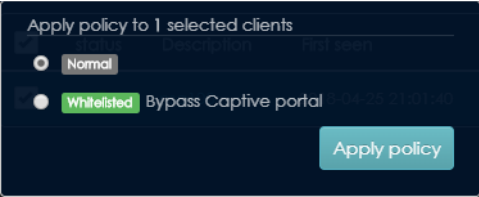



The following table describes the labels in this screen.

Table 42 Gateway &gt; Monitor &gt; Client

LABEL	DESCRIPTION
Security Gateway - Client	Select to view the device information and connection status in the past two hours, day, week or month.
y-axis	The y-axis shows the transmission speed of data sent or received by the client in kilobits per second (Kbps).

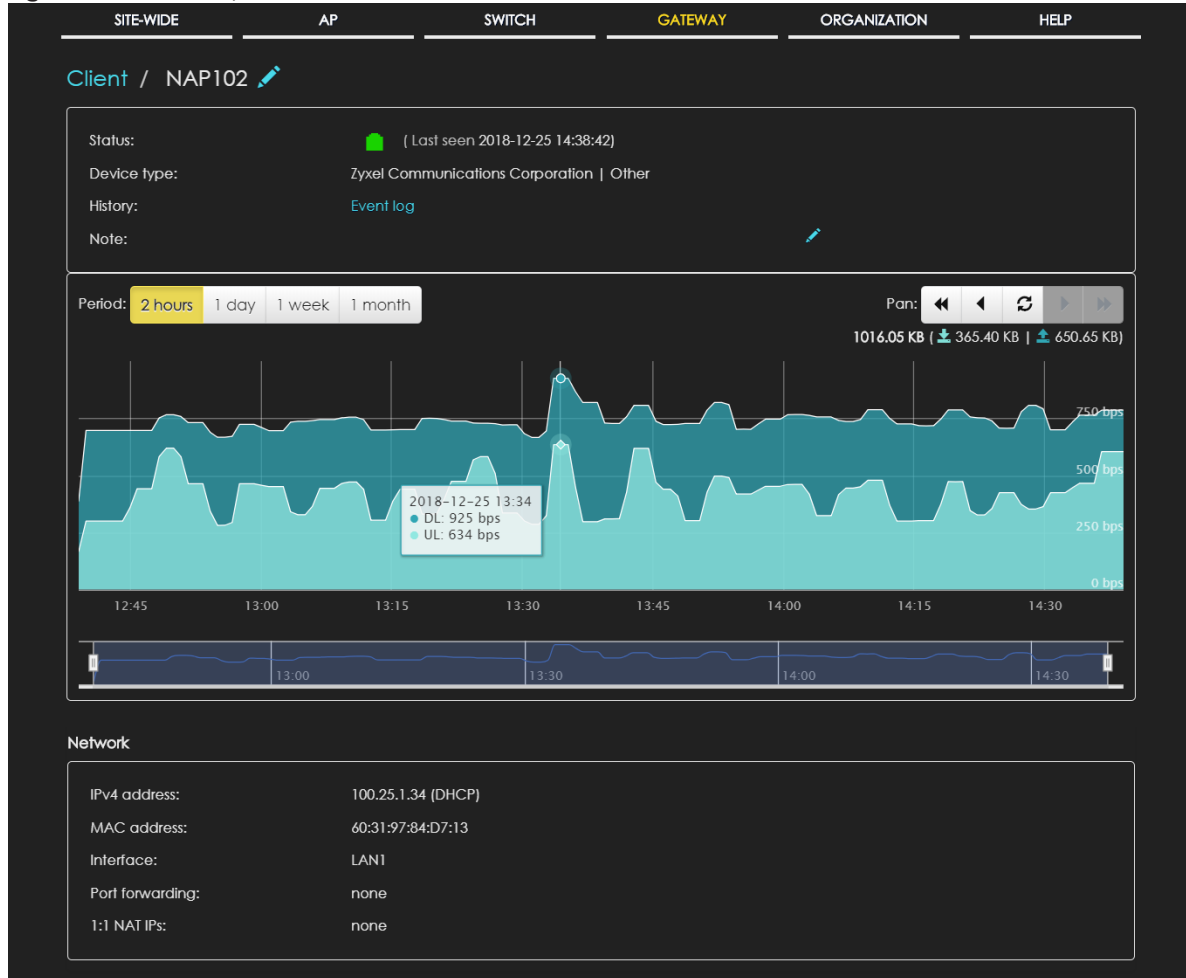
Table 42 Gateway &gt; Monitor &gt; Client (continued)

LABEL	DESCRIPTION
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Top 10 Ports	This shows top ten applications/services and the ports that identify a service. Click <b>More</b> to display port details. Click <b>Less</b> to hide them.
Port Details	
Name	This shows the service name and the associated port number(s).
Usage	This shows the amount of data consumed by the service.
% Usage	This shows the percentage of usage for the service.
Policy	Select the client(s) from the table below, and then choose the security policy that you want to apply to the selected client(s). To allow the selected clients to bypass captive portal authentication, choose <b>Whitelisted</b> . Otherwise, choose <b>Normal</b> and click <b>Apply policy</b> . 
Search	Specify your desired filter criteria to filter the list of clients.
client	This shows the number of clients connected to 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 switch'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 goes off-line (red).
Description	This shows the descriptive name of the client. Click the name to display the individual client statistics. See <a href="#">Section 6.2.2.1 on page 120</a> .
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.
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.
IPv4 address	This shows the IP address of the client.
MAC address	This shows the MAC address of the client. Click the MAC address to display the individual client statistics. See <a href="#">Section 6.2.2.1 on page 120</a> .
OS	This shows the operating system running on the client device.
Manufacturer	This shows the manufacturer of the client device.
Note	This shows additional information for the client.
Usage	This shows the amount of data transmitted by the client.
User	This shows the number of users currently connected to the network through the client device.
Interface	This shows the interface on the security gateway to which the client belongs.
Policy	This shows the security policy applied to the client.
	Click this icon to display a greater or lesser number of configuration fields.

### 6.2.2.1 Client Details

Click a client's descriptive name in the **Gateway > Monitor > Client** screen to display individual client statistics.

**Figure 58** Gateway > Monitor > Client: Client Details



The following table describes the labels in this screen.

**Table 43** Gateway > Monitor > Client: Client Details

LABEL	DESCRIPTION
Client	Click the edit icon to change the client name.
Status	This shows whether the client is online (green), or goes off-line (red). It also shows the last date and time the client was discovered.
Device type	This shows the manufacturer of the client device.
History	Click <b>Event log</b> to go to the <b>Gateway &gt; Monitor &gt; Event log</b> screen.
Note	This shows additional information for the client. Click the edit icon to modify it.
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.
y-axis	The y-axis shows the transmission speed of data sent or received by the client in kilobits per second (Kbps).



Table 43 Gateway &gt; Monitor &gt; Client: Client Details (continued)

LABEL	DESCRIPTION
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.
Interface	This shows the interface on the security gateway to which the client belongs.
Port forwarding	This shows the public IP address or DDNS host name and port mapping information if there is a virtual server rule configured for this client.
1:1 NAT IPs	This shows the public IP address information if there is a 1:1 NAT rule configured for this client.

## 6.2.3 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 even a time range to display only the log messages related to it.

Click **Gateway > Monitor > Event Log** to access this screen.

Figure 59 Gateway &gt; Monitor &gt; Event log

Security gateway - Event log

Keyword:  Category:  Before:   Before

< Newer Older > 1815 Event logs

Time	Category	Source	Destination	Detail
2018-08-30 15:33:49	client-status			Client is connected to lan1, IP address is 192.168.16.33, MAC address is 04:bf:6d:1f:c6:45
2018-08-30 15:34:11	client-status			Client was disconnected from lan1, IP address is 192.168.16.34, MAC address is 58:8b:f3:91:4d:31
2018-08-30 15:34:11	client-status			Client was disconnected from lan1, IP address is 192.168.16.51, MAC address is 80:b0:3d:68:59:12
2018-08-30 15:34:11	client-status			Client was disconnected from lan1, IP address is 192.168.16.62, MAC address is 28:b2:bd:5b:32:2c
2018-08-30 15:34:11	client-status			Client was disconnected from lan1, IP address is 192.168.16.74, MAC address is d8:8f:76:76:17:ce
2018-08-30 15:34:11	client-status			Client was disconnected from vlan201, IP address is 192.168.201.21, MAC address is f0:98:9d:6f:77:01
2018-08-30 15:34:15	client-status			Client is connected to lan1, IP address is 192.168.16.34, MAC address is 58:8b:f3:91:4d:31
2018-08-30 15:34:17	client-status			Client is connected to lan1, IP address is 192.168.16.36, MAC address is 24:18:1d:ab:d6:2b
2018-08-30 15:34:23	client-status			Client is connected to lan1, IP address is 192.168.16.64, MAC address is 1c:87:2c:d6:d5:22
2018-08-30 15:34:25	client-status			Client is connected to lan1, IP address is 192.168.16.62, MAC address is 28:b2:bd:5b:32:2c

1 2 3 4 5 ... 12 13 Go to 1 Results per page 10

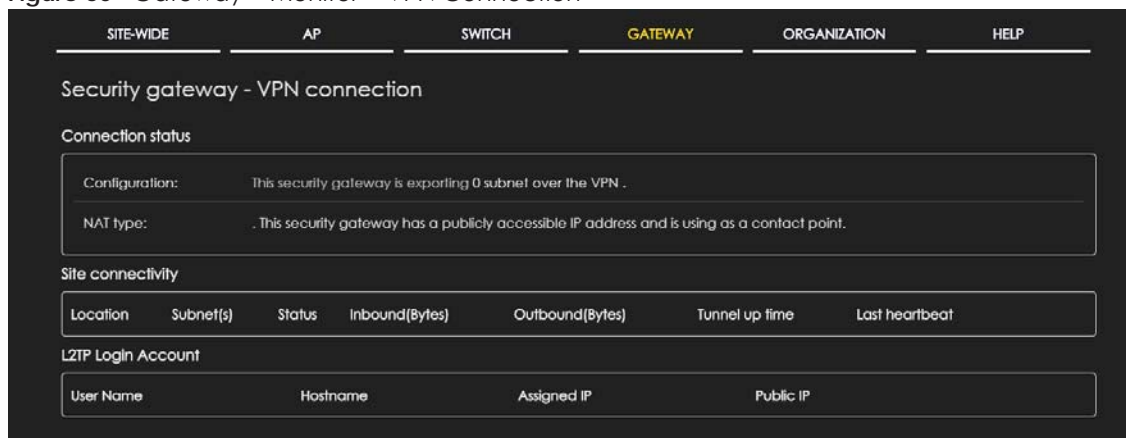
## 6.2.4 VPN Connection

Use this screen to view status of the site-to-site IPsec VPN connections and L2TP VPN sessions.

Note: If the peer gateway is not a Nebula device, go to the **Gateway > Configure > Site-to-Site VPN** screen to view and configure a VPN rule. See [Section 6.3.5 on page 146](#) for more information.

Click **Gateway > Monitor > VPN Connection** to access this screen.

**Figure 60** Gateway > Monitor > VPN Connection



The following table describes the labels in this screen.

**Table 44** Gateway > Monitor > VPN Connection

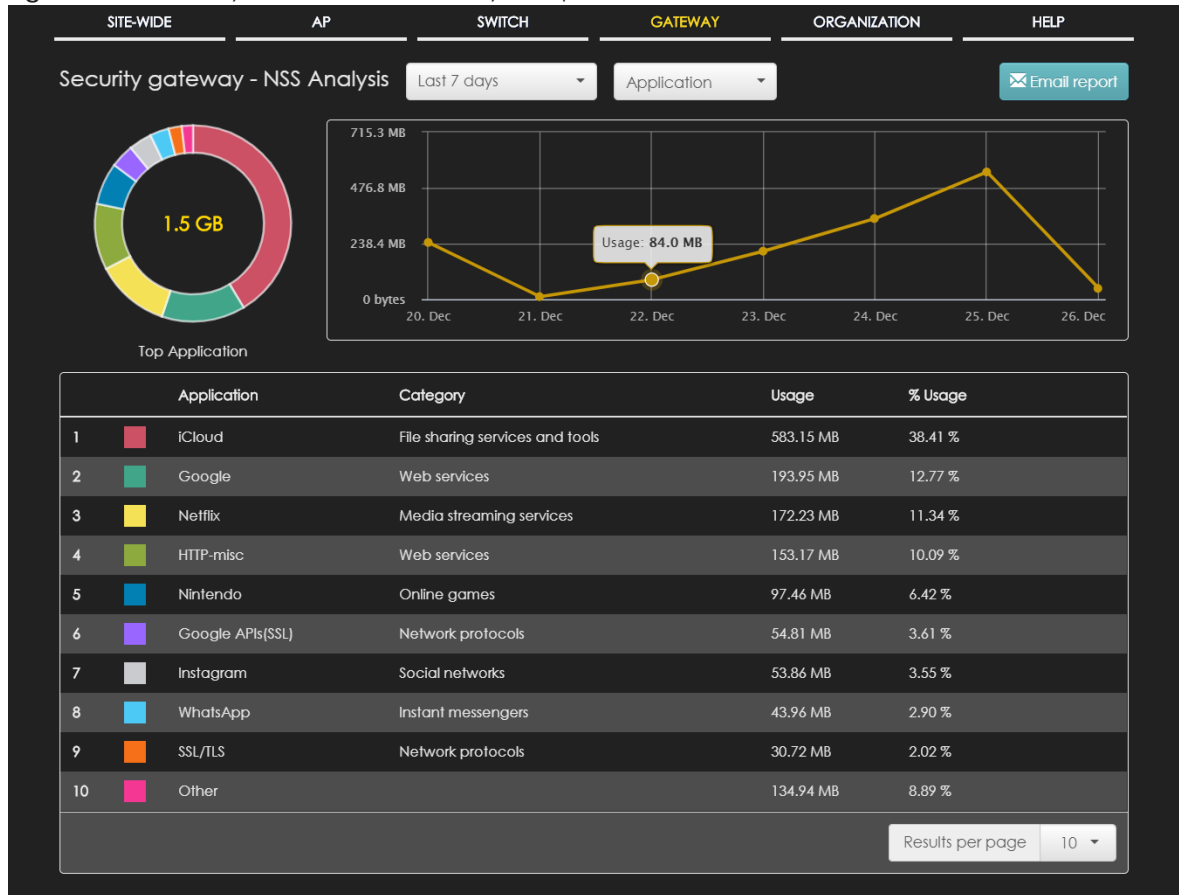
LABEL	DESCRIPTION
Connection Status	
Configuration	This shows the number and address of the local network(s) behind the security gateway, on which the computers are allowed to use the VPN tunnel.
NAT Type	This shows the public IP address or the domain name that is configured and mapped to the security 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>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 network(s) 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.
L2TP 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.
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.

## 6.2.5 NSS Analysis Report

Use this screen to view the statistics report for NSS (Nebula Security Service). The screen varies depending on the service type (**Application**, **Content Filtering**, or **Anti-Virus**) you select.

Click **Gateway** > **Monitor** > **NSS Analysis Report** to access this screen.

**Figure 61** Gateway > Monitor > NSS Analysis Report



The following table describes the labels in this screen.

Table 45 Gateway > Monitor > NSS Analysis Report

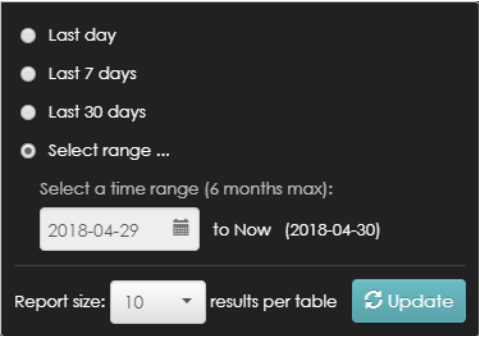
LABEL	DESCRIPTION
Security Gateway - NSS Analysis	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Select range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
	Select the type of service 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 a specific segment of the donut chart to view the IPv4 addresses of the clients who use that application. Click the number in the center of the donut 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.
IPv4 Address	<p>This shows the IPv4 address of the client who used the application.</p> <p>This field is available when you click a specific segment of the donut chart.</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 specific segment of the donut chart to view the IPv4 addresses of the clients who tried to access that web page. Click the number in the center of the donut 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.
IPv4 Address	<p>This shows the IPv4 address of the client who tried to access the web page.</p> <p>This field is available when you click a specific segment of the donut chart.</p>
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.

Table 45 Gateway &gt; Monitor &gt; NSS Analysis Report (continued)

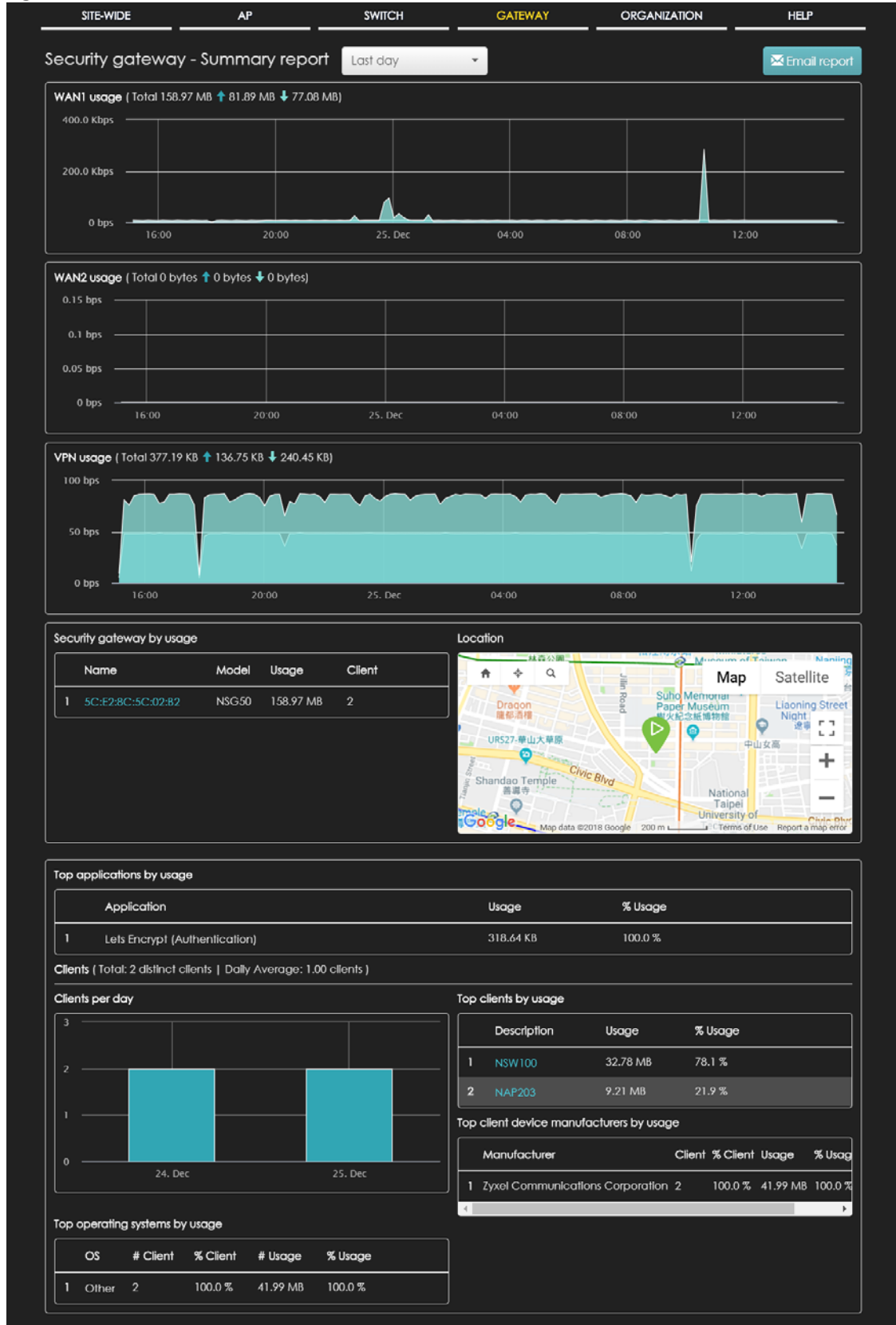
LABEL	DESCRIPTION
Anti-Virus	The following fields displays when you select to view the anti-virus statistics. Click a specific segment of the donut chart to view the IPv4 addresses of the clients who sent the virus. Click the number in the center of the donut chart to switch back to the previous screen.
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.
IPv4 Address	This shows the IPv4 address of the virus sender. This field is available when you click a specific segment of the donut chart.
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.

## 6.2.6 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 **Gateway > Monitor > Summary Report** to access this screen.

Figure 62 Gateway > Monitor > Summary Report



The following table describes the labels in this screen.

Table 46 Gateway > Monitor > Summary Report

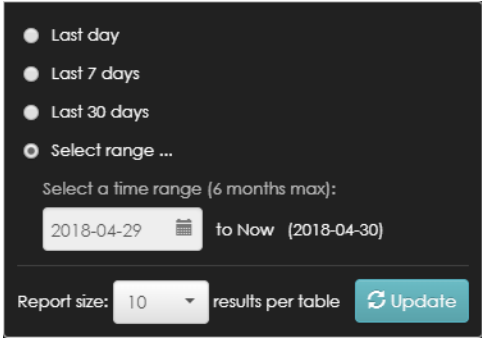
LABEL	DESCRIPTION
Security gateway - Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select <b>Select range...</b> to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click 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.
Usage	This shows the amount of data consumed by the application.
% Usage	This shows the percentage of usage for the application.
Clients	
Total	This shows the total number of clients connected to the Nebula device within the specified time period.
Daily Average	This shows the average daily number of clients within the specified time period.
Clients per day	
y-axis	The y-axis represents the number of clients.
x-axis	The x-axis represents the date.

Table 46 Gateway &gt; Monitor &gt; Summary Report (continued)

LABEL	DESCRIPTION
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	his shows the percentage of usage for the client device.

## 6.3 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 gateway of the selected site.

### 6.3.1 Interfaces 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 **Gateway > Configure > Interfaces addressing**.



Figure 63 Gateway &gt; Configure &gt; Interfaces addressing

The screenshot shows the 'Interfaces addressing' configuration page. At the top, there are navigation tabs: SITE-WIDE, AP, SWITCH, GATEWAY (highlighted), ORGANIZATION, and HELP. The main content is organized into several sections:

- Network wide:** Contains a 'Mode' section with two radio buttons: 'Network address translation (NAT)' (selected) and 'Router'. Below each radio button is a descriptive paragraph explaining the traffic handling.
- Port Group Setting:** A grid of radio buttons. The top row is for 'Port Group 1' and the bottom row is for 'Port Group 2'. The columns are labeled 'P3', 'P4', 'P5', and 'P6'. In the 'Port Group 1' row, the radio for P4 is selected. In the 'Port Group 2' row, the radio for P3 is selected.
- Interface:** A table with columns: Name, IP address, Subnet mask, VLAN ID, Port Group, and Guest. It lists two interfaces: LAN1 (100.24.1.1) and LAN2 (173.16.24.1). Each interface has a dropdown for 'Port Group' (set to 'Port Group 1' and 'Port Group 2' respectively) and a 'Guest' toggle (set to 'OFF'). There are '+Add' and 'Edit' buttons for each row.
- Static Route:** A table with columns: Name, Destination, Subnet mask, and Next hop IP. It includes a '+Add' button.
- Dynamic DNS:** A section with a toggle for 'Automatic registration' (set to 'OFF') and a descriptive paragraph.

The following table describes the labels in this screen.

Table 47 Gateway &gt; Configure &gt; Interfaces addressing

LABEL	DESCRIPTION
Network wide	
Mode	Select <b>Network address translation (NAT)</b> to have the gateway automatically use SNAT for traffic it routes from internal interfaces to external interfaces.  Select <b>Router</b> to have the gateway forward packets according to the routing policies. The gateway doesn't automatically convert a packet's source IP address.
Port Group Setting	Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.  The physical Ethernet ports are shown at the top and the port groups are shown at the bottom of the screen. Use the radio buttons to select for which port group (network) you want to use each physical port.  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.

Table 47 Gateway &gt; Configure &gt; Interfaces addressing (continued)



LABEL	DESCRIPTION
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	This shows the ID number of the VLAN with which the interface (network) is associated.
Port group	This shows the name of the port group to which the interface (network) belongs.
Guest	Select <b>On</b> to configure the interface as a Guest interface. Devices connected to a Guest interface will have Internet access but cannot communicate with each other directly or access network sources behind the gateway,  Otherwise, select <b>Off</b> to not use the interface as a Guest interface.
Edit	Click this button to modify the network settings. See <a href="#">Section 6.3.1.1 on page 132</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 6.3.1.1 on page 132</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 interface(s). It helps forward packets to their destinations.
	Click this icon to remove a static route.
Add	Click this button to create a new static route. See <a href="#">Section 6.3.1.3 on page 135</a> for detailed information
Dynamic DNS	
Automatic registration	Click <b>On</b> to use dynamic DNS. Otherwise, select <b>Off</b> to disable it.
General Settings	
DDNS provider	Select your Dynamic DNS service provider from the drop-down list box.  If you select <b>User custom</b> , create your own DDNS service
DDNS type	Select the type of DDNS service you are using.  Select <b>User custom</b> to create your own DDNS service and configure the <b>DYNDNS Server</b> , <b>URL</b> , and <b>Additional DDNS Options</b> fields below.
DDNS account	
Username	Enter the user name used when you registered your domain name.
Password	Enter the password provided by the DDNS provider.
Confirm password	Enter the password again to confirm it.
DDNS settings	
Domain name	Enter the domain name you registered.
Primary binding address	Use these fields to set how the 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.

Table 47 Gateway &gt; Configure &gt; Interfaces addressing (continued)

LABEL	DESCRIPTION
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 subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, <code>www.yourhost.dyndns.org</code> and still reach your hostname.</p>
Mail exchanger	<p>This option is only available with a DynDNS account.</p> <p>DynDNS can route e-mail for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes e-mail for <code>john-doe@yourhost.dyndns.org</code> to the host record specified as the mail exchanger.</p> <p>If you are using this service, type the host record of your mail server here. Otherwise, leave the field blank.</p>
Backup mail exchanger	<p>This option is only available with a DynDNS account.</p> <p>Select this check box if you are using DynDNS's backup service for 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>
URL	<p>This field displays when you select <b>User custom</b> from the <b>DDNS provider</b> field above.</p> <p>Type the URL that can be used to access the server that will host the DDSN service.</p>
Additional DDNS Options	<p>This field displays when you select <b>User custom</b> from the <b>DDNS provider</b> field above.</p> <p>These are the options supported at the time of writing:</p> <ul style="list-style-type: none"> <li>• <code>dyndns_system</code> to specify the DYNDNS Server type - for example, <code>dyndns@dyndns.org</code></li> <li>• <code>ip_server_name</code> which should be the URL to get the server's public IP address - for example, <code>http://myip.easylife.tw/</code></li> </ul>

### 6.3.1.1 Local LAN

Click the **Add** button or click the **Edit** button in the **Interface** section of the **Gateway > Configure > Interfaces addressing** screen.

**Figure 64** Gateway > Configure > Interfaces addressing: Local LAN

Local LAN
✕

---

**Interface properties**

Interface name

**IP address assignment**

IP address

Subnet mask

VLAN ID  (1-4094)

Port group

**DHCP setting**

DHCP

IP pool start address  Pool size

First DNS server

Second DNS server

Third DNS server

First WINS server  (Optional)

Second WINS server  (Optional)

Lease time

Infinite

days  hours (Optional)  minutes (Optional)

Extended options

Static DHCP Table

IP address	MAC	Description
<input type="text"/>	<input type="text"/>	<input type="text"/> ✕

The following table describes the labels in this screen.

Table 48 Gateway > Configure > Interfaces addressing: Local LAN

LABEL	DESCRIPTION
Interface properties	
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.)
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 server(s) 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 48 Gateway &gt; Configure &gt; Interfaces addressing: Local LAN (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 6.3.1.2 on page 134</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.

### 6.3.1.2 DHCP Option

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

Figure 65 Gateway &gt; Configure &gt; Interfaces addressing: Local LAN: DHCP Option

The screenshot shows a 'DHCP Option' configuration window. It includes a title bar with a close button. The main area contains the following fields and controls:

- Option:** A dropdown menu currently showing 'User Defined'.
- Name:** A text input field containing 'User\_Defined'.
- Code:** An empty text input field.
- Type:** A dropdown menu currently showing 'IP'.
- First IP address:** An empty text input field.
- Second IP address:** An empty text input field.
- Third IP address:** An empty text input field.

At the bottom right of the window, there are two buttons: 'Close' and 'OK'.

The following table describes the labels in this screen.

Table 49 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.
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.

### 6.3.1.3 Static Route

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

Figure 66 Gateway > Configure > Interfaces addressing: Static Route

The screenshot shows a dialog box titled "Static Route" with a close button (X) in the top right corner. The dialog contains four input fields: "Name", "Destination", "Subnet mask", and "Next hop IP address". At the bottom right of the dialog, there are two buttons: "Close" and "OK".

The following table describes the labels in this screen.

Table 50 Gateway > Configure > 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.

### 6.3.2 Firewall

By default, a LAN user can initiate a session from within the LAN zone and the security gateway allows the response. However, the security gateway blocks incoming traffic initiated from the WAN zone and destined for the LAN zone. Use this screen to configure firewall rules for outbound traffic, application patrol, schedule profiles and port forwarding rules for inbound traffic.

Click **Gateway > Configure > Firewall** to access this screen.



Figure 67 Gateway > Configure > Firewall

SITE-WIDE
AP
SWITCH
GATEWAY
ORGANIZATION
HELP

### Firewall

#### Security Policy

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

Outbound rules

	Source	Destination	Dst port	Schedule	Description
▼	e.g.: 192.168.1.1	e.g.: 192.168.1.1	e.g.: 80	Always ▼	
	Any	Any	Any	Any	Default rule

[+ Add](#)

Security gateway services

Service	Allowed remote IPs
Ping	any
Web (local status & configuration)	61.222.86.79

#### Application Patrol

Application monitor  ON

Enable this option to allow traffic analysis with application patrol.

Application profiles

	Name	Description
1	Profile 1	Block YouTube

[+ Add](#)

#### Schedule profiles

NewSchedule used by outbound rules	✎ 🗑
------------------------------------	-----

[+ Add](#)

#### NAT

1:1 NAT

	Uplink	Public IP	LAN IP	Allowed remote IP	Description
+ 1	WAN 1 ▼			any	

[+ Add](#)

Virtual server

	Uplink	Public IP	Public port	LAN IP	Local port	Allowed remote IP
+ 1	WAN 1 ▼	any				any

[+ Add](#)

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

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

The following table describes the labels in this screen.

Table 51 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.
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 signature(s). See <a href="#">Section 6.3.2.1 on page 139</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 address(es) 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 address(es) 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 port(s) 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> means any IP address.
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 6.3.2.1 on page 139</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.
	Click this icon to change the profile settings.

Table 51 Gateway &gt; Configure &gt; Firewall (continued)

LABEL	DESCRIPTION
	Click this icon to remove the profile.
Add	Click this button to create a new schedule profile. See <a href="#">Section 6.3.2.2 on page 141</a> for more information.
NAT	
1:1 NAT	
	Click the icon of a rule and drag the rule up or down to change the order.
Uplink	Select the interface of the security gateway on which packets for the NAT rule must be received.
Public IP	Specify to which translated destination IP address this NAT rule forwards packets.
LAN IP	Specify the destination IP address of the packets received by this NAT rule's specified interface.
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> means any IP address.
Description	Enter a description for the rule.
	Click this icon to remove the rule.
Add	Click this button to create a new 1:1 NAT mapping rule.
Virtual server	
	Click the icon of a rule and drag the rule up or down to change the order.
Uplink	Select the interface of the security gateway on which packets for the NAT rule must be received.
Public IP	Specify to which translated destination IP address this NAT rule forwards packets.
Public port	Enter the translated destination port or range of translated destination ports if this NAT rule forwards the packet.
LAN IP	Specify the destination IP address of the packets received by this NAT rule's specified interface.
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> means any IP address.
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.

### 6.3.2.1 Add application patrol profile

Click the **Add** button in the **Application Patrol** section of the **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 68** Gateway > Configure > Firewall: Add an application profile

The following table describes the labels in this screen.

**Table 52** Gateway > Configure > Firewall: Add an application profile

LABEL	DESCRIPTION
General settings	
Name	Enter a name for this profile for identifying 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.

### 6.3.2.2 Create new schedule

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

**Figure 69** Gateway > Configure > Firewall: Add a schedule profile

The following table describes the labels in this screen.

**Table 53** Gateway > Configure > Firewall: Add a schedule profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identifying 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 on this day. Otherwise, select <b>Off</b> to turn the associated rule off.
From - To	Specify the hour and minute when the schedule begins and ends each day
Time display	Select the time format in which the time is displayed.
Close	Click this button to exit this screen without saving.
Add	Click this button to save your changes and close the screen.

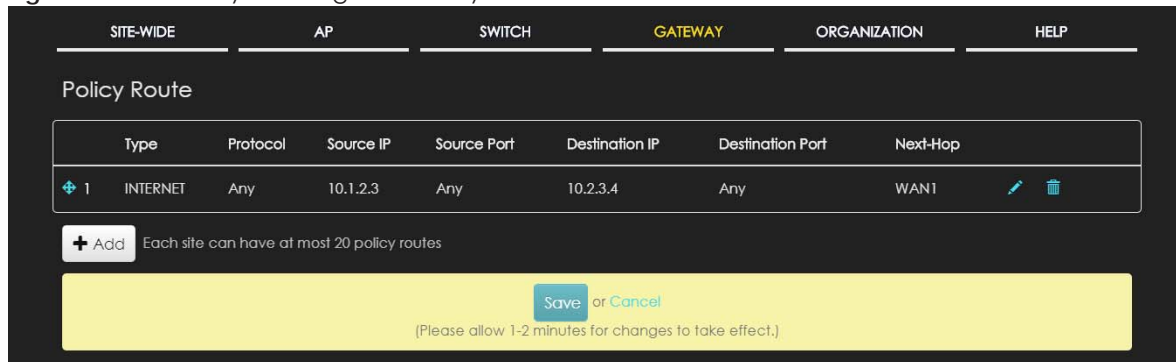
### 6.3.3 Policy Route

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 **Gateway > Configure > Policy Route** to access this screen.

**Figure 70** Gateway > Configure > Policy Route



The following table describes the labels in this screen.

**Table 54** Gateway > Configure > Policy Route

LABEL	DESCRIPTION
	Click the icon of a rule and drag the rule up or down to change the order.
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 address(es) from which the packets are sent.
Source Port	This displays the port the source IP address(es) 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 address(es) to which the packets are transmitted.
Destination Port	This displays the port the destination IP address(es) are using in this policy route rule. <b>Any</b> means all services.
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 6.3.2.1 on page 139</a> for more information.

#### 6.3.3.1 Add/Edit policy route

Click the **Add** button or an edit icon in the **Gateway > Configure > Policy Route** screen to access this screen.

**Figure 71** Gateway > Configure > Policy Route: Add/Edit

The following table describes the labels in this screen.

**Table 55** 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 via 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 (which is 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.

### 6.3.4 Content Filtering

Content filtering allows you to block access to specific web sites. It can also block access to specific categories of web site content.

Click **Gateway > Configure > Content Filtering** to access this screen.

Figure 72 Gateway > Configure > Content Filtering

SITE-WIDE
AP
SWITCH
GATEWAY
ORGANIZATION
HELP

### Content filtering

**General setting**

Enabled

Denied access message

Redirect URL

**Block/White list**

List	FQDN(support wildcard)
Black	<input type="text"/>
White	<input type="text"/>

**Category**

Action Block

Test URL 

Test

Templates Security

<input checked="" type="checkbox"/> Anonymizers	<input checked="" type="checkbox"/> Botnets	<input checked="" type="checkbox"/> Compromised
<input checked="" type="checkbox"/> Malware	<input checked="" type="checkbox"/> Network Errors	<input checked="" type="checkbox"/> Parked Domains
<input checked="" type="checkbox"/> Phishing & Fraud	<input checked="" type="checkbox"/> Spam Sites	<input type="checkbox"/> Advertisements & Pop-Ups
<input type="checkbox"/> Alcohol & Tobacco	<input type="checkbox"/> Arts	<input type="checkbox"/> Business
<input type="checkbox"/> Chat	<input type="checkbox"/> Child Abuse Images	<input type="checkbox"/> Computers & Technology
<input type="checkbox"/> Criminal Activity	<input type="checkbox"/> Cults	<input type="checkbox"/> Dating & Personals
<input type="checkbox"/> Download Sites	<input type="checkbox"/> Education	<input type="checkbox"/> Entertainment
<input type="checkbox"/> Fashion & Beauty	<input type="checkbox"/> Finance	<input type="checkbox"/> Forums & Newsgroups
<input type="checkbox"/> Gambling	<input type="checkbox"/> Games	<input type="checkbox"/> General
<input type="checkbox"/> Government	<input type="checkbox"/> Greeting Cards	<input type="checkbox"/> Hacking
<input type="checkbox"/> Hate & Intolerance	<input type="checkbox"/> Health & Medicine	<input type="checkbox"/> Illegal Drugs
<input type="checkbox"/> Illegal Software	<input type="checkbox"/> Image Sharing	<input type="checkbox"/> Information Security
<input type="checkbox"/> Instant Messaging	<input type="checkbox"/> Job Search	<input type="checkbox"/> Leisure & Recreation
<input type="checkbox"/> News	<input type="checkbox"/> Non-profits & NGOs	<input type="checkbox"/> Nudity
<input type="checkbox"/> Peer-To-Peer	<input type="checkbox"/> Personal Sites	<input type="checkbox"/> Politics
<input type="checkbox"/> Pornography/Sexually Explicit	<input type="checkbox"/> Private Ip Addresses	<input type="checkbox"/> Real Estate
<input type="checkbox"/> Religion	<input type="checkbox"/> Restaurants, Food & Dining	<input type="checkbox"/> School Cheating
<input type="checkbox"/> Search Engines & Portals	<input type="checkbox"/> SexEducation	<input type="checkbox"/> Shopping
<input type="checkbox"/> Social Networking	<input type="checkbox"/> Sports	<input type="checkbox"/> Streaming Media & Downloads
<input type="checkbox"/> Tasteless	<input type="checkbox"/> Translators	<input type="checkbox"/> Transportation
<input type="checkbox"/> Travel	<input type="checkbox"/> Violence	<input type="checkbox"/> Weapons
<input type="checkbox"/> Web-based Email		

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



The following table describes the labels in this screen.

Table 56 Gateway > Configure > Content Filtering

LABEL	DESCRIPTION
General setting	
Enabled	Click <b>ON</b> to enable the content filtering feature on the security gateway. Otherwise, click <b>OFF</b> to disable it.
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/White list	
Black	<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 subdomains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains.</p> <p>Use up to 127 characters (0-9a-z). The casing does not matter.</p>
White	<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 subdomains 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>
Category	
Action	<p>Select <b>Pass</b> to allow users to access web pages that match the categories that you select below.</p> <p>Select <b>Block</b> to prevent 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>

Table 56 Gateway &gt; Configure &gt; Content Filtering (continued)

LABEL	DESCRIPTION
Test URL	<p>You can check which category a web page belongs to. Enter a web site URL in the text box.</p> <p>When the content filter is active, you should see the web page's category. The query fails if the content filter is not active.</p> <p>Content Filtering can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. <b>Test URL</b> displays both results in the test.</p>
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>

### 6.3.5 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 **Gateway > Configure > Site-to-Site VPN** to access this screen.

Figure 73 Gateway &gt; Configure &gt; Site-to-Site VPN

The screenshot shows the 'Site-to-Site VPN' configuration page. At the top, there are navigation tabs: SITE-WIDE, AP, SWITCH, GATEWAY (highlighted), ORGANIZATION, and HELP. The main content area is titled 'Site-to-Site VPN' and contains several sections:

- Outgoing Interface:** A dropdown menu set to 'AUTO'.
- Prefer uplink:** A dropdown menu set to 'WAN1'.
- Local networks:** A table with columns 'Name', 'Subnet', and 'Use VPN'.
 

Name	Subnet	Use VPN
LAN1	192.168.1.0/24	<input type="checkbox"/> OFF
LAN2	192.168.2.0/24	<input type="checkbox"/> OFF
- Nebula VPN Topology:** A dropdown menu set to 'Server-and-Client'. Below it, a note says 'Split tunnel (send only site-to-site traffic over the VPN)'. Below that, another dropdown menu is set to 'Testing site'.
- Client-to-Client communication:** A toggle switch set to 'OFF'.
- Remote VPN participants:** A table with columns 'Network' and 'Subnet(s)'. The 'Network' column is currently empty.
- Site-wide settings:** A section with the text 'Options in this section apply to this Nebula gateway only.' Below it, a section titled 'Non-Nebula VPN peers' contains a table with columns: Name, Public IP, Private subnet, IPsec policy, Preshared secret, Availability, and Action. There is a '+ Add' button below this table.

At the bottom of the page, there are 'Save' and 'Cancel' buttons, and a note: '(Please allow 1-2 minutes for changes to take effect.)'

The following table describes the labels in this screen.

Table 57 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.
Use VPN	Select <b>ON</b> to allow the computers on the network to use the VPN tunnel. Otherwise, select <b>OFF</b> .
Nebula VPN Topology	This shows the VPN mode supported by the security gateway.  Select a VPN topology.  Select <b>Disable</b> to not set a VPN connection.  In the <b>Site-to-Site</b> VPN topology, the remote IPSec device has a static IP address or a domain name. This security gateway can initiate the VPN tunnel.  In the <b>Hub-and-Spoke</b> VPN topology, there is a VPN connection between each spoke router and the hub router, which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself.  In the <b>Server-and-Client</b> VPN topology, incoming connections from IPSec VPN clients are allowed. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
Hubs (peers to connect to)	This field is available when you set <b>Topology</b> to <b>Hub-and-Spoke</b> . The field is configurable only when the security gateway of the selected site is the hub router.  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.
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.
Server (client to connect to)	This field is available when you set <b>Topology</b> to <b>Server-and-Client</b> . The field is configurable only when the security gateway of the selected site is the VPN server.  You can select another site's name to have the gateway of that site act as the VPN server.
Client-to-Client communication	Select <b>On</b> to allow VPN traffic to transmit between VPN clients by going through the server. The field is configurable only when the security gateway of the selected site is the VPN server.
Remote VPN participants	This shows the remote (peer) Nebula gateway's network name and address.
Non-Nebula VPN peers	If the remote VPN gateway is not a Nebula device, use this section to set up a VPN connection between it and the Nebula security gateway.
Name	Enter the name of the peer gateway.
Public IP	Enter the public IP address of the peer gateway.
Private Subnet	Enter the local network address or subnet behind the peer gateway.
IPSec policy	Click to select a pre-defined policy or have a custom one. See <a href="#">Section 6.3.5.1 on page 148</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 57 Gateway &gt; Configure &gt; Site-to-Site VPN (continued)

LABEL	DESCRIPTION
Availability	Select <b>All Network</b> to allow the peer gateway to connect to any Nebula security gateway in the organization via a VPN tunnel.  Select <b>This site</b> and the peer gateway can only connect to the Nebula security gateway in this site via a VPN tunnel.  You can also configure any specific sites in the organization,
Action	Click the remove icon to delete the entry.
Add	Click this button to add a peer VPN gateway to the list.

### 6.3.5.1 Custom IPsec Policy

Click the **IPsec Policy** column in the **Non-Nebula VPN peers** section of the **Gateway > Configure > Site-to-Site VPN** screen to access this screen.

Figure 74 Gateway &gt; Configure &gt; Site-to-Site VPN: Custom IPsec Policy

Custom

Preset: Default

**Phase 1**

Encryption: 3DES

Authentication: SHA128

Diffie-Hellman group: 2

Lifetime (seconds): 86400

**Advanced**

Mode: Main

Local ID: Any

Peer ID: Any

**Phase 2**

	Encryption	Authentication
Set 1	3DES	SHA128
Set 2	(none)	(none)
Set 3	(none)	(none)

PFS group: Off

Lifetime (seconds): 86400

Close OK

The following table describes the labels in this screen.

Table 58 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).
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: <b>DES</b> - a 56-bit key with the DES encryption algorithm <b>3DES</b> - a 168-bit key with the DES encryption algorithm <b>AES128</b> - a 128-bit key with the AES encryption algorithm <b>AES192</b> - a 192-bit key with the AES encryption algorithm <b>AES256</b> - a 256-bit key with the AES encryption algorithm  The 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.
Authentication	Select which hash algorithm to use to authenticate packet data in the IKE SA.  Choices are <b>SHA128</b> , <b>SHA256</b> , <b>SHA512</b> and <b>MD5</b> . SHA is generally considered stronger than MD5, but it is also slower.  The remote IPsec router must use the same authentication algorithm.
Diffie-Hellman group	Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are:  <b>1</b> - use a 768-bit random number <b>2</b> - use a 1024-bit random number <b>5</b> - use a 1536-bit random number <b>14</b> - use a 2048-bit random number  The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Lifetime (seconds)	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.
Advanced	Click this to display a greater or lesser number of configuration fields.
Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are:  <b>Main</b> - this encrypts the security gateway's and remote IPsec router's identities but takes more time to establish the IKE SA  <b>Aggressive</b> - this is faster but does not encrypt the identities  The security gateway and the remote IPsec router must use the same negotiation mode.
Local ID	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.
Peer ID	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.
Phase 2	Phase 2 uses the SA that was established in phase 1 to negotiate SAs for IPsec.

Table 58 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>Off</b> - disable PFS</p> <p><b>1</b> - enable PFS and use a 768-bit random number</p> <p><b>2</b> - enable PFS and use a 1024-bit random number</p> <p><b>5</b> - enable PFS and use a 1536-bit random number</p> <p><b>14</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 reauthenticating.</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>

### 6.3.6 L2TP over IPSec Client

Use this screen to configure the L2TP VPN settings.

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 **Gateway > Configure > L2TP over IPSec client** to access this screen.

Figure 75 Gateway &gt; Configure &gt; L2TP over IPsec client

The following table describes the labels in this screen.

Table 59 Gateway &gt; Configure &gt; L2TP over IPsec client

LABEL	DESCRIPTION
Client VPN server	Click <b>ON</b> to enable the L2TP/IPsec VPN server feature on the security gateway. Otherwise, click <b>OFF</b> to disable it.
Client VPN subnet	Specify the IP addresses that the security gateway uses to assign to the L2TP 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 address(es).
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 address(es).
Secret	Enter the pre-shared key (password) which is used to set up the IPsec VPN tunnel.
Authentication	Select how the security gateway authenticates a remote user before allowing access to the L2TP VPN tunnel.

### 6.3.7 Network Access Method

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

Click **Gateway > Configure > Network access method** to access this screen.

Figure 76 Gateway &gt; Configure &gt; Network access method

The following table describes the labels in this screen.

Table 60 Gateway &gt; Configure &gt; Network access method

LABEL	DESCRIPTION
Interfaces	Select the gateway's interface (network) to which the settings you configure here is applied.
Network Access	<p>Select <b>Direct access</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 an authentication server that you have configured in the <b>Gateway &gt; Configure &gt; Network Servers</b> screen (see <a href="#">Section 6.3.12 on page 162</a>).</p>



Table 60 Gateway &gt; Configure &gt; Network access method (continued)

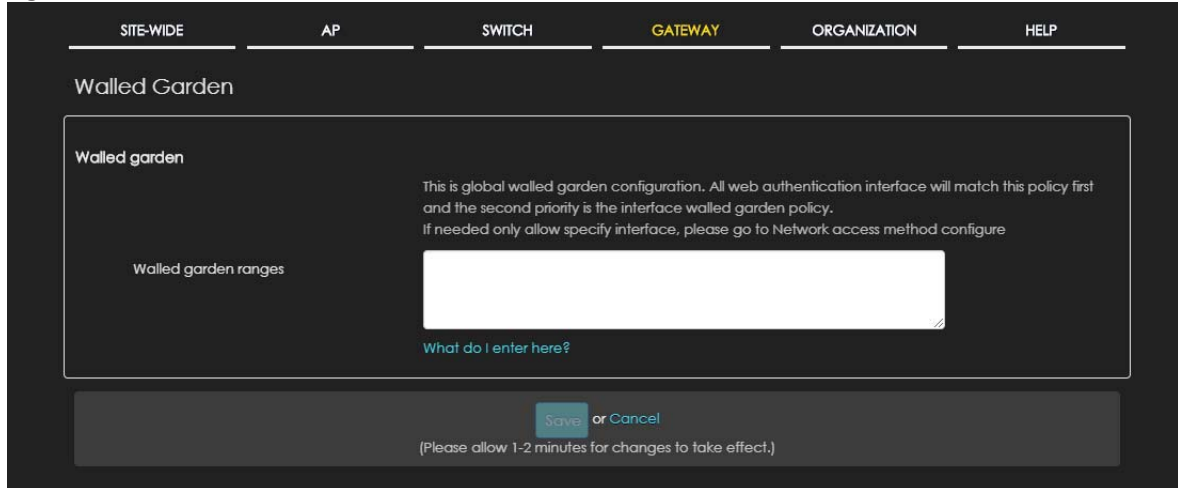
LABEL	DESCRIPTION
Walled garden	<p>Select to turn on or off the walled garden feature. This field is not configurable if you set <b>Network Access</b> to <b>Direct access</b>.</p> <p>With a walled garden, you can define one or more web site addresses that all users can access without logging in. These 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 don't 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>

### 6.3.8 Walled Garden

Use this screen to 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 **Gateway > Configure > Walled Garden** to access this screen.

Figure 77 Gateway &gt; Configure &gt; Walled Garden



The following table describes the labels in this screen.

Table 61 Gateway &gt; Configure &gt; Walled Garden

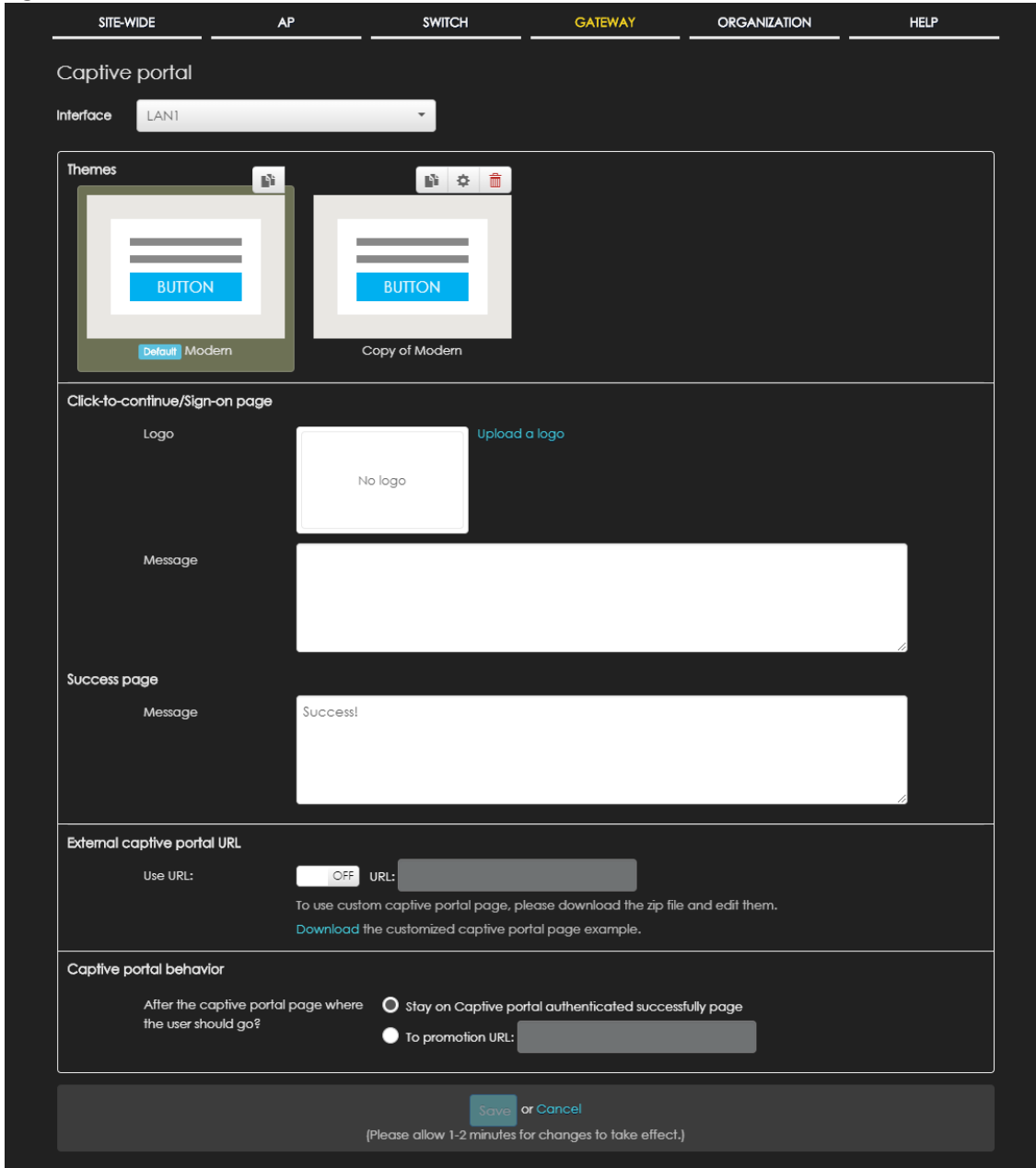
LABEL	DESCRIPTION
Walled garden	With a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example.
Walled garden ranges	Specify walled garden web site links, which use a domain name or an IP address for web sites that all users are allowed to access without logging in.

### 6.3.9 Captive Portal

Use this screen to configure captive portal settings for each interface. A captive portal can intercepts network traffic until the user authenticates his or her connection, usually through a specifically designated login web page.

Click **Gateway > Configure > Captive portal** to access this screen.

Figure 78 Gateway > Configure > Captive portal



The following table describes the labels in this screen.

Table 62 Gateway > Configure > Captive portal

LABEL	DESCRIPTION
Interface	Select the gateway's interface (network) to which the settings you configure here is applied.
Themes	Click the <b>Copy</b> icon at the upper right corner of the default theme image to create a new custom theme (portal page).  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 page(s). See <a href="#">Section 6.3.9.1 on page 156</a> .  Click the <b>Remove</b> icon to delete a custom theme.

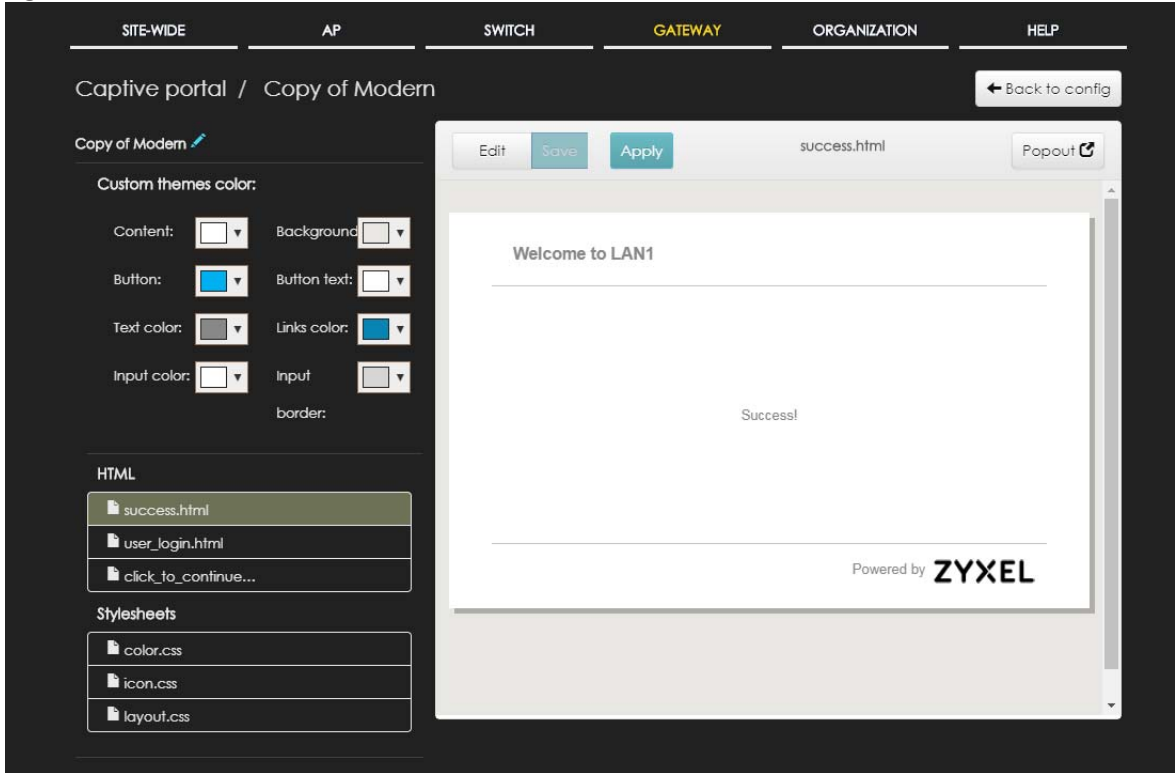
Table 62 Gateway &gt; Configure &gt; Captive portal (continued)

LABEL	DESCRIPTION
Click-to-continue/Sign-on page	
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> .

### 6.3.9.1 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 **Gateway > Configure > Captive portal** screen to access this screen.

Figure 79 Gateway > Configure > Captive portal: Edit



The following table describes the labels in this screen.

Table 63 Gateway > Configure > Captive portal: Edit

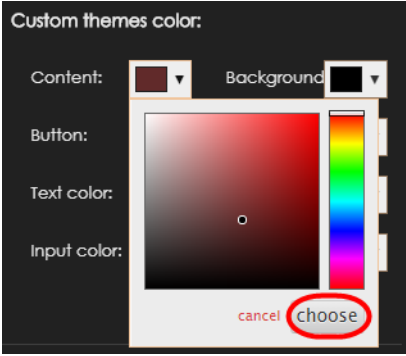
LABEL	DESCRIPTION
Back to config	Click this button to return to the <b>Captive portal</b> screen.
Copy of Modern	This shows the name of the theme. Click the edit icon the change it.
Custom themes color	<p>Customize the colors on the selected custom portal page (HTML file), such as the color of the button, text, window's background, links, borders, and etc.</p> <p>Select a color that you want to use and click the <b>Choose</b> button.</p> 
HTML	<p>This shows the HTML file name of the portal page created for the selected custom theme.</p> <p>Click a HTML file to display the portal page on the right side of the screen. You can also change colors and modify the CSS values of the selected HTML file.</p>
Stylesheets	This shows the name of the main CSS file created for the selected custom theme.

Table 63 Gateway &gt; Configure &gt; Captive portal: Edit (continued)

LABEL	DESCRIPTION
Edit/Preview	Click <b>Edit</b> 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 <b>Preview</b> to display the corresponding portal page.
Save	Click this button to save your color settings for the selected HTML file.
Apply	Click this button to apply your color settings to the selected HTML file.
Popout	Click this button to display the corresponding portal page in a popup window.

### 6.3.10 Traffic Shaping

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

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

Figure 80 Gateway > Configure > Traffic shaping



The following table describes the labels in this screen.

Table 64 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.

Table 64 Gateway &gt; Configure &gt; Traffic shaping (continued)

LABEL	DESCRIPTION
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>Weighted 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 can not 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 address(es) 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 number(s) (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 all services.</p>
Down/Up	<p>Set the maximum upstream/downstream bandwidth for traffic from an individual source IP address.</p> <p>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.</p>
Priority	<p>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.</p> <p>Traffic with a higher priority is given bandwidth before traffic with a lower priority.</p>



Table 64 Gateway &gt; Configure &gt; Traffic shaping (continued)

LABEL	DESCRIPTION
	Click this icon to remove the rule.
Add	Click this button to create a new rule.

### 6.3.11 Security Filtering

Use this screen to enable or disable Intrusion Detection and Prevention (IDP) and/or anti-virus on the security gateway. 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 **Gateway > Configure > Security Filtering** 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 81 Gateway &gt; Configure &gt; Security Filtering

The following table describes the labels in this screen.

Table 65 Gateway &gt; Configure &gt; Security Filtering

LABEL	DESCRIPTION
Intrusion Detection / Prevention	
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.
Anti-Virus	

Table 65 Gateway &gt; Configure &gt; Security Filtering (continued)

LABEL	DESCRIPTION
Enable	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 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>

### 6.3.12 Network Servers

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.

Click **Gateway > Configure > Network Servers** to access this screen.

Figure 82 Gateway &gt; Configure &gt; Network Servers

The screenshot shows the 'Network Servers' configuration page. At the top, there are navigation tabs: SITE-WIDE, AP, SWITCH, GATEWAY (highlighted), ORGANIZATION, and HELP. Below the tabs, the page title is 'Network Servers'. The main content area is divided into four sections:

- DNS**: Contains an 'Address Record' section with two input fields for 'FQDN' and 'IP Address', and a trash icon. Below it is a '+ Add' button.
- Domain Zone Forwarder**: Contains a table with columns 'Domain Zone', 'IP Address', and 'Interface'. The 'Interface' field has a dropdown menu showing 'LAN1' and a trash icon. Below it is a '+ Add' button.
- Authentication Server**: Contains a 'My AD Server' section with a table with columns: Name, Server address, Backup server address, Port, AD domain, Domain admin, Password, and Advanced. The 'Port' field has the value '389'. Below it is a '+ Add' button.
- My RADIUS Server**: Contains a table with columns: Name, Server address, Backup server address, Port, Secret, and Advanced. The 'Port' field has the value '1812'. Below it is a '+ Add' button.

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

The following table describes the labels in this screen.

Table 66 Gateway &gt; Configure &gt; Network Servers





LABEL	DESCRIPTION
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.

Table 66 Gateway &gt; Configure &gt; Network Servers (continued)

LABEL	DESCRIPTION
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.  Enter * if all domain zones are served by the specified DNS server(s).
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.
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 6.3.12.1 on page 165</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.
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 6.3.12.1 on page 165</a> .
	Click this icon to remove the server.
Add	Click this button to create a new server.

### 6.3.12.1 Advanced Settings

Click the **Advanced** column in the **Gateway > Configure > Network Servers** screen to access this screen.

**Figure 83** Gateway > Configure > Network Servers: Advanced

The following table describes the labels in this screen.

**Table 67** Gateway > Configure > Network Servers: 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 server(s) or the AD or server(s) 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).
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

# CHAPTER 7

# Organization

## 7.1 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.

## 7.2 Monitor

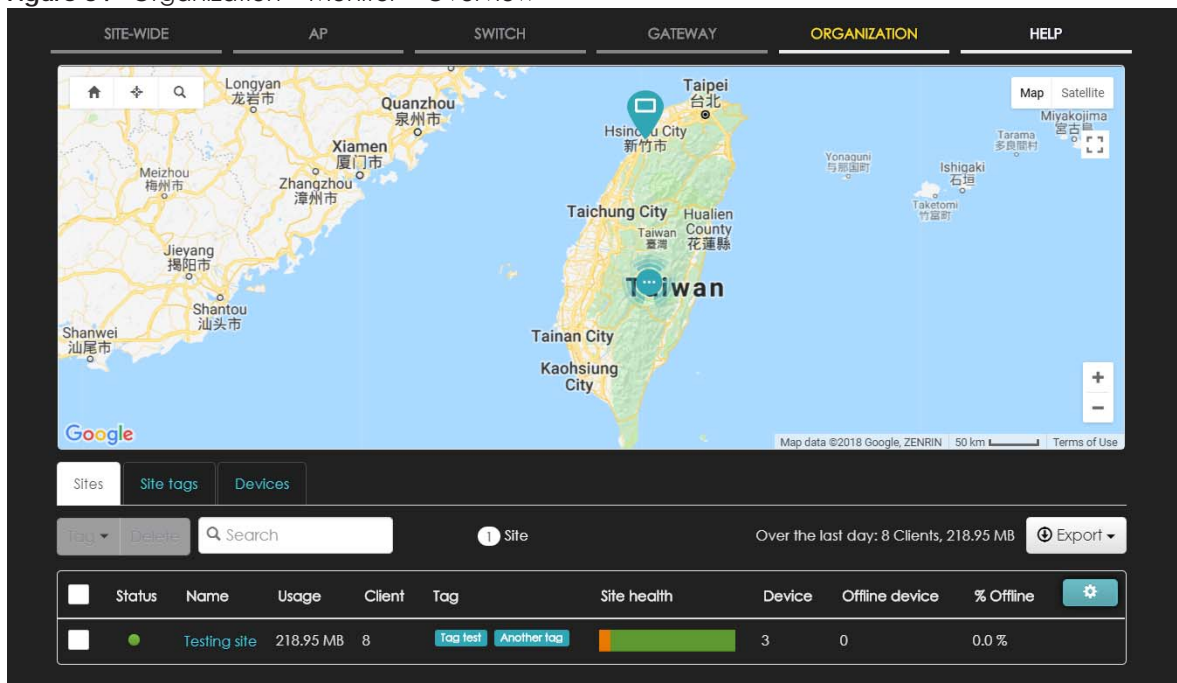
Use the Monitor menus to check the site and device information and change logs for the selected organization.

### 7.2.1 Organization Overview

This menu shows you the site locations on the Google map and the summary of sites, site tags and connected devices for the selected organization.

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

Figure 84 Organization > Monitor > Overview



### 7.2.1.1 Sites

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

**Figure 85** Organization > Monitor > Overview: Sites



The following table describes the labels in this screen.

**Table 68** Organization > Monitor > Overview: Sites

LABEL	DESCRIPTION
Tag	Select one or multiple sites and click this button to create a new tag for the site(s) or delete an existing tag.
Delete	Select the site(s) 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 whether the site is online (green), has generated alerts (amber), goes off-line during the past day (red) or has been off-line for at least one week (gray).
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 associated with 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>
Device	This shows the total number of Nebula devices deployed in the site.
Offline device	This shows the number of off-line Nebula devices deployed in the site.
% 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.

### 7.2.1.2 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 86 Organization &gt; Monitor &gt; Overview: Site tags

Status	Tag	Site	Offline device	Client	Usage	Device	Offline site	% Offline
●	test	1	0	7	3.41 GB	2	0	0.0 %
●	more	1	0	7	3.41 GB	2	0	0.0 %

The following table describes the labels in this screen.

Table 69 Organization &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 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 tag list as a CSV or XML file to your computer.
Status	This shows whether the device is online (green), has generated alerts (amber), or goes off-line during the past day (red) or has been off-line for at least one week (gray).
Tag	This shows the tag created and added to the site.
Site	This shows the name of the site to which the tag is added.
Offline device	This shows the number of off-line Nebula devices deployed in the site.
Client	This shows the number of clients associated with the site.
Usage	This shows the amount of data consumed by the site.
Device	This shows the total number of Nebula devices deployed in the site.
Offline site	This shows the number of off-line sites to which the tag is added.
% Offline	This shows what percentage of the sites are currently off-line.
	Click this icon to display a greater or lesser number of configuration fields.

### 7.2.1.3 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 87 Organization &gt; Monitor &gt; Overview: Devices

Status	Model	Name	Site	MAC address	Tag	Client	Usage
●	NAP102	Testing site	Testing site	58:8B:F3:91:4B:75	1	1	68.60 MB
●	NSG50	Testing site	Testing site	B8:EC:A3:28:60:38	3	3	0 bytes
●	NSW200-28P	Testing site	Testing site	B8:EC:A3:0F:DB:34	7	7	150.35 MB



The following table describes the labels in this screen.

Table 70 Organization > 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 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 device list as a CSV or XML file to your computer.
Status	This shows whether the device is online (green), has generated alerts (amber), or goes off-line during the past day (red) or has been off-line for at least one week (gray).
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.
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.

## 7.2.2 Change Log

Use this screen to view the logged messages for changes in the specified organization. Click **Organization > 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 88 Organization &gt; Monitor &gt; Change log

The following table describes the labels in this screen.

Table 71 Organization &gt; Monitor &gt; Change log

LABEL	DESCRIPTION
Keyword	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 to display only the log messages generated within a certain period of time (before the specified date/time).
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 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 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.

## 7.3 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.

### 7.3.1 Create Site

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

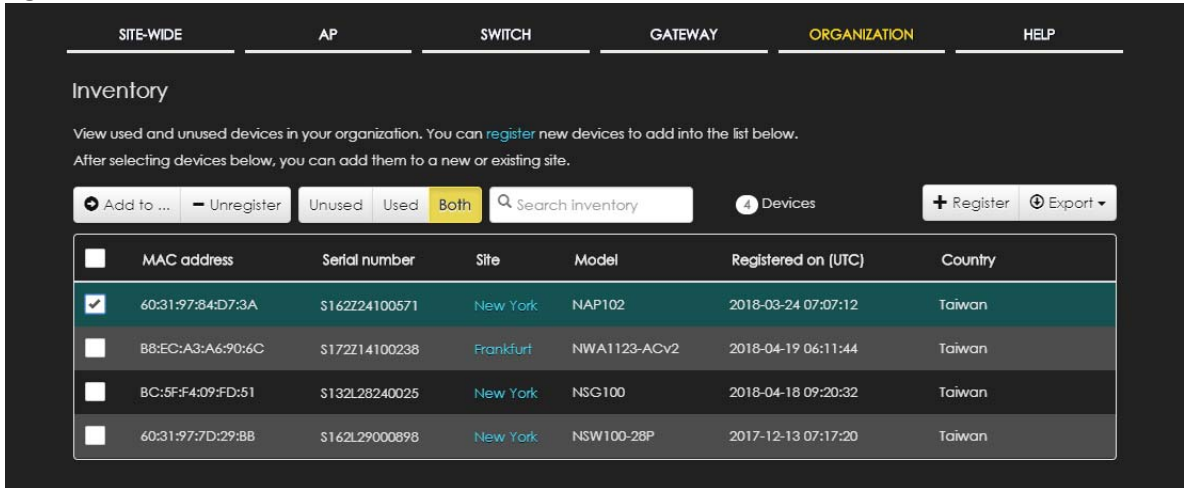
- 1 Enter a descriptive name for the site.
- 2 If you already have one or more than one sites in the organization and you want to copy the site settings of an existing one, select the **Clone from** checkbox and then the site name.
- 3 Choose the time zone of the site's location.
- 4 Enter the name of the registered device that is to be added to this site. If there is no registered Nebula devices in the organization, you can click **register** to claim one.
- 5 Click **Create site** to add the new site to your organization.

**Figure 89** Organization > Configure > Create Site

### 7.3.2 Inventory

Use this screen to view and manage the Nebula devices you registered for the selected organization. Click **Organization > Configure > Inventory** to access this screen.

Figure 90 Organization > Configure > Inventory



The following table describes the labels in this screen.

Table 72 Organization > Configure > Inventory

LABEL	DESCRIPTION								
Add to ...	Click this button to assign the selected device(s) to an existing site.								
Unregister	Click this button to remove the selected device(s) from the organization.								
Unused	Click this button to show the Nebula device(s) which is not assigned to a site yet.								
Used	Click this button to show the Nebula device(s) which has been assigned to a site.								
Both	Click this button to show all Nebula devices which are registered for the organization.								
Search	Enter a key word as the filter criteria to filter the list of connected devices.								
Devices	This shows the number of the devices in the list.								
Register	<p>Click this button to pop up a window where you can register a device by entering its MAC address and serial number even before the device is connected to a site.</p> <p>You can click <b>template</b> in the pop-up window to download the template (an example Excel file), add devices information in the Excel file, and then click <b>import</b> to register multiple devices quickly by importing the Excel file.</p> <div data-bbox="495 1297 1291 1801" style="border: 1px solid black; padding: 5px;"> <p>Register by MAC address and serial number <span style="float: right;">×</span></p> <p>Enter one or more MAC address and serial number. Or you can download the <a href="#">template</a> here and <b>import</b> multiple records for faster registration.</p> <p><a href="#">Where can I find these numbers?</a> <a href="#">What do I enter here?</a></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">MAC address</th> <th style="width: 30%;">Serial Number</th> <th style="width: 20%;">Model</th> <th style="width: 20%;">License</th> </tr> </thead> <tbody> <tr> <td><input style="width: 90%;" type="text"/></td> <td><input style="width: 90%;" type="text"/></td> <td></td> <td style="text-align: right;"></td> </tr> </tbody> </table> <p><span style="border: 1px solid gray; padding: 2px 5px;">+ Register another device</span></p> <p style="color: red; font-size: small;">Registered device will be added to Organization Creator account in myZyxel.com.</p> <p><input type="checkbox"/> Acknowledge</p> <p style="text-align: right;"><span style="border: 1px solid gray; padding: 2px 5px;">Close</span> <span style="border: 1px solid gray; padding: 2px 5px; background-color: #0070c0; color: white;">OK</span></p> </div>	MAC address	Serial Number	Model	License	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>		
MAC address	Serial Number	Model	License						
<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>								
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.								

Table 72 Organization &gt; Configure &gt; Inventory (continued)

LABEL	DESCRIPTION
Serial number	This shows the serial number 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	This shows the date and time that the device was registered at the NCC.
Country	This shows the country where the device is located.

### 7.3.3 License Management

Use this screen to view and manage the licenses for Nebula devices in the organization. Click **Organization > Configure > License management** to access this screen.

Note: Licenses for different Nebula devices in the same organization are re-calculated and set to expire on the same day.

The license credit (device points) varies depending on the type and number of Nebula devices you are managing and for how long you want to manage the devices using the NCC service.

#### Device and Organization

- When a Nebula device is registered and assigned to an organization at NCC for the first time, the organization can use the license credit that comes with the device, and the organization creator is the device owner at NCC.
- If a device is removed from an organization, you can only register it again for the original or other organizations that belong to the same organization creator. And the new organization cannot use the device's license credit.

Note: The account you use to create an organization is the administrator creator account that has full access to that organization. The organization creator account cannot be deleted by other organization administrators. See [Section 7.3.5 on page 178](#) for more information about administrator accounts.

#### Limited Lifetime License (LLL)

Zyxel offers a lifetime management license that will not expire for NCC services. The lifetime license is on a per organization basis. If you register a lifetime license key for your organization, each Nebula device in the organization must have a lifetime license. Make sure you have enough limited lifetime licenses for all Nebula devices in the organization. After upgrading to lifetime licenses, you cannot set the organization back to use non-lifetime licenses.

Note: The organization with lifetime licenses will not consume its non-lifetime license credit again even before the non-lifetime license expires.

Figure 91 Organization > Configure > License management

The screenshot shows the 'License management' page with tabs for SITE-WIDE, AP, SWITCH, GATEWAY, ORGANIZATION (selected), and HELP. It features two license summary cards, device lists, and a table of license keys.

**Nebula Control Center License Summary:**  
 NCC  
 Status: OK  
 Expiration date: 2019-02-23  
 Remaining: 170 days / 98 points

**Nebula Security Service License Summary:**  
 NSS-SP  
 Status: OK  
 Expiration date: 2019-08-29  
 Remaining: 357 days / 196 points

**Devices for NCC:**  
 NAP: 3  
 NSW: 2  
 NSG: 1  
 Nebula Points for 1 year of NCC service: 210

**Devices for NSS-SP:**  
 NSG100: 1 / 1  
 Nebula Security Points for 1 year of NSS-SP service: 200

**License Key Table:**

License key	Type	Service	Date (UTC)	Status	Action	Device	MAC address	Serial number
	Remove device	Empty	2018-09-03	ACTIVATED		NAP102	58:8b:F3:91:4B:33	S162Z03100019
	Remove device	Empty	2018-09-03	ACTIVATED		NAP102	60:31:97:F9:4E:2A	S162Z41100205
	Remove device	Empty	2018-08-28	ACTIVATED		NAP102	60:31:97:F9:4F:BF	S162Z41100340
	Add device	Empty	2018-08-28	ACTIVATED		NAP102	60:31:97:F9:4F:BF	S162Z41100340
	Remove device	Empty	2018-08-28	ACTIVATED		NAP102	60:31:97:F9:4F:BF	S162Z41100340
	Add device	Empty	2018-08-28	ACTIVATED		NAP102	60:31:97:F9:4F:BF	S162Z41100340
	Remove device	Empty	2018-08-28	ACTIVATED		NAP102	60:31:97:F9:4F:BF	S162Z41100340
	Add device	Empty	2018-08-28	ACTIVATED		NAP102	60:31:97:F9:4F:BF	S162Z41100340
	Remove device	Empty	2018-08-28	ACTIVATED		NAP102	60:31:97:F9:4F:BF	S162Z41100340
	Add device	Empty	2018-08-28	ACTIVATED		NAP102	60:31:97:F9:4F:BF	S162Z41100340

The following table describes the labels in this screen.

Table 73 Organization > Configure > License management

LABEL	DESCRIPTION
Nebula Control Center License / Nebula Security Service License	
Status	This shows whether the license is active.
Expiration date	This shows the date the license expires.
Remaining	This shows the number of days remaining before the license expires.

Table 73 Organization &gt; Configure &gt; License management (continued)

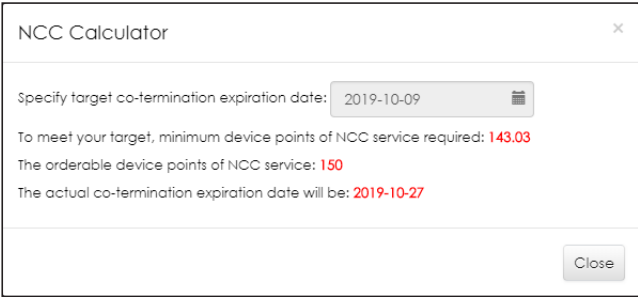
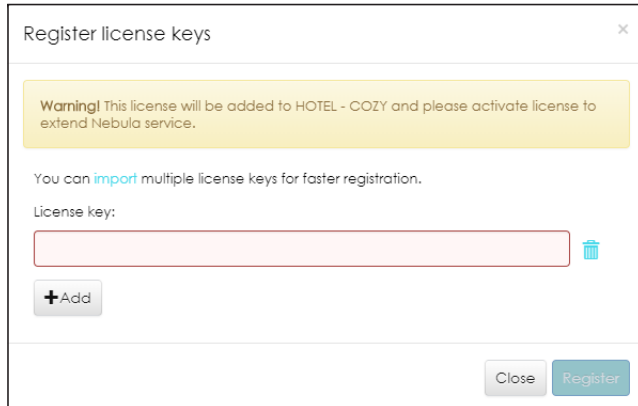
LABEL	DESCRIPTION
Calculator	<p>Click the button to open a screen where you can determine the additional license credit (device points) you should get to allow more time for the service.</p> <p>Select a date to which you want to extend the expiration date for the current license. You should purchase the device points in increments of 10. Therefore, the required minimum device points (based on the date you specified) might be different to the actual device points you can purchase. The screen also shows the actual date the license will expire after you get the device points.</p> 
Devices	This shows the model name and the number of Nebula devices that you can manage with the current license.
# SP / # Device	This shows how many security gateways have security services enabled and the total number of security gateways registered to the organization.
Nebula points for 1 year of NCC service	This shows the number of device points (license credit) you need to have one-year NCC service for the Nebula devices listed above in the <b>Devices</b> section.
Nebula Security Points for 1 year of NSS-SP service	This shows the number of device points (license credit) you need to have one-year NSS-SP service for the Nebula devices listed above in the <b>Devices</b> section.
Activated	Click this button to show the service that has been activated.
Registered	Click this button to show the service that has been registered.
Both	Click this button to show the service that has been registered and also activated
Register	<p>Click this button and enter your license key(s) to register a new service.</p> 
License Key	This shows the license key for the service.
Type	This shows how the service is registered.

Table 73 Organization &gt; Configure &gt; License management (continued)

LABEL	DESCRIPTION
Service	<p>This shows the type of the service.</p> <p>It shows <b>NCC-1Yr Bundle</b> if the Nebula managed device is offered one-year NCC service. The license will be automatically activated when the device is registered.</p> <p>It shows <b>Empty</b> if the device doesn't have any NCC service license.</p> <p>It shows <b>NCC Stay</b> or <b>NCC+NSS Stay</b> when the device is removed (unregistered) from the organization but the device's license credit is still valid and belongs to this organization. To transfer the license credit to another organization, please go to <b>Help &gt; Support request</b> to submit a ticket.</p> <p>It shows the number of <b>Nebula Points</b> or <b>Nebula Security Points</b> that have been transferred to another organization when the <b>Type</b> is <b>Transfer out</b>, or the number of points the organization received for free when the <b>Type</b> is <b>Promotion</b>.</p>
Activated at	This shows when the service is activated.
Status	This shows whether the service is registered (and activated).
Action	Click the <b>Activate</b> button to activate or extend the service with the license key. You can renew the license's expiration date.
Device	This shows the model name of the Nebula device which you can manage with the license.
MAC address	This shows the MAC address of the Nebula device which you can manage with the license.
Serial number	This shows the serial number of the Nebula device which you can manage with the license.

### 7.3.4 Organization Setting

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



Figure 92 Organization &gt; Configure &gt; Setting

The following table describes the labels in this screen.

Table 74 Organization &gt; Configure &gt; Setting

LABEL	DESCRIPTION
Name	Enter a descriptive name for the organization.
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 don't want the NCC to log out 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.
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.

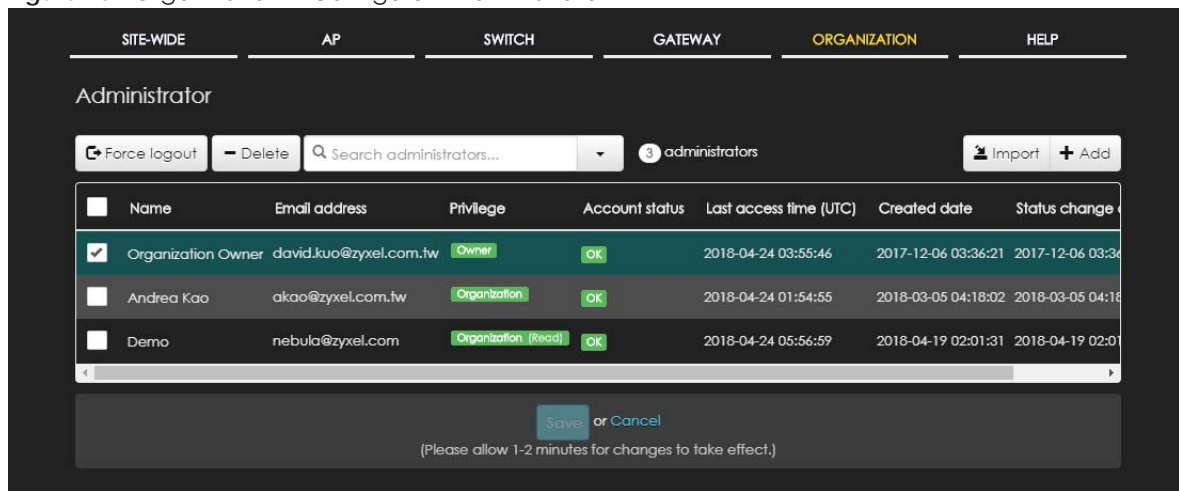
Table 74 Organization &gt; Configure &gt; Setting (continued)

LABEL	DESCRIPTION
Add certificate	Click this button to save a 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.
Add	Click this button to save your changes.
Cancel	Click this button to return the screen to its last-saved settings.
Delete this organization	Click the <b>Delete organization</b> button to remove the organization when it doesn't have any sites, devices or users.

### 7.3.5 Administrator

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

Figure 93 Organization &gt; Configure &gt; Administrator

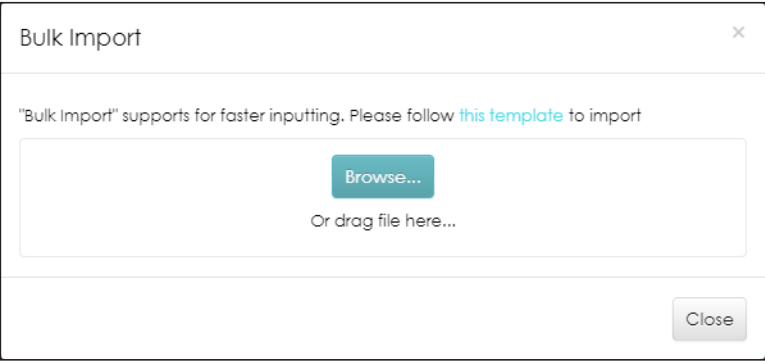


The following table describes the labels in this screen.

Table 75 Organization &gt; Configure &gt; Administrator

LABEL	DESCRIPTION
Force logout	Click this button to force the selected account(s) to log out of the NCC.
Delete	Click this button to remove the selected account(s).
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 75 Organization &gt; Configure &gt; Administrator (continued)

LABEL	DESCRIPTION
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> 
Add	Click this button to create a new administrator account. See <a href="#">Section 7.3.5.1 on page 179</a> .
Name	This shows the name of the administrator account.
Email address	This shows the email address of the administrator account.
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 the administrator account can register devices at a site.</p> <p><b>Owner</b> indicates the administrator account is the creator of the organization, who has full access to that organization and cannot be deleted by other administrators.</p>
Account status	This shows whether the administrator account has been validated ( <b>OK</b> ). It shows <b>Deactivate</b> if an administrator account has been created but can not 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.

### 7.3.5.1 Create/Update Administrator

In the **Organization > 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 94** Organization > Configure > Administrator: Create/Update administrator

The following table describes the labels in this screen.

**Table 76** Organization > 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 account you use to create an organization is the administrator 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.
Activated	Select <b>Yes</b> to enable the account or <b>No</b> to temporarily disable the account.
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 &gt; Monitor &gt; Overview: Sites</b> screen.

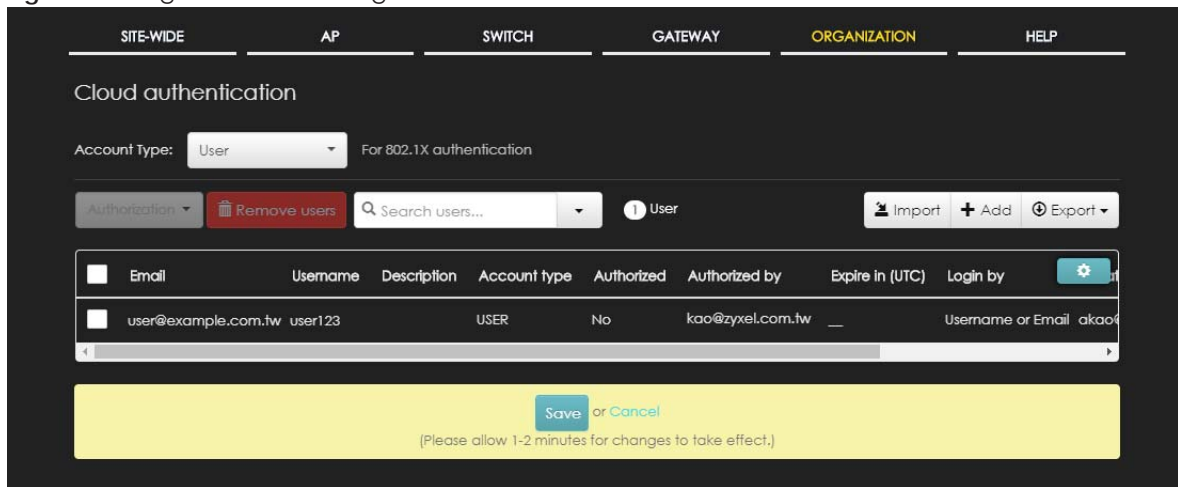
Table 76 Organization &gt; Configure &gt; Administrator: Create/Update administrator (continued)

LABEL	DESCRIPTION
Privilege	<p>This field is available only when you set the account's organization access to <b>Read-only</b> or <b>None</b>.</p> <p>Set the administrator account's access to the site.</p> <p>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).</p> <p>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 7.3.6 on page 181</a>).</p> <p><b>Installer</b> access allows an administrator to register devices at this site.</p>
Add	Click this button to create a new entry in order to configure the account's access to another site.
Close	Click this button to exit this screen without saving.
Create admin	Click this button to save your changes and close the screen.

### 7.3.6 Cloud Authentication

Use this screen to view and manage the user accounts which are authenticated using the NCC user database. Click **Organization > Configure > Cloud Authentication** to access this screen.

Figure 95 Organization &gt; Configure &gt; Cloud Authentication



The following table describes the labels in this screen.

Table 77 Organization > Configure > Cloud Authentication

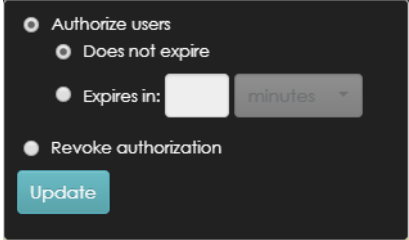
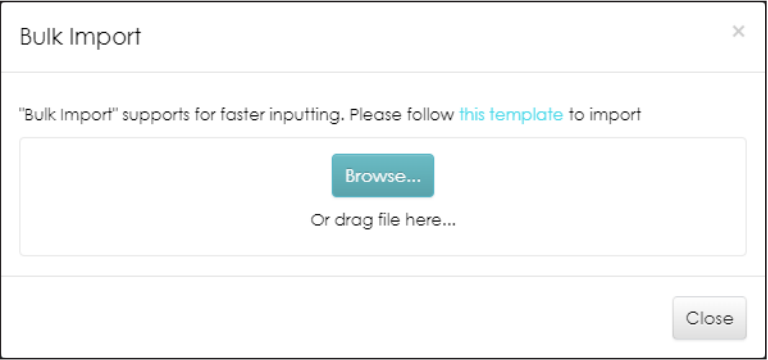

LABEL	DESCRIPTION
Account Type	<p>Select the type of user accounts that you want to display or create.</p> <p><b>User</b> - an internal user that can gain access to the networks by authenticating with a RADIUS server via the IEEE 802.1x or WPA2 authentication method or the captive portal.</p> <p><b>MAC</b> - an internal user that can gain access to the networks by authenticating with a RADIUS server via the MAC-based authentication method.</p> <p><b>Guest</b> - a guest that can gain access to the networks via the captive portal.</p> <p><b>VPN User</b> - a L2TP VPN client that can gain access to the networks by authenticating with the Nebula cloud authentication server.</p>
Authorization	<p>This button is available only when your administrator account has full access to the organization.</p> <p>Select one or more than one user account and click this button to configure the authorization settings for the selected user account(s).</p> 
Remove users	<p>This button is available only when your administrator account has full access to the organization.</p> <p>Select one or more than one user accounts and click this button to remove the selected user account(s).</p>
Search	<p>Enter a key word as the filter criteria to filter the list of user accounts.</p>
Users	<p>This shows how many user accounts of the selected type displayed in the list and how many user accounts match the filter criteria.</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 7.3.6.1 on page 183</a>.</p>
Export	<p>Click this button to save the account list as a CSV or XML file to your computer.</p>
Email	<p>This field is available only when the account type is set to <b>User</b>, <b>Guest</b> or <b>VPN User</b>.</p> <p>This shows the email address of the user account.</p>

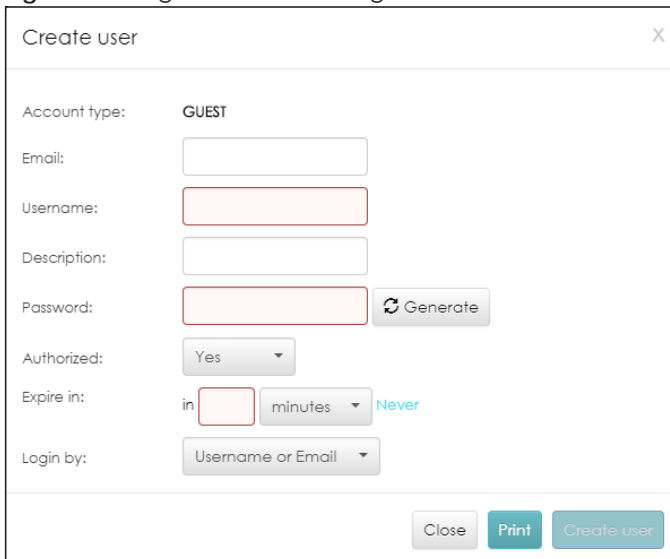
Table 77 Organization &gt; Configure &gt; Cloud Authentication (continued)

LABEL	DESCRIPTION
Username	This field is available only when the account type is set to <b>User</b> , <b>Guest</b> or <b>VPN User</b> . This shows the user name of the user account.
Description	This shows the descriptive name of the user account.
MAC address	This field is available only when the account type is set to <b>MAC</b> . This shows the MAC address of the user account.
Account type	This shows the type of the user account.
Authorized	This shows whether the user has been authorized or not.
Authorized by	This shows the email address of the administrator account that authorized the user.
Expire in	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.
Login by	This field is available only when the account type is set to <b>User</b> , <b>Guest</b> or <b>VPN User</b> . This shows whether the user needs to log in with the email address and/or user name.
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.

### 7.3.6.1 Create/Update User

In the **Organization > Configure > Cloud Authentication** screen, click the **Add new user** button to create a new user account or double-click an existing account entry to modify the account settings.

Figure 96 Organization &gt; Configure &gt; Administrator: Create/Update user



Create user
X

---

Account type: **GUEST**

Email:

Username:

Description:

Password:  Generate

Authorized: Yes ▾

Expire in: in  minutes ▾ Never

Login by: Username or Email ▾

Close Print Create user

The following table describes the labels in this screen.

Table 78 Organization > Configure > Administrator: Create/Update user

LABEL	DESCRIPTION
Account type	This is the type of the user account.
Email	Enter the email address of the user account, which is used to log into the networks.
Username	This field is not available when the account type is <b>MAC</b> . Enter the user name of this account.
Description	Enter a descriptive name for the account.
Password	This field is not available when the account type is <b>MAC</b> . Enter the password of this user account. It can consist of 4 - 31 alphanumeric characters. You can click <b>Generate</b> to have the NCC create a password for the account automatically, and select the checkbox to send the password to the user via email.
MAC address	This field is available only when the account type is <b>MAC</b> . Enter the MAC address of this account.
Authorized	Set whether you want to authorize the user of this account.
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. Otherwise, select <b>Never</b> and the user of this account will never be logged out.
Login by	This field is not available when the account type is <b>MAC</b> . Select whether the user needs to log in with the email address and/or user name.
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.

### 7.3.7 VPN Members

Use this screen to view and manage the VPN members in the organization.

Click **Organization > Configure > VPN Members** to access this screen.



Figure 97 Organization > Configure > VPN Members

SITE-WIDE
AP
SWITCH
GATEWAY
ORGANIZATION
HELP

VPN Topology BETA

**VPN members**

Topology: Hub-and-Spoke

Maximum site connectivity: 200

Connect site member: 25

Note: In an Organization, the maximum number of Site-to-Site VPN tunnels allowed is determined by the least capacity model. For example, have NSG50 and NSG100 connected, the maximum number is determined by NSG50.

**Hub status**

Site	Model	Subnet(s)	NSG status	Members	NAT traversal
Hub	NSG200	10.0.1.0/24 172.16.0.0/12 10.251.0.0/16 10.253.0.0/16	Online	25	

**Site connectivity**

Site	Model	Subnet(s)	NSG status	Join member	NAT traversal
Site01_GSBU_KH	NSG50	100.1.1.0/24	Offline	<input checked="" type="checkbox"/>	
Site02_AE	NSG50	100.2.1.0/25	Online	<input checked="" type="checkbox"/>	
Site03_AE_HS	NSG50	100.3.1.0/25 100.3.1.200/29	Online	<input checked="" type="checkbox"/>	
Site04_CSO_Jason	NSG50	100.4.1.0/24	Offline	<input checked="" type="checkbox"/>	127.0.0.1
Site05_GSBU_Joshua	NSG50	100.5.1.0/24	Online	<input checked="" type="checkbox"/>	
Site06_SVD_Steven	NSG50	100.6.1.0/24	Offline	<input checked="" type="checkbox"/>	122.116.217.2
Site07_SVD_Luke	NSG50	100.7.1.0/24	Offline	<input type="checkbox"/>	127.0.0.1
Site08_SVD_Mandy	NSG50	100.8.1.0/24	Online	<input checked="" type="checkbox"/>	123.195.193.205
Site09_SVD_Jon	NSG50	100.9.1.0/24	Online	<input checked="" type="checkbox"/>	123.192.85.15
Site10_NSG_RD_Daniel	NSG50	100.10.1.0/24	Offline	<input type="checkbox"/>	

1 2 3 4

Go to 1 Results per page 10

or

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

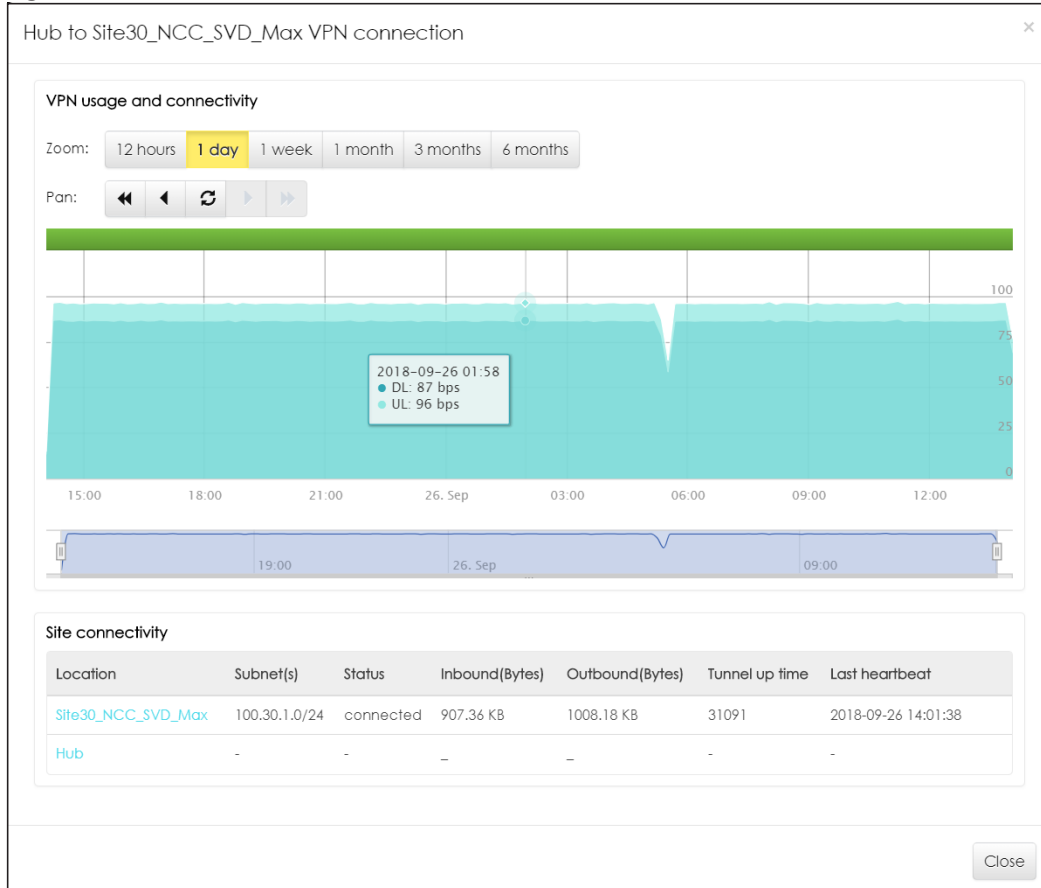
The following table describes the labels in this screen.

Table 79 Organization > Configure > VPN Members

LABEL	DESCRIPTION
VPN Topology	
The VPN topology specifies how the Nebula gateways in the organization are connected to each other via VPN. Each map pin depicts a site. Click a map pin to show its site name. Click a line to view the VPN usage and connectivity of the VPN connection between two sites.	
VPN Members	
Topology	This shows the VPN topology of the organization.
Maximum site connectivity	This shows the maximum number of Site-to-Site VPN tunnels allowed in the organization. It is determined by the maximum allowed for the smallest model.
Connect site member	This shows the number of Site-to-Site VPN tunnels which are currently set up in the organization.
Hub Status	This section displays when a Hub-and-Spoke VPN topology is used in the organization.
Hub	This shows the name of the site whose security gateway acts as the hub router in the Hub-and-Spoke VPN topology  Click the name to go to the <b>Site-Wide &gt; Dashboard</b> screen.
Model	This shows the model name of the security gateway assigned to the site.
Subnet(s)	This shows the address(es) of the local network behind the security gateway, on which the computers are allowed to use the VPN tunnel.
NSG status	This shows whether the security gateway is online or goes off-line.
Members	This shows the number of sites which set up a VPN connection with other sites in the organization.
NAR traversal	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	
Site	This shows the name of the site in this organization.  Click the name to go to the <b>Site-Wide &gt; Dashboard</b> screen.
Model	This shows the model name of the security gateway assigned to the site.
Subnet(s)	This shows the address(es) of the local network behind the security gateway, on which the computers are allowed to use the VPN tunnel.
NSG status	This shows whether the security gateway is online or goes off-line.
Join member	Select <b>ON</b> to set the VPN topology of the security gateway to <b>Site-to-Site</b> by default or <b>Hub-and-Spoke</b> when another site in the same organization has permitted the use of Hub-and-Spoke VPN topology. Otherwise, select <b>OFF</b> to not set a VPN connection.  This also change the VPN topology in the <b>Gateway &gt; Configure &gt; Site-to-Site VPN</b> screen (see <a href="#">Section 6.3.5 on page 146</a> ).
NAT traversal	This shows the public IP address or the domain name that is configured and mapped to the security gateway on the NAT router.

### 7.3.7.1 VPN Usage and Connectivity

From the **Organization > Configure > VPN Members** screen, click a green line in the VPN topology to view the VPN statistics and connection status between two sites.

**Figure 98** Organization > Configure > VPN Members: VPN Usage and Connectivity

The following table describes the labels in this screen.

**Table 80** Organization > Configure > VPN Members: VPN Usage and Connectivity

LABEL	DESCRIPTION
VPN 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 twelve hours, day, week, month, three months or six months.
Pan	Click to move backward or forward by 12 hours, one day or one week.
Site Connectivity	
Location	This shows the name of the site to which the gateway is assigned. Click the name to go to the <b>Gateway &gt; Configure &gt; Site-to-Site VPN</b> screen, where you can modify the VPN settings.
Subnet(s)	This shows the address(es) of the local network 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.

Table 80 Organization &gt; Configure &gt; VPN Members: VPN Usage and Connectivity (continued)

LABEL	DESCRIPTION
Last heartbeat	This shows the last date and time a heartbeat packet is sent to determine if the VPN tunnel is up or down.
Close	Click this button to exit this screen without saving.

## 7.3.8 Configuration Management

Configuration synchronization allows you to easily propagate 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 site or switch configurations to the NCC and restore the configuration at a later date.

Click **Organization > Configure > Configuration Management** to access this screen.

Figure 99 Organization &gt; Configure &gt; Configuration Management

The screenshot displays the Configuration Management interface. At the top, there is a navigation bar with tabs for SITE-WIDE, AP, SWITCH, GATEWAY, ORGANIZATION (selected), and HELP. The main content area is titled 'Configuration management' and is divided into three sections:

- Synchronization:** This section allows for propagating configurations. It features a 'Settings' dropdown menu set to 'Site-wide general settings', a 'From source site:' dropdown set to 'test', and a 'To site(s):' dropdown set to 'Select some sites'. A 'What will be synchronized?' link and a 'Sync' button are also present.
- Switch settings clone:** This section allows for cloning switch settings. It features a 'From source device:' dropdown set to 'Select a device', a 'To device(s):' dropdown set to 'Select some devices', and a checkbox for 'Include uplink port settings'. A 'What will be cloned?' link and a 'Clone' button are also present.
- Backup & restore (BETA):** This section allows for backing up and restoring configurations. It includes a table of backups for 'Site(s) settings':
 

Backup	Description	Date (UTC)	Admin
1	testing	2019-01-09 03:36:00	Bayardo Salgado
	Automatic backup	2019-01-09 03:19:59	System

 Below the table is an '+ Add' button, a 'Restore from backup:' dropdown set to 'Backup: testing', and a 'Restore to site(s):' dropdown set to 'Select some sites'. A 'What is this?' link and a 'Restore' button are also present.

At the bottom, there is a 'Switch settings' section with a '(No snapshot backups saved yet)' message, an '+ Add' button, a 'What is this?' link, and a 'Restore' button.

The following table describes the labels in this screen.

Table 81 Organization > 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	
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 site(s) to which you want to restore the specified configuration backup.
Restore	Click this button to overwrite the settings of the site(s) 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.

Table 81 Organization &gt; Configure &gt; Configuration Management (continued)

LABEL	DESCRIPTION
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 clickable only when you have at least one switch in the organization.
Restore from backup	Select the backup you want to restore.
Restore to device(s)	Select one or more Nebula switches to which you want to restore the specified configuration backup.  Note: You can restore the backup to the same switch or switches of the same model and registered to a site in the organization.
Restore	Click this button to overwrite the settings of the switch(es) with the selected configuration backup.

# CHAPTER 8

## 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 via the NCC.
- Make sure that you have registered your Nebula devices with the NCC. See [Section 7.3.2 on page 171](#).
- Make sure that you have created an organization and site and add the devices to the site. See [Create Organization on page 20](#) and [Section 7.3.1 on page 171](#).
- Check that the license has not expired.

## 8.1 Getting More Troubleshooting Help

Go to [support.zyxel.com](http://support.zyxel.com) at the Zyxel website for other technical information on the NCC.



# APPENDIX A

## Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See <http://www.zyxel.com/homepage.shtml> and also [http://www.zyxel.com/about\\_zyxel/zyxel\\_worldwide.shtml](http://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
- <http://www.zyxel.com>

### Asia

#### China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

#### India

- Zyxel Technology India Pvt Ltd
- <http://www.zyxel.in>

#### Kazakhstan

- Zyxel Kazakhstan
- <http://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
- <http://www.zyxel.com/tw/zh/>

### **Thailand**

- Zyxel Thailand Co., Ltd
- <http://www.zyxel.co.th>

### **Vietnam**

- Zyxel Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

## **Europe**

### **Austria**

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

### **Belarus**

- Zyxel BY
- <http://www.zyxel.by>

## **Belgium**

- Zyxel Communications B.V.
- <http://www.zyxel.com/be/nl/>
- <http://www.zyxel.com/be/fr/>

## **Bulgaria**

- Zyxel България
- <http://www.zyxel.com/bg/bg/>

## **Czech Republic**

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

## **Denmark**

- Zyxel Communications A/S
- <http://www.zyxel.dk>

## **Estonia**

- Zyxel Estonia
- <http://www.zyxel.com/ee/et/>

## **Finland**

- Zyxel Communications
- <http://www.zyxel.fi>

## **France**

- Zyxel France
- <http://www.zyxel.fr>

## **Germany**

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

## **Hungary**

- Zyxel Hungary & SEE
- <http://www.zyxel.hu>

## **Italy**

- Zyxel Communications Italy
- <http://www.zyxel.it/>

## **Latvia**

- Zyxel Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

## **Lithuania**

- Zyxel Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

## **Netherlands**

- Zyxel Benelux
- <http://www.zyxel.nl>

## **Norway**

- Zyxel Communications
- <http://www.zyxel.no>

## **Poland**

- Zyxel Communications Poland
- <http://www.zyxel.pl>

## **Romania**

- Zyxel Romania
- <http://www.zyxel.com/ro/ro>

## **Russia**

- Zyxel Russia
- <http://www.zyxel.ru>

## **Slovakia**

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

## **Spain**

- Zyxel Communications ES Ltd
- <http://www.zyxel.es>

## **Sweden**

- Zyxel Communications
- <http://www.zyxel.se>

## **Switzerland**

- Studerus AG

- <http://www.zyxel.ch/>

### **Turkey**

- Zyxel Turkey A.S.
- <http://www.zyxel.com.tr>

### **UK**

- Zyxel Communications UK Ltd.
- <http://www.zyxel.co.uk>

### **Ukraine**

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

## **Latin America**

### **Argentina**

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

### **Brazil**

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

### **Ecuador**

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

## **Middle East**

### **Israel**

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

### **Middle East**

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>

## North America

### USA

- Zyxel Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

## Oceania

### Australia

- Zyxel Communications Corporation
- <http://www.zyxel.com/au/en/>

## Africa

### South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

# APPENDIX B

## Legal Information

### Copyright

Copyright © 2019 by Zyxel Communications Corporation.

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 to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

### Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at [www.zyxel.com](http://www.zyxel.com). If you cannot find it there, contact your vendor or Zyxel Technical Support at [support@zyxel.com.tw](mailto:support@zyxel.com.tw).

To obtain the source code covered under those Licenses, please contact your vendor or Zyxel Technical Support at [support@zyxel.com](mailto:support@zyxel.com).