

User's Guide

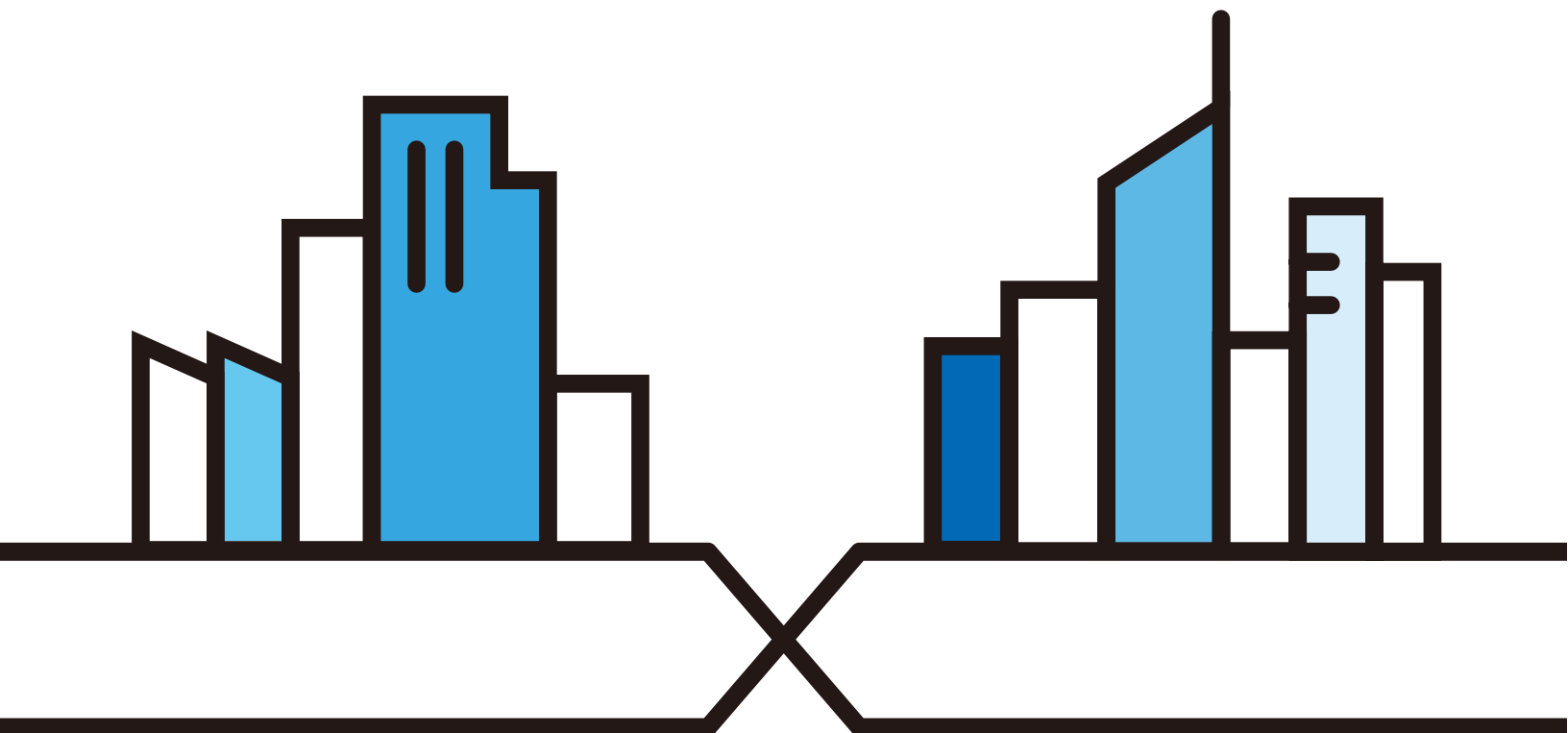
NCC

Nebula Control Center

Default Login Details

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

Version 10.1 Edition 1, 9/2020



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

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

Related Documentation

- Nebula Device Quick Start Guide

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

- Nebula Device User's Guide

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

- More Information

Go to **support.zyxel.com** to find other information on the NCC.



Table of Contents

Table of Contents	3
-------------------------	---

Part I: User's Guide	7
----------------------------	---

Chapter 1	
Introduction	8

1.1 NCC Overview	8
1.1.1 NCC Versions	9
1.1.2 NCC Version Differences	10
1.1.3 Relationship between Organizations, Sites and Accounts	13
1.2 Getting Started	15
1.2.1 Connect Nebula Managed Devices	15
1.2.2 Access the NCC Portal	15
1.3 NCC Portal Overview	21
1.3.1 Title Bar	22
1.3.2 Navigation Panel	24
1.4 Create Organization	28
1.5 Choose Organization	29

Chapter 2	
Setup Wizard	31

2.1 Access the Wizard	31
2.2 Use the Wizard	31
2.2.1 Step 1 Create an Organization and Site	32
2.2.2 Step 2 Add Your Devices	32
2.2.3 Step 3 Set up your WiFi Network	33
2.2.4 Step 4 Set up a Guest WiFi Network	33
2.2.5 Summary	34
2.2.6 Activate NCC Pro Pack and Security Services Trial Period	35

Part II: Technical Reference	36
------------------------------------	----

Chapter 3	
MSP	37

3.1 Overview	37
3.2 MSP Portal	37

3.3 License Transfer	38
3.4 MSP Branding	39

Chapter 4

Organization-wide.....41

4.1 Overview	41
4.2 Monitor	41
4.2.1 Organization Overview	41
4.2.2 Change Log	45
4.3 Configure	46
4.3.1 Create Site	46
4.3.2 Inventory	47
4.3.3 License Management	48
4.3.4 Organization Settings	53
4.3.5 Administrator	55
4.3.6 Cloud Authentication	59
4.3.7 VPN Members	65
4.3.8 Configuration Management	69
4.3.9 Configuration Template	71
4.3.10 Firmware Management	74

Chapter 5

Site-wide.....76

5.1 Monitor	76
5.1.1 Dashboard	76
5.1.2 Map & Floor Plans	78
5.1.3 Topology	80
5.1.4 Vouchers	81
5.1.5 Summary Report	84
5.2 Configure	87
5.2.1 General Settings	87
5.2.2 Alert Settings	90
5.2.3 Add Devices	92
5.2.4 Firmware Management	93
5.2.5 Cloud Authentication	96

Chapter 6

Security Gateway.....100

6.1 Overview	100
6.2 Monitor	100
6.2.1 Security Gateway	100
6.2.2 Clients	103
6.2.3 Event Log	108

6.2.4 VPN Connections	109
6.2.5 NSS Analysis Report	111
6.2.6 Summary Report	113
6.3 Configure	117
6.3.1 Interface Addressing	117
6.3.2 Link Aggregation Groups	125
6.3.3 Policy Route	133
6.3.4 Firewall	134
6.3.5 Security Service	140
6.3.6 Site-to-Site VPN	143
6.3.7 Remote Access VPN	149
6.3.8 Captive Portal	150
6.3.9 Network Access Method	153
6.3.10 Traffic Shaping	155
6.3.11 Gateway Settings	158

Chapter 7

Switch.....163

7.1 Overview	163
7.2 Monitor	163
7.2.1 Switches	163
7.2.2 Clients	173
7.2.3 Event Log	176
7.2.4 IPTV Report	176
7.2.5 Surveillance	180
7.2.6 Surveillance Port Details	181
7.2.7 Summary Report	182
7.3 Configure	185
7.3.1 Switch Ports	185
7.3.2 ACL	192
7.3.3 Advanced IGMP	193
7.3.4 RADIUS Policies	198
7.3.5 PoE Schedules	199
7.3.6 Switch Settings	201

Chapter 8

Access Point.....205

8.1 Overview	205
8.1.1 Nebula Smart Mesh	205
8.1.2 Smart Mesh Network Topology	206
8.2 Monitor	207
8.2.1 Access Points	207
8.2.2 Clients	215

8.2.3 Event Log	220
8.2.4 Wireless Health	220
8.2.5 Summary Report	223
8.3 Configure	226
8.3.1 SSID Overview	226
8.3.2 Authentication	228
8.3.3 Captive Portal	235
8.3.4 SSID Availability	239
8.3.5 Radio Settings	241
8.3.6 AP & Port Settings	245
Chapter 9	
Help	249
9.1 Support Request	249
Chapter 10	
Troubleshooting.....	252
10.1 Getting More Troubleshooting Help	253
Appendix A Customer Support	254
10.2 Zyxel Support	254
10.3 NCC Live Chat	259
Appendix B Legal Information	261
Index	262

PART I

User's Guide

CHAPTER 1

Introduction

1.1 NCC Overview

The Zyxel Nebula Control Center (NCC) is a cloud-based network management system that allows you to remotely manage and monitor Zyxel Nebula APs, Ethernet switches, and security gateways. You need to set up a myZyxel account in order to log into the NCC and manage your Nebula devices, as discussed in [Section 1.2.2 on page 15](#).

NCC feature support includes:

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

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

Table 1 Supported Nebula Devices

SECURITY GATEWAY	ETHERNET SWITCH	ACCESS POINT (AP)
<ul style="list-style-type: none"> NSG50 NSG100 NSG200 NSG300 	<ul style="list-style-type: none"> NSW100-10P NSW100-28P NSW200-28P GS1350 GS1920v2 series GS2220 series XGS1930 series XS3800-28 XS1930 series 	<ul style="list-style-type: none"> NAP102 NAP203 NAP303 NAP353 NWA110AX NWA210AX NWA1123-ACv2 NWA1123-AC HD NWA1123-AC PRO NWA1302-AC NWA5123-AC HD WAC500 WAC500H WAC5302D-Sv2 WAC6103D-I WAC6303D-S WAC6502D-S WAC6502D-E WAC6503D-S WAC6552D-S WAC6553D-E NWA110X NWA1123-ACv3 WAX50D WAX510D WAX610D WAX650S

1.1.1 NCC Versions

Zyxel offers two versions of the NCC: Nebula Professional Pack and Nebula Basic. The professional pack requires NCC licenses and provides the whole set of features you would need or expect to manage your network. Nebula Basic is the free version of NCC that has limited features (see [Section 1.1.2 on page 10](#)).

The two NCC versions are organization-based. You can create and manage either or both Nebula Professional Pack organization(s) and Nebula Basic 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 an 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.

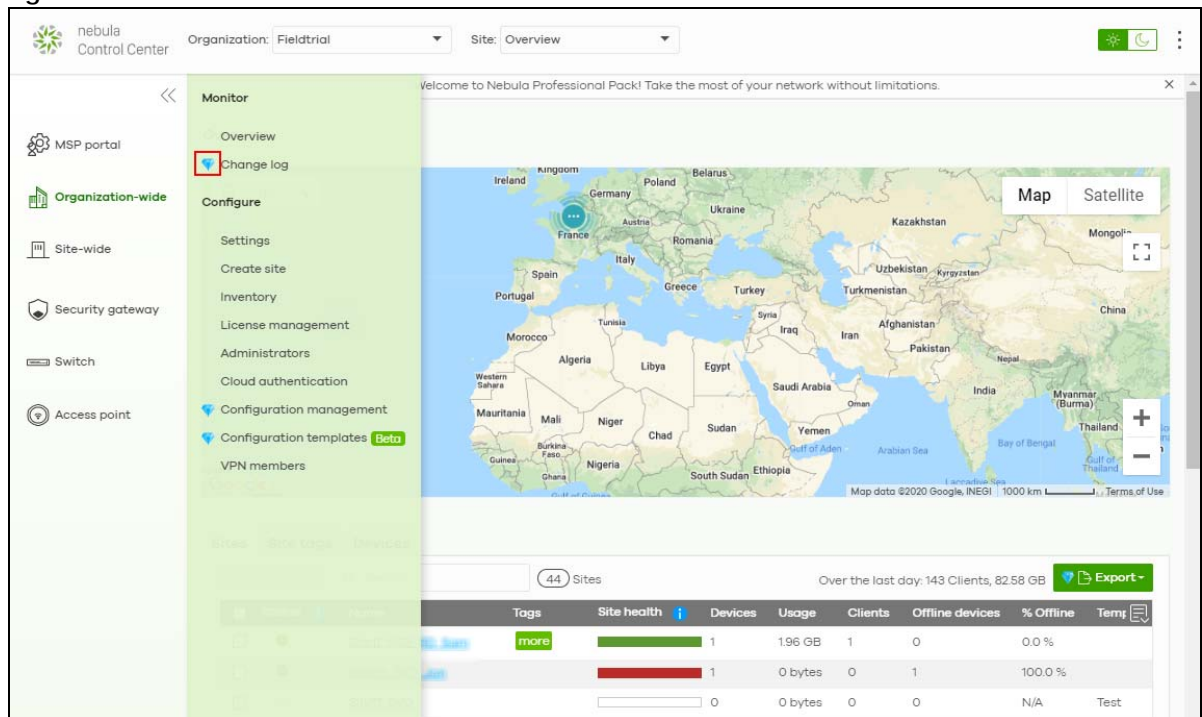
Nebula Basic (Free)

With a free Nebula 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 the number of days remaining before the license expires is greater than 90. See [Section 4.3.3 on page 48](#) for license management.

After logging into the NCC and selecting to manage a Nebula free organization, you will see the diamond icon (💎) next to a feature, which indicates the feature is available only for Nebula Professional Pack organizations and sites. 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

Figure 1 NCC Professional Pack Icon



1.1.2 NCC Version Differences

The differences of Nebula Basic (free version) from Nebula Professional Pack are listed below.

Table 2 NCC Version Differences

FEATURE	NEBULA BASIC	NEBULA PROFESSIONAL PACK	NCC LOCATION
Number of administrator accounts	5	No limit	Organization-wide > Configure > Administrators
Number of cloud authentication entries	100	No limit	Organization-wide > Configure > Cloud authentication

Table 2 NCC Version Differences

FEATURE	NEBULA BASIC	NEBULA PROFESSIONAL PACK	NCC LOCATION
Number of Nebula device (AP, switch or gateway) photos	1	5	Access point > Monitor > Access point > [Select AP]
Statistics or monitoring information	Up to 7 days	Up to 365 days	AP / SW / GW > Monitor > Event log
Custom range of up to 365 days on summary reports	No	Yes	Site-wide > Monitor > Summary report AP / SW / GW > Monitor > Summary report
Last 30 days on device monitoring screen	No	Yes	AP / SW / GW > Monitor > AP / SW / GW
Last 30 days on client monitoring screen	No	Yes	AP / SW / GW > Clients
Send summary reports by email immediately or on a schedule	No	Yes	Site-wide / AP / SW / GW > Summary report
Smart email alerts	No	Yes	Site-wide > Configure > Alert settings
In-app push notifications	Only send notifications about online/offline status	Yes	App Notification Center
Log changes to organization settings	No	Yes	Organization-wide > Monitor > Change log
Priority support requests (direct NCC)	No (Forum and regional support still available)	Yes	Help > Support request
Web Chat support	No	Yes	Whole website
MSP branding customization	No	Yes	MSP Portal
Viewing the site-wide network topology	No	Yes	Site-wide
Viewing organization VPN topology and per-tunnel usage	No	Yes	Organization-wide > Configure > VPN members
VPN provision script email: Send L2TP client provision by email for quick VPN setup.	No	Yes	Organization-wide > Configure > VPN members
Viewing AV/Application Patrol/Content Filtering/IDP usage & hits (NSS-SP license required)	Up to 7 days	Up to 365 days	AP / SW / GW > Monitor > AP / SW / GW > [Select AP / SW / GW]
Configuring AV/Application Patrol/Content Filtering/IDP settings (NSS-SP license required)	No	Yes	Security Gateway > Configure > Security Service
Viewing IPTV report and channel information	No	Yes	Switch > Monitor > IPTV report
Viewing surveillance devices information	No	Yes	Switch > Monitor > Surveillance
Adding clients for a managed AP or gateway	No	Yes	AP / GW > Monitor > Clients
Cloning site settings when creating a site	No	Yes	Organization-wide > Configure > Create site
Specifying login IP address ranges for an organization	No	Yes	Organization-wide > Configure > Setting
Exporting data to a CSV or XML file	No	Yes	Any monitoring screen with a table

Table 2 NCC Version Differences

FEATURE	NEBULA BASIC	NEBULA PROFESSIONAL PACK	NCC LOCATION
Creating firmware upgrade schedules on a per-device basis	No	Yes	Site-wide > Configure > Firmware Management
Creating firmware upgrade schedules for all devices in an organization	No	Yes	Organization-wide > Configure > Firmware management
Remote CLI connection on AP and gateway live tools	No	Yes	AP / GW > Monitor > AP / GW
Dynamic VLAN assignment with Nebula cloud authentication server on WPA2/ WPA3-Enterprise authentication	No	Yes	Organization-wide > Configure > Cloud authentication (Account type: User)
Captive portal third-party integration with customized URL parameter	No	Yes	Access point > Configure > Captive portal
Enabling RADIUS accounting with captive portal for an SSID profile	No	Yes	Access point > Configure > Authentication
Setting NAS ID for web authentication (captive portal) via RADIUS	No	Yes	Access point > Configure > Authentication
Broadcast storm control supported on 802.11ac wave2 and 802.11ax series APs with LAN ports	No	Yes	Access point > Monitor > Access point > [Select AP]
Configure wireless bridge on APs.	No	Yes	Access point > Monitor > Access point > [Select AP]
Sending AP traffic logs to a syslog server for NAT SSIDs	No	Yes	Site-wide > Configure > General settings
Vendor ID based VLAN assignment	No	Yes	Switch > Configure > Switch settings
Configuring IGMP snooping, IGMP filtering profiles and IGMP-related port settings	No	Yes	Switch > Configure > Advanced IGMP
Limit the ingress and egress bandwidth of the Switch ports	No	Yes	Switch > Configure > Switch ports > [Edit the Selected port]
Switch port extended range	No	Yes	Switch > Monitor > Surveillance
Switch port Auto Powered Device (PD) recovery	No	Yes	Switch > Monitor > Surveillance
Configuration management including site settings synchronizing, switch settings cloning and configuration backup/ restoration	No	Yes	Organization-wide > Configure > Configuration management
Creating configuration templates and binding sites	No	Yes	Organization-wide > Configure > Configuration templates
Setting a signal strength threshold for smart steering on a per-AP basis	No	Yes	Access point > Configure > Radio settings > [Edit the Selected AP]
Enabling web authentication with Facebook WiFi	No	Yes	Access point > Configure > Authentication
Dynamic Personal Pre-Shared Key (DPPSK)	No	Yes	Access point > Configure > Authentication

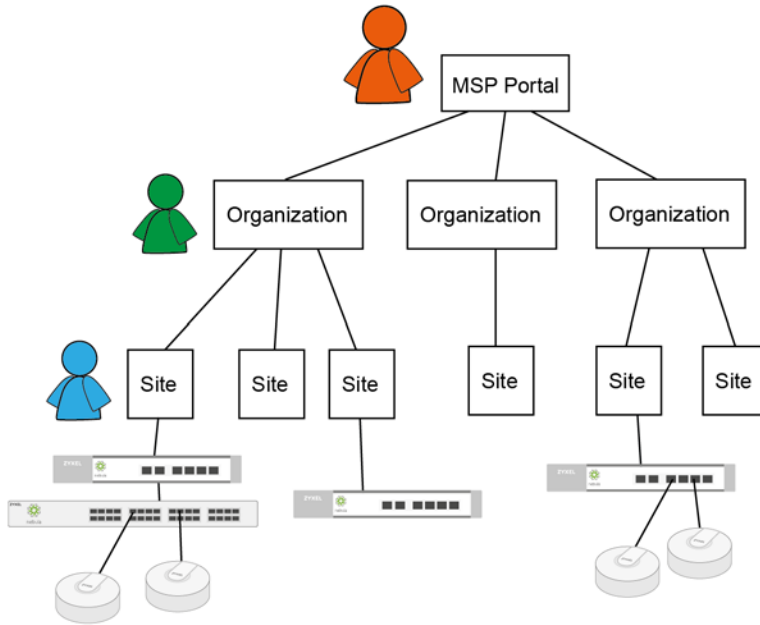
Table 2 NCC Version Differences

FEATURE	NEBULA BASIC	NEBULA PROFESSIONAL PACK	NCC LOCATION
Cloud Authentication DPPSK Account Type	No	Yes	Organization-wide > Configure > Cloud authentication (Account type: DPPSK)
Cloud Authentication Sign-in method by Voucher	No	Yes	Site-wide > Monitor > Vouchers Site-wide > Configure > General Settings Access Point > Configure > Authentication Access Point > Configure > Captive Portal > [Portal Theme]
Viewing wireless health report	No	Yes	Access point > Monitor > Wireless health

1.1.3 Relationship between Organizations, Sites and Accounts

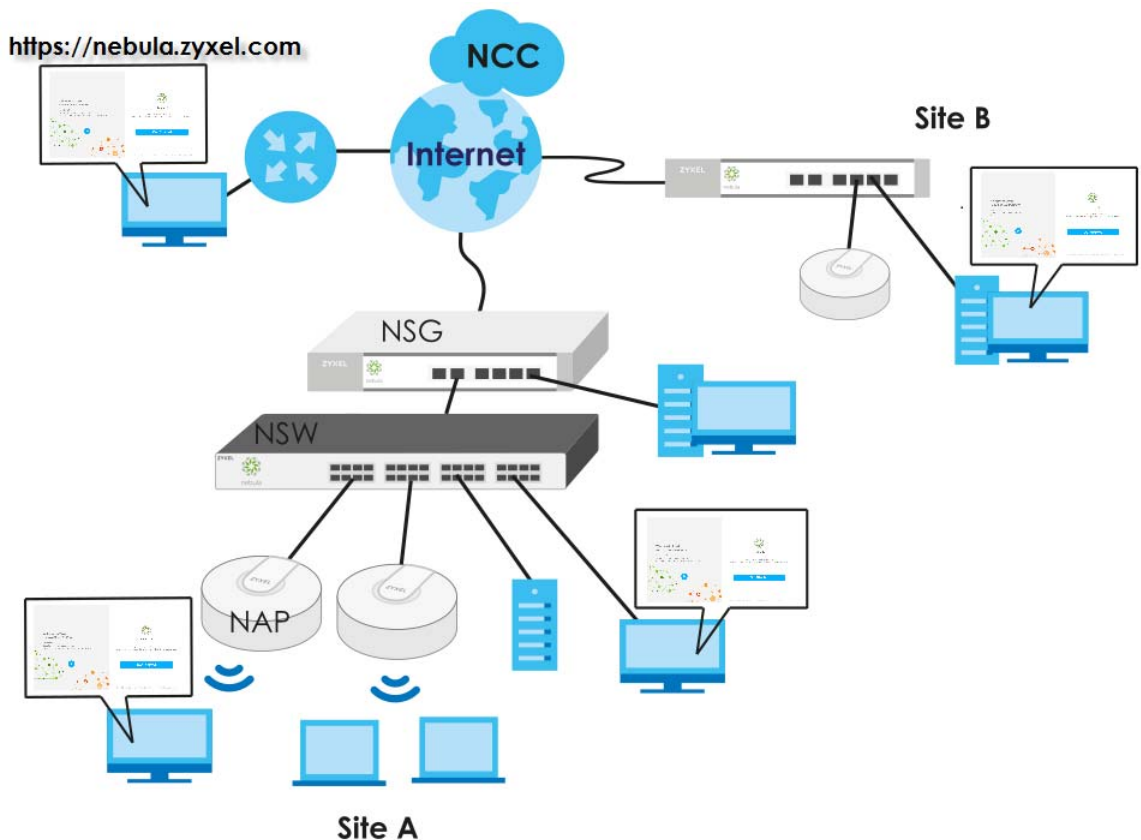
In the NCC, a site is a group of Nebula-managed devices in the same network. An organization is a group of sites. To use the NCC to manage your Nebula devices, each device should be assigned to a site and the site must belong to an organization.

- A site can have multiple Nebula devices, but can only belong to one organization.
- A site can be managed by more than one site/organization administrator.
- An organization can contain multiple sites and can be managed by more than one organization administrator.
- A myZyxel.com account can be an organization administrator and/or site administrator in the NCC (see [Section 4.3.5 on page 55](#)).
- A Managed Service Provider (MSP) network is a group of organizations that belong to the same organization administrator. The organization administrator can use the MSP portal page to view the organization summary and transfer licenses (see [Chapter 3 on page 37](#)).
- 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 2 NCC Example Network Topology



1.2 Getting Started

You can perform network management with the NCC using an Internet browser. Browsers supported are:

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

You can also download the Zyxel Nebula Mobile APP available on Google Play or the App Store.

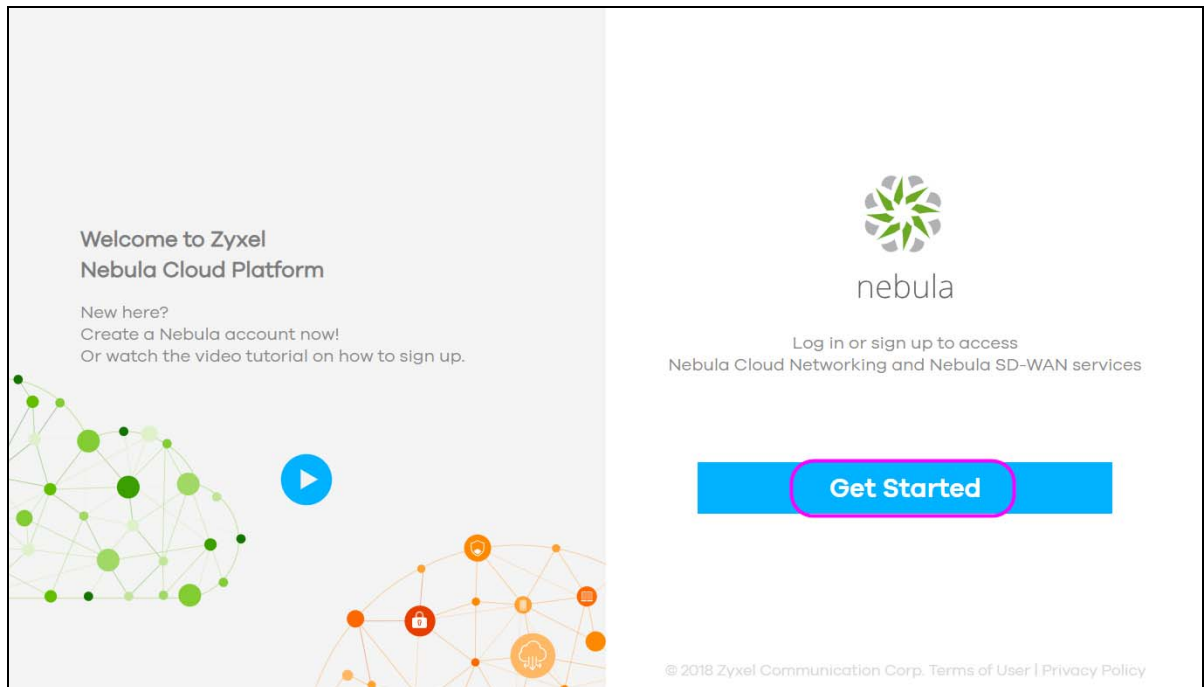
1.2.1 Connect Nebula Managed Devices

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.

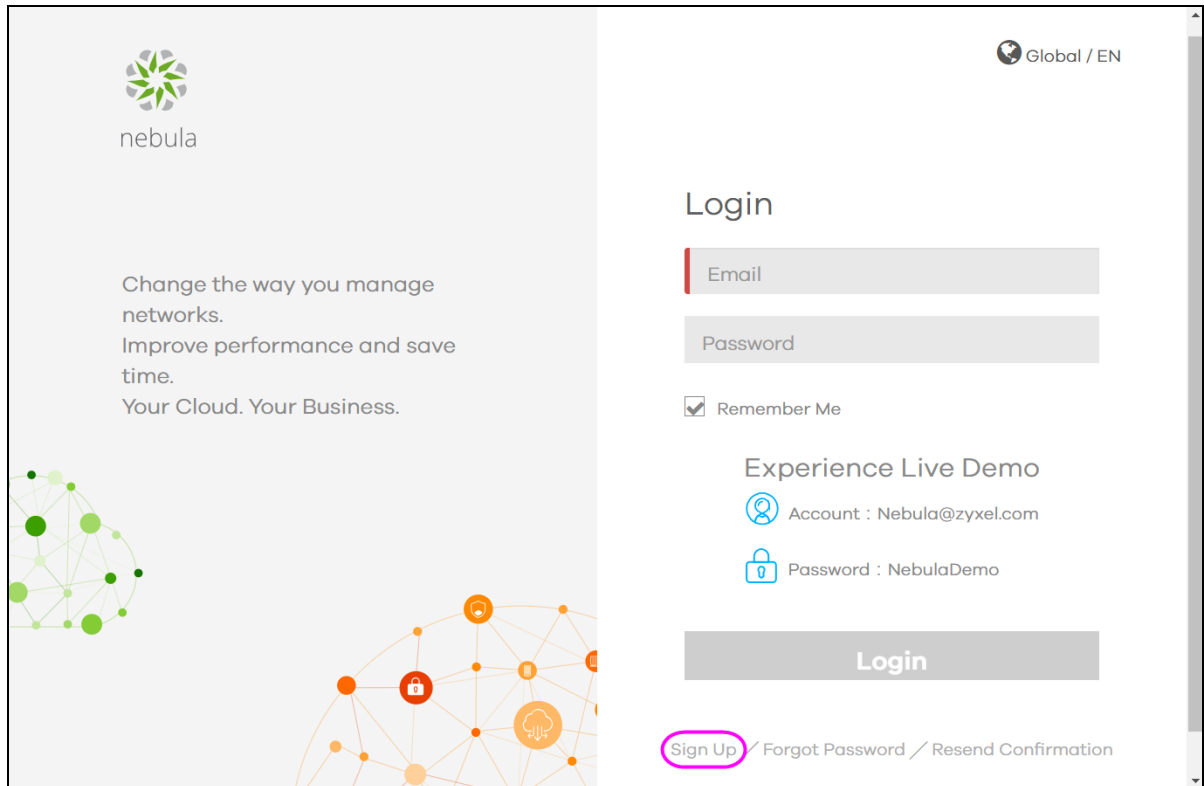
1.2.2 Access the NCC Portal

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 do not have a myZyxel account and create an account with your existing email address.



The image shows the Nebula login page. On the left, there is a Nebula logo and a tagline: "Change the way you manage networks. Improve performance and save time. Your Cloud. Your Business." Below this is a decorative network diagram. On the right, there is a "Login" section with input fields for "Email" and "Password", a "Remember Me" checkbox, and a "Login" button. Below the login section, there is a "Sign Up" link circled in pink, followed by "Forgot Password" and "Resend Confirmation" links. At the top right, there is a "Global / EN" link.

Global / EN

nebul
Change the way you manage networks.
Improve performance and save time.
Your Cloud. Your Business.

Login

Email

Password

☒ Remember Me

Experience Live Demo

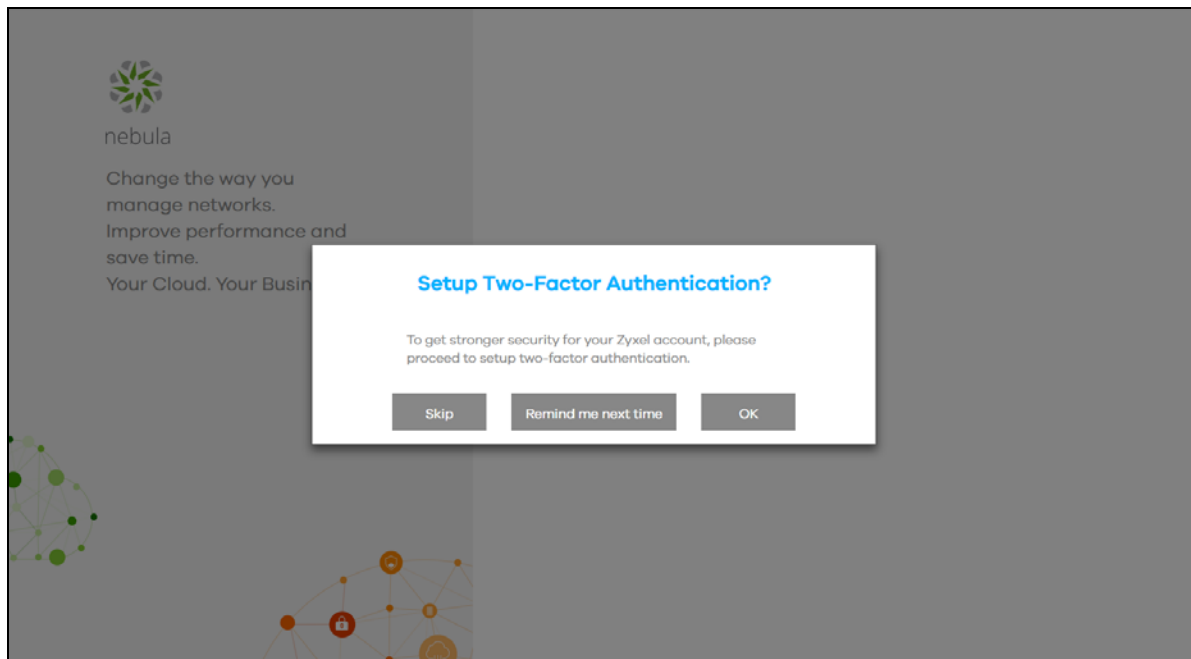
Account : Nebula@zyxel.com

Password : NebulaDemo

Login

Sign Up / Forgot Password / Resend Confirmation

- 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.



The image shows a dialog box titled "Setup Two-Factor Authentication?". The dialog contains the text: "To get stronger security for your Zyxel account, please proceed to setup two-factor authentication." Below this text are three buttons: "Skip", "Remind me next time", and "OK". The background of the page is dimmed, showing the same Nebula logo and tagline as the previous image.

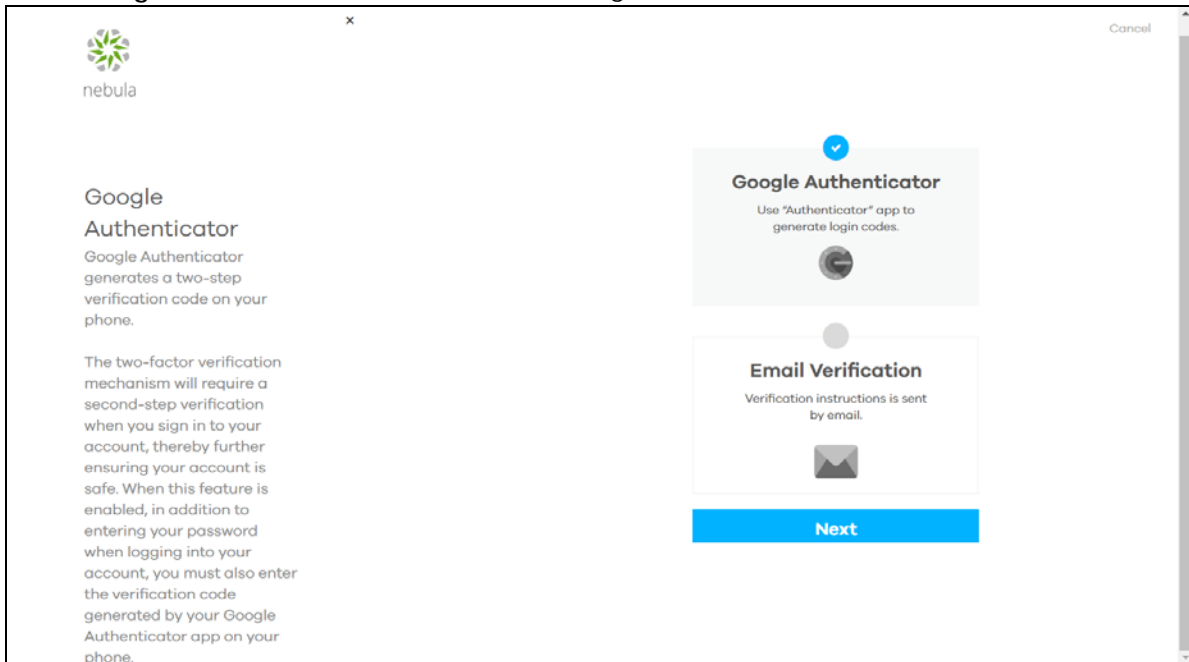
nebul
Change the way you manage networks.
Improve performance and save time.
Your Cloud. Your Business.

Setup Two-Factor Authentication?

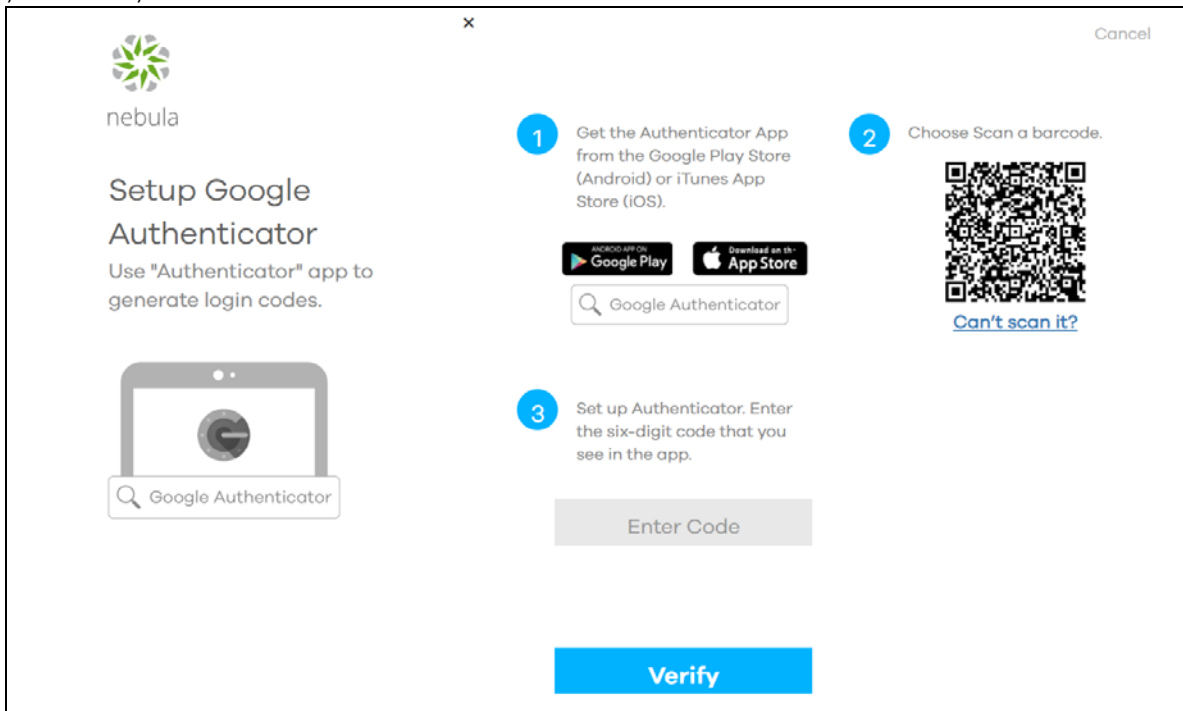
To get stronger security for your Zyxel account, please proceed to setup two-factor authentication.

Skip Remind me next time OK

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

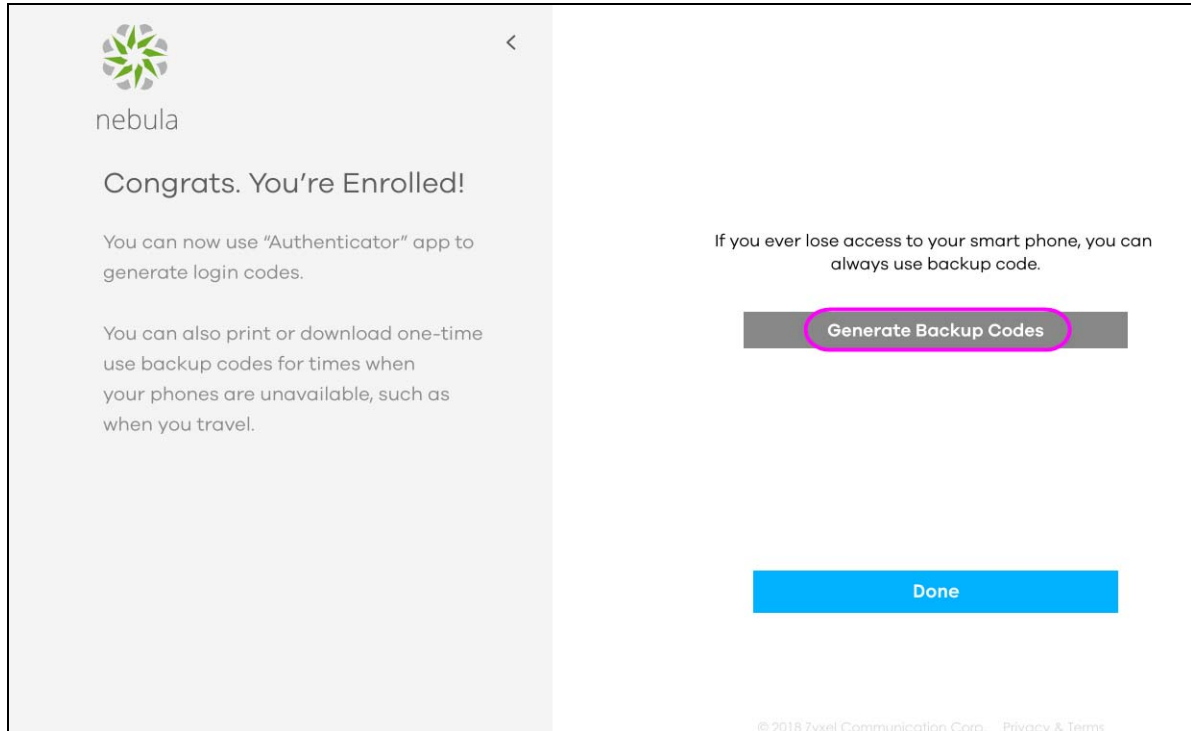


If you select **Google Authenticator**, install the app on your mobile phone and scan the QR code on the NCC web screen to get a six-digit one-time code. Then enter the code and click **Verify** to authenticate your identity.



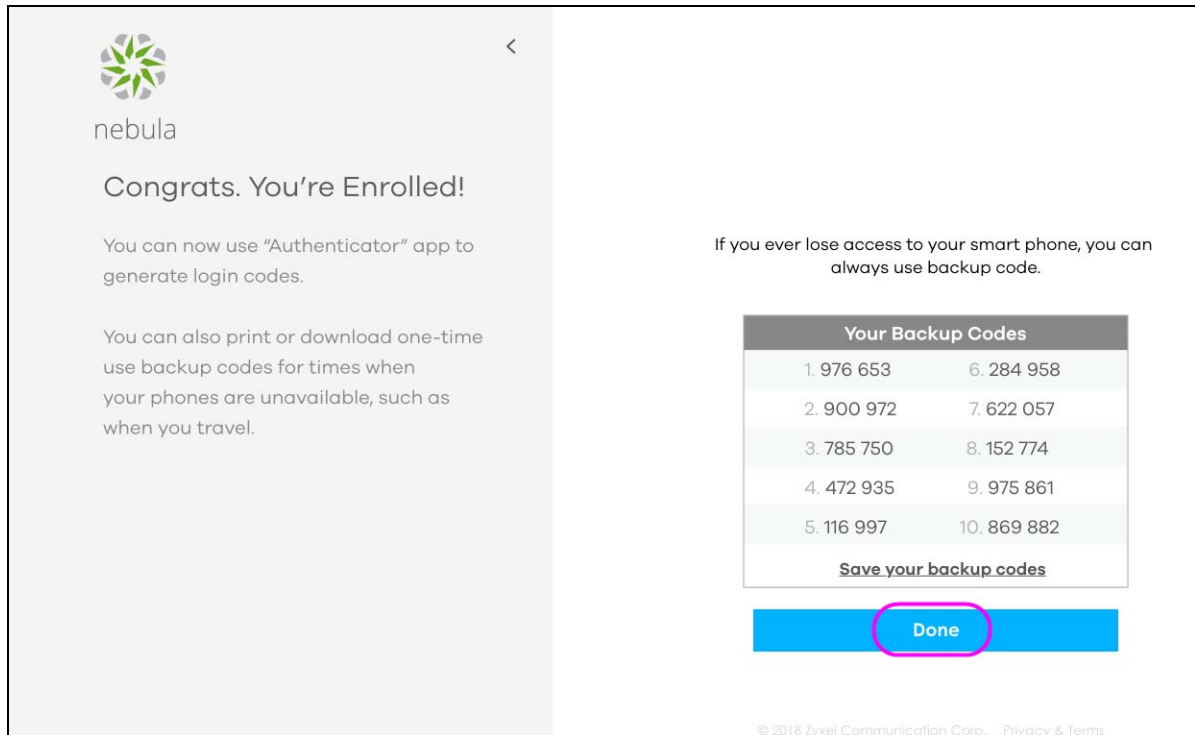
Click **Generate Backup Codes** to get 10 backup codes, which help regain access to your account in

case your phone is not available for 2FA the next time you need to log in again.

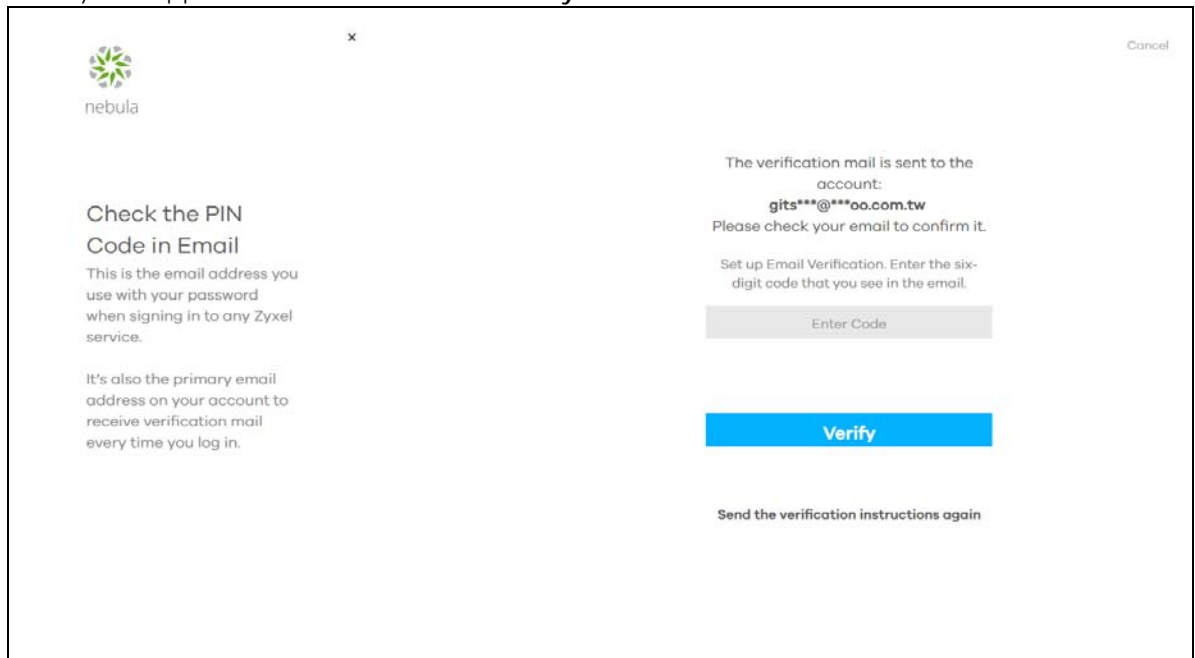


Write down or print out the backup codes for your account. You can enter the backup code on the NCC web page to authenticate your identity at the next login. Each code can only work once. Click **Done** to finish two-factor authentication.

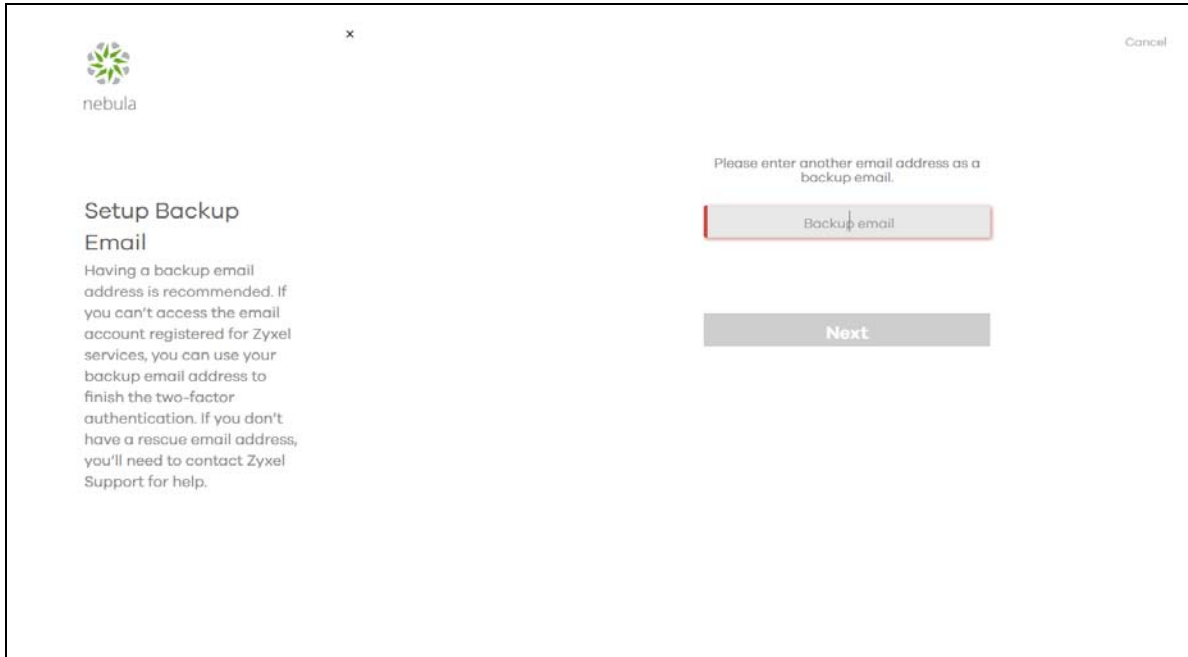
Note: If you generate a new set of backup codes, the old set will become inactive.



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**.



The screenshot shows a web interface for setting up a backup email. On the left, the Nebula logo is at the top. Below it, the heading "Setup Backup Email" is followed by a paragraph explaining the importance of a backup email for two-factor authentication. On the right, there is a text input field labeled "Backup email" with a red border, and a "Next" button below it. A "Cancel" link is in the top right corner.

nebulula

Setup Backup Email

Having a backup email address is recommended. If you can't access the email account registered for Zyxel services, you can use your backup email address to finish the two-factor authentication. If you don't have a rescue email address, you'll need to contact Zyxel Support for help.

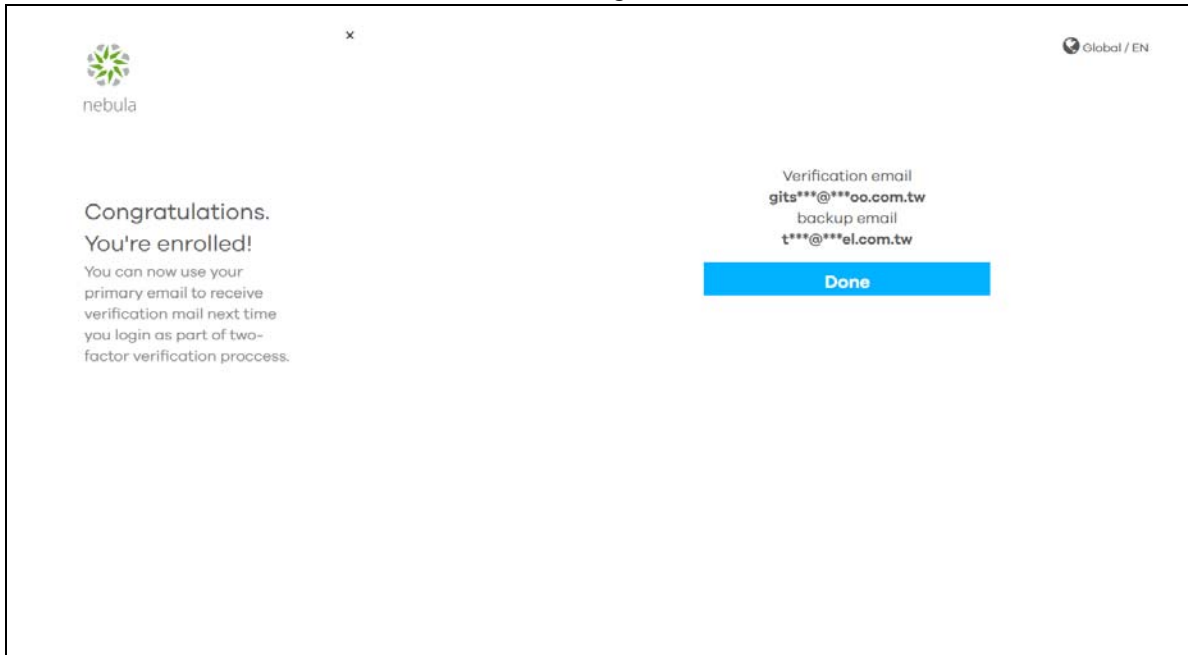
Please enter another email address as a backup email.

Backup email

Next

Cancel

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



The screenshot shows a confirmation screen. On the left, the Nebula logo is at the top. Below it, the heading "Congratulations. You're enrolled!" is followed by a paragraph stating that the user can now use their primary email for verification. On the right, the heading "Verification email" is followed by two email addresses: "gits***@***oo.com.tw" for the primary email and "t***@***el.com.tw" for the backup email. A blue "Done" button is at the bottom right. A "Global / EN" link is in the top right corner.

nebulula

Global / EN

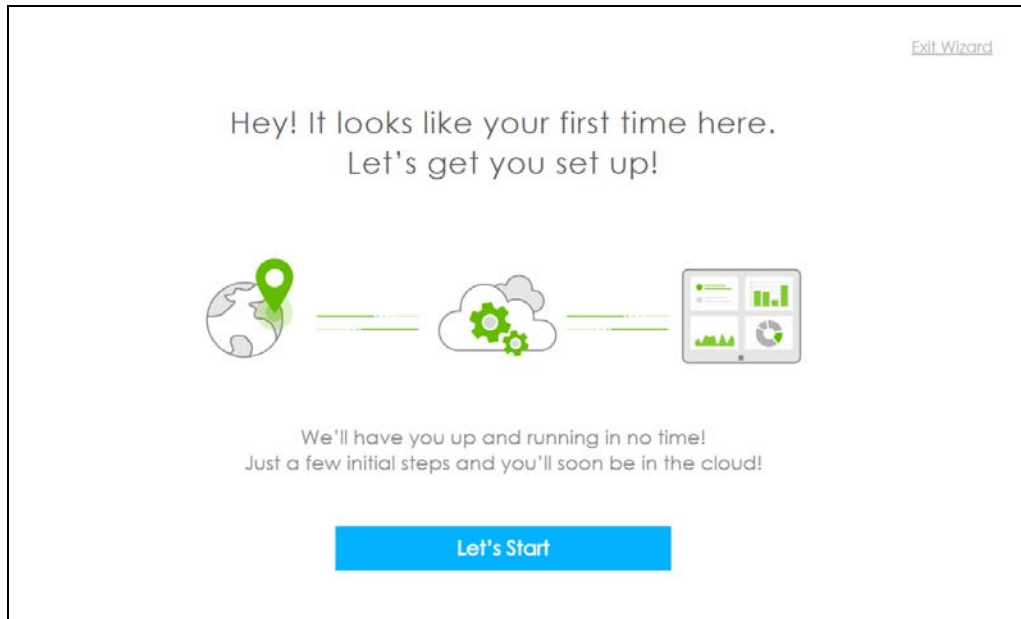
Congratulations.
You're enrolled!

You can now use your primary email to receive verification mail next time you login as part of two-factor verification process.

Verification email
gits***@***oo.com.tw
backup email
t***@***el.com.tw

Done

- 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 31](#) for how to use the wizard and [Chapter 4 on page 41](#) for detailed information about organization and sites.

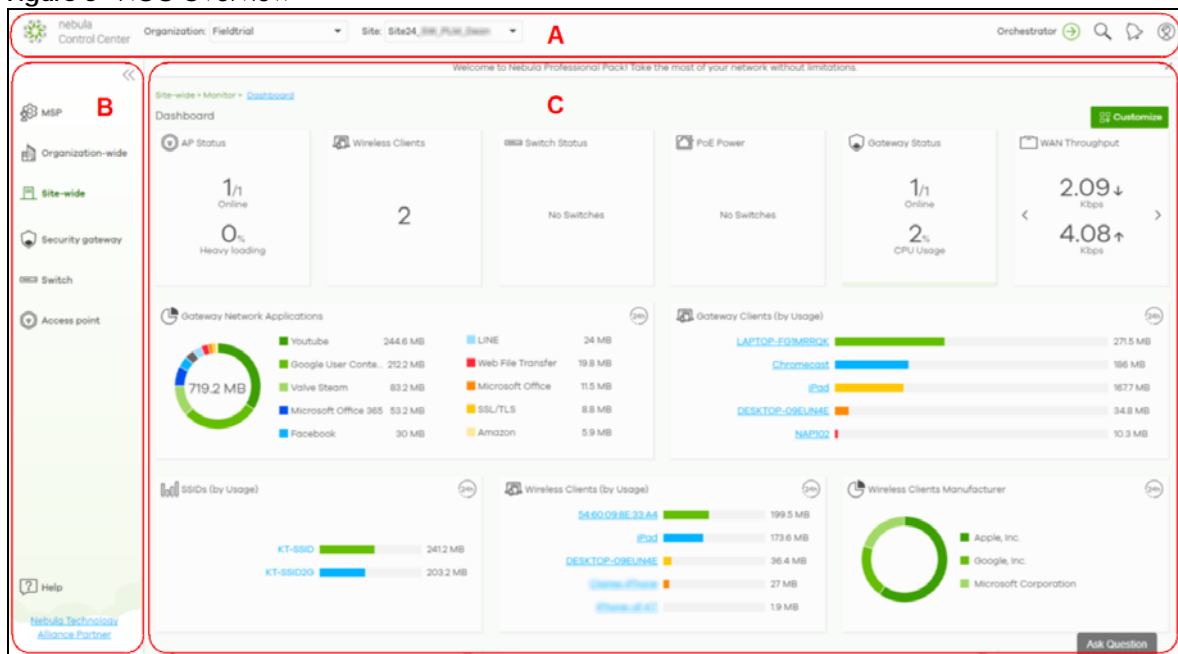


After a successful login, the Nebula user interface appears to manage and configure your Nebula devices.

1.3 NCC Portal Overview

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

Figure 3 NCC Overview



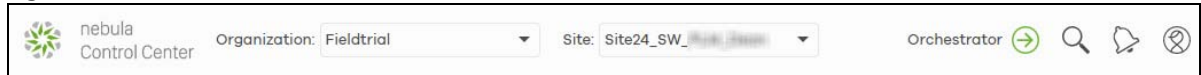
- A - Title Bar

- B - Navigation Panel
- C - Main Screen

1.3.1 Title Bar

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

Figure 4 NCC Title Bar

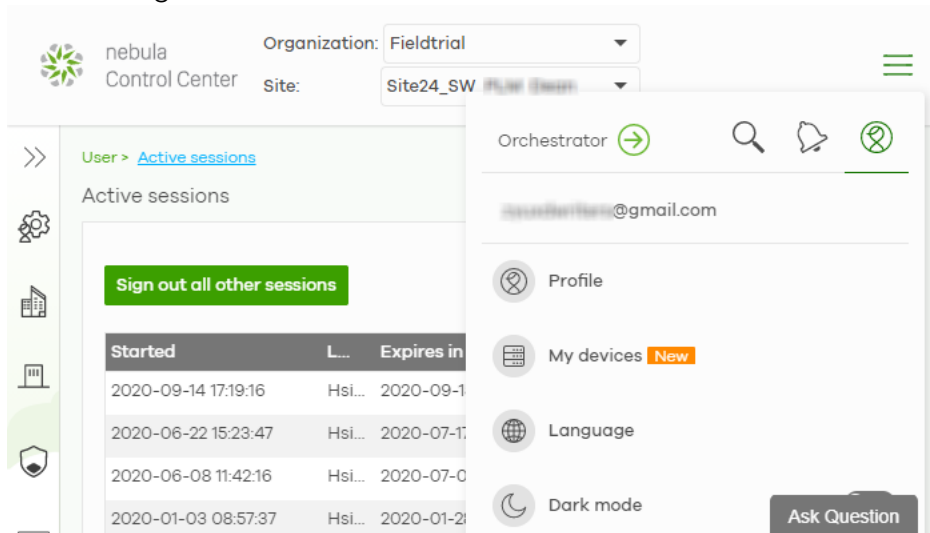


The icons provide the following functions.

Table 3 NCC Title Bar

LABEL	DESCRIPTION
Organization	This shows the name of the organization you are managing. Click to choose another organization, access the MSP portal or create a new organization.
Site	This shows the name of the site you are managing. Click to choose another site if you have multiple sites in the selected organization.
Orchestrator	Click this to go to the Nebula Orchestrator portal to manage your SD-WAN devices. See the SD-WAN user's guide.
Search	Enter a keyword as the filter criteria to filter the list of sites, devices and/or clients. At the time of writing, you can enter the name of the site, device or client. The field is case-sensitive.
Alert	Click this to view log messages.
Login Account	Click this to view your account information, login history and active sessions. You can also select a display language for the screens, or log out of the NCC portal.

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



1.3.1.1 Organization/Site

Select the organization and site that you want to manage.

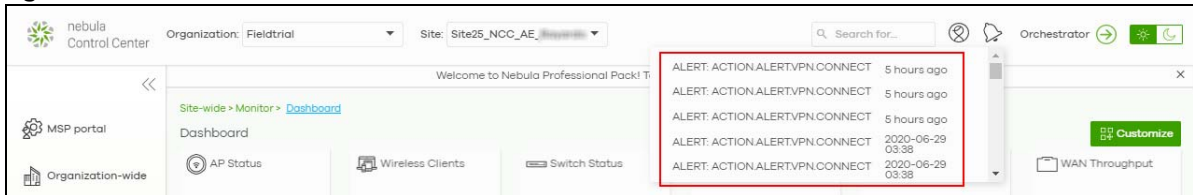
- If you have multiple organizations, select **MSP Portal** from the **Organization** drop-down list box to view your organization summary (see [Chapter 3 on page 37](#)).
- If you need to have more organizations, select **Create Organization** from the **Organization** drop-down list box to create a new one (see [Section 1.4 on page 28](#)).

Figure 5 NCC Title Bar: Organization/Site

Organization:	Fieldtrial	Site:	Hub
---------------	------------	-------	-----

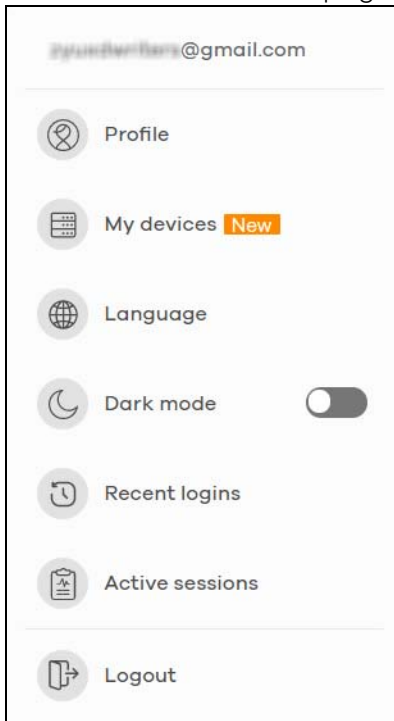
1.3.1.2 Alert

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

Figure 6 NCC Alert

1.3.1.3 Login Account

Click the user icon at the top right-hand corner of the screen to edit settings for your login account.

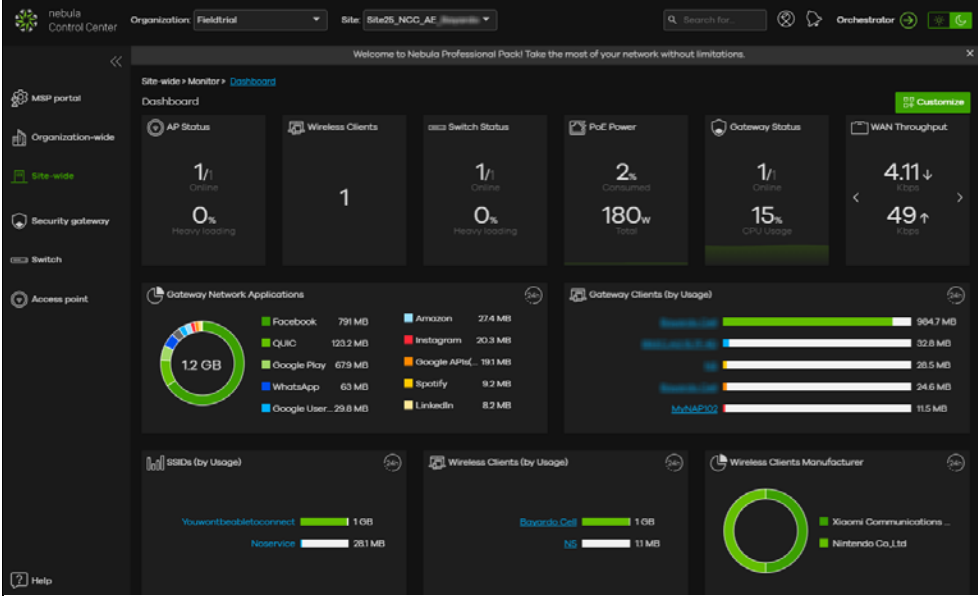


The following table describes this menu.

Table 4 Login Account Menu

LABEL	DESCRIPTION
Profile	This shows account information, such as name, address, and phone number.
My devices	This shows a list of all devices in NCC that have your login account as the owner. You can filter the list of devices by name, serial number, model, or organization.

Table 4 Login Account Menu

LABEL	DESCRIPTION
Language	Select the NCC display language. At the time of writing, the following languages are available: English, Chinese, Japanese, German, Russian, French.
Dark mode	Click this to apply a black background and white text to the white background and black text on the NCC screen. 
Recent logins	Shows the login history for this user account, including IP address, location, and time.
Active sessions	Shows all active web browser sessions for this login account. Click End Session to close a session and force the user to log into NCC again in that browser.
Logout	Log out of the NCC portal.

1.3.2 Navigation Panel

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

Table 5 NCC Menu Summary

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
MSP	Monitor	
	MSP Portal	Use this menu to view the status and general information about the organizations to which your account has at least read-only access.
	Configure	
	MSP branding	Use this menu to upload/replace/remove the dashboard logo. You can also set the support contact details.
	License Transfer	Use this menu to transfer licenses between organizations which you manage.

Table 5 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
Organization-wide	Monitor	
	Overview	Use this menu to view a list of sites belonging to the selected organization and detailed information about the devices connected to the sites.
	Change Log	Use this menu to view log messages about configuration changes in this organization.
	Configure	
	Settings	Use this menu to configure security settings or delete the organization.
	Create Site	Use this menu to create a new site.
	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.
	Administrators	Use this menu to view, remove, or create a new administrator account for this organization.
	Cloud Authentication	Use this menu to create or remove user accounts and grant user access to all sites in the selected organization via different authentication methods, such as MAC-based authentication, captive portal, or the IEEE 802.1x authentication method.
	Configuration Management	Use this menu to synchronize the configuration between sites or switch ports and back up or restore a configuration file.
	Configuration Templates	Use this menu to create or delete a configuration template or bind a site to the template.
	VPN Members	Use this menu to view and manage the VPN members in the organization.
	Firmware Management	Use this menu to upgrade firmware or schedule firmware upgrades for devices in the organization.
Site-wide	Monitor	
	Dashboard	Use this menu to view device connection status and traffic summary.
	Map & Floor Plans	Use this menu to locate devices on the world map or even on a floor plan.
	Topology	Use this menu to view the managed-device connections in your network.
	Vouchers	Use this menu to create, manage, and vouchers for wireless network authentication
	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.
	Configure	
	General Settings	Use this menu to change the general settings for the site, such as the site name, device login password and firmware upgrade schedule.
	Alert Settings	Use this menu to set which alerts are created and emailed or sent by the Zyxel Nebula Mobile app. You can also set the email address(es) to which an alert is sent.
	Add Devices	Use this menu to register a device and add it to the site.
	Firmware Management	Use this menu to upgrade firmware or schedule firmware upgrades for devices in the site.
	Cloud Authentication	Use this menu to add user accounts and grant user access to the selected site via different authentication methods, such as the MAC-based authentication, captive portal or the IEEE 802.1x authentication method.

Table 5 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
Security Gateway		Use these menus to monitor and configure the security gateway(s) managed by the NCC. The settings are applied when a Nebula gateway is registered and attached to the selected site.
	Monitor	
	Security Gateway	Use this menu to view the detailed information about a security gateway in the selected site.
	Clients	Use this menu to view the connection status and detailed information about a client in the selected site.
	Event Log	Use this menu to view all events on the gateway. An event is something that has happened to a managed device.
	VPN Connections	Use this menu to view status of the site-to-site VPN connections.
	NSS Analysis Report	Use this menu to view the statistics report for NSS (Nebula Security Service), such as content filtering, Intrusion Detection and Prevention (IDP), application patrol, and anti-virus.
	Summary Report	Use this menu to view network statistics specific to the gateway in the site.
	Configure	
	Interface Addressing	Use this menu to configure network mode, port grouping, interface address, static route and DDNS settings on the gateway.
	Policy Route	Use this menu to view and configure policy routes.
	Firewall	Use this menu to configure firewall rules for outbound traffic, application patrol, schedule profiles and port forwarding rules for inbound traffic.
	Security Service	Use this menu to enable content filtering and block access to specific web sites. You can also enable Anti-virus and Intrusion Detection and Prevention (IDP) on the security gateway.
	Site-to-Site VPN	Use this menu to configure VPN rules.
	Remote access VPN	Use this menu to enable and configure IPsec VPN or L2TP VPN settings.
	Captive Portal	Use this menu to configure captive portal settings for each gateway interface.
	Network Access Method	Use this menu to enable or disable web authentication on an interface.
	Traffic Shaping	Use this menu to configure the maximum bandwidth and load balancing.
	Gateway settings	Use this menu to configure the DNS server and address records and also set the external AD (Active Directory) server or RADIUS server that the security gateway can use in authenticating users. You can also specify walled garden web site links for all interfaces on the gateway.

Table 5 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
Switch		Use these menus to monitor and configure the switch(es) managed by the NCC. The settings are applied when a Nebula switch is registered and attached to the selected site.
	Monitor	
	Switches	Use this menu to view the list of switches added to the site.
	Clients	Use this menu to view detailed information about the clients which are connecting to the switches in the site.
	Event Log	Use this menu to view all events on the switch. An event is something that has happened to a managed device.
	IPTV Report	Use this menu to view available IPTV channels and client information.
	Surveillance	Use this screen to view information about Powered Devices (PDs) connected to ports on the switch.
	Summary Report	Use this menu to view network statistics specific to switches in the site.
	Configure	
	Switch Ports	Use this menu to view the switch port statistics and configure switch settings for the ports.
	ACL	Use this menu to configure the access control list in order to control access to the switches.
	Advanced IGMP	Use this menu to enable and configure IGMP snooping and create IGMP filtering profiles.
	RADIUS Policies	Use this menu to configure authentication servers and policies.
	PoE Schedules	Use this menu to set the schedule for switches in distributing power to powered devices.
	Switch Settings	Use this menu to configure global switch settings, such as (R)STP, QoS, port mirroring, voice VLAN and DHCP white list.

Table 5 NCC Menu Summary (continued)

LEVEL 1	LEVEL2/LEVEL3	FUNCTION
Access Point		Use these menus to monitor and configure the AP(s) managed by the NCC. The settings are applied when a Nebula AP is registered and attached to the selected site.
	Monitor	
	Access Points	Use this menu to view the list of APs added to the site.
	Clients	Use this menu to view WiFi clients which are connected to the APs in the site.
	Event Log	Use this menu to view all events on the AP. An event is something that has happened to a managed device.
	Wireless Health	Use this menu to view health of the wireless networks for the supported APs and connected clients.
	Summary Report	Use this menu to view network statistics specific to APs in the site.
	Configure	
	SSID Overview	Use this menu to enable and configure basic settings for SSID profiles.
	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.
	SSID Availability	Use this menu to configure SSID visibility settings and set whether the SSID is enabled or disabled on each day of the week.
	Radio Settings	Use this menu to configure global radio settings, such as maximum output power or channel width, and enable smart clients steering for all APs in the site.
	AP & Port Settings	Use this menu to configure load balancing settings and enable or disable a port on the managed AP and configure the port's VLAN settings.
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 only when the answer you are seeking cannot be found in the online documents and support forum. Use this menu to view or submit a new eITS ticket.
	Online Documents	Use this menu to view the documentation for the NCC and Nebula devices.
	Firewall Information	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.

1.4 Create Organization

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

Note: You have to contact Zyxel customer support if you need to change the device owner at myZyxel or remove an Organization from the NCC. But an administrator can remove sites without customer support. Please configure your device owners and organizations carefully. See also [Section 4.3.3 on page 48](#).

- 1 Click **Create Organization** from the **Organization** drop-down list box in the title bar. The Wizard starts. See [Chapter 2 on page 31](#) for detailed information about how to use the wizard to create an organization and site. Otherwise, click **Exit Wizard** to close the wizard and display the **Create Organization** screen.
- 2 Enter a name for your organization.
- 3 If you already have one or more than one organization under your account and you want to copy the organization settings of an existing one, select the organization name from the **Copy setting from** field before clicking the **Create organization** button.
- 4 Click the **Create organization** button to add a new organization.

Figure 7 Create Organization

The screenshot shows the 'Create organization' wizard in the Nebula Central Center interface. The title bar includes the 'Organization' dropdown menu, which is currently set to 'Create organization'. The main content area is titled 'Create organization' and contains a 'New Organization' section. This section includes a warning: 'Clone a new organization from one of your existing organization. Organization-wide settings for your new organization will be copied from the one you specify. This operation cannot be undone.' Below this, there are three input fields: 'Organization name' with the value 'Test', 'Country' with the value 'Taiwan', and 'Copy setting from' with the value '(None)'. At the bottom right of the form is a green button labeled 'Create organization'.

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

1.5 Choose Organization

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

Figure 8 Choose Organization

Accounts for kao@zyxel.com.tw

MSP Portal

Choose organization

Create organization

Name	Type
Org1	Nebula
Org2	Nebula

CHAPTER 2

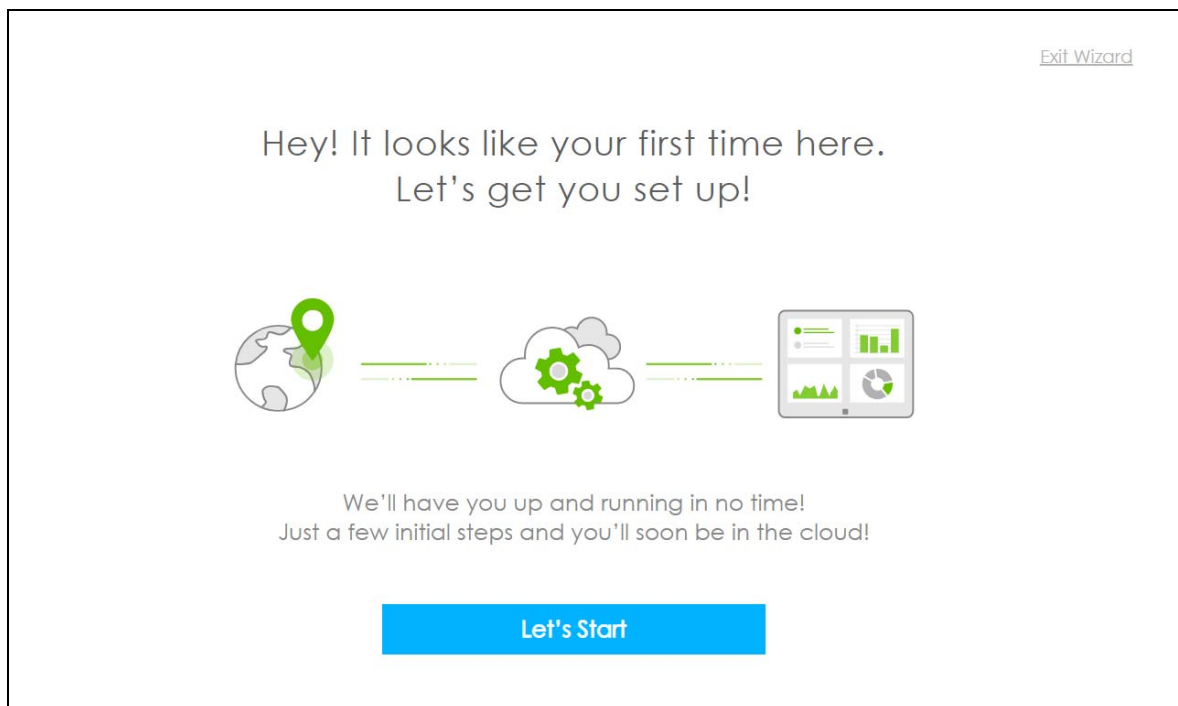
Setup Wizard

2.1 Access 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 Use the Wizard

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



2.2.1 Step 1 Create an Organization and Site

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

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.

First step is to create your Organization and Site

Organization

Site

Country

Timezone

[Exit Wizard](#)

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
MAC address

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		

[Exit Wizard](#)

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.

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

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

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.

03

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

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

You might just click Next to skip this step.

Let's get your WiFi set up

WiFi Name (SSID)

Password (Pre-Shared Key)

VLAN

Set up VLAN interface **Gateway**

Back **Next**

[Skip WiFi settings](#)

[Exit Wizard](#)

2.2.4 Step 4 Set up a Guest WiFi Network

Configure WiFi and VLAN settings for guest users who can wirelessly access the Internet or networks through Nebula devices. If you want to enable web authentication, select **Clicking "Agree" to access the network** to block network traffic until a client agrees to the policy of user agreement. Otherwise, select **Using their Facebook account to join the network** to block network traffic until the client logs in using his/her existing Facebook account.

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

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

If you enter a different VLAN ID other than the default one ("1") in the **VLAN** field, click the **Set up VLAN interface** link to create a gateway interface with the specified VLAN ID. You can set the gateway

interface as a guest interface, configure the IP address and subnet mask and enable the DHCP server function for this interface.

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

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.

[Exit Wizard](#)

04

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

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

You might just click Next to skip this step.

Need to set up a Guest WiFi?

WiFi Name (SSID)

Password (Pre-Shared Key)

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

☒ No captive web portal


☐ Clicking "Agree" to access the network

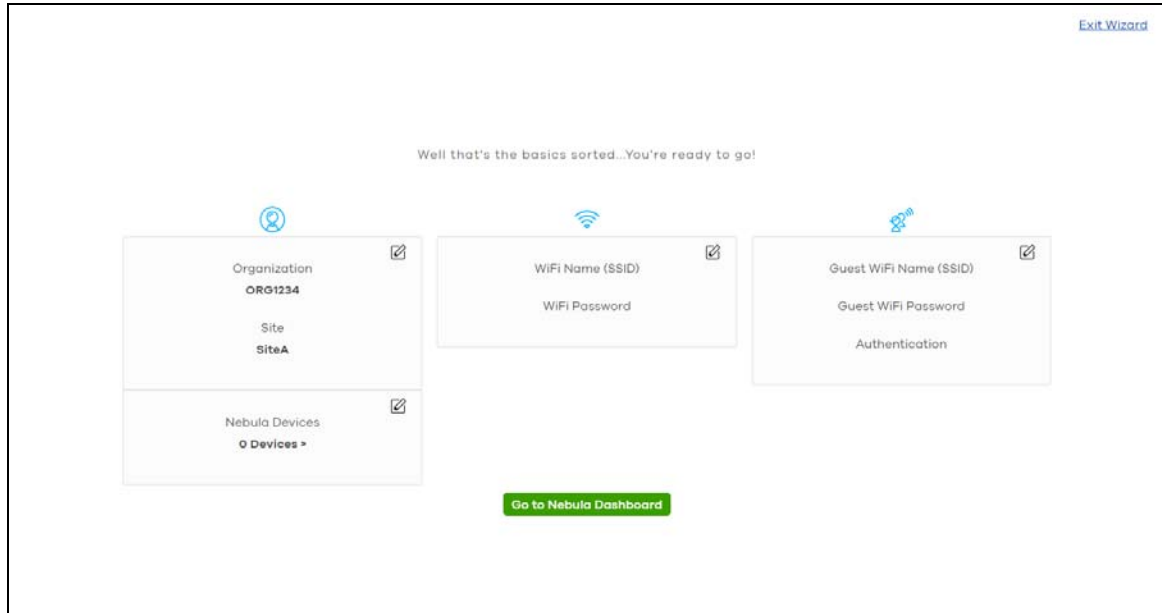
☐ Using their Facebook account to join the network

VLAN

Set up VLAN interface **Gateway**

2.2.5 Summary

A summary of the wizard configuration will display. You can click a section's 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.



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

[Exit Wizard](#)

Organization
ORG1234

Site
SiteA

Nebula Devices
0 Devices >

WiFi Name (SSID)

WiFi Password

Guest WiFi Name (SSID)

Guest WiFi Password

Authentication

[Go to Nebula Dashboard](#)

2.2.6 Activate NCC Pro Pack and Security Services Trial Period

After creating an organization, you can activate a one-month trial period of Nebula Pro Pack and Nebula Security Services for the organization. If you choose to activate the trial period, NCC will send you an email reminding you purchase the full license when the trial is close to expiring.



Notification ✕

Welcome to Nebula, we provide a free trial period for enjoying full Nebula Pro Pack & Security Service functions. You could continue with free trial or skip trial as you wish.

☒ I want to continue with my one month trial of Nebula.

☐ I'll start with Nebula without trial period.

[OK](#)

PART II

Technical Reference

CHAPTER 3

MSP

3.1 Overview

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

3.2 MSP Portal

This screen lists every organization to which your account has at least read-only access.

To access this screen, select **MSP portal** from the **Organization** drop-down list box in the title bar, or click **MSP > Monitor > MSP Portal** in the navigation panel. Click the entry of the organization that you want to manage to go to its **Site-wide > Monitor > Dashboard** screen.

Figure 9 MSP > Monitor > MSP Portal Screen



Status	Organization	Type	NCC license status	NCC license expiration (UTC)	Sites	Devices	NAP	NSW	NSG
●	Fieldtrial	Nebula Professional Pack	OK	2020-11-16	44	● 37 ● 0 ● 0 ● 36 26 11 36			
●	America Office	Nebula Professional Pack	OK	2022-12-26	3	● 1 ● 0 ● 0 ● 1 0 1 1			
○	Temp	Nebula	expired	2020-02-08	2	● 0 ● 0 ● 0 ● 0 0 0 0			
●	GS1350_test	Nebula Professional Pack	OK	2022-02-10	1	● 0 ● 0 ● 1 ● 1 1 1 0			

The following table describes the labels in this screen.

Table 6 MSP > Monitor > MSP Portal

LABEL	DESCRIPTION
Search	Specify your desired filter criteria to filter the list of organizations.
matches in	This shows the number of organizations that match your filter criteria after you perform a search.
organizations	This shows the number of organizations that you can manage.
Status	<div>This shows the status of devices in the organization.</div> <ul style="list-style-type: none">Green: All devices are online and have no alerts.Amber: Some devices have alerts.Red: Some devices are offline.Gray: All devices have been offline for 7 days or more.White: No devices.
Organization	This shows the descriptive name of the organization.
Type	This shows your NCC version type.

Table 6 MSP > Monitor > MSP Portal

LABEL	DESCRIPTION
NCC License Status	This shows whether the license is valid (ok), the license has expired and the organization downgraded from Nebula Professional Pack to Nebula Basic (expired), or this is a free Nebula organization and an NCC license is not required (N/A).
NCC License expiration (UTC)	This shows the date when the license will expire, or N/A when there is no Nebula device in the organization or if this is a free Nebula organization and an NCC license is not required.
Sites	This shows the number of sites belonging to this organization.
Devices	This shows the number of Nebula devices in this organization which are online (green), have recently had alerts (amber), recently went offline (red), or have been off-line for more than six days (gray).
NAP	This shows the number of Nebula APs connected to the sites in this organization.
NSW	This shows the number of Nebula switches connected to the sites in this organization.
NSG	This shows the number of Nebula security gateways connected to the sites in this organization.

3.3 License Transfer

You can transfer license credit between organizations that belong to the same organization creator (see [Devices in an Organization on page 49](#)). To access this screen, click **MSP > Configure > License Transfer**.

Figure 10 MSP > Configure > License Transfer

MSP > Configure > [License transfer](#)

License transfer

Transfer license points between organization

From organization:

License type:

To organization:

[Click to know limitation for license transfer](#)

The following table describes the labels in this screen.

Table 7 NCC MSP Portal > License Transfer

LABEL	DESCRIPTION
From organization	Select the organization from which the license credit (device points) will be transferred.
Nebula Points	This shows the current number of the selected organization's device points for the NCC service.
Nebula Security Points	This shows the current number of the selected organization's device points for the NSS-SP (Nebula Security Service – Security Pack) service.
License Type	Select the type of the license and specify the number of points to transfer.

Table 7 NCC MSP Portal > License Transfer (continued)

LABEL	DESCRIPTION
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 device points will be transferred.
Reset	Click this button to return the screen to its last-saved settings.
OK	Click this button to save your changes.

3.4 MSP Branding

The **Dashboard logo** section of this screen allows organization owners to replace the Nebula Control Center logo with a new MSP logo. The **Support contact** section allows addition of a customized message or MSP contact information in the **Help > Support** request page. To access this screen, click **MSP > Configure > MSP branding**.

Figure 11 MSP > Configure > MSP branding

MSP > Configure > [MSP branding](#)

MSP branding

Dashboard logo ⓘ

Your account is not owner of any PRO organization.

Upload new logo:

Upload a logo

No logo

Apply to:

☐ All current and new PRO organizations

☒ None

☐ Custom:

Support contact ⓘ

Support request page

☒ Show default Zyxel support cases ⓘ

☐ Customized MSP support contact information

Apply to:

☐ All current and new PRO organizations

☒ None

☐ Custom:

The following table describes the labels in this screen.

Table 8 NCC MSP Portal > MSP Branding

LABEL	DESCRIPTION
Dashboard logo	
Upload new logo	Click this to browse for the location of the image file to be used as your dashboard logo. <ul style="list-style-type: none"> Allowed image file formats: JPG/JPEG, PNG, GIF. Maximum image file size: 200KB. NCC converts the image file to a 160 x 44 pixel logo after uploading.
Replace this logo	Click this to browse for the location of the image file to replace your current dashboard logo.
Remove this logo	Click this to remove your current dashboard logo.
Apply to	Select All current and new PRO organizations to apply the logo to all Nebula Professional Pack organization dashboards. Select Custom to choose which Nebula Professional Pack organization to apply the logo. Select None if you only wish to upload the image file but will not apply it yet.
Support contact	
Support request page	
Show default Zyxel support cases	Select ON to display the standard Zyxel support contact information in the Help > Support request screen. Organization owners can choose to hide the default Help > Support screen section to only show their information to clients. But the organization owner and administrators with full privileges will still see the hidden default screen section.
Customized MSP support contact information	Create your own support contact information. Up to 1000 characters are allowed for this field including special characters inside the square quotes [~!@#\$%^&*()_+{} :"<>?-=[]\;',./].
Apply to	Select All current and new PRO organizations to apply the support contact information to all Nebula Professional Pack organization Help > Support request screens. Select Custom to choose which Nebula Professional Pack organization to apply the support contact information. Select None if you only wish to save the settings but will not apply it yet.

CHAPTER 4

Organization-wide

4.1 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.

4.2 Monitor

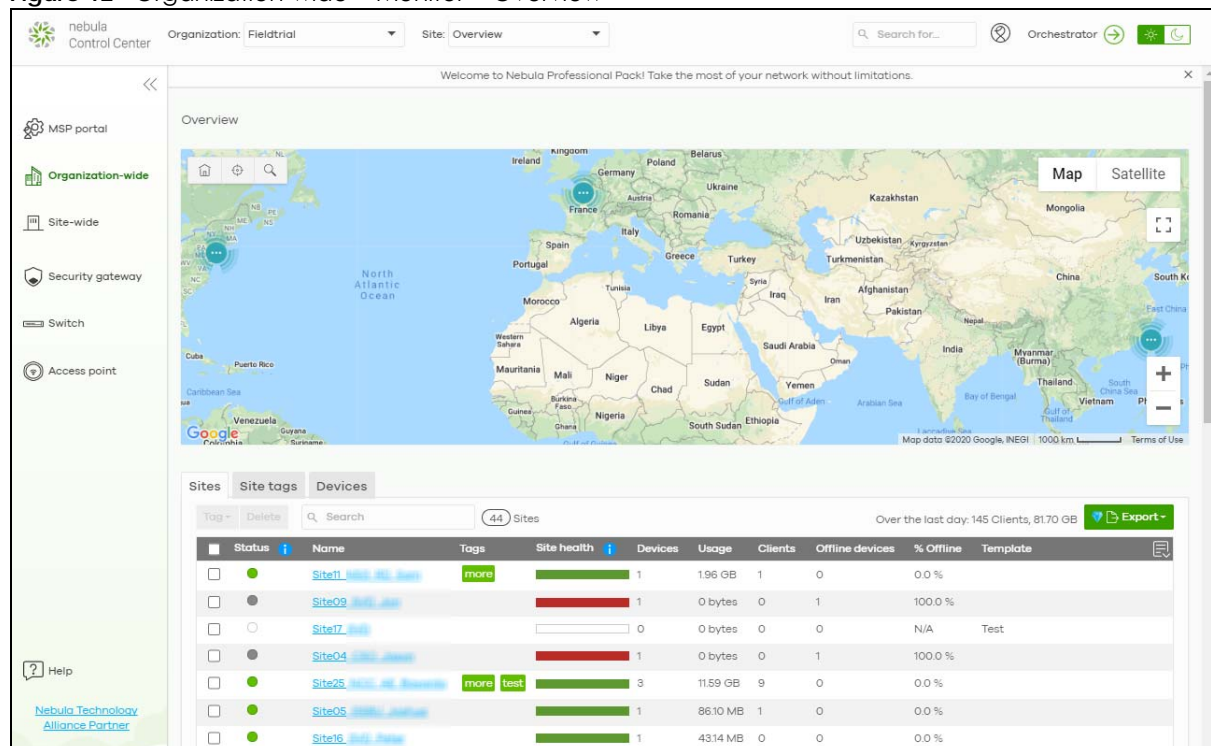
Use the **Monitor** menus to check the site and device information and change logs for the selected organization.

4.2.1 Organization Overview

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

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

Figure 12 Organization-wide > Monitor > Overview



4.2.1.1 Sites

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

Figure 13 Organization-wide > Monitor > Overview: Sites


Status	Name	Usage	Client	Tag	Site health	Device	Offline device	% Offline
Green	Site11_NSG_RD_Sam	37.57 MB	0		Green	1	0	0.0 %
Red	Site09_SVD_Jon	0 bytes	0		Red	1	1	100.0 %
White	Site17_SVD	0 bytes	0		White	0	0	N/A
Red	Site04_CSO_Jason	0 bytes	0		Red	1	1	100.0 %
Green	Site25_NCC_AE_Bayardo	12.09 GB	9	more test	Green	4	0	0.0 %
Green	Site05_GSBV_Joshua	204.27 MB	1		Green	1	0	0.0 %
Red	Site16_SVD_Peter	21.56 MB	0		Red	1	1	100.0 %
Red	Site01_GSBV_Justin	0 bytes	0		Red	1	1	100.0 %
Red	Site14_GSBV_AE_Frank	0 bytes	0		Red	1	1	100.0 %
Red	Site30_NCC_SVD_Max	11.36 GB	30		Red	6	1	16.7 %

The following table describes the labels in this screen.

Table 9 Organization-wide > 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 the status of devices in the site. <ul style="list-style-type: none"> Green: All devices are online and have no alerts. Amber: Some devices have alerts. Red: Some devices are offline. Gray: All devices have been offline for 7 days or more. White: No devices.
Name	This shows the descriptive name of the site.
Usage	This shows the amount of data consumed by the site.
Client	This shows the number of clients connected to Nebula devices in the site.
Tag	This shows the user-specified tag that is added to the site.
Site Health	This shows the percentage of uptime in a given time interval to indicate the site's network availability. <ul style="list-style-type: none"> Green: 95-100% Network uptime Dark green: 75-95% Network uptime Brown: 50-75% Network uptime Red: <50% Network uptime Grey: No uptime data

Table 9 Organization-wide > Monitor > Overview: Sites (continued)

LABEL	DESCRIPTION
Device	This shows the total number of Nebula devices deployed in the site.
Offline device	This shows the number of Nebula devices which are added to the site but not accessible by the NCC now.
% Offline	This shows what percentage of the connected clients are currently off-line.
	Click this icon to display a greater or lesser number of configuration fields.

4.2.1.2 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 14 Organization-wide > Monitor > Overview: Site tags



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

The following table describes the labels in this screen.

Table 10 Organization-wide > Monitor > Overview: Site tags

LABEL	DESCRIPTION
Search	Enter a key word as the filter criteria to filter the list of tags.
Site tags	This shows the number of site tags created and added to the sites in this organization.
Over the last day	This shows the number of clients associated with the sites in this organization and the total amount of data transmitted or received by the clients in the past day.
Export	Click this button to save the tag list as a CSV or XML file to your computer.
Status	This shows the status of devices in sites with the specified tag. <ul style="list-style-type: none"> Green: All devices are online and have no alerts. Amber: Some devices have alerts. Red: Some devices are offline. Gray: All devices have been offline for 7 days or more. White: No devices.
Tag	This shows the name of the specified tag.
Site	This shows the total number of sites with the specified tag.
Offline device	This shows the number of offline Nebula devices in all sites with the specified tag.
Client	This shows the number of clients in sites with the specified tag.
Usage	This shows the total amount of data consumed in all sites with the specified tag.
Device	This shows the total number of Nebula devices deployed all sites with the specified tag.
Offline site	This shows the number of offline sites with the specified tag.
% Offline	This shows what percentage of all sites with the specified tag are currently offline.
	Click this icon to display a greater or lesser number of configuration fields.

4.2.1.3 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 15 Organization-wide > Monitor > Overview: Devices


Client	MAC address	Model	Name	Site	Status	Tag	Usage
0	B8EC:A3:B4:CD:9F	NSG50	B8.EC:A3.B4:CD:9F	Site11 NSG_RD_Sam	Green		0 bytes
0	B8EC:A3:B4:CC:67	NSG50	B8.EC:A3.B4:CC:67	Site09_SVD_Jon	Red		0 bytes
0	B8EC:A3:B4:CF:B5	NSG50	B8.EC:A3.B4:CF:B5	Site04_CSO_Jason	Red		0 bytes
9	5C:E2:8C:5C:0F:FE	NSG50	Home GW	Site25_NCC_AE_Bayardo	Green		0 bytes
0	B8EC:A3:0F:C8:34	NSW200-28P	Office NSW200	Site25_NCC_AE_Bayardo	Green		0 bytes
3	58:8B:F3:91:45:75	NAP102	OfficeNAP102-MESH	Site25_NCC_AE_Bayardo	Green		0 bytes
5	4D:31:97:64:D7:13	NAP102	HomeNAP102	Site25_NCC_AE_Bayardo	Green	Home	2.61 GB
9	B8EC:A3:15:7F:4D	NSW100-10P	Home NSW100	Site25_NCC_AE_Bayardo	Green		2.69 GB
1	B8EC:A3:B4:CD:87	NSG50	B8.EC:A3.B4:CD:87	Site05_GSB_U_Joshua	Green		0 bytes
0	B8EC:A3:B4:CC:43	NSG50	B8.EC:A3.B4:CC:43	Site16_SVD_Peter	Red		0 bytes

The following table describes the labels in this screen.

Table 11 Organization-wide > Monitor > Overview: Devices

LABEL	DESCRIPTION
Search	Enter a key word as the filter criteria to filter the list of connected devices.
Devices	This shows the number of Nebula devices assigned to the sites in this organization.
Over the last day	This shows the number of clients associated with the sites in this organization and the total amount of data transmitted or received by the clients in the past day.
Export	Click this button to save the device list as a CSV or XML file to your computer.
Status	This shows the status of the device. <ul style="list-style-type: none"> Green: The device is online. Amber: The device recently had alerts. Red: The device was recently offline. Gray: The device has been offline line for more than 6 days.
Model	This shows the model number of the device.
Name	This shows the descriptive name of the device.
Site	This shows the name of the site to which the device is connected.
MAC address	This shows the MAC address of the device.
Tag	This shows the user-specified tag for the device.
Client	This shows the number of the clients which are currently connected to the device.
Usage	This shows the amount of data consumed by the device.
Serial number	This shows the serial number of the device.

Table 11 Organization-wide > Monitor > Overview: Devices (continued)

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

4.2.2 Change Log

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

When the log is full, it deletes older entries one by one to make room for new ones.

Figure 16 Organization-wide > Monitor > Change log

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

Change log

Search... Range From: 2019-10-18 05:57 To: 2019-10-25 05:57 UTC+0 Search

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

< Newer Older > 211 change logs within the time filtered. Changes date back to 2017-09-14 02:53 (UTC) Export

Time (UTC)	Site time	Admin	Site	SSID	Page	Label	Old ...	N...	
2019-10-25 05:25:28	2019-10-25 13:25:28 (UTC +8.0)	NCC_AE_Bayardo	Site25_N...		Capti...	ADD: ...		Site25...	
2019-10-25 05:25:28	2019-10-25 13:25:28 (UTC +8.0)	NCC_AE_Bayardo	Site25_N...		Capti...	ADD: ...		5a7d51...	
2019-10-25 05:25:28	2019-10-25 13:25:28 (UTC +8.0)	NCC_AE_Bayardo	Site25_N...		Authe...	CHAN...	SNS...	CLICK...	
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_SVD_Max	Site30_...		Firew...	CHAN...	60.24...	60.248...	
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_SVD_Max	Site30_...		Firew...	REMO...	HUB...		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_SVD_Max	Site30_...		Firew...	REMO...	WAN1		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_SVD_Max	Site30_...		Firew...	REMO...	false		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_SVD_Max	Site30_...		Firew...	REMO...	false		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_SVD_Max	Site30_...		Firew...	REMO...	86400		
2019-10-25 02:51:40	2019-10-25 10:51:40 (UTC +8.0)	NCC_SVD_Max	Site30_...		Firew...	REMO...	NONE		

Page 1 of 22 Results per page: 10

The following table describes the labels in this screen.

Table 12 Organization-wide > Monitor > Change log



LABEL	DESCRIPTION
Search	Click to enter one or more key words as the search criteria to filter the list of logs.
Range/Before	Select Range to set a time range or select Before to choose a specific date/time and the number of hours/minutes to display only the log messages generated within a certain period of time (before the specified date/time). The maximum allowable time range is 30 days.
Search	Click this to update the list of logs based on the search criteria.
Reset filters 	Click this to return the search criteria to the previously saved time setting.

Table 12 Organization-wide > Monitor > Change log (continued)

LABEL	DESCRIPTION
Newer/Older	Click to view a list of log messages with the most recent or oldest message displayed first.
	This shows the total number of the log messages that match the search criteria. It also shows the date and time the very first log was created.
Export	Click this button to save the log list as a CSV or XML file to your computer.
Time (UTC)	This shows the date and time in UTC+00:00 (or UTC+0) when the log was recorded. UTC is a standard time for use around the world (formerly known as Greenwich Mean Time or GMT). UTC is an international abbreviation that is neither French nor English. It means both "Temps Universel Coordonné" and "Coordinated Universal Time".
Site Time	This shows the date and time of the site, to which the change was applied, when the log was recorded.
Admin	This shows the name of the administrator who made the changes.
Site	This shows the name of the site to which the change was applied.
SSID	This shows the SSID name to which the change was applied.
Page	This shows the name of the NCC menu in which the change was made.
Label	This shows the reason for the log.
Old value	This shows the old setting that was discarded and overwritten with the new attribute value.
New value	This shows the new setting that was adopted.
	Click this icon to display a greater or lesser number of configuration fields.

4.3 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.

4.3.1 Create Site

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

- 1 Enter a descriptive name of up to 64 printable characters for the site.
- 2 If you already have one or more than one sites in the organization and you want to copy the site settings of an existing one, select the **Clone from** check box and then the site name.

If you have created a configuration template (see [Section 4.3.9 on page 71](#)), you can select to bind the new site to the specified template.
- 3 Choose the time zone of the site's location.
- 4 Search and select the name of the registered device that is to be added to this site. If there is no registered Nebula device in the organization, you can click **Register** to claim one.
- 5 Click **Create site** to add the new site to your organization.

Figure 17 Organization-wide > Configure > Create Site

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

Create site

Site name:

Configuration:

☒ Default configuration

☐ Clone from

☐ Bind to template

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

Local time zone:

Devices:

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

1 selected in 2 devices. + Register

	Device name	Serial Number	MAC address	Model
<input checked="" type="checkbox"/>		875A-875A-875A	875A-875A-875A	NSG50
<input type="checkbox"/>		875A-875A-875A	875A-875A-875A	NSG50

Create site

4.3.2 Inventory

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

Figure 18 Organization-wide > Configure > Inventory

Organization-wide > Configure > [Inventory](#)

Inventory

View used and unused devices in your organization. You can [register](#) new devices to add into the list below. After selecting devices below, you can add them to a new or existing site.

Add to ... Unregister Unused Used Both 2 devices. + Register Export

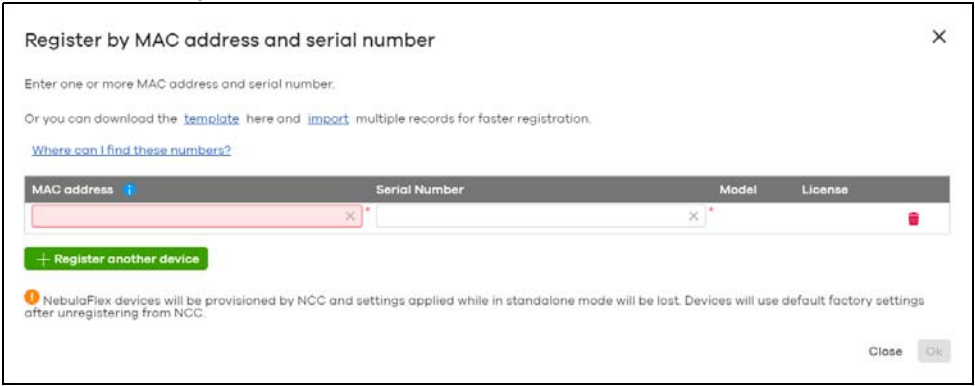
	MAC address	Serial Number	Site	Model	Registered on ...	Country
<input type="checkbox"/>	875A-875A-875A	875A-875A-875A	ThirdSite	NSG300	2020-04-22 03:16...	
<input type="checkbox"/>	875A-875A-875A	875A-875A-875A	testing	NSW200-28P	2020-01-15 03:11:57	Taiwan

The following table describes the labels in this screen.

Table 13 Organization-wide > 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.

Table 13 Organization-wide > Configure > Inventory (continued)

LABEL	DESCRIPTION
Search	Enter a key word as the filter criteria to filter the list of connected devices. Open the search box drop-down list to filter the search results by site, model, and country.
Devices	This shows the number of the devices in the list.
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 template in the pop-up window to download the template (an example Excel file), add devices information in the Excel file, and then click import to register multiple devices quickly by importing the Excel file.</p> 
Export	Click this button to save the device list as a CSV or XML file to your computer.
MAC address	This shows the MAC address of the device. Click on the MAC address to view the device details page.
Serial number	This shows the serial number of the device.
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.

4.3.3 License Management

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

Note: Nebula licenses are activated for a whole organization, rather than individual devices. To activate a license, you must purchase device points for every device in the organization.

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

4.3.3.1 Device Points

You must purchase device points in order to activate a license for an organization. There are two types of device points:

- Nebula points: Required to activate a Nebula Professional Pack license. For details, see [Section 1.1.1 on page 9](#).

- Nebula security points: Required to activate a Nebula Security Services (NSS) license.

The number of device points required varies depending on the number of Nebula devices in the organization, the types of devices, device models, and how long you want the license to be valid.

For information on how many points are needed for a specific set of devices, go to **Help > License Calculator**.

4.3.3.2 Nebula Points Example

At the time of writing, the number of Nebula points required for a 1-year Nebula Professional Pack license are: Access point = 30, Switch = 35, Gateway = 50.

Example: If you deploy 10 access points, 3 switches and 1 gateway in an organization, you need 420 Nebula points to activate a 1-year Nebula Professional Pack license.

$$(30 \times 10) + (35 \times 2) + (50 \times 1) = 420$$

4.3.3.3 Nebula Security Points Example

At the time of writing, the number of Nebula security points required for a 1-year NSS license are: NSG50 = 70, NSG100 = 200, NSG200 = 350, NSG300 = 500.

Example: If you deploy 10 NSG50s, 2 NSG100s, and 1 NSG200 in an organization, you need 1,400 Nebula Security Points to activate a 1-year Nebula Security Services license.

$$(70 \times 10) + (200 \times 2) + (350 \times 1) = 455$$

4.3.3.4 Bundled Licenses

Some Nebula-managed devices include a license with the purchase. When you register a device to an organization, Nebula automatically activates all bundled licenses and converts them into device points. For example, if you buy a gateway that includes a 1-year Nebula Professional Pack license, then this device receives 50 Nebula Points when you register the device to Nebula.

4.3.3.5 Devices in an Organization

- When a Nebula device is registered and assigned to an organization at NCC for the first time, the organization can use the device points that comes with the device, and the organization creator becomes the device owner.
- All devices in an organization share the same pool of device points. For example: If you register an NSG100 that is bundled with a 1-year Nebula Security Services license (200 Nebula security points) to an organization that contains one other NSG100, then each NSG100 receives 100 security points. This gives 6 months of Nebula Security Services to each NSG100.
- If a device is removed from an organization, you can only register it again to the original or other organizations that belong to the same organization creator. The new organization cannot use the device's bundled points.

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 4.3.5 on page 55](#) for more information about administrator accounts.

Trial License

Zyxel offers a 31-day trial license to the first 10 organizations created by an account within a 3-month period. Any number of devices can be registered in an organization. The 3 months will start counting once the user creates the first organization. After 3 months, the account can use a new 31-day trial license for another set of 10 organizations within a new 3 month period.

A trial license cannot be transferred to another organization, as no device points are used.

Device bundled license will not be activated during the trial license. When the trial license expires, the bundled license (if any) will be automatically activated and the organization will remain in the Nebula Professional Pack service with the bundled device points.

Single license keys can be activated during the trial license. NCC will only start to consume the points from activated license keys after the trial license has expired.

When the trial license and single license expires, the organization changes to a Nebula Basic (free) service.

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: An organization with lifetime licenses will not consume any device points. You should transfer any remaining device points to another organization.

Top-up Limited Lifetime License (Top-up LLL)

For Zyxel devices that are offered at least a 1-year NCC service license, such as the NAP series or APs and switches that support NebulaFlex or NebulaFlex Pro, you can select to register a top-up license key to upgrade to the lifetime license for NCC services. The APs or switches that support NebulaFlex can operate in either standalone or Nebula cloud management mode. The APs that support NebulaFlex Pro can operate in standalone, AC (AP Controller) management, or Nebula cloud management mode.

Note: If the device with a bundled NCC service license is re-registered to another organization, the device then cannot have a top-up lifetime license. A device's bundled license credit can only be used by the first organization to which the device is registered.

Figure 19 Organization-wide > Configure > License management

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

License management

Nebula Control Center License

NCC

Status: OK

Expiration date: 2020-07-23

Remaining: 31 days / 276 points

Devices	# Device
Access point	29
Switch	10
Gateway	41
Nebula Points for 1 year of NCC service:	3270

Nebula Security Service License

NSS-SP

Status: OK

Expiration date: 2021-05-29

Remaining: 341 days / 3176 points

Devices	# SP / # Device
NSG50	38 / 38
NSG100	2 / 2
NSG200	1 / 1
Nebula Security Points for 1 year of NSS-SP service:	3410

[Activate](#)
[Registered](#)
[Both](#)

[Calculator](#)
[Register](#)

License key	Type	Service	Date (UTC)	Status	Action	Devi
	Add device	Empty	2020-06-02 03:47:26	REGISTERED		NWA1
	Add device	Empty	2020-06-0110:09:57	REGISTERED		NSG5
	Remove device	Empty	2020-06-01 02:37:26			NSG5
	Add device	Empty	2020-05-22 02:42:19	REGISTERED		NWA1
	Add device	Empty	2020-05-19 05:12:14	REGISTERED		NSG5
	Remove device	Empty	2020-04-28 09:29:12			NSW1
	Add device	NCC-1Yr Bundle	2020-04-24 16:17:24	ACTIVATED		NSW1
	Add device	Empty	2020-04-18 03:19:13	REGISTERED		NSG1
	Remove device	NCC Stay	2020-04-10 02:56:45			NSW1
	Add device	Empty	2020-04-10 02:55:52	REGISTERED		NSW1
LIC-NCC-ZZ0006F202004091751	Add license	500 Nebula Points	2020-04-09 09:52:49	REGISTERED	Activate	
LIC-NCC-ZZ0006F202004091752	Add license	500 Nebula Points	2020-04-09 09:52:49	REGISTERED	Activate	
LIC-NSS-ZZ0006F202004091747	Activate license	500 Nebula Security Points	2020-04-09 09:49:56	ACTIVATED		
LIC-NSS-ZZ0006F202004091748	Add license	500 Nebula Security Points	2020-04-09 09:49:36	REGISTERED	Activate	

The following table describes the labels in this screen.

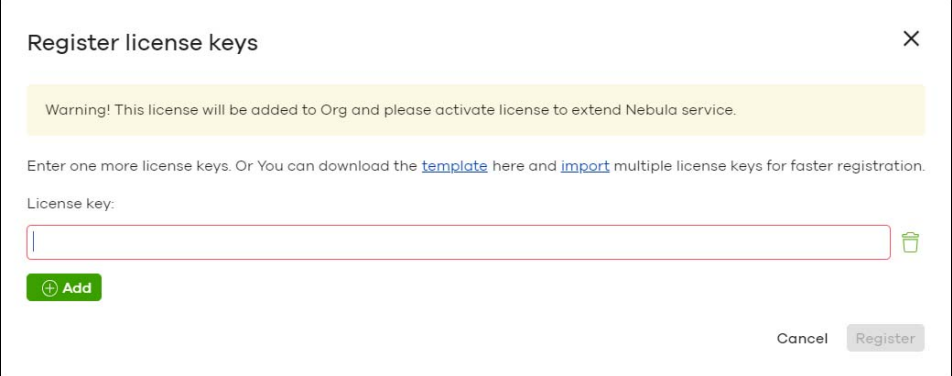
Table 14 Organization-wide > Configure > License management

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. It shows N/A for a lifetime license.
Remaining	This shows the number of days remaining before the license expires. It shows N/A for a lifetime license.

Table 14 Organization-wide > Configure > License management (continued)

LABEL	DESCRIPTION
Calculator	<p>This opens a screen where you can determine the additional device points you need to allow more time for the service in the current organization.</p> <p>Select a date to which you want to extend the expiration date for the current license. You can only purchase 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>
	<div><div>Calculator</div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><</div></div>

Table 14 Organization-wide > Configure > License management (continued)

LABEL	DESCRIPTION
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.
Service	<p>This shows the type of the service.</p> <p>It shows NCC-1Yr Bundle 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 Empty if the device does not have a NCC service license.</p> <p>It shows NCC Stay or NCC+NSS Stay 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 Help > Support request to submit a ticket.</p> <p>It shows the number of Nebula Points or Nebula Security Points that have been transferred to another organization when the Type is Transfer out or transferred from other organization(s) to this organization when the Type is Transfer in. It also shows the number of points the organization obtained when a service is registered with a new license key (Type is Add license) or received for free when the Type is Promotion.</p>
Date (UTC)	This shows when the service is activated.
Status	This shows whether the service is registered (and activated).
Action	Click the Activate 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.

4.3.4 Organization Settings

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

Figure 20 Organization-wide > Configure > Settings

Organization-wide > Configure > Settings

Settings

Organization information

Name: Temp

Country: Taiwan

Security

Idle Timeout: 0 minutes of inactivity will logout users.

Login IP ranges: Only allow access to Dashboard from IP addresses in the specified ranges.
This computer is using IP address : 61.222.86.79

Import certificate: Use my certificate

Name: (64 letters)

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

Password: (PKCS#12 only)

Delete this organization Beta

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

Please check your setting as below: [sites](#), [administrators](#), [users](#), [licenses](#), [inventory](#) of devices.

Delete organization

The following table describes the labels in this screen.

Table 15 Organization-wide > Configure > Settings

LABEL	DESCRIPTION
Name	Enter a descriptive name for the organization.
Country	Select the country where the organization is located. Note: This field is only for reference. It does not affect any other fields or features in NCC.
Security	
Idle timeout	Select ON and enter the number of minutes each user can be logged in and idle before the NCC automatically logs out the user. Select OFF if you do not want the NCC to log out idle users.
Login IP ranges	Select ON and specify the IP address range of the computers from which an administrator is allowed to log into the NCC. Select OFF to allow any IP address of the computer from which an administrator can log into the NCC.

Table 15 Organization-wide > Configure > Settings (continued)

LABEL	DESCRIPTION
Import certificate	Select ON 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 Edit to change the certificate name or password or replace the certificate.
Update certificate	Click this button to save a new certificate to the NCC.
Name	Enter a name for the certificate.
File Path	Click to find the certificate file you want to upload.
Password	Enter the certificate file's password.
Delete this organization	Click the Delete organization button to remove the organization when it does not have any sites, devices or users. Note: You will be redirected to the Choose organization page after this organization is deleted.

4.3.5 Administrator

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

Figure 21 Organization-wide > Configure > Administrator

Organization-wide > Configure > Administrators						
Administrators						
Activation	Force logout	Delete	Search administrators...	3 administrators	Change owner	Import
+	Add					
Name	Email address	Privilege	Account status	Last access time (UTC)	Create date (UTC)	Status change date (UTC)
<input type="checkbox"/> Zy TW	zytw@zyxel.com.tw	Owner	OK	2020-09-11 03:23:27	2020-01-07 03:43:24	2020-01-07 03:43:24
<input type="checkbox"/> Root	Root@zyxel.com.tw	Organization (Full)	OK	2020-06-09 05:47:15	2020-06-09 01:31:12	2020-06-09 05:47:15
<input type="checkbox"/> DelegateOwner	DelegateOwner@zyxel.com.tw	Organization (Delegated)	Deactivated	Never	-	2020-09-11 08:35:35

The following table describes the labels in this screen.


Table 16 Organization-wide > Configure > Administrator

LABEL	DESCRIPTION
Activation	Click this button to Activate/Deactivate the selected account(s). Then, click Update .
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 16 Organization-wide > Configure > Administrator (continued)

LABEL	DESCRIPTION
Change owner	<p>This button is only available if you are the organization owner.</p> <p>Click this button to transfer ownership of the organization to another user account. The new owner account must be an organization full administrator.</p> <div data-bbox="493 411 1305 848"> <p>Change organization owner ✕</p> <hr/> <p>Please select current organization admin to become new owner.</p> <div data-bbox="509 579 1279 625"> Tam - Thomas.Manning@quest.com/le ▼ </div> <p><input type="checkbox"/> This action will cause you lose ownership rights include Nebula devices under this organization. Do you want to continue?</p> <div data-bbox="1149 785 1279 831"> No Yes </div> </div> <p>After transferring ownership, NCC performs the following actions:</p> <ul style="list-style-type: none"> • Changes your account from organization owner to organization full administrator. • Transfers all devices and licenses in the organization to the new owner. • Sends the new owner an email, notifying them of the change.
Import	<p>Click this button to create administrator accounts in bulk by importing a complete list of all new administrators in an Excel file.</p> <div data-bbox="493 1062 1240 1415"> <p>Bulk Import ✕</p> <p>"Bulk Import" supports for faster inputting. Please follow this template to import</p> <div data-bbox="526 1192 1208 1318"> <div data-bbox="824 1213 909 1255">Browse</div> <p>Or drag file here...</p> </div> <div data-bbox="1143 1352 1208 1381">Close</div> </div>
Add	Click this button to create a new administrator account. See Section 4.3.5.1 on page 57 .
Name	This shows the name of the administrator account.
Email address	This shows the email address of the administrator account.

Table 16 Organization-wide > Configure > Administrator (continued)

LABEL	DESCRIPTION
Privilege	<p>This shows whether the administrator account has read-only, monitor-only, guest ambassador, or read and write (full) access to the organization and sites.</p> <p>Installer indicates that the administrator account can register devices at a site.</p> <p>Owner indicates that the administrator account is the creator of the organization, who has full access to that organization and cannot be deleted by other administrators.</p> <p>Organization (Delegated) means that the administrator account has delegated owner privileges. This type of account can perform all of the same actions as the organization owner, except for the following:</p> <ul style="list-style-type: none"> • Delete organization • Transfer organization ownership • Assign delegate owner privileges to an administrator account
Account status	This shows whether the administrator account has been validated (OK). It shows Deactivated if an administrator account has been created but cannot be used. This may happen since you can only have up to five active administrator account on Nebula (free).
Last access time	This shows the last date and time traffic was sent from the administrator account.
Create date	This shows the date and time the administrator account was created.
Status change date	This shows the last date and time the administrator account status was changed.
	Click this icon to display a greater or lesser number of configuration fields.

4.3.5.1 Create/Update Administrator

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

Figure 22 Organization-wide > Configure > Administrator: Create/Update administrator

Create administrator [X]

Name: [Text Input] [X] *

Email: [Text Input] [X] *

Organization access: Read-Only [v]

☐ Delegate owner's authority [i]

Activate: No [v]

Site	Privilege
[Dropdown]	Monitor-only [v] [X]

[+ Add]

[Close] [Create admin]

The following table describes the labels in this screen.

Table 17 Organization-wide > Configure > Administrator: Create/Update administrator

LABEL	DESCRIPTION
Name	Enter a descriptive name for the administrator account.
Email	Enter the email address of the administrator account, which is used to log into the NCC. This field is read-only if you are editing an existing account.
Organization access	<p>Set the administrator account's access to the organization.</p> <p>When an administrator account has read and write (Full) access, the administrator can create or delete other administrator accounts, create or delete a site, and add or renew licenses for Nebula devices in the organization.</p> <p>Note: The administrator account you use to create an organization is the organization creator account that has full access to that organization. The organization creator account cannot be deleted by other organization administrators.</p> <p>If you select Read-only, the administrator account can be the organization administrator (that has no write access to the organization) and also be a site administrator.</p> <p>If you select None, the administrator account can only be a site administrator.</p>

Table 17 Organization-wide > Configure > Administrator: Create/Update administrator (continued)

LABEL	DESCRIPTION
Delegate owner's authority	<p>This setting is only available when Organization access is set to Full.</p> <p>Select this setting to grant delegate owner privileges to an organization full administrator account. An account with delegate owner privileges can perform all of the same actions as the organization owner, except for the following:</p> <ul style="list-style-type: none"> • Delete organization • Transfer organization ownership • Assign delegate owner privileges to an administrator account
Activate	Select Yes to enable the account or No to temporarily disable the account.
YES, I want to do it.	<p>The check box displays only when an administrator that has full access to the organization selects No in the Activate field to disable his/her own account.</p> <p>Note: After you select the check box and click Update admin, you lose administrator privileges and cannot manage the organization again. If you have other organizations created on your account, you can click and select another organization to manage in the MSP Portal screen.</p>
Site	<p>This field is available only when you set the account's organization access to Read-only or None.</p> <p>Select the site to which you want to set the account's access. You can also select the site tag created using the Organization-wide > Monitor > Overview: Sites screen.</p>
Privilege	<p>This field is available only when you set the account's organization access to Read-only or None.</p> <p>Set the administrator account's access to the site.</p> <p>You can select from Read-only, Monitor-only, Guest Ambassador, Installer and Full (read and write).</p> <p>An administrator account that has Guest Ambassador access can create, remove or manage guest accounts using the Cloud Authentication screen (see Section 4.3.6 on page 59).</p> <p>Installer 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/Update admin	Click this button to save your changes and close the screen.

4.3.6 Cloud Authentication

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

The changes you made in this screen apply to all sites in the organization. To change the cloud authentication settings for a specific site, go to **Site-wide > Configure > Cloud Authentication** (see [Section 5.2.5 on page 96](#)).

Figure 23 Organization-wide > Configure > Cloud Authentication

Organization-wide > Configure > [Cloud authentication](#)

Cloud authentication

Account type: DPPSK For wireless secure connection

Authorization
Remove users
Print

2 selected in 5 Users
Import
Add
Export

<input type="checkbox"/>	Email	Username	Account type	DPPSK	VLAN id	Authorized	Expire in (UTC)	Created by	Created at (UT...)
<input checked="" type="checkbox"/>			DPPSK	●●●●●●●●	—	No	—	zyuxdwriters@g...	2020-07-02 05:48:28
<input checked="" type="checkbox"/>			DPPSK	●●●●●●●●	—	No	—	zyuxdwriters@g...	2020-07-02 05:48:28
<input type="checkbox"/>			DPPSK	●●●●●●●●	—	All sites	Never	zyuxdwriters@g...	2020-07-02 06:05:05
<input type="checkbox"/>			DPPSK	●●●●●●●●	—	All sites	Never	zyuxdwriters@g...	2020-07-02 06:05:05
<input type="checkbox"/>			DPPSK	●●●●●●●●	—	All sites	Never	zyuxdwriters@g...	2020-07-02 06:05:05

The following table describes the labels in this screen.

Table 18 Organization-wide > Configure > Cloud Authentication

LABEL	DESCRIPTION
Account Type	<p>Select the type of user accounts that you want to view, manage or create.</p> <p>Guest - a guest that can gain access to the networks via the captive portal.</p> <p>User - 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>VPN User - a L2TP VPN client that can gain access to the networks by authenticating with the Nebula cloud authentication server.</p> <p>MAC - an internal user that can gain access to the networks by authenticating with a RADIUS server via the MAC-based authentication method.</p> <p>DPPSK (Dynamic Personal Pre-Shared Key) - A user that can gain access to the networks by connecting to an SSID using a unique key that is linked to their user account. For details, see Section 8.3.2 on page 228.</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> <div> <input checked="" type="radio"/> Authorize users (All sites) <div> <input checked="" type="radio"/> Does not expire <div> <input type="radio"/> Expires in: <input type="text" value="X"/> minutes </div> </div> <input type="radio"/> Revoke authorization (Not authorized) <div>Update</div> </div>
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 account and click this button to remove the selected user account(s).</p>

Table 18 Organization-wide > Configure > Cloud Authentication (continued)

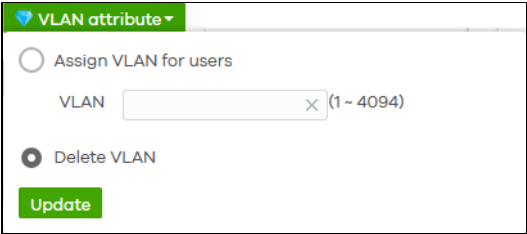

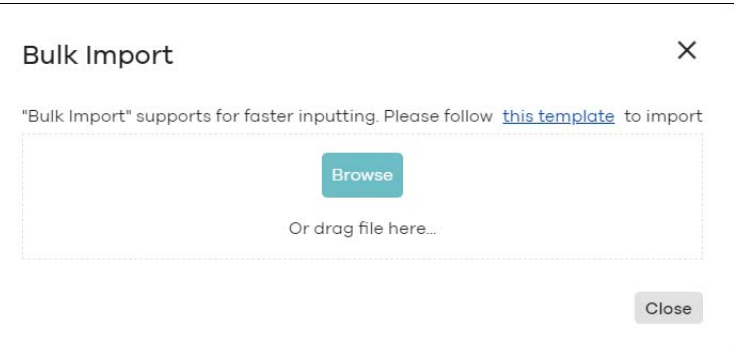

LABEL	DESCRIPTION
VLAN attribute	<p>This field is available when the account type is set to User.</p> <p>Assign a VLAN ID for all user account(s) or remove the VLAN ID. Then click Update.</p> 
Print	<p>This field is available when the account type is set to DPPSK.</p> <p>Print the unique dynamic personal pre-shared key (DPPSK) and expiry time of each selected user account. The account details can be cut into cards, and then given to users in order to grant them wireless network access.</p> <p style="text-align: center;">DPPSK</p> 
Search users	Enter a key word as the filter criteria to filter the list of user accounts.
User(s)	This shows how many user accounts match the filter criteria and how many user accounts of the selected type are created in total.
Import	<p>Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.</p> 
Add	Click this button to create a new user account. See Section 4.3.6.1 on page 62 .
Export	Click this button to save the account list as a CSV or XML file to your computer.
Email	<p>This field is available only when the account type is set to User, Guest or VPN User.</p> <p>This shows the email address of the user account.</p>
Username	<p>This field is available only when the account type is set to User, Guest or VPN User.</p> <p>This shows the user name of the user account.</p>
Description	This shows the descriptive name of the user account.

Table 18 Organization-wide > Configure > Cloud Authentication (continued)

LABEL	DESCRIPTION
MAC address	This field is available only when the account type is set to MAC . 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 (No). If the user is authorized, it shows All sites or the name of the site to which the user is allowed access.
Authorized by	This shows the email address of the administrator account that authorized the user. If the account has been authorized by different admins across different sites, it shows Multiple value .
Expire in (UTC)	This shows the date and time that the account expires. This shows - if authentication is disabled for this account. This shows Never if the account never expires. This shows Multiple value if the account has different Expire in values across different sites.
Login by	This field is available only when the account type is set to User , Guest or VPN User . 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.
VLAN assignment	This field is available only when the account type is set to User . This shows the VLAN assigned to the user.
	Click this icon to display a greater or lesser number of configuration fields.

4.3.6.1 Create/Update User

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

Note: If **Account type** is set to DPPSK, then clicking Add gives you a choice to add one account or multiple accounts For details on adding multiple accounts (batch create), see [Section 4.3.6.2 on page 64](#).

Figure 24 Organization-wide > Configure > Cloud Authentication: Create/Update user

Create user [X]

Account type: USER

Email: [Redacted] *

Username: []

Description: []

Password: [Redacted] * Generate

Authorized: Not authorized ▼

Login by: Email ▼

VLAN assignment: []

[Close] [Print] [Create user]

The following table describes the labels in this screen.

Table 19 Organization-wide > Configure > Cloud Authentication: 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 MAC . 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 MAC . Enter the password of this user account. It can consist of 4 - 31 alphanumeric characters. You can click Generate to have the NCC create a password for the account automatically.
DPPSK	This field is only available when the account type is DPPSK . Enter a dynamic personal pre-shared key (DPPSK) for this DPPSK user account. It can consist of 8- 31 alphanumeric characters. You can click Generate to have the NCC create a DPPSK for the account automatically.
MAC address	This field is available only when the account type is MAC . Enter the MAC address of this account.
Authorized	Set whether you want to authorize the user of this account. You can select to authorize the user's access to All Sites or Specified Sites in the organization. If you select Specified Sites , a field displays allowing you to specify the site(s) to which the user access is authorized.

Table 19 Organization-wide > Configure > Cloud Authentication: Create/Update user (continued)

LABEL	DESCRIPTION
Expire in	<p>This field is available only when the user is authorized.</p> <p>Click Change to specify the number of minutes/hours/days/weeks the user can be logged into the network in one session before the user of this account has to log in again.</p> <p>Note: If the account has been set with different Expire in values across different sites, it will show Multiple value and the Change link.</p> <p>Otherwise, select Never and the user of this account will never be logged out.</p>
Login by	<p>This field is not available when the account type is MAC.</p> <p>Select whether the user needs to log in with the email address and/or user name.</p>
VLAN assignment	<p>This field is only available when the account type is User.</p> <p>This allows you to assign a user to a specific VLAN based on the user credentials instead of using a RADIUS server.</p>
VLAN id	<p>This field is only available when the account type is DPPSK.</p> <p>This allows you to assign a user to a specific VLAN based on the user's dynamic personal pre-shared key (DPPSK).</p>
Email DPPSK to user	<p>This field is only available when the account type is DPPSK.</p> <p>Send a copy of the user account's dynamic personal pre-shared key (DPPSK) to the account email address.</p>
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.

4.3.6.2 Batch Create DPPSK Accounts

To have NCC create multiple DPPSK user accounts, each with a unique dynamic personal pre-shared key (DPPSK), go to the **Side-wide** or **Organization-wide > Configure > Cloud Authentication** screen, click **Add**, and then select **Batch Create DPPSK**.

Figure 25 Organization-wide > Configure > Cloud Authentication: Batch Create DPPSK

Batch create DPPSK user [X]

Account type: DPPSK

Number of accounts: 20 * (1-20)

VLAN id:

E-mail account info to:

Authorized: All sites

Expire in: Never [Change](#)

[Close] [Create user]

The following table describes the labels in this screen.

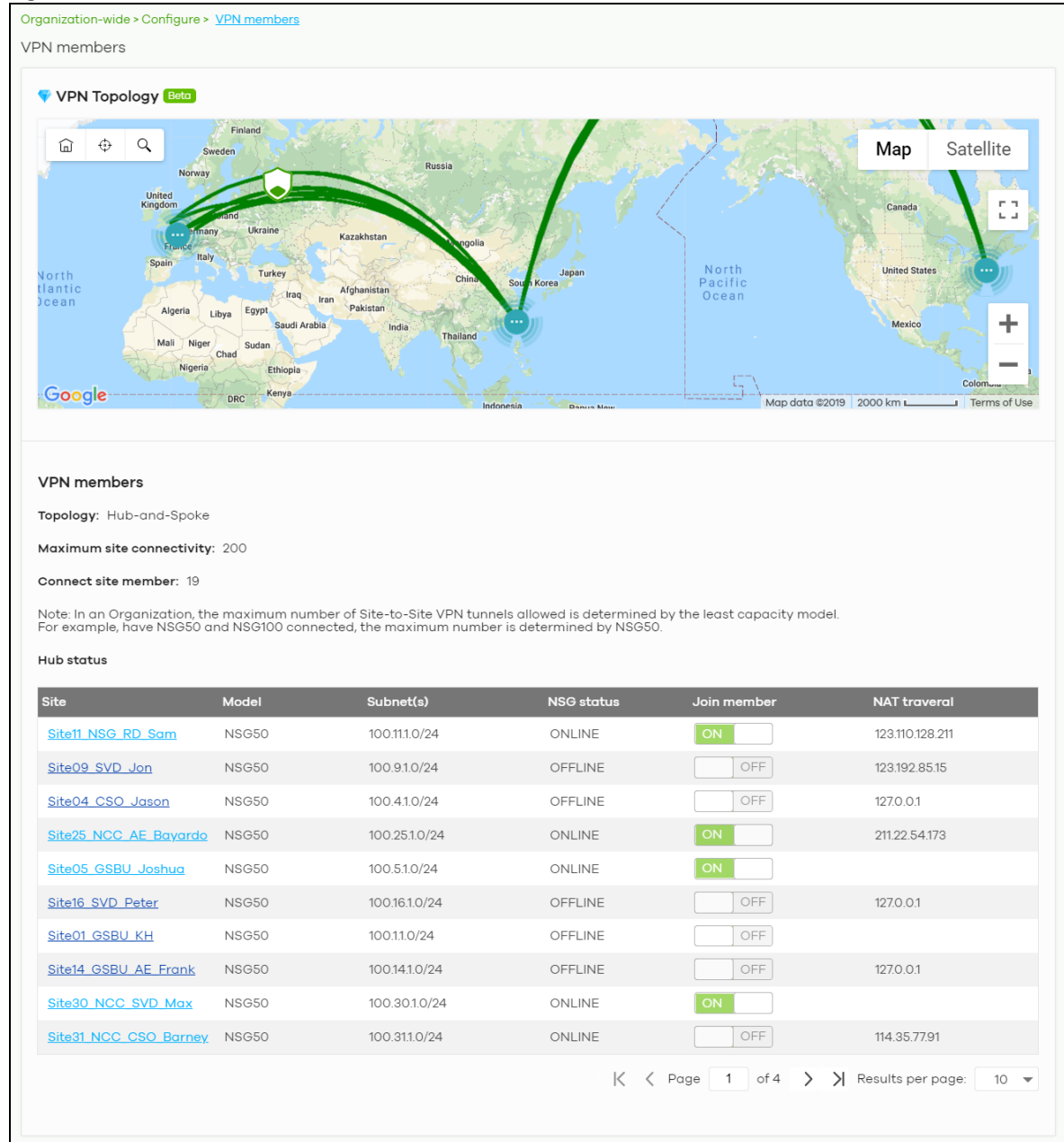
Table 20 Organization-wide > Configure > Cloud Authentication: Batch Create DPPSK

LABEL	DESCRIPTION
Number of accounts	Enter how many DPPSK user accounts you want to create.
VLAN id	Assign the users to a specific VLAN based on the user's dynamic personal pre-shared key (DPPSK).
E-mail account info to	Send a copy of each user account's dynamic personal pre-shared key (DPPSK) and expiry date to the specified email address. This information is in a printable format. The expiry date includes a time and date in UTC format.
Authorized	Set whether you want to authorize the user of this account. You can select to authorize the user's access to All Sites or Specified Sites in the organization. If you select Specified Sites , a field displays allowing you to specify the site(s) to which the user access is authorized.
Expire in	This field is available only when the user is authorized. Click Change to specify the number of minutes/hours/days/weeks the user can be logged into the network in one session before the user of this account has to log in again. Note: If the account has been set with different Expire in values across different sites, it will show Multiple value and the Change link. Otherwise, select Never and the user of this account will never be logged out.
Close	Click this button to exit this screen without saving.
Create user	Click this button to save your changes and close the screen.

4.3.7 VPN Members

Use this screen to view and manage the VPN members for all VPNs in an organization.

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

Figure 26 Organization-wide > Configure > VPN Members

The following table describes the labels in this screen.

Table 21 Organization-wide > Configure > VPN Members

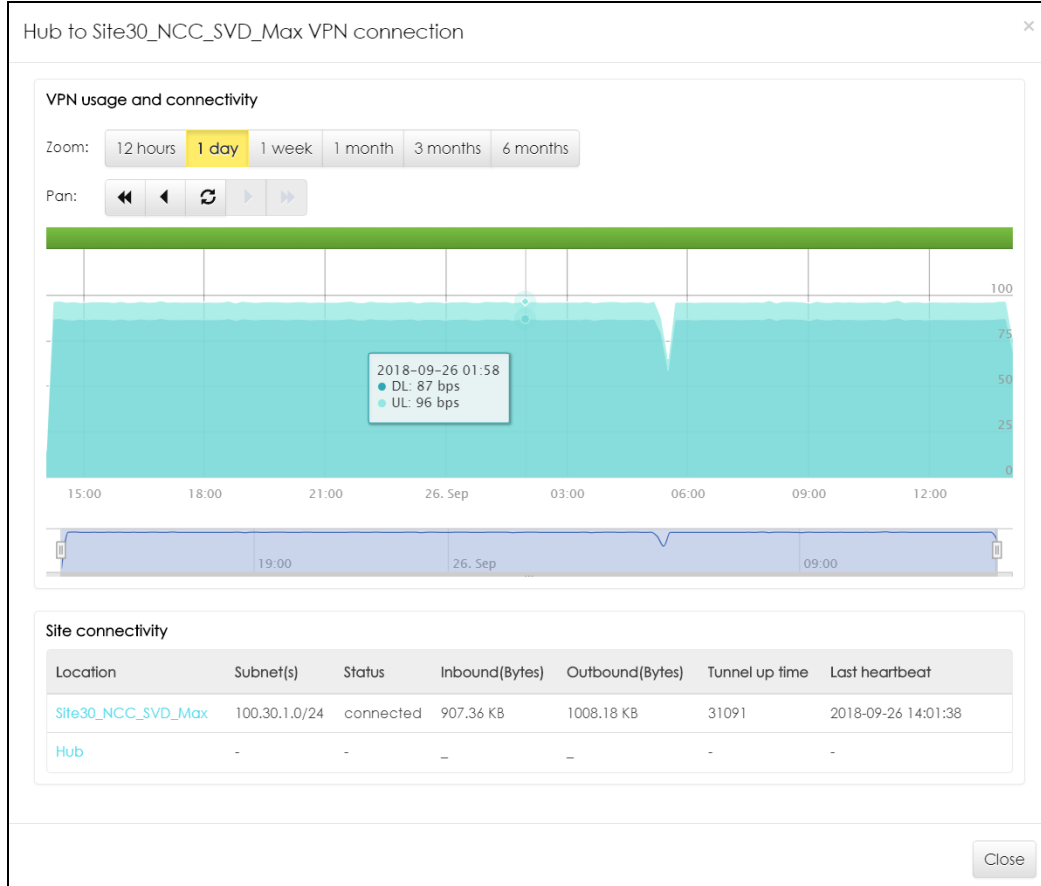
LABEL	DESCRIPTION
VPN Topology	The VPN topology specifies how the Nebula gateways in the organization are connected to each other via VPN. Each map pin depicts a site. Click a map pin to show its site name. Click a line to view the VPN usage and connectivity of the VPN connection between two sites.
VPN Members	
Topology	This shows the VPN topology of the organization.

Table 21 Organization-wide > Configure > VPN Members (continued)

LABEL	DESCRIPTION
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.
Site	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 Site-Wide > Dashboard 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 off-line.
Members	This shows the number of sites which set up a VPN connection with other sites in the organization.
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.
Site Connectivity	
Site	This shows the name of the site in this organization. Click the name to go to the Site-Wide > Dashboard 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 off-line.
Join member	Select ON to set the VPN topology of the security gateway to Site-to-Site by default or Hub-and-Spoke when another site in the same organization has permitted the use of Hub-and-Spoke VPN topology. Otherwise, select OFF to not set a VPN connection. This also changes the VPN topology in the Gateway > Configure > Site-to-Site VPN screen (see Section 6.3.6 on page 143).
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.

4.3.7.1 VPN Usage and Connectivity

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

Figure 27 Organization-wide > Configure > VPN Members: VPN Usage and Connectivity

The following table describes the labels in this screen.

Table 22 Organization-wide > 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 Gateway > Configure > Site-to-Site VPN 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 22 Organization-wide > Configure > 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.

4.3.8 Configuration Management

Configuration synchronization allows you to easily copy configurations from one site/device to another. Use this screen to synchronize the configuration between sites or switch ports. You can also back up the current configurations for sites or switches to the NCC and restore the configuration at a later date.

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

Figure 28 Organization-wide > Configure > Configuration Management

Organization-wide > Configure > Configuration management

Configuration management

Synchronization

Settings: Site-wide general settings

From source site: Hub

To site(s): Select some sites

[What will be synchronized?](#) Sync

Switch settings clone

From source device: Office NSW200

To device(s): Select some devices

☐ Include uplink port settings

[What will be cloned?](#) Clone

Backup & restore Beta

Site(s) settings

Backup	Description	Date (UTC)	Admin
1	<input type="text"/> X *		

+ Add [What is this?](#) Restore

Switch settings

Backup	Switch	Description	Model	Date (UTC)	Admin
1	<input type="text"/>	<input type="text"/> X *		Never	

+ Add [What is this?](#) Restore

The following table describes the labels in this screen.

Table 23 Organization-wide > Configure > Configuration Management

LABEL	DESCRIPTION
Synchronization	
Settings	Specify whether general site configuration or just SSID settings of a site will be propagated to other sites. Click What will be synchronized? to view detailed information.
From source site	Select the site from which you want to copy its site configuration to other sites.
To Site(s)	Select one or more sites to which you want to import the copied site configuration. You can also select the site tags created using the Organization > Monitor > Overview: Sites 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 Add to create a new backup, you need to enter a name for the backup in order to save it to the NCC.
Date (UTC)	This shows the date and time the backup was saved on the NCC server.
Admin	This shows the name of the administrator account who performed the backup.
Remove	Click the remove icon to delete the backup.
Add	Click this button to create a new configuration backup of all the sites in the organization.
Restore from backup	Select the backup you want to restore.
Restore to site(s)	Select one or more 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 Add to create a new backup, you need to enter a name for the backup in order to save it to the NCC.
Model	This shows the model number of the switch.
Date (UTC)	This shows the date and time the backup was saved on the NCC server.

Table 23 Organization-wide > Configure > 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 selectable 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.

4.3.9 Configuration Template

A configuration template is a virtual site. The settings you configured in a template will apply to the real sites which are bound to the template. If you do not want to apply any new settings from the template to a site, just unbind that site. If you want to configure some specific settings directly in a site after the site is bound to a template, turn on the local override function (see [Section 4.3.9.3 on page 73](#)).

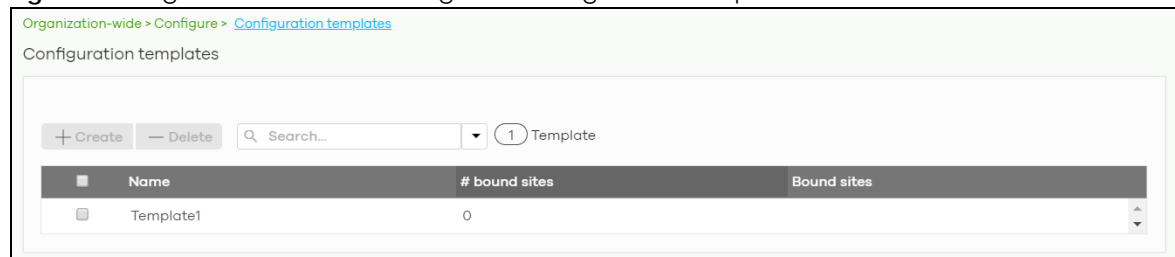
Use this screen to create and manage configuration templates. You then can bind or unbind a site from the template (see [Section 4.3.9.1 on page 72](#)).

Note: A site can only be bound to one template. The same template can be used by multiple sites. The site(s) and the template should belong to the same organization for binding.

Note: If the NCC service is downgraded from Nebula Professional Pack to Nebula Basic, all the sites will be unbound from the template(s) but retain the settings already applied from the template.

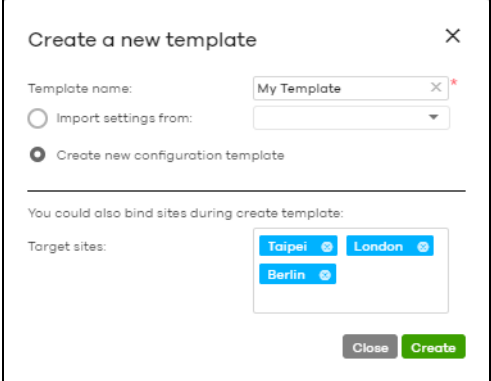
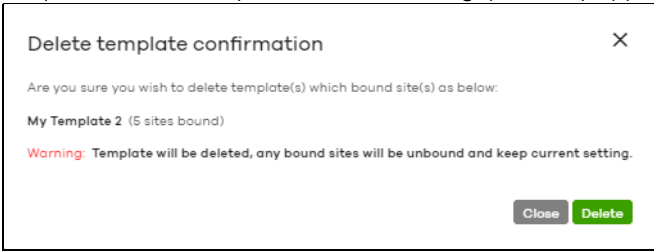
Click **Organization-wide > Configure > Configuration Template** to access this screen.

Figure 29 Organization-wide > Configure > Configuration Template



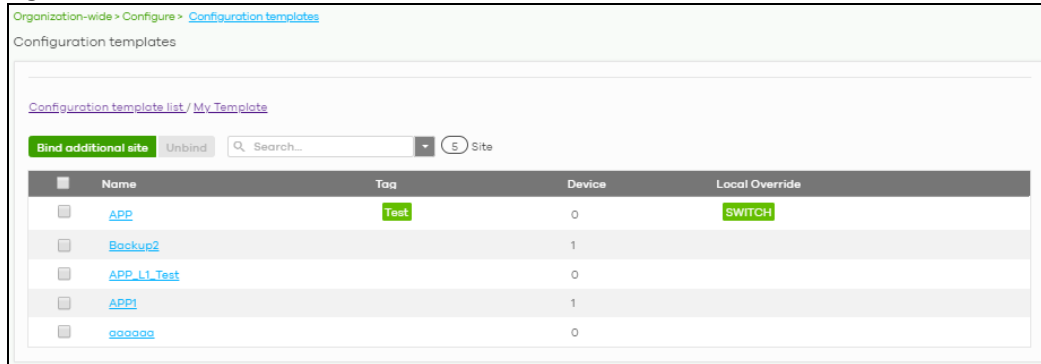
The following table describes the labels in this screen.

Table 24 Organization-wide > Configure > Configuration Template

LABEL	DESCRIPTION
Create	<p>Click this button to create a new configuration template. You can copy settings from an existing site or configuration template, or have a new template with default settings. It is optional to bind one or more sites to the template when you are creating a template.</p> 
Delete	<p>Click this button to remove the selected template(s). A window pops up asking you to confirm that you want to delete the template(s).</p> <p>If you remove a template that is being used by a site, the site will be unbound from the template automatically and retain the settings previously applied from the template.</p> 
Search	Enter a key word as the filter criteria to filter the list of templates.
Templates	This shows how many templates match the filter criteria and how many templates are created in total.
Name	This shows the name of the template.
# Bound sites	This shows the number of the site(s) bound to the template.
Bound sites	This shows the name of the site(s) bound to the template.

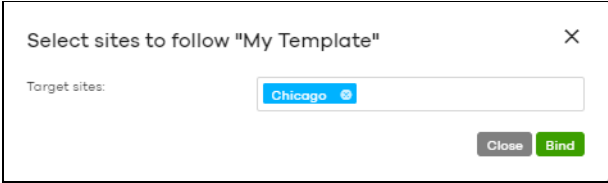
4.3.9.1 Site Binding

Use this screen to bind or unbind a site from a template. Click an existing template from the list in the **Organization-wide > Configure > Configuration Template** screen to access this screen. To go back to the previous screen, click the **Configuration template list** link.

Figure 30 Organization-wide > Configure > Configuration Template: Template

The following table describes the labels in this screen.

Table 25 Organization-wide > Configure > Configuration Template: Template

LABEL	DESCRIPTION
Bind additional site	Click this button to bind more sites to the template. A window displays. Select the name of the site(s) in the Target sites field and click Bind . 
Unbind	Click this button to remove the selected site(s) from the template. The site which is unbound from the template still retains the settings applied from the template.
Search	Enter a key word as the filter criteria to filter the list of sites.
Sites	This shows how many sites match the filter criteria and how many sites are bound to the template in total.
Name	This shows the name of the site bound to the template.
Tag	This shows the tag(s) added to the site.
Device	This shows the number of Nebula devices which are assigned to the site.
Local override	This shows which settings in the template do not apply to the site.

4.3.9.2 Template settings

An administrator that has full access to the organization can modify the template configurations. To access a template's configuration screen, select the template name from the **Site** field in the NCC title bar. It also shows the number of sites that are bound to the template on each configuration screen.

Note: At the time of writing, you can use a template to configure site-wide, switch, and access point settings.

4.3.9.3 Local Override

When a site is bound to a template, you can see the name of the template on the site's configuration screens (which are also available in a template and can be configured).

There is also an option to make the changes you made locally to a site persist. If you select the override check box of the site's configuration screen, all the configuration screens under the same menu tab (**Site-Wide** or **Switch**) are configurable. Settings in these screens will not be affected and modified by the

template. If the override check box is not selected, any changes of the same configuration screen in the template apply to the site.

4.3.9.4 Switch Port Profile and Configuration

Just as a configuration template is a virtual site, so is a profile to a switch. The settings you configured in a profile will apply to the switches which are bound to the profile. If you do not want to apply any new settings from the profile to a switch, just unbind that switch. If you want to configure some specific settings directly in a switch (For example, a port's **Broadcast (pps)** value. See [Section 7.3.1.1 on page 187](#) for details.) after the switch is bound to a profile, turn on the local override function (see [Section 4.3.9.3 on page 73](#)).

4.3.10 Firmware Management

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

Figure 31 Organization-Wide > Configure > Firmware management

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

Firmware management

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

Site: Any Device type: Any Firmware status: Any

Upgrade Now + Schedule Upgrade Reset 2 sites

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

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

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

4.3.10.1 Firmware Upgrade Priority



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

1. Individual device upgrade schedule (set at **Organization-Wide > Configure > Firmware management**).
2. Organization-wide or site-wide upgrade schedule. If both are set, the schedule that was most recently set takes priority.
3. NCC default per-device upgrade schedule (90 days after new firmware is released).

4.3.10.2 Firmware Management Screen

The following table describes the labels in this screen.

Table 26 Organization-Wide > Configure > Firmware management

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

CHAPTER 5

Site-wide

5.1 Monitor

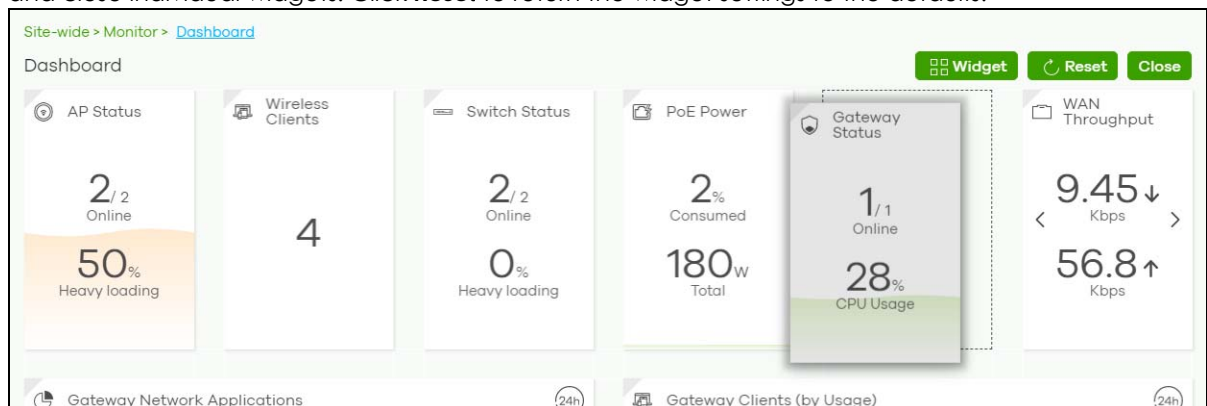
Use the **Monitor** menus to check the dashboard, summary report, map and floor plan, network topology and client list of the Nebula devices for the selected site.

5.1.1 Dashboard

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

It shows the status and information for all types of Nebula devices connected to the selected site by default.

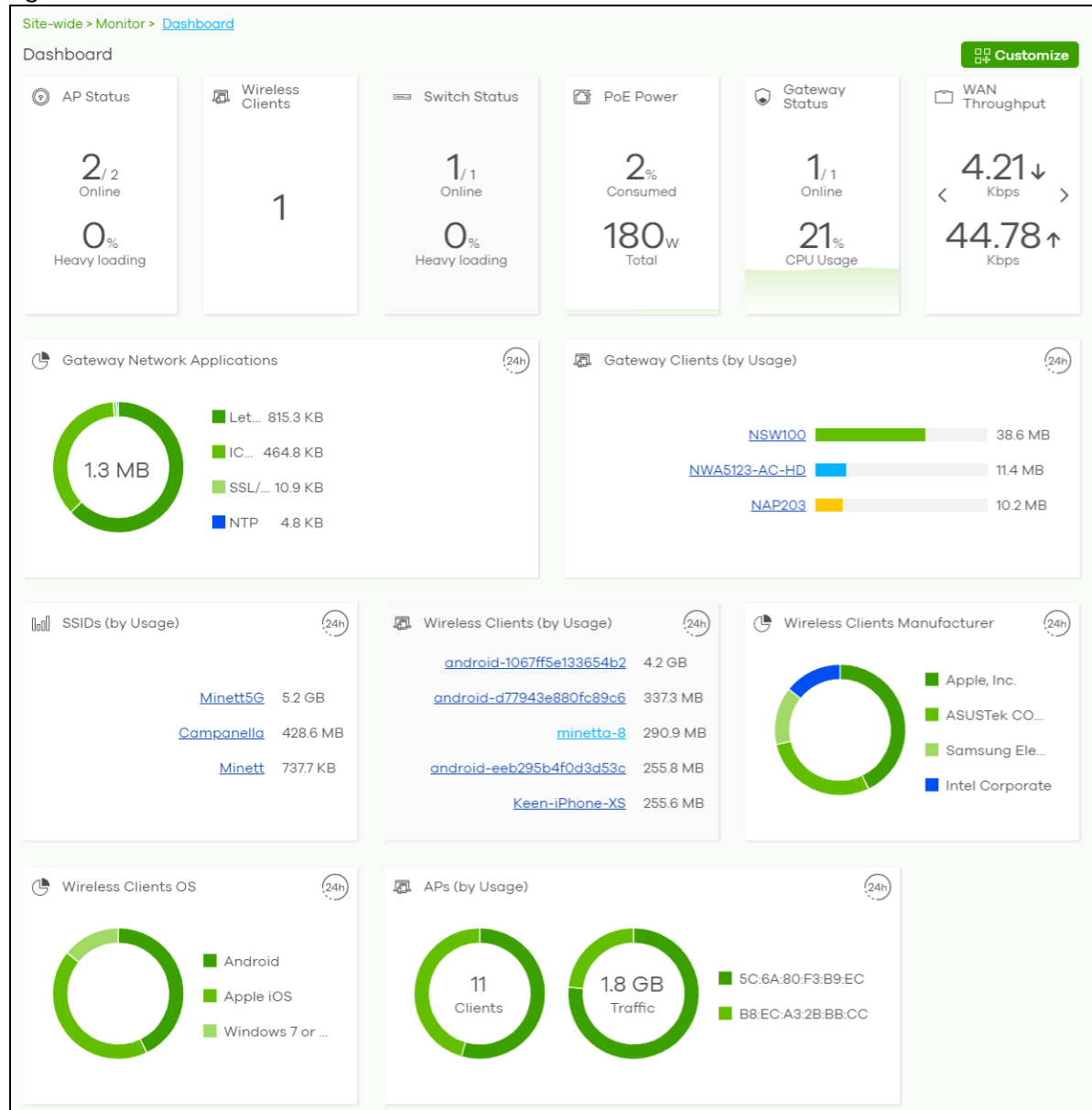
Click **Customize** to show the **Widget**, **Reset** and **Close** buttons. You can then rearrange widgets by selecting a block and holding it to move around. You can also click the **Widget** button to collapse, add and close individual widgets. Click **Reset** to return the widget settings to the defaults.



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

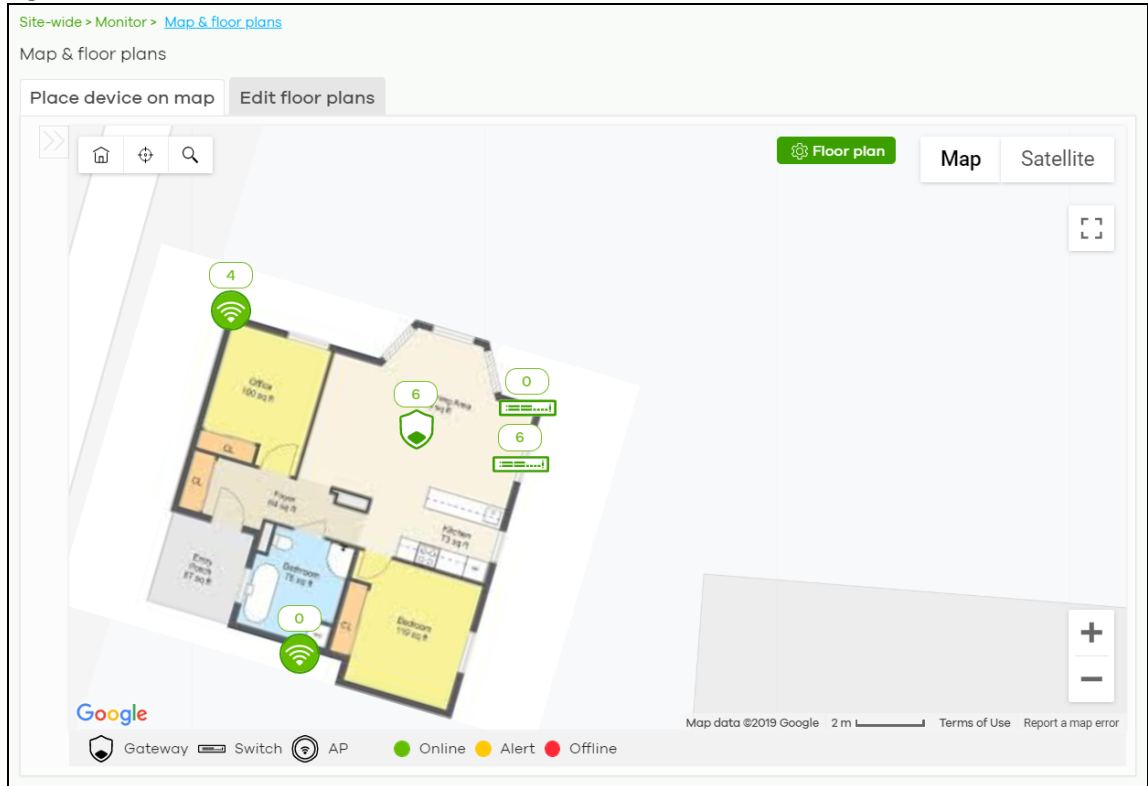
- **AP Status:** how many Nebula APs are assigned and connected, and what percentage of the APs become overloaded, that is, the number of online APs that exceed the maximum client device number (in **AP > Configure > Load Balancing**) by total number of online APs in the site.
- **Wireless Clients:** how many WiFi clients are currently connected to the managed AP(s).
- **Switch Status:** how many Nebula switches are assigned and connected, and what percentage of the switches become overloaded, that is, the number of online Nebula switches that exceed 70% of their upstream bandwidth by total number of online Nebula switches in the site.
- **PoE Power:** the total PoE power budget on the switch and the current amount of power consumed by the powered devices.
- **Gateway Status:** how many Nebula security gateways are assigned and connected, and what percentage of the gateway's processing capability is currently being used if the CPU goes over 93% usage.

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

Figure 32 Site-Wide > Monitor > Dashboard

5.1.2 Map & Floor Plans

This screen allows you to locate a device on the world map and use a floor plan to show where Nebula devices are physically located. Click **Site-Wide > Monitor > Map & floor plans** to access this screen.

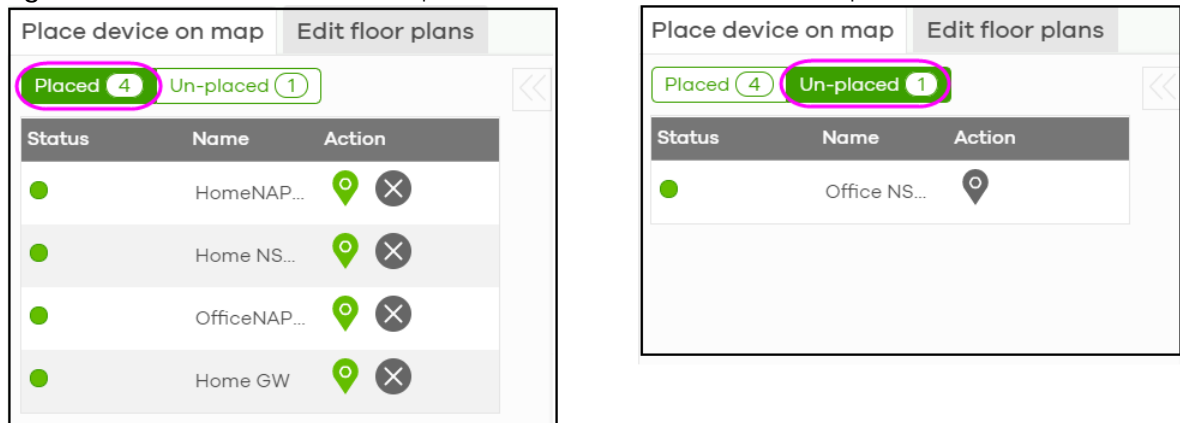
Figure 33 Site-Wide > Monitor > Map & Floor Plans

Place devices on map

You can mark on the map the places where the devices are located. Click the **Place device on map** tab to display the device list for the selected site. Click the arrow (<<) on the upper left corner of the **Map & floor plans** screen to collapse or expand the list.

Click the **Placed** button to show the devices that you have pinned on the map and/or the floor plan. Click the **Un-placed** button to show the devices that remain to be pinned on the map. To pin a device, select the device from the **Un-placed** list, then drag and drop it on to the map.

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

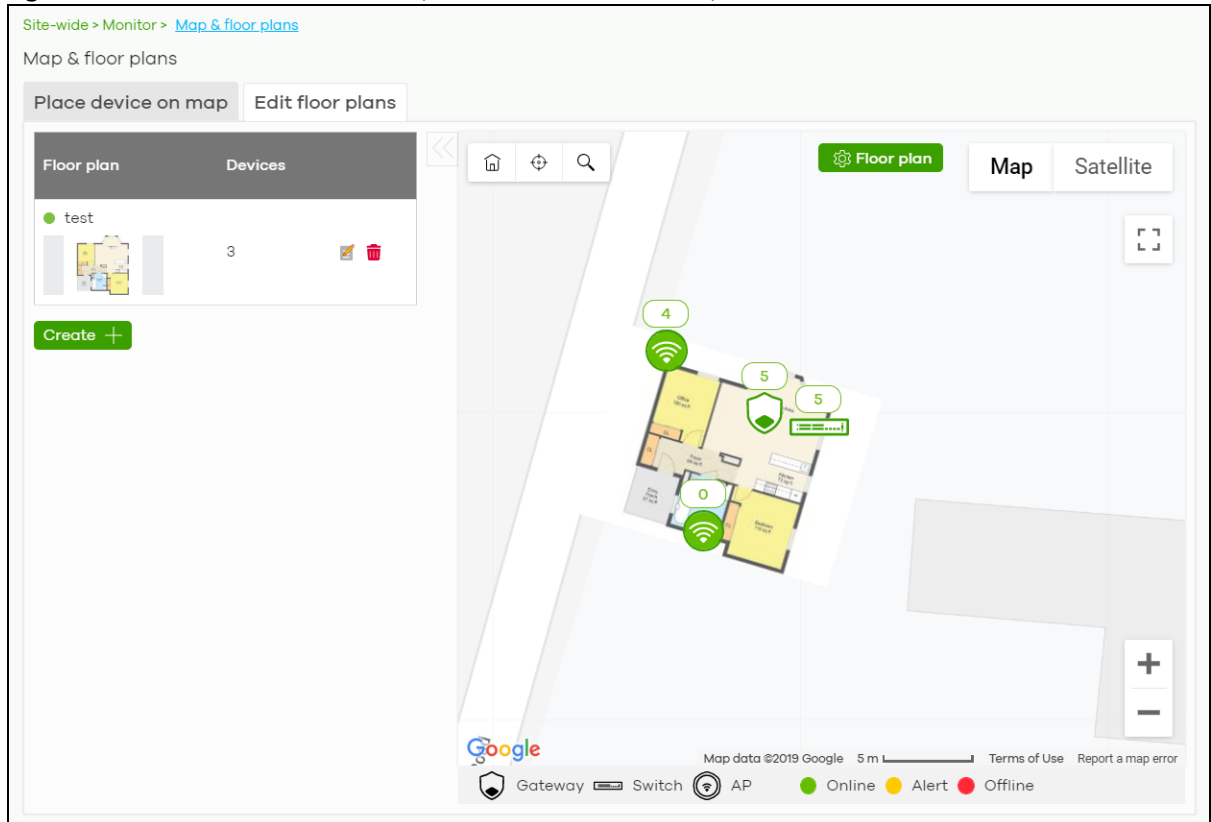
Figure 34 Site-Wide > Monitor > Map & Floor Plans: Place devices on map

Edit floor plans

Click the **Edit floor plans** tab to display the list of existing floor plan, a drawing that shows the rooms scaled and viewed from above. Click the arrow (<<) on the upper left corner of the **Map & floor plans** screen to collapse or expand the list.



Use the **Create+** button to upload a new floor plan. The floor plan then shows on the Google map at the right side of the screen. Use your mouse to move the floor plan, and use the icons at the top of the map to rotate, change the transparency, resize or hide the floor plan. Click **Set position** to apply your changes. If you want to relocate the floor plan, select the floor plan from the list and click its edit icon.

Figure 35 Site-Wide > Monitor > Map & Floor Plans: Edit floor plans



The following table describes the labels in this screen.

Table 27 Site-Wide > Monitor > Map & Floor Plans: Edit floor plans

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

5.1.3 Topology

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

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

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

Move the pointer over a link to view link details, such as type (Ethernet or wireless mesh), speed, and data usage from the past 24 hours. If the link is supplying power to a node using Power over Ethernet (PoE), you can click **Reset** to perform a power cycle on the port. This action temporarily disables PoE and then re-enables it, in order to reboot connected PoE devices.

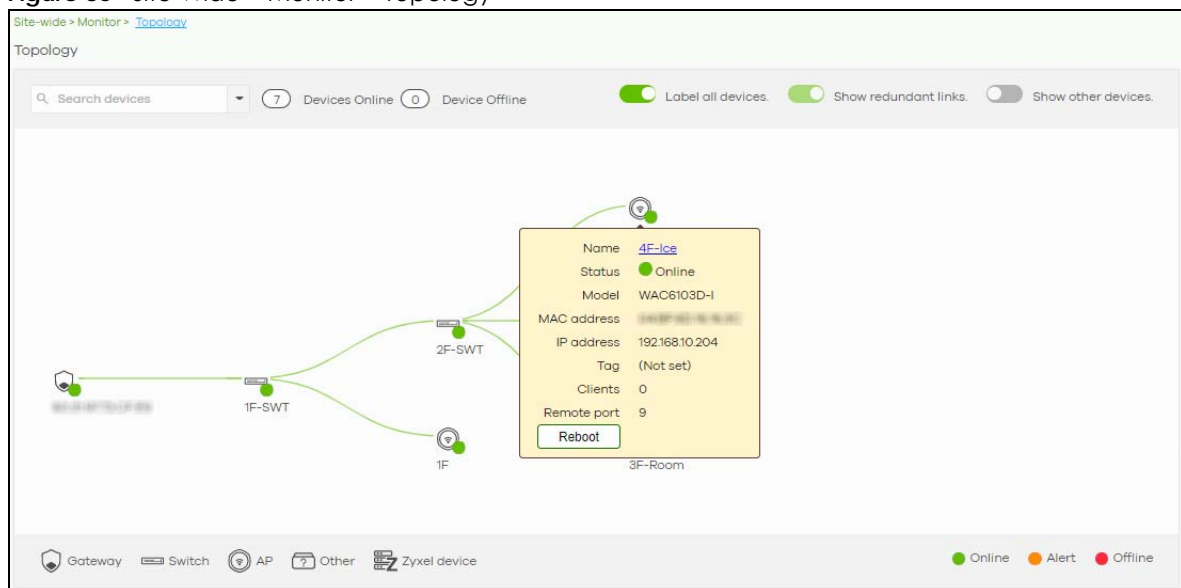
Enable **Label all devices** to show device information, such as MAC address in the network topology diagram.

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

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

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

Figure 36 Site-Wide > Monitor > Topology



5.1.4 Vouchers

A voucher is a unique printable code that allows a user to authenticate with a WiFi network for a limited period of time. A user connects to the WiFi network's SSID and then enters the code in a captive portal. After a successful login, the expiry time of the voucher starts counting down.

Vouchers are useful in situations where you want to give individual users time-limited WiFi access. For example: A customer can buy a voucher for two hours of Internet access in a hotel or coffee shop.

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

5.1.4.1 Using Vouchers

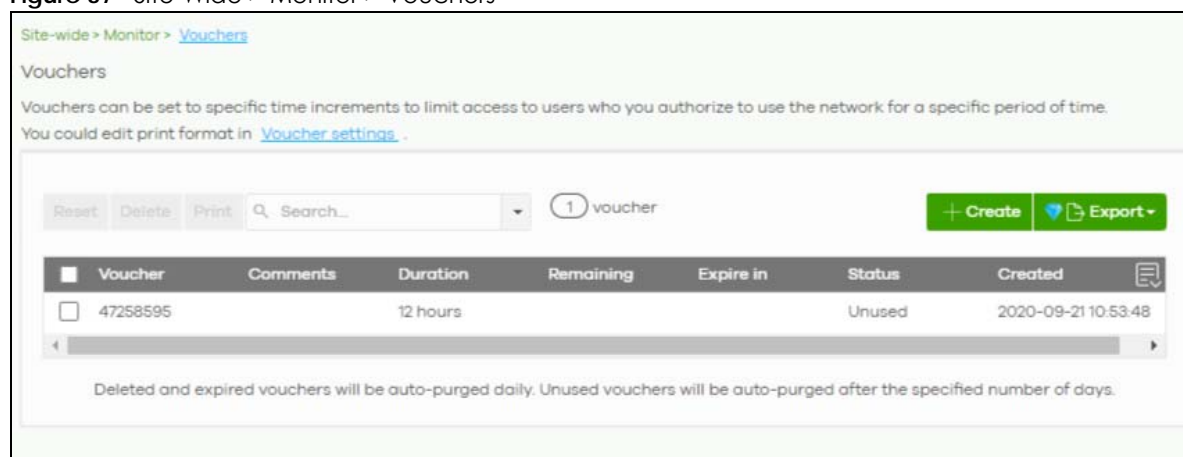
- 1 Go to **Access Point > Configure > SSID Overview**, and create a dedicated SSID for voucher-based WiFi access. For example, "Hotel_Guest_Network".
For details on configuring SSIDs, see [Section 8.3.1 on page 226](#).
- 2 Go to **Access Point > Configure > Authentication**, select the SSID, and then under **Sign-in method** select **Voucher**.
For details, see [Section 8.3.2 on page 228](#).
- 3 Go to **Site-wide > Configure > General settings > Voucher Settings** to configure how the vouchers will look when printed.
For details, see [Section 5.2.1 on page 87](#).
- 4 Go to **Site-Wide > Monitor > Vouchers**, and then click **Create** to create one or more vouchers.

5.1.4.2 Voucher Screen

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

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

Figure 37 Site-Wide > Monitor > Vouchers



The following table describes the labels in this screen.

Table 28 Site-Wide > Monitor > Vouchers

LABEL	DESCRIPTION
Reset	Select one or more vouchers and then click this button to reset the vouchers back to their original states. Each voucher's status is set to Unused and time remaining is reset to the time configured in Duration .
Delete	Select one or more vouchers and then click this button to delete the vouchers.
Print	Select one or more vouchers and then click this button to print the vouchers. You can modify how vouchers look when printed at Site-wide > Configure > General Settings .
Search	Use this field to search for vouchers, by voucher code, duration, and/or status.
Create	Click this button to create one or more new vouchers. For details, see Section 5.1.4.3 on page 83 .

Table 28 Site-Wide > Monitor > Vouchers (continued)

LABEL	DESCRIPTION
Export	Click this button to export the voucher table and all information in it to a CSV or XML file.
Voucher	This displays the voucher's unique authentication code.
Comments	This displays information about the voucher.
Duration	This displays how long the voucher is valid from when it is activated, in hours.
Remaining	This displays how much time is left before the voucher expires. NCC only starts counting this time after the voucher has been activated.
Expire in	This displays the date and time that the voucher will expire.
Status	<p>This displays the current status of the voucher:</p> <p>Unused: The voucher has not yet been used for authentication.</p> <p>Active: A user has used the voucher for authentication. NCC has started counting down the duration.</p> <p>Expire: The voucher has reached then end of its duration period and can no longer be used.</p> <p>Delete: The voucher is unused and has reached the time set under Purge after (days).</p> <p>Note: NCC automatically deletes vouchers with the status Expire or Delete after 24 hours. You can see a history of these automatic deletions in the NCC event log.</p>
Created	This displays the date and time that the voucher was created.

5.1.4.3 Create Vouchers Screen

Use this screen to create one or more new vouchers.

Figure 38 Site-Wide > Monitor > Vouchers > Create

Create vouchers [X]

Quantity: 1

Code length: 8

Comment: []

Duration (hours): 12

Purge after (days): 30

Print after created: ☒

Save as default: ☐

[Cancel] [Create]

The following table describes the labels in this screen.

Table 29 Site-Wide > Monitor > Vouchers > Create

LABEL	DESCRIPTION
Quantity	Sets the number of vouchers you want to create. The valid range for this setting is 1–999.
Code length	Sets the length of the unique code on each voucher. The valid range for this setting is 6–10.
Comment	Enter information about the voucher that might be useful for other administrators.
Duration (hours)	Sets how long the voucher is valid for after it has been activated, in hours. The valid range for this setting is 1–72.
Purge after (days)	Sets how long a non-activated voucher is valid for, in days. The valid range for this setting is 1–180.
Print after created	Select this to print the vouchers immediately after clicking Create .
Save as default	Click this to make the settings on this page the default settings for new vouchers.

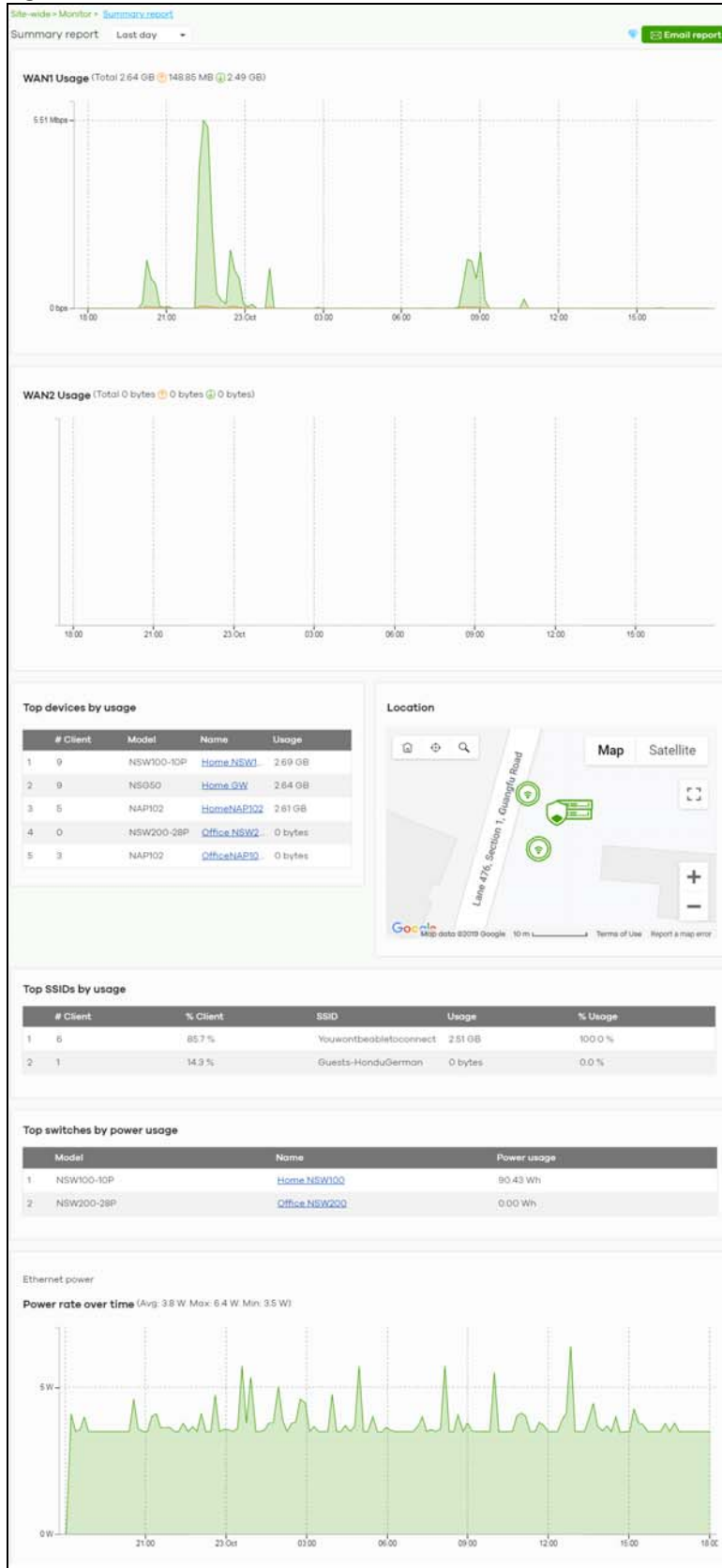
Note: Dynamic Personal Pre-Shared Keys (DPPSKs) also allow you to give individual users a printable password and time-limited WiFi access. For details, see [Section 8.3.2 on page 228](#).

5.1.5 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 39 Site-Wide > Monitor > Summary Report



The following table describes the labels in this screen.

Table 30 Site-Wide > Monitor > Summary Report

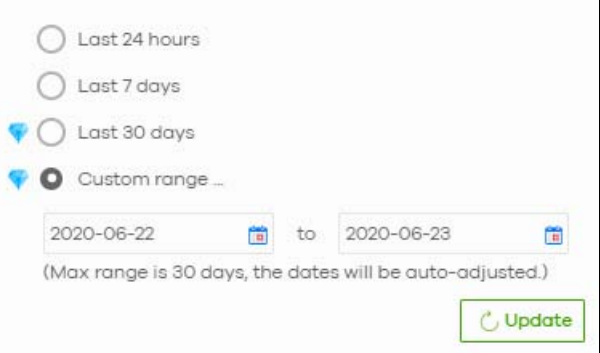
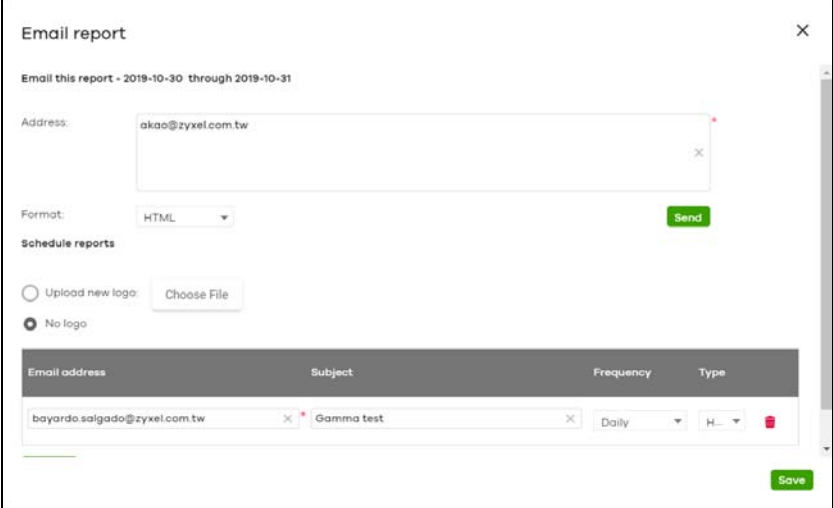
LABEL	DESCRIPTION
Summary Report	<p>Select to view the report for the past day, week or month. Alternatively, select Custom range... to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	<p>Click this button to send summary reports by email, change the logo and set email schedules.</p> 
WAN1/WAN2 usage	
This section is available when there is at least one Nebula managed security gateway installed in your network.	
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.
Top devices by usage	
#	This shows the index number of the Nebula device.
Name	This shows the descriptive name of the Nebula device.
Model	This shows the model number of the Nebula device.
Usage	This shows the amount of data 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.

Table 30 Site-Wide > Monitor > Summary Report (continued)

LABEL	DESCRIPTION
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.

5.2 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.

5.2.1 General Settings

Use this screen to change the general settings for the site, such as the site name, device login password and firmware upgrade schedule. Click **Site-Wide > Configure > General Settings** to access this screen.

Figure 40 Site-Wide > Configure > General settings

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

General settings

Site information

Site name: ✕*

Local time zone: ✕

Device configuration

Local credentials

Username:

Password: ✕*

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

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

Captive portal reauthentication

For my AD server users:

For my RADIUS server users:

For click-to-continue users:

For cloud authentication users: ⓘ

SNMP

SNMP access:

Reporting

Syslog server:

AP traffic log ⓘ **Beta** ☐

Voucher settings **Beta**

See [Using Vouchers](#) for more information

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

Access text: ✕ This text will precede the voucher code on the printed voucher

Show image: ☐

Promotion text: ✕ Optional (Maximum is 64 character)

Promotion URL: ✕ Optional (Maximum is 64 character)

Voucher image:

No logo

[Upload a logo](#)

API access ⓘ


API token:

The following table describes the labels in this screen.

Table 31 Site-Wide > Configure > General settings

LABEL	DESCRIPTION
Site Information	
Site name	Enter a descriptive name for the site.
Local time zone	Choose the time zone of the site's location.
Device configuration	
Local credentials	The default password is generated automatically by the NCC when the site is created. You can specify a new password to access the status page of the device's built-in web-based configurator. The settings here apply to all Nebula devices in this site.
Smart guest/ VLAN network	<p>Click On to enable this feature. This allows the NCC to check if the VLAN ID and guest network settings are consistent on the APs and security gateway in the same site to ensure guest network connectivity.</p> <p>The guest settings you configure for a gateway interface (in Security Gateway > Configure > Interfaces addressing) will also apply to the wireless networks (SSIDs) associated with the same VLAN ID (in AP > Configure > SSID overview). For example, if you set a gateway interface in VLAN 100 as a guest interface, the SSID that belongs to VLAN 100 will also act as a guest network.</p>
Captive portal reauthentication	
For my AD server users	Select how often the user (authenticated by an AD server) has to log in again.
For my RADIUS server users	Select how often the user (authenticated by 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 V1/V2c to allow SNMP managers using SNMP to access the devices in this site. Otherwise, select Disable .
SNMP community string	<p>This field is available when you select V1/V2c.</p> <p>Enter the password for the incoming SNMP requests from the management station.</p>
Reporting	
Syslog server	Click Add to create a new entry.
Server IP	Enter the IP address of the server.
Types	<p>Select the type of logs the server is for.</p> <p>Note: Besides sending Gateway traffic log to a syslog server, you can also set the security gateway (via its web configurator) to save a copy of the logs to a connected USB storage device. Gateway traffic log includes the traffic information (such as its source, destination or usage) of the gateway clients.</p>
Action	Click the Delete icon to remove the entry.
AP traffic log	<p>Log traffic for APs in the site that have NAT Mode set to Use Zyxel DHCP & NAT. You can also send the logs to a syslog server, by selecting AP traffic log under Syslog server > Types.</p> <p>For details on configuring NAT Mode, see Section 8.3.2 on page 228.</p>

Table 31 Site-Wide > Configure > General settings (continued)

LABEL	DESCRIPTION
Voucher settings	<p>Use these settings to configure how WiFi network authentication vouchers for this site look when printed.</p> <div data-bbox="527 317 1089 737">  </div> <p>For more information on vouchers, see Section 5.1.4 on page 81.</p>
Duration test	Sets the text that proceeds the duration on the voucher. The text must consist of 1–16 characters.
Access text	Sets the text that proceeds the access code on the voucher. The text must consist of 1–16 characters.
Show image	Sets whether to display an image at the top-left of the voucher. This image is optional.
Promotion text	Sets the promotional text on the voucher. This text is optional. The text must consist of 1–16 characters.
Promotion URL	Sets the promotional URL on the voucher. This URL is optional. The URL is displayed as a QR Code on the voucher.
Voucher image	This shows the uploaded image that will be displayed at the top-left of the voucher.
Upload a logo	Click this button to upload an image from your local computer.
Replace this logo	Click this button to change the uploaded image.
Remove this logo	Click this button to delete the uploaded image.
API access	API access allows third-party software to integrate with the DPPSK feature in NCC. For more information, please contact Zyxel.
Generate	Click this button to create a new API key.
Copy	Click this button to copy the API key to the system's clipboard.
Delete	Click this button to delete the API key.

5.2.2 Alert Settings

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 Settings** to access this screen.

Note: NCC's Smart Alert Engine uses knowledge of network topology and cross-device functionality to only generate alerts for unexpected events. This helps avoid unnecessary emails and notifications.

For example, an AP is receiving power from a PoE switch. If the AP loses power because its Ethernet cable is disconnected, NCC generates an alert. If the AP loses power because the switch has a PoE schedule that disables power to the AP, NCC does not generate an alert.

Figure 41 Site-Wide > Configure > Alert settings

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

Alert settings

Send alerts via email to

All site administrators ☐ off

Custom email addresses

Alert types

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

The following table describes the labels in this screen.

Table 32 Site-Wide > Configure > Alert settings

LABEL	DESCRIPTION
Send alerts via email to	
All site administrators	Click On 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 (Email) and/or have the Zyxel Nebula Mobile app send notifications (In-app push notifications) when the event occurs.</p> <p>If you select In-app push notifications, 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>

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

LABEL	DESCRIPTION
Switch alerts	<p>Select the check box to have the NCC generate and send an alert by email (Email) and/or have the Zyxel Nebula Mobile app send notifications (In-app push notifications) when the event occurs.</p> <p>If you select In-app push notifications, 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 (Email) and/or have the Zyxel Nebula Mobile app send notifications (In-app push notifications) when the event occurs.</p> <p>If you select In-app push notifications, 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.

5.2.3 Add Devices

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

Note: You have to contact Zyxel customer support if you need to change the device owner at myZyxel or remove an Organization from the NCC. Please configure your device owners and organizations carefully. See also [Section 4.3.3 on page 48](#).

Figure 42 Site-Wide > Configure > Add devices

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

Add devices

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

[Add to this site](#) (1) selected in (2) devices. [+ Register](#)

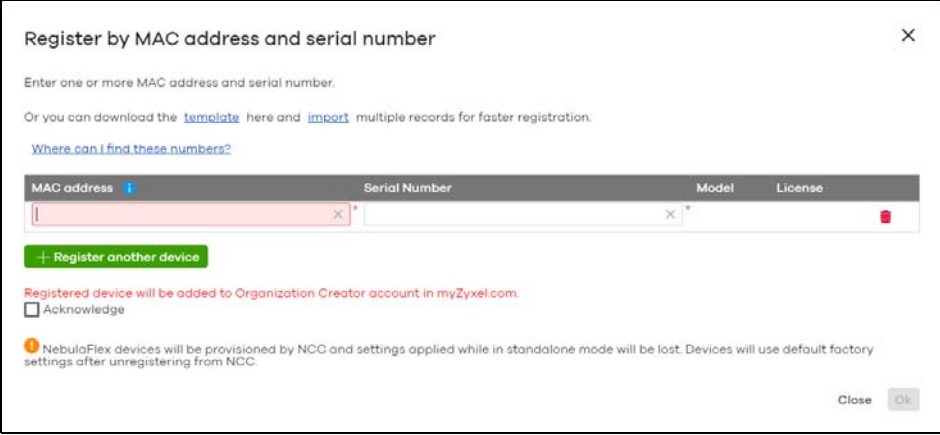
	Device name	Serial number	MAC Address	Model
<input checked="" type="checkbox"/>	NSG50-000000000000	000000000000	000000000000	NSG50
<input type="checkbox"/>	NSG50-000000000000	000000000000	000000000000	NSG50

The following table describes the labels in this screen.

Table 33 Site-Wide > Configure > Add devices

LABEL	DESCRIPTION
Add to this site	Click this button to assign the selected device(s) to the site.
device	This shows the number of registered devices which have not been assigned to a site.

Table 33 Site-Wide > Configure > Add devices (continued)

LABEL	DESCRIPTION
+ 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 template in the pop-up window to download the template (an example Excel file), add device information in the Excel file, and then click import to register multiple devices quickly by importing the Excel file.</p> 
	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.

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

Figure 43 Site-Wide > Configure > Firmware management

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

Firmware management


Upgrade time Monday 2am [What is this?](#)

 All APs

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

☐ 2020-06-09 00:00 UTC+8.0


☐ Upgrade now

 All Switches

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

☐ 2020-06-09 00:00 UTC+8.0

☐ Upgrade now

 Security Gateway

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

Status Any Device type Any Tag Any Model Any Current version Any Firmware status Any Locked Any

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

Status	Device t...	Model	MAC	S/N	Current...	Firmwa...	Upgrade sc...
<input type="checkbox"/> ●	Security g...	NSG200	88-07-14-0F...	2017061708...	V1.33(ABL...	Up to date	No
<input type="checkbox"/> ●	Switch	NSW100-10	88-07-14-0F...	2017061708...	V3.00(AB...	Upgrade a...	Follow upgrade
<input type="checkbox"/> ●	Access poi...	NAP102	88-07-14-0F...	2017061708...	V6.00(AB...	Custom	Follow upgrade

The following table describes the labels in this screen.


Table 34 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 Site-Wide > Configure > General setting screen after you click Save .
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 On to enable the schedule. The changes you make here also apply to the Site-Wide > Configure > General setting screen after you click Save .
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 On to enable the schedule. The changes you make here also apply to the Site-Wide > Configure > General setting screen after you click Save .

Table 34 Site-Wide > Configure > Firmware management (continued)

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

Table 34 Site-Wide > Configure > Firmware management (continued)

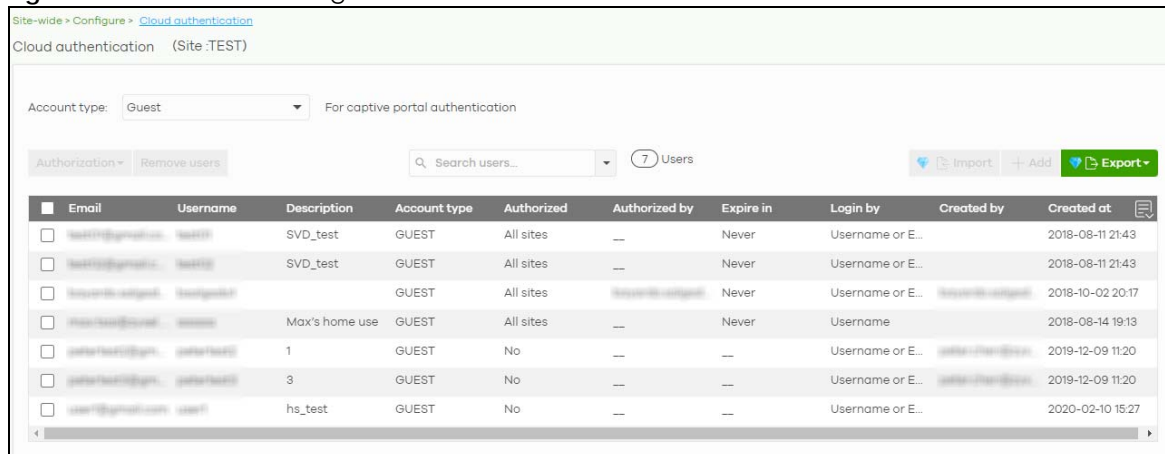
LABEL	DESCRIPTION
Current version	This shows the version number of the firmware the device is currently running. It shows N/A when the device goes off-line and its firmware version is not available.
Firmware status	This shows whether the firmware on the device is Up to date , there is firmware update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

5.2.5 Cloud Authentication

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

The changes you made in this screen apply only to the selected site. To change the cloud authentication settings for all sites in the organization, go to **Organization > Configure > Cloud Authentication** (see [Section 4.3.6 on page 59](#)).

Figure 44 Site-Wide > Configure > Cloud Authentication



Site-wide > Configure > Cloud authentication

Cloud authentication (Site:TEST)

Account type: **Guest** For captive portal authentication

Authorization Remove users Search users... 7 Users Import Add Export

Email	Username	Description	Account type	Authorized	Authorized by	Expire in	Login by	Created by	Created at
<input type="checkbox"/> test1@gmail.com	test1	SVD_test	GUEST	All sites	---	Never	Username or E...		2018-08-11 21:43
<input type="checkbox"/> test2@gmail.com	test2	SVD_test	GUEST	All sites	---	Never	Username or E...		2018-08-11 21:43
<input type="checkbox"/> test3@gmail.com	test3		GUEST	All sites	test3@gmail.com	Never	Username or E...	test3@gmail.com	2018-10-02 20:17
<input type="checkbox"/> test4@gmail.com	test4	Max's home use	GUEST	All sites	---	Never	Username		2018-08-14 19:13
<input type="checkbox"/> test5@gmail.com	test5	1	GUEST	No	---	---	Username or E...	test5@gmail.com	2019-12-09 11:20
<input type="checkbox"/> test6@gmail.com	test6	3	GUEST	No	---	---	Username or E...	test6@gmail.com	2019-12-09 11:20
<input type="checkbox"/> test7@gmail.com	test7	hs_test	GUEST	No	---	---	Username or E...		2020-02-10 15:27

The following table describes the labels in this screen.

Table 35 Site-Wide > Configure > Cloud Authentication

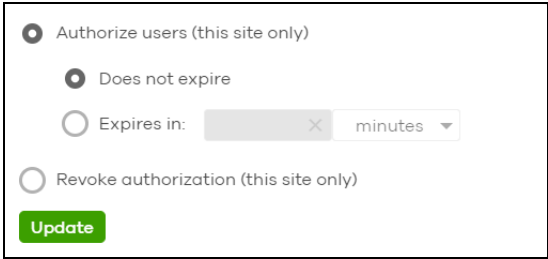
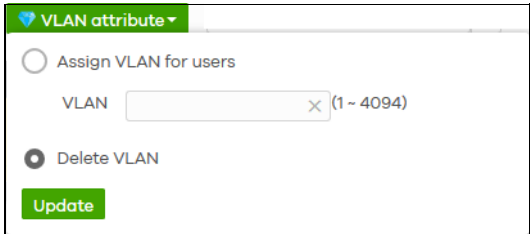
LABEL	DESCRIPTION
Account Type	<p>Select the type of user accounts that you want to view, manage or create.</p> <p>Guest - A user that can gain access to the networks via the captive portal.</p> <p>User - A user that can gain access to the networks by authenticating with a RADIUS server via the IEEE 802.1x or WPA2 authentication method or the captive portal.</p> <p>VPN User - A L2TP VPN client that can gain access to the networks by authenticating with the Nebula cloud authentication server.</p> <p>MAC - A user that can gain access to the networks by authenticating with a RADIUS server via the MAC-based authentication method.</p> <p>DPPSK (Dynamic Personal Pre-Shared Key) - A user that can gain access to the networks by connecting to an SSID using a unique key that is linked to their user account. For details, see Section 8.3.2 on page 228.</p>
Authorization	<p>This button is available only when your administrator account has full access or Guest Ambassador access to the site and at least one of the selected accounts is not granted access to all sites in 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) in this site.</p> <p>If you authorize the user's access to the network, it shows Yes in the Authorized field.</p> <p>If you cancel access authorization for the selected account(s), it shows No in the Authorized field. The account will not be able to access this site, but can still access other sites to which the user access is authorized.</p> 
Remove users	<p>This button is available only when your administrator account has full access to the site.</p> <p>Click this button to remove the selected user accounts. The following limitations apply:</p> <ul style="list-style-type: none"> The accounts must be one of the following types: Guest, User, MAC Address, VPN User, DPPSK. The user account must not be added to any other site.
VLAN attribute	<p>This field is available only when the account type is set to User.</p> <p>Assign a VLAN ID for all user account(s) or remove the VLAN ID. Then click Update.</p> 
Search	<p>Enter a key word as the filter criteria to filter the list of user accounts.</p>

Table 35 Site-Wide > Configure > Cloud Authentication (continued)

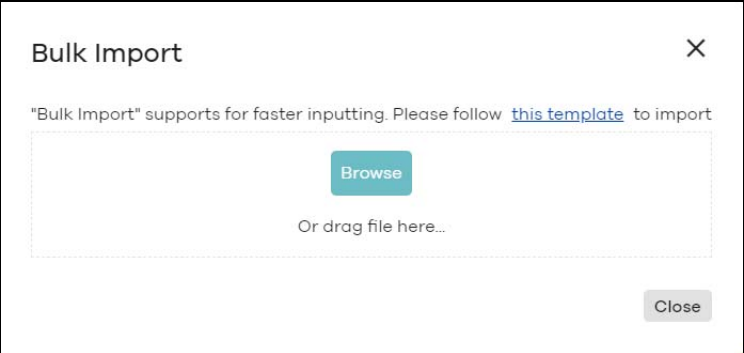

LABEL	DESCRIPTION
Users	This shows how many user accounts of the selected type displayed in the list and how many user accounts match the filter criteria.
Import	<p>Click this button to create user accounts in bulk by importing a complete list of all new users in an Excel file.</p>  <p>The dialog box titled "Bulk Import" has a close button (X) in the top right. It contains the text: "Bulk Import" supports for faster inputting. Please follow this template to import. Below this is a dashed box containing a "Browse" button. Below the dashed box is the text "Or drag file here...". In the bottom right corner is a "Close" button.</p>
Add	<p>Click this button to create a new user account. See Section 4.3.6.1 on page 62.</p> <p>Note: If Account type is set to DPPSK, then clicking Add gives you a choice to add one account or multiple accounts. For details on adding one account, see Section 4.3.6.1 on page 62. For details on adding multiple accounts (batch create), see Section 4.3.6.2 on page 64.</p> <p>To remove a user account, you need to go to Organization > Configure > Cloud Authentication (see Section 4.3.6 on page 59).</p>
Export	Click this button to save the account list as a CSV or XML file to your computer.
Email	<p>This field is available only when the account type is set to User, Guest or VPN User.</p> <p>This shows the email address of the user account.</p>
Username	<p>This field is available only when the account type is set to User, Guest or VPN User.</p> <p>This shows the user name of the user account.</p>
Description	This shows the descriptive name of the user account.
MAC address	<p>This field is available only when the account type is set to MAC.</p> <p>This shows the MAC address of the user account.</p>
Account type	This shows the type of the user account.
Authorized	<p>This shows whether the user's access to this site has been authorized or not.</p> <p>It shows All sites if the user account is granted access to all sites in the organization. To change the user's cloud authentication setting, go to Organization > Configure > Cloud Authentication (see Section 4.3.6 on page 59).</p>
Authorized by	This shows the email address of the administrator account that authorized the user.
Expire in	<p>This shows the date and time that the account expires.</p> <p>This shows - if authentication is disabled for this account.</p> <p>This shows Never if the account never expires.</p>
Login by	<p>This field is available only when the account type is set to User, Guest or VPN User.</p> <p>This shows whether the user needs to log in with the email address and/or user name.</p>
Created by	This shows the email address of the administrator account that created the user.
Created at	This shows the date and time that the account was created.

Table 35 Site-Wide > Configure > Cloud Authentication (continued)

LABEL	DESCRIPTION
VLAN assignment	This field is available only when the account type is set to User . This shows the VLAN assigned to the user.
	Click this icon to display a greater or lesser number of configuration fields.

CHAPTER 6

Security Gateway

6.1 Overview

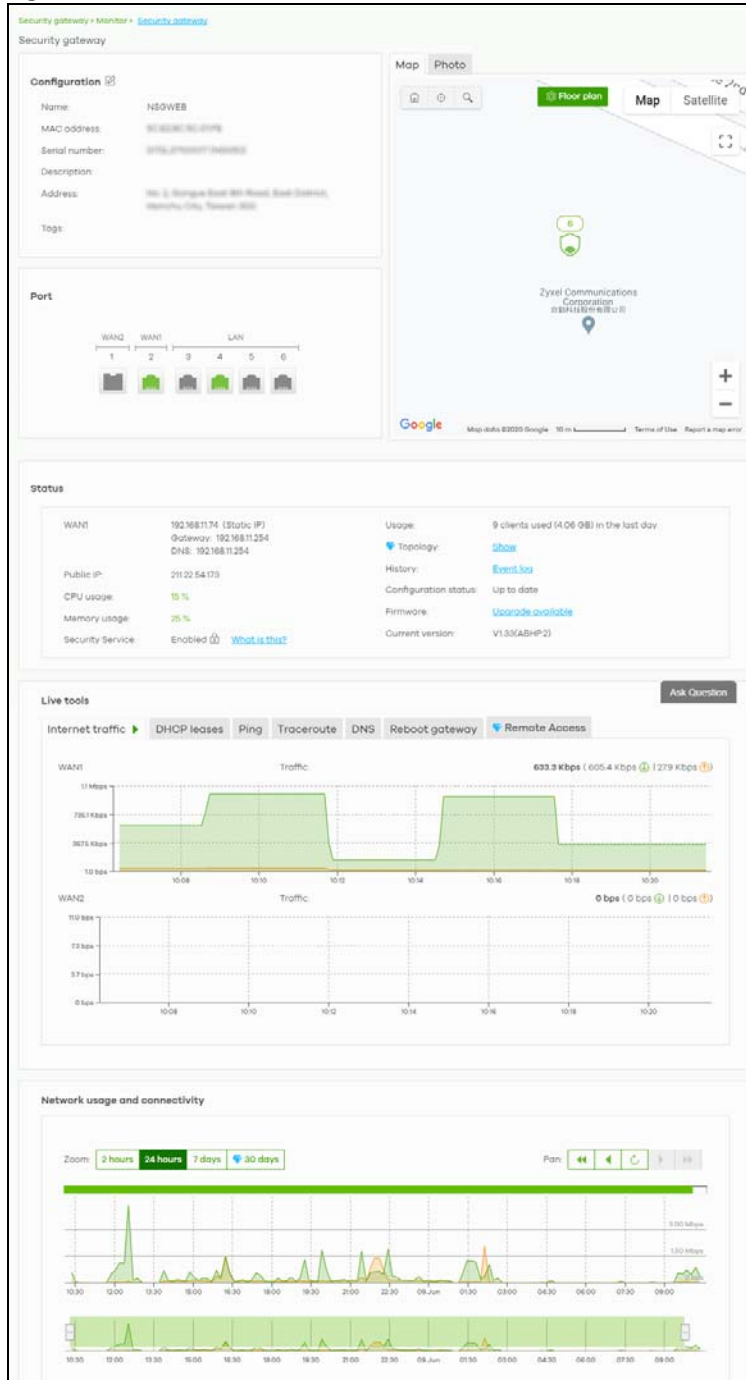
This chapter discusses the menus that you can use to monitor the Nebula managed security gateways in your network and configure settings even before a gateway is deployed and added to the site.

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 **Security Gateway > Monitor > Security Gateway** to access this screen.

Figure 45 Security Gateway > Monitor > Security Gateway

The following table describes the labels in this screen.

Table 36 Security Gateway > Monitor > Security Gateway

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

Table 36 Security Gateway > Monitor > Security Gateway (continued)

LABEL	DESCRIPTION
MAC address	This shows the MAC address of the gateway.
Serial number	This shows the serial number of the gateway.
Description	This shows the user-specified description for the gateway.
Address	This shows the user-specified address for the gateway.
Tags	This shows the user-specified tag for the gateway.
Port	<p>This shows the ports on the gateway.</p> <p>The port is highlighted in green color when it is connected and the link is up.</p> <p>Move the pointer over a port to see additional port information, such as its name, MAC address, type, and connection speed.</p>
Name	This shows the descriptive name of the port.
Status	This shows the connection status of the port.
MAC address	This shows the MAC address of the port.
Speed	This shows the current connection speed of the port. If the speed is unavailable, this displays "Ethernet".
LLDP	This shows the LLDP information received on the port.
Map	This shows the location of the gateway on the Google map.
Photo	This shows the photo of the gateway. Click Add to upload one or more photos. Click x to remove a photo.
Status	
WAN1/WAN2	This shows the IP address, gateway, DNS, and VLAN ID information for the active WAN connection.
Public IP	This shows the global (WAN) IP address of the 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:	<p>This shows whether Nebula Security Services (NSS) are enabled on the gateway. Click What is this? to view the type of enabled security services.</p> <p>When the gateway's NSS license expires, NSS is automatically disabled. This field displays an edit button which you can use to re-enable the services after renewing the NSS license.</p>
Usage	This shows the amount of data that has been transmitted or received by the gateway's clients.
Topology	Click Show to go to the Site-Wide > Monitor > Topology screen. See Section 5.1.3 on page 80 .
History	Click Event log to go to the Gateway > Monitor > Event log screen.
Configuration status	This shows whether the configuration on the gateway is up-to-date.
Firmware	This shows whether the firmware installed on the gateway is up-to-date.
Current version	This shows the firmware version currently installed on the device.
Live tools	
Internet traffic	<p>This shows the WAN port statistics.</p> <p>The y-axis represents the transmission rate in Kbps (kilobits per second).</p> <p>The x-axis shows the time period over which the traffic flow occurred.</p>
DHCP leases	This shows the IP addresses currently assigned to DHCP clients.
Ping	Enter the host name or IP address of a computer that you want to perform ping in order to test a connection and click Ping . You can select the interface through which the gateway sends queries for ping.

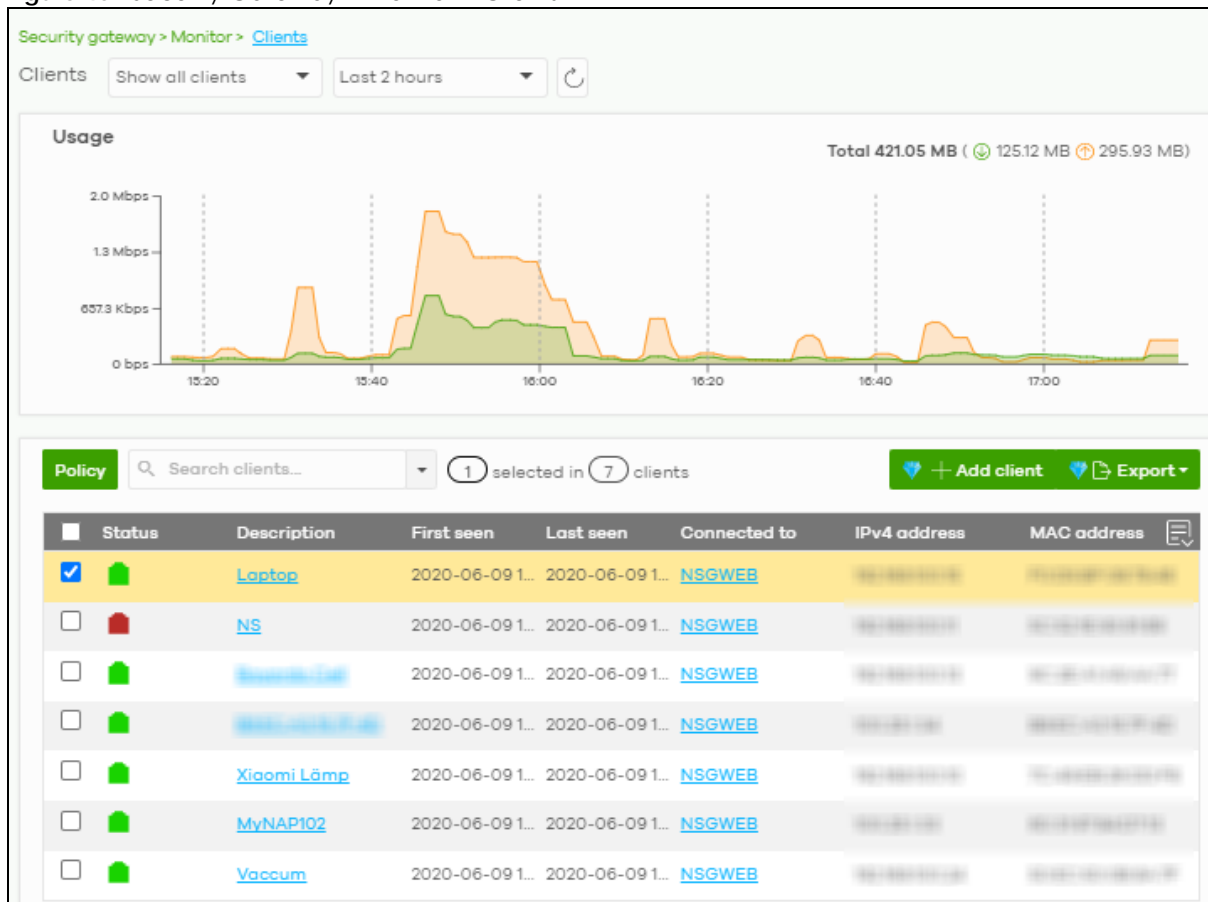
Table 36 Security Gateway > Monitor > Security Gateway (continued)

LABEL	DESCRIPTION
Traceroute	Enter the host name or IP address of a computer that you want to perform the traceroute function. This determines the path a packet takes to the specified computer.
DNS	Enter a host name and click Run to resolve the IP address for the specified domain name.
Reboot gateway	Click the Reboot button to restart the gateway.
Remote Access	This option is available only for the device owner. Establish a remote connection by specifying the Port number and clicking Establish .
Network usage and connectivity	
Move the cursor over the chart to see the transmission rate at a specific time.	
Zoom	Select to view the statistics in the past 2 hours, day, week, or month.
Pan	Click to move backward or forward by one day or week.

6.2.2 Clients

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

Figure 46 Security Gateway > Monitor > Clients



The following table describes the labels in this screen.

Table 37 Security Gateway > Monitor > Clients



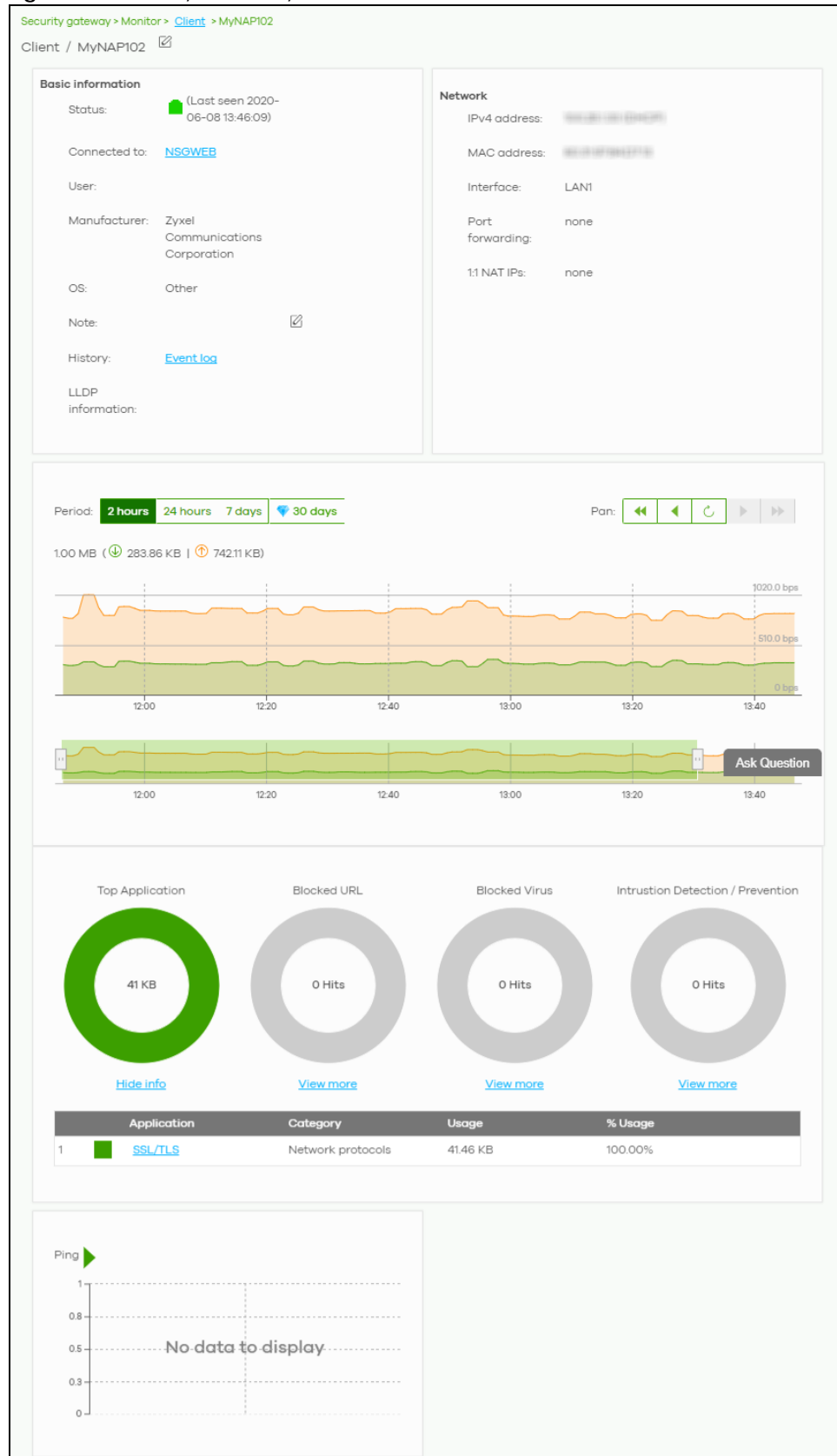
LABEL	DESCRIPTION
Clients	<p>Select to view the device information and connection status in the past two hours, day, week or month.</p> <ul style="list-style-type: none"> Select Show all clients to show clients that have been online during the selected time period. Select Show policy clients to show clients that have a whitelisted or blocked policy applied to them, regardless of when they were last online. The client's usage data is calculated according to the selected time period.
	Click this button to reload the data-related frames on this page.
Usage	<p>Move the cursor over the chart to see the transmission rate at a specific time.</p>
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	<p>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 Whitelisted. Otherwise, choose Normal and click Apply policy.</p> <div data-bbox="496 835 899 1050"> <p>Apply policy to 1 selected clients</p> <p><input checked="" type="radio"/> Normal</p> <p><input type="radio"/> Whitelisted Bypass Captive portal</p> <p>Apply policy</p> </div>
Search	Specify your desired filter criteria to filter the list of clients.
clients	This shows the number of clients connected to the gateway in the site network.
Add client	Click this button to open a window where you can specify a client's name and IP address to apply a policy before it is connected to the gateway's network.
Export	Click this button to save the client list as a CSV or XML file to your computer.
Status	<p>This shows whether the client is online (green) or offline (red), and whether the client is wired or wireless.</p> <p>Note: If a wireless client is connected to an access point that is connected to the gateway using Ethernet, then the clients will appear as wired.</p>
Description	<p>This shows the descriptive name of the client.</p> <p>Click the name to display the individual client statistics. See Section 6.2.2.1 on page 105.</p>
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	<p>This shows the name of the Nebula device to which the client is connected in this site.</p> <p>Click the device name to display the screen where you can view detailed information about the Nebula device.</p>
IPv4 address	This shows the IP address of the client.
MAC address	<p>This shows the MAC address of the client.</p> <p>Click the MAC address to display the individual client statistics. See Section 6.2.2.1 on page 105.</p>
OS	This shows the operating system running on the client device.
Manufacturer	This shows the manufacturer of the client device.

Table 37 Security Gateway > Monitor > Clients (continued)

LABEL	DESCRIPTION
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.
Download	This shows the amount of data (in bytes) received by the client since it was last connected.
Upload	This shows the amount of data (in bytes) transmitted from the client since it was last connected.
LLDP	This shows the LLDP (Link Layer Discovery Protocol) information received from 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 **Security Gateway > Monitor > Clients** screen to display individual client statistics.

Figure 47 Security Gateway > Monitor > Clients: Client Details

The following table describes the labels in this screen.

Table 38 Security Gateway > Monitor > Clients: Client Details

LABEL	DESCRIPTION
Client	Click the edit icon to change the client name.
Status	This shows whether the client is online (green) or offline (red). It also shows the last date and time the client was discovered, and whether the client is wired or wireless.
Connected to	This shows the name of the gateway to which the client is connected.
User	This shows the number of users currently connected to the network through the client device.
Manufacturer	This shows the manufacturer of the client device.
OS	This shows the operating system running on the client device, if known.
Note	Enter information about this device, for yourself or for other administrators.
History	Click Event log to go to the Security Gateway > Monitor > Event log screen.
LLDP information	This shows the LLDP (Link Layer Discovery Protocol) information received from the remote device.
Network	
IPv4 address	This shows the 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.
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).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Top Application	<p>A donut chart shows the percentage of usage for each application used by the client, if any. The number in the center of the donut chart indicates the amount of the application's traffic which has been transmitted or received by the client.</p> <p>Click View More to display the application statistics. Click Hide Info to hide them.</p>
Application	This shows the name of the application. Click an application name to view information about the clients who used the application. See Section 6.2.5 on page 111 .
Category	This shows the name of the category to which the application belongs.
Usage	This shows the total amount of data consumed by the application used by the client.
% Usage	This shows the percentage of usage for the application used by the client.
Blocked URL	<p>A donut chart shows the percentage of the hit counts for the web page visited by the client, if any. The number in the center of the donut chart indicates the number of hits on web pages that the gateway's content filter service has blocked.</p> <p>Click View More to display the content filtering statistics. Click Hide Info to hide them.</p>
Website	This shows the URL of the web page to which the gateway blocked access. Click a website URL to view information about the clients who tried to access the web page. See Section 6.2.5 on page 111 .
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 the client.
% Hits	This shows the percentage of the hit counts for the web page visited by the client.

Table 38 Security Gateway > Monitor > Clients: Client Details (continued)

LABEL	DESCRIPTION
Blocked Virus	A donut chart shows the percentage of the hit counts for the virus sent by the client, if any. The number in the center of the donut chart indicates the total number of viruses that the gateway has detected. Click View More to display the content filtering statistics. Click Hide Info to hide them.
Virus Name	This shows the name of the virus that the gateway has detected and blocked. Click a virus name to view information about the clients who sent the virus. See Section 6.2.5 on page 111 .
Hits	This shows how many times the gateway has detected the virus sent by the client.
% Hits	This shows the percentage of the hit counts for the virus sent by the client.
Intrusion Detection / Prevention	A donut chart shows the number of potential network attacks detected by the Intrusion Detection and Prevention (IDP) service, if any. The number in the center of the donut chart indicates the number of network attacks blocked by the IDP service. Click View More to display the IDP statistics. Click Hide Info to hide them.
Hits	This shows the total number of network attacks blocked by the IDP service
% Hits	This shows the number of network attacks blocked as a percentage of the total number of network requests scanned by the IDP service.
Ping	Click the button to ping the client's IP address from the gateway to test connectivity.

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 a time range to display only the log messages that match these criteria.

Select **Range** to set a time range or select **Before** to choose a specific date/time and the number of hours/minutes to display only the log messages generated within a certain period of time (before the specified date/time). Then click **Search** to update the list of logs based on the search criteria. The maximum allowable time range is 30 days.

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

Figure 48 Gateway > Monitor > Event log

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

Event log

Keyword: X

Category:

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

< Newer Older > 338 Event log Export

Time	Category	Source	Destination	Detail
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	ISAKMP SA [S201711070315] is disconnected
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	The cookie pair is : 0xa8c4726c50064617 / 0x6f8f4...
2019-10-29 09:56:53	VPN	61.216.142.42	192.168.11.74	Recv:[NOTIFY:NO_PROPOSAL_CHOSEN]
2019-10-29 09:56:53	VPN	61.216.142.42	192.168.11.74	The cookie pair is : 0x6f8f47eb7aac5173 / 0xa8c472...
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	Send:[SA][VID][VID][VID][VID][VID][VID][VID][...
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	Send Main Mode request to [61.216.142.42]
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	Tunnel [S201711070315] Sending IKE request
2019-10-29 09:56:53	VPN	192.168.11.74	61.216.142.42	The cookie pair is : 0xa8c4726c50064617 / 0x0000...
2019-10-29 09:58:18	VPN	192.168.11.74	61.216.142.42	ISAKMP SA [S201711070315] is disconnected
2019-10-29 09:58:18	VPN	192.168.11.74	61.216.142.42	The cookie pair is : 0x2d752e6167623ee9 / 0x5370b...

Page 1 of 34 Results per page: 10

6.2.4 VPN Connections


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

Note: If the peer gateway is not a Nebula device, go to the **Security Gateway > Configure > Site-to-Site VPN** screen to view and configure a VPN rule. See [Section 6.3.6 on page 143](#) for more information.

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

Figure 49 Security Gateway > Monitor > VPN Connections

Security gateway > Monitor > [VPN connections](#)

VPN connections 

Connection status

Configuration: This security gateway is exporting 1 subnet over the VPN: 100.251.0/24

NAT type: Manual. This security gateway has a publicly accessible IP address and is using 211.22.54.173 as a contact point.

Site connectivity

Location	Subnet(s)	Status	Inbound(Bytes)	Outbound(Bytes)	Tunnel up time	Last heartbeat
Hub	10.0.1.0/24 172.16.0.0/12 10.251.0.0/16 10.253.0.0/16	disconnected	0 bytes	0 bytes	-	-
Site25_NCC_AE_B...	-	-	0 bytes	0 bytes	-	-

Client to site VPN login account

User Name	Hostname	Assigned IP	Public IP

The following table describes the labels in this screen.

Table 39 Security Gateway > Monitor > VPN Connections


LABEL	DESCRIPTION
	Click this button to reload the data-related frames on this page.
Connection Status	
Configuration	This shows the number and address of the local 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 Security Gateway > Configure > Site-to-Site VPN 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.
Client to site VPN login account	
User Name	This shows the remote user's login account name.
Hostname	This shows the name of the computer that has this L2TP VPN connection with the gateway.

Table 39 Security Gateway > Monitor > VPN Connections (continued)

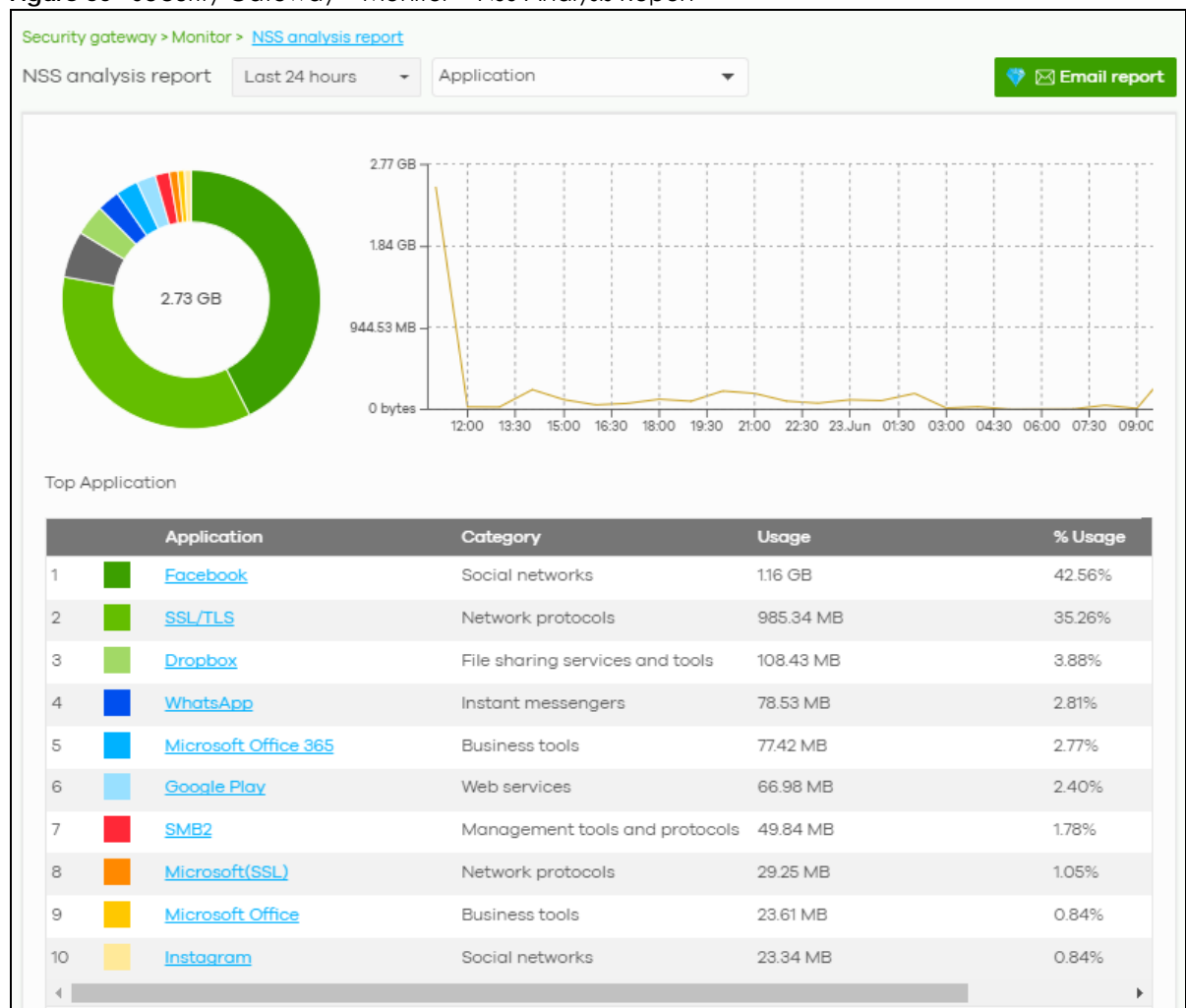
LABEL	DESCRIPTION
Assigned IP	This shows the IP address that the gateway assigned for the remote user's computer to use within the L2TP VPN tunnel.
Public IP	This shows the public IP address that the remote user is using to connect to the Internet.

6.2.5 NSS Analysis Report

Use this screen to view the statistics report for NSS (Nebula Security Service), such as content filtering, Intrusion Detection and Prevention (IDP), application patrol, and anti-virus. The screen varies depending on the service type (**Application**, **Content Filtering**, or **Anti-Virus**) you select.

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

Figure 50 Security Gateway > Monitor > NSS Analysis Report



The following table describes the labels in this screen.

Table 40 Security Gateway > Monitor > NSS Analysis Report

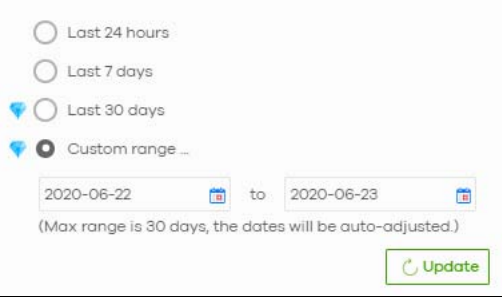
LABEL	DESCRIPTION
Security Gateway - NSS Analysis	<p>Select to view the report for the past day, week or month. Alternatively, select Custom range... to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
	Select the type of service for which you want to view the statistics report.
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
Application	<p>The following fields displays when you select to view the application statistics. Click an application name to view information about the clients who use that application. Click Top Application under the chart to switch back to the previous screen.</p>
y-axis	The y-axis shows the amount of the application's traffic which has been transmitted or received.
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Application	This shows the name of the application. Click an application name to view the IPv4 addresses of the clients who used the application.
Description	<p>This shows the name of the client who used the application.</p> <p>This field is available when you click the application name. Click the name to display the individual client statistics. See Section 6.2.2.1 on page 105.</p>
IPv4 Address	<p>This shows the IPv4 address of the client who used the application.</p> <p>This field is available when you click the application name.</p>
MAC Address	<p>This shows the MAC address of the client who used the application.</p> <p>This field is available when you click the application name.</p>
Category	This shows the name of the category to which the application belongs.
Usage	This shows the total amount of data consumed by the application used by all or a specific IPv4 address.
% Usage	This shows the percentage of usage for the application used by all or a specific IPv4 address.
Content Filtering	<p>The following fields displays when you select to view the content filtering statistics. Click a website URL to view information about the clients who tried to access that web page. Click Content Filtering under the chart to switch back to the previous screen.</p>
y-axis	The y-axis shows the number of hits on web pages that the gateway's content filter service has blocked.
x-axis	The x-axis shows the time period over which the web page is checked.
Website	This shows the URL of the web page to which the gateway blocked access. Click a website URL to view the IPv4 addresses of the clients who tried to access the web page.

Table 40 Security Gateway > Monitor > NSS Analysis Report (continued)

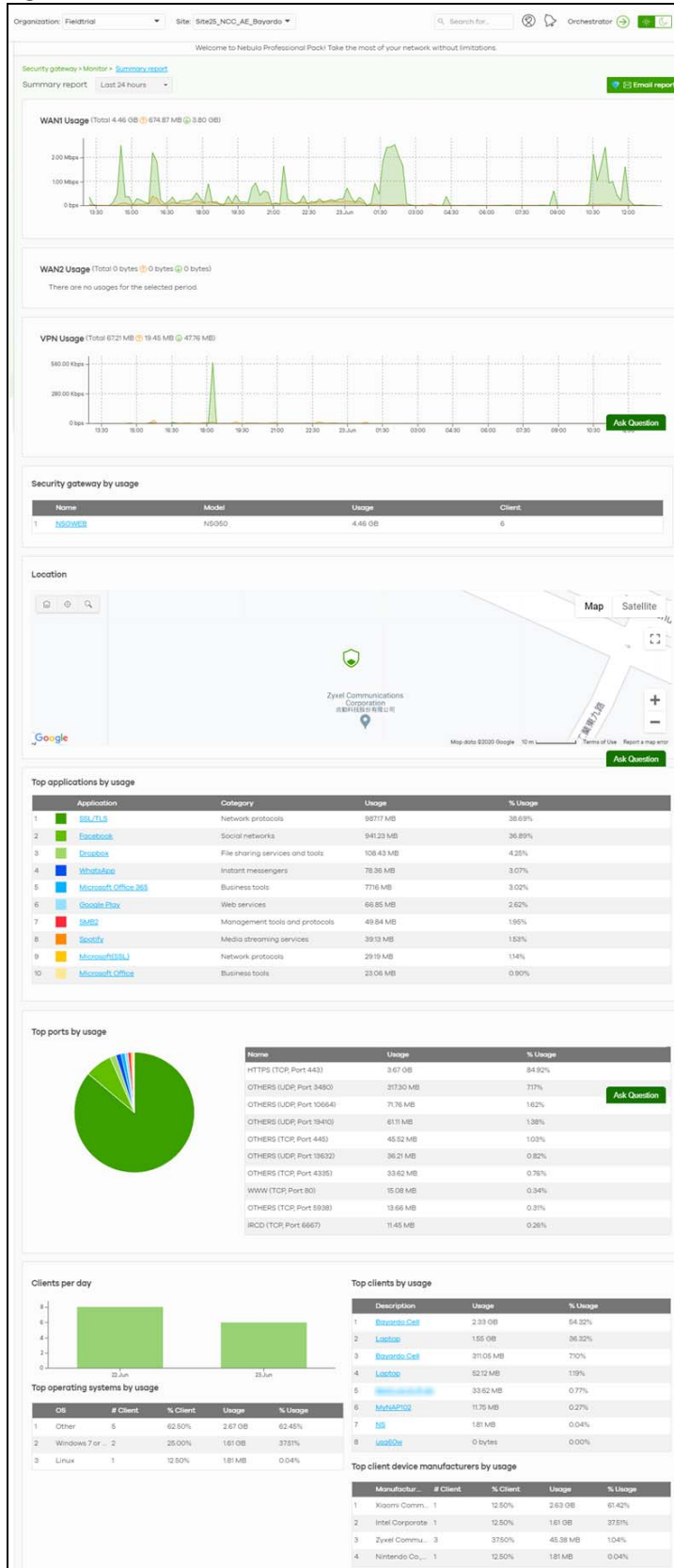
LABEL	DESCRIPTION
Description	This shows the name of the client who tried to access the web page. This field is available when you click the website URL. Click the name to display the individual client statistics. See Section 6.2.2.1 on page 105 .
IPv4 Address	This shows the IPv4 address of the client who tried to access the web page. This field is available when you click the website URL.
MAC Address	This shows the MAC address of the client who tried to access the web page. This field is available when you click the website URL.
Category	This shows the name of the category to which the web page belongs.
Hits	This shows the number of hits on the web page visited by all or a specific IPv4 address.
% Hits	This shows the percentage of the hit counts for the web page visited by all or a specific IPv4 address.
Anti-Virus The following fields are displayed when you select Anti-Virus . Click a virus name to view information about the clients who sent the virus. Click the number in the center of the donut chart or Anti-Virus under the chart to switch back to the previous screen.	
y-axis	The y-axis shows the total number of viruses that the gateway has detected.
x-axis	The x-axis shows the time period over which the virus is detected.
Virus Name	This shows the name of the virus that the gateway has detected and blocked. Click a virus name to view the IPv4 addresses of the clients who sent the virus.
Description	This shows the name of the client who sent the virus. This field is available when you click the virus name. Click the name to display the individual client statistics. See Section 6.2.2.1 on page 105 .
IPv4 Address	This shows the IPv4 address of the virus sender. This field is available when you click the virus name.
MAC Address	This shows the MAC address of the virus sender. This field is available when you click the virus name.
Hits	This shows how many times the gateway has detected the virus sent by all or a specific IPv4 address.
% Hits	This shows the percentage of the hit counts for the virus sent by all or a specific IPv4 address.
Intrusion Detection / Prevention The following fields are displayed when you select Intrusion Detection / Prevention . The donut chart shows the number of potential network attacks detected by the Intrusion Detection and Prevention (IDP) service, if any. The number in the center of the donut chart indicates the number of network attacks blocked by the IDP service.	
Signature Name	The name of the IDP signature that triggered the hit. The signature name identifies the type of intrusion pattern
Hits	This shows the total number of network attacks blocked by the IDP service
% Hits	This shows the number of network attacks blocked as a percentage of the total number of network requests scanned by the IDP service.

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 **Security Gateway > Monitor > Summary Report** to access this screen.

Figure 51 Security Gateway > Monitor > Summary Report



The following table describes the labels in this screen. Custom range...

Table 41 Security Gateway > Monitor > Summary Report

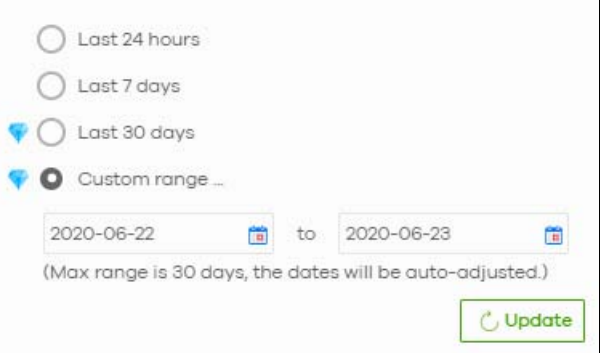
LABEL	DESCRIPTION
Security gateway - Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select Custom range... to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
WAN1/WAN2 usage	
y-axis	The y-axis shows the transmission speed of data sent or received through the WAN connection in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
VPN usage	
y-axis	The y-axis shows the transmission speed of data sent or received through the VPN tunnel in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Security gateway by usage	
	This shows the index number of the Nebula gateway.
Name	This shows the descriptive name of the Nebula gateway.
Model	This shows the model number of the Nebula gateway.
Usage	This shows the amount of data that has been transmitted through the gateway's WAN port.
Client	This shows the number of clients currently connected to the gateway.
Location	
This shows the location of the Nebula gateways on the map.	
Top applications by usage	
	This shows the index number of the application.
Application	This shows the application name.
Category	This shows the name of the category to which the application belongs.
Usage	This shows the amount of data consumed by the application.
% Usage	This shows the percentage of usage for the application.
Top ports by usage	
Name	This shows the service name and the associated port number(s).
Usage	This shows the amount of data consumed by the service.
% Usage	This shows the percentage of usage for the service.
Clients per day	

Table 41 Security Gateway > Monitor > Summary Report (continued)

LABEL	DESCRIPTION
y-axis	The y-axis represents the number of clients.
x-axis	The x-axis represents the date.
Top operating systems by usage	
	This shows the index number of the operating system.
OS	This shows the operating system of the client device.
# Client	This shows how many client devices use this operating system.
% Client	This shows the percentage of top client devices which use this operating system.
# Usage	This shows the amount of data consumed by the client device on which this operating system is running.
% Usage	This shows the percentage of usage for top client devices which use this operating system.
Top clients by usage	
	This shows the index number of the client.
Description	This shows the descriptive name or MAC address of the client.
Usage	This shows the total amount of data transmitted and received by the client.
% Usage	This shows the percentage of usage for the client.
Top client device manufacturers by usage	
	This shows the index number of the client device.
Manufacturer	This shows the manufacturer name of the client device.
Client	This shows how many client devices are made by the manufacturer.
% Client	This shows the percentage of top client devices which are made by the manufacturer.
Usage	This shows the total amount of data transmitted and received by the client device.
% Usage	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 the gateway of the selected site.

6.3.1 Interface Addressing

Use this screen to configure network mode, port grouping, interface address, static route and DDNS settings on the gateway. To access this screen, click **Security Gateway > Configure > Interface addressing**.

Note: If the gateway device of the site supports link aggregation, for example model NSG300, then the **Interface Addressing** screen changes to allow you to configure link aggregation groups. For details, see [Section 6.3.5 on page 140](#).

Figure 52 Security Gateway > Configure > Interface addressing

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

Security gateway > Configure > Interface addressing

Interface addressing

Network wide

Mode:

☒ Network address translation (NAT)
Client traffic to the Internet is modified so that it appears to have the security gateway as its source.

☐ Router
Client traffic to the Internet is by routing result, which means, the gateway will not automatically use SNAT for traffic it routes from internal interfaces to external interfaces.

Port Group Setting

	P3	P4	P5	P6
Port Group 1:	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Port Group 2:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Interface

Name	IP address	Subnet mask	VLAN ID	Port Group	Guest
LAN1	100.25.11	255.255.255.0		Port Group 1	<input type="checkbox"/>
LAN2	173.16.25.1	255.255.255.0		Port Group 2	<input checked="" type="checkbox"/>
VLAN100	192.168.100.1	255.255.255.0	100	Port Group 1	<input type="checkbox"/>
VLAN10	192.168.10.1	255.255.255.0	10	Port Group 1	<input checked="" type="checkbox"/>
VLAN250	192.168.250.1	255.255.255.0	250	Port Group 1	<input checked="" type="checkbox"/>

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

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

[+ Add](#)

Static Route

Name	Destination	Subnet mask	Next hop IP
s5	192.168.10.0	255.255.255.0	192.168.10.1

[+ Add](#)

Dynamic DNS

Automatic registration: ☒

Dynamic DNS updates a DNS record each time the public IP address of the security appliance changes.

General settings

DDNS provider:

DDNS type:

DDNS account

Username:

Password:

Confirm password:

DDNS settings

Domain name:

Primary binding address

Interface:

IP address:

Backup binding address

Interface:

IP address:

Enable wildcard: ☒

Mail exchanger: (Optional)

Backup mail exchanger: ☒

The following table describes the labels in this screen.

Table 42 Security Gateway > Configure > Interface addressing

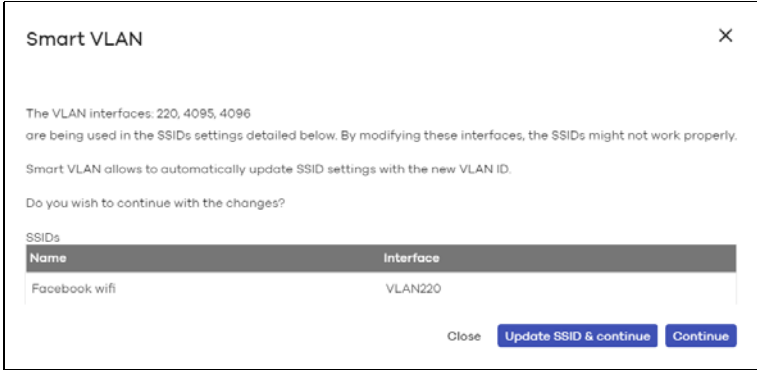
LABEL	DESCRIPTION
Network wide	
Mode	<p>Select Network address translation (NAT) to have the gateway automatically use SNAT for traffic it routes from internal interfaces to external interfaces.</p> <p>Select Router to have the gateway forward packets according to the routing policies. The gateway does not automatically convert a packet's source IP address.</p>
Port Group Setting	<p>Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.</p> <p>The physical LAN Ethernet ports are shown at the top (P3, P4, and so on) and the port groups are shown at the left of the screen. Use the radio buttons to select which ports are in each port group.</p> <p>For example, select a port's Port Group 1 radio button to use the port as part of the first port group. The port will use the first group's IP address.</p> <p>Note: You cannot select ports 1 and 2, as these ports are reserved for WAN usage.</p>
Interface	
By default, LAN1 is created on top of port group 1 and LAN2 is on top of port group 2.	
Name	This shows the name of the interface (network) on the gateway.
IP address	This shows the IP address of the interface (network).
Subnet mask	This shows the subnet mask of the interface (network).
VLAN ID	<p>This shows the ID number of the VLAN with which the interface (network) is associated.</p> <p>Note: If you have associated an SSID with the VLAN ID, the Smart VLAN screen displays after you change or delete the VLAN ID and click Save. You can exit the screen without saving, or apply your changes directly. If the Smart guest/VLAN network feature is enabled in the Site-Wide > Configure > General settings screen, you can select to apply the changes and update the SSID's VLAN setting as well.</p> 
Port group	This shows the name of the port group to which the interface (network) belongs.

Table 42 Security Gateway > Configure > Interface addressing (continued)





LABEL	DESCRIPTION
Guest	<p>Select On to configure the interface as a Guest interface. Devices connected to a Guest interface will have Internet access but cannot communicate with each other directly or access network sources behind the gateway.</p> <p>Otherwise, select Off to not use the interface as a Guest interface.</p> <p>Note: If the Smart guest/VLAN network feature is enabled in the Site-Wide > Configure > General settings screen, the guest settings you configure for an interface also apply to the wireless networks (SSIDs) associated with the same VLAN ID. For example, if you set an interface in VLAN 100 as a guest interface, the SSID that belongs to VLAN 100 will also act as a guest network.</p>
	Click this button to modify the network settings. See Section 6.3.1.1 on page 122 for detailed information.
	Click this icon to remove a VLAN entry.
Add	Click this button to create a VLAN, which is then associated with one Ethernet interface (network). See Section 6.3.1.1 on page 122 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 button to modify the static route settings. See Section 6.3.2.4 on page 132 for detailed information.
	Click this icon to remove a static route.
Add	Click this button to create a new static route. See Section 6.3.2.4 on page 132 for detailed information.
Dynamic DNS	
Automatic registration	Click On to use dynamic DNS. Otherwise, select Off to disable it.
General Settings	
DDNS provider	<p>Select your Dynamic DNS service provider from the drop-down list box.</p> <p>If you select User custom, create your own DDNS service.</p>
DDNS type	<p>Select the type of DDNS service you are using.</p> <p>Select User custom to create your own DDNS service and configure the DYNDNS Server, URL, and Additional DDNS Options fields below.</p>
DDNS account	
Username	Enter the user name used when you registered your domain name.
Password	Enter the password provided by the DDNS provider.
Confirm password	Enter the password again to confirm it.
DDNS settings	
Domain name	Enter the domain name you registered.
Primary binding address	Use these fields to set how the security gateway determines the IP address that is mapped to your domain name in the DDNS server. The security gateway uses the Backup binding address if the interface specified by these settings is not available.

Table 42 Security Gateway > Configure > Interface addressing (continued)

LABEL	DESCRIPTION
Interface	Select the interface to use for updating the IP address mapped to the domain name.
IP address	<p>Select Auto 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 Custom if you have a static IP address. Enter the IP address to use it for the domain name.</p> <p>Select Interface 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 Primary binding address settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name.
IP address	<p>Select Auto 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 Custom if you have a static IP address. Enter the IP address to use it for the domain name.</p> <p>Select Interface to have the security gateway use the IP address of the specified interface.</p>
Enable wildcard	<p>This option is only available with a DynDNS account.</p> <p>Enable the wildcard feature to alias sub-domains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.</p>
Mail exchanger	<p>This option is only available with a DynDNS account.</p> <p>DynDNS can route e-mail for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes e-mail for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger.</p> <p>If you are using this service, type the host record of your mail server here. Otherwise, leave the field blank.</p>
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 www.dyndns.org for more information about this service.</p>
DYNDNS Server	<p>This field displays when you select User custom from the DDNS provider field above.</p> <p>Type the IP address of the server that will host the DDSN service.</p>

Table 42 Security Gateway > Configure > Interface addressing (continued)

LABEL	DESCRIPTION
URL	This field displays when you select User custom from the DDNS provider field above. Type the URL that can be used to access the server that will host the DDNS service.
Additional DDNS Options	This field displays when you select User custom from the DDNS provider field above. These are the options supported at the time of writing: <ul style="list-style-type: none">• dyndns_system to specify the DYNDNS Server type - for example, dyndns@dyndns.org• ip_server_name which should be the URL to get the server's public IP address - for example, http://myip.easylife.tw/

6.3.1.1 Local LAN (Add VLAN)

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

Figure 53 Security Gateway > Configure > Interface addressing: Local LAN

Local LAN

Interface properties

Interface type: VLAN

Interface name: VLAN1

IP address assignment

IP address:

Subnet mask:

VLAN ID: 1 (1 - 4096)

Port group: LAN2

DHCP setting

DHCP: DHCP Server

IP pool start address:

Pool size: 200

First DNS server: NSG

Second DNS server: None

Third DNS server: None

First WINS server: (Optional)

Second WINS server: (Optional)

Lease time: ☐ Infinite

Close OK

The following table describes the labels in this screen.

Table 43 Security Gateway > Configure > Interface addressing: Local LAN (VLAN)

LABEL	DESCRIPTION
Interface properties	
Interface type	Select VLAN to add a virtual interface. Note: This field only appears if the gateway supports Link Aggregation Groups (LAGs). If the gateway does not support LAGs, then VLAN is the default interface type.

Table 43 Security Gateway > Configure > Interface addressing: Local LAN (VLAN) (continued)

LABEL	DESCRIPTION
Interface name	<p>This field is read-only if you are editing an existing interface.</p> <p>Specify a name for the interface.</p> <p>The format of interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (x). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.</p>
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	<p>Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)</p> <p>Note: NCC will show an error message when the VLAN ID in the NSG interface is configured to be the same as the WAN port's VLAN ID.</p>
Port group	Select the name of the port group to which you want the interface to (network) belong.
DHCP setting	
DHCP	<p>Select what type of DHCP service the security gateway provides to the network. Choices are:</p> <p>None - the security gateway does not provide any DHCP services. There is already a DHCP server on the network.</p> <p>DHCP Relay - the security gateway routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.</p> <p>DHCP Server - the security gateway assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The security gateway is the DHCP server for the network.</p>
These fields appear if the security gateway is a DHCP Relay .	
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 DHCP Server .	
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 Add new under Static DHCP Table .
Pool size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet mask . For example, if the Subnet mask is 255.255.255.0 and IP pool start address is 10.10.10.10, the 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	<p>Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses.</p> <p>Custom Defined - enter a static IP address.</p> <p>From ISP - select the DNS server that another interface received from its DHCP server.</p> <p>NSG - the DHCP clients use the IP address of this interface and the security gateway works as a DNS relay.</p>
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 43 Security Gateway > Configure > Interface addressing: Local LAN (VLAN) (continued)

LABEL	DESCRIPTION
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire days, hours, minutes - select this to enter how long IP addresses are valid.
Extended options	This table is available if you selected DHCP server . Configure this table if you want to send more information to DHCP clients through DHCP packets. Click Add new to create an entry in this table. See Section 6.3.2.3 on page 130 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 IP pool start address and Pool size . Click Add new to create an entry in this table.
IP address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry.
Close	Click Close to exit this screen without saving.
OK	Click OK to save your changes.

6.3.2 Link Aggregation Groups

A Link Aggregation Group (LAG) combines multiple Ethernet ports into a single logical interface, in order to increase network bandwidth and/or availability.

Ports in the group can all connect to a target simultaneously, combining their bandwidth. A LAG can also offer higher network availability; if any port in the group becomes disconnected, the LAG can continue sending data using another port.

6.3.2.1 Interface Addressing with Link Aggregation Groups

If the gateway of the selected site supports Link Aggregation Groups (LAGs), for example NSG300, you can create a LAG by clicking **Add**.

After you create a LAG, the **Port Group Settings** and **Interface** sections of the **Interface Addressing screen** change. The new screen layout allows you to view and configure which ports are in a LAG.

Figure 54 Security Gateway > Configure > Interface addressing (LAG Interface Type)

Security gateway > Configure > [Interface addressing](#)

Interface addressing

Network wide

Mode:

☒ Network address translation (NAT)
Client traffic to the Internet is modified so that it appears to have the security gateway as its source.

☐ Router
Client traffic to the Internet is by routing result, which means, the gateway will not automatically use SNAT for traffic it routes from internal interfaces to external interfaces.

Port Group Setting

	P3	P4	P5	P6	P7	P8
LAN1-6	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
LAG1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
LAG2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

Interface

Name	IP address	Subnet mask	VLAN ID	Port Group	Guest	
LAN1	0.0.0.0	0.0.0.0		LAN1	<input type="checkbox"/>	
LAN2	0.0.0.0	0.0.0.0		LAN2	<input type="checkbox"/>	
LAN3	0.0.0.0	0.0.0.0		LAN3	<input type="checkbox"/>	
LAN4	0.0.0.0	0.0.0.0		LAN4	<input type="checkbox"/>	
LAN5	0.0.0.0	0.0.0.0		LAN5	<input type="checkbox"/>	
LAN6	0.0.0.0	0.0.0.0		LAN6	<input type="checkbox"/>	
LAG1	192.168.1.10	255.255.255.0		LAN1	<input type="checkbox"/>	
LAG2	192.168.20.1	255.255.255.0		LAN5 LAN6	<input type="checkbox"/>	

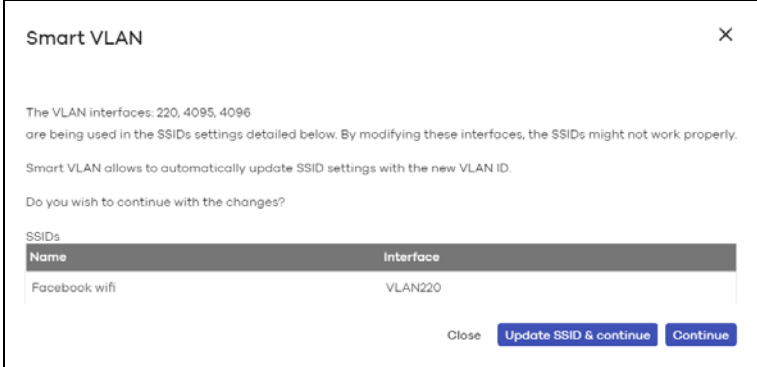


[+ Add](#)

Static Route

Table 44 Security Gateway > Configure > Interface addressing (LAG Interface Type)

LABEL	DESCRIPTION
Port Group Setting	Select which port group or Link Aggregation Group (LAG) an Ethernet port belongs to. When LAGs are enabled, NCC adds each available LAN Ethernet port (port 3 and higher) to a separate port group, named LAN1, LAN2, LAN3, and so on. These default port groups cannot be modified or renamed.
Interface	
Name	This shows the name of the interface (network) on the gateway.
IP address	This shows the IP address of the interface (network).
Subnet mask	This shows the subnet mask of the interface (network).

Table 44 Security Gateway > Configure > Interface addressing (LAG Interface Type) (continued)

LABEL	DESCRIPTION
VLAN ID	<p>This shows the ID number of the VLAN with which the interface (network) is associated.</p> <p>Note: If you have associated an SSID with the VLAN ID, the Smart VLAN screen displays after you change or delete the VLAN ID and click Save. You can exit the screen without saving, or apply your changes directly. If the Smart guest/VLAN network feature is enabled in the Site-Wide > Configure > General settings screen, you can select to apply the changes and update the SSID's VLAN setting as well.</p>  <p>The dialog box titled 'Smart VLAN' contains the following text: 'The VLAN interfaces: 220, 4095, 4096 are being used in the SSIDs settings detailed below. By modifying these interfaces, the SSIDs might not work properly. Smart VLAN allows to automatically update SSID settings with the new VLAN ID. Do you wish to continue with the changes?'. Below the text is a table with two columns: 'Name' and 'Interface'. The table has one row with 'Facebook wifi' under 'Name' and 'VLAN220' under 'Interface'. At the bottom right of the dialog are three buttons: 'Close', 'Update SSID & continue', and 'Continue'.</p>
Port group	<p>For an Ethernet port, this shows the name of the port group to which the port belongs.</p> <p>For a link aggregation group, this shows its member port groups.</p>
Guest	<p>Select On to configure the interface as a Guest interface. Devices connected to a Guest interface will have Internet access but cannot communicate with each other directly or access network sources behind the gateway.</p> <p>Otherwise, select Off to not use the interface as a Guest interface.</p> <p>Note: If the Smart guest/VLAN network feature is enabled in the Site-Wide > Configure > General settings screen, the guest settings you configure for an interface also apply to the wireless networks (SSIDs) associated with the same VLAN ID. For example, if you set an interface in VLAN 100 as a guest interface, the SSID that belongs to VLAN 100 will also act as a guest network.</p>
	<p>Click this button to modify the network settings. See Section 6.3.1.1 on page 122 for detailed information.</p> <p>If the interface is a member of a link aggregation group, you cannot edit the interface's network settings.</p>
	<p>Click this icon to delete a VLAN entry or link aggregation group.</p>
Add	<p>Click this button to create a VLAN or link aggregation group.</p> <ul style="list-style-type: none"> For details on creating a VLAN, see Section 6.3.1.1 on page 122. For details on creating a link aggregation group, see Section 6.3.2.2 on page 127.

6.3.2.2 Local LAN (LAG Interface Type)

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

Figure 55 Security Gateway > Configure > Interface addressing: Local LAN (LAG Interface Type)

Local LAN

Interface properties

Interface type: LAG

Interface name: LAG3

LAG configuration

Mode: active-backup

Link monitoring: Mii

Mii mon: 100

Updelay: 1

Downdelay: 0

IP address assignment

IP address:

Subnet mask:

Port group: LAN2

DHCP setting

DHCP: DHCP Server

IP pool start address:

First DNS server: NSG

Second DNS server:

Pool size: 200

Close OK

The following table describes the labels in this screen.

Table 45 Security Gateway > Configure > Interface addressing: Local LAN (LAG Interface Type)

LABEL	DESCRIPTION
Interface properties	
Interface type	Select LAG to add a link aggregation group. Note: This field only appears if the gateway supports Link Aggregation Groups (LAGs). If the gateway does not support LAGs, a VLAN is created by default.
Interface name	Specify a name for the interface. This must be "LAG" plus a number, for example "LAG1".
LAG Configuration	

Table 45 Security Gateway > Configure > Interface addressing: Local LAN (LAG Interface Type)

LABEL	DESCRIPTION
Mode	<p>Select a mode for this Link Aggregation Group (LAG) interface. Choices are as follows:</p> <ul style="list-style-type: none"> active-backup: Only one port in the LAG interface is active and another port becomes active only if the active port fails. 802.3ad (IEEE 802.3ad Dynamic link aggregation): Link Aggregation Control Protocol (LACP) negotiates automatic combining of ports and balances the traffic load across the LAG link by sending LACP packets to the directly connected device that also implements LACP. The ports must have the same speed and duplex settings. balance-alb (adaptive load balancing): Traffic is distributed according to the current load on each port by ARP negotiation. Incoming traffic is received by the current port. If the receiving port fails, another port takes over the MAC address of the failed receiving port.
Link Monitoring	<p>Select how each link is monitored.</p> <p>mii (Media Independent Interface) - The gateway monitors the state of the local interface only. The gateway can't tell if the link can transmit or receive packets.</p> <p>arp - The gateway monitors the link by sending ARP queries. The gateway then uses the reply to know if the link is up and that traffic is flowing through the link.</p>
Miimom	This field displays for mii Link Monitoring. Set the interval in milliseconds that the system polls the Media Independent Interface (MII) to get the link's status.
Updelay	This field displays for mii Link Monitoring. Set the waiting time in milliseconds to confirm that a member interface link is up.
Downdelay	This field displays for mii Link Monitoring. Set the waiting time in milliseconds to confirm that a member interface link is down.
IP address assignment	
IP address	Enter the IP address for this interface.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
VLAN ID	<p>Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)</p> <p>Note: NCC will show an error message when the VLAN ID in the NSG interface is configured to be the same as the WAN port's VLAN ID.</p>
Port group	Select the name of the port group to which you want the interface to (network) belong.
DHCP setting	
DHCP	<p>Select what type of DHCP service the security gateway provides to the network. Choices are:</p> <p>None - the security gateway does not provide any DHCP services. There is already a DHCP server on the network.</p> <p>DHCP Relay - the security gateway routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.</p> <p>DHCP Server - the security gateway assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The security gateway is the DHCP server for the network.</p>
These fields appear if the security gateway is a DHCP Relay .	
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 DHCP Server .	
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 Add new under Static DHCP Table .

Table 45 Security Gateway > Configure > Interface addressing: Local LAN (LAG Interface Type)

LABEL	DESCRIPTION
Pool size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet mask . For example, if the Subnet mask is 255.255.255.0 and IP pool start address is 10.10.10.10, the security gateway can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.
First DNS server Second DNS server Third DNS server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. Custom Defined - enter a static IP address. From ISP - select the DNS server that another interface received from its DHCP server. NSG - the DHCP clients use the IP address of this interface and the security gateway works as a DNS relay.
First WINS server Second WINS server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire days, hours, minutes - select this to enter how long IP addresses are valid.
Extended options	This table is available if you selected DHCP server . Configure this table if you want to send more information to DHCP clients through DHCP packets. Click Add new to create an entry in this table. See Section 6.3.2.3 on page 130 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 IP pool start address and Pool size . Click Add new to create an entry in this table.
IP address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry.
Close	Click Close to exit this screen without saving.
OK	Click OK to save your changes.

6.3.2.3 DHCP Option

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

Figure 56 Security Gateway > Configure > Interfaces addressing: Local LAN: DHCP Option

The screenshot shows a configuration window titled "DHCP Option". It includes a close button (X) in the top right corner. The form contains the following fields:

- Option:** A dropdown menu currently set to "User Defined".
- Name:** A text input field containing "User_Defined".
- Code:** A text input field containing "0".
- Type:** A dropdown menu currently set to "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, there are two buttons: "Close" and "OK".

The following table describes the labels in this screen.

Table 46 Security Gateway > Configure > Interfaces addressing: Local LAN: DHCP Option

LABEL	DESCRIPTION
Option	Select which DHCP option that you want to add in the DHCP packets sent through the interface.
Name	This field displays the name of the selected DHCP option. If you selected User_Defined in the Option field, enter a descriptive name to identify the DHCP option.
Code	This field displays the code number of the selected DHCP option. If you selected User_Defined in the Option field, enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. If you selected User_Defined in the Option field, select an appropriate type for the value that you will enter in the next field. Misconfiguration could result in interface lockout.
Value	Enter the value for the selected DHCP option. For example, if you selected TFTP Server Name (66) and the type is TEXT , enter the DNS domain name of a TFTP server here. This field is mandatory.
First IP address Second IP address Third IP address	If you selected Time Server (4) , NTP Server (41) , SIP Server (120) , CAPWAP AC (138) , or TFTP Server (150) , you have to enter at least one IP address of the corresponding servers in these fields. The servers should be listed in order of your preference.
First enterprise ID Second enterprise ID	If you selected VIVC (124) or VIVS (125) , you have to enter at least one vendor's 32-bit enterprise number in these fields. An enterprise number is a unique number that identifies a company.

Table 46 Security Gateway > Configure > Interfaces addressing: Local LAN: DHCP Option (continued)

LABEL	DESCRIPTION
First class Second class	If you selected VIVC (124) , enter the details of the hardware configuration of the host on which the client is running, or of industry consortium compliance.
First information Second information	If you selected VIVS (125) , enter additional information for the corresponding enterprise number in these fields.
First FQDN Second FQDN Third FQDN	If the Type is FQDN , you have to enter at least one domain name of the corresponding servers in these fields. The servers should be listed in order of your preference.
Close	Click Close to exit this screen without saving.
OK	Click OK to save your changes.

6.3.2.4 Static Route

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

Figure 57 Security Gateway > Configure > Interfaces addressing: Static Route

The following table describes the labels in this screen.

Table 47 Security 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 Close to exit this screen without saving.
OK	Click OK to save your changes.

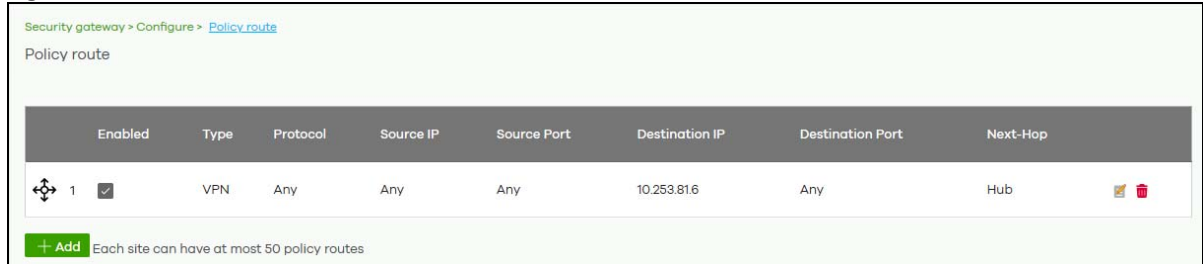
6.3.3 Policy Route

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

Figure 58 Security Gateway > Configure > Policy Route



The following table describes the labels in this screen.

Table 48 Security Gateway > Configure > Policy Route

LABEL	DESCRIPTION
	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box to turn off the rule.
Type	This shows whether the packets will be routed to a different gateway (INTRANET), VPN tunnel (VPN) or outgoing interface (INTERNET).
Protocol	This displays the IP protocol that defines the service used by the packets. Any means all services.
Source IP	This is the source IP address(es) from which the packets are sent.
Source Port	This displays the port that 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. Any 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 that the destination IP address(es) are using in this policy route rule. Any means all service ports.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel or outgoing interface.
	Click this icon to change the profile settings.
	Click this icon to remove the profile.
Add	Click this button to create a new policy route. See Section 6.3.4.1 on page 138 for more information.

6.3.3.1 Add/Edit policy route

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

Figure 59 Security Gateway > Configure > Policy Route: Add/Edit

The following table describes the labels in this screen.

Table 49 Security Gateway > Configure > Policy Route: Add/Edit

LABEL	DESCRIPTION
Type	<p>Select Internet Traffic to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).</p> <p>Select Intranet Traffic to route the matched packets to the next-hop router or switch you specified in the Next-Hop field.</p> <p>Select VPN Traffic to route the matched packets via the VPN tunnel you specified in the Next-Hop field.</p>
Protocol	Select TCP or UDP if you want to specify a protocol for the policy route. Otherwise, select Any .
Source IP	Enter a source IP address from which the packets are sent.
Source Port	Enter the port number (1-65535) from which the packets are sent. The gateway applies the policy route to the packets sent from the corresponding service port. Any means all service ports.
Destination IP	Enter a destination IP address to which the packets go.
Destination Port	Enter the port number (1-65535) to which the packets go. The gateway applies the policy route to the packets that go to the corresponding service port. Any means all service ports.
Next-Hop	<p>If you select Internet Traffic in the Type field, select the WAN interface to route the matched packets through the specified outgoing interface to a gateway connected to the interface.</p> <p>If you select Intranet Traffic in the Type field, enter the IP address of the next-hop router or switch.</p> <p>If you select VPN Traffic in the Type field, select the remote VPN gateway's site name.</p>
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 Firewall

By default, a LAN user can initiate a session from within the LAN and the security gateway allows the response. However, the security gateway blocks incoming traffic initiated from the WAN and destined

for the LAN. Use this screen to configure firewall rules for outbound traffic, application patrol, schedule profiles and port forwarding rules for inbound traffic.

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

Figure 60 Security Gateway > Configure > Firewall

Security gateway > Configure > [Firewall](#)

Firewall

Security policy

Inbound rules

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

Outbound rules

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

+ Add

Security gateway services

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

Application Patrol

Application monitor

on

Enable this option to allow traffic analysis with application patrol.

Application profiles

Name	Description
1 applications	

+ Add

Schedule profiles

There are no schedule profiles defined for this site.

+ Add

SIP ALG

SIP ALG

on

SIP Signaling Port

5060

ADVANCED OPTIONS

SIP Inactivity Timeout

on

SIP Media Inactivity Timeout

120 seconds

SIP Signaling Inactivity Timeout

1800 seconds

NAT

1:1 NAT

+ Add

Virtual Server

+ Add

There are no 1:1 NAT mappings.

There are no virtual server mappings.

The following table describes the labels in this screen.

Table 50 Security Gateway > Configure > Firewall





LABEL	DESCRIPTION
Security Policy	
Outbound rules	
	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box to turn off the rule.
Policy	Select what the firewall is to do with packets that match this rule. Select Deny to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select Allow to permit the passage of the packets. Select a pre-defined application patrol profile to have the firewall takes the action set in the profile when traffic matches the application patrol signature(s). See Section 6.3.4.1 on page 138 for how to create an application patrol profile.
Protocol	Select the IP protocol to which this rule applies. Choices are: TCP , UDP , and Any .
Source	Specify the source IP address(es) to which this rule applies. You can specify multiple IP addresses or subnets in the field separated by a comma (","),. Enter any to apply the rule to all IP addresses.
Destination	Specify the destination IP 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 any 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 any to apply the rule to all ports.
Schedule	Select the name of the schedule profile that the rule uses. Always means the rule is active at all times if enabled.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the rule.
	Click this icon to remove the rule.
Add	Click this button to create a new rule.
Security gateway services	
Service	This shows the name of the service.
Allowed remote IPs	Specify the IP address with which the computer is allowed to access the security gateway using the service. You can specify a range of IP addresses. any allows all IP addresses.
Application Patrol	
Application monitor	Click On to enable traffic analysis for all applications and display information about top 10 applications in the Site-wide > Monitor > Dashboard: Traffic Summary screen. Otherwise, select Off to disable traffic analysis for applications.
Application profiles	
Name	This shows the name of the application patrol profile.
Description	This shows the description of the application patrol profile.
	Click this icon to change the profile settings.
	Click this icon to remove the profile.
Add	Click this button to create a new application patrol profile. See Section 6.3.4.1 on page 138 for more information.
Schedule profiles	
	This shows the name of the schedule profile and the number of the outbound rules that are using this schedule profile.

Table 50 Security Gateway > Configure > Firewall (continued)







LABEL	DESCRIPTION
	Click this icon to change the profile settings.
	Click this icon to remove the profile.
Add	Click this button to create a new schedule profile. See Section 6.3.4.2 on page 139 for more information.
SIP ALG	
SIP ALG	<p>Session Initiation Protocol (SIP) is an application-layer protocol that can be used to create voice and multimedia sessions over Internet.</p> <p>Application Layer Gateway (ALG) allows the following applications to operate properly through the Nebula device's NAT.</p> <p>Turn on the SIP ALG to detect SIP traffic and help build SIP sessions through the Nebula device's NAT. Enabling the SIP ALG also allows you to use the application patrol to detect SIP traffic and manage the SIP traffic's bandwidth.</p>
SIP Signaling Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here.
ADVANCED OPTIONS	
SIP Inactivity Timeout	Select this option to have the Nebula device apply SIP media and signaling inactivity time out limits.
SIP Media Inactivity Timeout	<p>Use this field to set how many seconds (1~86400) the Nebula device will allow a SIP session to remain idle (without voice traffic) before dropping it.</p> <p>If no voice packets go through the SIP ALG before the timeout period expires, the Nebula device deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.</p>
SIP Signaling Inactivity Timeout	<p>Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the Nebula device.</p> <p>If the SIP client does not have this mechanism and makes no calls during the Nebula device SIP timeout, the Nebula device deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1~86400).</p>
NAT	
1:1 NAT	
<p>A 1:1 NAT rule maps a public IP address to the private IP address of a LAN server to give WAN users access.</p> <p>If a private network server will initiate sessions to the outside clients, 1:1 NAT lets the security gateway translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server.</p>	
	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box to turn off the rule.
Uplink	Select the interface of the security gateway on which packets for the NAT rule must be received.
Public IP	<p>Enter the destination IP address of the packets received by the interface specified in this NAT rule.</p> <p>Note: To enable NAT loopback, enter a specific IP address instead of any in this field. NAT loopback allows communications between two hosts on the LAN behind the security gateway via an external IP address.</p>
LAN IP	Specify to which translated destination IP address this NAT rule forwards packets.
Allowed remote IP	<p>Specify the remote IP address with which the computer is allowed to use the public IP address to access the private network server. You can specify a range of IP addresses.</p> <p>any allows all IP addresses.</p>

Table 50 Security Gateway > Configure > Firewall (continued)

LABEL	DESCRIPTION
Description	Enter a description for the rule.
	Click this icon to remove the rule.
Add	Click this button to create a new 1:1 NAT mapping rule.
Virtual server This makes computers on a private network behind the security gateway available to a public network outside the security gateway (like the Internet).	
	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box to turn off the rule.
Uplink	Select the interface of the security gateway on which packets for the NAT rule must be received.
Protocol	Select the protocol (TCP , UDP , or Any) used by the service requesting the connection.
Public IP	Enter the destination IP address of the packets received by the interface specified in this NAT rule. Note: To enable NAT loopback, enter a specific IP address instead of any in this field. NAT loopback allows communications between two hosts on the LAN behind the security gateway via an external IP address.
Public port	Enter the translated destination port or range of translated destination ports if this NAT rule forwards the packet.
LAN IP	Specify to which translated destination IP address this NAT rule forwards packets.
Local port	Enter the original destination port or range of destination ports this NAT rule supports.
Allowed remote IP	Specify the remote IP address with which the computer is allowed to use the public IP address to access the private network server. You can specify a range of IP addresses. any allows all IP addresses.
Description	Enter a description for the rule.
	Click this icon to remove the rule.
Add	Click this button to create a new virtual server mapping rule.

6.3.4.1 Add application patrol profile

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers).

An application patrol profile is a group of categories of application patrol signatures. For each profile, you can specify the default action the security gateway takes once a packet matches a signature (forward, drop, or reject a service's connections and/or create a log alert).

Click the **Add** button in the **Application Patrol** section of the **Security Gateway > Configure > Firewall** screen to access this screen. Use the application patrol profile screens to customize action and log settings for a group of application patrol signatures.

Figure 61 Security Gateway > Configure > Firewall: Add an application profile

The following table describes the labels in this screen.

Table 51 Security Gateway > Configure > Firewall: Add an application profile

LABEL	DESCRIPTION
Name	Enter a name for this profile for identification purposes.
Description	Enter a description for this profile.
Log	Select whether to have the security gateway generate a log (ON) or not (OFF) by default when traffic matches an application signature in this category.
Application management	
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box to turn off the rule.
Category	Select an application category.
Application	Select All or select an application within the category to apply the policy.
Policy	Select the default action for the applications selected in this category. Forward - the security gateway routes packets that matches these application signatures. Drop - the security gateway silently drops packets that matches these application signatures without notification. Reject - 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 Add to create an entry.
Close	Click this button to exit this screen without saving.
Create	Click this button to save your changes and close the screen.

6.3.4.2 Create new schedule

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

Figure 62 Security Gateway > Configure > Firewall: Add a schedule profile

Local time zone: (You can set this on [General setting](#))

Name: Template:

Day	Availability
Sunday	<input checked="" type="radio"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Monday	<input checked="" type="radio"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Tuesday	<input checked="" type="radio"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Wednesday	<input checked="" type="radio"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Thursday	<input checked="" type="radio"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Friday	<input checked="" type="radio"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00

Close

The following table describes the labels in this screen.

Table 52 Security Gateway > Configure > Firewall: Add a schedule profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for this schedule for identification purposes.
Templates	Select a pre-defined schedule template or select Custom schedule and manually configure the day and time at which the associated firewall outbound rule is enabled.
Day	This shows the day of the week.
Availability	Click On to enable the associated rule at the specified time on this day. Otherwise, select Off to turn the associated rule off at the specified time on this day. Specify the hour and minute when the schedule begins and ends each day.
Close	Click this button to exit this screen without saving.
Add	Click this button to save your changes and close the screen.

6.3.5 Security Service

Use this screen to enable or disable the features available in the security pack for your security gateway, such as content filtering, Intrusion Detection and Prevention (IDP) and/or anti-virus. As to application patrol, go to the **Firewall** screen to configure it since you need to have a firewall rule for outbound traffic.

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

Click **Security Gateway > Configure > Security Service** to access this screen.

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

Figure 63 Security Gateway > Configure > Security Service

Security gateway > Configure > Security service

Security service

Content filtering

Enabled ☒

Interface	
LAN1	<input checked="" type="checkbox"/>
LAN2	<input checked="" type="checkbox"/>
VLAN100	<input checked="" type="checkbox"/>
VLAN10	<input checked="" type="checkbox"/>
VLAN250	<input checked="" type="checkbox"/>

Denied access message: This category has been blocked. Please contact the network admin.

Redirect URL:

Block list:

White list:

Block Category

Templates: Security

Test URL:

Search category:

Category list

Anti-virus

Signature Information

Current Version: 10.0.20200106.0

Signature Number: 632627

Released Date: 2020-01-06 08:33 (UTC+08:00)

Enabled ☒

Block list:

File Pattern:

White list:

File Pattern:

Intrusion Detection / Prevention

Signature Information

Current Version: 3.1.4.391

Signature Number: 2143

Released Date: 2020-01-06 08:33 (UTC+08:00)

Detection ☒

Prevention ☒

The following table describes the labels in this screen.

Table 53 Security Gateway > Configure > Security Service

LABEL	DESCRIPTION
Content Filtering	
Enabled	Click ON to enable the content filtering feature on the security gateway. Otherwise, click OFF to disable it.
Interface	This shows the name of the interfaces created on the security gateway. Click ON to enable content filtering on the interface(s).
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/?:@&=+\$\._!~*()%). 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/?:@&=+\$\._!~*()%). For example, http://192.168.1.17/blocked access.</p>
Black list	<p>Sites that you want to block access to, regardless of their content rating, can be blocked by adding them to this list.</p> <p>Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are also blocked. For example, entering "bad-site.com" also blocks "www.badsite.com", "partner.bad-site.com", "press.bad-site.com", and so on. You can also enter just a top level domain. For example, enter .com to block all .com domains.</p> <p>Use up to 127 characters (0-9a-z-). The casing does not matter.</p>
White list	<p>Sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.</p> <p>Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All sub-domains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains.</p> <p>Use up to 127 characters (0-9a-z-). The casing does not matter.</p>
Block Category	
The security gateway prevents users from accessing web pages that match the categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Denied access message field along with the category of the blocked web page.	
Templates	Web pages are classified into a category based on their content. You can choose a pre-defined template that has already selected certain categories. Alternatively, choose Custom and manually select categories in this section to control access to specific types of Internet content.
Test URL	<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. Test URL displays both results in the test.</p>

Table 53 Security Gateway > Configure > Security Service (continued)

LABEL	DESCRIPTION
Search Category	Specify your desired filter criteria to filter the list of categories.
Category List	Click to display or hide the category list. These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.
Anti-Virus	
Signature Information	This shows the Current Version of the anti-virus definition, its Signature Number and the Released Date .
Enabled	Click On to enable anti-virus on the security gateway. Otherwise, select Off to disable it.
Black/White List	Use this to set up anti-virus black (blocked) and white (allowed) lists of virus file patterns.
File Pattern	<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"> Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. A question mark (?) lets a single character in the file name vary. For example, use "a?.zip" (without the quotation marks) to specify aa.zip, ab.zip and so on. Wildcards (*) let multiple files match the pattern. For example, use "*a.zip" (without the quotation marks) to specify any file that ends with "a.zip". A file named "testa.zip" would match. There could be any number (of any type) of characters in front of the "a.zip" at the end and the file name would still match. A file named "test.zipa" for example would not match. A * in the middle of a pattern has the 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. The whole file name has to match if you do not use a question mark or asterisk. If you do not use a wildcard, the security gateway checks up to the first 80 characters of a file name.
Intrusion Detection / Prevention	
Signature Information	This shows the Current Version of the anti-intrusion definition, its Signature Number and the Released Date .
Detection	Click On to detect malicious or suspicious packets. Otherwise, select Off to disable it.
Prevention	Click On to identify and respond to intrusions. Otherwise, select Off to disable it.

6.3.6 Site-to-Site VPN

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

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

Figure 64 Security Gateway > Configure > Site-to-Site VPN

Security gateway > Configure > Site-to-Site VPN

Site-to-Site VPN

Outgoing interface: WAN1

Local networks

Name	Subnet	Use VPN
LAN1	100.34.1.0/24	on
LAN2	173.16.34.0/24	off

Nebula VPN Topology: Split tunnel (send only site-to-site traffic over the VPN)

Disable

Site-wide settings

Options in this section apply to this Nebula gateway only.

Non-Nebula VPN peers

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

+ Add

The following table describes the labels in this screen.

Table 54 Security Gateway > Configure > Site-to-Site VPN

LABEL	DESCRIPTION
Outgoing Interface	Select the WAN interface to which the VPN connection is going. Select AUTO to send VPN traffic through a different WAN interface when the primary WAN interface is down or disabled.
Prefer uplink	Specify the primary WAN interface through which the security gateway forwards VPN traffic when you set Outgoing Interface to AUTO .
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 ON to allow the computers on the network to use the VPN tunnel. Otherwise, select OFF .

Table 54 Security Gateway > Configure > Site-to-Site VPN (continued)

LABEL	DESCRIPTION
Nebula VPN Topology	<p>This shows the VPN mode supported by the security gateway.</p> <p>Select a VPN topology.</p> <p>Select Disable to not set a VPN connection.</p> <p>In the Site-to-Site VPN topology, the remote IPSec device has a static IP address or a domain name. This security gateway can initiate the VPN tunnel.</p> <p>In the Hub-and-Spoke VPN topology, there is a VPN connection between each spoke router and the hub router, which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself.</p> <p>In the Server-and-Client VPN topology, incoming connections from IPSec VPN clients are allowed. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.</p>
Hubs (peers to connect to)	<p>This field is available when you set Topology to Hub-and-Spoke. The field is configurable only when the security gateway of the selected site is the hub router.</p> <p>You can select another site's name to have the gateway of that site act as the hub router in the Hub-and-Spoke VPN topology.</p>
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)	<p>This field is available when you set Topology to Server-and-Client. The field is configurable only when the security gateway of the selected site is the VPN server.</p> <p>You can select another site's name to have the gateway of that site act as the VPN server.</p>
Client-to-Client communication	Select On 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.
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box to turn off the rule.
Name	Enter the name of the peer gateway.
Public IP	Enter the public IP address of the peer gateway.
Private Subnet	Enter the local network address or subnet behind the peer gateway.
IPSec policy	Click to select a pre-defined policy or have a custom one. See Section 6.3.6.1 on page 145 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.
Availability	<p>Select All sites to allow the peer gateway to connect to any Nebula security gateway in the organization via a VPN tunnel.</p> <p>Select This site and the peer gateway can only connect to the Nebula security gateway in this site via a VPN tunnel.</p> <p>You can also configure any specific sites in the organization,</p>
Action	Click the remove icon to delete the entry.
Add	Click this button to add a peer VPN gateway to the list.

6.3.6.1 Custom IPSec Policy

Click an existing **IPSec Policy** button in the **Non-Nebula VPN peers** section of the **Security Gateway > Configure > Site-to-Site VPN** screen to access this screen.

Figure 65 Security Gateway > Configure > Site-to-Site VPN: Custom IPSec Policy

Custom [X]

Preset: Default

Phase 1

IKE version: IKEv1

Encryption: 3DES

Authentication: SHA128

Diffie-Hellman group: DH2

Lifetime (seconds): 86400

Advanced

Phase 2

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

PFS group: None

Lifetime (seconds): 86400

Close OK

The following table describes the labels in this screen.

Table 55 Gateway > Configure > Site-to-Site VPN: Custom IPSec Policy

LABEL	DESCRIPTION
Preset	Select a pre-defined IPSec policy, or select Custom to configure the policy settings yourself.
Phase 1	IPSec VPN consists of two phases: Phase 1 (Authentication) and Phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

Table 55 Gateway > Configure > Site-to-Site VPN: Custom IPSec Policy (continued)

LABEL	DESCRIPTION
IKE version	<p>Select IKEv1 or IKEv2.</p> <p>IKEv1 applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely.</p>
Encryption	<p>Select which key size and encryption algorithm to use in the IKE SA. Choices are:</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>AES128 - a 128-bit key with the AES encryption algorithm</p> <p>AES192 - a 192-bit key with the AES encryption algorithm</p> <p>AES256 - a 256-bit key with the AES encryption algorithm</p> <p>The security gateway and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IKE SA.</p> <p>Choices are SHA128, SHA256, SHA512 and MD5. SHA is generally considered stronger than MD5, but it is also slower.</p> <p>The remote IPSec router must use the same authentication algorithm.</p>
Diffie-Hellman group	<p>Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are:</p> <p>DH1 - use a 768-bit random number</p> <p>DH2 - use a 1024-bit random number</p> <p>DH5 - use a 1536-bit random number</p> <p>DH14 - use a 2048-bit random number</p> <p>The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.</p>
Lifetime (seconds)	<p>Type the maximum number of seconds the IKE SA can last. When this time has passed, the security gateway and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.</p>
Advanced	<p>Click this to display a greater or lesser number of configuration fields.</p>
Mode	<p>Select the negotiation mode to use to negotiate the IKE SA. Choices are:</p> <p>Main - this encrypts the security gateway's and remote IPSec router's identities but takes more time to establish the IKE SA</p> <p>Aggressive - this is faster but does not encrypt the identities</p> <p>The security gateway and the remote IPSec router must use the same negotiation mode.</p>
Local ID	<p>Type the identity of the security gateway during authentication. Any indicates that the remote IPSec router does not check the identity of the security gateway.</p>
Peer ID	<p>Type the identity of the remote IPSec router during authentication. Any indicates that the security gateway does not check the identity of the remote IPSec router.</p>
Phase 2	<p>Phase 2 uses the SA that was established in phase 1 to negotiate SAs for IPSec.</p>

Table 55 Gateway > Configure > 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>(none) - no encryption key or algorithm</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>AES128 - a 128-bit key with the AES encryption algorithm</p> <p>AES192 - a 192-bit key with the AES encryption algorithm</p> <p>AES256 - 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 None, MD5, SHA128, SHA256, and SHA512. 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>None - disable PFS</p> <p>DH1 - enable PFS and use a 768-bit random number</p> <p>DH2 - enable PFS and use a 1024-bit random number</p> <p>DH5 - enable PFS and use a 1536-bit random number</p> <p>DH14 - 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>
<p>VPN tunnel interface (optional)</p> <p>IPSec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.</p> <p>VTI allows static routes to send traffic over the VPN. The IPSec tunnel endpoint is associated with an actual (virtual) interface. Therefore many interface capabilities such as Policy Route, Static Route, Trunk, and BWM can be applied to the IPSec tunnel as soon as the tunnel is active. IPSec VTI simplifies network management and load balancing. Create a trunk using VPN tunnel interfaces for load balancing.</p> <p>This section is available when you select IKEv2 in the IKE Version field.</p>	
IP address	Enter the IP address of the VPN tunnel interface.
Subnet mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

6.3.7 Remote Access VPN

Use this screen to configure the VPN client settings.

Internet Protocol Security (IPSec) VPN connects IPSec routers or remote users using IPSec client software. This standards-based VPN offers flexible solutions for secure data communications across a public network. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first and then an L2TP tunnel is built inside it.

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

Figure 66 Security Gateway > Configure > Remote access VPN

Security gateway > Configure > Remote access VPN


Remote access VPN

Client VPN server	L2TP over IPSec client ▼
Client VPN subnet	192.168.11 ✕
DNS name servers	Specify nameserver ... ▼
Custom nameservers	192.168.11 ✕

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


Example:
192.168.11
192.168.37.10

WINS	No WINS servers ▼
Secret	***** 🔍
Authentication	Nebula Cloud Authentication ▼
VPN provision script ⓘ	E.g. nebula@zyxel.com

 Send Email

The following table describes the labels in this screen.

Table 56 Security Gateway > Configure > Remote access VPN

LABEL	DESCRIPTION
Client VPN server	Select to enable the IPSec client or L2TP over IPSec client feature on the security gateway. Otherwise, select Disable to turn it off.
Outgoing interface	Select the WAN interface to which the VPN connection is going. This field is available only when you select IPSec client in the Client VPN server field.
NAT traversal	Enter the IP address or domain name of the NAT router if the VPN tunnel must pass through NAT (there is a NAT router between the IPSec devices). This field is available only when you select IPSec client in the Client VPN server field.
Client VPN subnet	Specify the IP addresses that the security gateway uses to assign to the VPN clients.
DNS name servers	Specify the IP addresses of DNS servers to assign to the remote users. Select Use Google Public DNS to use the DNS service offered by Google. Otherwise, select Specify nameserver to enter a static IP address.
Custom nameservers	If you select Specify nameserver in the DNS name servers field, manually enter the DNS server IP 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 No WINS Servers to not send WINS server addresses to the users. Otherwise, select Specify nameserver to type the IP addresses of WINS servers to assign to the remote users.
Custom nameservers	If you select Specify nameserver in the WINS field, manually enter the WINS server IP address(es).
Secret	Enter the pre-shared key (password) which is used to set up the VPN tunnel.
Authentication	Select how the security gateway authenticates a remote user before allowing access to the VPN tunnel.
VPN provision script	Send an email to help automatically configure VPN settings on client devices so that the devices can remotely access this gateway. The email contains two scripts; one for macOS and iOS devices, and one for Windows 8 and Windows 10 devices. You can send the email to one or more email addresses. <ul style="list-style-type: none"> If Authentication is set to Nebula Cloud Authentication, the default email address list contains all authorized VPN user email addresses and your email address. If Authentication is set to AD and RADIUS Authentication, the default email address list contains your user email address. This field is available only when you select L2TP over IPSec client in the Client VPN server field.
 Download VPN Client	Click this icon to download VPN client software.

6.3.8 Captive Portal

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

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

Figure 67 Security Gateway > Configure > Captive portal


Security gateway > Configure > [Captive portal](#)

Captive portal


Interface LAN1

Captive portal on this interface is direct access. You can change this setting [here](#).


Themes



☐ **Default** Modern



☐ Copy of Modern



☒ Copy of Modern

Click-to-continue/Sign-on page

Logo

No logo

Upload a logo

Message

Terms go here!

Success page

Message

Success!

External captive portal URL

Use URL: ☐ off URL:

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

Captive portal behavior

After the captive portal page where the user should go?

☒ Stay on Captive portal authenticated successfully page

☐ To promotion URL:

[Save](#) or Cancel

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

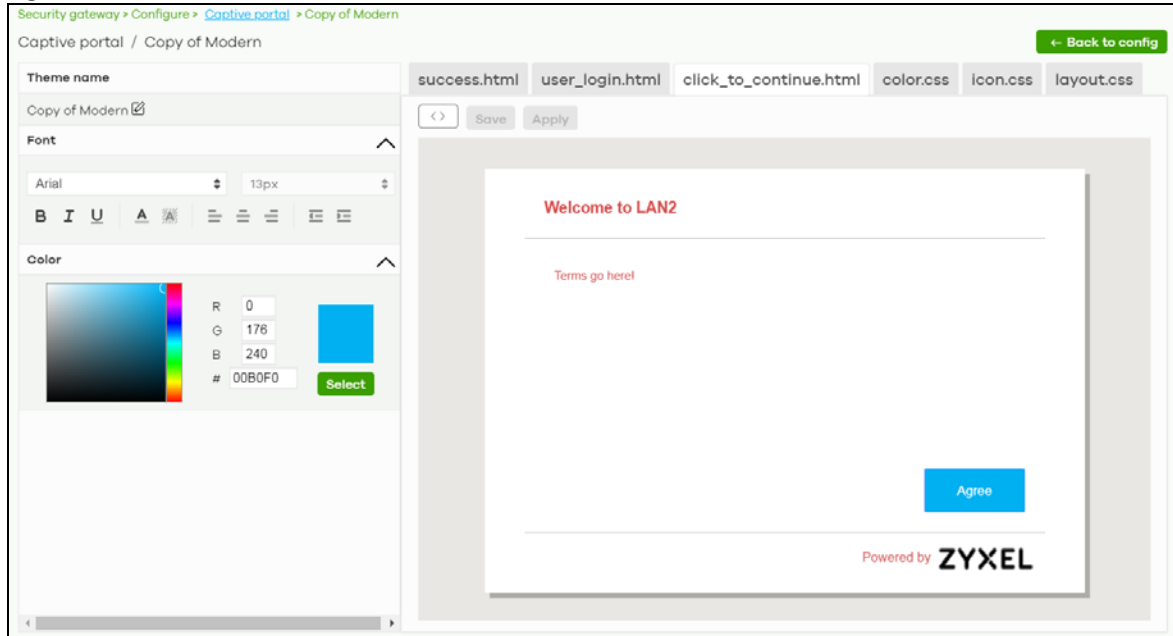
The following table describes the labels in this screen.

Table 57 Security Gateway > Configure > Captive portal

LABEL	DESCRIPTION
Interface	Select the gateway's interface (network) to which the settings you configure here is applied.
Themes	<p>This section is not configurable when External captive portal URL is set to ON.</p> <ul style="list-style-type: none"> Click the Preview icon at the upper right corner of a theme image to display the portal page in a new frame. Click the Copy icon to create a new custom theme (portal page). Click the Edit icon of a custom theme to go to a screen, where you can view and configure the details of the custom portal page(s). See Section 6.3.8.1 on page 152. Click the Remove icon to delete a custom theme. <p>Select the theme you want to use on the specified interface.</p>
Click-to-continue/Sign-on page	
This section is not configurable when External captive portal URL is set to ON .	
Logo	<p>This shows the logo image that you uploaded for the customized login page.</p> <p>Click Upload a logo and specify the location and file name of the logo graphic or click Browse to locate it. You can use the following image file formats: GIF, PNG, or JPG.</p>
Message	Enter a note to display below the title. Use up to 1024 printable ASCII characters. Spaces are allowed.
Success page	
Message	Enter a note to display on the page that displays when a user logs in successfully. Use up to 1024 printable ASCII characters. Spaces are allowed.
External captive portal URL	
Use URL	<p>Select On to use a custom login page from an external web portal instead of the one built into the NCC. You can configure the look and feel of the web portal page.</p> <p>Specify the login page's URL; for example, <code>http://IIS server IP Address/login.asp</code>. The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>
Captive portal behavior	
After the captive portal page where the user should go?	Select To promotion URL and specify the URL of the web site/page to which the user is redirected after a successful login. Otherwise, select Stay on Captive portal authenticated successfully page .

6.3.8.1 Custom Theme Edit

Use this screen to check what the custom portal pages look like. You can also view and modify the CSS values of the selected HTML file. Click a custom login page's **Edit** button in the **Security Gateway > Configure > Captive portal** screen to access this screen.

Figure 68 Security Gateway > Configure > Captive portal: Edit

The following table describes the labels in this screen.

Table 58 Security Gateway > Configure > Captive portal: Edit

LABEL	DESCRIPTION
Back to config	Click this button to return to the Captive portal screen.
Theme name	This shows the name of the theme. Click the edit icon to change it.
Font	Click the arrow to hide or display the configuration fields. To display this section and customize the font type and/or size, click on an item with text in the preview of the selected custom portal page (HTML file).
Color	Click the arrow to hide or display the configuration fields. Click on an item in the preview of the selected custom portal page (HTML file) to display this section and customize its color, such as the color of the button, text, window's background, links, borders, and so on. Select a color that you want to use and click the Select button.
HTML/CSS	This shows the HTML file name of the portal page created for the selected custom theme. This also shows the name of the CSS files created for the selected custom theme. Click a HTML file to display the portal page. You can also change colors and modify the CSS values of the selected HTML file.
<>	Click this button to view and modify the CSS values of the selected HTML file. It is recommended that you do NOT change the script code to ensure proper operation of the portal page.
🔍	Click this button to preview the portal page (the selected HTML file).
Save	Click this button to save your settings for the selected HTML file to the NCC.
Apply	Click this button to save your settings for the selected HTML file to the NCC and apply them to the security gateway in the site.

6.3.9 Network Access Method

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

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

Figure 69 Security Gateway > Configure > Network access method

Security gateway > Configure > Network access method

Network access method

Interfaces: LAN1

Network Access

☐ Disable
 Users can access the network directly

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

☒ Sign-on-with Nebula Cloud Authentication

Walled garden on

Walled garden ranges

[What do I enter here?](#)

One IP address/domain in one line to specify your walled garden.
 Example:
 *.zyxel.com
 www.zyxel.com
 192.168.1.0/24

Captive portal access attribute

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

Login on multiple client devices: Multiple devices access simultaneously

NCAS disconnection behavior ⓘ

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

☐ Limited:
 Only currently authorized clients and whitelisted client devices will be able to access the network

The following table describes the labels in this screen.

Table 59 Gateway > Configure > Network access method

LABEL	DESCRIPTION
Interfaces	Select the gateway's interface (network) to which the settings you configure here is applied.
Network Access	<p>Select Disable to turn off web authentication.</p> <p>Select Click-to-continue to block network traffic until a client agrees to the policy of user agreement.</p> <p>Select Sign-on with to block network traffic until a client authenticates with an external RADIUS or AD server through the specifically designated web portal page. Select Nebula Cloud Authentication or an authentication server that you have configured in the Security Gateway > Configure > Gateway Settings screen (see Section 6.3.11 on page 158).</p>
Walled garden	<p>This field is not configurable if you set Network Access to Disable.</p> <p>Select to turn on or off the walled garden feature.</p> <p>With a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example.</p>
Walled garden ranges	Specify walled garden web site links, which use a domain name or an IP address for web sites that all users are allowed to access without logging in.
Captive portal access attribute	
Self-registration	<p>This field is available only when you select Sign-on with Nebula Cloud authentication in the Network Access field.</p> <p>Select Allow users to create accounts with auto authorized or Allow users to create accounts with manual authorized to display a link in the captive portal login page. The link directs users to a page where they can create an account before they authenticate with the NCC. For Allow users to create accounts with manual authorized, users cannot log in with the account until the account is authorized and granted access. For Allow users to create accounts with auto authorized, users can just use the registered account to log in without administrator approval.</p> <p>Select Don't allow users to create accounts 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 Sign-on with in the Network Access field.</p> <p>Select Multiple devices access simultaneously if you allow users to log in as many times as they want as long as they use different IP addresses.</p> <p>Select One device at a time if you don't allow users to have simultaneous logins.</p>
NCAS disconnection behavior	<p>This field is available only when you select Sign-on with Nebula Cloud Authentication in the Network Access field.</p> <p>Select Allowed to allow any users to access the network without authentication when the NCAS (Nebula Cloud Authentication Server) is not reachable.</p> <p>Select Limited to allow only the currently connected users or the users in the white list to access the network.</p>

6.3.10 Traffic Shaping

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

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

Figure 70 Security Gateway > Configure > Traffic shaping

Security gateway > Configure > [Traffic shaping](#)

Traffic shaping

Uplink configuration

WAN1

Up(kb/s): 466623

Down(kb/s): 466623

WAN2

Up(kb/s): unlimited

Down(kb/s): unlimited

WAN load balancing algorithm: Failover

Prefer WAN: WAN1

WAN Connectivity check:

☒ Check Default Gateway

☐ Check this address: 8.8.8.8 (IP Address)

Global bandwidth limits

Per-client limit:

Source First IP	Source Last IP	Destination IPs	Port(s)
192.168.100.1	192.168.100.254	any	any

+ Add

Session Control

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


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

The following table describes the labels in this screen.

Table 60 Security Gateway > Configure > Traffic shaping

LABEL	DESCRIPTION
Uplink configuration	
WAN 1	Set the amount of upstream/downstream bandwidth for the WAN interface.
WAN 2	Click a lock icon to change the lock state. If the lock icon for a WAN interface is locked, the bandwidth limit you set applies to both inbound and outbound traffic. If the lock is unlocked, you can set inbound and outbound traffic to have different transmission speeds.
WAN load balancing algorithm	<p>Select a load balancing method to use from the drop-down list box.</p> <ul style="list-style-type: none"> Select Least Load First to send new session traffic through the least utilized WAN interface. Select Round Robin to balance the traffic load between interfaces based on their respective weights (bandwidth). An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of WAN 1 and WAN 2 interfaces is 2:1, the security gateway chooses WAN 1 for 2 sessions' traffic and WAN 2 for 1 session's traffic in each round of 3 new sessions. Select Failover to send traffic through a second WAN interface when the primary WAN interface is down or disabled.
Prefer WAN	<p>Specify the primary WAN interface through which the security gateway forwards traffic.</p> <p>This field is available when you set WAN load balancing algorithm to Failover.</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"> Select Check Default Gateway to use the default gateway for the connectivity check. Select Check this address to specify a domain name or IP address for the connectivity check. <p>Note: If you select Check this address but the IP address you specified cannot be reached through the primary WAN interface, the security gateway will switch to the other one even if the primary WAN connection is still up. Make sure your security gateway supports multiple WAN interfaces and both WAN connections are configured properly before you select Check this address.</p> <p>This field is available when you set WAN load balancing algorithm to Failover.</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 any 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. any means all service ports.
Protocol	<p>Select TCP or UDP if you want to specify a protocol for the rule. Otherwise select Any.</p> <p>Any means the rule is applicable to all services.</p>

Table 60 Security Gateway > Configure > Traffic shaping (continued)

LABEL	DESCRIPTION
Down/Up	Set the maximum upstream/downstream bandwidth for traffic from an individual source IP address. Click a lock icon to change the lock state. If the lock icon is locked, the bandwidth limit you set applies to both inbound and outbound traffic. If the lock is unlocked, you can set inbound and outbound traffic to have different transmission speeds.
Priority	Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority.
	Click this icon to remove the rule.
Add	Click this button to create a new rule.
Session Control	
UDP Session Time Out	Set how many seconds the security gateway will allow a UDP session to remain idle (without UDP traffic) before closing it.
Default Session per Host	Set a common limit to the number of concurrent NAT/Security Policy sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.

6.3.11 Gateway Settings

Use this screen to configure DNS settings and external AD (Active Directory) server or RADIUS server that the security gateway can use in authenticating users.

AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.

This screen also lets you configure the addresses of walled garden web sites that users can access without logging into the gateway. The settings in this screen apply to all networks (interfaces) on the security gateway. If you want to configure walled garden web site links for a specific interface, use the **Network access method** screen.

Click **Security Gateway > Configure > Gateway settings** to access this screen.

Figure 71 Security Gateway > Configure > Gateway settings

Security gateway > Configure > [Gateway settings](#)

Gateway settings

DNS

Address Record

FQDN	IP Address
d.nebula.zyxel.com	52.19.85.221
www.nebula.zyxel.com	52.84.248.13
s.nebula.zyxel.com	18.202.42.142

[+ Add](#)

Domain Zone Forwarder

Domain Zone	IP Address	Interface
		LAN1

[+ Add](#)

Authentication Server

My AD Server

Name	Server address	Backup server address	Port	AD domain
ADTest	192.168.8.1		389	zyxel.com

[+ Add](#)

My RADIUS Server

Name	Server address	Backup server address	Port	Secret
			1812	

[+ Add](#)

Walled garden

Global walled garden

This is global walled garden configuration. All web authentication interface will match this policy first and the second priority is the interface walled garden policy.
If needed only allow specify interface, please go to Network access method configure

[What do I enter here?](#)

The following table describes the labels in this screen.

Table 61 Security Gateway > Configure > Gateway settings





LABEL	DESCRIPTION
DNS	
Address Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, <code>www.zyxel.com.tw</code> is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain.
FQDN	Enter a host's fully qualified domain name. Use "*" as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the host's IP address.
	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Domain Zone Forwarder	This specifies a DNS server's IP address. The security gateway can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the security gateway needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, <code>zyxel.com.tw</code> is the domain zone for the <code>www.zyxel.com.tw</code> fully qualified domain name. Whenever the security gateway receives needs to resolve a <code>zyxel.com.tw</code> domain name, it can send a query to the recorded name server IP address.
IP Address	Enter the DNS server's IP address.
Interface	Select the interface through which the security gateway sends DNS queries to the specified DNS server.
	Click this icon to remove the entry.
Add	Click this button to create a new entry.
Authentication Server	
My AD Server	
Name	Enter a descriptive name for the server.
Server address	Enter the address of the AD server.
Backup server address	If the AD server has a backup server, enter its address here.
Port	Specify the port number on the AD server to which the security gateway sends authentication requests. Enter a number between 1 and 65535.
AD domain	Specify the Active Directory forest root domain name.
Domain admin	Enter the name of the user that is located in the container for Active Directory Users, who is a member of the Domain Admin group.
Password	Enter the password of the Domain Admin user account.
Advanced	Click to open a screen where you can select to use Default or Custom advanced settings. See Section 6.3.11.1 on page 161 .
	Click this icon to remove the server.
Add	Click this button to create a new server.
My RADIUS server	
Name	Enter a descriptive name for the server.
Server address	Enter the address of the RADIUS server.
Backup server address	If the RADIUS server has a backup server, enter its address here.


Table 61 Security Gateway > Configure > Gateway settings (continued)

LABEL	DESCRIPTION
Port	Specify the port number on the RADIUS server to which the security gateway sends authentication requests. Enter a number between 1 and 65535.
Secret	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the security gateway. The key is not sent over the network. This key must be the same on the external authentication server and the security gateway.
Advanced	Click to open a screen where you can select to use Default or Custom advanced settings. See Section 6.3.11.1 on page 161 .
	Click this icon to remove the server.
Add	Click this button to create a new server.
Walled garden	
Global Walled garden	With a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example. Specify walled garden web site links, which use a domain name or an IP address for web sites that all users are allowed to access without logging in.

6.3.11.1 Advanced Settings

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

Figure 72 Security Gateway > Configure > Gateway settings: Advanced



The following table describes the labels in this screen.

Table 62 Security Gateway > Configure > Gateway settings: Advanced

LABEL	DESCRIPTION
Preset	Select Default to use the pre-defined settings, or select Custom to configure your own settings.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the 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 ON if the server checks the case of the user name. Otherwise, click OFF to not configure your user name as case-sensitive.
NAS IP Address	This field is only for RADIUS. Type the IP address of the NAS (Network Access Server).

Table 62 Security Gateway > Configure > Gateway settings: Advanced (continued)

LABEL	DESCRIPTION
Close	Click this button to exit this screen without saving.
OK	Click this button to save your changes and close the screen.

CHAPTER 7

Switch

7.1 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.

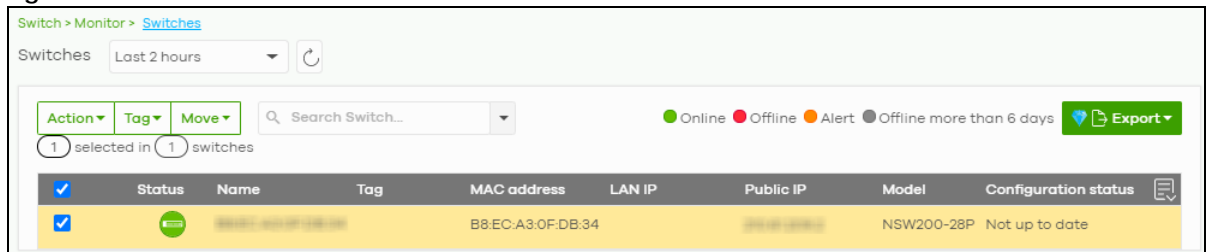
7.2 Monitor

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

7.2.1 Switches

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

Figure 73 Switch > Monitor > Switches




The following table describes the labels in this screen.

Table 63 Switch > Monitor > Switches

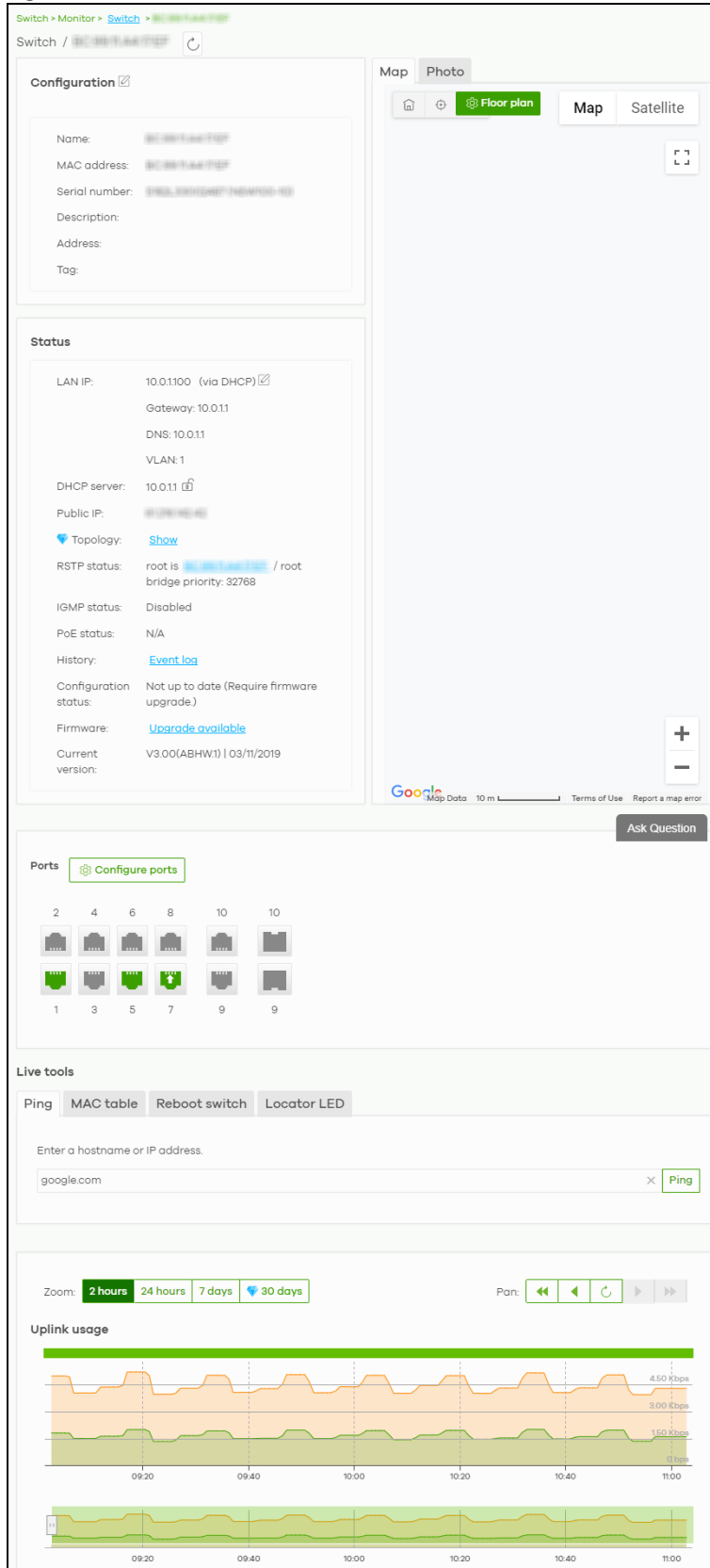
LABEL	DESCRIPTION
Switch	Select to view the device information and connection status in the past two hours, day, week or month.
	Click this button to reload the data-related frames on this page.
Action	Perform an action on the selected switches.
Reboot	Restart the switch.
Upgrade	Upgrade the firmware on the switch.
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.
Search	Specify your desired filter criteria to filter the list of switches.

Table 63 Switch > Monitor > Switches (continued)

LABEL	DESCRIPTION
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	<p>This shows the status of the switch.</p> <ul style="list-style-type: none"> Green: The device is online and has no alerts. Amber: The device has alerts. Red: The device is offline. Gray: The device has been offline for 7 days or more. <p>Move the cursor over an amber alert icon to view the alerts the NCC generates when an error or something abnormal is detected on the IPTV network.</p>
Name	This shows the descriptive name of the 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 switch's product description to explain what this switch is and also provides information about its features.
Connectivity	<p>This shows the switch connection status. Nothing displays if the switch is off-line.</p> <p>The gray time slot indicates the connection to the NCC is down, and the green time slot indicates the connection is up. Move the cursor over a time slot to see the actual date and time when a switch is connected or disconnected.</p>
Description	This shows the user-specified description for the switch.
Serial number	This shows the serial number of the switch.
Firmware status	This shows whether the firmware installed on the switch is up-to-date.
Current version	This shows the firmware version currently installed on the device.
Usage	This shows the amount of data that has been transmitted or received by the switch's clients.
	Click this icon to display a greater or lesser number of configuration fields.

7.2.1.1 Switch Details

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

Figure 74 Switch > Monitor > Switches: Switch Details

The following table describes the labels in this screen.

Table 64 Switch > Monitor > Switches: Switch Details


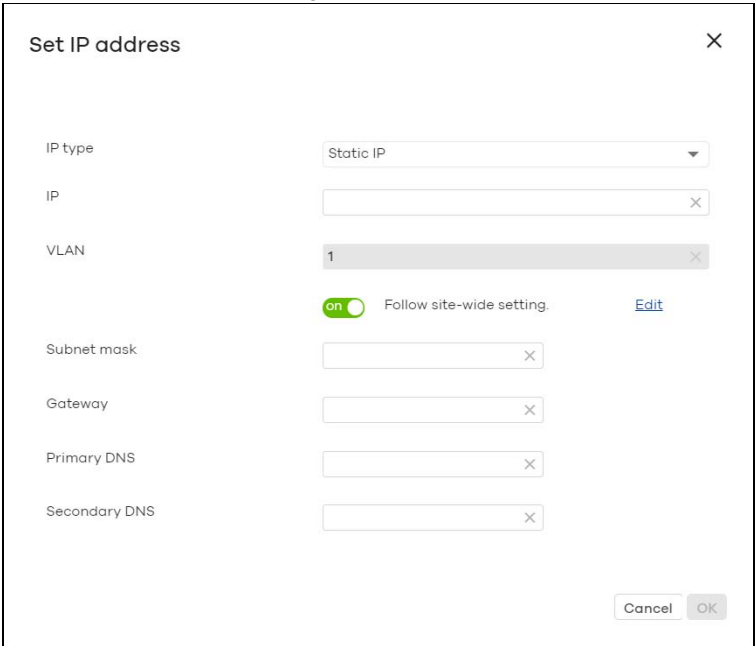
LABEL	DESCRIPTION
	Click this button to reload the data-related frames on this page.
Configuration Click the edit icon to change the device name, description, tags and address. You can also move the device to another site.	
Name	This shows the descriptive name of the switch.
MAC Address	This shows the 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> <div data-bbox="537 873 1287 1514">  <p>Set IP address [X]</p> <p>IP type: Static IP [v]</p> <p>IP: [] [X]</p> <p>VLAN: 1 [X]</p> <p><input checked="" type="radio"/> on Follow site-wide setting. Edit</p> <p>Subnet mask: [] [X]</p> <p>Gateway: [] [X]</p> <p>Primary DNS: [] [X]</p> <p>Secondary DNS: [] [X]</p> <p>[Cancel] [OK]</p> </div>
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 Show to go to the Site-wide > Monitor > Topology screen. See Section 5.1.3 on page 80 .
RSTP Status	This shows Disabled 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.

Table 64 Switch > Monitor > Switches: Switch Details (continued)



LABEL	DESCRIPTION
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. N/A displays if the switch does not support PoE.</p> <p>Click the edit icon to open the PoE Configuration screen. See Section 7.2.1.2 on page 168.</p>
History	Click Event log to go to the Switch > Monitor > Event log 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.
Current version	This shows the firmware version currently installed on the device.
Map	This shows the location of the switch on the Google map.
Photo	This shows the photo of the switch. Click Add to upload one or more photos. Click x to remove a photo.
<p>Ports</p> <p>This shows the ports on the switch. You can click a port to see the individual port statistics. See Section 7.2.1.3 on page 169. Move the pointer over a port to see additional port information. The port color indicates the connection status of the port.</p> <ul style="list-style-type: none"> Gray (#888888): The port is disconnected. Orange (#FF8900): The port is connected and is transmitting data at 10 or 100 Mbps. Green (#64BE00): The port is connected and is transmitting data at 1000 Mbps (1 Gbps). Azure (#0079FF): The port is connected and is transmitting data at 2.5 Gbps. Violet (#8800FF): The port is connected and is transmitting data at 5 Gbps. Blue (#004FEE): The port is connected and is transmitting data at 10000 Mbps (10 Gbps). <p>When the port is in the STP blocking state, a blocked icon displays on top of the port ( for example) in the diagram.</p>	
Name	This shows the descriptive name of the port.
Status	This shows the connection status of the port.
MAC address	This shows the MAC address of the port.
Type	This shows the port type (Trunk or Access), PVID, and allowed VLANs.
Speed	This shows the current connection speed of the port. If the speed is unavailable, this displays "Ethernet".
LLDP	This shows the LLDP information received on the port.
Configure ports	Click this button to go to the Switch > Configure > Switch ports screen, where you can view port summary. See Section 7.3.1 on page 185 .
Live tools	
Ping	Enter the host name or IP address of a computer that you want to perform ping in order to test a connection and click Ping .
Port Power Cycle	Enter the number of the port(s) and click the Reset 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 Reboot 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>

Table 64 Switch > Monitor > Switches: Switch Details (continued)

LABEL	DESCRIPTION
Uplink usage	Move the cursor over the chart to see the transmission rate at a specific time.
Zoom	Select to view the statistics in the past 12 hours, day, week, month, 3 months or 6 months.
Pan	Click to move backward or forward by one day or week.
Power Consumption	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.

7.2.1.2 PoE Configuration

Use this screen to set the PoE settings for the switch. To access this screen, click the edit icon next to **PoE Status** in the **Switch > Monitor > Switches: Switch Details** screen.

Note: To set PoE settings for an individual port, such as schedule, priority, and power mode, edit the switch's port settings. For details, see [Section 7.3.1 on page 185](#).

Figure 75 Switch > Monitor > Switches: Switch Details: PoE Configuration

The following table describes the labels in this screen.

Table 65 Switch > Monitor > Switches: Switch Details: PoE Configuration

LABEL	DESCRIPTION
PoE Mode	<p>Select the power management mode you want the switch to use.</p> <p>Classification mode - 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.</p> <p>Consumption mode - 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.</p>

Table 65 Switch > Monitor > Switches: Switch Details: PoE Configuration (continued)

LABEL	DESCRIPTION
Close	Click this button to exit this screen without saving.
Saving	Click this button to save your changes and close the screen.

7.2.1.3 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 > Switches: Switch Details** screen or click the **details** link next to a port in the **Switch > Configure > Switch ports** screen.

Figure 76 Switch > Monitor > Switches: Switch Details: Port Details



The following table describes the labels in this screen.

Table 66 Switch > Monitor > Switches: Switch Details: Port Details



LABEL	DESCRIPTION
	Click this button to reload the data-related frames on this page.
Switch / Port	Select to view the port information and connection status in the past two hours, day, week or month.
Port	<p>This drawing shows the ports on the switch.</p> <p>Click a port to go to the corresponding port details screen. The selected port is highlighted. Move the pointer over a port to see additional port information, such as its name, MAC address, type, and connection speed.</p> <p>The port color indicates the connection status of the port.</p> <ul style="list-style-type: none"> Gray (#888888): The port is disconnected. Orange (#FF8900): The port is connected and is transmitting data at 10 or 100 Mbps. Green (#64BE00): The port is connected and is transmitting data at 1000 Mbps (1 Gbps). Azure (#0079FF): The port is connected and is transmitting data at 2.5 Gbps. Violet (#8800FF): The port is connected and is transmitting data at 5 Gbps. Blue (#004FEE): The port is connected and is transmitting data at 10000 Mbps (10 Gbps). <p>When the port is in the STP blocking state, a blocked icon displays on top of the port ( for example) in the diagram.</p>
Name	This shows the descriptive name of the port.
Status	This shows the connection status of the port.
MAC address	This shows the MAC address of the port.
Type	This shows the port type (Trunk or Access), PVID, and allowed VLANs.
Speed	This shows the current connection speed of the port. If the speed is unavailable, this displays "Ethernet".
LLDP	This shows the LLDP information received on the port.
Configuration	
Click the edit icon to open the Switch ports screen and show the port(s) that match the filter criteria (the selected port number). See Section 7.3.1 on page 185 .	
Summary	This shows the port's VLAN settings.
RSTP	This shows whether RSTP is disabled or enabled on the port.
Port mirroring	This shows whether traffic is mirrored on the port.
Status	
Name	This shows the name of the port.
Status	This shows the status of the port.
LLDP	This shows the LLDP (Link Layer Discovery Protocol) information received on the port.
History	Click Event log to go to the Switch > Monitor > Event log screen.
Bandwidth Utilization	
Current Utilization	This shows what percentage of the upstream/downstream bandwidth is currently being used by the port.
Maximum Utilization	This shows the maximum upstream/downstream bandwidth utilization (in percentage).
Minimum Utilization	This shows the minimum upstream/downstream bandwidth utilization (in percentage).
y-axis	The y-axis represents the transmission rate in Kbps (kilobits per second).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Power Consumption	
Total	This shows the total power consumption of the port.

Table 66 Switch > Monitor > Switches: Switch Details: Port Details (continued)

LABEL	DESCRIPTION
Current Consumption	This shows the current power consumption of the port.
Maximum Consumption	This shows the maximum power consumption of the port.
Minimum Consumption	This shows the minimum power consumption of the port.
y-axis	The y-axis shows how much power is used in Watts.
x-axis	The x-axis shows the time period over which the power consumption is recorded.
Packets Counters	
TX/RX Unicast	This shows the number of good unicast packets transmitted/received on the port.
TX/RX Multicast	This shows the number of good multicast packets transmitted/received on the port.
TX/RX Broadcast	This shows the number of good broadcast packets transmitted/received on the port.
TX/RX Pause	This shows the number of 802.3x Pause packets transmitted/received on the port.
IGMP V2/V3	
Query Rx	This shows the number of IGMP query packets received on the port.
Report Rx	This shows the number of IGMP report packets received on the port.
Report Tx	This shows the number of IGMP report packets transmitted on the port.
Report Drops	This shows the number of IGMP report packets dropped on the port.
Leave Rx	This shows the number of IGMP leave packets received on the port.
Leave Tx	This shows the number of IGMP leave packets transmitted on the port.
Leave Drops	This shows the number of IGMP leave packets dropped on the port.
Error Packets	
RX CRC	This shows the number of packets received with CRC (Cyclic Redundant Check) 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	<p>This shows the IP address of the incoming frame which is forwarded on the port.</p> <p>Note: The IP address is obtained using one of the following three methods:</p> <ul style="list-style-type: none"> • LLDP remote information • Information collected by the Nebula Security Gateway (NSG) in this site. • Information collected by NCC when the client connected to Nebula.
MAC Address	This shows the MAC address of the incoming frame which is forwarded on the port.
VLAN	This shows the VLAN group to which the incoming frame belongs.
Cable Diagnostics	
Diagnose	Click Diagnose to perform a physical wire-pair test of the Ethernet connections on the port. The following fields display when you diagnose a port.
Channel	<p>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.</p> <p>This displays the descriptive name of the wire-pair in the cable.</p>

Table 66 Switch > Monitor > Switches: Switch Details: Port Details (continued)

LABEL	DESCRIPTION
Pair Status	<p>OK: The physical connection between the wire-pair is okay.</p> <p>Open: There is no physical connection (an open circuit detected) between the wire-pair.</p> <p>Short: There is a short circuit detected between the wire-pair.</p> <p>Unknown: The Switch failed to run cable diagnostics on the cable connected this port.</p> <p>Unsupported: The port is a fiber port or it is not active.</p>
Cable Length	<p>This displays the total length of the Ethernet cable that is connected to the port when the Pair Status is OK and the switch chipset supports this feature.</p> <p>This shows N/A if the Pair Status is Open or Short. Check the Distance to fault.</p> <p>This shows Unsupported if the switch chipset does not support to show the cable length.</p>
Distance to fault (m)	<p>This displays the distance between the port and the location where the cable is open or shorted.</p> <p>This shows N/A if the Pair Status is OK.</p> <p>This shows Unsupported if the switch chipset does not support to show the distance.</p>
DDMI	This section is available only on an SFP (Small Form Factor Pluggable) port.
DDMI	Click DDMI (Digital Diagnostics Monitoring Interface) to display real-time SFP transceiver information and operating parameters on the port. You can also see the alarm and warning thresholds for temperature, voltage, transmission bias, transmission and receiving power.
Port	This shows the number of the port on the switch.
Vendor	This shows the vendor name of the transceiver installed in the port.
PN	This shows the part number of the transceiver installed in the port.
SN	This shows the serial number of the transceiver installed in the port.
Revision	This shows the firmware version of the transceiver installed in the port.
Date-code	This shows the date the installed transceiver's firmware was created.
Transceiver	This shows the type and the Gigabit Ethernet standard supported by the transceiver installed in the port.
Calibration	This shows whether the diagnostic information is internally calibrated or externally calibrated.
Current	This shows the current operating parameters on the port, such as transceiver temperature, laser bias current, transmitted optical power, received optical power and transceiver supply voltage.
High Alarm Threshold	This shows the high alarm threshold for temperature, voltage, transmission bias, transmission and receiving power. A trap is sent when the operating parameter is above the threshold.
High Warn Threshold	This shows the high warning threshold for temperature, voltage, transmission bias, transmission and receiving power.
Low Warn Threshold	This shows the low alarm threshold for temperature, voltage, transmission bias, transmission and receiving power. A trap is sent when the operating parameter is below the threshold.
Low Alarm Threshold	This shows the low warning threshold for temperature, voltage, transmission bias, transmission and receiving power.

7.2.2 Clients

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

Figure 77 Switch > Monitor > Clients

Switch > Monitor > Clients

Clients Last 2 hours

Search clients... 7 clients

Export

Status	Description	MAC address	Connected to	Port	VLAN	First seen	Last seen	LLDP	IPv4
	NS	9C:42:1E:93:9F:88	Home NSW100	4	100	2019-10-30 00:54:17	2019-10-30 02:44:25		192.168.1.1
	NAPI02	8C:8F:8F:8F:8F:8F	Home NSW100	4	1	2019-10-30 00:54:17	2019-10-30 02:49:26		100.25.1.1
	Xiaomi Lamp	7C:4B:4B:3A:3A:3A	Home NSW100	4	100	2019-10-30 00:54:17	2019-10-30 02:49:26		192.168.1.1
	Mix2s	9C:3E:4F:4B:AA:77	Home NSW100	4	100	2019-10-30 00:54:17	2019-10-30 01:19:20		192.168.1.1
	Vaccum	5C:4C:5D:1B:8A:7F	Home NSW100	4	100	2019-10-30 00:54:17	2019-10-30 02:49:26		192.168.1.1
	bayardoipad	8C:2B:C7:4A:2A:77	Home NSW100	4	100	2019-10-30 00:54:17	2019-10-30 02:49:26		192.168.1.1
	Xiaomi A2	4B:3C:4D:5E:6F:7F	Home NSW100	4	100	2019-10-30 00:54:17	2019-10-30 02:49:26		192.168.1.1

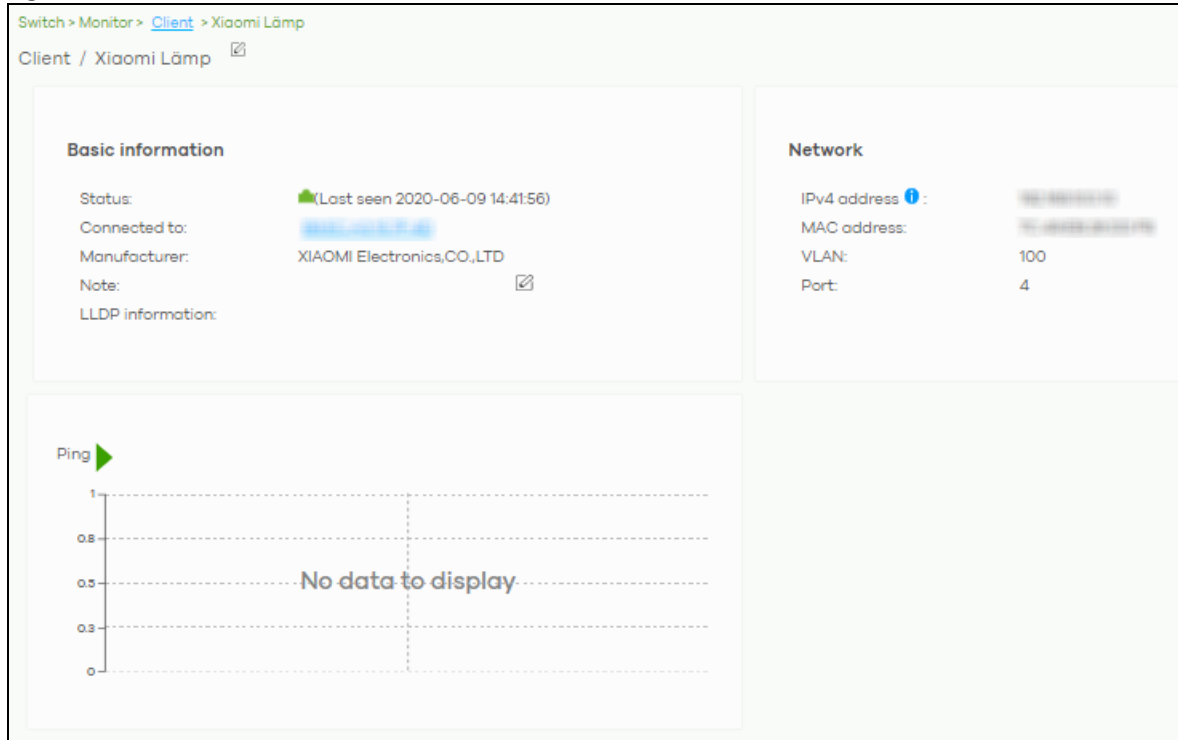
The following table describes the labels in this screen.

Table 67 Switch > Monitor > Clients

LABEL	DESCRIPTION
Switch - Client	Select to view the device information and connection status in the past two hours, day, week or month.
	Click this button to reload the data-related frames on this page.
Search	Specify your desired filter criteria to filter the list of clients.
Clients	This shows the number of clients connected to a switch in 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 offline (red).
Description	This shows the descriptive name of the client. Click the name to display the individual client statistics. See Section 7.2.2.1 on page 174 .
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 Section 7.2.1.1 on page 164 .
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. Move the cursor over the information icon to see how the IP address information is obtained.
	Click this icon to display a greater or lesser number of configuration fields.

7.2.2.1 Client Details

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

Figure 78 Switch > Monitor > Clients: Client Details

The following table describes the labels in this screen.

Table 68 Switch > Monitor > Clients: Client Details

LABEL	DESCRIPTION
Basic Information	
Status	This shows whether the client is online (green) or went off-line (red). It also shows the last date and time the client was discovered.
Connected to	This shows the name of the switch to which the client is connected.
Note	Enter information about this device, for yourself or for other administrators.
LLDP information	This shows the LLDP (Link Layer Discovery Protocol) information received from the remote device.
Manufacturer	This shows the manufacturer of the client device.
Network	
IPv4 address	This shows the IP address of the client. Note: The IP address is obtained using one of the following three methods: <ul style="list-style-type: none"> • LLDP remote information • Information collected by the Nebula Security Gateway (NSG) in this site. • Information collected by NCC when the client connected to Nebula.
MAC address	This shows the MAC address of the client.
VLAN	This shows the ID number of the VLAN to which the client belongs.
Port	This shows the switch port that the client is connected to. Note: If the client is connected wirelessly to an AP, then the port number shows the port that the AP is connected to.
Ping	Click the button to ping the client's IP address from the switch to test connectivity.

7.2.3 Event Log

Use this screen to view switch log messages. You can enter the switch name or a key word, select one or multiple event types, or specify a date/time or even a time range to display only the log messages related to it.

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

Figure 79 Switch > Monitor > Event log

Switch > Monitor > [Event log](#)

Event log

Switch: Keyword: Priority: Category:

Tag:

From: 10:20 To: 11:20 UTC+8

Range 8 Event log

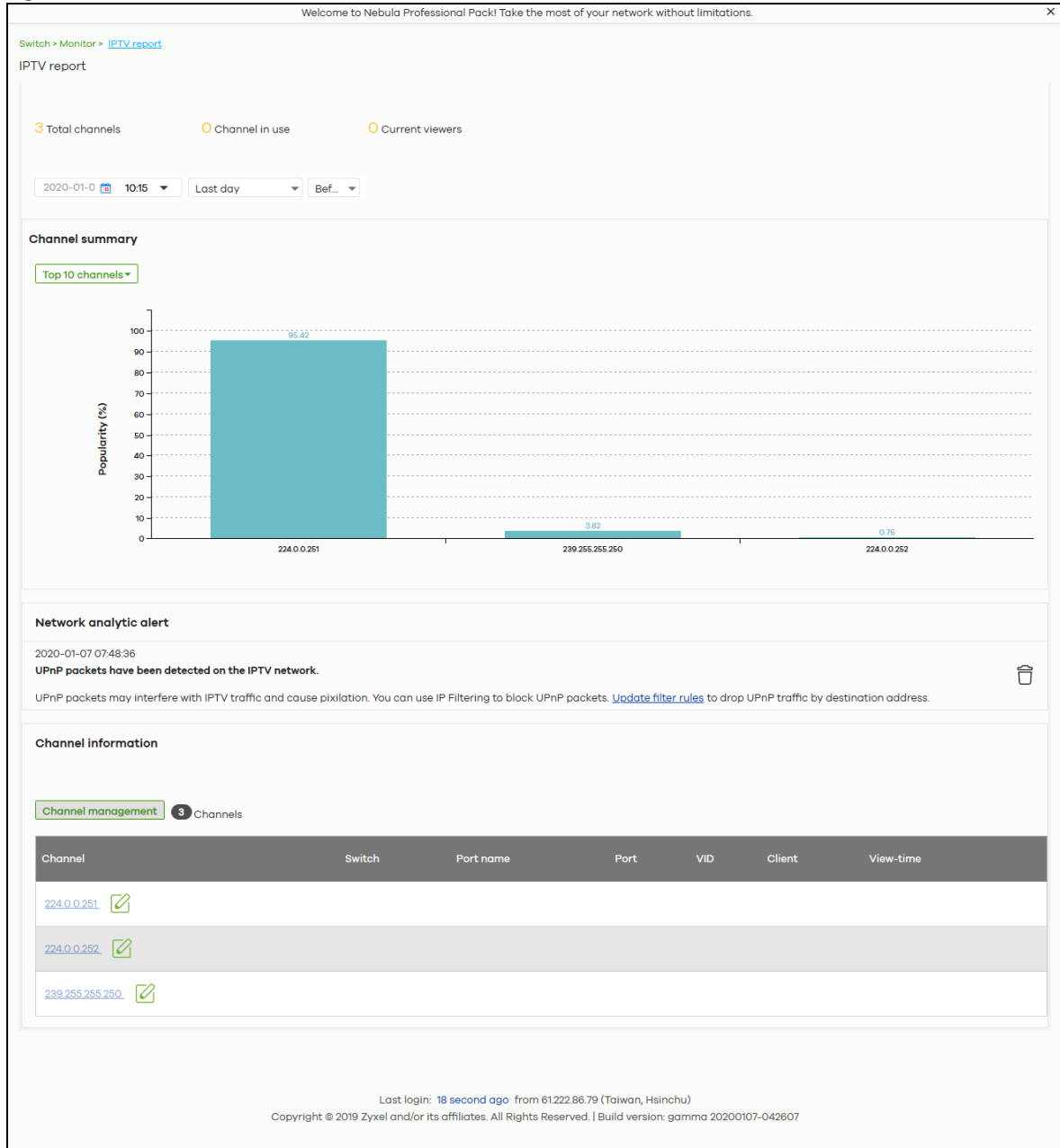
Time	Priority	Switch	Tag	Category	Detail
2019-10-29 20:26:11	Information	Home NSW100	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-29 20:45:...	Information	Home NSW100	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-29 22:17:50	Information	Home NSW100	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 06:13:...	Information	Home NSW100	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 07:04:...	Information	Home NSW100	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 08:31:52	Information	Home NSW100	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 08:44:...	Information	Home NSW100	interface	Interface	Broadcast storm detected on port 4 - P...
2019-10-30 09:04:...	Information	Home NSW100	interface	Interface	Broadcast storm detected on port 4 - P...

7.2.4 IPTV Report

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

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

Figure 80 Switch > Monitor > IPTV Report



The following table describes the labels in this screen.

Table 69 Switch > Monitor > 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 Search . You can also select Range in the second field, set a time range and click Search to display only the channels available within the specified period of time.

Table 69 Switch > Monitor > IPTV Report (continued)

LABEL	DESCRIPTION				
Channel Summary					
	<p>Select to view the channels according to the ranking. Alternatively, select Select channels to choose specific channels and click Apply.</p> <div data-bbox="537 359 901 716"> <p><input checked="" type="radio"/> Top 10 channels</p> <p><input type="radio"/> Top 11 to 20 channels</p> <p><input type="radio"/> Bottom 11 to 20 channels</p> <p><input type="radio"/> Bottom 10 channels</p> <p><input type="radio"/> Select channels (10 channels max)</p> </div>				
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 Management	<p>Download the channel list and import multiple records for faster channel naming. Click Add to download new channels and click OK.</p> <div data-bbox="537 1150 1393 1585"> <p>Channel management ✕</p> <p>You can download the channel list here and import multiple records for faster channel naming</p> <table border="1"> <thead> <tr> <th>Channel address</th> <th>Channel name</th> </tr> </thead> <tbody> <tr> <td>239.255.255.250 ✕ *</td> <td>Kids friendly channel ✕ *</td> </tr> </tbody> </table> <p>+ Add</p> <p>Close OK</p> </div>	Channel address	Channel name	239.255.255.250 ✕ *	Kids friendly channel ✕ *
Channel address	Channel name				
239.255.255.250 ✕ *	Kids friendly channel ✕ *				
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 Section 7.2.4.1 on page 179.</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.				

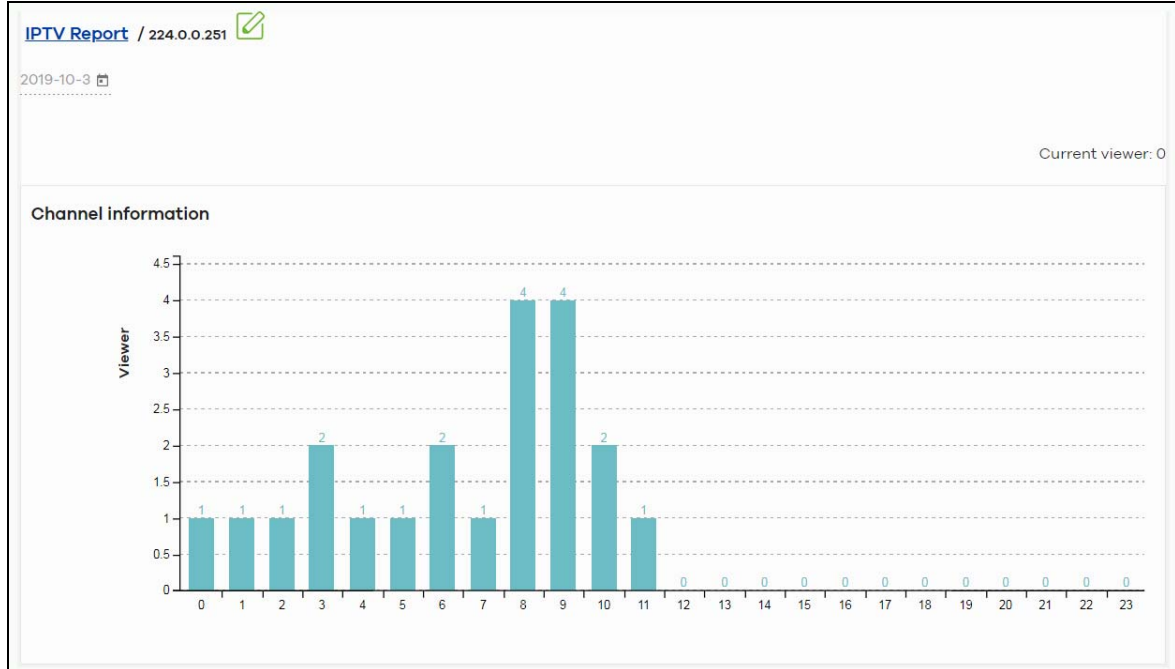
Table 69 Switch > Monitor > IPTV Report (continued)

LABEL	DESCRIPTION
Client	This shows the IP address of the client who is watching the TV program on the channel.
View-time	This shows the amount of time the client has spent watching the IPTV channel.

7.2.4.1 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 81 Switch > Monitor > IPTV Report: Channel Information



The following table describes the labels in this screen.

Table 70 Switch > Monitor > IPTV Report: Channel Information

LABEL	DESCRIPTION
	Select a specific date to display only the clients who watch the IPTV channel on that day.
Current Viewer	This shows the number of clients who are currently watching the IPTV channel.
y-axis	The y-axis shows the number of clients watching the IPTV channel.
x-axis	The x-axis shows the hour of the day in 24-hour format.
Switch	This shows the name of the 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.

7.2.5 Surveillance

Use this screen to view information about Powered Devices (PDs) connected to ports on the switch.

Click **Switch > Monitor > Surveillance** to access this screen.

Figure 82 Switch > Monitor > Surveillance

Switch/Port	Port name	PD health	Link speed	PoE draw(W)	Bandwidth (Kbps)	CRC	Extended range
GS1350-18HP/1	Port1	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Enable
GS1350-18HP/2	Port2	Auto-1000M	Auto-1000M	4.2W	Tx: 76.68 Rx: 0.93	0	Disable
GS1350-18HP/3	Port3	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable
GS1350-18HP/4	Port4	Auto-1000M	Auto-1000M	7.3W	Tx: 75.97 Rx: 0.06	0	Disable
GS1350-18HP/5	Port5	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable
GS1350-18HP/6	Port6	Auto-1000M	Auto-1000M	3.4W	Tx: 76.54 Rx: 1.05	0	Disable
GS1350-18HP/7	Port7	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable
GS1350-18HP/8	Port8	Auto-1000M	Auto-1000M	3.5W	Tx: 76.64 Rx: 1.01	0	Disable
GS1350-18HP/9	Port9	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable
GS1350-18HP/10	Port10	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable
GS1350-18HP/11	Port11	Offline	Offline	0.0W	Tx: 0.00 Rx: 0.00	0	Disable

The following table describes the labels in this screen.

Table 71 Switch > Monitor > Surveillance

LABEL	DESCRIPTION
Switch/Port	This shows the port number of the switch.
Port Name	This shows the port description on the switch.
PD Health	<p>This shows the status of auto PD recovery on this port.</p> <ul style="list-style-type: none"> Red: The switch failed to get information from the PD connected to the port using LLDP, or the connected PD did not respond to the switch's ping requests. Yellow: The switch is restarting the connected PD by turning the power off and turning it on again. Green: The switch successfully discovered the connected PD using LLDP or ping. --: Auto PD Recovery is not enabled on the switch and/or the port, or the switch is not supplying power to the connected PD. <p>Note: For details on configuring auto PD recovery on a port, see Section 7.3.1 on page 185.</p>
Link Speed	This shows the speed (either 10M for 10Mbps, 100M for 100Mbps, or 1G for 1 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device.

Table 71 Switch > Monitor > Surveillance

LABEL	DESCRIPTION
PoE Draw	This shows the total power that the connected PD draws from the port, in watts. This allows you to plan and use within the power budget of the switch.
Bandwidth Tx/Rx Kbps	Tx shows the number of kilobytes per second transmitted on this port. Rx shows the number of kilobytes per second received on this port.
CRC	This shows the number of packets received with CRC (Cyclic Redundant Check) errors.
Extended Range	This shows whether extended range is enabled on the port.
System name	This shows the name of the connected PD.
IP	This shows the IP address of the connected PD.
Discovered Devices	This shows how many devices are connected to the port. Click the number to go to the Surveillance Port Details screen.

7.2.6 Surveillance Port Details

Use this screen to view detailed information about a port on the **Surveillance** screen.

Go to **Switch > Monitor > Surveillance** and click on a value in the **Discovered Devices** column to access this screen.

Figure 83 Switch > Monitor > Surveillance > Port Details

Switch > Monitor > Surveillance > GS1350-18HP > Port 2

Surveillance / GS1350-18HP / Port 2
Last 2 hours

Status

Link speed:	Auto-1000M	Bandwidth Tx/Rx(Kbps):	82.90/0.62
PoE draw:	3.7 W	CRC:	0
PD health:		Power cycle:	<button>Reset</button>
Extended range:	Disable		

Neighbor detail

1 clients
Flush

Status	System name	Port	IP	Firmware	Description
	NAP102	1	192.168.137.32	ZLD 6.00(##.3)b1...	lan

The following table describes the labels in this screen.

Table 72 Switch > Monitor > Surveillance > Port Details

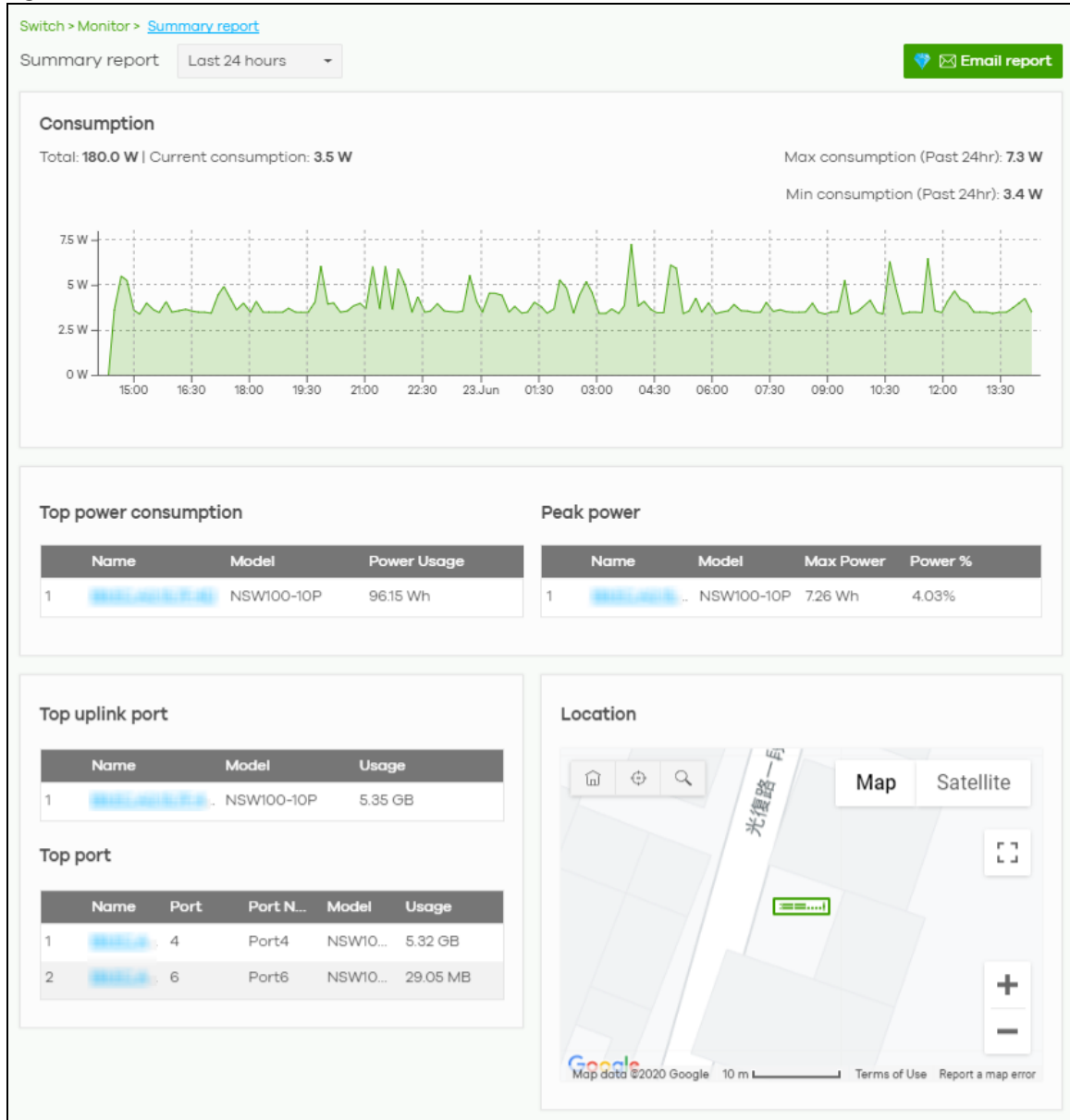
LABEL	DESCRIPTION
Status	
Link speed	This shows the speed (either 10M for 10Mbps, 100M for 100Mbps, or 1G for 1 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device.
PoE draw	This shows the total power that the connected PD draws from the port, in watts. This allows you to plan and use within the power budget of the switch.
PD health	<p>This shows the status of auto PD recovery on this port.</p> <ul style="list-style-type: none"> Red: The switch failed to get information from the PD connected to the port using LLDP, or the connected PD did not respond to the switch's ping requests. Yellow: The switch is restarting the connected PD by turning the power off and turning it on again. Green: The switch successfully discovered the connected PD using LLDP or ping. --: Auto PD Recovery is not enabled on the switch and/or the port, or the switch is not supplying power to the connected PD. <p>For details on configuring auto PD recovery on a port, see Section 7.3.1 on page 185.</p>
Extended range	This shows whether extended range is enabled on the port.
Bandwidth Tx/Rx (%)	Tx shows the number of kilobytes per second transmitted on this port. Rx shows the number of kilobytes per second received on this port.
CRC	This shows the number of packets received with CRC (Cyclic Redundant Check) errors.
Power cycle	Click Reset to power off the PD connected to the port, by temporarily disabling then re-enabling PoE.
Neighbor detail	This section shows all clients connected to the port.
Search clients	Search for one or more clients in the list by keyword, status, system name, port, IP address, or firmware version.
clients	This shows the number of clients connected to this port.
Flush	Click this to remove all offline clients from the list.
Status	This shows whether the client is online (green) or offline (red), and whether the client is wired or wireless.
System name	This displays the system name of the device.
Port	This displays the number of the device port that is connected to the switch.
IP	This shows the IP address of the device.
Firmware	This shows the firmware version currently installed on the device.
Description	This shows the descriptive name of the device.

7.2.7 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 84 Switch > Monitor > Summary Report



The following table describes the labels in this screen.

Table 73 Switch > Monitor > Summary Report

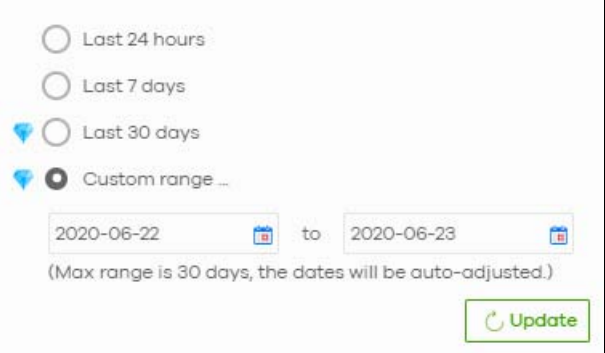
LABEL	DESCRIPTION
Switch - Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select Custom range... to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click this button to send summary reports by email, change the logo and set email schedules.
Consumption	
Total	This shows the total power consumption of the switch ports.
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 ranking of the Nebula switch.
Name	This shows the descriptive name of the Nebula switch.
Model	This shows the model number of the Nebula switch.
Power Usage	This shows the total amount of power consumed by the Nebula switch's connected PoE device(s) during the specified period of time.
Peak Power	
	This shows the ranking of the Nebula switch.
Name	This shows the descriptive name of the Nebula switch.
Model	This shows the model number of the Nebula switch.
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 by connected PoE powered devices.
Top uplink port	
	This shows the ranking of the Nebula switch.
Name	This shows the descriptive name of the Nebula switch.
Model	This shows the model number of the Nebula switch.
Usage	This shows the amount of data that has been transmitted through the switch's uplink port.
Top port	
	This shows the ranking of the Nebula switch port.

Table 73 Switch > Monitor > Summary Report (continued)

LABEL	DESCRIPTION
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.

7.3 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.

7.3.1 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 85 Switch > Configure > Switch ports

Switch > Configure > Switch ports

Switch ports Last 2 hours

Edit Aggregate Split Tag Search ports... 2 selected in 38 Switch ports Export

Switch / Port	# Port	Port name	Allowed VLAN	Broadcast (pps)	Connection	DLF (pps)	Enabled	LLDF
<input checked="" type="checkbox"/> Office NSW200/1 details	1	Port1	all	100		100	Enabled	Enable
<input checked="" type="checkbox"/> Office NSW200/2 details	2	Port2	all	100		100	Enabled	Enable
<input type="checkbox"/> Office NSW200/3 details	3	Port3	all	100		100	Enabled	Enable
<input type="checkbox"/> Office NSW200/4 details	4	Port4	all	100		100	Enabled	Enable
<input type="checkbox"/> Office NSW200/5 details	5	Port5	all	100		100	Enabled	Enable
<input type="checkbox"/> Office NSW200/6 details	6	Port6	all	100		100	Enabled	Enable
<input type="checkbox"/> Office NSW200/7 details	7	Port7	all	100		100	Enabled	Enable
<input type="checkbox"/> Office NSW200/8 details	8	Port8	all	100		100	Enabled	Enable
<input type="checkbox"/> Office NSW200/9 details	9	Port9	all	100		100	Enabled	Enable
<input type="checkbox"/> Office NSW200/10 details	10	Port10	all	100		100	Enabled	Enable

Page 1 of 4 Results per page: 10

The following table describes the labels in this screen.

Table 74 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.
	Click this button to reload the data-related frames on this page.
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. You can filter the search by selecting one or more switches. Under Ports, you can search for multiple ports separated by a comma, or a range separated by a hyphen. For example: 1,2,4-6.
Switch ports	This shows the number of ports on the switch.
Export	Click this button to save the switch port list as a CSV or XML file to your computer.
Switch/Port	This shows the switch name and port number. If the port is added to a trunk group, this also shows whether it is configured as a static member of the trunk group (Static) or configured to join the trunk group via LACP (LACP). If the port is connected to an uplink gateway, it shows Uplink . Click details to display the port details screen. See Section 7.2.1.3 on page 169 .
Port name	This shows the descriptive name of the port.
#Port	This shows the port number.
LLDP	This shows whether Link Layer Discovery Protocol (LLDP) is supported on the port.
Received broadcast packets	This shows the number of good broadcast packets received.
Received bytes	This shows the number of bytes received on this port.
Received packets	This shows the number of received frames on this port.
Sent broadcast packets	This shows the number of good broadcast packets transmitted.
Sent bytes	This shows the number of bytes transmitted on this port.
Sent multicast packets	This shows the number of good multicast packets transmitted.
Received multicast packets	This shows the number of good multicast packets received.
Sent packets	This shows the number of transmitted frames on this port.
Total bytes	This shows the total number of bytes transmitted or received on this port.
Enabled	This shows whether the port is enabled or disabled.
Link	This shows the speed of the Ethernet connection on this port. Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support.

Table 74 Switch > Configure > Switch ports (continued)

LABEL	DESCRIPTION
Connection	<p>This shows the connection status of the port.</p> <ul style="list-style-type: none"> Gray (#888888): The port is disconnected. Orange (#FF8900): The port is connected and is transmitting data at 10 or 100 Mbps. Green (#64BE00): The port is connected and is transmitting data at 1000 Mbps (1 Gbps). Azure (#0079FF): The port is connected and is transmitting data at 2.5 Gbps. Violet (#8800FF): The port is connected and is transmitting data at 5 Gbps. Blue (#004FEE): The port is connected and is transmitting data at 10000 Mbps (10 Gbps). <p>When the port is in the STP blocking state, a blocked icon displays.</p> <p>Move the cursor over a time slot to see the actual date and time when a port is connected or disconnected.</p>
RADIUS policy	This shows the name of RADIUS authentication policy applied to the port.
Allowed VLAN	This shows the VLANs from which the traffic comes is allowed to be transmitted or received on the port.
PoE	This shows whether PoE is enabled on the port.
RSTP	This shows whether RSTP is enabled on the port.
Status	<p>If STP/RSTP is enabled, this field displays the STP state of the port.</p> <p>If STP/RSTP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays Disabled.</p>
Schedule	This shows the name of the PoE schedule applied to the port.
Type	This shows the port type (Trunk or Access).
PVID	This shows the port VLAN ID. It is a tag that adds to incoming untagged frames received on the port so that the frames are forwarded to the VLAN group that the tag defines.
Tag	This shows the user-specified tag that the 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 Destination Lookup Failure (DLF) packets the switch accepts per second on this port.
Loop Guard	This shows whether loop guard is enabled or disabled on the port.
Network analytic alert	An amber alert icon displays if the NCC generates alerts when an error or something abnormal is detected on the port for the IPTV network. Move the cursor over the alert icon to view the alert details.
Number of IGMP Group	This shows the number of IGMP groups the port has joined.
	Click this icon to display a greater or lesser number of configuration fields.

7.3.1.1 Update ports

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

Figure 86 Switch > Configure > Switch ports: Edit

The following table describes the labels in this screen.

Table 75 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).
STP guard	This field is available only when RSTP is enabled on the port(s). Select Root guard to prevent the switch(es) attached to the port(s) from becoming the root bridge. Select BPDU guard to have the switch shut down the port(s) if there is any BPDU received on the port(s). Otherwise, select Disable .
LLDP	Select to enable or disable LLDP on the port(s).
Link	Select the speed and the duplex mode of the Ethernet connection on the port(s). Choices are Auto-1000M , 10M/Half Duplex , 10M/Full Duplex , 100M/Half Duplex , 100M/Full Duplex and 1000M/Full Duplex (Gigabit connections only).

Table 75 Switch > Configure > Switch ports: Edit (continued)

LABEL	DESCRIPTION
Extended range	<p>Select to enable or disable extended range.</p> <p>Extended range allows the port to transmit power and data at a distance of 250 meters.</p> <p>Note: When enabled, the port's PoE Power up mode is locked to 802.3at, and the port's link speed is limited to 10M/Full Duplex.</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>
RADIUS policy	<p>This field is available only when you select Access in the Type field.</p> <p>Select the name of the pre-configured RADIUS policy that you want to apply to the port(s). Select Open if you do not want to enable port authentication on the port(s).</p>
Bandwidth Control	Select to enable or disable bandwidth control on the port.
Ingress	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on the 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 cannot 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 Access to configure the port as an access port which can carry traffic for just one VLAN. Frames received on the port are tagged with the port VLAN ID.</p> <p>Select Trunk to configure the port as a trunk port which can carry traffic for multiple VLANs over a link. A trunk port is always connected to a switch or router.</p>
VLAN type	<p>This field is available only when you select Access in the Type field.</p> <p>None: This port is a regular access port and follows the device's access port rules.</p> <p>Vendor ID based VLAN: Apply the Vendor ID based VLAN settings from Switch > Configure > Switch settings to this port.</p> <p>Voice VLAN: Apply the Voice VLAN settings from Switch > Configure > Switch settings to this port.</p> <p>Note: For details on configuring Vendor ID based VLAN and Voice VLAN settings, see Section 7.3.6 on page 201.</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 75 Switch > Configure > Switch ports: Edit (continued)

LABEL	DESCRIPTION
Allowed VLANs	<p>This field is available only when you select Trunk in the Type field.</p> <p>Specify the VLANs from which the traffic comes is allowed to be transmitted or received on the port(s).</p>
PoE Settings	
PoE	Select Enable to provide power to a PD connected to the ports.
PoE schedule	<p>This field is available only when you enable PoE.</p> <p>Select a pre-defined schedule (created using the Switch > Configure > PoE schedule screen) to control when the switch enables PoE to provide power on the port(s).</p> <p>Note: You must select Unschedule in the PoE schedule field before you can disable PoE on the port(s).</p> <p>If you enable PoE and select Unschedule, PoE is always enabled on the port(s).</p>
PoE 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 Low to set the switch to assign the remaining power to the port after all critical and medium priority ports are served.</p> <p>Select Medium to set the switch to assign the remaining power to the port after all critical priority ports are served.</p> <p>Select Critical to give the highest PD priority on the port.</p>
Power up mode	<p>Set how the switch provides power to a connected PD at power-up.</p> <p>802.3at - 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> <p>802.3af - the switch follows the IEEE 802.3af Power over Ethernet standard to supply power to the connected PDs during power-up.</p> <p>Legacy - 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>Pre-802.3at - 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>
Auto PD recovery	<p>Select to enable or disable automatic PD recovery on the port.</p> <p>Automatic PD recovery allows the switch to restart a Powered Device (PD) connected to the port by turning the device on and off again.</p>
Detecting mode	<p>Select LLDP to have the Switch passively monitor current status of the connected Powered Device (PD) by reading LLDP packets from the PD on the port.</p> <p>Select Ping to have the Switch ping the IP address of the connected Powered Device (PD) through the designated port to test whether the PD is reachable or not.</p>

Table 75 Switch > Configure > Switch ports: Edit (continued)

LABEL	DESCRIPTION
Action	<p>Set the action to take when the connected Powered Device (PD) has stopped responding.</p> <p>Select Reboot-Alarm to have the Switch send an SNMP trap and generate a log message, and then turn off the power of the connected PD and turn it back on again to restart the PD.</p> <p>Select Alarm to have the Switch send an SNMP trap and generate a log message.</p>
Neighbor IP	<p>Set the IPv4 address of the Powered Device (PD) connected to this port.</p> <p>Note: If Detecting Mode is set to Ping and the PD supports LLDP, the connected PD's IPv4 address to which the Switch sends ping requests is displayed automatically.</p>
Polling Interval	<p>Specify the number of seconds the Switch waits for a response before sending another ping request.</p> <p>For example, the Switch will try to detect the PD status by performing ping requests every 20 seconds.</p>
Polling Count	Specify how many times the Switch resends a ping request before considering the PD unreachable.
Resume Polling interval (sec)	Specify the number of seconds the Switch waits before monitoring the PD status again after it restarts the PD on the port.
PD Reboot Count	<p>Specify how many times the Switch attempts to restart the PD on the port.</p> <p>The PD Reboot Count resets if any of the following conditions are true:</p> <ul style="list-style-type: none"> • The switch successfully pings the PD. • You modify any Auto PD Recovery settings and apply them. • The switch restarts.
Resume Power Interval (sec)	Specify the number of seconds the Switch waits before supplying power to the connected PD again after it restarts the PD on the port.
IPTV Setting	
Overwrite advanced IGMP setting	Select ON to overwrite the port's advanced IGMP settings (configured in the Configure > Advanced IGMP screen) with the settings you configure in the fields below. Otherwise, select OFF .

Table 75 Switch > Configure > Switch ports: Edit (continued)

LABEL	DESCRIPTION
Leave Mode	<p>Select Immediate Leave to remove this port from the multicast tree immediately when an IGMP leave message is received on this port. Select this option if there is only one host connected to this port.</p> <p>Select Normal Leave or Fast Leave 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 Enable and enter the maximum number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report received on this port will replace the earliest group entry in the multicast forwarding table.</p> <p>Otherwise, select Disable 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 No Select to remove restrictions and allow the port to join any multicast group.</p>
Fixed Router Port	<p>Select Auto 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.</p> <p>Select Fixed 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.</p>

7.3.2 ACL

ACL lets you allow or block traffic going through the switches according to the rule settings. Use this screen to configure ACL rules on the switches.

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

Figure 87 Switch > Configure > ACL

Switch > Configure > ACL

ACL

Management rules [What is this?](#)

To ensure management connectivity with Nebula Control Center (NCC), IP Address specified for management rules are added to the IP filtering list by default configuration. This implies that traffics to and from the listed management IP address are permitted on the devices.

Note: Security policy information are permitted on the devices at all time to ensure smooth network operation.

Nebula control center IP address

52.19.85.221


Customization rules

	Enabled	Policy	Protocol	Source MAC	Source IP	Src port	Destination MAC	Destinat
1	On	Allow	Any	e.g.00:12:34:00:00:00/00:00:00:00:00:00	e.g.192.168.1.0/24	any	e.g.00:12:34:00:00:00/00:00:00:00:00:00	e.g.192.
	Allow	Any	Any	Any	Any	Any	Any	Any

[+ Add](#)

The following table describes the labels in this screen.

Table 76 Switch > Configure > IP filtering

LABEL	DESCRIPTION
Management rules	The NCC automatically creates rules to allow traffic from/to the Nebula Control Center IP addresses in the list.
Customization rules	
	Click the icon of a rule and drag the rule up or down to change the order.
Enabled	Select the check box to turn on the rule. Otherwise, clear the check box to turn off the rule.
Policy	Select to allow or deny traffic that matches the filtering criteria in the rule.
Protocol	Select the type of IP protocol used to transport the traffic to which the rule is applied.
Source MAC	Enter the source MAC address of the packets that you want to filter.
Source IP	Enter the source IP address of the packets that you want to filter.
Src port	Enter the source port number(s) that defines the traffic type.
Destination MAC	Enter the destination MAC address of the packets that you want to filter.
Destination IP	Enter the destination IP address of the packets that you want to filter.
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.

7.3.3 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 88 Switch > Configure > Advanced IGMP

The screenshot displays the 'Advanced IGMP' configuration page. At the top, the breadcrumb 'Switch > Configure > Advanced IGMP' is visible. The page is divided into several sections:

- IGMP snooping:** A toggle switch is turned 'on'.
- IGMP-snooping VLAN:** A radio button is selected for 'Auto-detect'. Below it, a text input field is empty, and a note says 'User Assign VLANs.'.
- Unknown multicast drop:** A toggle switch is turned 'on'. Below it, a dropdown menu is set to 'All'.
- IGMP filtering profiles:** A section with a header 'IGMP filtering profiles' and a sub-header '2 IGMP filtering profiles'. It shows two profiles: 'Premium Service' used by 0 ports and 'Basic Channel' used by 0 ports. Each profile has edit and delete icons. A '+ Add' button is at the bottom.
- IPTV topology setup:** A section with tabs for 'IGMP snooping', 'Role', and 'Port settings'. The 'IGMP snooping' tab is active. It shows a table with columns: 'Switch name', 'IGMP snooping', 'Role', and 'Port settings'.

Switch name	IGMP snooping	Role	Port settings
<input checked="" type="checkbox"/> Office NSW200	on	Aggregator	Advanced setup
<input type="checkbox"/> Home NSW100	on	Querier	Advanced setup

 Below the table, there is a section for 'Querier IP interface' with columns 'VLAN', 'Querier IP interface', and 'Mask'. It shows a single entry for VLAN 1 with IP 100.25.1.35 and mask 255.255.255.0. There are edit and delete icons for each entry. A '+ Add' button is at the bottom.

The following table describes the labels in this screen.

Table 77 Switch > Configure > Advanced IGMP




LABEL	DESCRIPTION
IGMP snooping	Select ON to enable and configure IGMP snooping settings on all switches in the site. Select OFF to disable it.
IGMP-snooping VLAN	Select Auto-detect to have the switch learn multicast group membership information of any VLANs automatically. Select User Assigned VLANs 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 ON to discard the frame(s). Select OFF to send the frame(s) to all ports.
Drop on VLAN	This allows you to define the VLANs in which unknown multicast packets can be dropped.
IGMP filtering profiles	An IGMP filtering profile specifies a range of multicast groups that clients connected to the 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.
	Click the edit icon to change the profile settings. See Section 7.3.3.1 on page 196 .
	Click the remove icon to delete the profile.
Add	Click this button to create a new profile. See Section 7.3.3.1 on page 196 .
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 Port Settings screen, where you can change IGMP leave mode and IGMP filtering profile for the ports on the selected switch(es). See Section 7.3.3.2 on page 196 .
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 Settings	Click Advanced Setup to open the Port Settings screen, where you can change IGMP leave mode and IGMP filtering profile for the ports on the switch. See Section 7.3.3.2 on page 196 .
The following fields display when the IGMP role of a switch is set to Querier .	
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.

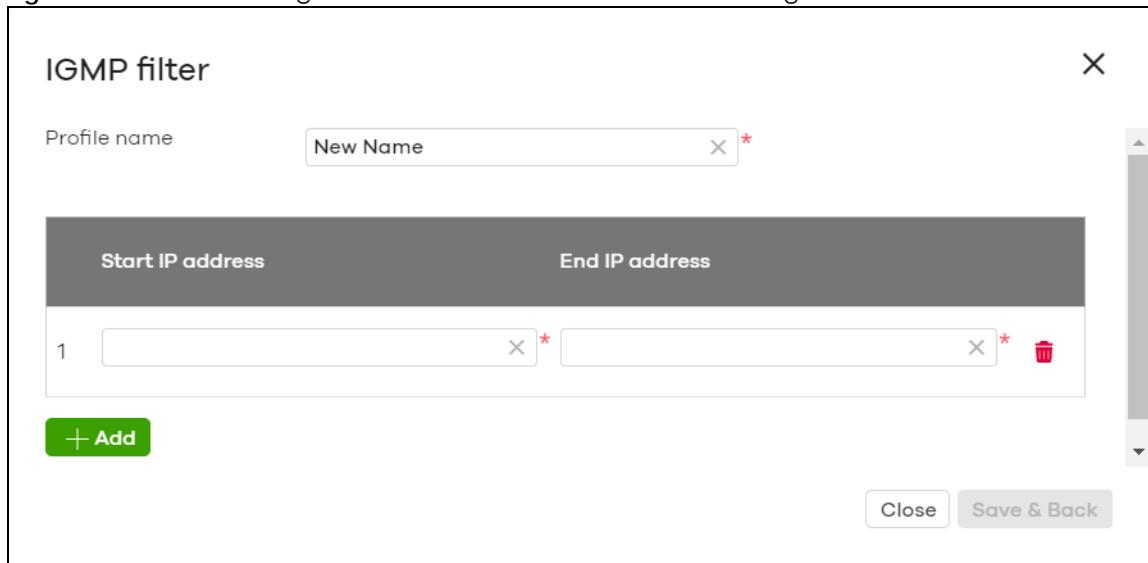
Table 77 Switch > Configure > Advanced IGMP (continued)

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

7.3.3.1 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 89 Switch > Configure > Advanced IGMP: Add IGMP Filtering Profile



The following table describes the labels in this screen.

Table 78 Switch > Configure > 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 Start IP Address and End IP Address fields.
	Click the remove icon to delete the rule.
Add	Click this button to create a new rule in this profile.
Close	Click this button to exit this screen without saving.
Save & Back	Click this button to save your changes and close the screen.

7.3.3.2 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 90 Switch > Configure > Advanced IGMP: Port Settings

Port settings X

Switch name Office NSW200

Role Aggregator

Leave mode Normal leave 4000 X*

Maximum group Disable

IGMP filtering profile No select

Close Save

The following table describes the labels in this screen.

Table 79 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 Immediate Leave 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 Normal Leave or Fast Leave 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 Enable and enter the maximum number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report received on this port will replace the earliest group entry in the multicast forwarding table.</p> <p>Otherwise, select Disable to turn off multicast group limits.</p>

Table 79 Switch > Configure > Advanced IGMP: Port Settings (continued)

LABEL	DESCRIPTION
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 No Select to remove restrictions and allow the port to join any multicast group.
Reset	Click this button to return the screen to its last-saved settings.
Close	Click this button to exit this screen without saving.
Save	Click this button to save your changes and close the screen.

7.3.4 RADIUS Policies

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

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

Figure 91 Switch > Configure > RADIUS policies

Switch > Configure > [RADIUS policies](#)

RADIUS policies

RADIUS server

	Host	Port	Secret
1	192.168.8.1	1812	XXXXXXXXXX

[+ Add](#)

RADIUS policy

Password for MAC-Base Auth:

RADIUS policy type	Guest VLAN	Port security	Limited numbers of MAC address	Switch ports (currently using this policy)
8021X	250	on	2	0
8021X	100	off	0	0

[+ Add](#)

The following table describes the labels in this screen.

Table 80 Switch > Configure > RADIUS policies




LABEL	DESCRIPTION
RADIUS server	
	Click the icon of a rule and drag the rule up or down to change the order.

Table 80 Switch > Configure > RADIUS policies (continued)

LABEL	DESCRIPTION
Host	Enter the IP address of the external RADIUS server.
Port	Enter the port of the RADIUS server for authentication (default 1812).
Secret	Enter a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch.
	Click the remove icon to delete the entry.
Add	Click this button to create a new RADIUS server entry.
RADIUS policy	
Password for MAC-Base Auth	Type the password the 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 MAC-Base if you want to validate access to the port(s) based on the MAC address and password of the client. Select 802.1x 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 On to enable port security on the port(s). Otherwise, select Off to disable port security on the port(s).
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.
	Click the remove icon to delete the profile.
Add	Click this button to create a new policy.

7.3.5 PoE Schedules

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

Note: The NCC will not generate an alert when PoE is disabled and the connected APs go off-line because of the pre-defined PoE schedules.

The table shows the name of the existing schedules and the number of ports to which a schedule is applied. Click a schedule's edit icon to modify the schedule settings or click the **Add** button to create a new schedule. See [Section 7.3.5.1 on page 200](#).

Figure 92 Switch > Configure > PoE schedules

7.3.5.1 Create new schedule

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

Figure 93 Switch > Configure > PoE schedule: Add

The following table describes the labels in this screen.

Table 81 Switch > Configure > PoE schedule: Add

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

Table 81 Switch > Configure > PoE schedule: Add (continued)

LABEL	DESCRIPTION
Availability	Click On to enable PoE at the specified time on this day. Otherwise, select Off to turn PoE off on the day and at the specified time. Specify the hour and minute when the schedule begins and ends each day.
Close	Click this button to exit this screen without saving.
Add	Click this button to save your changes and close the screen.

7.3.6 Switch Settings

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

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

Figure 94 Switch > Configure > Switch settings

Switch > Configure > [Switch settings](#)

Switch settings

VLAN configuration

Management VLAN: ✕

STP configuration

Rapid spanning tree protocol (RSTP): ☒

STP bridge priority: [?](#)

Switches	Bridge priority
Default	32768

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

Quality of service

Quality of service:

VLAN	Priority	Description
<input type="text" value="100"/> ✕	<input type="text" value="6"/>	<input type="text" value="Personal network"/> ✕
<input type="text" value="250"/> ✕	<input type="text" value="2"/>	<input type="text" value="Guest"/> ✕

[+ Add](#)

[What is this?](#)

Port mirroring

Port mirroring: [+ Add](#) [Ask Question](#)

Voice VLAN

Voice VLAN [?](#): ☒

Voice VLAN ID: ✕

Priority:

Assign VLAN by: [Model list](#)

DSCP:

Vendor ID based VLAN

Vendor ID based VLAN [Model list](#): ☒

Vendor OUI	VLAN	Priority
1 FC:FC:48 ✕	<input type="text" value="10"/> ✕	<input type="text" value="6"/>

[+ Add Vendor-ID on this network](#)

Access management

Access management [Model list](#): ☐

Management VLAN control [?](#)

Switch name	Control ports
1 192.168.1.1	<input type="text" value="All"/> ✕
Default	All

DHCP Server Guard

DHCP Server Guard: ☐

The following table describes the labels in this screen.

Table 82 Switch > Configure > Switch settings

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 On to enable RSTP on the switch. Otherwise, select Off .
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 Add to create a new entry.</p>
Port mirroring	
Port mirroring	<p>Click Add 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>
Voice VLAN	
Voice VLAN	<p>Select On to enable the Voice VLAN feature on the switch. Otherwise, select Off.</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.
Assign VLAN by	<p>Select how the switch assigns ports connected to VoIP devices to the Voice VLAN.</p> <p>OUI (Organizationally Unique Identifier): The switch assigns a port connected to a VoIP device to the Voice VLAN if the connected device's OUI matches any OUI in the list.</p> <p>LLDP-MED: The switch assigns a port connected to a VoIP device to the voice VLAN if the connected device is identified as a VoIP device using the LLDP-MED protocol.</p> <p>Note: The device must support LLDP-MED and have LLDP-MED enabled.</p>
OUI	<p>Click Add OUI on this network to add an OUI and a description for the OUI.</p> <p>An Organizationally Unique Identifier identifies a manufacturer. Typically, a device's OUI is the first three octets of the device's MAC address.</p> <p>For example, if you have an IP phone from Company A with MAC address 00:0a:95:9d:68:16, you can enter OUI <i>00:0a:95</i> to match all devices from Company A.</p>

Table 82 Switch > Configure > Switch settings (continued)

LABEL	DESCRIPTION
DSCP	Enter the Differentiated Services Code Point (DSCP) value for traffic on the voice VLAN. The value is defined from 0 through 63, and 0 is the default.
Vendor ID based VLAN	
Vendor ID based VLAN	Select On to enable the Vendor ID based VLAN feature on the switch. Otherwise, select Off . Click the button to define the vendor MAC address OUI, assign to which VLAN, and set the priority.
Access management	
Access management	Select On to enable the access management feature on the switch. Otherwise, select Off .
Allow IP range	Click the button to set the devices' starting and ending IP addresses that will be allowed to access the switches via telnet, SSH, HTTP, HTTPS, and FTP.
Management VLAN control	This allows the administrator to set the switch ports through which device management VLAN traffic is allowed. For example, 1, 10-15, or ALL. By default, Nebula allows the device management VLAN traffic through all ports (even if Allowed VLAN in the Switch > Configure > Switch port settings is restricted). This avoids the device disconnecting from NCC during configuration.
DHCP Server Guard	
DHCP Server Guard	Select On 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 Off to disable it.

CHAPTER 8

Access Point

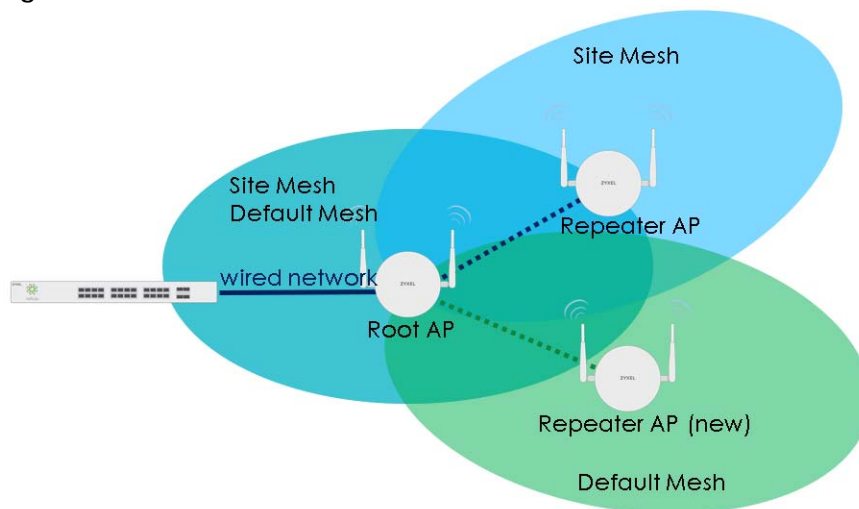
8.1 Overview

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.

8.1.1 Nebula Smart Mesh

Nebula Smart Mesh, also called Smart Mesh or AP Smart Mesh, is a WiFi mesh solution for Nebula APs. With Smart Mesh, you can have two or more Nebula APs automatically create a mesh network within your home or office, ensuring there are no areas with a weak wireless signal.

Figure 95 Nebula Smart Mesh



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

- **Root AP:** An AP that is connected to the network by Ethernet and can reach the gateway device.
- **Repeater AP:** An AP that is connected to the network wirelessly, or that is connected to the network by Ethernet but cannot reach the gateway device.

The Repeater APs rebroadcast the root AP's SSID, and then relay wireless traffic back to the gateway.

To create a Smart Mesh network, add two or more APs to the same Nebula-managed site and ensure that each AP has Smart Mesh enabled. Then connect one or more Nebula APs to your network's gateway using an Ethernet cable, so that you have at least one root AP. Finally, place one or more non-wired Nebula APs in areas where you want to extend wireless coverage.

8.1.2 Smart Mesh Network Topology

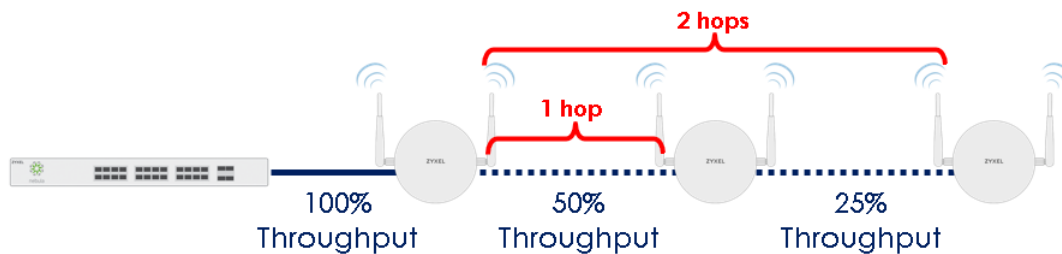
After you add a Nebula AP to an NCC site and then turn it on, the new AP automatically connects to a mesh network called the **default mesh**. The AP then tries to connect to a root AP and contact NCC. After the AP successfully contacts NCC and joins the site, the AP stops using the default mesh and instead connects to other APs in the site using a dedicated network called the **site mesh**.

8.1.2.1 Smart Mesh Wireless Hops

Each repeater AP tries to connect to the site gateway through a root AP. If a repeater AP cannot connect directly to a root AP, then the repeater AP relays its wireless traffic through another repeater AP. Each time traffic passes through a wireless connection in the mesh network, it counts as one **hop**.

Nebula Smart Mesh supports an unlimited number of hops. However, each hop in a mesh network reduces network throughput by up to half. Therefore, we recommend only allowing a maximum of two hops within your Smart Mesh network.

Figure 96 Nebula Smart Mesh Wireless Hops

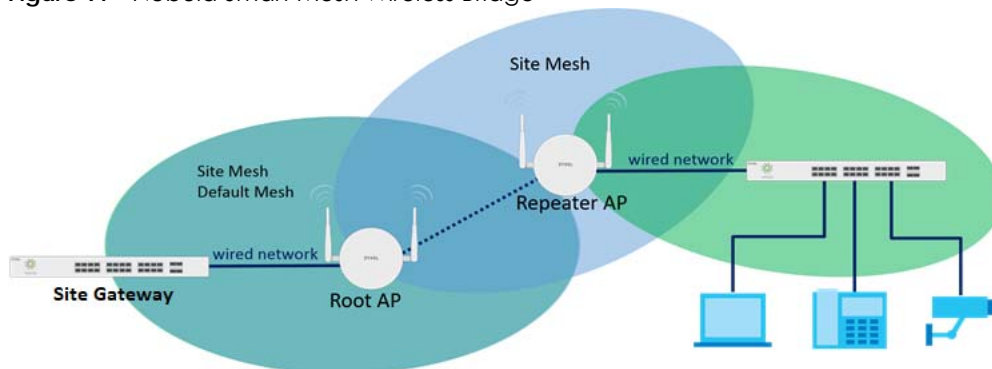


8.1.2.2 Wireless Bridge

Wireless bridge is a Smart Mesh feature that allows two Nebula APs to automatically connect two network segments together over a wireless connection. This is useful when you want to extend your wired network to a new area, but it is difficult to run cables to that area.

To use wireless bridge, enable **Wireless Bridge** on two APs in NCC. Then connect wired clients to one of the AP's LAN port. These wired clients form a new network segment and are able to reach the site gateway via the AP's wireless connection.

Figure 97 Nebula Smart Mesh Wireless Bridge



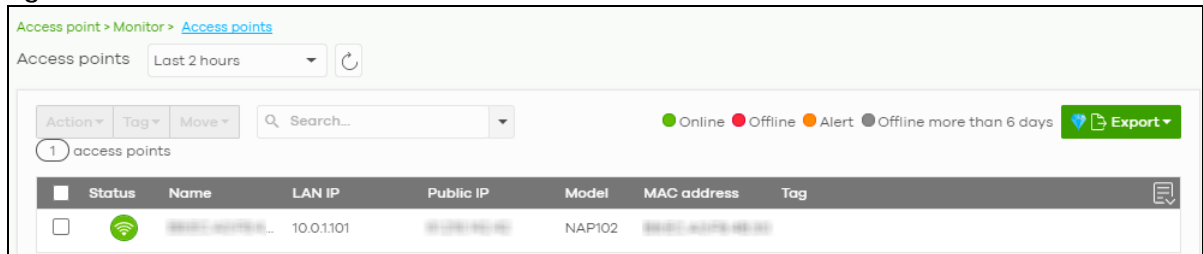
8.2 Monitor

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

8.2.1 Access Points

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

Figure 98 Access Point > Monitor > Access Points



The following table describes the labels in this screen.


Table 83 Access Point > Monitor > Access Points

LABEL	DESCRIPTION
Access point	Select to view device information and connection status in the past two hours, day, week or month.
	Click this button to reload the data-related frames on this page.
Action	Perform an action on the selected APs.
Reboot	Select this to restart the AP.
Upgrade	Select this to upgrade the firmware on the AP.
Tag	<p>Select one or multiple APs and click this button to create a new tag for the AP(s) or delete an existing tag.</p> <p>At the time of writing, there are two pre-defined tags. The LED tags have priority over the LED setting in the Site-Wide > General Setting screen.</p> <ul style="list-style-type: none"> LED_Off: this tag allows you to turn off the LED(s) (except the locator LED) on the selected APs. LED_On: this tag allows you to have the LEDs stay lit after the selected APs are ready.
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	<p>This shows the status of the AP.</p> <ul style="list-style-type: none"> Green: The AP is online and has no alerts. Amber: The AP has alerts. Red: The AP is offline. Gray: The AP has been offline for 7 days or more. : The AP is acting as a repeater. <p>For example, an alert is created and the status color is amber when the AP is transmitting data at 100 Mbps in full duplex mode or when the AP is in a Limited Power mode.</p>

Table 83 Access Point > Monitor > Access Points (continued)

LABEL	DESCRIPTION
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.
Channel Utilization	This shows the percentage of the channel ID usage.
Usage	This shows the amount of data consumed by the AP's clients.
% Usage	This shows the percentage of the AP's data usage.
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	<p>This shows the AP connection status.</p> <p>The red time slot indicates the connection to the NCC is down, and the green time slot indicates the connection is up. Move the cursor over a time slot to see the actual date and time when an AP is connected or disconnected.</p>
Ethernet 1	This shows the speed and duplex mode of the Ethernet connection on the AP's up-link port. It shows Down 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.
Uplink AP	This shows the role and descriptive name of the AP to which this AP is connected wirelessly.
Uplink Signal	Before the slash, this shows the signal strength the uplink AP (a root AP or a repeater) receives from this AP (in repeater mode). After the slash, this shows the signal strength this AP (in repeater mode) receives from the uplink AP.
Uplink Tx/Rx Rate	This is the maximum transmission/reception rate of the root AP or repeater to which the AP is connected.
Wireless bridge	<p>This shows whether wireless bridge is enabled on the AP.</p> <p>For more information about wireless bridge, see Section 8.1.2.2 on page 206.</p>
Uplink	This shows whether the AP is connected to the gateway via a wired Ethernet connection or wireless connection.

Table 83 Access Point > Monitor > Access Points (continued)


LABEL	DESCRIPTION
Power mode	<p>This shows the AP's power status.</p> <p>Full - the AP receives power using a power adapter and/or through a PoE switch/injector using IEEE 802.3at PoE plus. The PoE device that supports IEEE 802.3at PoE Plus can supply power of up to 30W per Ethernet port.</p> <p>Limited - the AP receives power through a PoE switch/injector using IEEE 802.3af PoE even when it is also connected to a power source using a power adapter. The PoE device that supports IEEE 802.3af PoE can supply power of up to 15.4W per Ethernet port.</p> <p>When the AP's power mode is Limited, the AP throughput decreases and has just one transmitting radio chain.</p> <p>It always shows Full if the AP does not support power detection.</p>
Firmware status	This shows whether the firmware installed on the AP is up-to-date.
Current version	This shows the firmware version currently installed on the AP.
	Click this icon to display a greater or lesser number of configuration fields.

8.2.1.1 AP Details

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

Figure 99 Access Point > Monitor > Access Points: AP Details Part 1







Access point > Monitor > [Access point](#) > 9F

Access point / 9F 







Configuration



Name:	9F
MAC address:	88:63:43:28:88:43
Serial number:	8754-234567-89012345
Description:	
Address:	
Tag:	
Load balancing:	

Status

LAN IP:	192.168.173.41 
	Gateway: 192.168.173.1 DNS: 192.168.173.1
Public IP:	88.138.234.187
Usage:	1.64 GB used in the last 24 hours.
Current clients:	4 client(s)
 Topology:	Show
Neighbor info:	88.138.234.187 (NSW100-10)/10/Uplink
Link:	Uplink: 1000M/Full LAN 1: Down
Ports:	LAN 1 PVID: 64 Allowed VLANs: 60, 62, 64
Channel (Band):	3 (DCS) [2.4GHz] 161*/157 [5GHz]
Channel utilization:	16% [2.4GHz] 1% [5GHz]
Power mode:	Full
Antenna:	Wall 
Smart mesh: Beta	Disabled 
 Wireless bridge: Beta	Disabled 
History:	Event log
Configuration status:	Up to date
Firmware status:	Up to date
Current version:	V6.10(ABFA.3)

Map Photo


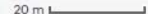
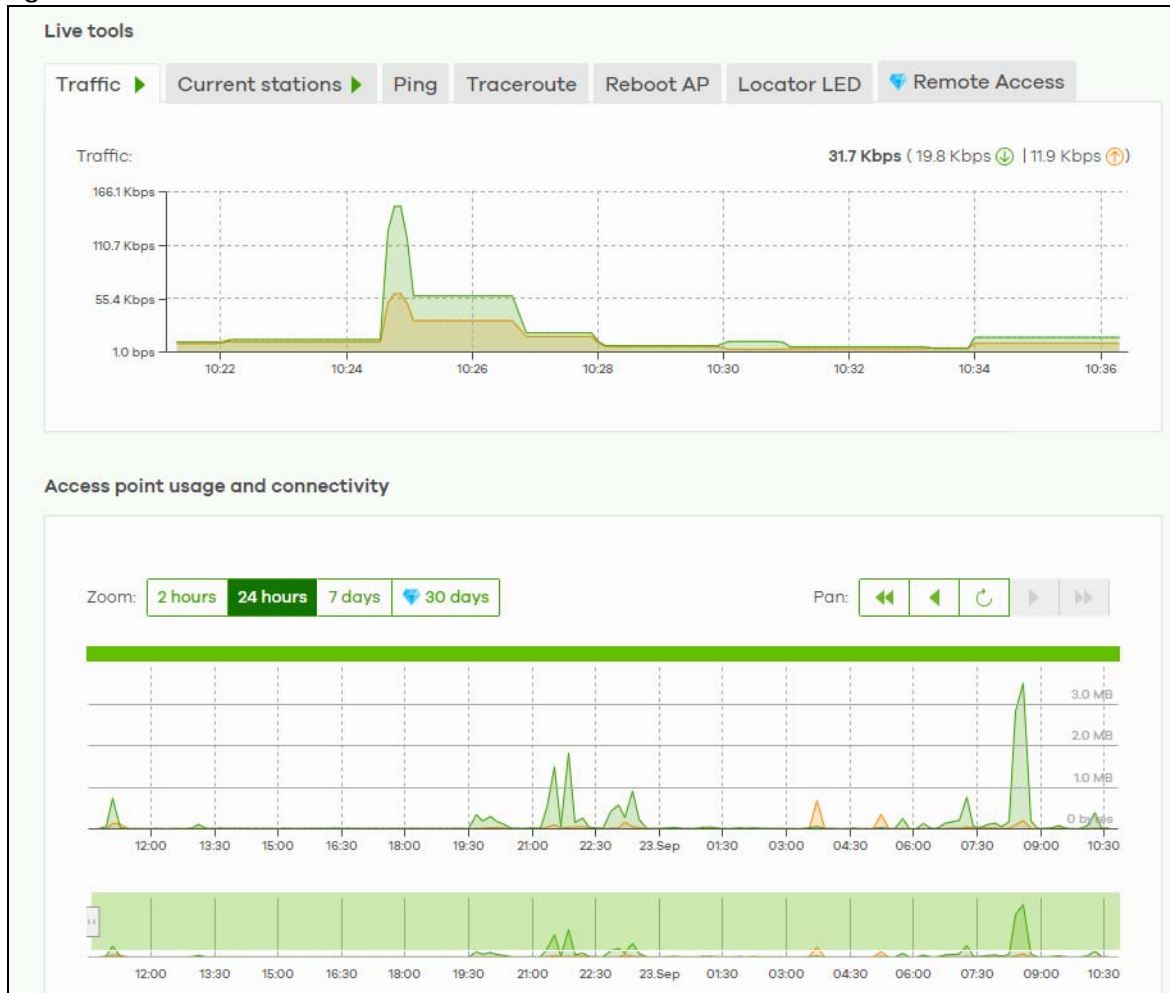

Map data ©2020 Google 20 m  [Terms of Use](#) [Report a map error](#)

Figure 100 Access Point > Monitor > Access Points: AP Details Part 2

The following table describes the labels in this screen.

Table 84 Access Point > Monitor > Access Points: AP Details

LABEL	DESCRIPTION
	Click this button to reload the data-related frames on this page.
Configuration	
Click the edit configuration icon to change the device name, description, tags and address. You can also move the device to another site.	
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.
Load balancing	This shows the load balancing group name that the AP belongs (up to 2 groups per AP). APs in the same group should be within the proximity. This allows them to share the load.
Status	

Table 84 Access Point > Monitor > Access Points: AP Details (continued)

LABEL	DESCRIPTION																																			
LAN IP	<p>This shows the local (LAN) IP address of the AP. It also shows the IP addresses of the gateway and DNS server.</p> <p>Click the edit icon to open a screen where you can change the IP addresses, VLAN ID number and tagging setting.</p> <div><div>Set IP Address</div><div><div>IP type</div><div>Static IP</div></div><div><div>IP</div><div></div></div><div><div>Management VLAN ID</div><div>1</div><div>(1-4094)</div></div><div><div><div>Untagged</div><div>Tagged</div></div></div><div><div>Subnet mask</div><div></div></div><div><div>Gateway</div><div></div></div><div><div>Primary DNS</div><div></div></div><div><div>Close</div><div>OK</div></div></div>																																			
Public IP	This shows the global (WAN) IP address of the AP.																																			
Usage	This shows the amount of data consumed by the clients.																																			
Current clients	<p>This shows the number of clients which are currently connecting to the AP and its details.</p> <div><div>Access point > Monitor > Clients</div><div>Clients Last 2 hours</div><div>Total 159.06 MB (@ 150.70 MB @ 8.96 MB)</div><div><div>2.3 Mbps</div><div>1.5 Mbps</div><div>768 Kbps</div><div>0 kbps</div><div>14:43 14:58 15:13 15:28 15:43 15:58 16:13 16:28 16:43</div></div><div><div>Policy</div><div>(status:online) AND (connec...)</div><div>1 selected, 4 matches in 5 clients</div><div><div>+</div><div>Add client</div></div><div><div>+</div><div>Export</div></div></div><table><thead><tr><th></th><th>Status</th><th>Description</th><th>Connected to</th><th>SSID name</th><th>Security</th><th>MAC address</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td></td><td>T-Lectec</td><td>HomeWiFi02</td><td>Youwontbeabiet...</td><td>WPA2-Personal</td><td>88:8E:8F:8A:8C:8D</td></tr><tr><td><input type="checkbox"/></td><td></td><td>Vaccum</td><td>HomeWiFi02</td><td>Youwontbeabiet...</td><td>WPA2-Personal</td><td>88:8E:8F:8A:8C:8D</td></tr><tr><td><input type="checkbox"/></td><td></td><td>Xiaomi Lemo</td><td>HomeWiFi02</td><td>Youwontbeabiet...</td><td>WPA2-Personal</td><td>88:8E:8F:8A:8C:8D</td></tr><tr><td><input type="checkbox"/></td><td></td><td>MS</td><td>HomeWiFi02</td><td>Youwontbeabiet...</td><td>WPA2-Personal</td><td>88:8E:8F:8A:8C:8D</td></tr></tbody></table></div>		Status	Description	Connected to	SSID name	Security	MAC address	<input checked="" type="checkbox"/>		T-Lectec	HomeWiFi02	Youwontbeabiet...	WPA2-Personal	88:8E:8F:8A:8C:8D	<input type="checkbox"/>		Vaccum	HomeWiFi02	Youwontbeabiet...	WPA2-Personal	88:8E:8F:8A:8C:8D	<input type="checkbox"/>		Xiaomi Lemo	HomeWiFi02	Youwontbeabiet...	WPA2-Personal	88:8E:8F:8A:8C:8D	<input type="checkbox"/>		MS	HomeWiFi02	Youwontbeabiet...	WPA2-Personal	88:8E:8F:8A:8C:8D
	Status	Description	Connected to	SSID name	Security	MAC address																														
<input checked="" type="checkbox"/>		T-Lectec	HomeWiFi02	Youwontbeabiet...	WPA2-Personal	88:8E:8F:8A:8C:8D																														
<input type="checkbox"/>		Vaccum	HomeWiFi02	Youwontbeabiet...	WPA2-Personal	88:8E:8F:8A:8C:8D																														
<input type="checkbox"/>		Xiaomi Lemo	HomeWiFi02	Youwontbeabiet...	WPA2-Personal	88:8E:8F:8A:8C:8D																														
<input type="checkbox"/>		MS	HomeWiFi02	Youwontbeabiet...	WPA2-Personal	88:8E:8F:8A:8C:8D																														
Topology	Click Show to go to the Site-Wide> Monitor > Topology screen. See Section 5.1.3 on page 80 .																																			
Neighbor info	This shows the LLDP information received on the up-link port.																																			
Link	<p>This shows the speed and duplex mode of the Ethernet connection on the AP's port(s).</p> <p>It shows Uplink: Wireless 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>																																			
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 Section 8.3.6 on page 245 for how to change the port's VLAN settings.</p>																																			

Table 84 Access Point > Monitor > Access Points: AP Details (continued)

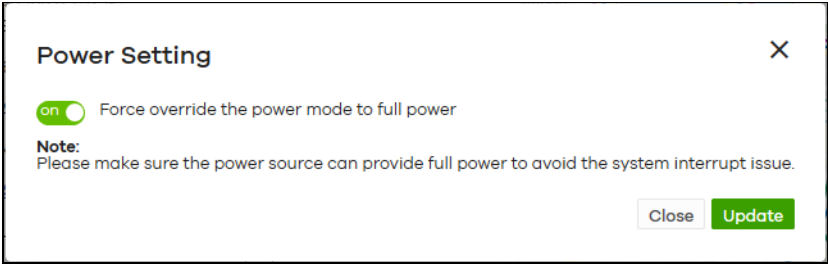
LABEL	DESCRIPTION
Storm control	Storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets received per second on the AP's Ethernet ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enabling this feature reduces broadcast, multicast and/or DLF packets in your network.
Channel (Band)	This shows the channel ID and WiFi frequency band currently being used by the AP.
Channel utilization	This shows the percentage of the channel ID usage.
Power mode	<p>This shows Full when the AP receives power directly through a power outlet.</p> <p>This shows Full (Power by DC) when the AP receives power using a power adapter.</p> <p>This shows Full (Power by PoE) when the AP receives power through a PoE switch/injector using IEEE 802.3at PoE plus. The PoE device that supports IEEE 802.3at PoE Plus can supply power of up to 30W per Ethernet port.</p> <p>This shows Limited (Require 802.3bt power) when the AP receives power through a PoE switch/injector using IEEE 802.3bt PoE even when it is also connected to a power source using a power adapter. The PoE device that supports IEEE 802.3bt PoE can supply power of up to 71.3W per Ethernet port.</p> <p>This shows Limited (Require 802.3at power) when the AP receives power through a PoE switch/injector using IEEE 802.3at PoE even when it is also connected to a power source using a power adapter. The PoE device that supports IEEE 802.3at PoE can supply power of up to 15.4W per Ethernet port.</p> <p>This field is blank when AP's firmware is older than version 5.50 or (WAX650S or WAX510D firmware is older than version 6.00P4C0). Or when the AP is offline.</p> <p>Click the edit icon to open a screen where you can enable full power mode.</p> <div data-bbox="537 1056 1360 1318">  </div> <p>Note: As of this writing, the following is a list of models that will show the edit icon for enabling full power mode: NAP303, NAP353, NWA1302-AC, NWA1123-AC HD, NWA5123-AC HD, WAC6303D-S, WAC6502D-E, WAC6502D-S, WAC6503D-S, WAC6552D-S, WAC6553D-S, WAX650S, NWA110AX, WAX510D.</p>
Antenna	This displays the antenna orientation settings for the AP that comes with internal antennas and also has an antenna switch.
Smart mesh	<p>This shows whether Nebula Smart Mesh is enabled on the AP.</p> <p>For more information about Smart Mesh, see Section 8.1.1 on page 205.</p>
Edit	Edit the AP's Smart Mesh settings.
Enabled	<p>Enable or disable Smart Mesh on the AP.</p> <p>This setting overrides the Smart Mesh settings configured for the AP's site in NCC.</p>

Table 84 Access Point > Monitor > Access Points: AP Details (continued)


LABEL	DESCRIPTION
Lock	<p>When enabled, the AP's local Smart Mesh settings overrides the Smart Mesh settings configured for the AP's site in NCC.</p> <p>Example 1: If Smart Mesh is enabled for the site in NCC, you can disable Smart Mesh on the AP by setting Lock to on and Enabled to off.</p> <p>Example 2: If Smart Mesh is disabled for the site in NCC, you can enable Smart Mesh on the AP by setting Lock to on and Enabled to on.</p>
Wireless bridge	<p>This shows whether wireless bridge is enabled on the AP.</p> <p>For more information about wireless bridge, see Section 8.1.2.2 on page 206.</p>
Edit	Edit the AP's wireless bridge settings.
Enabled	<p>Enable or disable wireless bridge on the AP.</p> <p>Note: If Smart Mesh is disabled for the site in NCC, then enabling wireless bridge automatically enables Smart Mesh on the AP.</p>
Allowed VLANs	<p>Enter the IDs of the VLANs that the AP will forward over the wireless bridge.</p> <p>By default, this field uses the VLANs allowed for LAN1 at AP > Configure > AP & Port Settings. For details, see Section 8.3.6 on page 245.</p>
History	Click Event log to go to the Access Point > Monitor > Event log 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.
Current version	This shows the firmware version currently installed on the device.
Map	This shows the location of the AP on Google map.
Photo	This shows the photo of the AP. Click Add to upload one or more photos. Click x to remove a photo.
Live tools	
Traffic	This shows the AP traffic statistics.
Current stations	This shows the AP's connected wireless client(s)' MAC address, SSID name, IPv4 Address, Signal strength, Security, Channel, Tx rate, Rx rate, Association time, and Capability .
Ping	<p>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 Ping.</p> <p>This can be used to determine if the AP and the computer are able to communicate with each other.</p>
Traceroute	Enter the domain name or IP address of a computer that you want to perform traceroute from the AP and click Run . This determines the path a packet takes to the specified computer.
Reboot AP	Click the Reboot button to restart the AP.
Locator LED	<p>Enter a time interval between 1 and 60 minutes. The locator LED will blink for the number of minutes set here once you turn on the Locator LED.</p> <p>Click the  button to turn on the locator feature, which shows the actual location of the AP between several devices in the network.</p>
Remote Access	<p>This allows you to establish a remote connection to this AP by specifying the port number. Then click Establish.</p> <p>This feature is available to the organization owner, organization administrators with full privileges, and site administrators with full privileges.</p>
Access point usage and connectivity	
Move the cursor over the chart to see the transmission rate at a specific time.	

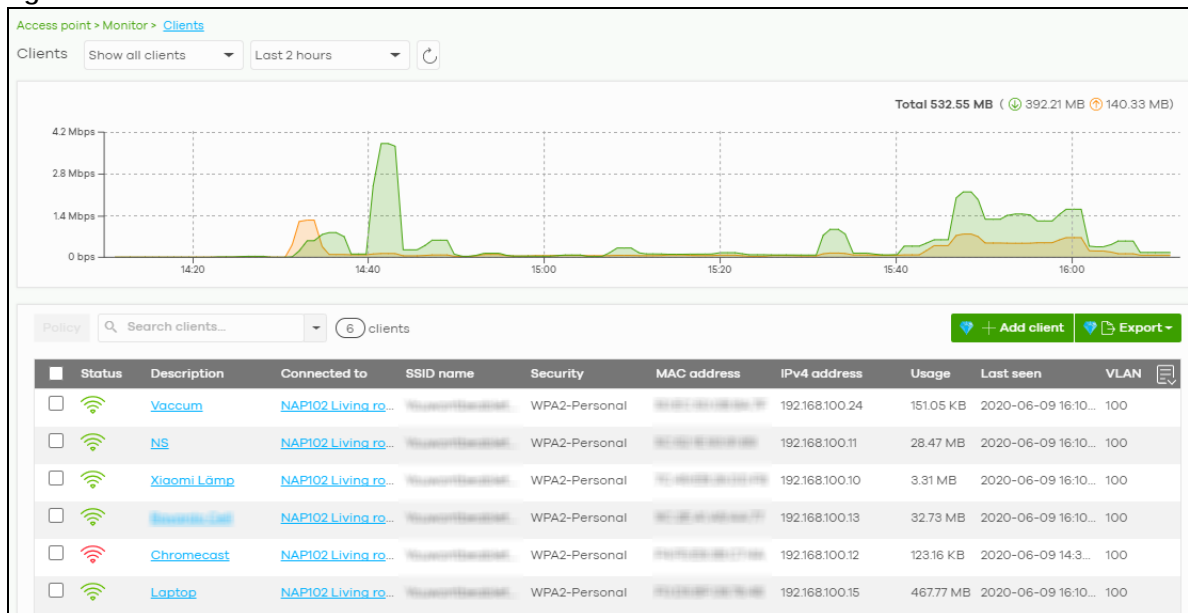
Table 84 Access Point > Monitor > Access Points: AP Details (continued)

LABEL	DESCRIPTION
Zoom	Select to view the statistics in the past 2 hours, day, week, or month.
Pan	Click to move backward or forward by one day or week.

8.2.2 Clients

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

Figure 101 Access Point > Monitor > Clients



The following table describes the labels in this screen.

Table 85 Access Point > Monitor > Clients

LABEL	DESCRIPTION
Clients	Select to view the device information and connection status in the past two hours, day, week or month. <ul style="list-style-type: none"> Select Show all clients to show clients that have been online during the selected time period. Select Show policy clients to show clients that have a whitelisted or blocked policy applied to them, regardless of when they were last online. The client's usage data is calculated according to the selected time period.
	Click this button to reload the data-related frames on this page.
y-axis	The y-axis shows the transmission speed of data sent or received by the client in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.

Table 85 Access Point > Monitor > Clients (continued)

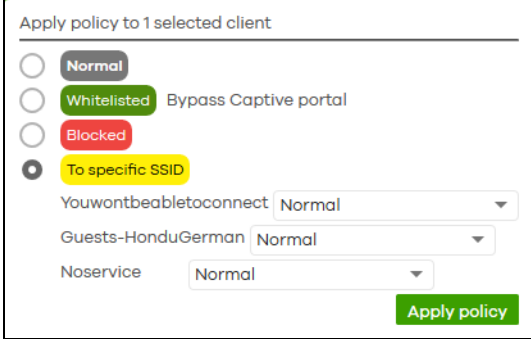

LABEL	DESCRIPTION
Policy	<p>Select the client(s) from the table below, and then choose the security policy that you want to apply to the selected client(s). Choose Normal to apply the captive portal authentication to the selected clients. To allow the selected clients to bypass captive portal authentication, choose Whitelisted. Choose Blocked when the selected clients fails the captive portal authentication. Choose To specific SSID to selectively apply captive portal authentication to specific SSIDs. Then, click Apply policy.</p> 
Search	Specify your desired filter criteria to filter the list of clients.
Clients	This shows the number of clients connected to an AP in the site network.
Add client	Click this button to open a window where you can specify a client's name and MAC address to apply a policy before it is connected to the AP's network.
Export	Click this button to save the client list as a CSV or XML file to your computer.
Status	This shows whether the client is online (green) or offline (red), and whether the client is wired or wireless.
Description	<p>This shows the descriptive name of the client.</p> <p>Click the name to display the individual client statistics. See Section 8.2.2.1 on page 217.</p>
Connected to	<p>This shows the name of the Nebula managed AP to which the client is connected.</p> <p>Click the name to display the individual AP statistics. See Section 8.2.1.1 on page 209.</p>
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	<p>This shows the RSSI (Received Signal Strength Indicator) of the client's wireless connection, and an icon showing the signal strength.</p> <p>Icon default thresholds:</p> <ul style="list-style-type: none"> Green/5 blocks: signal is greater than -67 dBm, strong signal Amber/4 blocks: signal -67 to -73 dBm, average signal Amber/3 blocks: signal -74 to -80 dBm, below average signal Red/2 blocks: signal is less than -80 dBm, weak signal
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.
Download	This shows the amount of data received by the client since it was last connected.
Upload	This shows the amount of data transmitted from the client since it was last connected.

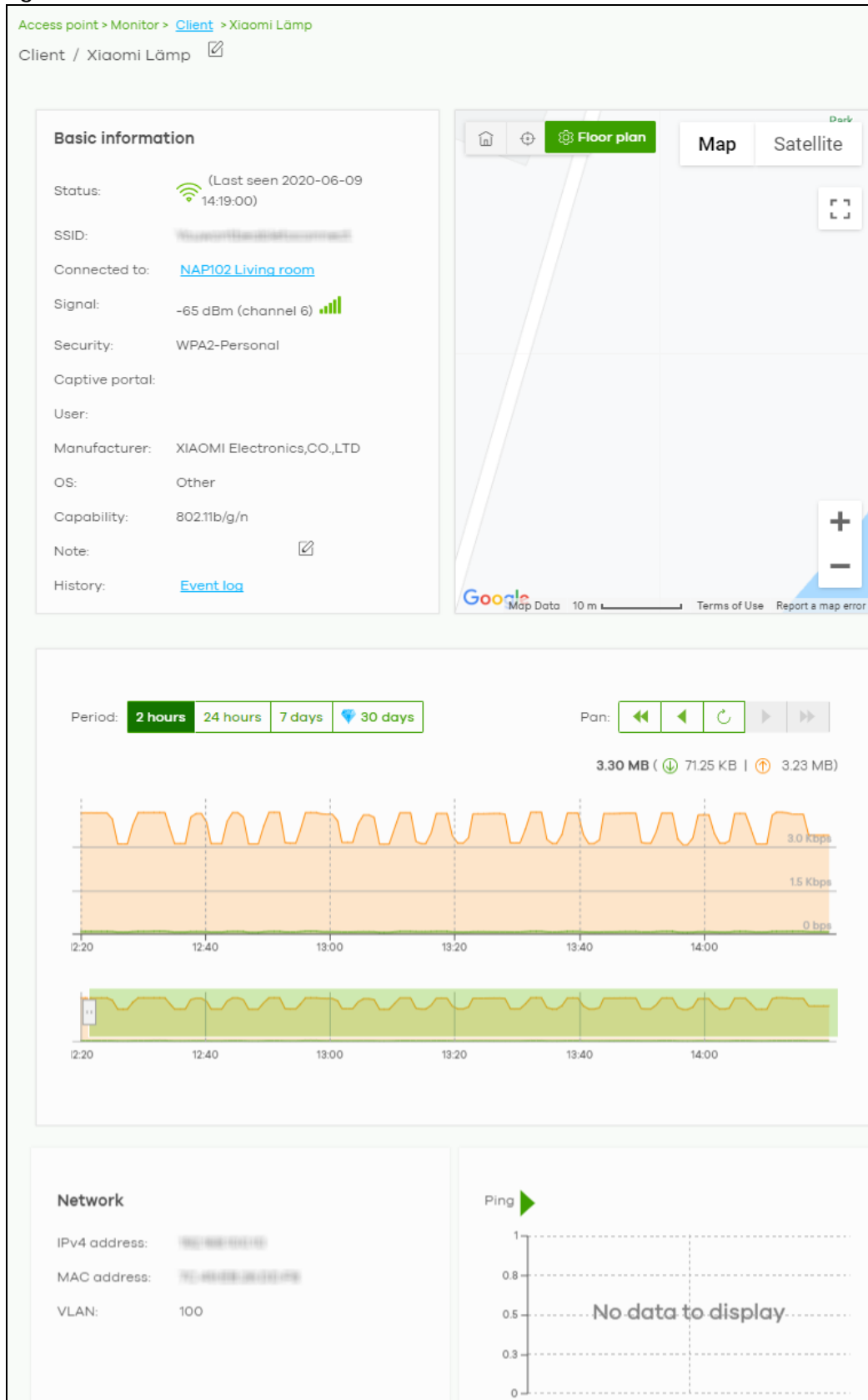
Table 85 Access Point > Monitor > Clients (continued)

LABEL	DESCRIPTION
Usage	This shows the amount of data consumed by the AP (upload + download) since it was last connected.
Association time	This shows the date and time the client associated with the Nebula device.
First seen	This shows the first date and time the client was discovered.
Last seen	This shows the last date and time the client was discovered.
Capability	This shows the WiFi standards supported by the client or the supported standards currently being used by the client.
Manufacturer	This shows the manufacturer of the client device.
Authentication	This shows the authentication method used by the client to access the network. This shows Unauthorized if the captive portal page displays but the client has not proceeded with the authentication process. The field is blank if web authentication is disabled.
User	This shows the user account information used to log into the NCC via captive portal, using Facebook login or 802.1x with Nebula cloud authentication or a RADIUS server. This field is blank if the user logs in via Facebook WiFi or web authentication is disabled.
OS	This shows the operating system running on the client device.
Policy	This shows the security policy applied to the client.
VLAN	This shows the ID number of the VLAN to which the client belongs.
Note	This shows additional information for the client.
	Click this icon to display a greater or lesser number of configuration fields.

8.2.2.1 Client Details

Click a client entry in the **Access Point > Monitor > Clients** screen to display individual client statistics.

Figure 102 Access Point > Monitor > Clients: Client Details



Period: **2 hours** 24 hours 7 days 30 days

Pan:

3.30 MB (71.25 KB | 3.23 MB)

12:20 12:40 13:00 13:20 13:40 14:00

0 bps 1.5 Kbps 3.0 Kbps

Network

IPv4 address:

MAC address:

VLAN: 100

Ping

1 0.8 0.5 0.3 0

No data to display

The following table describes the labels in this screen.

Table 86 Access Point > Monitor > Clients: Client Details

LABEL	DESCRIPTION
Status	This shows whether the client is online (green), or goes off-line (red). It also shows the last date and time the client was discovered.
SSID	This shows the name of the AP's wireless network to which the client is connected.
Connected to	This shows the name of the Nebula managed AP to which the client is connected. Click the name to display the individual AP statistics. See Section 8.2.1.1 on page 209 .
Signal	This shows the RSSI (Received Signal Strength Indicator) of the client's wireless connection, and an icon showing the signal strength. Icon default thresholds: <ul style="list-style-type: none"> Green/5 blocks: signal is greater than -67 dBm, strong signal Amber/4 blocks: signal -67 to -73 dBm, average signal Amber/3 blocks: signal -74 to -80 dBm, below average signal Red/2 blocks: signal is less than -80 dBm, weak signal
Security	This shows the encryption method used to connect to the AP.
Captive portal	This shows the web authentication method used by the client to access the network.
User	This shows the number of users currently connected to the network through the client device.
Manufacturer	This shows the manufacturer of the device connected to the AP.
OS	This shows the operating system running on the client device, if known.
Capability	This shows the WiFi standards supported by the client or the supported standards currently being used by the client.
Note	This shows additional information for the client. Click the edit icon to change it.
History	Click Event log to go to the Access Point > Monitor > Event log screen.
Map	This shows the location of the client on the Google map.
Period	Select to view the statistics in the past two hours, day, week or month.
Pan	Click to move backward or forward by two hours or one day.
y-axis	The y-axis shows the transmission speed of data sent or received by the client in kilobits per second (Kbps).
x-axis	The x-axis shows the time period over which the traffic flow occurred.
Network	
IPv4 address	This shows the IP address of the client.
MAC address	This shows the MAC address of the client. If you applied a security policy to a client using the Add client button in the Access Point > Monitor > Clients screen, and the client has never been connected to the AP's network, an edit icon appears allowing you to modify the client's MAC address.
VLAN	This shows the ID number of the VLAN to which the client belongs.
Ping	Click the button to ping the client's IP address from the Nebula AP to test connectivity.
Loss rate	This shows the rate of packet loss when you perform ping.
Average latency	This shows the average latency in ms when you perform ping.

8.2.3 Event Log

Use this screen to view wireless AP log messages. You can enter the AP name or a key word, select one or multiple event types, or specify a date/time or even a time range to display only the log messages related to it.

Click **Access Point > Monitor > Event Log** to access this screen.

Figure 103 Access Point > Monitor > Event log

Access point > Monitor > [Event log](#)

Event log

Access Point: Keyword: Category:

Before 17:12 1h UTC+8

135 Event log

Time	Access point	Category	Detail
2019-10-30 16:14:23	9c:5c:f9:61:f6:c1	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has associated on Channel: 6, SS...
2019-10-30 16:14:27	9c:5c:f9:61:f6:c1	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by Hostapd3 on Ch...
2019-10-30 16:14:27	9c:5c:f9:61:f6:c1	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by prev-Auth Failed ...
2019-10-30 16:14:27	9c:5c:f9:61:f6:c1	Wireless LAN	WPA authenticator requests disconnect: reason 1. Interf...
2019-10-30 16:14:27	9c:5c:f9:61:f6:c1	Wireless LAN	WPA authenticator requests disconnect: reason 2. Interf...
2019-10-30 16:19:26	9c:5c:f9:61:f6:c1	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has associated on Channel: 6, SS...
2019-10-30 16:19:30	9c:5c:f9:61:f6:c1	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by Hostapd3 on Ch...
2019-10-30 16:19:30	9c:5c:f9:61:f6:c1	Wireless LAN	Station: 9c:5c:f9:61:f6:c1 has blocked by prev-Auth Failed ...
2019-10-30 16:19:30	9c:5c:f9:61:f6:c1	Wireless LAN	WPA authenticator requests disconnect: reason 1. Interf...
2019-10-30 16:19:30	9c:5c:f9:61:f6:c1	Wireless LAN	WPA authenticator requests disconnect: reason 2. Interf...

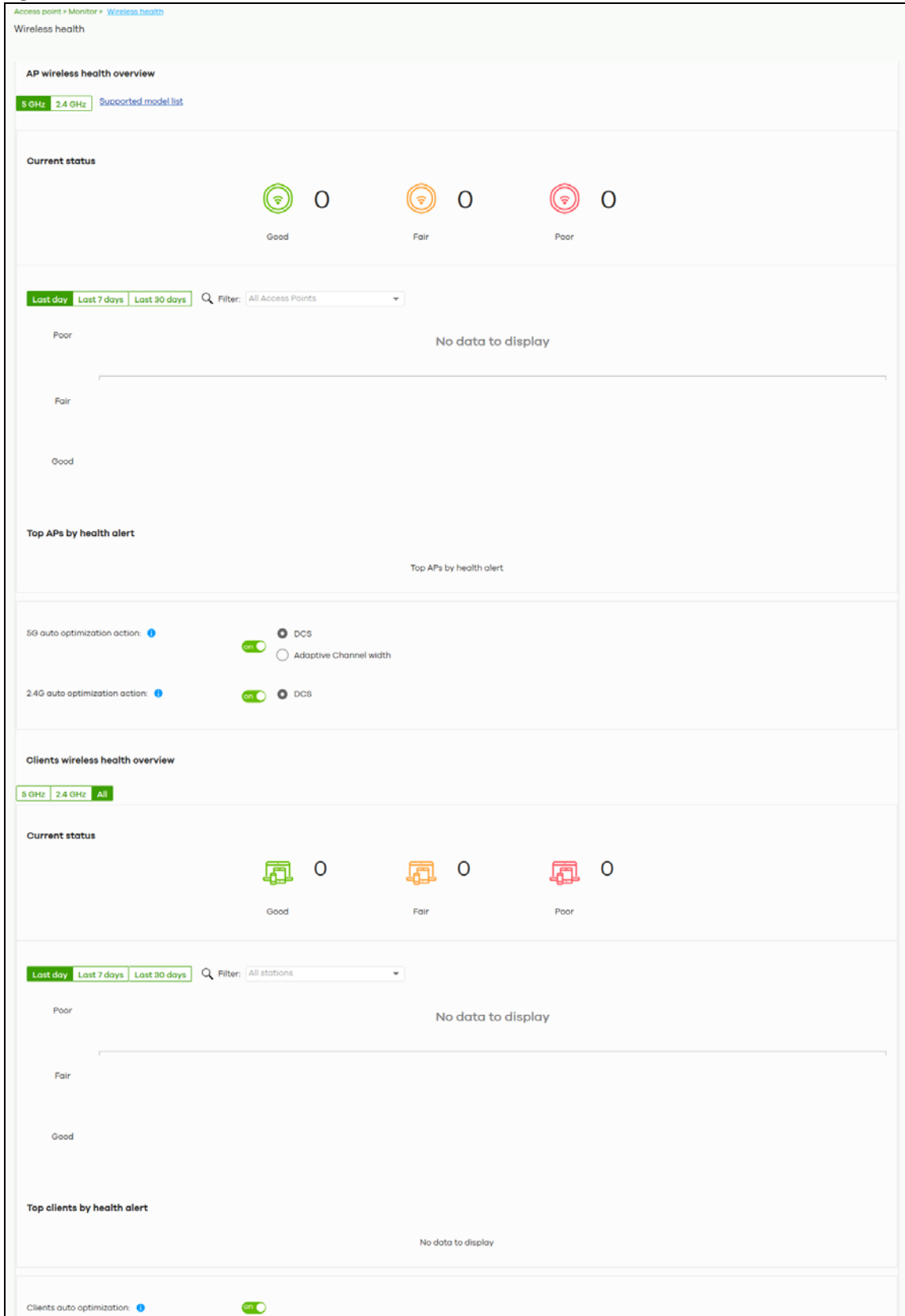
Page 1 of 14 Results per page: 10

8.2.4 Wireless Health

This screen lets you know health of wireless networks for your APs and connected wireless clients. You can take actions by enabling DCS, changing channel bandwidth and/or client steering to reduce interference and improve wireless network performance.

Click **Access Point > Monitor > Wireless Health** to access this screen.

Figure 104 Access Point > Monitor > Wireless Health



The following table describes the labels in this screen.

Table 87 Access Point > Monitor > Wireless Health

LABEL	DESCRIPTION
AP wireless health overview	
Move the cursor over the information icon to view the supported AP model list.	
Good/Fair/Poor	This shows the number of supported APs that are currently online, using the specified frequency band and in good, fair or poor wireless health.
AP radio health	Select to view the health of all supported AP wireless networks using the 5 GHz or 2.4 GHz band. You can select to view the health report for the past day, week or month, as well as filter the AP to view.
y-axis	The y-axis represents the state of wireless health.
x-axis	The x-axis shows the time period over which the AP health state is recorded.
Top APs by health alert	
Name	This shows the descriptive name of the AP.
Model	This shows the model number of the AP.
Alert	This shows how many times the AP is in a poor state of wireless health. The NCC generates a log when the AP is in poor wireless health. You can view the log messages in the Access Point > Monitor > Event Log screen.
5G auto optimization action	Select ON to enable and specify how the AP improves the wireless network performance. Otherwise, select OFF to disable it. <ul style="list-style-type: none"> Adaptive channel width - select this option to have the AP change the channel bandwidth from 80 MHz to 20 MHz to reduce the radio interference with other APs. <p>Note: In AP firmware version 6.10 and later, if adaptive channel width does not improve wireless performance then the AP also performs Dynamic Channel Selection (DCS).</p> <ul style="list-style-type: none"> DCS (Dynamic Channel Selection) - select this option to have the AP scan and choose a radio channel that has least interference.
2.4G auto optimization action	Select ON to enable and specify how the AP improves the wireless network performance. Otherwise, select OFF to disable it. <ul style="list-style-type: none"> DCS (Dynamic Channel Selection) - select this option to have the AP scan and choose a radio channel that has least interference.
Client wireless health overview	
Good/Fair/Poor	This shows the number of connected wireless clients that are currently online, using the specified frequency band and in good, fair or poor wireless health.
Client health	Select to view the health of all wireless clients which are connected to the supported APs using the 5 GHz or 2.4 GHz band. You can select to view the health report for the past day, week or month, as well as filter the wireless station to view.
y-axis	The y-axis represents the state of wireless health.
x-axis	The x-axis shows the time period over which the client health state is recorded.
Top clients by health alert	
Description	This shows the descriptive name of the client.

Table 87 Access Point > Monitor > Wireless Health (continued)

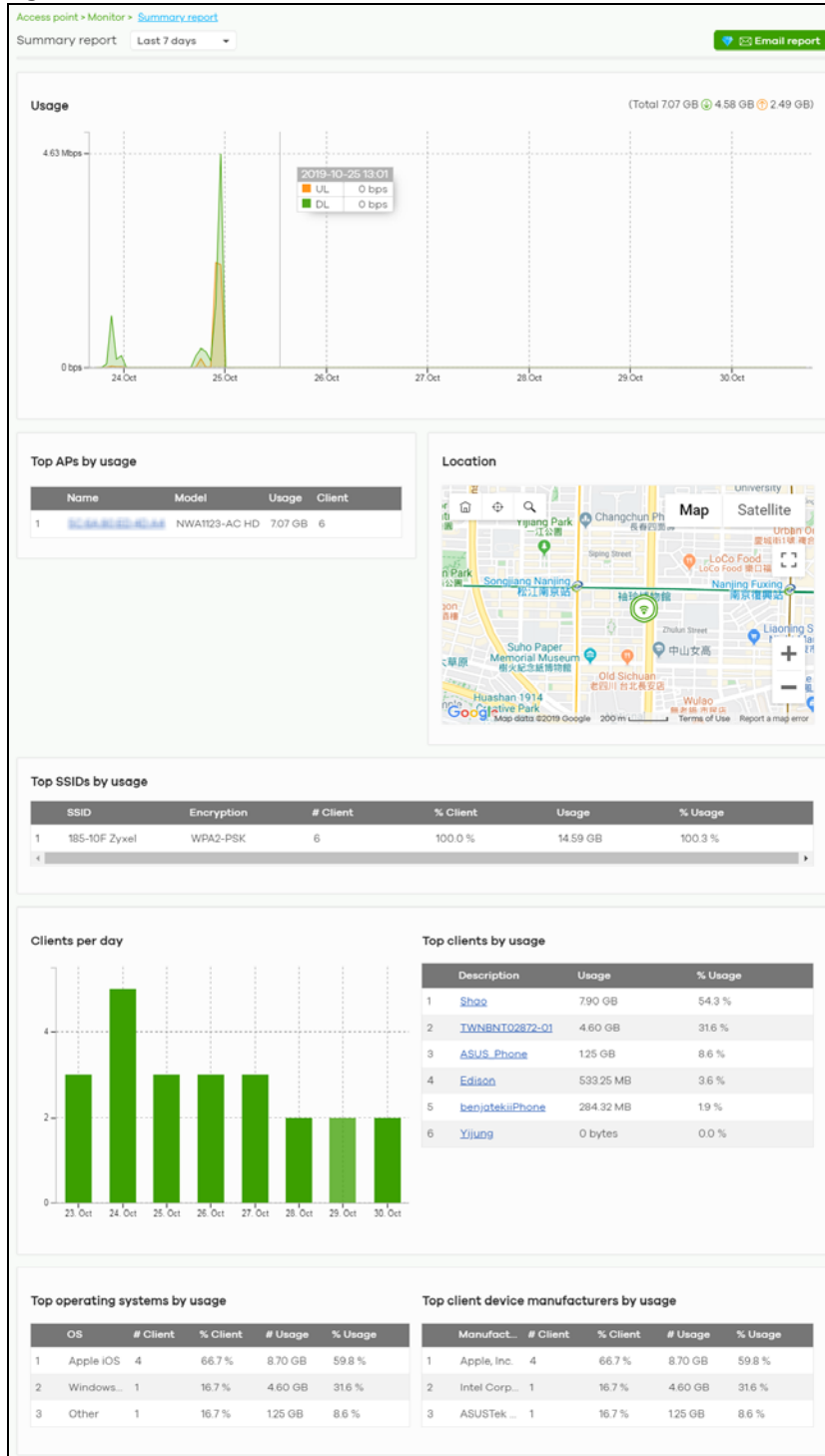
LABEL	DESCRIPTION
Alert	This shows how many times the client is in a poor state of wireless health. The NCC generates a log when the client is in poor wireless health. You can view the log messages in the Access Point > Monitor > Event Log screen.
Clients auto optimization	Select ON to have the AP try to steer the wireless clients in poor health to an AP or SSID with a strong signal every 30 minutes. Otherwise, select OFF to disable steering.

8.2.5 Summary Report

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

Click **Access Point > Monitor > Summary Report** to access this screen.

Figure 105 Access Point > Monitor > Summary Report



The following table describes the labels in this screen.

Table 88 Access Point > Monitor > Summary Report

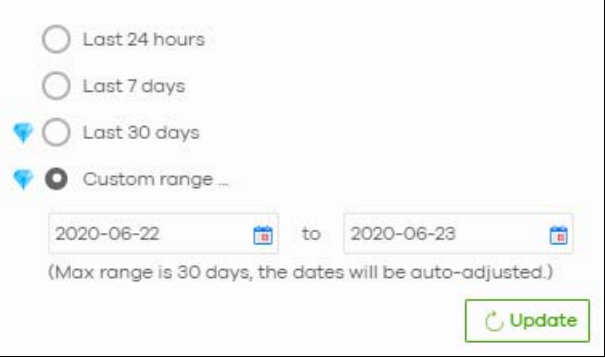
LABEL	DESCRIPTION
Summary report	<p>Select to view the report for the past day, week or month. Alternatively, select Custom range... to specify a time period the report will span. You can also select the number of results you want to view in a table.</p> 
Email report	Click this button to send summary 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 ranking of the Nebula AP.
Name	This shows the descriptive name of the Nebula AP.
Model	This shows the model number of the Nebula AP.
Usage	This shows the amount of data transmitted or received by the Nebula AP.
Client	This shows how many clients are currently connecting to the Nebula AP.
Location	
This shows the location of the Nebula APs on the map.	
Top SSIDs by usage	
	This shows the ranking of the SSID.
SSID	This shows the SSID network name.
Encryption	This shows the encryption method use by the SSID network.
# Client	This shows how many WiFi clients are connecting to this SSID.
% Client	This shows what percentage of associated WiFi clients are connecting to this SSID.
Usage	This shows the total amount of data transmitted or received by clients connecting to this SSID.
% Usage	This shows the percentage of usage for the clients connecting to this SSID.
Clients per day	
y-axis	The y-axis represents the number of clients.
x-axis	The x-axis represents the date.
Top clients by usage	
	This shows the ranking of the client.
Description	This shows the descriptive name or MAC address of the client.

Table 88 Access Point > Monitor > Summary Report (continued)

LABEL	DESCRIPTION
Usage	This shows the total amount of data transmitted and received by the client.
% Usage	This shows the percentage of usage for the client.
Top operating systems by usage	
	This shows the ranking of the operating system.
OS	This shows the operating system of the client device.
# Client	This shows how many client devices use this operating system.
% Client	This shows the percentage of top client devices which use this operating system.
# Usage	This shows the amount of data consumed by the client device on which this operating system is running.
% Usage	This shows the percentage of usage for top client devices which use this operating system.
Top client device manufacturers by usage	
	This shows the ranking of the manufacturer.
Manufacturer	This shows the manufacturer name of the client device.
# Client	This shows how many client devices are made by the manufacturer.
% Client	This shows the percentage of top client devices which are made by the manufacturer.
# Usage	This shows the amount of data consumed by the client device.
% Usage	This shows the percentage of usage for the client device.

8.3 Configure

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

8.3.1 SSID Overview

This screen allows you to configure up to eight different SSID profiles for your APs. An SSID, or Service Set Identifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the wireless network name when a person makes a connection to it.

Click **Access Point > Configure > SSID overview** to access this screen.

Figure 106 Access Point > Configure > SSID overview

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

SSID overview

[Show All](#) [Hide disable SSIDs](#)

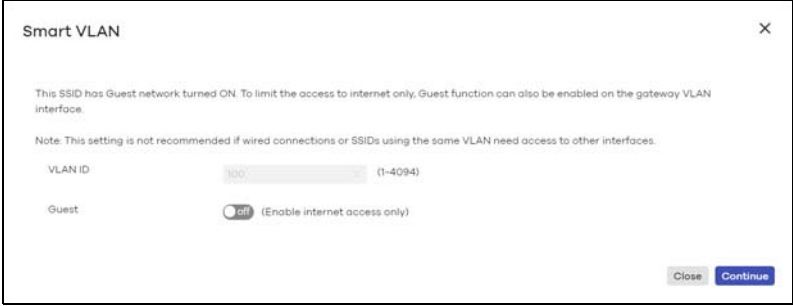
No.	1	2	
Name	<input type="text" value="Youwontbeabletoconnect"/> ✕ *	<input type="text" value="Guests-HonduGerman"/> ✕ *	No
Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tagging	<input type="text"/>	<input type="text"/>	<input type="text"/>
	Enable SSID on APs with any of the specified tags	Enable SSID on APs with any of the specified tags	Enc
Guest Network ⓘ	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication	Edit	Edit	
WLAN security	WPA2 Pre-shared key	Open	WP
Sign-in method	Disable	Sign-on with Facebook	Clic
Band	Concurrent operation(2.4GHz and 5GHz)	Concurrent operation(2.4GHz and 5GHz)	5GH
VLAN ID	100	250	1
Rate limiting	<input checked="" type="checkbox"/> unlimited Kb/s <input checked="" type="checkbox"/> unlimited Kb/s	<input checked="" type="checkbox"/> 4096 Kb/s <input checked="" type="checkbox"/> 4096 Kb/s	<input checked="" type="checkbox"/> u
Captive Portal	Edit	Edit	
Theme	test	Copy of Modern	Mod

The following table describes the labels in this screen.

Table 89 Access Point > Configure > SSID overview

LABEL	DESCRIPTION
Show All/Hide disabled SSIDs	Select to display all SSID profiles or the active SSID profiles only.
No.	This shows the index number of this profile.
Name	This shows the SSID name for this profile. Click the text box and enter a new SSID if you want to change it.
Enabled	Click to turn on or off this profile.
Tagging	Enter or select the tag(s) you created for APs in the Access Point > Monitor > Access Points screen. The SSID profile will only be applied to APs with the specified tag. If you leave this field blank, this SSID profile will be applied to all APs in the site.

Table 89 Access Point > Configure > SSID overview (continued)

LABEL	DESCRIPTION
Guest Network	<p>Select On to set this wireless network as a guest network. Layer 2 isolation and intra-BSS blocking are automatically enabled on the SSID. Wireless clients connecting to this SSID can access the Internet through the AP but cannot directly connect to the LAN or the wireless clients in the same SSID or any other SSIDs.</p> <p>Note: In your VLAN-enabled network, if the SSID's gateway MAC address and the AP's gateway MAC address are different and belong to different VLANs, you need to manually add the SSID's gateway MAC address to the layer 2 isolation list. See Section 8.3.2 on page 228.</p> <p>Note: If you have a Nebula security gateway installed in the site but the gateway interface with the same VLAN ID is not configured as a guest interface, Smart Guest/VLAN network tip, click here. displays after you select On. Click here to open a screen where you can directly select to use the interface as a Guest interface.</p>  <p>The image shows a 'Smart VLAN' dialog box with a close button (X) in the top right. The text inside reads: 'This SSID has Guest network turned ON. To limit the access to internet only, Guest function can also be enabled on the gateway VLAN interface.' Below this is a note: 'Note: This setting is not recommended if wired connections or SSIDs using the same VLAN need access to other interfaces.' There is a 'VLAN ID' field with a dropdown menu showing '100' and a range '(1-4094)'. Below that is a 'Guest' toggle switch which is currently turned 'On' with the text '(Enable internet access only)' next to it. At the bottom right are 'Close' and 'Continue' buttons.</p>
Authentication	
Edit	Click this button to go to the Authentication screen and configure the advanced settings, such as SSID availability, WiFi security, L2 isolation, intra-BSS traffic blocking and walled garden settings. See Section 8.3.2 on page 228 .
WLAN security	This shows the encryption method used in this profile.
Sign-in method	This shows the authentication method used in this profile.
Band	This shows whether the SSID use either 2.4 GHz band or the 5 GHz band. If it shows Concurrent operation , the SSID uses both frequency bands.
VLAN ID	This shows the ID number of the VLAN to which the SSID belongs.
Rate limiting	This shows the maximum incoming/outgoing transmission data rate (in Kbps) on a per-station basis.
Captive portal	
Edit	Click this button to go to the Captive Portal screen and configure the captive portal settings. See Section 8.3.3 on page 235 .
Theme	If captive portal is enabled, this shows the name of the captive portal page used in this profile.

8.3.2 Authentication

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

Click **Access Point > Configure > Authentication** to access this screen.

Figure 107 Access Point > Configure > Authentication Part 1

Access point > Configure > [Authentication](#)

Authentication

SSID:

Network access

☒ Open
 Users can connect without entering a password

☐ Enhanced-open [i](#)
 User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.

☐ WPA Personal With
 Users must enter the password to associate

☒ Dynamic personal psk [i](#) [Beta](#) [Model list](#)

☐ MAC-based Authentication with
 Use MAC address as a username and password

☐ WPA Enterprise with
 Use 802.1X authentication that requires a unique username and password
 WPA Enterprise with

Sign-in method:

☐ Disabled
 Users can access the network without any web authentication

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

☒ Voucher [Beta](#)
 Users must enter a voucher code then can access the network
 Create and manage voucher passcode on the [Vouchers](#) page.

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

Walled garden

Walled garden ranges: ☐

Captive portal access attribute

Login on multiple client devices:

Strict Policy:

Reauth time:

Figure 108 Access Point > Configure > Authentication Part 2

NCAS disconnection behavior ⓘ

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

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

NAT mode

☐ NAT mode: Use Zyxel DHCP & NAT ⓘ [Beta](#) [Model list](#)
Clients receive IP addresses in an isolated network.
Client cannot communicate with other clients associated with different AP.

Layer 2 isolation

☐ Enable layer 2 isolation ⓘ

Intra-BSS traffic blocking

☐ Enable Intra-BSS traffic blocking ⓘ

Band

☐ 2.4GHz band only

☐ 5GHz band only

☒ Concurrent operation(2.4GHz and 5GHz)

☐ Band select

VLAN ID

ⓘ (1-4094)

Rate limiting

Download (Kb/s) (1 - 160000)

Upload (Kb/s) (1 - 160000)

(Per client device traffic rate)

Assisted roaming

☐ Enable 802.11k/v

U-APSD

☐

The following table describes the labels in this screen.

Table 90 Access Point > Configure > Authentication

LABEL	DESCRIPTION
SSID	Select the SSID profile to which the settings you configure here is applied.
Network access	<p>Note: You cannot enable MAC authentication, 802.1X authentication and web authentication at the same time.</p> <p>Note: User accounts can be created and authenticated using the NCC user database. See Section 4.3.6 on page 59.</p>

Table 90 Access Point > Configure > Authentication (continued)

LABEL	DESCRIPTION
WLAN security	<p>Select Open to allow any client to associate this network without any data encryption or authentication.</p> <p>Select Enhanced-open to allow any client to associate this network without any password but with improved data encryption.</p> <p>Upon selecting Enhanced-open or WPA Personal With WPA3, transition mode generates 2 VAP so devices that do not support Enhanced-Open/WPA Personal With WPA3 can connect using Open/WPA Personal With WPA2 network. This is always on at the time of writing.</p> <p>Select WPA Personal With (WPA1/WPA2/WPA3) and enter a pre-shared key from 8 to 64 case-sensitive keyboard characters to enable WPA1/2/3-PSK data encryption. Upon selecting WPA Personal With WPA3, APs that do not support it will revert to WPA2.</p> <p>Note: Only the NWA110AX, WAX510D, WAX650S supports WPA3 as of this writing.</p> <ul style="list-style-type: none"> • Turn on 802.11r to enable IEEE 802.11r fast roaming on the AP. 802.11r fast roaming reduces the delay when the clients switch from one AP to another by allowing security keys to be stored on all APs in a network. Information from the original association is passed to the new AP when the client roams. The client does not need to perform the whole 802.1x authentication process. <p>Select Dynamic personal psk to have every user connect to the SSID using a unique pre-shared key (PSK) that is linked to their user account. This allows you to revoke a user's wireless network access by disabling their account.</p> <p>After enabling this option, you must create one or more DPPSK users in the site or organization at Configure > Cloud authentication > Account Type > DPPSK.</p> <ul style="list-style-type: none"> • For details on creating a site DPPSK user, see Section 4.3.6.1 on page 62. • For details on creating organization DPPSK users, see Section 5.2.5 on page 96. <p>Turn on MAC-based Authentication with to authenticate wireless clients by their MAC addresses. You can select My RADIUS server to use an external RADIUS server or select Nebula cloud authentication to use the NCC for MAC authentication.</p> <p>Select WPA-Enterprise with to enable 802.1X secure authentication. You can select My RADIUS server to use an external RADIUS server or select Nebula cloud authentication to use the NCC for 802.1X authentication.</p> <ul style="list-style-type: none"> • Turn on 802.11r to enable IEEE 802.11r fast roaming on the AP. 802.11r fast roaming reduces the delay when the clients switch from one AP to another by allowing security keys to be stored on all APs in a network. Information from the original association is passed to the new AP when the client roams. The client does not need to perform the whole 802.1x authentication process.

Table 90 Access Point > Configure > Authentication (continued)

LABEL	DESCRIPTION
Sign-in method	<p>Select Disable to turn off web authentication.</p> <p>Select Click-to-continue to block network traffic until a client agrees to the policy of user agreement.</p> <p>Select Voucher to require that a user logs in with a voucher code. For details on vouchers, see Section 5.1.4 on page 81.</p> <p>Note: Vouchers cannot be enabled if Dynamic Personal Pre-Shared Key (DPPSK) or WPA Enterprise are enabled. You can only enable voucher authentication for one SSID per site.</p> <p>Select Sign-on with and:</p> <ul style="list-style-type: none"> select Nebula cloud authentication to block network traffic until a client authenticates with the NCC through the specifically designated web portal page. select My RADIUS server to block network traffic until a client authenticates with an external RADIUS server through the specifically designated web portal page. select Facebook to block network traffic until a client authenticates with the NCC using Facebook Login. <p>Facebook Login is a secure and quick way for users to log into your app or website using their existing Facebook accounts. If you get the App ID for your app at the Facebook developers site, you can enter your Facebook App ID to obtain more information about your users using Facebook Analytics, such as user activity, age, gender, and so on.</p> <ul style="list-style-type: none"> select Facebook Wi-Fi to let users check in to a business on Facebook for free Internet access after connecting to the AP's wireless network. Users then have the option to like the Facebook fan page. You should already have set up a Facebook fan page associated with the business location. <p>Click here to open the Facebook Wi-Fi configuration screen in a new window, where you can select the Facebook Page associated with your location and configure bypass mode and session length.</p> <div data-bbox="537 1085 1078 1612"> <p>Facebook Wi-Fi Configuration S132L32200016</p> <p>Facebook Page To use Facebook Wi-Fi you need to be the admin of a local business Page that has a valid location associated with it. Select a Page</p> <p>Bypass Mode Your customers always have the option to skip checking in. They can do this by clicking on a link that lets them skip check-in, or by entering a Wi-Fi code that you provide to them. <input checked="" type="radio"/> Skip check-in link [?] <input type="radio"/> Require Wi-Fi code [?]</p> <p>Session Length Select the length of time your customers will have Wi-Fi for after they check in. Five hours</p> <p>Terms of Service <input type="checkbox"/> Optional: Add your own Terms of Service [?]</p> <p>Visit Help Center Save Settings</p> </div> <p>Note: When the NCC license of the organization expires, the SSID configured with Facebook Wi-Fi will be disabled automatically. To enable the SSID again, change its authentication method or register with a new license key.</p>

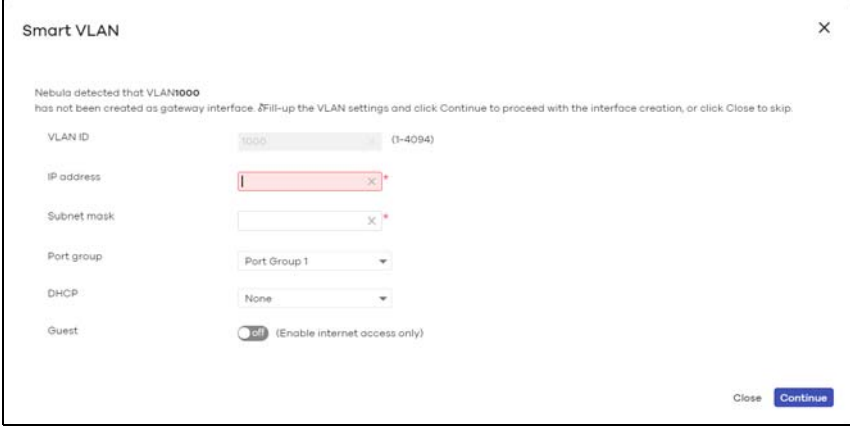
Table 90 Access Point > Configure > Authentication (continued)

LABEL	DESCRIPTION
RADIUS server	<p>This field is available only when you select to use the following:</p> <ul style="list-style-type: none"> • MAC-based Authentication with My RADIUS server or WPA2-Enterprise with My RADIUS server in the WLAN security field, or • when you select Sign-on with My RADIUS server in the Sign-in method field. <p>Click Add to specify the IP address/domain name, port number and shared secret password of the RADIUS server to be used for authentication.</p> <p>Note: APs with firmware version 5.50 or older will turn OFF this SSID when the Host field is configured with a domain name.</p>
NAS Identifier	<p>If the RADIUS server requires the AP to provide the Network Access Server identifier attribute with a specific value, enter it here.</p>
RADIUS accounting	<p>This field is available only when you select to use WPA2-Enterprise with My RADIUS server in the WLAN security field, or when you select Sign-on with My RADIUS server in the Sign-in method field.</p> <p>Select RADIUS accounting enabled to enable user accounting through an external RADIUS server.</p> <p>Select RADIUS accounting disabled to disable user accounting through an external RADIUS server.</p>
RADIUS accounting servers	<p>If you select RADIUS accounting enabled, click Add to specify the IP address, port number and shared secret password of the RADIUS server to be used for accounting.</p>
Walled garden	
Walled garden ranges	<p>This field is not configurable if you set Captive portal to Disable. With a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example.</p> <p>Select to turn on or off the walled garden feature.</p> <p>Specify walled garden web site links, which use a (wildcard) domain name or an IP address for web sites that all users are allowed to access without logging in.</p>
Captive portal access attribute	
Self-registration	<p>This field is available only when you select Sign-on with Nebula Cloud authentication in the Sign-in method field.</p> <p>Select Allow users to create accounts with auto authorized or Allow users to create accounts with manual authorized to display a link in the captive portal login page. The link directs users to a page where they can create an account before they authenticate with the NCC. For Allow users to create accounts with manual authorized, users cannot log in with the account until the account is authorized and granted access. For Allow users to create accounts with auto authorized, users can just use the registered account to log in without administrator approval.</p> <p>Select Don't allow users to create accounts 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 Sign-on with My RADIUS server or Sign-on with Nebula Cloud authentication in the Sign-in method field.</p> <p>Select Multiple devices access simultaneously if you allow users to log in as many times as they want as long as they use different IP addresses.</p> <p>Select One device at a time if you do not allow users to have simultaneous logins.</p>

Table 90 Access Point > Configure > Authentication (continued)

LABEL	DESCRIPTION
Strict policy	<p>Select Allow HTTPS traffic without sign-on to let users use HTTPS to access a web site without authentication.</p> <p>Select Block all access until sign-on to block both HTTP and HTTPS traffic until users authenticate their connections. The portal page will not display automatically if users try to access a web site using HTTPS. They will see an error message in the web screen.</p>
Reauth time	<p>Select Follow site-wide setting or select a specific time the user can be logged in through the captive portal in one session before having to log in again.</p>
NCAS disconnection behavior	<p>This field is available only when:</p> <ul style="list-style-type: none"> • you select Sign-on with Nebula Cloud authentication in the Sign-in method field • you turn on MAC-based Authentication with and you select Nebula cloud authentication <p>Select Allowed to allow any users to access the network without authentication when the NCAS (Nebula Cloud Authentication Server) is not reachable.</p> <p>Select Limited to allow only the currently connected users or the users in the white list to access the network.</p>
NAT mode	<p>Select Use Zyxel DHCP & NAT to have the AP create a DHCP subnet with its own NAT for the SSID. This simplifies wireless network management, as you do not need to configure a separate DHCP server.</p> <p>The following AP features do not work when Use Zyxel DHCP & NAT is enabled:</p> <ul style="list-style-type: none"> • 802.11r • Layer2 isolation • Dynamic VLAN (cloud authentication, RADIUS server)
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 Add to enter the MAC address of each device that you want to allow to be accessed by other devices in the SSID on which layer-2 isolation is enabled.</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 on to prevent crossover traffic from within the same SSID. Select off to allow intra-BSS traffic.</p>
Band	<p>Select to have the SSID use either 2.4 GHz band or the 5 GHz band.</p> <p>If you select Concurrent operation, the SSID uses both frequency bands. You can then turn on Band Select to have the dual-band AP steer the wireless clients to the 5 GHz band.</p>

Table 90 Access Point > Configure > Authentication (continued)

LABEL	DESCRIPTION
VLAN ID	<p>Enter the ID number of the VLAN to which the SSID belongs.</p> <p>Note: If you have a Nebula security gateway installed in the site but did not configure an identical VLAN interface on the gateway, Smart Guest/VLAN network tip, click here. displays. Click here to open a screen where you can create a gateway interface with the specified VLAN ID.</p>  <p>The image shows a 'Smart VLAN' dialog box with a close button (X) in the top right. The text inside reads: 'Nebula detected that VLAN1000 has not been created as gateway interface. Fill-up the VLAN settings and click Continue to proceed with the interface creation, or click Close to skip.' Below this text are several fields: 'VLAN ID' with a value of 1000 and a range of (1-4094); 'IP address' with a red error bar; 'Subnet mask' with a red error bar; 'Port group' with a dropdown menu showing 'Port Group 1'; 'DHCP' with a dropdown menu showing 'None'; and 'Guest' with a toggle switch that is currently turned on, labeled '(Enable internet access only)'. At the bottom right are 'Close' and 'Continue' buttons.</p>
Rate limiting	<p>Set the maximum data download and upload rates in Kbps, on a per-station basis.</p> <p>Click a lock icon to change the lock state. If the lock icon is locked, the limit you set applies to both download and upload traffic. If the lock is unlocked, you can set download and upload traffic to have different transmission speeds.</p>
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>

8.3.3 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 **Access Point > Configure > Captive portal** to access this screen.




Figure 109 Access Point > Configure > Captive portal

Access point > Configure > [Captive portal](#)

Captive portal


SSID

Themes



☒ **Default** ☐ Modern

Click-to-continue/Voucher/Sign-on page

Logo  [Upload a logo](#)

Message

Success page

Message

External captive portal URL

Use URL: ☐ URL:

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

Captive portal behavior

After the captive portal page where the user should go?

☒ Stay on Captive portal authenticated successfully page

☐ To promotion URL:

The following table describes the labels in this screen.

Table 91 Access Point > Configure > Captive portal

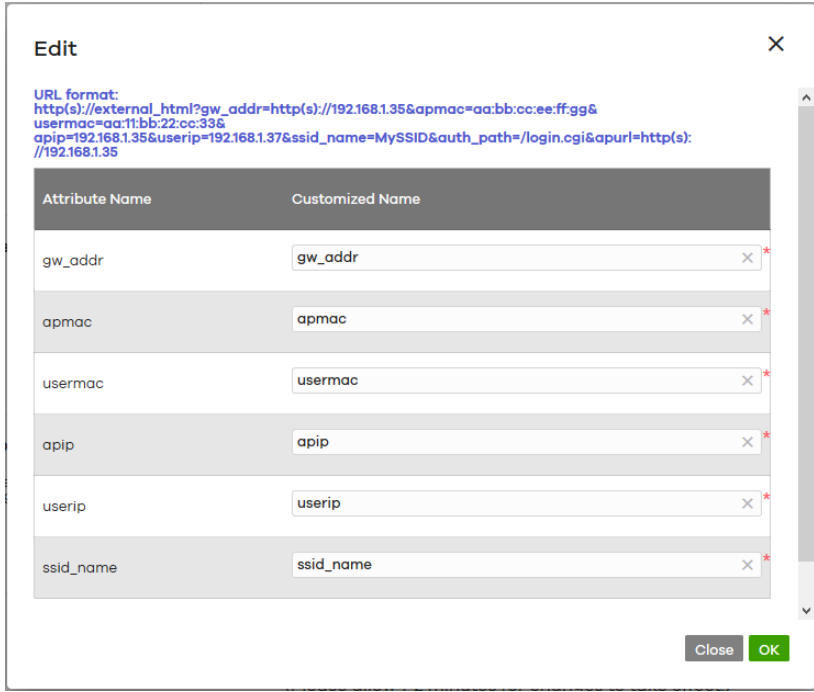
LABEL	DESCRIPTION
SSID	Select the SSID profile to which the settings you configure here is applied.
Themes	<p>This section is not configurable when External captive portal URL is set to ON.</p> <ul style="list-style-type: none"> Click the Preview icon at the upper right corner of a theme image to display the portal page in a new frame. Click the Copy icon to create a new custom theme (login page). Click the Edit icon of a custom theme to go to a screen where you can view and configure the details of the custom theme page(s). See Section 8.3.3.1 on page 238. Click the Remove icon to delete a custom theme page. <p>Select the theme you want to use on the specified SSID.</p>
Click-to-continue/Sign-on page	
This section is not configurable when External captive portal URL is set to ON .	
Logo	<p>This shows the logo image that you uploaded for the customized login page.</p> <p>Click Upload a logo and specify the location and file name of the logo graphic or click Browse to locate it. You can use the following image file formats: GIF, PNG, or JPG.</p>
Message	Enter a note to display below the title. Use up to 1024 printable ASCII characters. Spaces are allowed.
Success page	
Message	Enter a note to display on the page that displays when a user logs in successfully. Use up to 1024 printable ASCII characters. Spaces are allowed.
External captive portal URL	
Use URL	<p>Select On to use a custom login page from an external web portal instead of the one built into the NCC. You can configure the look and feel of the web portal page.</p> <p>Specify the login page's URL; for example, <code>http://IIS server IP Address/login.asp</code>. The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p> <p>Click Customization to rename the URL attributes.</p> 

Table 91 Access Point > Configure > Captive portal (continued)

LABEL	DESCRIPTION
Captive portal behavior	
After the captive portal page where the user should go?	Select To promotion URL and specify the URL of the web site/page to which the user is redirected after a successful login. Otherwise, select Stay on Captive portal authenticated successfully page .

8.3.3.1 Custom Theme Edit

Use this screen to check what the custom portal pages look like. You can also view and modify the CSS values of the selected HTML file. Click a custom login page's **Edit** button in the **Access Point > Configure > Captive portal** screen to access this screen.



Figure 110 Access Point > Configure > Captive portal: Edit

The following table describes the labels in this screen.

Table 92 Access Point > Configure > Captive portal: Edit

LABEL	DESCRIPTION
Back to config	Click this button to return to the Captive portal screen.
Theme name	This shows the name of the theme. Click the edit icon to change it.
Font	Click the arrow to hide or display the configuration fields. To display this section and customize the font type and/or size, click on an item with text in the preview of the selected custom portal page (HTML file).

Table 92 Access Point > Configure > Captive portal: Edit (continued)

LABEL	DESCRIPTION
Color	<p>Click the arrow to hide or display the configuration fields.</p> <p>Click on an item in the preview of the selected custom portal page (HTML file) to customize its color, such as the color of the button, text, window's background, links, borders, and so on.</p> <p>Select a color that you want to use and click the Select button.</p>
HTML/CSS	<p>This shows the HTML file name of the portal page created for the selected custom theme. This also shows the name of the CSS files created for the selected custom theme.</p> <p>Click a HTML file to display the portal page. You can also change colors and modify the CSS values of the selected HTML file.</p>
	Click this button to view and modify the CSS values of the selected HTML file. It is recommended that you do NOT change the script code to ensure proper operation of the portal page.
	Click this button to preview the portal page (the selected HTML file).
Save	Click this button to save your settings for the selected HTML file to the NCC.
Apply	Click this button to save your settings for the selected HTML file to the NCC and apply them to the APs in the site.

8.3.4 SSID Availability

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

Figure 111 Access Point > Configure > SSID availability

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

SSID availability

SSID:

SSID availability

Visibility:

Tagging:

Enable SSID on APs with any of the specified tags.

SSID schedule

Enabled ☒

Schedule: ☒

Schedule template:

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

Day	Availability
Sunday	<input checked="" type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Monday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Tuesday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Wednesday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Thursday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Friday	<input type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Saturday	<input checked="" type="checkbox"/> 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00

Each site can have at most 5 SSID schedules.

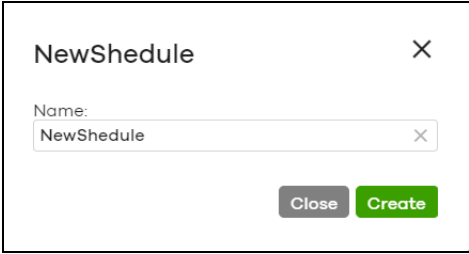
This schedule also used in SSID(s):
Guests-
HondurGerman

The following table describes the labels in this screen.

Table 93 Access Point > Configure > SSID availability

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

Table 93 Access Point > Configure > SSID availability (continued)

LABEL	DESCRIPTION
Visibility	<p>Select Hide this SSID 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 Broadcast this SSID.</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>
Tagging	<p>Enter the tag(s) you created for APs in the Access Point > Monitor > Access Points 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>
SSID schedule	
Enabled	Click On to enable and configure a schedule.
Schedule	Select a schedule to control when the SSID is enabled or disabled. You can click the edit icon to change the schedule name.
Schedule templates	Select a pre-defined schedule template or select Custom schedule and manually configure the day and time at which the SSID is enabled or disabled.
Day	This shows the day of the week.
Availability	<p>Click On to enable the SSID at the specified time on this day. Otherwise, select Off to disable the SSID on the day and at the specified time.</p> <p>Specify the hour and minute when the schedule begins and ends each day.</p>
Add	<p>Click this button to create a new schedule. A window pops up asking you to enter a descriptive name for the schedule for identification purposes.</p> 
Delete	Click this button to remove a schedule which is not used in any SSID profile.

8.3.5 Radio Settings

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

Figure 112 Access Point > Configure > Radio settings

Access point > Configure > [Radio settings](#)

Radio settings

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

160MHz-support [Beta](#) [Supported model list](#)

Go to the AP list in the bottom of this page, select the supported AP to apply 160MHz in 5GHz setting

DCS setting

☒ DCS time interval: 720 (60-1440 minutes)

☐ DCS schedule

☒ DCS client aware

☐ Avoid 5G DFS channel

☐ Blacklist DFS channels in the presence of radar [Beta](#)

2.4 GHz channel deployment: Three-Channel Deploy...

5 GHz channel deployment: Auto

Allow 80211ax/ac/n stations only: ☐

If turned ON, legacy clients including 80211a/b/g will not be allowed to associate.

Smart steering: ☐ Enable this function will steer the client to the better signal AP.

▲ ADVANCED OPTIONS

Edit DCS Now [List](#) [Map](#) [2.4GHz](#) [5GHz](#) [Hide transmit circles](#)

Access point	Radio #	Model	Channel	Transmit power	Channel width	Smart steering	Antenna
<input type="checkbox"/> NAPI02 Living ro...	1	NAPI02	6 (DCS)	23 dBm	20 MHz	Disable	

The following table describes the labels in this screen.

Table 94 Access Point > Configure > Radio settings

LABEL	DESCRIPTION
Country	Select the country where the AP is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs in order to prevent roaming failure and interference with other systems.
Maximum output power	Set the maximum target output power of the radio (in dBm).

Table 94 Access Point > Configure > Radio settings (continued)

LABEL	DESCRIPTION
Channel width	<p>Select the wireless channel bandwidth you want the AP to use.</p> <p>A standard 20 MHz channel offers transfer speeds of up to 144 Mbps (2.4 GHz) or 217 Mbps (5 GHz) whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps (2.4 GHz) or 450 Mbps (5 GHz). An IEEE 802.11ac-specific 80 MHz channel offers speeds of up to 1.3 Gbps.</p> <p>40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A 80 MHz channel consists of two adjacent 40 MHz channels. The wireless clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Note: It is suggested that you select 20 MHz when there is more than one 2.4 GHz AP in the network.</p> <p>Note: It is not possible to set channel bandwidth to 160 Mhz for the whole site. To configure an AP to use 160 Mhz, select a supported AP in the table at the bottom of the screen, click Edit, and then select 160 Mhz under Channel width.</p>
DCS setting	
DCS time interval	<p>Select ON 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 ON 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 ON to have the AP wait until all connected clients have disconnected before switching channels.</p>
Blacklist DFS channels in the presence of radar	<p>Select ON 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 Three-Channel Deployment to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels.</p> <p>Select Four-Channel Deployment to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the 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 Manual 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 Auto to have the AP automatically select the best channel.</p> <p>Select Manual to select the individual channels the AP switches between.</p> <p>Note: The method is automatically set to Auto when no channel is selected or any one of the previously selected channels is not supported.</p>
Allow 802.11ax/ac/n stations only	<p>Select ON to have the AP allow only IEEE 802.11n/ac/ax clients to connect, and reject IEEE 802.11a/b/g clients.</p>

Table 94 Access Point > Configure > Radio settings (continued)


LABEL	DESCRIPTION
Smart Steering	<p>Select ON 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 OFF to disable this feature on the AP.</p>
ADVANCED OPTIONS	Click this to display a greater or lesser number of configuration fields.
2.4G/5G Setting	
Station Signal Threshold	<p>Set a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold.</p> <p>-20 dBm is the strongest signal you can require and -105 is the weakest.</p>
Disassociate Station Threshold	<p>Set a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the AP disconnects the wireless client.</p> <p>-20 dBm is the strongest signal you can require and -105 is the weakest.</p>
Allow Station Connection after Multiple Retries	Select the check box to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.
Station Retry Count	Set the maximum number of times a wireless client can attempt to re-connect to the AP.
Edit	<p>Click this button to modify the channel, output power, channel width and smart steering settings for the selected AP(s).</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 Wall if you mount the AP to a wall. Select Ceiling if the AP is mounted on a ceiling. You can switch from Wall to Ceiling if there are still wireless dead zones, and vice versa. If you select Hardware Switch, you use the physical antenna switch to adjust coverage and apply the same antenna orientation settings to both radios.</p>  <p>Note: On this screen, you can set channel width to 160 Mhz for the 5Ghz channel, if the AP supports it.</p>

Table 94 Access Point > Configure > Radio settings (continued)

LABEL	DESCRIPTION
DCS Now	Click this button to have the selected APs immediately scan for and select a channel that has least interference.
List	Click this to display a list of all connected APs.
Map	Click this to display the locations of all connected APs on the Google map.
2.4 GHz	Click this to display the connected APs using the 2.4 GHz frequency band.
5 GHz	Click this to display the connected APs using the 5 GHz frequency band.
Hide transmit circles	Click this button to not show the transmission range on the Map.
Access point	This displays the descriptive name or MAC address of the connected AP.
Radio #	This displays the number of the connected AP's radio.
Model	This displays the model name of the connected AP.
Radio mode	This displays the type of Wi-Fi radio the AP is currently using, for example 802.11b/g/n.
Channel	This displays the channel ID currently being used by the connected AP's radio.
Transmit power	This displays the current transmitting power of the connected AP's radio. If the AP is off-line, this shows the maximum output power you configured for the AP.
Channel width	This displays the wireless channel bandwidth the connected AP's radio is set to use.
Smart steering	This displays whether smart client steering is enabled or disabled on the connected APs.
Antenna	This displays the antenna orientation settings for the AP that comes with internal antennas and also has an antenna switch.

8.3.6 AP & Port Settings

Use this screen to configure general AP settings and network traffic load balancing between the APs in the site. This screen also allows you to enable or disable a port on the managed AP and configure the port's VLAN settings. The port settings apply to all Nebula APs that are assigned to the site and have one or more than one Ethernet LAN port (except the uplink port).

Click **Access Point > Configure > AP & Port Settings** to access this screen.

Figure 113 AP > Configure > AP & Port Settings

Access point > Configure > [AP & port settings](#)

AP & port settings

General setting

AP LED lights ☒

AP Smart Mesh Beta ☐ [Model list](#)

Ethernet failover Beta ☐

Load balancing

☒ Disable

☐ Enable "By client device number" mode
Recommended for general use

2.4G Maximum client device number: × * (1-127)

5G Maximum client device number: × * (1-127)

☐ Enable "Smart Classroom" mode
Recommended for E-learning only

2.4G Maximum client device number: × * (1-127)

5G Maximum client device number: × * (1-127)

☐ Disassociate client device when overloaded

Port setting

LAN 1 ☒

PVID ×

Allowed VLANs i ×

LAN 2 ☒

PVID ×

Allowed VLANs i ×

LAN 3 ☒

PVID ×

Allowed VLANs i ×

Access point	Status	Port Setting
192.168.1.100	LAN 1: Enable	LAN 1: PVID 64 - Allowed VLANs 60,62,64
192.168.1.101	LAN 1: Enable	LAN 1: PVID 64 - Allowed VLANs 60,62,64

The following table describes the labels in this screen.

Table 95 AP > Configure > AP & Port Settings

LABEL	DESCRIPTION
General setting	
AP LED lights	Click to turn on or off the LED(s) on the APs.

Table 95 AP > Configure > AP & Port Settings (continued)

LABEL	DESCRIPTION
AP Smart Mesh	<p>Click to enable or disable the Nebula Smart Mesh feature on all APs in the site.</p> <p>Click Model list to see whether your AP supports Nebula Smart Mesh.</p> <p>Note: Nebula Smart Mesh is a WiFi mesh solution for Nebula APs. For details, see Section 8.1.1 on page 205.</p> <p>Note: You can override NCC settings and enable and disable Smart Mesh on individual APs. For details, see Section 8.2.1.1 on page 209.</p> <p>Note: Disabling AP Smart Mesh automatically disables wireless bridge on all APs in the site. For details on wireless bridge, see Section 8.2.1.1 on page 209.</p>
Ethernet failover	<p>When enabled, a wired AP in the site automatically changes its role from root AP to repeater AP if the AP is unable to reach the site's gateway.</p> <p>When disabled, a wired AP in the site automatically changes its role from root AP to repeater AP only if the AP's uplink Ethernet cable is unplugged.</p> <p>Note: For details on root and repeater APs, see Section 8.1.1 on page 205.</p>
Load balancing	
Disable	Select this option to disable load balancing on the AP.
Enable "By client device number" mode	Select this option to balance network traffic based on the number of specified client devices connected to the AP.
Maximum client device number	Enter the threshold number of client devices at which the AP begins load balancing its connections.
Disassociate client device when overloaded	<p>Select ON to disassociate wireless clients connected to the AP when it becomes overloaded.</p> <p>Select OFF 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"> • Idle Time - Devices that have been idle the longest will be kicked first. If none of the connected devices are idle, then the priority shifts to Signal Strength. • Signal Strength - Devices with the weakest signal strength will be kicked first.
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 Disassociate client device when overloaded function is enabled by default and the disassociation priority is always Signal Strength when you select this option.</p>
Maximum client device number	Enter the threshold number of client devices at which the AP begins load balancing its connections.
Port setting	
LAN x	<p>This is the name of the physical Ethernet port on the AP.</p> <p>This section lets you configure global port VLAN settings for all APs in the site. To modify port settings for a specific AP, use its Edit button in the table below.</p>
ON/OFF	Select ON to turn on the LAN port of the AP. Select OFF to disable the port.
PVID	<p>Enter the port's PVID.</p> <p>A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.</p>

Table 95 AP > Configure > AP & Port Settings (continued)

LABEL	DESCRIPTION
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.
Port Setting	This displays the port's VLAN settings for the managed AP.

8.3.6.1 Edit Port Settings

Click an entry in the **Port setting** table of the **AP > Configure > AP & Port Settings** screen to access this screen.

By default, all APs in the site use the global port settings. Use this screen to change the port settings on a per-device basis. You can turn on or off the port, modify its PVID or update the ID number of VLAN(s) to which the port belongs.

Figure 114 AP > Configure > AP & Port Settings: Edit

Edit

LAN 1

Enabled

on

PVID

64

Allowed VLANs

60,62,64

Close

OK

CHAPTER 9

Help

9.1 Support Request

If you need Zyxel customer support to help you find answers and/or solve problems, you can submit a ticket through the NCC.

Note: It is suggested that you check this user's guide first to seek help and then go to Zyxel Nebula Forum before you use this screen to send a ticket.

Click **Help > Support Request** to access this screen. The screen varies depending on whether you select to view the ticket details or create a new ticket.

Figure 115 Help > Support Request: My Cases

Help > Support request

Support request

Zyxel Support ☐ Invite Zyxel support as administrator

By enabling this, you are granting temporary access (21 days) to Zyxel support as administrator of your Organization. So they can help check your configuration & logs. This will automatically be switched off after 21 days, or you could turn it off right after your issue is solved. You might also edit the access privileges here.

My Cases

Open

4 items found, displaying all items. Page: 1

Case Number	Created	Last Updated	Creator	Subject	Priority	Status	Support Engineer
190600137	2019-09-04 15:59:25	2019-09-10 14:11:51	bayardo.salgado@zy...	Device online	Low	Open	
190600103	2019-08-14 14:04:15	2019-10-18 10:37:40	bayardo.salgado@zy...	Hello Support	Low	Open	
190600068	2019-06-19 10:40:32	2019-10-15 11:20:16	bayardo.salgado@zy...	Nebula Support requ...	Medium	Open	
180300006	2018-03-30 09:58:58	2019-10-09 17:35:20	bayardo.salgado@zy...	Nebula is great!	Low	Open	

The following table describes the labels in this screen.

Table 96 Help > Support Request

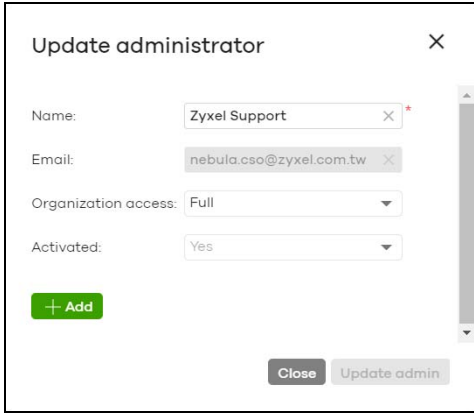

LABEL	DESCRIPTION
Zyxel Support	<p>Select ON to allow the Zyxel customer support account to access your organization temporarily, so that they can help check your configurations and log messages. The support account will be deactivated automatically after 21 days. You can also select OFF to immediately disable the support account's access to the organization after finding a solution to the problem.</p> <p>If you select ON, you can click here to change the support account's name and access right to the organization and sites.</p> <div data-bbox="496 527 967 936">  </div> <p>A Reset expire day button displays and becomes clickable when you select ON and the number of days remaining before the support account is deactivated is less than or equal to 14.</p>
My Cases	
	Click this button to reload the data-related frames for this section on the page.
Open/Closed	Select to view the details about the tickets that are still open or closed.
Case Number	This shows the number of the eITS ticket.
Created	This shows the first date and time the ticket was created.
Last Updated	This shows the last date and time the ticket was updated.
Creator	This shows the account name of the administrator that created this ticket.
Subject	This shows the subject of the ticket.
Priority	This shows the severity level of the ticket.
Status	This shows whether the ticket is open or closed.
Engineer	This shows the name of the support person who handles the ticket.
New Case	Click this button if you want to issue a new ticket. The following fields then appear allowing you to provide the necessary information and describe the issue encountered.
Subject	Enter the subject of the ticket.
Device	Select the NCC or the name of the device that cannot work properly.
Issue Description	Enter a complete and detailed description of your issue.
Priority	Select the severity level of the ticket. Click the Definition of priority link to see how to correctly identify a ticket's severity level. This can help to get your problem solved quickly.
Add Another File	Click this button to upload another file.
Choose File/Browse...	Click this button to locate the file you want to upload for reference.

Table 96 Help > Support Request (continued)

LABEL	DESCRIPTION
Delete	Click this button to remove the file you just uploaded before submitting the ticket.
Cancel	Click this button to close the New Case section without saving.
Submit	Click this button to send your ticket to the Zyxel customer support.

CHAPTER 10

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. See [Section 1.1 on page 8](#).
- If your device supports NebulaFlex or NebulaFlex Pro, make sure that the device is working in Nebula cloud manage mode with NCC Discovery enabled.
- Make sure that your device can connect to the NCC by checking your network's firewall/security settings. The following ports must be allowed:
 - TCP: 443, 4335 and 6667
 - UDP: 123

Note: Go to **Help > Firewall Information** to find the latest port information.

- Make sure that you have registered your Nebula devices with the NCC. See [Section 4.3.2 on page 47](#).
- Make sure that you have created an organization and site and add the devices to the site. See [Create Organization on page 28](#) and [Section 4.3.1 on page 46](#).

10.1 Getting More Troubleshooting Help

Go to support.zyxel.com at the Zyxel website for other technical information on the NCC.

APPENDIX A

Customer Support

10.2 Zyxel Support

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

See <https://www.zyxel.com/homepage.shtml> and also https://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml 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.
- <https://www.zyxel.com/cn/zh/>

India

- Zyxel Technology India Pvt Ltd.
- <https://www.zyxel.com/in/en/>

Kazakhstan

- Zyxel Kazakhstan

- <https://www.zyxel.kz>

Korea

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- Zyxel Philippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- Zyxel Communications Corporation
- <https://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd.
- <https://www.zyxel.com/th/th/>

Vietnam

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

Europe

Belarus

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

Belgium

- Zyxel Communications B.V.

- <https://www.zyxel.com/be/nl/>
- <https://www.zyxel.com/be/fr/>

Bulgaria

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

Czech Republic

- Zyxel Communications Czech s.r.o
- <https://www.zyxel.com/cz/cs/>

Denmark

- Zyxel Communications A/S
- <https://www.zyxel.com/dk/da/>

Estonia

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

Finland

- Zyxel Communications
- <https://www.zyxel.com/fi/fi/>

France

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

Germany

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

Hungary

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

Italy

- Zyxel Communications Ital
- <https://www.zyxel.com/it/it/>

Latvia

- Zyxel Latvia
- <https://www.zyxel.com/lv/lv/>

Lithuania

- Zyxel Lithuania
- <https://www.zyxel.com/lt/lt/>

Netherlands

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl/>

Norway

- Zyxel Communications
- <https://www.zyxel.com/no/no/>

Poland

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

Romania

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

Russia

- Zyxel Russia
- <https://www.zyxel.com/ru/ru/>

Slovakia

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

Spain

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

Sweden

- Zyxel Communications
- <https://www.zyxel.com/se/sv/>

Switzerland

- Studerus AG
- <https://www.zyxel.ch/de>
- <https://www.zyxel.ch/fr>

Turkey

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

UK

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en/>

Ukraine

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

South America

Argentina

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Brazil

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

Colombia

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Ecuador

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

South America

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Middle East

Israel

- Zyxel Communications Corporation
- <http://il.zyxel.com/>

Middle East

- Zyxel Communications Corporation
- <https://www.zyxel.com/me/en/>

North America

USA

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

Oceania

Australia

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

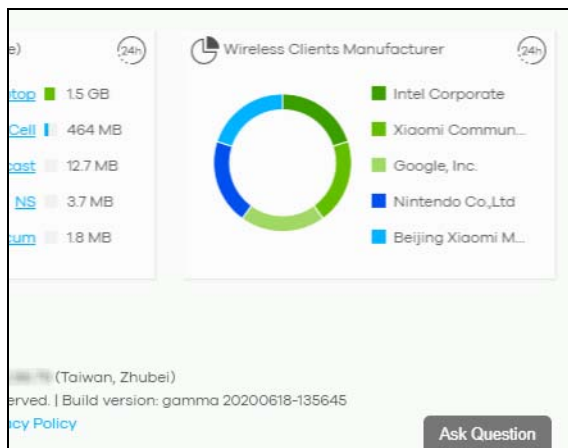
Africa

South Africa

- Nology (Pty) Ltd.
- <https://www.zyxel.com/za/en/>

10.3 NCC Live Chat

Clicking the **Ask Question** button at the bottom of NCC window prompts you to search for a solution on the Zyxel forum, and then connects you to a Zyxel technical support agent. If a technical support agent is not available, you can fill in a form to send your question to Zyxel by email.



Note: This is an NCC Pro-pack feature.

Note: Live chat might be limited to a certain number of hours per day. The time that live chat is available varies depending on your country.

APPENDIX B

Legal Information

Copyright

Copyright © 2020 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.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

Numbers

2FA [16](#)
802.11k neighbor lists [235](#)
802.11r fast roaming [231](#)
802.1X authentication [231](#)

A

access port [189](#)
account status [57](#)
ACL [192](#)
Active Directory [158](#)
AD server [158](#)
administrator accounts [55](#)
administrator creator account [49](#)
antenna orientation [213](#)
antenna switch [213](#)
AP connection status [208](#)
AP photo [214](#)
App ID [232](#)
application patrol profile [138](#)
assisted roaming [235](#)
Automatic Power Save Delivery [235](#)
auto-negotiation [186](#)

B

backup codes [18](#)
bandwidth utilization [171](#)
battery life [235](#)
bridge priority [203](#)
Browser support [15](#)
bulk import [98](#)
bypass mode [232](#)

C

calculator [52](#)
captive portal [150](#), [235](#)
certifications
 viewing [261](#)
channel bandwidth [222](#)
channel width [243](#)
Classification mode [168](#)
client steering [244](#)
cloud authentication [59](#), [96](#)
configuration backup [69](#)
configuration management [69](#)
configuration synchronization [69](#)
configuration template [71](#)
connectivity [45](#)
Consumption mode [168](#)
contact information [254](#)
content filtering [140](#)
copyright [261](#)
CPU usage [102](#)
CRC error [172](#)
create user account [62](#)
CSS values [152](#)
custom portal pages [238](#)
custom theme [237](#)
customer support [250](#), [254](#)
Cyclic Redundant Check [172](#)

D

data processing agreement [28](#)
DCS [222](#)
 time interval [243](#)
DDMI [173](#)
device points [28](#), [38](#)
device registration [48](#)

DH key [147](#)
DHCP relay [124, 129](#)
DHCP server [124, 129](#)
DHCP server guard [204](#)
DHCP service [124, 129](#)
Diffie-Hellman key group [147](#)
Digital Diagnostics Monitoring Interface [173](#)
disable account [59](#)
disclaimer [261](#)
DNS settings [158](#)
domain zone [160](#)

E

eITS ticket [28, 250](#)
email report [225](#)
event log [108, 176, 220](#)

F

Facebook App ID [232](#)
Facebook fan page [232](#)
Facebook Login [232](#)
Facebook login [217](#)
Facebook Wi-Fi [217, 232](#)
fan page [232](#)
fast roaming [231](#)
firewall [135](#)
firewall rules [28](#)
floor plan [78](#)
force logout [55](#)
FQDN [160](#)
full access [57](#)
Fully-Qualified Domain Name [160](#)

G

get started [15](#)
Google Authenticator app [16](#)
guest ambassador [57](#)

access [59](#)
Guest interface [120, 127](#)
guest VLAN [199](#)
guest WiFi network [33](#)

H

hub router [67](#)
Hub-and-Spoke VPN [145](#)

I

idle timeout [54](#)
IDP [140](#)
IEEE 802.11k/v [235](#)
IEEE 802.11r [231](#)
IGMP filtering profile [192](#)
IGMP multicast groups [178](#)
IGMP query port [192](#)
IGMP snooping [193](#)
import certificate [55](#)
in-app push notifications [91](#)
installer [57](#)
Installer access [59](#)
internal antennas [213](#)
Internet Protocol Security [149](#)
Intra-BSS traffic blocking [234](#)
intra-BSS traffic blocking [228](#)
Intrusion Detection and Prevention [140](#)
IPSec [149](#)
IPSec VPN [146](#)
IPTV channels [27, 177](#)
IPTV Report [27](#)
IPTV report [176](#)

L

L2 isolation [228](#)
L2TP [149](#)
L2TP VPN [149](#)

- Layer 2 Tunneling Protocol [149](#)
- layer-2 isolation [234](#)
- leave mode
 - fast [192](#)
 - normal [192](#)
- LED tags [207](#)
- license credit [28](#)
- license key [53](#)
- license management [48](#)
- license transfer [38](#)
- lifetime license [50](#)
- Limited Lifetime License [50](#)
- Link Layer Discovery Protocol [171](#)
- LLDP [171](#)
- LLL [50](#)
- load balancing [247](#)
- load balancing method [157](#)
- Local Override [73](#), [74](#)
- local override [71](#)
 - switch [74](#)
- locator LED [167](#)
- log message [176](#)
- log messages [220](#)
- login page [237](#)
- logo
 - remove [40](#)
 - replace [40](#)
 - upload [40](#)
- loop guard [187](#)

M

- MAC authentication [231](#)
- Managed Services Provider [37](#)
- management VLAN [203](#)
- map
 - pin a device [79](#)
- Memory usage [102](#)
- MSP branding [39](#)
- MSP Portal [37](#)
- myZyxel account [15](#)

N

- NAS [161](#)
- NAS Identifier [233](#)
- NAS IP Address [161](#)
- NAT traversal [67](#)
- NCAS [234](#)
- NCC
 - access [15](#)
 - change device owner [29](#)
 - create organization [28](#)
 - Dashboard [76](#)
 - example network [14](#)
 - license [9](#)
 - license expiration [38](#)
 - license extension [9](#)
 - license status [38](#)
 - license transfer [38](#)
 - login [15](#)
 - organization [13](#)
 - overview [8](#)
 - portal [252](#)
 - portal website [15](#)
 - service downgrade [9](#)
 - service upgrade [10](#)
 - setup wizard [20](#)
 - site [13](#)
 - two-factor authentication [16](#)
 - version differences [10](#)
 - versions [9](#)
- NCC alert [23](#)
- NCC log messages [23](#)
- NCC menu [24](#)
- NCC Menu Summary [24](#)
- NCC Portal [15](#)
- NCC portal [21](#)
 - title bar [22](#)
- NCC service [9](#)
 - device points [38](#)
- NCC, Nebula Control Center [8](#)
- Nebula Cloud Authentication Server [234](#)
- Nebula Forum [28](#)
- Nebula Mobile app [91](#)
- Nebula points [38](#)
- Nebula Professional Pack [9](#)
- Nebula security points [38](#)

Nebula Security Service [26, 38, 111](#)
Nebula Smart Mesh [247](#)
Network Access Server [161](#)
Network Access Server identifier [233](#)
network topology [81](#)
next hop [133](#)
NSS [26, 111](#)
NSS-SP service [38](#)

O

operating system [217](#)
organization access [58](#)
output power [242](#)
owner [57](#)

P

PD priority [190](#)
Perfect Forward Secrecy [148](#)
PFS [148](#)
PoE [199](#)
PoE mode [168](#)
PoE schedule [190, 199](#)
policy route [133](#)
port forwarding [107](#)
port groups [119](#)
port isolation [189](#)
port mirroring [171, 203](#)
port security [199](#)
port settings [245](#)
port VLAN ID [187, 189](#)
power consumption [171](#)
power management mode [167, 168](#)
Power over Ethernet [199](#)
power-up [190](#)
pre-shared key [145](#)
privacy policy [28](#)
privilege [57](#)
problems [252](#)
product registration [261](#)

profile
 switch [74](#)
PVID [189, 212](#)

R

radio settings [241](#)
RADIUS accounting [233](#)
RADIUS server [233](#)
rate limiting [228](#)
read and write access [57](#)
read-only [57](#)
recurring schedule [95](#)
register a device [25, 48, 92](#)
registration
 product [261](#)
restore configuration [71](#)
root bridge [166](#)
RSTP Status [166](#)

S

schedule firmware upgrade [25, 74, 93](#)
schedule template [200, 241](#)
security services [102](#)
serial number [48, 164](#)
Server-and-Client VPN [145](#)
Service Set IDentifier [226](#)
service type [53](#)
setup wizard [31](#)
severity level [250](#)
side-wide schedule [95](#)
site binding [72](#)
Site-to-Site VPN [145](#)
spanning tree [166](#)
SSID [226](#)
SSID profiles [226](#)
SSID schedule [239](#)
submit ticket [249](#)
summary report [78](#)
support account [250](#)

support request [249](#)
supported browsers [252](#)
supported Nebula devices [9](#)
switch connection status [164](#)

T

ticket details [249](#)
traffic shaping [155](#)
transmitting power [245](#)
troubleshooting [252](#)
trunk group [186](#)
trunk port [189](#)

U

U-APSD [235](#)
uplink AP [208](#)
user account type [60](#)

V

virtual private network [143](#)
Voice VLAN [203](#)
VPN [143](#)
VPN member [65](#)
VPN topology [66](#)

W

walled garden [158](#), [228](#), [233](#)
WAN throughput [77](#)
warranty [261](#)
 note [261](#)
web authentication [153](#)
WINS server [124](#), [130](#)
wireless channel bandwidth [243](#)
wireless health [220](#)
world map [78](#)