ZYXEL

Your Networking Ally

Application Note

Nebula Control Center

nebula

www.zyxel.com

Table of Contents

Introduction....3
Cloud Networking....4
Monitoring....5
Site-Wide monitoring and reporting....6
Network Deployment....7
Feature Highlights....7
Add Nebula device into NCC by QR code....8
Zero-Touch Settings....9
Pre-configured settings....9
Site-to-Site VPN Configuration....10
Cloud Services....12
On cloud firmware upgrades....12
NAP Captive portal with Cloud Authentication....13
Compatibility....15
Power over Ethernet on NSW switch ports....16

ZYXEL

www.zyxel.com

Introduction

Networks are the core components of today's communication, connecting people across different technologies and breaking frontiers and limitations within few steps to set up. However, with the increase of networks and business expansions, users are facing more challenging activities that require high investment in budget, human resources and time.

Nebula Cloud Networking allows the customers to focus in their core business, entrusting their networking issues on a very scalable, reliable and time saving business solution. We understand our small and medium business customers are committed to provide the best of them, and Nebula has been designed to provide a helpful, efficient and pleasant experience for networking duties with a cost-effective price that is unbeatable in the market.

Cloud Networking

Nebula Cloud networking and management solution has been carefully built to ensure that network administrators will be able to access their network from all over the world through internet access, but within a secure communication channel.

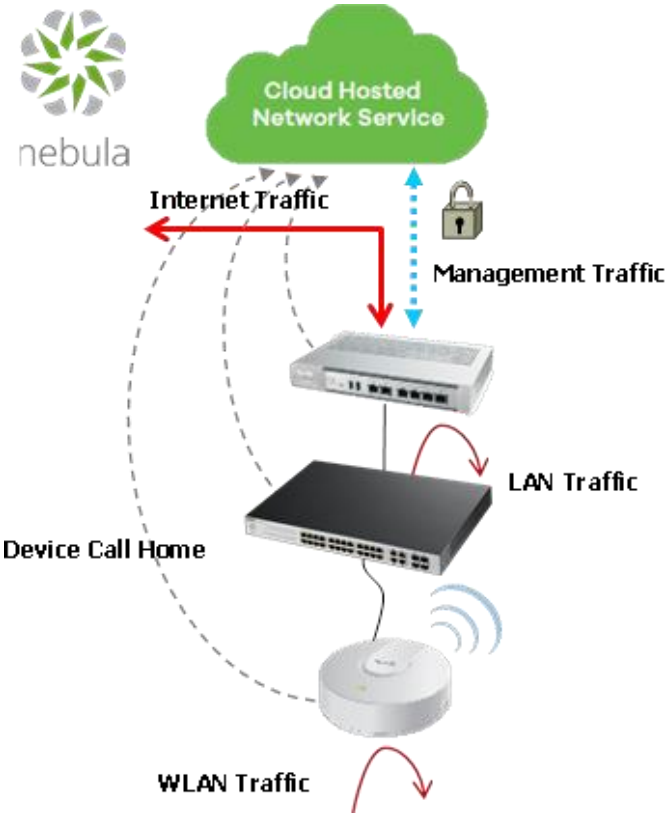


Figure 1 Nebula Product Portfolio and Management access

Nebula uses the NETCONF [1] protocol along with TLS[2] to ensure that neither management traffic nor user data will be compromise. Moreover, the use of NETCONF protocol allows each Nebula Product to use the *Call Home* feature which connects the device to Nebula Control center, synchronizing configuration and providing monitoring and management features.

The ability to load a predefined configuration from Nebula Control Center, in the first time the device is connected, makes possible the *Zero-touch provisioning*, saving time in the network deployments.

[1] Network Configuration Protocol: network management protocol

[2] Transport Layer Security: cryptographic protocol

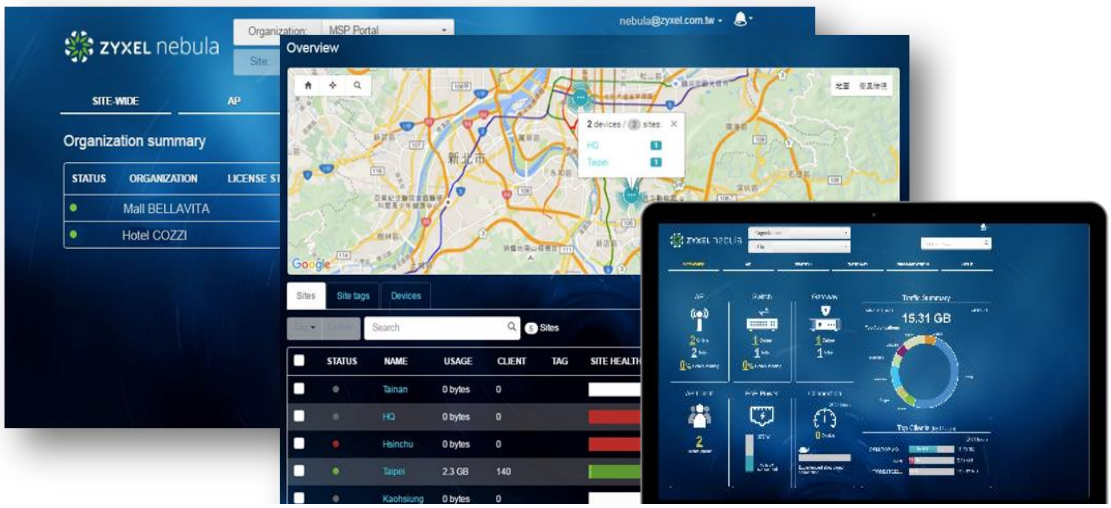
Monitoring

Traditionally

High skilled IT personnel are needed for network management and monitoring, who have to face a lack of complete multi-site unified network monitoring, reporting or measuring tools.

Nebula

Due to its Organization and Site management based, Nebula provides a 24/7 multi-Organization overview and site-wide monitoring with a complete informative dashboard.



MSP Portal, Organization Overview and Site Dashboard

Site-Wide monitoring and reporting

Site-wide > Summary Report

Displays overall site-wide network statistics based on TOP devices' bandwidth, power usage, TOP clients and SSIDs.

1. Period of time:

Network administrators are able to define a period of time (Last day, Last 7 days, Last 30 days, custom range) to analyze the site health.

2. Report Size:

Users can select a fixed number (1, 5, 10, 20 or 50) of TOP devices to display by table. Thus, TOP 1 will show the device with most usage, clients and TOP used SSID.

3. Email report:

Nebula is able to create reports out of the site-wide summary to send to emails accounts.

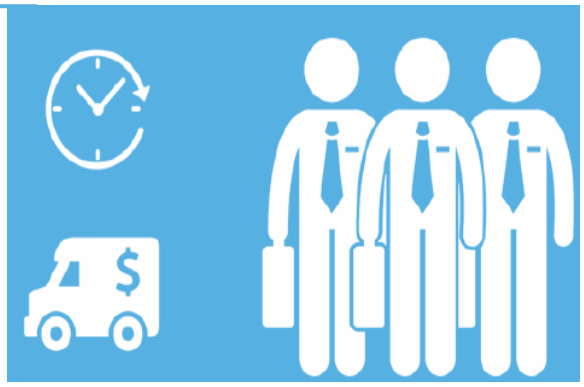
User could select two options:

- Provide email address and Format (HTML or Plain text) to send report instantaneously.
- Schedule reports, customizing emails with logo, destination email address, email subject, frequency of reporting and format (HTML or Plain text).

Network Deployment

Traditionally

Aside the hardware to be deployed, technical engineers need to move to the deployment site and carry all the necessary equipment as laptops and chargers, console cables and modems in order to set up the new network.



Nebula

Nebula solution provides a mobile APP for Android and iOS to monitor sites conditions and keeps network deployments easy by its adding devices mechanism.

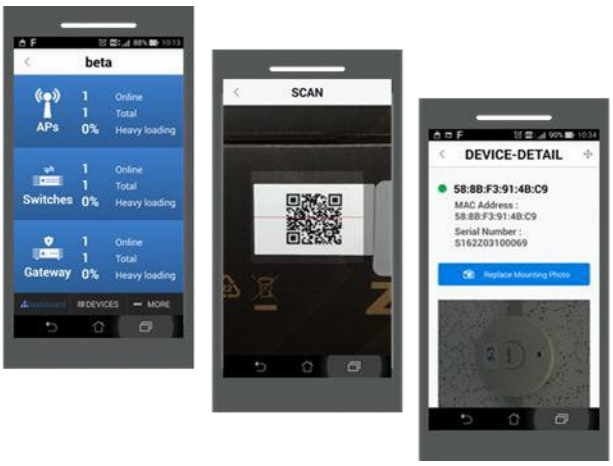
Nebula Mobile App Interface

<u>Feature Highlights</u>

- Built-in QR code scanner for quickly adding hundreds of devices.
- Photo capturing to upload the mounted device's location.
- Nebula uses the GPS information of the uploaded photo to determine device location in the Map & Floor plan section.
- Overview of active Nebula APs, Switches and Gateways by site.
- Quick selection between different sites.

Add Nebula device into NCC by QR code

In order to add a device by QR code, it is necessary to have your account with an **ORGANIZATION** and **SITE** previously created, and then proceed to install the Nebula Mobile APP in your cellphone.



Steps:

1. Sign-In using MyZyxel.com account.
2. Surf to the **ORGANIZATION** and **SITE** where the device is going to be added.
3. Click on the **Devices** tab and on "+" icon afterwards.
4. Scan the QR code which is labeled on the carton or stick on the device.

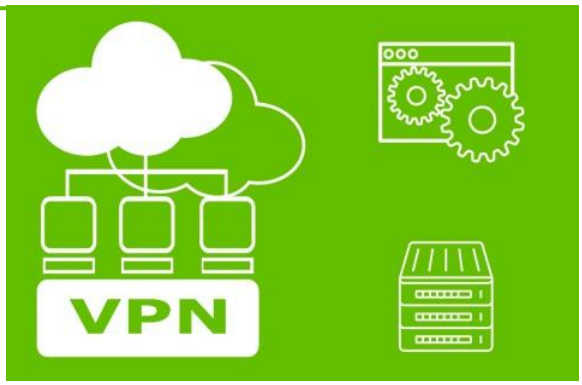
Zero-Touch Settings

Traditionally

Network administrators have to apply the same configuration to multiple devices, having to log in to each device which results in a very repetitive and time consuming task. Moreover, those tasks might involve certain level of complexity.

Nebula

Offers simple process to configure complex features as VPNs, NAT, Policy rules, etc., being able to apply settings to multiple devices at the same site due to its site based approach.



<u>Pre-configured settings</u>

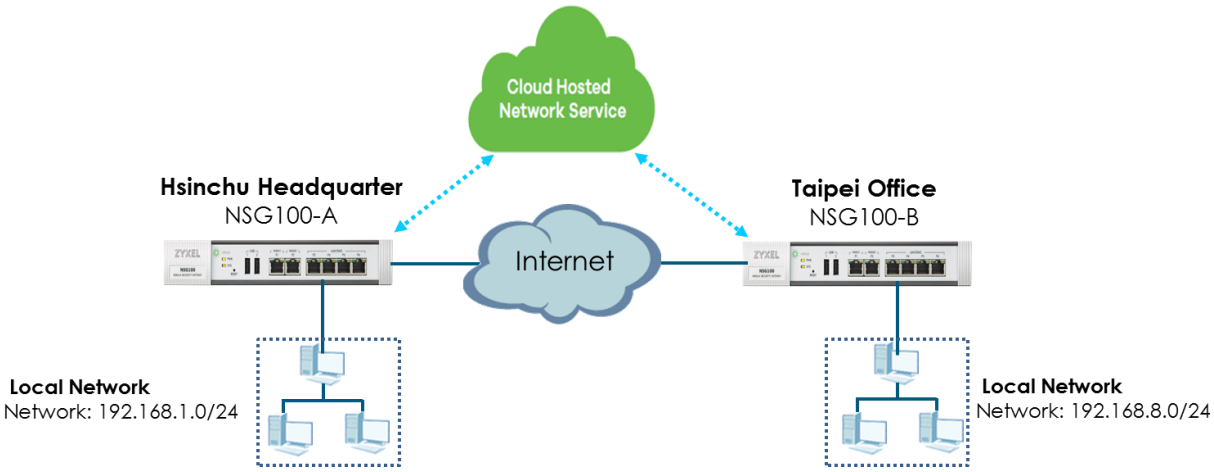
Manage traffic of internet applications might involve many steps such as investigate applications' network protocols and ports.

Nebula Application Patrol feature considerably reduce the procedure by having pre-configured multiple settings that network administrators can select and apply to policy rules in order to manage the traffic of most common applications.

Applications pre-configured with Application Patrol

Site-to-Site VPN Configuration

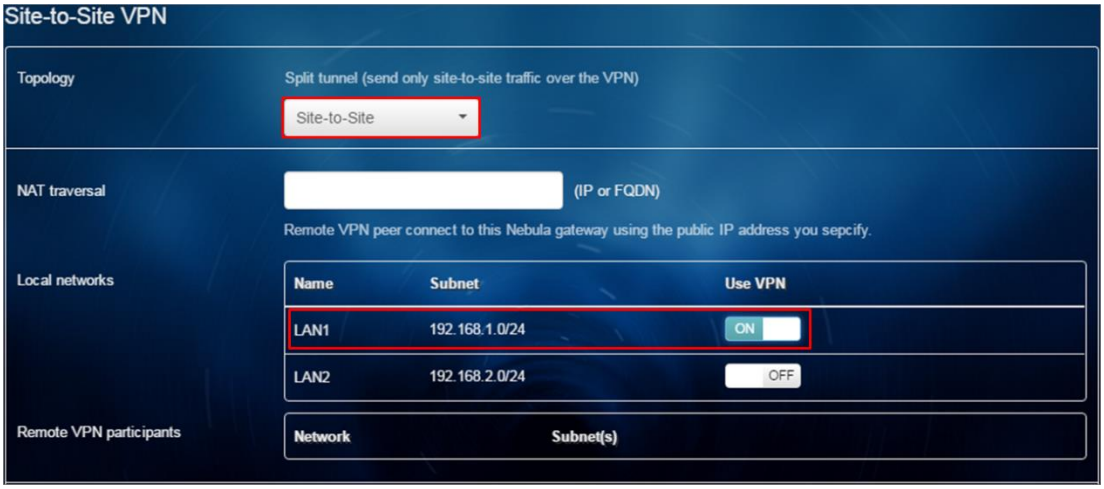
With Nebula, VPN tunnels are automatically established with just a few clicks on a single platform. Simply select the **VPN topology** and **IP networks** in each NSG and VPN tunnel is established afterwards.



Site 1: Hsinchu Headquarter

Gateway > Configure > Site-to-Site VPN

- Topology: Select **Site-to-Site** for tunnel creation between two sites.
- NAT trasversal (Optional): Create a NAT to define the Public IP address to which the remote peer will be connected. If not defined, the public IP address of the devices will be used for VPN.
- Local Networks: Select local networks to include into VPN connection.



Site 2: Taipei Office

Gateway > Configure > Site-to-Site VPN

- Topology: **Site-to-Site** will be the only option enabled to select once it has been set the same in the other site.
- NAT trasversal (Optional): Create a NAT to define the Public IP address to which the remote peer will be connected. If not defined, the public IP address of the devices will be used.
- Local Networks: Select local networks to include into VPN connection.
- Remote VPN participants: Shows the remote networks configured into VPN setting in the other Site

Connectivity Status

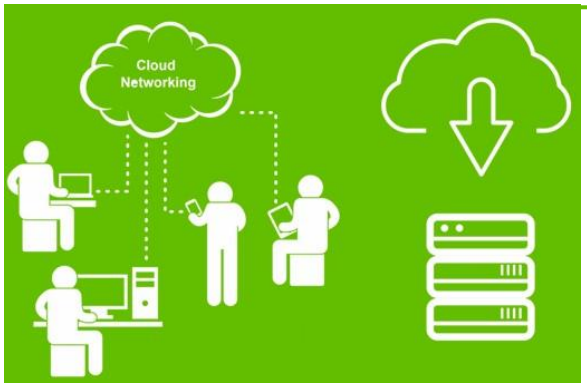
Gateway > Monitor > VPN Connection

Displays general information, status and uptime of VPN connections:

Cloud Services

Traditionally

Network administrators need to set different servers for services such as authentication management, which might take time, economic resources and effort.

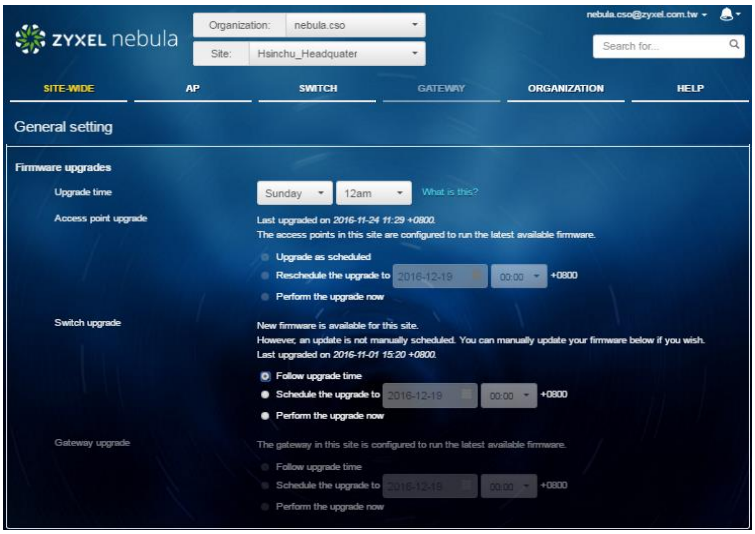


Nebula

Offers users cloud services that make things easier and faster, saving the money invested in servers. The services include: on cloud firmware upgrades, users' authentication database, alerts' emails, time synchronization.

<u>On cloud firmware upgrades</u>

Site-Wide > Configure > General Setting > Firmware upgrades



Site-Wide Firmware upgrades available

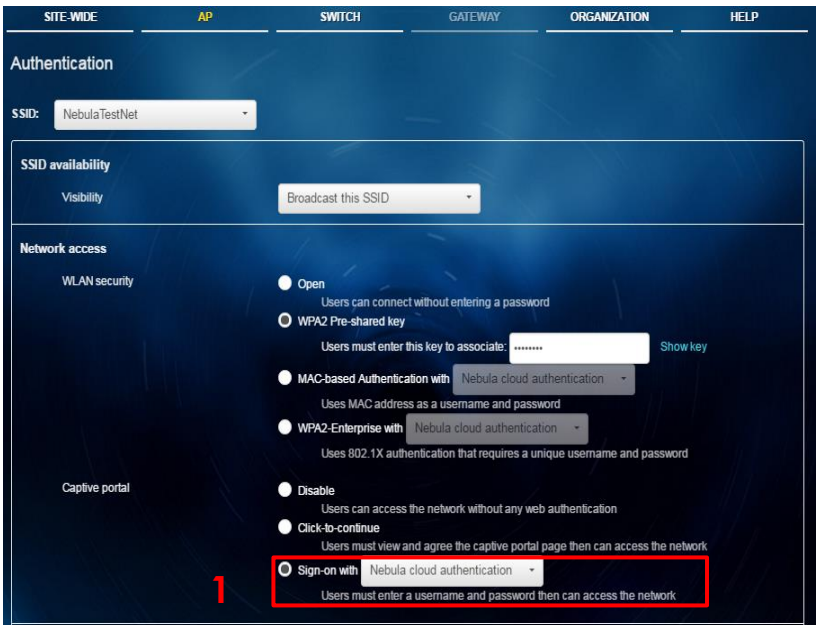
Having all the devices with the latest firmware available is crucial for a better network performance.

Nebula provides the chance to update all the site's devices at once when there is an upgrade available on the cloud. Moreover, users are able to schedule the upgrading time for a minor network impact.

NAP Captive portal with Cloud Authentication

Cloud Authentication provides user management for 802.1x authentication and MAC-based authentication (WLAN security access), captive portal (SSID's network access) and L2TP VPN authentication; without the need to setting up radius or active directory servers.

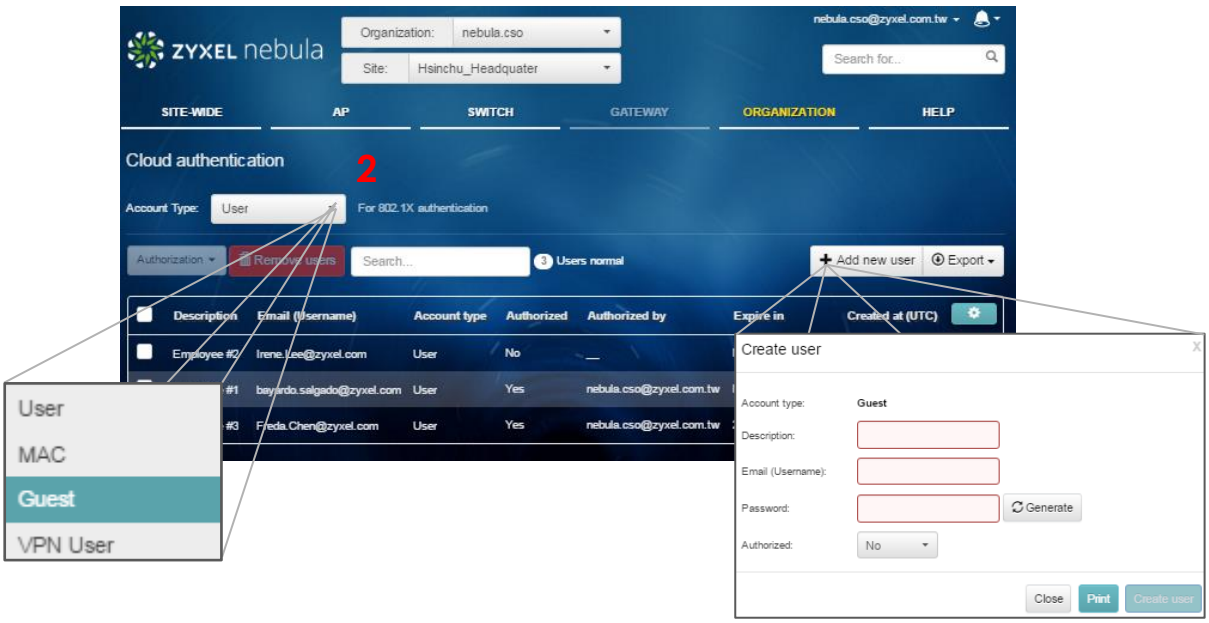
AP > Configure > Authentication



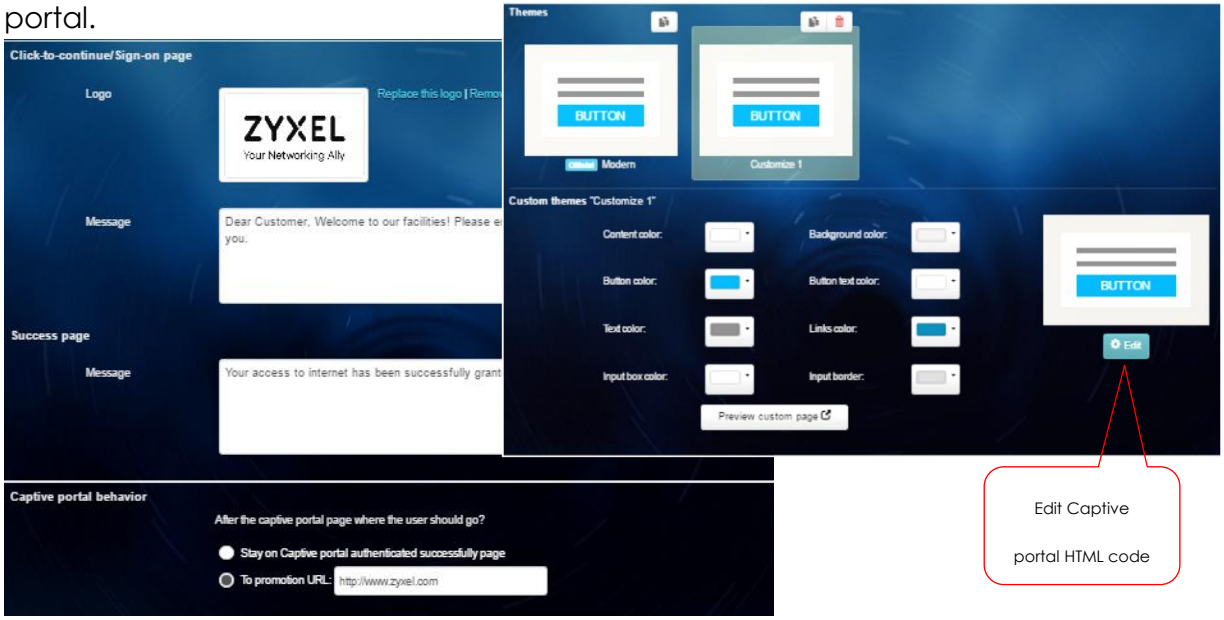
1. In Network access > Captive portal section, select **Sign-on with** radio button and **Nebula Cloud authentication** from the drop down menu.

2. In Cloud authentication, select the Account type **Guest** and **+ Add new user** login information: Email Description, Authorization, Password and expiring date.

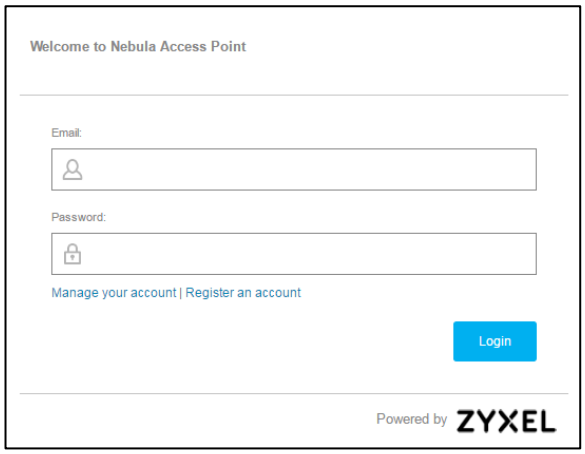
Organization > Cloud Authentication



3. Network administrators are able to customize NAP's captive portal design in **AP>Configure>Captive Portal,** adding logos, messages, and behavior after captive portal.

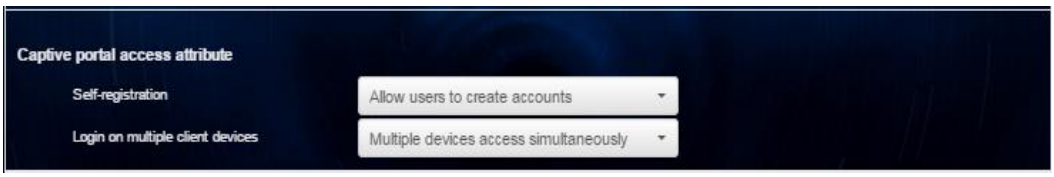


4. Once the user or guest is connected to the WLAN, the captive portal will be displayed and request the input of Email and password configure to login.



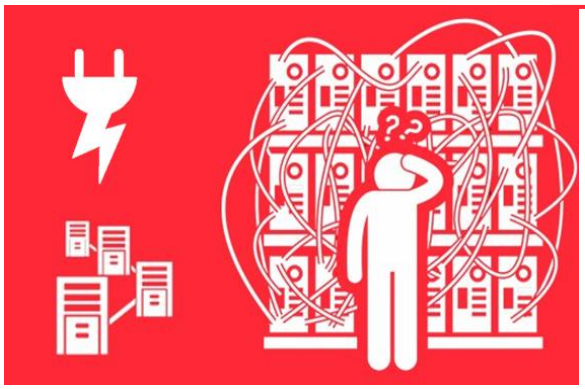
Users are able to see their account details by clicking "Manage your account" link, as well as "Register an account".

The **Self-registration** will depend on the settings configured in **AP>Configure>Authentication> Captive portal access attribute:**



By default, the self-registration is allowed and the user is able to use the account to **login on multiple client devices** simultaneously.

Compatibility



Traditionally

Network administrators have to include multiple devices to satisfy network requirements. The more devices the network has, the more time is spent to fix power and ethernet cables in order, and avoid messy arrangement.

Nebula

Offers wired and wireless product portfolio that satisfies most network needs, with an end-to-end solution to ensure operability through a plug and play process for network deployments.

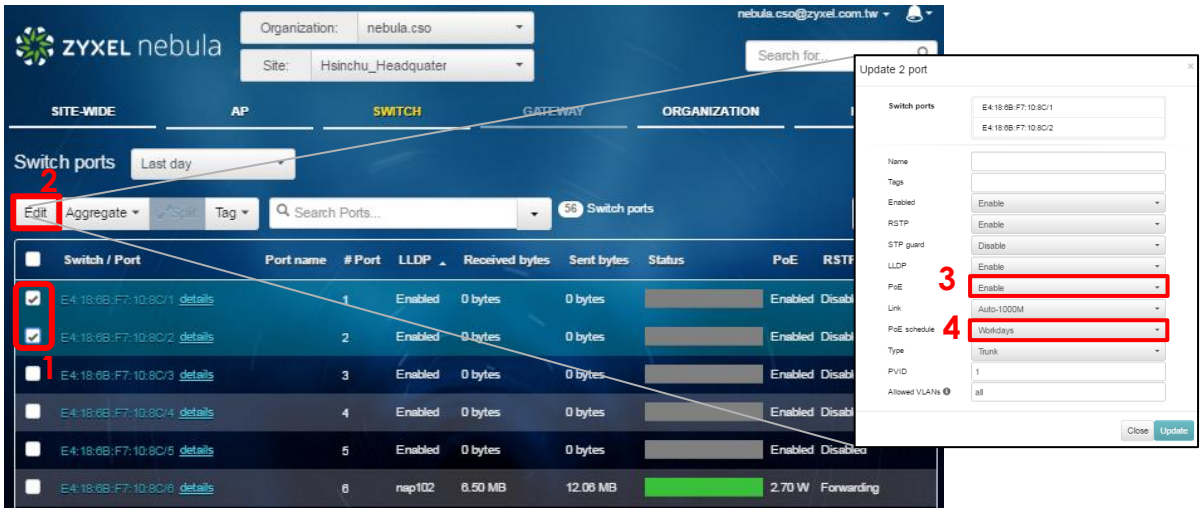
Nebula Solution is composed by three different network devices type: the **NSG** to guard the TCP/UDP traffic and take care of routing path and rules; the **NSW** to assign different VLANs for network segmentation, moreover, it can deliver the power up to 30W (IEEE 802.3at) to NAP's uplinks; the **NAP** to deliver high throughput and reliable coverage for superb Wi-Fi experience.

Nebula Product Family

Power over Ethernet on NSW switch ports

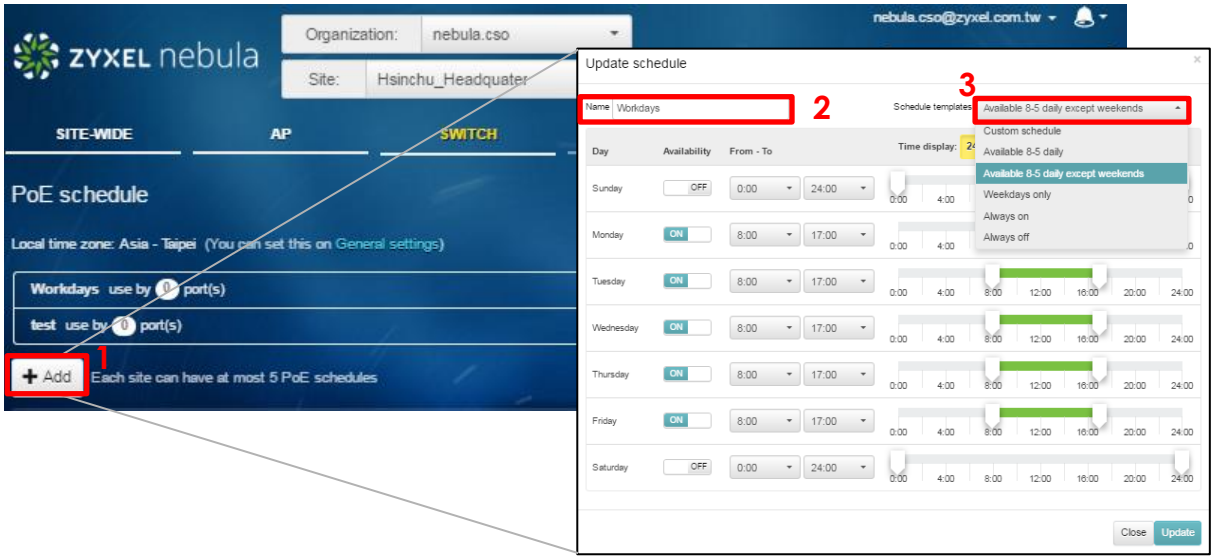
By default, both NSW100 and NSW200 are able to provide PoE+ (IEEE 802.3at, classification mode) through their first 24 ports.

Switch > Configure > Switch ports



1. To disable/enable PoE, select one or multiple ports at the same time.
2. Once the port(s) has been selected, click on the **Edit** button.
3. In the pop-up windows, select **PoE** and choose between Enable/Disable.
4. If desired, network administrators can define a schedule profile in which the switch ports will provide PoE (explained below), and select the profile in **PoE Schedule**.

Switch > Configure > PoE schedule



1. Click **+ Add** to create a Poe Schedule profile.
2. Write down a specific name for the profile.
3. Network administrators can select among different schedule templates to provide PoE:
   - Custom Schedule: the administrator can define the days' **Availability** and the time **From – To** with the drop down menu or the slide bar (green area means Poe provided)
   - Available 8-5 daily: schedule from 8am to 5pm, seven days of the week.
   - Available 8-5 daily except weekend: schedule from 8am to 5pm, from Monday to Friday.
   - Weekdays only: schedule all day long, from Monday to Friday.
   - Always on: PoE provided all day long, seven days of the week.
   - Always off: PoE is not provided at any time.