ZYXEL

# Application Note

## Setting up your Guest networks

**Supported devices:**
Nebula Security Gateway (NSG)
Nebula Access Points (NAPs) and NebulaFlex (Pro) APs

## Nebula Cloud Networking and Management Solution

# Introduction

Providing WiFi access to customers has become part of the basic needs in today's business demands, being a must for cafes, restaurants, chain stores and essential in sectors such as education and hospitality. But the need is not solved by just providing a WiFi connectivity, administrators need to ensure that the networks are built upon secure layers that allow business to keep both, guest and internal networks isolated and secured.

This document will guide users to set up their guest and intranet network using the Nebula Control Center and its supported devices - APs and NSG -, pointing out the different methods that Nebula offers. The information is focused on wireless networks but also including wired network

# Tuning up your existing networks

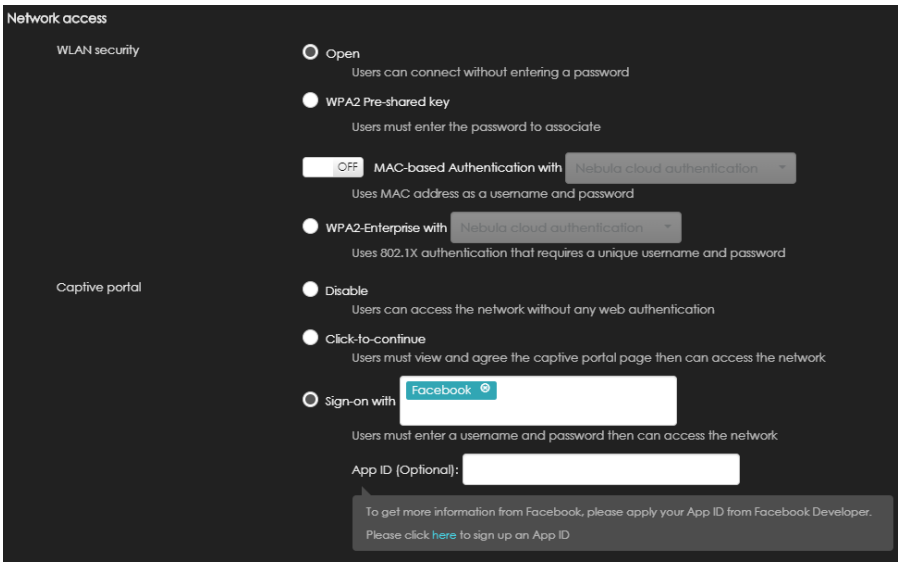
NCC provides a convenient wizard that will optionally allow you to set both, the internal or employee WiFi network and the guest WiFi network within simplify settings. The options here are simplified and the WiFi networks can be further set up following the next steps:

### SSID Authentication settings

Once you are up and running, your Wi-Fi authentication settings can be changed at any time, simply get into AP > Authentication, select the SSID that you wish to change and check the different *Network access* options available:

- **WLAN security:** these methods define how the Wi-Fi users are associated to the network.
    - WPA2 Pre-shared key: a simple, easy way with passphrase security and AES encryption.
    - MAC authentication: ensures that only the pre-defined devices' MAC address will be allowed to associate. It supports RADIUS and Nebula Cloud Authentication Servers (NCAS)
    - WPA2 Enterprise with 802.1x: with EAP authentication and AES encryption supporting RADIUS server and NCAS.

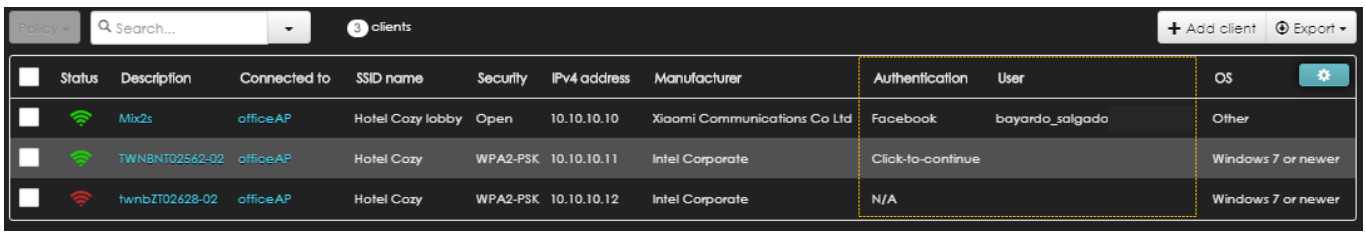
For guest WiFi in environments like chains stores, restaurants,etc., it's suggested to set Open or WPA2-PSK (providing password easily) for ease of authentication. Hotels and schools might add an extra layer of association as MAC authentication. For internal networks, it's recommend to set WPA2 Enterprise with 802.1x or WPA2-PSK with MAC authentication to guarantee security.




- **Captive portal:** web authentication page displayed to Wi-Fi users prior broader access to network resources.
    - Click-to-continue: users has to agree to terms or network message by clicking the "Agree" button.
    - Nebula Cloud Authentication: requiring user to enter username/password or allowing them to self-register an account. A service provided by Nebula, which accounts can be managed on Site-wide > Cloud authentication.
    - Facebook social login: uses a Facebook APP that provides user's Facebook account information (email, gender, locale and age rank).
    - Facebook Wi-Fi: requires users to check-in to the business's Facebook page.
    - My Radius server: requiring users to enter a username/password that has been defined in the company's Radius server.

It's highly recommend to set a captive portal authentication for a guest network. Click-to-continue is the most simple way for both admins and users, and it's recommended when there's no need to control who's getting access. Facebook Wi-Fi is an excellent tool to promote your business in social media, ideal for restaurants, cafes and chain stores. Facebook social login is a good method to to gather information from the WiFi users and use it for marketing purpose if desired.
In environments such as hotels, schools or even entreprises (internal networks), the Nebula cloud authentication or My Radius server are the ideal solutions as the users' DB can be easily controlled by the network admin.

Once the users are connected and authenticated, you could check the authentication information used in AP > Client. AP- Summary report emails also provide more information like age, gender and locale for SSIDs using Facebook social login.



## Gateway - Network access method

Most of the captive portal authentications can be applied at the gateway level instead, covering the wired guest networks. These settings are applied to the LAN/VLAN interfaces, and can be found on Gateway > Network access method:

- Click-to-continue and Nebula Cloud Authentication: similar to Wi-Fi option.
- Sign-on with authentication servers: requiring users to enter a username/password that has been defined in either Radius or Active Directory company's servers (configured on Gateway > Network servers > Authentication servers)

Enable captive portal on the gateway if the same VLAN interface will be used for the wireless and wired guest networks. Enable it on the AP for more social media options or when only a guest Wi-Fi is required. For the wired network, the Nebula switch ports also support 802.1x and MAC based authentication with Radius servers configurable on Switch > Switch configuration > Radius policy.

## AP and gateway guest features

Nebula provides a set of features that help to build an isolated guest network:

AP > Authentication

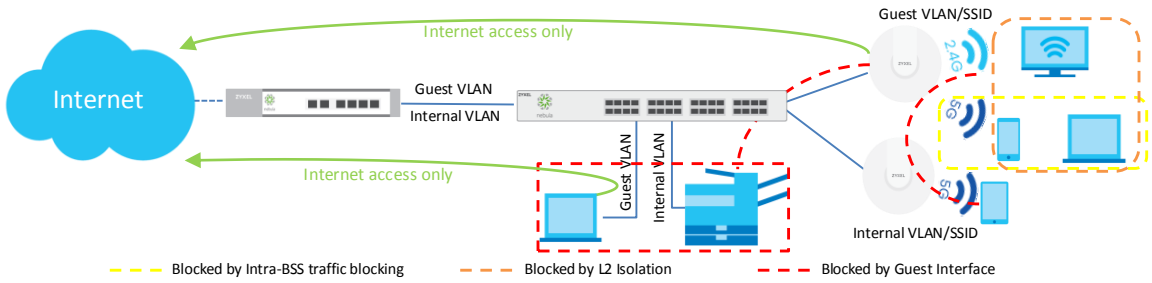
- **Intra-BSS traffic blocking:** prevent traffic between wireless clients connected to the same BSSID. Note that 2.4 Ghz and 5Ghz are defined as different BSSIDs.
- **L2 isolation:** limits wireless clients to only communicate with devices which MAC addresses have been added to the L2 isolation list, therefore, listing the gateway's MAC address is necessary to ensure connectivity to internet. Note that L2 isolation has a limitation, if the NSG's MAC address is added, any VLAN interface also configured on the same port group of gateway will be reachable.

AP > SSID

- **Guest network:** an easier way to enable L2 isolation on the SSID. The AP adds the gateway's MAC address of its management VLAN automatically; if the SSID uses a VLAN configured in another gateway/server or port group, the MAC address must be added.

Gateway > Interface addressing

- **Guest interface:** the VLAN interface is limited to internet access only, meaning that all the clients connected (either wireless or wired) will not be allowed to access any other non-guest VLAN, but they can still communicate with each other.




As illustrated above, guest networks can be totally isolated by enabling *Guest network* on AP and *Guest interface* on gateway. *Guest interfaces* complements *Guest network* by blocking inter-VLAN communication in L3 capability. Likewise, *Guest network* complements *Guest interface* by blocking the communication between wireless clients.

## Captive portal more options and themes

### AP > Authentication / Gateway > Network access method

While setting up the captive portal authentication methods, NCC provides more granular options that might be useful to tune your guest network.

- **Walled garden**: configurable per SSID and VLAN interface (GW), it allows inputting URLs that users can access before captive portal authenticating.
- **Self-registration:** only available with NCAS. It defines if users are allowed to create accounts through captive portal. If allowed, *manual authorized* require network admin to authorize the account created by the user; *auto authorized* allows users to authenticate as soon as they create the account. If not allowed, network admin needs to create the account manually in Site-wide > Cloud authentication.
- **Login on multiple client devices:** *Multiple devices access simultaneously* allows using the same account in multiple devices at the same time. *One device at a time* will restrict an account to be used on one device only.
- **Strict policy:** use this option to decide if users are *allowed to access HTTPS* websites before captive portal authenticating, or *block all access* until users successfully authenticate.

### AP/Gateway > Captive portal

Nebula also offers the option to customize the captive portal with different themes for businesses or hotels requiring greeting message, logo or link to external URL, where you can type in your desired marketing messages or terms and conditions to welcome your guests.

 It is recommended to set self-registration with auto authorized in environments where admin control is hard or not needed, such as restaurants, cafes, chain stores, etc. Not allowing self-registration can be implemented in environments such as hotels, where accounts can be created while user checks-in. Block all access with strict policy option is overall recommended to force users to authenticate through captive portal, and to ensure that mobile phone's Captive Network Assistant (CNA) will pop-up.

Lastly, captive portal might be a powerful tool to advertise or deliver a message to users; hence, choosing the right authentication method for your business is essential, along with the right customized design to engage users easily.

ZYXEL

Your Networking Ally