EnGenius®

User Manual

Distributed Network Management Solution

ezMaster

v0.11.12

Table of contents

Introduction

Overview

EnGenius ezMaster is a powerful and scalable enterprise-class centralized network management system that manages EnGenius Neutron Series products for building and managing enterprise grade Wi-Fi infrastructures for all sizes of businesses from a single console.

Through an intuitive user interface, Neutron devices are managed based on projects, enabling simplified WLAN configuration, firmware upgrades, centralized monitoring and much more, making managing thousands of devices as easy as managing a single device.

ezMaster Software

ezMaster is packaged as a virtualization appliance image for quick and easy deployments. It can be launched using VirtualBox, VMware or other virtualization products.

Compatible Access Points

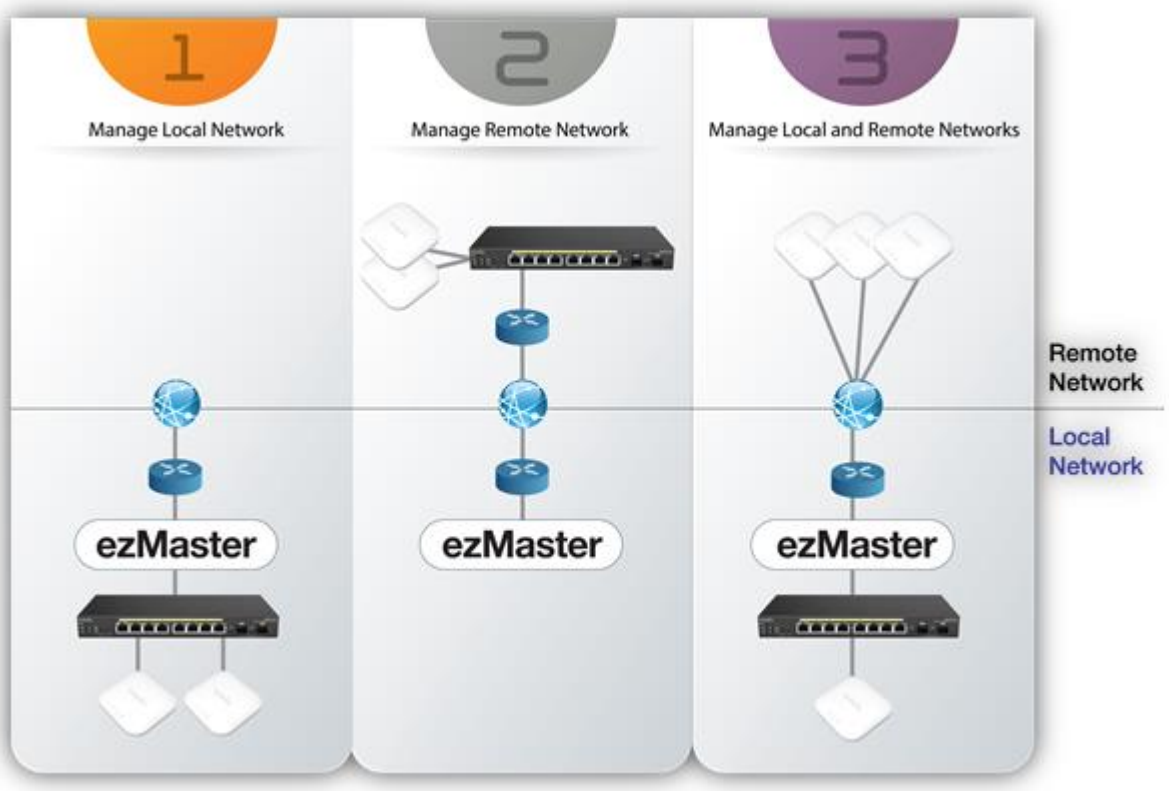
Before ezMaster is able to manage a device, the access point/switch must be running with the required firmware version.

This release (ezM v0.11.8) supports the following EnGenius EWS devices running firmware version **c1.8.x** or later:

Wireless Managed Access Points
EWS300AP Single Band Wireless N300 Managed Indoor Access Point
EWS310AP Dual Band Wireless N600 Managed Indoor Access Point
EWS320AP Dual Band Wireless N900 Managed Indoor Access Point
EWS350AP Dual Band Wireless AC1200 Managed Indoor Access Point
EWS360AP Dual Band Wireless AC1750 Managed Indoor Access Point
EWS500AP Single Band Wireless N300 Managed Wall Plate Access Point
EWS510AP Dual Band Wireless N600 Managed Wall Plate Access Point
EWS650AP Dual Band Wireless AC1200 Managed Outdoor Access Point; IP55
EWS660AP Dual Band Wireless AC1750 Managed Outdoor Access Point; IP55
EWS860AP Dual Band Wireless AC1750 Managed Outdoor Access Point; IP68

Wireless Management Switch
EWS1200D-10T 8-Port GbE Managed Smart Switch w/ WLAN Controller
EWS1200-28T 24-Port GbE Managed Smart Switch w/ WLAN Controller
EWS1200-52T 48-Port GbE Managed Smart Switch w/ WLAN Controller
EWS2910P 8-Port GbE PoE L2 Wireless Management Switch with 2 SFP Slots; 61.6w
EWS5912FP 8-Port GbE PoE+ L2 Wireless Management Switch with 2 GbE Ports and 2 SFP Slots; 130w
EWS7928P 24-Port GbE PoE+ L2 Wireless Management Switch with 4 SFP Slots; 185w
EWS7928FP 24-Port GbE PoE+ L2 Wireless Management Switch with 4 SFP Slots; 370w
EWS7952FP 48-Port GbE PoE+ L2 Wireless Management Switch with 4 SFP Slots; 740w

Deployment Scenario



Before you begin

For ezMaster to manage an AP or switch, the device must be able to communicate with the ezMaster server. Make sure that the ezMaster server, EWS AP and EWS switch can all be reachable via HTTP/HTTPS from outside your internal network.

System Requirements

Recommended environment for managing up to 500 APs
CPU: Intel i3 3.6GHz dual core or above
RAM: 4GB minimum
HDD: 500GB (actual requirement depending on log size)
OS: Microsoft Windows 7 or later + VirtualBox 4.3.30 (or similar virtualization products)

Recommended environment for managing up to 1000 APs
CPU: Intel i5 3.2GHz quad core or above
RAM: 4GB minimum
HDD: 500GB (actual requirement depending on log size)
OS: Microsoft Windows 7 or later + VirtualBox 4.3.30 (or similar virtualization products)

Browser Requirements
Internet Explorer 10 or better
Firefox 34.0 or better
Chrome 31.0 or better
Safari 8.0 or better

Network Topology Requirements
At sites where APs are deployed: a DHCP enabled network for APs to obtain IP address

Firewall Port Configuration

Depending on how your network is designed, you may need to open ports on your firewall.

The following **outbound** ports MUST be opened in the firewall at the site where the ezMaster server is located in order for ezMaster to register with the ezReg server.

Port	Description
TCP 80	HTTP port, ezReg communication
UDP 53	DNS port, ezReg communication

The following **inbound** ports MUST be opened in the firewall at the site where the ezMaster server is located in order for remote access points to communicate with the ezMaster server.

Port	Description
UDP 1234	Custom port, CAPWAP protocol
TCP 80 (default)	HTTP port, Captive Portal, *port can be defined by user*

The following **outbound** ports MUST be opened in the firewall at the remote site where the AP/switch is deployed in order to communicate with ezMaster.

Port	Description
UDP 1234	Custom port, CAPWAP protocol
TCP 80	HTTP port, ezReg communication
UDP 53	DNS port, ezReg communication
TCP 80 (default)	HTTP port, Captive Portal, *port can be defined by user*

Installing ezMaster

The instructions below will guide you through the process of installing ezMaster VM.

Getting a Virtualization Product

ezMaster VM is distributed as an Open Virtualization Appliance (OVA) which should be compatible with these virtual machine products.

- VirtualBox (v4.3.30 recommended*)
- VMWare Workstation Player 12

Note: At the time of release, VirtualBox v5 has known issues with bridging NICs: https://www.virtualbox.org/ticket/14558. We recommend using VirtualBox v4.3.30.

Getting the ezMaster Virtual Machine Image

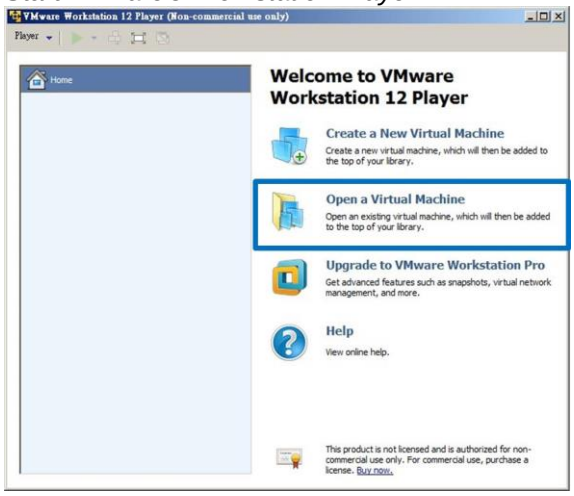
The ezMaster VM file can be downloaded from the EnGenius website. Due to the size, it may take some time to download.

Importing the ezMaster VM Image

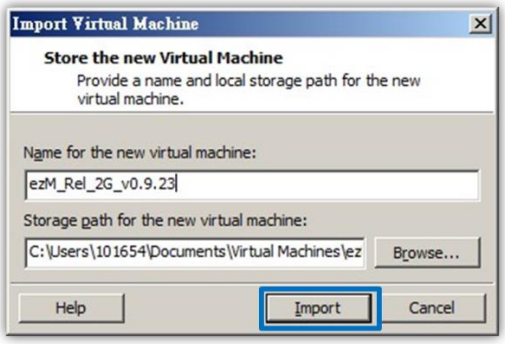
Each virtualization product has different methods for using a VM appliance. The tested methods are as below. Procedures for launching ezMaster on other virtualization products are similar.

Launching the ezMaster VM image using VMware Workstation Player 12

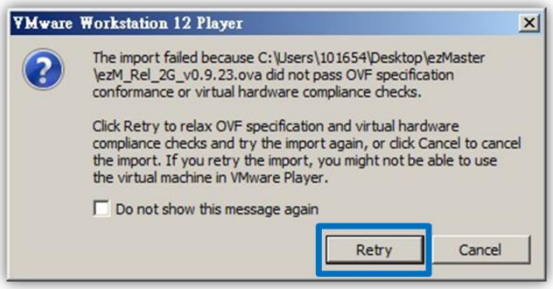
1. Start *VMware® Workstation Player* and click on "***Open a Virtual Machine".***



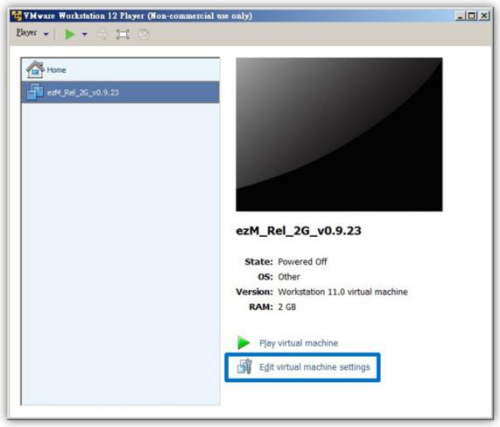
2. Locate and select the ezMaster VM image file (.ova), then press ***"Import"***.



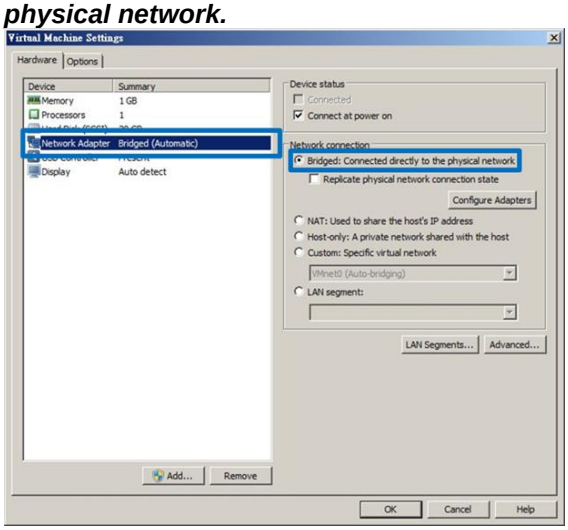
Additional Information
When importing the .ova file, you may see this error:
The import failed because .ova did not pass the OVF specification conformance or virtual hardware compliance checks.
If you see this error, click Retry with lower specifications to relax the specification and start the import.



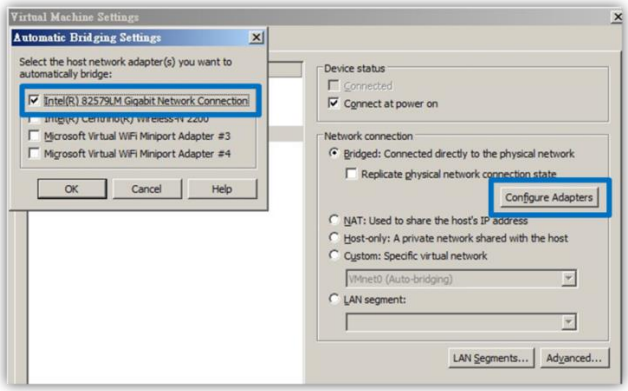
3. The VM should now be visible in the list. Click on **"Edit virtual machine settings"**.



4. Under the ***Hardware*** tab, click on ***Network Adapter*** and select ***Bridged: Connect directly to the physical network.***

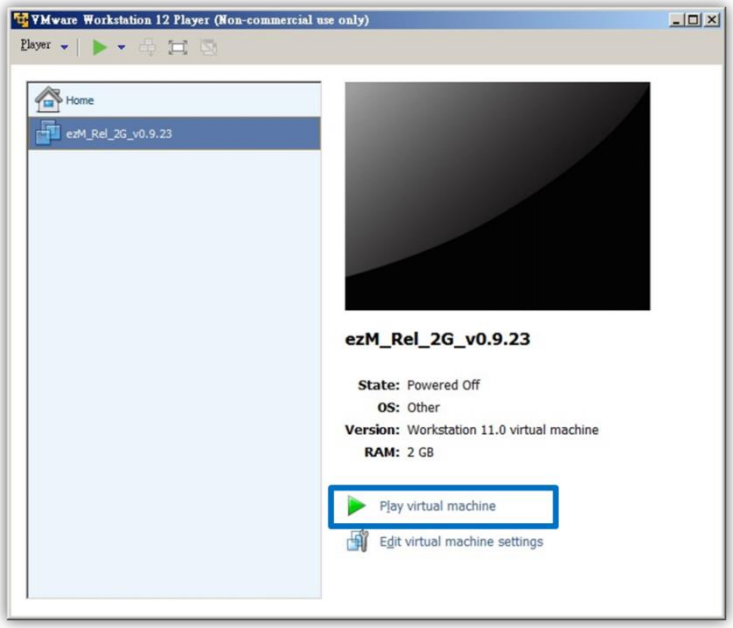


If your PC has more than one network adapter, click on ***Configure Adapters*** and choose the network adapter that your computer uses to connect to the Internet (WAN). Choose only one wired LAN adapter. DO NOT select a Wireless LAN adapter or other virtual adapters.



5. Click on ***OK*** to save and apply settings.

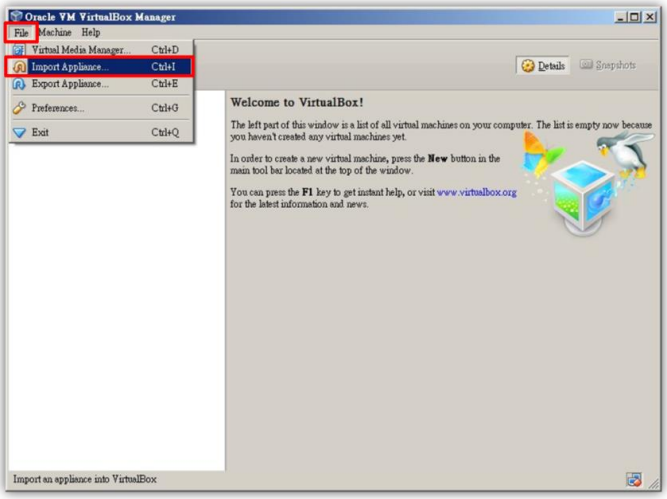
6. After setting up your network adapter, press **"*Play Virtual Machine"*** to launch the ezMaster image.



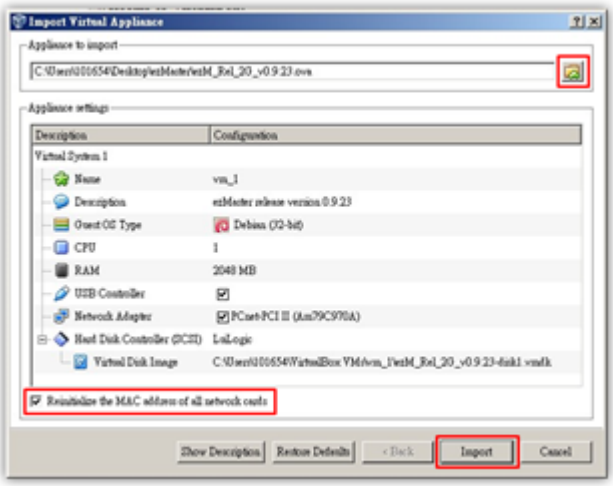
Launching the ezMaster VM image using VirtualBox 4.3.30

1. Download and install VirtualBox 4.3.30 for Windows.
   https://www.virtualbox.org/wiki/Download_Old_Builds_4_3

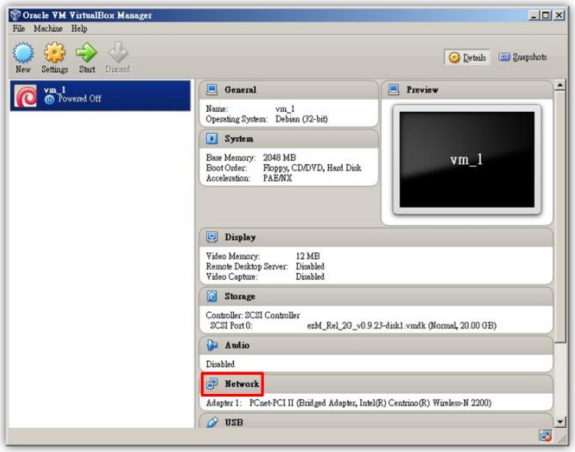
2. Start VirtualBox and click on ***File > Import Appliance…***



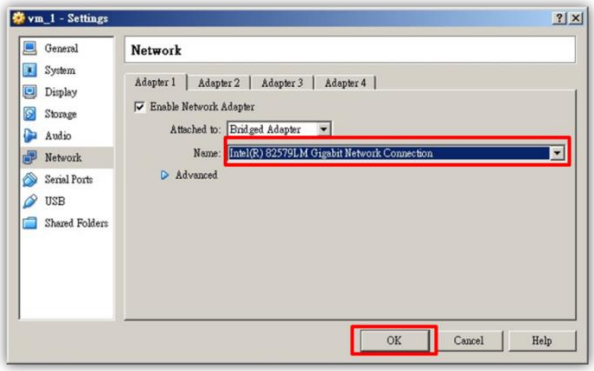
3. Locate and select ezMaster image, select the ***"Reinitialize the MAC address of all network cards"*** checkbox, then click on ***Import***.



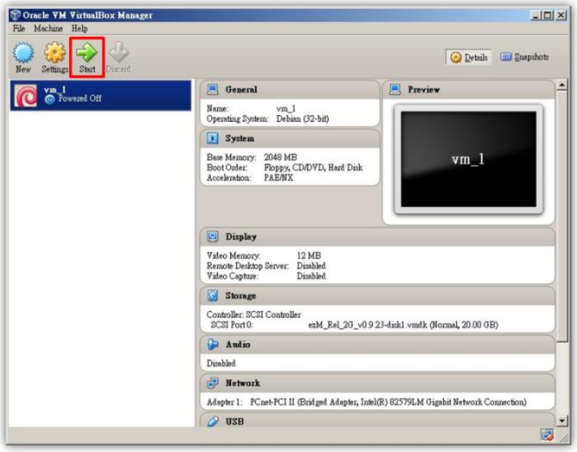
4. After importing the image, click on ***Network***.



5. From the drop-down box, select the network adapter that your computer uses to connect to the Internet (WAN). DO NOT select a Wireless LAN adapter or other virtual adapters. Click on ***OK*** to continue.

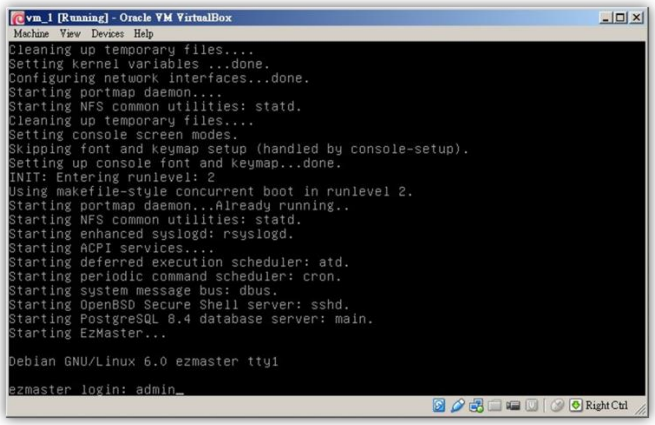


6. Click on the ***Start*** button to launch the ezMaster image.

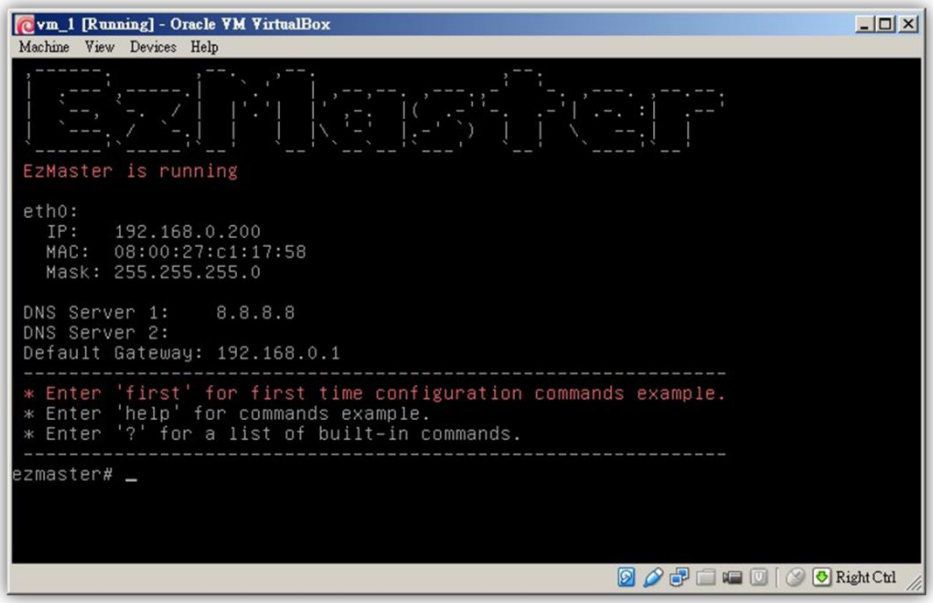


Setting up ezMaster Server

1. After launching the image, once the installation script finishes running, you will be prompted to enter login and password for ezMaster. For login enter ***admin***, for the password enter ***password***.



2. Once the ***ezmaster#*** command prompt appears, start entering network settings for your ezMaster server.
   (Tip: Use *Network Adapter Properties* to check the info of your network adapter.)



   ****network settings below are for reference example use.***

   a) Enter ezMaster *Server IP* and *Netmask*:
   config ip eth0 *10.0.92.70 255.255.255.0*
   (eg. LAN Adapter IP is *10.0.92.69* so an unused IP Address *10.0.92.70* is chosen to be used as ezMaster's server IP address)

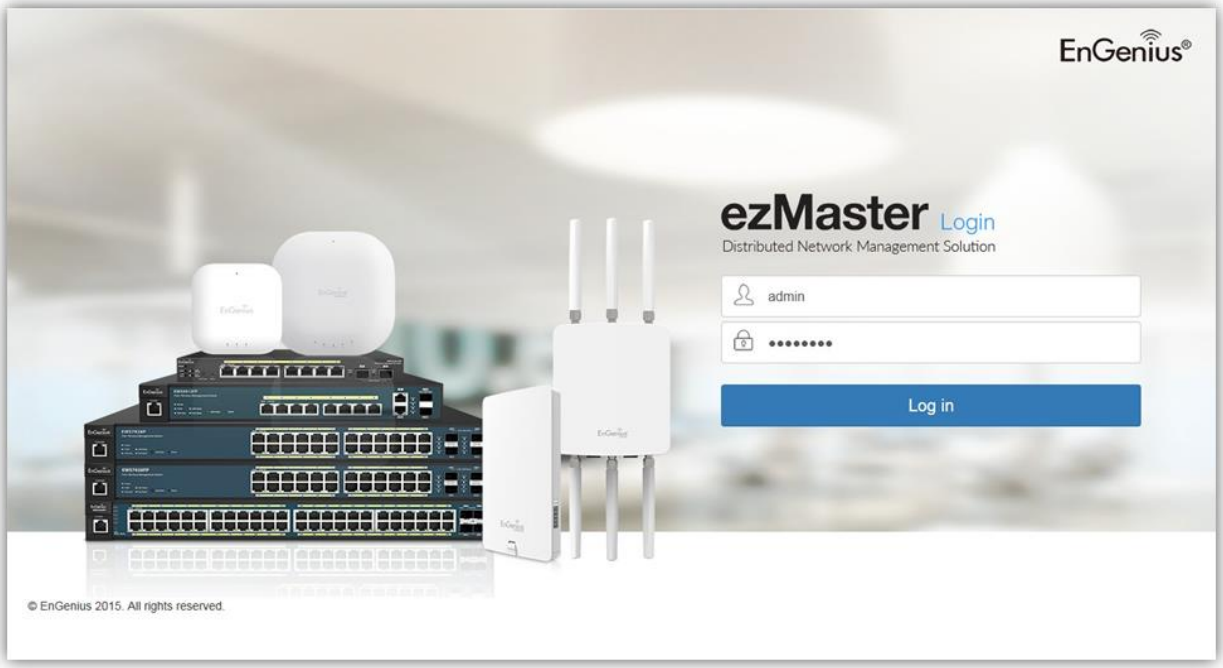
   b) Enter ezMaster Server gateway:
   config gateway *10.0.92.254*

   c) Enter ezMaster DNS Server:
   config dns *10.0.92.240*

You have completed installing ezMaster.

Logging into ezMaster

1. Open a web browser and type the IP address of the ezMaster server you've assigned.
2. Once the log in screen appears, enter the username (**admin**) and password (**password**) to log in.

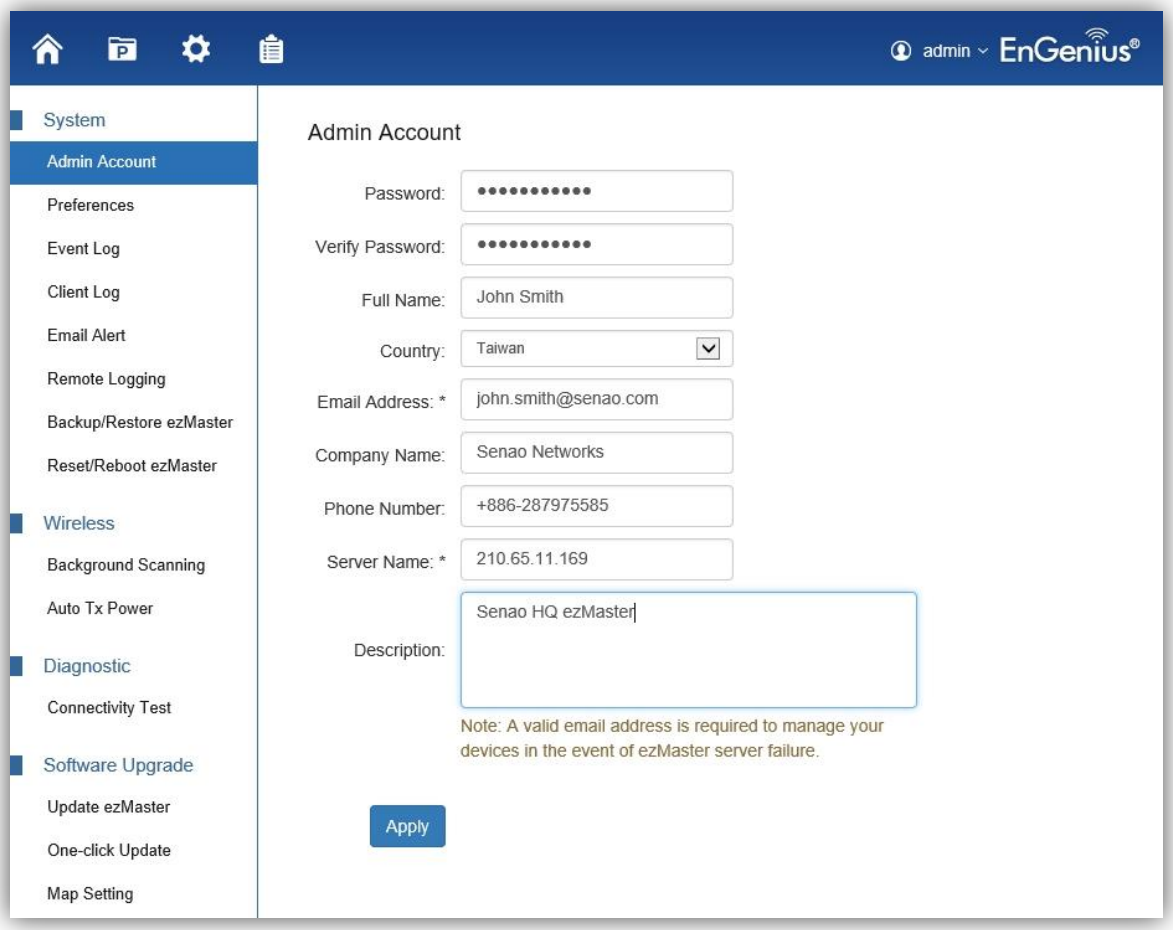


Registering ezMaster to ezRegistration Server

In order to manage remote device using ezMaster, you must first register ezMaster to the ezRegistration server. You may skip this section if you are managing only local devices or if you are manually redirecting each AP to ezMaster.

1. In the ezMaster user interface, click on the ***Global Settings*** menu.

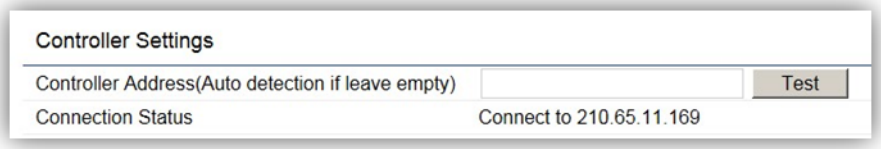
2. Under ***Admin Account***, fill in the fields and click ***Apply*** to register your ezMaster to the ezRegistration server.
   Take note that a valid email address is required for you to unregister your devices in the event of ezMaster server failure.



Getting Started

Before ezMaster is able to manage a Neutron device, the access point/switch must be running with the required firmware version. All Neutron devices will need to be running firmware version ***c1.8.x or later***.

With ezMaster, you'll be able to manage both local and remote access points. The table below lists the methods of how access points are managed.

AP Location	Details
Local	All local devices (in same subnet) will be automatically detected and ready for management in the ***"Pending Approval"*** list under ***Device Management > Device Config*** in each project. (Note: ezMaster does not need to be registered to the ezRegistration server if you are only managing local access points)
Remote	Register ezMaster to the ezRegistration server. Then "claim" your access points to add them to ezMaster's ***"Device Inventory"***. Devices successfully claimed will automatically be listed in the ***"Pending Approval"*** list under ***Device Management > Device Config*** in each project.
Remote	Manually assign the ezMaster server URL from the AP user interface (under ***Management > Controller Settings***). If configured successfully, the access point will connect directly the ezMaster and it will be automatically detected and ready for management in the ***"Pending Approval"*** list under ***Device Management > Device Config*** in each project. (Note: ezMaster does not need to be registered to the ezRegistration server if you are managing access points using this method). 

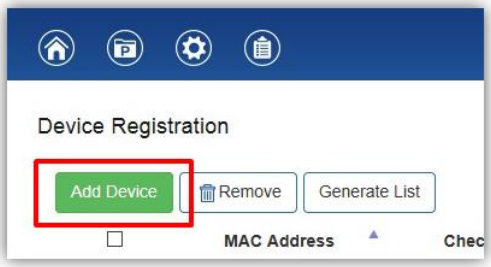
Tip: Offline provisioning is possible for remote devices by simply redirecting the device's IP Address to ezMaster or registering the device to ezMaster before installing these devices at the desired location.

Adding devices to ezMaster Device Inventory

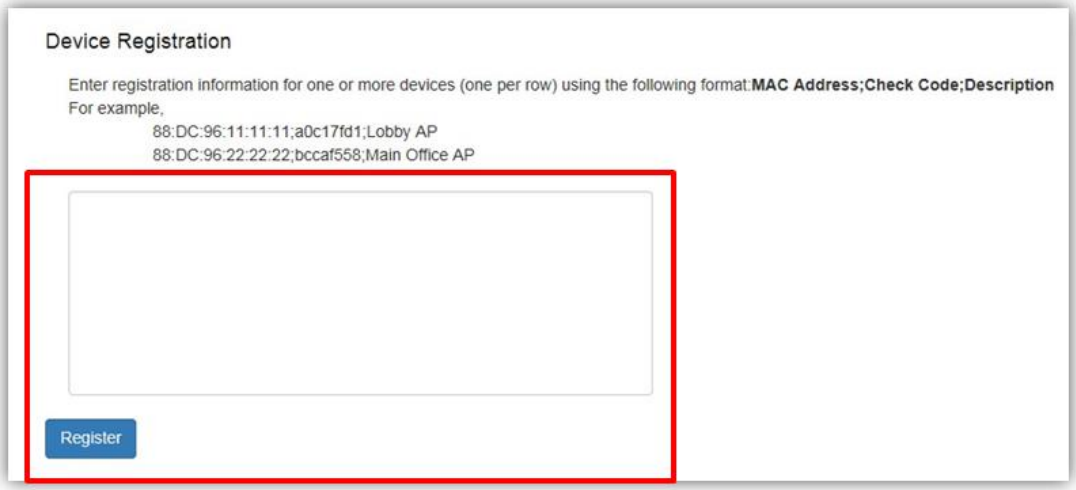
Before managing a remote AP/switch, you must first bind the AP to ezMaster's Device Inventory by 'registering' the device. Skip this section if you are managing only local devices or if you are manually redirecting each AP to ezMaster.

1. Once ezMaster has been registered with the ezRegistration server, you can start registering your APs and adding them to ezMaster's device inventory by clicking on the ***'Device Inventory'*** icon.

2. Next, click on the 'Add Device' button.



3. Enter the **MAC Address**, **Check Code** and **Description** of the device you want to register using a semi-colon (;) to separate each field. eg. ***MAC Address;Check Code;Description***
To register more than one device at the same time, enter the information of one device per row by pressing Enter. Click the ***"Register"*** button once you are done.



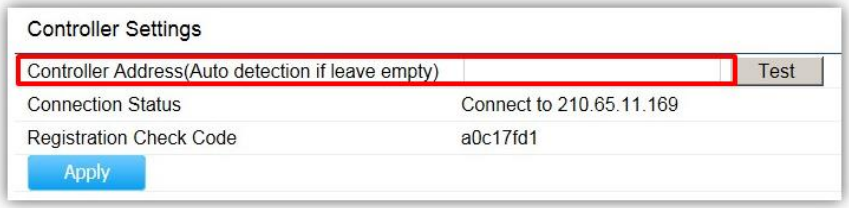
Note: *The 'check code' of the AP can be found on either the device label at the bottom of the AP. If not, access the AP's user interface and find it under the* ***"Management > Controller Settings"****. Contact your local dealer if you are having problems locating the check code.*

4. The message below will be displayed upon successfully claiming an AP. Click on ***"OK"*** to proceed.

5. The registered AP will be listed in your Device Inventory.

Manually redirecting AP to ezMaster

From the AP's web user interface, select 'Management'. Under Controller Settings, fill in the IP Address of the ezMaster server you wish to redirect to AP to. The 'Test' button can be used to test whether the AP can successfully connect with the ezMaster server. Click on 'Apply' to save your settings.



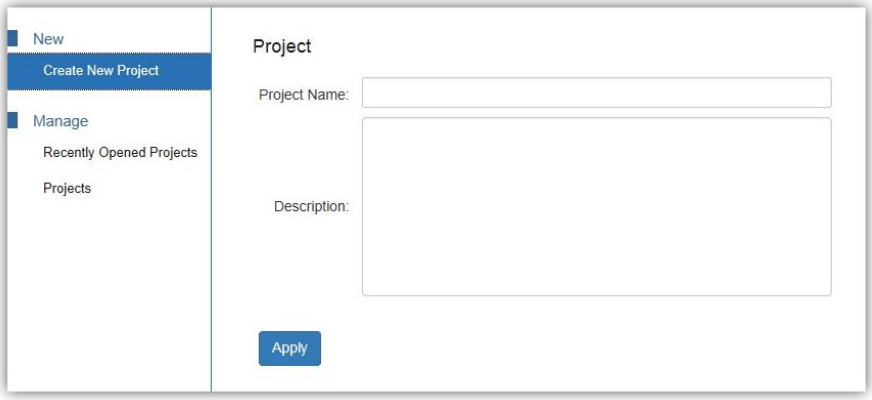
Managing devices using ezMaster

In order to start managing and monitoring Neutron devices, these devices must first be added to a project.

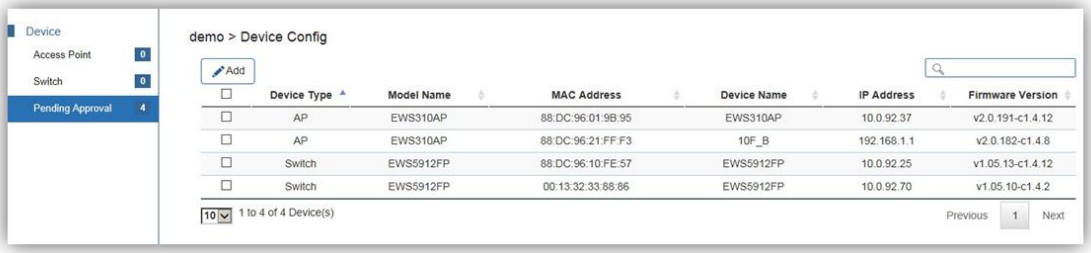
1. Make sure that your Neutron device is connected to a network with a DHCP server and can access the Internet.

2. Click on the ***"Project"*** icon to create a new project. A 'Project' is similar to a 'profile' which can be used to classify/represent different sites or floors of your deployment.

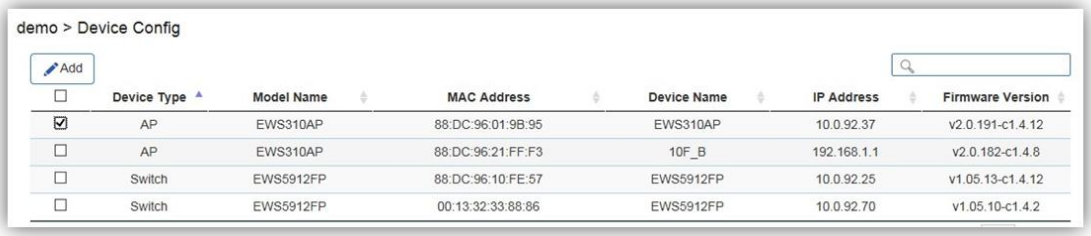
3. Click on ***"Create New Project"*** and enter a project name and description. Click on ***Apply*** when you are done.



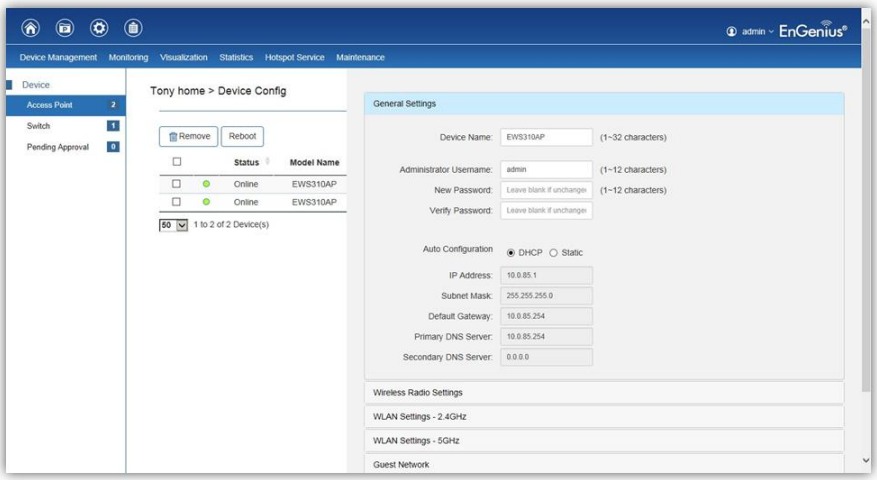
4. You'll be automatically redirected to the **'Pending Approval'** list after successfully creating a profile. The **'Pending Approval'** list will display a list of AP/switches in your local network (same network as ezMaster) and also remote AP/switches claimed by ezMaster.



5. Select the AP(s) you wish to add to your profile by selecting the checkbox and click on the ***"Add"*** button.



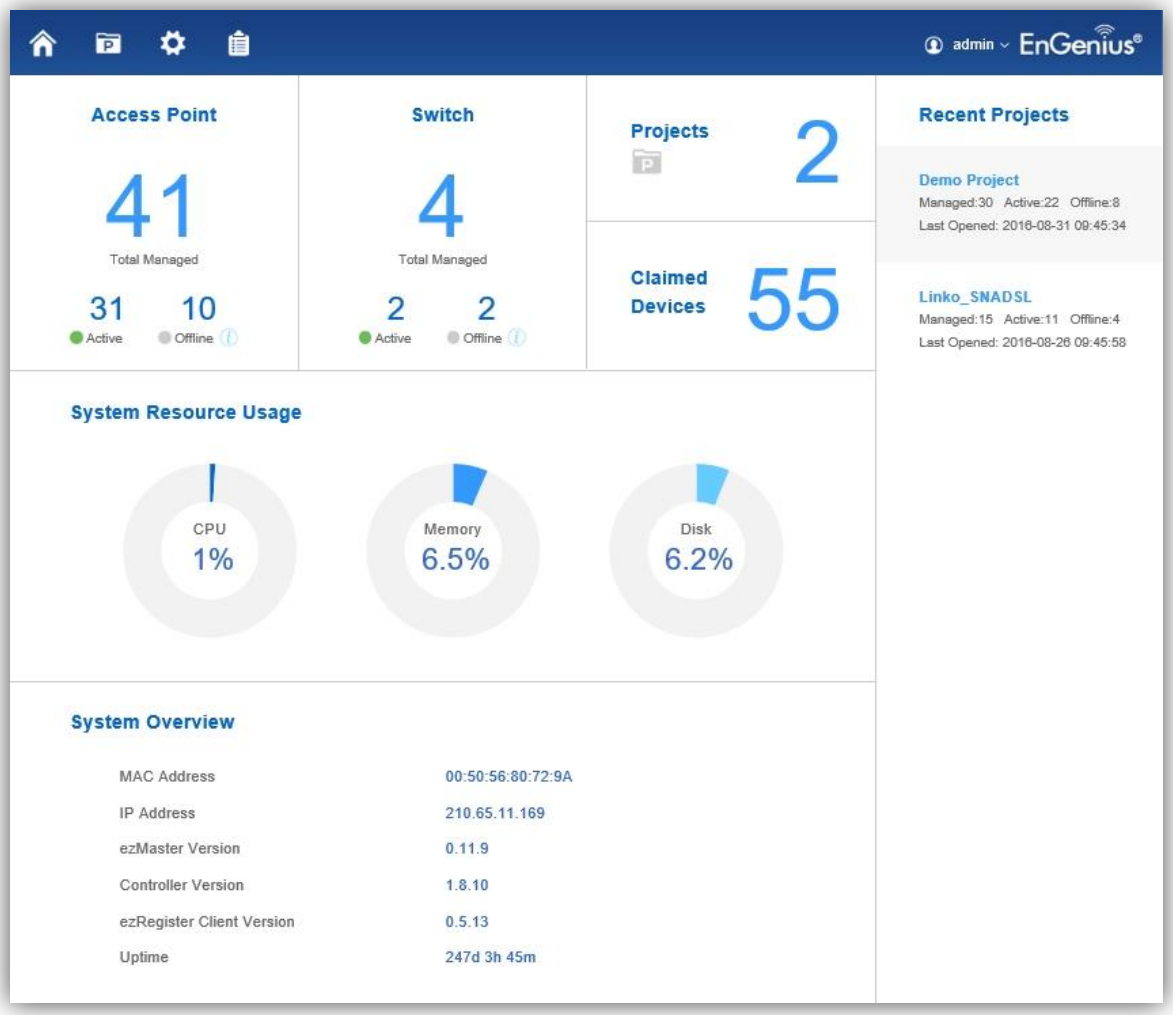
6. You'll be automatically redirected to the device page. Once the AP is online (green), to configure your AP, click on the ***'Device Name'*** link of your AP to bring up the configuration menu.



Note: In order to manage an EWS Switch, the Controller State of the EWS Switch must first be set to ***"Disabled"*** in the EWS switch web interface. A switch with Controller State **"Enabled"** will not be discovered by ezMaster.

Working with ezMaster

Main Dashboard

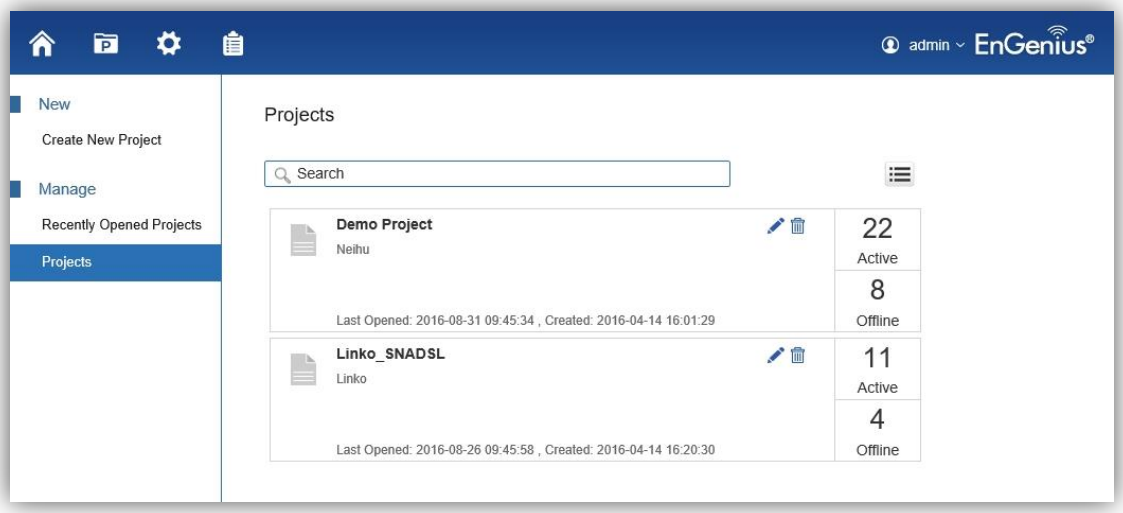


After logging in to the ezMaster web interface, the Dashboard is the first page that appears. The Dashboard provides a quick summary of the number of devices managed and ezMaster system information including system resource usage status, system information and software version.

The main menu on the upper left consist of 4 tabs:

- Home: Return to dashboard
- Project: Create/manage a project
- Global Settings: ezMaster related system settings
- Device Inventory: Allows you to claim remote devices you wish to manage

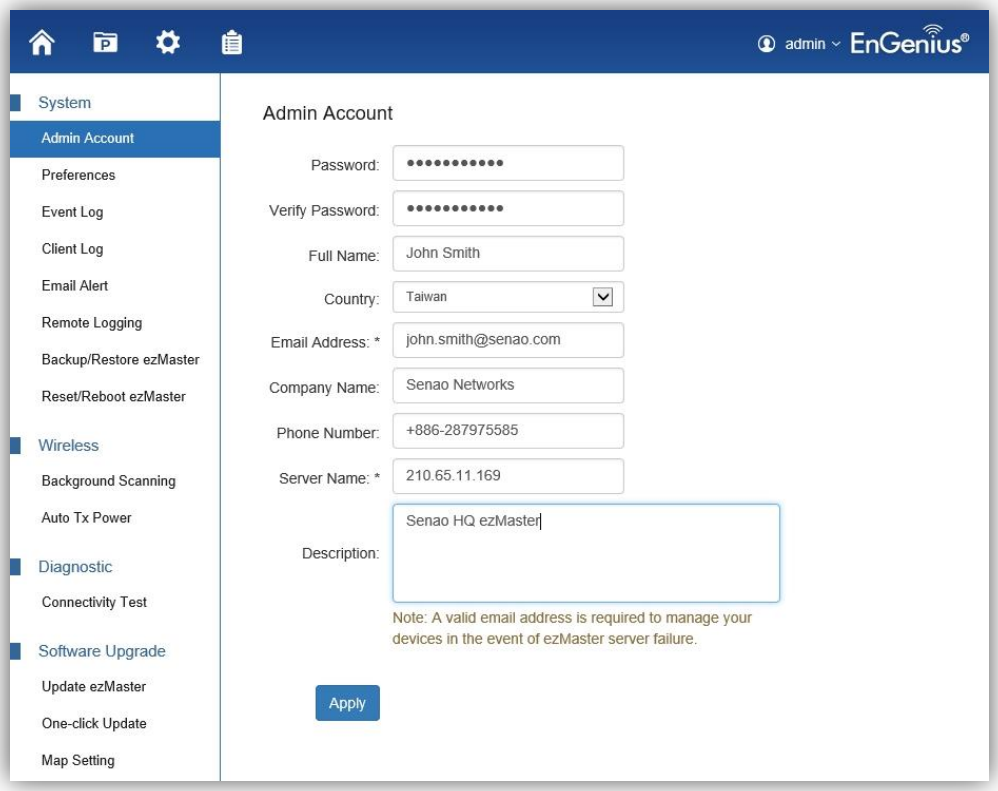
Projects



A ‘project’ is concept similar to a 'profile' which can be used to classify/represent different floors or sites of your deployment.

On this page, you'll be able to manage existing projects as well as create new projects.

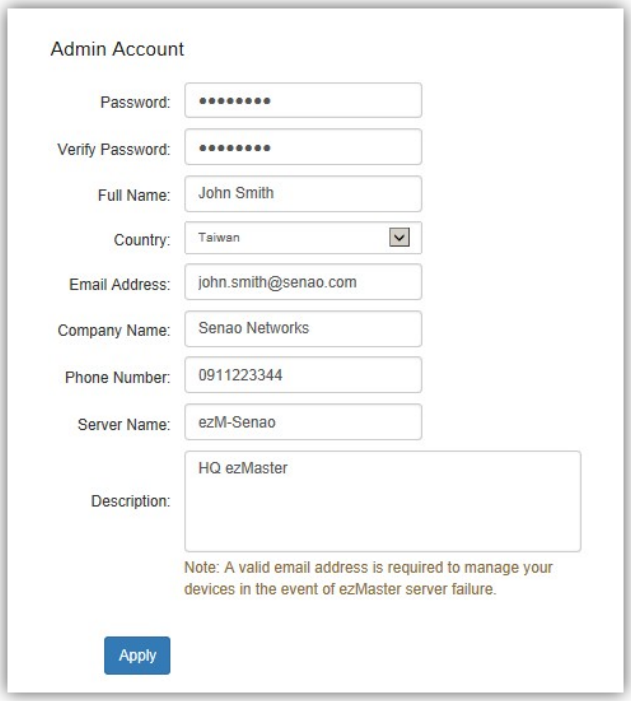
Global Settings



The page allows you set up global and general settings for ezMaster including administrator account settings, log related settings, backup/restore settings, connectivity tests, software upgrades.

System

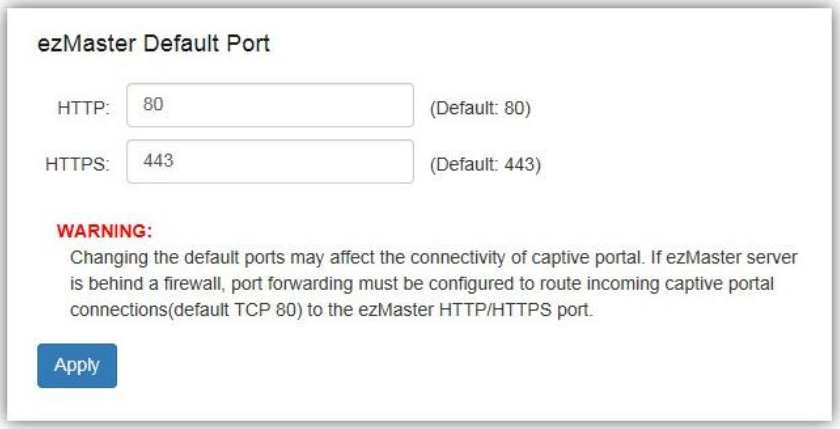
Admin Account



Use this page to register your ezMaster to the ezReg server. A valid email address is required for you to unregister your devices in the event of ezMaster server failure.

Also, on this page you can change the ezMaster login password. For security purposes, it is recommended to change the default password.

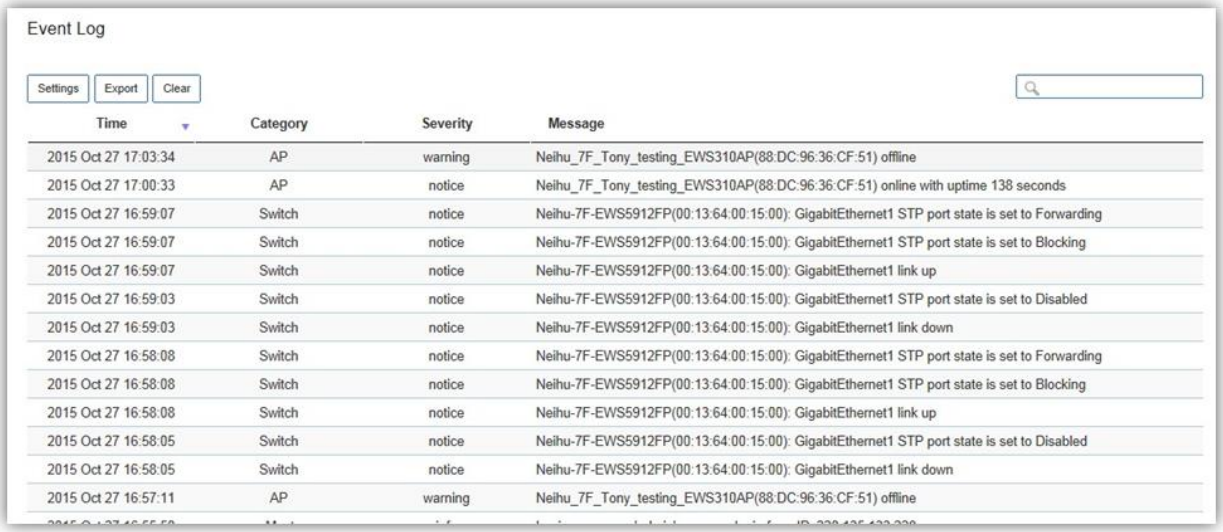
Preferences



By default, the ezMaster web server will operate on port 80 and 443. Users can change HTTP/HTTPS ports from their default assignments.

After modifying the default ports, be sure to check your firewall settings and make sure that incoming captive portal connections can be successfully routed to ezMaster's HTTP port.

Event Logs

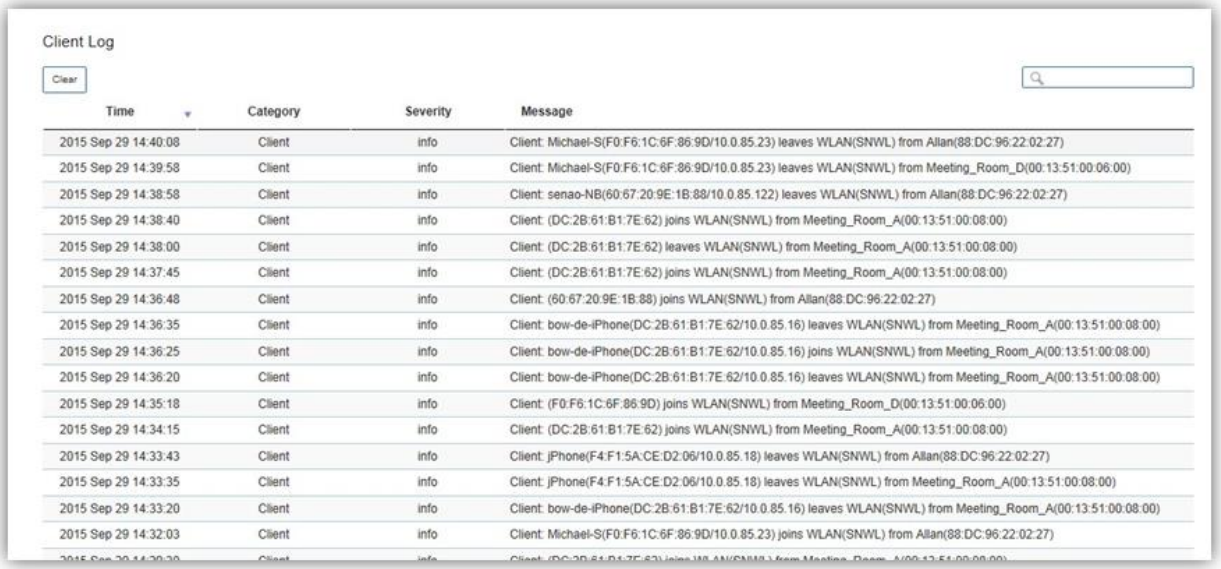


The Event Log is designed to monitor the operation of ezMaster by recording the event messages it generates during normal operation. These events may provide vital information about system activity that can help in the identification and solutions of system problems.

This page displays the most recent records. Log entries are listed in reverse chronological order (with the latest logs at the top of the list). Click a column header to sort the contents by that category.

Use the **Settings** button to choose which types of events and severity level you would like to display.
Use the **Export** button to export the event log to a file.
Use the **Clear** button to clear all log entries from ezMaster's database.

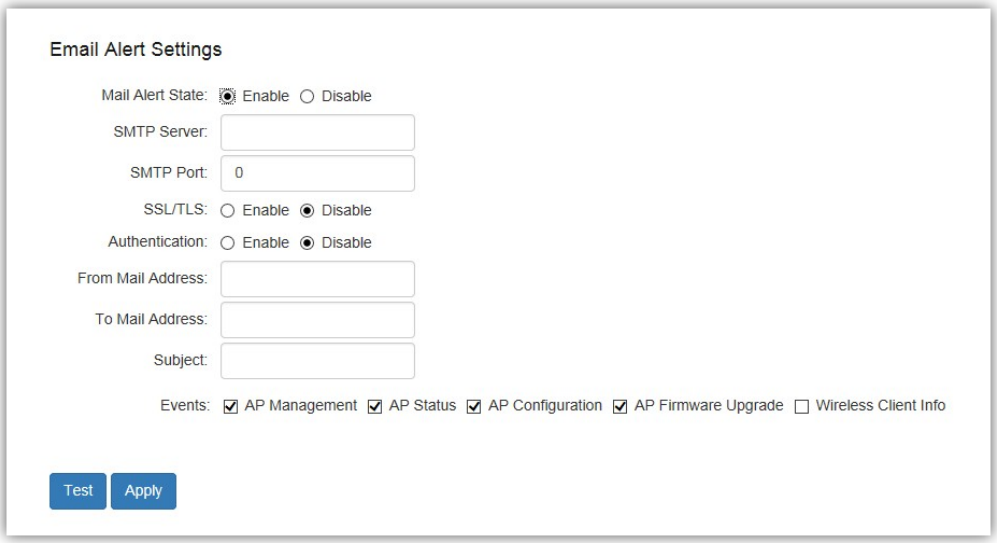
Client Log



The Client Log is used to monitor wireless client information and may be helpful in identifying client related system problems.

Use the **Export** button to export the client log to a file.
Use the **Clear** button to clear all client log entries from ezMaster's database.

Email Alert



If an event is detected, ezMaster will record it in the event log. ezMaster can also be configured to send email notifications upon detecting selected events.

Mail Alert State: Select whether to Enable/Disable email notification.

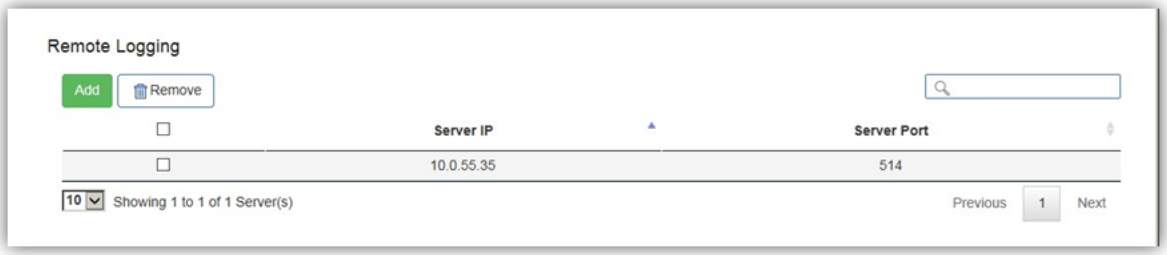
Mail Information Setting

- **SMTP Server**: Enter the name of the mail server.
- **SMTP Port**: Enter the SMTP port.
- **SSL/TSL**: Enable this option if your mail server uses SSL/TLS encryption.
- **Authentication**: Select this option to enable authentication.
    - **User Name**: Enter the username required by the mail server.
    - **Password**: Enter the password required by the mail server.
- **From Mail Address**: Enter the email address that will appear as the sender of the email alert.
- **To Mail Address**: Enter the email address which the ezMaster will send alarm messages to. You can only send alarm messages to a single email address.
- **Subject**: Enter the subject of the email notification.
- **Event**: Select the types of events which ezMaster will send an email notification.

Test: Used to verify that ezMaster can send email notifications using the SMTP settings you configured.

Apply: Click **Apply** to save settings.

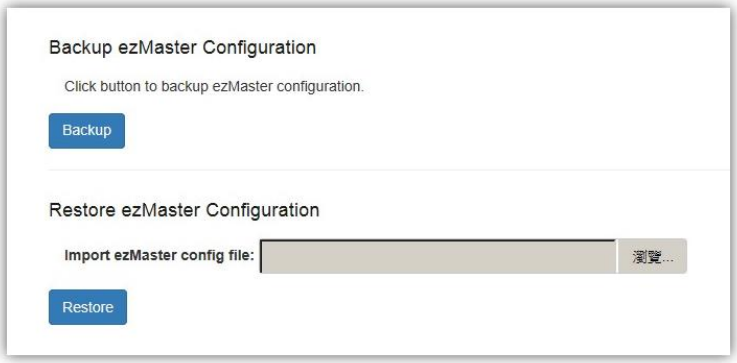
Remote Logging



The internal log of ezMaster has a fixed capacity; at a certain level, ezMaster will start deleting the oldest entries to make room for the newest. If you want a permanent record of the logs, you can set up a syslog

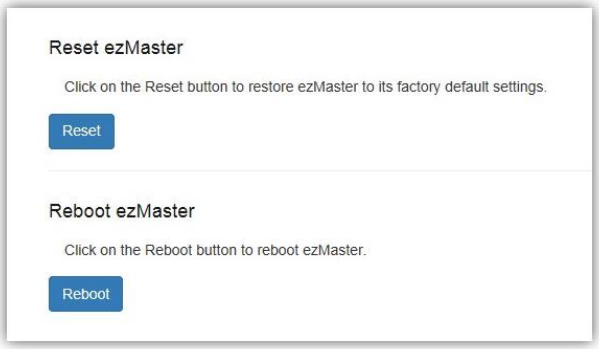
server to receive log contents from the ezMaster. Use this page to direct all logging to the syslog server. Click the **Add** button to create a new entry and define your syslog server.

Backup/Restore ezMaster



After you have finished setting and configuring your ezMaster, you may want to backup the full configuration. This configuration file can be used to restore your settings if for some reason you ezMaster server crashes. Use the **Backup** button to export your settings, and use the **Restore** button to upload your settings file.

Reset/Reboot ezMaster

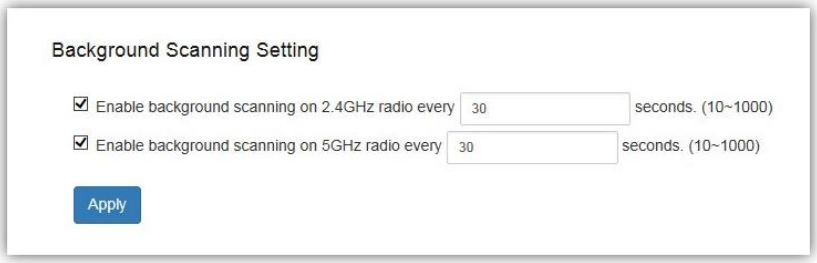


If for any reason you need to reset or reboot you ezMaster server, you may do so here.

Warning: Resetting ezMaster will erase all configurations made. Remember to backup your setting beforehand.

Wireless

Background Scanning



Using Background Scanning, ezMaster periodically samples RF activity of all Access Points including channel utilization and surrounding devices in all available channels. Background scanning is the basis of Auto Channel, Auto Tx Power and Rogue AP detection, and must be enabled for these features to operate. You may, if you prefer, disable it if you feel it's not helpful, or adjust the scanning frequency, if you want scans at greater or fewer intervals.

Note: For latency-sensitive applications such as VoIP, it is recommended to set the background scan interval to a higher value, e.g. 5 or 10 minutes. For regular application, the recommended value is 30 seconds. This value will also be directly related on how long it takes for the AP to scan for rogue devices.

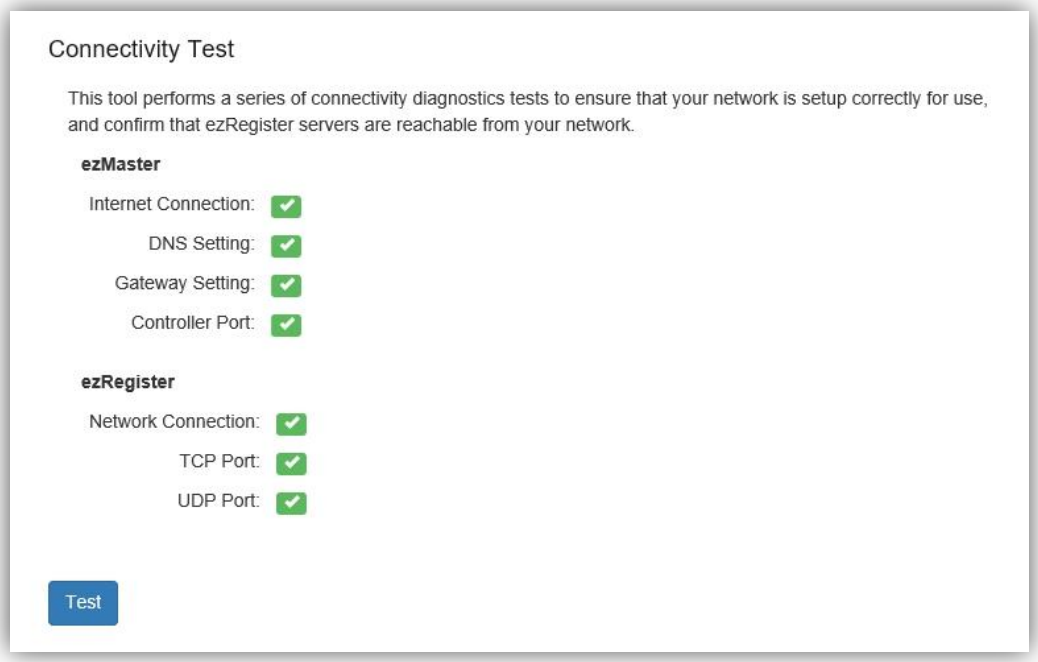
Auto Tx Power

Using the information collected by Background Scanning, APs can automatically adjust their transmit power to optimize coverage. When enabled, APs will optimize their transmit power based on the time interval configured for Background Scanning.

*Note: Background Scanning must be **enabled** and Tx Power of APs must be set to **Auto** (under Wireless Radio Settings) for this feature to operate.*

Diagnostic

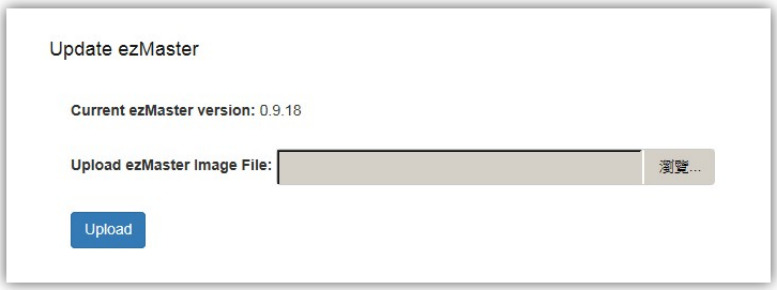
Connectivity Test



Connectivity Test is used to ensure that your network is setup correctly. Use the Test button to check your network connection.

Software Upgrade

Update ezMaster



Use this page to upgrade your ezMaster server to a later version.

Note: We recommend backing up ezMaster settings before performing a ezMaster server software update.

Warning: Upgrading ezMaster will temporarily disable device management. To minimize network disruption,we recommend performing the upgrade procedure at an off-peak time.

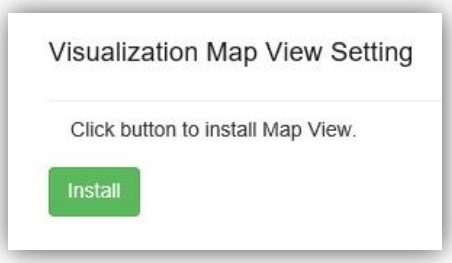
One-click Update

One-click Update allows users to check for AP software updates from the EnGenius server instead of manually downloading the firmware and upgrading your APs one by one. Click on the ***Check for Updates*** button for ezMaster to check for the latest firmware. Select the devices you wish to update and click on ***Update*** button to begin the updating process.

Note: Both ezMaster server and the browser on the PC must be able to access the Internet for this function to work. One Click Update might also not be available if you are using a proxy server for Internet connections.

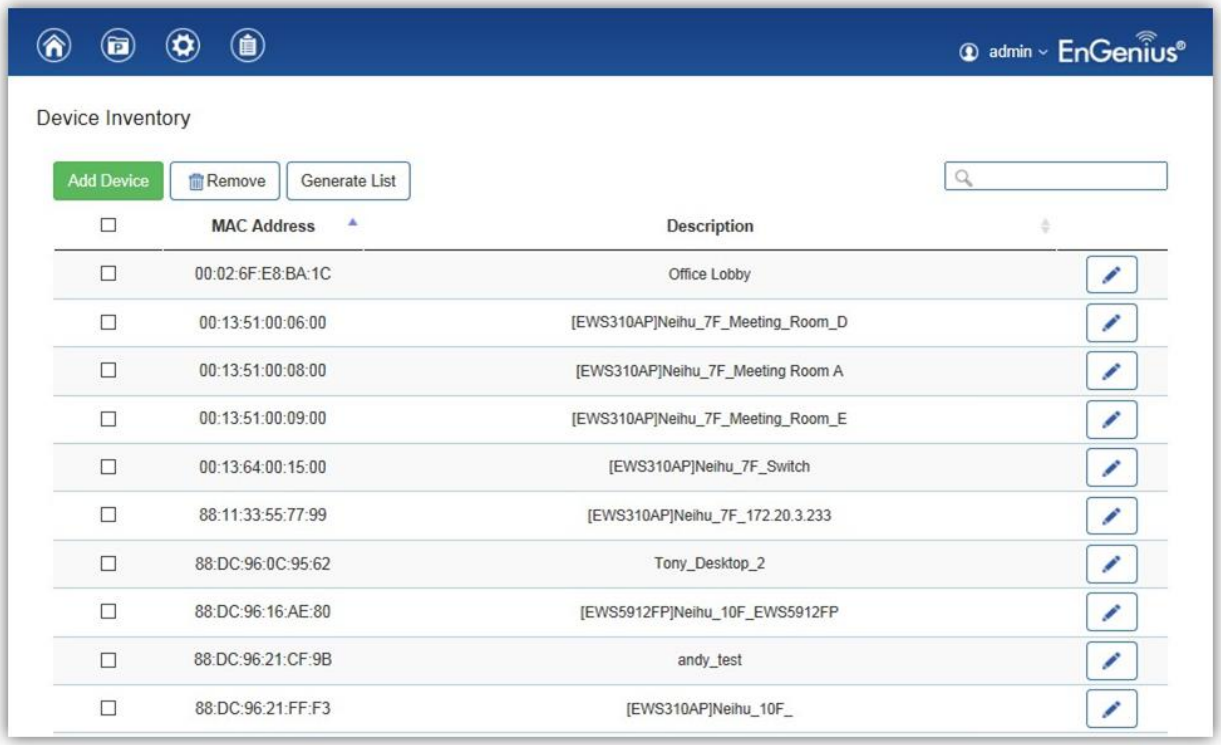
Warning: Upgrading APs will temporarily disconnect all associated clients from the network. To minimize network disruption, we recommend performing the upgrade procedure at an off-peak time.

Map View Settings



Before using the Map View feature available under the Visualization tab of each project, the Maps plugin must be installed from this page. After installing the Map plugin, use this page to check for newer maps from the server or uninstall the Maps plugin.

Device Inventory



In order to manage devices which are in a different network from ezMaster, you must first register these devices into ezMaster's device inventory. Once added to your inventory, you will be able to manage these devices from your projects.

On this page, you can register/unregister devices from your ezMaster.

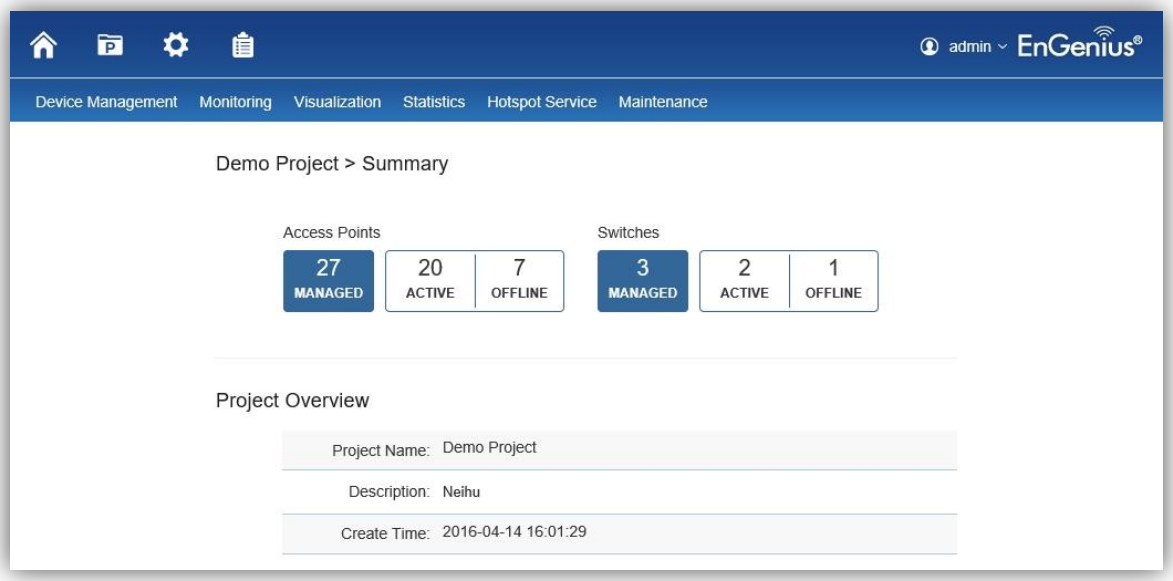
Note: Local devices (devices in the same network as ezMaster) can be managed without registering to ezMaster inventory and will appear automatically under the Pending Approval list under each project.

Working with Projects

A ‘project’ is concept similar to a 'profile' which can be used to classify/represent different floors or sites of your deployment.

Device Management

Summary



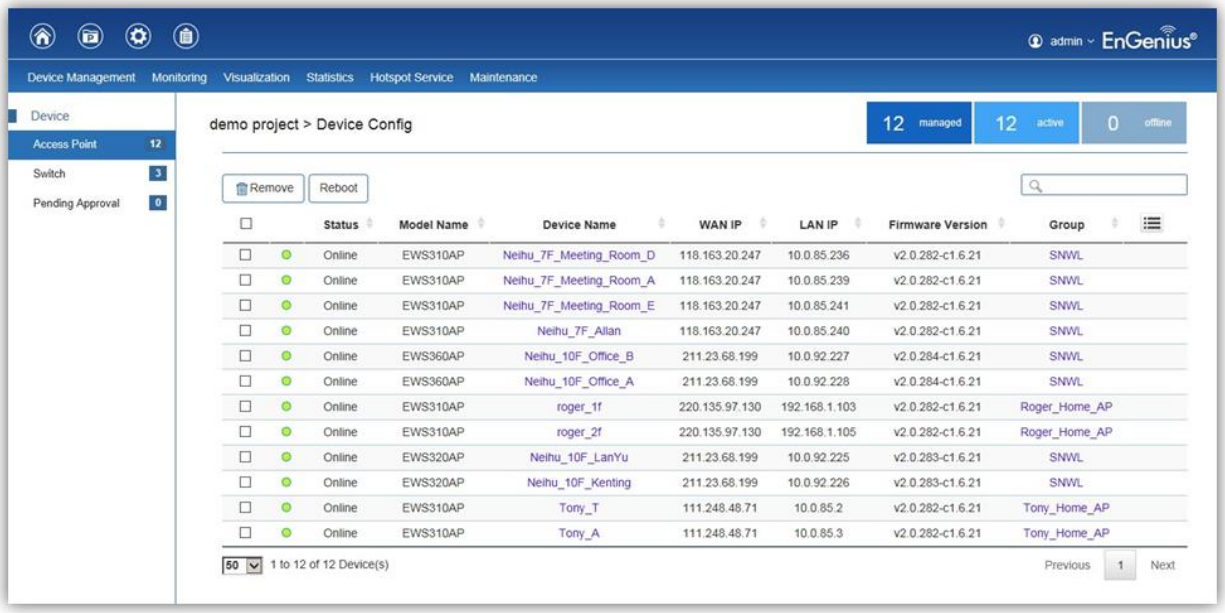
The Summary page provides a quick overview of the selected project.

Device Config

This page displays the status of all devices that are currently being managed by the selected project. From the menu on the left, you can select whether to display the list of managed APs or switches, and also display a list of devices that are currently pending approval.

Use the *Pending Approval* page to add new devices to your project.

Access Point



Dashboard
The Dashboard on the upper right shows the current number of APs that is being managed by the selected project.

Remove
The Remove button removes selected Access Point(s) from the project. Access Points removed will be automatically set to standalone mode with all settings restored to their factory default settings, and will appear in the Pending Approval list.

Reboot
The Reboot button reboots the selected Access Point(s).

Search Bar
Use the Search Bar to search the list of managed Access Points using the following criteria: Status, model name, MAC Address, Device name, IP address, Firmware Version, Group.

Status
This indicates the current status of the managed Access Point.

Status	Explanation
Online	AP is connected and managed by ezMaster.
Provisioning	AP is currently in the process of connecting to ezMaster.
Applying Change	AP is currently applying system changes.
Connecting	AP is currently connecting to ezMaster.
Offline	AP is currently offline.
Resetting	AP is resetting.
Firmware Upgrading	AP is currently undergoing firmware upgrade process.
Invalid IP	1. Unable to obtain IP address from DHCP server. 2. When using Static IP, the subnet of managed AP's IP address is incorrect.
Incompatible Version	AP firmware is not compatible with ezMaster.
Checking Certificate	ezMaster is checking the SSL Certificate of the AP.

Model Name
Shows the model name of the managed Access Point.

MAC Address
Shows the MAC address of the managed Access Point.

Device Name
Displays the device name of the managed Access Point.

- When the AP is not configured to a Group, click on this field and you'll be redirected to the configuration page where you can configure AP settings such as device name, IP Address, Wireless Radio settings.
- When the AP is configured to a Group, click on this field to configure settings for individual Access Points by overriding the cluster settings.

WAN IP
Shows the WAN IP address of the managed Access Point.

LAN IP
Shows the LAN IP address of the managed Access Point.

SKU
Shows the SKU of the managed Access Point.

Firmware Version
Shows the firmware version of the managed Access Point.

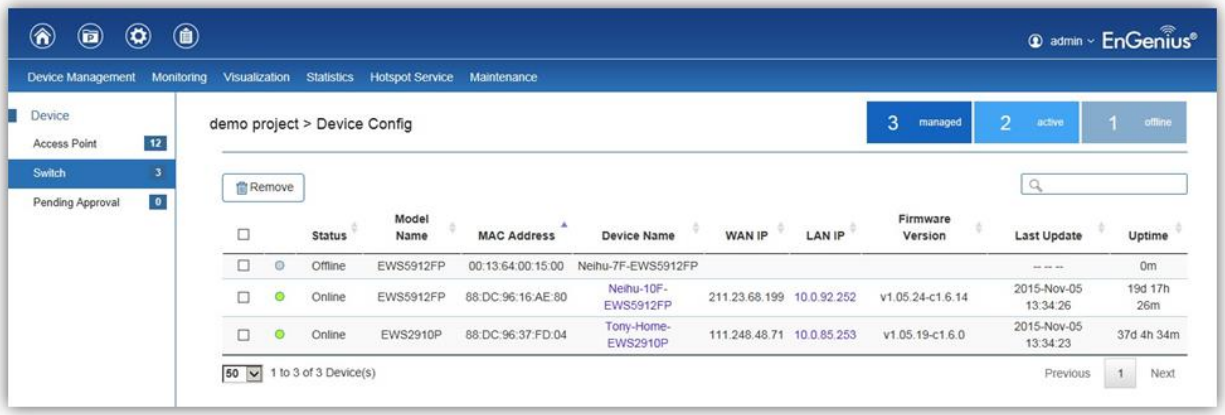
Last Update
Display the time the Access Point was last detected and the information was last updated.

Group
Displays the Group the Access Point is currently assigned to.

Operating Channel
Displays the channel/band that the AP is operating on.

Column Filter
Shows or hides fields in the Access Point list.

Switch

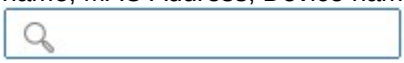


Dashboard
The Dashboard on the upper right shows the current number of EWS Switches that are being managed by the selected project.

Remove
The Remove button removes selected EWS Switches from the project.

Reboot
The Reboot button reboots the selected EWS Switches.

Search Bar
Use the Search Bar to search the list of managed EWS Switches using the following criteria: Status, model name, MAC Address, Device name, IP address, Firmware Version.



Status
This indicates the current status of the managed EWS Switch.

Status	Explanation
Online	EWS Switch is connected and managed by ezMaster.
Provisioning	EWS Switch is currently in the process of connecting to ezMaster.
Applying Change	EWS Switch is currently applying system changes.
Connecting	EWS Switch is currently connecting to ezMaster.
Offline	EWS Switch is currently offline.
Resetting	EWS Switch is resetting.
Firmware Upgrading	EWS Switch is currently undergoing firmware upgrade process.
Invalid IP	1. Unable to obtain IP address from DHCP server. 2. When using Static IP, the subnet of managed device's IP address is incorrect.
Incompatible Version	EWS Switch firmware is not compatible with ezMaster.
Checking Certificate	ezMaster is checking the SSL Certificate of the EWS Switch.

Model Name
Shows the model name of the managed EWS Switch.

MAC Address
Shows the MAC address of the managed EWS Switch.

Device Name
Displays the device name of the managed EWS Switch. Click on the link to modify the device name, configure port and PoE settings.

WAN IP
Shows the WAN IP address of the managed EWS Switch.

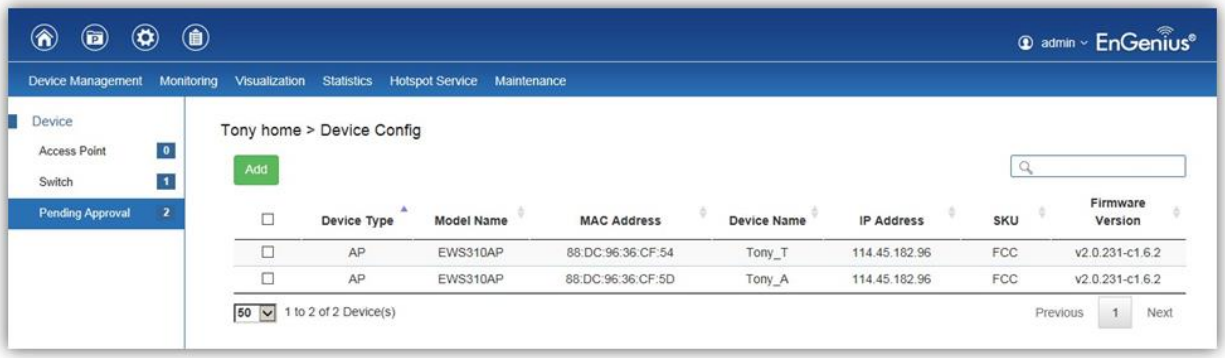
LAN IP
Shows the LAN IP address of the managed EWS Switch.

Firmware Version
Shows the firmware version of the managed EWS Switch.

Last Update
Display the time the EWS Switch was last detected and the information was last updated.

Uptime:
Displays the number of days, hours, and minutes since the EWS Switch last restarted.

Pending Approval



Add
Use the Add button to add selected devices into your project.

Search Bar
Use the Search Bar to search the list of devices using the following criteria: device type, model name, MAC address, device name, IP address, SKU, firmware version.

Device Type
Indicates whether the device pending approval is an AP or EWS Switch.

Model Name
Shows the model name of the device pending approval.

MAC Address
Shows the MAC address of the device pending approval.

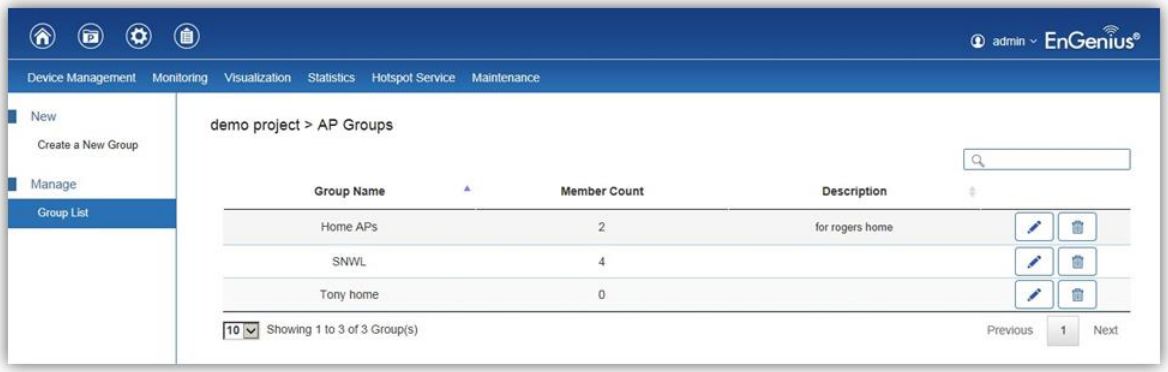
Device Name
Displays the device name of the device pending approval.

IP Address
Shows the IP address of the device pending approval.

SKU
Shows the SKU of the device pending approval.

Firmware Version
Shows the firmware version of the device pending approval.

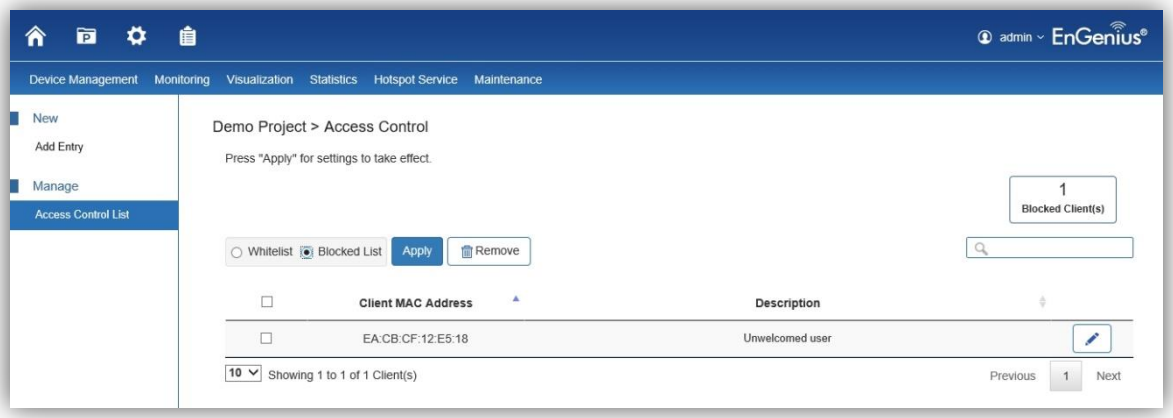
AP Groups



AP Groups can be used to define configuration options and applying these settings to multiple APs at once without having to modify each AP's settings individually. If your wireless network covers a large physical environment and you want to provide wireless services with different settings and policies to different areas of your environment, you can use AP Groups to do this instead of having to modify the settings of each AP individually. For example, if your wireless network covers two floors and you need to provide wireless access to visitors on the 1st Floor, you can simply setup two different AP Groups with different settings and policies to suit your application.

Overwriting Group Settings
Group settings can be overridden by individual AP settings. For example, if you want to set the transmit power to a lower setting for only a few specific APs, under the Device Config screen click on the Device Name field of the Access Point (which is already in a group) you wish to configure and you will be directed to a screen where you can configure override settings for the selected Access Point.

Access Control



This page displays the list of wireless clients that have been previously blocked from your network (using the Ban function from the *Monitoring* > *Active Clients*) as well as Whitelisted clients. If for any reason, you need to block a client device from your network or add a whitelist client to your network, you can do so from this page by creating a new rule and entering the client's MAC address.

Blocking a Specific Client Device
Follow the steps below to permanently block a specific client device from the network.

1. Click the **Add** button to create a new rule.
2. Enter the *MAC Address* and *Description* of the wireless client device you wish to block.
3. Click on **Apply** to create a new rule.
4. After being redirected back to the **Access Control List** page, make sure to select **Blocked List**.
5. Click on the **Apply** button on the upper right (beside the Remove button) to save settings made on this page.

Unblocking a Previously Blocked Client Device

1. In the **Access Control List** page, select **Blocked List** and click on the **Remove** button on the client device you wish to unblock.
2. Click on the **Apply** button to save settings made on this page.

Adding a Client Device to the Whitelist

Follow the steps below to add a client device to the whitelist.

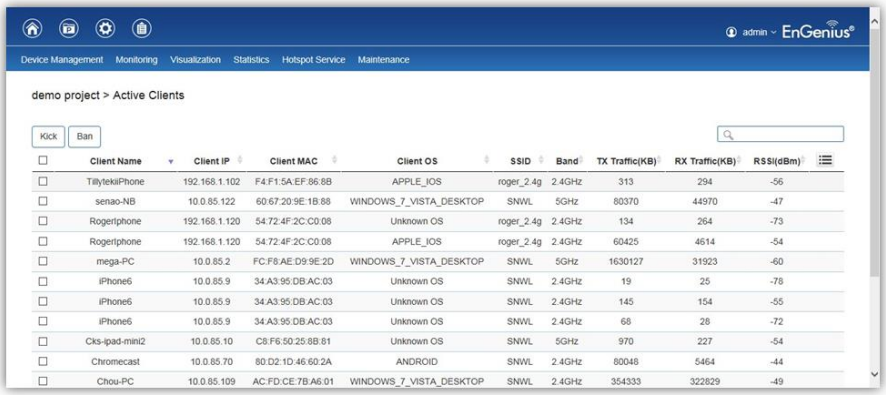
1. Click the **Add** button to create a new rule.
2. Enter the *MAC Address* and *Description* of the wireless client device you wish to add to the whitelist.
3. Click on **Apply** to create a new rule.
4. After being redirected back to the **Access Control List** page, make sure to select **Whitelist**.
5. Click on the **Apply** button on the upper right (beside the Remove button) to save settings made on this page.

Removing a Client Device from the Whitelist

1. In the **Access Control List** page, select **Whitelist** and click on the **Remove** button on the client device you wish to remove.
2. Click on the **Apply** button to save settings made on this page.

Monitoring

Active Clients



From here, you can view information, temporarily disconnect and permanently block the wireless clients that are associated with the managed Access Points. ezMaster is able to identify client devices by their Operating System, device type and host name, if available. If there are multiple Access Points in your project, use the search bar to find an Access Point by its name.

Kick Client
Use this function to temporarily disconnect a wireless client from the network. The disconnected client can simply reconnect manually if they wish to.

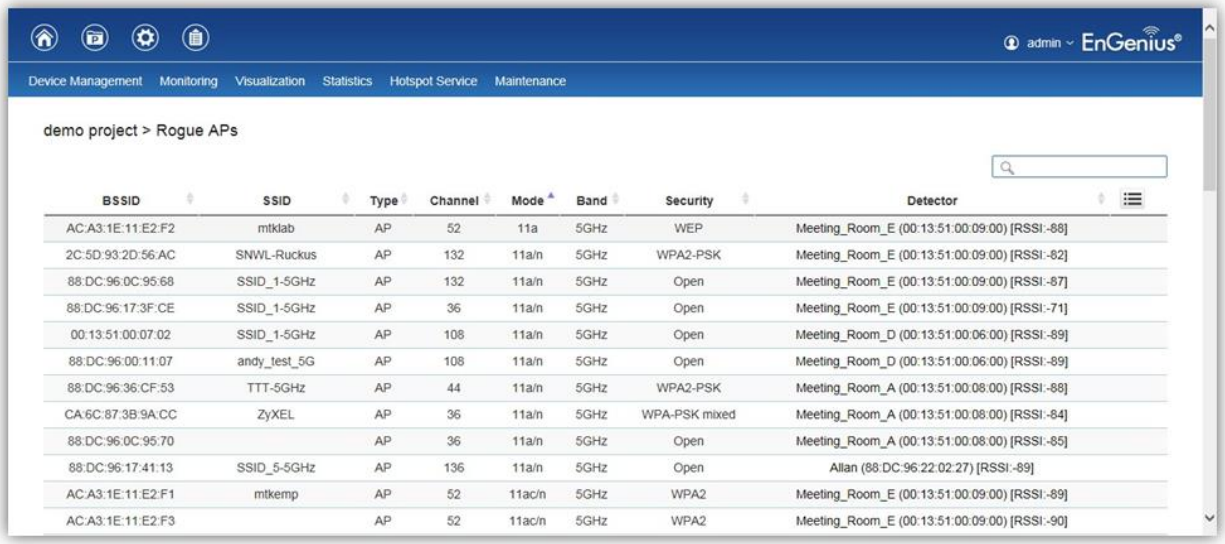
Ban Client
Use this function to permanently block a wireless client from the network. Go to ***Device Management > Access Control*** to unblock the wireless client.

Search Bar
Use the Search Bar to search for connected wireless clients using the following criteria: Client Name, Client IP, Client MAC Address, Client OS, AP Device Name, AP MAC Address, Model Name, SSID, Band.

Client Name	Displays the name of the wireless client connected to the Access Point.
Client IP	Displays the IP address of the wireless client connected to the Access Point.
Client MAC	Displays the MAC address of the wireless client connected to the Access Point.
Client OS	Displays the type of operating system the wireless client connected to the Access Point is running on.
AP Device Name	Displays the name of the Access Point which the client is connected to.
BSSID	Displays the BSSID of the Access Point which the client is connected to.
Model Name	Displays the model name of the Access Point which the client is connected to
SSID	Displays the SSID of the Access Point which the client is connected to.
AP MAC	Displays the MAC address of the Access Point which the client is connected to.
Band	Displays whether the wireless client is connected to the 2.4GHz or 5GHz radio.
TX Traffic (KB)	Displays the total traffic transmitted to the Wireless Client.
RX Traffic (KB)	Displays the total traffic received from the Wireless Client.
RSSI (dBm)	Displays the received signal strength indicator in terms of dBm.

Column Filter
Shows or hides fields in the Active Clients list.

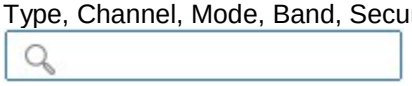
Rogue AP Detection



BSSID	SSID	Type	Channel	Mode	Band	Security	Detector
AC:A3:1E:11:E2:F2	mtklab	AP	52	11a	5GHz	WEP	Meeting_Room_E (00:13:51:00:09:00) [RSSI:-88]
2C:5D:93:2D:56:AC	SNWL-Ruckus	AP	132	11a/n	5GHz	WPA2-PSK	Meeting_Room_E (00:13:51:00:09:00) [RSSI:-82]
88:DC:96:0C:95:68	SSID_1-5GHz	AP	132	11a/n	5GHz	Open	Meeting_Room_E (00:13:51:00:09:00) [RSSI:-87]
88:DC:96:17:3F:CE	SSID_1-5GHz	AP	36	11a/n	5GHz	Open	Meeting_Room_E (00:13:51:00:09:00) [RSSI:-71]
00:13:51:00:07:02	SSID_1-5GHz	AP	108	11a/n	5GHz	Open	Meeting_Room_D (00:13:51:00:06:00) [RSSI:-89]
88:DC:96:00:11:07	andy_test_5G	AP	108	11a/n	5GHz	Open	Meeting_Room_D (00:13:51:00:06:00) [RSSI:-89]
88:DC:96:36:CF:53	TTT-5GHz	AP	44	11a/n	5GHz	WPA2-PSK	Meeting_Room_A (00:13:51:00:08:00) [RSSI:-88]
CA:6C:87:3B:9A:CC	ZyXEL	AP	36	11a/n	5GHz	WPA-PSK mixed	Meeting_Room_A (00:13:51:00:08:00) [RSSI:-84]
88:DC:96:0C:95:70		AP	36	11a/n	5GHz	Open	Meeting_Room_A (00:13:51:00:08:00) [RSSI:-85]
88:DC:96:17:41:13	SSID_5-5GHz	AP	136	11a/n	5GHz	Open	Allan (88:DC:96:22:02:27) [RSSI:-89]
AC:A3:1E:11:E2:F1	mtkemp	AP	52	11ac/n	5GHz	WPA2	Meeting_Room_E (00:13:51:00:09:00) [RSSI:-89]
AC:A3:1E:11:E2:F3		AP	52	11ac/n	5GHz	WPA2	Meeting_Room_E (00:13:51:00:09:00) [RSSI:-90]

Rogue Access Points refer to those unauthorized and often unmanaged APs attached to an existing wired network which could bring harm to the network or may be used to deliberately gain access to confidential company information. With ***Background Scanning*** enabled, the Rogue AP Detection feature can be used to periodically scan 2.4 GHz and 5 GHz frequency bands to identify rogue wireless Access Points not managed by the ezMaster.

Search Bar
Use the Search Bar to search for Rogue Access Points detected using the following criteria: BSSID, SSID, Type, Channel, Mode, Band, Security, Detector.

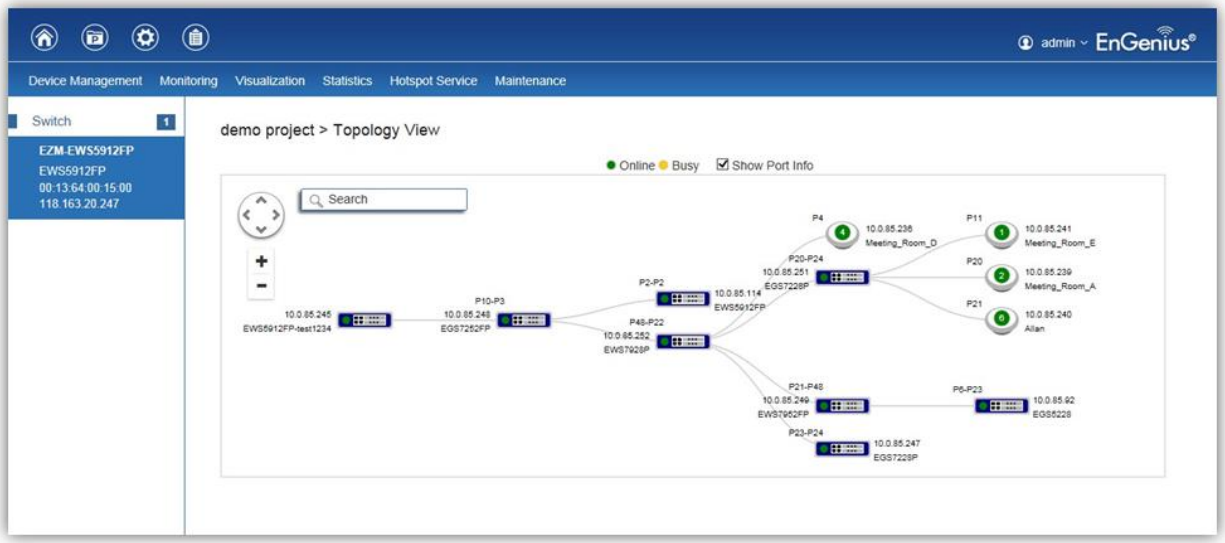


BSSID	Displays the BSSID of the rogue device detected.
SSID	Displays the SSID of the rogue device detected.
Type	Displays the type of the rogue device detected.
Channel	Displays the channel of the rogue device detected.
Mode	Displays the wireless mode of the rogue device detected.
Band	Displays the band of the rogue device detected.
Security	Displays the encryption method of the rogue device detected.
Detector	Displays the name and MAC address of the managed AP which detected the rogue device.

Column Filter
Shows or hides fields in the list.

Visualization

Topology View



If you have an EWS Switch deployed in your network, you will be able to see a visual view of the topology of all supported devices in the network. The Topology View feature will automatically maps your network deployment and displays the device relationships across your network infrastructure. An essential feature for troubleshooting network issues that would otherwise require manual mapping, overlay monitoring software, or manually keeping track of MAC address tables.

Use the directional pad and the plus or minus buttons to navigate your view of the network. You can also search for Access Points/EWS Switches in the network via their IP or MAC address. Check the Show Port Info box to show whether you wish the search query to show port information.

AP Status	Description
Online	The managed device is currently online.
Offline	The managed device is currently offline.
Busy	The managed device is currently applying new configuration settings.

Navigating Tips

Use  to scroll up, down, left, or right.

Use  to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

Mouse over a device to show information about the device.

Left click on the Switch bring up a menu where you can redirect to switch or collapse topology tree.

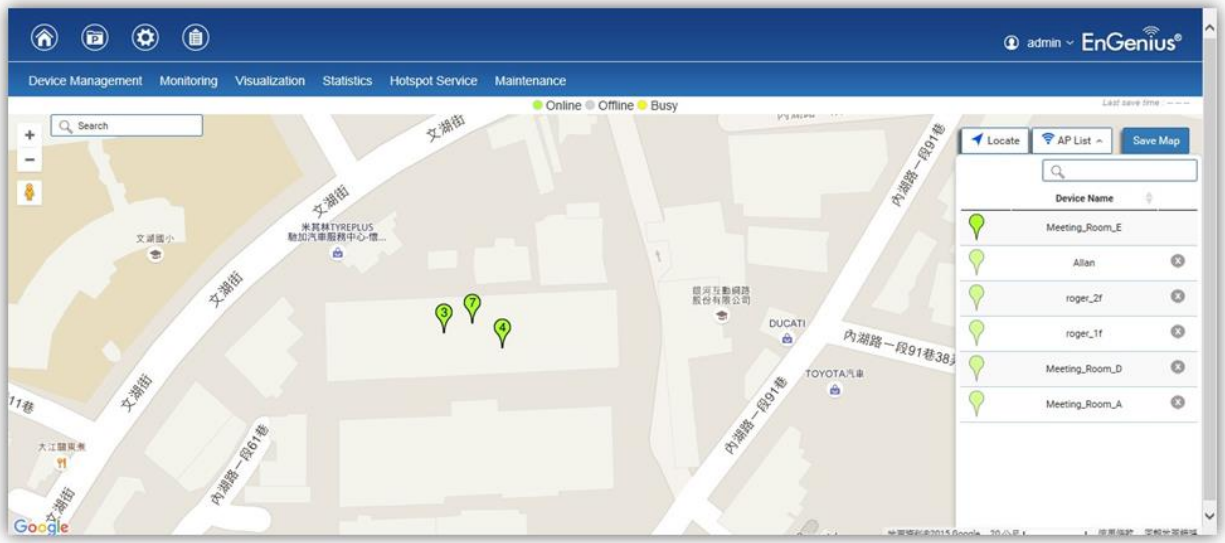
Left click on the Access Point to bring up a menu where you can remove AP from management list, reboot AP, or redirect to the Active Clients page.

You can search for a device using the IP Address or MAC address.

Click on ☑ Show Port Info to show or hide port information.

Note: ezMaster can only generate topologies when there is an EnGenius EWS Series Switch in the network. EnGenius EGS L2 Series and EGS Smart Series v2 models can be displayed in the topology if connected under a network with an EWS Switch. Non-EnGenius switches will be marked as “Uncontrollable LAN Switches” in the generated topology.

Map View



From here, you can view a geographical representation of Access Points in the network. Click on *AP List* to display the list of Access Points managed by the selected project then simply drag-and-drop the AP marker to the desired location on the map.

AP Status	Description
Online	The managed AP is currently online.
Offline	The managed AP is currently offline.
Busy	The managed AP is currently applying new configuration settings.

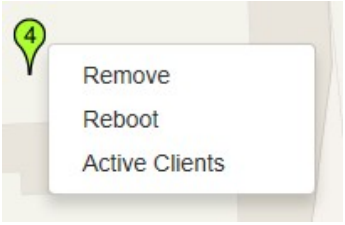
Navigating Tips

Use  to scroll up, down, left, or right.

Use the slider bar to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

Use the **Search box** to search for locations by typing an address or the name of a landmark.

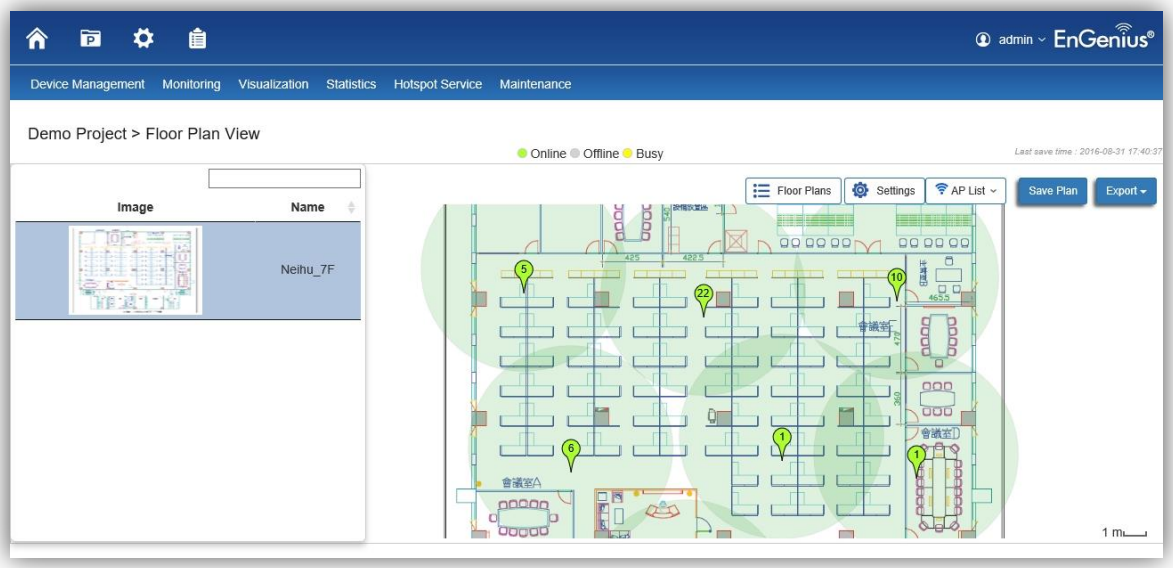
Use the **Locate** button to pinpoint the map to your current location. Note that the location provided is calculated based on your IP address and results might be inaccurate.



Left click on the Access Point marker to bring up a menu where you can remove AP from management list, reboot AP, or redirect to the Active Clients page.

Click on Save Map to save the changes made.

Floor Plan View



After importing your floor plan image, you can distribute markers that represent the APs to the correct locations by clicking on **AP List** and dragging each marker icon to its correct location on the floor plan. Also, Wireless Coverage Display can be toggled on to indicate the coverage range of each AP, assisting IT managers to easily and accurately plan and deploy wireless networks in any indoor environment. Click on **Save Plan** when you're done to save settings.

Floor Plans: Click to select floor plans uploaded to system.

AP List: Click to reveal a list of managed APs.

Settings: Click to reveal *Wireless Coverage Display* settings.

AP Info
AP Information: Select to toggle on/off AP detailed information to be shown on your floor plan.
2.4GHz / 5GHz: Select whether to display signal coverage of 2.4GHz or 5GHz radio. The wireless coverage displayed will be based on the transmit power settings of the Access Point.
Scaling Tool: Use the scaling tool to determine the exact distance on the floorplan.
Signal Indicator: The colored indicator displays the reference signal strength covered.

RF Coverage
Enable: Select to display wireless coverage on your floor plan.
RSSI Value: Adjust RSSI value to emulate using the slider bar.
Calibration Offset: Use the slider bar to adjust the offset value based on the deployment.
RSSI Range Simulate: Check the **RSSI Simulate** box to display RSSI reference on your floor plan. Adjust RSSI coverage range to emulate using the slider bar.

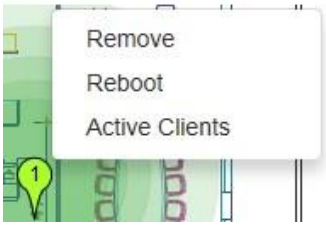
Navigating Tips

Use  to scroll up, down, left, or right.

Use  to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

Mouse over a device to show information about the device.

The number in the marker represents the number of wireless clients that are currently connected to the Access Point.

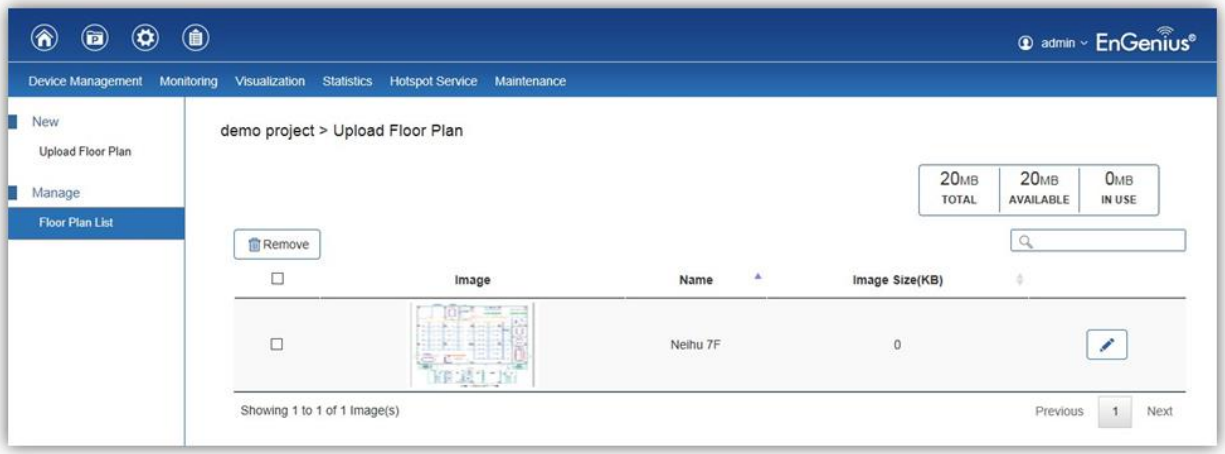


Left click on the Access Point marker to bring up a menu where you can configure AP settings, remove AP from management list, reboot AP, redirect to the Active Clients page or redirect to troubleshooting page.

Click on  for the settings to take effect.

Click on  to export floorplan image to a file.

Upload Floor Plan



From here, the administrator can add or delete a custom map or floor plan image. An unlimited number of floor plan images can be imported to the EWS Switch. However, the total
file size of all imported floor plans is limited to 20MB and the maximum file size per image is 2MB (a smaller image loads faster). Valid image file formats are .PNG, .GIF or .JPG.

Status Dashboard
Total: Displays the total memory storage space allocated for uploading custom floor plans.
Available: Display the memory storage space that is currently available.
In Use: Displays the memory storage space that is currently in use.

Statistics

This page displays a visual chart of network traffic of all the AP managed by ezMaster.

Access Points

The page displays a visual chart of the top 10 network traffic of the Access Points managed by the ezMaster.

Navigating Tips
Click **Sort** to sort the order from ascending/descending, depending on your preference.

Click **Rx** to display Rx transmission, **Tx** to display Tx transmission or **Total** to display combined Rx and Tx transmission.

Click **1 day** or **1 week** button to select a time increment to monitor statistics by.

Place the mouse cursor over the bar on the chart to show detailed information.

Click on the bar in the Managed APs chart to display the traffic of the selected AP.

Wireless Clients

In addition to viewing information based on specific Access Points, you can view data via specific clients as well for security purposes.

Navigating Tips
Click **Sort** to sort the order from ascending/descending, depending on your preference.

Click **Rx** to display Rx transmission, **Tx** to display Tx transmission or **Total** to display combined Rx and Tx transmission.

Click **1 day** or **1 week** button to select a time increment to monitor statistics by.

Place the mouse cursor over the bar on the chart to show detailed information.

Click on the bar in the Managed APs chart to display the wireless clients that has associated with the selected AP.

Real Time Throughput

This page displays the real-time network activity of the selected Access Point.

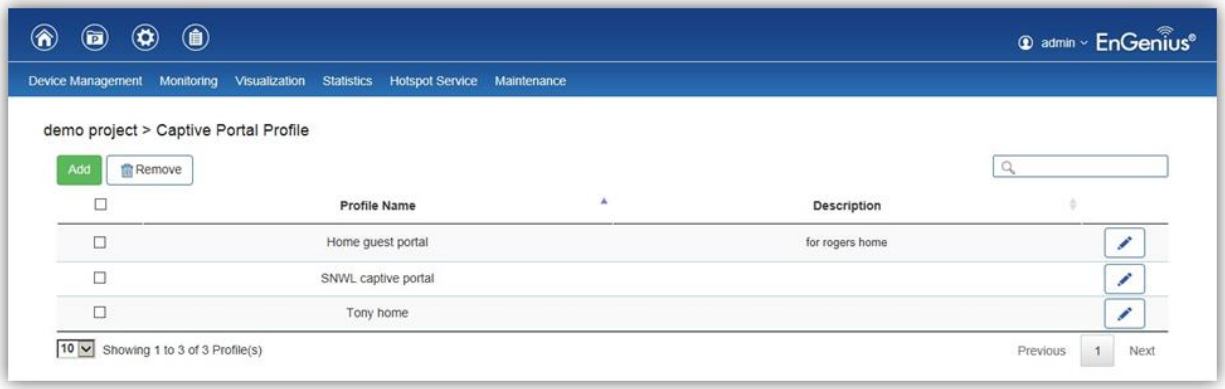
Hotspot Service

A hotspot is a wireless network that provides access through a captive portal. Use this feature to setup captive portal related configurations.

A captive portal provides registered users with network access while containing unregistered users. Users will need to enter a valid user name and password before they are allowed access to the Internet through the hotspot. Once a Captive Portal Profile is created, the administrator can apply this profile to multiple Guest Networks SSIDs.

Note: Captive portal profiles can only be assigned to the **Guest Network SSIDs**.

Captive Portal



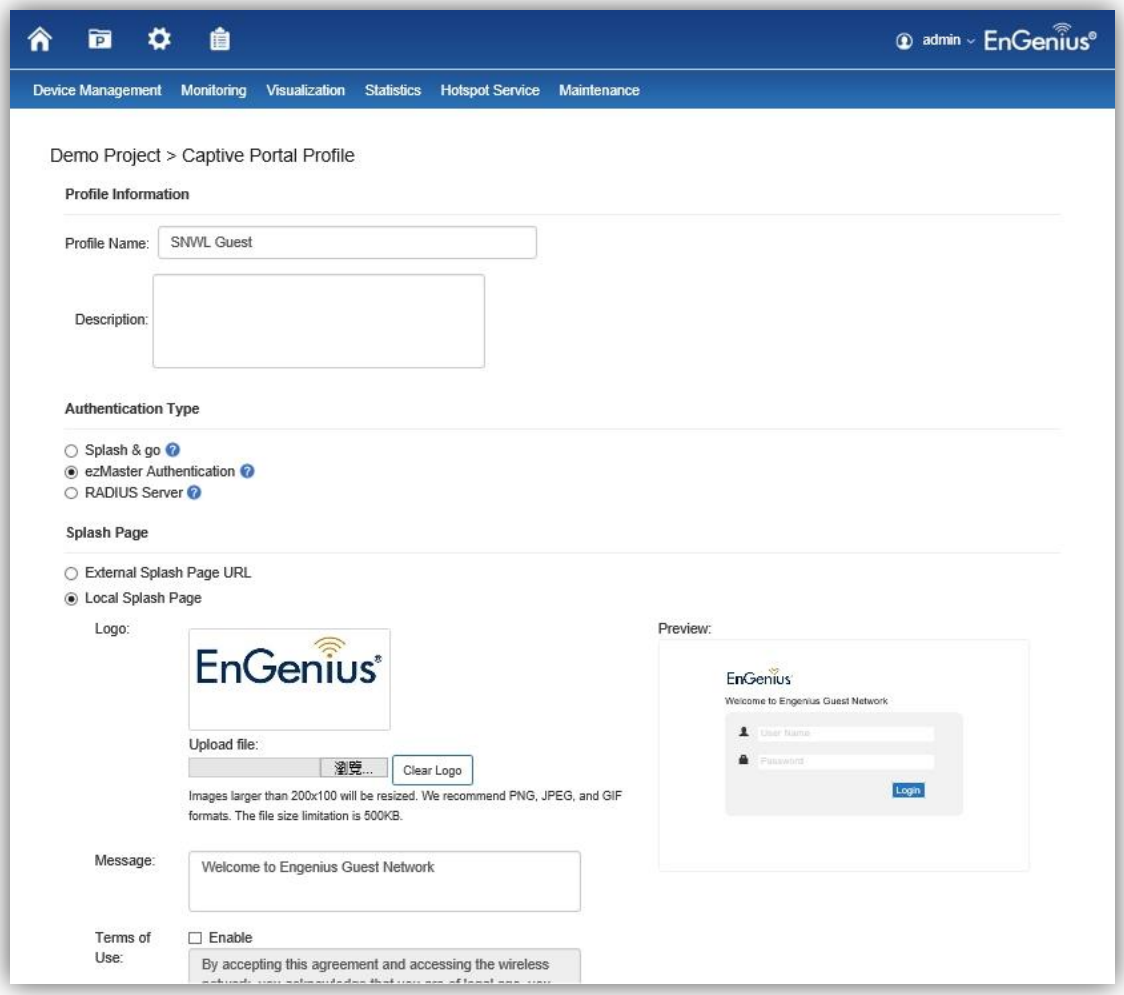
On this page, you can create captive portal profiles to apply to your network's guest network.

Add: Create a new captive portal profile.

Remove: Delete the selected captive portal profile.

Edit: Edit the settings of the selected captive portal profile.

Captive Portal Settings



Profile Name: Enter a name for this captive portal profile.

Description: Enter a brief description for this captive portal profile.

Authentication Type: Defines the mechanism by which a wireless client gains access to the network after the client has associated to the SSID.

Splash & Go	The wireless client is granted network access without any further authentication as soon as it is associates to the SSID.
ezMaster Authentication	The wireless client is authenticated using ezMaster's Local Database (from *Hotspot Service > Guest Account*).
RADIUS Server	The wireless client is authenticated using an external RADIUS server.

Splash Page: A splash page is the web page which prompts the user to log in with a user name and password, or accept a network use policy once the client has associated to the SSID. ezMaster supports both local and external splash page.

Local Splash Page	Use the splash page hosted locally by ezMaster server. The local splash page enable administrators to eliminate the need to set up a local web server. Basic customizations like displaying a corporate logo, custom message and term of use is available.
External Splash Page	External splash page enables the administrator to host their own the splash page web server, rather than having it hosted by ezMaster.

Redirect Behavior: Configure where users will be redirected after successful login. You could redirect them to the page that they want to visit, or you could set a different page where users will be redirected.

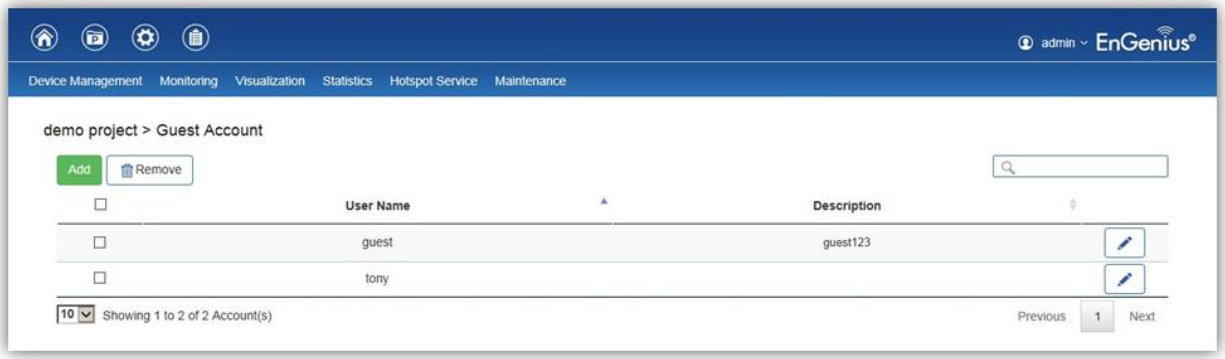
Redirect to the URL that the user was trying to visit	Select this option for ezMaster to cache the initial website from the client during the authentication process and then forward it to the originally targeted web server after the user successfully authenticates.
Redirect users to a specified URL after login	Select this option to redirect users to a specific URL after users successfully authenticates.

User Session: Configure session timeout and ideal timeout period.

Session Timeout	Specify a time limit after which users will be disconnected and required to log in again.
Idle Timeout	Specify a time limit for an idle client after which users will be disconnected and required to log in again.

Walled Garden: This option allows users to define network destinations that users can access before authentication. For example, your company's website.

Guest Account



On the Access Control page, an administrator can create, edit, and remove user accounts used for captive portal's local database authentication.

Add: Create a new user account.

Remove: Delete the selected user account.

Edit: Edit the settings of the selected user account.

Creating a basic captive portal using ezMaster authentication

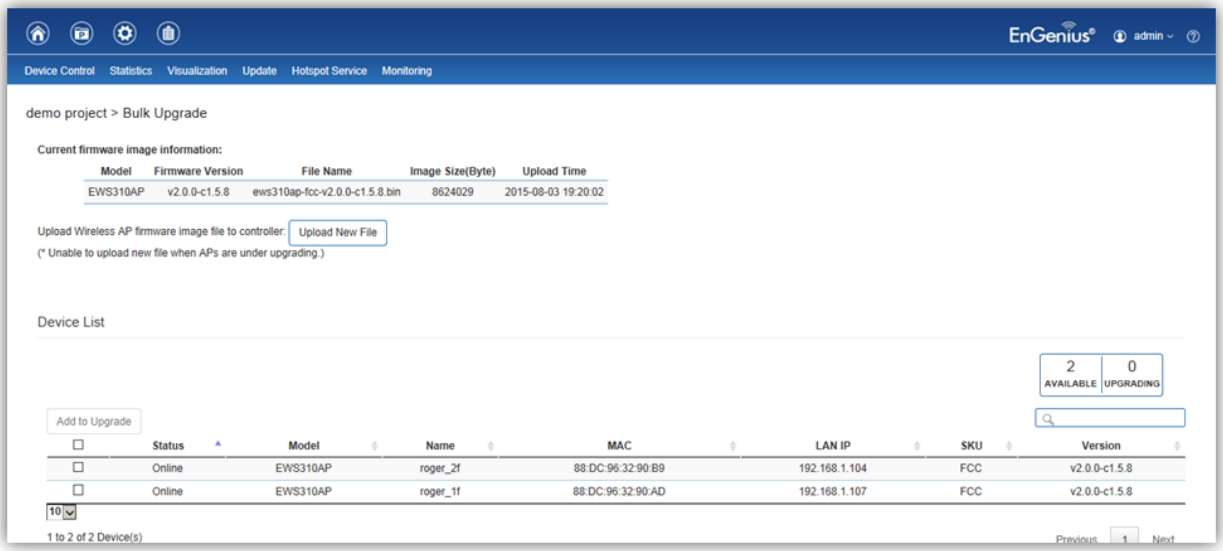
The steps below will guide you to create a basic captive portal using ezMaster authentication.

1. Select a project and navigate to *Hotspot Service* > *Captive Portal*.
2. Click on ***Add***.
3. Fill in the *Profile Name* and *Description*.
4. For *Authentication Type*, select ***ezMaster Authentication***.
5. For *Splash Page*, select ***Local Splash Page*** and customize your splash page by uploading a logo, entering a custom message, and terms or use if desired.
6. Scroll to the bottom of the page and click on ***Save Changes***.
7. Next, navigate to *Hotspot Service* > *Guest Account*.
8. Click on ***Add***.
9. Create a new entry by filling in the user name, password and description.
10. Click on ***Apply*** to continue.
11. Navigate to *Device Management* > *Device Config* > *Access Point*.
12. Click on the device name (or group name) of the AP (or group) you wish to apply captive portal settings to.
13. Under *Guest Network*, choose ***Enable*** and select the captive profile you just created (make sure your 2.4GHz/5GHz Guest Network SSID is enabled).
14. Scroll to the bottom of the page and click on ***Apply***.

Once the above procedure is completed, a wireless client will be re-directed to the splash page every time it associates to your Guest Network.

Maintenance

Bulk Upgrade



The Bulk Upgrade feature allows administrators to upgrade the firmware of multiple Access Points at the same time. After uploading the firmware of an AP, the system will automatically display a list of Access Points the system is currently managing that the uploaded firmware is for.

To upgrade, please follow the steps below:
1. Click on Upload New File to mount AP firmware onto ezMaster's flash.
2. Once the Access Point firmware is uploaded successfully, a list of Access Points that the uploaded firmware is for will appear in the Device List.
3. Select the Access Points you wish to upgrade and click Add to Upgrade to start the firmware upgrading process.

Warning: Upgrading APs will temporarily disconnect all associated clients from the network. To minimize network disruption, we recommend performing the upgrade procedure at an off-peak time.

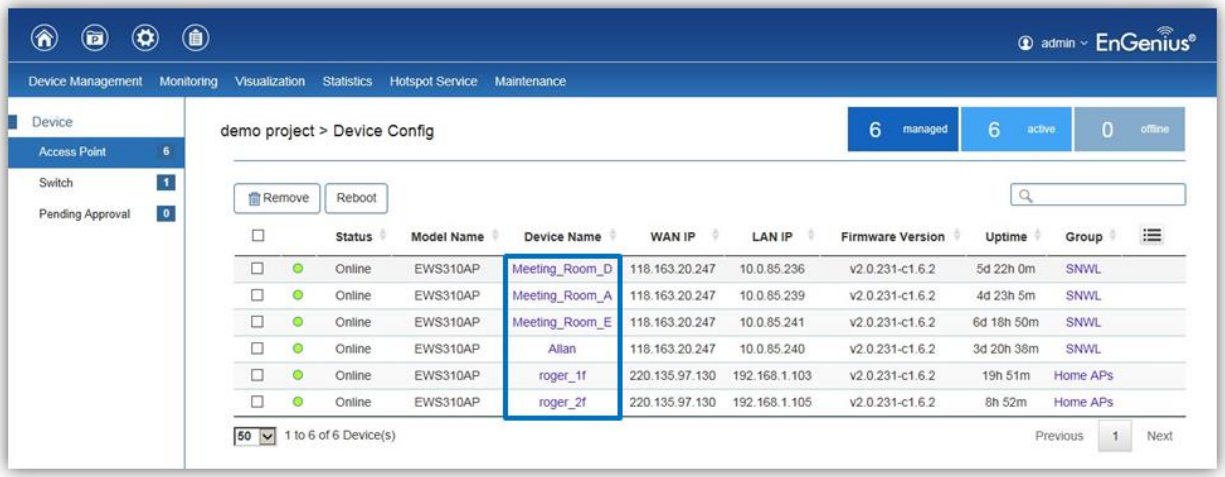
Bulk Upgrade (Switch)

Similar to the Bulk Upgrade (AP) feature, the Bulk Upgrade (Switch) feature allows administrators to upgrade the firmware of multiple EWS switches managed by ezMaster at the same time. After uploading the firmware of an EWS Switch, the system will automatically display a list of switches the system is currently managing that the uploaded firmware is for.

To upgrade, please follow the steps below:
1. Click on Upload New File to mount switch firmware onto ezMaster's flash.
2. Once the switch firmware is uploaded successfully, a list of switches that the uploaded firmware is for will appear in the Device List.
3. Select the switches you wish to upgrade and click Add to Upgrade to start the firmware upgrading process.

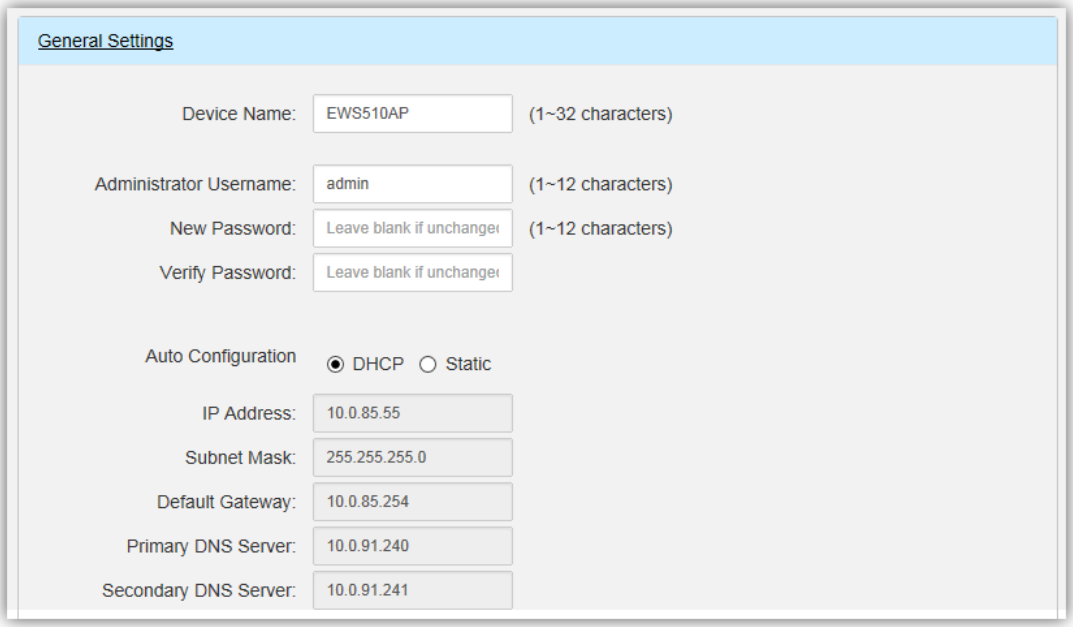
Warning: Upgrading switches will temporarily disconnect all wired devices connected. To minimize network disruption, we recommend performing the upgrade procedure at an off-peak time.

Access Point Configuration



Under *Device Management* > *Device Config* > *Access Point*, you can configure AP settings by clicking on the ***Device Name*** link of the device.

General Settings



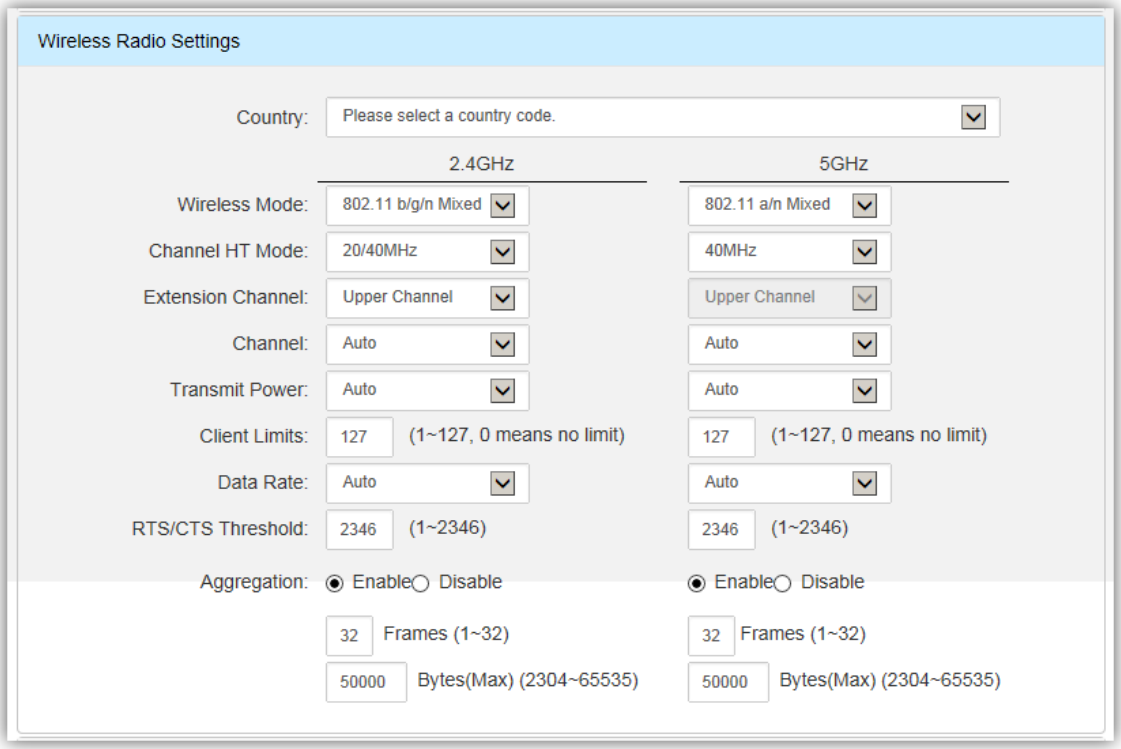
Device Name: The device name of the Access Point. Users can enter a custom name for the Access Point if they wish.

Administrator Username: Displays the current administrator login username for the Access Point. Enter a new Administrator username for the Access Point if you wish to change the username. The default username is: *admin*.
New Password: Enter a new password of between 1~12 alphanumeric characters.
Verify Password: Enter the password again for confirmation.

IP Settings: Select whether the device IP address will use the static IP address specified in the IP address field or be obtained automatically when the device connects to a DHCP server.
IP Address: Enter the IP address for the Access Point.
Subnet Mask: Enter the Subnet Mask for the Access Point.

Default Gateway: Enter the Default Gateway for the Access Point.
Primary/Secondary DNS Server: Enter the Primary/Secondary DNS server name.

Wireless Radio Settings



Country: Select a Country/Region to conform to local regulations. Different regions have different rules that govern which channels can be used for wireless communications.

Wireless Mode: Select from the drop-down menu to set the wireless mode for the Access Point.

Channel HT Mode: Use the drop-down menu to select the channel width for 2.4GHz. A wider channel improves the performance, but some legacy devices operate only on either 20MHz or 40 MHz. This option is only available for 802.11n modes.

Extension Channel: Use the drop-down menu to set the Extension Channel as Upper or Lower channel. An extension channel is a secondary channel used to bond with the primary channel to increase this range to 40MHz allowing for greater bandwidth. This option is only available when Wireless Mode is 802.11n and Channel HT Mode is 20/40MHz or 40MHz.

Channel: Select Auto or manually assign a channel for the 2.4GHz or 5GHz radio. The list of available channels that can be assigned to radios is determined based on which country the Access Points are deployed in.

Transmit Power: Allows you to manually set the transmit power on 2.4GHz or 5GHz radios. Optimizing channel assignments reduces channel interference and channel utilization for the network, thereby improving overall network performance and increasing the network's client capacity.
Note: With Background Scanning and Auto Tx Power enabled, setting the Transmit Power to **Auto** will dynamically adjust the AP's transmit power according to the RF information collected by background scanning.

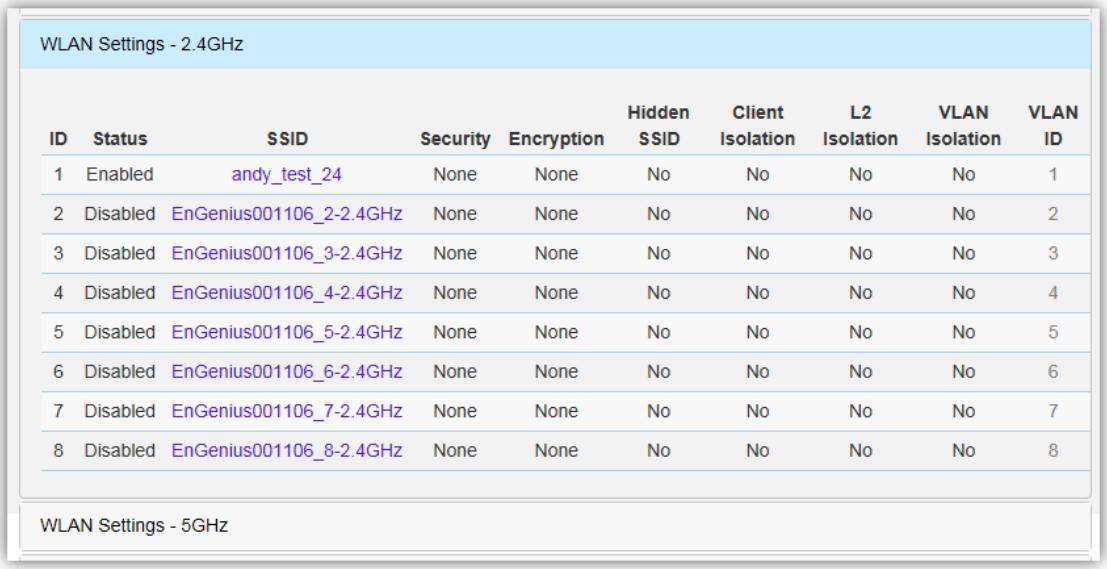
Client Limits: Limit the total number of clients that can associate with this Access Point.

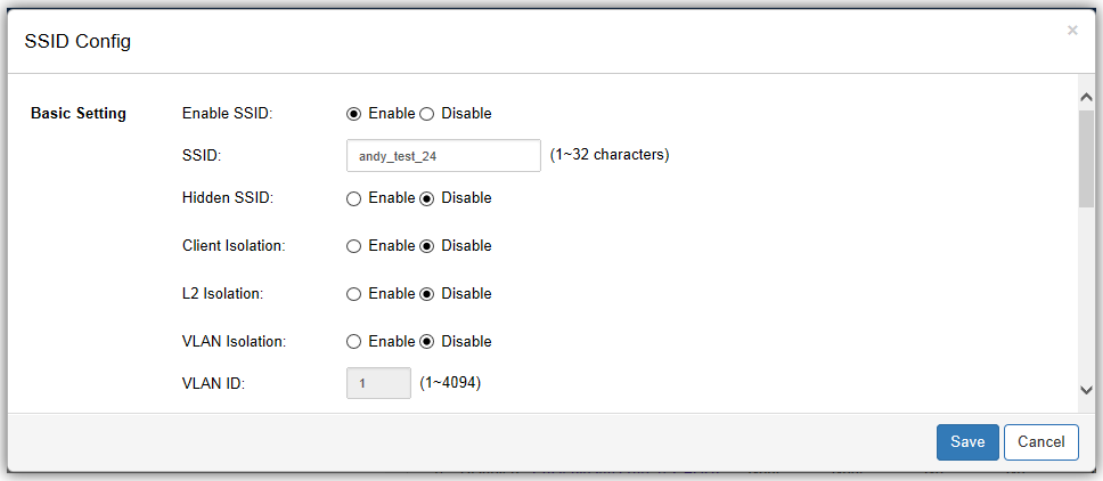
Data Rate: Use the drop-down list to set the transmit data rate permitted for wireless clients. The data rate affects the throughput of the access point. The lower the data rate, the lower the throughput, but the longer transmission distance.

RTS/CTS Threshold: Enter a Request to Send (RTS) Threshold value between 1~2346. Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same Access Point. Changing the RTS threshold can help control traffic flow through the Access Point. If you specify a lower threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the Access Point. Sending out more RTS packets can help the network recover from interference or collisions which might occur on a busy network or on a network experiencing electromagnetic interference.

Aggregation: Select whether to enable or disable Aggregation for the Access Point. This function merges data packets into one packet, reducing the number of packets. This also increases the packet sizes, so please keep this in mind. Aggregation is useful for increasing bandwidth throughput in environments that are prone to high error rates. This mode is only available for 802.11n modes. Fill in the frame rate limit you wish to use. The range is from 1~32. Next, fill in the max byte limit. The range is from 2304~65535.

WLAN Settings - 2.4GHz/5GHz





Basic Setting

Enable SSID: Select to enable or disable the SSID broadcasting.

SSID: Enter the SSID for the current profile. This is the name that is visible to wireless clients on the network.

Hidden SSID: Enable this option if you do not want to broadcast this SSID. This can help to discourage wireless users from connecting to a particular SSID.

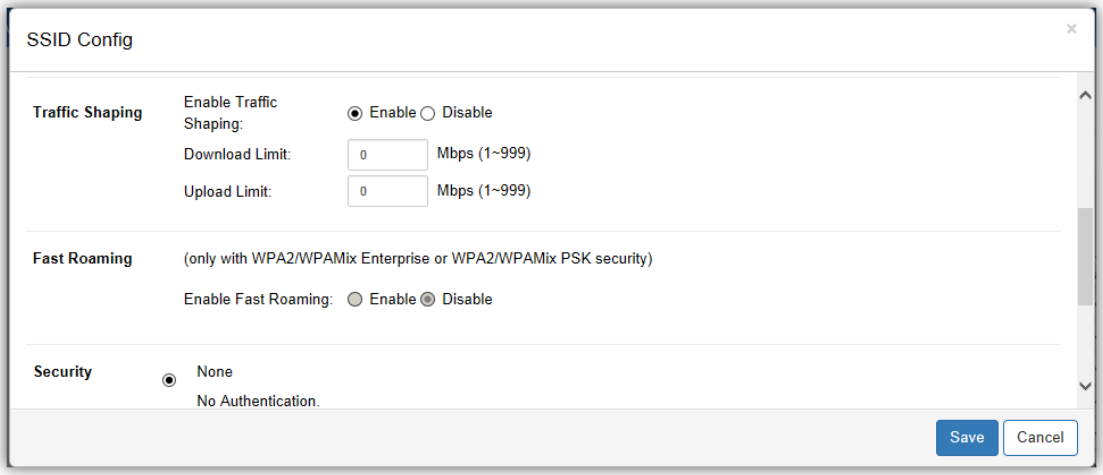
Client Isolation: When enabled, all communication between wireless clients connected to the same AP will be blocked.

L2 Isolation: When enabled, wireless client traffic from all hosts and clients on the same subnet will be blocked.

VLAN Isolation: When enabled, all communications between wireless clients and any other devices on different VLANs will be blocked. All frames from wireless clients connected to this SSID will be tagged a corresponded 802.1Q VLAN tag when going out from Ethernet port.

VLAN ID: Enter the VLAN ID for the SSID profile. The range is from 1~4094. When VLAN tagging is configured per SSID, all data traffic from wireless users associated to that SSID is tagged with the configured VLAN ID. Multiple SSIDs also can be configured to use the same VLAN tag. For instance, a

single VLAN ID could be used to identify all wireless traffic traversing the network, regardless of the SSID. When the AP receives VLAN-tagged traffic from the upstream switch or router, it forwards that traffic to the correct SSID. The AP drops all packets with VLAN IDs that are not associated to the SSID.

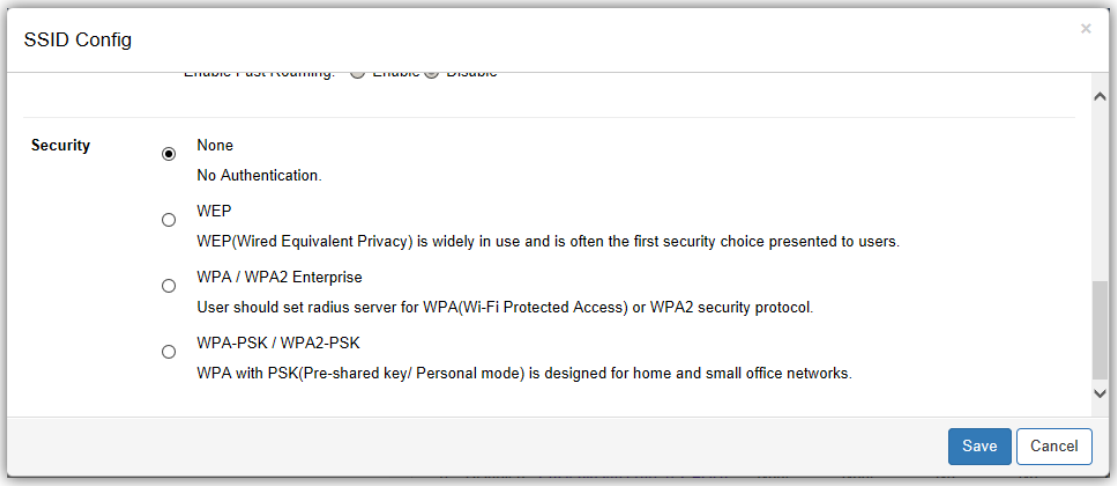


Traffic Shaping: Traffic Shaping regulates the allowed maximum downloading/uploading throughput per SSID. Select to enable or disable Wireless Traffic Shaping for the SSID.

- **Download Limit**: Specifies the allowed maximum throughput for downloading.
- **Upload Limit**: Specifies the allowed maximum throughput for uploading.

Fast Roaming: This feature uses protocols defined in 802.11r to allow continuous connectivity for wireless devices in motion, with fast and secure roaming from one AP to another. Coupled with 802.11k, wireless devices are able to quickly identify nearby APs that are available for roaming and once the signal strength of the current AP weakens and your device needs to roam to a new AP, it will already know which AP is the best to connect with. Note that not every wireless client supports 802.11k and 802.11r. Both the SSID and security options must be the same for this fast roaming to work. Fast Roaming is available when the following security methods are well configured:

WPA2-Enterprise	RADIUS server required
WPA-Mixed Enterprise	
WPA2-PSK	No RADIUS server required
WPA-Mixed	



Security: Select encryption method (WEP, WEP / WPA2 Enterprise, WPA-PSK / WPA2-PSK, or none) and encryption algorithm (AES or TKIP).

WEP: Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks which scrambles all data packets transmitted between the Access Point and

the wireless clients associated with it. Both the Access Point and the wireless client must use the same WEP key for data encryption and decryption.

- **Mode**: Select Open System or Shared Key.
- **WEP Key**: Select the WEP Key you wish to use.
- **Input Type**: ASCII: Regular Text or HEX. Select the key type. Your available options are ASCII and HEX.
  - **ASCII Key**: You can choose upper and lower case alphanumeric characters and special symbols such as @ and #.
  - **HEX Key**: You can choose to use digits from 0~9 and letters from A~F. Select the bit-length of the encryption key to be used in the WEP connection. Your available options are: 64, 128, and 152-bit password lengths.
- **Key Length**: Select the desired option and ensure the wireless clients use the same setting. Your choices are: 64, 128, and 152-bit password lengths.
- **Key1/2/3/4**: Enter the Key value or values you wish to use.

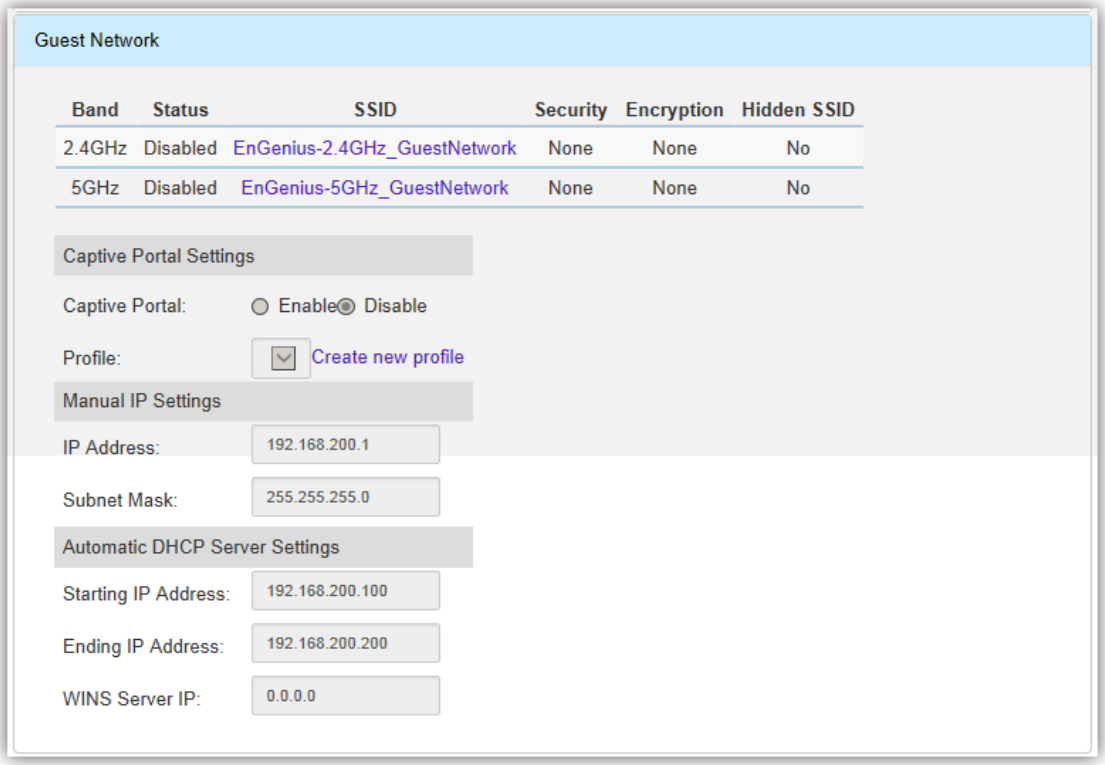
WPA / WPA2 Enterprise: WPA and WPA2 are Wi-Fi Alliance IEEE 802.11i standards, which include AES and TKIP mechanisms.

- **Type**: Select the WPA type to use. Available options are Mixed, WPA and WPA2. Choose Mixed if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **Encryption**: Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).
  Note: Since TKIP is not permitted for 802.11n-based transmissions, setting the encryption algorithm to TKIP when you are using an 802.11n or 802.11ac AP will cause the network to operate in 802.11g mode.
- **RADIUS Server**: Enter the IP address of the RADIUS server.
- **RADIUS Port**: Enter the port number used for connections to the RADIUS server.
- **RADIUS Secret**: Enter the secret required to connect to the Radius server.
- **Update Interval**: Specify how often, in seconds, the group key changes. Select 0 to disable.
- **RADIUS Accounting**: Enables or disables the accounting feature.
- **RADIUS Accounting Server**: Enter the IP address of the RADIUS accounting server.
- **RADIUS Accounting Port**: Enter the port number used for connections to the RADIUS accounting server.
- **RADIUS Accounting Secret**: Enter the secret required to connect to the RADIUS accounting server.
- **Accounting Group Key Update Interval**: Specify how often, in seconds, the accounting data sends. The range is from 60~600 seconds.

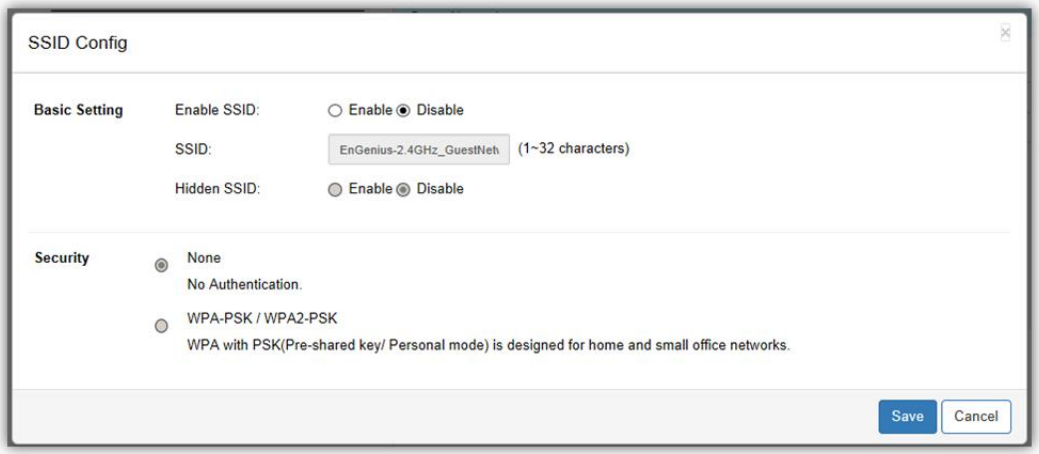
WPA-PSK / WPA2-PSK: WPA with PSK (Pre-shared key / Personal mode), designed for home and small office networks that don't require the complexity of an 802.1X authentication server.

- **Type**: Select the WPA-PSK type to use. Available options are Mixed, WPA-PSK and WPA2-PSK. Choose Mixed if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **Encryption**: Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).
  Note: Since TKIP is not permitted for 802.11n-based transmissions, setting the encryption algorithm to TKIP when you are using an 802.11n or 802.11ac AP will cause the network to operate in 802.11g mode.
- **WPA Passphrase**: Enter the Passphrase you wish to use. If you are using the ASCII format, the Key must be between 8~64 characters in length.
- **Group Key Update Interval**: Specify how often, in seconds, the Group Key changes.

Guest Network



Guest Network: The Guest Network feature allows administrators to grant Internet connectivity to visitors or guests while keeping other networking devices and sensitive personal or company information private and secure.



Basic Setting

Enable SSID: Select to enable or disable the SSID broadcasting.

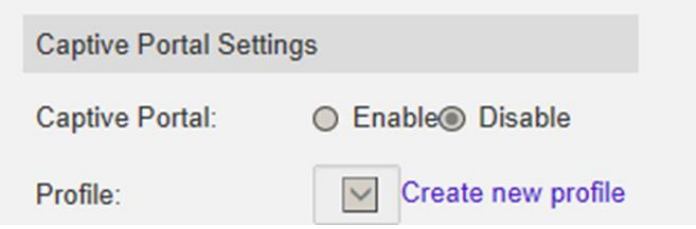
SSID: Enter the SSID for the current profile. This is the name that is visible to wireless clients on the network.

Hidden SSID: Enable this option if you do not want to broadcast this SSID. This can help to discourage wireless users from connecting to a particular SSID.

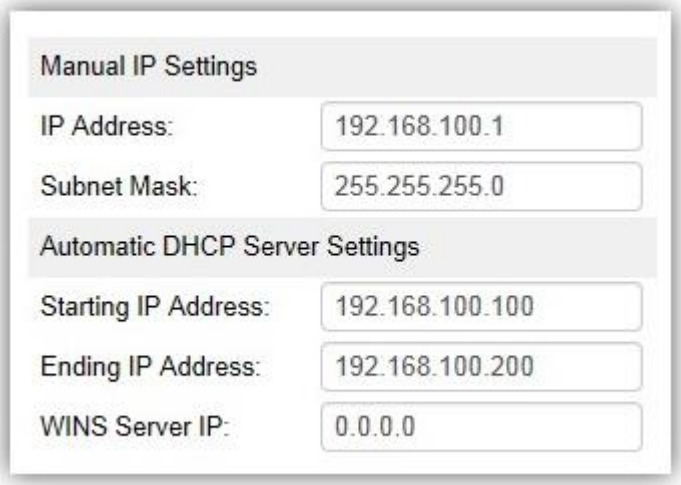
Security: Select encryption method (WPA-PSK / WPA2-PSK, or none) and encryption algorithm (AES or TKIP).

WPA-PSK / WPA2-PSK: WPA with PSK (Pre-shared key / Personal mode), designed for home and small office networks that don't require the complexity of an 802.1X authentication server.

- **Type**: Select the WPA-PSK type to use. Available options are Mixed, WPA-PSK and WPA2-PSK. Choose Mixed if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **Encryption**: Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).
  Note: Since TKIP is not permitted for 802.11n-based transmissions, setting the encryption algorithm to TKIP when you are using an 802.11n or 802.11ac AP will cause the network to operate in 802.11g mode.
- **WPA Passphrase**: Enter the Passphrase you wish to use. If you are using the ASCII format, the Key must be between 8~64 characters in length.
- **Group Key Update Interval**: Specify how often, in seconds, the Group Key changes.



Captive Portal: Enable/disable Captive Portal for Guest Network. Refer to *Section: Hotspot Service > Captive Portal* for more information.
Profile: Select to apply an existing Captive Portal Profile to the Guest Network or Create a New Captive Portal Profile.



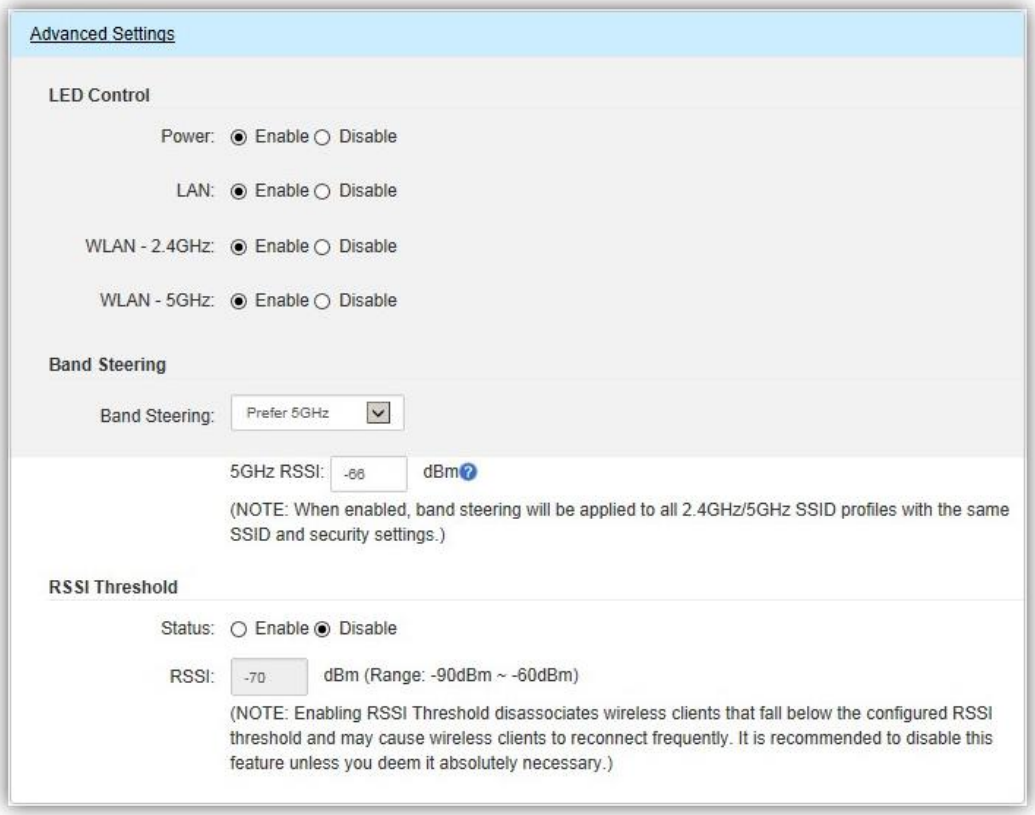
Manual IP Settings

- **IP Address**: Enter the IP address for the default gateway of clients associated to the Guest Network.
- **Subnet Mask**: Enter the Subnet mask for the Guest Network.

Automatic DHCP Server Settings

- **Starting IP Address/Ending IP Address**: Enter the pool range of IP addresses available for assignment.
- **WINS Server IP**: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

Advanced Settings



LED Control: In some environments, the blinking LEDs on APs are not welcomed. This option allows you to enable or disable the devices LED indicators. Note that only indoor models support this feature.

Band Steering: When enabled, when the wireless client first associates with the AP, the AP will detects whether or not the wireless client is dual-band capable, and if it is, it will force the client to connect to the less congested 5GHz network to relieve congestion and overcrowding on the mainstream 2.4GHz frequency. It does this by actively blocking the client's attempts to associate with the 2.4GHz network. ***Note: For Band Steering to take effect, both 2.4GHz and 5GHz SSIDs must have the same SSID and security settings. Wireless clients must be in both 2.4GHz and 5GHz wireless coverage zone when authenticating with the AP for the Band Steering algorithm to take effect.***

- **Prefer 5GHz:** All dual-band clients with 5GHz RSSI above the threshold will be connected to the 5GHz band.
- **Force 5GHz:** All dual-band client will connect to the 2.4GHz.
- **Band Balance:** Automatically balances the number of newly connected clients across both 2.4GHz and 5GHz bands.

IMPORTANT INFORMATION: Band Steering only defines the action when a wireless client associates with an AP for the first time, and the wireless client must be in both 2.4GHz and 5GHz wireless coverage zone when authenticating with the AP for the Band Steering algorithm to take effect.

RSSI Threshold: With this feature enabled, in order to minimize the time the wireless client spends to passively scanning for a new AP to connect to, the AP will send a disassociation request to the wireless client upon detecting the wireless client's RSSI value lower than specified. The RSSI value can be adjusted to allow for more clients to stay associated to this Access Point. Note that setting the RSSI value too low may cause wireless clients to reconnect frequently. It is recommended to disable this feature unless you deem it absolutely necessary.

Appendix

Appendix A: ezMaster CLI

Show system information

- Cmd:
  show <ip|dns|gateway|ezmaster|date|timezone>
  e.g. show ip

Start/Stop/Restart ezMaster

- Cmd:
  ezmaster <start|stop|restart>
  e.g. ezmaster restart

IP/DNS/Gateway setting

- Cmd:
  config ip eth0 <IP Address> <Netmask>
  e.g. config ip eth0 192.168.0.200 255.255.255.0

- Cmd:
  config dns <Server Address>
  e.g. config dns 8.8.8.8

- Cmd:
  config gateway <Gateway Address>
  e.g. config gateway 192.168.0.1

Time/ Date setting

- Cmd :
  config date <YYYY-MM-DD> <HH:MM:SS>
  e.g. config date 2015-06-11 17:28:00

Timezone setting

- Cmd :
  config timezone