# Table of contents

Introduction..................................................................................................................4
  Overview ....................................................................................................................4
  ezMaster Software.....................................................................................................4
  Deployment Scenario .................................................................................................4
Installing ezMaster .........................................................................................................5
  Firewall Ports to be opened for ezMaster .................................................................5
  Server System Requirements ....................................................................................5
  Before you begin .........................................................................................................5
  Installing and setting up VMware Player .................................................................5
  Installing and setting up ezMaster .............................................................................7
Logging into ezMaster .................................................................................................9
Getting Started ............................................................................................................10
  Connecting devices to ezMaster ..............................................................................11
  Registering ezMaster to ezRegistration Server .......................................................11
  Adding devices to ezMaster Device Inventory .........................................................12
  Manually redirecting devices to ezMaster ...............................................................14
  Managing Access Points .........................................................................................14
Working with ezMaster ...............................................................................................16
  Main Dashboard .......................................................................................................17
  Projects ......................................................................................................................17
  Global Settings .........................................................................................................18
  Device Inventory .......................................................................................................19
Working with Projects ..............................................................................................20
  Device Control .........................................................................................................21
    Summary ................................................................................................................21
    Device Config .........................................................................................................21
    Group ......................................................................................................................23
    Access Control .......................................................................................................23
Visualization .................................................................................................................24
  Topology View ..........................................................................................................25
  Map View ..................................................................................................................26
  Floor View ...............................................................................................................28
Update .........................................................................................................................29
  Bulk Upgrade ..........................................................................................................30
Hotspot Service ...........................................................................................................30
  Captive Portal ...........................................................................................................31
  Guest Account ..........................................................................................................33
Monitoring ..................................................................................................................33
  Active Clients ...........................................................................................................34
  Event Logs ...............................................................................................................35
Access Point Configuration .........................................................................................35
  General Settings .......................................................................................................36
  Wireless Radio Settings ...........................................................................................36
  WLAN Settings .........................................................................................................38
Guest Network ........................................................................................................... 41
Advanced Settings ...................................................................................................... 43
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 VMware image for quick and easy deployments. It can be launched using the free VMware Player or other commercial VMware.

Deployment Scenario
**Installing ezMaster**

**Firewall Ports to be opened for ezMaster**

The table below lists the ports that must be opened for ezMaster to function properly.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP destination port 1234</td>
<td>CAPWAP protocol</td>
</tr>
<tr>
<td>TCP destination port 80 (HTTP)</td>
<td>For captive portal splash page redirect</td>
</tr>
<tr>
<td>TCP destination port 433 (HTTPS)</td>
<td>For captive portal splash page redirect</td>
</tr>
</tbody>
</table>

**Server System Requirements**

Recommended environment for managing up to 1000 APs
- CPU: Intel i3 3.5GHz dual core or above
- RAM: 4GB minimum
- HDD: 500GB (actual requirement depending on log size)
- OS: Microsoft Windows 7 or later + VMware Player 7.0.0 or later

**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.

**Installing and setting up VMware Player**

1. Download VMware Player (7.0.0 or later) from the link below: [https://my.vmware.com/web/vmware/downloads](https://my.vmware.com/web/vmware/downloads)

2. After successfully installing VMware Player, start the program and click on “Open a Virtual Machine”
3. Locate and select the ezMaster image file.

![Image of ezMaster image file]

4. Once the ezMaster image has been mounted, select: Player > Manage > Virtual Machine Settings…

![Image of Virtual Machine Settings dialog box]
5. Under the “Hardware” tab, click on “Network Adapter” and select “Bridged: Connect directly to the physical network”.

6. 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.

7. Click on “OK” to save apply settings.
Installing and setting up ezMaster

1. After setting up your network adapter, select “Play Virtual Machine” to launch the ezMaster image.

2. When prompted to choose whether the image was moved or copied, select “I Copied It”.

3. Once the installation script finishes running, you will be prompted to enter a login id and password for ezMaster. Enter admin/password. Tip: Use Ctrl + Alt to return to Windows desktop
4. When the command prompt appears, assign the ezMaster Server URL. (Tip: use Network Adapter Properties to check the info of your network adapter)

- Enter ezMaster Server IP and netmask:
  ```sh
cfg ip eth0 10.0.92.5 255.255.255.0
```
  (eg. LAN Adapter IP is 10.0.92.4 so I choose to use an unused IP Address 10.0.92.5 is chosen to be used as ezMaster IP)

- Enter ezMaster Server gateway:
  ```sh
cfg gateway 10.0.92.254
```

- Enter ezMaster DNS Server:
  ```sh
cfg 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.

2. Once the log in screen appears, enter the username and password to log in. The default is **admin/password**.
Getting Started

Connecting devices to ezMaster

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.

<table>
<thead>
<tr>
<th>Access Point</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>All local devices (in same subnet) will be automatically detected and ready for management in the “Pending Approval” list under “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)</td>
</tr>
<tr>
<td>Remote</td>
<td>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 Config” in each project.</td>
</tr>
<tr>
<td>Remote</td>
<td>Manually assign the ezMaster server URL from the access point’s user interface (under Management &gt; Controller Settings). If configured successfully, the access point will connect directly to the ezMaster and it will be automatically detected and ready for management in the “Pending Approval” list under “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).</td>
</tr>
</tbody>
</table>
Registering ezMaster to ezRegistration Server

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 Account Setting, fill in your e-mail and assign a password, then click Apply to register with the ezRegistration server.
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 'Device Registration' button on the side menu.

3. Enter the MAC Address, Check Code and Description of your AP/Switch 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 Register once you are done.

Note: The 'check code' of the AP can be found in the AP's user interface under the "Management" menu > "Controller Settings".

*In the future (official release), the check code will be printed on the device label at the bottom of each AP. The check code will also be displayed in the "Device" menu in the EWS Switch user interface.
4. The message below will be displayed upon successfully claiming an AP and you will see the AP under the Device List.

**Message**

Device registration successfully!

**OK**

**Manually redirecting devices 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 settings.
Managing Access Points

Same as on the EWS Switch, EWS Access Points will have to be added to the “Managed AP” list in order to configure and monitor the APs.

1. 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.

2. Click on ‘Create New Project’ and enter a project name and description. Click on Apply when you are done.

3. You'll be automatically redirected to the ‘Device 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.

4. Select the AP(s) you wish to add to your profile by selecting the checkbox and click on the ‘Add’ button.

5. You’ll be automatically redirected to the device page. Once the AP is online (green), to configure your AP, click on the ‘Device Name’ of your AP to bring up the configuration menu.
# General Settings

<table>
<thead>
<tr>
<th>Device Name:</th>
<th>EW635GAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Username:</td>
<td>admin</td>
</tr>
<tr>
<td>MAC Password:</td>
<td>Leave blank if unchanged</td>
</tr>
<tr>
<td>Verify Password:</td>
<td>Leave blank if unchanged</td>
</tr>
<tr>
<td>Auto Configuration:</td>
<td>DHCP or Static</td>
</tr>
<tr>
<td>IP Address:</td>
<td>192.168.0.37</td>
</tr>
<tr>
<td>Subnet Mask:</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway:</td>
<td>192.168.0.254</td>
</tr>
<tr>
<td>Primary DNS Server:</td>
<td>192.168.249</td>
</tr>
<tr>
<td>Secondary DNS Server:</td>
<td>192.168.192</td>
</tr>
</tbody>
</table>

# Wireless Radio Settings

- WLAN Settings - 2.4GHz
- WLAN Settings - 5GHz
- Guest Network
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 ezMaster system displaying information such as system 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

This page contains ezMaster related settings.

<待補>
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.

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.
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 Control

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 this page to add new EWS Access Points and EWS Switches to your project.

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

Remove AP
The Remove button removes selected Access Point(s) from list. 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 AP
The Reboot button will reboot the selected Access Point(s).

Search Bar
Use the Search Bar to search for 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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>AP is connected and managed by EWS Switch.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>AP is currently in the process of connecting to the EWS Switch.</td>
</tr>
<tr>
<td>Applying Change</td>
<td>AP is currently applying system changes.</td>
</tr>
<tr>
<td>Connecting</td>
<td>AP is currently connecting to EWS Switch.</td>
</tr>
<tr>
<td>Offline</td>
<td>AP is currently offline.</td>
</tr>
<tr>
<td>Resetting</td>
<td>AP is resetting.</td>
</tr>
<tr>
<td>Firmware Upgrading</td>
<td>AP is currently undergoing firmware upgrade process.</td>
</tr>
<tr>
<td>Invalid IP</td>
<td>The subnet of managed AP’s IP address is not the same as the EWS Switch.</td>
</tr>
<tr>
<td>Incompatible Version</td>
<td>Please remove AP and reconfigure AP to the correct setting.</td>
</tr>
<tr>
<td>Checking Certificate</td>
<td>AP firmware is not compatible with EWS Switch.</td>
</tr>
</tbody>
</table>

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 edit 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.

**IP Address**
Shows the IP address 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.

**Uptime:**
Displays the number of days, hours, and minutes since the AP last restarted.

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

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

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 Point 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.
Access Control

This page displays the list of wireless clients previously blocked from your network (using the Ban function from the Active Clients list). If for any reason, you need to block a client device from 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 block 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. Click on the Apply button on the upper right to save settings made on this page.

Unblocking a Previously Blocked Client Device
1. Click on the Delete button on the client device you wish to unblock.
2. Click on the Apply button on the upper right to save settings made on this page.
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 EWS Switch 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 Access Points 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.

<table>
<thead>
<tr>
<th>AP Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>The managed AP is currently online</td>
</tr>
<tr>
<td>Offline</td>
<td>The managed AP is currently offline</td>
</tr>
<tr>
<td>Busy</td>
<td>The managed AP is currently busy (applying new configuration settings)</td>
</tr>
<tr>
<td>Unmanaged</td>
<td>The AP is not managed by the controller</td>
</tr>
<tr>
<td>Topology</td>
<td>There is a change in topology for this device</td>
</tr>
<tr>
<td>Change</td>
<td></td>
</tr>
</tbody>
</table>

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 configure AP settings, remove AP from management list, reboot AP, redirect to the Active Clients page or redirect to troubleshooting page.

You can search for an Access Point using the IP Address or MAC address.

Click on to show or hide port information on the Controller.

Click on for the Controller to save the current network topology. Changes will be displayed upon detecting a topology change.

**Note:** The EWS Switch can only generate topologies with EnGenius L2 Series switches. 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 AP List to display the list of Access Points managed by the selected project then simply click-and-drag the AP marker to the desired location on the map.

<table>
<thead>
<tr>
<th>AP Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>The managed AP is currently online</td>
</tr>
<tr>
<td>Offline</td>
<td>The managed AP is currently offline</td>
</tr>
<tr>
<td>Busy</td>
<td>The managed AP is currently busy (applying new configuration settings)</td>
</tr>
</tbody>
</table>

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 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.
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.

**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 floor plan.
  - **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.

AP List: Click to reveal a list of APs that the EWS Switch is currently managing.

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.
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.

**NOTE:** Upgrading APs will temporarily disconnect them (and any associated clients) from the network. To minimize network disruption, we recommend performing the firmware upgrading procedure at an off-peak time.
Hotspot Service

Captive Portal

demo project > Captive Portal

Profile Information

Profile Name: Home guest portal

Description: for rogers home

Authentication Type

- Splash & go (No authentication required)
- Local Database
  - Public Port: 80
  - Enable Https: □

- External RADIUS Server
- Cloud4Wi

Splash Page

- Local Splash Page:
  - Logo:
    - Upload file: Clear Logo

Images larger than 200x100 will be resized. We recommend PNG, JPEG, and GIF formats.

Message: Welcome to Rogers home

Term of Use:

- Enable
  - and agree to be bound by this agreement. (*) The wireless network service is provided by the property owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason.
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.

**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. |
| Local Database | The wireless client is authenticated using ezMaster’s Local Database (from the Guest Account page). |
| External RADIUS Server | The wireless client is authenticated using an external RADIUS server. |
| Cloud4Wi | The wireless client is authenticated using a third party Hotspot Management platform: Cloud4Wi. For more information, visit http://www.cloud4wi.com/. **Note**: In the beta release, this feature is still under development and does not work. |

**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. 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 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 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 to a different URL | Select this option to redirect users to a specific URL after users successfully authenticates. |
**User Session**: Configure session timeout and ideal timeout period.

<table>
<thead>
<tr>
<th>Session Timeout</th>
<th>Specify a time limit after which users will be disconnected and required to log in again</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Timeout</td>
<td>Specify a time limit for an idle client after which users will be disconnected and required to log in again</td>
</tr>
</tbody>
</table>

**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.
From here, you can view information, temporarily disconnect and permanently block the wireless clients that are associated with the Access Points. ezMaster is able to identify client devices by their Operating System, device type and host name, if available. If multiple Access Points are connected to the network, 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 Wireless Clients managed by the EWS Switch using the following criteria:
Client Name, Client IP, Client MAC Address, Client OS, AP Device Name, AP MAC Address, Model Name, SSID, Band, TX Traffic, RX Traffic.

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

**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.
Access Point Configuration

On this page, you can edit the AP’s name and password, manually assign an IP address, or change the channel selection, transmit power and other wireless settings of a managed Access Point.

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.

Auto Configuration: 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.

- **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. The list of available channels that can be assigned to radios is determined based on which country the Access Points are deployed in.

- **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 available transmit data rates 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

**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:

<table>
<thead>
<tr>
<th>Security Type</th>
<th>RADIUS Server Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2-Enterprise</td>
<td>Required</td>
</tr>
<tr>
<td>WPA-Mixed Enterprise</td>
<td>Required</td>
</tr>
<tr>
<td>WPA2-PSK</td>
<td>Required</td>
</tr>
<tr>
<td>WPA-Mixed</td>
<td>No RADIUS server required</td>
</tr>
</tbody>
</table>

**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**

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.

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


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 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, the AP 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: Both 2.4GHz and 5GHz SSIDs must have the same security settings.*

**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.