User Manual

EWS-Series WLAN Gateway-Controller
ECH-Series Wireless Hotspot Gateway

Verion 3.43.00

Table of Content

1 Edgecore WLAN Quick Deployment

1.1 Check your Network Environment

Before installing the Edgecore WLAN controller, careful network planning is required in order to meet the networking needs with the most efficient utilization of network resources. IT staff of any organization should assess the available network resources at hand, and design a suitable network topology with resiliency, capacity, and survivability in mind.

Typically, organization networks today are a combination of manageable wired and wireless LANs, sometimes even remote LANs. Designed to fulfill most deployment needs, the two main categories of network topologies supported are:

- Layer 2 Topology
- Layer 3 Topology

Layer 2 Topology aims to build a managed Local Area Network (LAN) which consists of both wired and wireless capabilities to provide network services to a limited physical area such as office building, hotel, school premises, and etc.

- Always connect hierarchically. If there are multiple switches in a building, use an aggregation switch.
- Locate the aggregation switch close to the network core (e.g. mainframe housing)
- Locate edge switches close to users (e.g. one per floor)

Layer 3 Topology aims to build a managed Local Area Network (LAN) which consists of both wired and wireless capabilities to provide network services to local and remote physical areas such as enterprise buildings, hotel chains, college campuses, and etc.

- Always connect hierarchically whether in local LAN or remote LAN. If there are multiple switches in a building, use an aggregation switch.
- Locate the aggregation switch close to the network core (e.g. mainframe housing)
- Locate edge switches close to users (e.g. one per floor)
- Remote site's device (Edgecore AP or Edgecore EWS Controller) uplink should either have a public IP address or an IP address in the same subnet as the main EWS Controller's WAN IP address.

1.2 How to enable your Service Zone

Service Zone is a logic partition of WLAN controller's LAN. The concept of Service Zone is that it is a virtual gateway with customizable login portal page with its own gateway properties (such as VLAN tag, LAN IP address, DHCP server settings, authentication options, etc.). With up to nine independent Service Zone profiles, the WLAN controller is capable of servicing multiple hotspot franchises with a single device.

Administrators are able to check the Service Zone status from "*Main › System › Service Zone*" and click the hyperlink of Service Zone Name for further configuration about its own VLAN tag, LAN IP address, DHCP server settings, authentication options, etc. For more details, please refer to *“chapter 3 How to configure Service Zone.”*

1.3 How to add an User Accounts

Local User is a type of user whose account credential is stored in the WLAN controller’s built-in database named “Local”. The WLAN controller’s “Local” database capacity varies with different model. A local user account does not have an expiration date once they are created. If administrator wishes to delete local accounts, this must be done manually from the Web Management Interface.

Administrators are able to check the existed Local User Accounts from *“Main › Users › Internal Authentication › Local Authentication › Local User List”* and simply create one by clicking “Add” button with desired Username and Password. For more details, please refer to *“session 4.1.1 Local User Database”*

On-Demand User is a type of user whose account credential is stored in the WLAN controller’s built-in database named “On-Demand”. The WLAN controller’s “On-Demand” database capacity varies with different model. On-Demand User is designed for short term usage purpose; it has time or volume constraints and an expiration period. An On-Demand account record will be recycled for creating new On-Demand account if it has expired for over 15 days or has been deleted by the Administrator/Manager manually.

Administrators need to generate an On-Demand billing plan first form *“Main › Users › Internal Authentication › On-Demand Authentication › Billing Configuration”* by clicking the hyperlink of the billing plan number. Furthermore, administrators are able to check the existed On-Demand User Accounts from “*Main › Users › On-Demand Accounts › Account Creation”* and simply create one or multiple accounts by clicking “Create Single” or “Create Batch” button with desired Username and Password, respectively. For more details, please refer to *“session 4.1.2 On-Demand User Database” and “session 4.1.3 On-Demand Account Creation”*

1.4 How to add an Access Point

There are couples of methodology to add the access point into management by WLAN controller. It depends on what network topology it is. Simply, LAPM is for Layer 2 network topology (”session 7.2 AP adding and configuration”), WAPM without tunnel is for L3 network topology without client authentication (”session 8.3.1 AP discovery”), WAPM with complete tunnel is for L3 network topology with fully controlling clients traffic (”session 8.3.3 CAPWAP with complete tunnel”), while WAPM with split tunnel is for L3 network topology with authentication and traffic flow optimization(”session 8.3.4 CAPWAP with split tunnel”).

2 How to configure System Setup

2.1 System General Setting

This section relates to fundamental system configuration.

The *General* displays the following tabs:

- General Settings
- System Time

General Settings

System Name: This is a mnemonic name admin can give to the controller. Once configured, it will show on the web browser's frame.

Contact Information: This is the email, cell phone, or other means of contact, displayed on the clients' web browser in the event of internet disconnection.

HTTPS Certificate: HTTPS network certificate as site safety verification, which is able to be uploaded and selected from *"Utilities > Certificates > System Certificate, chapter 15.2"*.

User HTTPS Login: Presents the option to allow end users authenticated with HTTPS for encrypted content transfer. The *Disable* option indicates the user will be redirected to HTTP login page, while the *Enable* option to HTTPS login page. The *Secure* option supports only "High" encryption cipher suites i.e. SSLv3 and TLSv1.

HTTPS Automatic Redirects provides an option for allowing or denying HTTPS requests when a user first connects to a network. When enabled, HTTPS traffic will be redirected but may prompt a certificate security warning. When HTTPS is disabled, all HTTPS traffic is denied and will be timed-out. This option will effectively prevent all security warnings being shown on the user's devices. When HTTPS requests are timed-out, some browsers may automatically request a HTTP webpage to redirect to a Captive Portal.

- Enable HTTPS Automatic Redirect: users browsing with HTTPS may be shown a certificate security alert when browsing before they access the Captive Portal.
- Block HTTPS Automatic Redirect: users browsing with HTTPS will be timed-out, meaning their webpage will appear blank since they never reach their destination
- Bypass non-HTTP Traffic Prior to Sign-In: all HTTPS websites are allowed for browsing even though the user have not accepted the disclaimer page or completed the sign-in process on the Captive Portal.

Internal Domain Name: A fully qualified domain name (FQDN) of the system. Ideal for accessing the Controller instead of remembering the IP address of the LAN interfaces. When the administrator enters a desired domain name in the Internal Domain Name field, the entered Internal Domain Name will be shown in the URL of the Login Success page instead of a LAN IP address. In addition, when HTTPS is enabled, enter the domain name of the uploaded certificate will increase login speed and the URL in the User Login page will be changed. On the Social Media Login, this Internal Domain Name help redirect the login succeeded clients back the Login Success page.

Portal URL Exceptions (User Agent): The desired landing page may be directed after users' initial login except specific opened browsers listed here.

User Log Access IP Address: Once configured, user logs can only be accessed via the administrator matching the entered IP.

UAM Filter: The Universal Access Method (UAM) Filter drops non-browser http requests from user agents before authentication to prevent system overloading from excessive traffic.

Management IP Address List: This allows the network administrator to enter a selection of reserved IP addresses/ range that are authorized to see the Web Management Interface, which is configured in *"System > General > Management IP Address List, chapter2.2"*. The remote console interface is disabled by default.

SNMP: Presents an option to enable or disabled system info retrieval via SNMP protocal. Administrators can choose to assign specific port to transmit SNMP trap messages. Detailed thresholds such as CPU Usage, Memory Usage, DHCP Scope, and Heart Beat Period may be configured.

Suspend Warning Message: A field for administrator to enter the message to users when a Service Zone's service is temporarily suspended

System Time

Current Time: The system time right away following below configuration.

Time Zone: a dropdown list to select the local time zone the system is.

Time Update (NTP): The system completes automatic time synchronization by specifying external NTP servers in the order of NTP Server 1 to 5. The checkbox of *Use this controller as an NTP server* is checked by default so as to synchronize the time of managed-APs.

Time Update (Manually Set Up): The system time is manually configured.

2.2 WMI Management Access

The administrator can grant access to the WMI by specifying a list specific IP addresses or ranges of IP addresses, both from WAN or from LAN, in web-based or in console-based.

The *Management IP List* displays the following tabs:

- Management Service
- Management Service Zone List
- Management IP Address List

Management Service

SSH Service: The encrypted remote console interface in port 22. For security purposes, SSH Service is recommended to disable to prevent malicious users from accessing the system. However, if the remotely troubleshooting is required by Edgecore Support team, please help enable in advance.

Telnet Service: The non-encrypted remote console interface in port 23. For security purposes, Telnet Service is disabled by default to prevent malicious users from accessing the system.

Management Service Zone List
Given the enabled Service Zone(s), which is configured in *"System > Service Zone, chapter2.4"*, administrators could *Active* to let the devices matching the range of IP address could access the WMI of the system.

Management IP Address List
For remote access purpose, the IP Address/ Segment could be customized for the administrators to access the WMI of the system. Please confirm the entries are *Active* in the table by checking the checkboxes. For example, entering "192.168.3.1" and "192.168.1.0/24" means that only the device at 192.168.3.1 and devices in the range of 192.168.1.0 to 192.168.1.255 are able to reach the web management interface.

If administrators would like to type a specific IP address, there is not necessary to type the segment. (type 192.168.5.44, instead of 192.168.5.44/32)

2.3 WAN Configuration

The Edgecore EWS-series Gateway-Controllers have at least 2 physical WAN ports for supporting most ISP. To complete accessing the WAN IP address is important in the very beginning configuration.

The *WAN* screen displays the following tabs:

- WAN Configuration
- WAN2 Configuration
- WAN2 Functions

WAN Configuration
Physical Mode: a drop-down list allows administrators to choose the speed and duplex of the WAN connection. When Auto-Negotiation is ON, the system chooses the highest performance transmission mode (speed/duplex/flow control) that both the system and the device connected to the interface support.
Static: Manually specifying the IP address of the WAN port.
Dynamic: It is only applicable for a network environment where the DHCP server is available in the upstream network. Renew button to get an IP address automatically.
PPPoE: It is for PPPoE dialup connection provided by your ISP, and the ISP will issue you an account with a password so as to complete the configuration.
PPTP: Some IPSs (in European countries) may provide PPTP protocol for dialup connection. The issued PPTP account and password for PPTP server are required.
Transmission Option (EWS5204, EWS5207 only): Edgecore carrier grade models designed with SFP fiber ports, which could be configured as

- Ether Port: Deploy the copper Ethernet WAN port for service.
- Fiber Port: Deploy the SFP fiber port for service.

- Fiber Port and Ether Port: Bridge Fiber port and Ethernet port, physically only connect one uplink either via SFP port or Ether port.
- Bonding: Deploy both SFP port and copper Ethernet port for service. This option aggregates the two connections and will result in aggregated higher throughput.

WAN2 Configuration

Physical Mode: a drop-down list allows administrators to choose the speed and duplex of the WAN connection. When Auto-Negotiation is ON, the system chooses the highest performance transmission mode (speed/duplex/flow control) that both the system and the device connected to the interface support.

Static: Manually specifying the IP address of the WAN port.

Dynamic: It is only applicable for a network environment where the DHCP server is available in the upstream network. Renew button to get an IP address automatically.

PPPoE: It is for PPPoE dialup connection provided by your ISP, and the ISP will issue you an account with a password so as to complete the configuration.

Transmission Option (EWS5204, EWS5207 only): Edgecore carrier grade models designed with SFP fiber ports, which could be configured as

- Ether Port: Deploy the copper Ethernet WAN port for service.
- Fiber Port: Deploy the SFP fiber port for service.
- Fiber Port and Ether Port: Bridge Fiber port and Ethernet port, physically only connect one uplink either via SFP port or Ether port.
- Bonding: Deploy both SFP port and copper Ethernet port for service. This option aggregates the two connections and will result in aggregated higher throughput.

WAN Traffic Settings

Bandwidth Limitation: Disable by default. The limitation is combined for both WAN1 and WAN2, while the bandwidth is still bounded by the network speed of the ISP operator.

Function of WAN2: these functions only when WAN2 is enabled

- Disable: WAN2 acts as another uplink for the system without Load Balancing and WAN Failover
- Load Balancing: Select the option for administrator to spread the system traffic across WAN1 and WAN2 ports based on percentage load, calculated using session, bytes, or packets.
- WAN Failover: Select the option for WAN2 taking into service the traffic originally handled by WAN1 if WAN1 is down. If the nested option is selected, service will be returned to WAN1 link if it is up again. This feature is not available to be used concurrently with Load Balancing.

Address for Detecting Internet Connection: Up to three outbound sites as detection target for verifying whether the uplink service is alive or down. A field of warning message text may be customized which will be displayed on the user’s web browser when all three detecting targets fail to respond.

2.4 LAN Configuration

The LAN of WLAN controller is managed by Edgecore unique Service Zone, which is configured in *"System > Service Zone, chapter2.4"*, while administrators could decide one of the Service Zone modes to serve in this page.

The *LAN* screen displays the following tabs:

- LAN Ports
- Management Port

Note: If HA feature is in *Enabled* status, LAN1 will be transformed into a dedicated HA port and will not be able to service any Service Zone.

LAN Ports

LAN Port Mode: select the option for identifying the port and Service Zone mapping

- Port-based: Each physical LAN port can be mapped to an enabled Service Zone or disabled from providing service. Noted that the maximum amount of Service Zones available to actually provide service is determined by the number of LAN ports on the Controller.
- Tag-based: Different Service Zones are identified by VLAN ID no matter which physical LAN ports. This means that Tag-Based mode dynamically maps a client to a Service zone based on the VLAN ID tagged on the traffic packet.

Port – Service Zone Mapping: the configuration of the physical LAN port by enabled Service Zone when Port-based mode is selected.

Management Port (EWS5204, EWS5207 only)

An open WMI available in default IP 172.30.0.1/16 when administrators connect to the physical MGMT port.

2.5 Advanced features in System

There are several powerful features applied for different advanced application. For details on a specific page, refer to the appropriate chapter

- High Availability (HA), refer to "*chapter 12 High Availability*"
- PMS Interface, refer to "*chapter 14 PMS Integration*"
- Utilities for WLAN Controller, refer to "*chapter 15 Utilities for WLAN Controller*"
- Advanced Settings for Network Environment, refer to "*chapter 16 Advanced Settings for Network Environment*"

3 How to configure Service Zone

Service Zones are virtual partitions of the physical LAN side of a Edgecore Controller. Similar to VLANs, they can be separately managed and defined, having their own user landing pages, network interface settings, DHCP servers, authentication options, policies and security settings, and so on. By associating a unique VLAN Tag (when it is tag-based) and an SSID with its Service Zone, administrator can flexibly separate the wired and wireless networks easily.

There are dozens of features for each Service Zone

- VLAN, Isolation, NAT/Router Mode
- DHCP Server Option
- Authentication Settings
- Page Customization

3.1 VLAN/IP, Isolation, NAT/Router Mode

VLAN/IP
IP address will act as the Controller IP to a user connected to this Service Zone. Subnet mask defines the size of your Service Zone network and defines the range of IP's allowed to access this Service Zone. To allow users using addresses that are out of range, enter the IP's in the Network Alias List and check Enable. Always remember to click Apply upon completion.

Isolation

- Inter-VLAN Isolation: 2 clients within the same VLAN will not see each other when coming in from different ports. Note that Isolation is done when traffic passes through the gateway. When a switch or AP is being deployed, Station Isolation has to be enabled on the AP/switch.
- Clients Isolation: All clients on the same Layer 2 network are isolated from one another in this Service Zone.
- None: No isolation will be applied to clients in this Service Zone.

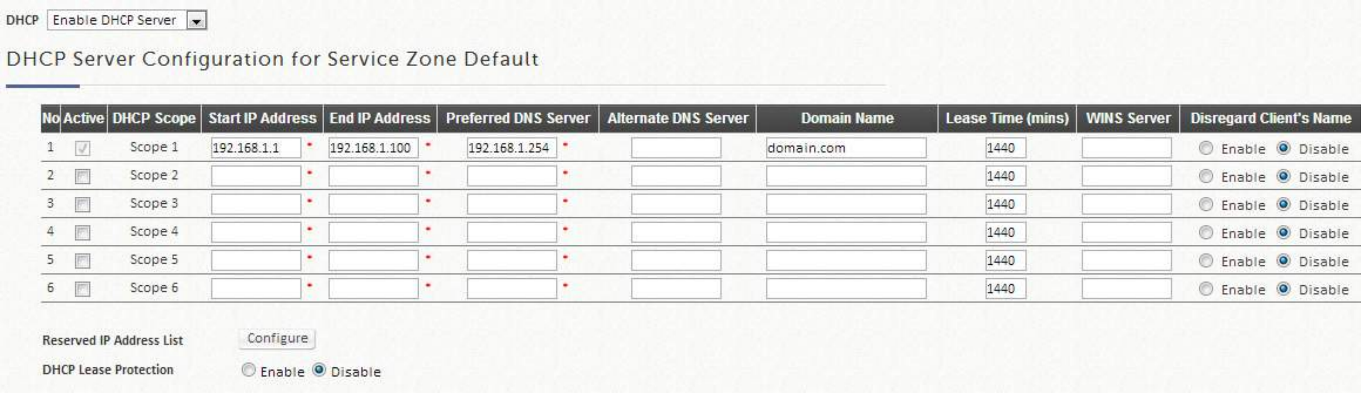
Note that when "None" is selected, a switch port connecting to the LAN port of the WLAN controller may be shut down if the switch has loop protection enabled and there are more than 2 VLANs belong to one Service Zone.

NAT/Router Mode
NAT is the acronym for Network Address Translation which translates private IP addresses for devices on the LAN side of a controller to routable IP before forwarding into uplink network. Private IP addresses are invisible to devices or routers on the WAN side of the controller, only the controller deploying the NAT knows their corresponding translation. This mode not only protects users on the LAN from being 'seen' by external devices but also solves the problem of limited public IP's.

Router mode as the name suggests, is a network operating without address translation in and out of the Controller. Router mode is selected when using public IP or under circumstances where the downstream devices requires a routable IP address to upstream routers.

3.2 DHCP Server Option

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network. WLAN controllers supports independent DHCP settings for each Service Zone profile. Options include Disable DHCP option, Enable built-in DHCP server or DHCP Relay.



DHCP: Enable DHCP Server

DHCP Server Configuration for Service Zone Default

No	Active	DHCP Scope	Start IP Address	End IP Address	Preferred DNS Server	Alternate DNS Server	Domain Name	Lease Time (mins)	WINS Server	Disregard Client's Name
1	☑	Scope 1	192.168.1.1 *	192.168.1.100 *	192.168.1.254 *		domain.com	1440		○ Enable ● Disable
2	□	Scope 2	*	*	*			1440		○ Enable ● Disable
3	□	Scope 3	*	*	*			1440		○ Enable ● Disable
4	□	Scope 4	*	*	*			1440		○ Enable ● Disable
5	□	Scope 5	*	*	*			1440		○ Enable ● Disable
6	□	Scope 6	*	*	*			1440		○ Enable ● Disable

Reserved IP Address List: Configure

DHCP Lease Protection: ○ Enable ● Disable

- DHCP Server Configuration – The default setting for DHCP Server is “Enable”. Select other options from the drop-down list.
- Define the IP range for issuing when using Enable DHCP Server (built-in). There are a total of six DHCP pools for configuration.
- Lease Time at each pool cannot be smaller than the twice value of Idle Timeout.
- Reserving IP addresses – A configuration list for reserving certain IP’s within the DHCP Server IP range for specific devices, for example an internal file server.
- DHCP lease protection – This is an optional checking mechanism on the Controller when Enabled, will check to see if the lease expired IP is currently online. If yes, the Controller will halt the issuing of this IP address until the user session terminates.
- Click “Apply” to activate changes.

3.3 Authentication Settings

Once the administrator has properly configured the authentication servers under the Main Menu, each Service Zone can select the authentication option preferred to downstream clients for login. Note that Authentication is always enabled by default.

Authentication Options: Administrators can designate configured auth servers for use. Postfix will be used as auth server identifier when more than one auth server is enabled for service.
Portal URL: The specification of a desired landing page may be configured here. When enabled, the administrator can choose to set the URL of an opened browser after users' initial login.
MAC Authentication: RADIUS MAC authentication feature once enabled, if the connected device has its MAC address entered in the configured RADIUS Server, the Controller will automatically authenticate and grant access immediately if authentication succeeds. Users will experience transparent login.
PPP Authentication: Point-to-Point Protocol (PPP) is a data link protocol commonly used in establishing a direct connection between two networking nodes. When this feature is enabled for service, end users may configure a dial-up connection setting with a valid username and password (support only Local and RADIUS users). Once the dial-up connection has been established, the user would have been authenticated successfully without further UAM login.
IP Address Range Assignment field configures the starting IP range which PPP can assign IP addresses to dial-up virtual interfaces. The assigned interface IP address is used to route between the networks on both side of the tunnel.

3.4 Page Customization

Each Service Zone can be configured to have unique Login Pages or Message Pages. There are 3 types of Login Pages: The General Login Page, PLM Open Type Login Page (for Port Location Mapping free access), and PMS Billing Plan Selection Page. A Service Disclaimer page can be enabled if required. These pages are fully customizable to give administrators complete flexibility. Message Pages can also be customized and message pages include: Login Success Pages, Login Success Page for On-Demand Users, Login Fail Page, Device Logout Page, Logout Success Page, Logout Failed Page, and Online Device List.

There are three customization options to choose from apart from the Edgecore Default Page: Customize with Template, Upload Your Own, and Use External Page.

Edgecore Default: The gateway has a standard Edgecore Default Login Page with the Edgecore logo and Administrators can choose to enable a Service Disclaimer if needed.
Customize with Template: For this option, a template is prepared for the administrator's easy customization. The general layout has been set for the administrator but the contents can be customized to his preference. A color theme and a logo can be uploaded, and contents field such as Service Disclaimer, text colors can entered within the template presentation layout.
Upload Your Own: The Administrator has the option to upload a html file as the Login Page. The "Download HTML Sample File" gives administrators a sample HTML code to edit from. Once this sample HTML code is downloaded, open the file with any browser, right click and select "View Page Source". You may edit the HTML code with any text editor as long as the file is saved in .html format.
Use External Page: The Login Page can be a defined external URL. This option requires extensive knowledge of URL parameter utilization that works together with the Message Pages and should be organized carefully. For more details on External Login Page customization, please refer to the Technical Guide.

For a Preview of the custom page, click “Apply” followed by the “Preview” button. Similarly, the four options are available for Message Pages.

4 How to enable User Authentication Databases

4.1 Internal Authentication

Internal authentication database is a storage device where users' credentials in the system may be inquired for validity. Each type has its own application in different scenarios

- Local User Database
- On-Demand User Database
- Guest User Database

4.1.1 Local User Database

This type of authentication method checks the local database that stores user, often the staff and credentials internally. The Local user database is designed to store static accounts which will not be deleted unless manually performed by administrator.

Local User List

- Add: To create one or multiple accounts with account information, including Username, Password, MAC Address, Group, Account Span, and Remark

Note:

1. The fields with red asterisk are mandatory fields while the others are optional.
2. MAC Address field once configured will bind this particular account under the condition that it may only be granted access using the device specified.
3. The Group field specifies the group profile of the account being created.
4. Remark is for any additional note administrator would like to stress. It will be shown on the user list.
5. You can check the Enable Local VPN checkbox to build up a secure VPN tunnel between the device using the account and the controller.
6. Expiration is optional time constraints which may be enforced to this account if the Account Span option is checked. This is a useful attribute if used in complement with Multiple Login, ideal to provide network access to a group of people for a specified amount of time, for instance during a seminar event.

- Delete: To deleted individually or entirely by selecting the "Select All" checkbox
- Backup: To export user credentials as a text file in csv format in a new window.
- Upload: To import the accounts back into the Local user database which is a convenient way to create a great amount of Local accounts.
- Edit Account Information: For existing user accounts, further modification is possible simply by clicking the username hyperlink on the page to reconfigure account attributes.

Note:

1. The txt files generated may be inter-used by all WLAN controller series as the defined csv format is consistent for all models.
2. Duplicated accounts will result in upload failure and a warning message will be displayed.

Account Roaming Out
802.1X Authentication

4.1.2 On-Demand User Database

The On-Demand user database is designed for guest user account provisioning with time or traffic volume constraints. Ideal for deployment needs of Hotels, Hotspot venues, Enterprise visitor reception, and more. The On-Demand Authentication option offers plenty of options for customization. POS/Web tickets can be customized to businesses' needs, and multiple payment options are also available on the WLAN controllers.

- On-Demand Billing Plans
- On-Demand Authentication
- Web Printout
- POS Tickets and Terminal Server
- Payment Gateway
- SMS Gateway
- Email Verification
- Account Roaming Out

On-Demand Billing Plans
Usage-time: Users can access internet as long as account is valid with remaining quota (usable time). Users need to activate the purchased account within a given time period by logging in. This is ideal for short term usage such as in coffee shops, airport terminals etc. Quota is deducted only while in use, however the count down to Expiration Time is continuous regardless of logging in or out. Account expires when *Expiration* has been used up or quota depleted as expiration time is enabled,

- Activation is the time period for which the user must execute a first login. Failure to do so in the time period set in Account Activation will result in account expiration.
- Expiration is the valid time period for using. After this time period, even with remaining quota the account will still expire.
- Quota is the total period of time (xx *days* yy *hrs* zz *mins*), during which On-Demand users are allowed to access the network. The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeeming.
- Unit Price is the unit price of this plan.
- Group will be the applied Group to users created from this plan.

- Reference field allows administrator to input additional information.

Volume: Users can access internet as long as account is valid with remaining quota (traffic volume). Account expires when *Valid Period* is used up or quota is depleted. This is ideal for small quantity applications such as sending/receiving mail, transferring a file etc. Count down of Valid Period is continuous regardless of logging in or out.

- Activation is the time period for which the user must execute a first login. Failure to do so in the time period set in Account Activation will result in account expiration.
- Expiration is the valid time period for using. After this time period, the account expires even with quota remaining.
- Quota is the total Mbytes (1~$_{1000000}$), during which On-Demand users are allowed to access the network.
- Number of devices is to define the number of allowed simultaneous logged in devices per account. (0: unlimited)
- Unit Price is the unit price of this plan.
- Group will be the applied Group to users created from this plan.
- Reference field allows administrator to input additional information.

Hotel Cut-off-time is the clock time (normally check-out time) at which the On-demand account is cut off (made expired) by the system on the following day or many days later.

- Cut-off Time: On the account creation UI of this plan, operator can enter a Unit value which is the number of days to Cut-off-time according to customer stay time. For example: Unit = 2 days, Cut-off Time = 13:00 then account will expire on 13:00 two days later.
- Grace Period is an additional, short period of time after the account is cut off that allows user to continue to use the On-Demand account to access the Internet without paying additional fee.
- Number of Devices is to define the number of allowed simultaneous logged in devices per account.
- Unit Price is a daily price of this billing plan. This is mainly used in hotel venues to provide internet service according to guests' stay time.
- Group will be the applied Group to users created from this plan.
- Reference field allows administrator to input additional information.

Duration Time with Elapsed Time: Account is activated upon account creation. Count down begins immediately after account is created and is continuous regardless of logging in or out. Account expires once the *Elapsed Time* is reached. This is ideal for providing internet service immediately after account creation throughout a specific period of time.

- Begin Time is the time that the account will be activated for use. It is set to account creation time.
- Elapsed Time is the time interval for which the account is valid for internet access (xx *hrs* yy *mins*).
- Number of Devices is to define the number of allowed simultaneous logged in devices per account.
- Price is the unit price of this plan.
- Group will be the applied Group to users created from this plan.
- Reference field allows administrator to input additional information.

Duration Time with Cut-off Time: It is the clock time at which the On-Demand account is cut off (made expired) by the system on that day. For example if a shopping mall is set to close at 23:00; operators selling On-Demand tickets can use this plan to create ticket set to be Cut-off on 23:00. If an account of this kind is created after the Cut-off Time, the account will automatically expire.

- Begin Time is the time that the account will be activated for use. It is set to account creation time.
- Cut-off Time is the clock time when the account will expire.
- Number of Devices is to define the number of allowed simultaneous logged in devices per account.
- Price is the unit price of this plan.
- Group will be the applied Group to users created from this plan.
- Reference field allows administrator to input additional information.

Duration Time with Begin-and-End Time: The *Begin Time* and *End Time* of the account are defined explicitly. Count down begins immediately after account activation and expires when the *End Time* has been reached. This is ideal for providing internet service throughout a specific period of time. For example during exhibition events or large conventions such as Computex where each registered participant will get an internet account valid from 8:00 AM Jun 1 to 5:00 PM Jun 5 created in batch like coupons.

- Begin Time is the time that the account will be activated for use, defined explicitly by the operator.
- End Time is the time that the account will expire defined explicitly by the operator.
- Number of Devices is to define the number of allowed simultaneous logged in devices per account.
- Price is the unit price of this plan.
- Group will be the applied Group to users created from this plan.
- Reference field allows administrator to input additional information.

On-Demand Authentication

User Postfix: The User Postfix is used for the system to identify which authentication option will be used for the specific user account when multiple options are concurrently in use

Currency: to indicate the price of each On-Demand credential

Expired Account Cache: the day to eliminate the On-Demand accounts from database since which have been expired already

Out-of-quota Account Cache: the day to eliminate the On-Demand accounts from database since which have been out of quota already

Web Printout

When printers, except POS printer, are deployed for account generation, there is a set of Wi-Fi service information for customizing the On-Demand tickets, including Background Image, WLAN SSID Name, Wireless Key, Receipt header and Receipt footer. Simply click the “Preview” button to check the layout and then press “Printout” button for laptop printout setting.

POS Tickets and Terminal Server

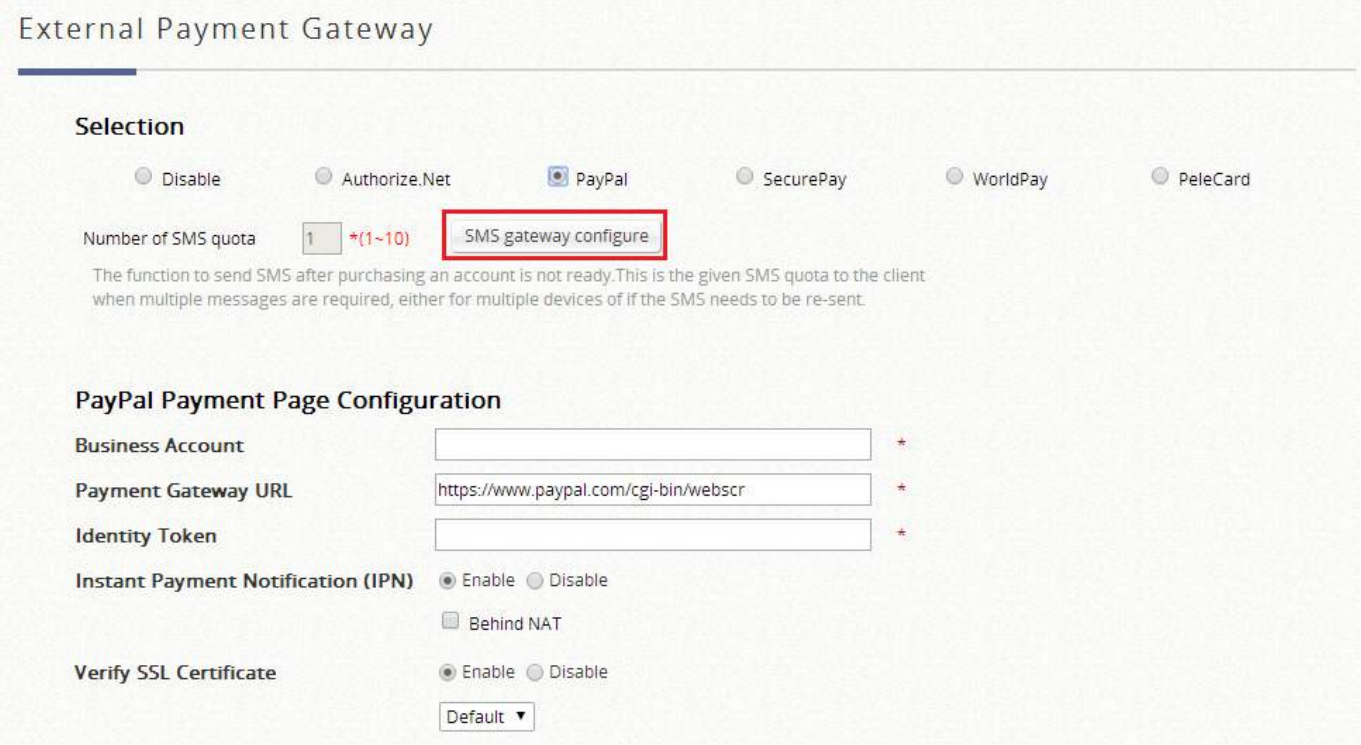
When Terminal Servers (such as the SDS200W) are deployed for account generation, remember to configure the IP and Port in Terminal Server configuration.

Payment Gateway

The WLAN controller supports different types of payment gateway options depending on the account types possessed by the operator, including Authorize.net, PayPal, SecurePay, WorldPay, and PeleCard. The most commonly used PayPal is used as an illustration example below.

Before setting up "PayPal", it is required that the hotspot owners have a valid PayPal "Business Account". After opening a PayPal Business Account, the hotspot owners should find the "Identity Token" of this PayPal account to continue "PayPal Payment Page Configuration".

Fill in the necessary merchant account credentials in the Payment Page Configuration. Please be careful that if your controller's WAN IP is under a NAT, you will need to configure IP forwarding information in the Instant Payment Notification (IPN) field in order for the paying end user to receive transaction outcome.



External Payment Gateway

Selection

○ Disable ○ Authorize.Net ● PayPal ○ SecurePay ○ WorldPay ○ PeleCard

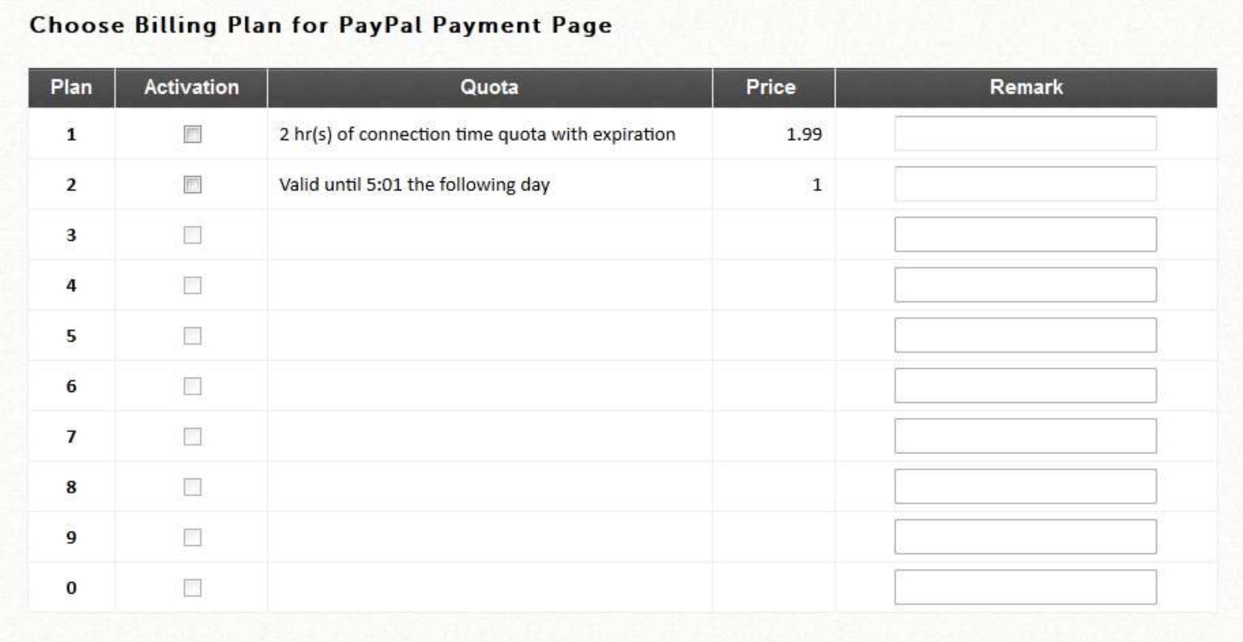
Number of SMS quota: 1 *(1~10)

The function to send SMS after purchasing an account is not ready.This is the given SMS quota to the client when multiple messages are required, either for multiple devices of if the SMS needs to be re-sent.

PayPal Payment Page Configuration

Business Account	*
Payment Gateway URL	https://www.paypal.com/cgi-bin/webscr *
Identity Token	*
Instant Payment Notification (IPN)	● Enable ○ Disable □ Behind NAT
Verify SSL Certificate	● Enable ○ Disable Default ▼

Select the enabled billing plans that are allowed for end users to self-purchase through the payment gateway.

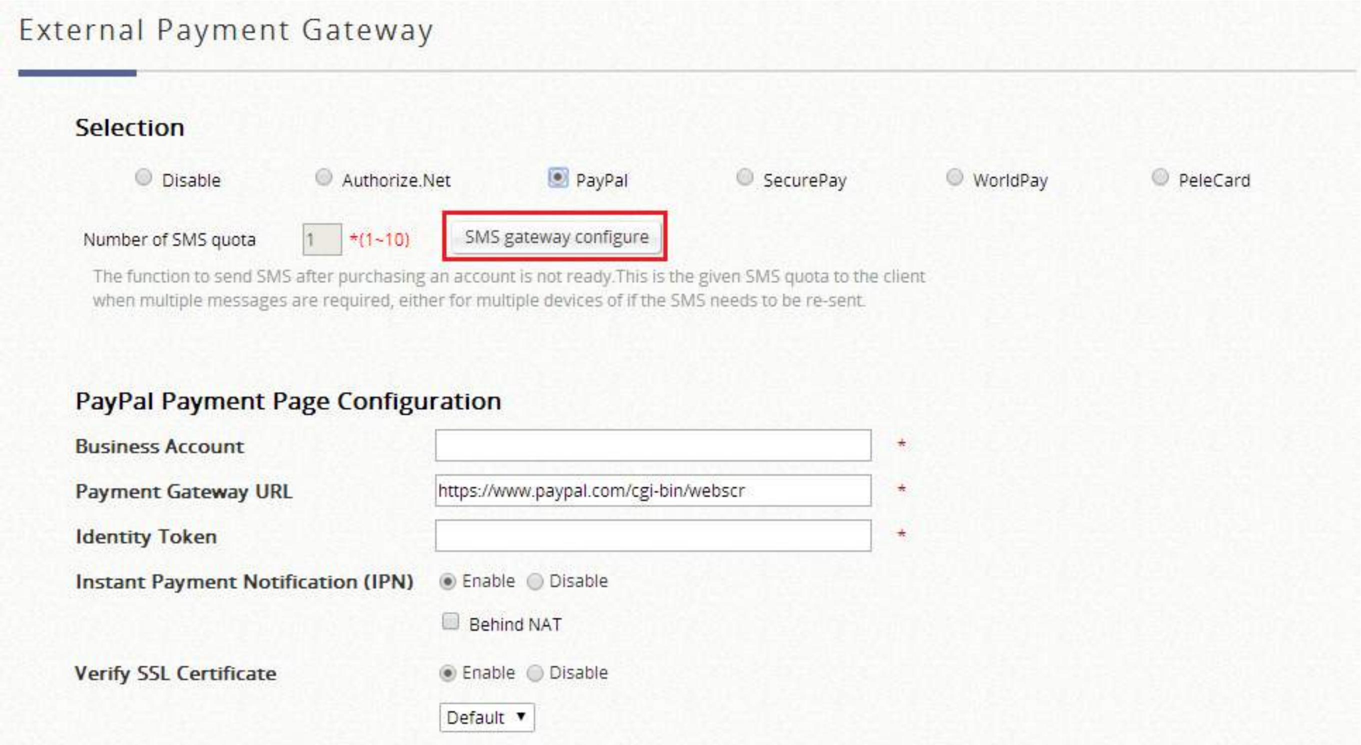


Choose Billing Plan for PayPal Payment Page

Plan	Activation	Quota	Price	Remark
1	□	2 hr(s) of connection time quota with expiration	1.99	
2	□	Valid until 5:01 the following day	1	
3	□			
4	□			
5	□			
6	□			
7	□			
8	□			
9	□			
0	□			

The service disclaimer can be customized by configuring Web Page Customization.
Subsequently after the configuration of your external payment gateway, the login page will be shown with a hyperlink which guides the end user step by step to purchase an account with a valid credit card.

In order for users to get account info via SMS after buying a new account online, and eliminate the risk of forgetting his/her username and password at the next time of login, administrators may choose to integrate SMS gateway with the payment gateway.



External Payment Gateway

Selection

○ Disable ○ Authorize.Net ● PayPal ○ SecurePay ○ WorldPay ○ PeleCard

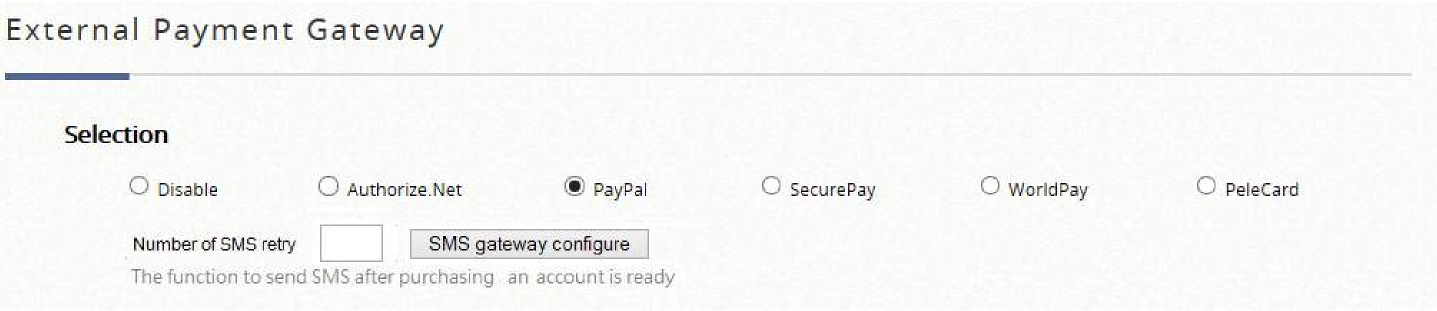
Number of SMS quota 1 *(1~10) SMS gateway configure

The function to send SMS after purchasing an account is not ready.This is the given SMS quota to the client when multiple messages are required, either for multiple devices of if the SMS needs to be re-sent.

PayPal Payment Page Configuration

Business Account	*
Payment Gateway URL	https://www.paypal.com/cgi-bin/webscr *
Identity Token	*
Instant Payment Notification (IPN)	● Enable ○ Disable □ Behind NAT
Verify SSL Certificate	● Enable ○ Disable Default ▼

Upon successful set up, the Number of SMS Quota field will be available.



External Payment Gateway

Selection

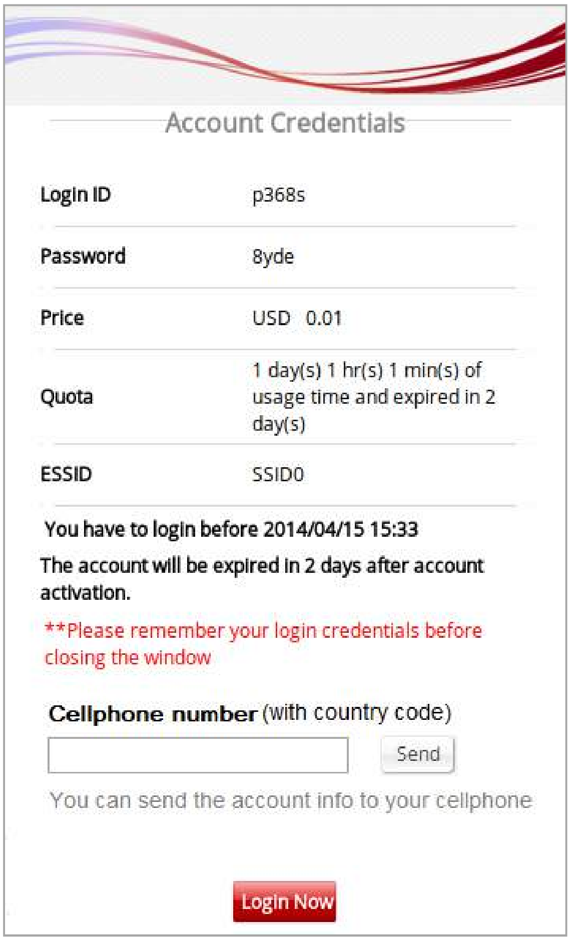
○ Disable ○ Authorize.Net ● PayPal ○ SecurePay ○ WorldPay ○ PeleCard

Number of SMS retry

The function to send SMS after purchasing an account is ready

Account buyers enter a cellphone number after paying a fee for the account online. The account buyers can then re-send the SMS no more than the configured number.

To preview your External Payment Portal, click “Configure” for Web Page Customization at the bottom of the page. Just like all customizable web pages in the system, this page also supports customization with templates, uploading html, or using an external page. An example of what will be displayed when External Payment Gateway is used with SMS Gateway is shown below:



Account Credentials

Login ID	p368s
Password	8yde
Price	USD 0.01
Quota	1 day(s) 1 hr(s) 1 min(s) of usage time and expired in 2 day(s)
ESSID	SSID0

You have to login before 2014/04/15 15:33

The account will be expired in 2 days after account activation.

**Please remember your login credentials before closing the window

Cellphone number (with country code)

You can send the account info to your cellphone

SMS Gateway

With a set of Clickatell account Username/Password, the SMS Gateway can be configured to send SMS messages upon On-Demand account creation. The SMS service can be used for free access, paid access with payment gateway integration, or both. Define an API ID and activate the desired billing plans. Multiple Billing Plans may be activated if needed. To prevent the SMS Gateway from being flooded by SMS queries for account generation, an Account Registration Control option is available. In addition, the administrator has an option of allowing or disallowing users to register for new accounts prior to account expiration. To block valid accounts from requesting new accounts, set option to "Enabled".

Clickatell

Selection: Disabled, Clickatell or SMS API. Choose the preferred service and option.

Version: Old (Prior to November 2016) version is the Clickatell API in REST protocol in JSON format for API ID, User Name, Password. New version is only required API Key in HTTPs protocol for integration

Send SMS for – Account Registration: to allow Wi-Fi users to self-register and receive a Wi-Fi account via SMS.

Send SMS for – Account purchases via Payment Gateway: to enable the SMS feature for Wi-Fi users who purchased an On-Demand account via an online Payment Gateway. They will be given an option to send the purchased account to their mobile device using SMS.

Send SMS for – Both: to enable the above two options

API URL: The link for sending an SMS request to the Clickatell API server. Default is http://api.clickatell.com/http/sendmsg

Registration before Accounts Expired: Allow will allow the same mobile number to request a 2nd On-Demand account even though the 1st account hasn't expired or been used yet. Block will restrict users to sending a 2nd On-Demand account only after their 1st account has expired.

Billing Plans: Created and "Active" Billing Plans are displayed and used for creating On-Demand account via SMS. Noted that at least 1 Billing Plan must be selected.

Account Registration Control: Disable, Black List, White List. Disable to not restrict or allow only specified mobile numbers. Black List will deny specific mobile numbers from registering. White List will only allow specific mobile numbers to register.

Web Page Customization: Customize the Service Disclaimer and Billing Plan Selection Page using the Default, Customize with Template, Upload Your Own and Use External Page options.

SMS API

Selection: Disabled, Clickatell or SMS API. Choose the preferred service and option.

Send SMS for – Account Registration: to allow Wi-Fi users to self-register and receive a Wi-Fi account via SMS.

Send SMS for – Account purchases via Payment Gateway: to enable the SMS feature for Wi-Fi users who purchased an On-Demand account via an online Payment Gateway. They will be given an option to send the purchased account to their mobile device using SMS.

Send SMS for – Both: to enable the above two options

API URL: The link for sending an SMS request to an API server.

Registration before Accounts Expired: Allow will allow the same mobile number to request a 2nd On-

Demand account even though the 1st account hasn't expired or been used yet. Block will restrict users to sending a 2nd On-Demand account only after their 1st account has expired.

Parameter: API parameters and values for sending an SMS request.

Response Format: JSON or HTML. Selected choice will depend on the type of response provided by the SMS service. The Response Format will be used by the WLAN controller to determine whether the SMS text message has been sent successfully.

Key of JSON Array: Key Path of the value from the SMS request's response in JSON format. Example: ['data'][0]['status']

Return Value of Successful Request: The text of the successful response is entered here.

Send Test Message: A mobile number is entered and a "test" SMS message is sent. On-Demand accounts will not be created when sending the SMS message. Noted that the "Test" button can be used to troubleshoot your SMS request and view the response message sent from your SMS provider.

Message Content: Customize the SMS Text Message received by Wi-Fi users in the Message Editor box. Four parameters regarding the created On-Demand account can be entered; the username, username without the postfix, password, and the quota description.

Parameter	Definition
$username	Username of the created On-Demand account.
$Username_without_postfix	Same as $username, but without the postfix.
$password	Password of the created On-Demand account.
$quota	Quota description for the created On-Demand account.

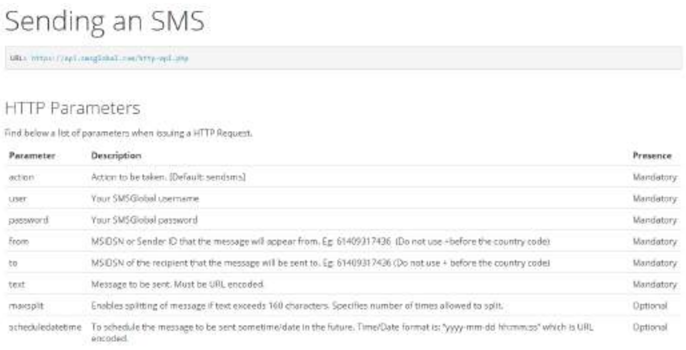
Billing Plans: Created and "Active" Billing Plans are displayed and used for creating On-Demand account via SMS. Noted that at least 1 Billing Plan must be selected.

Account Registration Control: Disable, Black List, White List. Disable to not restrict or allow only specified mobile numbers. Black List will deny specific mobile numbers from registering. White List will only allow specific mobile numbers to register.

Web Page Customization: Customize the Service Disclaimer and Billing Plan Selection Page using the Default, Customize with Template, Upload Your Own and Use External Page options.

SMS API Log: a helpful log during the integration on the page of *Main › Status › Logs and Reports › SMS API Log*

Taking the SMS Global as example, the WLAN controller is able to follow the SMS API indication from SMSGlobal website (HTTP API) https://www.smsglobal.com/http-api/?_ga=2.178049571.763118347.1504837619-1430890374.1504837619.



Sending an SMS

URL: https://api.smsglobal.com/http-api.php

HTTP Parameters

Find below a list of parameters when issuing a HTTP Request.

Parameter	Description	Presence
action	Action to be taken. [Default: sendsms]	Mandatory
user	Your SMSGlobal username	Mandatory
password	Your SMSGlobal password	Mandatory
from	MSIDSN or Sender ID that the message will appear from. Eg: 61409317436 (Do not use +before the country code)	Mandatory
to	MSIDSN of the recipient that the message will be sent to. Eg: 61409317436 (Do not use + before the country code)	Mandatory
text	Message to be sent. Must be URL encoded.	Mandatory
maxsplit	Enables splitting of message if text exceeds 160 characters. Specifies number of times allowed to split.	Optional
scheduledatetime	To schedule the message to be sent sometime/date in the future. Time/Date format is: "yyyy-mm-dd hh:mm:ss" which is URL encoded.	Optional

API URL: https://www.smsglobal.com/http-api.php

Registration before Accounts Expired: Allow

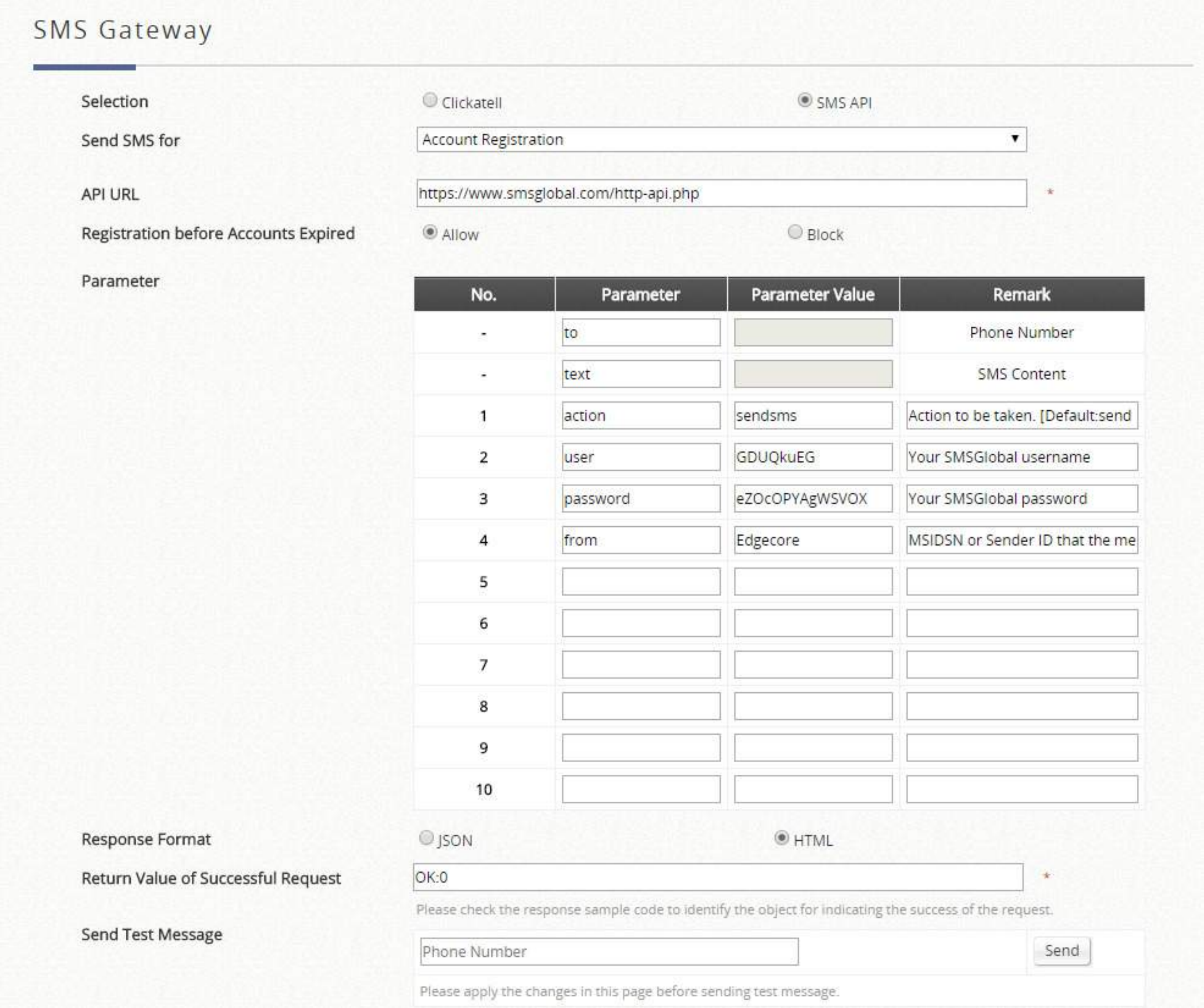
Parameter

No.	Parameter	Parameter Value	Remark
-	to		Phone Number
-	Text		SMS Content
1	Action	sendsms	Action to be taken. [Default: sendsms]
2	User	G*******	Your SMSGlobal username
3	Password	eZ************	Your SMSGlobal password
4	from	Edgecore	MSIDSN or Sender ID that the message will appear from. Eg: 61409317436 (Do not use +before the country code)

Response Format: HTML (due to we integrate with HTTP API)

Return Value of Successful Request: OK: 0

Send Test Message: this help verify the integration with current configuration



SMS Gateway

Selection ○ Clickatell ● SMS API

Send SMS for: Account Registration ▾

API URL: https://www.smsglobal.com/http-api.php *

Registration before Accounts Expired ● Allow ○ Block

Parameter

No.	Parameter	Parameter Value	Remark
-	to		Phone Number
-	text		SMS Content
1	action	sendsms	Action to be taken. [Default:send
2	user	GDUQkuEG	Your SMSGlobal username
3	password	eZOcOPYAgWSVOX	Your SMSGlobal password
4	from	Edgecore	MSIDSN or Sender ID that the me
5			
6			
7			
8			
9			
10			

Response Format ○ JSON ● HTML

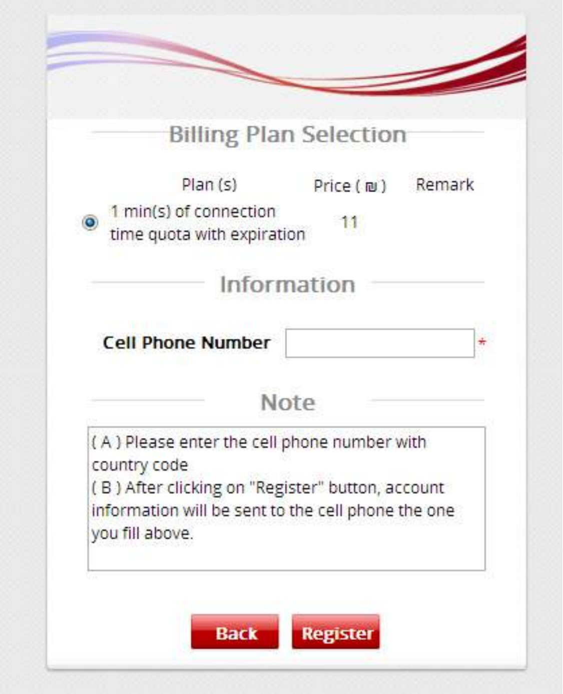
Return Value of Successful Request: OK:0 *

Please check the response sample code to identify the object for indicating the success of the request.

Send Test Message: Phone Number

Please apply the changes in this page before sending test message.

With the SMS Gateway enabled, the Billing Plan selection page will appear as such



Billing Plan Selection

Plan (s)	Price (₪)	Remark
● 1 min(s) of connection time quota with expiration	11	

Information

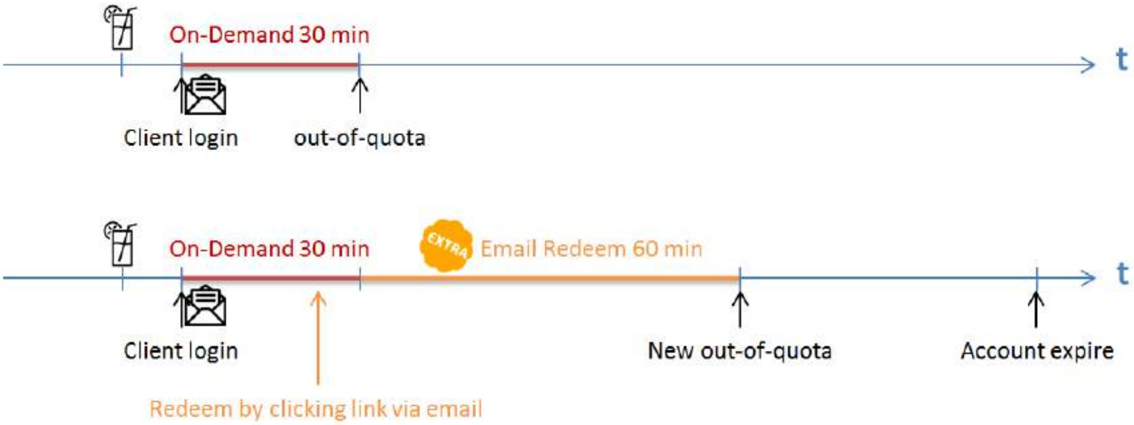
Cell Phone Number *

Note

(A) Please enter the cell phone number with country code
(B) After clicking on "Register" button, account information will be sent to the cell phone the one you fill above.

Email Verification

For email verification option, clients are able to access additional quota of On-Demand accounts by activating the link sent to clients' mail box. What's more, administrators could check the Logs and Reports to realize what the client status and related information for further marketing purposes.



Selection: to enable or disable the feature

Choose Billing Plan for Redeeming Account via Email (only Usage Time Selectable): to choose the configured billing plans, while only Usage type billing plan support this feature

- Activation: to select which billing plan allowed email verification feature
- Quota: to view the current summary of each billing plan
- Redeem Quota: the usage time that can be additionally used when redeeming
- Price: to view the current price of each billing plan
- Remark: a custom field for identity of each walled garden entry

SMTP Server Settings: to assign SMTP server for sending the mail for redeem clients. This SMTP is shared with Guest Email Verification. Please refer to "*session 17.5.1 SMTP Setting*". Taking Gmail as SMTP server, the configurations are

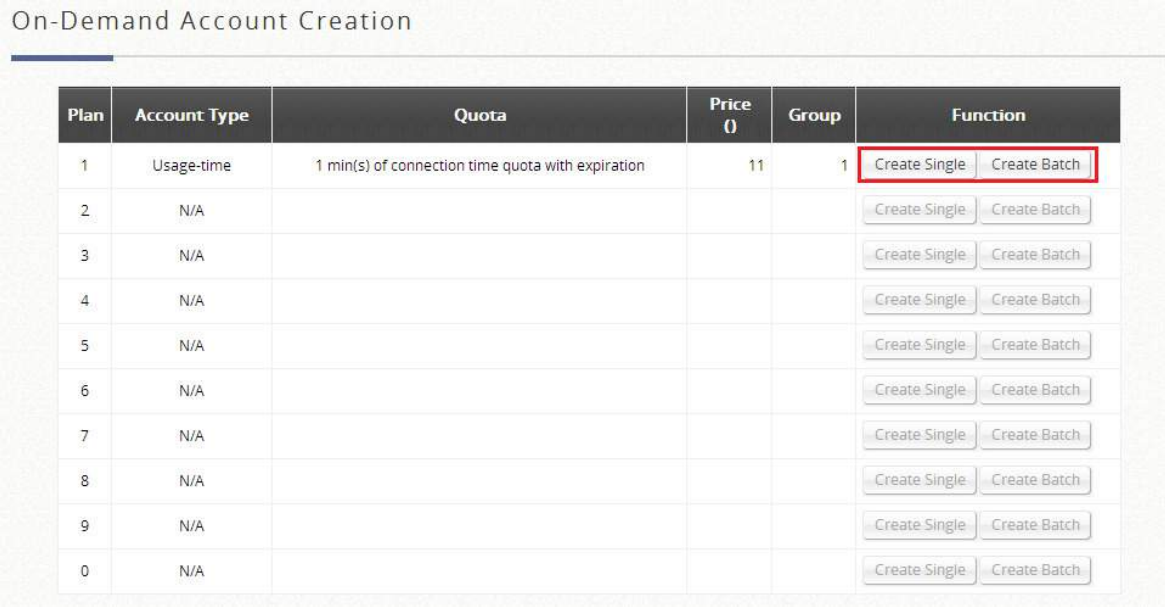
- SMTP server address: smtp.gmail.com
- SMTP port: 465
- Encryption: SSL
- Authentication: Login: Account Name: admin's Gmail email address
- Authentication: Login: Password: admin's Gmail email's password
- Sender Email Address: admin's Gmail email address

Sender Name: The Sender Name displays in the client mail box.
Activation Email Subject: customizable email subject displays in the client mail box
Activation Email Content: customizable email content displays in the client mail box (max. 2000 characters)
Activation Link: the name with hyperlink to redeem the account in the client email content
Web Page Customization: different customized types are selectable, but now only support *Edgecore Default* and *Customize with Template*

Account Roaming Out
Please refer to "*session 4.5.2 Local/ On-Demand Account Roaming Out"*

4.1.3 On-Demand Accounts Creation and List

Account Creation
After enabling the selected Billing Plans, On-Demand Accounts generation can be done on **On-Demand Account Creation**. On-Demand accounts can be created individually or in batches. For potential hotspot operators who may wish to pre-generate guest accounts for sale, On-Demand feature has a batch create functionality which allows the administrator or operator with access authority to On-Demand page, to create multiple accounts for an enabled billing plan in batch, and send them to POS printer for generating physical ticket printout for sale.



On-Demand Account Creation

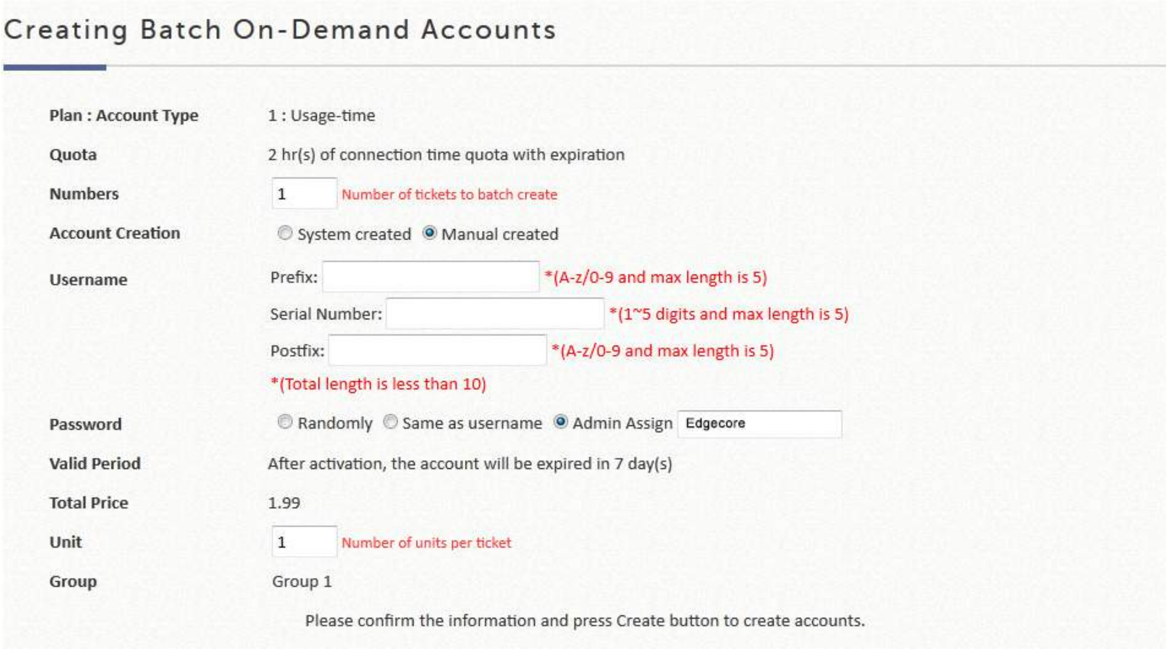
Plan	Account Type	Quota	Price ()	Group	Function
1	Usage-time	1 min(s) of connection time quota with expiration	11	1	Create Single Create Batch
2	N/A				Create Single Create Batch
3	N/A				Create Single Create Batch
4	N/A				Create Single Create Batch
5	N/A				Create Single Create Batch
6	N/A				Create Single Create Batch
7	N/A				Create Single Create Batch
8	N/A				Create Single Create Batch
9	N/A				Create Single Create Batch
0	N/A				Create Single Create Batch

Account Creation – System Created: to use system randomly generated Usernames and Passwords

- Password: the generated passwords can be short (4 characters) or long (8 characters).

Account Creation – Manual Created: to generate Usernames and Passwords by manually typing

- Username: the Prefix and Postfix will be kept constant while the Serial Number for the accounts will have single increments.
- Password: the generated password can be Randomly, Same as username, or Admin Assign

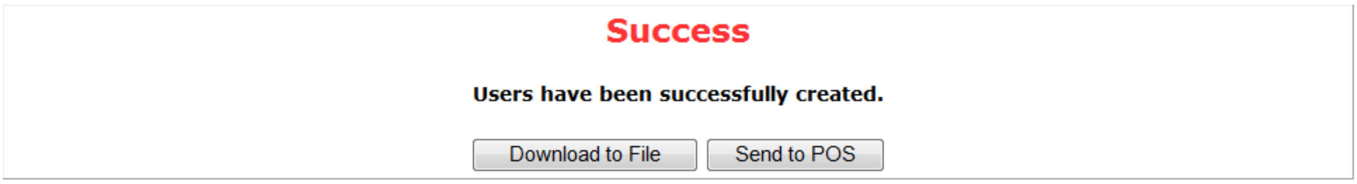


Creating Batch On-Demand Accounts

Plan : Account Type	1 : Usage-time
Quota	2 hr(s) of connection time quota with expiration
Numbers	1 Number of tickets to batch create
Account Creation	○ System created ● Manual created
Username	Prefix: ___ *(A-z/0-9 and max length is 5) Serial Number: ___ *(1~5 digits and max length is 5) Postfix: ___ *(A-z/0-9 and max length is 5) *(Total length is less than 10)
Password	○ Randomly ○ Same as username ● Admin Assign Edgecore
Valid Period	After activation, the account will be expired in 7 day(s)
Total Price	1.99
Unit	1 Number of units per ticket
Group	Group 1

Please confirm the information and press Create button to create accounts.

The generated accounts may be downloaded for safe keeping, or sent to printer for batch printout.



Success

Users have been successfully created.

Account List

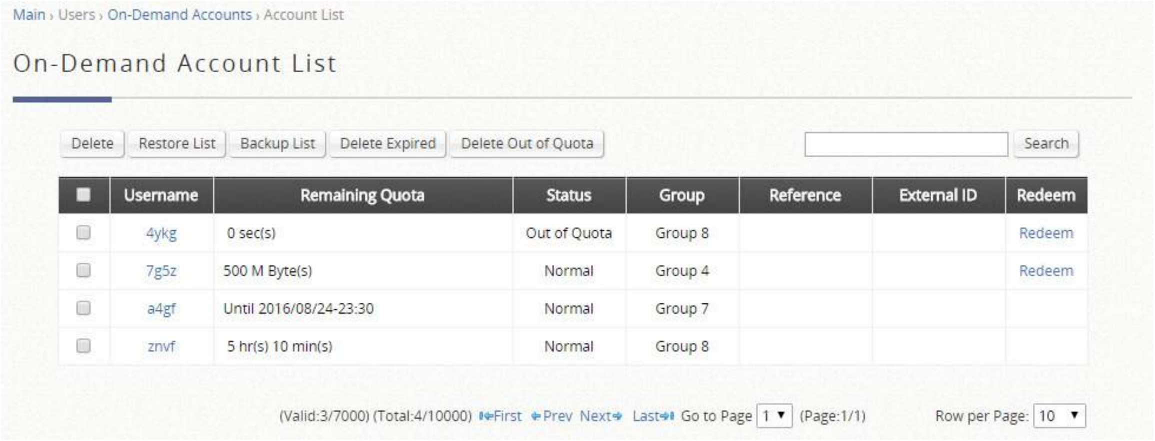
The On-Demand Accounts List houses all the existing On-Demand accounts. Each account's status, quota, etc. will be displayed for reference. On-Demand account import, export, deletion and Admin Redeem are also performed on this page.

The status of On-Demand accounts are defined as valid, out of quota and expired.

Valid = On-Demand account in active or quota remaining

Total = Valid + Out-of-Quota + Expired

Besides, the valid and total numbers of On-Demand accounts are informed in the end of this list.



□	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
□	4ykg	0 sec(s)	Out of Quota	Group 8			Redeem
□	7g5z	500 M Byte(s)	Normal	Group 4			Redeem
□	a4gf	Until 2016/08/24-23:30	Normal	Group 7			
□	znvf	5 hr(s) 10 min(s)	Normal	Group 8			

(Valid:3/7000) (Total:4/10000) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 10

4.1.4 Guest User Database

The Guest Authentication Option is not technically a user database, but rather a specially designed option to allow a user to access and surf the network without any user account or password. It allows the user to associate with a particular Service Zone, enter a specified string of text which may be a social security number, email, etc. defined by the administrator, and use the network without actual authentication.

The terms of use as well as usage constraints may be configured in the Guest authentication option profile.

Group: the User Group the guest-login clients belong to, which can be mapped to specific Service Zone and applied with limitation of user policy profile.
Guest Information: Some information of the accounts is available for administrators' further analysis or marketing purposes. Account emails and other questionnaire-enabled fields are able to be downloadable for administrators' data manipulation. It doesn't clear the entries automatically, but having email notification when 1000 remaining entries (11000/12000, maximum is 12000 entries).

- Download: Administrators are able to download the collected guest information
- Delete All: Administrators are able to delete all the stored data. Administrator can delete all entries after export to keep the list up-to-date.

Questionnaire: it provides administrators with options to customize extra questions on the login page for guest login, where the access information from guest users would be collected and viewed in the Guest Information list
Guest Access Time: to define the user time constrain based on MAC addresses

- Unlimited: there is no limitation about the allowance usage time
- 1 Day Access: clients are enforced with a usage time constraint
- Multi-Day Access: clients are enforced with a usage time constraint

Quota: the permitted duration and volume for each social-media-login client
Reactivation (1 Day Access only): to define a new session will be possible once the time has elapsed
Access Limit (1 Day Access only): to define how many times a device can request for a free account in a day

Email Verification: to ensure that the entered email is a valid email address. The client has to activate this account within the activation time to extend his/her usage time by clicking a link in the mail sent by the mail server. Note that the activation is merely a timer and does not add to the account's Quota.

SMTP Server Settings: to assign SMTP server for sending the mail for redeem clients. This SMTP is shared with Guest Email Verification. Please refer to "*session 17.5.1 SMTP Setting*." Taking Gmail as SMTP server, the configurations are

- SMTP server address: smtp.gmail.com
- SMTP port: 465
- Encryption: SSL
- Authentication: Login: Account Name: admin's Gmail email address
- Authentication: Login: Password: admin's Gmail email's password
- Sender Email Address: admin's Gmail email address

Sender Name: The Sender Name displays in the client mail box.

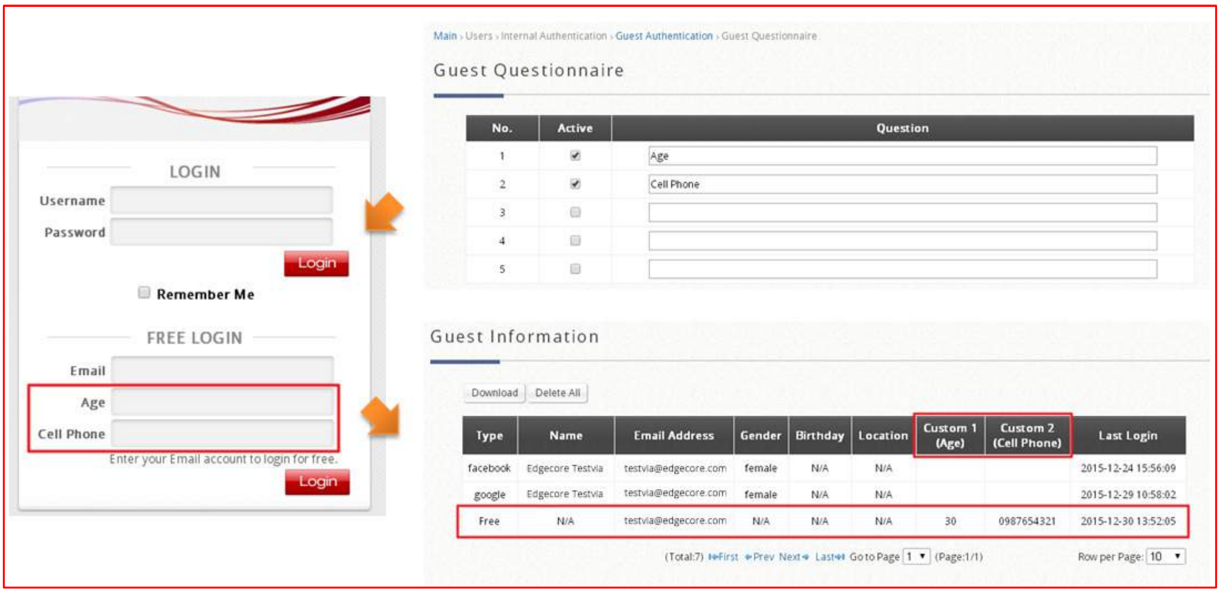
Activation Email Subject: customizable email subject displays in the client mail box

Activation Email Content: customizable email content displays in the client mail box (max. 2000 characters)

Activation Link: the name with hyperlink to redeem the account in the client email content

Guest Quota List: to check how many times of allowance remaining for the access-limited Guest accounts by MAC address and Email Address. (It would be automatically refreshed daily at the midnight, and the oldest entries are removed when reaching maximum).

Email Denial List: to check the email domains for login permission, if prevention of junk mailboxes is desired



Main › Users › Internal Authentication › Guest Authentication › Guest Questionnaire

Guest Questionnaire

No.	Active	Question
1	☑	Age
2	☑	Cell Phone
3	□	
4	□	
5	□	

Guest Information

Download Delete All

Type	Name	Email Address	Gender	Birthday	Location	Custom 1 (Age)	Custom 2 (Cell Phone)	Last Login
facebook	Edgecore Testvia	testvia@edgecore.com	female	N/A	N/A			2015-12-24 15:56:09
google	Edgecore Testvia	testvia@edgecore.com	female	N/A	N/A			2015-12-29 10:58:02
Free	N/A	testvia@edgecore.com	N/A	N/A	N/A	30	0987654321	2015-12-30 13:52:05

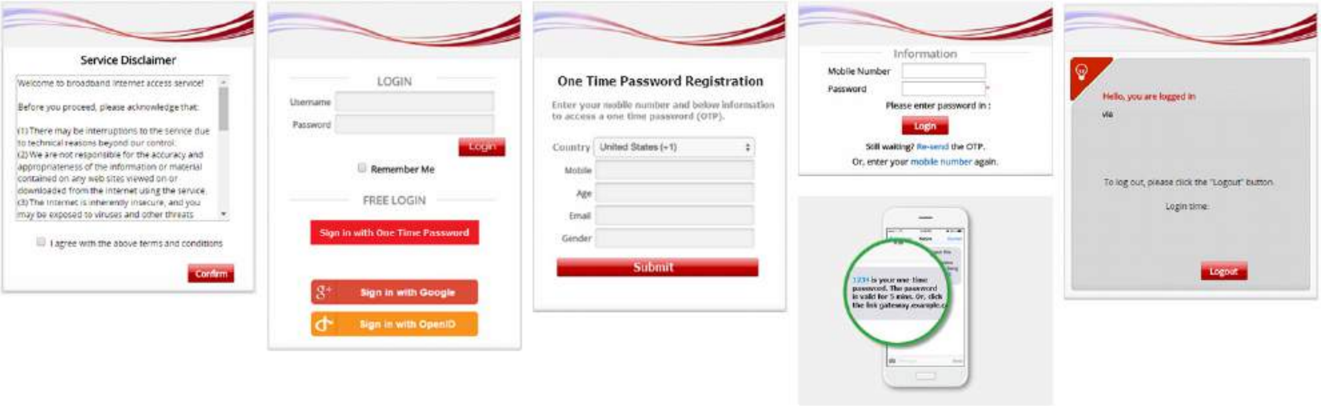
(Total:7) ⇤First ←Prev Next→ Last⇥ Go to Page 1 ▾ (Page:1/1) Row per Page: 10 ▾

The Sender Name, Email Subject, and Email Content (max. 2000 characters) are all customizable as soon as the SMTP server is ready. SMTP server configuration is done by clicking the "Assign SMTP Server" button.

4.1.5 One Time Password

For One Time Password (OTP) authentication option, clients are able to access the internet by entering their own mobile numbers and then receiving an SMS message with one time password which is needed to enter in the authentication page. Later, clients can start surfing the Internet.

Typically, the user login flow as below figure



Service Disclaimer

Welcome to broadband internet access service!

Before you proceed, please acknowledge that:

(1) There may be interruptions to the service due to technical reasons beyond our control.
(2) We are not responsible for the accuracy and appropriateness of the information or material contained on any web sites viewed on or downloaded from the internet using the service.
(3) The internet is inherently insecure, and you may be exposed to viruses and other threats

□ I agree with the above terms and conditions

One Time Password Registration

Enter your mobile number and below information to access a one time password (OTP).

Country: United States (+1)

Please enter password in :

Still waiting? Re-send the OTP.
Or, enter your mobile number again.

1234 is your one time password. The password is valid for 5 mins. Or, click the link gateway.example.c

Hello, you are logged in
via

To log out, please click the "Logout" button.

Login time:

A. **Service Disclaimer:** (if enabled) to agree with the terms and service to continue the login process
B. **General Login Page:** to choose different login options which is compatible with existed settings
C. **OTP Registration Page:** to enter their mobile number and, if enabled, other questionnaires
D. **Receive SMS with OTP:** to client's mobile and the text with the passcode will be received
E. **OTP Authentication Page:** to enter the OTP to verify and authenticate
F. **Login Success Page:** great, it's time to surf the Internet

One Time Password Authentication

Group: the OTP-authenticated clients will be applied by configured User Policy in each Service Zone

OTP Client Information: Clients' information collected who have asked the one time password

- **Download**: Administrators are able to download the collected OTP clients' information
- **Delete All**: Administrators are able to delete all the stored data. Administrator can delete all entries after export to keep the list up-to-date.

Default Country Code: to set the default country code displayed in the login page

Length of Mobile Number: to set the mobile number format with amount of digits

Quota (Duration Time): to specify the OTP-authenticated clients' duration. The max. duration is 364 days 23 hours 59 Minutes.

Questionnaire: 5 entries displayed in *OTP Registration Page*

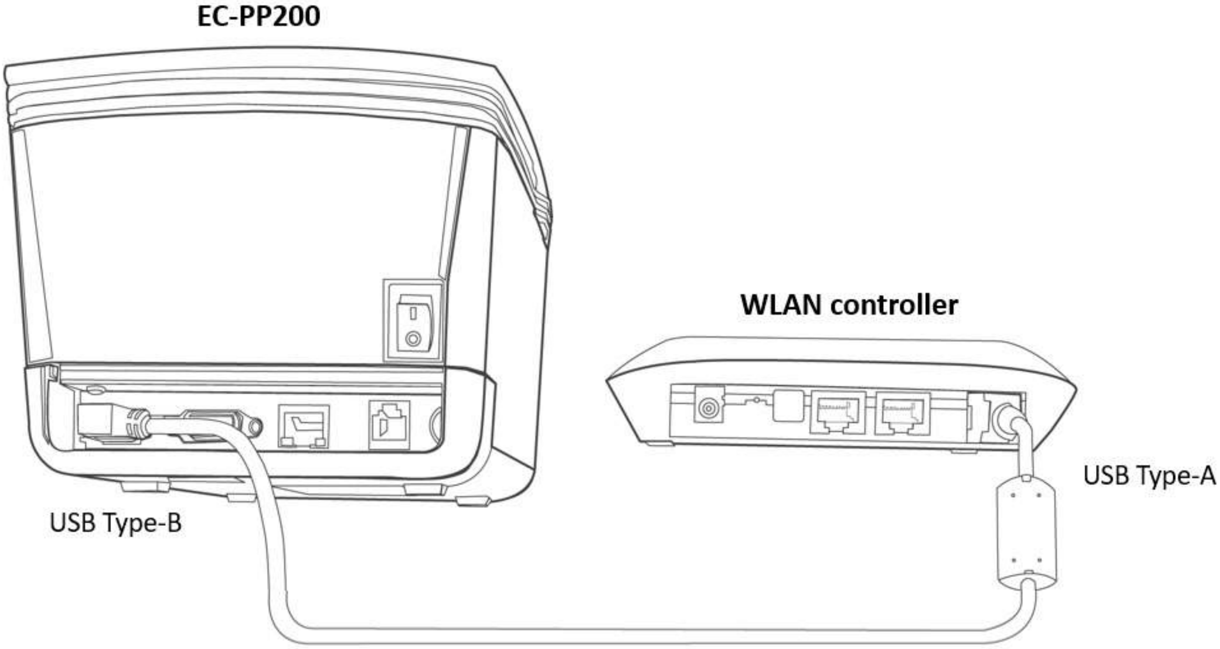
SMS Gateway: Clickatell (Legacy/ New), and SMS API (confirm the text content customization), related setting please refer to SMS Gateway setting in *"session 4.1.2 On-Demand User Database"*

Web Page Customization: different customized types are selectable, but now only support *Edgecore Default* and *Customize with Template*

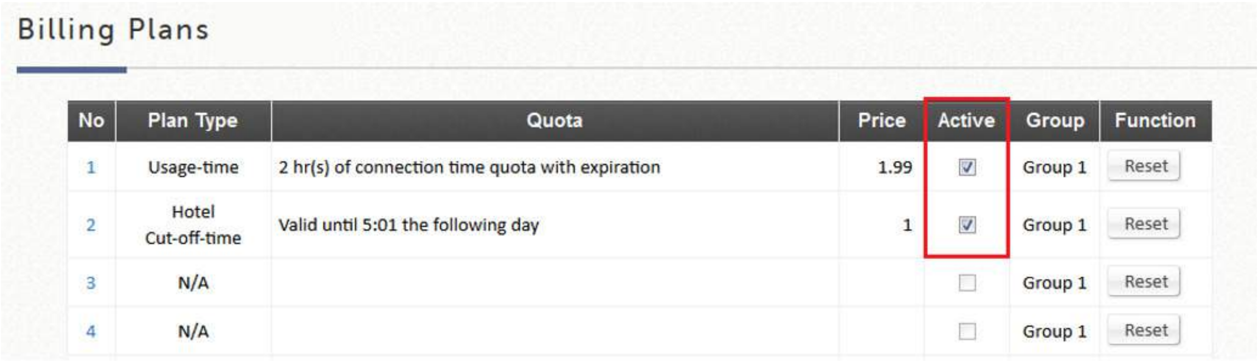
4.2 How to integrate Edgecore EC-PP200 printer

Manual setup

To connect the EC-PP200 to the WLAN controller via an USB cable.



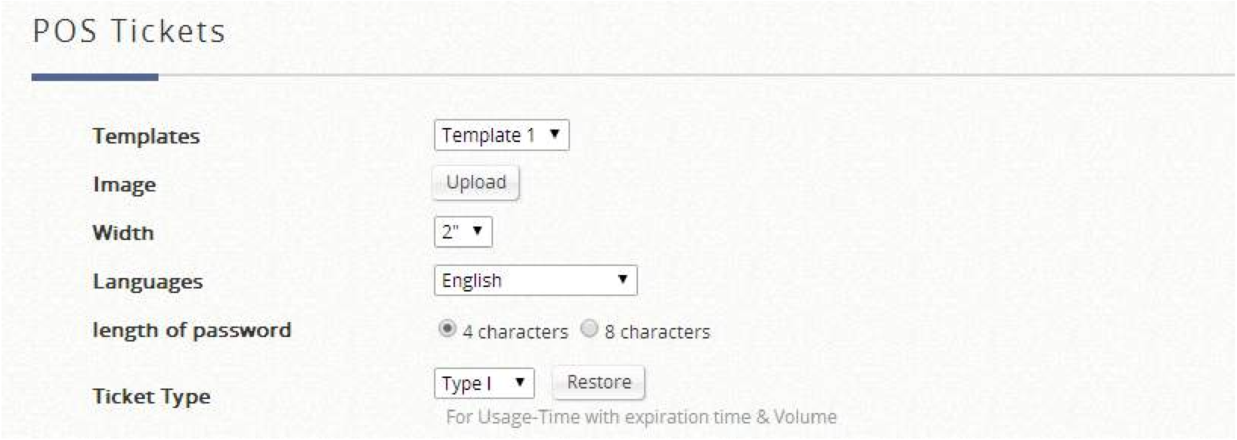
Configure and Active Billing Plans



Billing Plans

No	Plan Type	Quota	Price	Active	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	1.99	☑	Group 1	Reset
2	Hotel Cut-off-time	Valid until 5:01 the following day	1	☑	Group 1	Reset
3	N/A			□	Group 1	Reset
4	N/A			□	Group 1	Reset

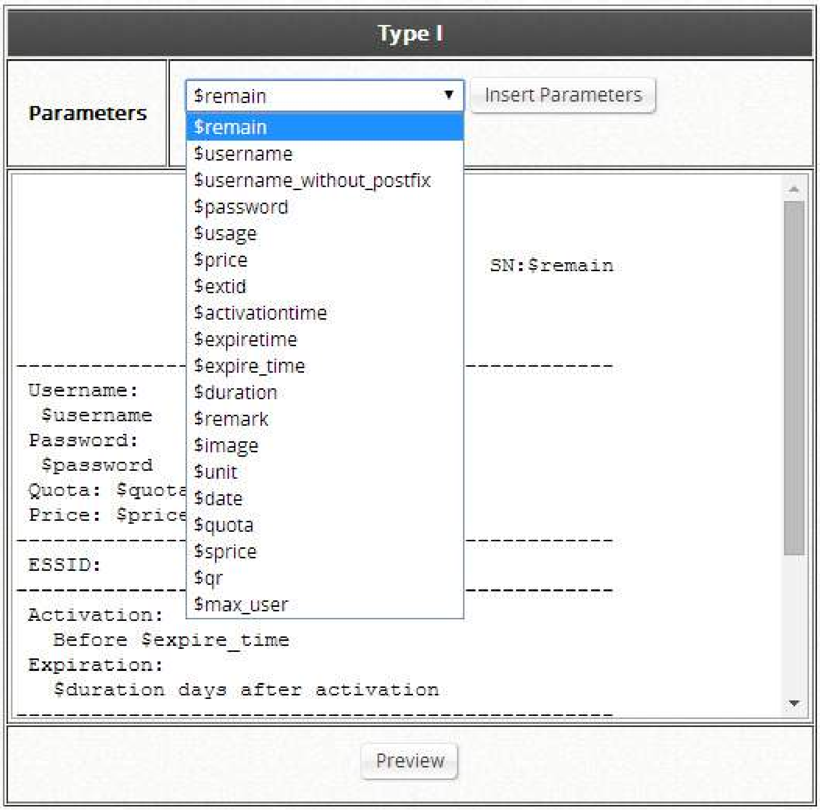
For deployment flexibility on your hotspot, customization of POS tickets using templates is supported on the WLAN controller. Up to 5 ticket templates can be saved on the system.



POS Tickets

Templates	Template 1 ▼
Image	Upload
Width	2" ▼
Languages	English ▼
length of password	● 4 characters ○ 8 characters
Ticket Type	Type I ▼ Restore For Usage-Time with expiration time & Volume

Image: an image can be uploaded (such as your company logo) in TMB format if needed.
Width: there are 2 Width types, 2” for PRT100 and 3” for EC-PP200.
Language: to select the desired language for the configured ticket template. WLAN controller supports English, French, German, Japanese, Spanish, Simplified Chinese, and Traditional Chinese.
Length of Password: for accounts generated with the SDS200W, passwords are random, but the administrator has the option of selecting between a 4-character and an 8-character password.
Ticket Type: to select the appropriate Ticket Type depending on the configured billing plan.

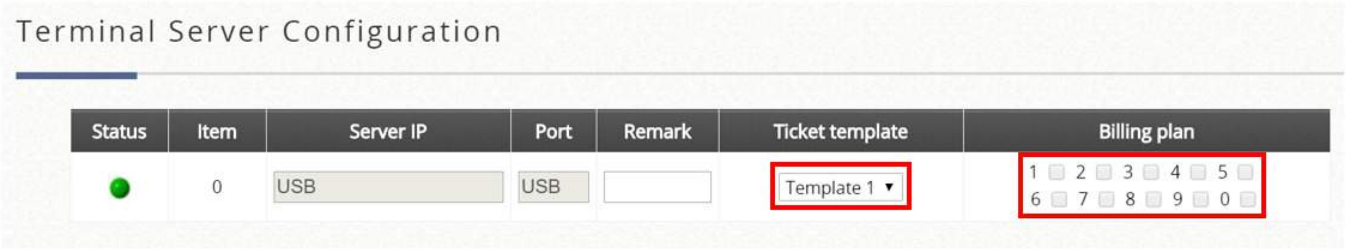


```
                                    SN:$remain



-------------                --------------
Username:
 $username
Password:
 $password
Quota: $quota
Price: $price
-------------                --------------
ESSID:
-------------                --------------
Activation:
  Before $expire_time
Expiration:
  $duration days after activation
----------------------------------------------
```

Administrators may start customizing your POS ticket from the window below manually typing or by inserting parameters from the drop-down list as shown in the above example. Once this is done, you may start assigning Billing Plans and Ticket Templates for your Terminal Servers.

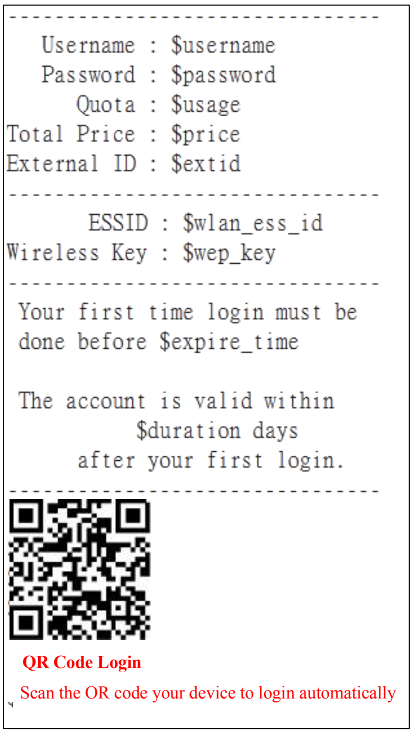


Terminal Server Configuration

Status	Item	Server IP	Port	Remark	Ticket template	Billing plan
●	0	USB	USB		Template 1 ▾	1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 0 □

The administrator can now select the desired Ticket Template for a specific ticket generator from the drop-down list.

Applications for QR Code Log-in



```
-------------------------------
   Username : $username
   Password : $password
      Quota : $usage
Total Price : $price
External ID : $extid
-------------------------------
      ESSID : $wlan_ess_id
Wireless Key : $wep_key
-------------------------------
 Your first time login must be
 done before $expire_time

 The account is valid within
           $duration days
      after your first login.
-------------------------------
```

QR Code Login

Scan the OR code your device to login automatically

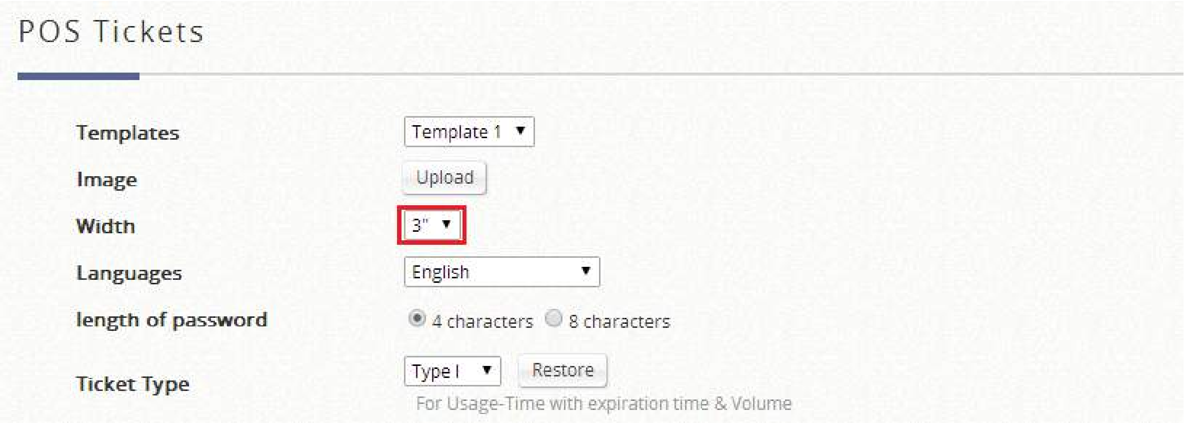
On-Demand Account generation with a ticket generator is a very common deployment for hotspot providers. What makes it a hassle is to manually enter the Username and Password of the account, especially for mobile devices which require typing on small keyboards and are not easy on the eyes.

Log-in credentials including your Username, Password, Usage quota, Price and etc. are all embedded in the QR code.

Simply associate with the SSID, scan QR Code, and you are ready to surf the internet!

Configuring your web ticket to support QR Code

The ticket needs to be customized in order to support the printing of QR Code.
Under *Main Menu > Users > Authentications*, click On-Demand User and Configure for Ticket Template Customization.



POS Tickets

Templates: Template 1 ▾

Image: Upload

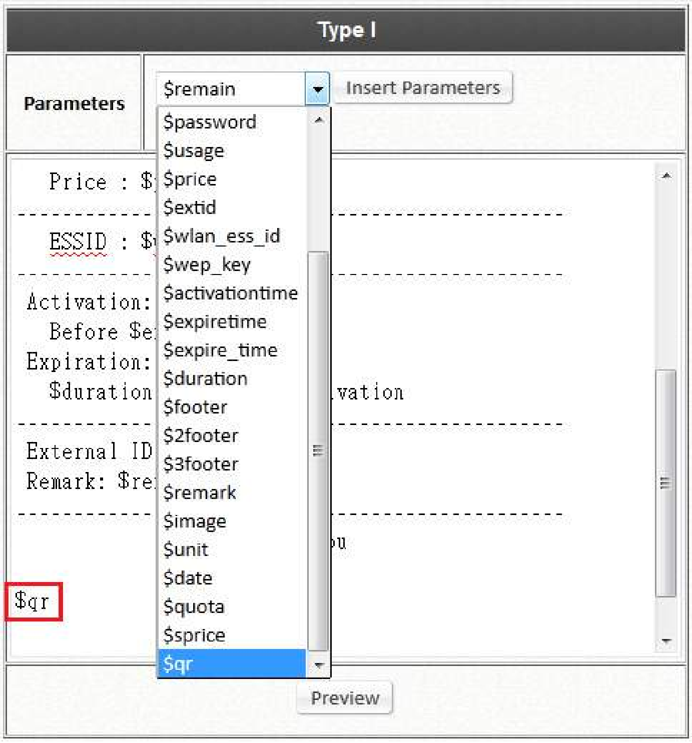
Width: 3" ▾

Languages: English ▾

length of password: ● 4 characters ○ 8 characters

Ticket Type: Type I ▾ Restore

For Usage-Time with expiration time & Volume



For the utilized Billing Plan, the corresponding ticket template needs to be customized to support QR Code.

The width needs to be changed to 3” (default value = 2”)

The parameter needs to be added by typing in “$qr” on the template, or select “$qr” from the drop-down menu and click Insert Parameters.

Note: Only Edgecore EC-PP200 thermal printers support the printing of QR code. If clients has installed a QR Code scanning App (such as QuickMark, QR Reader, Barcode Scanner), the login process is simple now.

Note: Switch off Auto-Join and Auto-Login to prevent the mobile device from jumping back to the remembered network.

4.3 External Authentication

The WLAN controllers are equipped with a variety of external authentication options so as to support account roaming and adapt to existing network. There are

- POP3
- LDAP
- RADIUS
- NT Domain
- SIP
- Social Media

4.3.1 POP3

POP3 is a common mail service protocol where e-mail is kept by a certain Internet server. The WLAN controllers offer administrator a way of authentication in which users are granted the Internet service by typing in their email addresses and passwords stored in the POP3 server.

Server 5 by default is configured to use POP3 authentication. Click on the Server Name and a detailed configuration page will show up to inquire necessary settings including POP3 server address, secondary POP3 server specification etc.

4.3.2 LDAP

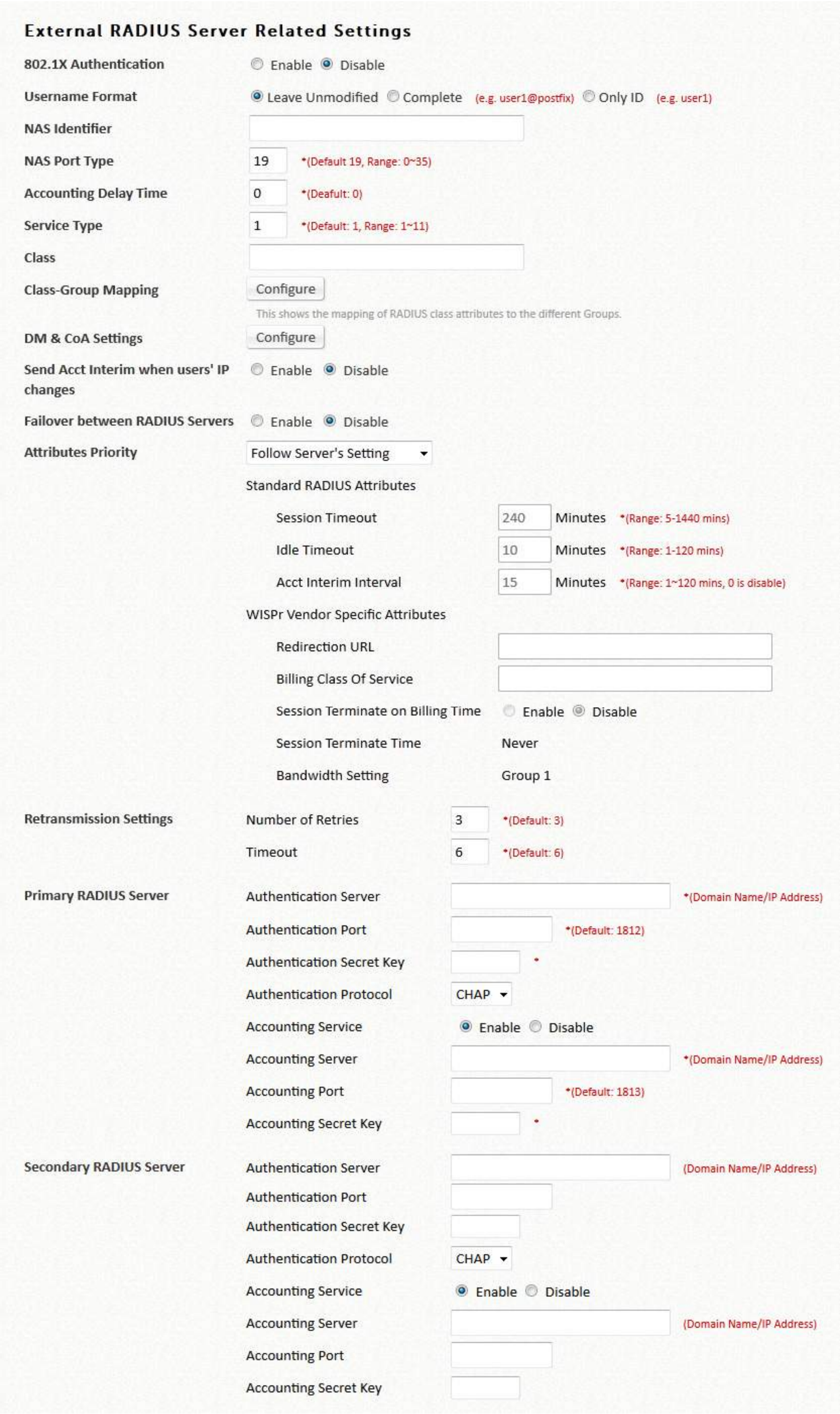
The Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an IP network. If you wish to deploy LDAP server for user authentication, proceed for a complete setup.

Server 4 by default is selected to use LDAP database for user credential check.
Click on the Server Name to enter the detailed setup page of LDAP (a secondary LDAP server can be designated as a backup server). Furthermore, LDAP configuration page has an Attribute-Group Mapping page which maps LDAP attributes to different groups on the WLAN controller, enabling different accounts to be incorporated into different Groups.

4.3.3 RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for clients to connect and use a network service. It is also the most commonly used external authentication mechanism today. How to deploy WLAN controller to different scenarios is described in session 4.5 RADIUS Authentication Application

Server 2 by default is configured to use RADIUS authentication. The WLAN controllers support RADIUS authentication, RADIUS class mapping, and RADIUS transparent login with 802.1X. Below is the detailed configuration page of RADIUS settings. Attributes of the Primary RADIUS Server and Secondary RADIUS Server can be configured depending on service deployment.



External RADIUS Server Related Settings

802.1X Authentication	○ Enable ● Disable		
Username Format	● Leave Unmodified ○ Complete (e.g. user1@postfix) ○ Only ID (e.g. user1)		
NAS Identifier			
NAS Port Type	19	*(Default 19, Range: 0~35)	
Accounting Delay Time	0	*(Deafult: 0)	
Service Type	1	*(Default: 1, Range: 1~11)	
Class			
Class-Group Mapping	Configure This shows the mapping of RADIUS class attributes to the different Groups.		
DM & CoA Settings	Configure		
Send Acct Interim when users' IP changes	○ Enable ● Disable		
Failover between RADIUS Servers	○ Enable ● Disable		
Attributes Priority	Follow Server's Setting		
	Standard RADIUS Attributes		
	Session Timeout	240 Minutes	*(Range: 5-1440 mins)
	Idle Timeout	10 Minutes	*(Range: 1-120 mins)
	Acct Interim Interval	15 Minutes	*(Range: 1~120 mins, 0 is disable)
	WISPr Vendor Specific Attributes		
	Redirection URL		
	Billing Class Of Service		
	Session Terminate on Billing Time	○ Enable ● Disable	
	Session Terminate Time	Never	
	Bandwidth Setting	Group 1	
Retransmission Settings	Number of Retries	3	*(Default: 3)
	Timeout	6	*(Default: 6)
Primary RADIUS Server	Authentication Server		*(Domain Name/IP Address)
	Authentication Port		*(Default: 1812)
	Authentication Secret Key		*
	Authentication Protocol	CHAP	
	Accounting Service	● Enable ○ Disable	
	Accounting Server		*(Domain Name/IP Address)
	Accounting Port		*(Default: 1813)
	Accounting Secret Key		*
Secondary RADIUS Server	Authentication Server		(Domain Name/IP Address)
	Authentication Port		
	Authentication Secret Key		
	Authentication Protocol	CHAP	
	Accounting Service	● Enable ○ Disable	
	Accounting Server		(Domain Name/IP Address)
	Accounting Port		
	Accounting Secret Key		

Another important setting field is the Class-Group Mapping on the page. It is a translation setting which maps RADIUS classes attributes to different groups on the WLAN controller, enabling different RADIUS accounts to be incorporated into different Groups.

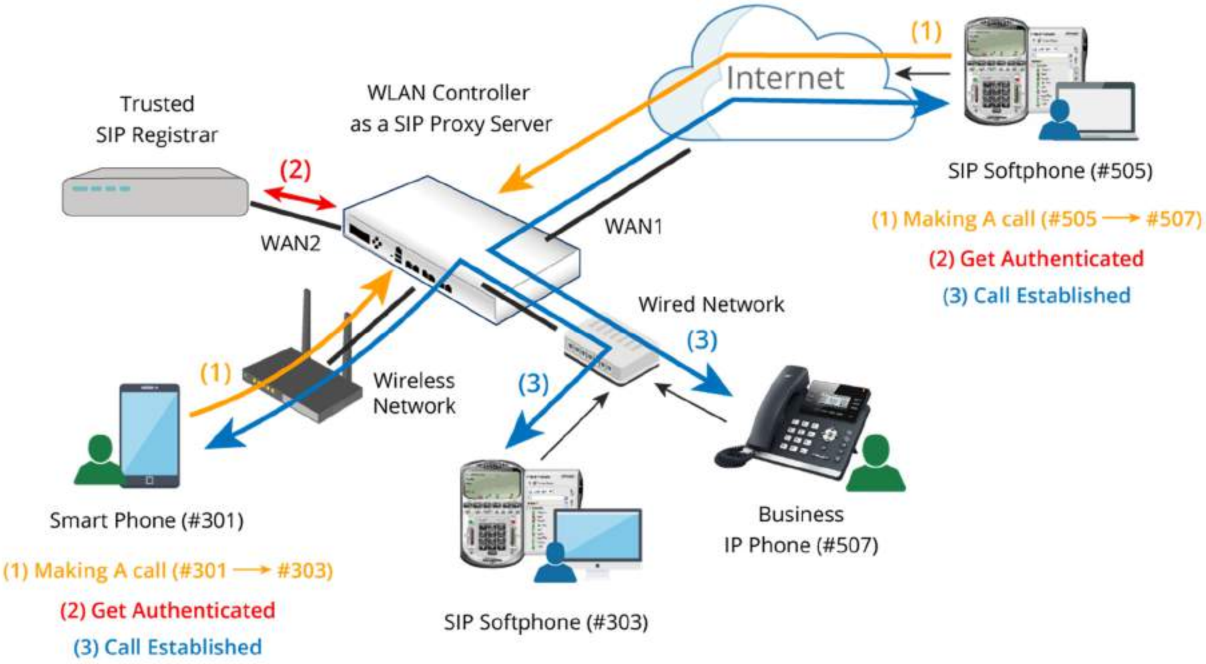
4.3.4 NT Domain

NT Domain option supports Windows Domain databases to perform user credential authentication.

By default Server 3 is selected to use NT Domain. The administrator is only required to enter the Domain Controller IP address where the user credentials are housed. Additionally, if Windows Active Directory is deployed as identity check for device access, Transparent Login feature may be enabled to grant access to device and network with a single login action.

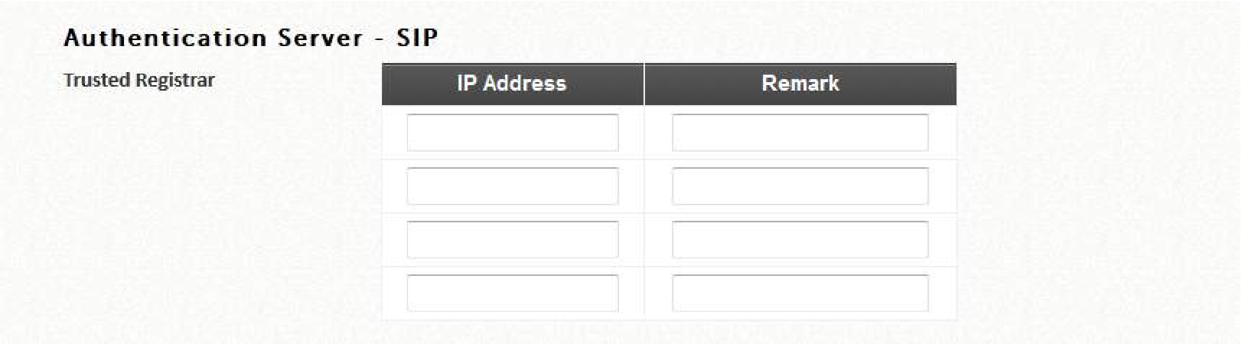
4.3.5 SIP

SIP, or the session initiation protocol, is the IETF protocol defined for Voice over Internet Protocol (VoIP) and other multi-media sessions. The WLAN controllers support SIP authentication as well as the use of SIP phones. In addition to a WLAN controller, admin has to set up other devices as to making successful SIP phone calls. This includes: A valid SIP Registrar, SIP phones.



(1) A user is making a call through a SIP-based phone (e.g. #301 --> #303).
(2) The user gets authenticated transparently, if the user is registered in the SIP Registrar.
(3) The call is established successfully.

By default SIP is not selected as database for any Auth option. Enable SIP from Authentication Settings in the respective Service Zones. The administrator will need to enter at least one valid SIP Registrar as the call center to provide call service; up to four may be specified. Please note that the corresponding Group profile should have its QoS settings appropriately configured to support voice applications.



Authentication Server - SIP

Trusted Registrar

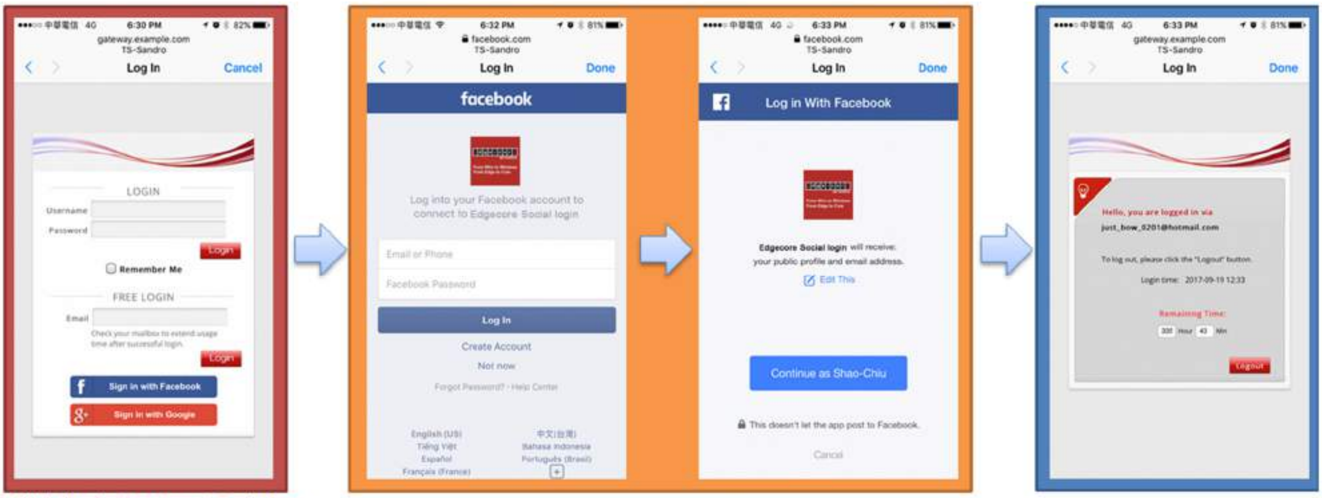
IP Address	Remark

Please also make sure that the corresponding Service Zone also has ‘Enable’ checked in the SIP Interface Configuration in order to function properly.

4.3.6 Social Media

Social Media Login allows Wi-Fi users to access internet without going through a tedious account registration process. The WLAN controller supports six kinds of social media accounts, LINE, Facebook, Google+, Weibo, VK and Open ID. All administrators have to do is to apply the corresponding Application ID and secret.

When a user clicks the button to sign in with social media accounts, he/ she will be redirected to the social media sites for login and granting permissions. It is not necessary to be bothered by the walled garden dilemma. Connected clients will get 5 minutes free permission as long as they are clicking one of the social login buttons. Then, they have to complete the login process with the required social account information during 5 minutes. Later, it is time to start surfing the internet as below figure.



Click the button to get 5min free permission to complete login flow

Complete these operation in 5 min

Get free Wi-Fi Service

Social Media Login

Group: the User Group the social-media-login clients belong to, which can be mapped to specific Service Zone and applied with limitation of user policy profile.

Social Media Account Information: Some information of the accounts is available for administrators’ further analysis or marketing purposes. Account names, account emails, gender, birthdays, and location on the Social Media Account List are able to be downloadable for administrators' data manipulation (if Social Medias permit to provide). It doesn't clear the entries automatically, but having email notification when 1000 remaining entries (11000/12000, maximum is 12000 entries).

- Download: Administrators are able to download the collected guest information
- Delete All: Administrators are able to delete all the stored data. Administrator can delete all entries after export to keep the list up-to-date.

Social Media Account Access Time: when set to "Limited" will enforce a usage time constraint based on MAC addresses
Quota: the permitted duration and volume for each social-media-login client
Reactivation: to define a new session will be possible once the time has elapsed
Access Limit: to define how many times a device can request for a free account in a day
Social Account Quota List: to check how many times of allowance remaining for the access-limited Guest accounts by MAC address and Email Address. (It would be automatically refreshed daily at the midnight, and the oldest entries are removed when reaching maximum).
Punishment List: if the pre-authorized clients have not completed the login process within 5 minutes. The client entry would be displayed in the table. If the clients have retried to click the social login button in 3 times and still failed, it takes 15 minutes as punishment. Administrators could help release the restriction in Punishment List.

Social API Credentials
LINE: visit the website at LINE Developers site (https://developers.line.me/console/) and apply for "LINE Login" APP to get the Channel ID and Channel secret as the App type is WEB.
Facebook: visit the website at Facebook Developers site (https://developers.facebook.com/) and apply for "Facebook Login" APP to get the app ID and app secret.
Google+: visit the website at Google Developers Console (https://console.developers.google.com/) and apply for "Google+ API" to get the client ID and secret.
Weibo: visit the website at Weibo Developers site (http://open.weibo.com/liveapi/index.php) and apply for "LINE Login" APP to get the Channel ID and Channel secret as the App type is WEB.
VK: visit the website at VK Developers site (https://vk.com/dev) and apply for "LINE Login" APP to get the Channel ID and Channel secret as the App type is WEB.
Open ID: the login path must be traversed and added into OpenID Walled Garden and the redirection target depends on OpenID provider.

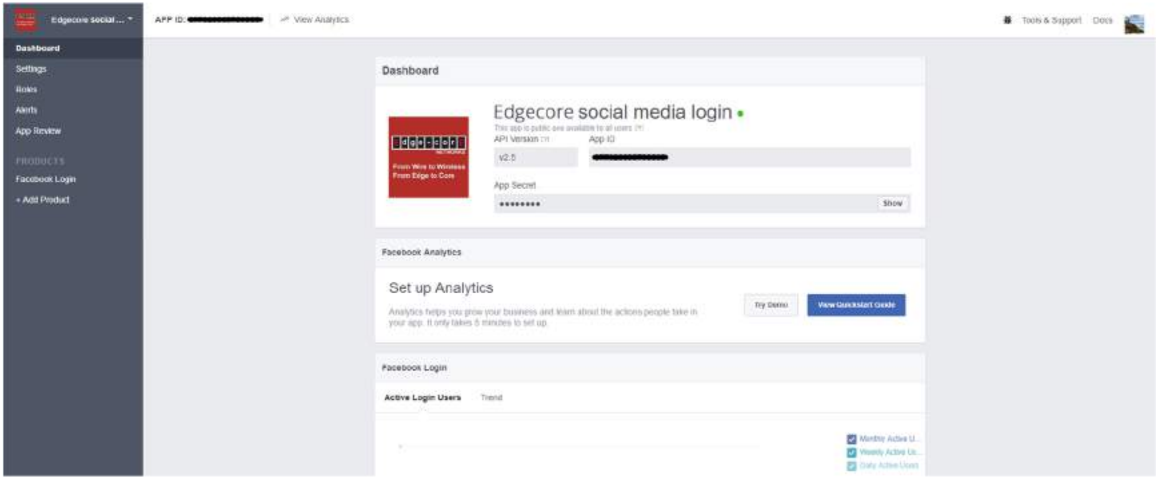
Note: there are some tips for applying the API from the social media developer site. Please fill in some important URI as below and noted that the gateway.example.com is the WLAN controllers' default internal domain name which can be configured at *Main › System › General*. The step-by-step application procedures could be referred to Technical Guide.
Site URI: http://gateway.example.com/
Redirect URI: http://gateway.example.com/loginpages/line_login.shtml

4.4 How to apply Social Media Login

The WLAN controllers also provide a convenient method for Social Media Login which enables clients to access internet by logging in with their own Social Media Accounts, ex. LINE, Facebook, Google+, Weibo, VK, and Open ID.

Step 1. Prepare the desired Social API Credential with access the App ID and Secret by entering social developers' site

All administrators have to do is to copy and paste for a corresponding ID and secret.
Facebook developer website



APP ID: [redacted]

Dashboard

Edgecore social media login

This app is public and available to all users

API Version: v2.5

App ID: [redacted]

App Secret: •••••••• Show

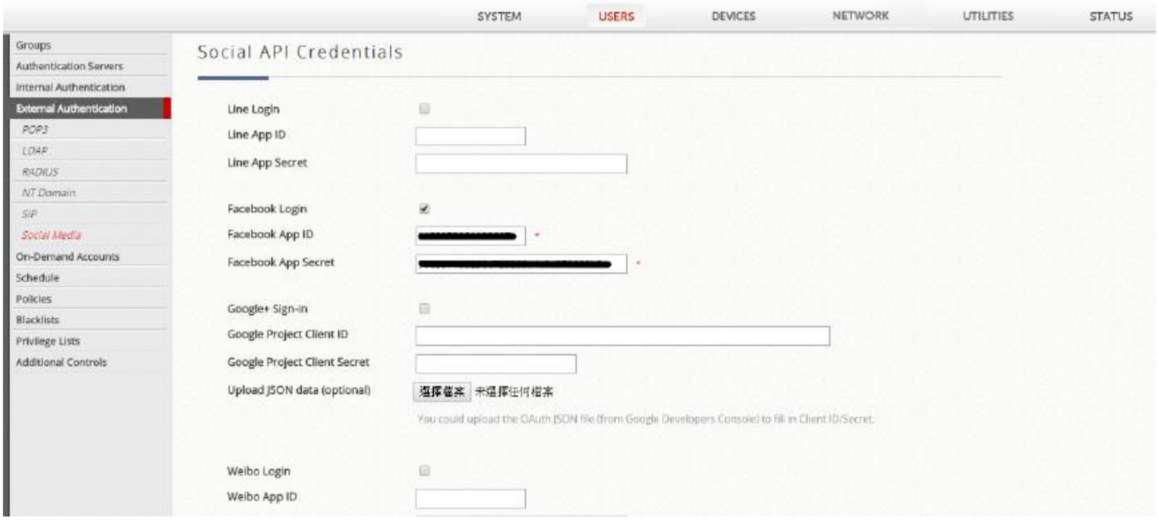
Facebook Analytics

Set up Analytics

Analytics helps you grow your business and learn about the actions people take in your app. It only takes 5 minutes to set up.

Facebook Login

WLAN controller configuration



Social API Credentials

Line Login ☐

Line App ID

Line App Secret

Facebook Login ☑

Facebook App ID [redacted] *

Facebook App Secret [redacted] *

Google+ Sign-in ☐

Google Project Client ID

Google Project Client Secret

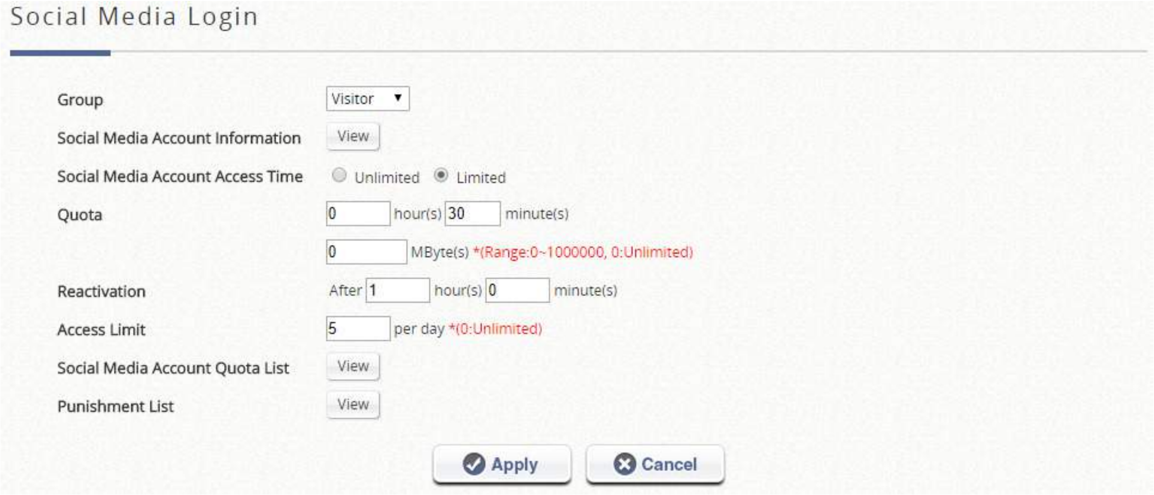
Upload JSON data (optional) 選擇檔案 未選擇任何檔案

You could upload the OAuth JSON file (from Google Developers Console) to fill in Client ID/Secret.

Weibo Login ☐

Weibo App ID

Step 2. Define the free Wi-Fi service, including Quota in Unlimited/Limited Access Time

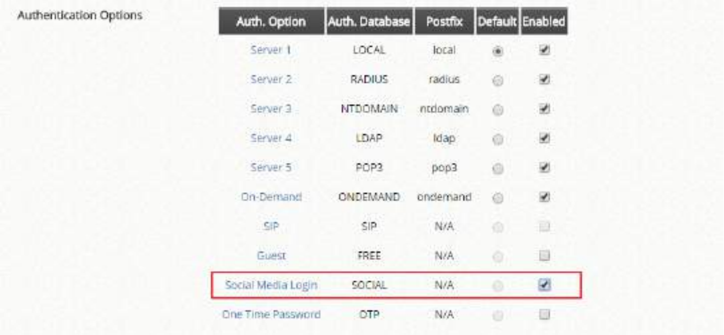


Social Media Login

Group	Visitor ▼
Social Media Account Information	View
Social Media Account Access Time	○ Unlimited ● Limited
Quota	0 hour(s) 30 minute(s)
	0 MByte(s) *(Range:0~1000000, 0:Unlimited)
Reactivation	After 1 hour(s) 0 minute(s)
Access Limit	5 per day *(0:Unlimited)
Social Media Account Quota List	View
Punishment List	View

Step 3. Implement into specific Service Zones and login pages

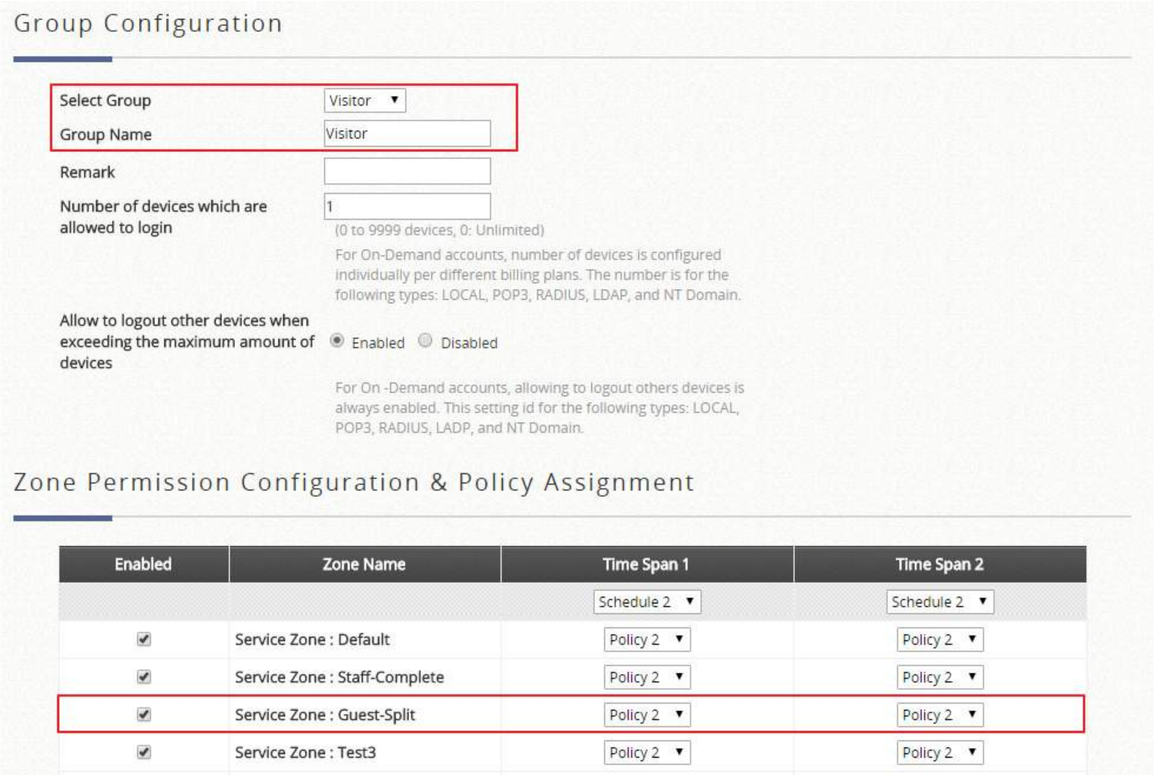
Choose the desired Service Zone where you would like to apply the Guest authentication option - Go to "*Main Menu > System > Service Zone > Configure*." Scroll down the page to Authentication Options. Check to enable the option for Social Media Login Option as shown in the figure below.



Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	●	☑
Server 2	RADIUS	radius	○	☑
Server 3	NTDOMAIN	ntdomain	○	☑
Server 4	LDAP	ldap	○	☑
Server 5	POP3	pop3	○	☑
On-Demand	ONDEMAND	ondemand	○	☑
SIP	SIP	N/A	○	□
Guest	FREE	N/A	○	□
Social Media Login	SOCIAL	N/A	○	☑
One Time Password	OTP	N/A	○	□

Complete the mapping of the Social User Group, Service Zone, User Policy and Schedule



Group Configuration

Select Group	Visitor ▼
Group Name	Visitor
Remark	
Number of devices which are allowed to login	1 (0 to 9999 devices, 0: Unlimited) For On-Demand accounts, number of devices is configured individually per different billing plans. The number is for the following types: LOCAL, POP3, RADIUS, LDAP, and NT Domain.
Allow to logout other devices when exceeding the maximum amount of devices	● Enabled ○ Disabled For On -Demand accounts, allowing to logout others devices is always enabled. This setting id for the following types: LOCAL, POP3, RADIUS, LADP, and NT Domain.

Zone Permission Configuration & Policy Assignment

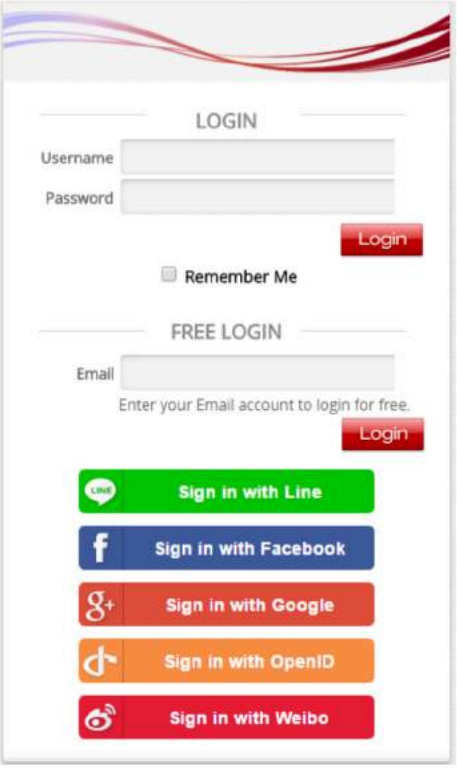
Enabled	Zone Name	Time Span 1	Time Span 2
		Schedule 2 ▼	Schedule 2 ▼
☑	Service Zone : Default	Policy 2 ▼	Policy 2 ▼
☑	Service Zone : Staff-Complete	Policy 2 ▼	Policy 2 ▼
☑	Service Zone : Guest-Split	Policy 2 ▼	Policy 2 ▼
☑	Service Zone : Test3	Policy 2 ▼	Policy 2 ▼

Step 4. Clients are now able to access the login pages

Consequently, after going through configurations from STEP 1 to STEP 3, end users will see that the an additional “Sign-in with Social button(s)” will show on the Service Zone’s login page.

By clicking Social Media Login button, approving the terms and condition of free accessing public Wi-Fi, the free users will be able to access the network with constraints specified in Social Media Login Option profile and the Group profile. MAC address will be checked to avoid malicious use of free access.

Note: When Social Media Login is enabled, the controller collects information from the clients. Please enable Disclaimer or customized login page to include claims and reminders.

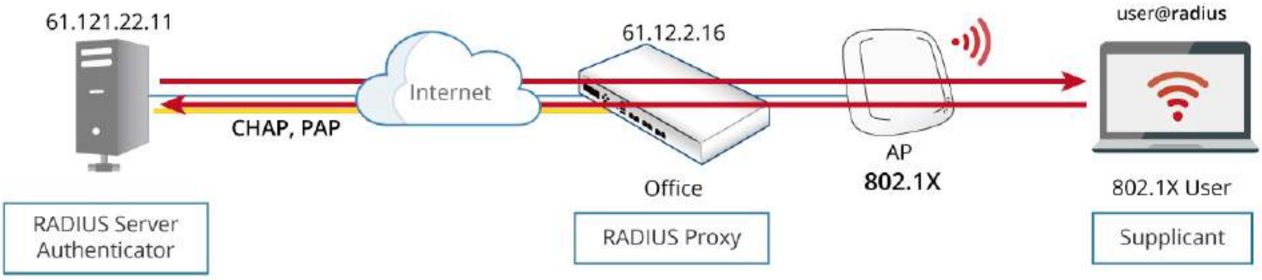


Step 5. Clients are now able to access the login pages

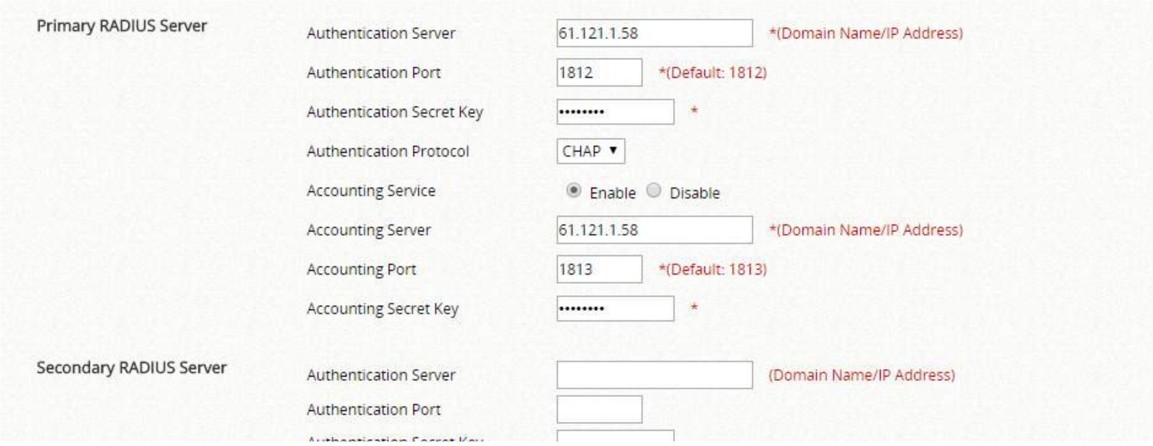
Consequently, after going through configurations from STEP 1 to STEP 3, end users will see that the an additional “Sign-in with Social button(s)” will show on the Service Zone’s login page.

4.5 RADIUS Authentication Application

4.5.1 802.1X Authentication/ WPA2-Enterprise Authentication

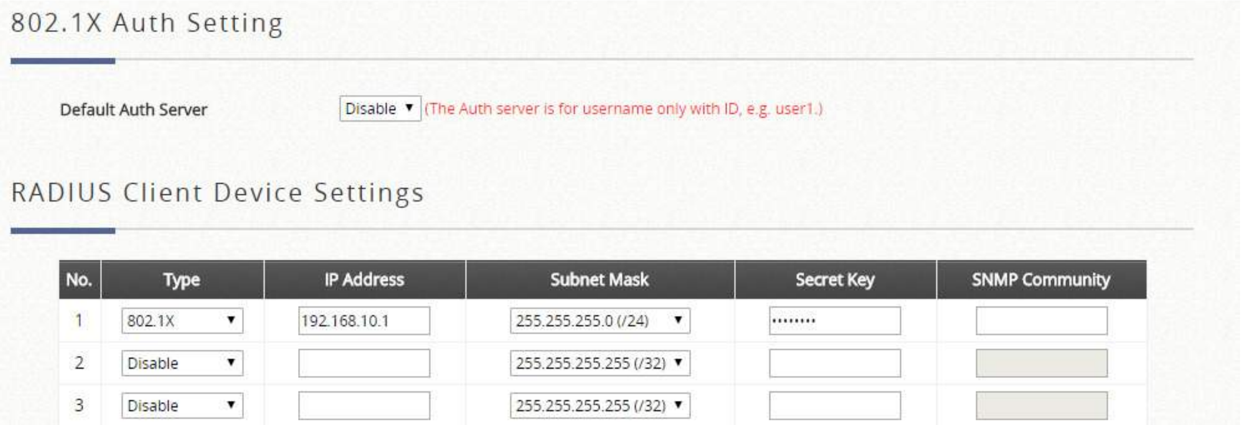


WLAN controller configuration
Since the WLAN controller needs to communicate with external RADIUS server, the authentication server and accounting server settings should follow the RADIUS server.



Primary RADIUS Server	Authentication Server	61.121.1.58	*(Domain Name/IP Address)
	Authentication Port	1812	*(Default: 1812)
	Authentication Secret Key	••••••••	*
	Authentication Protocol	CHAP ▼	
	Accounting Service	● Enable ○ Disable	
	Accounting Server	61.121.1.58	*(Domain Name/IP Address)
	Accounting Port	1813	*(Default: 1813)
	Accounting Secret Key	••••••••	*
Secondary RADIUS Server	Authentication Server		(Domain Name/IP Address)
	Authentication Port		

For the clients associated to the managed APs, the RADIUS Client Device Settings should set the 802.1x service range as the managed APs with the corresponding RADIUS Secret Key.



802.1X Auth Setting

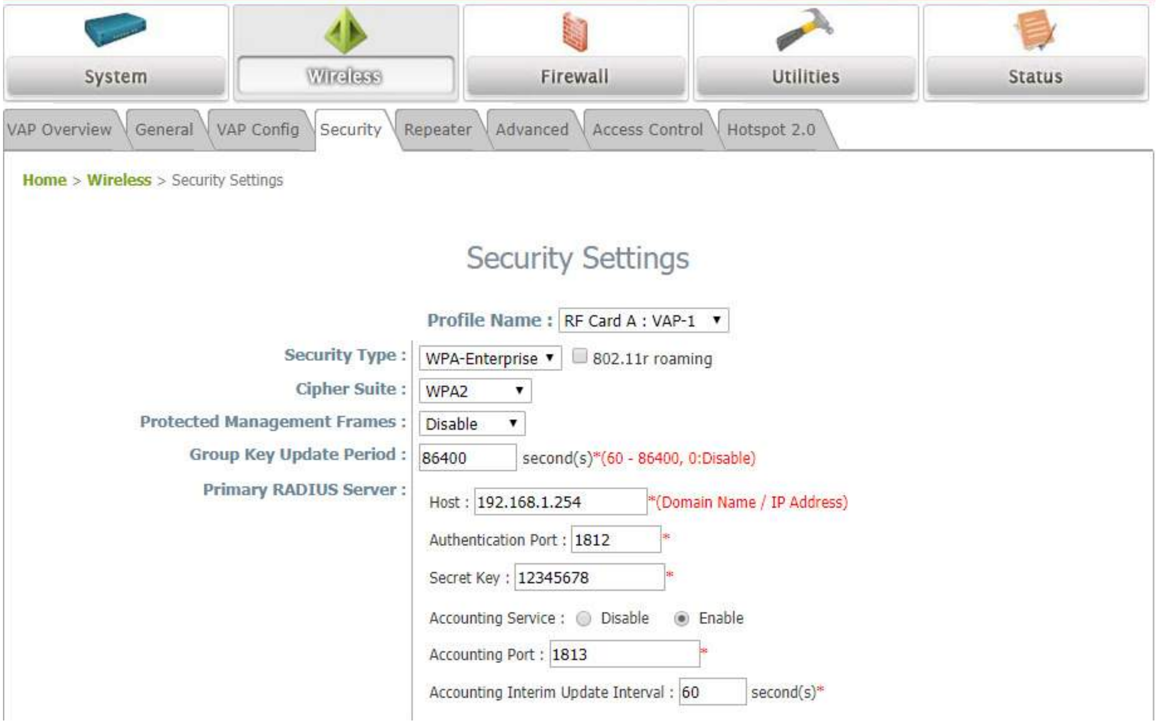
Default Auth Server: Disable ▼ (The Auth server is for username only with ID, e.g. user1.)

RADIUS Client Device Settings

No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	802.1X ▼	192.168.10.1	255.255.255.0 (/24) ▼	••••••••	
2	Disable ▼		255.255.255.255 (/32) ▼		
3	Disable ▼		255.255.255.255 (/32) ▼		

AP Configuration
For the clients associated to the managed APs, they should provide the VAP with the WPA2-Enterprise security which should direct to the Service Zone of the target WLAN controller. Therefore, the clients can

start the RADIUS authentication request and follow the AAA settings from the WLAN controller and the RADIUS server.



Security Settings

Profile Name : RF Card A : VAP-1

Security Type : WPA-Enterprise □ 802.11r roaming

Cipher Suite : WPA2

Protected Management Frames : Disable

Group Key Update Period : 86400 second(s)*(60 - 86400, 0:Disable)

Primary RADIUS Server :

Host : 192.168.1.254 *(Domain Name / IP Address)

Authentication Port : 1812 *

Secret Key : 12345678 *

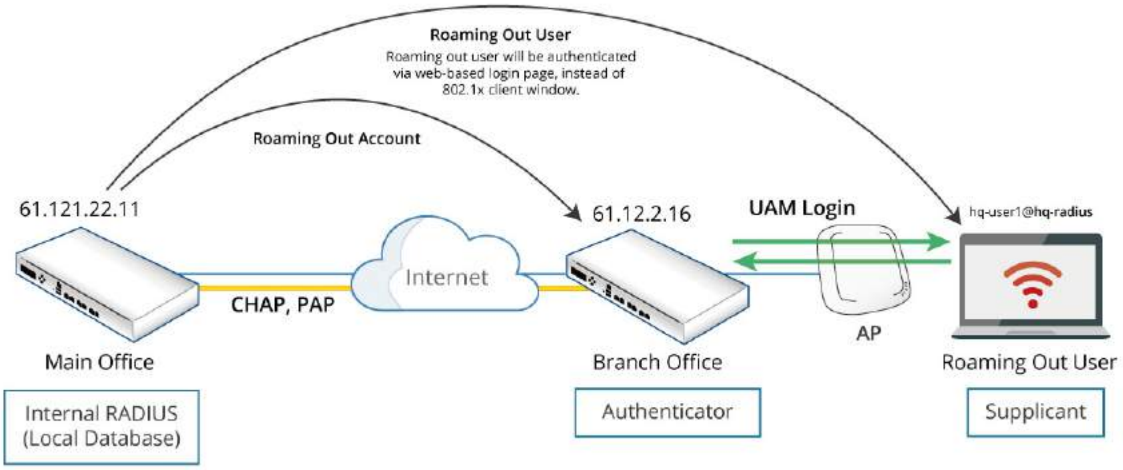
Accounting Service : ○ Disable ● Enable

Accounting Port : 1813 *

Accounting Interim Update Interval : 60 second(s)*

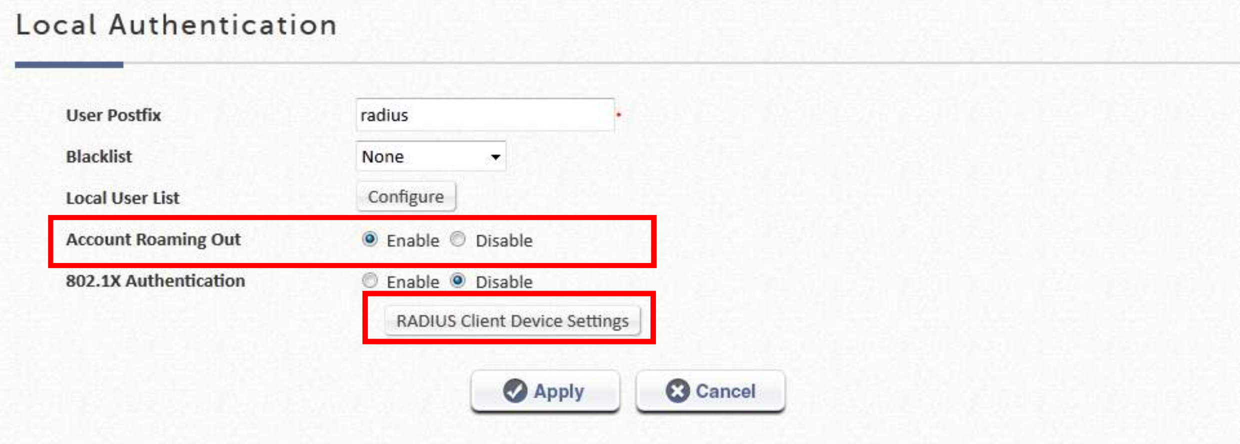
4.5.2 Local/ On-Demand Account Roaming Out

The built-in user account databases both Local and On-Demand of the WLAN controller may be used for other WLAN controllers as their external RADIUS authentication database. This application offers the ability to refer to a single central WLAN controller for account credential lookup during the authentication process, and is ideal for enterprises or businesses with multiple branch offices.



Main Office Configuration

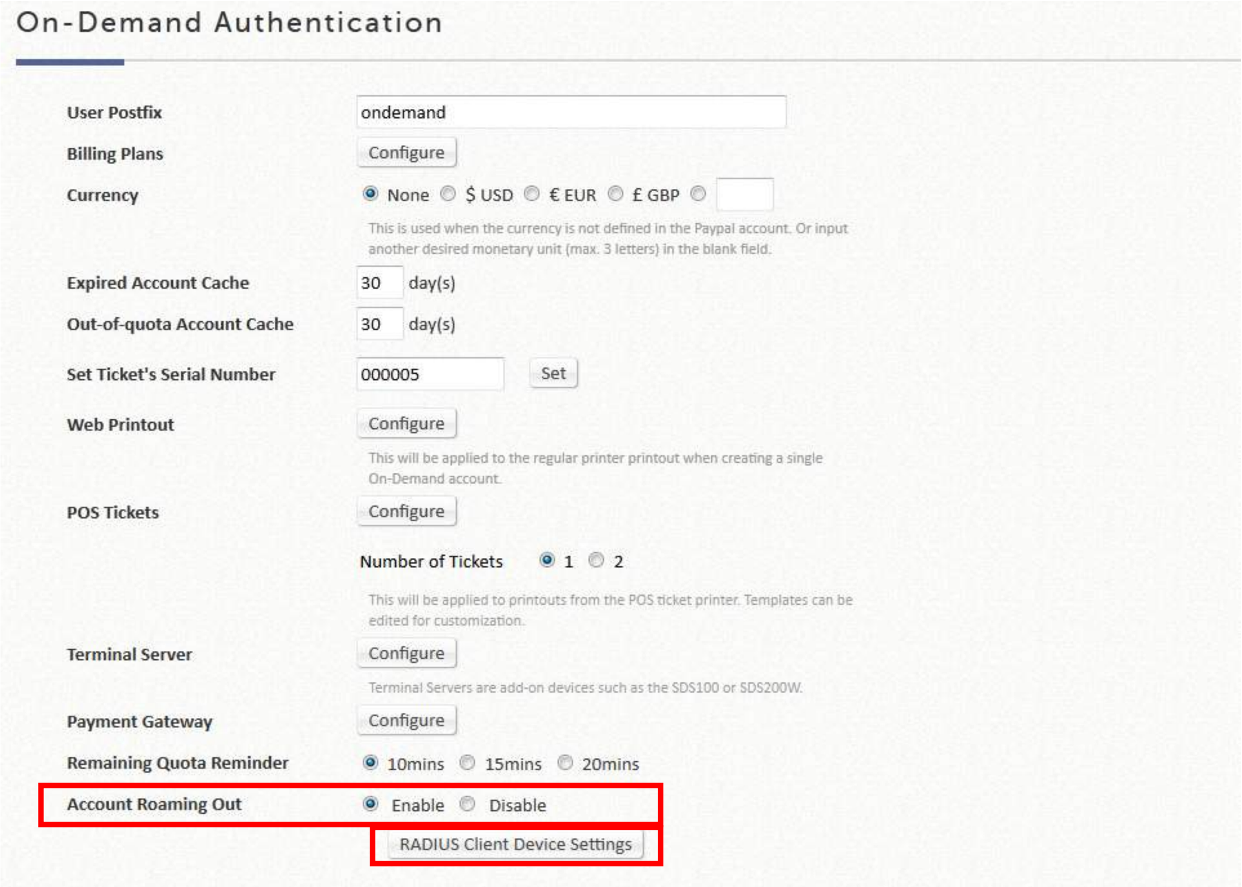
To use Local user database as the RADIUS database of another controller, configured at the page ”*Main Menu > Users > Internal Authentication > Local*“



Local Authentication

User Postfix	radius
Blacklist	None
Local User List	Configure
Account Roaming Out	● Enable ○ Disable
802.1X Authentication	○ Enable ● Disable
	RADIUS Client Device Settings

To use On-Demand user database as the RADIUS database of another controller, configuration at the page “*Main Menu > Users > Internal Authentication > On-Demand”*



On-Demand Authentication

User Postfix: ondemand

Billing Plans: Configure

Currency: ● None ○ $ USD ○ € EUR ○ £ GBP ○

This is used when the currency is not defined in the Paypal account. Or input another desired monetary unit (max. 3 letters) in the blank field.

Expired Account Cache: 30 day(s)

Out-of-quota Account Cache: 30 day(s)

Set Ticket's Serial Number: 000005 Set

Web Printout: Configure

This will be applied to the regular printer printout when creating a single On-Demand account.

POS Tickets: Configure

Number of Tickets ● 1 ○ 2

This will be applied to printouts from the POS ticket printer. Templates can be edited for customization.

Terminal Server: Configure

Terminal Servers are add-on devices such as the SDS100 or SDS200W.

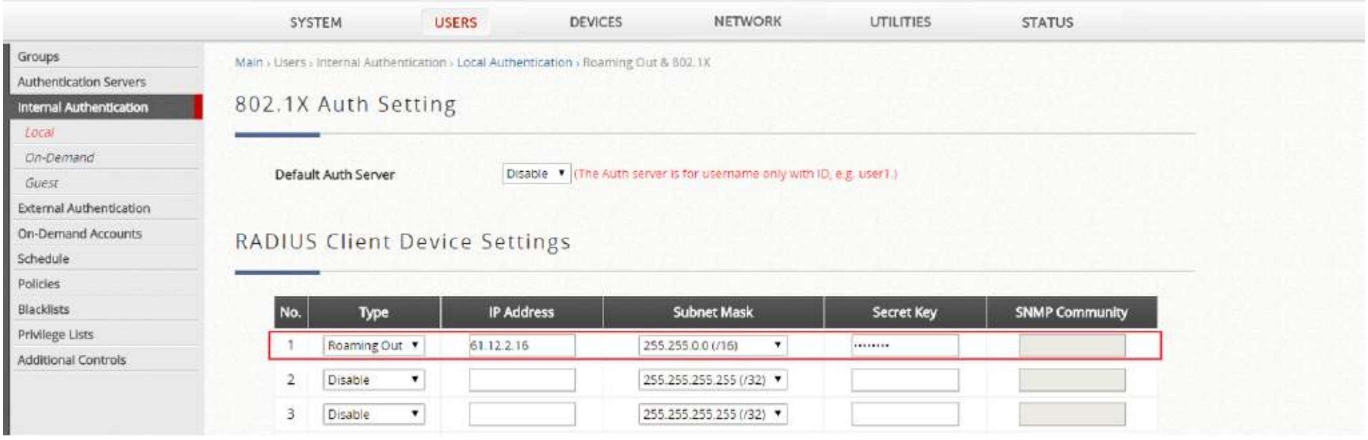
Payment Gateway: Configure

Remaining Quota Reminder: ● 10mins ○ 15mins ○ 20mins

Account Roaming Out: ● Enable ○ Disable

RADIUS Client Device Settings

After enabling the Account Roaming Out feature for Local or On-Demand database, administrators are able to click the button of RADIUS Client Device Settings to specify the WLAN controller IP Address/Subnet Mask which is allowed to behave as a RADIUS client and authenticate against this WLAN controller's built-in databases.



Main › Users › Internal Authentication › Local Authentication › Roaming Out & 802.1X

802.1X Auth Setting

Default Auth Server: Disable (The Auth server is for username only with ID, e.g. user1.)

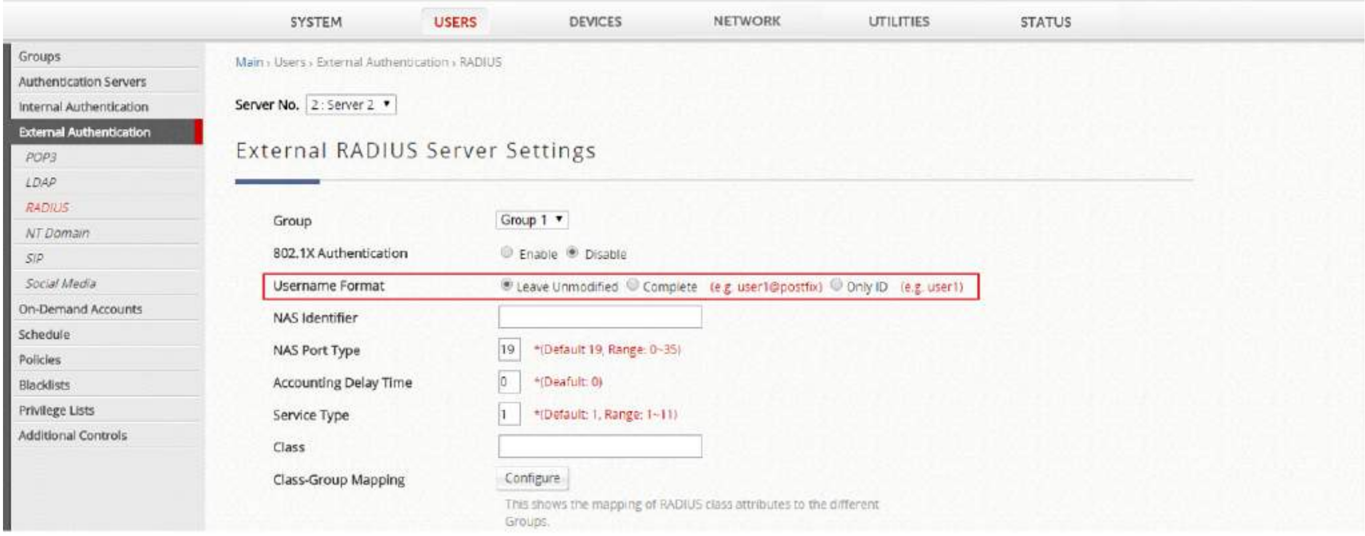
RADIUS Client Device Settings

No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	Roaming Out	61.12.2.16	255.255.0.0 (/16)	••••••••	
2	Disable		255.255.255.255 (/32)		
3	Disable		255.255.255.255 (/32)		

Note: Please make sure that the user database postfixes are configured without conflicting with one another over the two Controllers.

Branch Office Gateway Configuration

It is recommended to select “Leave Unmodified” for Username Format
Leave Unmodified: WLAN controller will directly transfer what client types in Username
Complete: both the username and postfix will be transferred to the RADIUS server for authentication
Only ID: only the username will be transferred to the external RADIUS server for authentication

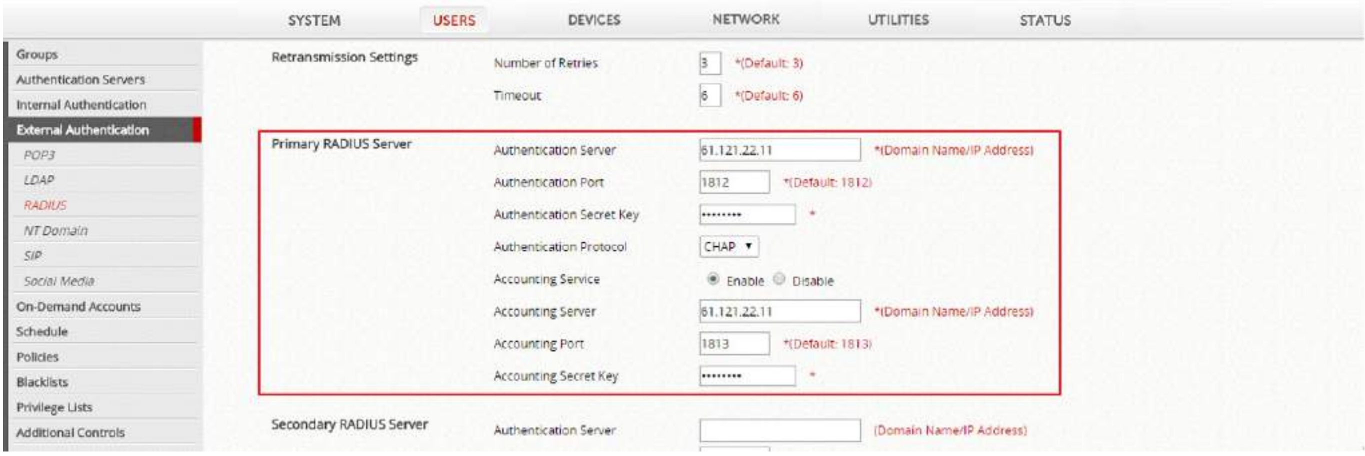


Server No. 2 : Server 2 ▾

External RADIUS Server Settings

Group: Group 1 ▾
802.1X Authentication: ○ Enable ● Disable
Username Format: ● Leave Unmodified ○ Complete (e.g. user1@postfix) ○ Only ID (e.g. user1)
NAS Identifier:
NAS Port Type: 19 *(Default 19, Range: 0~35)
Accounting Delay Time: 0 *(Deafult: 0)
Service Type: 1 *(Default: 1, Range: 1~11)
Class:
Class-Group Mapping: Configure
This shows the mapping of RADIUS class attributes to the different Groups.

The Main Office Gateway acts as Primary RADIUS Server. The related configuration follows the network environment of main office gateway.



Retransmission Settings
Number of Retries: 3 *(Default: 3)
Timeout: 6 *(Default: 6)

Primary RADIUS Server
Authentication Server: 61.121.22.11 *(Domain Name/IP Address)
Authentication Port: 1812 *(Default: 1812)
Authentication Secret Key: •••••••• *
Authentication Protocol: CHAP ▾
Accounting Service: ● Enable ○ Disable
Accounting Server: 61.121.22.11 *(Domain Name/IP Address)
Accounting Port: 1813 *(Default: 1813)
Accounting Secret Key: •••••••• *

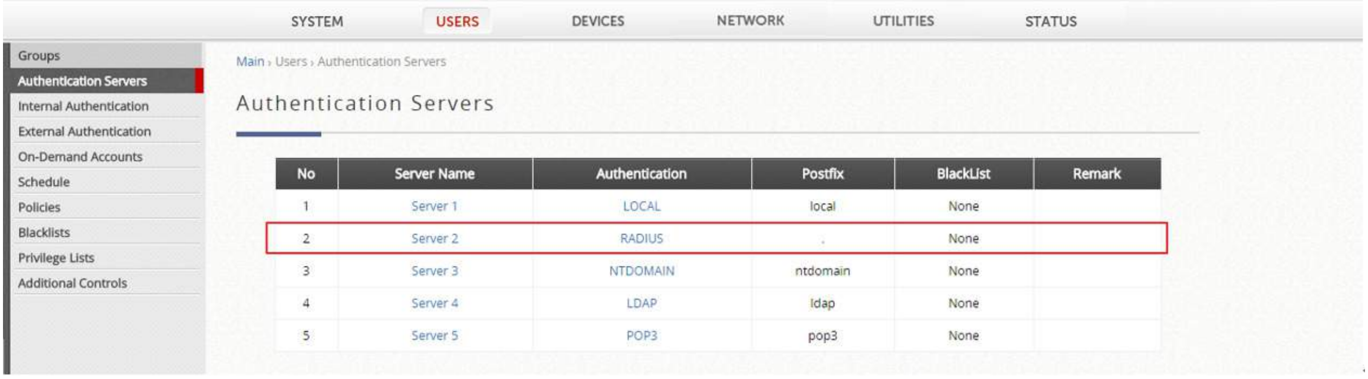
Secondary RADIUS Server
Authentication Server: (Domain Name/IP Address)

Administrators should confirm the postfix of RADIUS authentication method on the Authentication Servers page.

Note: Make sure that the Local/ On-demand postfix at main gateway is not duplicated in any postfix on the remote gateway

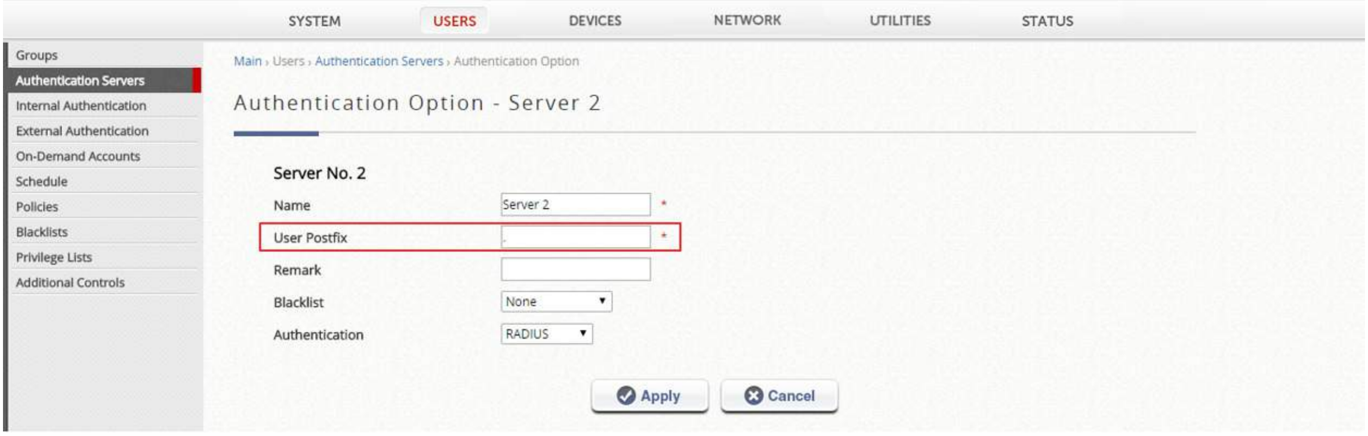
Main Office Gateway		Remote Office Gateway	
Local	@Edgecore.com	Local	local
Ondemand	od	Ondemand	ondemand
RADIUS	radius	RADIUS	.
NTDomain	ntdomain	NTDomain	ntdomain
LDAP	ldap	LDAP	ldap
POP3	pop3	POP3	pop3

Note: If both the Local and On-Demand databases are configured as roaming out server, please set the Postfix in the remote controller as "." (dot).



Authentication Servers

No	Server Name	Authentication	Postfix	BlackList	Remark
1	Server 1	LOCAL	local	None	
2	Server 2	RADIUS	.	None	
3	Server 3	NTDOMAIN	ntdomain	None	
4	Server 4	LDAP	ldap	None	
5	Server 5	POP3	pop3	None	



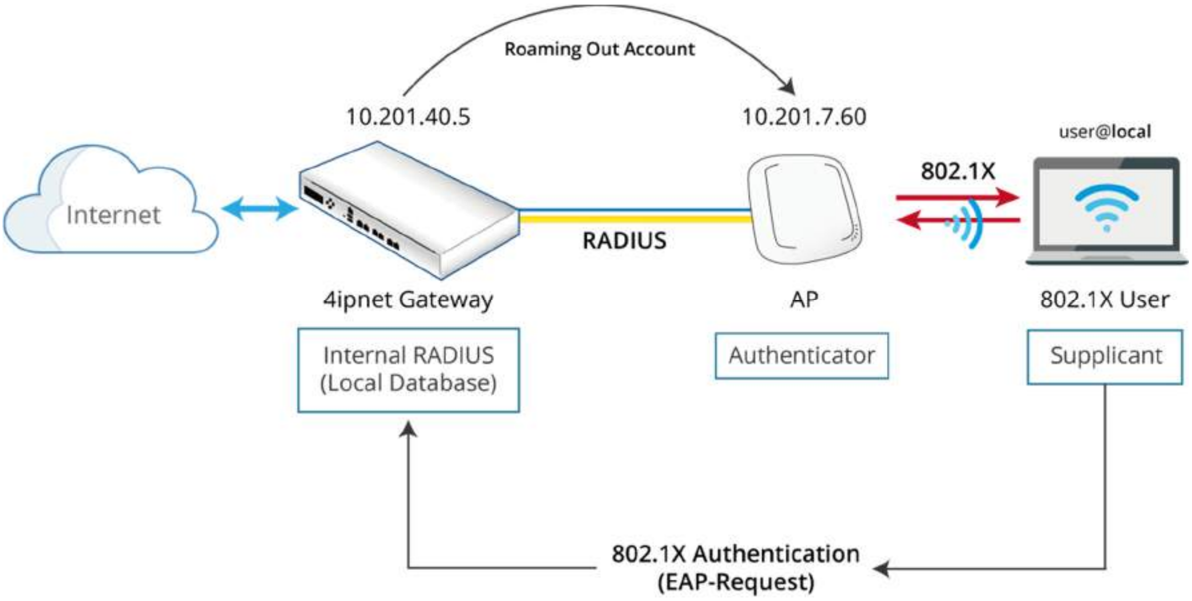
Authentication Option - Server 2

Server No. 2

Name	Server 2 *
User Postfix	. *
Remark	
Blacklist	None
Authentication	RADIUS

4.5.3 WLAN Controller as an Internal RADIUS Server

Thanks to the built-in Local and On-Demand database, the WLAN controller is able to act as the RADIUS server and the gateway in the same box. The Edgecore AP can act as the authenticator for clients with 802.1x authentication. Please check below topology and configuration.

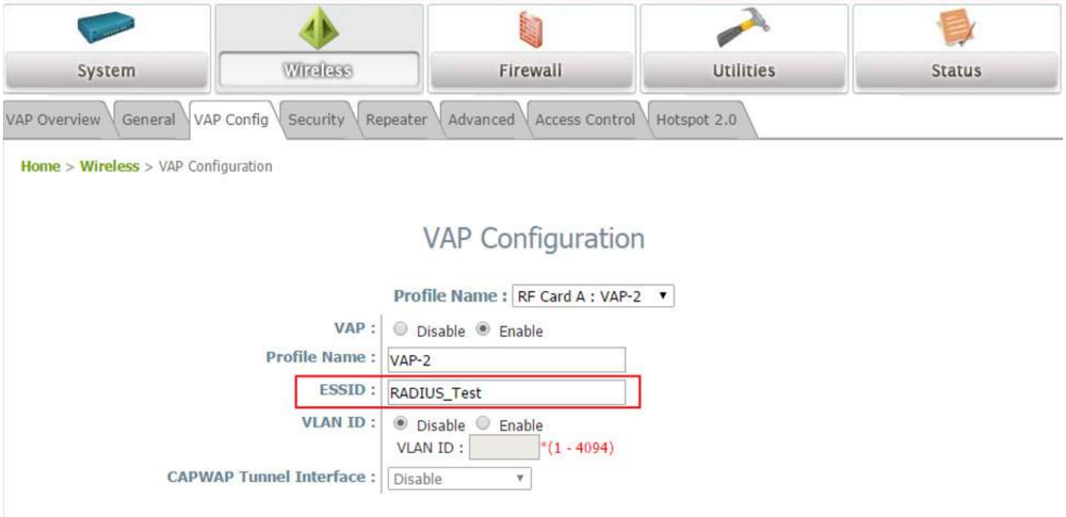


WLAN Controller Configuration

Select "Roaming Out" under Type, enter the WAN IP address of the Access Point (Access point acts as a RADIUS authenticator), and select the appropriate subnet mask and enter a secret key. (ie. 12345678)

AP Configuration

Enable a VAP and give it an appropriate SSID, ie. RADIUS_Test



VAP Configuration

Profile Name : RF Card A : VAP-2

VAP : ○ Disable ● Enable

Profile Name : VAP-2

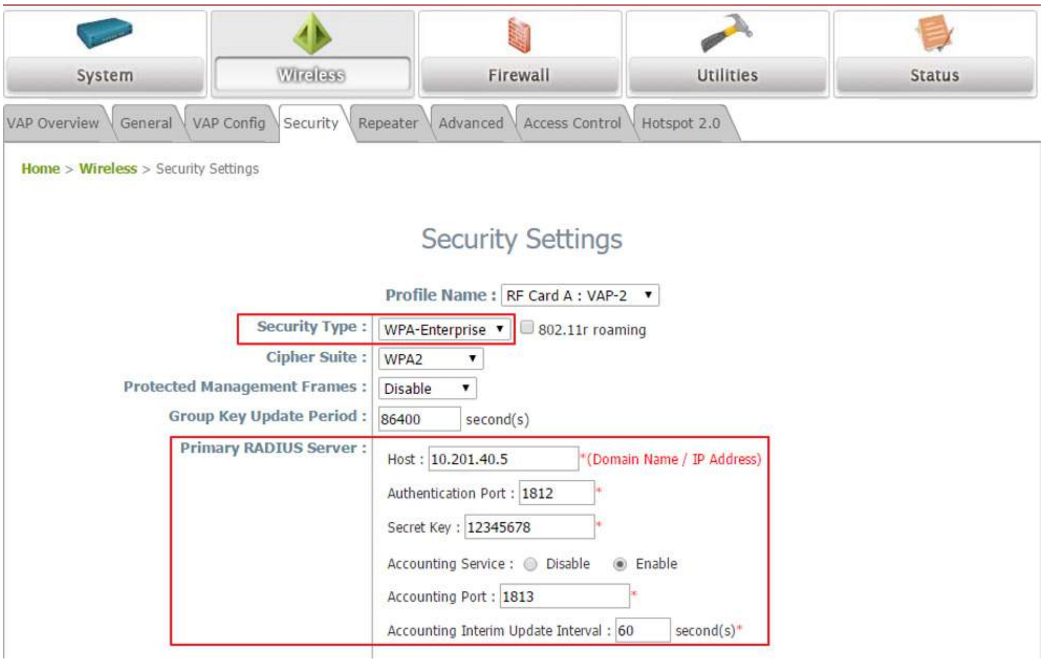
ESSID : RADIUS_Test

VLAN ID : ● Disable ○ Enable

VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface : Disable

Go to Security Settings within the same VAP and select WPA-Enterprise as the security type, which supports 802.1x RADIUS authentication. Then, administrators type in the Gateway's IP address as primary RADIUS Server. In this case, enabling accounting service is not mandatory.



Home > Wireless > Security Settings

Security Settings

Profile Name : RF Card A : VAP-2

Security Type : WPA-Enterprise □ 802.11r roaming

Cipher Suite : WPA2

Protected Management Frames : Disable

Group Key Update Period : 86400 second(s)

Primary RADIUS Server :

Host : 10.201.40.5 *(Domain Name / IP Address)

Authentication Port : 1812 *

Secret Key : 12345678 *

Accounting Service : ○ Disable ● Enable

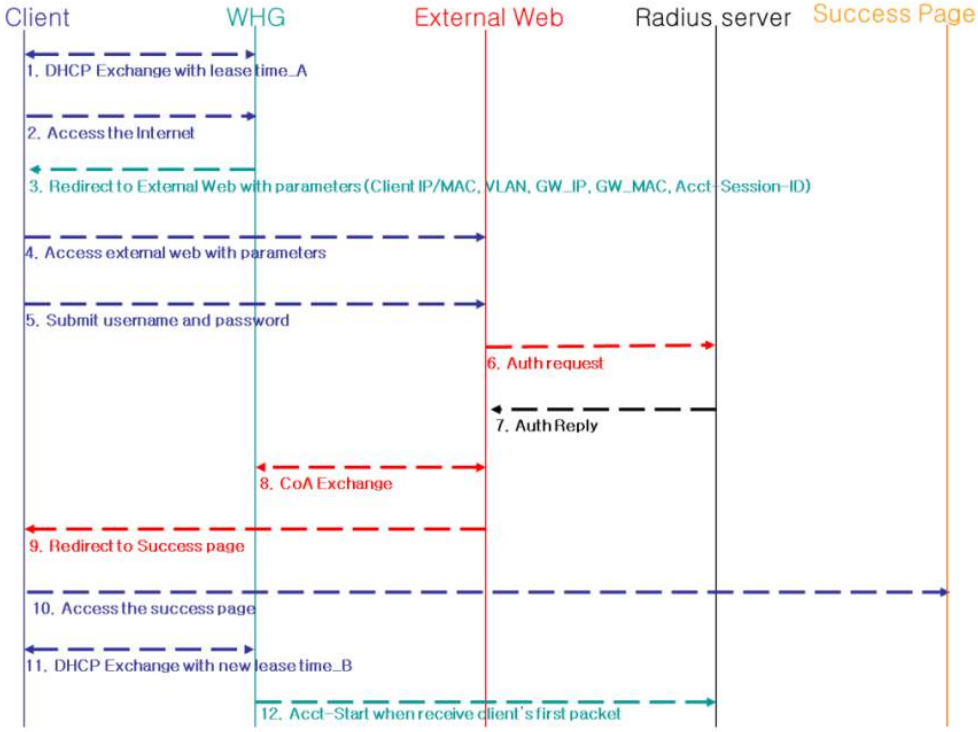
Accounting Port : 1813 *

Accounting Interim Update Interval : 60 second(s)*

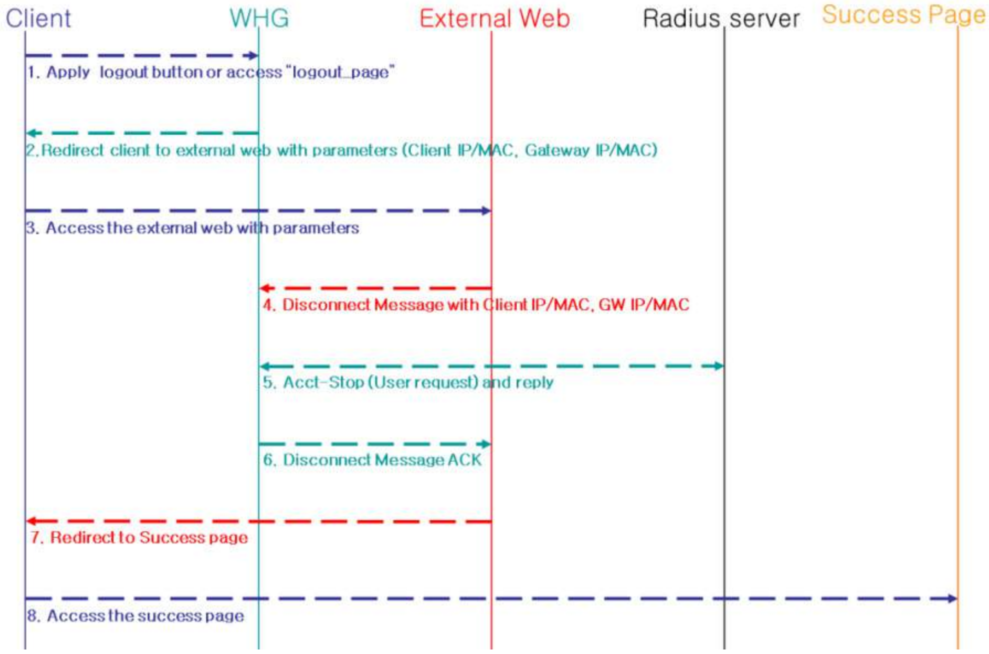
4.5.4 DM and CoA

The WLAN controller supports RADIUS authentication through UAM (Universal Access Method), which is to say that the auth-request is sent out by the WLAN controller. The DM&CoA feature allows an External Web Server to directly send auth-requests to the RADIUS Server. Subsequently, the External Web Server sends the authentication result to the WLAN controller in the form of CoA exchange. Likewise, the WLAN controller is able to accept Disconnect Messages from the External Web Server.

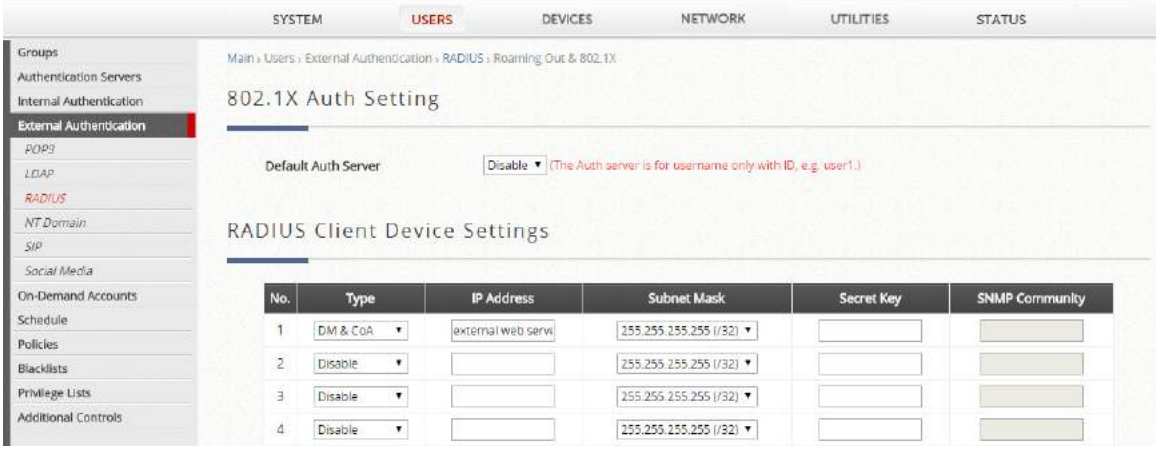
The following illustrates the authentication flow via CoA


Client
WHG
External Web
Radius server
Success Page
1. DHCP Exchange with lease time_A
2. Access the Internet
3. Redirect to External Web with parameters (Client IP/MAC, VLAN, GW_IP, GW_MAC, Acct-Session-ID)
4. Access external web with parameters
5. Submit username and password
6. Auth request
7. Auth Reply
8. CoA Exchange
9. Redirect to Success page
10. Access the success page
11. DHCP Exchange with new lease time_B
12. Acct-Start when receive client's first packet

The following illustrates the authentication flow via CoA


Client
WHG
External Web
Radius server
Success Page
1. Apply logout button or access "logout_page"
2.Redirect client to external web with parameters (Client IP/MAC, Gateway IP/MAC)
3. Access the external web with parameters
4. Disconnect Message with Client IP/MAC, GW IP/MAC
5. Acct-Stop (User request) and reply
6. Disconnect Message ACK
7. Redirect to Success page
8. Access the success page

WLAN controller DM&CoA configuration over *Main › Users › External Authentication › RADIUS › Roaming Out & 802.1X*



Main › Users › External Authentication › RADIUS › Roaming Out & 802.1X

802.1X Auth Setting

Default Auth Server: Disable ▾ (The Auth server is for username only with ID, e.g. user1.)

RADIUS Client Device Settings

No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	DM & CoA ▾	external web serv	255.255.255.255 (/32) ▾		
2	Disable ▾		255.255.255.255 (/32) ▾		
3	Disable ▾		255.255.255.255 (/32) ▾		
4	Disable ▾		255.255.255.255 (/32) ▾		

DM & CoA Supported Attributes

Authentication with CoA-Request requires the following attributes:

1. Called-Station-Id (Controller WAN's MAC)
2. Calling-Station-Id (Client's MAC)
    User-Name
    Framed-IP-Address

Change of Authorization with CoA-Request for an authenticated user requires the following attributes:

1. Called-Station-Id (Controller WAN's MAC)
2. Calling-Station-Id or User-Name or Acct-Session-Id

Disconnect Request for an authenticated user requires the following attributes:

1. Called-Station-Id (Controller WAN's MAC)
2. Calling-Station-IdorUser-Name or Acct-Session-Id

Supported Vendor Specific Attributes include:

Idle-Timeout
Session-Timeout
Acct-Interim-Interval
Class
WISPr-Bandwidth-Min-Up
WISPr-Bandwidth-Max-Up
WISPr-Bandwidth-Min-Down
WISPr-Bandwidth-Max-Down
WISPr-Session-Terminate-Time
WISPr-Session-Terminate-End-Of-Day
WISPr-Billing-Class-Of-Service
ZVendor-Byte-Amount-4GB
ZVendor-Byte-Amount

ZVendor-MaxByteIn-4GB
ZVendor-MaxByteIn
ZVendor-MaxByteOut-4GB
ZVendor-MaxByteOut
ZVendor-Group
Chargeable-User-Identity

HTTPparameters sent from the WLAN controller to the External Web Server includes:

1. loginurl (Login URL)
2. remainingurl (Remaining URL)
3. vlanid (VLAN ID)
4. iface (Service Zone)
5. gwip (Controller'sIP)
6. gwmac (Controller'sMAC)
7. client_ip (Client IP)
8. ipv6_addr (Client IPv6 Address)
9. umac (Client MAC)
10. acct_session_id (Ifapplicable)

4.5.5 MAC ACL in the WLAN Controller

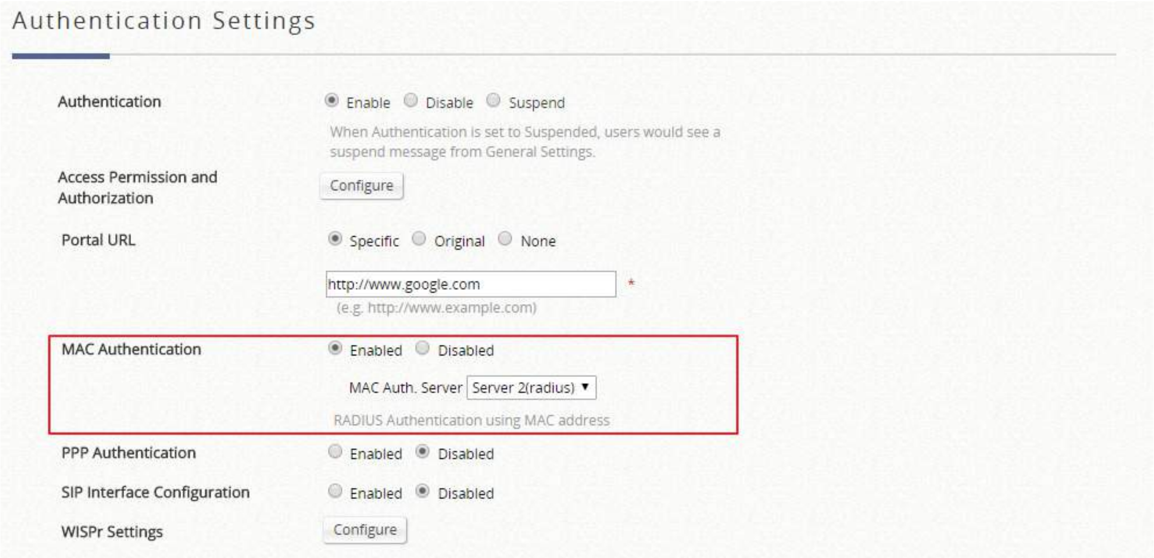
MAC ACL is a MAC Address Access Control List where specific MAC addresses may be listed for access filtering, either allow, deny or disable which can be configured in the page *Main › Users › Additional Control › MAC Address Control*

MAC Access Control List: The administrator may configure restraining measures to MAC address, either MAC allow or deny list. User authentication is still required for MAC ACL Allowed users.

Note: The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. Colons will be automatically inserted by the system.

4.5.6 MAC Address Authentication

MAC Authentication: the RADIUS MAC authentication feature in each Service Zone is enabled, if the connected device has its MAC address entered in the configured RADIUS Server, the Controller will automatically authenticate and grant access immediately if authentication succeeds. Users will experience transparent login.



Authentication Settings

Authentication ● Enable ○ Disable ○ Suspend

When Authentication is set to Suspended, users would see a suspend message from General Settings.

Access Permission and Authorization [Configure]

Portal URL ● Specific ○ Original ○ None

http://www.google.com *

(e.g. http://www.example.com)

MAC Authentication ● Enabled ○ Disabled

MAC Auth. Server: Server 2(radius) ▼

RADIUS Authentication using MAC address

PPP Authentication ○ Enabled ● Disabled

SIP Interface Configuration ○ Enabled ● Disabled

WISPr Settings [Configure]

Primary RADIUS Server: to configured the RADIUS authentication server from *Main › Users › External Authentication › RADIUS*

Authentication Server: to enter the IP address of RADIUS authentication server
Authentication Port: to enter the port number of RADIUS authentication server, default is 1812
Authentication Secret Key: to enter the shared secret that will be used to validate communication with the RADIUS authentication server.
Authentication Protocol: normally first tries CHAP and falls back to PAP if the server rejects the CHAP request.
Accounting Server: to enter the IP address of RADIUS accounting server
Accounting Port: to enter the port number of RADIUS accounting server, default is 1813
Accounting Secret Key: to enter the shared secret that will be used to validate communication with the RADIUS accounting server.

4.5.7 PPP Authentication

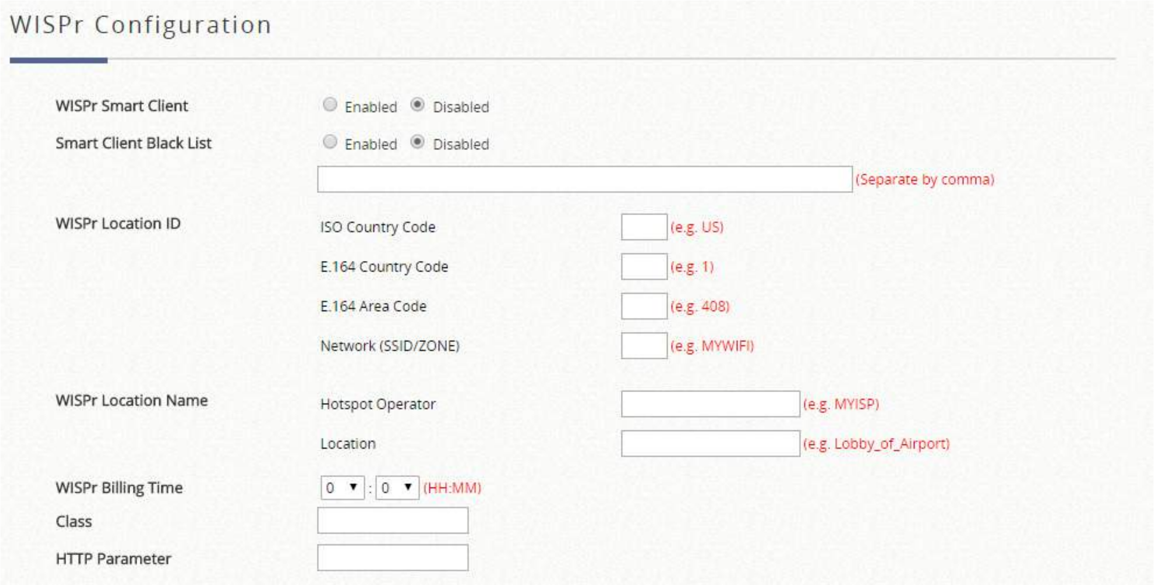
Point-to-Point Protocol (PPP) is a data link protocol commonly used in establishing a direct connection between two networking nodes. When this feature is enabled for service in each Service Zone, end users may configure a dial-up connection setting with a valid username and password (support only Local and RADIUS users). Once the dial-up connection has been established, the user would have been authenticated successfully without further UAM login.

4.5.8 WISPr for ISP Roaming

Roaming capability is an essential feature requirement for large scale deployments or alliance co-operation for operators who seek to provide network access for other ISP subscribers to generate more sources of profit.

WISPr or Wireless Internet Service Provider roaming - Pronounced "whisper," is a draft protocol submitted to the Wi-Fi Alliance that allows users to roam between wireless internet service providers, in a fashion similar to that used to allow cell phone users to roam between carriers. A RADIUS server is used to authenticate the subscriber's credentials.

WLAN controllers support the WISPr attributes required to establish roaming relationship with most roaming brokers in the market such as Boingo, iPass Connect etc. If a RADIUS server has been configured, the WISPr attributes used during RADIUS authentication can be defined here in each Service Zone .



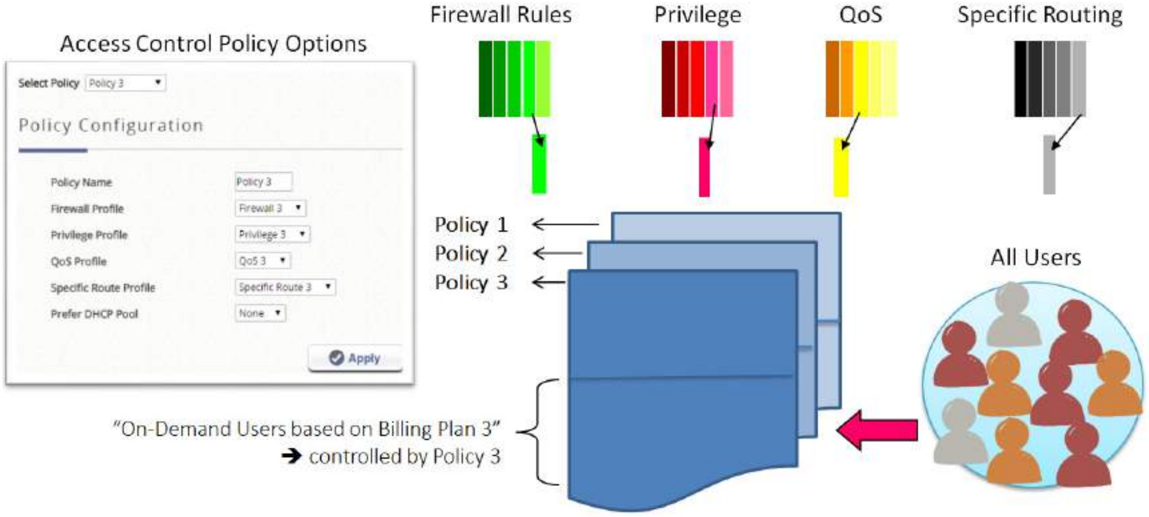
WISPr Configuration

WISPr Smart Client	○ Enabled ● Disabled	
Smart Client Black List	○ Enabled ● Disabled	
	(Separate by comma)	
WISPr Location ID	ISO Country Code	(e.g. US)
	E.164 Country Code	(e.g. 1)
	E.164 Area Code	(e.g. 408)
	Network (SSID/ZONE)	(e.g. MYWIFI)
WISPr Location Name	Hotspot Operator	(e.g. MYISP)
	Location	(e.g. Lobby_of_Airport)
WISPr Billing Time	0 : 0 (HH:MM)	
Class		
HTTP Parameter		

WISPr Smart Client: to enable if you wish to allow customers with a roaming account from a WISPr agent (iPass, WiFi Skype, Boingo, and etc.) to access your internet. Make sure to Enable the HTTPS Protected Login field under "*System > General*" in order for roaming software on the client's device to work properly.
Smart Client Black List: Fill in the WISPr agent names and enable to block users from that particular WISPr roaming agent to access your internet. For example, if you fill in "ipassconnect", the iPass clients will be denied roaming access in your network.
WISPr Location ID: These attributes, which enable wireless hotspot providers to customize their web portals, are based on the client device location and are RADIUS vendor-specific attributes (VSAs).
WISPr Location Name: These attributes, which enable wireless hotspot providers to customize their web portals, are based on the client device location and are RADIUS vendor-specific attributes (VSAs).
WISPr Billing Time: to set RADIUS account billing time.

5 How to configure User Policies

User Policy, as the term suggests, are profiles of network governing constraints which are enforced upon users, including firewall rules, login schedule, routing rules and session allowances. There is a Global policy, which will be applied if a user belongs to a Group not bound to any Policy. The number of Policy profiles will be model dependent.



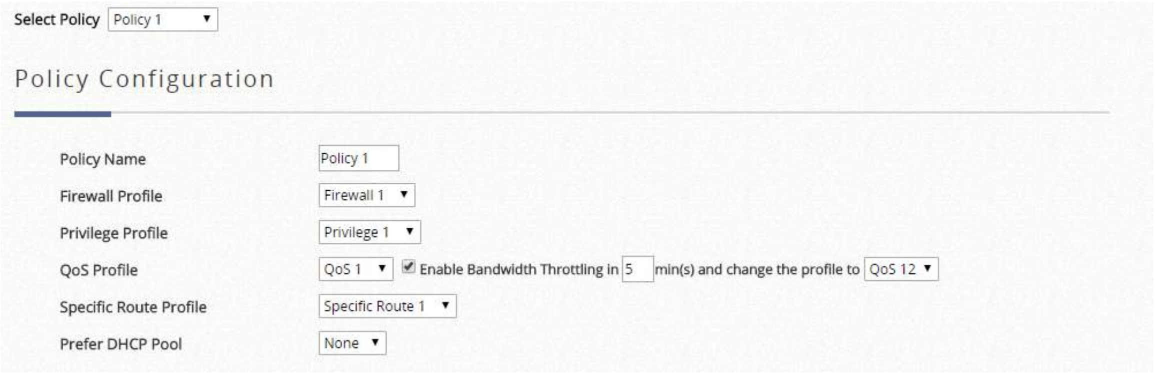
Select Policy: Policy 3

Policy Configuration

Policy Name: Policy 3
Firewall Profile: Firewall 3
Privilege Profile: Privilege 3
QoS Profile: QoS 3
Specific Route Profile: Specific Route 3
Prefer DHCP Pool: None

"On-Demand Users based on Billing Plan 3"
➔ controlled by Policy 3

1.1 User Policy



Select Policy: Policy 1

Policy Configuration

Policy Name	Policy 1
Firewall Profile	Firewall 1
Privilege Profile	Privilege 1
QoS Profile	QoS 1 ☑ Enable Bandwidth Throttling in 5 min(s) and change the profile to QoS 12
Specific Route Profile	Specific Route 1
Prefer DHCP Pool	None

Select Policy: to choose which User Policy profile to configure.

Firewall Profile: to specify the protocols & rules that will be enforced to users governed by User Policy

- Service Protocol: This link leads to a policy's Service List page where the administrator can defined a list of services by protocols (TCP/UDP/ICMP/IP). The service names defined here forms a choice list for configuring firewall rules.
- User Firewall Rules: This link leads to the policy's Firewall Rules page. Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on. Each firewall rule is defined by Source, Destination, a Service out of the policy's Service List and a Pass/Block action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced; it can be set to Always, Recurring or One Time.

Privilege Profile: to configure the flexibility and privilege for each user.

- Password Change: to set “Allow” so that when a user with the applied Privilege Profile has the flexibility to change their login password
- Maximum Concurrent Sessions: when a user with this Privilege Profile reaches the session limit, this user will be implicitly suspended from any new connection for a fixed time period.
- Disable timeout for this group: to set “Enable” so that the clients who are applied by this policy will not be logged out automatically. Note that enable this option may increase the loading of the system

QoS Profile: to edit traffic configuration. If the bandwidth throttling is required, administrators are able to check the checkbox and select the second QoS after the specific duration when clients complete authentication.

- Traffic Class: Each policy can be configured its own traffic class and different Traffic Class Remarking can be set for IPv4 and IPv6 in the same Traffic Profile.
- Group Total Downlink: to define the maximum bandwidth allowed to be shared by clients within this group.
- Group Total Uplink: to define the maximum bandwidth allowed to be shared by clients within this group.
- Individual Maximum Downlink: to define the maximum bandwidth allowed for an individual client within this group; the Individual Maximum Downlink cannot exceed the value of Group Total Downlink.
- Individual Maximum Uplink: to define the maximum bandwidth allowed for an individual client within this group; the Individual Maximum Uplink cannot exceed the value of Group Total Uplink.
- Individual Request Downlink: to define the guaranteed minimum bandwidth allowed for an individual client within this group; the Individual Request Downlink cannot exceed the value of Group Total Downlink and Individual Maximum Downlink.
- Individual Request Uplink: to define the guaranteed minimum bandwidth allowed for an individual client within this group; the Individual Request Uplink cannot exceed the value of Group Total Uplink and Individual Maximum Uplink.

Specific Route Profile: The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.

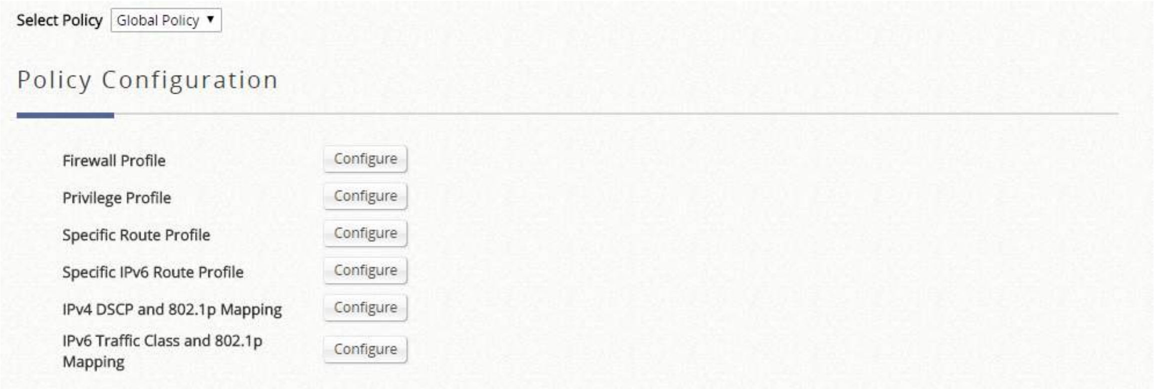
Preferred DHCP Pool: if the authenticated users release the expired DHCP IP addresses, the system will issue IP addresses within the preferred DHCP Pool. It can be configured in Service Zone DHCP.

Note: if the clients associate to the managed APs under split tunnel, only firewall profile setting can be applied. However, selected 802.11ac wave 2 APs support QoS profile, which means there is a bandwidth control function for each authenticated client under split tunnel.

Note: Policy 1-x (model dependent) can be applied to specific group of users in different Service Zones. Policy 1 has the highest priority, and Policies with the higher number shall be the first applied Policy.

Note: If a user is not applied by any User Policy, at least, the Global Policy will take effect.

1.2 Global Policy



Select Policy Global Policy ▼

Policy Configuration

Firewall Profile — Configure

Privilege Profile — Configure

Specific Route Profile — Configure

Specific IPv6 Route Profile — Configure

IPv4 DSCP and 802.1p Mapping — Configure

IPv6 Traffic Class and 802.1p Mapping — Configure

Firewall Profile: to specify the protocols & rules that will be enforced to users governed by Global Policy.

- Service Protocol: This link leads to a policy's Service List page where the administrator can defined a list of services by protocols (TCP/UDP/ICMP/IP). The service names defined here forms a choice list for configuring firewall rules.
- User Firewall Rules: This link leads to the policy's Firewall Rules page. Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on. Each firewall rule is defined by Source, Destination, a Service out of the policy's Service List and a Pass/Block action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced; it can be set to Always, Recurring or One Time.
- DoS Protection:

Privilege Profile: to configure the maximum concurrent sessions for each user. When a user with this Privilege Profile reaches the session limit, this user will be implicitly suspended from any new connection for a fixed time period.

Specific Route Profile: The routing rules to be applied to all users.

Specific IPv6 Route Profile: The routing rules to be applied to all users.

IPv4 DSCP and 802.1p Mapping: This criteria enables the static mapping configuration from IPv4 DSCP tag into the desired IEEE 802.1p traffic class for sending in the managed VLAN network.

IPv6 Traffic Class and 802.1p Mapping: This criteria enables the static mapping configuration from IPv6 traffic class tag into the desired IEEE 802.1p traffic class for sending in the managed VLAN network.

Select one of the policies in the drop-down list and start configuring each attribute by clicking Configure. After the setting, remember to always click Apply to save the changes made. Note again that the Global Policy is the policy that applies to all users in all service zones that is not explicitly governed by a policy profile.

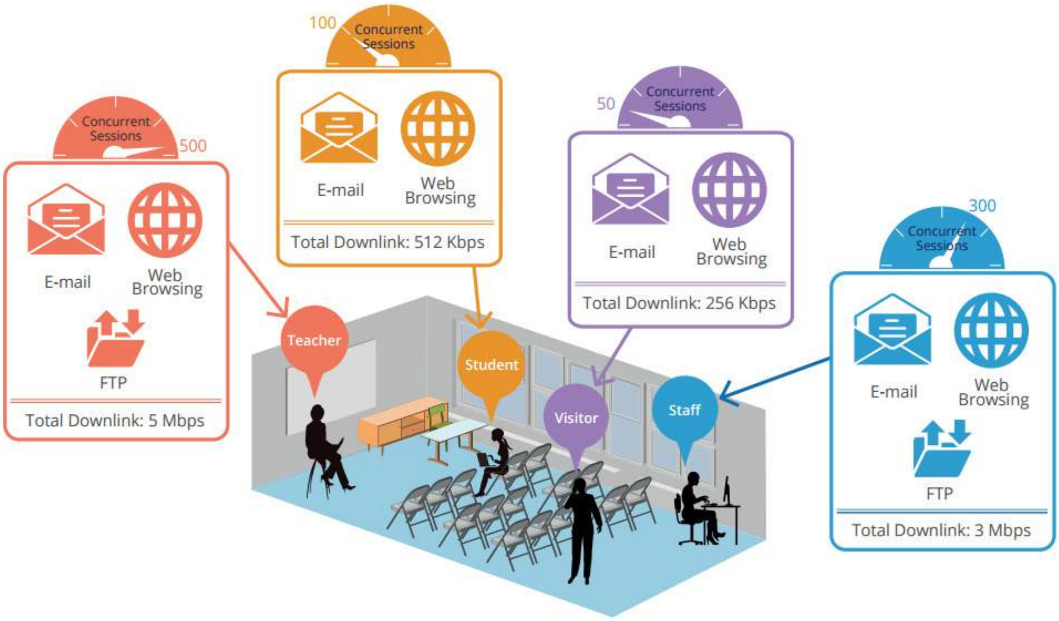
Note: The Policy enforcement priority is as below. Therefore, if the administrator does not specify a Group or Policy in the hierarchy of configurations for a particular user, the system will govern them by Global Policy.

Group-Service Zone Mapping > Service Zone default Policy > Global Policy

6 How to generate your scenarios

6.1 User Groups, User Policies, Service Zones and Schedule

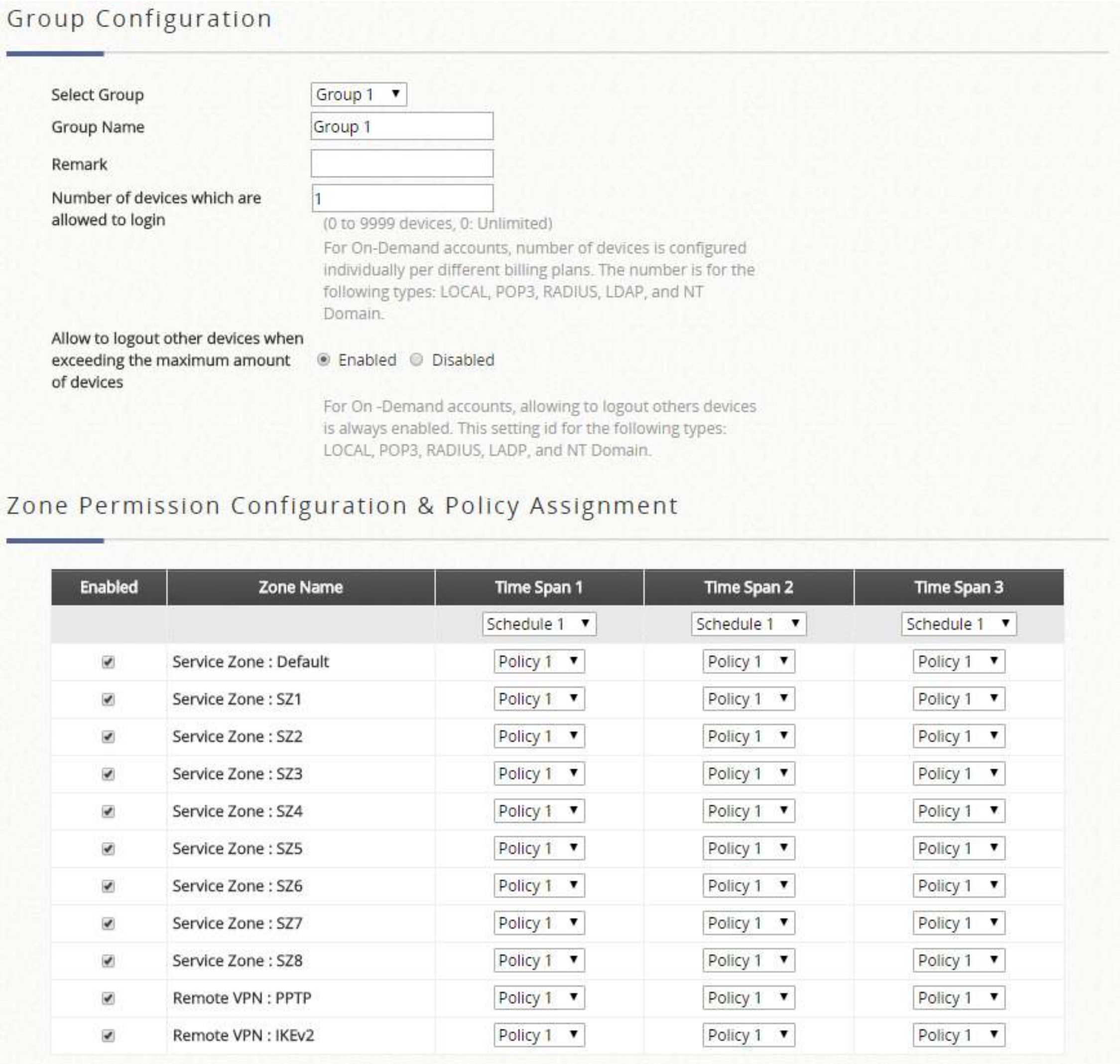
A User Group within different Service Zones can be applied with different policies, or the administrator can select one of the defined policies to apply it to groups within a certain Service Zone. For example, students can be applied with different network access right while accessing from classroom region instead of teacher or staff office region.



Service Zone Permission Configuration & Policy Assignment

Group and Policy profiles are separated for more flexibility. This allows users of the same Groups to be bound with different Policies according to Service Zone Permission Configuration & Policy Assignment settings the administrator defines. Check the Enabled checkboxes to allow users of this Group to access the corresponding Service Zones.

For instance, a local account user from group 1 may be imposed by policy 1 in service zone 1, but policy 3 when he goes to service zone 3. While an on-demand account user from group 3 may be imposed by policy 3 in service zone 3, and he/she cannot access the service zone 1.



Group Configuration

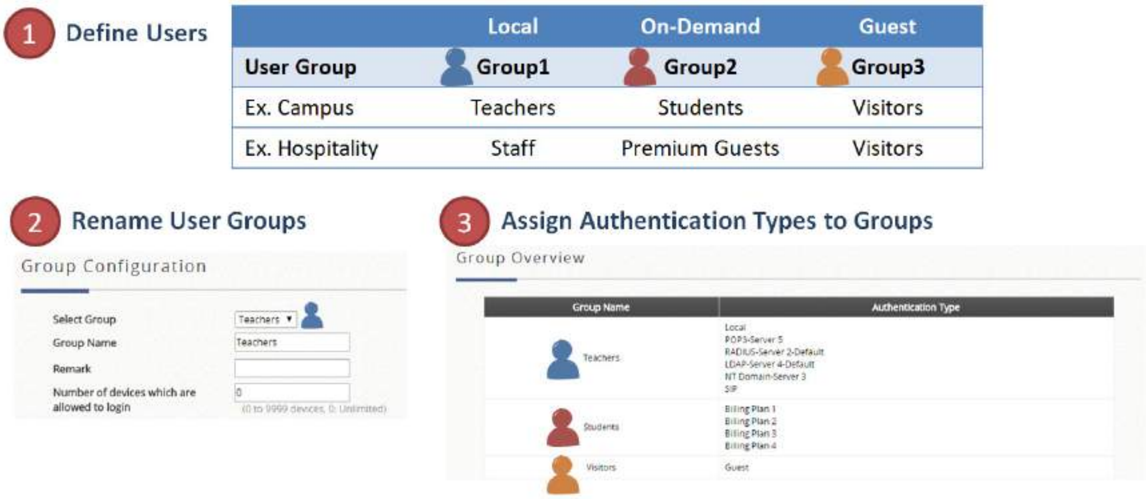
Select Group	Group 1 ▼
Group Name	Group 1
Remark	
Number of devices which are allowed to login	1 (0 to 9999 devices, 0: Unlimited) For On-Demand accounts, number of devices is configured individually per different billing plans. The number is for the following types: LOCAL, POP3, RADIUS, LDAP, and NT Domain.
Allow to logout other devices when exceeding the maximum amount of devices	● Enabled ○ Disabled For On -Demand accounts, allowing to logout others devices is always enabled. This setting id for the following types: LOCAL, POP3, RADIUS, LADP, and NT Domain.

Zone Permission Configuration & Policy Assignment

Enabled	Zone Name	Time Span 1	Time Span 2	Time Span 3
		Schedule 1 ▼	Schedule 1 ▼	Schedule 1 ▼
☑	Service Zone : Default	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ1	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ2	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ3	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ4	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ5	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ6	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ7	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ8	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Remote VPN : PPTP	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼
☑	Remote VPN : IKEv2	Policy 1 ▼	Policy 1 ▼	Policy 1 ▼

Group Overview

User Group is a set of users that admin considers they share some extent of similar characteristics, i.e. role based. For example, in campus, there are teachers, students, and visitor, in general. Therefore an IT staff may set up three Groups that distinguish these three categories of Internet service users apart by giving these Group different permissions of Internet accessibility.



1 Define Users

	Local	On-Demand	Guest
User Group	Group1	Group2	Group3
Ex. Campus	Teachers	Students	Visitors
Ex. Hospitality	Staff	Premium Guests	Visitors

2 Rename User Groups

Group Configuration

Select Group	Teachers ▼
Group Name	Teachers
Remark	
Number of devices which are allowed to login	0 (0 to 9999 devices, 0: Unlimited)

3 Assign Authentication Types to Groups

Group Overview

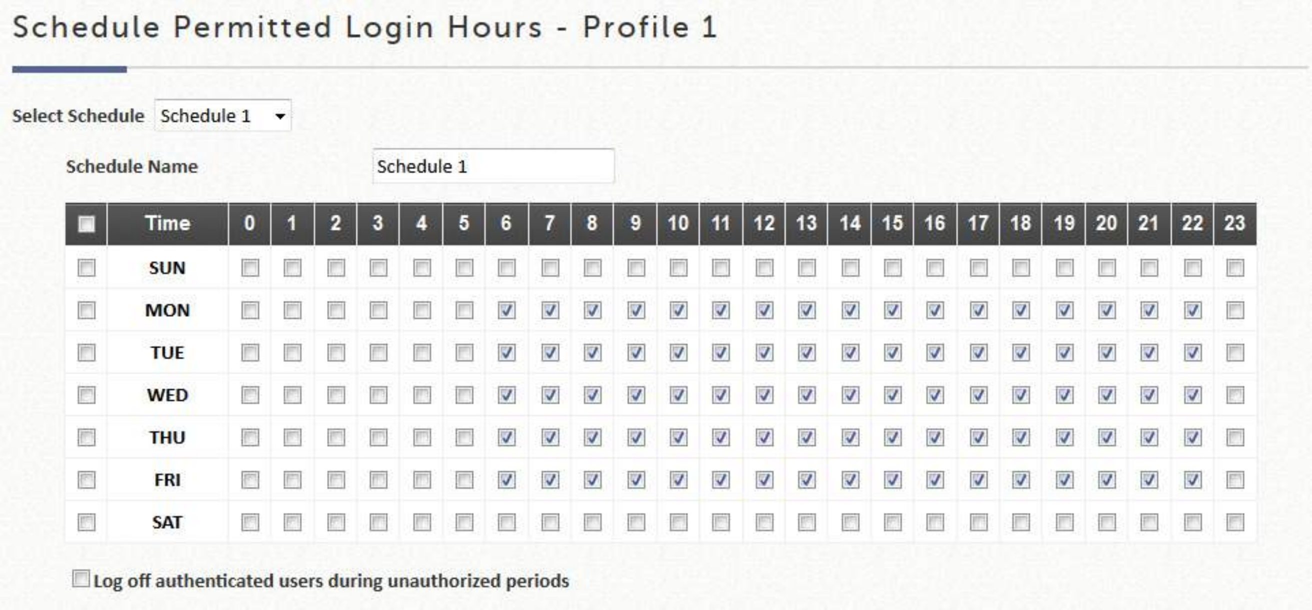
Group Name	Authentication Type
Teachers	Local POP3-Server 5 RADIUS-Server 2-Default LDAP-Server 4-Default NT Domain-Server 3 SIP
Students	Billing Plan 1 Billing Plan 2 Billing Plan 3 Billing Plan 4
Visitors	Guest

In the WLAN controllers, there are eight to twenty-four Group profiles, depending on the model capacity. Besides, the system does provide several flexibilities for mapping from different authentication options

Auth Options	Assigned User Group by	Configuration Path
Local	Each Local account	*Users > Authentication > Local > Configure > Local User List > username* (There is an Applied Group row for admin to determine the attribute)
On-Demand	Each On-Demand billing plan	*Main › Users › Internal Authentication › On-Demand Authentication › Billing Configuration*
Guest	All belong to the same User Group	*Main › Users › Internal Authentication › Guest Authentication*
One Time Password	All belong to the same User Group	*Main › Users › Internal Authentication › One Time Password Authentication*
POP3	All belong to the same User Group	*Main › Users › External Authentication › POP3*
LDAP	LDAP Attributes	*Main › Users › External Authentication › LDAP › LDAP Attributes Mapping*
RADIUS	RADIUS Class Attributes	*Main › Users › External Authentication › RADIUS › RADIUS Class Mapping*
NT Domain	All belong to the same User Group	*Main › Users › External Authentication › NT Domain*
SIP	All belong to the same User Group	*Main › Users › External Authentication › SIP*
Social Media Login	All belong to the same User Group	*Main › Users › External Authentication › Social Media Login*

Schedule

The Schedule is the assignment of allowed user login periods from clock time on an hourly basis. The unchecked time slots imply that user under this policy will be unable to login under that specific time interval.



Schedule Permitted Login Hours - Profile 1

Select Schedule: Schedule 1

Schedule Name: Schedule 1

□	Time	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
□	SUN	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	MON	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□
□	TUE	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□
□	WED	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□
□	THU	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□
□	FRI	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□
□	SAT	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

□ Log off authenticated users during unauthorized periods

Defined Schedules are then applied in Group Configuration.

6.2 Blacklists and Privilege Lists

Network operators may want to limit the accessibility of certain accounts or devices from authentication or association from time to time. This section describes the ways in which user or device restrictions may be achieved.

- Blacklists
- IP Privilege List
- IPv6 Privilege List
- MAC Privilege List
- MAC Access Control List

6.2.1 Blacklists

Blacklist profiles can be defined and each active authentication option may be configured with one of these blacklist profiles. A user account listed on the blacklist is not allowed to log into the system, the client's access will be denied.
Select Blacklist: to select one blacklist from the drop-down menu and this blacklist will be applied to this specific authentication option.
Blacklist Name: names on the Blacklists can be configured to be case insensitive.
Case Insensitive with blacklist:
Add/Delete: Up to 40 Usernames can be added to a blacklist with the User Name in the format without postfix, since the blacklist is applied to specific authentication server (Main › Users › Authentication Servers › Authentication Option)

6.2.2 IP Privilege List

The Privilege function supports three types of privilege list based on IP address, MAC address and IPv6 address. Devices specified in the list require NO authentication to access the network. Note that a User Group can be assigned to Devices on the IP Privilege List but not on the MAC Privilege List.

Add: IP Address in IPv4 format and User Group fields are required. MAC Address field can be an option for the matching condition with the IP Address. Noted that the privileged clients are still able be applied the user policy.
Delete: to delete the selected existed IP privilege entry
Backup List: to back up the whole entries in txt file for further application
Restore List: it is helpful to batch create the privilege entries by upload a .txt file with IP Address, Remark, MAC Address, Group

6.2.3 IPv6 Privilege List

The Privilege function supports three types of privilege list based on IP address, MAC address and IPv6 address. Devices specified in the list require NO authentication to access the network.

Add: IP Address in IPv6 format and User Group fields are required. MAC Address field can be an option for the matching condition with the IP Address. Noted that the privileged clients are still able be applied the user policy.
Delete: to delete the selected existed IP privilege entry
Backup List: to back up the whole entries in txt file for further application
Restore List: it is helpful to batch create the privilege entries by upload a .txt file with IP Address, Remark, MAC Address, Group

6.2.4 MAC Privilege List

The Privilege function supports three types of privilege list based on IP address, MAC address and IPv6 address. Devices specified in the list require NO authentication to access the network.

Add: MAC Address field is required. Noted the privileged clients will NOT be applied any user policy.
Delete: to delete the selected existed IP privilege entry
Backup List: to back up the whole entries in txt file for further application
Restore List: it is helpful to batch create the privilege entries by upload a .txt file with MAC Address, Reserved, Remark

6.2.5 MAC Access Control List

MAC ACL is a MAC Address Access Control List where specific MAC addresses may be listed for access filtering, either allow, deny or disable.
MAC Access Control List: The administrator may configure restraining measures to MAC address, either MAC allow or deny list. User authentication is still required for MAC ACL Allowed users.

Note: The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. Colon will be automatically inserted by the system.

6.3 Additional Control

Additional configurations are in this section. They are User Session Control, Built-in RADIUS Server Settings, Customization, Remaining Time Reminder, and MAC ACL.

User Session Control
Idle Timeout: Configure the time base without activity to deem as idle timeout.
Idle Detect Interval: The time interval for checking for whether the idle criteria are reached. Successive accumulation of idle intervals exceeding the Idle time configure above, will induce an idle timeout action where the user will be logged out.

Traffic Direction for Idle Timeout: The user’s activity inspection may be checked as uplink or both.
Threshold for Idle Traffic Detection: Designate the threshold where traffic flow smaller than the value configured will be considered as being idle.
Charge Traffic to/from Host in Walled Garden List: For usage or volume type accounts in the On-Demand user database, administrator has the option to charge or not charge visits to websites that are listed in the walled garden or walled garden ad list.
Kick out user when user’s IP change: An option for the administrator whether or not disconnection is forced by the system whenever a user changes IP address.
Log NAT Mapped in User Session Log: To show mapping for each connection from Private IP/Port to Public IP/Port, this option must be enabled.

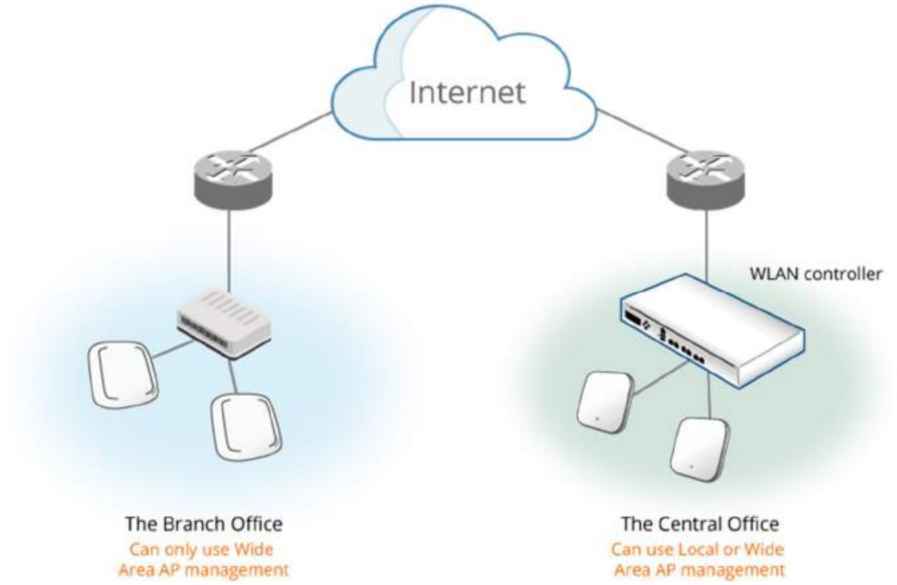
Built in RADIUS Server Settings
Session Timeout: For created sessions generated by users authenticated via build-in RADIUS server (could be account roaming user), the timeout range may be configured here manually. Please configure this attribute carefully.
Idle Timeout: For users authenticated via build-in RADIUS server (could be account roaming user), the idle timeout range may be configured here manually. Please configure this attribute carefully.
Interim Update: For users authenticated via build-in RADIUS server (could be account roaming user), the accounting interval may be configured here manually. Please configure this attribute carefully.
Certificate: Certificate for built-in RADIUS server will be selectable

Remaining Quota Reminder
Time and Cut-off reminder: This is the option for the system to display a warning message to On-Demand users that their time based account quota is about to run out.
Volume Reminder: This is the option for the system to display a warning message to On-Demand users that their volume based account quota is about to run out.
Reminder Refresh Time: The Login Success page with the remaining quota can set to refresh every 10/15/20 minutes to show the updated remaining quota.

MAC Access Control List
Please refer to “*session 6.2.5 MAC Access Control List*”

7 How to configure Access Point in LAPM

Management of access points are always of vital importance for a network administrator. Thus Edgecore delivers a simple, straightforward set of management tools to help you achieve it. Generally, we suggest a centralized network with a controller in charge of access points both on the WAN side and the LAN side. We call the WAN-side AP management 'Wide Area AP Management,' due to its scalability across the Internet or intranet, and the LAN-side AP management 'Local Area AP Management.' Below illustrates the concept of these two types of management.


Internet
WLAN controller
The Branch Office
Can only use Wide Area AP management
The Central Office
Can use Local or Wide Area AP management

Edgecore WLAN controller models have different manageability with Edgecore access points, i.e., admin should make sure what AP models your WLAN controller supports.

This chapter further explores how a wireless network environment can be set up in terms of AP management, explaining the aspects such AP discovery & Adding, general AP settings, and so on. It is noteworthy that this section only deals with a clear setting process of various common AP management settings, not advanced ones, for instance, "rogue AP detection" or "AP load balancing." The higher-level applications are introduced in the reference guide.

- AP List and Overview
- AP Adding and Configuration
- Template
- AP Firmware Management
- WDS Management
- Rogue AP Detection
- AP Load Balancing

7.1 AP List and Overview

All of the supported APs under management of the system will be shown Overview table and in the AP

List. The AP's name will be shown as a hyperlink. Click the hyperlink of each managed AP to further configure (General Setting, LAN Setting, Wireless LAN, Layer 2 Firewall) the AP. Click the hyperlink of the shown Status of each managed AP for detailed status information of the AP (System Status, Service Zone Status, Wireless Status, Access Control Status, and Associated Client Status).

Add: This is elaborated in Section 7.2 AP Adding and Configuration
Reboot: Check the checkboxes and click "Reboot" to restart the selected Access Points if needed
Enable: Check the checkboxes and click "Enable" to change the AP Management Status if needed
Disable: Check the checkboxes and click "Disable" to change the AP Management Status if needed
Delete: Check the checkboxes and click "Delete" to remove the selected Access Points from the AP List
Apply Template: Check the checkboxes and click "Apply Template" to apply a pre-configured template to the selected APs. Templates can be configured at Main Menu › Access Points › Local Area AP Management › Templates. Select 1 of the 3 templates from the drop-down list and click "Apply”
Reset to Default: Check the checkboxes and click "Reset" to factory default and restart the selected Access Points. The AP will be erased from AP List.
Apply by Service Zone: Check the checkboxes and click "Apply by Service Zone" to specify which VAPs are to be enabled on the Access Points. These VAPs map to the enabled Service Zones on the Controller. Check the checkboxes of the desired corresponding Service Zones and click "Apply" to apply Service Zones. Note that this option is only available when the system is in Tag-Based Mode.

7.2 AP Adding and Configuration

Once all AP’s are properly connected, admin can then start adding them to the management list. This can be accomplished by clicking “Add” above the AP List. APs can be added individually or in batches. This is determined by the Add Method; Select “Add AP” from the drop-down list to add APs individually, or select “Find Multiple APs” to add in batches.

Add AP
To add an AP, specify an AP Name and enter its IP and MAC address. After filling in all the fields, click Apply at the bottom of the page to add the AP (to add an AP, it doesn’t necessarily have to be online). Check the AP List to confirm the adding.

Find Multiple APs
AP Type: to specify the AP model, only select one model at a time
Service Zone: to re-assign the IP addresses for scanned APs based on the Service Zone configuration
VLAN for Management: following the specific Service Zone and select the allowed VLAN as AP management VLAN
Admin Settings Used to Discover: the recommended discovery method is Factory Default due to AP’s default setting. Just click Scan Now without changing any of the configurations on their AP’s.
Manual: the other option used if the IP addresses of the AP’s have been changed to those other than 192.168.1.1. Type in the range of the IP addresses you would like to scan through, enter the AP’s admin password, and click Scan Now.

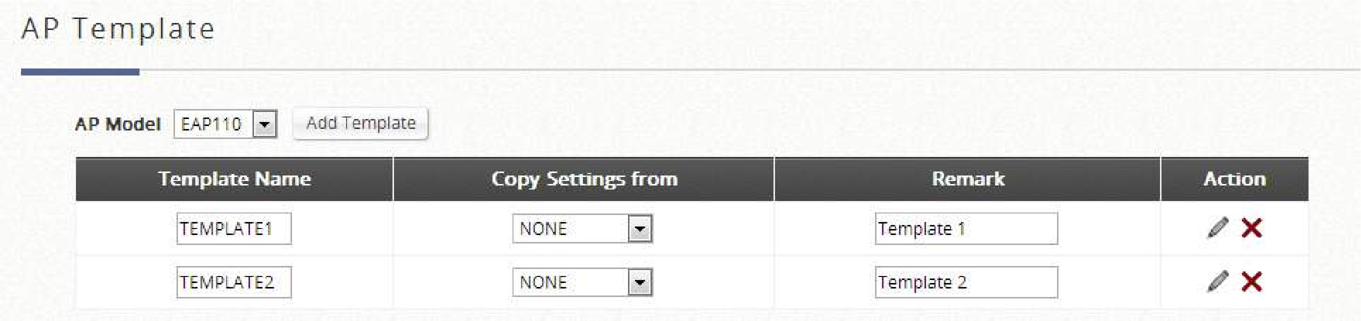
Background AP Discovery: the feature could be enabled to scan the wireless environment every fixed period of time based on admin's setting. Click Configure to set up the function and the configurations are similar to above method.

Discovery Results: the table displays all the AP's found currently alive. After finding the AP, admin can further set up the template to be applied and the operating channel, and furthermore put the AP under a specific service zone you have enabled.

Noted: It might take some time for the controller to discover AP's. Please wait for a moment until the AP you are scanning for is displayed on the Discovery Results list.

7.3 Template

As said in the introduction, admin is capable of utilizing AP configuration templates to eliminate tedious AP configuration tasks one by one. Click Configure for more detailed settings, such as the subnet mask and the default gateway. Up to eight templates can be saved for each AP model. Click the "Add Template" button to increase templates and click the "Edit" icon represented under the Action column to edit configurations.

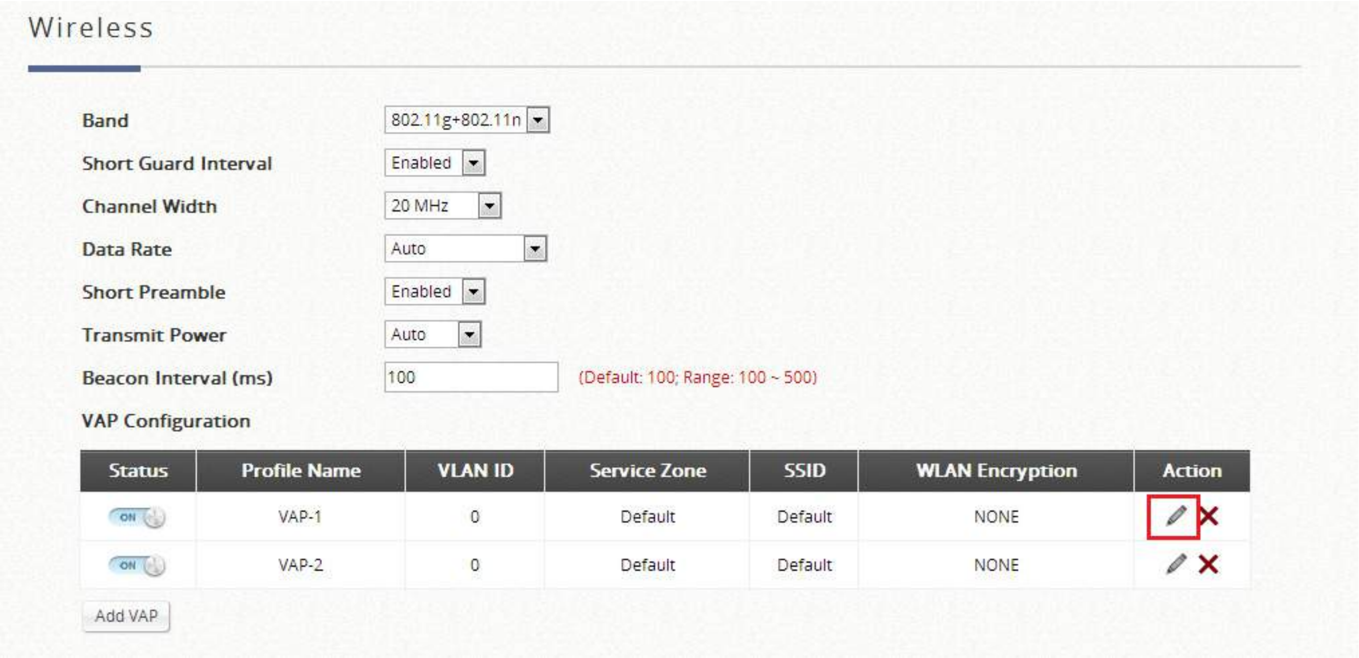


AP Template

AP Model: EAP110

Template Name	Copy Settings from	Remark	Action
TEMPLATE1	NONE	Template 1	✎ ✕
TEMPLATE2	NONE	Template 2	✎ ✕

General Settings such as the Default Gateway of the AP and etc. are configured here. Wireless Settings and applicable Service Zones/SSIDs are also configurable here.



Wireless

Band	802.11g+802.11n
Short Guard Interval	Enabled
Channel Width	20 MHz
Data Rate	Auto
Short Preamble	Enabled
Transmit Power	Auto
Beacon Interval (ms)	100 (Default: 100; Range: 100 ~ 500)

VAP Configuration

Status	Profile Name	VLAN ID	Service Zone	SSID	WLAN Encryption	Action
ON	VAP-1	0	Default	Default	NONE	✎ ✕
ON	VAP-2	0	Default	Default	NONE	✎ ✕

The SSID and Wireless Security can be specified per Service Zone. Depending on deployment needs, access filtering may be imposed on individual Service Zone's managed AP devices. The Wireless Settings section under the VAP Configuration list allows the specification of wireless settings including Access Control list.

For each Service Zone, administrators can set up the wireless security profile, including Authentication and Encryption. The options available are Open System, Share Key, WPA, WPA2 or WPA/WPA2 Mixed.

WEP: When Authentication is Open System or Share Key, WEP will be enabled.
WPA: When Authentication is WPA, WPA-PSK or WPA-RADIUS will be the options of WPA. For WPA-PSK, Passphrase or HEX can be selected.
WPA2: When Authentication is WPA, WPA-PSK or WPA-RADIUS will be the options of WPA. For WPA-PSK, Passphrase or HEX can be selected.
WPA/WPA2 Mixed: When Authentication is WPA, WPA-PSK or WPA-RADIUS will be the options of WPA. For WPA-PSK, Passphrase or HEX can be selected.

The MAC address field is for admin to type in the MAC addresses you would like to deny or allow. Status 'Denied' implies that you are configuring a black list. 'Allowed' implies that you are configuring a white list. 'Disable' implies that no access filtering is imposed regardless of the MAC entries configured below.

Status	MAC Address	The Action taken by the controller
Disabled		Controller does not enforce any MAC ACL on APs of this Service Zone
Allowed	Enabled	AP only allows devices with these addresses to associate with the APs of this Service Zone
Allowed	Disabled	AP does not allow devices with these addresses to associate with the APs of this Service Zone

Denied	Disabled	It allows devices with these addresses to associate with the APs of this Service Zone
Denied	Enabled	AP does not allow devices with these addresses to associate with the APs of this Service Zone

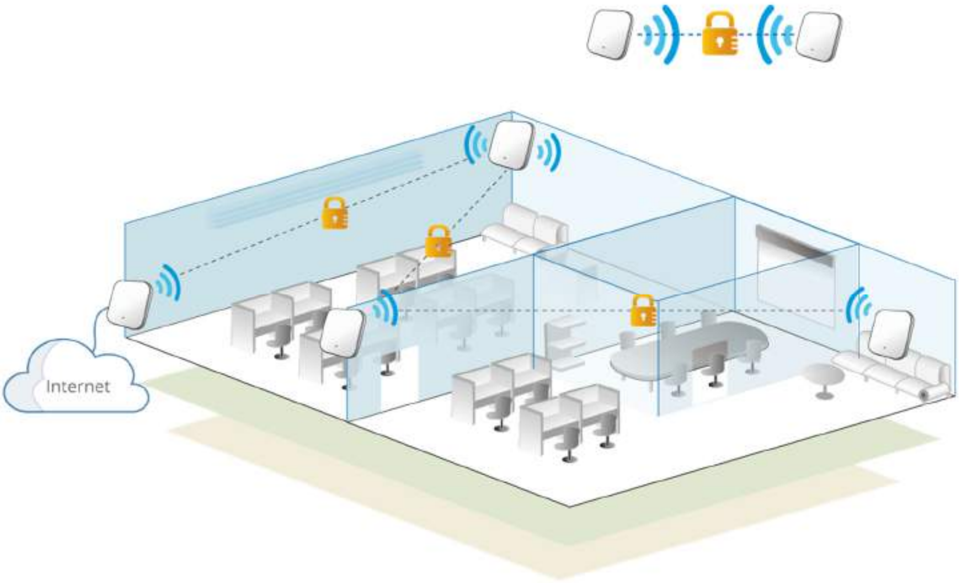
7.4 AP Firmware Management

Firmware upgrade matters because much of the software enhancements are released periodically for enhanced standards / features. The system offers an easy firmware upgrade process from the controller's AP management interface, allowing the administrator to upgrade multiple AP devices at once.
1. First add a firmware and select the firmware file at *"Devices > Local Area AP Management > Firmware"* and click Upload next to the row to store the AP firmware within the Controller.
2. Upgrade the necessary AP's by going to *"Devices > Local Area AP Management > Upgrade"*, select the AP's you would like to import the version to. When done with the selection, click Upgrade at the bottom of the page.

Noted: Please read through the release note of each AP firmware release to avoid any unexpected outcome.

7.5 WDS Management

WDS is the acronym for Wireless Distribution System, a function for extending the wireless coverage of the network with additional APs. The WDS management function helps administrators plan and setup a "Tree" structure of WDS network with managed APs.



WDS Status
The table shows the added APs in the WDS Tree with Security and Channel settings. More than one WDS

Tree can be set up in your network. This list can be set to refresh automatically at fixed intervals (10s, 20s, 30s, 40s, 50s, 60s).
Edit: Click "Edit" to change the WDS connection settings for the associated WDS Tree.

WDS Update
Add WDS Connection: to select New Parent AP and New Child AP from the respective drop-down list and click "Add". Note that a new WDS Tree will be added if the selected Parent AP is not in any of the current WDS Trees.
Move WDS Connection: to update the current WDS tree, select Update Parent AP and Update Child AP from the respective drop-down list and click "Move". Note that the link to the original parent AP of the selected Update Child AP will be removed.
Delete WDS Link: to delete a WDS link, select the AP from the drop-down list and click "Delete". Note that all WDS connections of the selected AP will be deleted including the WDS connections to its Child APs, and the Child APs without wired connection will become unreachable.

7.6 Rogue AP Detection

Rogue AP detection is another essential way of protecting your network environment. Local AP Management supports the detection of non-authorized access points present in the vicinity. Non-authorized access points pose a possible problem in terms of wireless interference.

General Configuration
Rogue AP Detection: to enable or disable the feature, if enabled, the system may take another effort to detect them.
Scanning Interval: to determine the scanning period
Sensor List: to select RF cards (only selected AP models) for the scanning job as sensor. It is able to check the scanning log by clicking the hyperlink of “View”
Trust APs: to add AP’s shown in the suspected rogue AP list to the trusted list for further management if it can be manually identified as a safe source.

Rogue AP List
Discovered access points are temporarily put in the Rogue AP list. Click one of the hyperlinked BSSID’s to see its detailed information. However, if admin recognized some of the listed APs as trusted, just check the checkboxes before the BSSID column and then click Add to Trusted AP List. This action will be recorded in the Trusted AP Configuration.

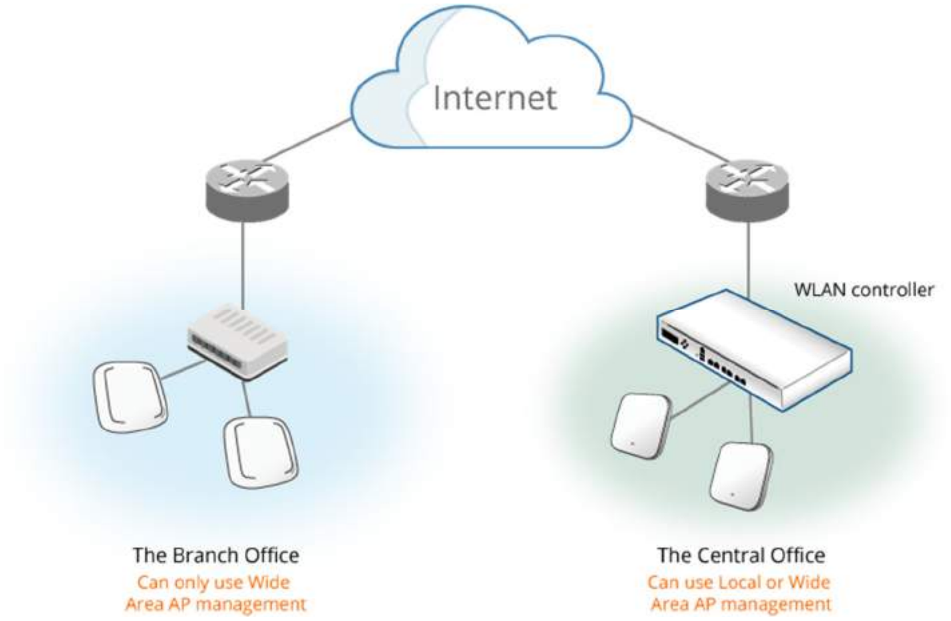
7.7 AP Load Balancing

This is a function that prevents managed APs from overloading. When the system detects the occurrence of APs' associated-client numbers exceeding a predefined threshold at circumstances and other APs in the same group are still below the threshold, the balancing function will be activated to decrease the overloading APs' transmit power and increase other available APs' transmit power; this will let other available APs have more chance to be associated. The system can divide the managed APs into groups; define the group threshold, and a time interval which will trigger the AP load balancing.

LAPM Load Balancing: to enable or disable the feature
Balance Internal: to initiate criteria of enforcement interval to trigger the AP load balancing
Cluster: The system can divide the managed APs into 3 different groups and perform transmit power management, each with individual client threshold
Device List: The grouping of AP devices can be done on the Device List page.

8 How to configure Access Point in WAPM

Management of access points are always of vital importance for a network administrator. Thus Edgecore delivers a simple, straightforward set of management tools to help you achieve it. Generally, we suggest a centralized network with a controller in charge of access points both on the WAN side and the LAN side. We call the WAN-side AP management 'Wide Area AP Management,' due to its scalability across the Internet or intranet, and the LAN-side AP management 'Local Area AP Management.' Below illustrates the concept of these two types of management.


Internet
WLAN controller
The Branch Office
Can only use Wide Area AP management
The Central Office
Can use Local or Wide Area AP management

Edgecore WLAN controller models have different manageability with Edgecore access points, i.e., admin should make sure what AP models your WLAN controller supports. It is worth noting that WAN-side AP's are supposed to have public IP addresses that are routable on the Internet. Main Benefits of Wide Area AP Management:

- Cross Layer 3 IP network management
- Centralized traffic forwarding for distributed remote AP sites.
- Graphical Map utility for easy reference and deployment planning.
- Traffic transmit statistics for 3rd party AP devices.
- CAPWAP support, complete tunnel and split tunnel.
- To manage APs physically deployed on the WAN side and LAN side of the controller

This section goes on to explain how to centrally manage the access points on the WAN from a WLAN controller.

- AP List
- Graphical Monitoring
- AP Adding and Configuration
- Template
- AP Firmware Management

- WDS Management
- Rogue AP Detection
- AP Load Balancing

8.1 AP List

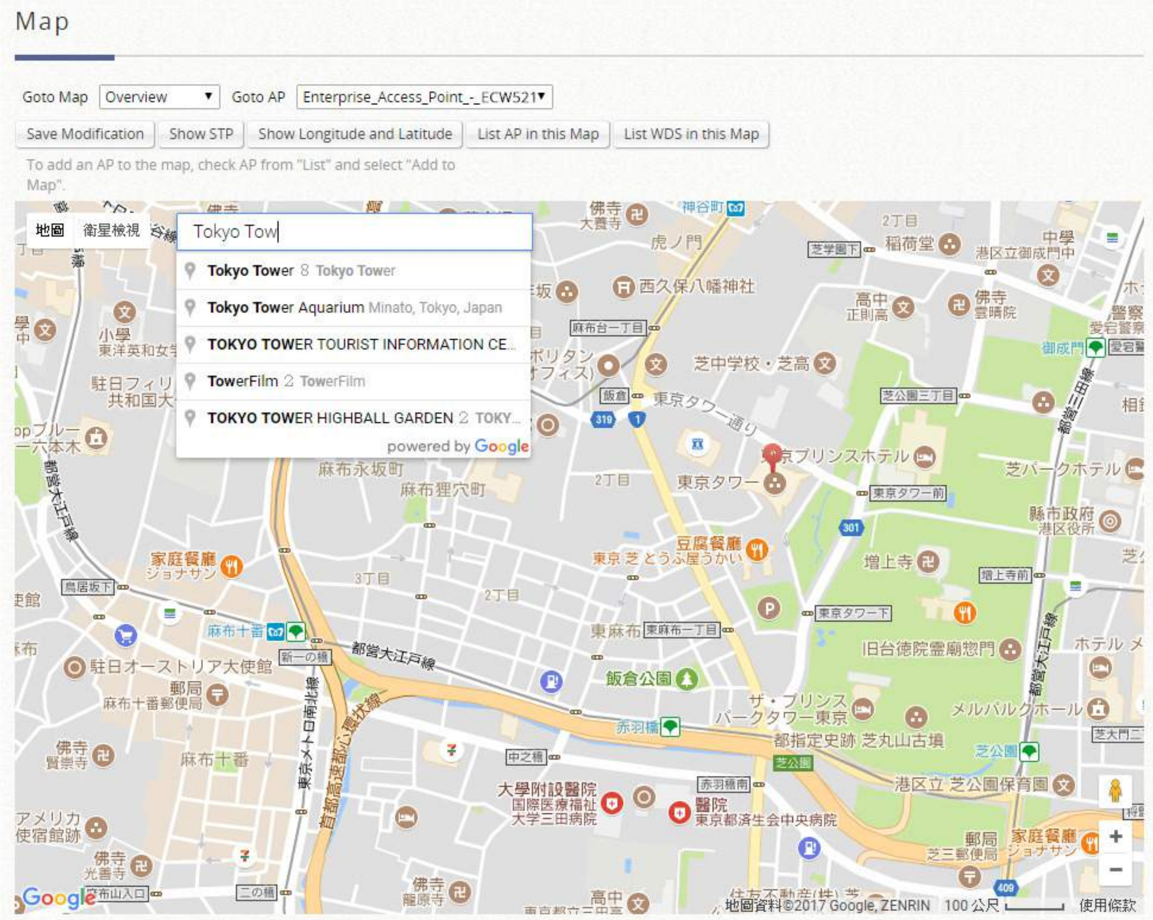
All of the supported APs under management of the system will be shown on the list. The administrator can add supported APs from the Adding tabs or CAPWAP tunnel back from AP. After APs are added, this list will show the current managed APs including AP type, AP name, IP Address, MAC Address, Status, number of Clients, Tunnel Status, AP Firmware Version, and geographic location.

Add: This is elaborated in Section 8.2 AP Adding and Configuration
Delete: Check the checkboxes and click "Delete" to remove the selected Access Points from the AP List
Add to Map/ Floor Plan: Check the checkboxes and click "Add to Map/ Floor Plan" to place the selected AP on the Map/Floor Plan chosen from the drop down list. If no map/floor plan profile has been configured, there will be no available map/floor plan to choose in the drop down list.
Backup Config: Check the checkboxes and click "Backup Config" to save the chosen AP's configuration settings into a .db file stored in the WLAN controller's memory. The Backup up files are listed under Backup Config tab page for download or deletion.
Restore Config: Check the checkboxes and click "Restore Config" to restore the chosen AP's configuration settings using a .db file stored locally in administrator PC or in the WLAN controller's memory.
Upgrade: Check the checkboxes and click "Upgrade" to upgrade the chosen AP's firmware using a firmware file stored locally in administrator PC or in the WLAN controller's memory (under Firmware tab page).
Apply Settings: Check the checkboxes and click "Apply Template" to apply the already prepared WAPM templates so as to implement some AP's configuration or change AP Admin's password for certain administration application.
Reboot: Check the checkboxes and click "Reboot" to restart the selected Access Points if needed

8.2 Graphical Monitoring

8.2.1 Google Map Integration

The Map is implemented with Google Map API version3 which allows administrators to view at a glance the whereabouts of all of the AP's under Wide Area AP Management (WAPM). This feature is helpful when it comes to network planning and management.
Once the administrator has added APs to the managed list, these APs can be tagged or marked on the Google Map API to show its' geographical location, as shown below:



Map

Goto Map: Overview

Goto AP: Enterprise_Access_Point_-_ECW521

To add an AP to the map, check AP from "List" and select "Add to Map".

Save Modification
Show STP
Show Longitude and Latitude
List AP in this Map
List WDS in this Map
地圖
衛星檢視
Tokyo Tow
Tokyo Tower 8 Tokyo Tower
Tokyo Tower Aquarium Minato, Tokyo, Japan
TOKYO TOWER TOURIST INFORMATION CE...
TowerFilm 2 TowerFilm
TOKYO TOWER HIGHBALL GARDEN 2 TOKY...
powered by Google
東京タワー
麻布十番
飯倉公園
増上寺
Google
地圖資料©2017 Google, ZENRIN
100 公尺
使用條款

Map

Goto Map: When you have configured multiple map profiles, this function allows switching between different maps.

Goto AP: This function is for administrator to select an AP on the list, and the map will shift to show the selected AP in the center of the map.

Save Modification: This function is for saving the changes made to the map and overwriting the maps' profile attributes. For instance if you have altered or panned the original map, clicking this button will save the changes made.

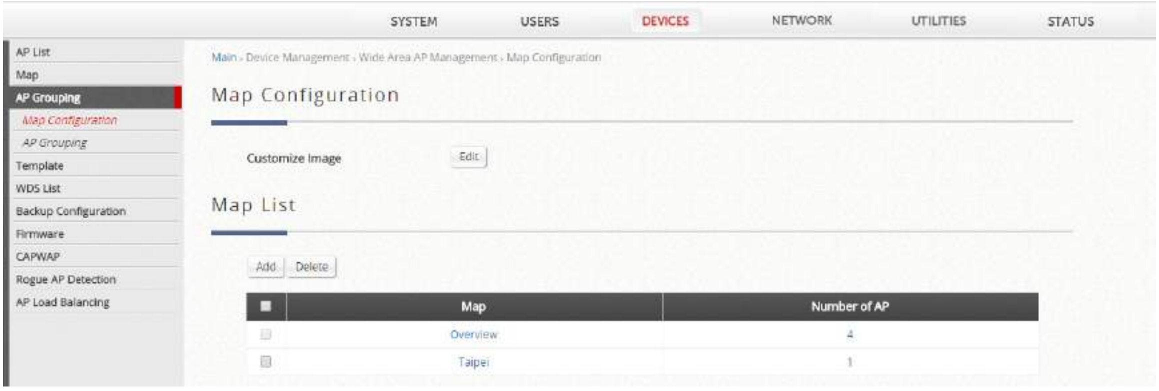
Show Longitude and Latitude: This function when pressed will display in a pop up window the longitude and latitude of the map's current center point.

List AP in this Map: to open a new page on your browser redirecting to the List tab page for displaying a list of APs in the Map.

List WDS in this Map: to open a new page on your browser redirecting to the WDS List tab page for displaying a list of WDS links on the Map.

Map/Satellite: to switch the view of graphical view or real satellite images

Search: to find locations or places from Google Map, instead of searching the managed APs



Map Configuration

Customize Image Edit

Map List

Add Delete

■	Map	Number of AP
□	Overview	4
□	Taipei	1

Map Configuration

Customize Image: Administrator can upload desired images for each AP model that will be used as AP markers on the MAP.

Add a New Map: Click to add a new map profile.

Delete this Map: Delete the current map profile.

Edit this Map: Click to modify the current map's attribute settings.

Procedure to create a Map

Step 1. Get a Public IP Address from your ISP and configure this address to WAN interface.

Step 2. Apply for a Google Maps Registration key.

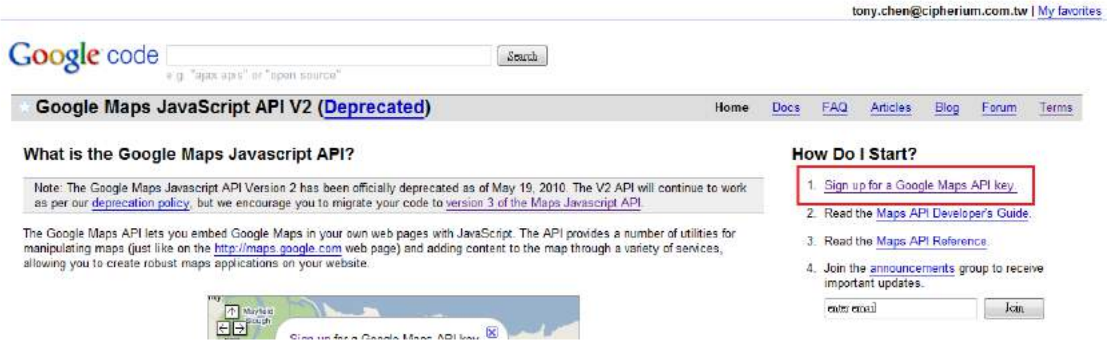
Step 3. Click Add a New Map button on the Map page. Configure Map Name and registration key.

Step 4. Discover APs and Add these APs to managed List.

Step 5. From the List page, add some APs to the created Map.

The necessary steps required to configure your map with AP information are described in the subsequent sections.

Before starting to add a new map in wide-area AP management, it's necessary to sign up for a Google account or if the Google account is already available, this step can be skipped; this account will be used to apply for a Google Maps API v3 key. For details, please follow the instructions from Google at https://developers.google.com/maps/documentation/javascript/v2/introduction to obtain such Maps API v3 key and provide the key info into the field of "Google Maps Registration Key" under **Map Configuration page.**


tony.chen@cipherium.com.tw | My favorites
Google code
Search
e.g. "ajax apis" or "open source"
Home
Docs
FAQ
Articles
Blog
Forum
Terms
Sign up for a Google Maps API key

Google Maps JavaScript API V2 (Deprecated)

What is the Google Maps Javascript API?

Note: The Google Maps Javascript API Version 2 has been officially deprecated as of May 19, 2010. The V2 API will continue to work as per our deprecation policy, but we encourage you to migrate your code to version 3 of the Maps Javascript API.

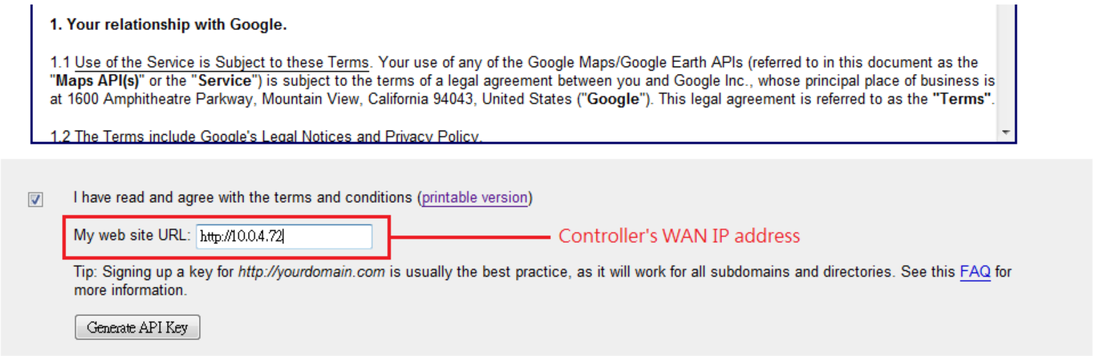
The Google Maps API lets you embed Google Maps in your own web pages with JavaScript. The API provides a number of utilities for manipulating maps (just like on the http://maps.google.com web page) and adding content to the map through a variety of services, allowing you to create robust maps applications on your website.

How Do I Start?

1. Sign up for a Google Maps API key.
2. Read the Maps API Developer's Guide.
3. Read the Maps API Reference.
4. Join the announcements group to receive important updates.

enter email Join

Click on "**Sign up for a Google Maps API key**".



1. Your relationship with Google.

1.1 Use of the Service is Subject to these Terms. Your use of any of the Google Maps/Google Earth APIs (referred to in this document as the "**Maps API(s)**" or the "**Service**") is subject to the terms of a legal agreement between you and Google Inc., whose principal place of business is at 1600 Amphitheatre Parkway, Mountain View, California 94043, United States ("**Google**"). This legal agreement is referred to as the "**Terms**".

1.2 The Terms include Google's Legal Notices and Privacy Policy.

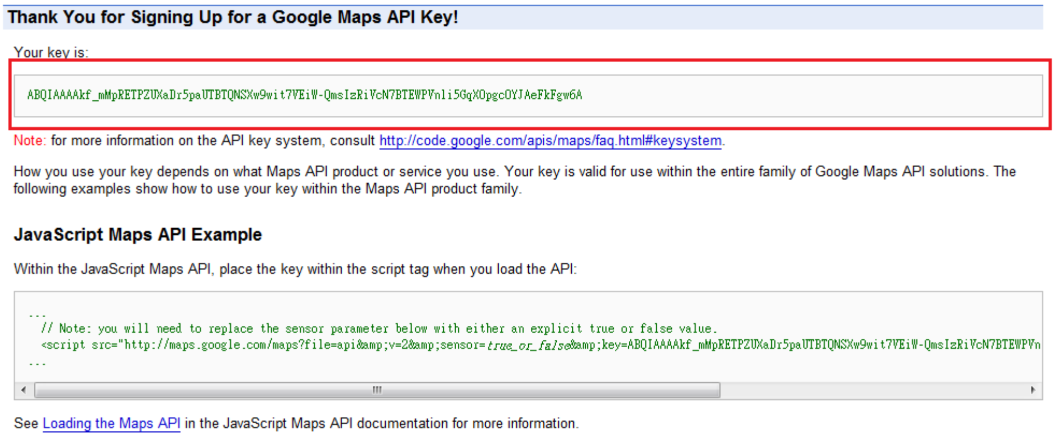
☑ I have read and agree with the terms and conditions (printable version)

My web site URL: http://10.0.4.72

Controller's WAN IP address

Tip: Signing up a key for *http://yourdomain.com* is usually the best practice, as it will work for all subdomains and directories. See this FAQ for more information.

Click the terms and conditions check box and fill in your WLAN controller's WAN IP address. Google will generate an API key for your WLAN controller.



Thank You for Signing Up for a Google Maps API Key!

Your key is:

```
ABQIAAAAkf_mMpRETPZUXaDr5paUTBTQNSXw9wit7VEiW-QmsIzRiVcN7BTEWPVnli5GqXOpgcOYJAeFkFgw6A
```

Note: for more information on the API key system, consult http://code.google.com/apis/maps/faq.html#keysystem.

How you use your key depends on what Maps API product or service you use. Your key is valid for use within the entire family of Google Maps API solutions. The following examples show how to use your key within the Maps API product family.

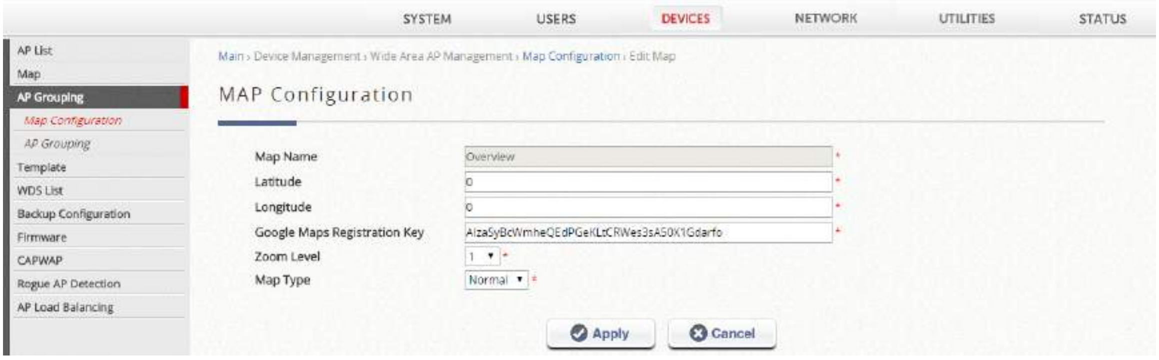
JavaScript Maps API Example

Within the JavaScript Maps API, place the key within the script tag when you load the API:

```
...
  // Note: you will need to replace the sensor parameter below with either an explicit true or false value.
  <script src="http://maps.google.com/maps?file=api&amp;v=2&amp;sensor=true_or_false&amp;key=ABQIAAAAkf_mMpRETPZUXaDr5paUTBTQNSXw9wit7VEiW-QmsIzRiVcN7BTEWPVn
...
```

See Loading the Maps API in the JavaScript Maps API documentation for more information.

Now, return to the **Map** tab page in WLAN controller's WMI and Scroll down to the bottom of the page, click on the **Add a New Map** button.

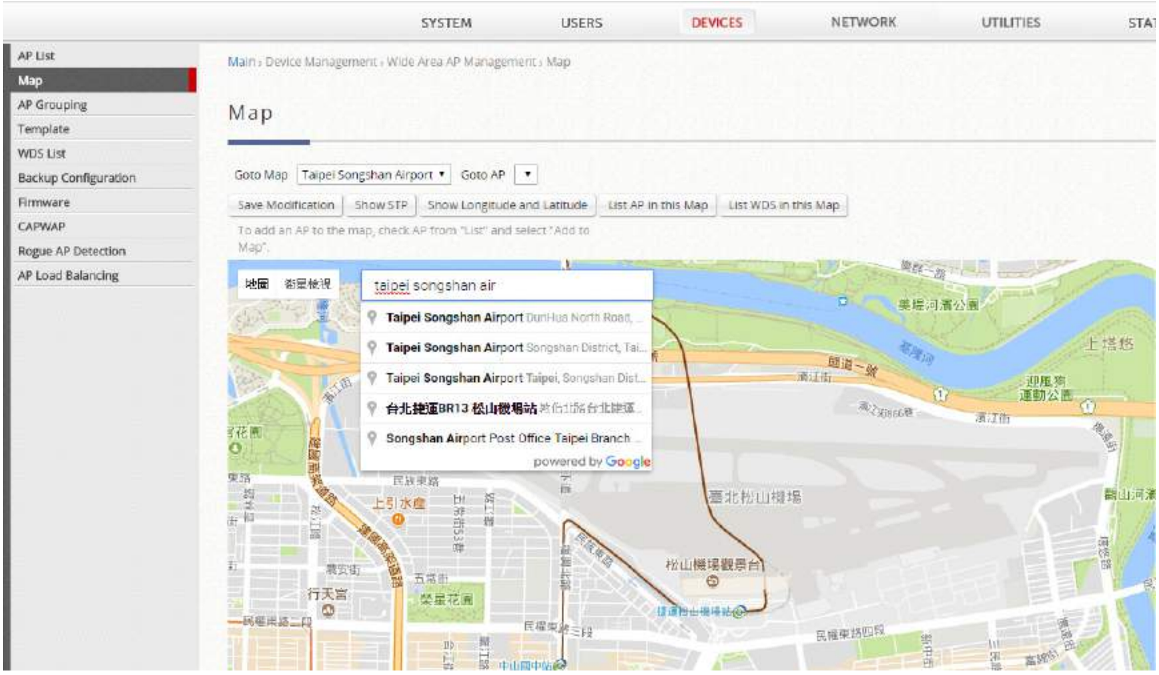


Main › Device Management › Wide Area AP Management › Map Configuration › Edit Map

MAP Configuration

Map Name	Overview *
Latitude	0 *
Longitude	0 *
Google Maps Registration Key	AIzaSyBcWmheQEdPGeKLtCRWes3sA50X1Gdarfo *
Zoom Level	1 *
Map Type	Normal *

An editing page will open for configuration, please fill in a **Map Name** for this map and its geographical location as defined by **Longitude** and **Latitude**, remember to also fill in the **Key** issued by Google. Finally choose the **Zoom Level** and **Map Type** and click the *Save* button.



Main › Device Management › Wide Area AP Management › Map

Map

Goto Map: Taipei Songshan Airport ▾ Goto AP ▾

To add an AP to the map, check AP from "List" and select "Add to Map".

taipei songshan air

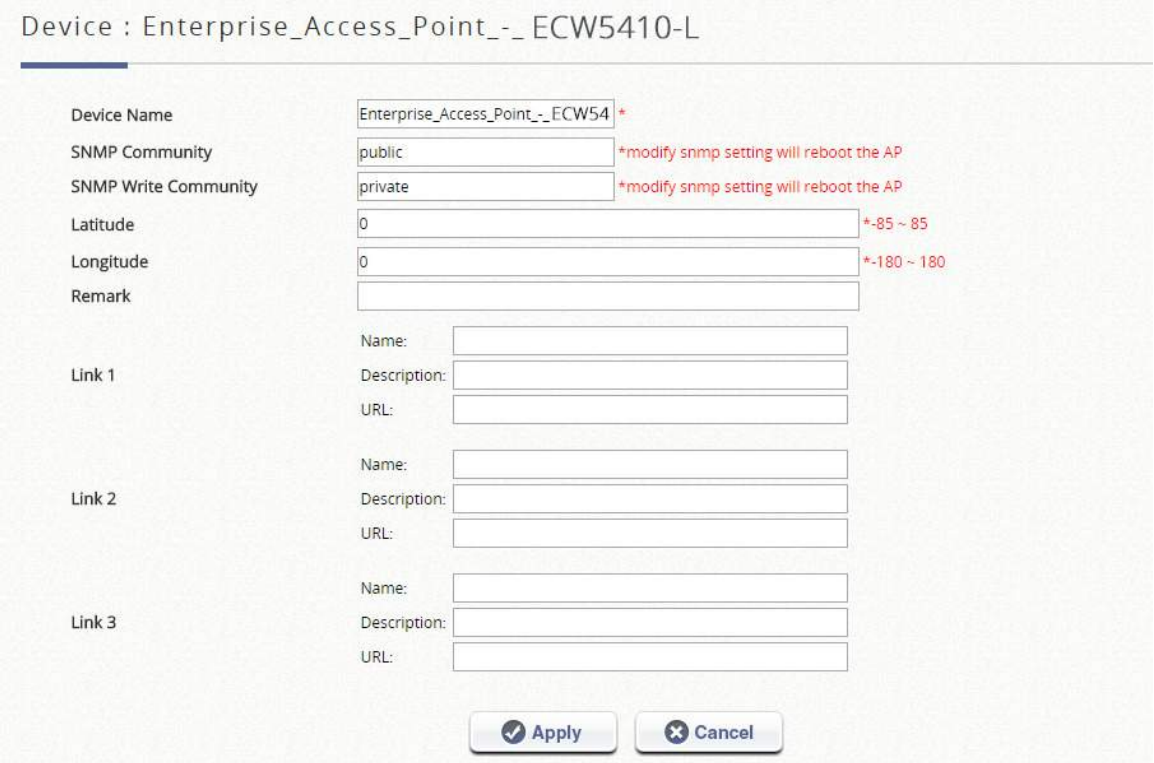
- Taipei Songshan Airport DunHua North Road, ...
- Taipei Songshan Airport Songshan District, Tai...
- Taipei Songshan Airport Taipei, Songshan Dist...
- 台北捷運BR13 松山機場站 ...
- Songshan Airport Post Office Taipei Branch ...

powered by Google

The above screenshot is an example showing Taipei City with Map Name as Taipei Songshan Airport, Zoom Level of 14 and Normal Map Type.

If you have several APs deployed and listed in List under Wide Area AP Management, their geographical location can be marked on a particular map.

Firstly, go to the List tab page and click on the Edit button of the AP's that you wish to mark on the map. In the AP configuration page, set the coordinates (Latitude and Longitude) of this AP and the radius of signal coverage.

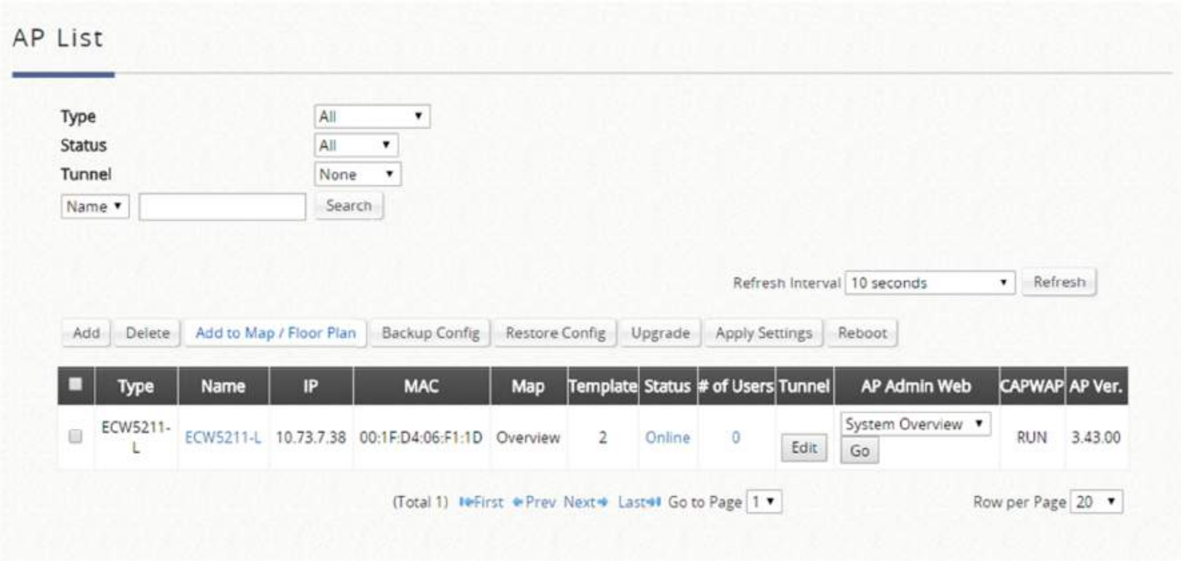


Device : Enterprise_Access_Point_-_ECW5410-L

Device Name	Enterprise_Access_Point_-_ECW54	*
SNMP Community	public	*modify snmp setting will reboot the AP
SNMP Write Community	private	*modify snmp setting will reboot the AP
Latitude	0	*-85 ~ 85
Longitude	0	*-180 ~ 180
Remark		
Link 1	Name: Description: URL:	
Link 2	Name: Description: URL:	
Link 3	Name: Description: URL:	

Fill in the coordinates where you wish to mark this particular AP. Link 1 ~ Link 3 is for configuring a http link that will show up in the dialogue box on the map for referencing additional information related to this AP; for instance the IP address of a IP surveillance camera connected to this AP or the URL of the Venue Website where this AP is deployed.

Administrator can upload customized thumbnail images shown on the map. After configuring all the necessary settings and uploading your images, click *Apply* button and return to AP List page.
Check the AP's that you wish to mark on the map and click the "Add to Map" button, choose the name of the map on which you wish to mark these APs and click *OK* button.

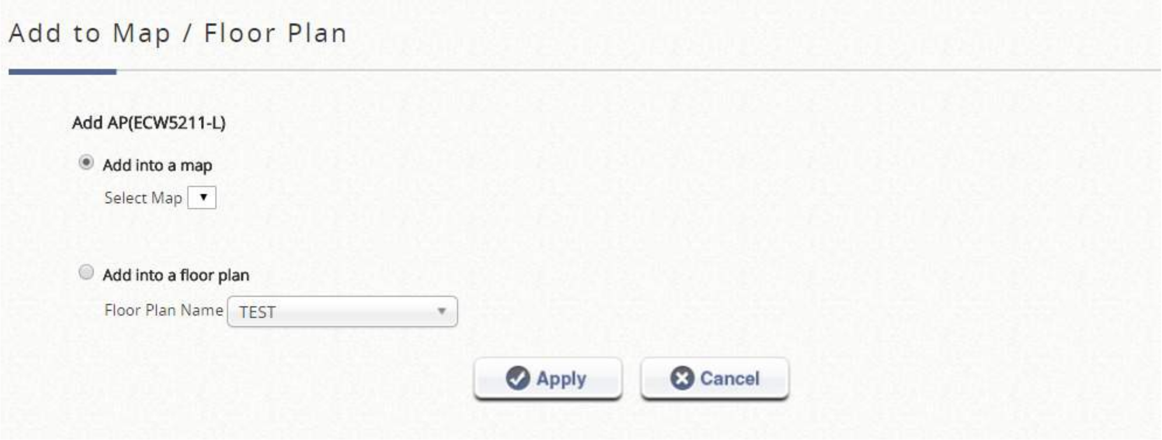


AP List

Type: All
Status: All
Tunnel: None
Name:

■	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.
□	ECW5211-L	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D	Overview	2	Online	0	Edit	System Overview Go	RUN	3.43.00

(Total 1) First Prev Next Last Go to Page 1 Row per Page 20



Add to Map / Floor Plan

Add AP(ECW5211-L)

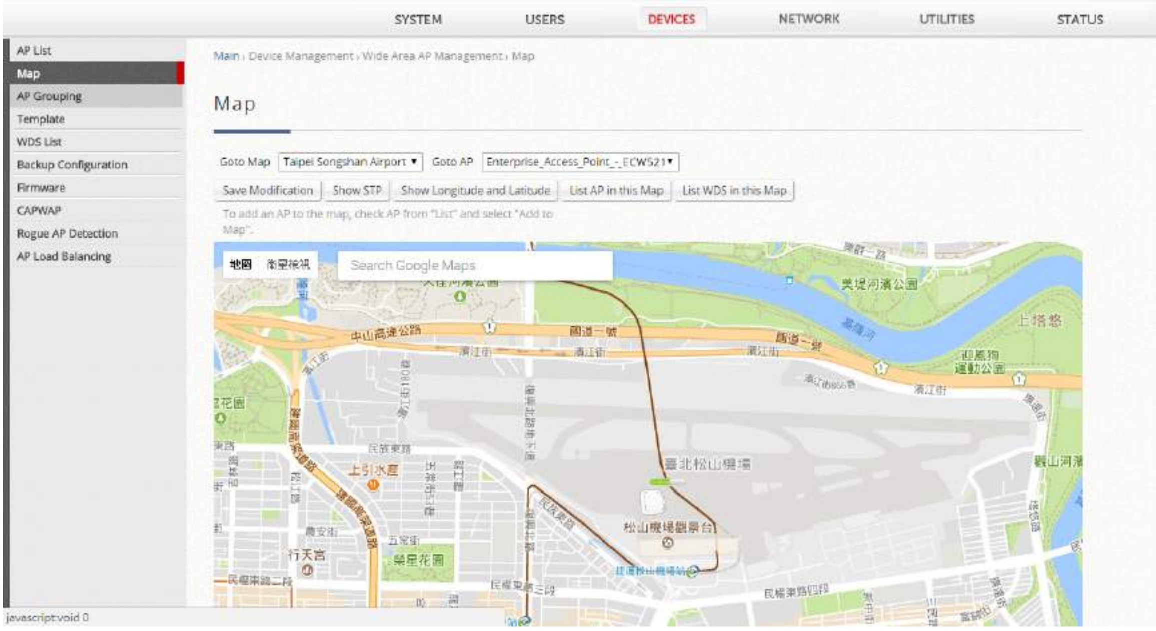
● Add into a map

Select Map

○ Add into a floor plan

Floor Plan Name: TEST

The selected APs will show up as marker images on the map at the physical coordinates configured, as shown below.



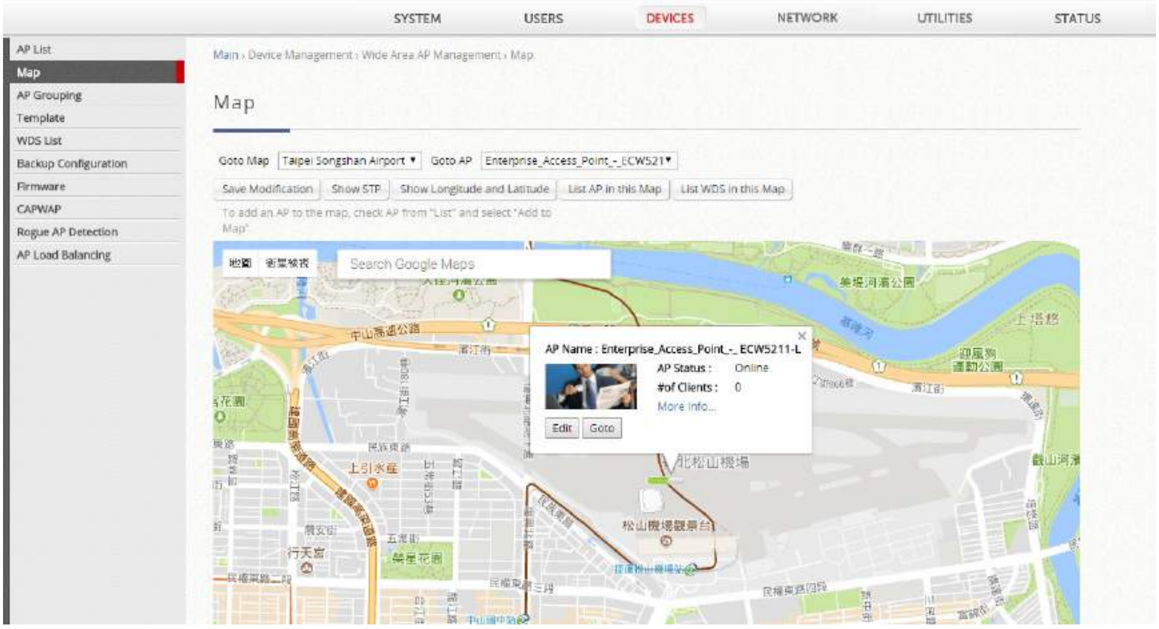
Main › Device Management › Wide Area AP Management › Map

Map

Goto Map: Taipei Songshan Airport ▾ Goto AP: Enterprise_Access_Point_-_ECW521▾

To add an AP to the map, check AP from "List" and select "Add to Map".

Administrators are able to click on the AP icon to see the dialogue box for additional information or links that you have configured. Besides, administrators can click the more info link for information on AP Link, AP Statistic, AP Status, Client List, WDS List and Links related to this AP, which are collected from the remote AP via SNMP.



Main › Device Management › Wide Area AP Management › Map

Map

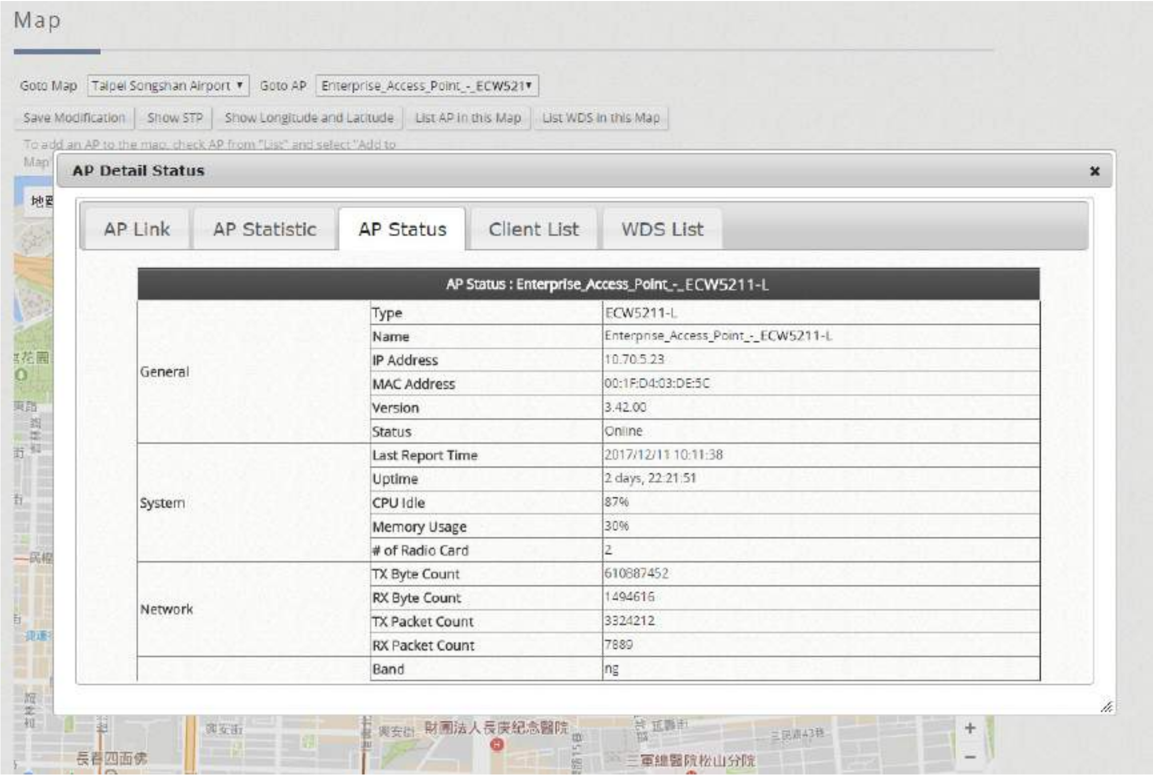
Goto Map: Taipei Songshan Airport ▾ Goto AP: Enterprise_Access_Point_-_ECW521▾

To add an AP to the map, check AP from "List" and select "Add to Map".

AP Name : Enterprise_Access_Point_-_ECW5211-L

AP Status : Online

#of Clients : 0



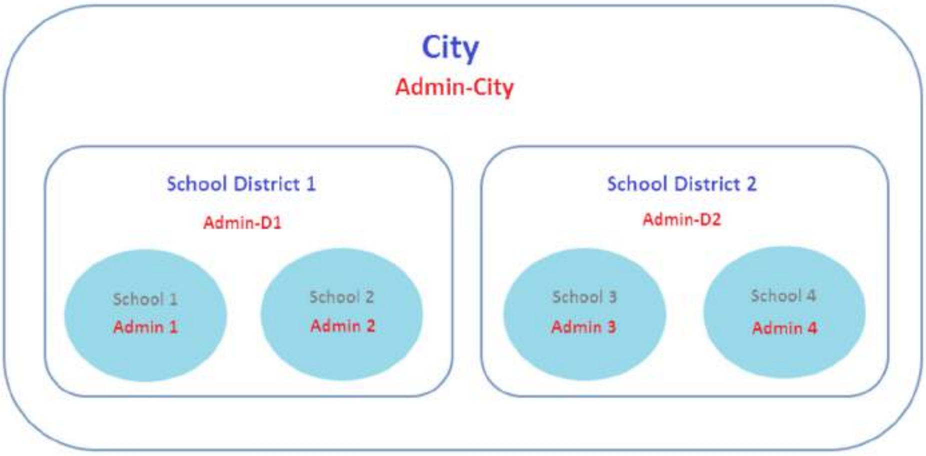
To add an AP to the map, check AP from "List" and select "Add to Map

AP Status : Enterprise_Access_Point_-_ECW5211-L		
General	Type	ECW5211-L
	Name	Enterprise_Access_Point_-_ECW5211-L
	IP Address	10.70.5.23
	MAC Address	00:1F:D4:03:DE:5C
	Version	3.42.00
	Status	Online
System	Last Report Time	2017/12/11 10:11:38
	Uptime	2 days, 22:21:51
	CPU Idle	87%
	Memory Usage	30%
	# of Radio Card	2
Network	TX Byte Count	610887452
	RX Byte Count	1494616
	TX Packet Count	3324212
	RX Packet Count	7889
	Band	ng

8.2.2 AP Grouping

In Wide Area AP Management, all the managed APs must be designated to an AP Group by Maps. Each AP must be configured to belong to a map. All APs will be added to the Default Map, or you may create a new map for selection before you add a new AP.

AP grouping allows different levels of administrators to manage APs by different AP group. An AP Group can include multiple maps and AP templates. On the other hand, a map can be included by different AP groups. You may assign different administrator groups to have different read/write permission for each AP group.



Edgecore controller supports adding AP’s on Google Map. The process is shown below:

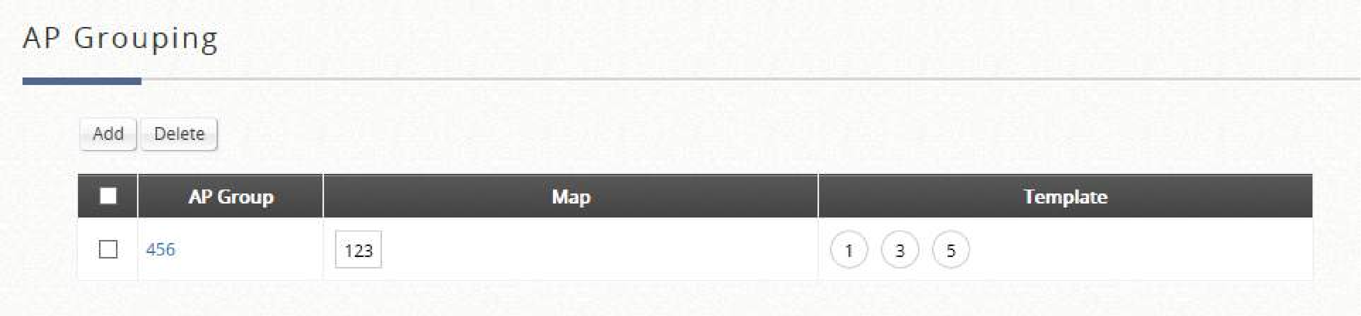
Create your own map by clicking **Add** under **Map List** at the bottom page and then fill in the necessary

fields shown in the popup window. Click Apply.
Add the deployment location of the AP in the AP's attribute profile (longitude and latitude). *"Main Menu > Devices > Wide Area AP Management > List - AP Attribute (Edit)"*

Go back to the List page, choose the AP, and then click the Add to Map button, and choose the desired map. After the settings, admin should be able to see an icon of the AP on the selected map.

Overview path: *"Main Menu > Devices > Wide Area AP Management > Map"*

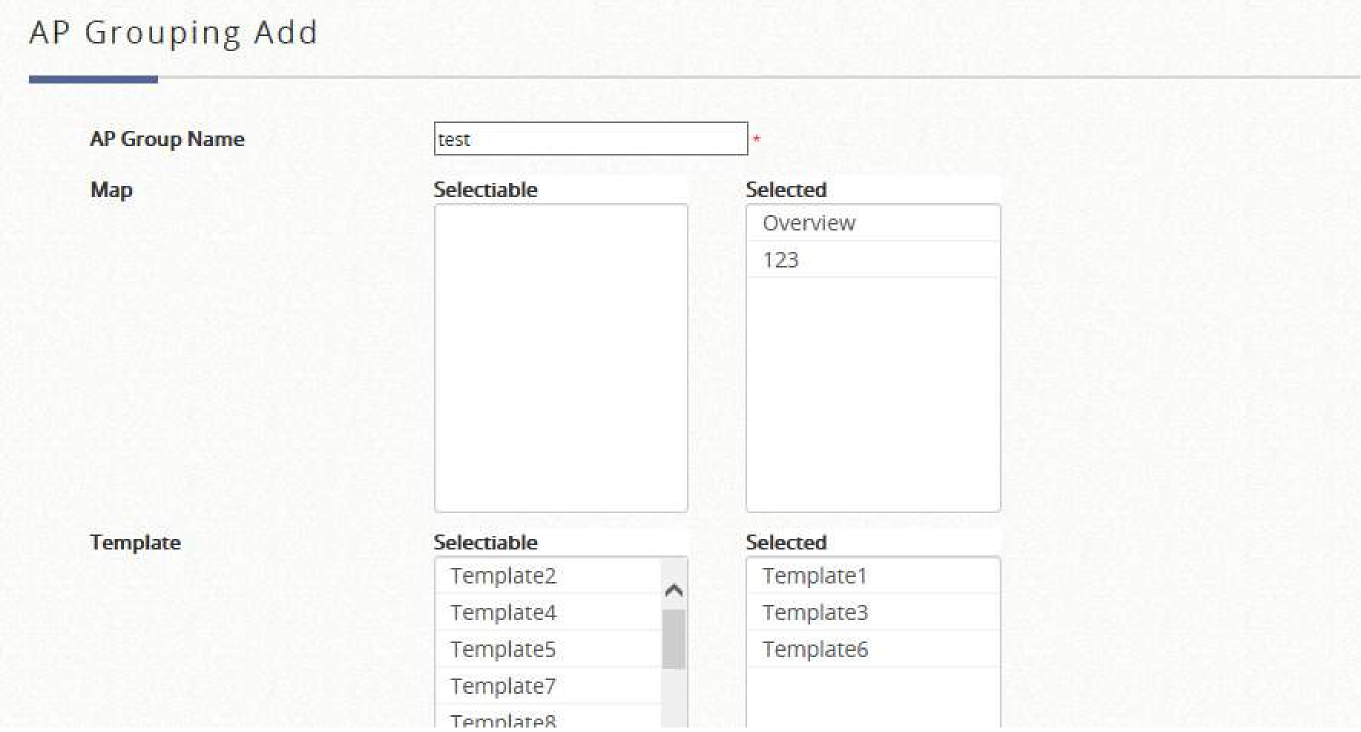
Go to *"Main Menu > Devices > Wide Area AP Management > AP Grouping > AP Grouping List"* to add or delete the AP group.



AP Grouping

■	AP Group	Map	Template
□	456	123	1 3 5

Click Add to add an AP group, each AP group can include maps and templates to be managed.



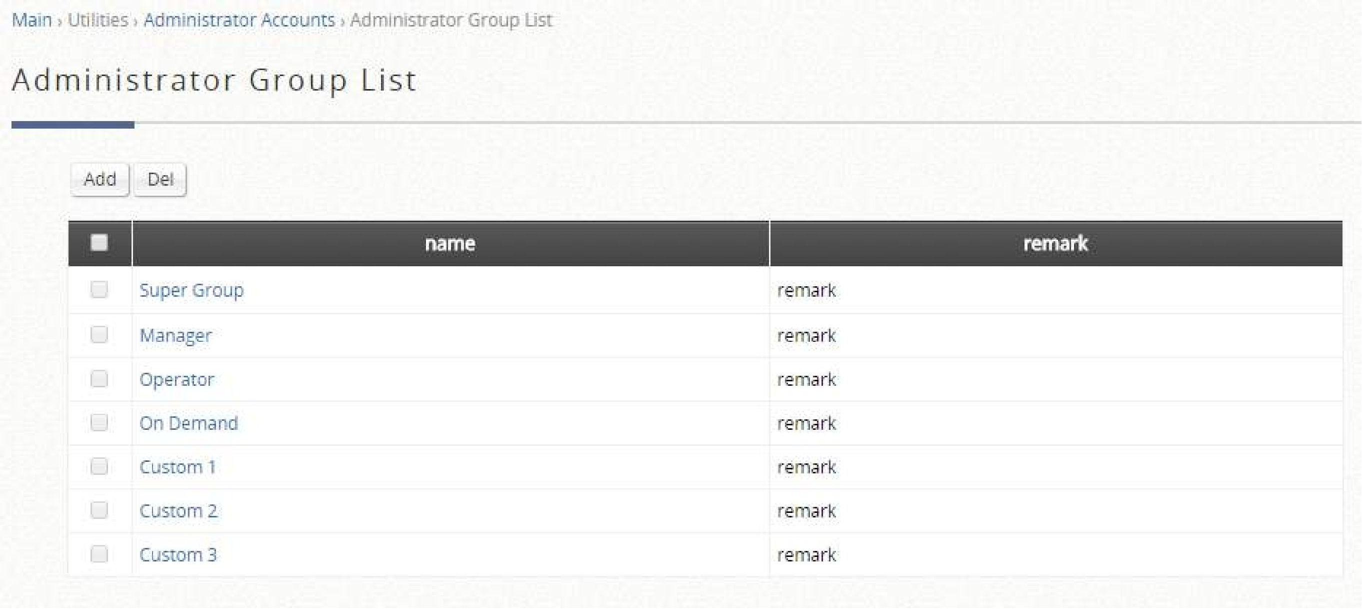
AP Grouping Add

AP Group Name: test *

Map
Selectiable:
Selected: Overview, 123

Template
Selectiable: Template2, Template4, Template5, Template7, Template8
Selected: Template1, Template3, Template6

After an AP group is created, you may assign access permission to each AP group by adding an Administrator Group to the Administrator Group List.

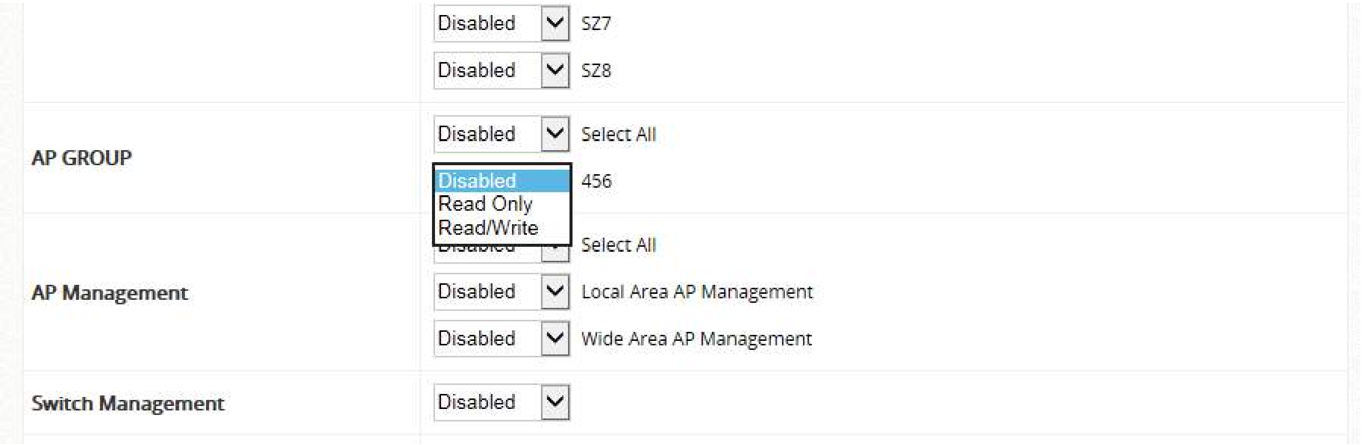


Main › Utilities › Administrator Accounts › Administrator Group List

Administrator Group List

□	name	remark
□	Super Group	remark
□	Manager	remark
□	Operator	remark
□	On Demand	remark
□	Custom 1	remark
□	Custom 2	remark
□	Custom 3	remark

Assigning permission to an AP group.



	Disabled SZ7
	Disabled SZ8
AP GROUP	Disabled Select All
	Disabled 456
AP Management	Disabled Select All
	Disabled Local Area AP Management
	Disabled Wide Area AP Management
Switch Management	Disabled

8.3 AP adding and configuration

8.3.1 AP discovery

Add an AP

The Adding page allows administrator to directly add a single Access Point to the management list regardless of its Status.

Device Type: to specify the AP model

Device IP: no matter the device is online/offline, just enter IP address for the managed entry

Device Name: to identify the device by setup the device name

Login ID: the administration username for accessing the permission of managing AP

Password: the administration password for accessing the permission of managing AP

SNMP Community: default is “public” for SNMP

SNMP Write Community: default is “private” for SNMP

Map: to specify the managed device in certain Map for tier administration or graphical view

Discovery AP

With the AP Discovery feature, administrator can scan for APs regardless of their physical location as long as their IP addresses can be reached.

Device Type: to select the target Device Type

Admin Settings Used to Discover: to define the scan IP range and Admin Settings, then click "Discover"

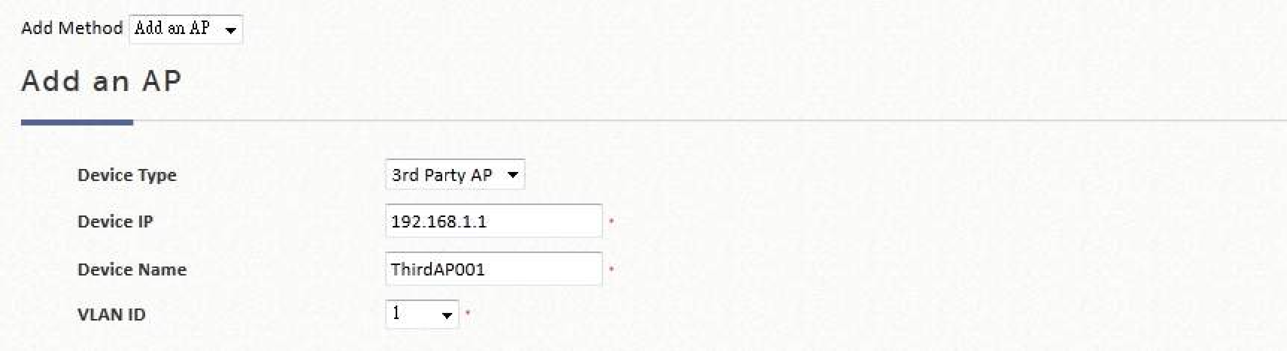
Login ID: the administration username for accessing the permission of managing AP

Password: the administration password for accessing the permission of managing AP

After the discovery process, newly found AP's will be listed under Device Results where the administrators can specify the individual APs Device Name and SNMP Community string. Select and click the Add button and the discovered APs will be added into AP List.

Third Party AP Management

Add a third party AP by selecting "3rd Part AP" from Device Type. Add to AP List manually by specifying third party AP's Device IP, Device Name and VLAN ID. Click Add to finish adding and check lists to List icon.



Add Method: Add an AP

Add an AP

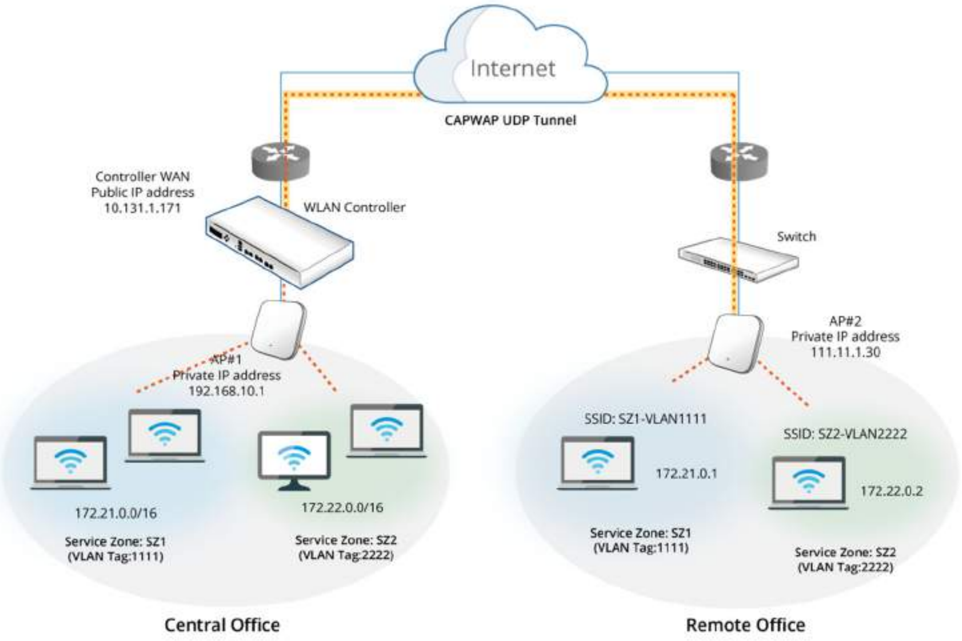
Device Type	3rd Party AP
Device IP	192.168.1.1 *
Device Name	ThirdAP001 *
VLAN ID	1 *

To check and manage the List of third Party AP; go to: "*Access Points > Enter Wide Area AP Management > List.*"

Manage this third party AP from the Type Lists. Edit its AP Attribute and Administration from the column. Go to Map icon. The added third party AP could also be placed on Google Map features and all map functions.

8.3.2 How to prepare CAPWAP application

CAPWAP is a standard interoperable protocol that enables a WLAN controller to manage a collection of wireless access points. Two tunneling options are available: complete tunnel and split tunnel.



On WLAN controller side

CAPWAP Status: to enable the CAPWAP feature for establish CAPWAP tunnel between system and managed APs

Apply Certificate to AP: to make sure that the Controllers' CAPWAP settings use a security certificate that is issued by the same CA. Upload the necessary security certificate into the AP in order for the Controller to validate CAPWAP discovery and join requests. For information on Certificate management on the controller please refer to the subsequent chapter in this guide.

IP Address for Control Channel: to specify the control channel IP range for the managed CAPWAP-established APs, each with its own control channel.

IP Netmask for Control Channel: to specify the control channel IP range for the managed CAPWAP-established APs, each with its own control channel.

Control Channel IP Range: The IP pool for assigning to AP side, establishing the control channel to communicate. The number of IPs is defined by above IP Address and IP Netmask For Control Channel.

Access Controller IP List: The AC can statically designate other CAPWAP supported ACs as backup AC for CAPWAP APs in case it can no longer provide service. The number designates the priority of these backup ACs to the AP, in the event that the original AC is down, the AP will first attempt to join the No. 1 backup AC and so on.

On AP Side

Enable the CAPWAP function from "*System > CAPWAP*", where the administrator will see several discovery methods to be activated, namely:

DNS SRV Discovery: This type of discovery utilizes a DNS server to complete the discovery method. Through the DNS SRV record acquired, the AP will recognize the Controller to send CAPWAP join request.

DHCP Option Discovery: Administrator should enable the CAPWAP feature and the DHCP server of the controller in order for the AP to get an IP address that is in the same subnet of that of the Edgecore WLAN controller it is trying to connect.

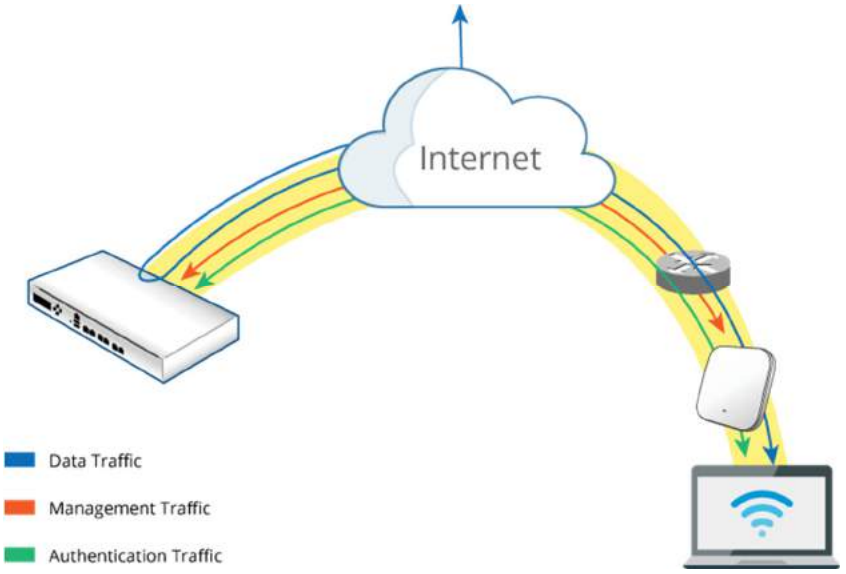
Broadcast Discovery: The AP sends broadcast requests to all the IP addresses in a subnet. Edgecore WLAN controllers, and other gateways mostly, do not allow broadcasts to go over subnets. Make sure the controller is in the same subnet as the AP when you enable the function.

Multicast Discovery: Multicast discovery works by sending a multicast discover packet to the network in hopes of the correct controller responding to it. This function should go with a proper setup on the routing paths of the AP. Please make sure you enable it with the related settings in place.

Static Discovery (most recommended): Static discovery is the most recommended discovery method since it is intuitive to implement without any pre-settings to complete in advance. Simply enable the function and type in the IP address of the WLAN controller you want this AP to join to.

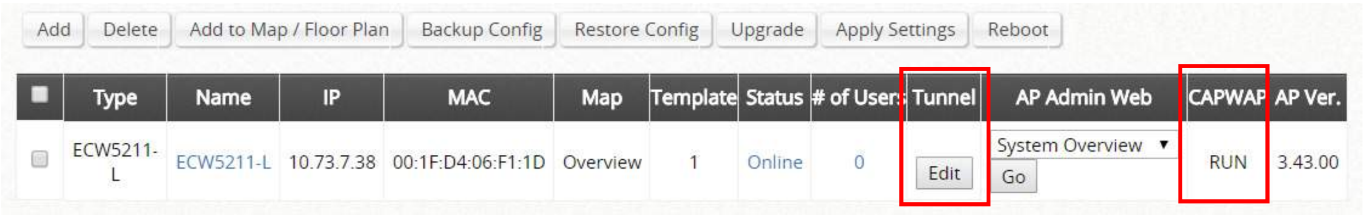
8.3.3 CAPWAP with Complete Tunnel

Complete Tunnel uses the CAPWAP protocol to communicate with an Access Point so that all management traffic, authentication traffic and data traffic from the service area AP provided are transmitted back to the Controller, before forwarding data traffic to the internet. The WLAN controller is able to implement role-based policies over Layer 3 networks, with user access control available in the remote sites. This feature allows the WLAN controller to fully support centralized AP management and user management.



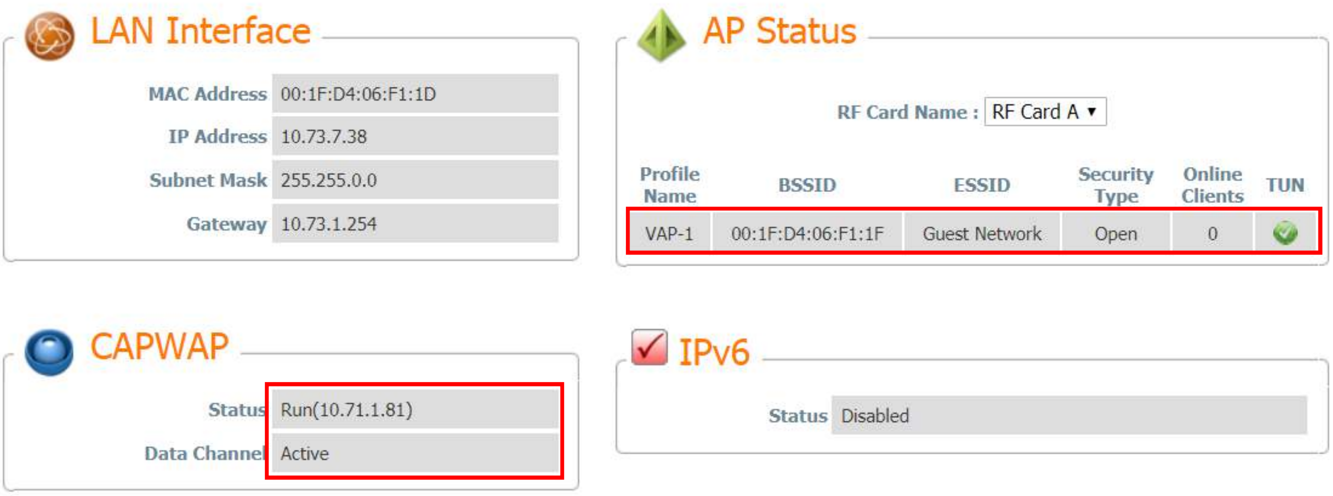
The following procedures may be helpful

1. On AP: to type the IP address for Static Discovery, and wait until the CAPWAP column displays a “RUN” status.
2. On Controller: to prepare Template of the VAP configuration with CAPWAP Tunnel Interface – “Complete Tunnel”
3. On Controller: to apply the prepared Template to the CAPWAP-establish AP and the Tunnel status will show a clickable “Edit” button in black if a VAP is configured to be tunneled back to the controller.



☐	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.
☐	ECW5211-L	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D	Overview	1	Online	0	Edit	System Overview ▼ Go	RUN	3.43.00

4. On AP: to check the AP WMI showing Data Channel is "Active" with the VAP tunnel status in "Green" light on the System Overview page



LAN Interface

MAC Address	00:1F:D4:06:F1:1D
IP Address	10.73.7.38
Subnet Mask	255.255.0.0
Gateway	10.73.1.254

AP Status

RF Card Name : RF Card A ▼

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	00:1F:D4:06:F1:1F	Guest Network	Open	0	✓

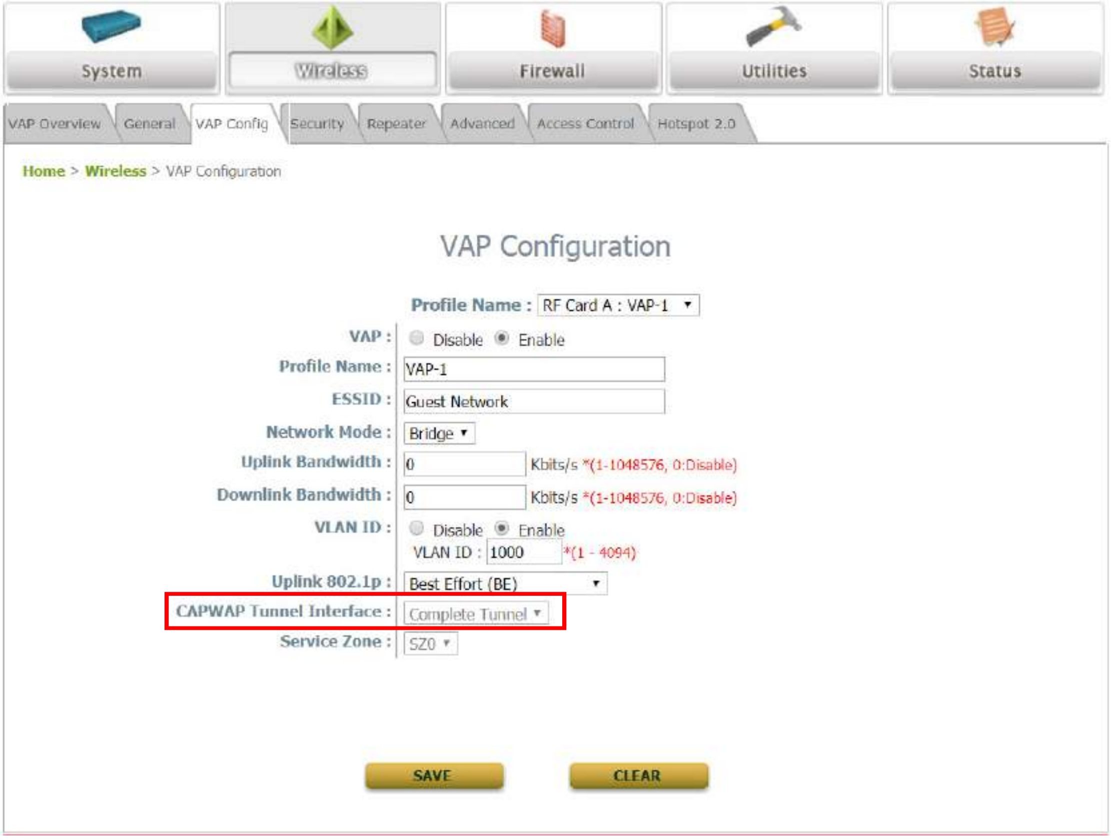
CAPWAP

Status	Run(10.71.1.81)
Data Channel	Active

IPv6

Status	Disabled

5. On AP: to reconfirm the specific VAP Configuration is under Complete Tunnel



Home > Wireless > VAP Configuration

VAP Configuration

Profile Name : RF Card A : VAP-1 ▼

VAP : ○ Disable ● Enable

Profile Name : VAP-1

ESSID : Guest Network

Network Mode : Bridge ▼

Uplink Bandwidth : 0 Kbits/s *(1-1048576, 0:Disable)

Downlink Bandwidth : 0 Kbits/s *(1-1048576, 0:Disable)

VLAN ID : ○ Disable ● Enable
VLAN ID : 1000 *(1 - 4094)

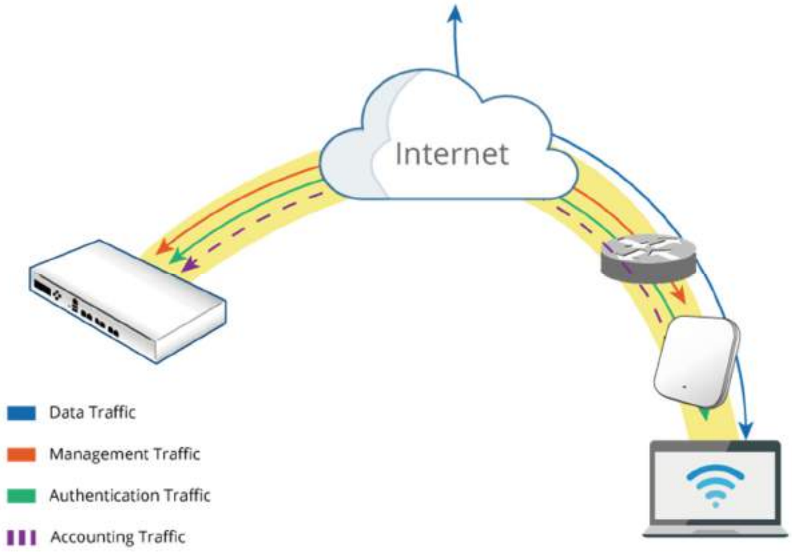
Uplink 802.1p : Best Effort (BE) ▼

CAPWAP Tunnel Interface : Complete Tunnel ▼

Service Zone : SZ0 ▼

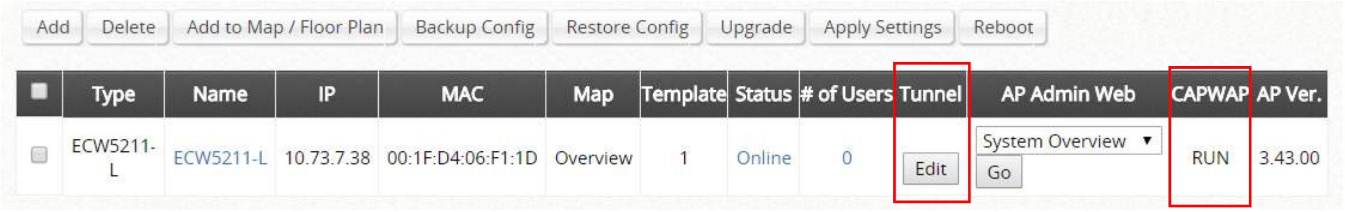
8.3.4 CAPWAP with Split Tunnel

For Split tunnel, only user authentication related traffic will be directed back to the controller. For authenticated users, data traffic will go to the Internet through the local network directly. The user data can be transmitted with a shorter path and the network load of the controller can also be reduced.



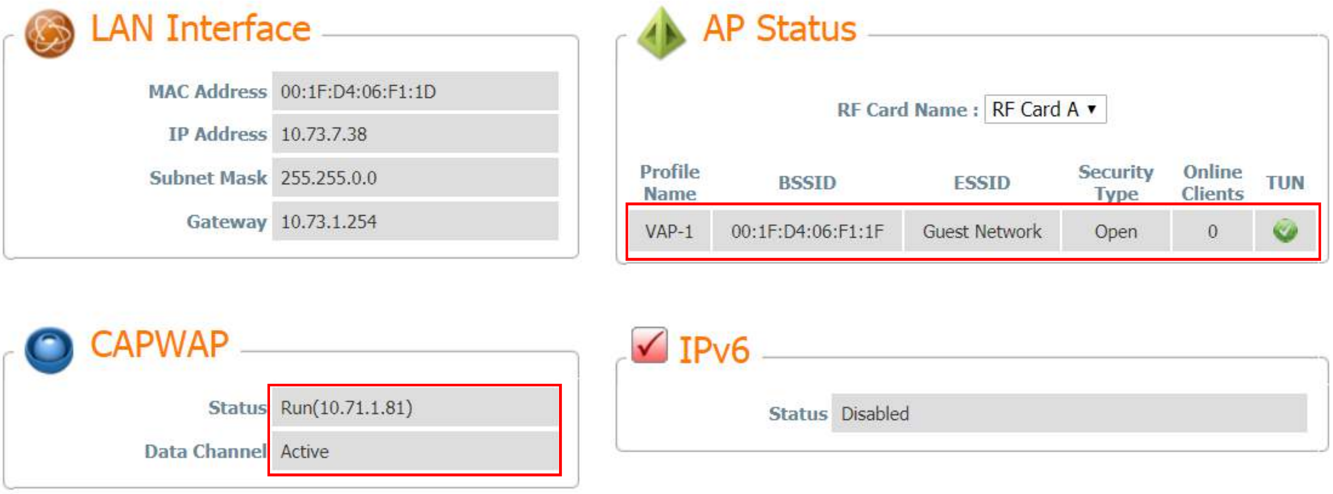
The following procedures may be helpful

1. On AP: type the IP address for Static Discovery, and wait until the CAPWAP column displays a "RUN" status.
2. On Controller: prepare Template of the VAP configuration with CAPWAP Tunnel Interface – "Split Tunnel"
3. On Controller: apply the prepared Template to the CAPWAP-establish AP and the Tunnel status will show a clickable "Edit" button in black if a VAP is configured to be tunneled back to the controller.



□	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.
□	ECW5211-L	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D	Overview	1	Online	0	Edit	System Overview ▾ Go	RUN	3.43.00

4. On AP: to check the AP WMI showing Data Channel is "Active" with the VAP tunnel status in "Green" light on the System Overview page



LAN Interface

MAC Address	00:1F:D4:06:F1:1D
IP Address	10.73.7.38
Subnet Mask	255.255.0.0
Gateway	10.73.1.254

AP Status

RF Card Name : RF Card A ▾

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	00:1F:D4:06:F1:1F	Guest Network	Open	0	✓

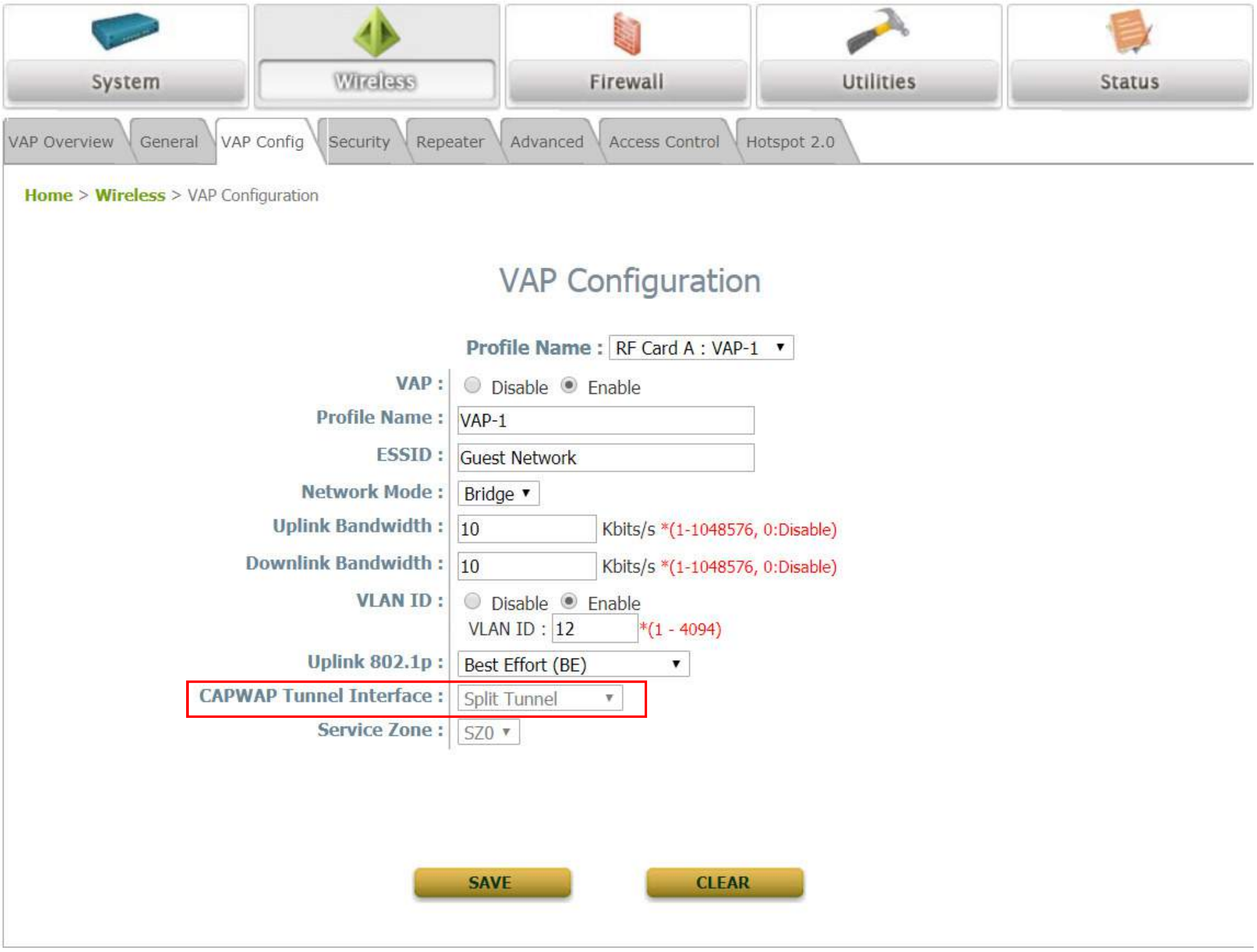
CAPWAP

Status	Run(10.71.1.81)
Data Channel	Active

IPv6

Status	Disabled

5. On AP: to reconfirm the specific VAP Configuration is under Split Tunnel



Home > Wireless > VAP Configuration

VAP Configuration

Profile Name : RF Card A : VAP-1 ▾

VAP :	○ Disable ● Enable
Profile Name :	VAP-1
ESSID :	Guest Network
Network Mode :	Bridge ▾
Uplink Bandwidth :	10 Kbits/s *(1-1048576, 0:Disable)
Downlink Bandwidth :	10 Kbits/s *(1-1048576, 0:Disable)
VLAN ID :	○ Disable ● Enable VLAN ID : 12 *(1 - 4094)
Uplink 802.1p :	Best Effort (BE) ▾
CAPWAP Tunnel Interface :	Split Tunnel ▾
Service Zone :	SZ0 ▾

8.4 Template

Select a country code depending on the firmware version on your Access Point.This dynamically changes the available channels on your access point.

General Settings

RF Card Name: Select an RF Card for your AP.

Band: Depending on the AP model template you are editing, there are different modes to select, 802.11a, 802.11b, 802.11g, 802.11a+802.11n, 802.11b+802.11g, 802.11g+802.11n and 802.11ac.

Short Preamble: The short preamble with a 56-bit synchronization field can improve WLAN transmission efficiency. Select *Enable* to use Short Preamble or *Disable* to use Long Preamble with a 128-bit synchronization field.

Channel Width (802.11g+n, 802.11a+n and 802.11ac only): Choose between 20MHz, 40MHz or Auto. Doubling channel bandwidth to 40 MHz is supported to enhance throughput. 80MHz is available for selection in 802.11ac mode.

Channel: Select the appropriate *channel* from the drop-down menu to correspond with your network settings.

Max Transmit Rate: The default is set to Auto. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, Auto, to allow the Access Point to automatically use the fastest rate possible. For 802.11n the selectable data rates range from MCS0 to MCS15, and for 802.11ac, select data rates up to MCS9.

Transmit Power: On select AP models, the signal strength transmitted from the system can be selected by Levels. Each level signifies a decrement of 1 dBm from the highest power. Level 1 is the actual highest power, Level 2 is the highest power minus 1 dBm, so on and so forth.

Beacon Interval (ms): Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal is transmitted between the access point and the wireless network.

ACK Timeout: The time interval for waiting for the “acknowledgement (ACK) frame”. If the ACK is not received within the interval then the packet will be re-transmitted. Higher ACK Timeout interval will decrease the packet lost, but the throughput will be decreased/worsened.

Airtime Fairness: When set to “Fair Access”, this feature ensures all devices with different band compatibilities have the same air time. When set to “Preferred Access”, N clients are prioritized. This feature is ideal for networks with devices supporting different bands.

Packet Delay Threshold (ms): This is the Tx Queue flushing mechanism, which purpose is to drop packets and immediately process others if the queue has been processed for more than x milliseconds. This is disabled by default (=0).

Idle Timeout (s): Clients disconnects when inactivity reaches the configured amount of time in seconds, where default = 300s.

Band Steering: When enabled, clients with 5GHz connectivity will be steered towards the 5GHz band to reduce congestion in the 2.4GHz band. This is applicable only when the AP is set to 2.4GHz and 5GHz on the 2 RF Cards. When “Aggressive” is checked, clients with 5GHz connectivity are forced to connect to the 5GHz band.

Interference Detection: When utilization of the current channel reaches the configured threshold (in %), the AP switches to a different Channel.

Transmission Rate Threshold: The associated client will be kicked when transmission rate is lower than the configured threshold. This ensures high connection speed for all associated clients.

WME Configuration: Access priority can be configured using with different parameters. CW Min: Contention Window Minimum, CW Max: Contention Window Maximum, AIFS: Arbitration Inter Frame

Spacing, TXOP Limit: Transmission Opportunity Limit.

VAP Configuration

VAP: *Enable* or *Disable* this VAP.

Profile Name: The profile name of a specific RF card and its VAP for identity / management purposes.

ESSID: ESSID (Extended Service Set ID) serves as an identifier for clients to associate with the specific VAP. It can be coupled with different service levels like a variety of wireless security types.

VLAN ID: The Edgecore Access Point supports tagged VLANs (virtual LANs). To enable VLAN function, each VAP shall be given a unique VLAN ID with valid values ranging from 1 to 4094. Once VLAN is Enabled, QoS is supported on the VAP.

CAPWAP Tunnel Interface: Select dropdown to designate traffic for the VAP to pass through CAPWAP Tunnel established between the AP and the controller. When CAPWAP Tunnel Interface is “Complete” or “Split Tunnel”, you may then select the Service Zone to be mapped to this VAP.

Security Settings

Select the desired Security Type from the drop-down menu, which includes Open, WEP, 802.1X, WPA-Personal, and WPA-Enterprise.

Advanced Wireless Settings

RTS Threshold: Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the fragment to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the AP or in areas where the clients are far apart and can detect only the AP but not each other.

Fragmentation Threshold (802.11a, 802.11b and 802.11g Modes): Enter a value between 256 and 2346. A packet size larger than this threshold will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

DTIM Period: Input the DTIM Interval that is generated within the periodic beacon at a specified frequency. Higher DTIM will allow the wireless client to save more energy, but the throughput will be lowered.

Consecutive Retries Threshold: This is the maximum number of transmission retries the AP will attempt when packet transmission is dropped before deciding the client is out of transmission reach. When transmission retries fails for the set number of times, the Access Point kicks the client to optimize performance for other connected clients.

Broadcast SSID: Disabling this function will stop the system from broadcasting its SSID. If broadcast of the SSID is disabled, only devices that have the correct SSID can connect to the system.

Wireless Station Isolation: By enabling this function, all stations associated with the system are isolated and can only communicate with the system.

WMM: The default is *Disable.* Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.

<To receive the benefits of WMM QoS>

The application must support WMM.

WMM shall be enabled on the Access Point.

WMM shall be enabled in the wireless adapter on client's computer.

IAPP: IAPP (Inter Access Point Protocol) is a protocol by which access points share information about the stations connected to them. When this function is enabled, the system will automatically broadcast information of associated wireless stations to its peer access points. This will help wireless stations roam smoothly among IAPP-enabled access points in the same wireless LAN.

Multicast-to-Unicast Conversion: When Multicast-to-Unicast Conversion is enabled, the Access Point intelligently forwards traffic only to those ports that request multicast traffic. Adversely, when disabled, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.

Multicast/Broadcast Rate: Bandwidth configuration for multicast/broadcast packets. If your wireless clients require a larger or smaller bandwidth for sending multicast/ broadcast packets, the administrator can customize the Access Point's multicast/ broadcast bandwidth here.

Management Frame Rate: This feature controls the bandwidth for Management Frames. The higher the rate it, the shorter range the transmission covers

Receiving RSSI Threshold: To ensure connected stations have quality connection speeds, a station will not be able to associate to the network unless its receiving sensitivity meets the configured threshold.

8.5 WDS Management

This list is to show the information of each WDS link configured in the managed AP, including Peer AP, Band, Channel, Security, TX Power, Link Speed, SNR, TX Bytes, TX Packets, STP and Status.

The WDS link if established between APs listed on List will be listed here with related information such as the Band and Channel of the link, Security settings if any and the Transmit Power, Byte, Packets etc.

8.6 AP Firmware management

8.6.1 Backup Configuration

Backed up Config files can be used to restore an AP's settings in List. When administrator backs up an AP's configuration settings, all the backup files are listed on the Backup Config tab page and can be downloaded to a local storage device or deleted from WLAN controller's memory.

8.6.2 Firmware

The WLAN controller can store AP’s firmware in its’ built-in memory. Under the Firmware tab page administrator can upload new AP firmware to the WLAN controller’s memory allowing for easy remote AP upgrade and restore operations from the AP List page. The AP firmware listed under this page can be downloaded or deleted from WLAN controller memory if desired.

8.7 Rogue AP Detection

Rogue AP detection is another essential way of protecting your network environment. Wide AP Management supports the detection of non-authorized access points present in the vicinity. Non-authorized access points pose a possible problem in terms of wireless interference.

General Configuration
Rogue AP Detection: to enable or disable the feature, if enabled, the system may take another effort to detect them.
Scanning Interval: to determine the scanning period
Channel Switching: AP will scan all channels and choose the one with the least utilization rate
Sensor List: to select RF cards (only selected AP models) for the scanning job as sensor. The AP will broadcast probe requests to collect surrounding APs' information. It is able to check the scanning log by clicking the hyperlink of “View”
Trust APs: to add AP’s shown in the suspected rogue AP list to the trusted list for further management if it can be manually identified as a safe source.

Rogue AP List
Discovered access points are temporarily put in the Rogue AP list. Click one of the hyperlinked BSSID’s to see its detailed information. However, if admin recognized some of the listed APs as trusted, just check the checkboxes before the BSSID column and then click Add to Trusted AP List. This action will be recorded in the Trusted AP Configuration.

8.8 AP Load Balancing

This is a function that prevents managed APs from overloading. When the system detects the occurrence of APs' associated-client numbers exceeding a predefined threshold at circumstances and other APs in the same group are still below the threshold, the balancing function will be activated to decrease the overloading APs' transmit power and increase other available APs' transmit power; this will let other available APs have more chance to be associated. The system can divide the managed APs into groups; define the group threshold, and a time interval which will trigger the AP load balancing.

Load Balancing: to enable or disable the feature
AP Distance: This parameter allows the administrator to specify the distance which will be used as a

measure of grouping managed APs. The unit is in meters, the administrator can configure an integer ranging from 0 ~ 999 where 0 signifies that the function is Disabled. APs which are distanced within the configured distance from one another will be regarded as the same group.

Internal: to initiate criteria of enforcement interval to trigger the AP load balancing

Threshold: This parameter allows the administrator to select between client loading Number of Client or traffic loading Number of Packets as the measure of an AP's system load. Administrator can specify the system threshold which will initiate the load balancing mechanism.

Cluster: The system can divide the managed APs into 3 different groups and perform transmit power management, each with individual client threshold

Device List: The grouping of AP devices can be done on the Device List page.

9 How to configure Switch Management

The Edgecore SW1024 is a powerful 24+2 Port VLAN switch with 500W of power budget. The WLAN controller gives administrators one comprehensive interface for managing your Edgecore equipment including the Edgecore SW1024.

There are several features for centralized managed switches

- Switch List
- PoE Schedule Template
- Backup Configuration

9.1 Switch List

A Edgecore SW1024 switch connected either to a WAN port or LAN port of the WLAN controller can be added manually or by discovery. In the Switch List, the Switch's name will be shown as a hyperlink in the Switch List. Administrators can click the hyperlink of each managed SW1024 for further configuration (General Setting, PoE Setting, VLAN Membership Setting, Port Setting, PoE Schedule) on the switch.

Add: The "Add" function is used to set up a switch via filling in the required information. After the switch is added to the List, the switch's status will display "online" or "offline".
Delete: Select the switches you wish to remove from the list by clicking the corresponding checkboxes followed by the Delete button.
Restart: Select the switches you wish to reboot from the list by clicking the corresponding checkboxes followed by the Restart button.
Backup: The "Backup" button saves the configuration .db file for the switch on the controller. This file can be used for restoring settings on a switch.
Restore: When a Backup configuration file is saved on the controller, check the checkbox for the switch and click the "Restore" button to restore settings on a switch.

9.2 PoE Schedule Template

There are prepared template for further application in the template table. The first template (Template Name is Default) is the default template and cannot be deleted. The Template Name may be customized for easy reference (eg. Switch-Core1). Administration can click "Configure", illustrated by the pencil icon, to enter settings for the Template while click "Delete", illustrated by the red cross to erase the template. The template can be copied from existed template. The following can be set on the PoE Schedule Template:

Power Supply Schedule: to check the desired hour in the schedule table of each template
Apply to: to select the managed switch first and assign the port with scheduled PoE transmittance. The indication of the PoE Mode and Connected Device are helpful when configuration.

9.3 Backup Configuration

The list gives an overview of the backed up configurations. Administrators may download the configuration file for restoration, or check the checkboxes to delete the selected configuration files.

10 How to realize Wi-Fi Monitor

WiFi Monitor allows the administrator to simulate WiFi signal coverage of Access Points; be it a virtual area or a real managed APs signal coverage. It also monitors AP statuses and statistic information of the managed APs.

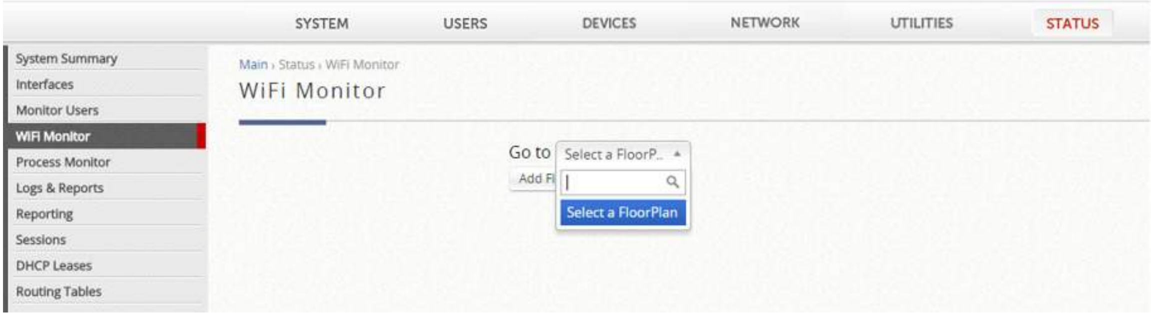
This is designed to help administrators with network survey, planning and performance enhancement during the initial installation stage, and also monitoring managed APs in an existing deployment.

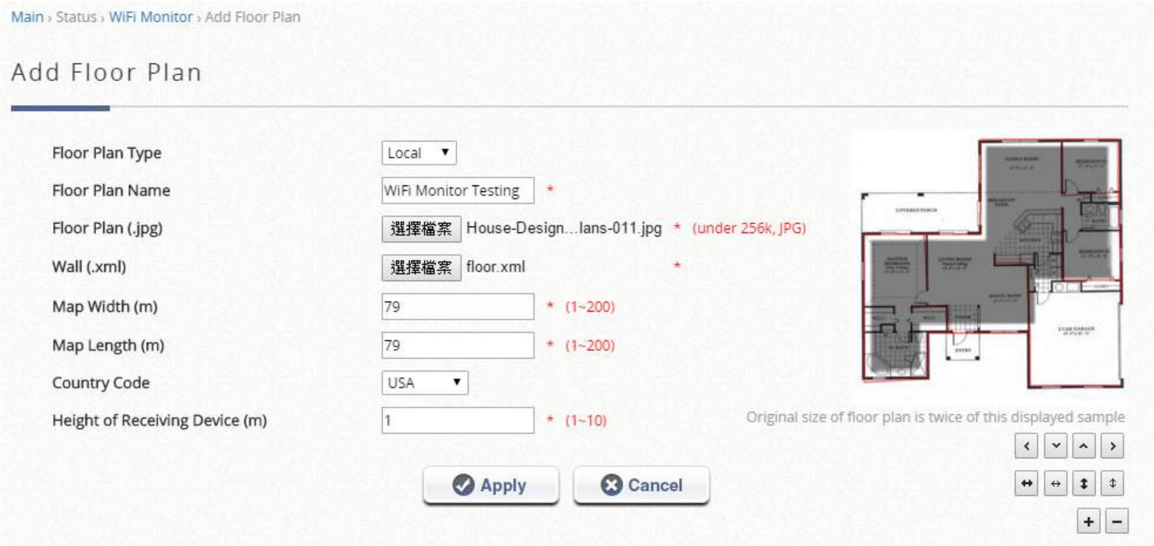
There are 3 different type of floorplan: Virtual, Local, and Wide .

Models currently supporting the AP Simulation Utility are: EWS100, EWS5203, EWS5204, EWS5207.

10.1 Add a Floor Plan

The WiFi Monitor is designed to help administrators decide where APs should be placed and whether the number of APs would satisfy the throughput requirement during initial installation. First, a map or a floor plan in .jpg format is required, with partitions drawn in .xml format.




Main › Status › WiFi Monitor › Add Floor Plan

Add Floor Plan

Floor Plan Type	Local
Floor Plan Name	WiFi Monitor Testing *
Floor Plan (.jpg)	選擇檔案 House-Design...lans-011.jpg * (under 256k, JPG)
Wall (.xml)	選擇檔案 floor.xml *
Map Width (m)	79 * (1~200)
Map Length (m)	79 * (1~200)
Country Code	USA
Height of Receiving Device (m)	1 * (1~10)

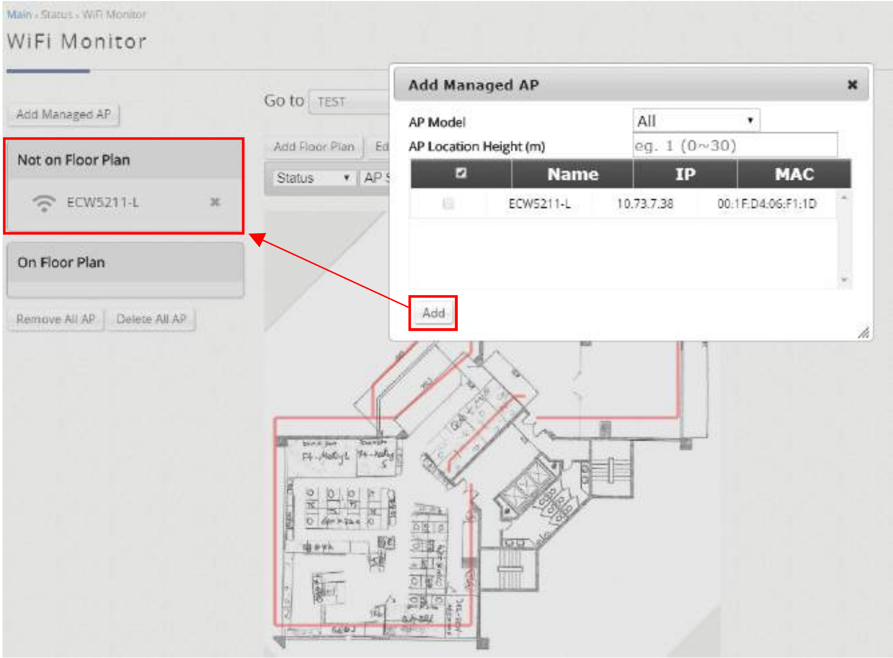
Original size of floor plan is twice of this displayed sample

Floor Plan Type: Determine if floor plan will be used for Local Area Managed APs or Wide Area Managed APs.
Floor Plan Name: Self-defined name for Administrator's reference.
Floor Plan: Select file for floor plan (.jpg format).

Wall: Select file for wall (.xml format).
Map Width: Actual width of floor plan.
Map Length: Actual length of floor plan.
Country Code: Select the country code (EU/US). This will determine the max output power of access points
Height of Receiving Device (m): The assumed average height of receiving client devices.

Managed AP Simulation is a used for monitoring of Access Points based on location. The APs on the Managed AP Simulation floor plan are real managed Access Points on the Controller (either by Local AP Management or Wide AP Management).

Access Points here are linked to APs managed by the WLAN controller, and we can see real AP information such as the IP address, MAC address, and Associated Client number. This allows the administrator to easily visualize the wireless network with respect to the APs' location.



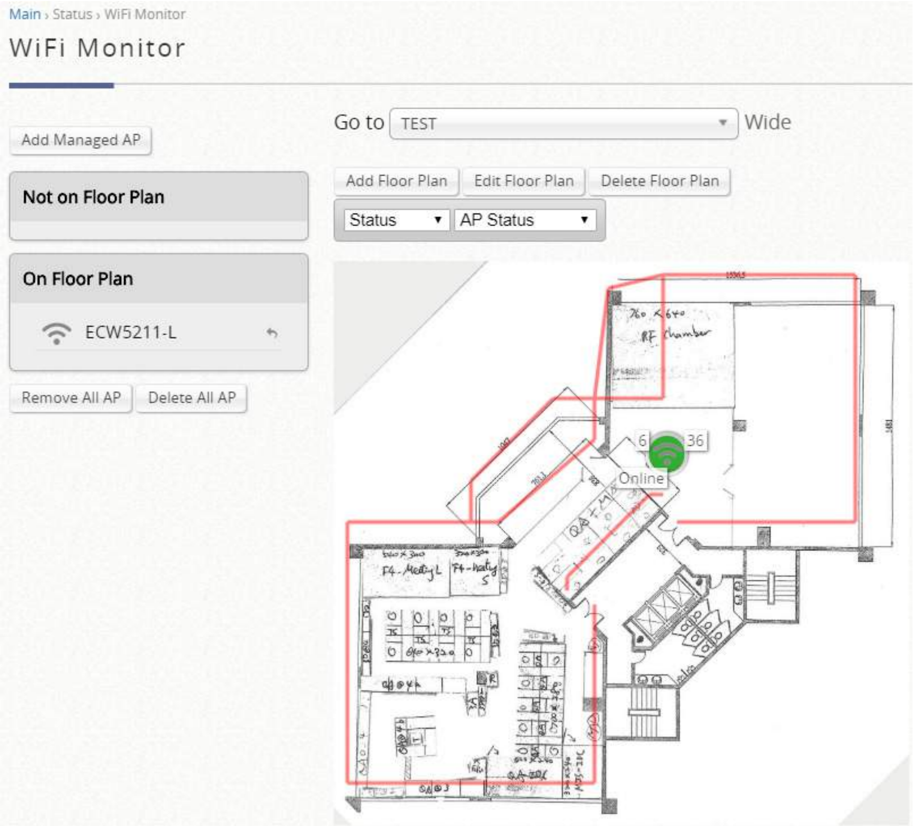
Add Managed AP

AP Model: All
AP Location Height (m): eg. 1 (0~30)

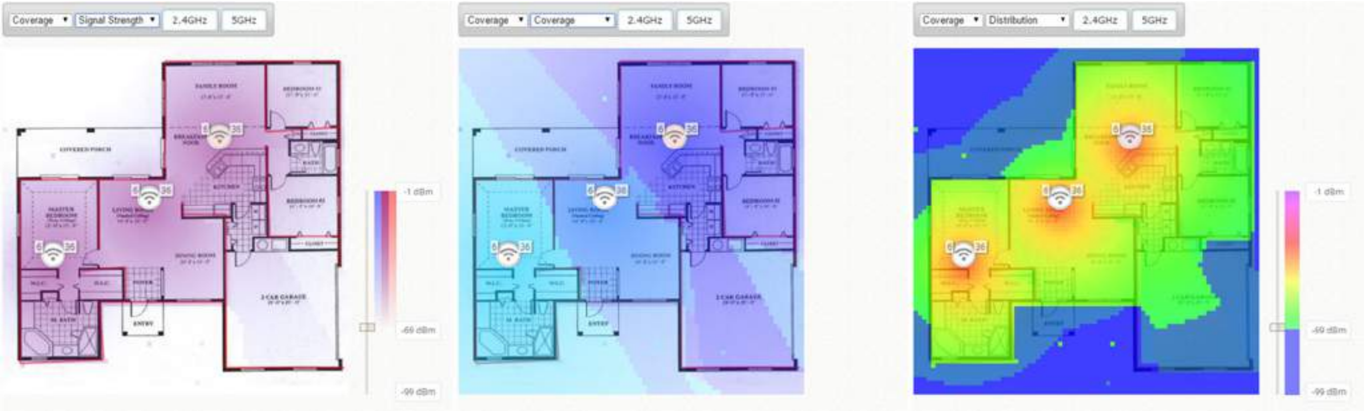
☑	Name	IP	MAC
□	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D

Once these managed APs are created, simply drag and drop these APs onto the floor plan. 2.4GHz is indicated blue and 5GHz is indicated red for signal strength (hence purple when both bands are overlapping).

Signal Strength: The darker the color, the stronger the signal strength is.
Coverage: Different colors depict the different coverage area of each AP.
Distribution: Use different colors to illustrate the strength of signals.



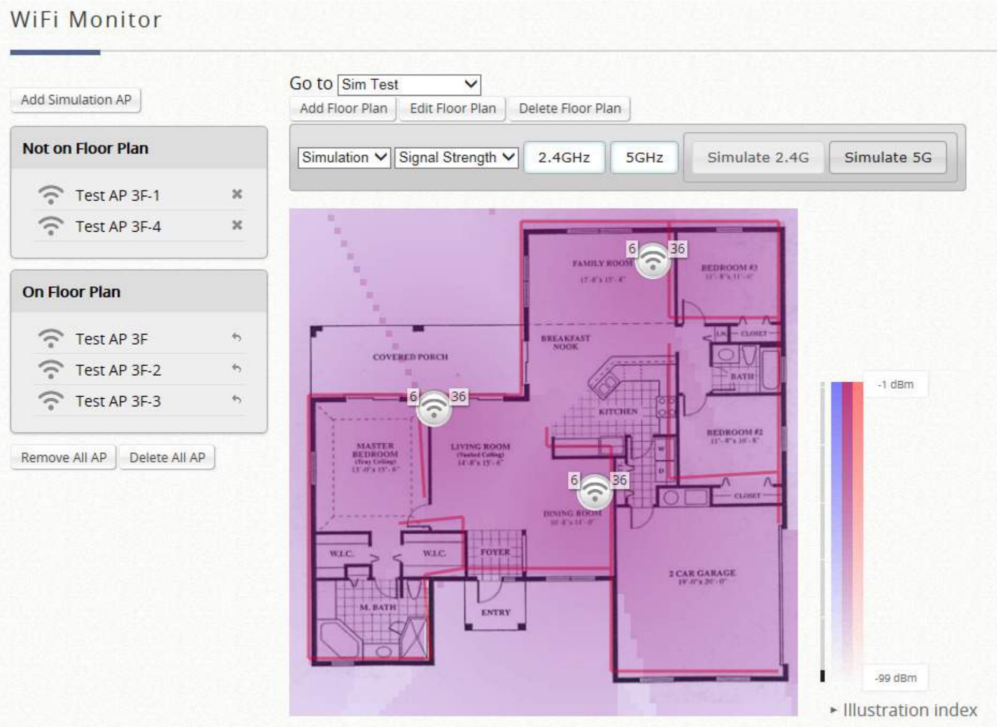
The Signal Strength and Coverage of the managed APs would depend on factors such as the AP model, transmit power, AP Height, and etc.



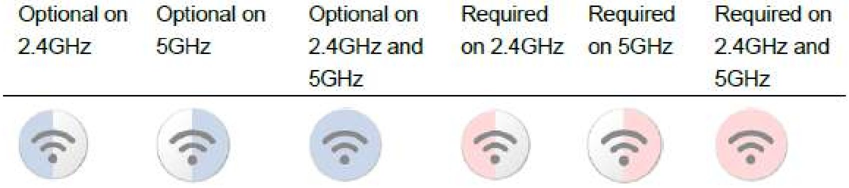
10.2 Simulation AP

WiFi Monitor is able to simulated Edgecore APs, placing into the floor plan and checking the correlated configuration in optimization. Meanwhile, the Signal Strength and Coverage of the simulation APs would depend on factors such as the AP model, transmit power, AP Height, and etc.

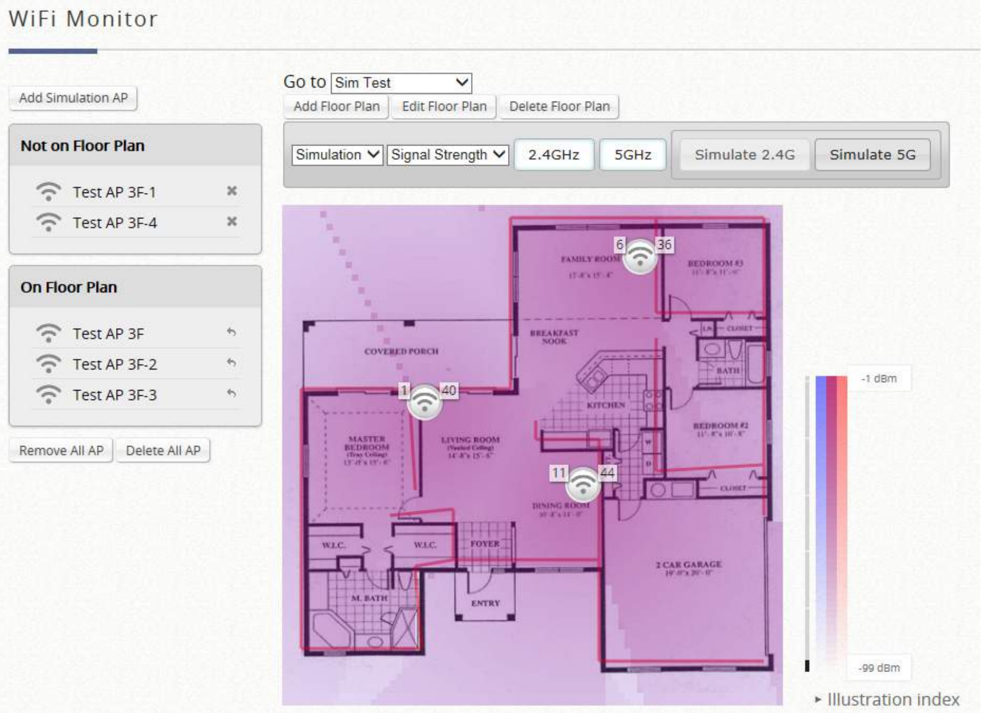
With the floor plan and partitions in place, simulation APs can now be added to the floor plan for simulation as shown below.



Click “Simulate 2.4G” or “Simulate 5G” to see if the deployed APs are adequate for your requirement.

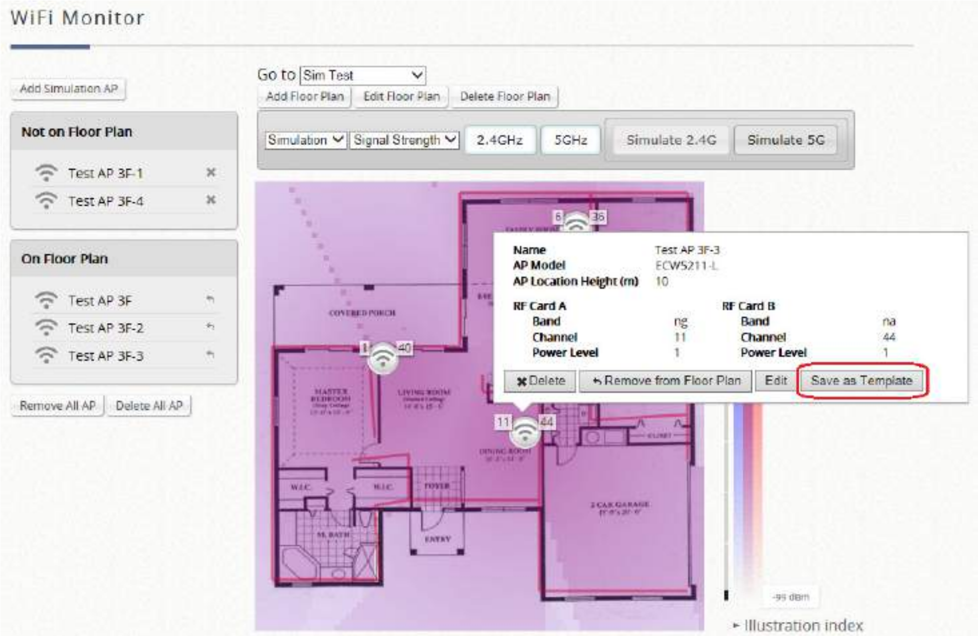


When simulation is done successfully, the recommended channel allocation will be shown next to the Simulation AP.



WiFi Monitor

Go to Sim Test



WiFi Monitor

Go to Sim Test

Name Test AP 3F-3
AP Model ECWS211-L
AP Location Height (m) 10

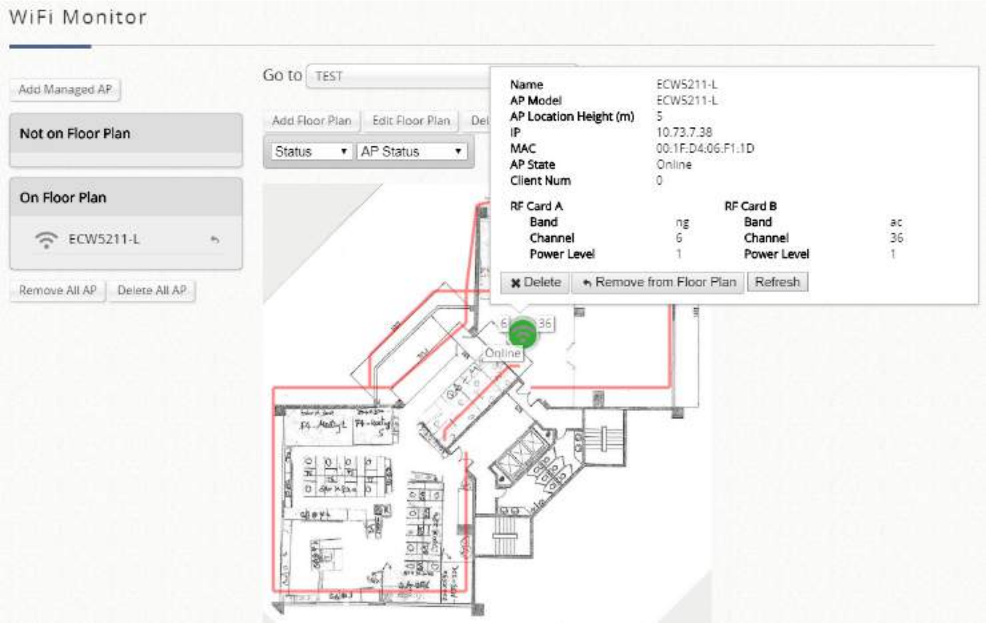
RF Card A
Band ng
Channel 11
Power Level 1

RF Card B
Band na
Channel 44
Power Level 1

Configurations can then be saved conveniently to a template to be used for AP Management.

10.3 AP Monitoring on Floor Plan

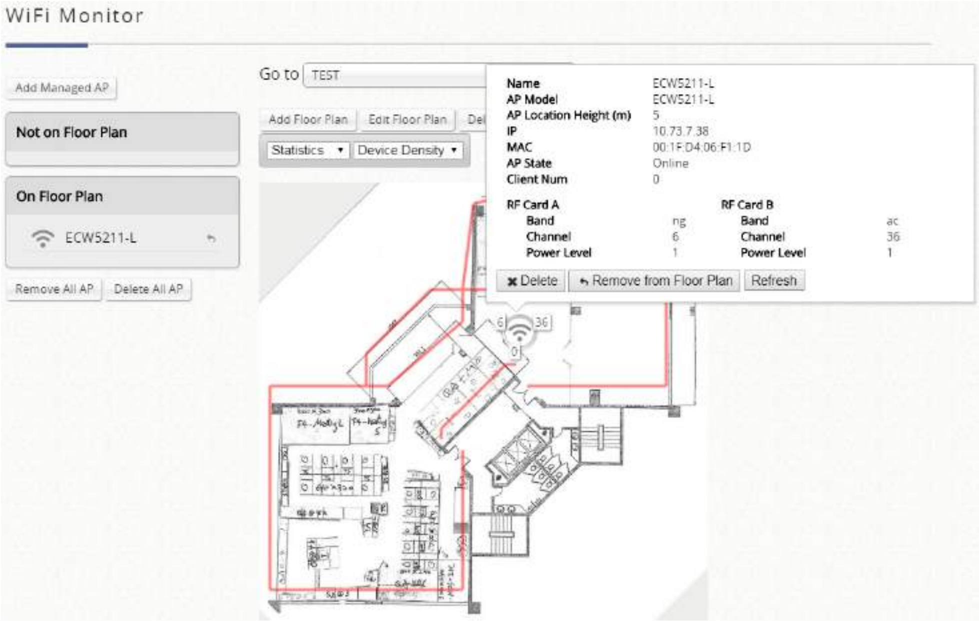
In an area with operating APs, administrators may view AP statuses from the created floorplan. The AP status shows Online, Offline or Disabled. Administrators may also obtain CPU Idle and Memory Usage when APs are managed by Wide area AP Management.



Name	ECW5211-L
AP Model	ECW5211-L
AP Location Height (m)	5
IP	10.73.7.38
MAC	00:1F:D4:06:F1:1D
AP State	Online
Client Num	0

RF Card A		RF Card B	
Band	ng	Band	ac
Channel	6	Channel	36
Power Level	1	Power Level	1

AP statistic information, such as AP density and AP average traffic, and AP average traffic are also supported when APs are managed using Wide area AP Management.



Name	ECW5211-L
AP Model	ECW5211-L
AP Location Height (m)	5
IP	10.73.7.38
MAC	00:1F:D4:06:F1:1D
AP State	Online
Client Num	0

RF Card A		RF Card B	
Band	ng	Band	ac
Channel	6	Channel	36
Power Level	1	Power Level	1

11 How to enable VPN feature

Multiple types of VPN are available on the system: Remote VPN, and Site-to-Site VPN. For Remote VPN, the system allows the VPN tunnel between a remote client and the system to encrypt the data transmission via PPTP or IKEv2. For the Site-to-Site VPN, an IPSec tunnel can be used to connect to other IPSec capable device over the Internet.

11.1 Remote VPN PPTP

WLAN controller supports Remote VPN for user login to system from a remote area. After the user is logged in to system from the outside network of WAN, it will appear to the user that the login to WLAN controller is under the service zone locally. Policy can also be applied and users are controlled by system to access the network.

All settings are similar to the settings in a Service Zone. Remote VPN can also be setup with a SIP WAN Interface, Authentication Options, Group Permission, and Applied Policy.
Function: to enable or disable the Remote VPN PPTP feature in the system
Allocate IP Address from: the IP range for VPN clients. Default is 172.29.0.1/24
WISPr: to include some attributes in RADIUS protocol when integrate with RADIUS authentication server
Authentication Options: Databases for IKEv2 are built-in LOCAL database, external RADIUS authentication server, NTDomain, LDAP, and POP3 server

Note: PPTP, IKEv2 and Site-to-site VPN can work respectively
Note: the Remote VPN clients can be applied by different user policies at the page of
Main › Users › Groups › Configuration

11.2 Remote VPN IKEv2

Currently, some Operating Systems have decided not to support the PPTP connection such as iOS10, macOS Sierra or newer OS. Therefore, for maintaining the remote VPN feature, IKEv2 solution, a modern protocol developed by Microsoft and Cisco, was chosen as a default VPN type in OS X 10.11 (El Capitan) and Windows since 7. It supports strong encryption, auto reconnection on network change, easy configuration and more.

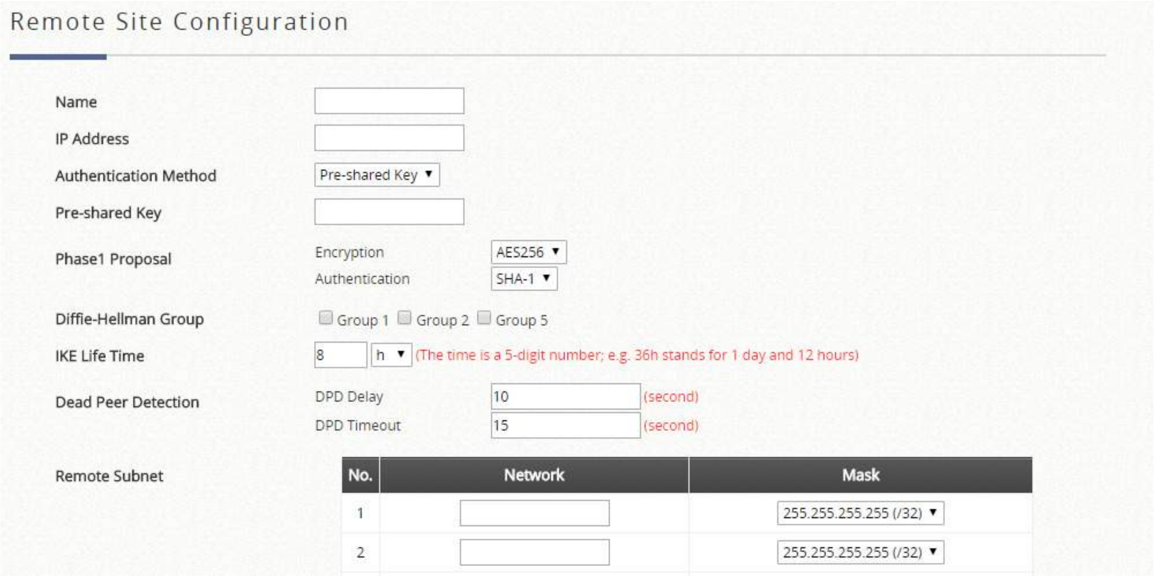
Function: to enable or disable the Remote VPN IKEv2 feature in the system
Allocate IP Address from: the IP range for VPN clients. Default is 172.16.0.1/24
Certificate: to assign the legal certificate for IPSec tunnel used
WISPr: to include some attributes in RADIUS protocol when integrate with RADIUS authentication server
Authentication Options: Databases for IKEv2 are only built-in LOCAL database and external RADIUS authentication server.

Note: PPTP, IKEv2 and Site-to-site VPN can work respectively
Note: the Remote VPN clients can be applied by different user policies at the page of
Main › Users › Groups › Configuration

11.3 Site-to-site VPN

WLAN controller supports Site-to-Site VPN for more than 2 WLAN controllers to create VPN tunnel to each other over the WAN network. It is based on open source site-to-site VPN protocol and it is backward compatible with previous WLAN controllers' site-to-site VPN feature. For example, if there are 2 WLAN controllers, you can create a VPN tunnel to let a subnet of one WLAN controller to access the subnet of another WLAN controller.

First, you need to add a Remote Site with at least one remote subnet. The IPSec settings in both sites must be same.



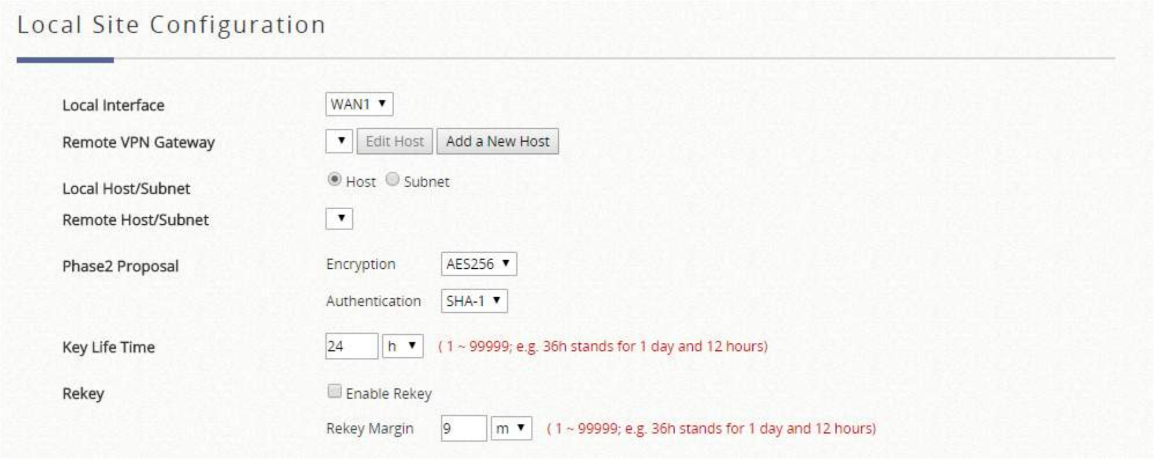
Remote Site Configuration

Name		
IP Address		
Authentication Method	Pre-shared Key ▼	
Pre-shared Key		
Phase1 Proposal	Encryption	AES256 ▼
	Authentication	SHA-1 ▼
Diffie-Hellman Group	□ Group 1 □ Group 2 □ Group 5	
IKE Life Time	8 h ▼ (The time is a 5-digit number; e.g. 36h stands for 1 day and 12 hours)	
Dead Peer Detection	DPD Delay	10 (second)
	DPD Timeout	15 (second)

Remote Subnet

No.	Network	Mask
1		255.255.255.255 (/32) ▼
2		255.255.255.255 (/32) ▼

Then create a Local Site with subnet for mapping to the remote site. Such as "192.168.11.0/24" of WLAN controller_A >> "192.168.111.0/24" of WLAN controller_B, after the tunnel is created, the users within these two subnets can reach each other.



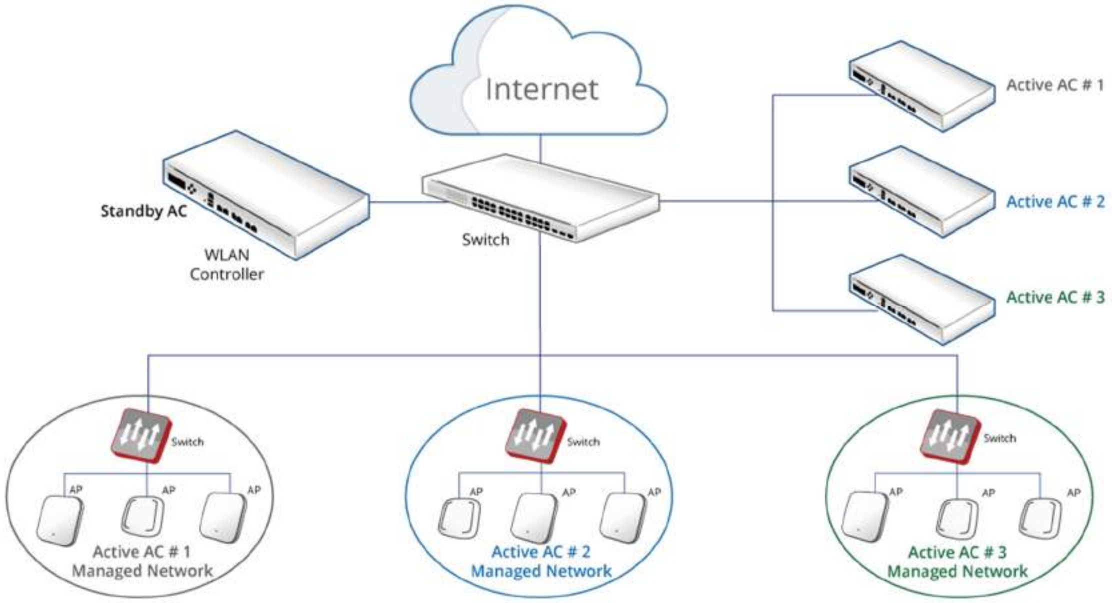
Local Site Configuration

Local Interface	WAN1 ▼	
Remote VPN Gateway	▼ Edit Host Add a New Host	
Local Host/Subnet	● Host ○ Subnet	
Remote Host/Subnet	▼	
Phase2 Proposal	Encryption	AES256 ▼
	Authentication	SHA-1 ▼
Key Life Time	24 h ▼ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)	
Rekey	□ Enable Rekey	
	Rekey Margin	9 m ▼ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)

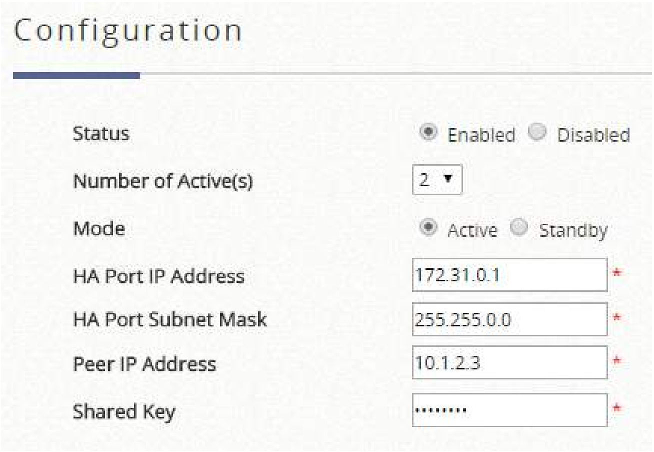
Note: You can create more than one VPN tunnel, but the IP segment mapping cannot be overlap, because one IP segment cannot have two routing rules.

12 High Availability

The Edgecore HA design principle is to use redundancy in achieving higher availability with minimum impact during service transition. The Edgecore HA approach implements a dedicated message link between ACs (Access Controller) to create an N + 1 redundancy system where N is ≤ 3. Once the HA link has been established, the Active ACs will be servicing all network traffic while the Standby AC will be in hot-standby ready to take over network service in case an Active AC can no longer provide service.

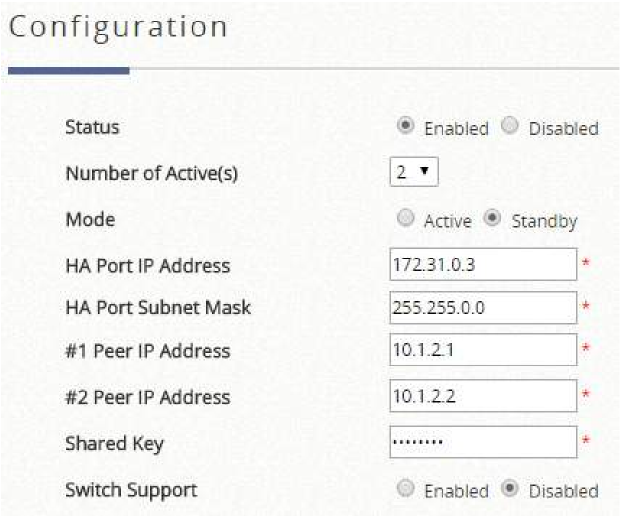


1. Edgecore HA feature is software determined to be enabled or disabled.
   - When enabled, LAN1 port will become the dedicated HA port.
   - When disabled, LAN1 remain its normal function as LAN port.
2. The Web UI has a configuration item to designate this AC as either “Active” or “Standby” when HA feature is enabled.
3. All HA configuration are manually applied. This includes AC role as an Active or Standby as well as the HA pair restoration after an AC goes down.



Configuration

Status	● Enabled ○ Disabled
Number of Active(s)	2 ▼
Mode	● Active ○ Standby
HA Port IP Address	172.31.0.1 *
HA Port Subnet Mask	255.255.0.0 *
Peer IP Address	10.1.2.3 *
Shared Key	•••••••• *



Configuration

Status	● Enabled ○ Disabled
Number of Active(s)	2 ▼
Mode	○ Active ● Standby
HA Port IP Address	172.31.0.3 *
HA Port Subnet Mask	255.255.0.0 *
#1 Peer IP Address	10.1.2.1 *
#2 Peer IP Address	10.1.2.2 *
Shared Key	•••••••• *
Switch Support	○ Enabled ● Disabled

4. HA link once established synchronizes all system configurations, user databases, user online status, system resource status, managed AP profile from the Active AC to the Standby AC.

5. There is a HA link monitoring mechanism by the standby AC when HA links have been established. This link monitoring module checks the status of the Active ACs. During an event when an Active AC is not responding, this module will regard this AC as no longer providing service and take over network service.
6. Local APM managed APs will experience little network interruption as they are L2 devices. Clients associated to locally managed AP will experience the same scenario (little or no network interruption) as wired clients during service switchover.
7. Wide Area managed APs (manually or via CAPWAP) over L3 device with tunnels established will be able to resume service within 5 min max (approximation) after service switchover with full AP management capacity.
8. HA Status Changes Email Notification can be configured "*Status > Reporting > Notification Settings > High Availability Mode Change*." For HA N+1, the email will be sent by new Active AC when it replaces to provide service; besides, there is a Standby-AC-is-DOWN email will be sent from Active AC(s) when there is no Standby AC detected when HA is already enabled.
9. HA feature can only be enabled for up to 3 ACs of the same brand and same FW version and build number.

HA Configuration

Status: This feature can be turn on or off here.

Number of Active(s): Selecting up to 3 Actives for N+1 HA

Mode: The role of this particular controller must be determined here manually.

HA Port IP Address: The IP address configured for the dedicated HA port. Should make sure that all WLAN controller's HA port IP are under the same subnet.

HA Port Subnet Mask: The subnet mask for HA communication.

Peer IP Address: Fill in the IP address of the peer Controller's HA port.

Shared Key: Enter a secret string on both of the controller. The Shared Key must be the same for a successful HA connection.

Switch Support: when HA N+1, N=2 or 3, the Edgecore SW1024 is required since the related LAN port and VLAN IDs can automatically be modified when HA is happening. If administrators would like to set port1, port 4 and port 2 on SW1024 for #1 Active AC with VLAN 101, 41, 42, respectively, please enter 1,4,2 on #1 Active Related Port(s) and type 101, 41, 42 on #1 Active LAN Port VLAN ID(s).

Action: This function may be triggered on the primary controller, switching service to the secondary controller manually. (available on 1+1 HA only)

HA Current Status

Dedicated Port: Currently port LAN1 is dedicated as the HA port for all WLAN controller models.

Status: to reflect the current status of the HA link.

Link to Peer's UI: to have a quick access to the peer Web UI by selecting the page

Version: to show the HA feature revision.

13 Port Location Mapping

The Port Location Mapping feature allows each Service Zone to own multiple VLANs (as if each VLAN is a port) in order to identify where the clients are coming from. Administrator could use Port Location Mapping feature to map a location (such as a hotel room) to a VLAN port of VLAN switch or a DSLAM device. Each Room is mapped to a VLAN Tag. And each Room can be assign to different Service Zone to get different policy. Furthermore, according to your application, you can configure the different rooms to different Port Type: Open, Block, or Auth. Required.

Open: this port type means the user can access internet in this room without any charge.
Block: If you do not want to provide any internet access right in the rooms, you may change the Port type of the rooms to Block. If the user opens a browser and tries to access internet, it will pop up a Blocking message to notify the user.
Auth. Required: this port type is used mainly for hospitality application to charge users. When the user opens a browser and tries to access internet, a page with disclaimer and billing plan options will be displayed. The user can select the desired plan and click confirm button to purchase an account. The account cost will be sent to the PMS and added to the hotel bill via the configured middleware.

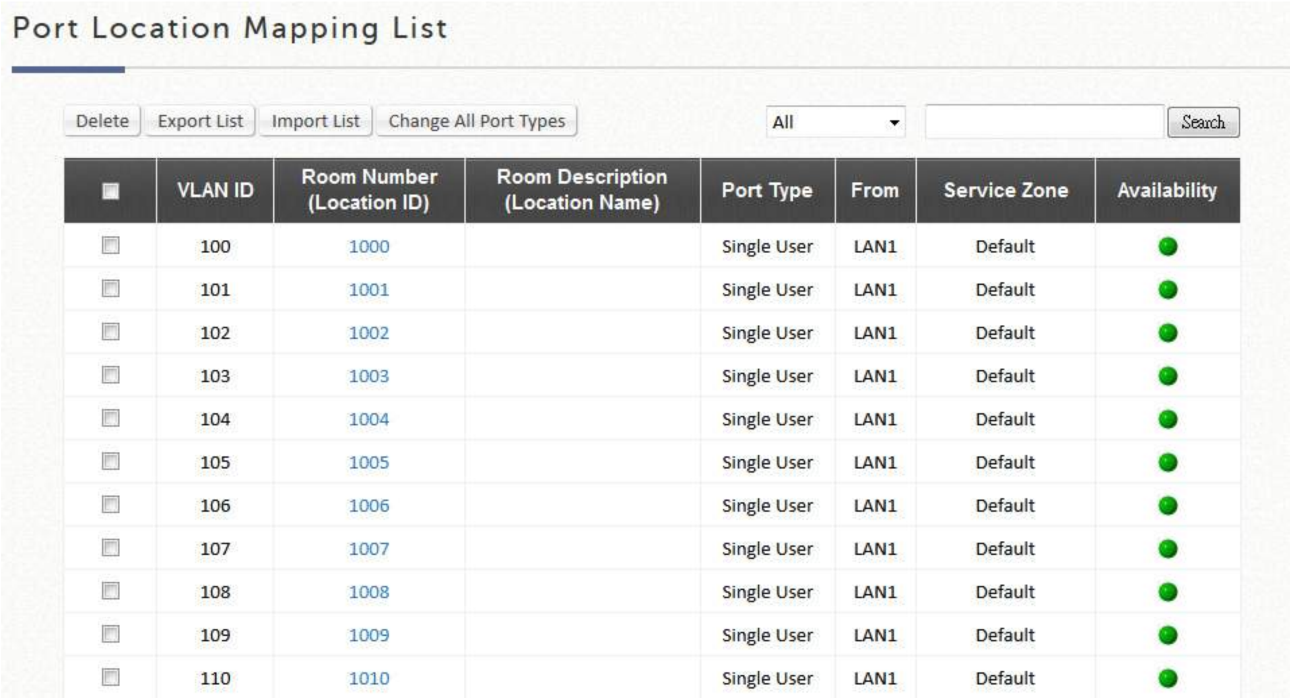
Create Single Mapping
Port Type: The default state of the rooms, it may be: Open, Block, Auth. Required.
Choose LAN Port: Select the LAN Port for which traffic is received
Service Zone: The service zone profile used to provide internet service to the corresponding location.
DHCP Scope: Select which DHCP Scope to use from corresponding Service Zone.
Assign VLAN ID: The starting VLAN ID.
Location ID: A numeric identification number (or typically the room number).
Location Description: Optional description for reference.
User Limit: Maximum number of users in batch on corresponding port
NAS Identifier: An optional parameter for RADIUS attribute.
Class: An optional parameter for RADIUS attribute.
HTTP Parameter: Used only when an External Login Page is configured and additional HTTP parameters are required.

Create Multiple Mappings
Port Type: The default state of the rooms, it may be: Free, Block, Single User, Multiple User.
Choose LAN Port: Select the LAN Port for which traffic is received
Service Zone: The service zone profile used to provide internet service to the corresponding location.
DHCP Scope: Select which DHCP Scope to use from corresponding Service Zone.
Assign VLAN ID From: The starting VLAN ID.
Number of VLAN: The total number of VLAN.
Location ID: A numeric identification number (or typically the room number).
Location ID Prefix: The prefix (of room number).
Location ID Postfix: The postfix (of room number).

User Limit Per Port: Maximum number of users in batch on corresponding port.
NAS Identifier From/Prefix/Postfix: An optional RADIUS Attribute

Note: VLAN Ports may be created one by one or batch at once. Subsequent changes are possible by Change Port Type configuration box.
Note: The VLAN Tags configured in Port Location Mapping must not conflict with any of the VLAN Tags that has been assigned to each Service Zone.

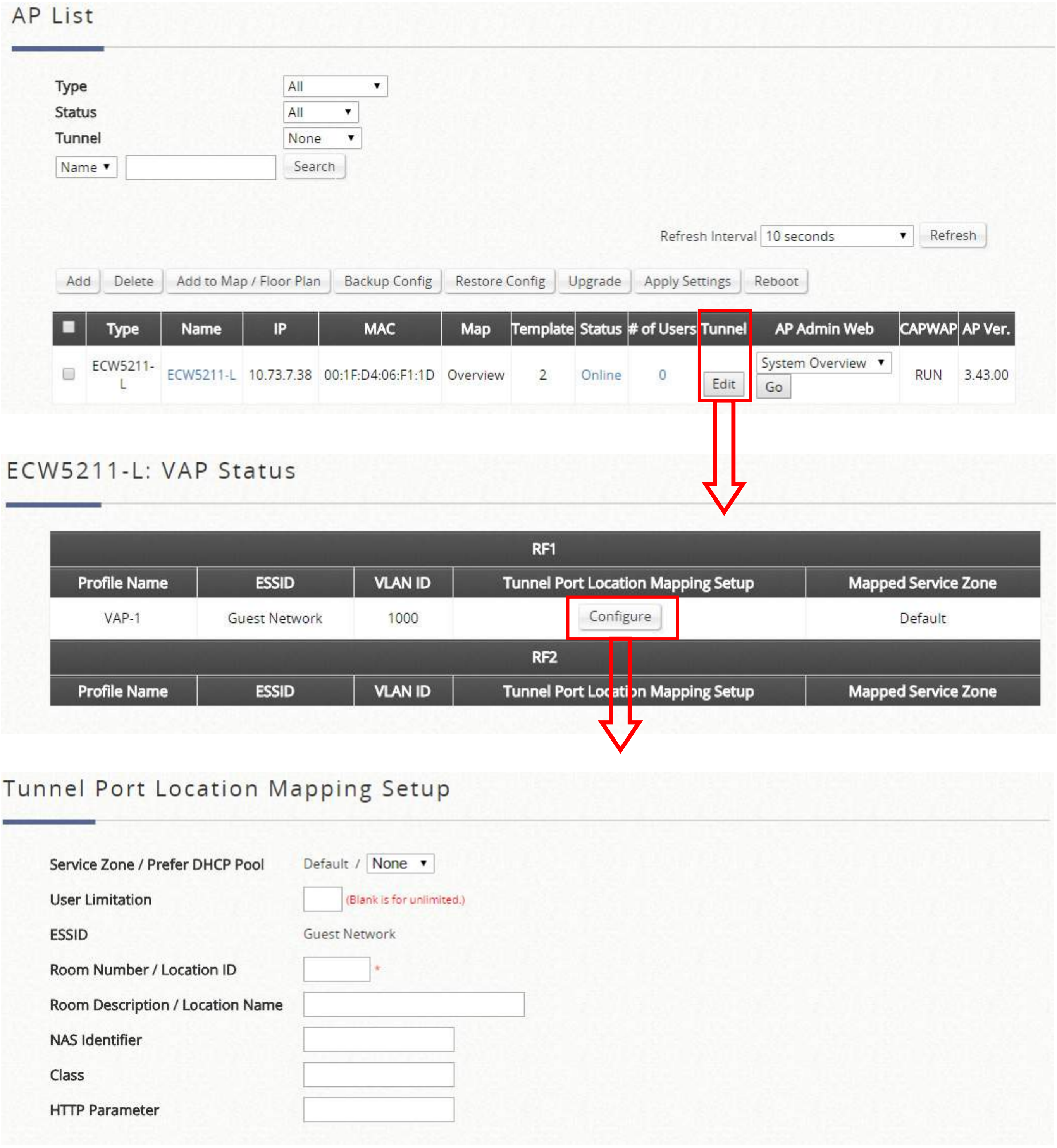
Port Location Mapping List
The Port Location Mapping List displays all the profile entries with information such as its' VLAN ID, Room Num/Location ID, Port Type and Service Zone.
Delete: to erase an individual Port Location Mapping profile
Export List: to back up the existed Port Location Mapping List
Import List: to restore the Port Location Mapping List
Change All Port Type: To configure Port Type for all rooms: Free, Block, Single User, Multiple User.



■	VLAN ID	Room Number (Location ID)	Room Description (Location Name)	Port Type	From	Service Zone	Availability
□	100	1000		Single User	LAN1	Default	●
□	101	1001		Single User	LAN1	Default	●
□	102	1002		Single User	LAN1	Default	●
□	103	1003		Single User	LAN1	Default	●
□	104	1004		Single User	LAN1	Default	●
□	105	1005		Single User	LAN1	Default	●
□	106	1006		Single User	LAN1	Default	●
□	107	1007		Single User	LAN1	Default	●
□	108	1008		Single User	LAN1	Default	●
□	109	1009		Single User	LAN1	Default	●
□	110	1010		Single User	LAN1	Default	●

Tunnel Port Location Mapping List
For VAPs which are tunneled back to the controller from remote APs. Administrator may wish to allocate a NAS Identifier as well as designate an IP pool for service.

In the managed AP list in Wide Area AP Management, administrator can allocate NAS Identifier and designate an IP pool for service for each VAP of a Managed AP. This can be configured while establishing tunnels between the AP and Controller.



AP List

Type	All
Status	All
Tunnel	None
Name	

☐	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.
☐	ECW5211-L	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D	Overview	2	Online	0	Edit	System Overview Go	RUN	3.43.00

ECW5211-L: VAP Status

Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
RF1				
VAP-1	Guest Network	1000	Configure	Default
RF2				
Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone

Tunnel Port Location Mapping Setup

Service Zone / Prefer DHCP Pool	Default / None
User Limitation	(Blank is for unlimited.)
ESSID	Guest Network
Room Number / Location ID	*
Room Description / Location Name	
NAS Identifier	
Class	
HTTP Parameter	

Once the VAP tunneled back, complete tunnel or split tunnel, has been configured with PLM (Port Location Mapping), remote sites may also benefit from the PMS system or other centrally managed hotspot operations which require location attributes or information.

14 PMS Integration

Administrator may choose to select the interfacing protocol that is compatible with their site's hospitality management system or PMS system.

- Net Retriever
- Micros Opera

Net Retriever

Net Retriever Setup: Enter the Secret, Interface Port, MI ID, AC ID, and Link Test Interval for Middleware connection.

Secret: The secret key between Guest Service Device and PMS Middleware for challenge and response (MD5 Hash) to test the authenticity of the link. It should contain one or more lowercase letters, uppercase letters, numbers and symbols. It should also be between 8 ~ 16 characters.

Interface Port: The port used by Net Retriever, the default is "8324".

MI ID: The ID of the Middleware.

AC ID: The ID of the Access WLAN controller (the gateway).

Link Test Interval: The time interval for the gateway to perform Link Test, the default is "300" seconds.

User Account Log: The events occurred in the background relating to this feature are recorded and may be displayed here.

Delete Account on Check Out: The user account status bundled with a room may be forcefully expired from use should the administrator desires upon room check out.

Micros Opera

Micros Opera Setup: Enter the PMS IP and PMS Port for Middleware connection.

PMS IP: Enter the IP used by the Micros Fidelio PMS.

PMS Port: Enter the Port used by the Micros Fidelio PMS.

Account Credentials: Administrators may define User Account credentials using a combination of RN (Room number), GN (Guest Name), G# (Guest Number) or G+ (Profile Name) to designate the Micros protocol parameter for carrying the username and password information.

Room Bill Description: to enter description will appear on Room Bills via PMS integration.

Login Error Message: to customize the error message content

User Account Log: The events occurred in the background relating to this feature are recorded and may be displayed here.

Synchronize Data with PMS: to synchronize data with the PMS server to ensure database is up to date.

PMS External Page Customization API: PMS API provides administrator a flexible implement with customized login page, where login information, billing plan chosen, purchase unit and so on could complete the accessing process.

- External Page Validity Verification: Administrator also could utilize its own username and password to secure the API protocol between external web server and WLAN controller.
- Sample External Login Page: there is a downloadable example which administrator could easily realize how to integrate and modify

- All req_type could use the filed “format” with Json
- req_type=1 (equals: bpinfo) could show the billing plan information, if add the fields “all”, it would show all billing plans, including inactive one
- req_type=2 (equals:check) confirm available billing plans, units and the users whether is allowed to buy a certain billing plan, if there is any error, it would return the error code and message for admin
- req_type=3 (equals:userinfo) could show the user’s information and status. If add the fields “all”, it would show the value of customized attributes A0-A9. If add the specific fields (A5, A9), it would show the corresponding values.
- Before testing, it is noted that the administrator’s password of WLAN controller which is used in the function send_req
- For the corresponding Service Zone, please customize the login page with Use External Page

15 Utilities for WLAN Controller

15.1 Network Utilities

There are dozens of built-in Network Utilities for troubleshooting or setup verification.

- IPv4
- IPv6
- Sniff
- IP Discovery

15.1.1 IPv4

Ping: It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.
Trace Route: It allows administrator to recover the real path of packets from the gateway to a destination using IP address or Host domain name.
ARPing: Allows the administrator to send ARP request for a specific IP address or domain name.
VLAN ID: to check the VLAN ID of the entering IP/MAC address and clicking “Find” button
ARP Table: It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).
Status: When the administrator is executing any Network Utilities features, the status of the operation is displayed here.
Result: The operation result is displayed here.

15.1.2 IPv6

Ping: It allows administrator to detect a device using IPv6 address or Host domain name to see if it is alive or not.
Trace Route 6: It allows administrator to recover the real path of packets from the gateway to a destination using IPv6 address or Host domain name.
Neighbor Discovery: The administrator can use this feature to learn about IPv6 Neighbor nodes that are on the same IP segment or domain name.
Neighbor Cache: a node that manages the information about its neighbors in the Neighbor Cache. This feature allows the administrator to view the information stored on system’s neighbor cache.
Status: When the administrator is executing any Network Utilities features, the status of the operation is displayed here.
Result: The operation result is displayed here.

15.1.3 Sniff

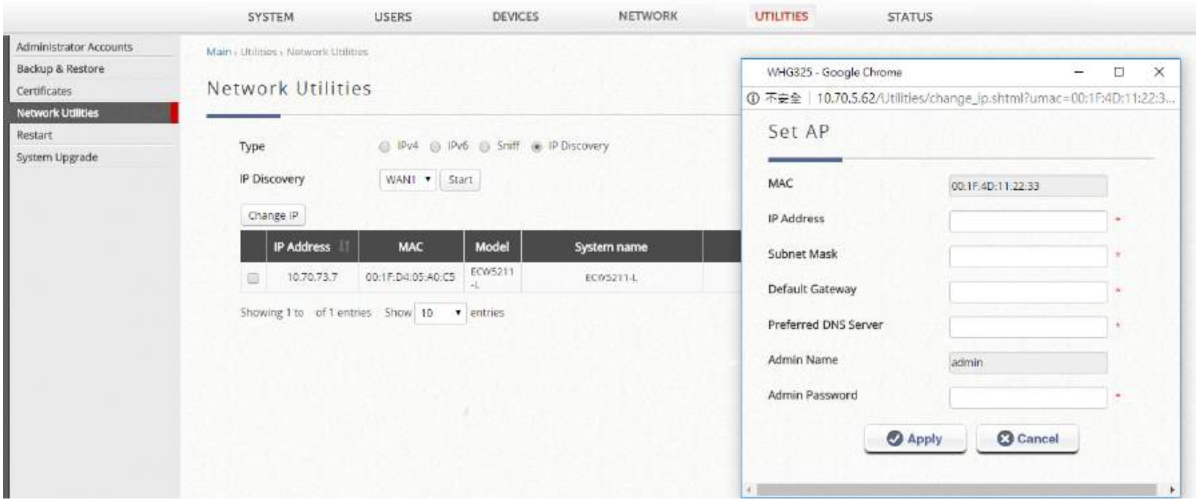
With this feature the administrator can listen for packets from selected Interfaces. The administrator can further filter the types of packets to capture by using tcpdump commands under the Expression field.

15.1.4 IP Discovery

The network administrators need to access or modify some information without entering AP interface, such as forget the IP address of the AP, forget the admin's password, or configure the IP address of the AP.

All they need to do is connect Edgecore AP within the same Layer 2 from the ports of the WLAN controller, select the interface, WAN or LAN, and press the "Start" button to execute the IP Discovery Utilities. The scanning results would be devices' corresponding IP address, MAC address, Model, System Name, SSID (each VAP), VLAN ID. The WAN/ LAN ports of devices could connect through switch to other devices (APs).

This powerful and proprietary built-in utility is now both in our controller and access point.



Network Utilities

Type ○ IPv4 ○ IPv6 ○ Sniff ● IP Discovery

IP Discovery WAN1 ▾ Start

	IP Address	MAC	Model	System name
□	10.70.73.7	00:1F:D4:05:A0:C5	ECW5211-L	ECW5211-L

Showing 1 to of 1 entries Show 10 ▾ entries

不安全 | 10.70.5.62/Utilities/change_ip.shtml?umac=00:1F:4D:11:22:3...

Set AP

MAC: 00:1F:4D:11:22:33
IP Address: *
Subnet Mask: *
Default Gateway: *
Preferred DNS Server: *
Admin Name: admin
Admin Password: *

15.2 Certificates

WLAN controller can issue certificates to APs that it manages in its private network. Administrator can sign certificates issues by the system's root CA and load these certificates to managed APs. These security certificates will be used in verifying the identity and authenticity of CAPWAP discovery requests between AP and AC. Also, they could be used for authentication of Built-in RADIUS Server users roaming out. 'Certificate Management' gives a summary of certificates available and which are currently in use.

The "Used By" column indicates current in use certificates and their corresponding applications. To further configure the different types of certificates, click the "Pencil" icon.

15.2.1 System Certificate

This is the certificate that identifies the system. These certificates may be used for applications such as HTTPS login, CAPWAP, and etc. The Controller has a built-in Factory Default Certificate (gateway.example.com) that cannot be removed, but allows certificates to be uploaded. To view details of the certificate, click the corresponding "View" button.

Certificate: to upload the certificate file in .crt, matching Private Key and Intermediate CA (if applicable)
Private Key: to upload the private key in .key file, matching Certificate and Intermediate CA (if applicable)
Intermediate CA: to upload the Intermedia CA in .crt, matching Certificate and Private Key (if applicable)
Get CERT: to download the certificate onto your local disk
Get Key: to download the public key onto your local disk

select the appropriate files

15.2.2 Internal Root CA

The administrator can upload an Internal Root CA, or generate a root CA for private use. The created root CA certificate can be downloaded and used to sign certificates generated by the system. Note that the system only allows one Internal Root CA to be created.

To upload an Internal Root CA, click browse to select the Certificate and matching Private Key from your local disk, and click "Upload Files".
Once an Internal Root CA is uploaded/generated, details will be shown in the following format.

To view details of the certificate, click the "View" button.

15.2.3 Internally Issued Certificate

Internally Issued Certificates can be generated on this page. Note that an Internal Root CA needs to be created first before Internally Issued Certificates can be signed. Certificate Information is an overview that displays all current Internally Issued Certificates. To view details of the certificate, click the corresponding "View" button.

15.2.4 Trusted Certificate Authorities

Apart from self-signed certificate and system's root CA, administrators can also upload other certificates signed by other CA entities or Trusted CAs into the system. These trusted root CA certificates are intended for the Controller to recognize and trust certificates of External Payment Gateway and/or CAPWAP capable APs. To upload a Trusted CA, click browse to select the Certificate and click "Upload Files". To view details of the certificate, click the corresponding "View" button.

15.3 Administrator Accounts

General Settings

Password Complexity: to limit how the passwords the sub-admins use should be formed.

- Min Password Length: to set a limit on the minimum length of a password string
- Min Password Category: to allow an admin to define how complex the passwords of the sub-admins are required. Below shows what each number stands for:

Number	Definition
0	passwords will not be checked
1	Passwords should include at least 1 form (capitalized letters/ small letters/ digits/ special characters)
2	Passwords should include at least 2 forms
3	Passwords should include at least 3 forms
4	Passwords should include at least 4 forms

Limit Login Attempts: the number of times you would like sub-admins to retry their passwords. If trying out more than this number, the sub-admins are not allowed to type in strings again.

Password Expiration: the number of days the password will expire in. A valid period can be defined for each password, counting from the first login. When a password expires, the operator will need to setup a new password for future use. Expired passwords cannot be reused.

Password Limits: to determine how many utilized passwords in the past should be checked. For instance, if the admin enters '5,' the system will check if the newly added password is identical to one of the five most-recent ones; if it is, the server would ask the admin to choose a new password string again.

Access Permission: to configure the accessibility and permission of the WMI and the managed AP grouping for each Administrator Group. There are 6 categories a sub-admin can fall into – Super Group, Manager, Operator, OnDemand Manager, Custom1, Custom2, and Custom3. Click configure at the right of the drop-down list to see and modify the differences. Be aware that the authority limits of "Super Group" are unchangeable.

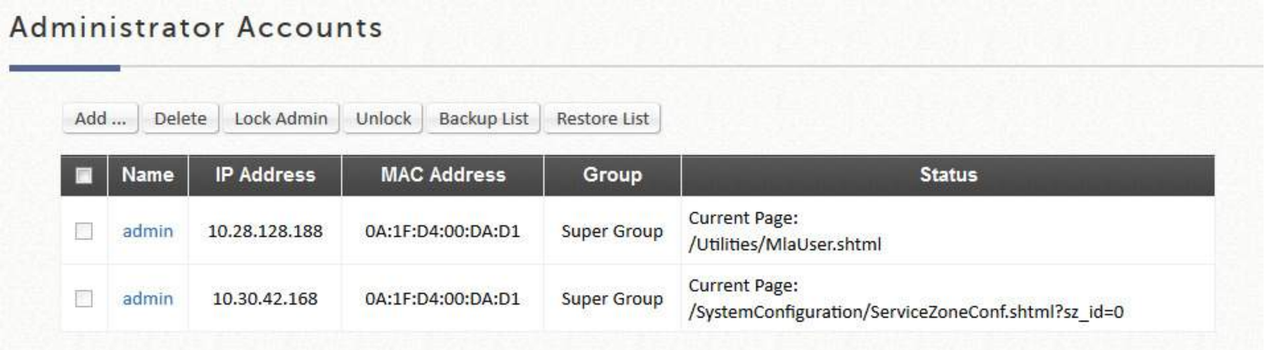
- Add: to generate a new Administrator Group if the customization is necessary
- Delete: to remove the existed Administrator Group
- Admin Group Name: to help simply identify which administrator group is belonged to
- Remark: a custom field for each administrator group
- AP Group: once the AP Group is generated by assigning the selected APs, the administrator group can manage them by clicking the checkbox of them (refer to "*session 8.2.2 AP Group*")
- On-Demand API: to enable administrator to create On-Demand Account through external interfaces
- Permission-Disabled: the specific page cannot be viewed by the sub-admin group
- Permission-Read Only: the specific page can only be viewed only, instead of modified the configuration in each item or table

- Permission-Read/Write: the specific page can be configured, edited, monitored, viewed or everything administrator desire to do.

Administrator Accounts

Admin has authority to change his/her own password or add more accounts to the admin list to take (some of) the management responsibility.

Administrator Accounts List: to serve as a list for admins to track the dynamics of each management accounts, including the number of the online admins and the state of each sub-admin. Besides, admin can also click the hyperlinks in the “Name” column to edit admins’/ sub-admins’ related settings.



Administrator Accounts

■	Name	IP Address	MAC Address	Group	Status
□	admin	10.28.128.188	0A:1F:D4:00:DA:D1	Super Group	Current Page: /Utilities/MlaUser.shtml
□	admin	10.30.42.168	0A:1F:D4:00:DA:D1	Super Group	Current Page: /SystemConfiguration/ServiceZoneConf.shtml?sz_id=0

Add: to create a sub-admin and define his/her authority limits. In case the administrator forgets his/her password, by entering both email and the Elementary School Name, the account credential will be email to the assigned email address. Note that an SMTP Server needs to be setup for the system to send email reminders.

Delete: to remove the existed accounts. Please note that only the created sub-admins can be deleted.

Lock: to check the boxes to lock to forbid certain sub-admins to access the management page.

Unlock: to check the boxes to unlock to forbid certain sub-admins to access the management page.

Backup List: To export user credentials as a text file in csv format in a new window.

Restore List: To import the accounts back into the Local user database which is a convenient way to create a great amount of Local accounts.

15.4 Backup/ Restore Configuration

Backup System

General Backup: to save the current system configurations to a backup file on a local disk of the management console. A backup file can be restored to the system by clicking *Browse* button to choose the backup file and then clicking *Restore* button to execute the process.

Period Backup: Backup can be done periodically over FTP. Enable this feature by clicking on the *Configure* button to setup the Primary and/or Secondary Folder and configure the FTP server from Main › Status › Reporting › FTP Settings. The backup file will be transmitted to FTP Server on the specific time of each day (Day), day of each week (Week), date of each month (Month) depending on the configuration.

Restore System

Restore System Settings: Click *Browse* to search for a .db database backup file created by the controller and click *Restore* to restore to the same settings at the time when the backup file was saved. There are some options to check to decide whether to keep the system current settings instead of overwrite by the .db file.

- Keep WAN1 setting. (default checked)
- Keep Management IP Address List. (default checked)
- Keep LAN, Alias, DHCP Setting, Management Service Zone List and Management IP Address List
- Keep Certificates
- Keep Local Area AP Management setting
- Keep Wide Area AP Management setting
- Keep Switch Management setting
- Keep Internal Authentication Server accounts.

Reset to Default

Reset to Factory Default: Click *Reset* to load the factory default settings of the controller. The process needs to restart the system. There are several options to define whether to retain the system current settings

- Keep WAN1 setting. (default checked)
- Keep Management IP Address List. (default checked)
- Keep LAN, Alias, DHCP setting, Management Service Zone List and Management Service Zone List
- Keep Certificate.
- Keep Local Area AP Management setting.
- Keep Wide Area AP Management setting.
- Keep Switch Management setting.
- Keep Account.
- Keep Logs, Reports and Traffic History.

15.5 Restart

This function allows the administrator to safely restart WLAN controller, and the process might take several minutes to complete. Click *Apply* to restart WLAN controller. If the power needs to be turned off, it is highly recommended to restart WLAN controller first and then turn off the power after completing the restart process. The administrator may enter Reason for Restart for maintenance purposes and saved in the Configuration Change Log.

Note: The connection of all online users of the system will be disconnected when system is in the process of restarting.

15.6 System Upgrades

The administrator can obtain the latest firmware from Edgecore’s Partner Center or Edgecore’s Support Team and upgrade the system. Click *Browse* to search for the firmware file on your local drive and click *Apply* to firmware upgrade. It might take a few minutes before the upgrade process completes and the system needs to be restarted afterwards to activate the new firmware.

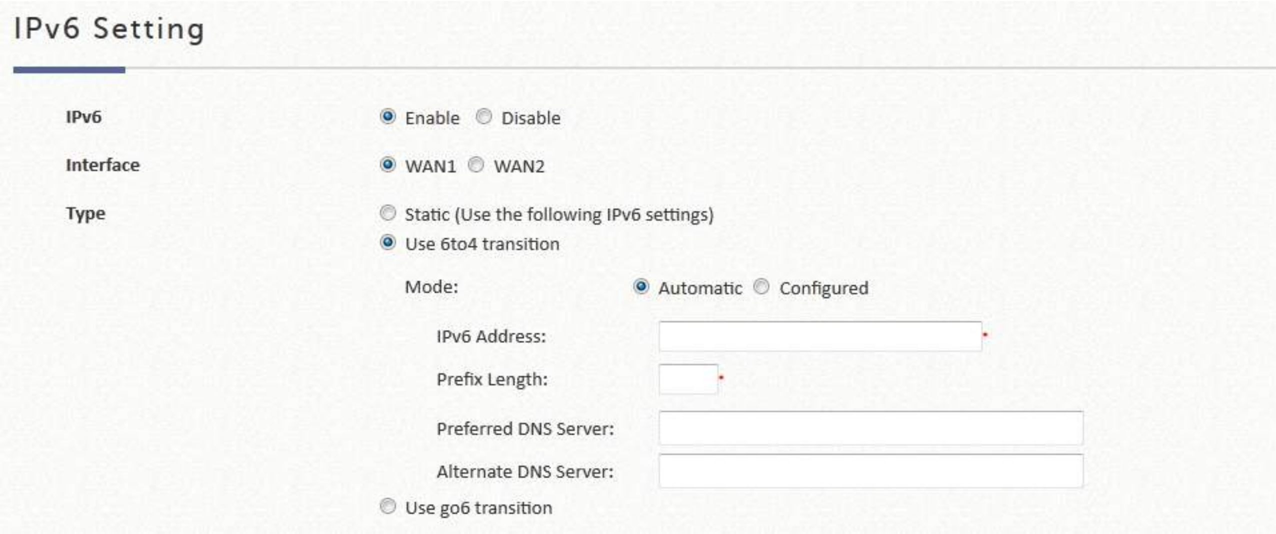
FTP firmware upgrade is also an option, enter the FTP server IP address, FTP server port, and the FTP account name and password, and lastly specify the complete firmware filename stored on the FTP server that will be used to upgrade the system.

Note:Before performing an upgrade, the system checks for version compatibility ensure system sanity. You may contact the Edgecore Support Team regarding version compatibility.
Note: The system must be rebooted before resetting to factory defaults after firmware upgrade.

16 Advanced Settings for Network Environment

16.1 IPv4/ IPv6 Dual Stack Network

WLAN controller supports operating in an IPv6 networking environment. When IPv6 configuration option is enabled, administrator may assign IPv4 IP address as well as IPv6 address to either WAN1 or WAN2 of the network interface. There are three ways to configure an IPv6 address for the chosen WAN interface, namely Static, 6to4, and go6. Please select the option applicable to your environment.



IPv6 Setting

IPv6 ● Enable ○ Disable

Interface ● WAN1 ○ WAN2

Type
○ Static (Use the following IPv6 settings)
● Use 6to4 transition
Mode: ● Automatic ○ Configured
IPv6 Address: *
Prefix Length: *
Preferred DNS Server:
Alternate DNS Server:
○ Use go6 transition

Status: to enable or disable IPv6 support on the selected WAN interface.
Interface: to select the external interface of the device that will be configured with an IPv6 address.
Type: to select one of the IPv6 methodologies

- Static: Manually enter all the related IPv6 information. Red asterisk are mandatory fields. Ideal if your internet package comes with static IPv6 addresses issues by your ISP.
- 6to4: 6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network (generally the IPv4 internet) without the need to configure explicit tunnels. 6to4 option can only be chosen when the selected WAN interface is set with a static IPv4 address.
- Go6: Go6 is based on the provision of dedicated servers, called Tunnel Brokers, to automatically manage tunnel requests from users. A set of Username and Password will be provided by the ISP for authentication. The Username, Password and Server Address are the only mandatory fields for go6 transition. The list of Tunnel Brokers is growing and administrators can choose to define a specific Tunnel Broker by enabling "Assign Broker Address" and entering the Broker Address.

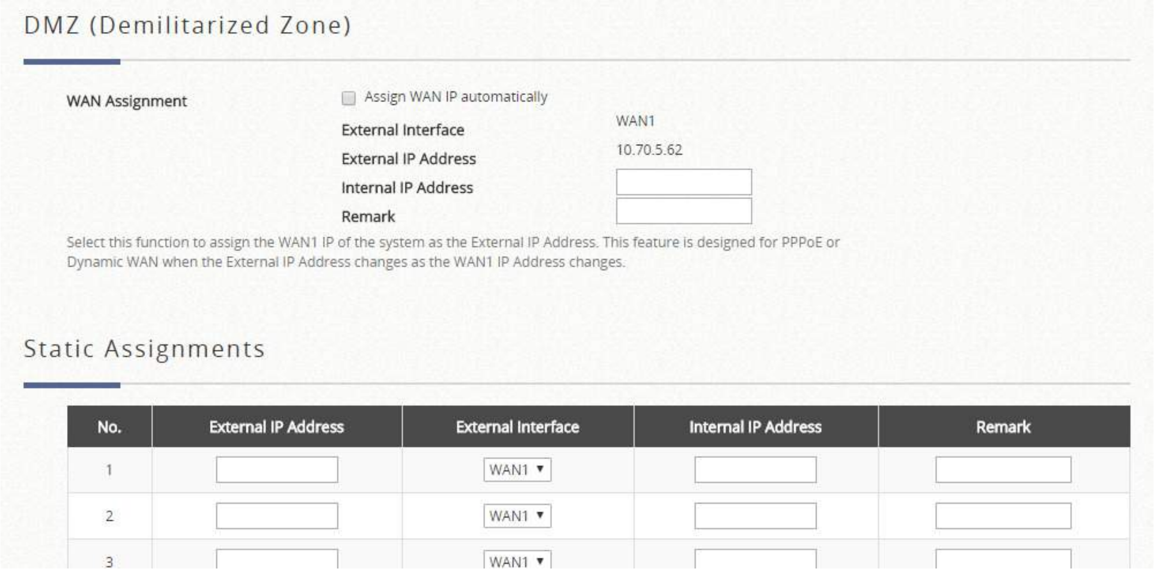
16.2 NAT

The NAT function supports 3 types of network address translation

- DMZ (Demilitarized Zone)
- Public Accessible Server
- IP/Port Forwarding

DMZ (Demilitarized Zone)

The system supports specific sets of Internal IP address (LAN) to External IP address (WAN) mapping in the Static Assignments. The External IP Address of the Automatic WAN IP Assignment is the IP address of External Interface (WAN1) that will change dynamically if WAN1 Interface is Dynamic. When Assign WAN IP Automatically is checked, the entered Internal IP Address under will be bound to the WAN1 interface. Each Static Assignment could be bound with the chosen External Interface, WAN1 or WAN2. There are specific sets of static Internal IP Address and External IP Address available. Internal and External IP Addresses are entered as a set. After the setup, accessing the WAN will be mapped to access the Internal IP Address. These settings will become effective immediately after clicking the *Apply* button.



DMZ (Demilitarized Zone)

WAN Assignment

□ Assign WAN IP automatically

External Interface WAN1

External IP Address 10.70.5.62

Internal IP Address

Remark

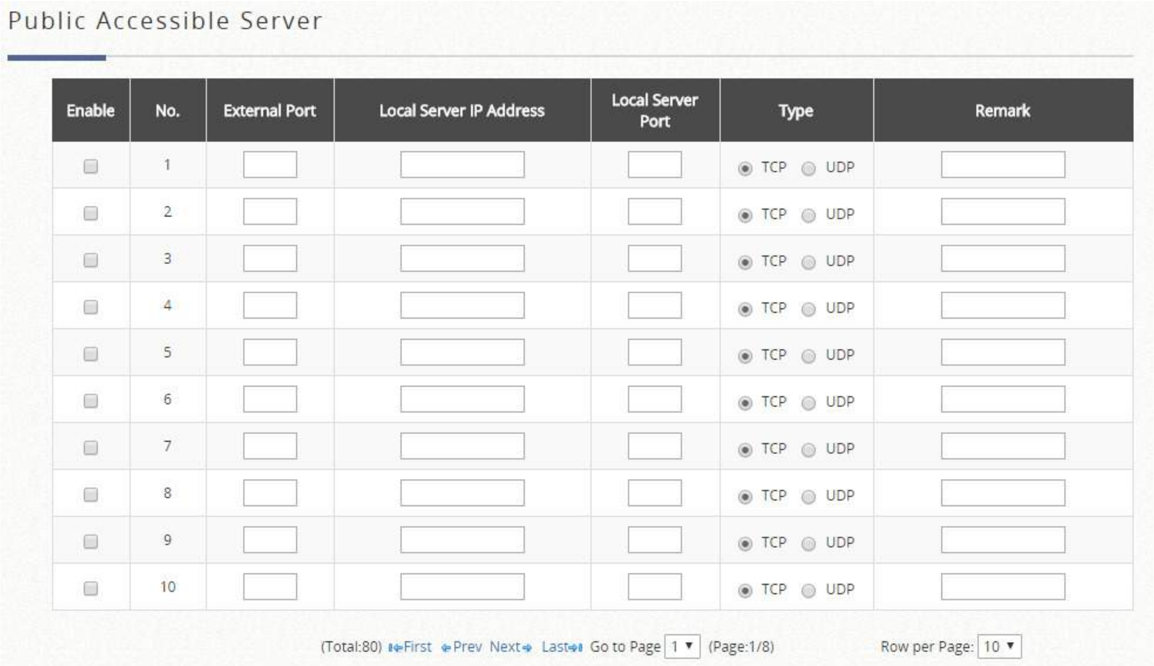
Select this function to assign the WAN1 IP of the system as the External IP Address. This feature is designed for PPPoE or Dynamic WAN when the External IP Address changes as the WAN1 IP Address changes.

Static Assignments

No.	External IP Address	External Interface	Internal IP Address	Remark
1		WAN1 ▾		
2		WAN1 ▾		
3		WAN1 ▾		

Public Accessible Servers

Public Accessible Servers allow the administrator to set virtual servers, so that client devices outside the managed network can access these servers within the managed network. Different virtual servers can be configured for different sets of physical services, such as TCP and UDP services in general. Enter the "External Service Port", "Local Server IP Address" and "Local Server Port". Select "TCP" or "UDP" for the service's type. In the Enable column, check the desired server to enable. These settings will become effective immediately after clicking the *Apply* button.



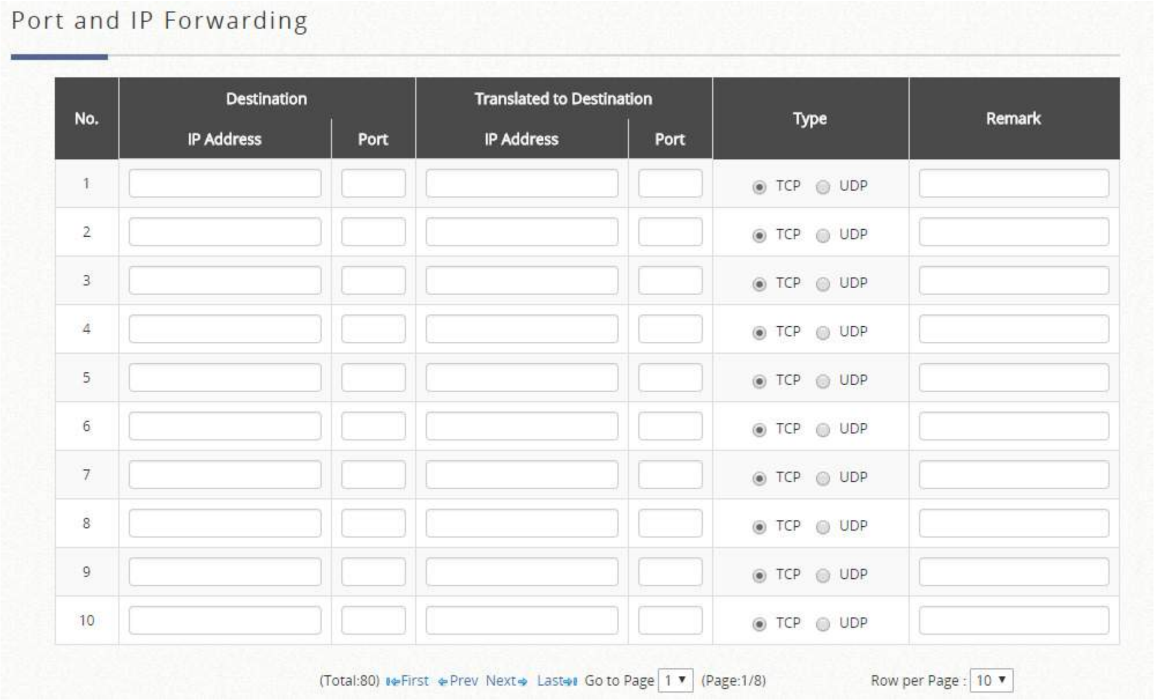
Public Accessible Server

Enable	No.	External Port	Local Server IP Address	Local Server Port	Type	Remark
□	1				● TCP ○ UDP	
□	2				● TCP ○ UDP	
□	3				● TCP ○ UDP	
□	4				● TCP ○ UDP	
□	5				● TCP ○ UDP	
□	6				● TCP ○ UDP	
□	7				● TCP ○ UDP	
□	8				● TCP ○ UDP	
□	9				● TCP ○ UDP	
□	10				● TCP ○ UDP	

(Total:80) First Prev Next Last Go to Page 1 ▾ (Page:1/8) Row per Page: 10 ▾

Port & IP Forwarding

This function allows the administrator to set specific sets of the IP addresses at most for redirection purpose. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the "IP Address" and "Port" of Destination, and the "IP Address" and "Port" of Translated to Destination. Select "TCP" or "UDP" for the service's type. These settings will become effective immediately after clicking *Apply*.



Port and IP Forwarding

No.	Destination		Translated to Destination		Type	Remark
	IP Address	Port	IP Address	Port		
1					● TCP ○ UDP	
2					● TCP ○ UDP	
3					● TCP ○ UDP	
4					● TCP ○ UDP	
5					● TCP ○ UDP	
6					● TCP ○ UDP	
7					● TCP ○ UDP	
8					● TCP ○ UDP	
9					● TCP ○ UDP	
10					● TCP ○ UDP	

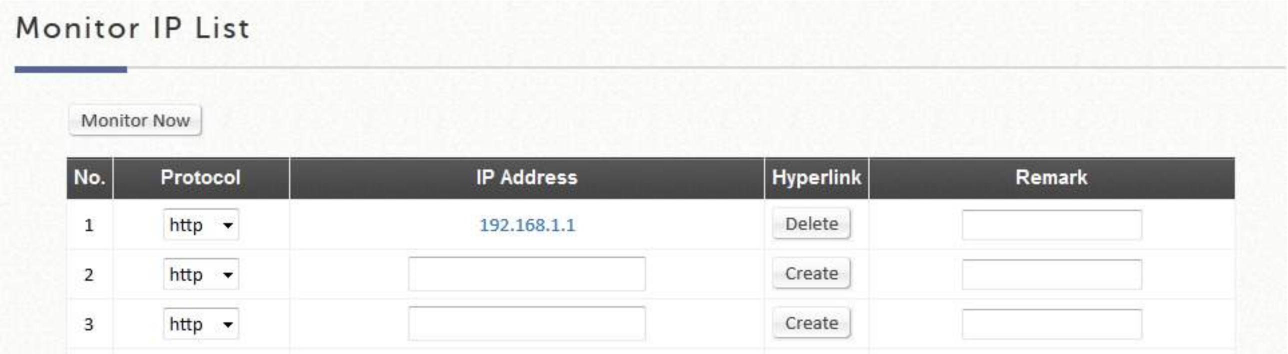
(Total:80) First Prev Next Last Go to Page 1 ▾ (Page:1/8) Row per Page : 10 ▾

This function allows the administrator to set specific sets of the IP addresses at most for redirection purpose. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the "IP Address" and "Port" of Destination, and the "IP Address" and "Port" of Translated to Destination. Select "TCP" or

"UDP" for the service's type. These settings will become effective immediately after clicking *Apply*.

16.3 Monitor IP List

Multiple IP addresses can be defined in the Monitor IP function. System can monitor these IP based network devices and periodically report online status via email based on a configurable interval. These monitored devices can be accessed via HTTP or HTTPS connection. The management interface of the monitored device can be accessed via a hyperlink of device's IP address when the system is operated under NAT mode.



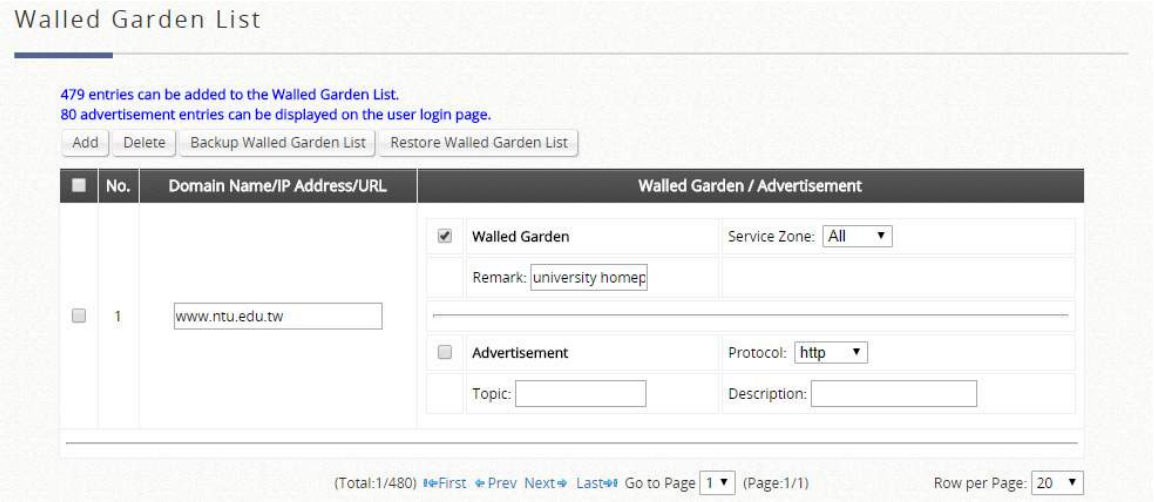
Monitor IP List

Monitor Now

No.	Protocol	IP Address	Hyperlink	Remark
1	http ▾	192.168.1.1	Delete	
2	http ▾		Create	
3	http ▾		Create	

16.4 Walled Garden and Advertisement

This function provides certain free services for users to access the websites listed here before login and authentication. Specific addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Enter the website IP Address or Domain Name in the list and click *Apply* to save the settings. The Walled Garden List can be backed up or restored.



Walled Garden List

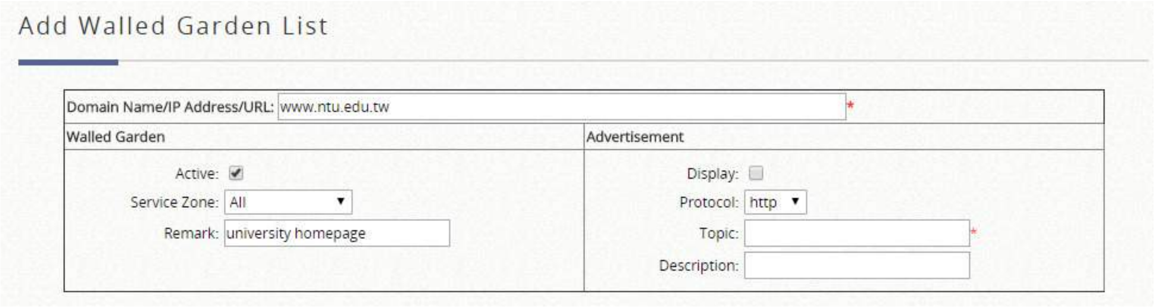
479 entries can be added to the Walled Garden List.
80 advertisement entries can be displayed on the user login page.

Add | Delete | Backup Walled Garden List | Restore Walled Garden List

□	No.	Domain Name/IP Address/URL	Walled Garden / Advertisement
□	1	www.ntu.edu.tw	☑ Walled Garden — Service Zone: All ▾ Remark: university homep □ Advertisement — Protocol: http ▾ Topic: — Description:

(Total:1/480) First Prev Next Last Go to Page 1 ▾ (Page:1/1) Row per Page: 20 ▾

Walled Garden Advertisements are advertisement links for clients to access before they are authenticated by the system. For example, guests without the network access right in hotels can still visit these sites free of charge.


Add Walled Garden List

Domain Name/IP Address/URL: www.ntu.edu.tw *	
Walled Garden	Advertisement
Active: ☑	Display: □
Service Zone: All	Protocol: http
Remark: university homepage	Topic: *
	Description:

Add: to create a new walled garden entry.

- Domain Name/IP Address/URL: which pages should be added into walled garden list. However, the entries selected as Walled Garden Ad must be a URL, not an IP address with prefix.
- Active: to activate the specific walled garden entry
- Service Zone: to allow the clients in which service zone are able to access the walled garden
- Remark: a custom field for identity of each walled garden entry

- Display: to display advertisement hyperlinks on the login pages, corresponding to Service Zone configuration. If the Display checkbox is checked, please make sure the walled garden Active checkbox has been checked as well.
- Protocol: the format of HTTP or HTTPs of the advertisement hyperlink in the login page clients are accessing
- Topic: the wording of the advertisement hyperlink in the login page clients are accessing
- Description: a custom field for identity of each walled garden advertisement

Delete: to remove the existed walled garden entry

Backup Walled Garden List: to save the current walled garden entries from the system

Restore Walled Garden List: to load a list of the walled garden entries with a .tar file

16.5 VPN

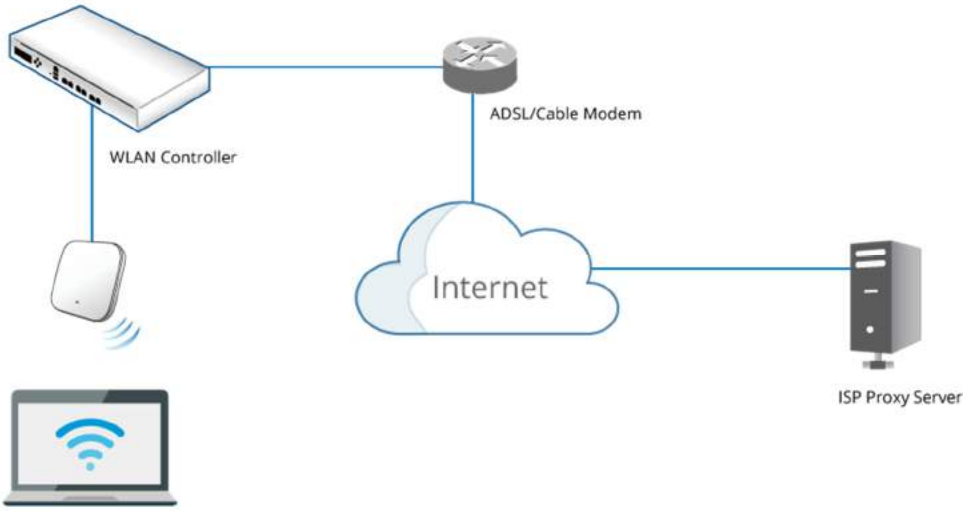
Multiple VPN protocols are available in WLAN controller, including Remote VPN and Site-to-Site VPN. Please refer to "*chapter 11 How to enable VPN feature*" for more details.

16.6 Proxy Server

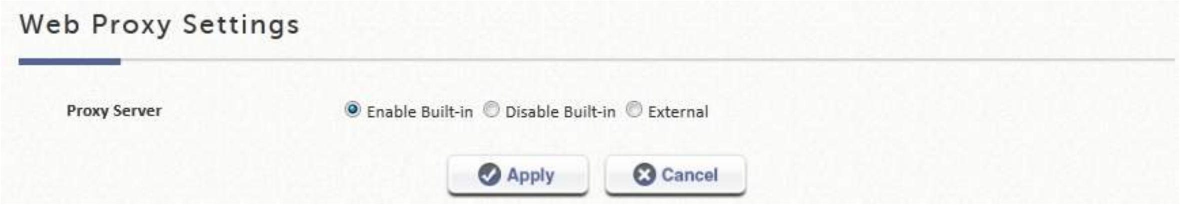
After successful authentication, the clients will be redirected back to the desired proxy servers. Basically, a proxy server can help clients access the network resources more quickly. This section presents basic examples for configuring the proxy server settings of the WLAN controller. The system provides

- (Using Internet Proxy Server) Built-in Proxy Server
- (Using External Proxy Server) External Proxy Server

Using Internet Proxy Server



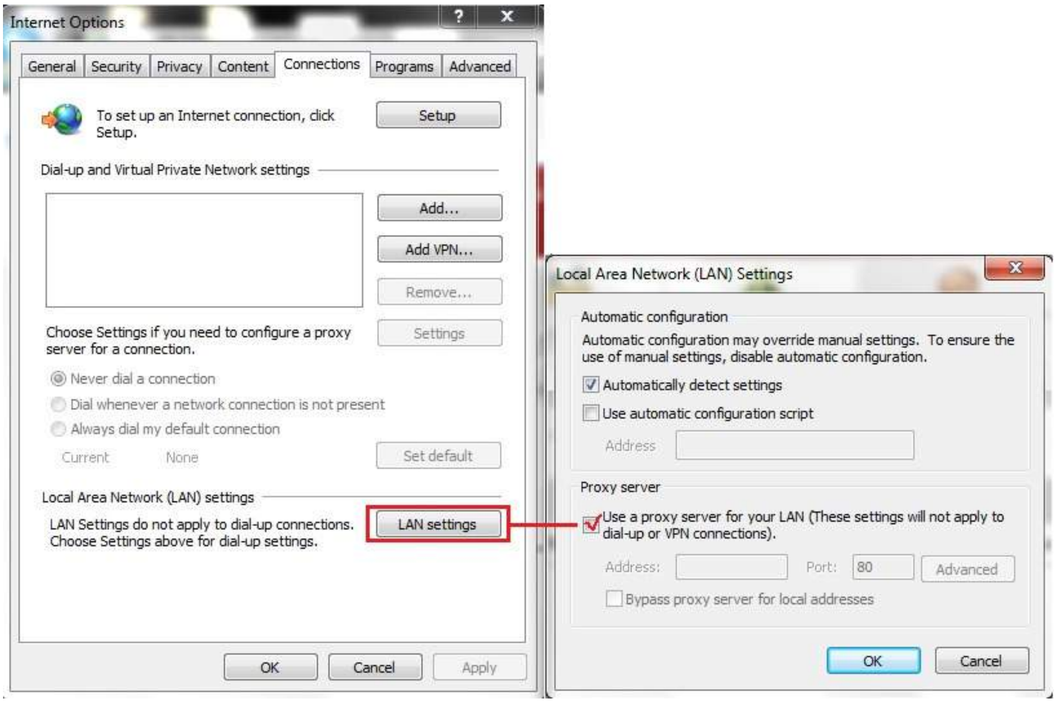
Enable Built-in: A built-in proxy server in the WLAN controller can be enabled, even with a Proxy Server placed outside the LAN environment or in the Internet. For example, the above diagram illustrates how a proxy server of an ISP is used.



Web Proxy Settings

Proxy Server ● Enable Built-in ○ Disable Built-in ○ External

Step 6. Select Enable Built-in and click *Apply* to save the settings
Step 7. Enable Proxy Server Settings in Internet Options on Client Stations.
Step 8. By enabling the built-in Proxy Server, all traffic is forwarded to the local Proxy Server on the controller.



Internet Options

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings
□ Use automatic configuration script

Address

Proxy server

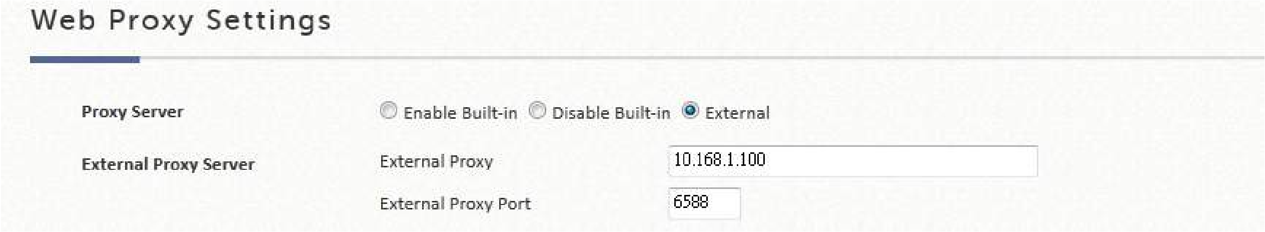
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

Using an External Proxy Server

External: to specify an External Proxy Server and fill in the appropriate IP address of the Proxy Server and the utilized port. Please refer the following steps to complete the proxy configuration:



Web Proxy Settings

Proxy Server: ○ Enable Built-in ○ Disable Built-in ● External

External Proxy Server

External Proxy: 10.168.1.100

External Proxy Port: 6588

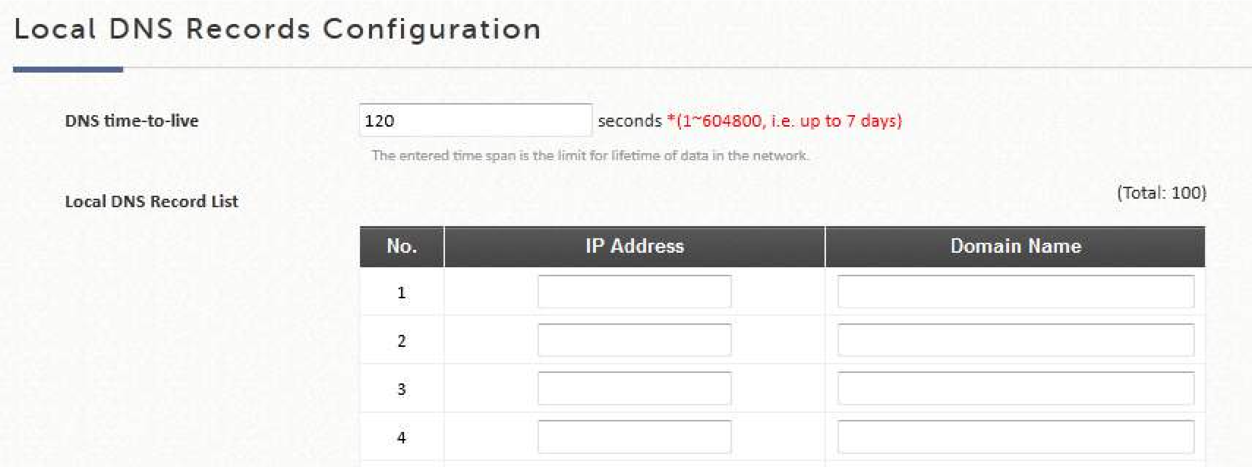
Step 9. Add the External Proxy IP address and External Port Number into External Proxy Servers setting. Click *Apply* to save the settings

Step 10. Enable Proxy Server Settings in Internet Options on Client Stations.

Note: By Enabling the Proxy Server, clients are required to manually check Proxy Server Settings on client stations' Internet Options. To apply Transparent Proxy, please use Port and IP forwarding.

16.7 Local DNS Records

The administrator could statically assign a Domain Name to IP mappings for all clients connected to the WLAN controller's LAN network. This feature can be used to dispatch clients to preferred IP address for certain Domain Names.



Local DNS Records Configuration

DNS time-to-live: 120 seconds *(1~604800, i.e. up to 7 days)

The entered time span is the limit for lifetime of data in the network.

Local DNS Record List (Total: 100)

No.	IP Address	Domain Name
1		
2		
3		
4		

16.8 Dynamic Routing

The function supports three dynamic routing protocols:

- IS-IS
- OSPF/OSPF v3
- RIP

ISIS Configuration

It is a routing protocol designed to move information efficiently within a computer network, a group of physically connected computers or similar devices. You can configure each interface Circuit Type to Level 1 or Level 2.

Net ID: It is the ISO address Network Entity Title (NET). The NET is used just like an IP address to uniquely identify a router on the inter-network.

Route Level: Level 1 systems route within an area; when the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other routing domains. The level type of each network interface can be assigned.

OSPF Configuration

It is an adaptive routing protocol for Internet Protocol (IP) networks. You can configure each interface Area, Stub and authentication.

Area: An Area is a set of networks and hosts within a routing domain that have been administratively grouped together. Area 0, known as the *backbone area*, resides at the top level of the hierarchy and provides connectivity to the non-backbone areas (numbered 1, 2).

Stub: Are areas through which or into which AS external advertisements are not flooded.

Authentication: Allows the authenticating of OSPF neighbors. The authentication method "none" means that no authentication is used for OSPF and it is the default method. With MD5 authentication, enter the MD5 password, the password does not pass over the network.

Advertise as Default Gateway: Inform neighboring nodes that this controller is the default gateway.

Advertise Global Policy Route: Inform neighboring nodes the Global Policy route on this controller.

Re-distribute RIP: Check this option to enable using OSPF to distribute routing information acquired via RIP.

OSPF v3 Configuration

IPv6 dynamic routing configuration

RIP Configuration

It is a dynamic routing protocol used in local and wide area networks. You can configure each interface to be a Passive or supportive version, and authentication.

Passive: RIP packets will not be sent from network interfaces if they are checked as Passive.

Version: Select the RIP version for this interface, RIPv1 uses broadcast to deliver RIP packets, RIPv2 uses Multicast to deliver RIP packets, both uses broadcast and multicast.

Authentication: Allows the authenticating of RIP neighbors. The authentication method "none" means that no authentication is used for RIP and it is the default method. The two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication.

Advertise as Default Gateway: Inform neighboring nodes that this controller is the default gateway.

Advertise Global Policy Route: Inform neighboring nodes the Global Policy route on this controller.

Re-distribute OSPF: Check this option to enable using RIP to distribute routing information acquired via OSPF.

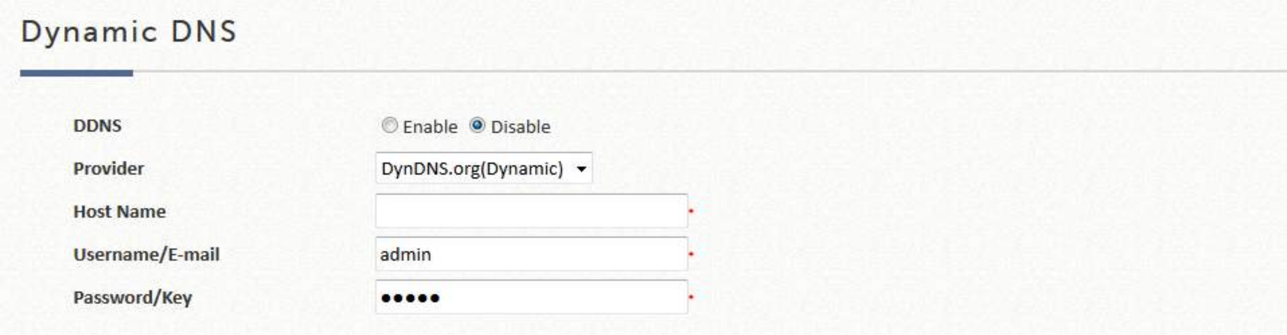
RIP Timer – Update timer: Specify the time in seconds when the system will request for immediate update in routing information.

RIP Timer – Timeout Timer: Routes are only kept in the routing table for a limited amount of time. A

special *Timeout* timer is started whenever a route is installed in the routing table. Whenever the router receives another *RIP Response* with information about that route, the route is considered "refreshed" and its *Timeout* timer is reset. When this timer expires, the route is marked as invalid.
RIP Timer – Garbage Collect Timer: Specify the time in seconds before erasing invalid route from the routing table.

16.9 DDNS

Before activating this function, you must have your Dynamic DNS hostname registered with a Dynamic DNS provider. WLAN controller supports DNS function to create aliases from the dynamic IP address for the WAN port to a static domain name, allowing the administrator to easily access WLAN controller's WAN. If the dynamic DHCP is activated at the WAN port, it will update the IP address of the DNS server periodically. These settings will become effective immediately after clicking ***Apply***.



Dynamic DNS

DDNS	○ Enable ● Disable
Provider	DynDNS.org(Dynamic)
Host Name	
Username/E-mail	admin
Password/Key	•••••

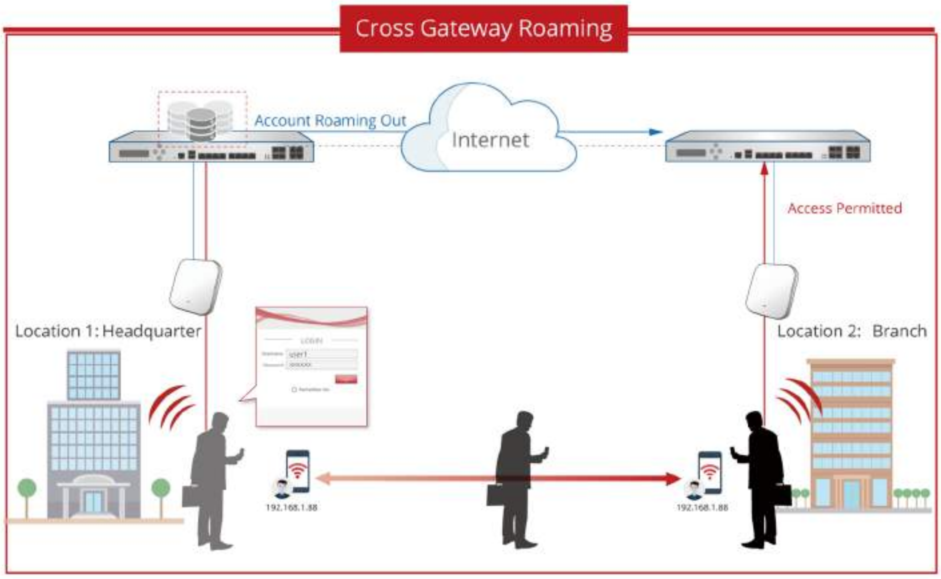
DDNS: to enable or disable this function
Provider: to select the DNS provider
Host name: The IP address/domain name of the WAN port
Username/E-mail: The register ID (username or e-mail) for the DNS provider
Password/Key: The register password for the DNS provider

16.10 Client Mobility

IP PNP: Enable this feature so devices with static/ DHCP IP, DNS, and Gateways can obtain internet access from the controller.

Cross Gateway Roaming
Cross Gateway roaming feature enables an end user to seamlessly move around large network deployment where there are multiple WLAN controllers in service. Normally when a user moves from edge AP to another edge AP that is managed by another WLAN controller, the user would experience network disconnection and would require re-login procedure in order to continue surfing the net.

With Cross Gateway roaming enabled, the end user would experience without network interruption. The traffic would be tunneled back to the original Controller for forwarding into the internet.



Cross Gateway roaming architecture design adopted is a star topology design where one Master Node may have up to 15 Slave Node peers. The term Master Node simply means that this node takes its place in the center of the star topology.

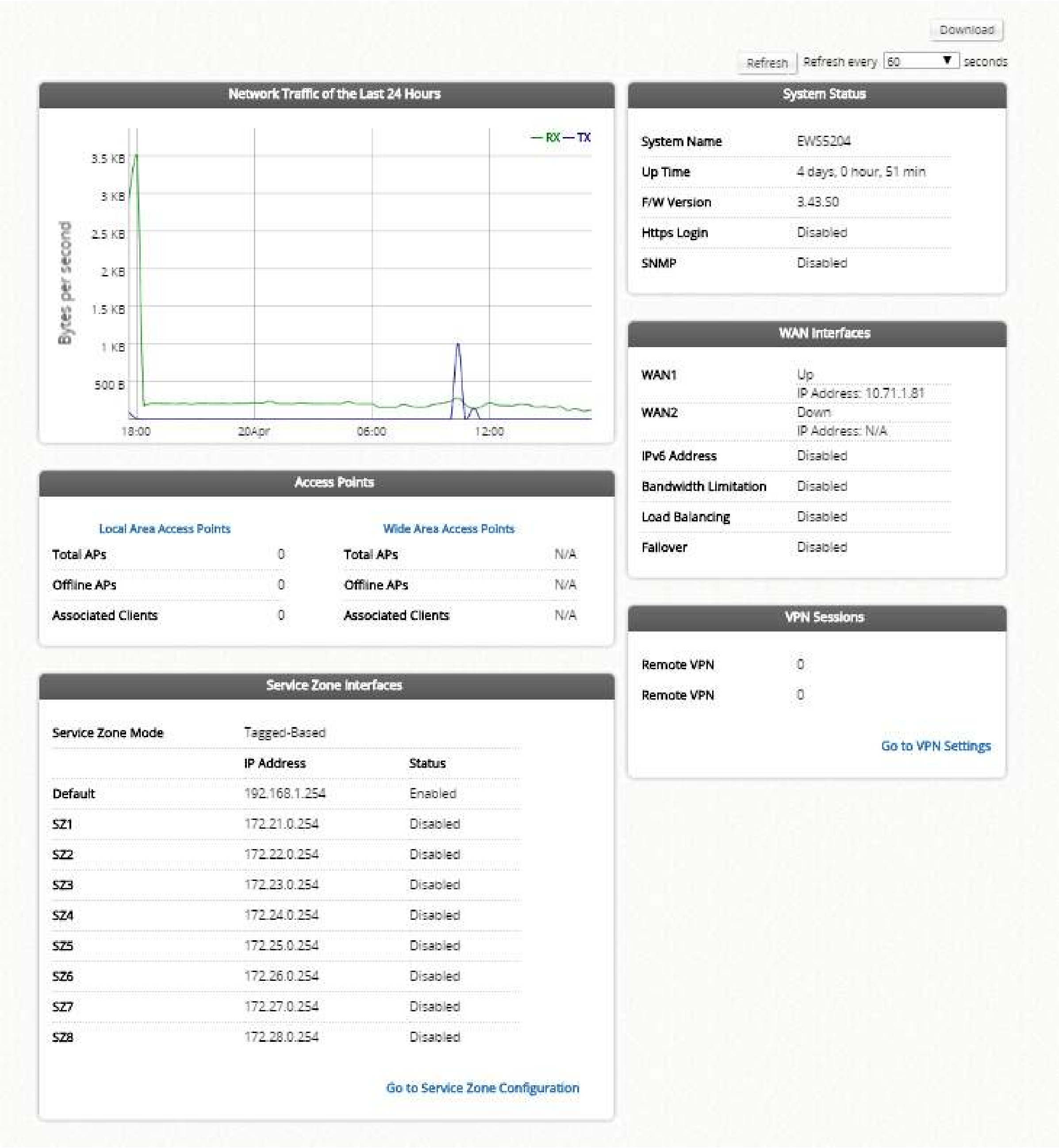
The role determination is completely dependent on the administrator settings. To establish roaming partnership, configure a WLAN controller to be Master Node, and another WLAN controller to be Slave Node. Make sure that the Secret Key and both WLAN controllers' WAN interface are routable.

Master mode: to input the Slave Nodes Settings (up to 15 slaves), Remote IP Address, Secret Key and Remark.
Slave mode: to input Master Node Setting, including Remote IP Address, Secret Key and Remark.

17 Status for Logs and Reports

17.1 Dashboard

This page displays important system related information that the administrator might need to be aware of at a glance, which includes General System settings, Network Interface and Online Users etc. The download button on the top-right corner is a tool that captures system settings. This is used for maintenance or troubleshooting purposes.



System Status

System Name	EWS5204
Up Time	4 days, 0 hour, 51 min
F/W Version	3.43.50
Https Login	Disabled
SNMP	Disabled

WAN Interfaces

WAN1	Up IP Address: 10.71.1.81
WAN2	Down IP Address: N/A
IPv6 Address	Disabled
Bandwidth Limitation	Disabled
Load Balancing	Disabled
Failover	Disabled

Access Points

Local Area Access Points		Wide Area Access Points	
Total APs	0	Total APs	N/A
Offline APs	0	Offline APs	N/A
Associated Clients	0	Associated Clients	N/A

VPN Sessions

Remote VPN	0
Remote VPN	0

Go to VPN Settings

Service Zone Interfaces

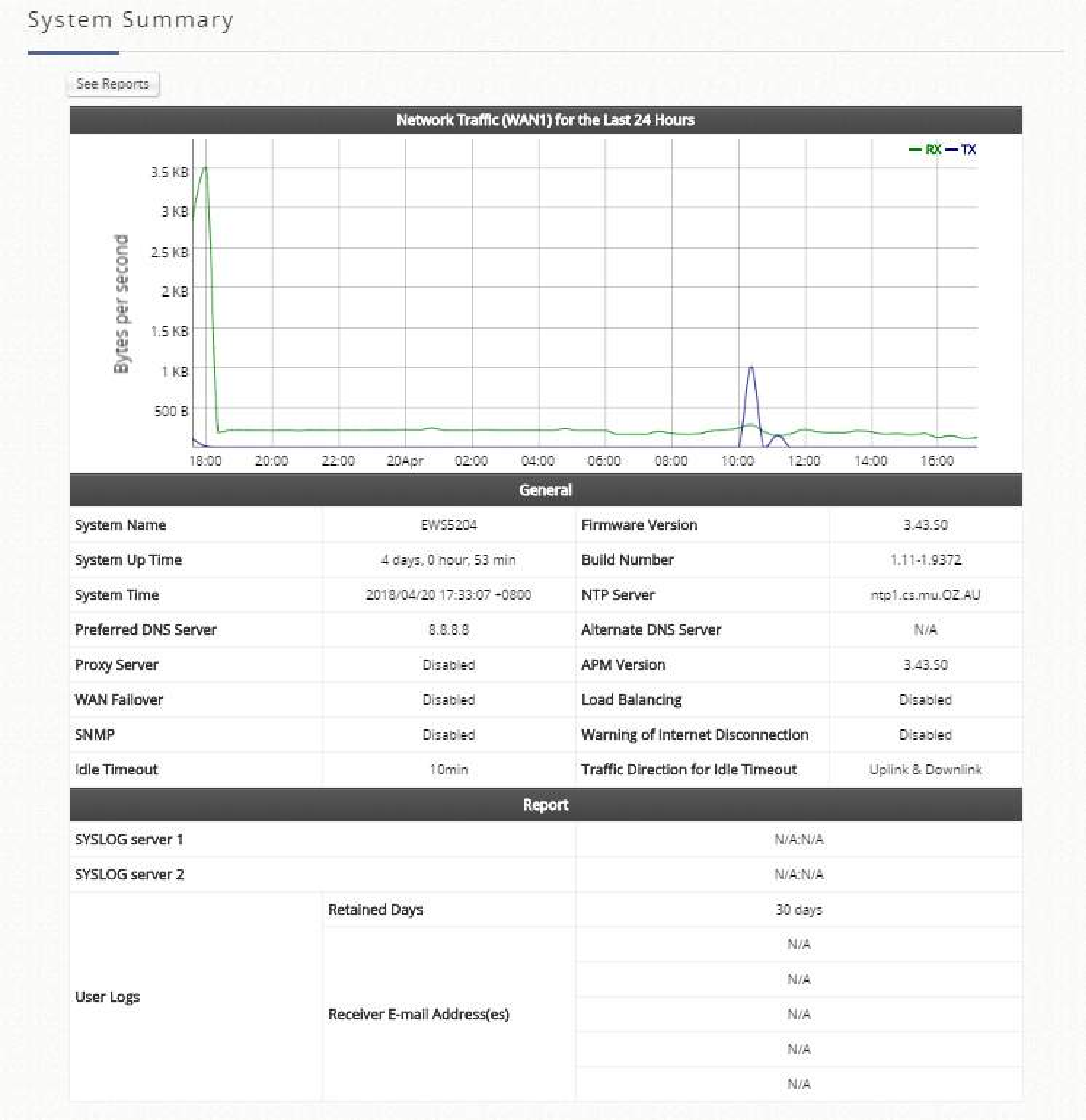
Service Zone Mode	Tagged-Based	
	IP Address	Status
Default	192.168.1.254	Enabled
SZ1	172.21.0.254	Disabled
SZ2	172.22.0.254	Disabled
SZ3	172.23.0.254	Disabled
SZ4	172.24.0.254	Disabled
SZ5	172.25.0.254	Disabled
SZ6	172.26.0.254	Disabled
SZ7	172.27.0.254	Disabled
SZ8	172.28.0.254	Disabled

Go to Service Zone Configuration

17.2 System Related Status

17.2.1 System Summary

The system summary displays a table of contents including firmware version, report servers configured, WAN optional settings, User log profile, system time and session control settings. For detailed status, please proceed to corresponding configuration pages.



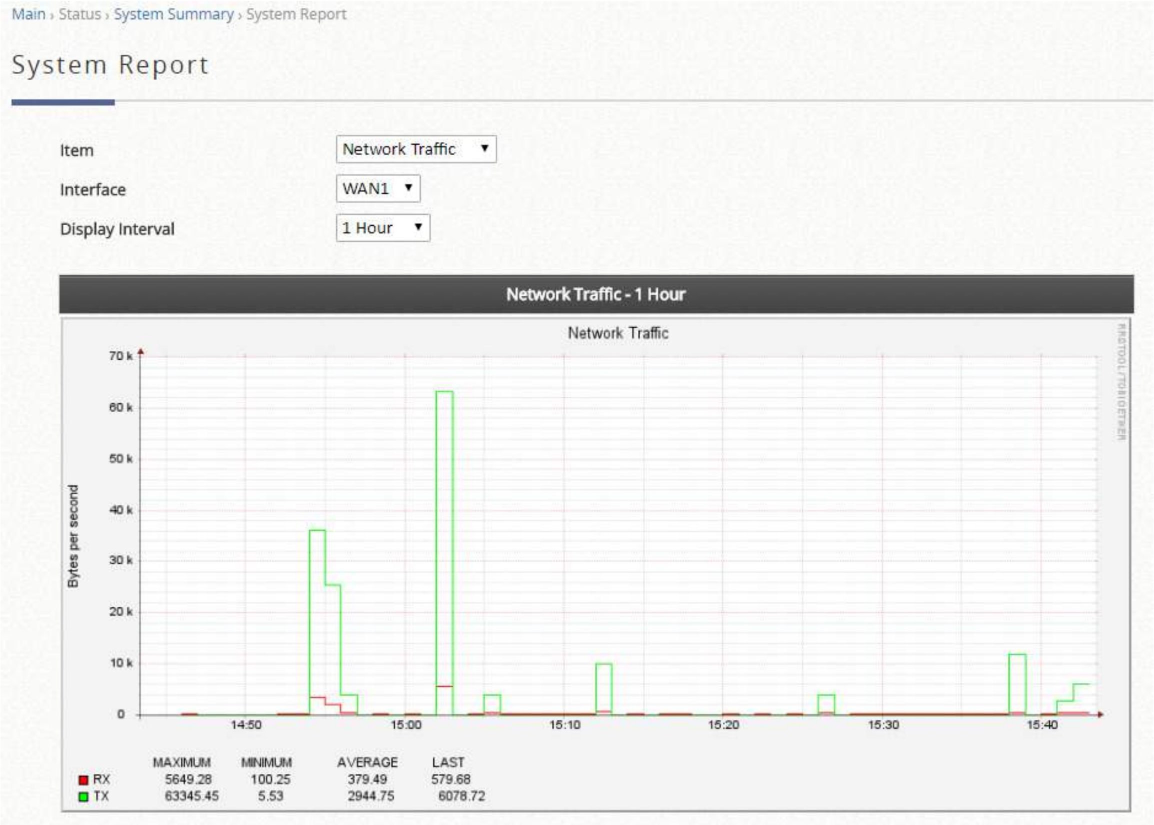
General

System Name	EWS5204	Firmware Version	3.43.50
System Up Time	4 days, 0 hour, 53 min	Build Number	1.11-1.9372
System Time	2018/04/20 17:33:07 +0800	NTP Server	ntp1.cs.mu.OZ.AU
Preferred DNS Server	8.8.8.8	Alternate DNS Server	N/A
Proxy Server	Disabled	APM Version	3.43.50
WAN Failover	Disabled	Load Balancing	Disabled
SNMP	Disabled	Warning of Internet Disconnection	Disabled
Idle Timeout	10min	Traffic Direction for Idle Timeout	Uplink & Downlink

Report

SYSLOG server 1		N/A:N/A
SYSLOG server 2		N/A:N/A
User Logs	Retained Days	30 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
		N/A
		N/A

A selection of reports is available when the “See Reports” button is clicked. These reports can be sorted based on interface and intervals.



Main › Status › System Summary › System Report

System Report

Item	Network Traffic
Interface	WAN1
Display Interval	1 Hour

Network Traffic - 1 Hour

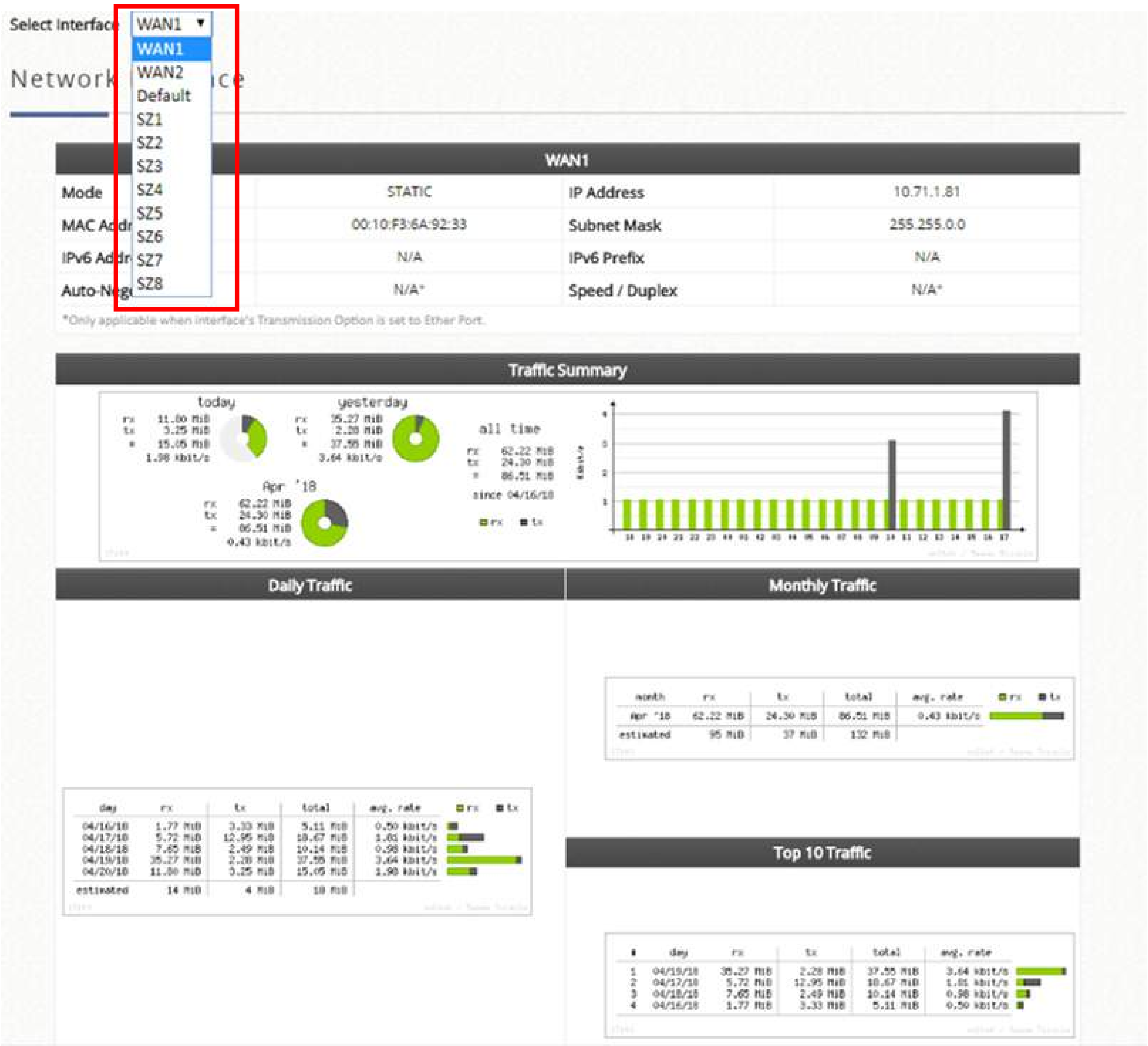
	MAXIMUM	MINIMUM	AVERAGE	LAST
🟥 RX	5649.28	100.25	379.49	579.68
🟩 TX	63345.45	5.53	2944.75	6078.72

17.2.2 Network Interface

This section provides the details of each of the network interfaces for the administrator to inspect, including WAN1, WAN2, SZ Default, SZ1 ~ SZ8.

Select the network interface that you are interested to see. If the selected interface is enabled, the corresponding network settings will be displayed. Scrolling down the page, the traffic statistics for different scales, including traffic summary, traffic of the day, traffic of the month, and traffic of the top 10 days is presented in a graphical manner.

Note: If statistics are required to be saved for long term keeping, See Report & Notification section for instructions to send and save network traffic on external servers.



WAN1			
Mode	STATIC	IP Address	10.71.1.81
MAC Addr	00:10:F3:6A:92:33	Subnet Mask	255.255.0.0
IPv6 Addr	N/A	IPv6 Prefix	N/A
Auto-Neg	N/A*	Speed / Duplex	N/A*

*Only applicable when interface's Transmission Option is set to Ether Port.

Traffic Summary

today	
rx	11.80 MiB
tx	3.25 MiB
=	15.05 MiB
	1.98 kbit/s

yesterday	
rx	35.27 MiB
tx	2.28 MiB
=	37.55 MiB
	3.64 kbit/s

Apr '18	
rx	62.22 MiB
tx	24.30 MiB
=	86.51 MiB
	0.43 kbit/s

all time	
rx	62.22 MiB
tx	24.30 MiB
=	86.51 MiB
since 04/16/18	

Daily Traffic

day	rx	tx	total	avg. rate
04/16/18	1.77 MiB	3.33 MiB	5.11 MiB	0.50 kbit/s
04/17/18	5.72 MiB	12.95 MiB	18.67 MiB	1.01 kbit/s
04/18/18	7.65 MiB	2.49 MiB	10.14 MiB	0.98 kbit/s
04/19/18	35.27 MiB	2.28 MiB	37.55 MiB	3.64 kbit/s
04/20/18	11.80 MiB	3.25 MiB	15.05 MiB	1.98 kbit/s
estimated	14 MiB	4 MiB	18 MiB	

Monthly Traffic

month	rx	tx	total	avg. rate
Apr '18	62.22 MiB	24.30 MiB	86.51 MiB	0.43 kbit/s
estimated	95 MiB	37 MiB	132 MiB	

Top 10 Traffic

#	day	rx	tx	total	avg. rate
1	04/19/18	35.27 MiB	2.28 MiB	37.55 MiB	3.64 kbit/s
2	04/17/18	5.72 MiB	12.95 MiB	18.67 MiB	1.01 kbit/s
3	04/18/18	7.65 MiB	2.49 MiB	10.14 MiB	0.98 kbit/s
4	04/16/18	1.77 MiB	3.33 MiB	5.11 MiB	0.50 kbit/s

17.2.3 Process Monitor

It is an engineer quick overview of the active status for each network utility process daemon on the gateway. Administrators can choose to Enable or Disable the Process Monitor. If enable, the green light of the status indicates the process daemon works normally.

17.2.4 Routing

This status page displays all the User Policy Route rules, and Global Policy Route rules will be listed here. It provides a fast reference window for the administrator to see the routing rules enforcements for users belonging to different Policies. It also shows the System Route rules specified for each network interface.

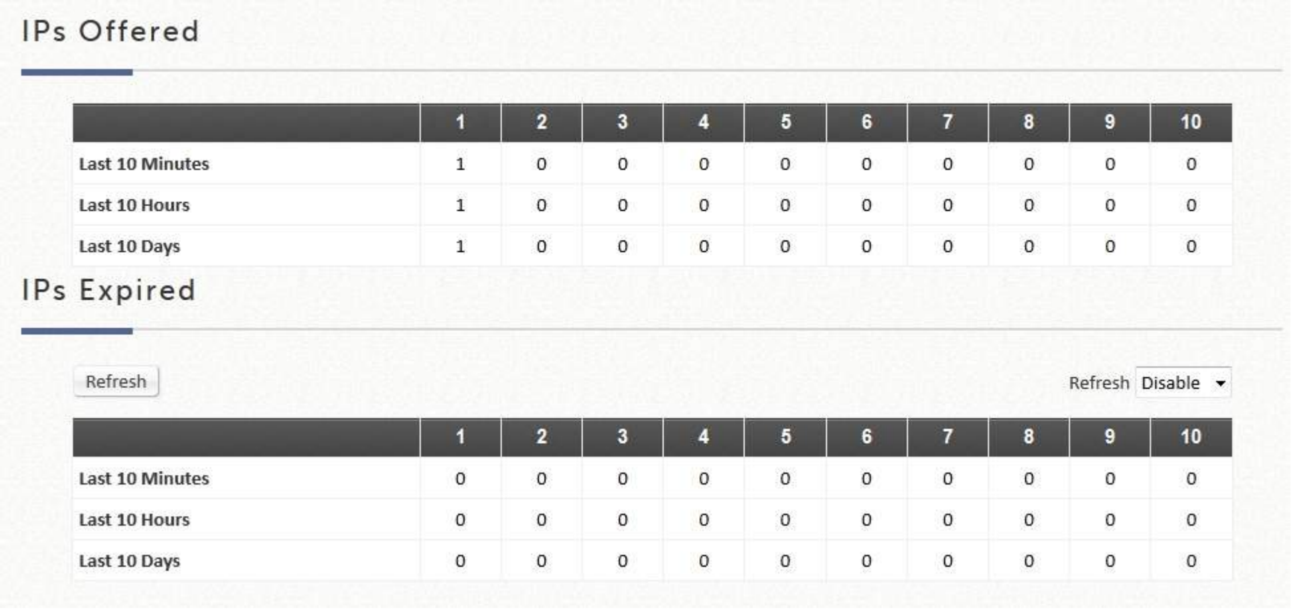
IPv6 are available for Global policy, and the rules configured there will also be shown in the IPv6 routing table page along with System interface settings for IPv6 traffic.

17.2.5 DHCP Server

The DHCP IP lease statistics can be viewed after clicking on *Show* Statistics List on this page.

Statistics of offered list: Valid lease counts of the Last 10 Minutes, Hours and Days are shown here. The header 1 ~ 10 are unit multipliers; for instance the number under column 2 indicates the lease count in the last 20 minutes/hours/days, the number under column 3 indicated the lease count in the last 30 minutes/hours/days and so on.

Statistics of expired list: IP leased to clients that have expired in the Last 10 Minutes, Hours and Days are shown here. The header 1 ~ 10 are unit multipliers; for instance the number under column 2 indicates the expired count in the last 20 minutes/hours/days, the number under column 3 indicated the expired count in the last 30 minutes/hours/days and so on.



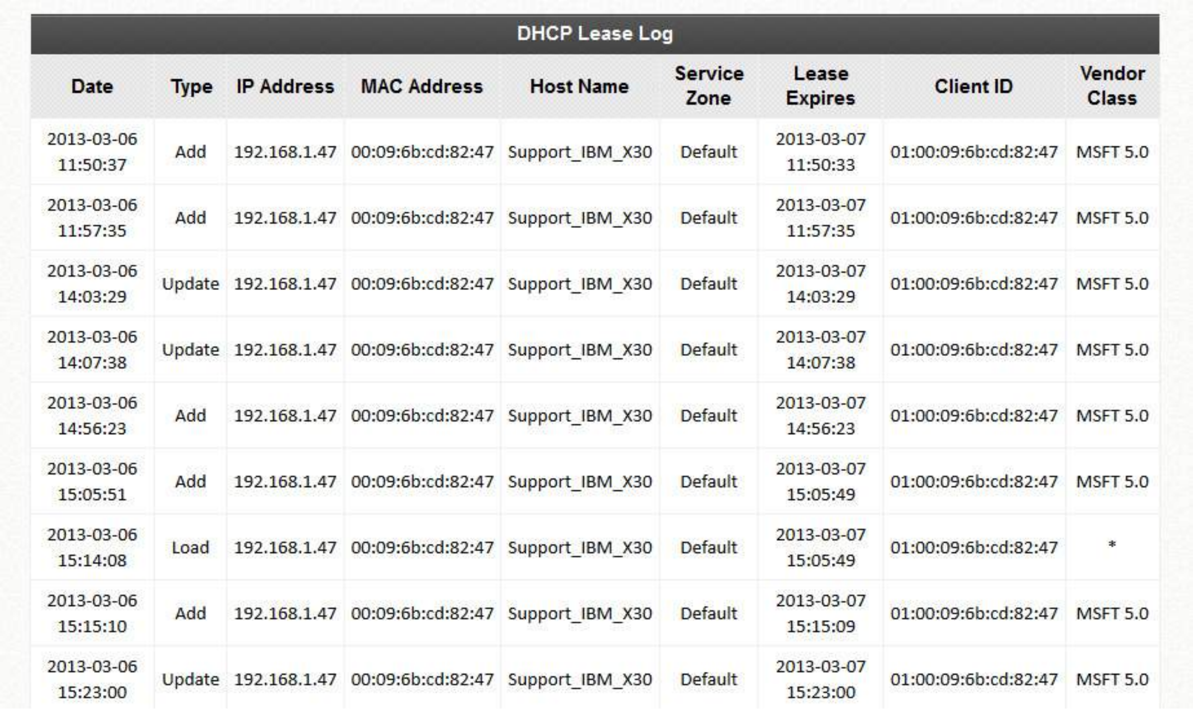
IPs Offered

	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	1	0	0	0	0	0	0	0	0	0
Last 10 Hours	1	0	0	0	0	0	0	0	0	0
Last 10 Days	1	0	0	0	0	0	0	0	0	0

IPs Expired

	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	0	0	0	0	0	0	0	0	0	0
Last 10 Hours	0	0	0	0	0	0	0	0	0	0
Last 10 Days	0	0	0	0	0	0	0	0	0	0

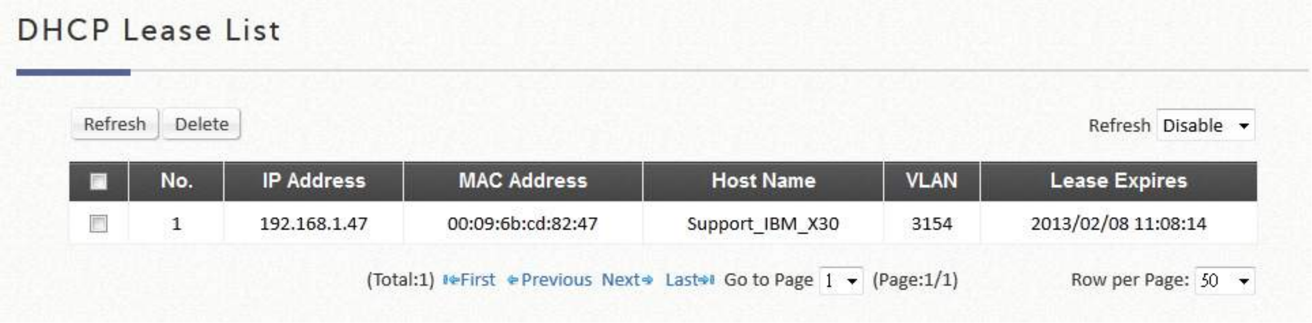
DHCP Lease Log: The DHCP Lease Log is displayed here and a search can be performed by IP Address, MAC Address or Service Zone.



DHCP Lease Log

Date	Type	IP Address	MAC Address	Host Name	Service Zone	Lease Expires	Client ID	Vendor Class
2013-03-06 11:50:37	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 11:50:33	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 11:57:35	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 11:57:35	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 14:03:29	Update	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 14:03:29	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 14:07:38	Update	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 14:07:38	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 14:56:23	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 14:56:23	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 15:05:51	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 15:05:49	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 15:14:08	Load	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 15:05:49	01:00:09:6b:cd:82:47	*
2013-03-06 15:15:10	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 15:15:09	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 15:23:00	Update	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 15:23:00	01:00:09:6b:cd:82:47	MSFT 5.0

DHCP Lease List: Valid IP addresses issued from the DHCP Server and related information of the client using this IP address is displayed here.



DHCP Lease List

Refresh Disable

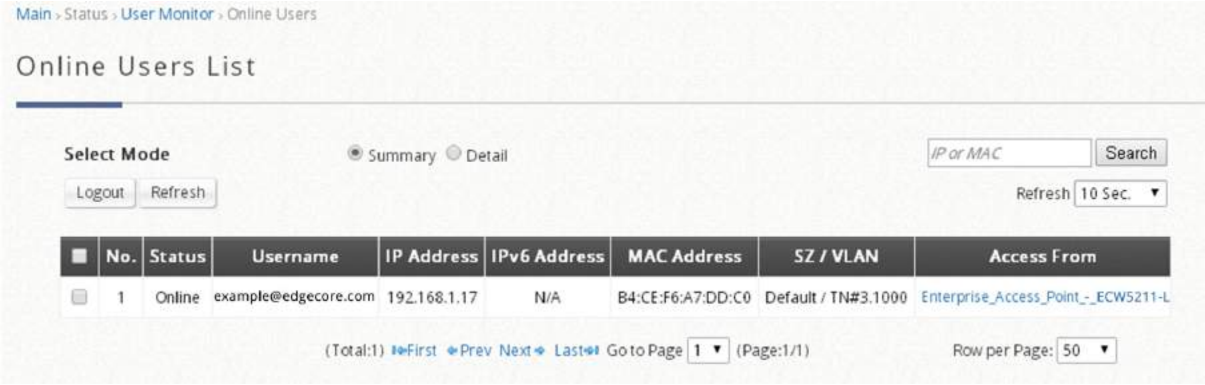
□	No.	IP Address	MAC Address	Host Name	VLAN	Lease Expires
□	1	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	3154	2013/02/08 11:08:14

(Total:1) First Previous Next Last Go to Page 1 (Page:1/1) Row per Page: 50

17.3 Client Related Status

17.3.1 Online User

Users displayed on this page are the ones that are authenticated by this Controller under its managed network either LAN or remotely tunneled site.



Main › Status › User Monitor › Online Users

Online Users List

Select Mode ● Summary ○ Detail

Refresh 10 Sec.

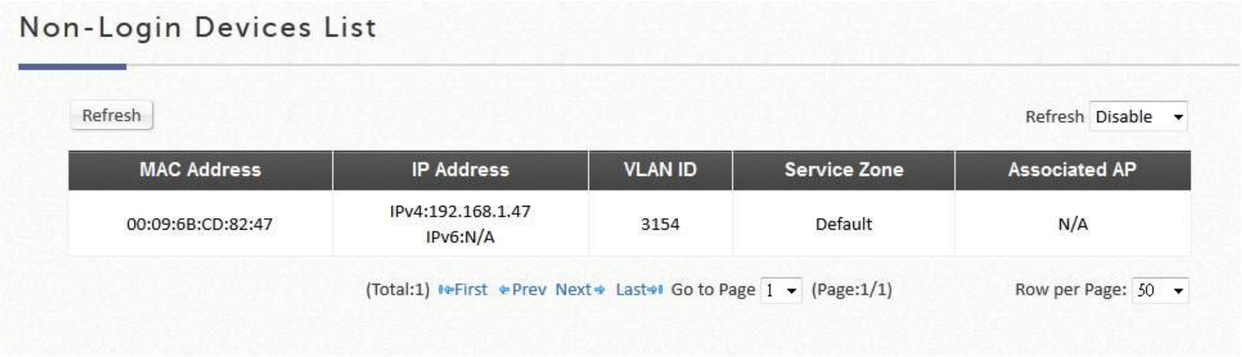
□	No.	Status	Username	IP Address	IPv6 Address	MAC Address	SZ / VLAN	Access From
□	1	Online	example@edgecore.com	192.168.1.17	N/A	B4:CE:F6:A7:DD:C0	Default / TN#3.1000	Enterprise_Access_Point_-_ECW5211-L

(Total:1) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 50

There are 2 modes to select from. Select ‘Detail’ to display more information, such as Pkts In/Out, Bytes In/Out and etc. Administrators can force out a specific online user by clicking *Kick Out* and check the user access AP status by clicking the hyperlink of the AP name for Access From. A “Search” tool is available for searching IP or MAC address of specific online user. Click *Refresh* to update the current users list or you can select the time interval for automatic refresh from the drop-down box in the lower right corner of this page.

17.3.2 Associated Non Login Users

This page shows users that have acquired an IP address from the system’s DHCP server but have not yet been authenticated, either under the LAN or remotely tunneled site. This feature is designed for administrators to keep track of systems’ resources from being exhausted. The list shows the client’s MAC Address, IP Address and associated VLAN ID, Service Zone as well as Associated AP if the client uses wireless connection.



Non-Login Devices List

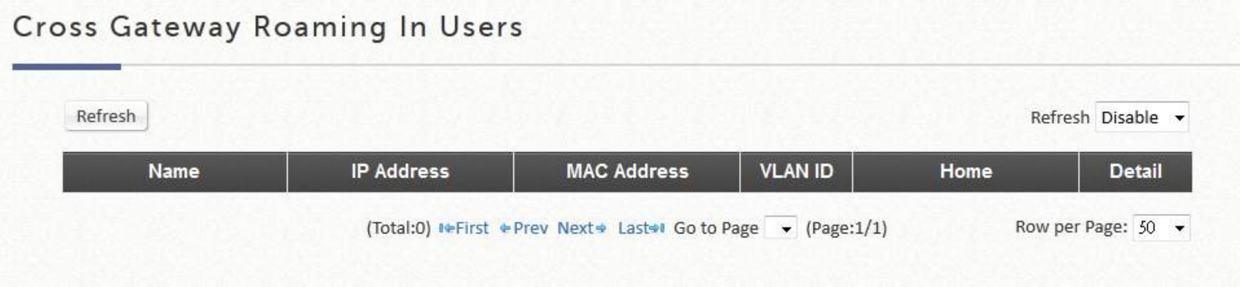
Refresh Disable

MAC Address	IP Address	VLAN ID	Service Zone	Associated AP
00:09:6B:CD:82:47	IPv4:192.168.1.47 IPv6:N/A	3154	Default	N/A

(Total:1) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 50

17.3.3 Cross Gateway Roaming Users

This page displays the users that are physically under this controller but are authenticated by a roaming peer controller. The users listed here will have their traffic tunneled back to their home controller and forwarded into the internet.



Cross Gateway Roaming In Users

Refresh

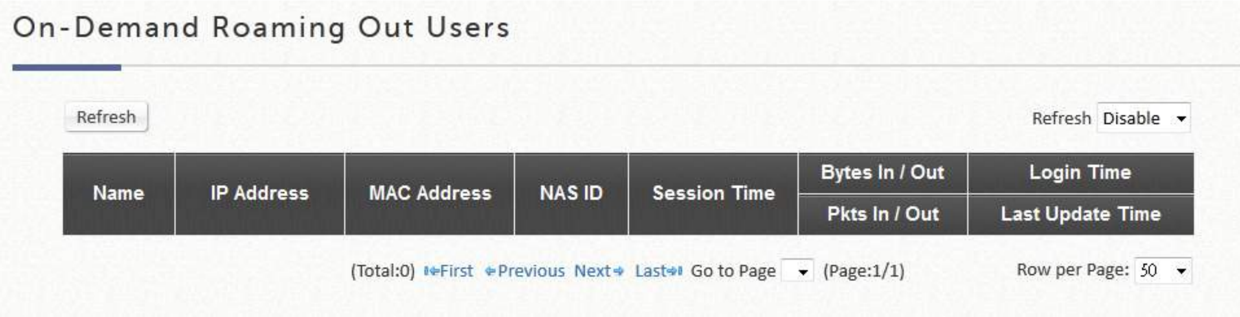
Refresh Disable

Name	IP Address	MAC Address	VLAN ID	Home	Detail

(Total:0) First Prev Next Last Go to Page (Page:1/1) Row per Page: 50

17.3.4 On-Demand Roaming Out User

This page shows the users that are authenticated by other Controllers using this Controller’s On-Demand database as RADIUS database.



On-Demand Roaming Out Users

Refresh

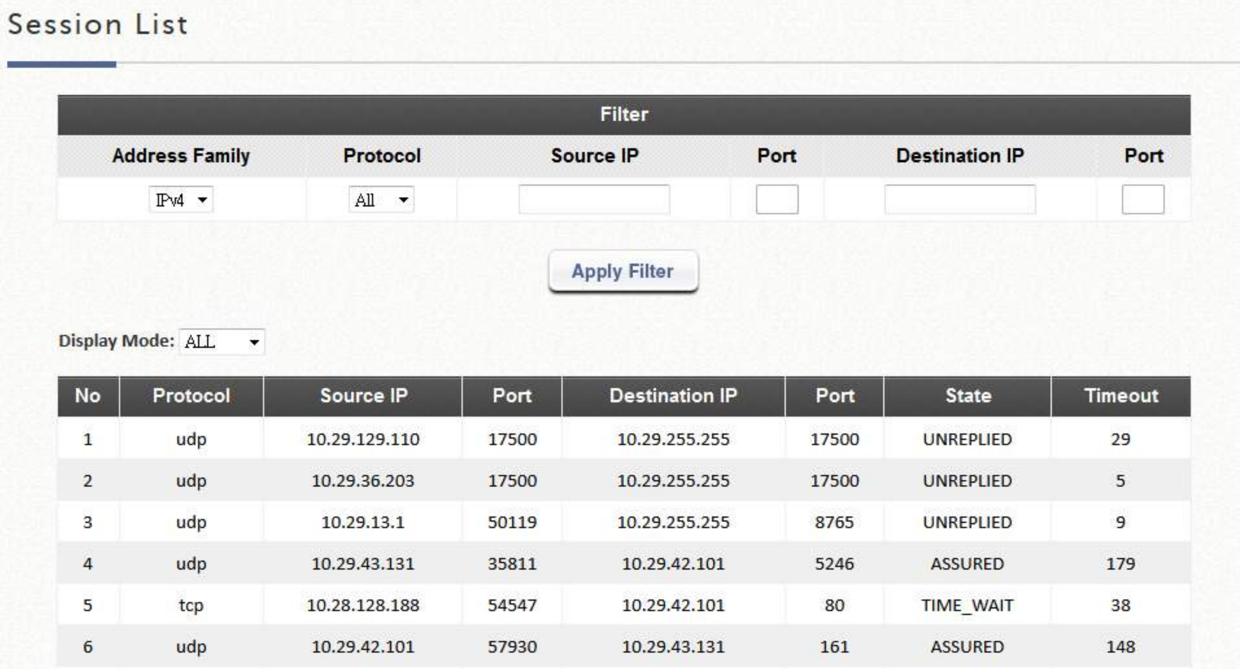
Refresh Disable

Name	IP Address	MAC Address	NAS ID	Session Time	Bytes In / Out	Login Time
					Pkts In / Out	Last Update Time

(Total:0) First Previous Next Last Go to Page (Page:1/1) Row per Page: 50

17.3.5 Session List

This page allows the administrator to inspect sessions currently established between a client and the system. Each result displays the IP and Port values of the Source and Destination. You may define the filter conditions and display only the results you desire.



Session List

Filter					
Address Family	Protocol	Source IP	Port	Destination IP	Port
IPv4	All				

Apply Filter

Display Mode: ALL

No	Protocol	Source IP	Port	Destination IP	Port	State	Timeout
1	udp	10.29.129.110	17500	10.29.255.255	17500	UNREPLIED	29
2	udp	10.29.36.203	17500	10.29.255.255	17500	UNREPLIED	5
3	udp	10.29.13.1	50119	10.29.255.255	8765	UNREPLIED	9
4	udp	10.29.43.131	35811	10.29.42.101	5246	ASSURED	179
5	tcp	10.28.128.188	54547	10.29.42.101	80	TIME_WAIT	38
6	udp	10.29.42.101	57930	10.29.43.131	161	ASSURED	148

17.4 Logs and Reports

17.4.1 System Related Logs and Reports

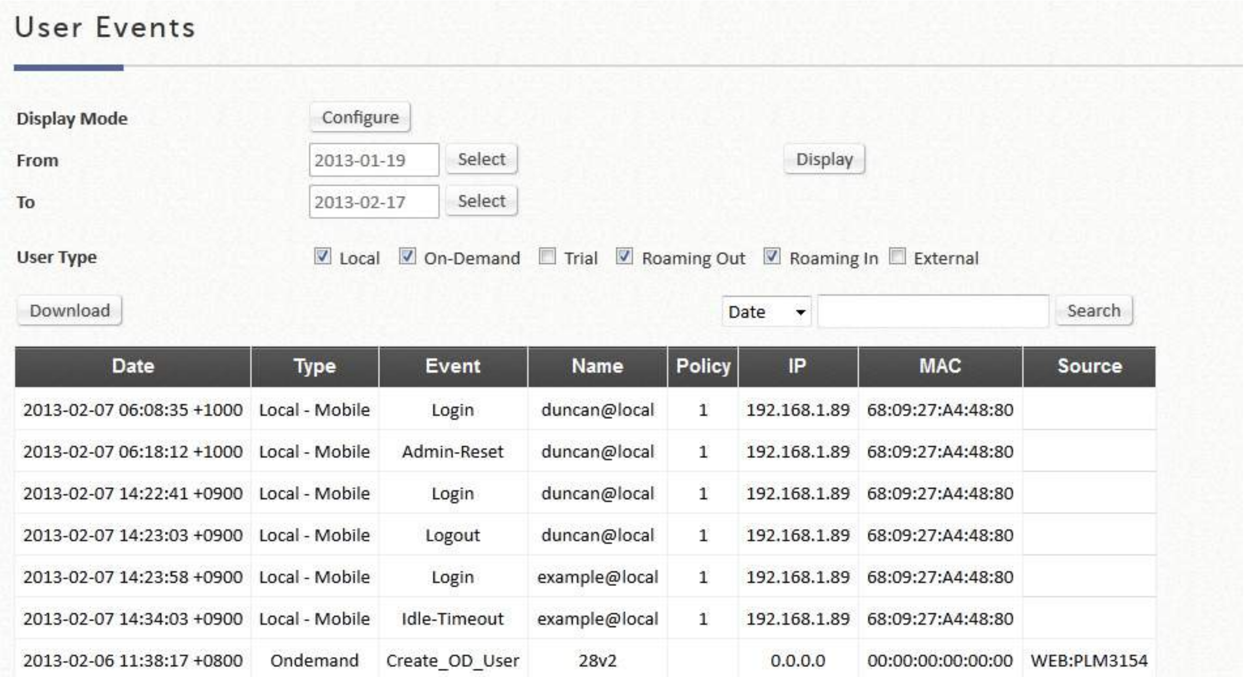
This page displays the system’s local log and User events since system boot up. Administrators can examine the log entries of various events. However, since all these information are stored on volatile memory, they will be lost during a restart/reboot operation. Therefore if the log information needs to be documented, the administrator will need to make back up manually.

CAPWAP Log: This page shows the CAPWAP message communicated between the Controller and CAPWAP enabled APs.
Configuration Change Log: This page shows the account, and IP of the person that has made changes to Controllers WMI configurations.
Local Monthly Usage: This page shows the aggregated statistics for Local users, showing the transmitted traffic for the month
Local Web Log: This page shows which of the web pages have been accessed on the Controllers built-in web server.
On-Demand User Billing Report Log: This page displays a summary of On-Demand account transactions.
RADIUS Server Log: This page displays the RADIUS messages that pass through the controller.
SIP Call Usage: The log provides the login and logout activities of SIP clients (device and soft clients) such as Start Time, Caller, Callee and Duration (seconds)
System Log: This page displays system related logs for event tracing.
UAMD Log: Displays the UAM related information output from the UAM daemon.
User Events: Displays all user related information customizable to administrator's preference.

17.4.2 User Events

This page is packed with all user logs and events. User logs and events can be stored up to 40 days. Displays all user related information customizable to administrator's preference. The administrator gets to choose the number of rows (20, 40, 60, 80, 100) to display per page. Select the Begin and End date from the calendar to filter unwanted User Events. After the Begin and End dates are selected, click "Display" to display all User Events within the selected dates.

The "Download" button downloads the displayed User Events into a comma separated .txt file. Save as a new file with .csv extension to sort the downloaded data into cells. The "Clear" button deletes current User Events displayed on the User Interface.



User Events

Display Mode [Configure]

From 2013-01-19 [Select] [Display]

To 2013-02-17 [Select]

User Type ☑ Local ☑ On-Demand □ Trial ☑ Roaming Out ☑ Roaming In □ External

[Download] Date ▾ [Search]

Date	Type	Event	Name	Policy	IP	MAC	Source
2013-02-07 06:08:35 +1000	Local - Mobile	Login	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 06:18:12 +1000	Local - Mobile	Admin-Reset	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:22:41 +0900	Local - Mobile	Login	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:23:03 +0900	Local - Mobile	Logout	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:23:58 +0900	Local - Mobile	Login	example@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:34:03 +0900	Local - Mobile	Idle-Timeout	example@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-06 11:38:17 +0800	Ondemand	Create_OD_User	28v2		0.0.0.0	00:00:00:00:00:00	WEB:PLM3154

Note that different User Types contain different user information. Categories will be left blank if inapplicable to the User Type.

Applicable User Event categories for Local Users:
Date, Type, Name, IP, IPv6, MAC, Pkts In, Bytes In, Pkts Out, Bytes Out, VLAN ID, Group, Policy, MaxDnLoad, MaxUpload, ReqDnLoad, and ReqUpload.

Applicable User Event categories for On-Demand Users:
Date, System Name, Type, Name, Unit, Price, Total Price, IP, IPv6, MAC, Pkts In, Bytes In, Pkts Out, Bytes Out, Activation Time, 1st Login Expiration Time, Account Valid Through, Remark, VLAN ID, Group, Policy, MaxDnLoad, MaxUpload, ReqDnLoad, and ReqUpload.

Applicable User Event categories for Roaming Out Users:
Date, Type, Name, NSID, NASIP, NASPort, UserMAC, SessionID, SessionTime, Bytes in, Bytes Out, Pkts In, Pkts Out and Message.

Applicable User Event Categories for Roaming In Users:
Date, Type, Name, NSID, NASIP, NASPort, UserMAC, UserIP, SessionID, SessionTime, Bytes in, Bytes Out, Pkts In, Pkts Out and Message.

17.5 Reports and Notification

WLAN controller can automatically send various kinds of user and/or system related reports by pre-configuration of E-mail addresses, SYSLOG Servers, or FTP Server.

17.5.1 SMTP Settings

Allows the configuration of 5 recipient E-mail addresses and necessary mail server settings where various user related logs will be sent to.

SMTP Server: Enter the IP address of the sender's SMTP server.
SMTP Port: By default the port number is 25. Administrator can specify other ports if the SMTP server runs SMTP over SSL.
Encryption: Enable this option if your SMTP server runs SMTP over TLS or SSL.
Authentication: The system provides four authentication methods, Plain, Login, CRAM-MD5 and NTLMv1, or None to use none of the above. Depending on which authentication method is selected, enter the Account Name, Password and Domain.

- Plain is standardized authentication mechanisms, using a UNIX login and password. Netscape uses Plain.
- CRAM-MD5 is standardized authentication mechanisms. Pegasus uses CRAM-MD5 but which method to be used cannot be configured.
- Login is Microsoft proprietary mechanisms, using a UNIX login and password. Outlook and Outlook express use Login as default, although they can be set to use NTLMv1. Pegasus uses Login as well but which method to be used cannot be configured.
- NTLMv1, a Microsoft proprietary mechanisms, is not currently available for general use. Pegasus uses

Sender E-mail Address: The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
Receiver E-mail Address (1 ~ 5): Up to 5 E-mail addresses can be set up here to receive notifications.
Send Test E-mail: to send an email into the receivers' mailbox following above configuration when first setup the SMTP server

Taking Gmail as SMTP server as example, the configurations are

- SMTP server address: smtp.gmail.com
- SMTP port: 465
- Encryption: SSL
- Authentication: Login: Account Name: admin's Gmail email address
- Authentication: Login: Password: admin's Gmail email's password
- Sender Email Address: admin's Gmail email address

17.5.2 SYSLOG Settings

Allows the configuration of two external SYSLOG servers where selected users logs as well as system logs will be sent to.

SYSLOG Destinations: Up to two external SYSLOG servers may be configured. Please enter the IP

address and port number of the external SYSLOG server here.
System Log: This controls the enabling/disabling of the SYSLOG logging feature. When enabled, the selected logs from “Notification Settings” will be sent to the SYSLOG server configured above. However, when it is disabled, no logs will be sent to the SYSLOG server configured above.

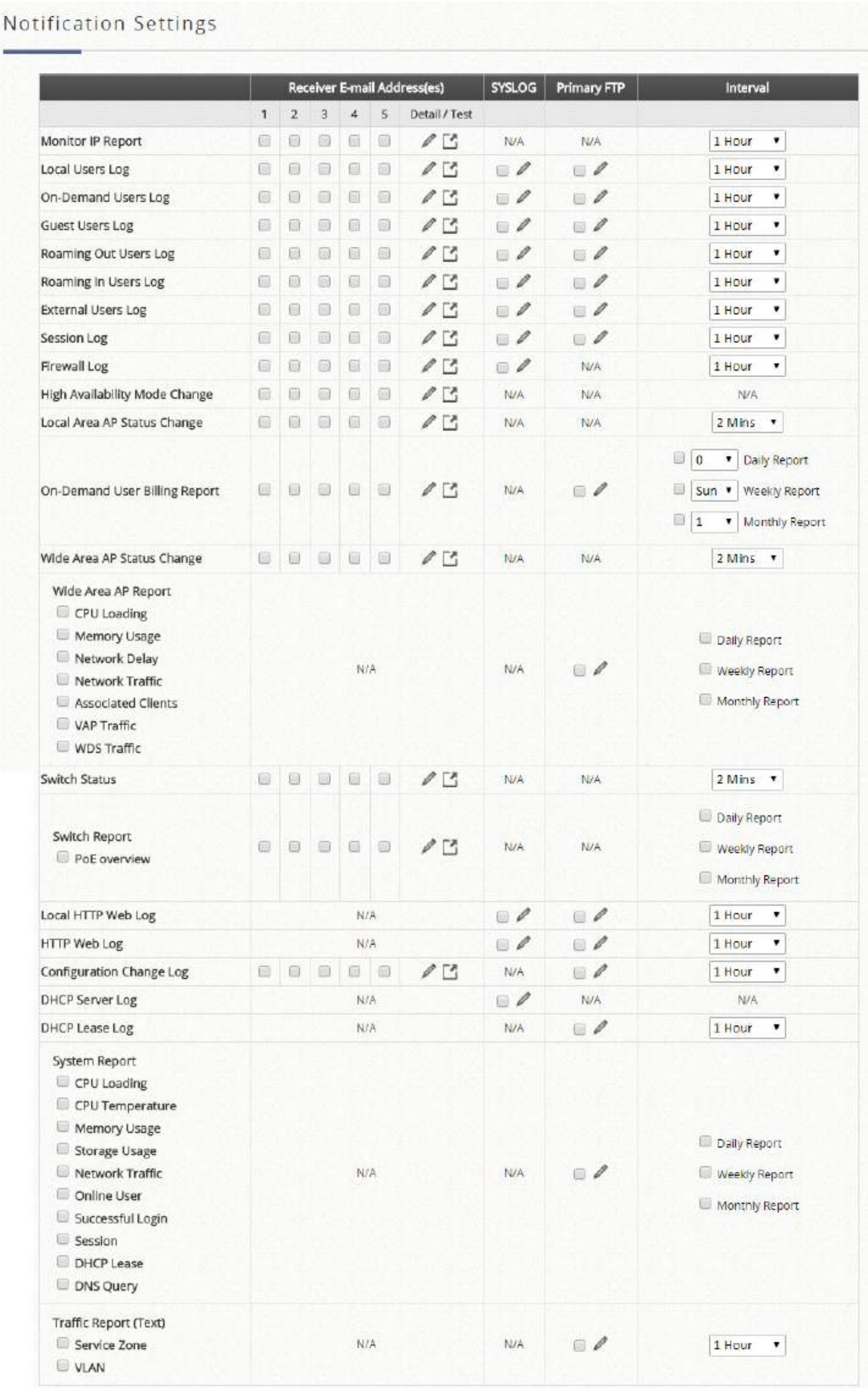
17.5.3 FTP Settings

Allows the configuration of an external FTP Server where selected users logs as well as system logs will be sent to. The outputted log files to the FTP server will be named according to the format $Topic_$ExtraDesc_$SystemName_$Date_Time.txt. For example: HTTPWebLog_GW1_2010-10-15_0800.txt

FTP Settings: Allows the configuration of an external FTP Server where selected users logs as well as system logs will be sent to.
FTP Destination: This specifies the IP address and port number of your FTP server. If your FTP needs authentication, enter the Username and Password. The “Send Test File” button can be used to send a test log for testing your current FTP destination settings.

17.5.4 Notification Settings

WLAN Controller provides an overview of all the available users and system logs for selection. Selected logs can be sent to the chosen location (E-mail, SYSLOG, FTP) on customizable time intervals.



Notification Settings

	Receiver E-mail Address(es)						SYSLOG	Primary FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	□	□	□	□	□	✎ ↗	N/A	N/A	1 Hour ▾
Local Users Log	□	□	□	□	□	✎ ↗	□ ✎	□ ✎	1 Hour ▾
On-Demand Users Log	□	□	□	□	□	✎ ↗	□ ✎	□ ✎	1 Hour ▾
Guest Users Log	□	□	□	□	□	✎ ↗	□ ✎	□ ✎	1 Hour ▾
Roaming Out Users Log	□	□	□	□	□	✎ ↗	□ ✎	□ ✎	1 Hour ▾
Roaming In Users Log	□	□	□	□	□	✎ ↗	□ ✎	□ ✎	1 Hour ▾
External Users Log	□	□	□	□	□	✎ ↗	□ ✎	□ ✎	1 Hour ▾
Session Log	□	□	□	□	□	✎ ↗	□ ✎	□ ✎	1 Hour ▾
Firewall Log	□	□	□	□	□	✎ ↗	□ ✎	N/A	1 Hour ▾
High Availability Mode Change	□	□	□	□	□	✎ ↗	N/A	N/A	N/A
Local Area AP Status Change	□	□	□	□	□	✎ ↗	N/A	N/A	2 Mins ▾
On-Demand User Billing Report	□	□	□	□	□	✎ ↗	N/A	□ ✎	□ 0 ▾ Daily Report □ Sun ▾ Weekly Report □ 1 ▾ Monthly Report
Wide Area AP Status Change	□	□	□	□	□	✎ ↗	N/A	N/A	2 Mins ▾
Wide Area AP Report □ CPU Loading □ Memory Usage □ Network Delay □ Network Traffic □ Associated Clients □ VAP Traffic □ WDS Traffic	N/A						N/A	□ ✎	□ Daily Report □ Weekly Report □ Monthly Report
Switch Status	□	□	□	□	□	✎ ↗	N/A	N/A	2 Mins ▾
Switch Report □ PoE overview	□	□	□	□	□	✎ ↗	N/A	N/A	□ Daily Report □ Weekly Report □ Monthly Report
Local HTTP Web Log	N/A						□ ✎	□ ✎	1 Hour ▾
HTTP Web Log	N/A						□ ✎	□ ✎	1 Hour ▾
Configuration Change Log	□	□	□	□	□	✎ ↗	N/A	□ ✎	1 Hour ▾
DHCP Server Log	N/A						□ ✎	N/A	N/A
DHCP Lease Log	N/A						N/A	□ ✎	1 Hour ▾
System Report □ CPU Loading □ CPU Temperature □ Memory Usage □ Storage Usage □ Network Traffic □ Online User □ Successful Login □ Session □ DHCP Lease □ DNS Query	N/A						N/A	□ ✎	□ Daily Report □ Weekly Report □ Monthly Report
Traffic Report (Text) □ Service Zone □ VLAN	N/A						N/A	□ ✎	1 Hour ▾

Appendix A. Hardware Overview

EWS100		
1	Reset	Press and hold for over 3 seconds and status of LED on front panel will start to blink, release button at this stage to restart the system. Press and hold the Reset button for more than 10 seconds and status of LED on the front panel will turn from blinking to off, release at this stage to reset the system to default configuration.
2	Power button	Main ON/OFF power of the system.
3	LED Displays	Power: Power LED lights up as constant green when power supply is on. Status: Blinking indicates that the system OS is booting up. When the system is ready for operation, the LED is lit up constantly.
4	Port1	WAN port (10/100/1000 Base-T RJ-45) for uplink connections to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
5	Port2	WAN2 or LAN1 (10/100/1000 Base-T RJ-45) function configurable.
6	Port3-Port5	Gigabit LAN ports for servicing LAN traffic (10/100/1000 Base-T RJ-45)
7	USB	USB console interface. The cable should be the combination of below 3 cables - 1 Port USB to RS232 DB9 Serial Adapter Cable - M/M - RS232 DB9 Serial Adapter Cable to RS232 DB9 Serial Adapter Cable - F/F - RS232 DB9 Serial Adapter Cable to 1 Port USB - M/M

EWS5203		
1	Reset	Press and hold the Reset button for about 5 seconds and status of LED on front panel will start to blink before restarting the system. Press and hold the Reset button for more than 10 seconds and status of LED on the front panel will start to speed up blinking before resetting the system to default configuration.
2	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft's Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.
3	USB1/USB2	Reserved for future use.
4	WAN1/WAN2	Dual Gigabit WAN ports (10/100/1000 Base-T RJ-45) for uplink connections to the external network, such as the ADSL Router from Internet Service Provider.
5	LAN1 ~ LAN2	Two Gigabit LAN ports for servicing LAN traffic (10/100/1000 Base-T RJ-45).
6	LED Indicators	There are two LED indicators, Power and Status, to indicate different status of the system.

EWS5204		
1	LCD Display	Allows network administrator to check important system settings such as network interface, SZ configurations, etc. The navigation buttons from left to right respectively are “Esc”, “Up”, “Down”, and “Enter”.
2	Reset	Press and hold the Reset button for about 5 seconds and status of LED on front panel will start to blink before restarting the system. Press and hold the Reset button for more than 10 seconds and status of LED on the front panel will start to speed up blinking before resetting the system to default configuration.
3	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft’s Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.
4	USB1/USB2	Reserved for future use.
5	WAN1/WAN2	Dual Gigabit WAN ports (10/100/1000 Base-T RJ-45) for uplink connections to the external network, such as the ADSL Router from Internet Service Provider.
6	LAN1 ~ LAN2	Two Gigabit LAN ports for servicing LAN traffic (10/100/1000 Base-T RJ-45).
7	LED Indicators	There are two LED indicators, Power and Status, to indicate different status of the system.

EWS5207		
1	LED Indicators	There are three LED indicators, Power, Status and Hard-disk, to indicate different status of the system.
2	LCD Display	Allows network administrator to check important system settings such as network interface, SZ configurations, etc. The navigation buttons from left to right respectively are “Esc”, “Up”, “Down”, and “Enter”.
3	Reset	Press and hold the Reset button for about 5 seconds and status of LED on front panel will start to blink before restarting the system. Press and hold the Reset button for more than 10 seconds and status of LED on the front panel will start to speed up blinking before resetting the system to default configuration.
4	Console	The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft’s Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.
5	USB	Reserved for future use.
6	WAN1/ WAN2	Dual Gigabit WAN ports (10/100/1000 Base-T RJ-45) for uplink connections to the external network, such as the ADSL Router from Internet Service Provider.
7	LAN1 ~ LAN4	Four Gigabit LAN ports for servicing LAN traffic (10/100/1000 Base-T RJ-45).

P/N: V34300180423