



# User Manual VEWS Controller

Version 3.60.00

---

## Copyright Notification

### Edgecore Networks Corporation

© Copyright 2023 Edgecore Networks Corporation.

The information contained herein is subject to change without notice. This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered by Edgecore Networks Corporation. Edgecore Networks Corporation shall not be liable for technical or editorial errors or omissions contained herein.

## **Copyright**

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission of Edgecore, INC.

## **Disclaimer**

Edgecore, INC. does not assume any liability arising out the application or use of any products, or software described herein. Neither does it convey any license under its parent rights nor the parent rights of others. Edgecore further reserves the right to make changes in any products described herein without notice. The publication is subject to change without notice.

## **Trademarks**

Edgecore is a registered trademark of Edgecore, INC. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Table of Contents

<b>Chapter 1. Introduction</b>	<b>1</b>
1.1 EWS WLAN Gateway-Controller Series	1
1.2 EWS Controller Models	3
1.3 Edgecore Solution Overview	3
1.4 Key Terms & Concepts	5
1.5 Recommended Configuration Sequence	8
1.5.1 Common Settings	8
1.5.2 Advanced Settings and Application	8
<b>Chapter 2. WMI &amp; Setup Wizard</b>	<b>10</b>
2.1. Web Management Interface	10
2.2 Running the Wizard	12
<b>Chapter 3. Basic Network Settings</b>	<b>16</b>
3.1. Network Planning	16
3.2. Uplink (WAN side) Configuration	19
3.2.1 WAN Settings	19
<b>Chapter 4. User Authentication Database</b>	<b>21</b>
4.1. Authentication Database Configuration	21
4.2. Built-in Authentication Databases	23
4.2.1. Local User Database	23
4.2.2. On-Demand User Database	26
4.2.3. The Guest Authentication Option	31
4.2.4. One Time Password	36
4.3. External Authentication Options	37
4.3.1. RADIUS	37
4.3.2. POP3	40
4.3.3. LDAP	41
4.3.4. NT Domain	41
4.3.5. SIP	42
4.3.6. Social Media	44
<b>Chapter 5. Group Attributes &amp; Policy Rules</b>	<b>47</b>
5.1 Overview of the Concept	47
5.2 Practical Setups of Group and Policies	49
<b>Chapter 6. Basic Service Zone Configuration</b>	<b>56</b>
6.1 The Concept of Service Zone	56
6.2 Service Zone Setup	56
6.2.1. NAT Mode or Router Mode	56
6.2.2. Service Zone Network Interface	57
6.2.3. DHCP Server options	58
6.2.4. Authentication Options	59
6.2.5. Captive Portal Customization	62
<b>Chapter 7. Basic AP Management</b>	<b>65</b>
7.1. Introduction	65
7.2 Wide Area AP Management	66
7.2.1. Adding an Access Point	67
7.2.2. AP Discovery to find Multiple Access Points	68
7.2.3 AP Configuration with Templates	69
7.2.4 AP auto Discovery and Configuration using CAPWAP	71
7.2.5 Tunneled VAP Location Mapping Setup	77
7.2.6 Access Points Monitoring on Google Map	78
7.2.7 AP Grouping	84
7.2.8 Rogue AP Scanning	86
7.2.9 AP Load Balancing Feature	87
<b>Chapter 8. Advanced Settings for Network Environment</b>	<b>90</b>

8.1 IPv4 / IPv6 Dual Stack Network .....	90
8.2 User Access Control .....	94
8.3 Certification.....	97
8.3.1. System Certificate .....	97
8.3.2. Internal Root CA .....	99
8.3.3. Internally Issued Certificate.....	100
8.3.4. Trusted Certificate Authorities .....	100
8.4 Management Access .....	101
<b>Chapter 9. Utilities for Controller Management.....</b>	<b>102</b>
9.1 EWS Controller Management .....	102
9.2 Configuration Backup & Restore .....	104
9.3 Firmware Upgrade .....	106
9.4 Restart.....	106
<b>Chapter 10. Reports and Logs for Monitoring .....</b>	<b>108</b>
10.1 System Related Status.....	108
10.1.1 The Dashboard.....	108
10.1.2 System Summary .....	109
10.1.3 Network Interface.....	111
10.1.4 Routing.....	112
10.1.5 DHCP Server .....	113
10.2 Client Related Status .....	114
10.2.1 Online User .....	114
10.2.2 Associated Non Login Users .....	115
10.2.3 Cross Gateway Roaming Users.....	116
10.2.4 On-Demand Roaming Out Users.....	116
10.2.5 MAC Login Devices .....	117
10.2.6 Authenticated Users .....	117
10.2.7 Smart Login Users.....	118
10.2.8 Session List .....	119
10.3 Logs and Reports .....	120
10.3.1 System Related.....	120
10.3.2 User Events.....	121
10.4 Reports & Notification .....	122
<b>Chapter 11. Hotspot Application .....</b>	<b>125</b>
11.1 On-Demand Billing Plans .....	125
11.2 On-Demand Billing Plan Types.....	126
11.2.1 Usage-time with Expiration Time .....	126
11.2.2. Usage-time with No Expiration Time .....	128
11.2.3. Hotel Cut-off-time.....	130
11.2.4. Volume.....	131
11.2.5. Duration-time with Elapsed Time .....	133
11.2.6. Duration-time with Cut-off Time .....	135
11.2.7. Duration-time with Begin-and-End Time .....	136
11.3 POS Printer Setup .....	137
11.4 Customizing POS Tickets .....	141
11.5 Creating Accounts .....	145
11.6 User Self Service.....	147
<b>Chapter 12. PMS Integration .....</b>	<b>152</b>
12.1 Hotel Room Location Mapping .....	152
12.2 PMS Configuration .....	154
<b>Chapter 13. Account Roaming.....</b>	<b>157</b>
13.1 Roaming Related .....	157
13.2 WISPr for ISP Roaming .....	157
13.3 Cross Gateway Roaming .....	159

13.4 Local / On-Demand Account Roaming Out .....	160
<b>Chapter 14. VPN .....</b>	<b>163</b>
14.1 Site-to-Site.....	163
14.2 Remote Client .....	165
<b>Chapter 15. Switch Management .....</b>	<b>167</b>
15.1 Switch List.....	167
15.2 PoE Schedule Template .....	168
15.3 Backup Configuration .....	169
<b>Chapter 16. Platform Dependent Features .....</b>	<b>170</b>
16.1 WiFi Monitor .....	170
16.1.1. Add a Floor Plan .....	170
16.1.2. Simulation AP .....	172
16.1.3. AP Monitoring on floorplan .....	174
<b>Appendix A. VEWS Installation on Linux System .....</b>	<b>176</b>
<b>Appendix B. External Pages .....</b>	<b>181</b>
<b>Appendix C. Useful Management &amp; Evaluation Tools .....</b>	<b>194</b>
<b>Appendix D. On-Demand Account Types .....</b>	<b>196</b>
<b>Appendix E. UI Reference Index .....</b>	<b>202</b>
I. Dashboard .....	202
II. Setup Wizard .....	203
A. System .....	204
1) General .....	204
2) WAN .....	207
3) IPv6.....	207
4) Service Zones .....	208
5) Port Location Mapping .....	214
6) PMS Interface .....	217
B. Users.....	219
1) Groups .....	219
2) Internal Authentication.....	220
a) Local Authentication .....	221
b) On-Demand Authentication .....	222
c) Guest Authentication .....	228
d) One Time Password .....	229
3) External Authentication .....	230
a) Social Media Authentication .....	230
4) On-Demand Accounts.....	231
5) Schedule .....	232
6) Policies .....	232
7) Blacklists .....	234
8) Privilege Lists.....	235
9) Additional Control .....	235
C. Devices.....	238
1) Wide Area AP Management .....	238
a) AP List .....	238
b) AP Grouping .....	241
c) Map .....	248
d) Discovery .....	250
e) Adding .....	251
f) Template.....	252
g) WDS List .....	258
h) Backup Config.....	259
i) Firmware.....	259
j) CAPWAP.....	260

k) Rogue AP Detection .....	261
l) AP Load Balancing .....	261
m) Third Party AP Management.....	262
2) Switches.....	264
a) Switch List.....	264
b) PoE Schedule Template .....	264
c) Backup Configuration .....	266
E. Network.....	267
1) NAT .....	267
2) Monitor IP.....	269
3) Walled Garden and Walled Garden Ad.....	269
4) VPN .....	270
5) Proxy Server .....	271
6) Local DNS Record .....	274
7) Dynamic Routing .....	274
8) DDNS.....	278
9) Client Mobility .....	279
F. Utilities.....	280
1) Administrator Account.....	280
2) Backup & Restore .....	283
3) Certificates .....	285
4) Network Utilities .....	287
5) Restart.....	289
6) System Upgrade.....	289
G. Status .....	290
1) System Summary .....	290
2) Interface .....	292
3) Monitor Users.....	294
4) WiFi Monitor.....	294
5) Process Monitor .....	297
6) Logs & Reports.....	297
7) Reporting .....	299
8) Session List .....	306
9) DHCP Lease .....	306
10) Routing Table .....	308

# Chapter 1. Introduction

## 1.1 EWS WLAN Gateway-Controller Series

Edgecore EWS WLAN Gateway-Controllers are feature rich network edge devices designed for network service provisioning, authentication, security, and management. Depending on the scale of deployment, there are a selection Edgecore EWS WLAN Gateway-Controller models to meet the network demands with various scale of capacities.

Edgecore EWS Controllers are designed to cater for the fundamental needs of any network environment, namely triple A (AAA) which stands for Authentication, Authorization, and Accounting. With Edgecore EWS Controllers, various users are authenticated based on user role, from there it will define the user's accessible network segments, the user's network portfolio including accessible time, QoS, routing rules, firewall rules, usage terms and privileges which are collectively known as authorization. Finally accounting are performed by Edgecore EWS Controllers periodically while a client is using the network, updating the accounting information for this client to either the internal user database or an external user database depending on deployment.

Wireless network provisioning is no easy task when the scale reaches multiple AP deployments.

Edgecore EWS Controllers are equipped with comprehensive AP management feature to cover not only 4ipent AP devices deployed locally under the Local Area Network (LAN) but also Edgecore AP devices deployed remotely in the Wide Area Network (WAN), relative to the location of your Edgecore EWS Controllers. Furthermore, with a 3<sup>rd</sup> party AP management interface, Edgecore EWS Controllers are capable of performing generic AP management features including associated online user monitoring, shortcut to GUI interface, and location planning for non-Edgecore APs.

Network safety and traffic control are other big areas of concern for network owners, hoteliers as these are major factors in determining the quality and stability of your network environment as a whole.

Edgecore EWS Controllers addresses these needs with the following major features: equipped with static and dynamic routing features for optimized path selection, QoS mapping for enforcing bandwidth control to each individual user, system uplink bandwidth control, and customization firewall protocols and rules.

Common networking features can be found well packed into the [Edgecore EWS Controllers](#). Providing three varieties of NAT function, Walled Garden for free website surfing, Network device monitoring tool, Static DNS translation, Proxy Server, VPN and more. [Edgecore EWS Controllers](#) simplify network deployment by incorporation multiple networking features into one device, avoiding the need to setup external NAT servers, Proxy servers, VPN gateway, etc. thereby reducing deployment complexity.

Network Maintenance and Network monitoring tasks are made easy with built in displays of system traffic, system resource utilization such as CPU usage and memory consumption, online user record, DHCP lease record, and more. Event logs can be sent to external servers for long term record keeping or in depth analysis.



## 1.2 EWS Controller Models

Edgecore EWS Controller product line comes with the following models for targeting network deployment of variable scale.

SMB & Enterprise WLAN Gateway-Controllers

EWS101, EWS5203

Large Enterprise & Carrier Grade Controllers

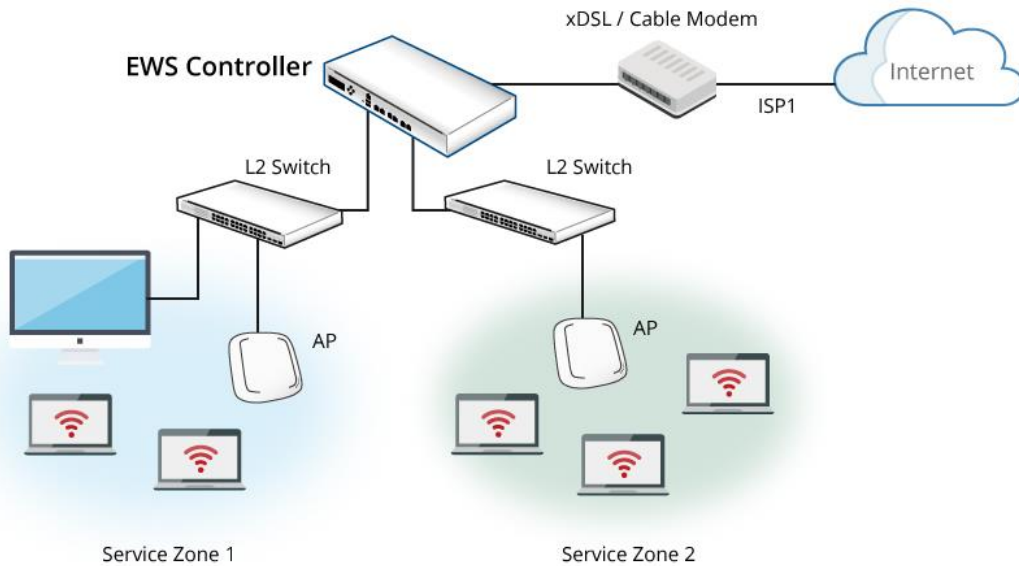
EWS5204, EWS5207

Note: Edgecore may continue to introduce new platforms, and may retire old platforms, please refer to our website <http://www.Edgecore.com> for the latest product line status. For more detailed listing of each model hardware and installation know how, please refer to **Appendix A**.

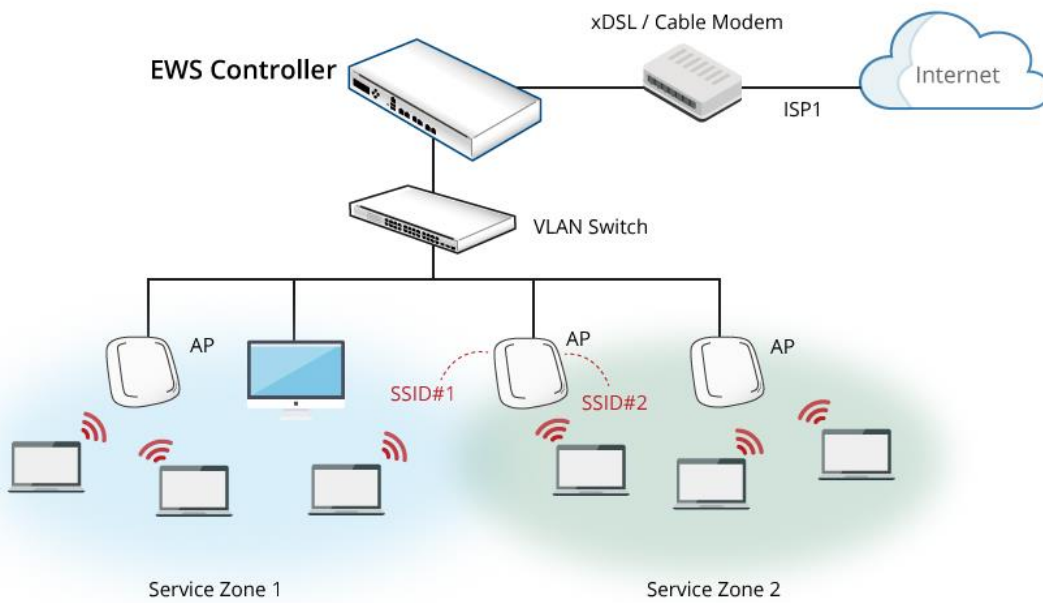
## 1.3 Edgecore Solution Overview

Edgecore EWS Controllers are designed for network management over almost all current network architectures, Layer 2 (Data Link Layer) and Layer 3 (Network Layer).

Layer 2 networks are relative simple network deployment topology that span physically under the LAN ports of Edgecore EWS Controllers, two deployment scenarios are illustrated below.

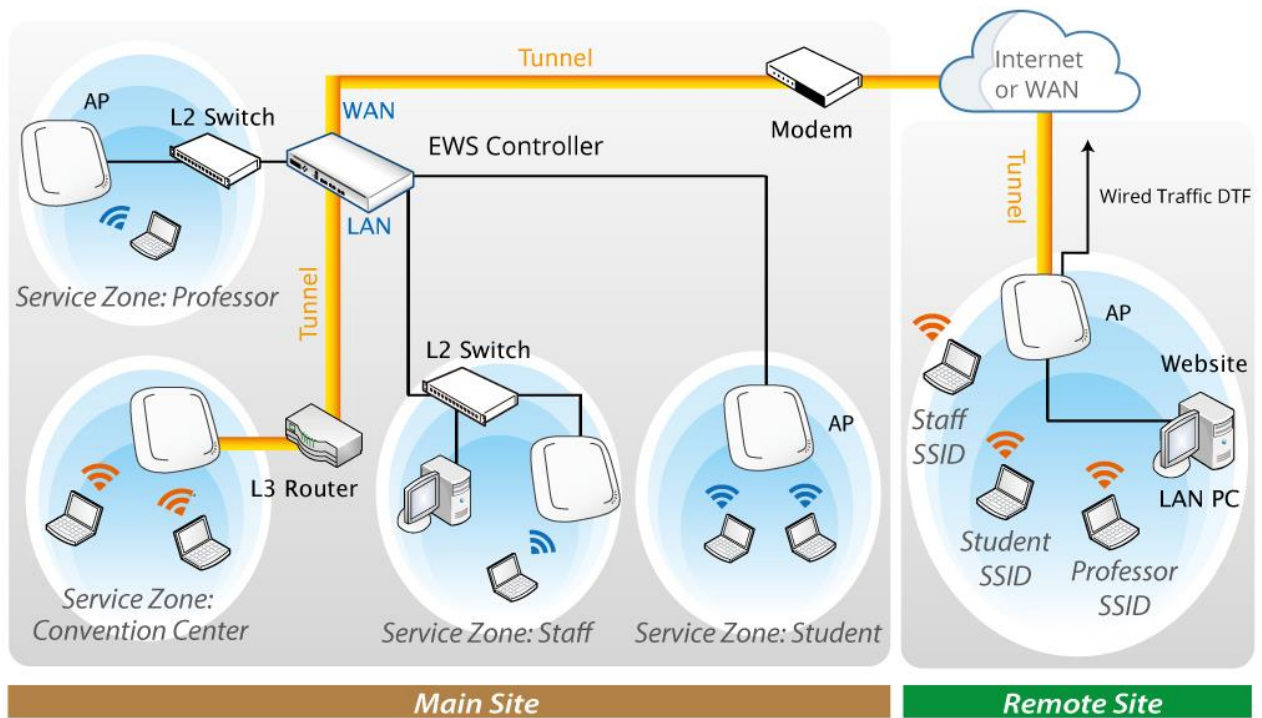


**【Layer 2 Network in Port Based Mode】**



**【Layer 2 Network in Tag Based Mode】**

Layer 3 networks not only span physically under the LAN ports of Edgecore EWS Controller, it is also capable of reaching over different IP networks to manage remote sites with routable IP address via tunnels.



【Layer 3 Network with tunnels】

## 1.4 Key Terms & Concepts

**Gateway** is an edge device or network node where a small network attaches to a bigger network. Edgecore EWS Controllers are in essence gateways in a network environment. Conventionally, the bigger network is referred as the WAN side or upstream network (physically connected via the WAN port), while the small network is referred as the LAN side.

**Local User** is a type of user whose account credential is stored in the Edgecore EWS Controller's built-in database named "Local". The Edgecore EWS 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. In addition, Edgecore EWS Controller's Local database can be configured as an external RADIUS database for another Edgecore EWS Controller for account roaming.

**On-Demand User** is a type of user whose account credential is stored in the Edgecore EWS Controller's built-in database named "On-Demand". The Edgecore

EWS 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. In addition, Edgecore EWS Controller's On-Demand database can be configured as an external RADIUS database for another Edgecore EWS Controller for account roaming.

**External Authentication Database** is a user account database that is not built-in the Edgecore EWS Controller. Besides Local database and On-Demand database, Edgecore EWS Controller supports four additional types of External Authentication databases namely RADIUS, POP3, LDAP (including Active Directory), and NTDomain (Win2K's NTDS). External Authentication Database is useful for both implementing account roaming and centralized account management.

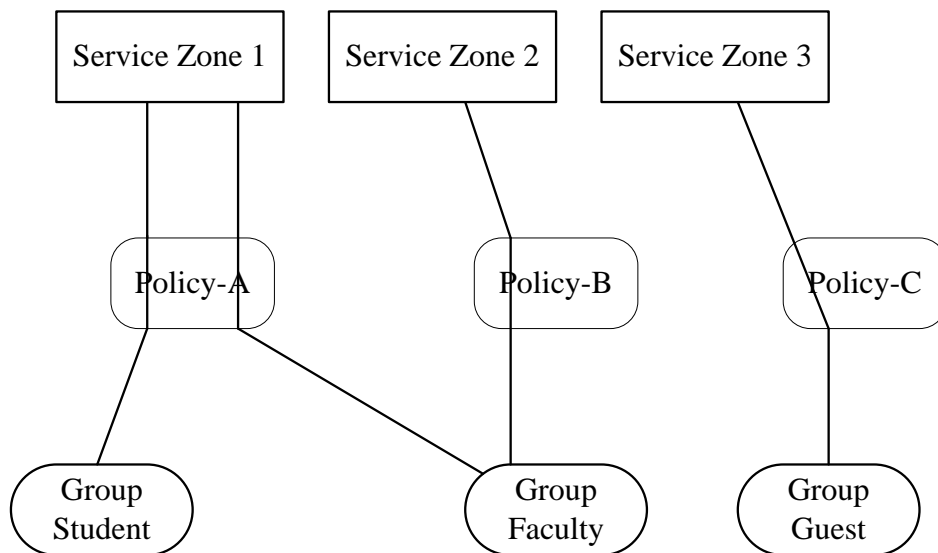
**Service Zone** is a logic partition of Edgecore EWS Controller's LAN. The concept of Service Zone is that it is a virtual gateway with customizable login portal page with its own gateway properties (such as LAN IP address, DHCP server settings, authentication options, etc.). With up to nine independent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

**Group** is a user role profile which defines the accessibility of a user to different Service Zones and in turn defines the QoS properties as well as network policy when access is granted. Each and every connected user will belong to a Group, determined by the type of user account used for authentication. If the administrator does not assign a new account to any specific Group or for users not required to authenticate, they will belong to a catch-all group named "None" by default.

**Policy** is the second tier of user control once a user's Group profile has been determined. Policy defines the firewall rules, privileges, login schedule, routing rules and session limit which will be enforced to users of a particular Group. A user may only belong to one Group but can be governed by different policies while accessing different Service Zones.

For users belonging to the “None” group or users not explicitly assigned a network Policy, they will be governed by a default catch-all policy named ‘Global-Policy’. The Global-Policy is a base policy which will be applied to all users if not applied with another policy.

The following Figure is an example that depicts the relationship between Service Zone, Group and Policy. In this example, Students and faculties logging into Service Zone 1 will be governed by Policy-A. Guests only have access to Service Zone 3, and will be bounded by Policy-C. Faculties have the access to both Service Zone 1 and Service Zone 2 under two different policies.



**【Relationship of Service Zone, Group and Policy】**

## 1.5 Recommended Configuration Sequence

- Set up system's Time Zone, NTP server, DNS server and WAN1 address
- Configure LAN address range for at least one Service Zone, and enable its authentication.
- Create user accounts to test the login page via wire line in the enabled Service Zone.
- Try to generate an On-Demand user and test the account.
- Configure Wireless Settings of Service Zone and add in AP.
- Configure necessary Service Zones based on applications.
- Set up Group and Policy (including Firewall rules and Session Limit).
- Customize the portal login page and add walled garden Advertisement links if needed.
- Set up Payment gateway to allow end user credit card self-payment for On-Demand accounts if needed.
- Load SSL certificate for the Web Server before operation.
- Monitor generated status pages and reports.
- Perform other advanced setting for other specific application.

### 1.5.1 Common Settings

For the most commonly deployed scenarios in a standard network, please refer to Chapters 3 to 7.

**Chapters 3 to 7** contain configuration topics that encompass the most commonly used features in a typical network environment. It is recommended for users to start from Chapter 3 and proceed through Chapter 7 for any deployment.

### 1.5.2 Advanced Settings and Application

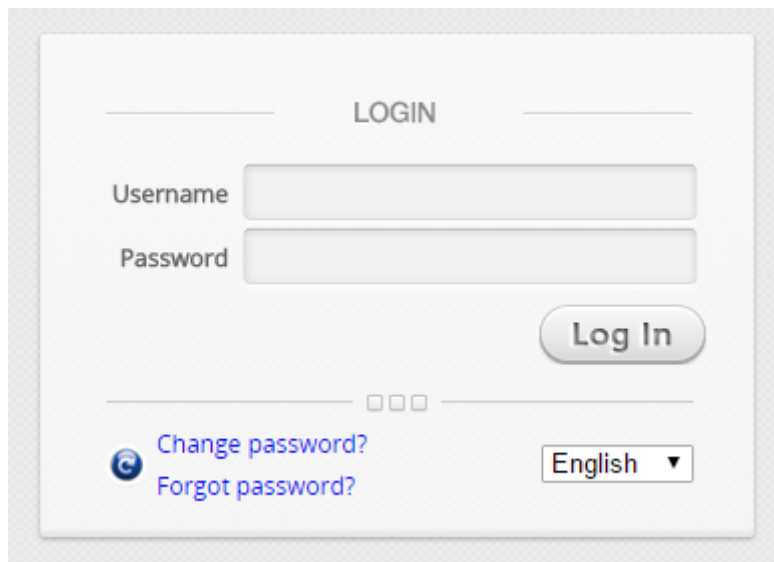
**Chapters 8 to 10** discuss about security, system maintenance, and monitoring. These contents are useful once you have successfully configured the necessary functionalities and are for operation usage once your network is up and running.

Customers with needs to fulfill specific applications, integration with 3<sup>rd</sup> party devices, customization etc., please refer to **Chapters 11** and beyond for advanced feature setup.

# Chapter 2. WMI & Setup Wizard

## 2.1. Web Management Interface

The Web Management Interface (WMI) of the EWS controller can be accessed through a web browser (Firefox, Chrome, and Safari recommended) of any PC connected to the LAN interface with the default IP address of **192.168.1.254**.



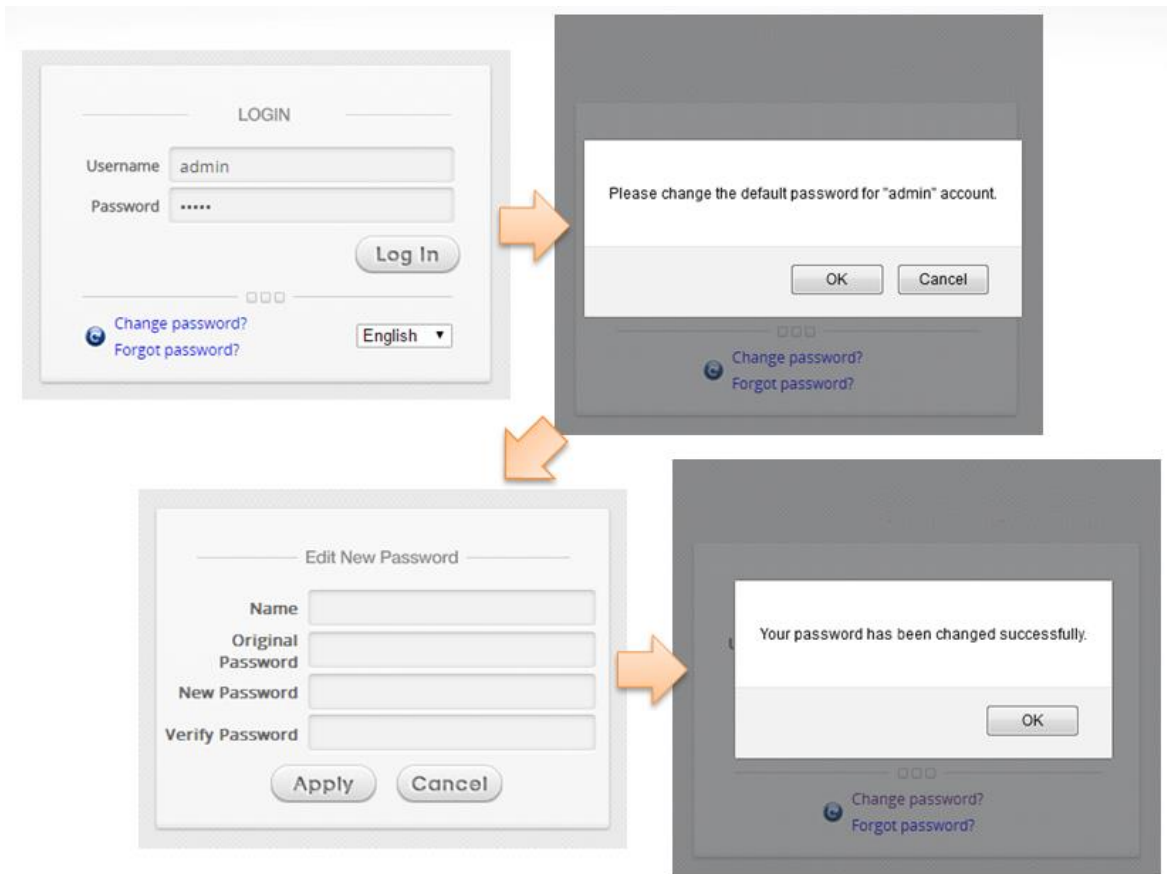
The default administrator account and password is:

- Username: "admin"
- Password: "admin"

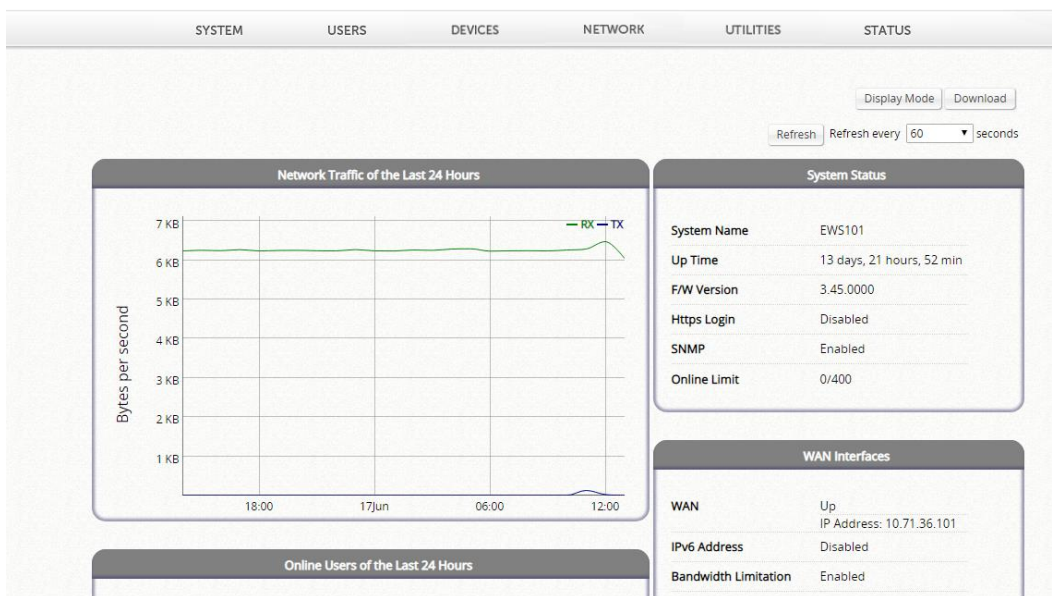
Upon the first login, the system prompts for the administrator to change password to enforce system security. The password needs to be at least 6 characters long and include at least one alphabet and one number.

You may refer to part E. of Appendix F for details on admin accounts configuration.





The Dashboard page is as shown below after a successful administrator login.



## NOTE

1. To logout, simply click the **Logout** icon on the upper right corner of the interface to return to the login screen.

## 2.2 Running the Wizard

The Setup Wizard provides a collection of configuration steps which are essential in the setup and operation of your network with minimum configurations.

To quickly configure EWS by using the **Setup Wizard**, click on the **Setup Wizard** button on the top right corner of the WMI homepage to start the configuration process.

### Step 1. General

- Select an appropriate time zone from the **Time Zone** drop-down list.
- Click **Next** to continue.



The screenshot shows the 'General' configuration step of the Setup Wizard. At the top, there is a progress bar with four steps: 1. FIRST STEP (Set Time Zone), 2. SECOND STEP (Configure WAN1), 3. THIRD STEP (Create A Local User), and 4. YOU'RE DONE (Restart the System). The first step is highlighted. Below the progress bar, there is a warning message: 'It is recommended to select an appropriate time zone for the system.' The main area is titled 'General' and contains a 'Time Zone' dropdown menu with '(GMT+08:00)Taipei' selected. At the bottom right, there are two buttons: 'Exit' and 'Next'.

### Step 2. Select Connection Type for WAN1 Port

- There are three types of WAN connections to be selected from: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**. Select a proper Internet connection type. Below depicts an example of using Dynamic IP connection.
- Click **Next** to continue.
- For **Static IP Address** or **PPPoE Client**, follow the instructions on the screen.

1 FIRST STEP Set Time Zone    2 SECOND STEP Configure WAN1    3 THIRD STEP Create A Local User    4 YOU'RE DONE Restart the System

Please select connection type of the WAN1 interface and configure the settings.

### WAN1 Interface

Static (Use the following IP settings)  
 Dynamic (IP settings assigned automatically)  
 PPPoE

Exit    Back    Next

### Step 3. Add Local User Account (Optional)

- A new user can be added to the Local User database. To add a user here, enter the **Username** (e.g. testuser), **Password** (e.g. testuser), and assign an **Applied Group** to this particular user (or use the default **Group 1**).
- Click **Next** to continue.

1 FIRST STEP Set Time Zone    2 SECOND STEP Configure WAN1    3 THIRD STEP Create A Local User    4 YOU'RE DONE Restart the System

You can choose to add local user accounts for a quick configuration.

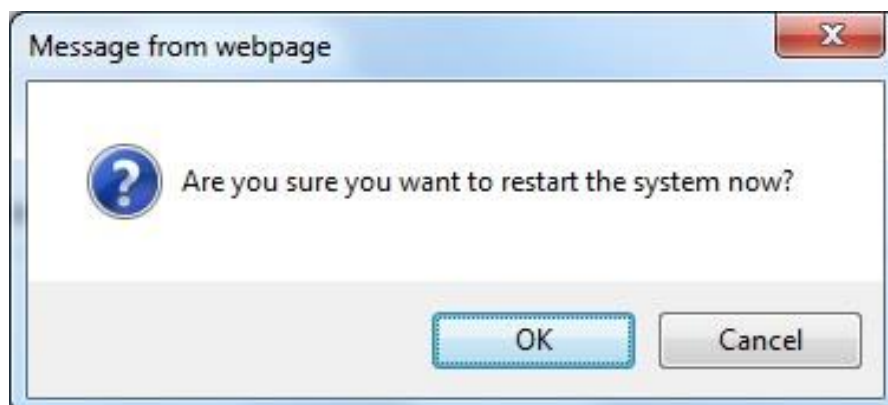
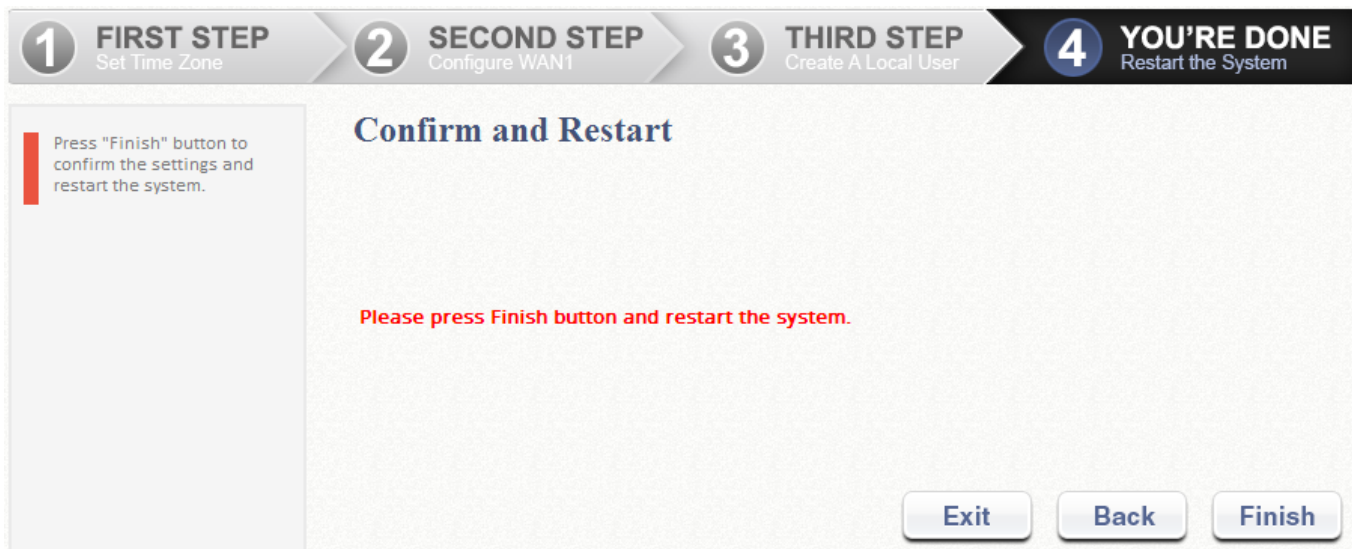
### Local User Account (Optional)

Username:   
 Password:   
 Group:

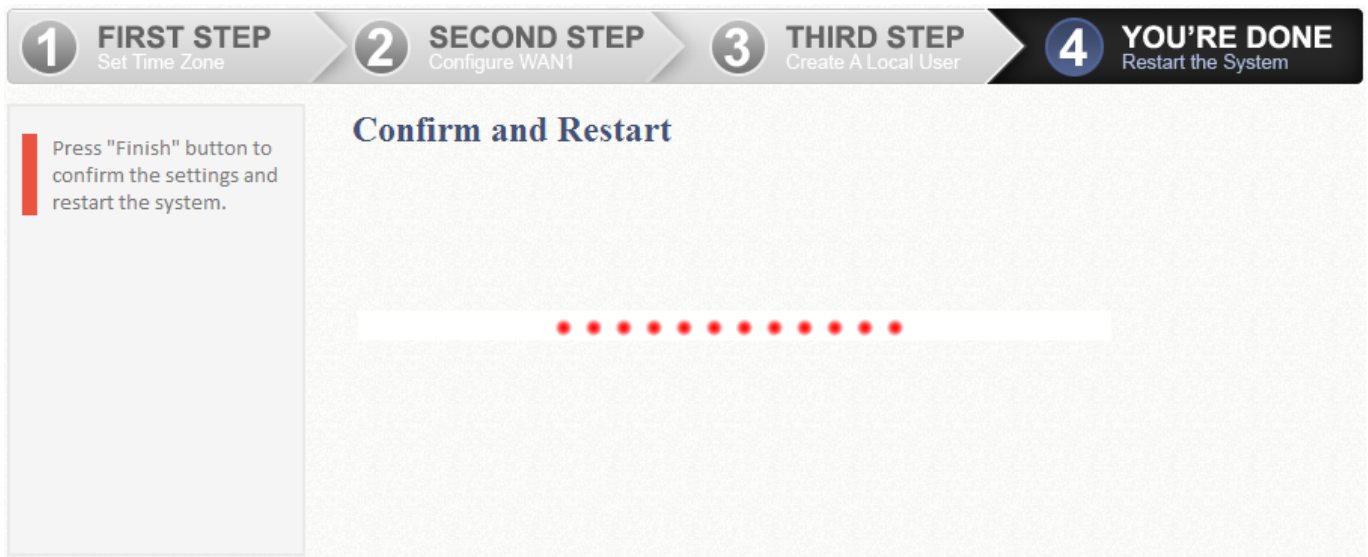
Exit    Back    Skip    Next

## Step 4. Confirm and Restart EWS

- Click **Finish** to save current settings and restart the system.
- A confirmation dialog box will then appear. Click **OK** to continue.

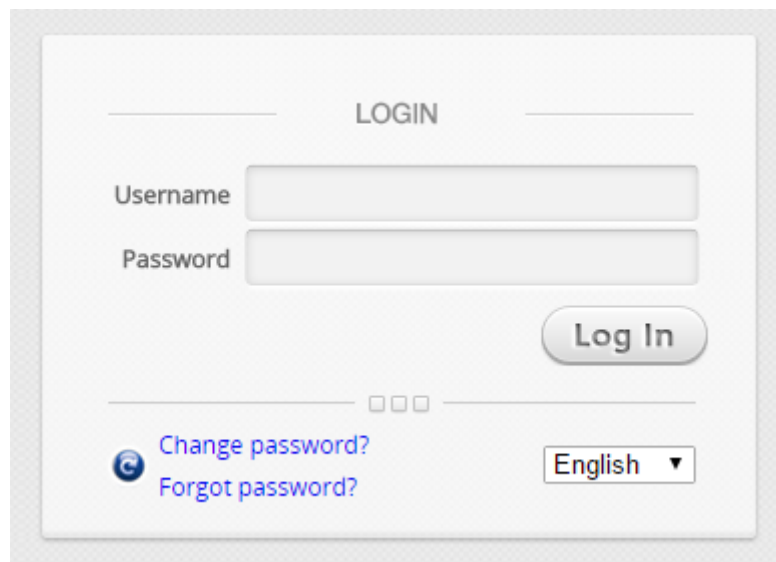


- A **Confirm and Restart** message will appear on the screen during the restarting process. Please do not interrupt the system until the Administrator Login Page appears.



Please do NOT interrupt EWS restart process until the admin login page reappears – which indicates the restart process has been completed.

Restart process complete.



# Chapter 3. Basic Network Settings

## 3.1. Network Planning

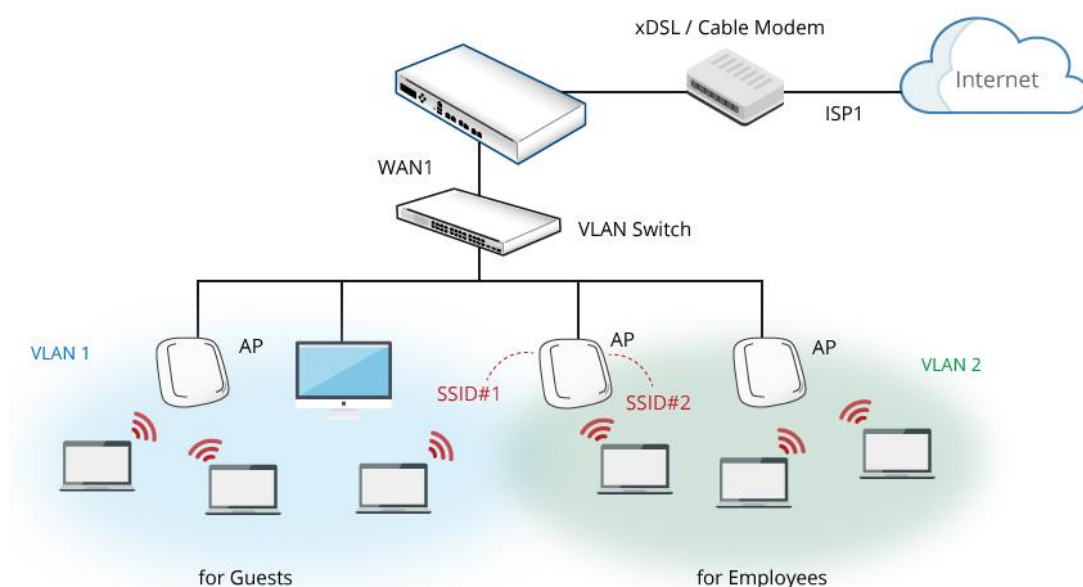
Before installing the Edgecore EWS Controller, careful network planning is required in order to meet the networking needs with the most efficient utilization of network resources. IT staff of any organization should assess the available network resources at hand, and design a suitable network topology 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 by Edgecore EWS Controllers are:

- 1) Layer 2 Topology
- 2) Layer 3 Topology

### Layer 2 Topology

This network 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.



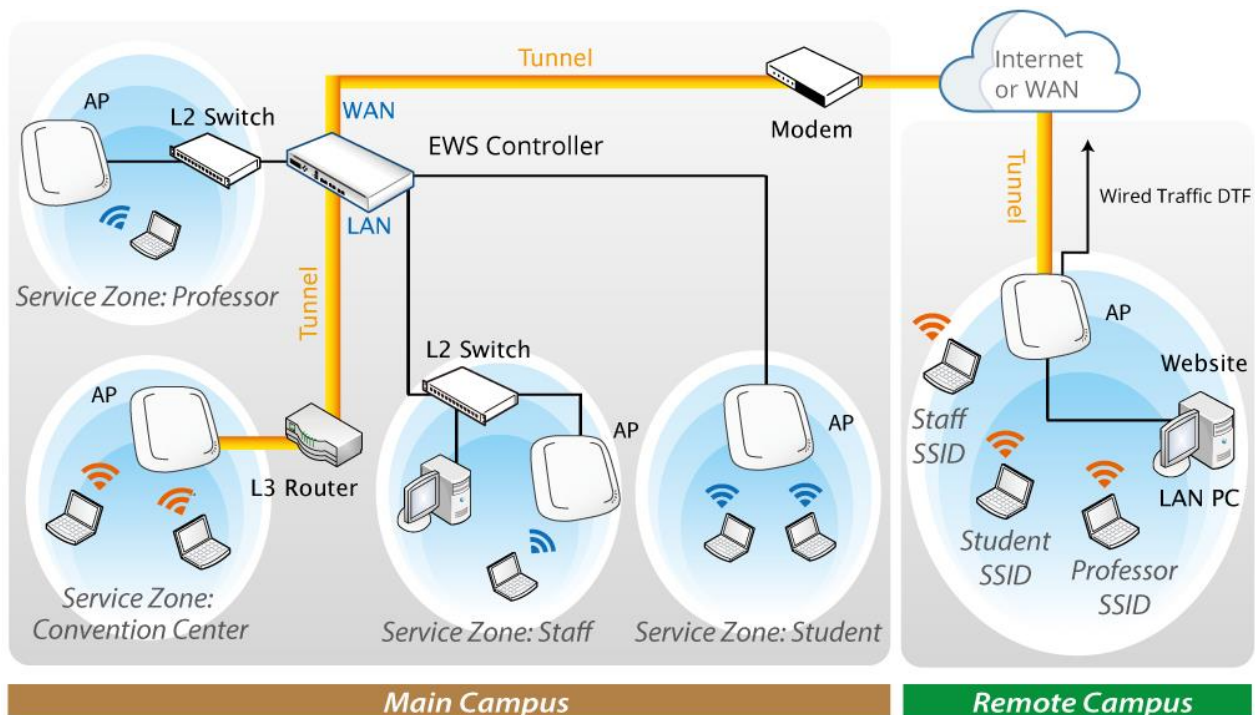
【 Graphical Illustration of Layer 2 Topology 】

## Layer 2 Network Design Guidelines

- 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

This network 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.



【Graphical Illustration of Layer 3 Topology】

## Layer 3 Network Design Guidelines

- 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.

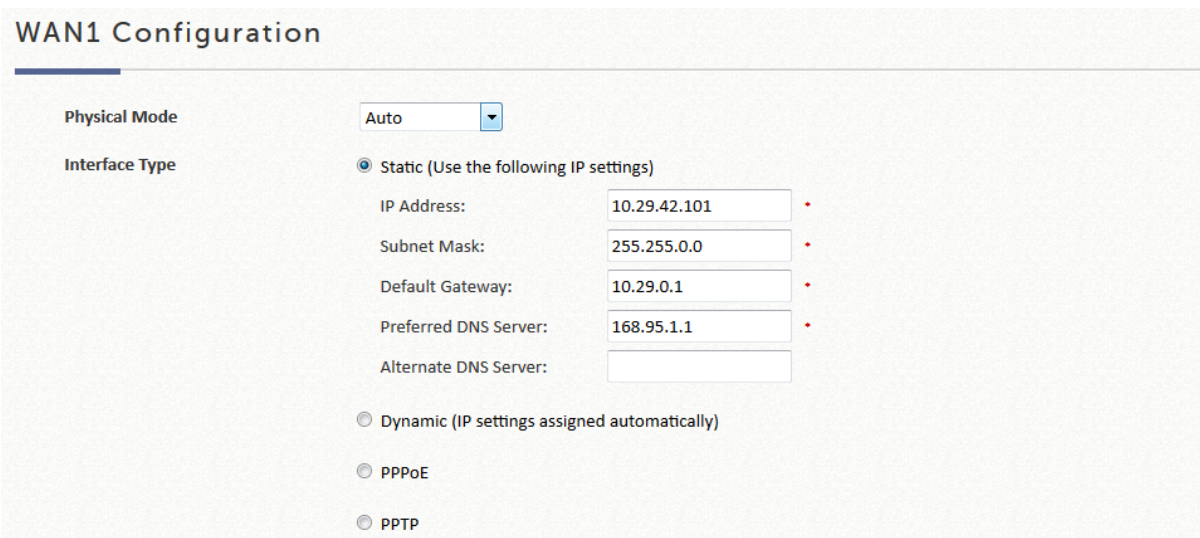


## 3.2. Uplink (WAN side) Configuration

### 3.2.1 WAN Settings

Configuration Path: [Main Menu >> System >> WAN](#)

The WAN port supports four connection configurations **Static**, **Dynamic**, **PPPoE** and **PPTP**. These connection types are adequate enough to support most ISP. The **Physical Mode** 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.



The screenshot shows the 'WAN1 Configuration' interface. Under 'Physical Mode', a dropdown menu is set to 'Auto'. Under 'Interface Type', the 'Static (Use the following IP settings)' option is selected. The static IP settings are as follows:

Field	Value	Required
IP Address:	10.29.42.101	Yes
Subnet Mask:	255.255.0.0	Yes
Default Gateway:	10.29.0.1	Yes
Preferred DNS Server:	168.95.1.1	Yes
Alternate DNS Server:		No

Other interface type options include Dynamic (IP settings assigned automatically), PPPoE, and PPTP.

Depending on ISP's interfacing device the WAN port is connecting, you need to select the connection type applicable to you. For example, if your ISP is Cable modem issuing Dynamic address, then you would select **Dynamic** connection.

**Static:** Manually specifying the IP address of the WAN Port. The fields with red asterisks are required to be filled in.

**Dynamic:** It is only applicable for a network environment where the DHCP server is available on the upstream network. Click the **Renew** button to get

an IP address automatically.

**PPPoE:** If your ISP provides PPPoE Dialup connection, then the ISP will issue you an account with a password. You would need to enter the account credential in the WAN configuration page for dialing up to the ISP.

**PPTP:** Although not a popular method, PPTP protocol for dialup connections is adapted by some ISPs (in European Countries). Your PPTP ISP will issue you an account with a password as well as the PPTP server address.

#### **NOTE**

1. When in doubt, please consult your ISP provider regarding details of your subscribed uplink service.
-

# Chapter 4. User Authentication Database

## 4.1. Authentication Database Configuration

Authentication database is a storage device where users' credentials may be inquired for validity. When a user is associated to an authentication enabled in Service Zone, the Edgecore EWS controller checks the database to see if the submitted user ID and password combination exists, in order for the user to get network access. Edgecore EWS controllers support built-in and external authentication databases.

All the authentication options are listed below:

### Built-in Authentication options

**Local** with user credentials stored in the built-in Local database.

**On-Demand** with user credentials stored in the built-in On-Demand database.

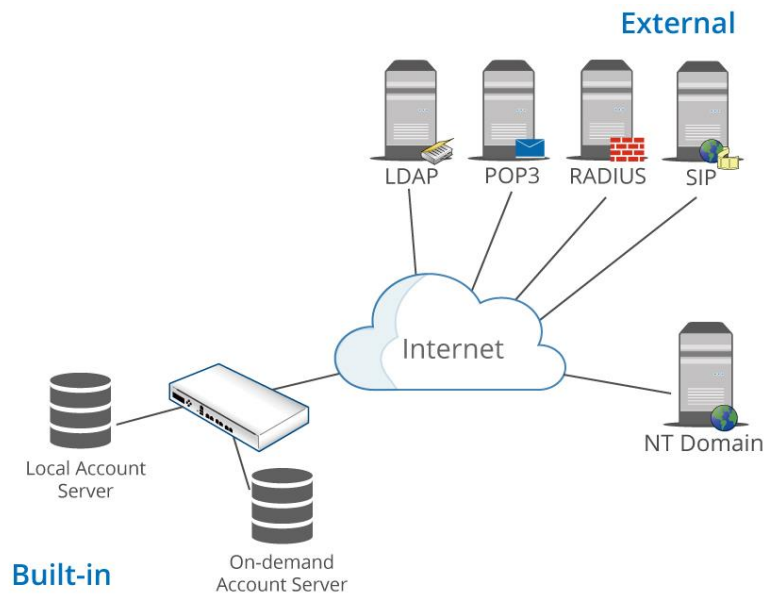
**Guest** an access option that allows users to access networks with any specified identity token on the login page.

**One Time Password** an access option that allows users to access networks with a password sent by SMS which is valid for only one login session.

### External Authentication Options

These options use external servers to implement the authentication process.

Edgecore EWS controllers support some of the most common external authentication options, including: **RADIUS, LDAP, NT Domain, POP3, SIP,** and **Social Media.**



【Graphical illustration of authentication databases in relation to EWS Controller】

Authentication Options					
Auth. Option	Auth. Database	Postfix	Default	Enabled	
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>	
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>	
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>	
Guest	FREE	N/A	<input type="radio"/>	<input type="checkbox"/>	
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>	
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>	

The configurations of authentication options for Internal and External authentication are done separately. The 5 external authentication servers (RADIUS, POP3, LDAP, NT Domain, and SIP) are customizable and can be enabled concurrently.

**NOTE**

1. Auth Options may be selectively enabled or disabled to authenticate users in each Service Zone profile.

## 4.2. Built-in Authentication Databases

Configuration Path: [Main Menu >> Users >> Internal Authentication](#)

### 4.2.1. 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.

Configuration Path: [Main Menu >> Users >> Internal Authentication >> Local >> Local User List](#)

#### Account generation

Click **Add User** to create one or multiple accounts.

Local User List

Buttons: Add... Delete Backup List Upload Search

No	Status	Username	Password	MAC	Group	Activation	Expiration	Local VPN	Remark
----	--------	----------	----------	-----	-------	------------	------------	-----------	--------

(Total:0/6000) First Prev Next Last Go to Page (Page:1/1) Row per Page: 10

Username	Password	MAC Address	Group	Local VPN	Account Span	Remark
example	••••••••		Group 1	<input type="checkbox"/>	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	<input type="checkbox"/>	

**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** are 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.
  7. The maximum length of **Username and Password** field is 1-64 characters. Only "0~9", "A~Z", "a-z", ".", "-", and "\_" are acceptable.
- 

## Account Import and Export

The Local user database can import and export user credentials by using the Upload and Download functions respectively. The download file will be a text file in csv format displayed in a new browser window, administrator can perform "save as" to backup the user accounts in PC storage for future use. Upload operation is performed by browsing for a backed up txt file and import the accounts back into the Local user database.

Local User List

Add...
Delete
Backup List
Upload

Search

■	No	Status	Username	Password	MAC	Group	Activation	Expiration	Local VPN	Remark
(Total:0/6000) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a>										

Go to Page 
(Page:1/1)
Row per Page:

## NOTE

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

## Modifications to Account Credentials

For existing user accounts, further modification is possible simply by clicking the username hyperlink on the page to reconfigure account attributes.

Local User List

Add... Delete Backup List Upload  Search

<input type="checkbox"/>	No	Status	Username	Password	MAC	Group	Activation	Expiration	Local VPN	Remark
<input type="checkbox"/>	1	Valid	<a href="#">example</a>	example		Group 1			Disable	

Editing Existing User Data

Username  \*

Password  \*

MAC Address

Applied Group

Enable Local VPN

Remark

Enable Expire Time

Begin Date

End Date

## Deleting Accounts

Accounts in the Local user database may be deleted individually or entirely by selecting the "Select All" checkbox. There will be a popup window asking if you are sure to carry out the action.

Local User List

Add... Delete Backup List Upload

Search

No	Status	Username	Password	MAC	Group	Activation	Expiration	Local VPN	Remark
1	Valid	example	example		Group 1			Disable	

#### 4.2.2. 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 tickets can be customized to businesses' needs, and multiple payment options are also available on the EWS Controllers.

Configuration Path: [Main Menu >> Users >> Internal Authentication >> On-Demand](#)



## On-Demand Authentication

User Postfix	<input type="text" value="ondemand"/>
Billing Plans	<input type="button" value="Configure"/>
Currency	<input type="radio"/> None <input type="radio"/> \$ USD <input type="radio"/> € EUR <input type="radio"/> £ GBP <input type="text"/>
	<small>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.</small>
Expired Account Cache	<input type="text" value="30"/> day(s)
Out-of-quota Account Cache	<input type="text" value="30"/> day(s)
Set Ticket's Serial Number	<input type="text" value="000001"/> <input type="button" value="Set"/>
Web Printout	<input type="button" value="Configure"/>
	<small>This will be applied to the regular printer printout when creating a single On-Demand account.</small>
POS Tickets	<input type="button" value="Configure"/>
	Number of Tickets <input checked="" type="radio"/> 1 <input type="radio"/> 2
	<small>This will be applied to printouts from the POS ticket printer. Templates can be edited for customization.</small>
Terminal Server	<input type="button" value="Configure"/>
	<small>Terminal Servers are add-on devices such as the SDS100 or SDS200W.</small>
Payment Gateway	<input type="button" value="Configure"/>
SMS Gateway	<input type="button" value="Configure"/>
Account Roaming Out	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

### On-Demand Account Settings

1. **General Settings** for the On-Demand Account database can be configured on this page. General Settings include the customization of POS/Web tickets, Payment Gateway options, and etc. When ticket printers (such as EC-PP200) are deployed for account generation, remember to configure the IP and Port in Terminal Server configuration. The EWS Controller can work in hand with Clickatell SMS server for On-Demand accounts credentials to be sent to users via SMS message.

## SMS Gateway

### Selection

Disable  Clickatell

### Send SMS for

Account purchases via Payment Gateway  Free Account Registration  Both

### Clickatell Configuration

API ID  \*

User Name  \*

Password  \*

API URL  \*

Registration before Accounts Expired  Allow  Block

Query Balance

### Billing Plans for Clickatell

Plan	Activation	Quota	Price	Remark
1	<input type="checkbox"/>			<input type="text"/>
2	<input type="checkbox"/>			<input type="text"/>
3	<input type="checkbox"/>			<input type="text"/>
4	<input type="checkbox"/>			<input type="text"/>
5	<input type="checkbox"/>			<input type="text"/>
6	<input type="checkbox"/>			<input type="text"/>
7	<input type="checkbox"/>			<input type="text"/>
8	<input type="checkbox"/>			<input type="text"/>
9	<input type="checkbox"/>			<input type="text"/>
0	<input type="checkbox"/>			<input type="text"/>

### Account Registration Control

Disable  Black List  White List

### Web Page Customization

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".

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

Plan (s)	Price ( ₪ )	Remark
<input checked="" type="radio"/> 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.

[Back](#) [Register](#)

Note that the Billing Plan selection page may be customized if needed.

2. Define account usage terms in **Billing Plans**. Up to 10 billing plan profiles are available for the administrator to customize the terms of use by selecting an appropriate account type. The User Group profile for each Billing Plan is also assigned here.

## Billing Plans

No	Plan Type	Quota	Price	Active	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	2	<input checked="" type="checkbox"/>	Group 1	Reset
2	Volume	500 Mbyte(s) of traffic volume quota	5	<input checked="" type="checkbox"/>	Group 2	Reset
3	Hotel Cut-off-time	Valid until 12:00 the following day	10	<input checked="" type="checkbox"/>	Group 3	Reset
4	Duration-time	Valid for 4 hour(s) elapsed time	3.99	<input checked="" type="checkbox"/>	Group 4	Reset
5	N/A			<input type="checkbox"/>	Group 1	Reset
6	N/A			<input type="checkbox"/>	Group 1	Reset
7	N/A			<input type="checkbox"/>	Group 1	Reset
8	N/A			<input type="checkbox"/>	Group 1	Reset
9	N/A			<input type="checkbox"/>	Group 1	Reset
0	N/A			<input type="checkbox"/>	Group 1	Reset

### NOTE

1. For more detailed information on the four major account types, please refer to **Appendix D**.
2. For more detailed information on Ticket Customization, please refer to Online Help or the Edgecore Application Note on Ticket Customization.

## On-Demand Accounts

Configuration Path: [Main Menu >> Users >> On-Demand Accounts](#)

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.

**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, such valid and total number of On-Demand accounts are informed in the end of this list.

Main > Users > On-Demand Accounts > Account List

### On-Demand Account List

Delete Restore List Backup List Delete Expired Delete Out of Quota  Search

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

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

### 4.2.3. The Guest Authentication Option

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.

This feature 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.

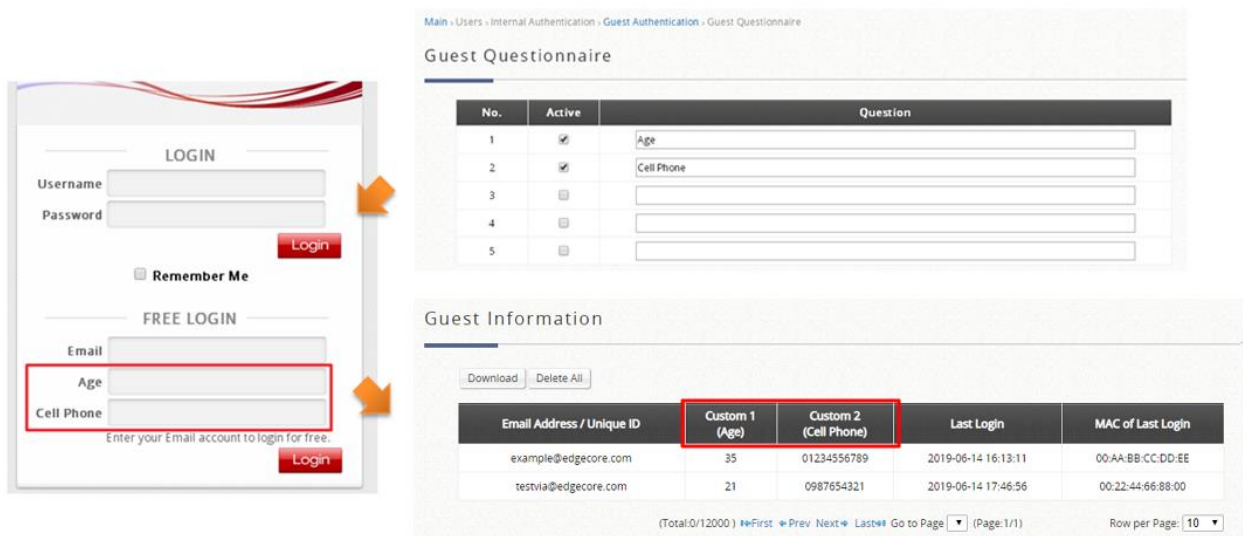
Configuration Path: [Main Menu >> Users >> Internal Authentication >> Guest](#)

**Step1:** Setting up the Guest Authentication profile

## Guest Authentication

Group	Group 1 ▾
Guest Information	View
Guest Questionnaire	Configure
Guest Access Time	<input type="radio"/> Unlimited <input checked="" type="radio"/> 1 Day Access <input type="radio"/> Multi-Day Access
Quota	0 hour(s) 30 minute(s) 0 MByte(s) *(Range:0~1000000, 0:Unlimited)
Reactivation	After 0 hour(s) 1 minute(s)
Access Limit	30 per day *(0:Unlimited)
Email Verification	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Guest Quota List	View
E-mail Denial List	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <span>Configure</span>

The **E-mail Denial List** checks the email domains for login permission, if prevention of junk mailboxes is desired. **Guest Questionnaire** 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** when set to "Limited" will enforce a usage time constraint based on MAC addresses. If the **Quota** is set to 30 minutes, each device may only be allowed 30 minutes of usage, and a new session will only be possible once the **Reactivation** time has elapsed. Administrators also get to decide how many times a device can request for a free account in a day by configuring **Access Limit**. Guest users are then mapped to a selected User Group for policies application. **Guest Quota List** provides administrators 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 quota of 12000).



**Email verification** ensures that the entered email is a valid email address. When this option is enabled, an activation time is allocated to the client. The client then 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. The Sender Name, Email Subject, 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.

**Email Verification**  Disable  Enable

**Email activation time**  hour(s)  minute(s)

**Sender name**

**Activation email subject**

**Activation email content**

**Activation link**

**Guest Account List**

SMTP server is not ready

Some information of the accounts are available for collection in the **Guest Information** list for administrators' further analysis or marketing purposes. E-mail address, device MAC address, last login time, and the answer for the Guest Questionnaire.

Guest Information

Download Delete All

Email Address / Unique ID	Custom 1 (Age)	Custom 2 (Phone No.)	Last Login	MAC of Last Login
example@edgecore.com	35	01234556789	2019-06-14 16:13:11	00:AA:BB:CC:DD:EE
testvia@edgecore.com	21	0987654321	2019-06-14 17:46:56	00:22:44:66:88:00

(Total:0/12000) First Prev Next Last Go to Page (Page:1/1) Row per Page: 10

Administrators are able to download the collected guest information by clicking "Download" button, besides, a "Delete All" button is available for deleting all the stored data. Administrator can delete all entries after export to keep the list up-to-date.

## NOTE

- When **Guest Questionnaire** is enabled, the controller collects information from the clients. Please enable Disclaimer or customized login page to include claims and reminders.

### Step2: 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 Guest Authentication Option as shown in the figure below.



Authentication Options					
Auth. Option	Auth. Database	Postfix	Default	Enabled	
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>	
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>	
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>	
Guest	FREE	N/A	<input type="radio"/>	<input checked="" type="checkbox"/>	

Consequently, after going through configurations from STEP 1 and STEP 2, end users will see that an additional section for guest access will show on the Service Zone's login page.

By typing an email address and click login, approving the terms and condition of free accessing public Wi-Fi, the guest users will be able to access the network with constraints specified in Guest Authentication Option profile and the Group profile. MAC address will be checked to avoid malicious use of free access.

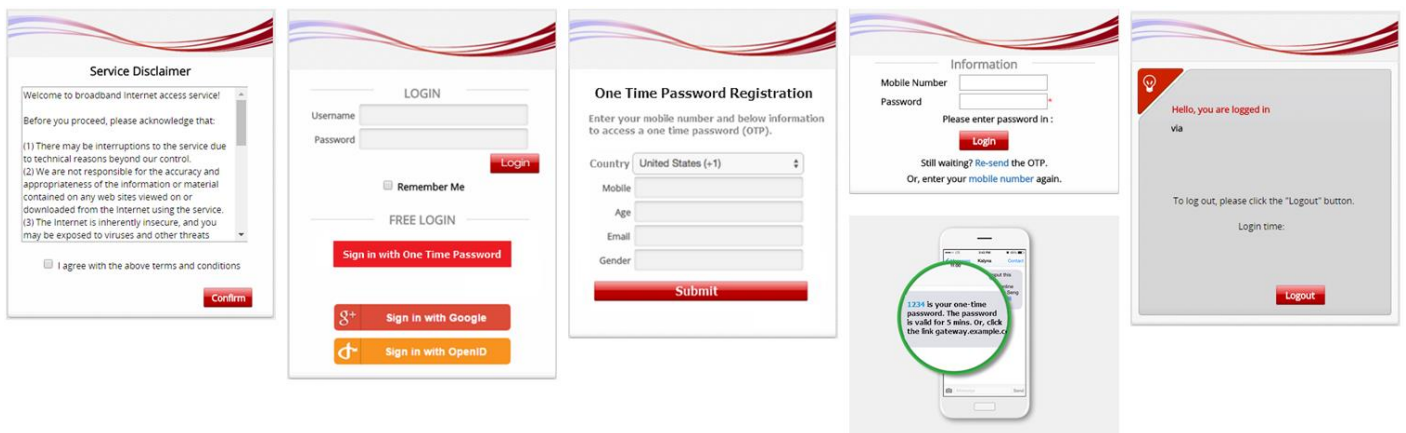
The image shows a login interface with two distinct sections. The top section is titled 'LOGIN' and contains two input fields: 'Username' and 'Password'. Below these fields is a red 'Login' button. The bottom section is titled 'FREE LOGIN' and contains an 'Email' input field. Below the email field is the text 'Enter your Email account to login for free.' and another red 'Login' button. The interface has a decorative header with blue and red wavy lines.

## 4.2.4. 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.

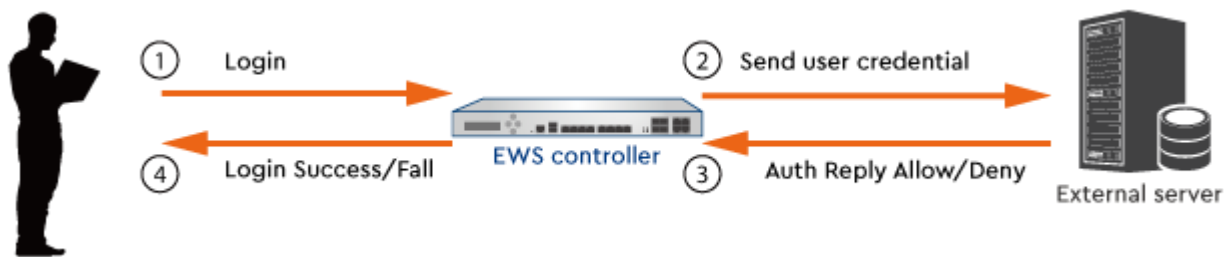
Typically, the user login flow may involve the following steps and pages:

- A. **Service Disclaimer:** (if enabled) to agree with the terms and service to continue the login process
- B. **General Login Page:** click the button of sign in with one time password
- 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



## 4.3. External Authentication Options

Most organizations have already established a centralized user account servers. Consequently, Edgecore EWS controllers are equipped with a variety of external authentication options so as to support account roaming and adapt to existing network. A simple illustration of using external authentication is shown below.



### NOTE

1. Please note that having configured the authentication options whether using built-in or external databases, they will need to be enabled in each enabled Service Zones individually.

### 4.3.1. RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. It is also the most commonly used external authentication mechanism in use today.

Configuration Path: [Main Menu >> Users >> External Authentication](#)

Server No. 2: Server 2

### External RADIUS Server Settings

---

Group	<span>Group 1</span>
Local VPN	<input type="checkbox"/> Enable Local VPN
802.1X Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username Format	<input checked="" type="radio"/> Leave Unmodified <input type="radio"/> Complete (e.g. user1@postfix) <input type="radio"/> Only ID (e.g. user1)
NAS Identifier	<input type="text"/>
NAS Port Type	<input type="text" value="19"/> *(Default 19, Range: 0~35)
Accounting Delay Time	<input type="text" value="0"/> *(Default: 0)
Service Type	<input type="text" value="1"/> *(Default: 1, Range: 1~11)
Class	<input type="text"/>
Class-Group Mapping	<input type="button" value="Configure"/>

Server 2 by default is configured to use RADIUS authentication. Edgecore EWS 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  \*(Default 19, Range: 0~35)

Accounting Delay Time  \*(Default: 0)

Service Type  \*(Default: 1, Range: 1~11)

Class

Class-Group Mapping

This shows the mapping of RADIUS class attributes to the different Groups.

DM & CoA Settings

Send Acct Interim when users' IP changes  Enable  Disable

Failover between RADIUS Servers  Enable  Disable

Attributes Priority

### Standard RADIUS Attributes

Session Timeout  Minutes \*(Range: 5-1440 mins)

Idle Timeout  Minutes \*(Range: 1-120 mins)

Acct Interim Interval  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

Bandwidth Setting

### Retransmission Settings

Number of Retries  \*(Default: 3)

Timeout  \*(Default: 6)

### Primary RADIUS Server

Authentication Server  \*(Domain Name/IP Address)

Authentication Port  \*(Default: 1812)

Authentication Secret Key

Authentication Protocol

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

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 to different groups on the Edgecore EWS controller, enabling different RADIUS accounts to be incorporated into different Groups.

### 4.3.2. POP3

POP3 is a common mail service protocol where e-mail is kept by a certain Internet server. Edgecore EWS 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.

Configuration Path: [Main Menu >> Users >> External Authentication](#)

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.

Server No. 5: Server 5

### POP3 Server Settings

Group: Group 1

Local VPN:  Enable Local VPN

Username Format:  Complete  Only ID  
Example of a Only ID username: user1.

Primary POP3 Server Settings

Server:  \*(Domain Name/IP Address)

Port:  \*(Default: 110)

SSL Connection:  Enable

Secondary POP3 Server Settings

Server:

Port:

SSL Connection:  Enable

### 4.3.3. 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.

Configuration Path: [Main Menu >> Users >> External Authentication](#)

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 Edgecore EWS controller, enabling different accounts to be incorporated into different Groups.

The screenshot shows the LDAP configuration interface. At the top, there is a 'Group' dropdown menu set to 'Group 1'. Below it is a 'Local VPN' section with an 'Enable Local VPN' checkbox. The 'Primary LDAP Server Settings' section contains the following fields: 'Server' (text input with a red asterisk and note '\* (Domain Name/IP Address)'), 'Port' (text input with a red asterisk and note '\* (e.g. 389 for LDAP, 636 for LDAPS)'), 'Service Protocol' (radio buttons for LDAP, LDAPS, and LDAP+StartTLS, with LDAP selected), 'Base DN' (text input with a red asterisk and note '\* (e.g. cn=users,dc=domain,dc=com)'), 'Binding Type' (dropdown menu set to 'User Account'), and 'Account Attribute' (radio buttons for UID and CN, with UID selected). The 'Secondary LDAP Server Settings' section has identical fields but is currently empty. At the bottom, the 'Group Mapping' section has a label 'Attribute-Group Mapping' and a 'Configure' button.

### 4.3.4. NT Domain

NT Domain option supports Windows Domain databases to perform user

credential authentication.

Configuration Path: [Main Menu >> Users >> External Authentication](#)

Server No. 3 : Server 3

### NT Domain Server Settings

Group Group 1

Local VPN  Enable Local VPN

NTDomain Server Settings Server  \*

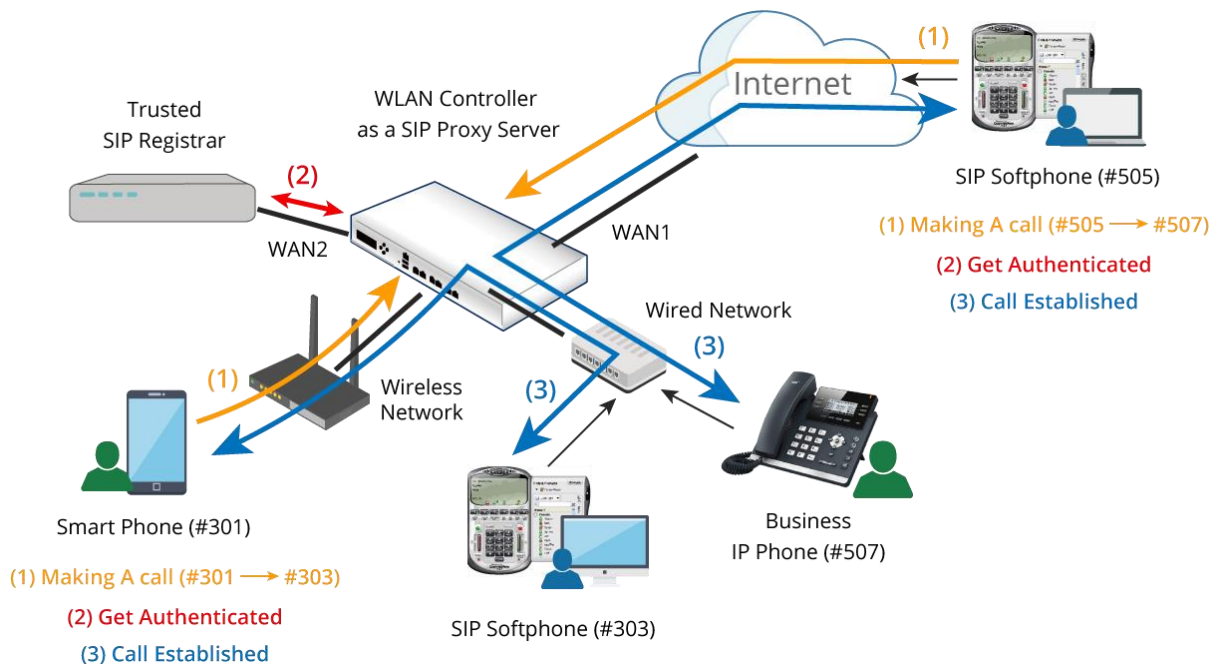
Transparent Login  Enable  Disable (Windows 2000, 2003 or above)

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. Edgecore EWS controllers support SIP authentication as well as the use of SIP phones. In addition to an Edgecore EWS 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.

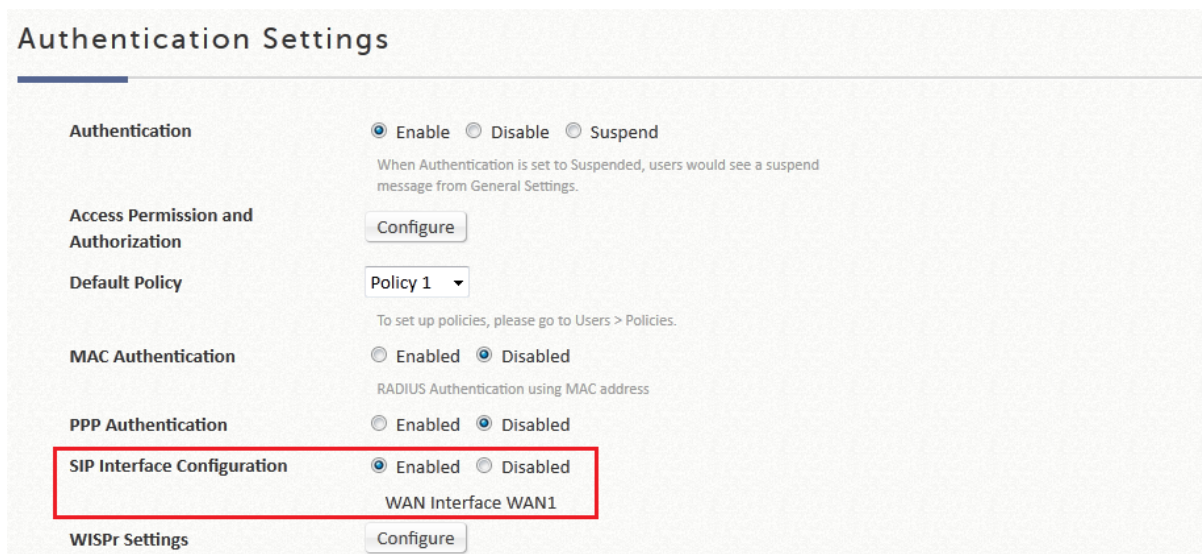
Configuration Path: [Main Menu >> Users >> External Authentication](#)

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
	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>

Please also make sure that the corresponding Service Zone also has 'Enable'

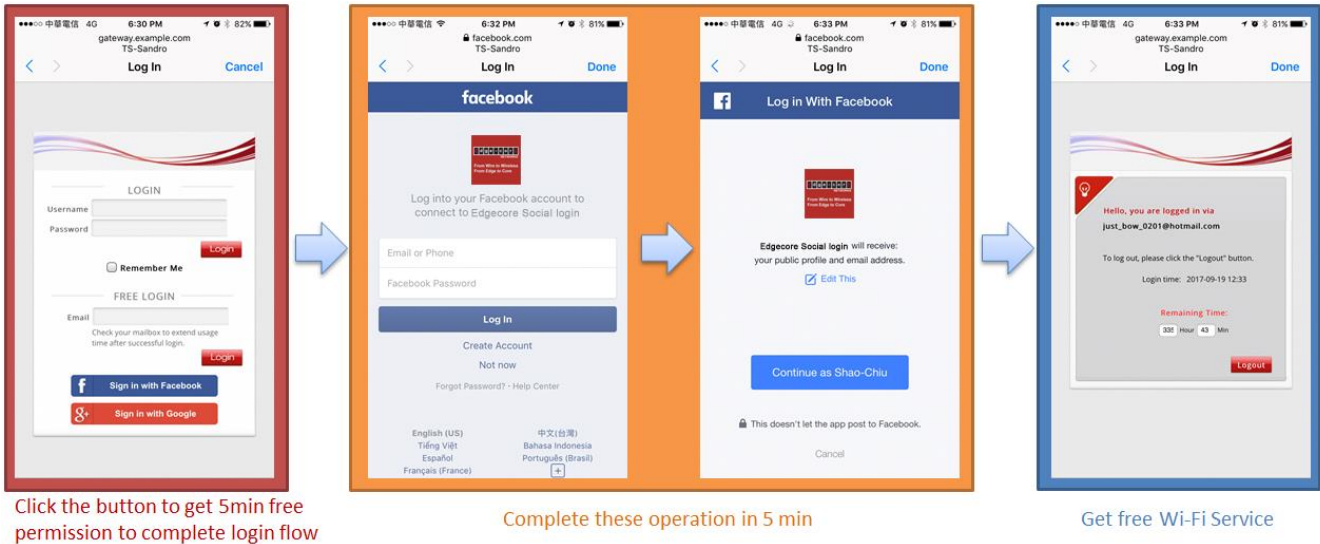
checked in the SIP Interface Configuration in order to function properly.



#### 4.3.6. Social Media

Social Media Login allows Wi-Fi users to access internet without going through a tedious account registration process. Edgecore EWS-Series Controller supports several kinds of social media accounts, LINE, Facebook, Twitter, Weibo, VK, dAccount, and Open ID. All administrators have to do is to apply the corresponding 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.



This configuration page is where how Controller to connect with social media sites.

- 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.
- Twitter: visit the website at Twitter developers site (<https://developer.twitter.com/>) and apply for "Twitter API" to get the API key and API 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.
- dAccount: visit the website at dAccount Connect site ([https://id.smt.docomo.ne.jp/src/index\\_business.html?btn01](https://id.smt.docomo.ne.jp/src/index_business.html?btn01)) and apply for getting the client ID and client secret.
- Open ID: the login path must be traversed and added into OpenID Walled Garden and the redirection target depends on OpenID provider.

## Social API Credentials

Line Login	<input type="checkbox"/>
Line App ID	<input type="text"/>
Line App Secret	<input type="text"/>
Facebook Login	<input type="checkbox"/>
Facebook App ID	<input type="text"/>
Facebook App Secret	<input type="text"/>
Twitter Login	<input type="checkbox"/>
Twitter API Key	<input type="text"/>
Twitter API Secret	<input type="text"/>
Weibo Login	<input type="checkbox"/>
Weibo App ID	<input type="text"/>
Weibo App Secret	<input type="text"/>
VK Login	<input type="checkbox"/>
VK App ID	<input type="text"/>
VK App Secret	<input type="text"/>
dAccount Login	<input type="checkbox"/>
dAccount Client ID	<input type="text"/>
dAccount Client Secret	<input type="text"/>
OpenID Login	<input type="checkbox"/>

Please use a valid and trusted HTTPS certificate when enabling dAccount login.

Apply

Cancel

# Chapter 5. Group Attributes & Policy Rules

All Edgecore EWS Controller models utilize 'Group' and 'Policy' to define user accessibility and network privileges in order to set constraints on users' behavior. Since grouping, policy setting, and service zones are intertwined with one another, this section will proceed to clarify the concepts of grouping, policy, and their relationship with the Service Zone, followed by practical setup processes on these three attributes.

## 5.1 Overview of the Concept

- **Group**



A Group is a set of users that admin considers they share some extent of similar characteristics, i.e. role based. For example, in a university, there are students, the faculty staff, and guests, 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. In the Edgecore EWS models, there are eight to twenty-four Group profiles, depending on the model capacity.

On-Demand users, Local users, may be assigned to different Groups per account. As for those who are authenticated by external servers, Edgecore EWS controllers also offer Group assignment per account for RADIUS and LDAP option

via Class-Group Mapping and Attribute-Group Mapping respectively.

In each Group profile, there are several attributes that can be defined by administrator:

1. **Quality of Service (QoS):**

Traffic class choice of Voice, Video, Best effort, and background.

Total uplink and downlink rates shared by all groups' members

Individual maximum downlink and uplink rates

2. **Privilege Profile:**

*On-Demand account privilege* to enable authenticated users of a certain Group to generate On-Demand accounts in Controller's default / template login success page.

*Password change privilege* to allow users to change their own passwords subsequent to a successful login in Controller's default / template login success page.

*Maximum Concurrent Sessions* determines the number of concurrent log-ins allowed per user.

3. **Service Zone accessibility:**

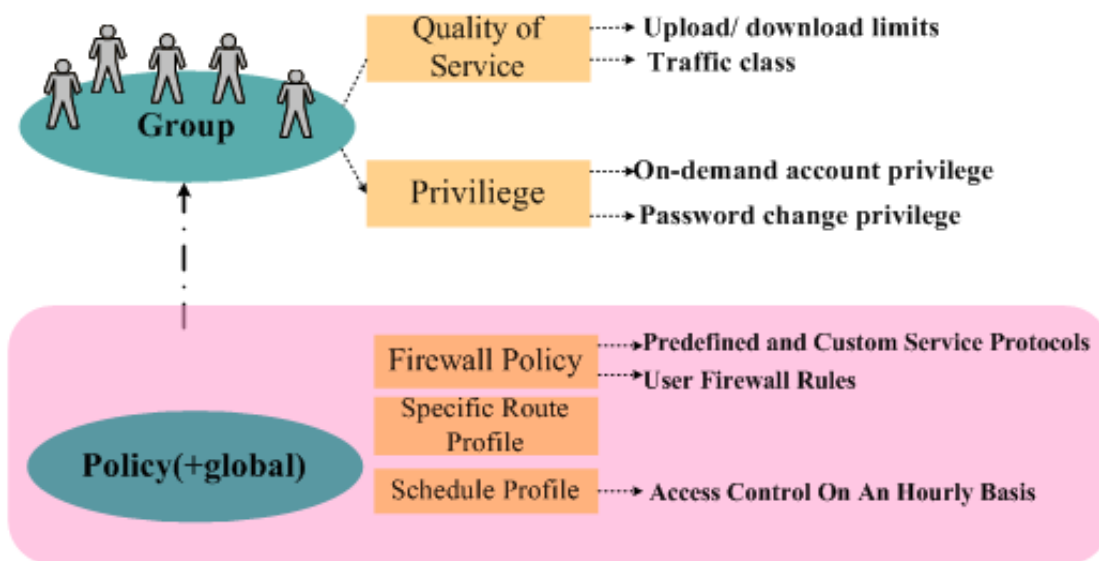
The permission to access or deny access to particular Service Zones as well as the Policy bundled may be configured.

● **Policy**

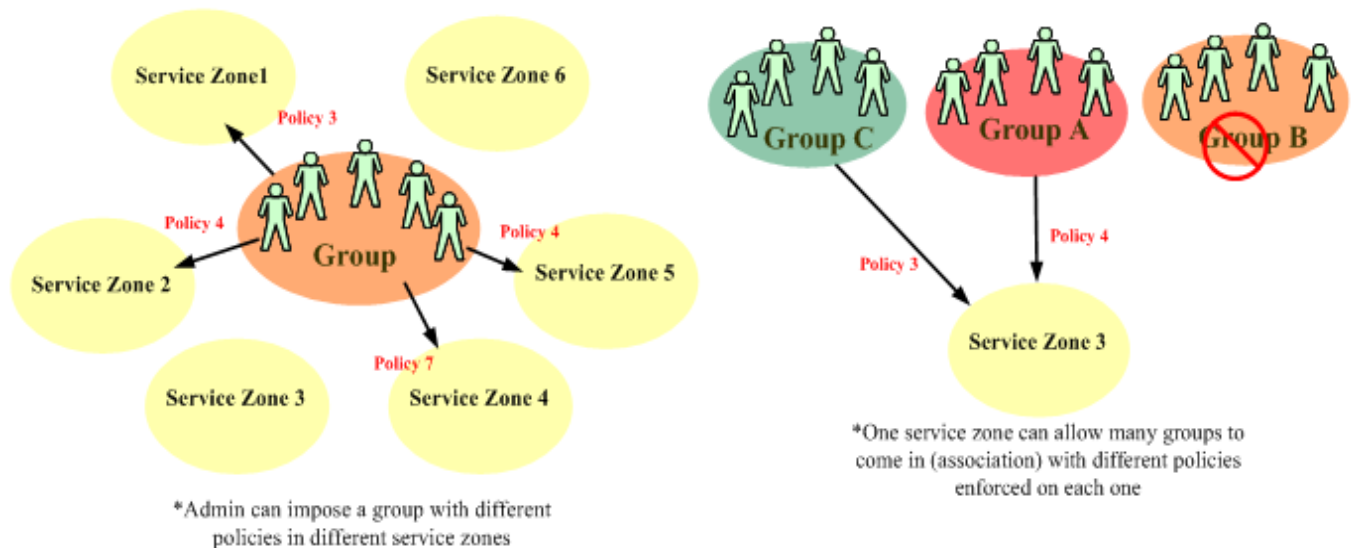
Policy, as the term suggests, are profiles of network governing constraints which are enforced upon users, including firewall rules, login schedule, routing rules and session allowances. There is a **Global** policy, which will be applied if a user belongs to a Group not bound to any Policy. The number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

Group and Policy profiles are separated for more flexibility. This allows users of the same Groups to be bound with different Policies according to Group-Service Zone permission mapping settings the administrator defines. For instance, a user from group 1 may be imposed by policy 1 in service zone 1, but policy 3 when he goes to service zone 3.

- **Relationship Between Group, Policy, and Service Zones**



The first figure displays the relationship between group and policy and the attributes that can be defined in each category. Admin can define the relationships between policy, group, and service zone from two points of view- the view of mapping groups to service zones and the other way around. Please see visual explanation below:



## 5.2 Practical Setups of Group and Policies

This section demonstrates with screenshots on how to practically set up the groups

and policies on the WMI of the Edgecore EWS Controller.

- **Group Overview**

Configuration Path: [Main Menu >> Users >> Groups >> Overview](#)

The **Group Overview** table gives a summary of which Authentication Servers are used for each corresponding Group. User Groups assigned to a Billing Plan for the On-Demand Authentication Database are also shown here.

Group Overview

Group Name	Authentication Type
Group 1	Local Billing Plan 1 Trial POP3-Server 4 RADIUS-Server 2-Default LDAP-Server 3-Default SIP-Server 1
Group 2	Billing Plan 2
Group 3	Billing Plan 3
Group 4	Billing Plan 4
Group 5	
Group 6	
Group 7	

- **Group Settings**

Configuration Path: [Main Menu >> Users >> Groups >> Configuration](#)

The **Group Configuration – Group x** table is for Policy settings to be defined for the Group. Multiple Device Login (except for On-Demand) can be enabled here.

The **Zone Permission Configuration & Policy Assignment – Group x** table enables admin to determine the relationships between Group, Policy, and Service Zones.



## Group Configuration

Select Group

Group Name

Remark

Number of devices which are allowed to login   
(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 1	Schedule 1
<input checked="" type="checkbox"/>	Service Zone : Default	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ1	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ2	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ3	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ4	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ5	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ6	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ7	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ8	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Remote VPN : IKEv2	Policy 1	Policy 1

Check the **Status** checkboxes to allow users of this Group to access the corresponding Service Zones. To configure from a Service Zone’s perspective please go to Access Permission and Authorization in Service Zone Settings.

## 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

### Default Policy

Policy 1

To set up policies, please go to Users > Policies.

### MAC Authentication

Enabled  Disabled

RADIUS Authentication using MAC address

### PPP Authentication

Enabled  Disabled

### SIP Interface Configuration

Enabled  Disabled

### WISPr Settings

Configure

### Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enable
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>

## Group Overview - SZ1

Name	Status	Time Span 1	Time Span 2	Time Span 3
Group 1	<input checked="" type="checkbox"/>	Policy 1	Policy 1	Policy 1
Group 2	<input checked="" type="checkbox"/>	Policy 2	Policy 2	Policy 2
Group 3	<input checked="" type="checkbox"/>	Policy 3	Policy 3	Policy 3
Group 4	<input checked="" type="checkbox"/>	Policy 4	Policy 4	Policy 4
Group 5	<input checked="" type="checkbox"/>	Policy 5	Policy 5	Policy 5
Group 6	<input checked="" type="checkbox"/>	Policy 6	Policy 6	Policy 6
Group 7	<input checked="" type="checkbox"/>	Policy 7	Policy 7	Policy 7
Group 8	<input checked="" type="checkbox"/>	Policy 8	Policy 8	Policy 8
Group 9	<input checked="" type="checkbox"/>	Policy 9	Policy 9	Policy 9

## ● Policy Settings

Configuration Path: [Main Menu >> Users >> Policies >> Policy Configuration](#)

1. **Select Policy** allows administrator to choose which Policy Profile to configure.
2. **Firewall Profile** is for defining service protocols, user firewall rules, and IPv6 firewall rules.
3. **Privilege Profile** configures the On-Demand Account creation, Password change privileges and Maximum concurrent sessions.
4. **QoS Profile** allows administrator to edit traffic configuration.
5. **Specific Route Profile** is where the administrator may statically assign routing nodes to forward traffic to a certain destination.

6. *IPv6 traffic class and 802.1p mapping* (for global policy only) - to map IPv6 traffic class to 802.1p when IPv6 traffic is being forwarded into VLAN IPv4 networks.

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.

- **Schedule**

Configuration Path: [Main Menu >> Users >> 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 Name:

	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
<input type="checkbox"/>	SUN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	MON	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	TUE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	WED	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	THU	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	FRI	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	SAT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Log off authenticated users during unauthorized periods

Defined Schedules are then applied in Group Configuration.

- **Grouping Users**

A Group is determined by authentication servers, class (RADIUS), attribute (LDAP),

or accounts individually (Local, On-Demand).

Generally a Group is assigned to all users of an authentication option

Users > Authentication > Auth Option > Group


**However, there are the following flexibilities:**

- Local accounts may be assigned a Group per account individually upon creation or from the following path for existing accounts Users > Authentication > Local > Configure > [Local User List](#) > [username](#) (There is an **Applied Group** row for admin to determine the attribute)
- On-Demand accounts may be assigned a Group per account individually upon creation.
- RADIUS users can have users assigned to different Groups based on RADIUS class. The mapping can be configured at Users > Authentication > RADIUS > Configure > [Class-Group Mapping](#) > [Configure](#)
- LDAP users can have users assigned to different Groups based on LDAP attributes, the mapping can be configured at Users > Authentication > LDAP > Configure > [Map LDAP Attributes to Group](#)

● **Policy Priority**

Policy can be configured at Group-Service Zone permission mapping and Service Zone profile.

## Authentication Settings

<b>Authentication</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> Suspend <small>When Authentication is set to Suspended, users would see a suspend message from General Settings.</small>
<b>Access Permission and Authorization</b>	<input type="button" value="Configure"/>
 <b>Default Policy</b>	Policy 1 ▾ <small>To set up policies, please go to Users &gt; Policies.</small>
<b>MAC Authentication</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <small>RADIUS Authentication using MAC address</small>
<b>PPP Authentication</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<b>SIP Interface Configuration</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<b>WISPr Settings</b>	<input type="button" value="Configure"/>

The Policy enforcement priority is as follows:

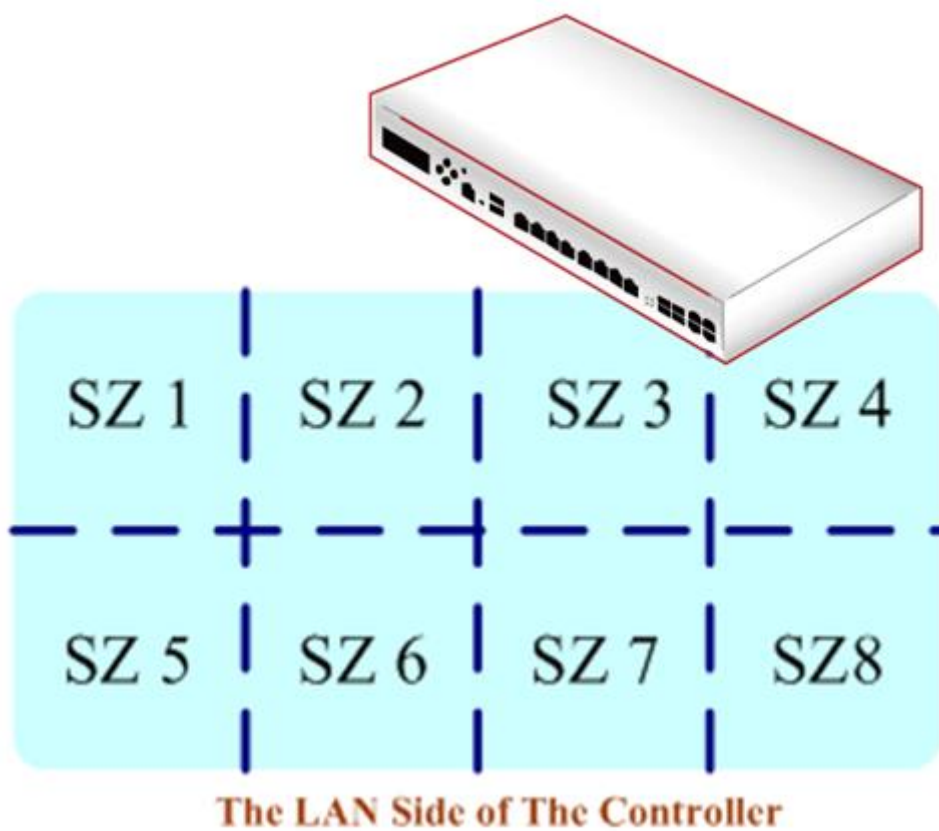
Group-Service Zone Mapping > Service Zone default Policy > Global Policy

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.

# Chapter 6. Basic Service Zone Configuration

## 6.1 The Concept of Service Zone

Service Zones are virtual partitions of the physical LAN side of an 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 and an SSID with its Service Zone, administrator can flexibly separate the wired and wireless networks easily.



## 6.2 Service Zone Setup

### 6.2.1. NAT Mode or Router Mode

Configuration Path: [Main Menu >> System >> Service Zones >> Configure](#)

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.

### 6.2.2. Service Zone Network Interface

Configuration Path: [Main Menu >> System >> Service Zones >> Configure](#)

**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.

There are 3 isolation options : **Inter-VLAN Isolation**, **Clients Isolation**, and **None**.

- 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 EWS may be shut down if the switch has loop protection enabled and there are more than 2 VLANs belong to one Service Zone.

**NOTE**

1. Default Service Zone can't be disabled.

### 6.2.3. DHCP Server options

Configuration Path: [Main Menu >> System >> Service Zones >> Configure](#)

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. Edgecore EWS Controllers supports independent DHCP settings for each Service Zone profile. Options include Disable DHCP option, Enable built-in DHCP server or DHCP Relay.

DHCP

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	<input checked="" type="checkbox"/>	Scope 1	192.168.1.1	192.168.1.100	192.168.1.254		domain.com	1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
2	<input type="checkbox"/>	Scope 2						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
3	<input type="checkbox"/>	Scope 3						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
4	<input type="checkbox"/>	Scope 4						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
5	<input type="checkbox"/>	Scope 5						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
6	<input type="checkbox"/>	Scope 6						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Reserved IP Address List

DHCP Lease Protection  Enable  Disable

1. DHCP Server Configuration – The default setting for DHCP Server is “Enable”. Select other options from the drop-down list.
2. Define the IP range for issuing when using Enable DHCP Server (built-in). There are a total of six DHCP pools for configuration.
3. DHCP Lease Time at each pool cannot be smaller than the twice value of Idle



Timeout.

4. 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.
5. 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.
6. Click "Apply" to activate changes.

#### **6.2.4. Authentication Options**

Configuration Path: [Main Menu >> System >> Service Zones >> Configure](#)

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.

##### **1. Databases**

Administrator 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.

Authentication Options					
Auth. Option	Auth. Database	Postfix	Default	Enabled	
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>	
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>	
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>	
Guest	FREE	N/A	<input type="radio"/>	<input type="checkbox"/>	
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>	
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>	

## 2. 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.

### 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

Default Policy    
To set up policies, please go to Users > Policies.

Portal URL  Specific  Original  None  
   
(e.g. http://www.example.com)

MAC Authentication  Enabled  Disabled  
RADIUS Authentication using MAC address

PPP Authentication  Enabled  Disabled

SIP Interface Configuration  Enabled  Disabled

WISPr Settings

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>

## 3. MAC address 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.

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

Default Policy Policy 1 ▾  
To set up policies, please go to Users > Policies.

Portal URL  Specific  Original  None  
 \*  
(e.g. http://www.example.com)

**MAC Authentication**  Enabled  Disabled  
RADIUS Authentication using MAC address

PPP Authentication  Enabled  Disabled

SIP Interface Configuration  Enabled  Disabled

WISPr Settings

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input type="radio"/>	<input checked="" type="checkbox"/>

#### 4. PPP dial-up 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.

## 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**

**Default Policy** Policy 1 ▾  
To set up policies, please go to Users > Policies.

**MAC Authentication**  Enabled  Disabled  
MAC Auth Server Server 2(radius) ▾  
RADIUS Authentication using MAC address

**PPP Authentication**  Enabled  Disabled

Assign IP Address From 172.50.0.1

Authentication Options

Auth Option	Auth Database	Postfix	Enable
Local	LOCAL	local	<input checked="" type="checkbox"/>
Server 2	RADIUS	radius	<input type="checkbox"/>

The **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.

### 6.2.5. Captive Portal Customization

Configuration Path: [Main Menu >> System >> Service Zones >> Configure](#)

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.

### Login Page Customization

Service Disclaimer	Default	<input checked="" type="radio"/> Default <input type="radio"/> Customize with Template <input type="radio"/> Upload Your Own <input type="radio"/> Use External Page
General Login Page	Default	Enable Disclaimer <input type="checkbox"/> <input type="button" value="Preview"/>
PLM Open Type Login Page	Default	
PMS Billing Plan Selection Page	Default	

---

### Theme for Template

Button Color:  Grey  Orange  Green  Blue  Black

Upload Logo:  No file selected.  
 No File

The recommended dimension of the image is 360x120 with a size limit of 512 kB. It will be adjusted if the dimension does not fit.

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

**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 an 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 Appendix C of the User Manual.

**Editor:** The Login Page can be edited with a What You See Is What You Get (WYSIWYG) editor. With the editor, administrator can add, delete, or configure the elements in the page in a simple and intuitive way. Currently, this option is only available for General Login Page.

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

Message Page Customization

Login Success Page	Default
Login Success Page For On-Demand Users	Default
Login Failed Page	Default
Device Logout Page	Default
Logout Success Page	Default
Logout Failed Page	Default
Online Device List	Default

Default  Customize with Template  Upload Your Own  Use External Page

Preview

Apply Cancel

# Chapter 7. Basic AP Management

## 7.1. Introduction

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.

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

Manageable Edgecore Access Points for Wide Area AP Management may be checked at:

[Main Menu >> Devices >> Wide Area AP Management >> Overview.](#)

AP List

Type: All  
Status: All  
Tunnel: None  
Name: [ ] Search

Refresh Interval: Disable Auto Refresh Refresh

Add Delete Add to Map Backup Config Restore Config Upgrade Apply Settings Reboot Export

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
------	------	----	-----	-----	----------	--------	------------	--------	--------------	--------	---------	---------------

(Total 0) First Prev Next Last Go to Page Row per Page 20

Individual AP configuration is very time consuming and impractical when it comes to large scale AP deployments.

Under Wide Area AP Management, there also are templates for the administrator to configure AP by central management.

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.

#### NOTE

1. Before the adding of AP's to any service zone, admin should set up a general wireless environment for the zone in advance, which will be only be applied to Locally managed APs.
  2. Each AP will also be assigned one distinctive IP address once under management.
- 

## 7.2 Wide Area AP Management

Configuration path: [Main Menu >> Devices >> Wide Area AP Management](#)

This section goes on to explain how to centrally manage the access points on the WAN from an Edgecore EWS controller. 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 3<sup>rd</sup> party AP devices.
- CAPWAP support, complete tunnel and split tunnel.

An Overview of Wide Area Managed Access Points is available on the AP List.



Configuration path: [Main Menu >> Access Points >> Wide Area AP Management >> AP List](#)

AP List

Type  Status  Tunnel

Name

Refresh Interval

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
------	------	----	-----	-----	----------	--------	------------	--------	--------------	--------	---------	---------------

(Total 0)     Go to Page  Row per Page

**NOTE**

1. Wide Area AP Management can be used to manage APs physically deployed on the WAN side and LAN side of the controller.

### 7.2.1. Adding an Access Point

Configuration path: [Main Menu >> Access Points >> Wide Area AP Management >> AP List >> Add](#)

The Adding page allows administrator to directly add a single Access Point to the management list regardless of its Status. Simply configure the device’s IP address, name and login credentials, set a SNMP community string and click the Apply button.

Add Method **Add an AP** ▼

### Add an AP

---

Device Type	ECW100 ▼
Device IP	<input type="text"/> *
Device Name	<input type="text"/> *
Login ID	admin *
Password	admin *
SNMP Community	public *
SNMP Write Community	private *
Map	Overview ▼

## 7.2.2. AP Discovery to find Multiple Access Points

Configuration path: [Main Menu >> Access Points >> Wide Area AP Management >> AP List >> Add](#)

With the AP Discovery feature, administrator can scan for APs regardless of their physical location as long as their IP addresses can be reached. An IP scanning range may be configured. Select the target Device Type, define the scan IP range and Admin Settings, and then click "Discover". After the discovery process, newly found AP's will be listed under Device Results where the administrator can specify the individual AP's Device Name and SNMP Community string. Select and click the Add button and the discovered APs will be added into List.

## Discovery AP

Discover

Device Type

ECW5211-L

Admin Settings Used to Discover

Start IP Address

End IP Address

Login ID

Password

## Device Results

Add

Delete

	Device Type	IP Address	Device Name	SNMP Community
--	-------------	------------	-------------	----------------

### 7.2.3 AP Configuration with Templates

Configuration with templates is supported on selected models for Wide Area AP Management.

Configuration path: [Main Menu >> Devices >> Wide Area AP Management >> Template](#)

## Template AP Setting

Select Product Type	Legacy	▼
Select Template	1: Template 1	▼
Template Name	Template 1	Apply
Country	USA	▼
General Settings	Configure	
VAP Configuration	Configure	
Security Settings	Configure	
Advanced Wireless Settings	Configure	
Hotspot 2.0 Settings	Configure	
Firewall Settings	Configure	
Linkyfi's Location Engine	Configure	
Copy Settings to	None	▼ Apply

Templates are available and all functions configurable for wireless on the access point can be configured from the template. For more details on the number of Templates of each model hardware, please refer to Appendix A of the User Manual.

There are two product types of templates which can be selected: **Legacy** and **New Generation**.

- **Legacy**

**General Settings** on the Access Point include basic wireless settings such as the Band, Channel, Transmit Power, Transmit Rates and etc. **VAP Settings** allows the administrator to enable/disable a VAP, designate an ESSID, and assign VLAN ID with/ without corresponding tunnel if needed. Configure **Security Settings**, such as WEP, 802.1X, WPA-Personal, and WPA-Enterprise if needed. **Advanced Wireless Settings** allows the administrator to fine-tune performance and efficiency on the Access Points to maintain good wireless connection quality for associated clients. **Hotspot 2.0 Settings** is for supporting roaming between WLAN networks of different service provider. In **Firewall Settings**, proxy ARP feature is allowed to be enabled/disabled. As for **Linkyfi's Location Engine**, RTLS and DPI DNS can be enabled to integrate with Linkyfi Location Engine for user tracking.

Template AP Setting

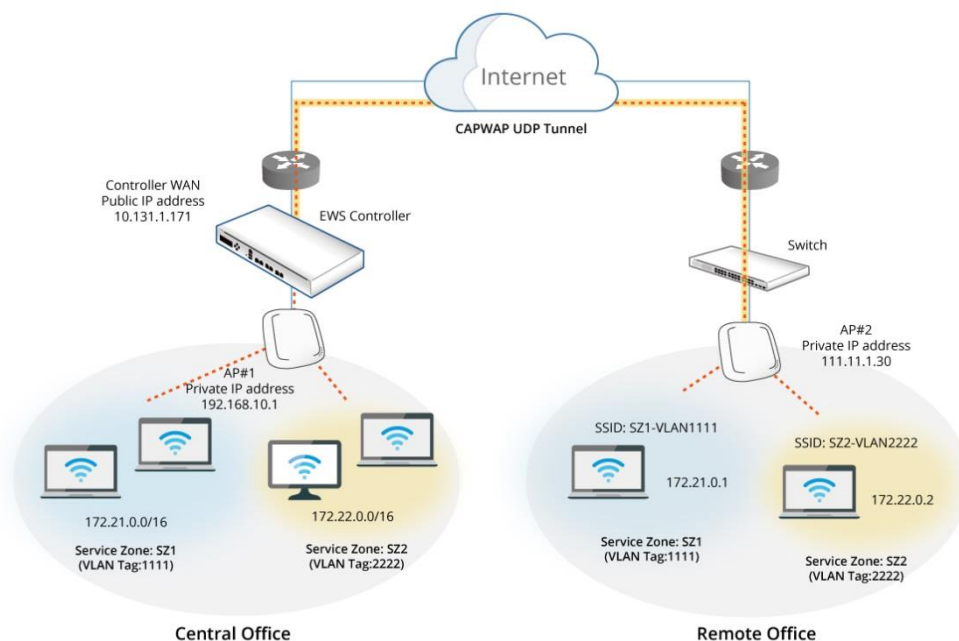
Select Product Type	New Generation	
Select Template	10: Template 10	
Template Name	Template 10	Apply
Country	United States	
Radio	Configure	
Wireless Network	Configure	
VLAN Settings	Configure	
Services	Configure	
Copy Settings to	None	Apply

- **New Generation**

**Country** is to select the same country code as access point. **Radio** on the Access Point include basic wireless settings such as the Band, Channel, Transmit Power and etc. **Wireless Network** allows the administrator to enable/disable a VAP, designate an SSID, and assign security such as WPA-Personal/Enterprise, WPA2-Personal/Enterprise, WPA3 Personal/Enterprise, WPA3 Personal/Enterprise Transition, WPA3 Enterprise 192-bit, and OWE if needed. **VLAN Settings** is for creating VLAN Id to be used into the SSID. In **Services**, iBeacon is allowed to be enabled/disabled.

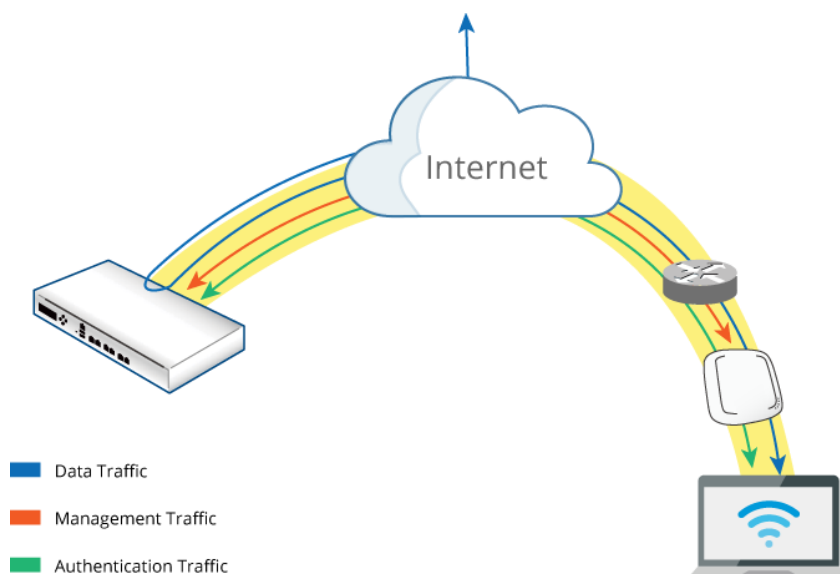
### 7.2.4 AP auto Discovery and Configuration using CAPWAP

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

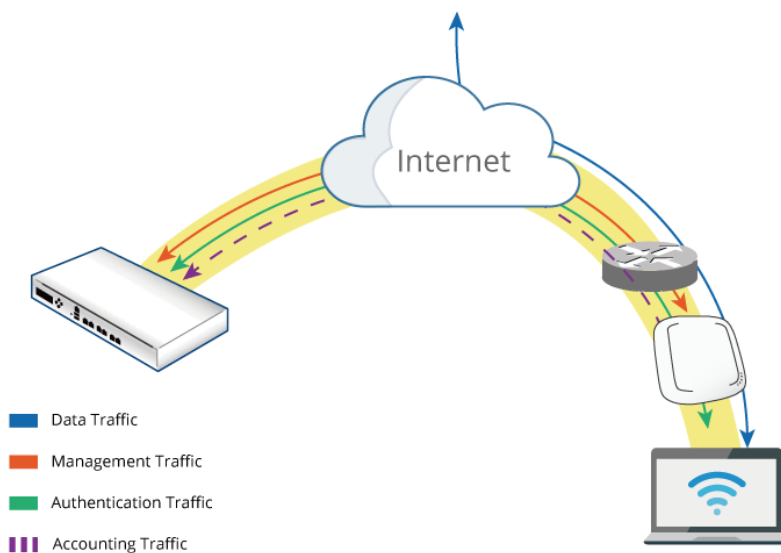


**Complete Tunnel** uses the CAPWAP protocol to communicate with an Access Point so that all management traffic, authentication traffic and data traffic from the service area AP provided are transmitted back to the Controller, before forwarding data traffic to the internet. The EWS Controller is able to implement role-based

policies over Layer 3 networks, with user access control available in the remote sites. This feature allows the Edgecore EWS Controller to fully support centralized AP management and user management.



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.



### Configuration Steps:

1. On the Edgecore controller: Enable CAPWAP from [Main Menu >> Devices >> Wide Area AP Management >> CAPWAP](#)

2. Make sure that the Controllers' CAPWAP settings uses a security certificate that is issued by the same CA. For information on Certificate management on the controller please refer to the subsequent chapter in this guide.

Main > Device Management > Wide Area AP Management > CAPWAP

### CAPWAP Configuration

CAPWAP Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Apply Certificate to APs	DEFAULT ▾
Trusted Certificate Authority(CA)	DEFAULT ▾
IP Address For Control Channel	100.64.145.254
IP Netmask For Control Channel	255.255.255.0 (253) ▾
Control Channel IP Range	100.64.144.1 ~ 100.64.145.253

3. Upload the necessary security certificate into the AP in order for the Controller to validate CAPWAP discovery and join requests.
4. Configure the CAPWAP template from VAP Settings in the Template. VAP traffic may be selected to be tunneled back to the controller's enabled SZ profile. There are three types of tunnel interfaces. **Disabled** doesn't establish any tunnel, **Complete Tunnel** creates the tunnel that transfers all data back to the Controller, while **Split Tunnel** collects only management traffic and authentication traffic back for the Controller. Only the latter two tunnel interface require the administrator to select mapping Service Zones for each VAP.

### VAP Configuration - 1: Template 1

Profile Name	RF Card A : VAP-1
VAP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Profile Name	VAP-1
ESSID	4ipnetAP-A1
Network Mode	Bridge
Uplink Bandwidth	0 Kbits/s *(1-1048576, 0:Disable)
Downlink Bandwidth	0 Kbits/s *(1-1048576, 0:Disable)
VLAN ID	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
	VLAN ID 1234 *( 1 - 4094 )
CAPWAP Tunnel Interface	Split Tunnel
<b>Service Zone</b>	Default
Service Schedule	24/7 Service
Access Control Type	<input checked="" type="radio"/> Disable <input type="radio"/> MAC ACL Allow List <input type="radio"/> MAC ACL Deny List

5. On the AP side: Enable the CAPWAP function from System >> CAPWAP, where the administrator will see several discovery methods to be activated, namely:

(1) **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.

(2) **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 Edgcore EWS controller it is trying to connect.

(3) **Broadcast Discovery**

The AP sends broadcast requests to all the IP addresses in a subnet. Edgcore EWS 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.

(4) **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.

### (5) Static Discovery

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 Edgecore EWS controller you want this AP to join to.

Successful CAPWAP joining will lead to the AP being listed in the managed AP list, as illustrated below:

CAPWAP column will display a 'RUN' status, and the tunnel status will show a clickable 'edit' button in black if a VAP is configured to be tunneled back to the controller.

The screenshot shows the 'AP List' management interface. It includes filter dropdowns for Type, Status, Map, and Tunnel, and a search box. Below the filters are buttons for 'Add', 'Delete', 'Add to Map / Floor Plan', 'Backup Config', 'Restore Config', 'Upgrade', 'Apply Settings', 'Reboot', and 'Export'. A table lists APs with the following data:

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
ECW100	ECW100_AP1	10.131.7.38	00:11:22:33:44:55	MAP1	1	Online	0	Edit	System Overview Go	RUN	3.45.0000	EC1234567890

AP WMI will show with the VAP enabled and tunnel status as well 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

The VAP Configuration on the AP WMI also displays which kind of CAPWAP Tunnel Interface is operation in different VAP.

System

Wireless

Firewall

Utilities

Status

VAP Overview

General

VAP Config

Security

Repeater

Advanced

Access Control

Hotspot 2.0

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 ▼

SAVE
CLEAR

## NOTE

1. AP tunnels will be established automatically when the CAPWAP template has selected VAP to be enabled and tunneled back to a SZ.
2. If the CAPWAP discovery process fails, please check the certificate settings used on the Controller and the certificate uploaded into the AP.

3. Controllers CAPWAP Log may be referenced during trouble shooting process.

## 7.2.5 Tunneler VAP Location Mapping Setup

Configuration path: [Main Menu >> Devices >> Wide Area AP Management >> 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:  Search

Refresh Interval: Disable Auto Refresh Refresh

Add Delete Add to Map Backup Config Restore Config Upgrade Apply Settings Reboot Export

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
ECW5211-L	ECW5211-L	10.71.36.55	00:1F:D4:07:42:CD	Overview	1	Online	0	<a href="#">Edit</a>	System Overview Go	RUN	3.45.0000	EC1912000687

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

### ECW5211-L: VAP Status

RF1				
Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
VAP-1	ECW5211-L-A1	1000	<a href="#">Configure</a>	Default
RF2				
Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
VAP-1	ECW5211-L-B1	1000	<a href="#">Configure</a>	Default

### Tunnel Port Location Mapping Setup

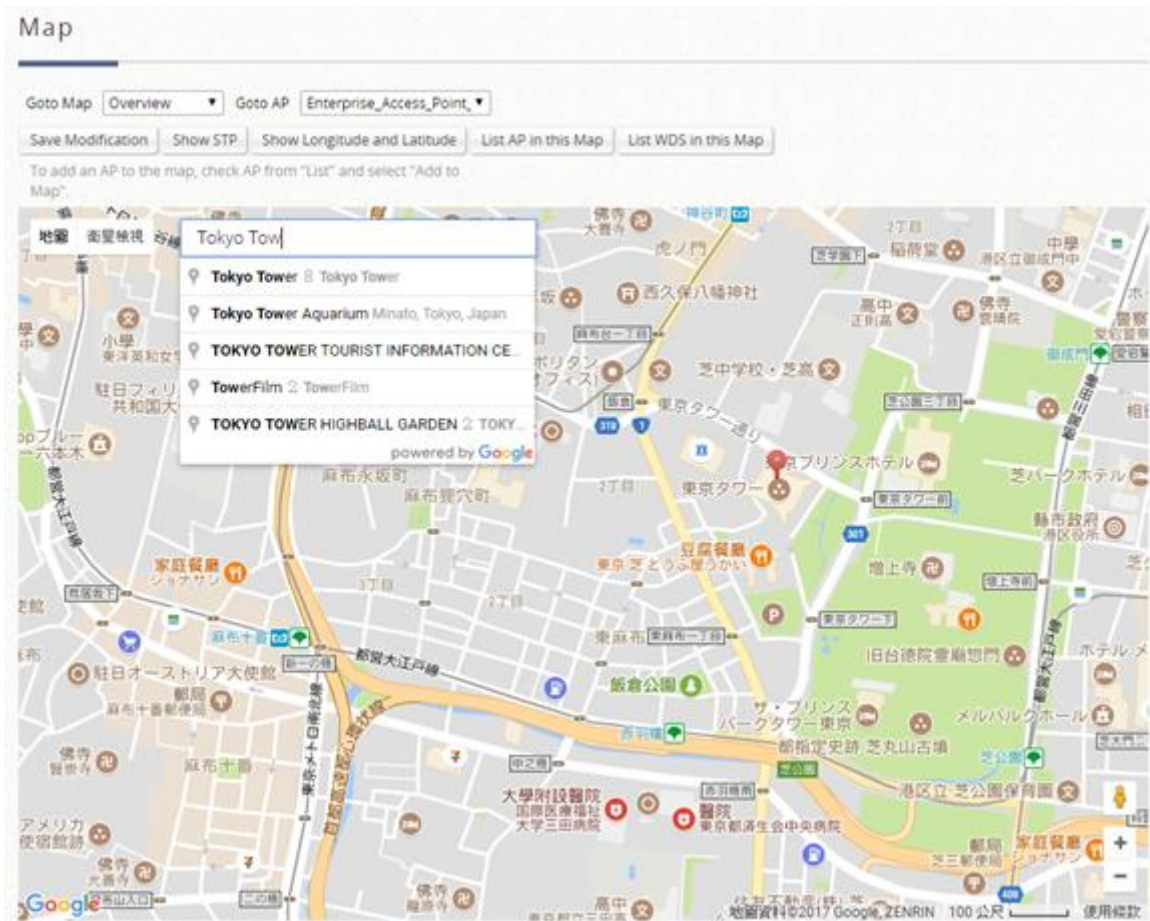
Service Zone / Prefer DHCP Pool	Default / <input type="text" value="None"/>
User Limitation	<input type="text"/> (Blank is for unlimited.)
ESSID	ECW5211-L-A1
Room Number / Location ID	<input type="text"/> *
Room Description / Location Name	<input type="text"/>
NAS Identifier	<input type="text"/>
Class	<input type="text"/>
HTTP Parameter	<input type="text"/>

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.

## 7.2.6 Access Points Monitoring on Google Map

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:



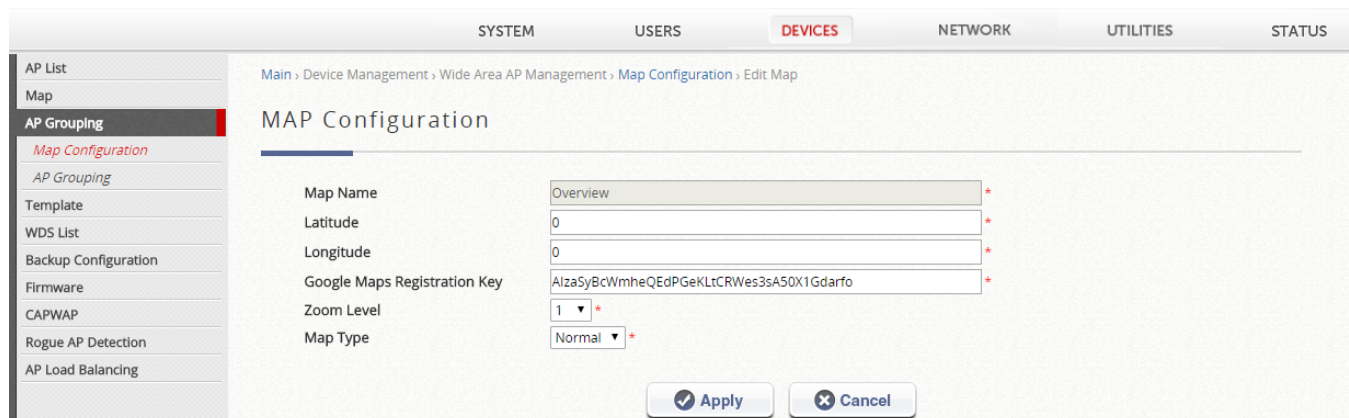
Here is the procedure to create a Map:

- 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.

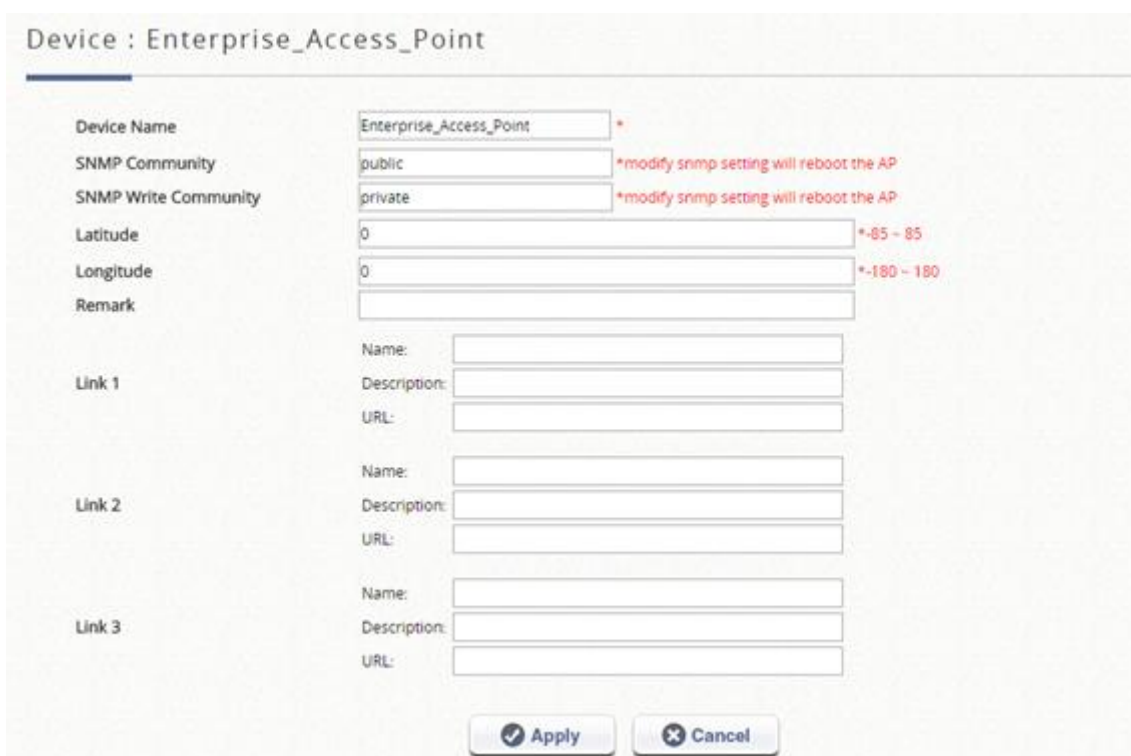
Before starting to add a new map in Wide-Area AP Management, it is necessary to sign up for a Google account. This account will be used to apply for a Google Maps API v3 key. For more details, please follow the instructions from Google at <https://developers.google.com/maps/documentation/javascript/v2/introduction> to

obtain Maps API v3 key. The key info into the field of "Google Maps Registration Key" under Map Configuration page.



In this Map Configuration page, you can also configure the Map Name for this map and its geographical location as defined by Longitude and Latitude, choose the Zoom Level and Map Type to be displayed.

To add APs to a map, firstly you have to go to the AP List and click the AP name to define the latitude and longitude of the APs. The latitude and longitude should be around the location of the target map. In this page, administrator can also set up links and remarks to be shown on the map for each AP.



After defining the location for each AP, return to the AP List page. Select 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  
 Map: None  
 Tunnel: None  
 Name:  Search

Refresh Interval: Disable Auto Refresh Refresh

Add Delete **Add to Map / Floor Plan** Backup Config Restore Config Upgrade Apply Settings Reboot Export

	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
<input checked="" type="checkbox"/>	ECW5211-L	ECW5211-L	10.71.36.55	00:1F:D4:07:42:CD	Overview	1	Online	0	Edit	System Overview Go	RUN	3.45.0000	EC1912000685

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

Add to Map / Floor Plan

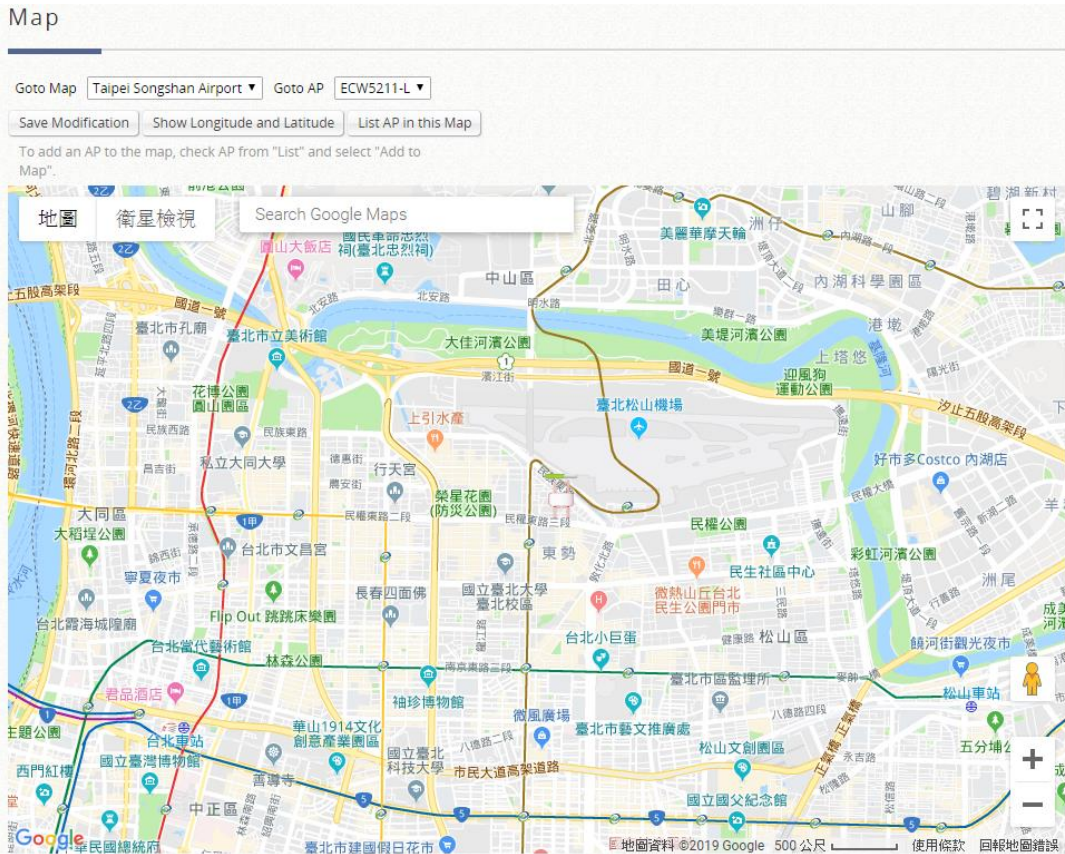
Add AP(ECW5211-L)

Add into a map  
 Select Map: Taipei Songshan Airport

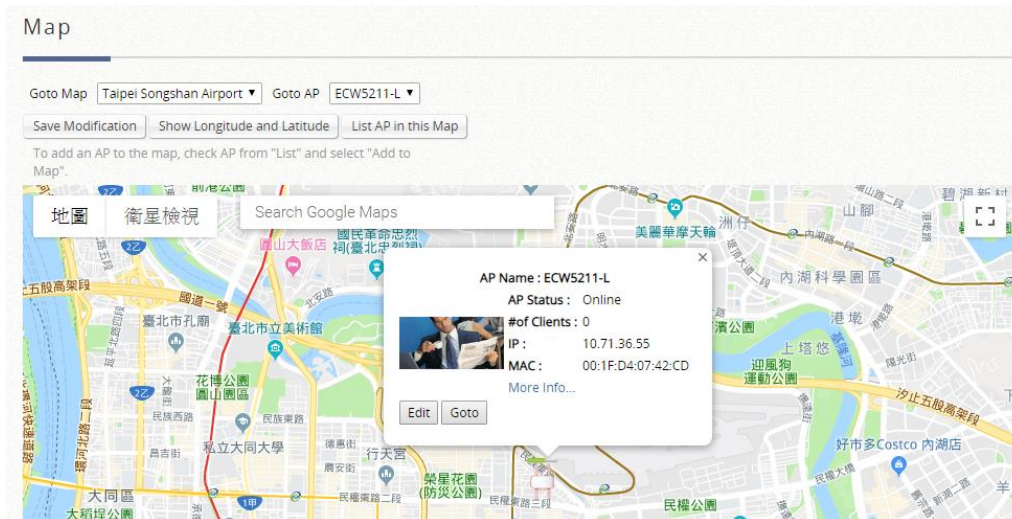
Add into a floor plan  
 Floor Plan Name: Select an Option

Apply Cancel

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



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.





Map

Goto Map  Goto AP

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

**AP Detail Status** ✕

AP Link   AP Statistic   **AP Status**   Client List

AP Status : ECW5211-L		
General	Type	ECW5211-L
	Name	ECW5211-L
	IP Address	10.71.36.55
	MAC Address	00:1F:D4:07:42:CD
	Version	3.45.0000
	Status	Online
System	Last Report Time	2019/07/24 16:07:25
	Uptime	22:06:31
	CPU Idle	95%
	Memory Usage	49%
	# of Radio Card	2
Network	TX Byte Count	145567
	RX Byte Count	0
	TX Packet Count	395628
	RX Packet Count	0

## NOTE

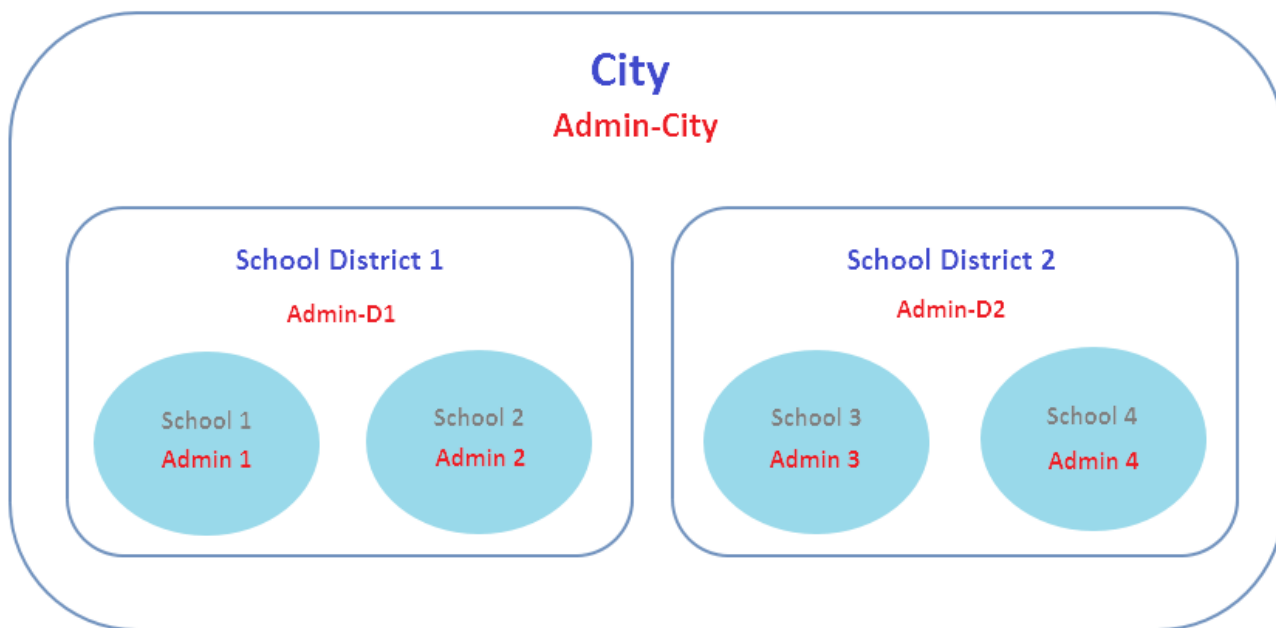
1. The "Overview" map is the default map of the system. This map provides an overview for all managed APs.
2. When an AP is added to the managed list, it belongs to "Overview" map.
3. After an AP is added to a map, it can still be monitored in the "Overview" map.

## 7.2.7 AP Grouping

Configuration path: [Main Menu >> Devices >> Wide Area AP Management >> AP Grouping >> Map Configuration](#)

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.



【A simple concept diagram illustrating AP Grouping】

To use AP grouping function, go to [Main Menu >> Devices >> Wide Area AP Management >> AP Grouping >> AP Grouping List](#) to add or delete the AP group.

## AP Grouping

<input type="checkbox"/>	AP Group	Map	Template
<input type="checkbox"/>	456	123	<input type="radio"/> 1 <input type="radio"/> 3 <input type="radio"/> 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

\*

Map

Selectable

Selected

Overview
123

Template

Selectable

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.

## Administrator Group List

Add Del

<input type="checkbox"/>	name	remark
<input type="checkbox"/>	Super Group	remark
<input type="checkbox"/>	Manager	remark
<input type="checkbox"/>	Operator	remark
<input type="checkbox"/>	On Demand	remark
<input type="checkbox"/>	Custom 1	remark
<input type="checkbox"/>	Custom 2	remark
<input type="checkbox"/>	Custom 3	remark

### Assigning permission to an AP group.

	Disabled	SZ7
	Disabled	SZ8
<b>AP GROUP</b>	Disabled	Select All
	Disabled	456
	Read Only	
	Read/Write	
	Disabled	Select All
<b>AP Management</b>	Disabled	Local Area AP Management
	Disabled	Wide Area AP Management
<b>Switch Management</b>	Disabled	

## 7.2.8 Rogue AP Scanning

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. Go to [Main Menu >> Devices >> Enter Local Area AP Management >> Rogue AP Detection](#) to set up the function. Admin should then determine the scanning interval, select an AP for the scanning job as sensors, and 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.

The screenshot shows a web interface with two main sections. The top section, titled "General Configuration", contains several settings: "Rogue AP Detection" with radio buttons for "Enable" and "Disable" (selected), an "Apply" button, "Scanning Interval" with a text input set to "0" and the label "minutes", "Channel Switching" with radio buttons for "Enable" and "Disable" (selected), "Sensor List" with a value of "0/0" and a "Configure" button, and "Trusted APs" with a value of "0/40" and a "Configure" button. The bottom section, titled "Rogue AP List", features "Add to Trusted AP List" and "Delete" buttons, an "ESSID" dropdown menu, a search input field, and a "Search" button. Below this is a table with the following headers: a checkbox, "No", "Rogue AP BSSID", "ESSID", "Type", "Channel", "Encryption", "RSSI", and "Report Time". At the bottom of the table area, there is a status bar showing "(Total:0)", navigation links "First Prev Next Last", a "Go to Page" dropdown, "(Page:1/1)", and "Row per Page: 10" with a dropdown arrow.

The discovered access points are temporarily put in the Rogue AP list. Click on one of the hyperlinked BSSID's to see its detailed information. However, if admin recognizes 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**.

## 7.2.9 AP Load Balancing Feature

It is a function to prevent managed APs from overloading. When the system detects the occurrence of APs' associated-client numbers or network traffic exceeding a predefined threshold at circumstances and other APs in the same cluster 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 would increase chances for other available APs to be associated. The system can divide the managed APs into clusters; define the threshold, and a time interval which will trigger the AP load balancing.

Wide Area AP Management feature also supports the clustering of various managed

APs and perform transmit power management to spread the network load as evenly as possible among APs of the same cluster.

The administrator can specify the criteria under which AP load balancing feature will be enforced. The attributes that can be customized for creating your own load balancing initiation criteria includes the enforcement interval and the associated client or traffic threshold.

The image shows two configuration pages from a network management interface. The top page is titled "WAPM Load Balancing" and contains the following settings:

- Load Balancing:** Radio buttons for "Enable" and "Disable", with "Disable" selected.
- AP Distance:** A text input field containing "100" followed by "meter(s)".
- Interval:** A text input field containing "0" followed by "minute(s)".
- Threshold:** Radio buttons for "Number of Clients" and "Number of Packets", with "Number of Clients" selected. A text input field next to it contains "15" followed by "clients".
- An "Apply" button is located to the right of the threshold options.

The bottom page is titled "Map Cluster Setting" and contains the following elements:

- Map:** A dropdown menu with the text "Pick one" and a downward arrow.
- Cluster:** A text input field containing "0".
- Buttons for "Configure", "Create", and "Delete" are positioned to the right of the cluster input field.
- Below these elements is a table with the following columns: Cluster, Device Name, IP Address, RF, Power Level, # of Users, and Log.

To create AP load balancing clusters, the administrator must add the APs to maps. The APs in the same load balancing cluster must be in the same map. After adding APs to the map, go to [Main Menu >> Devices >> Wide Area AP Management >> AP Load Balancing](#) to select map under Map Cluster Setting. Then, click the Create button to automatically generate clusters on this map based on the distance between each pair of APs. After the clusters are created, you can click the Configure button to enable/disable AP load balancing function for each cluster.

If the location of an AP is modified (e.g. drag the AP icon to different location on the map and click "Save Modification" button), the APs will not be re-clustered automatically. The administrator have to delete the existing clusters on the map first, and click the Create button to generate clusters according to the updated

location information.

On the other hand, if "AP Distance" is modified, the existing clusters will be deleted automatically. You have to click the Create button to generate clusters based on the updated criteria of clustering.

Finally, once AP load balancing function is enabled on a cluster, the logs of transmit power management actions for each AP are available for check.

# Chapter 8. Advanced Settings for Network Environment

## 8.1 IPv4 / IPv6 Dual Stack Network

Configuration Path: [Main Menu >> System >> IPv6](#)

Edgecore EWS 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

- **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.



## ■ IPv4 / IPv6 Network Utilities

Configure Network Utility; go to: [Main Menu >> Utilities >> Network Utilities](#)

The system provides network utilities to help administrators manage the network easily.

### Network Utilities

Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Sniff <input type="radio"/> IP Discovery
Ping	<input type="text" value="IP/Domain Name"/> <input type="button" value="Ping"/>
Trace Route	<input type="text" value="IP/Domain Name"/> <input type="button" value="Start"/> <input type="button" value="Stop"/>
ARPing	<input type="text" value="IP/Domain Name"/> Interface <input type="text" value="WAN1"/> <input type="button" value="ARPing"/>
VLAN ID	<input type="text" value="IP/MAC"/> <input type="button" value="Find"/>
ARP Table	<input type="button" value="Show"/>
Status	
Result	<div style="border: 1px solid #ccc; height: 100px;"></div>

### Network Utilities

Type	<input type="radio"/> IPv4 <input type="radio"/> IPv6 <input checked="" type="radio"/> Sniff <input type="radio"/> IP Discovery
Sniff	<p><b>Controls:</b></p> <p>The Sniff tool is for the administrator to capture packets from the selected "Interface". The "Packet" field is to determine how many packets to capture. If the information of the link layer is to be displayed, check the "Link Layer" box. If the packet information is to be displayed in hexadecimal format, check the "Hex" box.</p> <p>To further filter the types of packets, please enter the filtering "Expression" below following the syntax of Linux tcpdump command. Example 1, to capture only TCP related packets occurring at port 23, type in "tcp port 23" Example 2, to capture only ARP related packets, type in "arp" Example 3, to capture only ICMP related packets, type in "icmp"</p> <p>Interface <input type="text" value="WAN1"/> Packet <input type="text" value="1 - 1000"/> <input type="checkbox"/> Link Layer <input type="checkbox"/> Hex</p> <p>Expression <input type="text"/></p> <p><input type="button" value="Capture"/> <input type="button" value="Stop"/></p>
Status	
Result	<div style="border: 1px solid #ccc; height: 100px;"></div>



Item	Description
<b>IPv4</b>	<ul style="list-style-type: none"> <li>▪ <b>Ping:</b> It allows administrator to detect a device using IP address or Host domain name to see if it is responding.</li> <li>▪ <b>Trace Route:</b> It allows administrator to recover the real path of packets from the gateway to a destination using IP address or Host domain name.</li> <li>▪ <b>ARPing:</b> Allows administrator to send ARP request for a specific IP address or domain name.</li> <li>▪ <b>ARP Table:</b> It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).</li> </ul>
<b>IPv6</b>	<ul style="list-style-type: none"> <li>▪ <b>Ping:</b> It allows administrator to detect a device using IPv6 address or Host domain name to see if it is responding.</li> <li>▪ <b>Trace Route 6:</b> It allows administrator to recover the real path of packets from the gateway to a destination using IPv6 address or Host domain name.</li> <li>▪ <b>Neighbor Discovery:</b> The administrator can use this feature to learn about IPv6 Neighbor nodes that are on the same IP segment or domain name.</li> <li>▪ <b>Neighbor Cache:</b> a node manages the information of its neighbors in the Neighbor Cache. This feature allows the administrator to view the information stored on system's neighbor cache.</li> </ul>
<b>Sniff</b>	<p>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 <b>Expression</b> field.</p>

<b>IP Discovery</b>	With this feature, controller can discover the IP address of the APs connected within the same Layer 2 network. Administrator can also modify the IP configuration for the discovered APs.
<b>Status</b>	When the administrator is executing any Network Utilities features, the status of the operation is displayed here.
<b>Result</b>	The operation result is displayed here.

## 8.2 User Access Control

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.

### 8.2.1 Black List

Configuration Path: [Main Menu >> Users >> Black List](#)

The black list is a tool for user access control. Each black list can hold specific user accounts that will be denied of network access. The administrator can use the pull-down menu to select the desired black list profile to edit.

Select Blacklist 1: Blacklist1

### Blacklist Settings

Blacklist Name

	User Name	Remark
(Total:0/40) <First> <Prev> Next> <Last> Go to Page (Page:1/1) Row per Page: 10		

## Adding User(s) to Blacklist1

40 users can be added to this Blacklist.

No.	Username	Remark
1	<input type="text" value="User1"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

After entering the usernames in the **Username** blanks fields and the related information in the **Remark** blank fields (not required), click **Apply** to add the users.

To remove a user from the black list, select the user's **Delete** hyperlink to remove that user from the black list.

Select Blacklist 1: Blacklist1

### Blacklist Settings

Blacklist Name

<input type="checkbox"/>	User Name	Remark
<input checked="" type="checkbox"/>	User1	

After the Black List is setup completed, select the Black List in the desired Authentication Server for it to become effective.

### Local Authentication

User Postfix: local

Blacklist: 1 : Blacklist1

Local User List: Configure

Account Roaming Out:  Enable  Disable

802.1X Authentication:  Enable  Disable

## 8.2.2 MAC ACL

Configuration Path: [Main Menu >> Users >> Additional Controls](#)

**MAC ACL** is a MAC address Access Control List where specific MAC addresses may be listed for access filtering, either allow or deny. User authentication is still required for MAC ACL Allowed users. Click **Configure** to enter the **MAC Address Control** list. Click **Add MACs** to fill in the desired MAC addresses, select **Allow** or **Deny** and then click **Apply**.

### MAC Access Control List

MAC Access Control List: Configure

MAC Access Control is used to grant or deny permission to access the User Login Page.

List Type:  Allow  Deny  Disable Apply

### Access Control List

Add MACs Delete

No.	MAC Address
(Total:0/400) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a> Go to Page <input type="text"/> (Page:1/1) Row per Page: <input type="text" value="20"/>	

**NOTE**





1. 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.

## 8.3 Certification

Configuration path: [Main Menu >> Utilities >> Certificate](#)

EWS Access 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.

Certificate Management

Cert Name	Common Name	Used by
System Certificate 		
Default Certificate	CN=gateway.example.com	WEB Server, Built-in RADIUS, CAPWAP
Internal Root CA 		
Internal Root CA	N/A	
Internally Issued Certificate 		
N/A	N/A	
Trusted Certificate Authorities (CA) 		
N/A	N/A	

To enter settings, click "Edit" icon on the top-left corner of each category.

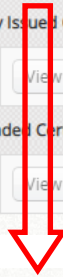
### 8.3.1. System Certificate

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. The Re-generate button allows administrator to automatically generate a unique certificate based on the MAC address of the gateway. To view details of the certificate, click the corresponding "View" button.

### System Certificate

Cert Name	Common Name	Operation	
Factory Default Certificate			
Factory Default Certificate	CN=gateway.example.com	<a href="#">View</a>	<a href="#">Regenerate</a>
Internally Issued Certificate			
N/A	N/A	<a href="#">View</a>	<a href="#">Delete</a>
Uploaded Certificate			
N/A	N/A	<a href="#">View</a>	<a href="#">Delete</a> <a href="#">Upload Intermediate/Root CA</a> <a href="#">Verify</a>



### Certificate

DEFAULT	
Subject	C=US ST=US L=CA O=EXAMPLE,INC CN=gateway.example.com
Issuer	C=US ST=US L=CA O=EXAMPLE,INC CN=gateway.example.com
Validity	2020/08/13 10:36:37
<a href="#">Get CERT</a> <a href="#">Get Key</a>	

Click "Get CERT" and "Get Key" to download the certificate and public key onto your local disk.

To Upload a Certificate/Private Key/Intermediate CA, click "Browse", select the appropriate files, and click Upload Files.



## Upload System Certificate

Certificate	<input type="text"/>	<input type="button" value="Browse..."/>
Private Key	<input type="text"/>	<input type="button" value="Browse..."/>
Intermediate CA	<input type="text"/>	<input type="button" value="Browse..."/>
Certification Path Verification	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<input type="button" value="Upload Files"/>		

### 8.3.2. 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.

## Generate Root CA

Common Name	<input type="text"/>
Email Address	<input type="text"/>
Country Name	<input type="text"/>
State or Province Name	<input type="text"/>
Locality Name	<input type="text"/>
Organization Name	<input type="text"/>
Organization Unit Name	<input type="text"/>
Key Type	<input type="text" value="RSA"/>
Key Length	<input type="text" value="512"/>
<input type="button" value="Generate Certificate"/>	

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.

## Internal Root CA

Cert Name	Common Name	Operation
Internal Root CA		
Root CA	CN=4ipnet.com	<a href="#">View</a> <a href="#">Delete</a>

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

### 8.3.3. 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.

## Certificate Information

Cert Name	Common Name	Operation
Internally Issued Certificate		
cert1	CN=4iptest.com	<a href="#">View</a> <a href="#">Delete</a>

## Use Internal Root CA to generate certificate

Common Name	<input type="text"/>
Email Address	<input type="text"/>
Country Name	<input type="text"/>
State or Province Name	<input type="text"/>
Locality Name	<input type="text"/>
Organization Name	<input type="text"/>
Organization Unit Name	<input type="text"/>
Key Type	RSA ▾
Key Length	512 ▾
<input type="button" value="Generate Certificate"/>	

### 8.3.4. 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.

Trusted Certificate Authorities (CA)

Cert Name	Common Name	Operation
Certificate Authorities (CA)		
N/A	N/A	<input type="button" value="View"/> <input type="button" value="Delete"/>

Upload Trusted CAs

Certificate

## 8.4 Management Access

Configuration path: [Main Menu >> System >> General >> Management IP Address](#)

On the EWS Access Controller, the administrator can grant access to the web management interface by specifying a list specific IP addresses or ranges of IP addresses, both from WAN or from LAN. 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.

The Console interface may be accessed remotely when the **Remote Console** is enabled. For security purposes, console access is disabled by default to prevent malicious users from accessing the system.

# Chapter 9. Utilities for Controller Management

## 9.1 EWS Controller Management

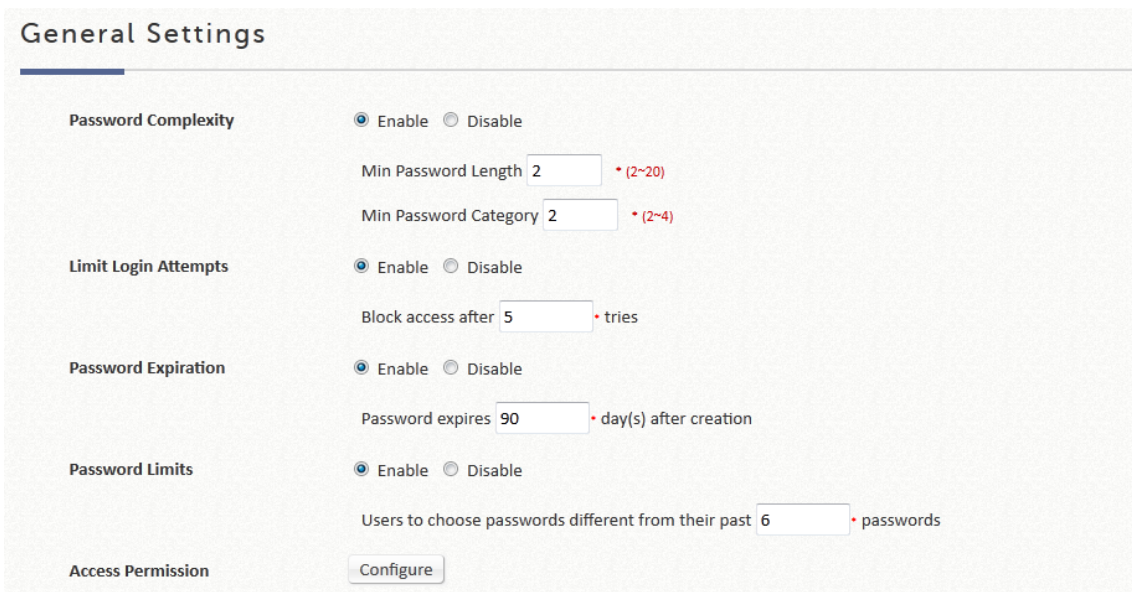
Configuration path: [Main Menu >> Utilities >> Administrator Account](#)

The EWS controller's root management account is the "admin" account with full access, modification and application privilege and authority. There are however, 2<sup>nd</sup> tier accounts with less authority which may be created for management personnel to access their designated assigned areas of authority, a necessary feature for large scale deployment requiring multiple management personnel.

This configuration path will lead to the page for assigning authority property, and generation of other management accounts customizable to suit the needs of your network.

There is only one management account under default status. **Group Permission Settings** will allow you to customize the accessible WMI pages for a particular management group and in turn, create management accounts for that group.

### Step 1: Configure Password Safety Settings



The screenshot shows the 'General Settings' page for password safety. It includes several sections with radio buttons for 'Enable' and 'Disable', and input fields for numerical values. The 'Access Permission' section has a 'Configure' button.

Section	Option	Value	Constraint	
Password Complexity	Enable (selected)			
	Disable			
	Min Password Length	2	(2~20)	
		Min Password Category	2	(2~4)
Limit Login Attempts	Enable (selected)			
	Disable			
		Block access after	5	tries
Password Expiration	Enable (selected)			
	Disable			
		Password expires	90	day(s) after creation
Password Limits	Enable (selected)			
	Disable			
		Users to choose passwords different from their past	6	passwords
Access Permission				<button>Configure</button>

Password Safety can be enabled to protect the Web Management Interface from unauthorized personnel. Note that these settings are disabled by default.

## Step 2: Configure Group Access property

Main > Utilities > Administrator Accounts > Administrator Group > Administrator Group Edit

### Administrator Group Edit

Admin Group Name	Custom 1 *
Remark	
Service Zone	<ul style="list-style-type: none"><li>Disabled Select All</li><li>Disabled Default</li><li>Disabled SZ1</li><li>Disabled SZ2</li><li>Disabled SZ3</li><li>Disabled SZ4</li><li>Disabled SZ5</li><li>Disabled SZ6</li><li>Disabled SZ7</li><li>Disabled SZ8</li></ul>
AP GROUP	
AP Management	<ul style="list-style-type: none"><li>Disabled Select All</li><li>Disabled Local Area AP Management</li><li>Disabled Wide Area AP Management</li></ul>
Switch Management	Disabled
On-Demand API	<input type="checkbox"/> Enable administrator to create On-Demand Account through external interfaces
Setup Wizard	Disabled

The Controller supports customizable administration account types, namely Super Group, Manager, On-Demand Manager or Operator. Admin is classified under Super Group, with all access and configuration authorities. Only Super Group members can generate other administrative accounts (Manager, On-Demand Manager and Operator). Permission Settings for all administrative accounts can be customized. With the exception of the Super Group members, other administrative accounts can be configured to have read-write or read-only access.

**Step 3:** An Administrator Accounts List is available to display Administrator Accounts information and their statuses. Create an account by clicking “Add”, then inputting the desired account name, password and the assigned authority group. Subsequent to clicking **Apply**, the newly generated account will be displayed in the

table below.

**Administrator Accounts**

Add ... Delete Lock Admin Unlock Backup List Restore List

<input type="checkbox"/>	Name	IP Address	MAC Address	Group	Status
<input type="checkbox"/>	admin	10.29.129.162	DC:0E:A1:27:F4:63	Super Group	Current Page: /Utilities/MlaUser.shtml
<input type="checkbox"/>	admin	10.30.42.168		Super Group	Current Page: /SystemConfiguration/SCAPList.shtml?sz_id=0

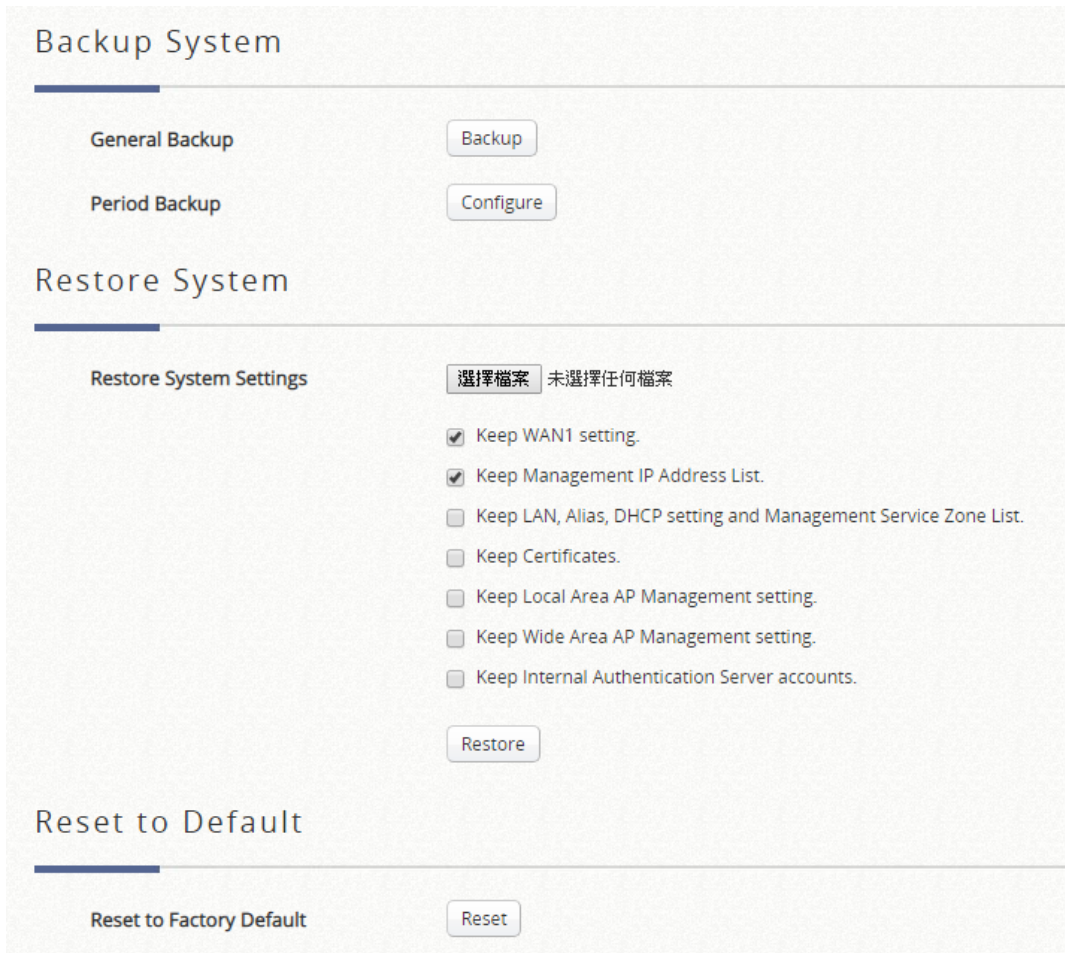
## NOTE

1. The Password Safety Settings contain constraints or rules which must be followed upon management account creation or password change.
2. Admin List will display all existing management accounts and login status if this account is currently accessing the WMI.
3. Admin account is the root account and may not be deleted or have its authority modified.

## 9.2 Configuration Backup & Restore

Configuration path: [Main Menu >> Utilities >> Backup & Restore](#)

This function is used to backup/restore the EWS Controller settings. Backup can be done periodically via FTP. Furthermore, EWS Controller can be restored to the factory default settings here.



## NOTE

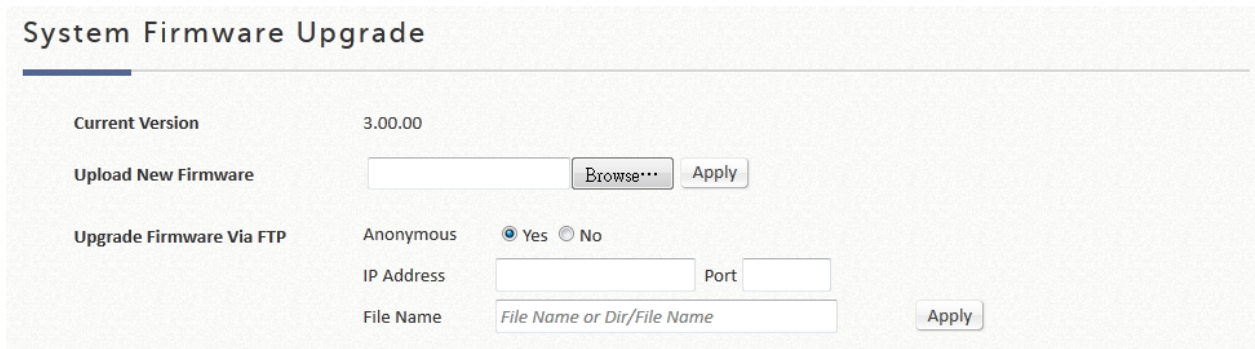
1. The General Backup feature will lead to a pop up window prompting to save a db file.
  2. Restoring previous db configurations may be performed with options such as keep WAN settings to prevent the loss of WMI connection if this action is performed remotely.
  3. Resetting to factory default will erase all configurations and restore the controller to factory configuration. This action also has additional options to keep critical settings.
-

## 9.3 Firmware Upgrade

Configuration path: [Main Menu >> Utilities >> System Upgrade](#)

The administrator can obtain the latest firmware from Edgecore's website 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.

Before performing an upgrade, the system checks for version compatibility ensure system sanity. You may contact the Edgecore Support Team regarding version compatibility.



The screenshot shows the 'System Firmware Upgrade' configuration page. It displays the current version as 3.00.00. There are two main sections: 'Upload New Firmware' and 'Upgrade Firmware Via FTP'. The 'Upload New Firmware' section has a text input field, a 'Browse...' button, and an 'Apply' button. The 'Upgrade Firmware Via FTP' section includes an 'Anonymous' section with 'Yes' (selected) and 'No' radio buttons, an 'IP Address' input field, a 'Port' input field, a 'File Name' input field with a placeholder 'File Name or Dir/File Name', and an 'Apply' button.

### NOTE

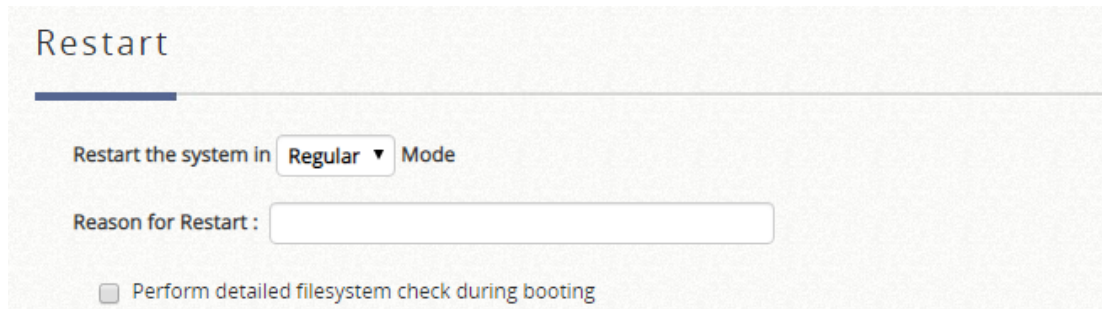
The system **MUST** be restarted before resetting to factory defaults after firmware upgrade.

## 9.4 Restart

Configuration path: [Main Menu >> Utilities >> Restart](#)



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



Restart

Restart the system in **Regular** Mode

Reason for Restart :

Perform detailed filesystem check during booting

## NOTE

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

# ***Chapter 10. Reports and Logs for Monitoring***

## **10.1 System Related Status**

### **10.1.1 The 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. A drop-down menu is available for selecting the information refresh rate for this page, or you may click the "Refresh" button to refresh manually.

The "Display Mode" button on the top-right corner allows the administrator to decide items displayed in Dashboard.

The download button on the top-right corner is a tool that captures system settings. This is used for maintenance or troubleshooting purposes.



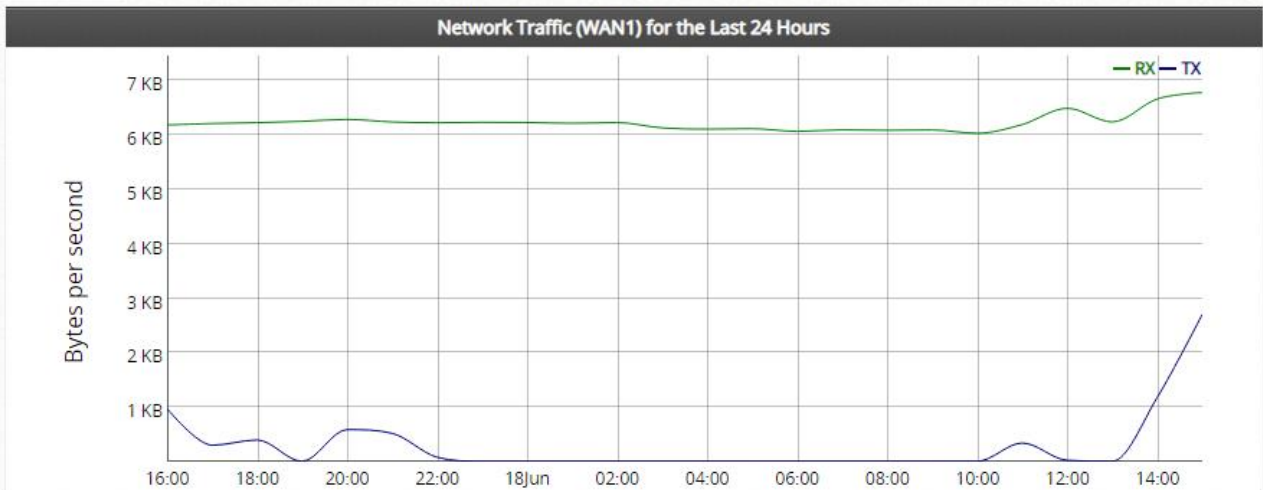
## 10.1.2 System Summary

Configuration path: [Main Menu >> Status >> System Summary](#)

The system status page displays a table of contents including system firmware version, report servers configured, WAN optional settings, User log profile, system time and session control settings. This overview is designed for main configuration items. For detailed status, please proceed to corresponding configuration pages.

# System Summary

[See Reports](#)

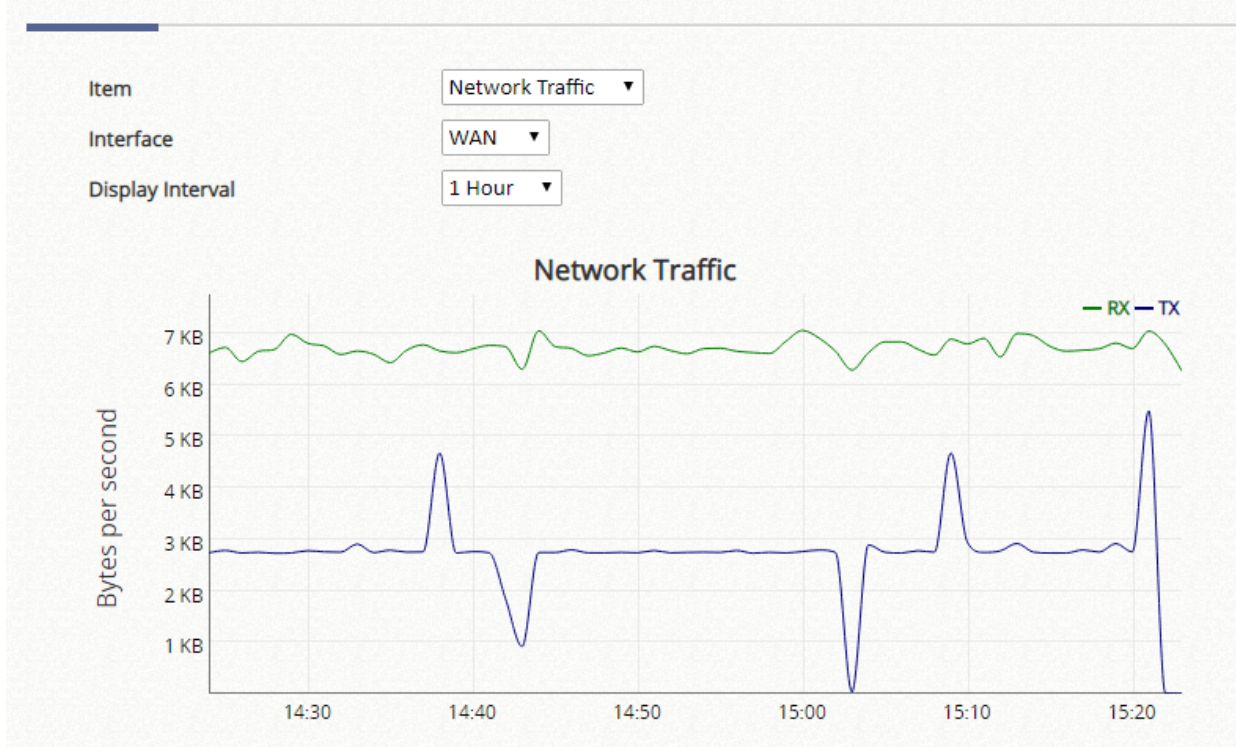


General			
System Name	EWS101	Firmware Version	3.45.0000
System Up Time	14 days, 23 hours, 27 min	Build Number	1.36-1.9737
System Time	2019/06/18 15:20:58 +0800	NTP Server	ntps1.pads.ufrj.br
Preferred DNS Server	8.8.8.8	Alternate DNS Server	N/A
Proxy Server	Disabled	APM Version	3.45.0000
SNMP	Enabled	Warning of Internet Disconnection	Disabled
Idle Timeout	10min	Traffic Direction for Idle Timeout	Uplink & Downlink
Num of Current Users	0	Num of Maximum Users	400

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.

## System Report



### 10.1.3 Network Interface

Configuration path: [Main Menu >> Status >> 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.

Select Interface: WAN1

Network Interface: WAN1

WAN1			
Mode	STATIC	IP Address	10.29.42.101
MAC Addr	00:10:F3:23:D3:54	Subnet Mask	255.255.0.0
IPv6 Addr	N/A	IPv6 Prefix	N/A
Auto-negotiation	On	Speed / Duplex	100Mb/s Full

summaryTraffic

today

rx: 9.09 MiB  
tx: 7.08 MiB  
= 16.17 MiB  
2.84 kbit/s

yesterday

rx: 18.74 MiB  
tx: 11.45 MiB  
= 30.18 MiB  
2.86 kbit/s

all time

rx: 1.29 GiB  
tx: 697.30 MiB  
= 1.97 GiB

since 01/11/13

rx: 366.76 MiB  
tx: 153.05 MiB  
= 519.81 MiB  
7.54 kbit/s

Feb '13

rx: 953.68 MiB  
tx: 544.25 MiB  
= 1.46 GiB  
4.58 kbit/s

Jan '13

dailyTraffic

day	rx	tx	total	avg. rate
01/12/13	7.48 MiB	516 KiB	7.99 MiB	0.76 kbit/s
01/13/13	7.49 MiB	507 KiB	7.99 MiB	0.76 kbit/s
01/14/13	55.38 MiB	35.24 MiB	90.62 MiB	8.59 kbit/s
01/15/13	26.90 MiB	46.95 MiB	73.85 MiB	7.00 kbit/s
01/16/13	241.00 MiB	54.98 MiB	295.98 MiB	28.06 kbit/s
01/17/13	109.16 MiB	42.05 MiB	151.22 MiB	14.34 kbit/s
01/18/13	59.43 MiB	25.99 MiB	85.42 MiB	8.10 kbit/s
01/19/13	10.43 MiB	415 KiB	10.83 MiB	1.03 kbit/s
01/20/13	8.86 MiB	328 KiB	9.18 MiB	0.87 kbit/s
01/21/13	55.97 MiB	27.50 MiB	83.48 MiB	7.91 kbit/s
01/22/13	19.56 MiB	17.41 MiB	36.97 MiB	3.51 kbit/s
01/23/13	12.89 MiB	9.13 MiB	22.02 MiB	2.09 kbit/s
01/24/13	25.80 MiB	25.10 MiB	51.90 MiB	4.92 kbit/s
01/25/13	21.04 MiB	39.55 MiB	60.59 MiB	5.74 kbit/s
01/28/13	35.32 MiB	84.39 MiB	119.70 MiB	11.35 kbit/s
01/29/13	62.02 MiB	10.35 MiB	72.36 MiB	6.86 kbit/s
01/30/13	44.33 MiB	24.44 MiB	68.77 MiB	6.52 kbit/s
01/31/13	62.56 MiB	22.97 MiB	85.52 MiB	8.11 kbit/s
02/01/13	58.17 MiB	22.20 MiB	80.36 MiB	7.62 kbit/s
02/02/13	52.07 MiB	9.17 MiB	61.24 MiB	5.81 kbit/s
02/03/13	51.87 MiB	9.07 MiB	60.94 MiB	5.78 kbit/s
02/04/13	58.45 MiB	22.98 MiB	81.43 MiB	7.72 kbit/s
02/05/13	41.68 MiB	15.80 MiB	57.48 MiB	5.45 kbit/s
02/05/13	215 KiB	579 KiB	794 KiB	0.07 kbit/s
02/07/13	12.53 MiB	26.12 MiB	38.65 MiB	3.66 kbit/s
02/08/13	13.70 MiB	11.40 MiB	25.11 MiB	2.38 kbit/s
02/09/13	48.57 MiB	15.24 MiB	64.31 MiB	6.15 kbit/s
02/06/13	1.57 MiB	0.98 MiB	2.55 MiB	0.24 kbit/s
02/06/13	18.74 MiB	11.45 MiB	30.18 MiB	2.86 kbit/s
02/07/13	9.09 MiB	7.08 MiB	16.17 MiB	2.84 kbit/s
estimated	16 MiB	12 MiB	28 MiB	

monthlyTraffic

month	rx	tx	total	avg. rate
Jan '13	953.68 MiB	544.25 MiB	1.46 GiB	4.58 kbit/s
Feb '13	366.76 MiB	153.05 MiB	519.81 MiB	7.54 kbit/s
estimated	1.53 GiB	655 MiB	2.17 GiB	

top10Traffic

#	day	rx	tx	total	avg. rate
1	01/15/13	241.00 MiB	54.98 MiB	295.98 MiB	28.06 kbit/s
2	01/11/13	88.07 MiB	75.49 MiB	163.56 MiB	15.51 kbit/s
3	01/17/13	109.16 MiB	42.05 MiB	151.22 MiB	14.34 kbit/s
4	01/28/13	35.32 MiB	84.39 MiB	119.70 MiB	11.35 kbit/s
5	01/14/13	55.38 MiB	35.24 MiB	90.62 MiB	8.59 kbit/s
6	01/31/13	62.56 MiB	22.97 MiB	85.52 MiB	8.11 kbit/s
7	01/18/13	59.43 MiB	25.99 MiB	85.42 MiB	8.10 kbit/s
8	01/21/13	55.97 MiB	27.50 MiB	83.48 MiB	7.91 kbit/s
9	02/04/13	58.45 MiB	22.98 MiB	81.43 MiB	7.72 kbit/s
10	02/01/13	58.17 MiB	22.20 MiB	80.36 MiB	7.62 kbit/s

## NOTE

1. 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.

## 10.1.4 Routing

Configuration path: [Main Menu >> Status >> Routing Tables >> IPv4/IPv6](#)

This status page displays all the **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.

### 10.1.5 DHCP Server

Configuration path: [Main Menu >> Status >> DHCP Leases](#)

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

Refresh Refresh Disable ▾

	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 List**

Valid IP addresses issued from the DHCP Server and related information of the client using this IP address is displayed here.

## DHCP Leases

Statistics List Show  
DHCP Lease Log Show

## DHCP Lease List

Refresh Delete Refresh Disable ▾

<input type="checkbox"/>	No.	IP Address	MAC Address	Host Name	VLAN	Lease Expires
<input type="checkbox"/>	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  (Page:1/1) Row per Page:

## 10.2 Client Related Status

### 10.2.1 Online User

Page path: [Main Menu >> Status >> Monitor Users >> Online Users](#)

Users displayed on this page are the ones that are authenticated by this Controller under its managed network either LAN or remotely tunneled site.



## NOTE

1. User information (Username) is not shown in the Online users list when any Tunnel is not used if AP is located on WAN side of the controller.

Online Users List

Select Mode  Summary  Detail     Refresh

No.	Username	IP Address	IPv6 Address	MAC Address	SZ / VLAN	Access From (AP/SSID)
1	test@local	192.168.1.72	N/A	00:AA:BB:CC:DD:EE	Default / TN#1.1000	ECW05211-L/ECW05211-B1

(Total:1) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page  (Page:1/1) Row per Page:

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.

### 10.2.2 Associated Non Login Users

Page path: [Main Menu >> Status >> Monitor Users >> Non-Login Devices](#)

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

MAC Address	IP Address	VLAN ID	Service Zone	Associated AP/SSID
D0:13:FD:45:5B:07	IPv4:192.168.1.72 IPv6:N/A	TN#1.1000	Default	Seb05211/Seb05211-B1

(Total:1) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page  (Page:1/1) Row per Page:

### 10.2.3 Cross Gateway Roaming Users

Page path: [Main Menu >> Status >> Monitor Users >> Roaming In 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

Name	IP Address	MAC Address	VLAN ID	Home	Detail
------	------------	-------------	---------	------	--------

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page  (Page:1/1) Row per Page:

### 10.2.4 On-Demand Roaming Out Users

Page path: [Main Menu >> Status >> Monitor Users >> Roaming Out Users](#)

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 ▾

### 10.2.5 MAC Login Devices

Page path: [Main Menu >> Status >> Monitor Users >> MAC Login Devices](#)

This page displays the devices that are not able to complete MAC authentication by itself. The administrator can select the devices and click “MAC Authenticate” button to manually help them authenticate. The authentication results will be shown in the text area in this page.

Main > Status > User Monitor > MAC Login Devices

MAC Login Devices List

MAC Authenticate Refresh Refresh Disable ▾

<input type="checkbox"/>	No.	MAC Address	IP Address	Service Zone
Result				

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page  (Page:1/1) Row per Page: 50 ▾

### 10.2.6 Authenticated Users

Page path: [Main Menu >> Status >> Monitor Users >> Authenticated Users](#)

This page displays the authentication-completed users whose IP information is unknown to the controller. For some types of authentication (802.1X, MAC authentication, PPP authentication, CoA Login), the users must authenticate for network access before granted for network access. Therefore, the users can only request for IP address via DHCP after the authentication is complete.

Once an authenticated user obtains IP address and starts using network, he/she will be moved from Authenticated Users List to Online Users List.

Administrator can logout the authenticated users by selecting the users and click the "Logout" button.

Main > Status > User Monitor > Authenticated Users

### Authenticated Users List

Logout Refresh Refresh Disable ▾

No.	Username	MAC Address	Auth. Database	Auth. Method
-----	----------	-------------	----------------	--------------

(Total:0) First Prev Next Last Go to Page ▾ (Page:1/1) Row per Page: 50 ▾

## 10.2.7 Smart Login Users

Page path: [Main Menu >> Status >> Monitor Users >> Smart Login Users](#)

Smart Login is a convenient feature for On-Demand users. When enabling Smart Login, once an On-Demand user is login successfully, the device will be login automatically within a defined duration even if he/she has logged out.

This page displays the On-Demand users within the Smart Login period. The user in this list will login automatically when he/she accesses the network next time.

Administrator can delete the users in the Smart Login Users list. The deleted users have to login manually next time.

### Smart Login User Information

Delete All Delete

	MAC	Name	Last Login
--	-----	------	------------

(Total:0/2000) First Prev Next Last Go to Page ▾ (Page:1/1) Row per Page: 10 ▾

## 10.2.8 Session List

Configuration path: [Main Menu >> Status >> Sessions](#)

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 ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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

## 10.3 Logs and Reports

### 10.3.1 System Related

Configuration path: [Main Menu >> Status >> 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.
- **Alarm:** Displays error or warning messages for the selected items. An alarm message remains on the alarm list until the fault is resolved. Alarm items can be configured in the "Alarms & Events Settings" page.
- **Management Event:** Displays logs for the selected management events.

Management Events can be configured in "Alarms & Events Settings" page.

### 10.3.2 User Events

Configuration path: [Main Menu >> Status >> Logs and Reports >> 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, and 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.

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

The "Configure" button for Display Mode allows administrator to modify the

columns shown in User Events.

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.

## 10.4 Reports & Notification

Configuration path: [Main Menu >> Status >> Reporting](#)

EWS Controller can automatically send various kinds of user and/or system related reports to configured E-mail addresses, SYSLOG Servers, or FTP Server.



## Notification Settings

	Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval		
	1	2	3	4	5				Detail / Test	
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼	
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼	
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼	
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼	
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼	
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼	
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼	
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼	
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼	
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A	
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼	
On-Demand User Billing Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/>	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼	
Wide Area AP Report									<input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Delay <input type="checkbox"/> Network Traffic <input type="checkbox"/> Associated Clients <input type="checkbox"/> VAP Traffic <input type="checkbox"/> WDS Traffic	<input type="checkbox"/> N/A <input type="checkbox"/> N/A <input type="checkbox"/> <input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report
Switch Status	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼	
Switch Report									<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report	
Local HTTP Web Log							<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
HTTP Web Log							<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Configuration Change Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/>	1 Hour ▼	
DHCP Server Log							<input type="checkbox"/>	N/A	N/A	
DHCP Lease Log							N/A	<input type="checkbox"/>	1 Hour ▼	
System Report									<input type="checkbox"/> CPU Loading <input type="checkbox"/> CPU Temperature <input type="checkbox"/> Memory Usage <input type="checkbox"/> Storage Usage <input type="checkbox"/> Network Traffic <input type="checkbox"/> Online User <input type="checkbox"/> Successful Login <input type="checkbox"/> Session <input type="checkbox"/> DHCP Lease <input type="checkbox"/> DNS Query	<input type="checkbox"/> N/A <input type="checkbox"/> N/A <input type="checkbox"/> <input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report
Traffic Report (Text)								<input type="checkbox"/>	<input type="checkbox"/> Service Zone <input type="checkbox"/> VLAN	1 Hour ▼

- **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.
- **SYSLOG Settings:** Allows the configuration of two external SYSLOG servers where selected users logs as well as system logs will be sent to.
- **FTP Settings:** Allows the configuration of an external FTP Server where selected users logs as well as system logs will be sent to.
- **Notification Settings:** 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, and FTP) on customizable time intervals.

- **Alarms & Events Settings:** Provides a list of the available management events for selection. If an item is selected as Management Events, the related logs will be recorded on the Management Events page and Dashboard. If an item is selected as Alarm, the warning message or error message will be displayed when related faults occur. Once the fault is resolved, the message will be removed from Alarm, while it is still recorded as Management Events.

# Chapter 11. Hotspot Application

## 11.1 On-Demand Billing Plans

Configuration path: [Main Menu >> Users >> Internal Authentication >> On-Demand >> Billing Plans](#)

Billing plan profiles define the terms and conditions of guest internet access. Click the **Billing Plan Number** link to enter the configuration page of a selected Billing Plan profile. Once you have finished configuring a billing plan profile, go back to the screen of **Billing Plans**, check the **Active** checkbox and click **Apply** to activate.

Billing Plans

No	Plan Type	Quota	Price	Active	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	1.99	<input checked="" type="checkbox"/>	Group 1	Reset
2	N/A			<input type="checkbox"/>	Group 1	Reset
3	N/A			<input type="checkbox"/>	Group 1	Reset
4	N/A			<input type="checkbox"/>	Group 1	Reset
5	N/A			<input type="checkbox"/>	Group 1	Reset

- **Plan:** The number of the selected Billing Plan profile.
- **Plan Type:** The account type chosen for this plan. Different account types have different properties. A suitable account type should be selected that will best meet guest usage requirements.
- **Quota:** The usage terms on how much or how long an On-Demand users are allowed to access the network.
- **Price:** The unit price of the respective billing plan.
- **Active:** Check the checkbox to activate the billing plan. Deactivated billing plans cannot be used to generate On-Demand guest accounts.
- **Group:** Group assignment of On-Demand users associated with the respective billing plan.
- **Function:** Click the "Reset" button to clear settings on the selected Billing plan Profile.

## 11.2 On-Demand Billing Plan Types

### 11.2.1 Usage-time with Expiration 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 countdown to Expiration Time is continuous regardless of logging in or out. Account expires when **Valid Period** has been used up or quota depleted.

- **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.
- **Account 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.
- **Valid Period** is the valid time period for using. After this time period, even with remaining quota the account will still expire.
- **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.

# Billing Plan Configuration

Plan Number: 1

Plan Type: Usage-time

Activation: User's First time login must be done within 0 day(s) 2 hour(s)  
The value for hour(s) has to be between 0~23; Day(s) and hour(s) cannot be both zeros.

Expiration:  Enable  Disable  
 Account will expire in 7 day(s) after activation

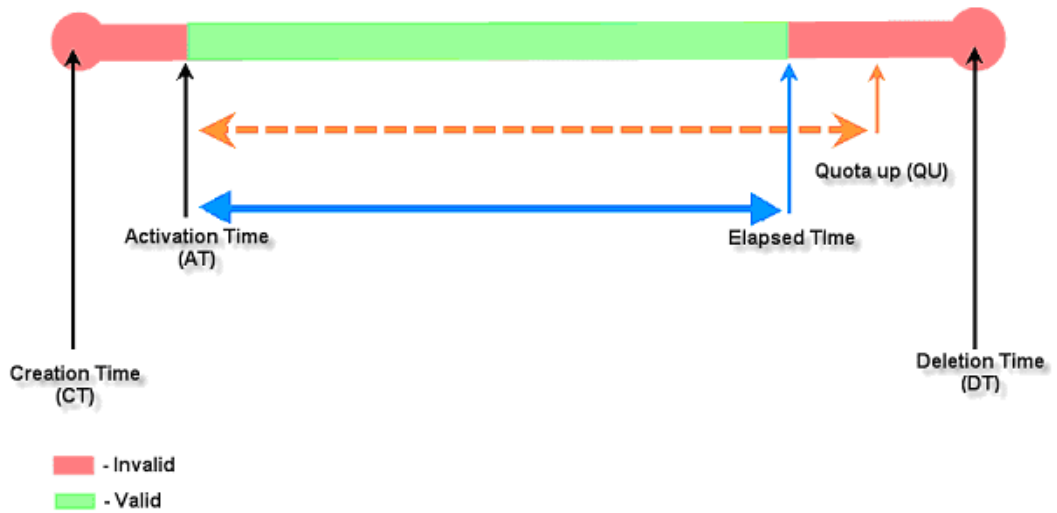
Quota: 0 day(s) 2 hr(s) 0 min(s)  
The value for day(s) cannot exceed 364; The value for hr(s) has to be 0~23; The value for min(s) has to be between 0~59.

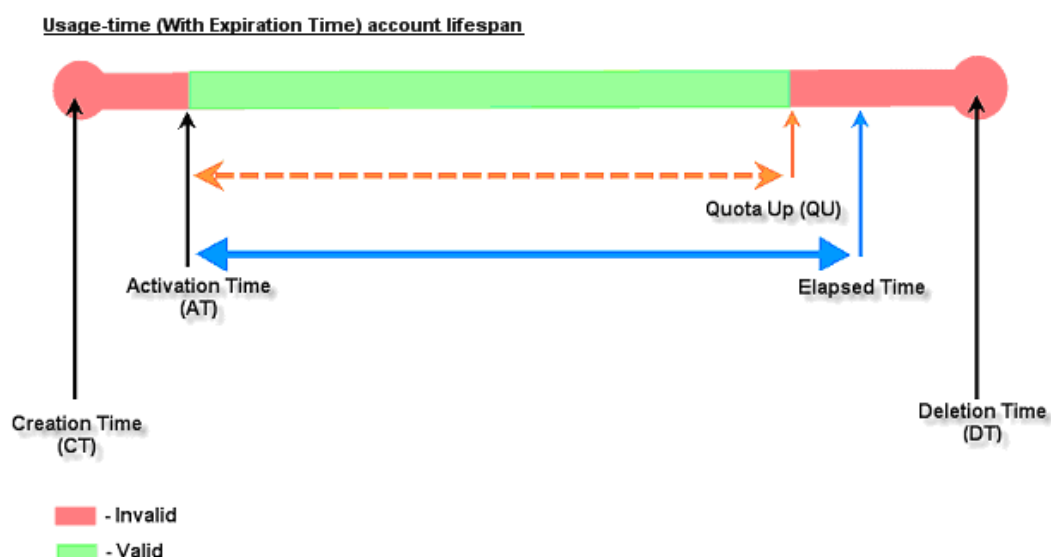
Unit Price: 1.99  
The unit price cannot exceed 100000, and can take values up to two decimal places.

Group: Group 1

Reference:

### Usage-time (With Expiration Time) account lifespan





### 11.2.2. Usage-time with No Expiration Time

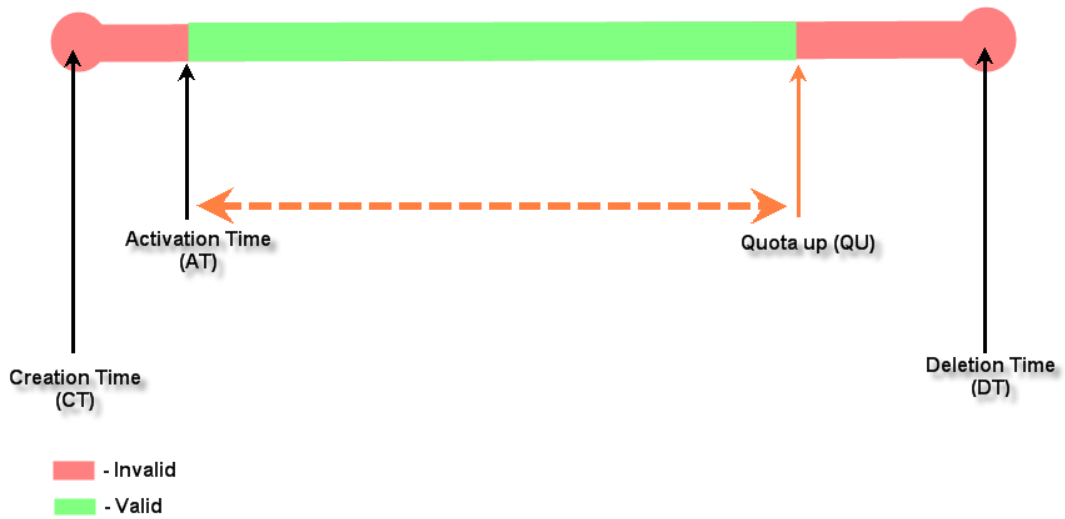
Users can access internet as long as account has remaining quota (usable time). Users need to activate the purchased account within a given time period by logging in. This is ideal for short term usage such as in coffee shops, airport terminals etc. Quota is deducted only while in use and account expires only when quota is depleted.

- **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 redeem.
- **Account 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.
- **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.

# Billing Plan Configuration

Plan Number	1
Plan Type	Usage-time
Activation	User's First time login must be done within 0 day(s) 2 hour(s) <small>The value for hour(s) has to be between 0~23; Day(s) and hour(s) cannot be both zeros.</small>
Expiration	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Quota	0 day(s) 2 hr(s) 0 min(s) <small>The value for day(s) cannot exceed 364; The value for hr(s) has to be 0~23; The value for min(s) has to be between 0~59.</small>
Unit Price	1.99 <small>The unit price cannot exceed 100000, and can take values up to two decimal places.</small>
Group	Group 1
Reference	

## Usage-time (No Expiration) account lifespan



### 11.2.3. Hotel Cut-off-time

**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. 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.

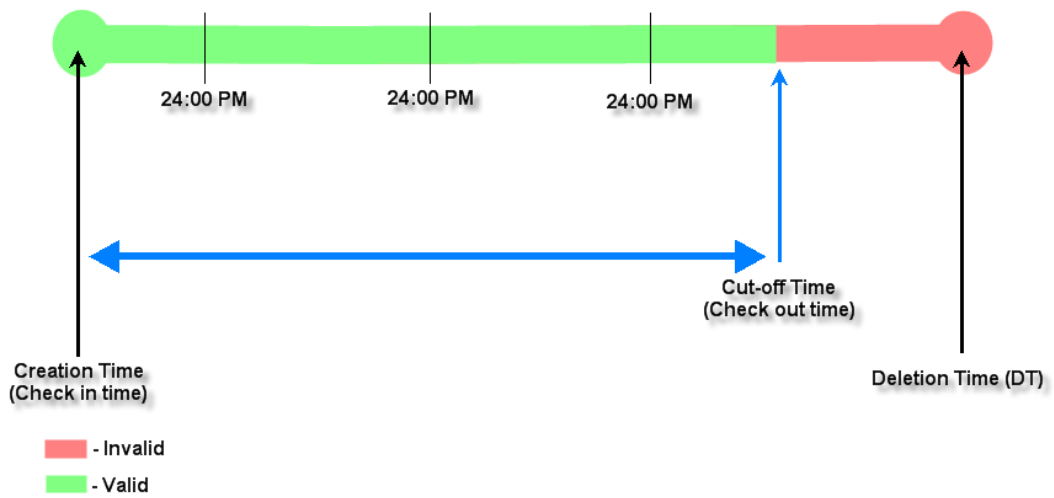
Billing Plan Configuration

---

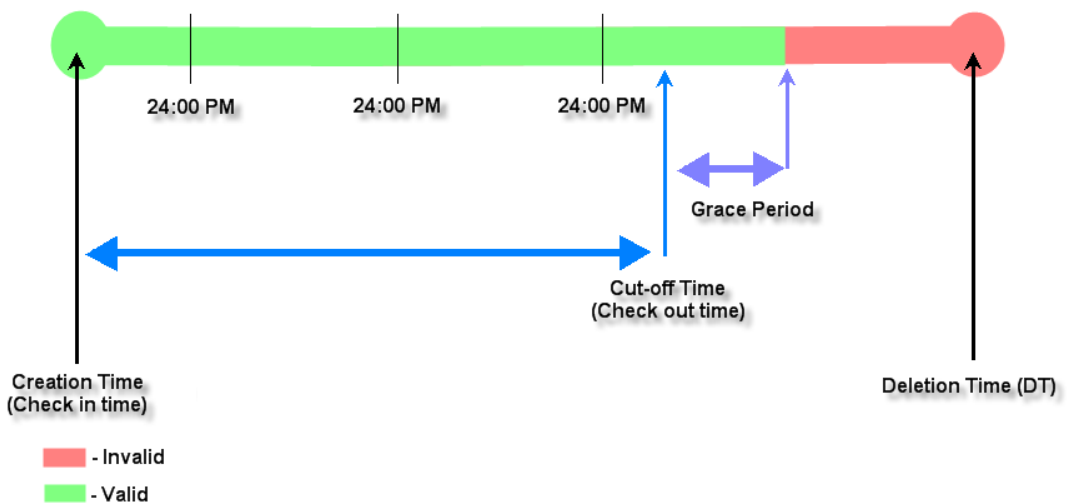
Plan Number	1
Plan Type	Hotel Cut-off time ▾
Cut-off Time	<input type="text"/> : <input type="text"/> <small>The cut-off time has to be between 00:00~23:59 in the form of hh:mm.</small>
Grace Period	0 ▾ hour(s) after Cut-off
Number of devices	1 <input type="text"/> device(s) <small>Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).</small>
Unit Price	11 <input type="text"/> per day <small>The unit price cannot exceed 100000, and can take values up to two decimal places.</small>
Group	Group 1 ▾
Reference	<input type="text"/>



Hotel Cut-off-time account lifespan (3 night stay example)



Hotel Cut-off-time account lifespan (3 night stay example with Grace Period)



### 11.2.4. Volume

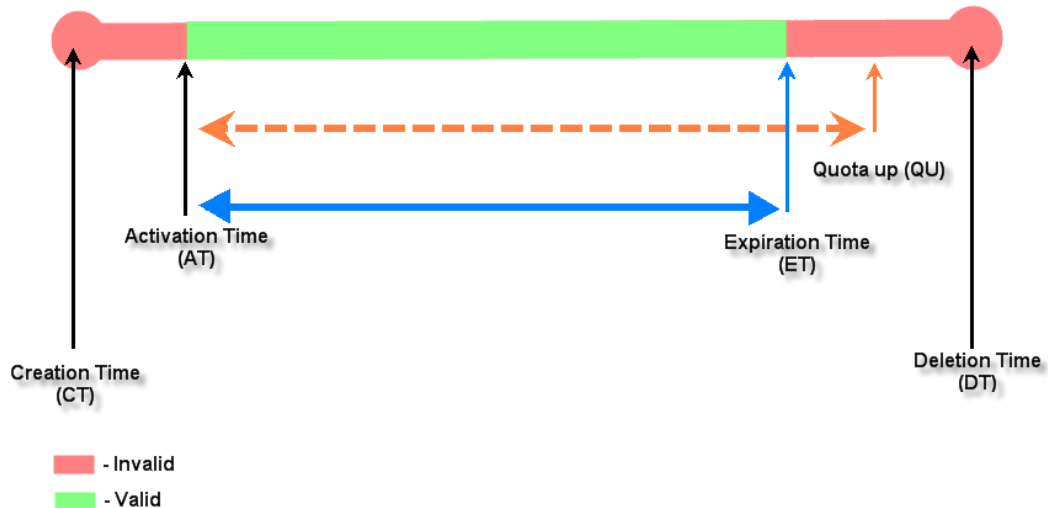
Users can access internet as long as account is valid with remaining quota (traffic volume). Account expires when *Valid Period* is used up or quota is depleted. This is ideal for small quantity applications such as sending/receiving mail, transferring a file etc. Count down of Valid Period is continuous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

- **Account 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.

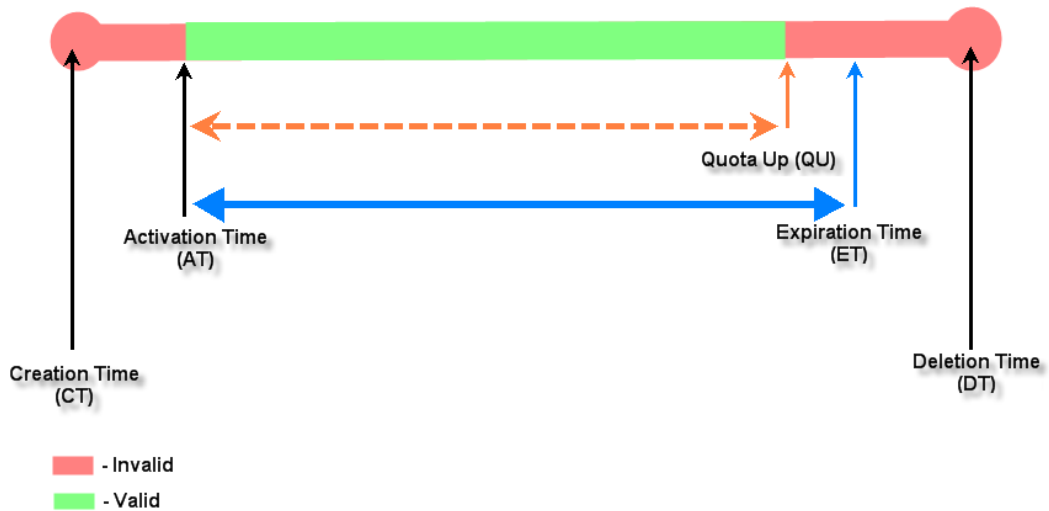
### Billing Plan Configuration

Plan Number	1
Plan Type	Volume ▾
Activation	User's First time login must be done within <input type="text" value="0"/> day(s) <input type="text" value="2"/> hour(s) <small>The value for hour(s) has to be between 0~23; Day(s) and hour(s) cannot be both zeros.</small>
Expiration	Account will expire in <input type="text" value="7"/> day(s) after activation
Quota	<input type="text" value="100"/> MByte(s) <small>*( Range : 1 ~ 1000000 )</small>
Number of devices	<input type="text" value="3"/> device(s) <small>Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).</small>
Unit Price	<input type="text" value="2"/> <small>The unit price cannot exceed 100000, and can take values up to two decimal places.</small>
Group	Group 1 ▾
Reference	<input type="text"/>

### Volume account lifespan



### Volume account lifespan



## 11.2.5. 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



## 11.2.6. Duration-time with Cut-off Time

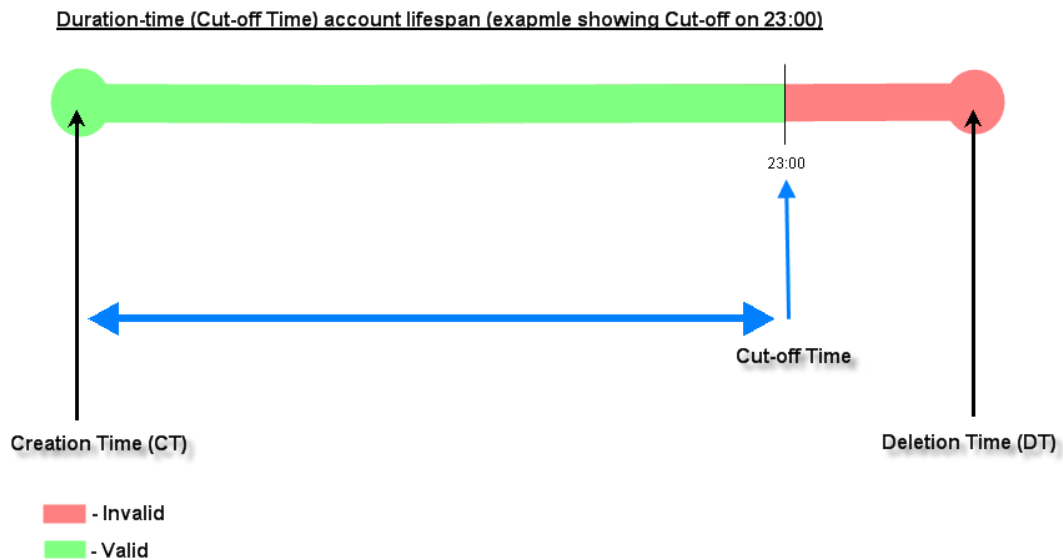
**Cut-off Time** is the clock time at which the On-Demand account is cut off (made expired) by the system on that day. For example if a shopping mall is set to close at 23:00; operators selling On-Demand tickets can use this plan to create ticket set to be Cut-off on 23:00. If an account of this kind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

Billing Plan Configuration

---

Plan Number	1
Plan Type	Duration-time ▾
Duration Type	<input type="radio"/> Elapsed Time <input type="radio"/> Begin-and-End Time <input checked="" type="radio"/> Cut-off Time
Begin Time	Upon Account Creation
Cut-off Time	<input type="text"/> : <input type="text"/> <small>The cut-off time has to be between 00:00~23:59 in the form of hh:mm.</small>
Number of devices	<input type="text" value="1"/> device(s) <small>Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).</small>
Unit Price	<input type="text" value="11"/> <small>The unit price cannot exceed 100000, and can take values up to two decimal places.</small>
Group	Group 1 ▾
Reference	<input type="text"/>



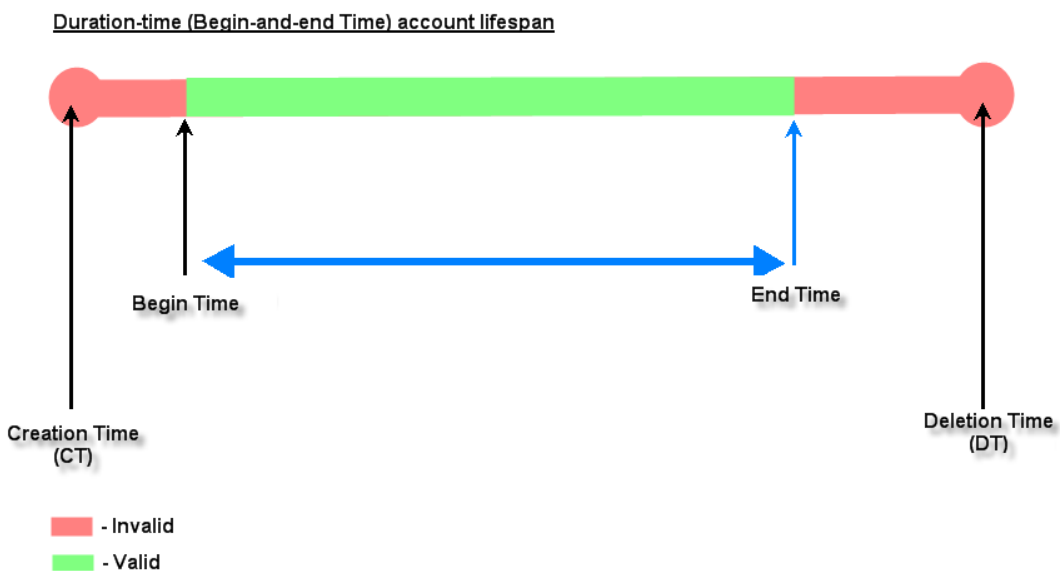
### 11.2.7. Duration-time with Begin-and-End Time

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.

## Billing Plan Configuration

Plan Number	1
Plan Type	Duration-time
Duration Type	<input type="radio"/> Elapsed Time <input checked="" type="radio"/> Begin-and-End Time <input type="radio"/> Cut-off Time
Begin Time	-- : -- , -- --
End Time	-- : -- , -- --
Number of devices	1 device(s) <small>Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).</small>
Unit Price	11 <small>The unit price cannot exceed 100000, and can take values up to two decimal places.</small>
Group	Group 1
Reference	



## 11.3 POS Printer Setup

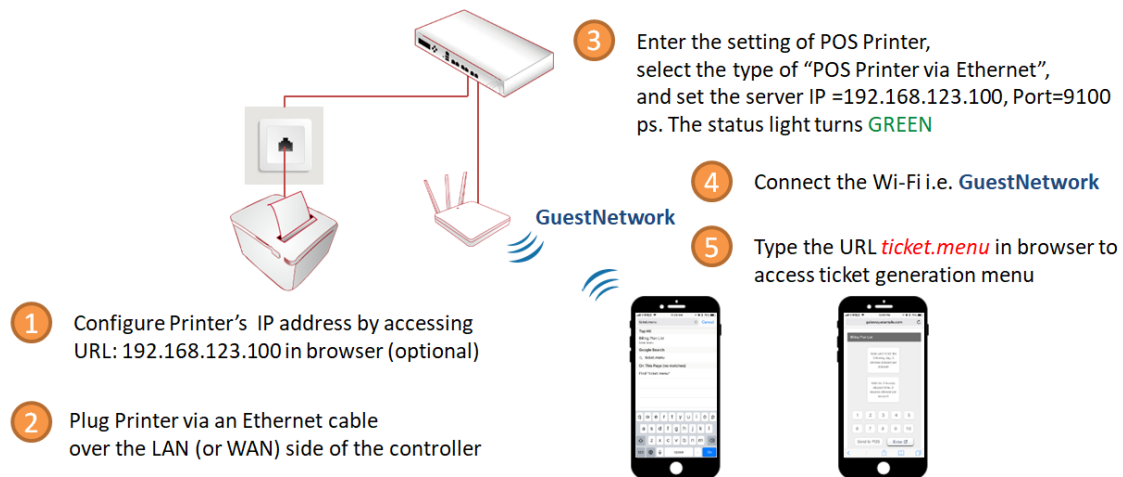
### Overview of Network Ticket Generator

Designed to support On-Demand account generation, EC-PP200 is able to print

tickets using the built-in On-Demand billing plan feature inside Edgecore Wireless LAN Controllers. What is noteworthy is that, EC-PP200 can be connected to 4pnet Controllers via Ethernet without additional equipment.

## Including EC-PP200 into Your Network

The following diagram shows a simple use case and quick setup to utilize EC-PP200 in your network.



1. Configure the IP address of EC-PP200.
2. Attach the EC-PP200 with Controller via Ethernet cable.
3. Fill the IP address and Port of the EC-PP200 in Terminal Server page of Controller.
4. Connect the network via Wi-Fi or Ethernet.
5. Access the Web Management Interface of the Controller to access ticket generation menu.

## Managing EC-PP200 on the Web Management Interface

EC-PP200 is designed specifically to operate in conjunction with all Edgecore Gateways/Controllers. Before connecting EC-PP200 to your Edgecore Gateway/Controller, some configurations steps are required.

Go to the Web Management Interface (WMI) for EC-PP200's relevant configurations.

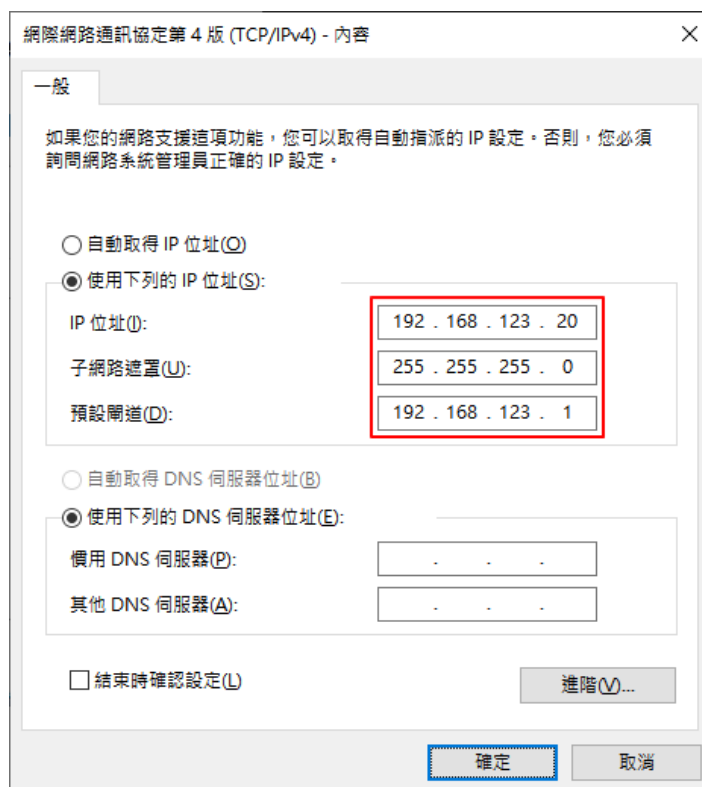


The default values are:

**IP address: 192.168.123.100**

**Subnet Mask: 255.255.255.0**

Remember to set the TCP/IP settings of the computer you use with a static IP address that is under the same subnet as EC-PP200. For example: 192.168.123.20.



In WMI of EC-PP200, modify the IP configuration in "Configure Interface" page. Make sure "Fixed IP Address" is configured.

## Ethernet WebConfig Version 1.00

Interface Status  
Printer Status  
Configure Interface

Reboot

**Configure Interface**  
Settings for the Ethernet Interface .

IP Address:  DHCP Client:  
DHCP Timeout (s) 90

Fixed IP Address:  
Device IP Address 192.168.1.123  
Subnet Mask 255.255.0.0  
Gateway Address 192.168.1.254

Restore Default Save Exit

After reboot the EC-PP200, use the new IP address to access the WMI, and check "Interface Status" of EC-PP200 is correct.

## Ethernet WebConfig Version 1.00

Interface Status  
Printer Status  
Configure Interface

Reboot

**Interface Status**  
View the current status of the interface module.

Mac Address 0-71-80-146-86-140  
IP Address 192.168.1.123  
Subnet Mask 255.255.0.0  
Gate Way 192.168.1.254  
DHCP Disabled  
DHCP Timeout 90

Refresh

### Setting Up EC-PP200 with the Edgecore Gateway/Controller

Configuration path: [Main Menu >> Users >> Internal Authentication >> On-Demand Authentication >> POS Printer Configuration](#)

Edgecore Gateway/Controller supports managing multiple POS Printers. To utilize EC-PP200 to print account tickets, administrator must add the IP address of the printers to Controller's list. Please follow the steps below to manage EC-PP200:

1. Create and enable Billing Plans. (Please refer to 11.1 and 11.2)
2. Configure POS ticket templates. (Please refer to 11.4)
3. Select "POS Printer via Ethernet", enter the IP address of the POS printer in the Server IP field. Select ticket template, and check the billing plans to be enabled.

## NOTE

1. When adding EC-PP200 to POS printer list, the port must be **9100**.

Main > Users > Internal Authentication > On-Demand Authentication > POS Printer Configuration

### POS Printer Configuration

Printer Type  POS Printer with Wireless Smart Device Serve  POS Printer via Ethernet

Status	Item	USB Printer ID	type	Remark	Ticket template	Billing plan
<input type="checkbox"/>	1	<input type="text"/>	USB	<input type="text"/>	Template 1 ▾	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>

(Total: 1) [First](#) [Prev](#) [Next](#) [Last](#)

Status	Item	Server IP	Port	Remark	Ticket template	Billing plan
<input type="checkbox"/>	1	10.73.36.123	9100	<input type="text"/>	Template 1 ▾	1 <input checked="" type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
<input type="checkbox"/>	2	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▾	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
<input type="checkbox"/>	3	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▾	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/>

## 11.4 Customizing POS Tickets

Configuration path: [Main Menu >> Users >> Internal Authentication >> On-Demand >> POS Tickets](#)

For deployment flexibility on your hotspot, customization of POS tickets using templates is supported on the EWS 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	<input checked="" type="radio"/> 4 characters <input type="radio"/> 8 characters
Ticket Type	Type 1 ▾ <input type="button" value="Restore"/>

For Usage-Time with expiration time & Volume

- An image can be uploaded (such as your company logo) in TMB format if needed.
- There are 2 Width types, 3" is recommended for EC-PP200.
- Select the desired language for the configured ticket template. EWS supports English, French, German, Japanese, Spanish, Simplified Chinese, and Traditional Chinese.
- For accounts generated with Ticket Menu, passwords are random, but the administrator has the option of selecting between a 4-character and an 8-character password.
- Select the appropriate Ticket Type depending on the configured billing plan.

**Type I**

<b>Parameters</b>	<div style="border: 1px solid black; padding: 2px;"> <span style="border-bottom: 1px solid black; display: inline-block; width: 100%;">\$remain</span> ▼         </div> <ul style="list-style-type: none"> <li style="background-color: #007bff; color: white; padding: 2px;">\$remain</li> <li>\$username</li> <li>\$username_without_postfix</li> <li>\$password</li> <li>\$usage</li> <li>\$price</li> <li>\$extid</li> <li>\$activationtime</li> <li>\$expiretime</li> <li>\$expire_time</li> <li>\$duration</li> <li>\$remark</li> <li>\$image</li> <li>\$unit</li> <li>\$date</li> <li>\$quota</li> <li>\$sprice</li> <li>\$qr</li> <li>\$max_user</li> </ul>	<input type="button" value="Insert Parameters"/>
Username: \$username Password: \$password Quota: \$quota Price: \$price ESSID: Activation: Before \$expire_time Expiration: \$duration days after activation	SN: \$remain	
<input type="button" value="Preview"/>		

You 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
●	1	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
●	2	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
●	3	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
●	4	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>

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 QR 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

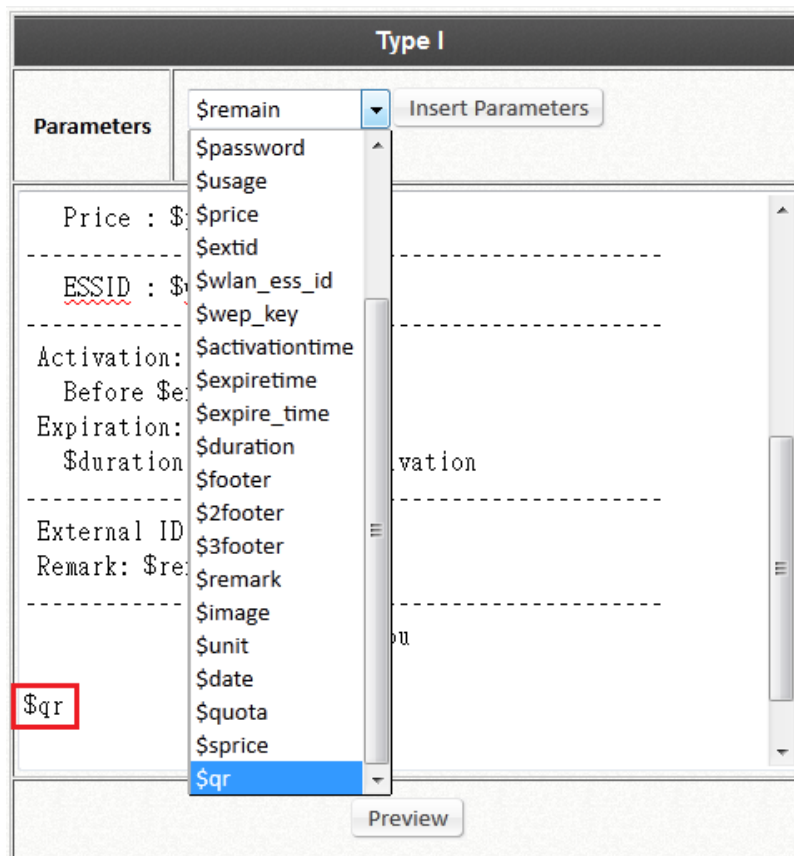
The ticket needs to be customized in order to support the printing of QR Code.

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	<input checked="" type="radio"/> 4 characters <input type="radio"/> 8 characters
Ticket Type	Type I ▾ <input type="button" value="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.

- 1) The width needs to be changed to 3" (default value = 2")
- 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.

## 11.5 Creating Accounts

Configuration path: [Main Menu >> Users >> On-Demand Accounts >> Accounts Creation](#)

Administrators have the option of creating single accounts or batch accounts. 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

Administrator can choose to use random generated Usernames and Passwords or custom-create them when creating batch On-Demand accounts. For random generated passwords, they can be short (4 characters) or long (8 characters).

## Creating Batch On-Demand Accounts

**Plan : Account Type** 1 : Usage-time

**Quota** 2 hr(s) of connection time quota with expiration

**Numbers**  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

**Valid Period** After activation, the account will be expired in 7 day(s)

**Total Price** 1.99

**Unit**  Number of units per ticket

**Group** Group 1

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

When creating custom Usernames, the Prefix and Postfix will be kept constant while



the Serial Number for the accounts will have single increments.

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

**Success**

Users have been successfully created.

## 11.6 User Self Service

### Credit Card via External Payment Gateway

Configuration path: [Main Menu >> Users >> Authentication >> On-Demand User >> External Payment Gateway](#)

EWS 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  \*(1~10)

[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 or if the SMS needs to be re-sent.

### PayPal Payment Page Configuration

Business Account  \*

Payment Gateway URL  \*

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	<input type="checkbox"/>	2 hr(s) of connection time quota with expiration	1.99	<input type="text"/>
2	<input type="checkbox"/>	Valid until 5:01 the following day	1	<input type="text"/>
3	<input type="checkbox"/>			<input type="text"/>
4	<input type="checkbox"/>			<input type="text"/>
5	<input type="checkbox"/>			<input type="text"/>
6	<input type="checkbox"/>			<input type="text"/>
7	<input type="checkbox"/>			<input type="text"/>
8	<input type="checkbox"/>			<input type="text"/>
9	<input type="checkbox"/>			<input type="text"/>
0	<input type="checkbox"/>			<input type="text"/>

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  \*(1~10) 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 or if the SMS needs to be re-sent.

**PayPal Payment Page Configuration**

Business Account  \*

Payment Gateway URL  \*

Identity Token  \*

Instant Payment Notification (IPN)  Enable  Disable  
 Behind NAT

Verify SSL Certificate  Enable  Disable

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

External Payment Gateway

**Selection**

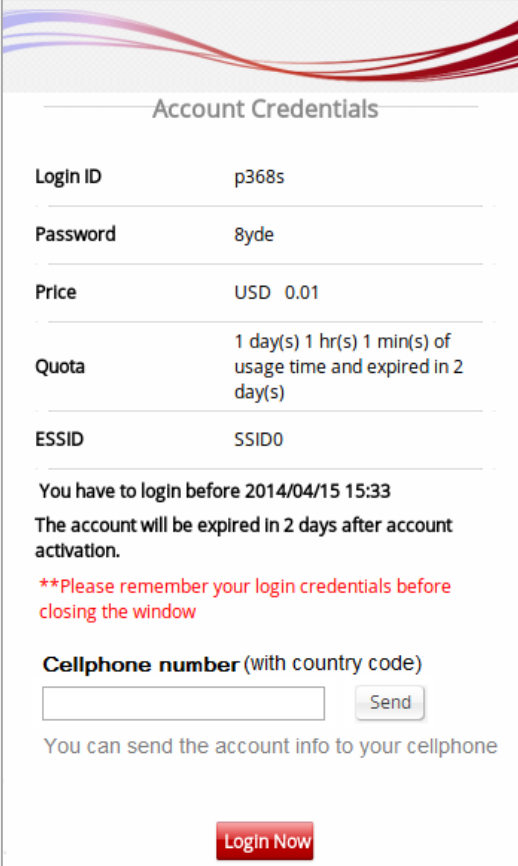
Disable  Authorize.Net  PayPal  SecurePay  WorldPay  PeleCard

Number of SMS retry  SMS gateway configure

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:



The screenshot shows a web page titled "Account Credentials" with a decorative header. It contains several fields and a "Login Now" button. The fields are:

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

Below the fields, there is a warning message: "You have to login before 2014/04/15 15:33. The account will be expired in 2 days after account activation." followed by a red note: "\*\*Please remember your login credentials before closing the window".

There is a section for "Cellphone number (with country code)" with an input field and a "Send" button. Below this is the text "You can send the account info to your cellphone".

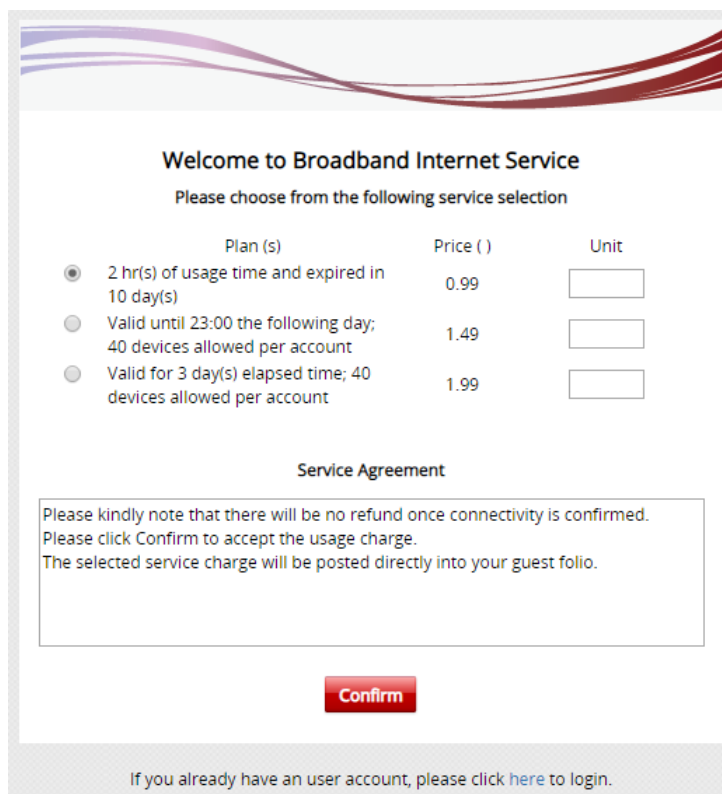
At the bottom, there is a red "Login Now" button.

## PMS Self Service

After planning your VLAN network and completing all the Port Location Mapping settings, you should verify whether the configurations are working properly. According to the Port Type set, when a user tries to access the internet from a VLAN mapped room, the pages or messages displayed are as follows:

When a user tries to access internet from a room, the browser will show the Login page with a list of available plans and service agreement. The Service

Agreement body can be configured at the applied Service Zone's Custom Pages settings. User may choose a billing plan, click the Confirm button and the system will display the generated account name and password. If you already have a user account, you can click the "**here**" link to login with the user account that you possess.



**Welcome to Broadband Internet Service**

Please choose from the following service selection

Plan (s)	Price ( )	Unit
<input checked="" type="radio"/> 2 hr(s) of usage time and expired in 10 day(s)	0.99	<input type="text"/>
<input type="radio"/> Valid until 23:00 the following day; 40 devices allowed per account	1.49	<input type="text"/>
<input type="radio"/> Valid for 3 day(s) elapsed time; 40 devices allowed per account	1.99	<input type="text"/>

**Service Agreement**

Please kindly note that there will be no refund once connectivity is confirmed. Please click Confirm to accept the usage charge. The selected service charge will be posted directly into your guest folio.

**Confirm**

If you already have an user account, please click [here](#) to login.

## Chapter 12. PMS Integration

This section introduces the Port Location Mapping feature used with PMS integration. This feature is designed for creating multiple VLAN divisions (as if they were separate LAN ports) under a Service Zone and mapping these VLANs to different locations individually. This feature can be utilized to provide separate VLAN to separate clients in MTU/MDU deployments where a VLAN switch is deployed under the gateway to provide VLAN connection to individual rooms.

The Port Location Mapping feature is also commonly used in hospitality venues to manage the internet service for their guest rooms and public areas. In addition it can operate in conjunction with third party hospitality applications and has been tested with the Net Retriever middleware which provides seamless integration between the gateway and the popular High Speed Internet Access (HSIA) hardware and Front Office System (FOS) software.

Each Port Location Mapping entry can be configured to provide charged (single or multiple user), free or blocked internet service at the location corresponding to the entry's VLAN Tag. Please note that for charged service to work, it is required that at least one or more On-Demand Billing Plans are created, allowing the user to choose a desired plan to pay for their internet access.

### NOTE

1. EWS Controllers default support Micros PMS, InnKeyPMS, and IDS interfaces. If you require dedicated support in creating or customizing your own interfacing hospitality software, please contact your Edgecore sales representative.
- 

### 12.1 Hotel Room Location Mapping

Configuration path: [Main Menu >> System >> 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. Before the configuration of the PMS Middleware or adding VLANs to a Service Zone, the Port Mapping feature must be enabled first.

The screenshot shows a web interface for configuring Port Location Mapping. The 'Create' section is highlighted with a red box, indicating the 'Status' field is the focus. The 'Status' field has two radio buttons: 'Enable' (selected) and 'Disable'. An 'Apply' button is next to it. Below this, there are several other fields: 'Mapping' with a 'Create' button; 'Subinterface' with a 'Use LAN Port' dropdown set to 'LAN1', a 'Subinterface ID' text input with a placeholder 'Enter a Number Here', and a 'Remark' text input with a placeholder 'Optional'. At the bottom of this section are 'Add' and 'Cancel' buttons. Below the 'Create' section is a 'Lists' section with three rows: 'PLM List', 'Subinterface List', and 'Tunnel PLM List', each with a 'Show' button.

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.
- 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** 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.

## NOTE

1. VLAN Ports may be created one by one or batch at once. Subsequent changes are possible by Change Port Type configuration box.
2. 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.

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. Clicking the **Delete** link can erase an individual Port Location Mapping profile. Clicking **Delete All** button will erase all of the Port Location Mapping profiles.

Port Location Mapping List

All ▾

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

## 12.2 PMS Configuration

Configuration path: [Main Menu >> System >> PMS Interface](#)

In PMS Interface Configuration page, administrator may choose to select the interface type that is compatible with their site's hospitality management system or PMS system.



## PMS Interface Configuration

---

<b>PMS Interface Type</b>	<input type="radio"/> Disable <input checked="" type="radio"/> <b>Micros Opera</b> <input type="radio"/> InnKeyPMS <input type="radio"/> IDS		
<b>PMS IP Address</b>	<input type="text" value="10.29.42.101"/>		
<b>PMS Port</b>	<input type="text" value="5010"/>		
<b>Account Credentials</b>	Username	<input type="text" value="RN ▼"/>	
	Password	<input type="text" value="RN ▼"/>	
<b>Room Bill Description</b>	<input type="text" value="Wireless Access"/>		
<b>Login Error Message</b>	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">An error has occurred during login. Please contact the front desk for assistance.</div>		
<b>User Account Log</b>	<input type="button" value="View"/>		
<b>Synchronize Data with PMS</b>	<input type="button" value="Sync"/>		
<b>PMS External Page Customization API</b>	<input type="radio"/> Disable <input checked="" type="radio"/> <b>Enable</b>		
<b>External Page Validity Verification</b>	Username	<input type="text" value="adminkey"/>	
	Password	<input type="text" value="adminkey"/>	
<b>Sample External Login Page</b>	<input type="button" value="Download"/>		

### Micros Opera / IDS

When the interface type is Micros Opera or IDS, fill in the PMS IP and Port as configured on the PMS system end. 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 protocol parameter for carrying the username and password information. More information on Micros Opera Users may also be monitored from the On-Demand Account List.

## On-Demand Account List

Buttons: Delete, Restore List, Backup List, Delete Expired, Delete Out of Quota, **PMS Micros Opera**, Search

■	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
<input type="checkbox"/>	1	16 hr(s) 9 min(s) 8 sec(s)	Expired	Group 1			
<input type="checkbox"/>	pf3k	Until 2013/10/29-12:30	Expired	Group 1	roomN-100-9C:EB:EB:0B:76:8B		
<input type="checkbox"/>	8krm	Until 2013/10/29-22:11	Expired	Group 1	122		
<input type="checkbox"/>	gtum	Until 2013/10/29-22:11	Expired	Group 1	aaaa		
<input type="checkbox"/>	6uw5	Until 2013/10/29-22:11	Expired	Group 1	111		
<input type="checkbox"/>	4257	Until 2013/10/29-22:11	Expired	Group 1	xx		
<input type="checkbox"/>	qr6e	Until 2013/10/29-22:11	Expired	Group 1	aaq		

## Micros Opera User List

Buttons: On-Demand Account List, Search

G#	GN	RN	Username	Password	Remaining Quota	Status	Group
0123456789	0123456789	102	102	0123456789	Until 2013/11/06-22:11	Normal	Group 1

## Innkey PMS

When the interface type is Innkey PMS, Query API, Post API and Shared Key of the PMS system are requisite information for integration. Room Number and Guest Number will be the user account credentials.

## PMS API for External Login Page

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. Administrator also could utilize its own username and password to secure the API protocol between external web server and EWS Controller. Furthermore, there is a downloadable example which administrator could easily modify from.

Please note that PMS API for External Login Page is available for Micros Opera and IDS interface only.

# **Chapter 13. Account Roaming**

## **13.1 Roaming Related**

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.

EWS Controllers support the WISPr attributes required to establish roaming relationship with most roaming brokers in the market such as Boingo, iPass Connect etc.

For more in depth support regarding compatibility and technical evaluation on your telecom operator, please contact Edgecore support team.

## **13.2 WISPr for ISP Roaming**

Configuration path: [Main Menu >> System >> Service Zones >> Service Zone Configuration](#)

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.

If a RADIUS server has been configured, the WISPr attributes used during RADIUS authentication can be defined here in this Service Zone.

## WISPr Configuration

<b>WISPr Smart Client</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>Smart Client Black List</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
	<input type="text"/>
	<small>(Separate by comma)</small>
<b>WISPr Location ID</b>	ISO Country Code <input type="text"/> <small>(e.g. US)</small>
	E.164 Country Code <input type="text"/> <small>(e.g. 1)</small>
	E.164 Area Code <input type="text"/> <small>(e.g. 408)</small>
	Network (SSID/ZONE) <input type="text"/> <small>(e.g. MYWIFI)</small>
<b>WISPr Location Name</b>	Hotspot Operator <input type="text"/> <small>(e.g. MYISP)</small>
	Location <input type="text"/> <small>(e.g. Lobby_of_Airport)</small>
<b>WISPr Billing Time</b>	<input type="text" value="0"/> : <input type="text" value="0"/> <small>(HH:MM)</small>

**WISPr Smart Client:** Select 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:** Set RADIUS account billing time.

## 13.3 Cross Gateway Roaming

Configuration path: [Main Menu >> Network >> Client Mobility](#)

Cross Gateway roaming feature enables an end user to seamlessly move around large network deployment where there are multiple Controllers in service. Normally when a user moves from edge AP to another edge AP that is managed by another 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 not experience 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 Controller to be Master Node, and another Controller to be Slave Node. Make sure that the Secret Key and both Controller's WAN interface are routable.

Configure Slave Node's IP address and secret key.

### Cross Gateway Roaming

Mode  Disable  Master Mode  Slave Mode

Status

Slave Nodes Setting	No.	Active	Remote IP Address*	Secret Key*	Remark
	1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Configure the Slave Node's Master Node and secret key.

### Cross Gateway Roaming

Mode  Disable  Master Mode  Slave Mode

Status

Master Node Setting

Remote IP Address  \*

Secret Key  \*

Remark

## 13.4 Local / On-Demand Account Roaming Out

The built-in user account databases both Local and On-Demand of the EWS Controller may be used for other Controllers as their external RADIUS authentication database.

This application offers the ability to refer to a single central Controller for account credential lookup during the authentication process, and is ideal for enterprises or businesses with multiple branch offices.

To use Local user database as the RADIUS database of another Controller:

Configuration path: [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](#)

[Apply](#) [Cancel](#)

To use On-Demand user database as the RADIUS database of another Controller: Configuration path: [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)

On-Demand Access Code:  Enable to login with an On-Demand Access Code, not only an On-Demand Account

Smart Login:  Enable to allow On-Demand users to login automatically within 10 Days

Set Ticket's Serial Number: 000020 [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.

POS Printer: [Configure](#)

Payment Gateway: [Configure](#)

SMS Gateway: [Configure](#)

Email Verification: [Configure](#)

Account Roaming Out:  Enable  Disable

Blacklist: None

[RADIUS Client Device Settings](#)

## RADIUS Client Device Settings

No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	Roaming Out	10.30.40.45	255.255.255.255 (/32)	••••	
2	Disable		255.255.255.255 (/32)		
3	Roaming Out		255.255.255.255 (/32)		
4	802.1X DM & CoA		255.255.255.255 (/32)		
5	Disable		255.255.255.255 (/32)		
6	Disable		255.255.255.255 (/32)		
7	Disable		255.255.255.255 (/32)		
8	Disable		255.255.255.255 (/32)		

After enabling the Roaming out feature for Local or On-Demand, click the RADIUS Client Device Settings hyperlink. The redirected page allows the administrator to specify the Controller IP which is allowed to behave as a RADIUS client and authenticate against this Controller's enabled user databases.

### NOTE

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



# Chapter 14. VPN

## 14.1 Site-to-Site

Configuration path: [Main Menu >> Network >> VPN](#)

EWS Controller supports **Site-to-Site VPN** for more than 2 EWS Controllers to create VPN tunnel to each other over the WAN network. For example, if there are 2 EWS Controllers, you can create a VPN tunnel to let a subnet of one EWS Controller to access the subnet of another EWS Controller.

Site-to-Site VPN

Local Sites

Add... Delete

No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Test Tunnel to Remote IP
-----	-------------------	-----------------	--------------------	--------------------	--------------------------

Remote Sites

Add... Delete

No.	Name	IP Address	Pre-shared Key
-----	------	------------	----------------

Apply Cancel

First, you need to add a Remote Site with at least one remote subnet.

### Remote Site Configuration

Name

IP Address

Authentication Method

Pre-shared Key

Phase1 Proposal Encryption   
Authentication

Diffie-Hellman Group  Group 1  Group 2  Group 5

IKE Life Time   (The time is a 5-digit number; e.g. 36h stands for 1 day and 12 hours)

Dead Peer Detection DPD Delay  (second)  
DPD Timeout  (second)

Remote Subnet

No.	Network	Mask
1	<input type="text"/>	<input type="text" value="255.255.255.255 (32)"/>
2	<input type="text"/>	<input type="text" value="255.255.255.255 (32)"/>

**NOTE**

1. The IPsec settings in both sites must be same.

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

### Local Site Configuration

Local Interface

Remote VPN Gateway

Local Host/Subnet  Host  Subnet

Remote Host/Subnet

Phase2 Proposal Encryption   
Authentication

Key Life Time   ( 1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)

Rekey  Enable Rekey  
Rekey Margin   ( 1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)

Perfect Forward Secrecy  Enable PFS  
PFS Group

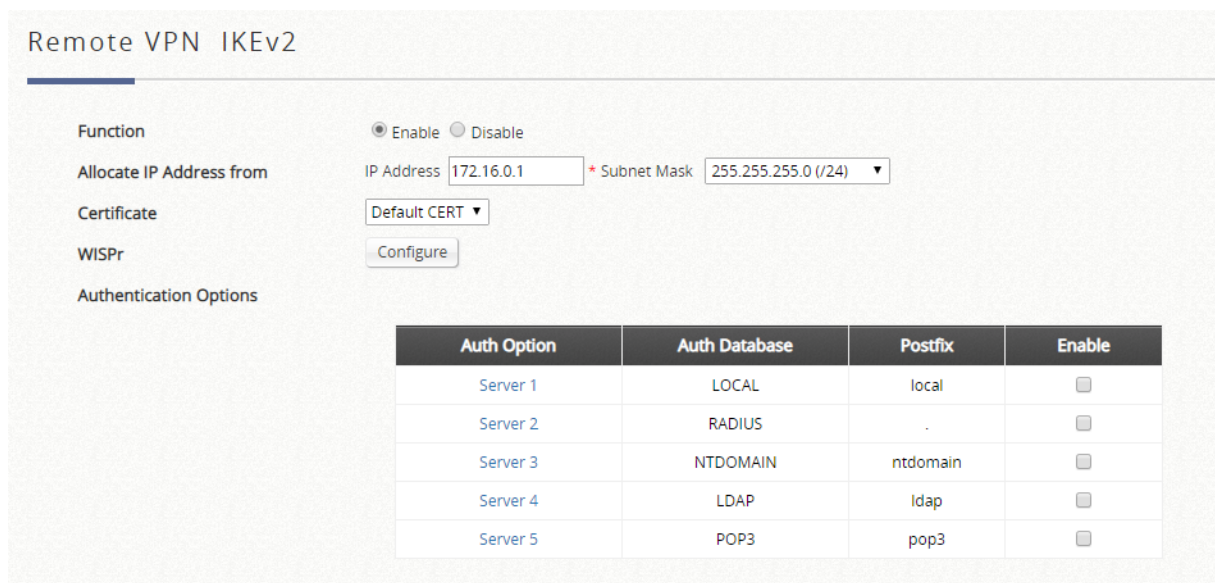
## NOTE

1. 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.

## 14.2 Remote Client

Configuration path: [Main Menu >> Network >> VPN](#)

EWS 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 EWS Controller is under the service zone locally. The data transferred between the remote user and the controller will be encrypted with **IKEv2** VPN tunnel. Policy can also be applied and users are controlled by system to access the network.



Remote VPN IKEv2

Function  Enable  Disable

Allocate IP Address from IP Address  \* Subnet Mask  ▾

Certificate  ▾

WISPr

Authentication Options

Auth Option	Auth Database	Postfix	Enable
Server 1	LOCAL	local	<input type="checkbox"/>
Server 2	RADIUS	.	<input type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="checkbox"/>
Server 4	LDAP	ldap	<input type="checkbox"/>
Server 5	POP3	pop3	<input type="checkbox"/>

All settings are similar to the settings in a Service Zone. Remote VPN can also be setup with a dedicated **subnet**, **Certificate**, **WISPr** configuration and **Authentication Options**.

After Remote VPN is enabled, users can use the VPN tool on the client devices to setup the VPN link with the username and password from enabled authentication

options.

#### **NOTE**

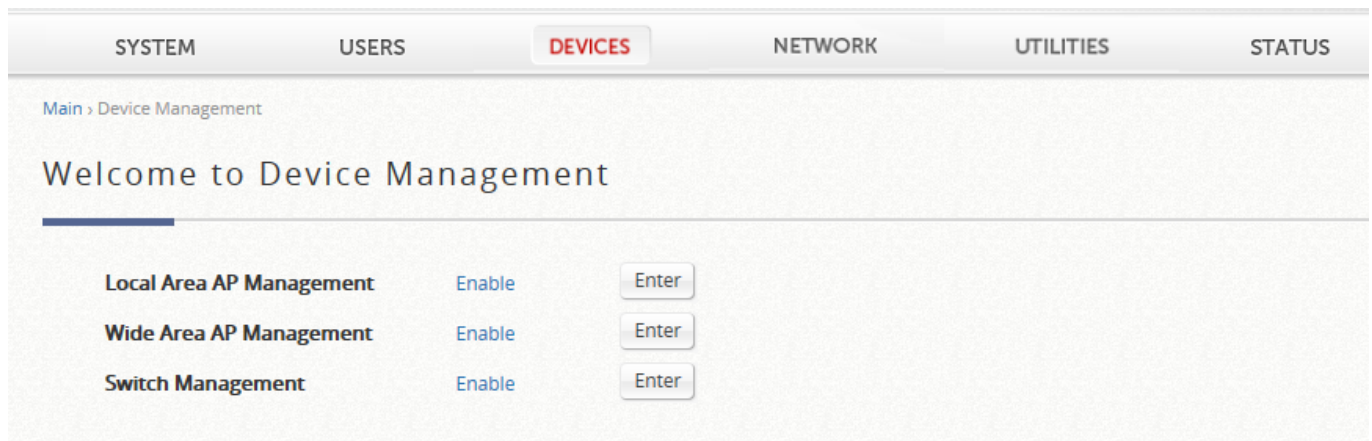
1. The Remote VPN clients can be applied by different user policies at the page of [Main Menu >> Users >> Groups >> Configuration](#).
-

# Chapter 15. Switch Management

The EWS Controller gives administrators one comprehensive interface for managing your Edgecore switches.

## 15.1 Switch List

Configuration path: [Main Menu >> Devices >> Switch Management >> Switch List](#)



Switches connected either to a WAN port or LAN port of the EWS Controller can be added manually or by discovery.

The screenshot shows the 'Add Switch' form. At the top, there is a dropdown menu for 'Add Method' set to 'Add Switch'. Below the title 'Add Switch', there are several input fields:

- Device Type: ECS2100-10P (dropdown)
- Device IP: [ ] \*
- Device MAC: [ ] \*
- Device Name: [ ] \*
- Login ID: admin
- Password: [ ] \*
- SNMP Community Read: [ ] \*

Once the Switch is successfully added to the list, we can see that its Status is now shown:

## Switch List

Status

<input type="checkbox"/>	Name	Type	Status	IP address	MAC address	Total allocated/Used/Max supply power [W]	Switch UI
<input type="checkbox"/>	TestSW	ECS2100-10P	Offline	10.73.36.210	AA:BB:CC:DD:EE:FF	Switch Offline	<input type="button" value="Go to"/>

The Switch List displays the Switch Name, Switch Type, Status, IP Address, MAC Address, Power Budget, and a shortcut link to the Switch’s management web interface.

## 15.2 PoE Schedule Template

Configuration path: [Main Menu >> Devices >> Switch Management >> PoE Schedule Template](#)

The PoE Schedule Template allows administrators to set a schedule for delivering power on the assigned ports of the managed switch. This function can be used to control AP schedules when the APs are powered by PoE from the managed switch.

Main > Switches > PoE Template

### PoE Schedule Template

Template Name	Copy Settings From	Remark	Action
<input type="text" value="Default"/>	<input type="text" value="NONE"/>	<input type="text"/>	<input type="button" value="✎"/>

Templates may be added, or customized by clicking the pencil icon.

## Template Edit - Power supply schedule : Template\_2

<input type="checkbox"/>	Day	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
<input type="checkbox"/>	Sun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Mon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Tue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Wed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Thu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Fri	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Sat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## Apply to

Refresh  ▾

<input type="checkbox"/>	Port	PoE Mode	Connected Device	<input type="checkbox"/>	Port	PoE Mode	Connected Device
<input type="checkbox"/>	1			<input type="checkbox"/>	13		
<input type="checkbox"/>	2			<input type="checkbox"/>	14		
<input type="checkbox"/>	3			<input type="checkbox"/>	15		
<input type="checkbox"/>	4			<input type="checkbox"/>	16		
<input type="checkbox"/>	5			<input type="checkbox"/>	17		
<input type="checkbox"/>	6			<input type="checkbox"/>	18		
<input type="checkbox"/>	7			<input type="checkbox"/>	19		
<input type="checkbox"/>	8			<input type="checkbox"/>	20		
<input type="checkbox"/>	9			<input type="checkbox"/>	21		
<input type="checkbox"/>	10			<input type="checkbox"/>	22		
<input type="checkbox"/>	11			<input type="checkbox"/>	23		
<input type="checkbox"/>	12			<input type="checkbox"/>	24		

## 15.3 Backup Configuration

Configuration path: [Main Menu >> Devices >> Switch Management >> Backup Configuration](#)

Backup Configuration displays a list of backed up configuration from a managed switch. Configuration can be saved to this list by selecting a switch and clicking "Backup".

# Chapter 16. Platform Dependent Features

## 16.1 WiFi Monitor

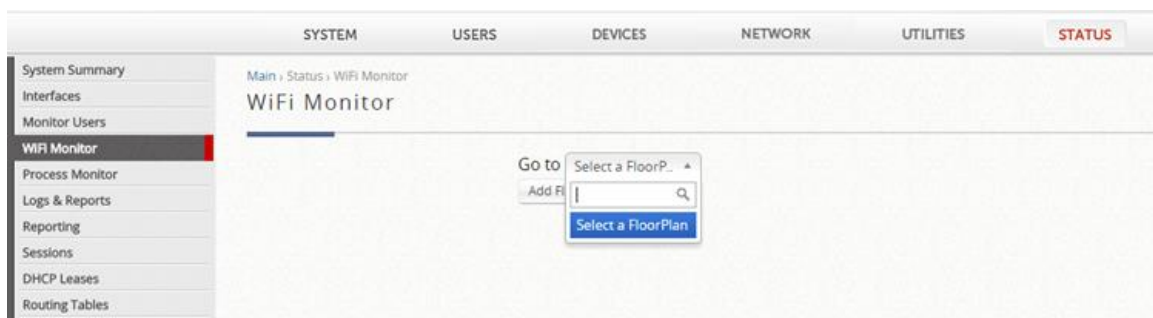
WiFi Monitor allows the administrator to simulate WiFi signal coverage of Access Points; be it a virtual area or a real managed APs signal coverage. It also monitors AP statuses and statistic information of the managed APs.

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.

### 16.1.1. 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 or .osm 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

Apply Cancel



Managed AP Simulation is 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.

Access Points here are linked to APs managed by the EWS 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.

Main > Status > WiFi Monitor

### WiFi Monitor

Add Managed AP

Go to TEST

Add Floor Plan Edit

Status AP

Not on Floor Plan

ECW5211-L

On Floor Plan

Remove All AP Delete All AP


Add Managed AP

AP Model: All

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

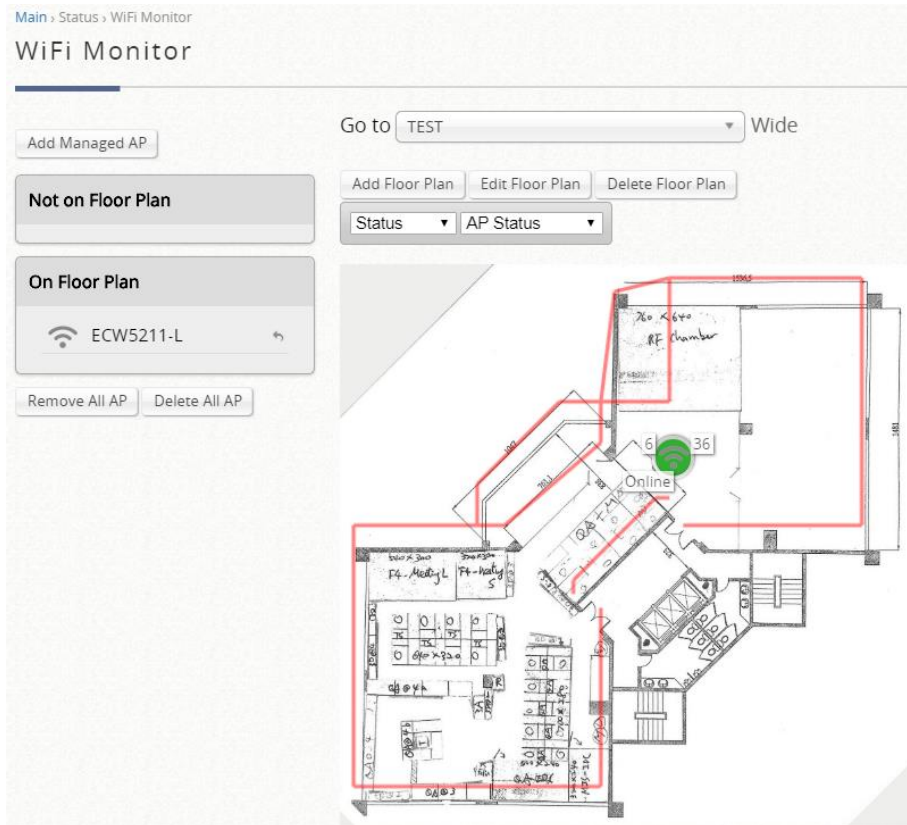
<input checked="" type="checkbox"/>	Name	IP	MAC
<input type="checkbox"/>	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D

Add

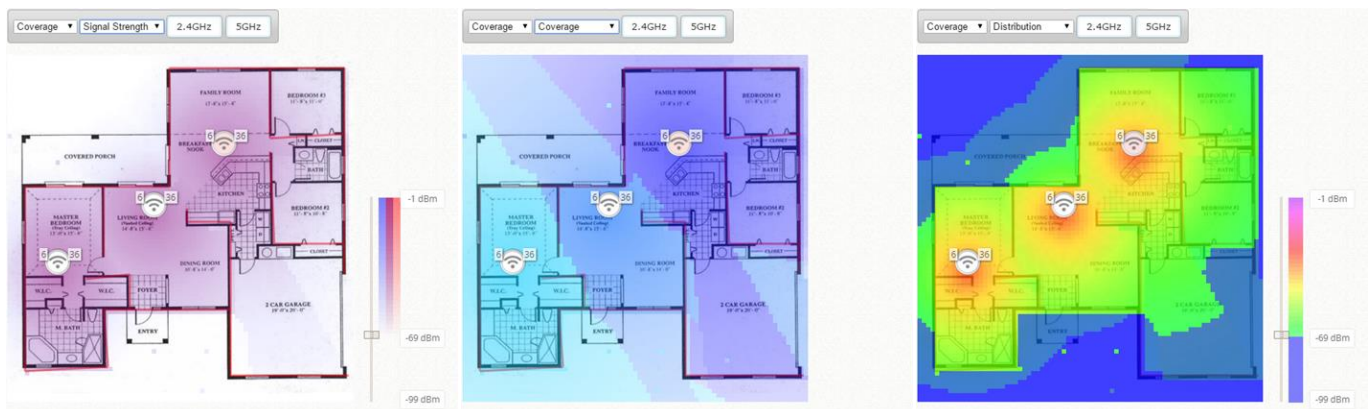


Once these managed APs are created, simply drag and drop these APs onto the floor plan. 2.4GHz is indicated blue and 5GHz is indicated red for signal strength

(hence purple when both bands are overlapping).



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



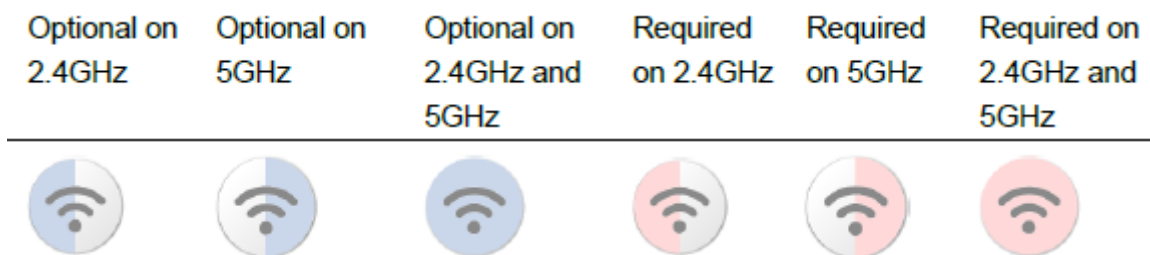
### 16.1.2. Simulation AP

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.

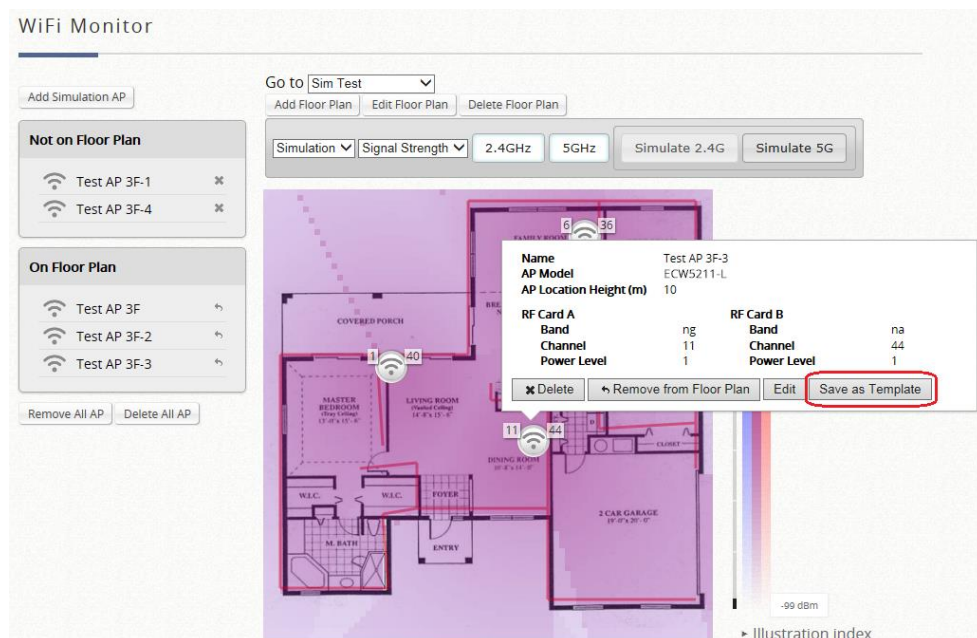
With the floor plan and partitions in place, simulation APs can now be added to the floor plan for simulation as shown below.



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.



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

### 16.1.3. AP Monitoring on floorplan

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.

WiFi Monitor

Go to TEST

Add Managed AP

Not on Floor Plan

On Floor Plan

ECW5211-L

Remove All AP Delete All AP

Add Floor Plan Edit Floor Plan Del

Status AP Status

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

Delete Remove from Floor Plan Refresh

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.

WiFi Monitor

Go to TEST

Add Managed AP

Not on Floor Plan

On Floor Plan

ECW5211-L

Remove All AP Delete All AP

Add Floor Plan Edit Floor Plan Del

Statistics Device Density

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

Delete Remove from Floor Plan Refresh

# Appendix A. VEWS Installation on Linux System

## Prerequisite

- One Server running on Linux system. Ubuntu v18.04 is used as an example in this document.
- VEWS image file in qcow2 format. Please contact [ecwifi@edge-core.com](mailto:ecwifi@edge-core.com) to get the image file.
- Setting file of VM environment "V-EWS.xml". Please contact [ecwifi@edge-core.com](mailto:ecwifi@edge-core.com) to get the template file.
- VEWS voucher code. Please contact Edge-core sales or [ecwifi@edge-core.com](mailto:ecwifi@edge-core.com) to get the voucher code for corresponding license

## Step 1. Install KVM on Ubuntu system

Please open terminal and run "sudo apt install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils virtinst"

```
root@v-ews:/# apt install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils virtinst
```

After installation, to verify that libvirt daemon is running, run "systemctl is-active libvirtd"

```
root@v-ews:/var/lib/libvirt/images# systemctl is-active libvirtd
active
```

## Step 2. Modify system network configuration

To make sure the VM can access the network via the physical interface, it is required to create a bridge interface to bridge the physical Ethernet interface and the virtual network interface. The screenshot below shows an example to configure the network via Netplan tool. In this example, the bridge interface is named as br0 and the physical network interface is ens33.

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: false
  bridge:
    br0:
      dhcp4: true
      interfaces:
        - ens33
  version: 2
```

### Step 3. Edit XML file to match the environment

- Modify VM name in <domain> <name> element.

Below screenshot shows an example with using the name "V-EWS".

```
<domain type='kvm'>
  <name>V-EWS</name>
  <memory unit='KiB'>1048576</memory>
  <currentMemory unit='KiB'>1048576</currentMemory>
  <vcpu placement='static'>2</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
```

- Modify VM disk path in <domain> <device> <disk> <source> element. The path of the VEWS image file should be filled here.

Below screenshot shows an example when the VEWS image path is

"/var/lib/libvirt/images/Edgecore\_V-EWS\_3.43.S0\_1.55.4.1-1.9481.2.33.2.38.qcow2"

```
<disk type='file' device='disk'>
  <driver name='qemu' type='qcow2' />
  <source file='/var/lib/libvirt/images/Edgecore_V-EWS_3.43.V1_1.5-1.9481.2.46.4.8.qcow2' />
  <target dev='vda' bus='virtio' />
  <alias name='virtio-disk0' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0' />
</disk>
```

- Modify VM NIC in <domain> <device> <interface> <source> element.

In the example, the mode is "bridge" and the NIC of the VM will be bridge into br0.

```
<interface type='bridge'>
  <source bridge='br0' />
  <target dev='vnet0' />
  <model type='virtio' />
  <alias name='net0' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0' />
</interface>
```

### Step 4. Copy image file

Copy the VEWS image file to "/var/lib/libvirt/images/".

```
root@vincent-Aspire-4752:/var/lib/libvirt/images# ls -al
total 149132
drwx--x--x 2 root      root      4096  五  23 14:58 .
drwxr-xr-x 7 root      root      4096  五  23 13:27 ..
-rw-r--r-- 1 libvirt-qemu kvm 152698880  五  23 12:10 Edgecore_V-EWS_3.43.V1_1.5-1.9481.2.46.4.8.qcow2
-rw-r--r-- 1 root      root      1792   五  23 14:58 V-EWS.xml
root@vincent-Aspire-4752:/var/lib/libvirt/images#
```

## Step 5. Create and start VM

Use the commands below to create and start the VM.

- virsh define V-EWS.xml.

```
root@vincent-Aspire-4752:/var/lib/libvirt/images# virsh define V-EWS.xml
Domain V-EWS defined from V-EWS.xml
```

- virsh start V-EWS

```
root@vincent-Aspire-4752:/var/lib/libvirt/images# virsh start V-EWS
Domain V-EWS started
```

- virsh list (make sure VM is running)

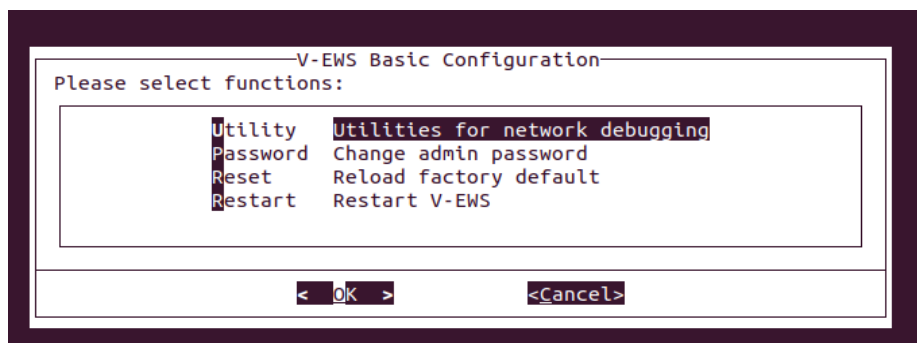
```
root@vincent-Aspire-4752:/var/lib/libvirt/images# virsh list
 Id   Name           State
-----
  1   V-EWS          running
```

## Step 6. Get default IP from console of VM

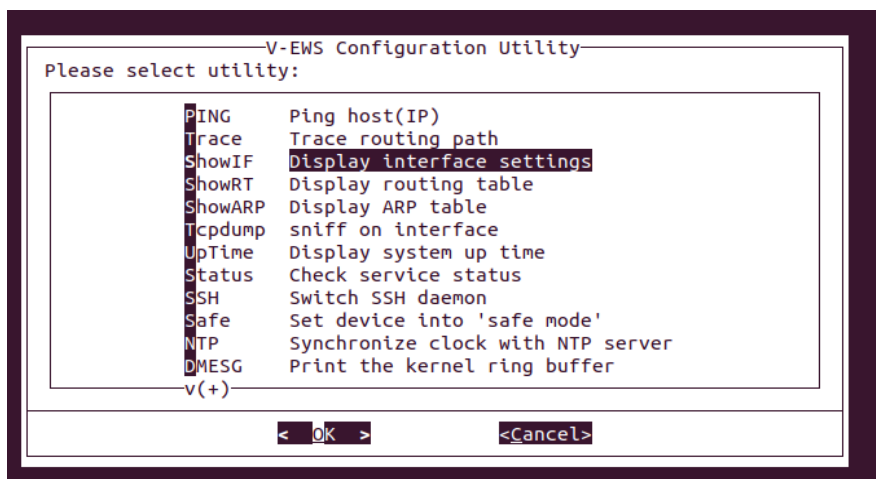
- Run "virsh console V-EWS" to enter console mode.

```
root@vincent-Aspire-4752:/var/lib/libvirt/images# virsh console V-EWS
Connected to domain V-EWS
Escape character is ^]
^]
```

- Press "Enter", and select "Utility"



- Select "ShowIF"





- Check the IP address of WAN1

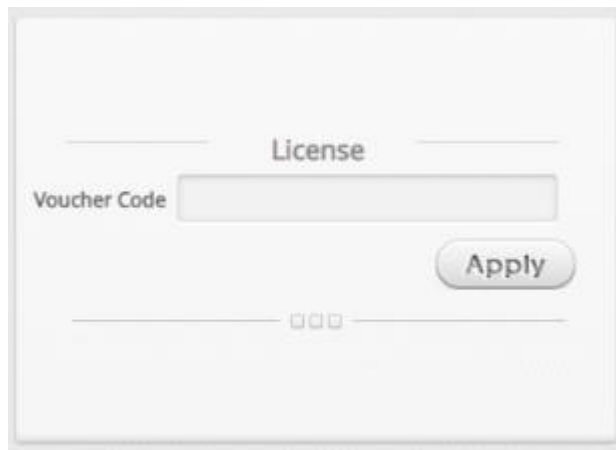
```
WAN1:
  Link encap:Ethernet  HWaddr 52:54:00:24:8C:86
  inet addr:10.71.1.120  Bcast:10.71.255.255  Mask:255.255.0.0
  UP BROADCAST RUNNING MULTICAST  MTU:1400  Metric:1
  RX packets:5318 errors:0 dropped:633 overruns:0 frame:0
  TX packets:403 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:510213 (498.2 KiB)  TX bytes:58533 (57.1 KiB)

Default:
  Link encap:Ethernet  HWaddr FA:61:66:87:D7:E7
  inet addr:192.168.1.254  Bcast:192.168.255.255  Mask:255.255.0.0
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

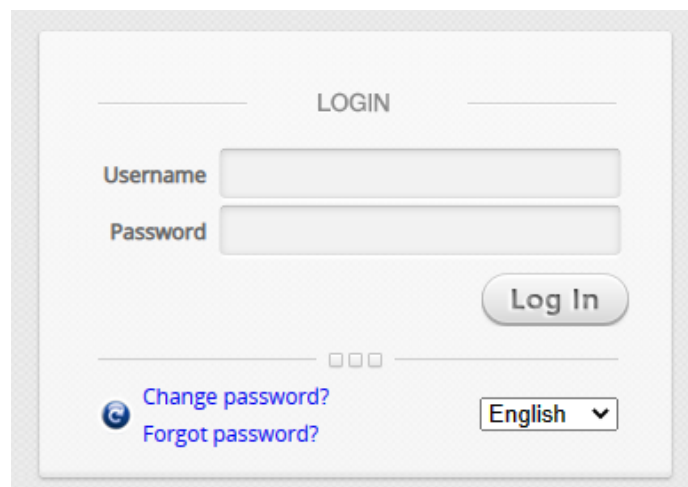
Press ENTER to continue
```

### Step 7. Activate VEWS

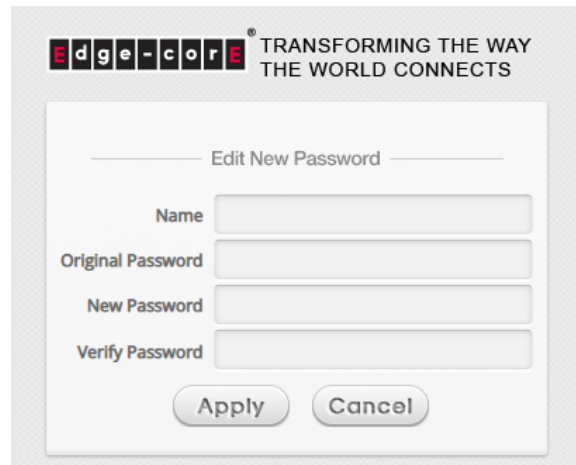
- Open the browser and connect to <http://<WAN1 IP>/>.



- Input the voucher code and click Apply. If the voucher code is valid, it will be redirected to the login page.

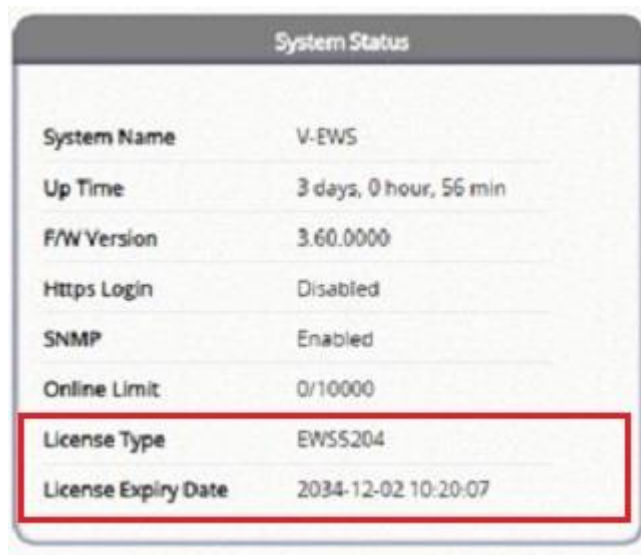


- Enter the default username is "admin" and the default password is "admin". Follow the instruction to change the password and then you can login with the new password.



The image shows the Edge-CorE logo at the top left, with the tagline "TRANSFORMING THE WAY THE WORLD CONNECTS" to its right. Below the logo is a form titled "Edit New Password". The form contains four input fields: "Name", "Original Password", "New Password", and "Verify Password". At the bottom of the form are two buttons: "Apply" and "Cancel".

- The license information can be checked in the dashboard.



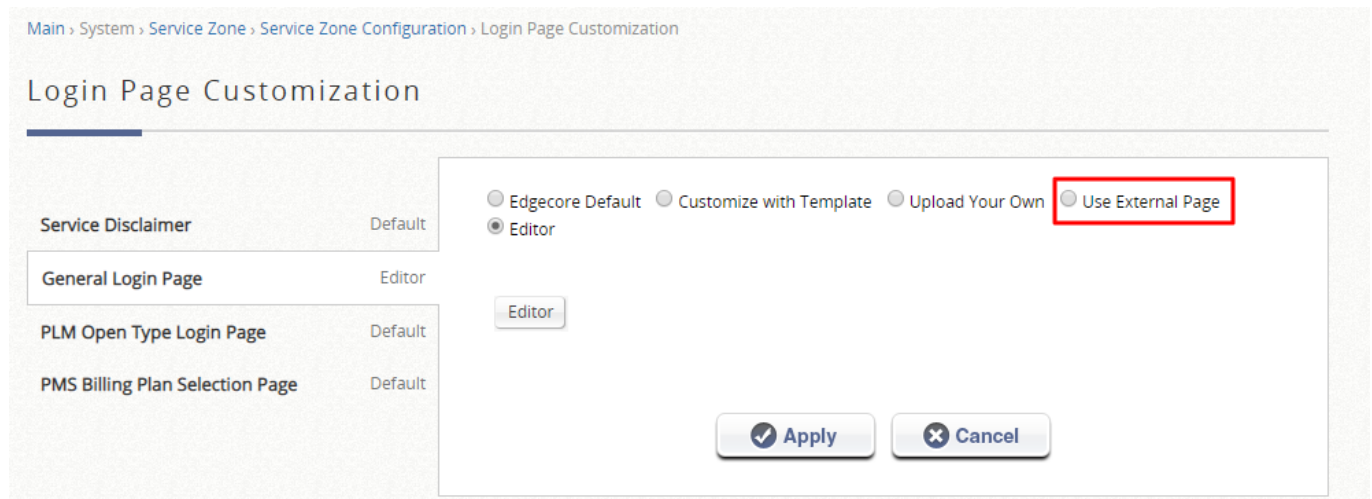
The image shows a screenshot of the "System Status" dashboard. The dashboard displays various system parameters in a table format. The "License Type" and "License Expiry Date" rows are highlighted with a red border.

System Status	
System Name	V-EWS
Up Time	3 days, 0 hour, 56 min
F/W Version	3.60.0000
Https Login	Disabled
SNMP	Enabled
Online Limit	0/10000
License Type	EWSS204
License Expiry Date	2034-12-02 10:20:07

## Appendix B. External Pages

### External Page Concept

Choose External Page if you desire to use an external web page for your custom pages. Simply enter the URL of your external webpage, click Preview button to check if it is reachable, take a look at how your external webpage will be displayed, then click Apply button.



*Main Menu>System>Service Zone>Service Zone Configuration>Login Page*

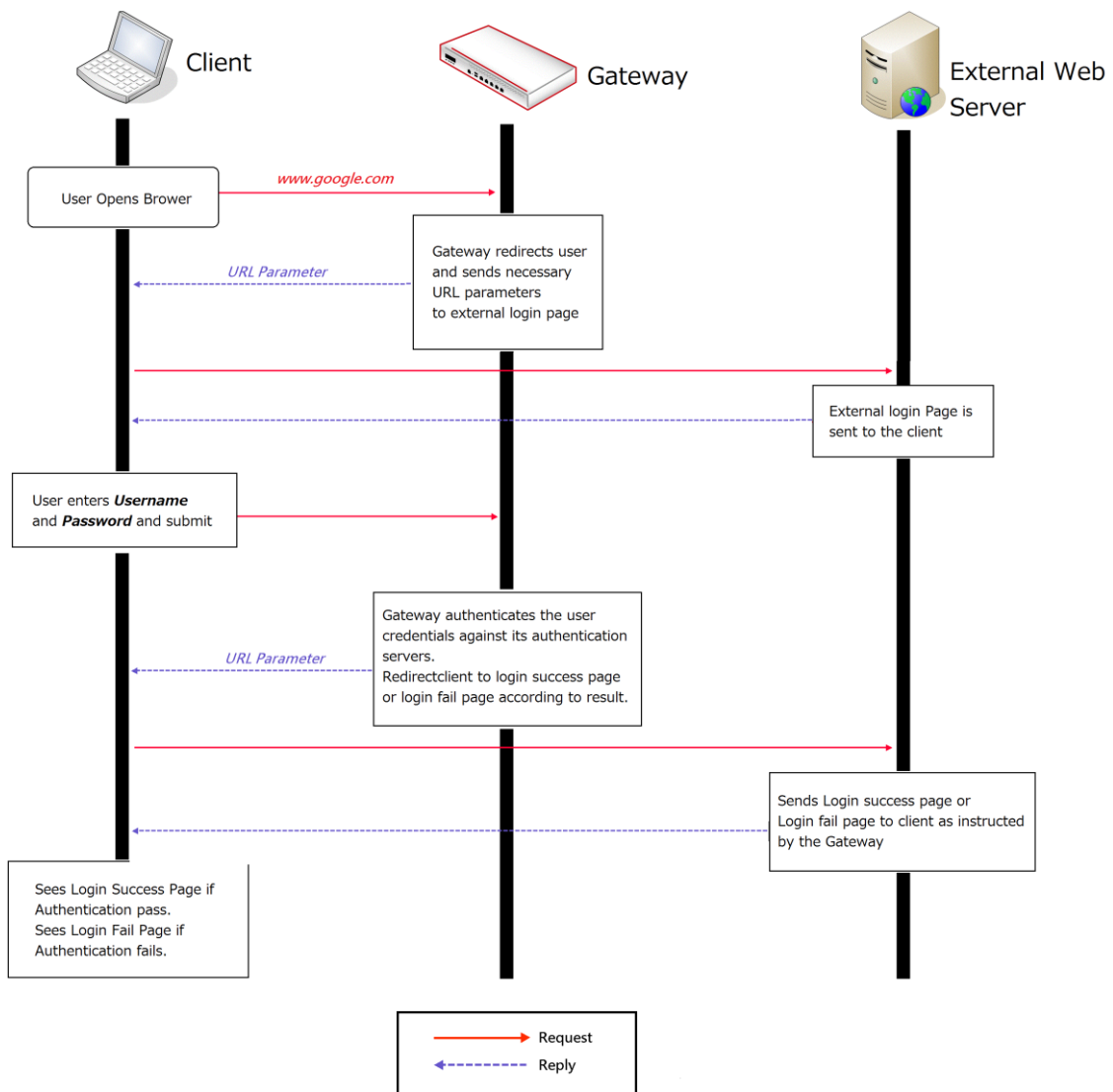
When a user connects to this Service Zone, opens a web browser and attempts to access the internet, the system will address the user to the external login page configured. Gateway while addressing users to the external web page will also send URL parameters required for the operation, for instance user authentication.

Therefore, each self-defined external page (*Login, Logout, Login Success, Logout Success, etc.*) requires codes to handle **URL parameters** to and from the Gateway. A simple example is illustrated below for Login Page. Please refer to **External Login Page Parameters** for URL parameter relating to other pages such as *Login Success Page ...* and etc.

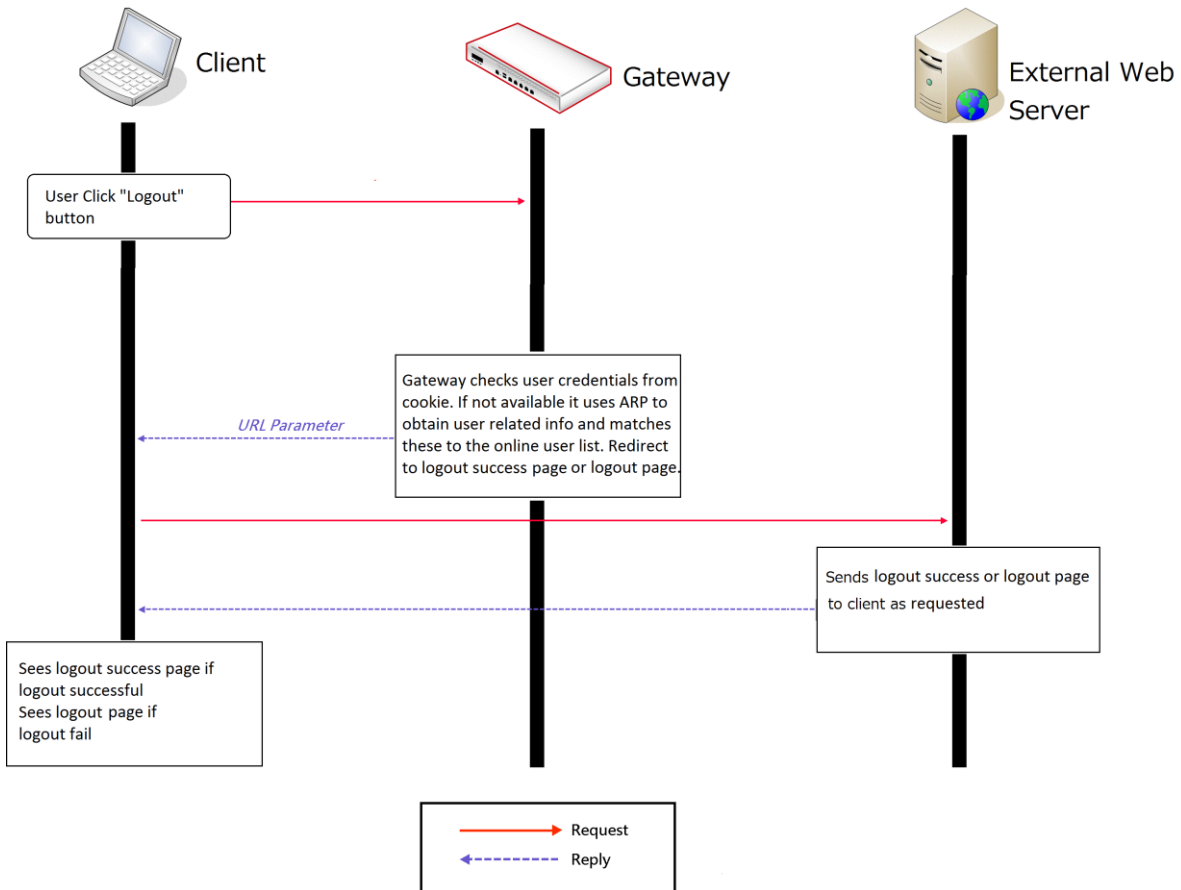
Therefore it is important that your external pages are designed by someone with good knowledge of URL parameter utilization.

The diagram below explains how External Page operates using user login/logout flow as illustration:

## Login:



## Logout:



The URL parameters sent by the Gateway to the external login page are as follows:

Field	Value	Description
loginurl	String (URL encoded)	The URL to be submitted when a user logs in.
remainingurl	String (URL encoded)	The URL to be submitted when a user wants to get remaining quota.
vlanid	Integer (1 ~ 4094)	VLAN ID
iface	Integer (0~8)	Service Zone ID, 0 for default service zone
gwip	IP format	Gateway activated WAN IP address
gwmac	MAC format (separated by ':')	Gateway activated WAN MAC address
client_ip	IP format	Client IP address

ipv6_addr	IPv6 format	Client IPv6 address
umac	MAC format (separated by ':')	Client MAC address
session	String	Encrypted session information, includes: client IP address, MAC address, date, and return URL.

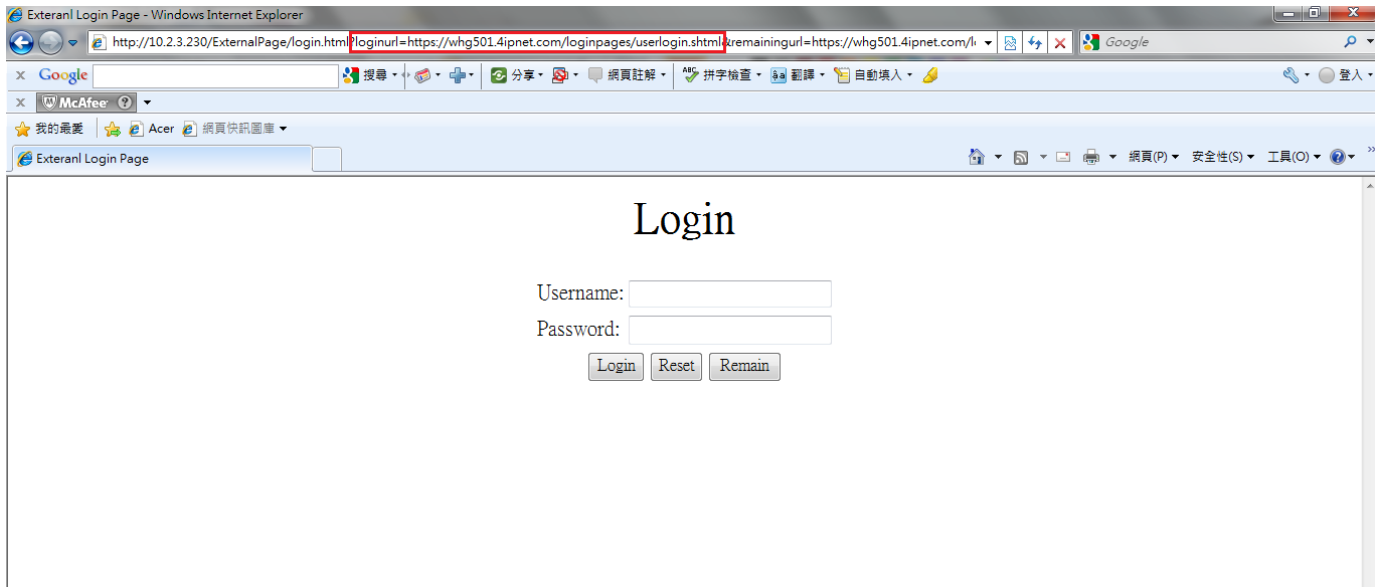
You will need to parse the required parameters in your html code. The following HTML code segment is an example of parsing *loginurl* parameter with a self-defined JavaScript function:

```
<FORM action="" method="post" name="form">
<script language="Javascript">
form.action = getVarFromURL(window.location.href, 'loginurl');
</script>
<INPUT type="text" name="myusername" size="25">
<INPUT type="password" name="mypassword" size="25">
<INPUT name="button_submit" type="submit" value="Enter">
<INPUT name="button_clear" type="button" value="Clear">
</FORM>
```

The following shows the corresponding self-defined JavaScript function used to parse the *loginurl* parameter:

```
function getVarFromURL(url, name) {
    if(name == "" || url == "") { return ""; }
    name = name.replace(/[\]/|"\\\\"/).replace(/[\]/|"\\\\"/);
    var regObj = new RegExp("[\\?&]" + name + "=(^[&#]*)");
    var result = regObj.exec(url);
    if(result == null) { return ""; }
    else { return decodeURIComponent(result[1]); }
}
```

An external page example that the user will see upon launching a browser is shown, and you can see the URL parameters sent from the system highlighted in red:



## External Page Design Variables

This section displays all the URL parameters that are sent from the Gateway to the various external pages. It is essential to use the correct variable for your self-designed user page to function properly.

### 1. External Login Page

#### Variables:

Field	Value	Description
loginurl	String (URL encoded)	The URL to be submitted when a user logs in.
remainingurl	String (URL encoded)	The URL to be submitted when a user wants to get remaining quota.
vlanid	Integer (1 ~ 4094)	VLAN ID
iface	Integer (0~8)	Service Zone ID, 0 for default service zone
gwip	IP format	Gateway activated WAN IP address
gwmac	MAC format (separated by ':')	Gateway activated WAN MAC address
client_ip	IP format	Client IP address
ipv6_addr	IPv6 format	Client IPv6 address
umac	MAC format (separated by ':')	Client MAC address
nat_ip	IP format	The internal IP address for identifying the client from split tunnel.

### 2. Login Successful Page

#### Variables:

Field	Value	Description
uid	String	User ID (postfix is included)
original_uid	String	Original User ID
utype	String (LOCAL, RADIUS, ONDEMAND, POP3, LDAP, SIP, NT Domain)	Authentication server name

umac	MAC format (separated by ':')	Client MAC address
sessionlength	Integer (Sec.)	RADIUS user session length (Only available for RADIUS user)
byteamount	Integer (Bytes)	RADIUS user volume limit (Only available for RADIUS user)
idletimeout	Integer (Sec.)	Idle timeout
acct-interim-interval	Integer (Sec.)	RADIUS accounting interim update interval (Only available for RADIUS user)
logouturl	String (URL encoded)	The URL to be submitted when a user wants to log out.
change_passwd_url	String (URL encoded)	The URL to be submitted when a user wants to change password. (Only available for LOCAL users)
ondemand_creation_url	String (URL encoded)	The URL to be submitted when a user wants to create an On-Demand user. (Only available for LOCAL users)
vlanid	Integer (1~4094)	VLAN ID
gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
ipv6_addr	IPv6 format	Client IPv6 address
sz	Integer	Service Zone ID
group	Integer	Group index
policy	Integer	Policy index
available_plan	billing plan:usage, billing plan: usage,	For local user to create on demand user
max_uplink	Integer (b/s)	Maximum up-link rate
max_downlink	Integer (b/s)	Maximum down-link rate
req_uplink	Integer (b/s)	Minimum up-link rate
req_downlink	Integer (b/s)	Minimum down-link rate
next_page	String	Leads client to URL
CLASS	String	RADIUS CLASS attribute (Only available for RADIUS user)
WISPR-REDIRECTION-URL	String	Leads client to URL
WISPR-SESSION-TERMINATE-TIME	String, format: YYYY-MM-DDThh:mm:ssTZD	WISPr Session-Terminate-Time attribute (Only available for RADIUS user)
WISPR-SESSION-TERMINATE-END-OF-DAY	Integer (0/1)	WISPr Session-Terminate-End-Of-Day attribute, 0 or 1 to indicate termination rule. (Only available for RADIUS user)
WISPR-BILLING-CLASS-OF-SERVICE	String	WISPr Billing-Class-Of-Service attribute (Only available for RADIUS user)
WISPR-LOCATION-ID	String	WISPr Location-ID attribute (Only available for RADIUS user)
WISPR-LOCATION-NAME	String	WISPr Location-Name attribute (Only available for RADIUS user)
WISPR-BILLING-TIME	String, format: HH:MM	WISPr Billing-Time attribute (Only available for RADIUS user)
split_tunnel	Integer (0/1)	1 if the client is from split tunnel; 0 otherwise.
nat_ip	IP format	The internal IP address for identifying the client from split tunnel.
custom	String	Customization parameter



### 3. External Error Page

#### Variables:

Field	Value	Description
msg	<p>String, includes:</p> <p>The system is busy. Please try again later.</p> <p>Cannot find session related information. &lt;BR&gt;Please enable the Cookie in the browser setting or open a website to get a Cookie.</p> <p>Invalid IP address. Please check the IP address and try again.</p> <p>Invalid MAC address. Please check the MAC address and try again.</p> <p>Sorry, your account is not usable, because the authentication option is currently disabled.&lt;BR&gt; Please contact your network administrator.</p> <p>Sorry, your account is not usable, because the authentication option (associated with the postfix) is not found.&lt;BR&gt;Please contact your network administrator.</p> <p>Sorry, you are not allowed to log in, because your account is currently on the Black List.</p> <p>Sorry, you are not allowed to log in, because it is currently not the service hour for your account.</p> <p>You have already logged in.</p> <p>Sorry, there is a system problem checking the information of your account (XXX).&lt;BR&gt;Please contact your network administrator.</p> <p>Invalid username or password.&lt;BR&gt;Please check your username and password and try again.</p> <p>Cannot identify the policy for your account.&lt;BR&gt;Please contact your network administrator.</p> <p>User of this device (the MAC address) is not allowed to use this account.&lt;BR&gt;Please contact your network administrator.</p>	Error message

	Sorry, the external authentication server is currently unreachable.  Please contact your network administrator.  Sorry, you are not allowed to create a remote VPN connection.  Reply-message form radius server. (radius attribute: Reply-Message)	
loginurl	String (URL encoded)	The URL which shall be submitted when user login.
remainingurl	String (URL encoded)	The URL which shall be submitted when user wants to get remaining quota.
vlanid	Integer (1~4094)	VLAN ID
iface	Integer	Service Zone ID, 0 for default service zone
client_ip	IP format	Client IP address
gwip	IP format	Gateway activated IP address
ipv6_addr	IPv6 format	Client IPv6 address
umac	MAC format (separated by ':')	Client MAC address
original_uid	String	Original User ID
nat_ip	IP format	The internal IP address for identifying the client from split tunnel.
custom	String	Customization parameter

#### 4. External Logout Successful Page

##### Variables:

Field	Value	Description
uid	String	User ID (postfix is included)
original_uid	String	Original User ID
vlanid	Integer (1~4094)	VLAN ID
gwip	IP format	Gateway activated IP address
used_time	Integer	User's Used time

#### 5. External On-Demand/Guest login successful page

##### Variables:

Field	Value	Description
uid	String	User ID (postfix is included)
original_uid	String	Original User ID
utype	String (LOCAL, RADIUS, ONDEMAND, POP3, LDAP, SIP, NT Domain)	Authentication server name
umac	MAC format (separated by ':')	Client MAC address
sessionlength	Integer (Sec.)	On-Demand user's quota of time type
byteamount	Integer (byte)	On-Demand user's quota of volume type
chargetype	String	User Accounting Type
idletimeout	Integer (Sec.)	Idle timeout

logouturl	String (URL encoded)	Logout URL
redeemurl	String (URL encoded)	Redeem URL
Vlanid	Integer (1~4094)	VLAN ID
gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
ipv6_addr	IPv6 format	Client IPv6 address
sz	Integer	Service Zone ID
group	Integer	Group index
policy	Integer	Policy index
next_page	String	Leads client to URL
max_uplink	Integer (b/s)	Maximum up-link rate
max_downlink	Integer (b/s)	Maximum down-link rate
req_uplink	Integer (b/s)	Minimum up-link rate
req_downlink	Integer (b/s)	Minimum down-link rate
nat_ip	IP format	The internal IP address for identifying the client from split tunnel.

## 6. External Logout Fail Page

### Variables:

Field	Value	Description
uid	String	User ID
gwip	IP format	Gateway activated WAN IP address
vlanid	Integer (1~4094)	VLAN ID

## External Page Design Variables

The following section collects and shows all the variables that are can be accepted by the Controller from the external pages. Some are mandatory. The destination path is also specified for designer reference.

### 1. User Login

#### Path:

[\(LAN IP address or Internal Domain Name\) /loginpages/userlogin.shtml](#)

#### Input:

Field	Required	Value	Description
myusername alternative variables: (username, user, account)	Required	String	User ID
mypassword alternative variables (passwd, password, pass)	Required	String	User password
session	Optional	String	Encoded string which contains some information of this session, default is taken from cookie.

**Output:**

No output, return user to login successful page.

**2. User Logout****Path:**

(LAN IP address or Internal Domain Name) /loginpages/logoff.shtml

**Input:**

Field	Required	Value	Description
uid	Optional	String	User ID, default is taken from cookie

**Output:**

No output, return user to logout successful page.

**3. Remaining quota (Credit balance)****Path:**

(LAN IP address or Internal Domain Name) /loginpages/reminder.shtml

**Input:**

Field	Required	Value	Description
myusername  alternative variables: (username, user, account)	Required	String	User name
mypassword  alternative variables (passwd, password, pass)	Required	String	Password
ret_url	Optional	String (URL encoded)	Returned URL, default is pop_reminder.shtml
command	Optional	String	getValue: If command is set to "getValue", the return URL would be ignored, and the page would only print out the available quota.

**Output:**

If command is set to "getValue", the output is simply a "value".(secs. or bytes according to user type)

If command is not set and there is no ret\_url presented, client would be led to pop\_reminder.shtml page, which shows the remaining quota in our UI style. If ret\_url is presented, client would be returned to ret\_url, and gateway would add these four variables in URL.

Field	Value	Description
msg	String, including:	Result and error messages

	<p>Remaining Quota: XXX byte(s)</p> <p>Credit Balance: XXXXXX</p> <p>Sorry, this feature is available for On-Demand user only.</p> <p>Sorry, this account or password is incorrect.</p> <p>Sorry, this account is out of quota.</p> <p>Sorry, this account is expired.</p> <p>Sorry, this account is redeemed.</p>	
value	<p>Integer (Sec. Or Byte)</p> <p>or error no.</p> <p>-1: Account not found.</p> <p>-2: Out of quota.</p> <p>-3: Expired.</p> <p>-4: Redeemed.</p>	<p>Remaining quota, if user is time type, the value is remaining seconds, if user is volume type, the value remaining bytes.</p>
uname	String	User name
type	<p>String, includes:</p> <p>TIME: Time type</p> <p>DATA: Volume type</p> <p>CUTOFF: Cut-off type</p>	On-Demand user billing type

#### 4. Change Password

##### Path:

[\(LAN IP address or Internal Domain Name\)/loginpages/user\\_change\\_password.shtml]((LAN IP address or Internal Domain Name)/loginpages/user_change_password.shtml)

##### Input:

Field	Required	Value	Description
save	Required	1 (has to be 1)	
opw	Required	String	Old password
npw	Required	String	New password
npwc	Required	String	Confirmed new password
ret_url	Required	String (URL encoded)	Return URL

##### Output:

Client would return to ret\_url and gateway would add result in ret\_url which indicates the result of changing password.

Field	Value	Description
result	<p>String, including:</p> <p>Change password successfully</p> <p>User password is incorrect</p> <p>Invalid password format</p>	Result and error messages

## 5. Redeem (On-Demand user)

### Path:

(LAN IP address or Internal Domain Name) /loginpages/redeemuserlogin.shtml

### Input:

Field	Required	Value	Description
username	Optional	String	Current user ID (If not presented, user name stored in cookie is the default value)
upassword	Optional	String	Current user password (If not presented, password stored in cookie is the default value)
myusername	Required	String	Redeem user ID
mypassword	Required	String	Redeem user password
ret_url	Optional	String (URL encoded)	Return URL, login successful page is the default value

### Output:

If no ret\_url is presented, client would be led to the login successful page, and in addition, a JavaScript window would pop-up and show the result. If ret\_url is presented, client would be returned to ret\_url and gateway would add an additional variable rmsg to indicate redeem procedure result.

Field	Value	Description
rmsg	String, including:  Redeem process completed.  Original user name cannot be found from the database.  Redeem user name cannot be found from the database.  Original user password is incorrect.  Redeem user password is incorrect.  Original user type and on demand user type do not match.  Original user has not logged in.  Redeem user logged in already.  Had been redeemed before.  User has run out of quota.  Maximum allowable time has exceeded.	Result and error messages

	<p>Maximum allowable memory space has exceeded.</p> <p>Wrong postfix please check it.</p> <p>This account is expired.</p>	
--	---	--

# **Appendix C. Useful Management & Evaluation Tools**

## **Useful Management Tools**

Here are the top six open source IT management products that do a solid job of replacing the big suites from HP, IBM, CA and BMC. Each offer low-cost professional services and free software downloads. They differ primarily in the features they offer and in the operating systems they support.

### **QUEST BIG BROTHER**

This Web-based systems and network monitor supports most Windows, Unix and Linux OSes, plus a repository of user-contributed scripts allow you to easily customize Big Brother to your network. Its GUI features a universally understood color code, where red means bad and green means good.

### **GROUNDWORK MONITOR PROFESSIONAL**

Launched in 2004, it's one of the first enterprise-scale open source network management offerings. It integrates more than 100 best-of-breed open source projects, including Nagios, Apache and NMap, onto one framework with additional features, such as a Web-based interface. Monitor Professional provides centralized management and monitoring of your enterprise network, including Linux, Unix and Windows servers, apps, databases and network boxes.

### **HYPERIC HQ ENTERPRISE**

Aimed at the [datacenter](#), Hyperic's software is built to manage and monitor all layers of Web infrastructures, including hardware, middleware, virtualization and Web and open applications. It also offers trending and analysis. It supports Apache, JBoss, Linux and more.

### **OPENNMS**

This Java-based network management tool focuses on service polling, data collection and event and notification management. It currently supports a variety of open operating systems, including Linux, Mandrake and Solaris, as well as Mac OS X; Windows support is planned for OpenNMS 2.0.

### **OPENQRM**

Also targeting datacenter management, OpenQRM can manage thousands of Linux and Windows servers as well as track your datacenter's usage and utilization. It also does automatic, policy-based provisioning. It, too, integrates Nagios for monitoring.

### **ZENOSS CORE**

Written mostly in Python, this management platform offers events management and availability and performance monitoring of servers, network devices, OSes and applications. Zenoss runs on Linux, FreeBSD and Mac OS X; it will run on Windows with a VMplayer and the Zenoss Virtual Appliance.

## **Evaluation Tools**



## **Wireshark (for packet capturing and debug analysis)**

Wireshark is the world's foremost network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions.

Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998.

<http://www.wireshark.org/>

## **inSSIDer (for wireless scanning & frequency analyzer)**

inSSIDer is a useful tool for scanning the air for nearby AP signals and in depth frequency, channel analysis of deployment site.

You can:

- Inspect your Wi-Fi and surrounding networks
- Scan and filter hundreds of nearby access points
- Troubleshoot competing access points and clogged Wi-Fi channels
- Highlight access points for areas with high Wi-Fi concentration
- Track the strength of received signals in dBm over time
- Sort results by MAC Address, SSID, Channel, RSSI, Time Last Seen
- Export Wi-Fi and GPS data to a KML file in Google Earth

<http://www.metageek.net/products/inssider/>

## Appendix D. On-Demand Account Types

There are four main types of On-Demand account type:

- **Usage-time** (Buy quota: usable time)
- **Volume** (Buy quota: usable traffic volume)

*Pre-paid concept, only deducts quota while using. Account expires when quota is depleted or account expiration time reached.*

- **Hotel Cut-off** (Buy the time interval for a valid account)
- **Duration-time** (Buy the time interval for a valid account)

*Define the time interval for usage. Count down begins when account activated and expires when the expiration time/date reached.*

### Usage-time

- Users can access internet as long as account valid with remaining quota and need to activate the purchased account within a given time period by logging in.

- Usage-time accounts have the option of selecting:

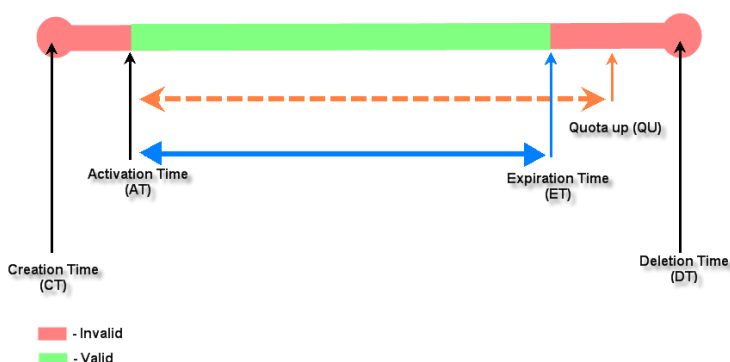
#### □ With Expiration Time

- Counting down begins immediately after first login. Account expires when *Valid Period* is used up or quota is depleted.

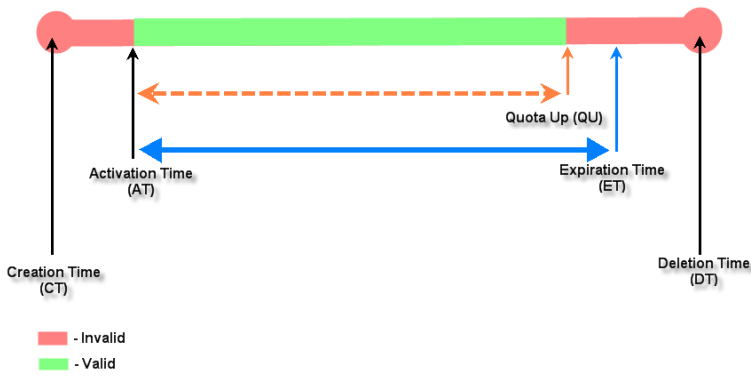
#### □ No Expiration Time

- Account expires only when quota is used up.

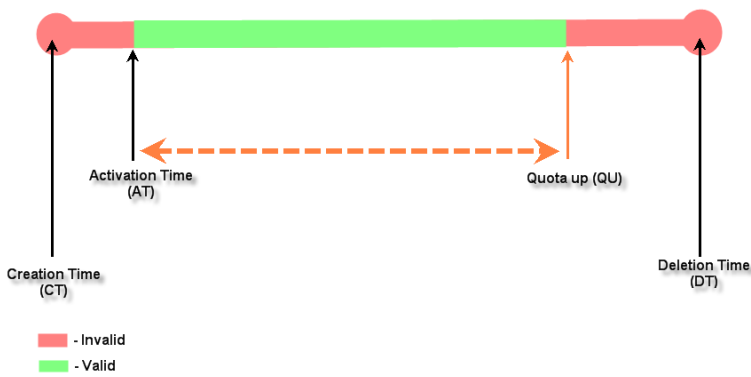
Usage-time account lifespan



Usage-time account lifespan



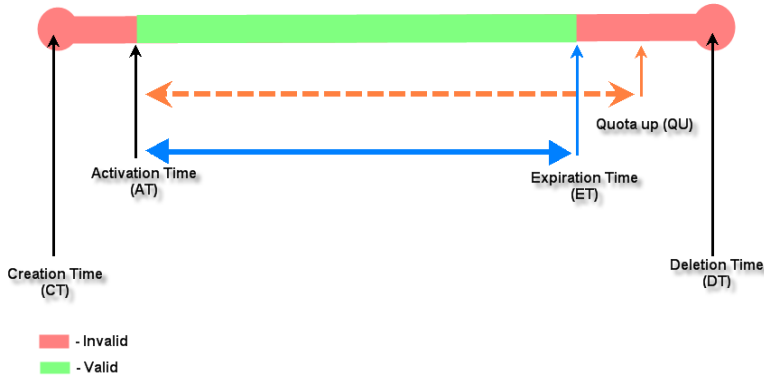
Usage-time account lifespan

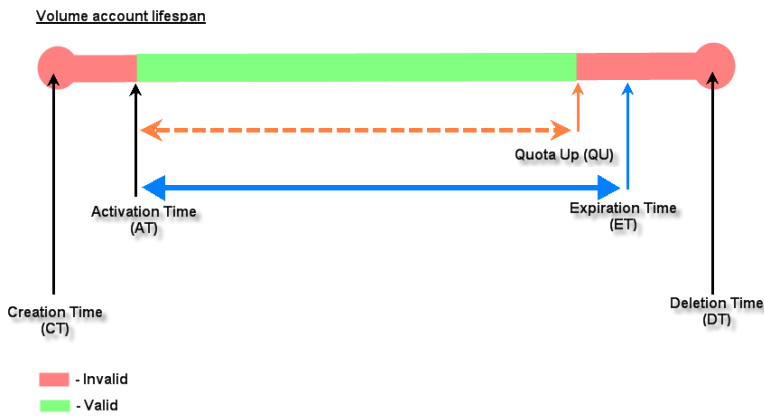


## Volume

- Users can access internet as long as account is valid with remaining quota and need to activate the purchased account within a given time period by logging in.
- Account expires when *Valid Period* is used up or quota is depleted.

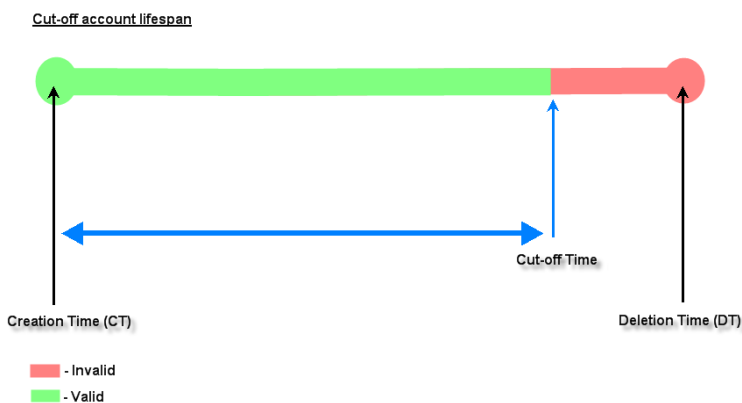
Volume account lifespan

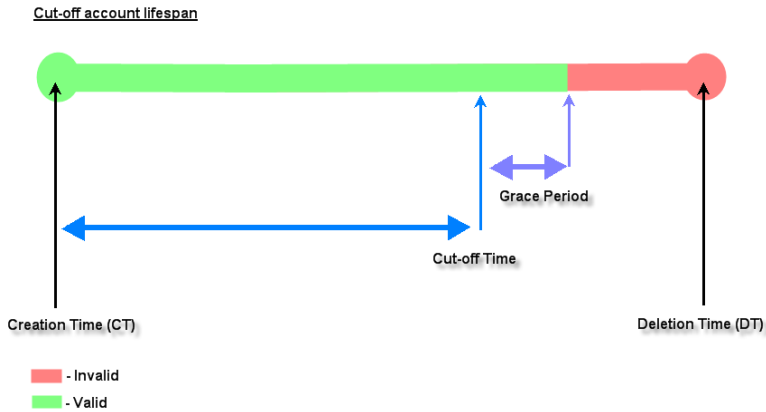




## Hotel Cut-off Time

- Operator can set the clock time for when the account will expire.
- Account automatically activates when it is created.
- Unit is the number of days to execute "Cut-off". For example: Unit = 2 days, Cut-off Time = 10:00 then account will expire at 10:00AM two days after creation.
- Account usability disabled once *Cut-off-time* has been reached unless it has been granted a *Grace Period*.
- Primarily used in hotel venues to provide internet service according to guests' stay time.

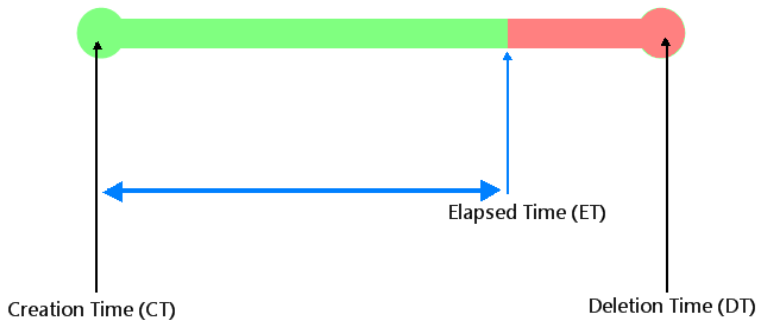




## Duration Time

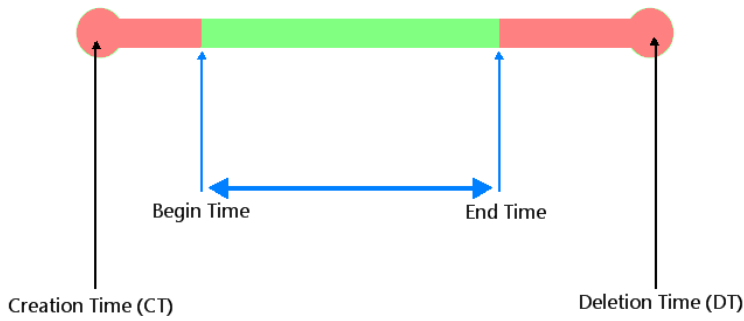
- Users can access internet while account is within valid time interval. Count down begins once account activates and expires when *Expiration Time* is reached.
- Duration-time accounts can be further classified into:
  - **Elapsed Time**
    - Relative to *Activation Time* which is the account creation time. Account expires when the *Expiration Time* has been reached.
  - **Begin-End Time**
    - Define explicitly the *Begin Time* and *End Time* of the account. Account expires when the *End Time* has been reached.
  - **Cut-off Time**
    - Define explicitly the clock time to “Cut-off” within the day of creation.

Duration-time Elapsed account lifespan



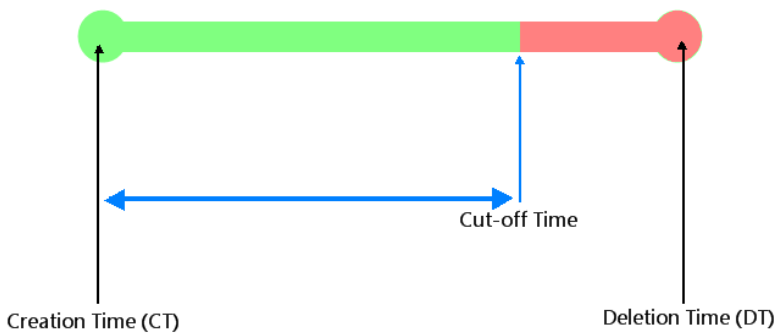
■ - Invalid  
■ - Valid

Duration-time Begin-End Account lifespan



■ - Invalid  
■ - Valid

Duration-time Cut-off account lifespan



■ - Invalid  
■ - Valid

**NOTE**

1. Since there are only 10 billing plans, if you wish to create accounts of the same type but with various quotas, this may be achieved via the Unit field.

## On-Demand Account Creation

Plan	Account Type	Quota	Price	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	1.99	1	<input type="button" value="Create Single"/> <input type="button" value="Create Batch"/>
2	Hotel Cut-off-time	Valid until 5:01 the following day	1	1	<input type="button" value="Create Single"/> <input type="button" value="Create Batch"/>



## Creating an On-Demand Account

Plan : Account Type    1 : Usage-time

Quota    2 hr(s) of connection time quota with expiration

Account Creation     System created    Manual created

Valid Period    After activation, the account will be expired in 7 day(s)

Total Price    1.99

**Unit**     Units per ticket

Group    Group 1

Reference     Add a reference related to this account (for example, the customer's name)

External ID     Enter an external ID such as a Library ID No.

Please confirm the information and press Create button to create an account.

Network operator is able to multiply the quota by an integer ranging from 1 to 9 in the **Unit** field. Please note that only Usage-time, Volume, and Duration-Elapsed time account types support multiple unit quota generation for a single account.



SN:xxxxxx

Welcome!

Username	xxxx@ondemand
Password	xxxxxxxxxx
Plan : Account Type	1 : Usage-time
Quota	xx hr(s) xx min(s)
Unit	Units
Total Price	1.99
Max User	1
Reference	Customer xxx
External ID	SSID0
ESSID : SSID0	
Shared Wireless Key: None (Open System)	
Your account is activated at	
The account will be expired in 2019/06/25 15:33	
You have to login before	
The account will be expired in after account activation.	

Thank You!

# Appendix E. UI Reference Index

## I. 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. A drop-down menu is available for selecting the information refresh rate for this page.

The “Download” button on the top-right corner is a tool that provides system status snapshot. The information can be used for maintenance or troubleshooting purpose.

In addition, administrator can choose the items to show in Dashboard by editing “Display Mode”. Dashboard can be customized only to show necessary information.





## II. Setup Wizard

This wizard is to provide express setup procedures. Follow the instructions given at each step to change the system admin password; select time zone; configure WAN1 interface, and create local user accounts. Upon completing the setup procedures, the system has to be restarted to have the setting take effect. The system is ready for operation after restart with minimal configuration.

The screenshot shows the 'General' configuration screen of a setup wizard. At the top, there are four steps: 1. FIRST STEP (Change Password), 2. SECOND STEP (Configure WAN1), 3. THIRD STEP (Create A Local User), and 4. YOU'RE DONE (Restart the System). The first step is currently active. On the left, a red vertical bar highlights a note: 'It is recommended to change administrator's password and select an appropriate time zone for the system.' The main area is titled 'General' and contains three fields: 'New Password' and 'Verify Password' (both masked with black dots), and a 'Time Zone' dropdown menu set to '(GMT+08:00)Taipei'. At the bottom right, there are 'Exit' and 'Next' buttons.

**1 FIRST STEP**  
Change Password

**2 SECOND STEP**  
Configure WAN1

**3 THIRD STEP**  
Create A Local User

**4 YOU'RE DONE**  
Restart the System

It is recommended to change administrator's password and select an appropriate time zone for the system.

### General

New Password: ●●●●●●

Verify Password: ●●●●●●

Time Zone: (GMT+08:00)Taipei

Exit Next

## A. System

**System:** This section relates to system configuration. It includes, General Information, WAN Configurations, LAN Ports, Service Zones, and etc.

### 1) General

The image shows two screenshots of a web-based configuration interface. The top screenshot is titled "General Settings" and contains the following fields and options:

- System Name:** EWS101
- Contact Information:** (Empty text box)
- HTTPS Certificate:** Default CERT (Dropdown menu)
- User HTTPS Login:**  Enable  Disable
- Secure:**  Secure
- HTTPS Automatic Redirect:**  Allow  Block  Bypass
- Internal Domain Name:**  Use the name on SSL certificate  
mknhhi.example.com
- Portal URL Exceptions (User Agent):** IEMobile/7.0,XBLWP7  
(e.g. IEMobile/7.0,XBLWP7, separate by comma)
- User Log Access:** Enter IP Address Here
- UAM Filter:** Configure
- Management IP Address:** Configure
- SNMP:**  Enable  Disable  
Configure
- Suspend Warning Message:** Sorry! The service is suspended. \*
- NMS Setting:** Configure

The bottom screenshot is titled "System Time" and contains the following fields and options:

- Current Time:** 2019/06/25 17:26:12
- Time Zone:** (GMT+08:00)Taipei (Dropdown menu)
- Time Update:**  NTP  Manually set up
- NTP Server 1:** time.nist.gov
- NTP Server 2:** ntp1.fau.de
- NTP Server 3:** clock.cuhk.edu.hk
- NTP Server 4:** ntps1.pads.ufrj.br
- NTP Server 5:** ntp1.cs.mu.OZ.AU
- Use this controller as an NTP server

- **System Name:** This is a mnemonic name you 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 which will be

- displayed on the web browser of the client in the event of internet disconnection.
- **HTTPS Certificate:** Your own network certificate may be selected here as site safety verification. Certificate can be uploaded and managed at “Utilities > Certificates > System Certificate”.
  - **User HTTPS Login:** Presents the option to allow end users authenticated with HTTPS for encrypted content transfer. The ‘Secure’ option supports only “High” encryption cipher suites.
  - **HTTPS Automatic Redirect:** 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 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 configuration button allows the network administrator to enter a selection of reserved IP addresses/ range that are authorized to see the Web Management Interface. The remote console interface is disabled by default.
  - **SNMP:** Presents an option to enable or disabled system info retrieval via SNMP protocol. 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
  - **Time:** This section presents manual system time configuration option or automatic time synchronization by specifying external NTP servers.
    - **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.

## Management Service

SSH Service  Enable  Disable  
Telnet Service  Enable  Disable

## Management Service Zone List

Active	Status	Service Zone	IP Address/Segment
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Default	192.168.1.254/255.255.0.0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SZ1	10.1.1.254/255.255.0.0
<input type="checkbox"/>	<input checked="" type="checkbox"/>	SZ2	10.2.1.254/255.255.0.0
<input type="checkbox"/>	<input type="checkbox"/>	SZ3	10.3.1.254/255.255.0.0
<input type="checkbox"/>	<input type="checkbox"/>	SZ4	10.4.1.254/255.255.0.0
<input type="checkbox"/>	<input type="checkbox"/>	SZ5	10.5.1.254/255.255.0.0
<input type="checkbox"/>	<input type="checkbox"/>	SZ6	10.6.1.254/255.255.0.0
<input type="checkbox"/>	<input checked="" type="checkbox"/>	SZ7	10.7.1.254/255.255.0.0
<input type="checkbox"/>	<input type="checkbox"/>	SZ8	10.8.1.254/255.255.0.0

## Management IP Address List

No.	Active	IP Address/Segment
1	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0/0.0.0.0"/>
2	<input checked="" type="checkbox"/>	<input type="text" value="10.71.1.1/255.255.0.0"/>
3	<input type="checkbox"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>

- **Management Service:** Options to enable or disable remote console management interface.
  - **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 Edgework 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) WAN

### WAN1 Configuration

Physical Mode:

Interface Type:  Static (Use the following IP settings)

IP Address:  \*

Subnet Mask:  \*

Default Gateway:  \*

Preferred DNS Server:  \*

Alternate DNS Server:

Dynamic (IP settings assigned automatically)

PPPoE

PPTP

- **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 ISPs (in European countries) may provide PPTP protocol for dialup connection. The issued PPTP account and password for PPTP server are required.

## 3) IPv6

### IPv6 Setting

IPv6:  Enable  Disable

Interface:  WAN1  WAN2

Type:  Static (Use the following IPv6 settings)

IPv6 Address:  \*

Prefix Length:  \*

Default Gateway:  \*

Preferred DNS Server:

Alternate DNS Server:

Use 6to4 transition

Use go6 transition

- **Status:** Enable or Disable IPv6 support on the selected WAN interface.
- **Interface:** Select the external interface of the device that will be configured with an IPv6 address.
- **Type:** 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 was set with a static IPv4 address.

## 4) Service Zones

The table will list the Service Zones and related settings.

- **Status:** Status of each Service Zone. It is always “ON” for Default Service Zone.
- **Service Zone Name:** The name of service zone.
- **IP Address:** The IP address of the Controller for each Service Zone.
- **IPv6 Address:** The IPv6 address of the Controller for each Service Zone.
- **VLAN Tag:** The VLAN tag number mapped to each Service Zone.
- **Default Auth. Option:** The default authentication server designated for each Service Zone.
- **Network Alias:** Alias subnets for each Service Zone.
- **DHCP Pool:** The DHCP server status or the IP range for DHCP Pools.

### Service Zone Settings

Status	Service Zone Name	IP Address	IPv6 Address	VLAN Tag	Default Auth. Option	Network Alias	DHCP Pool
	Default	192.168.1.254	N/A	N/A	Server 1	N/A	192.168.1.1 ~ 192.168.1.100
	SZ1	10.1.1.254	N/A	1	Server 1	N/A	10.1.1.1 ~ 10.1.1.100
	SZ2	10.2.1.254	N/A	2	Server 1	N/A	10.2.1.1 ~ 10.2.1.100
	SZ3	10.3.1.254	N/A	3	Server 1	N/A	10.3.1.1 ~ 10.3.1.100
	SZ4	10.4.1.254	N/A	4	Server 1	N/A	10.4.1.1 ~ 10.4.1.100

## Basic Settings

**Service Zone Status**  Enabled  Disabled

**Service Zone Name**

**Network Interface**

VLAN Tag  \* (Range: 1 ~ 4094)

Tag-based Isolation  Inter-VLAN Isolation  Clients Isolation  None

Note: When set to "None", the port on a switch connecting to the gateway's LAN port may be shut down if "Loop Protection" is enabled on the switch and there are 2 VLANs belonging to this Service Zone.

Operation Mode  NAT  Router

IP Address  \* Subnet Mask  \*

Network Alias List

This list defines other IP Addresses (range) that are routable in this Service Zone.

**DHCP** Enabled

### Router Mode

## Basic Settings

**Service Zone Status**  Enabled  Disabled

**Service Zone Name**

**Network Interface**

VLAN Tag  \* (Range: 1 ~ 4094)

Tag-based Isolation  Inter-VLAN Isolation  Clients Isolation  None

Note: When set to "None", the port on a switch connecting to the gateway's LAN port may be shut down if "Loop Protection" is enabled on the switch and there are 2 VLANs belonging to this Service Zone.

Operation Mode  NAT  Router

IP Address  \* Subnet Mask  \*

Network Alias List

This list defines other IP Addresses (range) that are routable in this Service Zone.

**DHCP** Enabled

### NAT Mode

- **Service Zone Status:** Each service zone can be enabled or disabled except for the default service zone.
- **Service Zone Name:** The name of service zone could be input here.

#### Network Interface:

- **VLAN Tag:** The VLAN tag number that is mapped to the Service Zone.
- **Tag-Based Isolation:** Administrators can choose different isolation options in each Service Zone.
  - **Inter-VLAN Isolation:** 2 clients within the same Service Zones will not see each other when coming in from different VLANs and different LAN 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.

➤ **Operation Mode**

- **NAT:** The acronym for Network Address Translation mode. 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:** A network operating mode 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.

➤ **IP Address:** The IP Address of this Service Zone.

➤ **Subnet Mask:** The subnet mask of this Service Zone.

➤ **IPv6 Settings:** The IPv6 Address and configuration of this Service Zone (only when IPv6 is enabled).

➤ **Network Alias List:** Administrator may optionally set many alias network segments for a service zone. This feature can allow a single service zone to be seen as many service zones, also hide the IP address of a Service Zone's network interface and to some degree, provide protection from possible attacks from LAN clients. Click the **Configure** button to enter the Network Alias List page.

### Network Alias List - SZ1

Enable	No.	IP Address	Subnet Mask	Operation Mode
<input type="checkbox"/>	1	<input type="text"/>	255.255.255.255 (B2)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	2	<input type="text"/>	255.255.255.255 (B2)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	3	<input type="text"/>	255.255.255.255 (B2)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	4	<input type="text"/>	255.255.255.255 (B2)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	5	<input type="text"/>	255.255.255.255 (B2)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	6	<input type="text"/>	255.255.255.255 (B2)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	7	<input type="text"/>	255.255.255.255 (B2)	<input checked="" type="radio"/> NAT <input type="radio"/> Router

- ◆ Fill in the desired alias IP address and select the preferred Subnet Mask, Operation mode, check the Enable box and click **Apply** button to activate the settings.

➤ **DHCP:** From the drop down menu, DHCP server for this particular service zone may be Disabled, Enabled or Relayed.

Please note that when "Enable DHCP Relay" is enabled, fill in the IP address of the external DHCP Server, and the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this service zone. A redundant DHCP server can be configured when set to DHCP Server Relay mode. Please note that Controller should be in the same subnet as the DHCP server.

DHCP  Enable DHCP Server

#### DHCP Server Configuration for Service Zone SZ1

No	Active	DHCP Pool	Start IP Address	End IP Address	Preferred DNS Server	Alternate DNS Server	Domain Name	Lease Time (mins)	WINS Server	Disregard Client's Name
1	<input checked="" type="checkbox"/>	Scope 1	172.21.0.1 *	172.21.0.100 *	172.21.0.254 *	<input type="text"/>	domain.com	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
2	<input type="checkbox"/>	Scope 2	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
3	<input type="checkbox"/>	Scope 3	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
4	<input type="checkbox"/>	Scope 4	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
5	<input type="checkbox"/>	Scope 5	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
6	<input type="checkbox"/>	Scope 6	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Reserved IP Address List

DHCP Lease Protection  Enable  Disable



- **Start IP Address / End IP Address:** A range of IP addresses that are built in DHCP server will be assigned to clients. Note: please change the Management IP Address List accordingly (at System Configuration >> System Information >> Management IP Address List) to permit the administrator to access the EWS CONTROLLER admin page after the default IP address of the network interface is changed.
  - **Preferred DNS Server:** The primary DNS server that is used by this Service Zone.
  - **Alternate DNS Server:** The substitute DNS server that is used by this Service Zone.
  - **Domain Name:** Enter the domain name for this service zone.
  - **WINS Server:** The IP address of the WINS (Windows Internet Naming Service) server that if WINS server is applicable to this service zone.
  - **Lease Time:** This is the time period that the IP addresses issued from the DHCP server are valid and available.
  - **Disregard Client Name:** When enabled the system will not record the name of the device requesting for an IP address. On the other hand, when disabled is selected, the system will record the device's name when issuing IP addresses. The devices name (Host Name) can be seen under **DHCP Lease** tab.
- 
- **Reserved IP Address List:** A configuration list for reserving certain IP's within the DHCP Server IP range for specific devices (MAC), for example an internal file server. Click the **Configure** button to edit the Reserved IP List.
- 
- **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.
- 
- **Assigned IP Address for AP Management:** IP segment for IP address assignment to the managed AP when the newly discovered AP by LAPM is added into the service zone.

### Assigned IP Address for AP Management

---

<b>IP Range</b>	Start IP Address	<input style="width: 90%;" type="text" value="192.168.10.1"/>
	End IP Address	<input style="width: 90%;" type="text" value="192.168.10.254"/>

This defines the range of IP addresses Access Points would use for Local Access Point Management.

### **Authentication Settings**

The system supports several authentication options, namely: Local, On-Demand, Guest, One Time Password, RADIUS, SIP, LDAP, NT Domain, POP3, and Social Media. All authentication option can be enabled and applied concurrently. This is to be emphasized in the next section "Users".

## 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

RADIUS Authentication using MAC address

**PPP Authentication**  Enabled  Disabled

**SIP Interface Configuration**  Enabled  Disabled

**WISPr Settings** [Configure](#)

**Authentication Options**

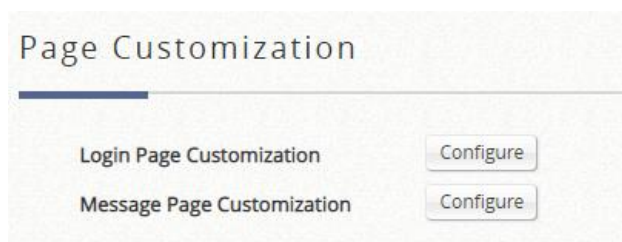
Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
Server 2	RADIUS	.	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 3	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>
Guest	FREE	N/A	<input type="radio"/>	<input type="checkbox"/>
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>

- **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.
- **Assign IP Address From:** 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.

### 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 an 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.

## APs with VAP mapped to this Service Zone

AP Type

AP Type	AP Name	IP Address	MAC Address	Status
---------	---------	------------	-------------	--------

- **Managed AP(s):** APs managed with LAPM and operating under the Service Zone will be listed here. The list is organized by AP Types, and APs can be configured by clicking the shortcut links on the AP Names (link to Main > Access Points > Local Area AP Management > List > AP Configuration). This works like a summary and provides administrators with a quick status check in a glance.

## 5) 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 Zones to get different policy. Furthermore, according to your application, you can configure the different rooms to different Port Type: **Authentication Required**, **Open** or **Block**.

### Create

Status  Enable  Disable

Mapping

Subinterface Use LAN Port

Subinterface ID

Remark

### Lists

PLM List

Subinterface List

Tunnel PLM List

- **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. If the user opens a browser and tries to access internet, a page with disclaimer and billing plan options will be displayed. 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

The screenshot shows a web form titled 'Create One' under the 'Method' 'Create Single Mapping'. The form contains the following fields:

Port Type	Open
Choose LAN Port	LAN1
Service Zone	Default
DHCP Scope	None
Assign VLAN ID	Range from 1 - 4094 *
Location ID	A number
Location Description	Optional
User Limit	Unlimited if left blank
NAS Identifier	NAS Identifier
Class	
HTTP Parameter	

- **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 Pool to use from corresponding Service Zone.
- **Assign VLAN ID:** The 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**

Method Create Multiple Mappings ▾

### Create Batch

---

Port Type Open ▾

Choose LAN Port LAN1 ▾

Service Zone Default ▾

DHCP Scope None ▾

Assign VLAN ID From Range from 1 - 4094 \*

Number of VLANs A number \*

Location ID From A number

Location Prefix Optional

Location Postfix Optional

User Limit Per Port Unlimited if left blank

NAS Identifier From Optional

NAS Identifier Prefix Optional

NAS Identifier Postfix Optional

- **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

➤ **Subinterface**

A Subinterface ID can be entered to allow multiple VLAN headers to be incorporated into a single Ethernet frame. This feature is commonly used in large networks which requires more than a single VLAN header for further segregation

➤ **Port Location Mapping List**

### Port Location Mapping List

---

Delete Export List Import List Change All Port Types
All ▾ Search

<input type="checkbox"/>	VLAN ID	Room Number (Location ID)	Room Description (Location Name)	Port Type	From	Service Zone	Availability
<input type="checkbox"/>	100	1000		Single User	LAN1	Default	<span style="color: green;">●</span>
<input type="checkbox"/>	101	1001		Single User	LAN1	Default	<span style="color: green;">●</span>
<input type="checkbox"/>	102	1002		Single User	LAN1	Default	<span style="color: green;">●</span>
<input type="checkbox"/>	103	1003		Single User	LAN1	Default	<span style="color: green;">●</span>

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:** Erase an individual Port Location Mapping profile.
- **Export List:** Back up the existed Port Location Mapping List.
- **Import List:** Restore the Port Location Mapping List.
- **Change All Port Type:** To configure Port Type for all rooms: Free, Block, Single User, Multiple User.

➤ **Tunnel PLM List**

Tunnel Port Location Mapping List

Delete All Search

	ESSID	Location ID	Location Description	Port Type	From	Service Zone
(Total:0) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a> (Page:1/1)						

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.

## 6) PMS Interface

By setting up the connection to the PMS interface, the system can listen to specific messages from PMS server. When hotel guest is buying an in-room billing plan for Internet access, the system will post a record to PMS server.

PMS Interface Configuration

PMS Interface Type  Disable  Micros Opera  InnKeyPMS  IDS

PMS IP Address

PMS Port

Account Credentials Username  RN   
 Password  RN

Room Bill Description

Login Error Message

User Account Log

Synchronize Data with PMS

PMS External Page Customization API  Disable  Enable

External Page Validity Verification Username   
 Password

Sample External Login Page

- **PMS Interface Type:** Select the PMS interface type to be integrated.

### Micros Opera / IDS

- **PMS IP:** Enter the IP used by the Micros Opera PMS.
- **PMS Port:** Enter the Port used by the Micros Opera 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.
  - **Case and Diacritics Insensitive for Password:** When using Guest Name as password, case and diacritics will exactly follow the information stored in the PMS server. Enable this option to ignore case and diacritics.
- **Room Bill Description:** The entered 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:** Click “Sync” 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

### Innkey PMS

- **Query API:** Enter the IP for Query API.



- **Post API:** Enter the IP for Post API.
- **Shared Key:** Enter the shared key for Innkey PMS APIs.
- **Account Credential:** Room Number and Guest Number will be the user name and password for user login.
- **Case and Diacritics Insensitive for Password:** Enable this option to ignore case and diacritics when verifying password.
- **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.

## B. Users

**Users:** This section relates to user authentication, authorization and accounting. It includes Groups Configuration, Internal/External Authentication Configuration, On-Demand Accounts, Policies Configuration, Privilege Lists Configuration and Additional Controls.

### 1) Groups

The Group Overview page gives a summary of which Authentication Servers are used for the corresponding Group.

Main > Users > Groups > Overview

This page gives a summary of which Authentication Servers are used for the corresponding Group.

#### Group Overview

Group Name	Authentication Type
Group 1	Local Billing Plan 1 Billing Plan 2 Billing Plan 3 Guest Social Media Login OTP POP3-Server 5 RADIUS-Server 2-Default LDAP-Server 4-Default NT Domain-Server 3 SIP
Group 2	
Group 3	
Group 4	
Group 5	
Group 6	
Group 7	
Group 8	

16 sets of Group options (models dependency) and Zone Permission Configuration & Policy Assignment can be defined respectively to enforce the access management for different groups of users in different Service Zones. The correspondence can be configured on the “Group Configuration” page.

This page gives a summary of access permissions for each Group in different Service Zones.

## Group Configuration

Select Group:

Group Name:

Remark:

Number of devices which are allowed to login:   
(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 1	Schedule 1
<input checked="" type="checkbox"/>	Service Zone : Default	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ1	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ2	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ3	Policy 1	Policy 1

To allow multiple devices to log in with the same account credentials, define the number here at “Number of devices which are allowed to login”. Multiple device login for the On-Demand authentication option can be configured at selected Billing Plans.

## 2) Internal Authentication

The system supports multiple authentication options, which include both internal and external databases. Internal Authentication databases include “Local”, “On-Demand”, and “Guest”.

### Authentication Option - Server 1

**Server No. 1**

Name:  \*

User Postfix:  \*

Remark:

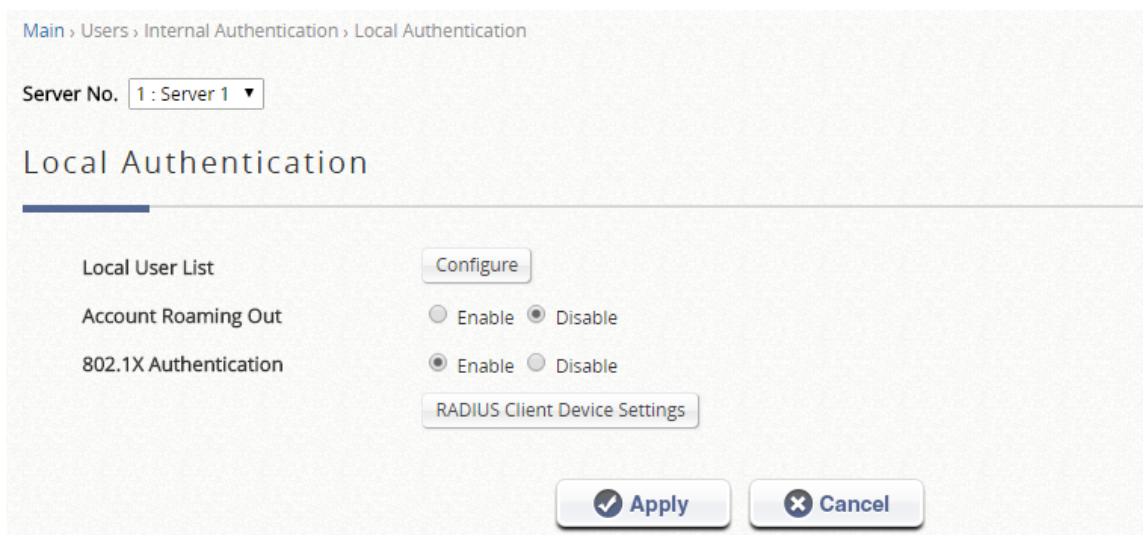
Blacklist:

Authentication:

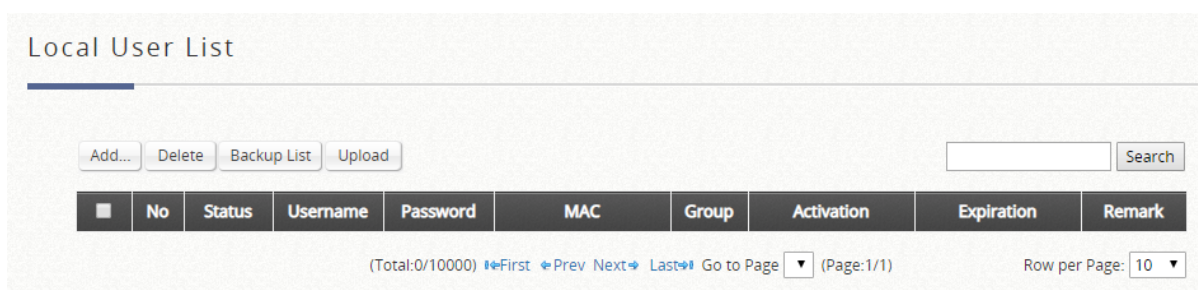
## a) Local Authentication

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.

The default Authentication for “Local” is set at Authentication Server 1. 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. To manipulate Local accounts, go to “Configure” for Local User List.



- **Local User List:** Click “Configure” to view Local Account list and configure the accounts.
- **Account Roaming Out:** Enable/Disable Local account database when the Controller is used as RADIUS server for external RADIUS authentication requests.
- **802.1X Authentication:** Enable/Disable Local account database when the Controller is used as RADIUS server for external 802.1X authentication requests.
  - **RADIUS Client Device Settings:** Configure the client list and secret key for those devices allowed to do RADIUS or 802.1X authentication with the Controller.



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

10000 users can be added to this local user list.

Username	Password	MAC Address	Group	Account Span	Remark
<input type="text"/>	<input type="text"/>	<input type="text"/>	Group 1 ▼	<input type="checkbox"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	Group 1 ▼	<input type="checkbox"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	Group 1 ▼	<input type="checkbox"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	Group 1 ▼	<input type="checkbox"/>	<input type="text"/>

- **Username:** The username for the new local account. Mandatory when adding new account.
- **Password:** The password for the new local account. Mandatory when adding new account.
- **MAC Address:** Bind this particular account under the condition that it may only be granted access using the device with the specified MAC address.
- **Group:** The group profile of the account being created.
- **Account Span:** Time constraints which will be enforced to this account.
- **Remark:** Additional note administrator would like to stress. It will be shown on the user list.

## b) On-Demand Authentication

The On-Demand Authentication option is typically used for short term usage, such as public hotspots. Settings related to the On-Demand Authentication option can be configured here, such as Billing Plan profiles, POS ticket customization, Terminal Server list, External Payment Gateway setup and etc.

### On-Demand Authentication

---

**User Postfix**

**Billing Plans**

**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**  day(s)

**Out-of-quota Account Cache**  day(s)

**Set Ticket's Serial Number**

**Web Printout**

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

**POS Tickets**

**Number of Tickets**  1  2

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

**Terminal Server**

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

**Payment Gateway**

**SMS Gateway**

**Account Roaming Out**  Enable  Disable

- **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.
- **Billing Plans:** Click "Configure" button to edit billing plans.
- **Currency:** 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.
- **On-Demand Access Code:** Allow/Disallow On-Demand users login with Access Code, other than username and password.
- **Smart Login:** Allow/Disallow On-Demand users to be logged-in automatically within a specific time period.
- **Set Ticket's Serial Number:** Set the serial number for the next POS ticket print out.
- **Web Printout:** Click "Configure" button to customize the account information page when creating a single On-Demand account. You can also preview the result here.
- **POS Tickets:** Click "Configure" button to customize account tickets to be printed out by POS printer.
- **POS Printer:** Click "Configure" button to add/delete POS printers.
- **Payment Gateway:** Click "Configure" button to setup payment gateway interface, which allows users to buy account by themselves.
- **SMS Gateway:** Click "Configure" button to setup SMS gateway integration. On-Demand account information can be sent via SMS message upon account creation.
- **Email Verification:** Click "Configure" button to setup Email verification feature. Users are able to access additional quota for the account by activating the link sent via Email.
- **Account Roaming Out:** Enable/Disable On-Demand account database when the Controller is used as RADIUS server for external RADIUS authentication requests.
  - **RADIUS Client Device Settings:** Configure the client list and secret key for those devices allowed to do RADIUS or 802.1X authentication with the Controller.

## Billing Plans

Billing Plans						
No	Plan Type	Quota	Price	Active	Group	Function
1	N/A			<input type="checkbox"/>	Group 1	Reset
2	N/A			<input type="checkbox"/>	Group 1	Reset
3	N/A			<input type="checkbox"/>	Group 1	Reset
4	N/A			<input type="checkbox"/>	Group 1	Reset
5	N/A			<input type="checkbox"/>	Group 1	Reset
6	N/A			<input type="checkbox"/>	Group 1	Reset
7	N/A			<input type="checkbox"/>	Group 1	Reset
8	N/A			<input type="checkbox"/>	Group 1	Reset
9	N/A			<input type="checkbox"/>	Group 1	Reset
0	N/A			<input type="checkbox"/>	Group 1	Reset

10 billing plans can be configured at most. There are 4 types of billing plans: Usage-time, Volume, Hotel Cut-off Time, and Duration-time. The concept of the billing plan types, please see Appendix D.

## Payment Gateway

## External Payment Gateway

### Selection

Disable  Authorize.Net  PayPal  SecurePay  WorldPay  PeleCard

Number of SMS quota  \*(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 or if the SMS needs to be re-sent.

### PayPal Payment Page Configuration

Business Account	<input type="text"/>	*
Payment Gateway URL	<input type="text" value="https://www.paypal.com/cgi-bin/webscr"/>	*
Identity Token	<input type="text"/>	*
Instant Payment Notification (IPN)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="checkbox"/> Behind NAT	
Verify SSL Certificate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="Default"/>	
Currency	<input type="text" value="USD (U.S. Dollar)"/>	*

- **Payment Page Configuration:** There are different required information to be filled for each type of payment gateways. You should be able to find those information in your payment gateway accounts.
- **Instant Payment Notification (IPN):** (Paypal only) When enabling IPN, Paypal will send notification to the controller when transaction is occurring. Please be careful that if your controller's WAN IP is under a NAT, you will need to configure IP forwarding information in order for the paying end user to receive transaction outcome.
- **Choose Billing Plans for Payment Page:** Select available billing plans when users purchase account.
- **Web Page Customization:** Click "Configure" to customize Service Disclaimer Page, Billing Plan Selection Page, and Account Credential Page.

### SMS Gateway

- **Selection:** Type of SMS Gateway to be integrated.
  - **Clickatell:** Connect with Clickatell API to send SMS messages.
  - **SMS API:** Generic option to integrate with the HTTP API of SMS gateways. The controller will send HTTP request to the specified API URL with the parameters configured, and identify whether the request is successful or not with defined pattern.
- **Version (Clickatell only):** Old (Prior to November 2016) version is the Clickatell API in REST protocol in JSON format for API ID, User Name, and Password. New version is only required API Key in HTTPs protocol for integration.
- **Send SMS for:** Select under what condition the controller will send SMS messages.
  - **Account Registration:** Allow users to self-registration and receive a Wi-Fi account via SMS.
  - **Account Purchases via Payment Gateway:** 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.
  - **Both:** Enable both options.
- **API Key (Clickatell only):** The authentication key for Clickatell API which is used to call and unlock the specific integration service.
- **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:** Select allow to allow the same mobile number to request a 2nd On-Demand account even though the 1st account hasn't expired or been used yet. Select block to restrict users to sending a 2nd On-Demand account only after their 1st account has expired

## SMS Gateway

**Selection**  Disable  Clickatell  SMS API  
**Version**  Old (Prior to November 2016)  New  
**Send SMS for**   
**API key**  \*  
**API URL**  \*  
**Registration before Accounts Expired**  Allow  Block  
**Billing Plans**

Plan	Activation	Quota	Price	Remark
1	<input type="checkbox"/>			
2	<input type="checkbox"/>			
3	<input type="checkbox"/>			
4	<input type="checkbox"/>			
5	<input type="checkbox"/>			
6	<input type="checkbox"/>			
7	<input type="checkbox"/>			
8	<input type="checkbox"/>			
9	<input type="checkbox"/>			
10	<input type="checkbox"/>			

**Account Registration Control**  Disable  Black List  White List  
**Web Page Customization**

- **Parameter (SMS API only):** API parameters and values for sending an SMS request.
- **Response Format (SMS API only):** 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 (SMS API only):** Key Path of the value from the SMS request's response in JSON format. Example: ['data'][0]['status']
- **Return Value of Successful Request (SMS API only):** The text of the successful response is entered here.
- **Send Test Message (SMS API only):** 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 (SMS API only):** 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
<b>\$username</b>	Username of the created On-Demand account.
<b>\$Username_without_postfix</b>	Same as \$username, but without the postfix.
<b>\$password</b>	Password of the created On-Demand account.
<b>\$quota</b>	Quota description for the created On-Demand account.

## SMS Gateway

Disable     Clickatell     SMS API

Send SMS for:

API URL:  \*

Registration before Accounts Expired:  Allow     Block

No.	Parameter	Parameter Value	Remark
-	<input type="text"/>	<input type="text"/>	Phone Number
-	<input type="text"/>	<input type="text"/>	SMS Content
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>

Response Format:  JSON     HTML

Key of JSON Array:  \*

Return Value of Successful Request:  \*

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

Send Test Message:

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

**Message Editor**

Parameter	Value
<input type="text" value="\$username"/>	<input type="text" value="On-Demand Username"/>
<input type="button" value="Insert Parameter"/>	

Billing Plans

Plan	Activation	Quota	Price	Remark
1	<input type="checkbox"/>			<input type="text"/>
2	<input type="checkbox"/>			<input type="text"/>
3	<input type="checkbox"/>			<input type="text"/>
4	<input type="checkbox"/>			<input type="text"/>
5	<input type="checkbox"/>			<input type="text"/>
6	<input type="checkbox"/>			<input type="text"/>
7	<input type="checkbox"/>			<input type="text"/>
8	<input type="checkbox"/>			<input type="text"/>
9	<input type="checkbox"/>			<input type="text"/>
10	<input type="checkbox"/>			<input type="text"/>

Account Registration Control:  Disable     Black List     White List

Web Page Customization:

- **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.

## Email Verification

### Email Verification

Selection  Disable  Enable

Choose Billing Plan for Redeeming Account via Email (Only Usage Time selectable)

Plan	Activation	Quota	Redeem Quota	Price	Remark
1	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
2	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
3	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
4	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
5	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
6	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
7	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
8	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
9	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
10	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		

SMTP Server Settings

SMTP server is not ready

Sender Name	<input type="text" value="Internet Service"/>	*(name@domain)
Activation Email Subject	<input type="text" value="Please activate your account"/>	
Activation Email Content	<input type="text" value="Congratulations! You are eligible for free access. Please click the link below to activate your account for extended usage time."/>	
Activation Link	<input type="text" value="Click Here!"/>	

Web Page Customization

- **Selection:** Enable or disable the feature.
- **Choose Billing Plan for Redeeming Account via Email (only Usage Time Selectable):** Choose the configured billing plans, while only Usage type billing plan support this feature.
  - **Activation:** Select which billing plan allowed email verification feature
  - **Quota:** View the current summary of each billing plan.
  - **Redeem Quota:** The usage time that can be additionally used when redeeming.
  - **Price:** View the current price of each billing plan.
  - **Remark:** A custom field for identity of each walled garden entry.
- **SMTP Server Settings:** Assign SMTP server for sending the mail for redeem clients. This SMTP is shared with Guest Email Verification.
- **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

## c) Guest Authentication

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. This feature allows the user to associate with a particular Service Zone, enter guest email or a specified string of text by guest questionnaire which may be social security number etc. defined by the administrator, and use the network without actual authentication.

The screenshot shows the 'Guest Authentication' configuration interface. It includes the following fields and options:

- Group:** Group 1
- Guest Information:** View
- Guest Questionnaire:** Configure
- Guest Access Time:** Radio buttons for Unlimited, 1 Day Access (selected), and Multi-Day Access.
- Quota:** 0 hour(s) 30 minute(s); 1000 MByte(s) \*(Range:0~1000000, 0:Unlimited)
- Reactivation:** After 0 hour(s) 1 minute(s)
- Access Limit:** 30 per day \*(0:Unlimited)
- Email Verification:** Radio buttons for Disable and Enable (selected).
- Email Activation Time:** 0 hour(s) 10 minute(s)
- Sender Name:** Internet Service \*(name@domain)
- Activation Email Subject:** Please activate your account
- Activation Email Content:** Congratulations! You are eligible for free access. Please click the link below to activate your account for extended usage time.
- Activation Link:** Click Here!
- Guest Quota List:** View
- E-mail Denial List:** Radio buttons for Disable (selected) and Enable, with a Configure button.

On the right side, there is a button 'Assign SMTP server' and a status message: 'SMTP server is not ready'.

- **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 Guest 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 On-Demand Email Verification. Taking Gmail as SMTP server 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:** Administrator'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.

## d) 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.

### One Time Password Authentication

---

Group	Group 1 ▼
OTP Client Information	View
Default Country Code	AF - AFGHANISTAN (+93) ▼ <input type="checkbox"/> only display default country code
Length of Mobile Number	0 <span style="color: red;">*(0: Unlimited)</span>
Quota	0 day(s) 0 hour(s) 30 minute(s) *
Questionnaire	Configure
SMS Gateway	Configure
OTP Page Customization	Configure

- **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 maximum 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 On-Demand User Database"

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

### 3) External Authentication

Up to 5 External Authentication servers can be set up and enabled concurrently to facilitate existing user account databases on your network. External Authentication options include RADIUS, POP3, LDAP, NT Domain, and SIP.

Authentication Options				
Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
Server 2	RADIUS	.	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>
Guest	FREE	N/A	<input type="radio"/>	<input checked="" type="checkbox"/>
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>

#### a) Social Media Authentication

- **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 Media Login

Group:

Social Media Account Information:

Social Media Account Access Time:  Unlimited  1 Day Access  Multi-Day Access

Quota:  hour(s)  minute(s)  
 MByte(s) \*(Range:0~1000000, 0:Unlimited)

Reactivation: After  hour(s)  minute(s)

Access Limit:  per day \*(0:Unlimited)

Social Media Account Quota List:

Punishment:  Enable  Disable

Punishment List:

- **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:** Enable/Disable the punishment mechanism. 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.
- **Punishment List:** The clients being punished are listed here. Administrators could help release the restriction in Punishment List.

## 4) On-Demand Accounts

### On-Demand Account Creation

Plan	Account Type	Quota	Price	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	1.99	1	<input type="button" value="Create Single"/> <input type="button" value="Create Batch"/>
2	Hotel Cut-off-time	Valid until 5:01 the following day	1	1	<input type="button" value="Create Single"/> <input type="button" value="Create Batch"/>
3	N/A				<input type="button" value="Create Single"/> <input type="button" value="Create Batch"/>
4	N/A				<input type="button" value="Create Single"/> <input type="button" value="Create Batch"/>
5	N/A				<input type="button" value="Create Single"/> <input type="button" value="Create Batch"/>

- **Account Creation:** Administrators can choose to create a single account or multiple accounts using the "Batch Create" function. Before accounts can be created, at least one Billing Plan needs to be set up and activated. Accounts can be created with random Usernames and Passwords or created manually (up to 8 characters). Usernames and Passwords can also be created manually for batch creation. (E.g. Prefix = ABC, Postfix = DEF, Serial Number 0001.)

## On-Demand Account List

<input type="checkbox"/>	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
<input type="checkbox"/>	28v2	Until 2013/02/07-02:00	Expired	Group 1	roomN-3154-00:09:6B:CD:82:47		
<input type="checkbox"/>	e69w	Until 2013/02/19-01:00	Expired	Group 1			
<input type="checkbox"/>	9u2u	Until 2013/02/19-03:03	Expired	Group 1			
<input type="checkbox"/>	ep4r	Until 2013/02/19-05:01	Expired	Group 1			

(Total:4/9000)    
 Go to Page  (Page:1/1)
 Row per Page:

- **Account List:** All created On-Demand accounts and related information are listed on this page. The list also allows administrators to manipulate On-Demand accounts, such as restoring/deleting accounts and Admin Redeem.

## 5) Schedule

The Administrator gets to set different Login Hour permissions to be applied to User Groups in enabled Service Zones. To apply the configured Schedule Profile, go to Groups Configuration.

### Schedule Permitted Login Hours - Profile 1

Select Schedule

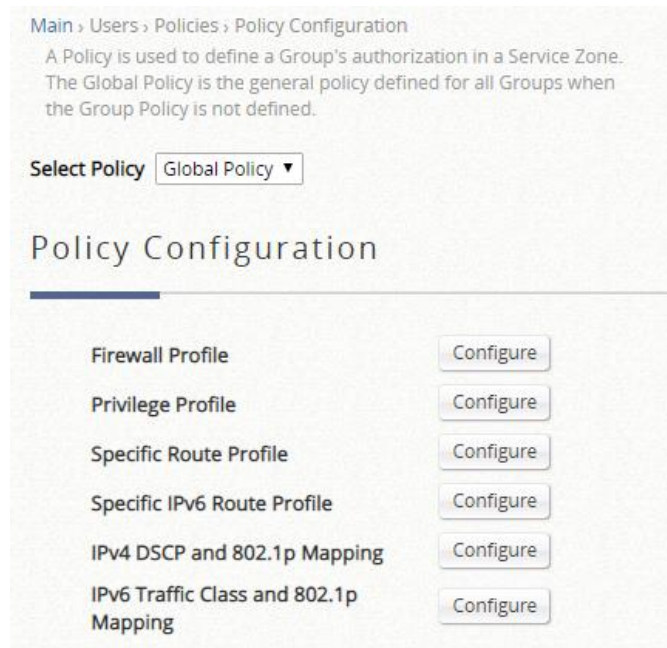
Schedule Name

<input type="checkbox"/>	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
<input type="checkbox"/>	SUN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MON	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	TUE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	WED	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	THU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	FRI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SAT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Log off authenticated users during unauthorized periods

## 6) Policies

Global policy is the system's universal policy including **Firewall Profile**, **Specific Route Profile**, **Schedule Profile**, and **Maximum Concurrent Sessions** management which will be applied to all users unless the user has been regulated and applied to another policy.



Each policy consists of **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** and **Maximum Concurrent Sessions** management as well. Policies can be defined in the Policy tab. The administrator can select one of the defined policies to apply it to groups within a certain Service Zone. A group of users within different Service Zones can be applied with different policies. For example, sales can be applied with different network access right while accessing from sales department region or finance department region.

- **Select Policy:** The number of different policy profiles available depends on the model type.
- **Firewall Profile:** Firewall profile specifies the protocols & rules that will be enforced to users governed by this policy. Each Policy profile has its own customizable firewall profile.
  - **Service Protocol:** This link leads to a policy's Service List page where the administrator can define 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 (Global Profile only):** Configure the options for protect against DoS attacks.
- **Privilege Profile:** User generated session number limit may be configured here. Please adjust this attribute carefully based on your network usage
  - **Password Change (Non-Global Profile only):** 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 (Non-Global Profile only):** 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 (Non-Global Policy only):** 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 routing rules to be applied to users under this policy may be set here.
- **Specific IPv6 Route Profile:** The routing rules to be applied to users under this policy may be set here.
- **IPv4 DSCP and 802.1p Mapping (Global Policy only):** This criteria enables the static mapping configuration from IPv4 DSCP tag into the desired 802.1p traffic class for sending in the managed VLAN network.
- **IPv6 Traffic Class and 802.1p Mapping (Global Policy only):** This criteria enables the static mapping configuration from IPv6 traffic tag into the desired 802.1p traffic class for sending in the managed VLAN network.

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 priority shall be the first applied Policy.

Select Policy Policy 1 ▾

### Policy Configuration

---

Policy Name	<input type="text" value="Policy 1"/>
Firewall Profile	<span>Firewall 1 ▾</span>
Privilege Profile	<span>Privilege 1 ▾</span>
QoS Profile	<span>QoS 1 ▾</span> <input type="checkbox"/> Enable Bandwidth Throttling in <input type="text" value="5"/> min(s) and change the profile to <span>QoS 1 ▾</span>
Specific Route Profile	<span>Specific Route 1 ▾</span>
Prefer DHCP Pool	<span>None ▾</span>

A Preferred DHCP Pool (defined in Service Zone DHCP configurations) may be selected here as well.

## 7) 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. The administrator may select one blacklist from the drop-down menu and this blacklist will be applied to this specific authentication option. Note that names on the Blacklists can be configured to be case insensitive.



Select Blacklist 1: Blacklist1

## Blacklist Settings

Blacklist Name:

Case Insensitive with blacklist:  Disable  Enable

	User Name	Remark
(Total:0/40) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a> Go to Page <input type="text"/> (Page:1/1) Row per Page: <input type="text" value="10"/>		

## 8) Privilege Lists

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.

SYSTEM **USERS** ACCESS POINTS NETWORK UTILITIES STATUS

Main > Users > Privilege List > IP Address

### IP Privilege List

No.	IP Address	MAC Address	Group	Remark
(Total:0/200) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a> Go To Page <input type="text"/> (Page:1/1) Row per Page: <input type="text" value="10"/>				

- **Privilege List:** There are three types of authentication free lists where the administrator can designate privileged individual access without the need of authentication. This may be achieved either via IP address, IPv6 Address or MAC address.

## 9) 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. The administrator can control user session such as idle timeout in User Session Control. Three functions are provided in Built-in RADIUS Server Settings such as session timeout. In Customization, the administrator can upload certificate to the system. Remaining Time Reminder provides remaining time information to clients on the screen. The administrator can manage the access control to the system via clients' MAC address in the MAC ACL (Access Control List).

## User Session Control

---

**Idle Timeout**  minute(s) \*(1-5040)  
**Detection Interval**  second(s) \*(1-600)  
**Traffic Direction for Idle Timeout**  ▾  
**Timeout Threshold**  byte(s) \*(0-1048576, 0 is Disabled)

**User Options**
 Charge Traffic to/from Hosts in Walled Garden List  
 Kick user when user's IP change  
 Log NAT Mapped in User Session Log

---

## Built-in RADIUS Server Settings

---

**Session Timeout**  minute(s) \*(5-43200)  
**Idle Timeout**  minute(s) \*(1-5040)  
**Interim Update**  minute(s) \*(1-120)  
**Certificate**  ▾

---

## Remaining Quota Reminder

---

**Time and Cut-off Reminder**  Enable  Disable  
**Volume Reminder**  Enable  Disable  
**Reminder Refresh Time**  10mins  15mins  20mins

---

## MAC Access Control List

---

**MAC Access Control List**

MAC Access Control is used to grant or deny permission to access the User Login Page.

### 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 by uplink traffic only or both direction.
- **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**

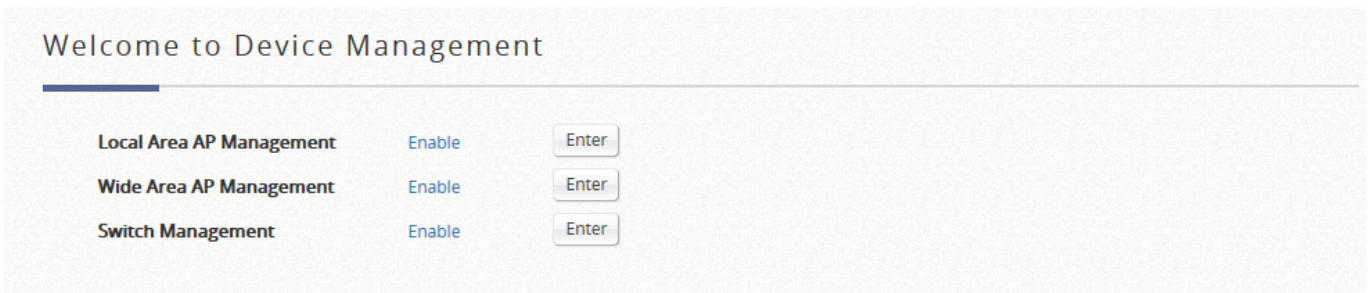
- **Time and Cut-off reminder:** This is the option for the system to display a warning message to On-Demand users that their time based account quota is about to run out.
- **Volume Reminder:** This is the option for the system to display a warning message to On-Demand users that their volume based 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**

- **MAC ACL:** The administrator may configure restraining measures to MAC address, either MAC allow or deny list.

## C. Devices

**Devices:** This section is used to manage the APs and switches. Besides showing the various attributes of APs and switches, there are different functions provided for various configurations.



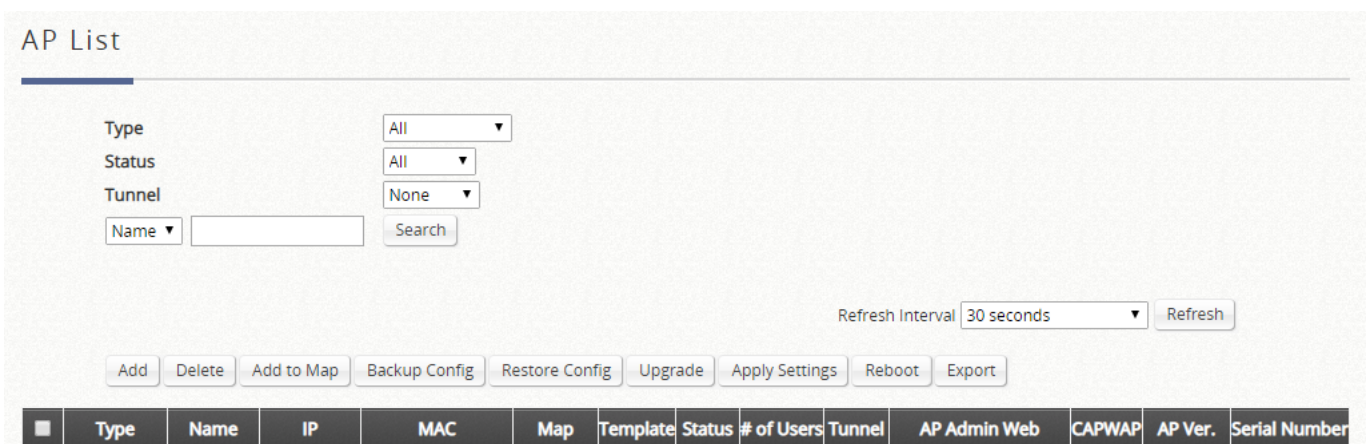
### 1) Wide Area AP Management

#### a) AP List

A list is to show the information of each managed AP, including Type, Name, IP Address, MAC Address, AP Online/ Offline Status, # of Users, tunnel Status, AP Firmware version, and Geographic location.

Functions in this section also include the operations such as Delete, Add to Map, Backup Config, Restore Config, Upgrade, Applying Settings, and Reboot.

All of the supported APs under management of the system will be shown on the list. In the beginning, the list is empty. The administrator can add supported APs from the Discovery or Adding tabs. 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. The administrator can Delete, Add to Map, Backup Config, Restore Config, Upgrade, Applying Settings, Reboot the managed AP by checking the check box in front of each individual AP or select all the APs together by checking the top check box.



After adding APs to the managed List, some operations can be executed for managing the listed AP's.

- **Go:** The EWS Controller cannot directly configure Wide Area AP's settings remotely. However, the Goto button is a convenient link for accessing the remote AP's WMI.

Please note that the **Goto** button will only become active when the listed AP's status is Online.

The screenshot shows the 'AP List' interface. At the top, there are filters for Type (All), Status (All), and Tunnel (None), along with a search box. Below the filters are buttons for Add, Delete, Add to Map / Floor Plan, Backup Config, Restore Config, Upgrade, Apply Settings, and Reboot. A 'Refresh Interval' dropdown is set to 120 seconds. The main table has columns: Type, Name, IP, MAC, Map, Template, Status, # of Users, Tunnel, AP Admin Web, CAPWAP, and AP Ver. One AP is listed: ECWS211-L, ECWS211-L, 10.73.7.38, 00:1F:D4:06:F1:1D, Overview, 1, Online, 0. The 'AP Admin Web' column has a dropdown menu open, showing options: System Overview (selected), VAP Overview, WDS Overview, System Upgrade, Reboot, WDS Status, Associated Clients, and Event Log.

The drop down list on the column header is for specifying which WMI page to go to.

- **Delete:** Remove the checked AP from the List.
- **Add to Map/Floor Plan:** Clicking this button will open a popup window. Administrator can Mark the selected APs on the Map or on the floor plan from the drop down list. If no map profile or floor plan has been configured, there will be no available map/floor plan to choose in the drop down list.
- **Backup Config:** Clicking this button will open a popup window where administrator can backup the chosen AP's configuration settings into a .db file stored in the EWS Controller's storage. The Backup up files are listed under Backup Config tab page for download or deletion.
- **Restore Config:** Clicking this button will open a popup window where administrator can restore the chosen AP's configuration settings using a .db file stored locally in administrator PC or in the EWS Controller's storage.
- **Upgrade:** Clicking this button will open a popup window where administrator can upgrade the chosen AP's firmware using a firmware file stored locally in administrator PC or in the EWS Controller's memory (under **Firmware** tab page).
- **Apply Settings:** Apply the already prepared WAPM templates to selected AP so as to implement some AP's configuration or change AP Admin's password for certain administration application.
- **Reboot:** clicking this button will restart the selected AP.
- **Export:** Export current AP List with selectable columns.
- **Edit (AP Name):** Click this button to enter the AP's attribute editing page where administrator can specify the Device Name and SNMP community. If the AP is to be marked on a map, this page also allows administrator to configure the geographical location, coverage, related links and customize marker or icon images that will be displayed on the map.
- **Edit (Tunnel Status):** Click this button to setup Port Location Mapping parameters of the complete tunnel VAPs. Administrator can allocate NAS Identifier and designate an IP pool for service for each

complete-tunneled VAP of a Managed AP.

Go to: **Main >> Devices >> Wide Area AP Management >> AP List.**

AP List

Type: All  
Status: All  
Tunnel: None  
Name:  Search

Refresh Interval: Disable Auto Refresh Refresh

Add Delete Add to Map Backup Config Restore Config Upgrade Apply Settings Reboot Export

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
ECW5211-L	ECW05211-L	10.71.36.55	00:1F:D4:07:42:CD	Overview	1	Online	0	<b>Edit</b>	System Overview Go	RUN	3.45.0000	N/A



### Enterprise\_Access\_Point\_-\_ECW5211-L: VAP Status

Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
VAP-1	ECW5211-L-1	1000	<b>Configure</b>	Default



### Tunnel Port Location Mapping Setup

Service Zone / Prefer DHCP Pool: Default / None

User Limitation:  (Blank is for unlimited.)

ESSID: ECW5211-L-1

Room Number / Location ID:

Room Description / Location Name:

NAS Identifier:

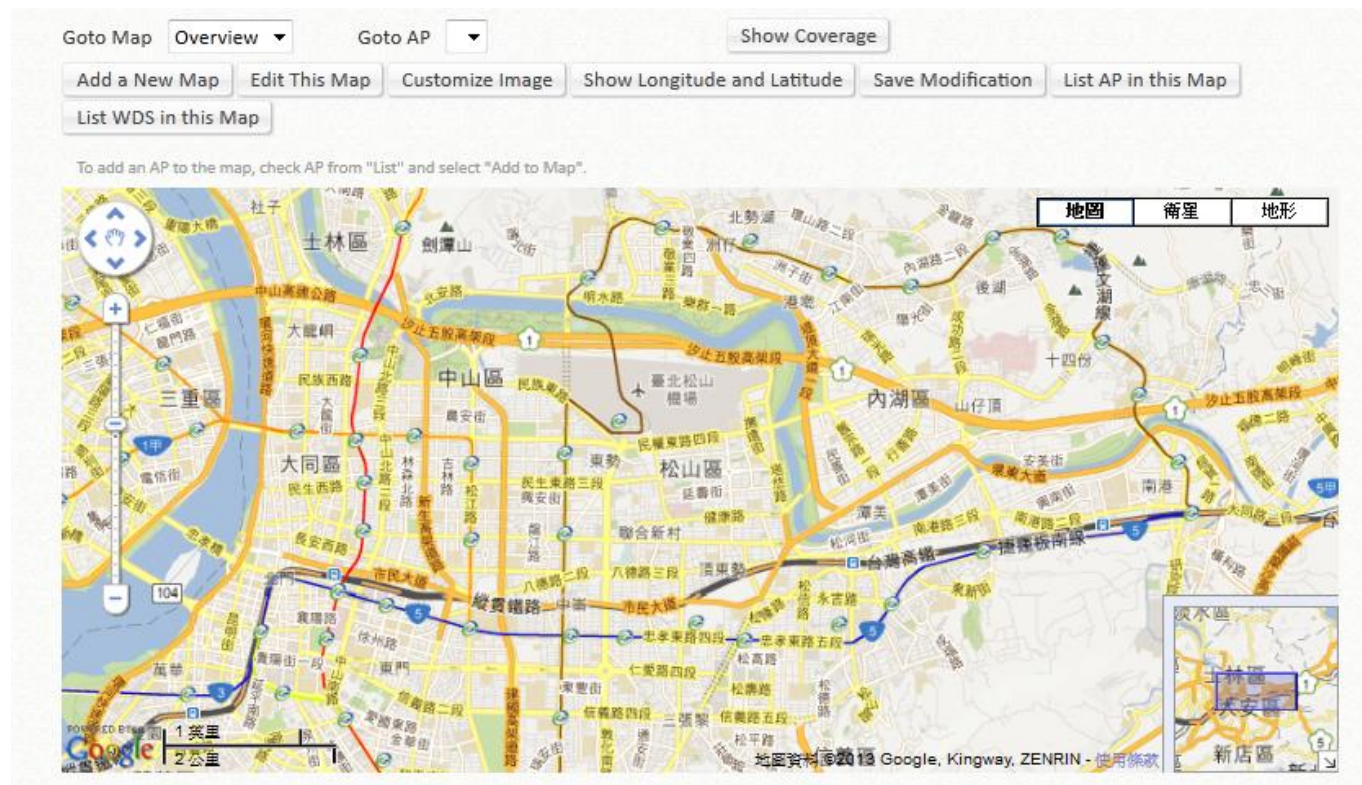
- **Service Zone / Prefer DHCP Pool:** This field entry shows the SZ to which this VAP will be tunneled to. Preferred DHCP pool allows the admin to specify the IP pool allocated to issuing IP to clients in this VAP.
- **User Limitation:** Administrator can specify the number of clients which can be allocated an IP address for service from this VAP.
- **ESSID:** The ESSID of this VAP is displayed here.
- **Room Number / Location ID:** Administrator can input a string of text describing the location ID of this VAP.
- **Room Description/ Location Name:** Administrator can input a string of text describing the location name of this VAP.
- **NAS Identifier:** Administrator can assign an additional NAS ID to be coupled with this VAP if necessary.

## b) AP Grouping

### Map Configuration

The Map tab page is implemented with Google Map API version 3 which allows administrators to view at a glance the whereabouts of all of the AP's under Wide Area AP Management. 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:



#### **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://cloud.google.com/maps-platform/> to obtain such Maps API v3 key and provide the key info into the field of **Google Maps Registration Key** under **Map Configuration page**.

Google code

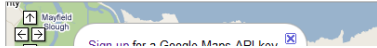
e.g. "ajax apis" or "open source"

**★ Google Maps JavaScript API V2 (Deprecated)** Home Docs FAQ Articles Blog Forum Terms

**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.

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:  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 EWS Controller's WAN IP address.

Google will generate an API key for your EWS Controller.

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

Your key is:

ABQIAAAAKf\_mMpRETFZUaDr5paUTBTQNSKw9wi47VEiW-QmsIzRiVcN7BTEWPFVn15GqX0pgc0YJAeFkFgv6A

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

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&v=2&sensor=true_or_false&key=ABQIAAAAKf_mMpRETFZUaDr5paUTBTQNSKw9wi47VEiW-QmsIzRiVcN7BTEWPFVn
...
    
```

See [Loading the Maps API](#) in the JavaScript Maps API documentation for more information.

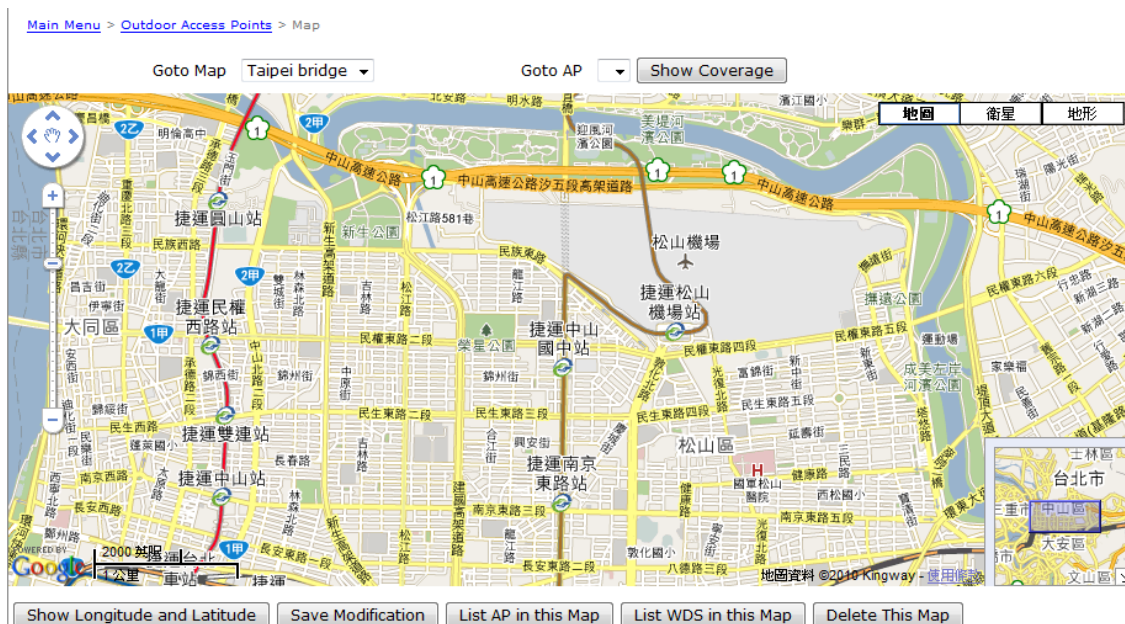
Now, return to the **Map** tab page in EWS Controller's WMI and Scroll down to the bottom of the page, click on the **Add a New Map** button.



## MAP Configuration

Map Name	Taipei Bridge
Latitude	25
Longitude	121
Google Maps Registration Key	AlzaSyDzjF1tWlf6158aJw7zGAXBYscY-L8Dtd8
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.



The above screenshot is an example showing Taipei City with Map Name as Taipei Bridge, 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 : ECW5211-L

Device Name	<input type="text" value="ECW5211-L"/>	*
SNMP Community	<input type="text" value="public"/>	*modify snmp setting will reboot the AP
SNMP Write Community	<input type="text" value="private"/>	*modify snmp setting will reboot the AP
Latitude	<input type="text" value="0.0"/>	*-85 ~ 85
Longitude	<input type="text" value="0.0"/>	*-180 ~ 180
Remark	<input type="text"/>	
Link 1	Name:	<input type="text"/>
	Description:	<input type="text"/>
	URL:	<input type="text"/>
Link 2	Name:	<input type="text"/>
	Description:	<input type="text"/>
	URL:	<input type="text"/>
Link 3	Name:	<input type="text"/>
	Description:	<input type="text"/>
	URL:	<input type="text"/>

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/Floor Plan**" button, choose the name of the map on which you wish to mark these APs and click **OK** button.

AP List

Type:  Status:  Tunnel:  Name:  Search

Refresh Interval:  Refresh

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
ECW5211-L	ECW05211-L	10.71.36.55	00:1F:D4:07:42:CD	Overview	1	Online	0	<input type="button" value="Edit"/>	<input type="text" value="System Overview"/> <input type="button" value="Go"/>	RUN	3.45.0000	N/A

Add to Map - Google Chrome

⚠ 不安全 | <https://10.71.36.101/OutdoorEquipmentManagement/AddToMap.shtml>

### Add to Map

Add AP(ECW5211-L)

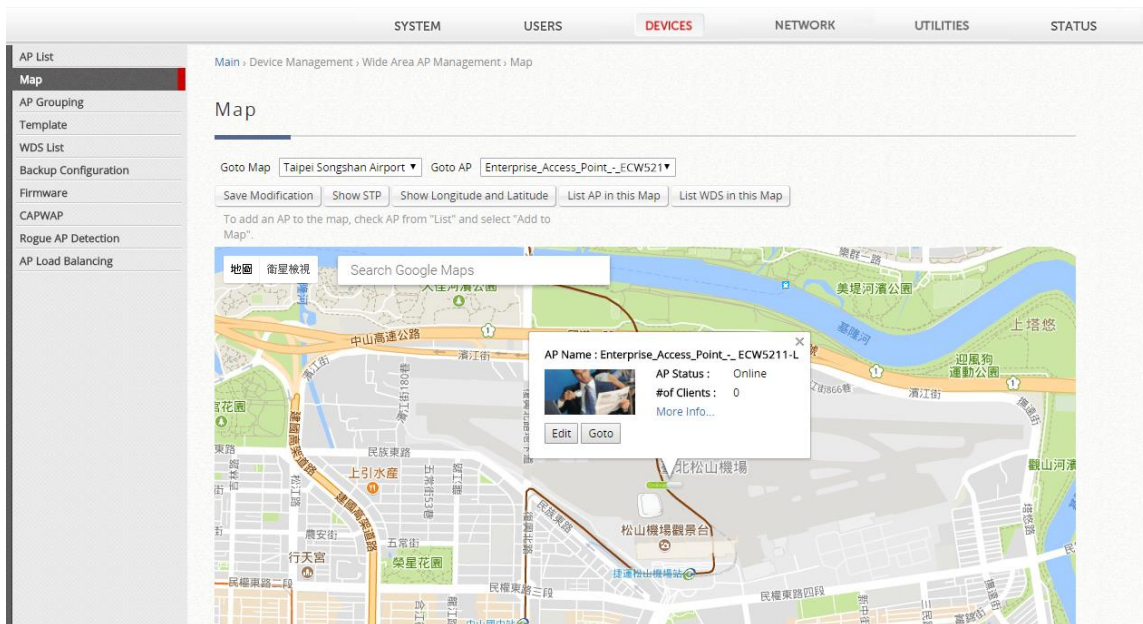
Add into a map

Select Map:

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



You can click on the AP icon to see the dialogue box for additional information or links that you have configured. Click the **more info** link for information on **AP status**, **Client List**, **WDS List** and **Links** related to this AP.



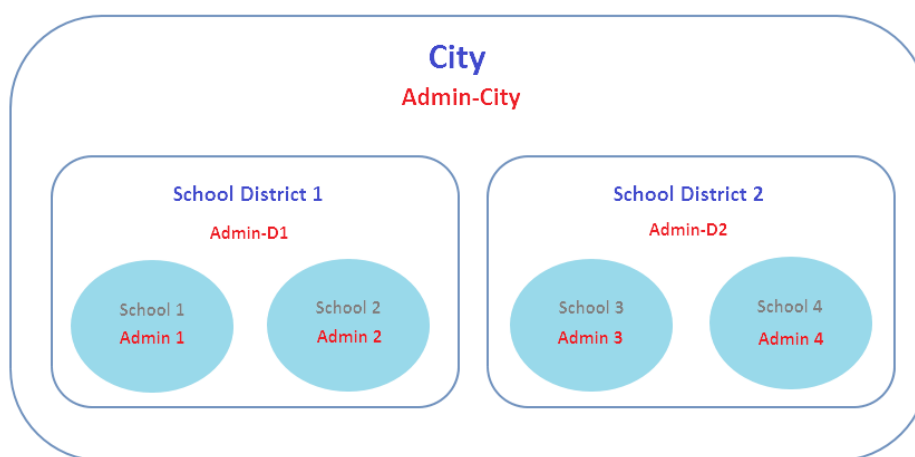


AP status, Client List and WDS List information listed are collected from the remote AP via SNMP.

### 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:

1. 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**.
2. 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)"

3. Go back to the List page, choose the AP, and then click the **“Add to Map/Floor Plan”** button, and choose the desired map. After the settings, admin should be able to see an icon of the AP on the selected map.
4. Overview path: *“Main Menu > Devices > Wide Area AP Management > Map”*
5. Go to *“Main Menu > Devices > Wide Area AP Management > AP Grouping > AP Grouping List”* to add or delete the AP group.

### AP Grouping

Add Delete

AP Group	Map	Template
<input type="checkbox"/> 456	<input type="text" value="123"/>	<input type="radio"/> 1 <input type="radio"/> 3 <input type="radio"/> 5

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

### AP Grouping Add

AP Group Name:

Map

Selectable	Selected
	Overview
	123

Template

Selectable	Selected
Template2	Template1
Template4	Template3
Template5	Template6
Template7	
Template8	

7. 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.

## Administrator Group List

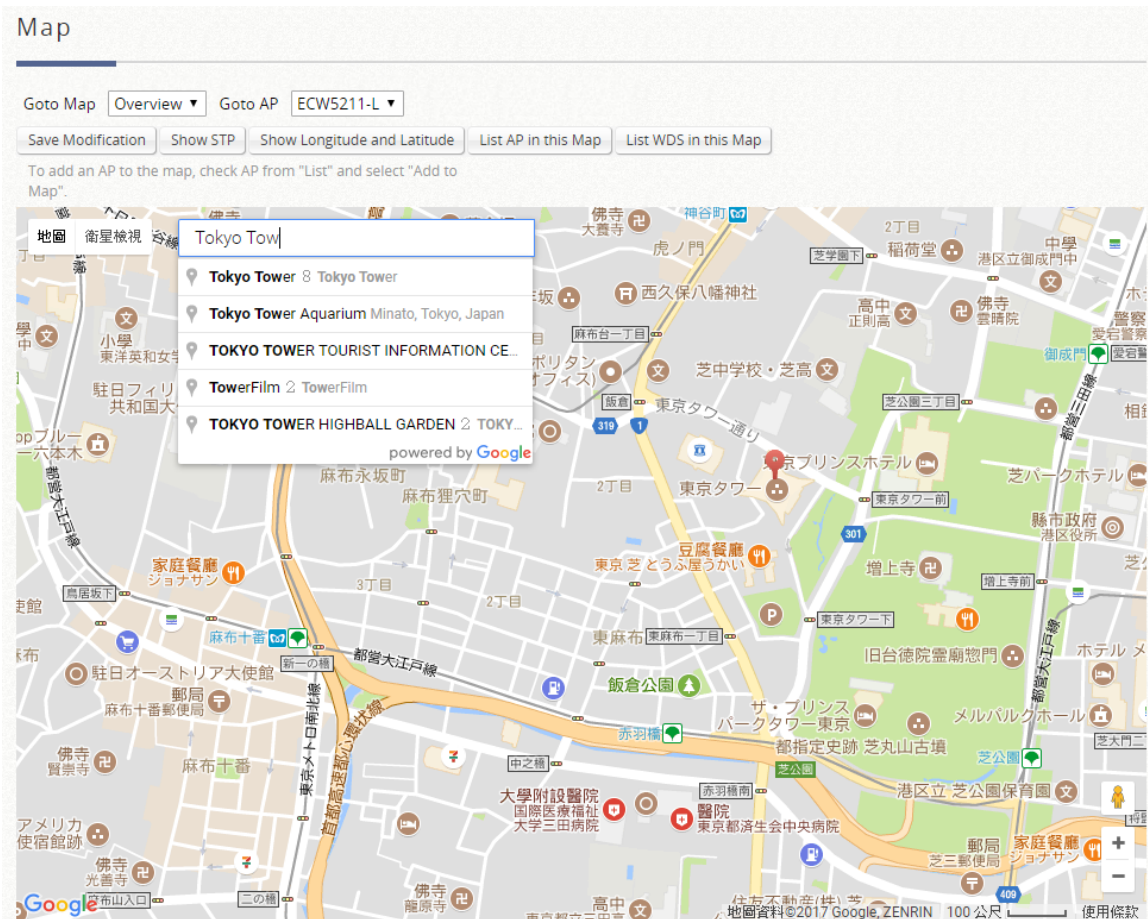
<input type="checkbox"/>	name	remark
<input type="checkbox"/>	Super Group	remark
<input type="checkbox"/>	Manager	remark
<input type="checkbox"/>	Operator	remark
<input type="checkbox"/>	On Demand	remark
<input type="checkbox"/>	Custom 1	remark
<input type="checkbox"/>	Custom 2	remark
<input type="checkbox"/>	Custom 3	remark

### 8. Assigning permission to an AP group.

	Disabled	SZ7
	Disabled	SZ8
AP GROUP	Disabled	Select All
	Disabled	456
	Read Only	
	Read/Write	
	Disabled	Select All
AP Management	Disabled	Local Area AP Management
	Disabled	Wide Area AP Management
Switch Management	Disabled	

### c) Map

Map shows the managed APs and their WDS links on Google Maps. It is a utility for wireless network planning and management.



- **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 (except Overview map):** 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:** Clicking this button will 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:** Clicking this button will 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.
- **Distance Calculation:** Calculation the distance between the two selected APs.

## d) Discovery

This Discovery function is to detect the supported types of APs through Internet or Intranet. The discovered AP can be added into managed devices, and automatically assigned the SNMP read community string, which will be used for periodical status collection. To Discover APs, click **Add** from the AP List and select **Discovery** from the Add Method dropdown list.

When the administrator tries to discover a new AP, select the Device Type. Second, enter the current IP range of the APs; Login ID and Password. Then click Discovery button. If the new AP is discovered, it will appear in the following Discovery Results list.

Add Method Discovery ▾

### Discovery AP

Device Type ECW100 ▾

Admin Settings Used to Discover

Start IP Address  \*

End IP Address

Login ID  \*

Password  \*

### Device Results

■	Device Type	IP Address	Device Name	SNMP Community	SNMP Write Community	Map
---	-------------	------------	-------------	----------------	----------------------	-----

- **Start / End IP address:** Administrator needs to specify the IP address range for AP discovery, and the specified IP address can be external or internal network IP addresses. This is useful when scanning for multiple devices connected to the managed network. APs with an IP address that is not within the specified range will not be listed after discovery.
- **Login ID / Password:** Filling in the Login ID and Password of the target AP's management interface will allow the administrator to remotely configure the AP's SNMP community.
- **Discover:** When the administrator tries to discover a new AP, select the **Device Type**. Second, enter the current IP range of the APs, **Login ID** and **Password**. Then click **Discover** button. If the new AP is discovered, it will appear in the following Discovery Results list. The administrator may stop the controller from scanning at any time during the discovery process.
- **Device Results:** When the discovery process is complete, the APs found will be listed here. The administrator can click **Add** to register the APs to the List for management.
  - **Device Type:** The AP model of the discovered AP.
  - **IP Address:** The IP address of the discovered AP.
  - **Device Name:** To identify the device by setup the device name.
  - **SNMP Community:** The SNMP Read Community string used for status access.
  - **SNMP Write Community:** The SNMP Write Community string used for configuration modification.
  - **Map:** To specify the managed device in certain Map for tier administration or graphical view.

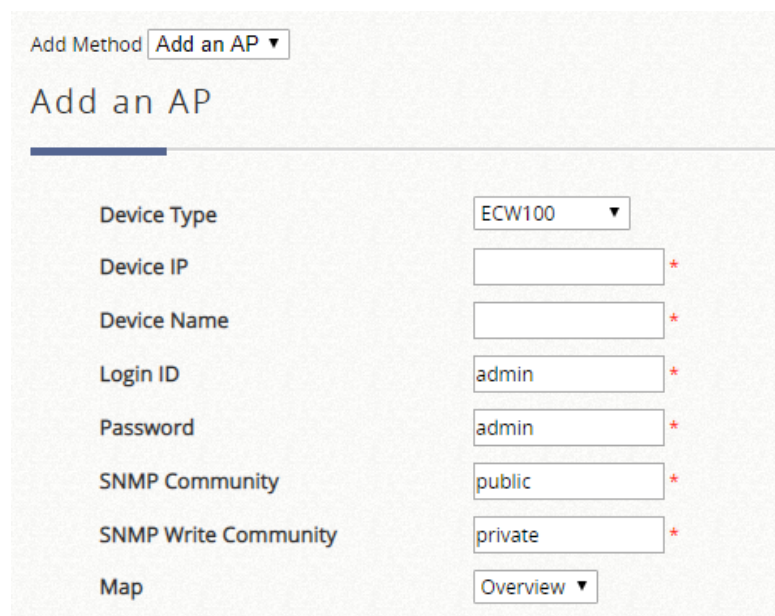


## e) Adding

The Adding function is used to manually set up an AP via filling in the required information for that AP.

Besides the **Discovery** feature that can search and list multiple APs for adding to the management list, administrators can also select **Add an AP** to directly add a single Access Point to the management list. Simply configure the devices IP address, name and login credentials, set a SNMP community string and click the **Apply** button.

The administrator can add supported APs onto the List table manually here. A manually added AP will show up with a status of "offline" in the AP List initially. The system will attempt to connect to the AP by SNMP protocol. After successful SNMP Reads, the manually added AP will become online.



The screenshot shows a web interface for adding a new Access Point (AP). At the top, there is a section labeled 'Add Method' with a dropdown menu set to 'Add an AP'. Below this is the main heading 'Add an AP'. The form contains several input fields and a dropdown menu:

- Device Type:** A dropdown menu with 'ECW100' selected.
- Device IP:** An empty text input field with a red asterisk indicating it is required.
- Device Name:** An empty text input field with a red asterisk indicating it is required.
- Login ID:** A text input field containing 'admin' with a red asterisk indicating it is required.
- Password:** A text input field containing 'admin' with a red asterisk indicating it is required.
- SNMP Community:** A text input field containing 'public' with a red asterisk indicating it is required.
- SNMP Write Community:** A text input field containing 'private' with a red asterisk indicating it is required.
- Map:** A dropdown menu with 'Overview' selected.

- **Device Type:** The device type of Wide Area APs.
- **Device IP:** The IP address of the AP to add to the management list.
- **Device Name:** The mnemonic name given to this AP device.
- **Login ID:** The Device's management interface login name.
- **Password:** The Device's management interface login password.
- **SNMP Community:** The SNMP Read Community string used for status access.
- **SNMP Write Community:** The SNMP Write Community string used for configuration modification.
- **Map:** To specify the managed device in certain Map for tier administration or graphical view.

## f) Template

Template AP Setting

Select Template	1: Template 1 ▾	
Template Name	Template 1	Apply
General Settings	Configure	
VAP Configuration	Configure	
Security Settings	Configure	
Advanced Wireless Settings	Configure	
Hotspot 2.0 Settings	Configure	
Firewall Settings	Configure	
Copy Settings to	None ▾	Apply

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**

## General Settings - 1: Template 1

RF Card Name	<input type="text" value="RF CARD A"/>
Band	<input type="text" value="802.11g+802.11n"/> <input type="checkbox"/> Pure 11n
Short Preamble	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Short Guard Interval	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Channel Width	<input type="text" value="20 MHz"/>
Channel	<input type="text" value="6"/>
Antenna Mode	<input type="text" value="Max"/>
Transmit Power	<input type="text" value="Level 1"/>
ACK Timeout	<input type="text" value="0"/> *(0 - 255, 0:Auto, Unit:4 micro seconds)
Beacon Interval	<input type="text" value="100"/> millisecond(s) *(100 - 500ms)
Airtime Fairness	<input checked="" type="radio"/> Disable <input type="radio"/> Fair Access <input type="radio"/> Preferred Access
Packet Delay Threshold	<input type="text" value="0"/> millisecond(s) *(100 - 5000ms, 0:Disable)
Idle Timeout	<input type="text" value="300"/> second(s) *(60 - 60000)
Band Steering	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="checkbox"/> Aggressive
Interference Detection	Adjacent Channel Utilization Threshold <input type="text" value="0"/> % *(60 - 99, 0:Disable) Latency <input type="text" value="10"/> second(s) *(10 - 999) Co-Channel Utilization Threshold <input type="text" value="0"/> % *(60 - 99, 0:Disable) Invalid Packet Rate <input type="text" value="90"/> % *(60 - 99) Latency <input type="text" value="10"/> second(s) *(10 - 999)
WME Configuration	<input type="text" value="Configure"/>
Transmission Rate Threshold	<input type="text" value="1001"/> kbps *(0:Disable)
CCA Minimum Power	<input checked="" type="radio"/> Auto <input type="radio"/> Dense Deployment <input type="radio"/> Sparse Deployment <input type="radio"/> Other <input type="text" value="-95"/> *( $\leq$ -75)
UAPSD	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

- **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.
- **Short Guard Interval (available when Band is 802.11g+802.11n or 802.11a+802.11n):** The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. In order to further boost throughput with 802.11n, short guard interval is half of what it used to be; please select *Enable* to use Short Guard Interval or *Disable* to use normal Guard Interval.
- **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. When configured as “Auto” and Band is “802.11a”, “802.11a+n”, or “802.11ac”, there is a channel selector table when the chosen channel is interfered or DFS channel signal is detected.
- **Antenna Mode (802.11g+n, 802.11a+n and 802.11ac only):** Configure the number of spatial streams for transmission and receiving.
- **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”, 802.11n and 802.11ac 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, latency, and invalid packet rate of the current channel or adjacent channels reaches the configured threshold, 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:** Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. 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.
- **UAPSD:** U-APSD stands for Unscheduled Automatic Power Save Delivery, an 802.11 power save mechanism that works with WMM. When a client device is in Power Save mode (i.e. its receiver is turned off and thus cannot receive any data frames), the AP will temporarily buffer all frames destined to the client.

➤ VAP Configuration

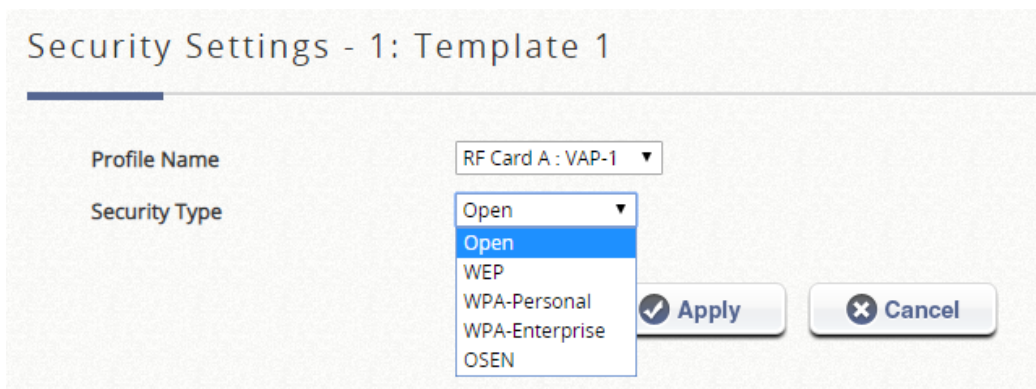
VAP Configuration - 1: Template 1

Profile Name	RF Card A : VAP-1
VAP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Profile Name	VAP-1
ESSID	Guest Network
Network Mode	Bridge
VLAN ID	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
	VLAN ID <input type="text"/> *( 1 - 4094 )
CAPWAP Tunnel Interface	Disabled
Service Schedule	24/7 Service
Access Control Type	<input checked="" type="radio"/> Disable <input type="radio"/> MAC ACL Allow List <input type="radio"/> MAC ACL Deny List

- **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.
- **Network Mode:** The operating mode for the VAP.
  - **Bridge Mode:** The VAP operates transparently (i.e. no NAT, no DHCP) such that client devices will be assigned a dynamic IP address from a DHCP server on the LAN side. The source IP address of client traffic seen by the uplink gateway/switch will remain the original IP address of the client.
  - **NAT Mode:** The VAP operates like a Network Address Translation (NAT) device with a built-in DHCP server on this SSID such that client devices will be assigned a dynamic IP address from the configured DHCP pool on this SSID. After NAT conversion, the source IP address of client traffic seen by the uplink gateway/switch will be the IP address of the AP.
- **Uplink Bandwidth:** Uplink bandwidth control is configurable on the VAP in Kbits per second. Set 0 for unlimited bandwidth control. Only configurable when VLAN is enabled. The VAPs with the same VLAN ID must have the same uplink bandwidth limitation.
- **Downlink Bandwidth:** Downlink bandwidth control is configurable on the VAP in Kbits per second. Set 0 for unlimited bandwidth control. Only configurable when VLAN is enabled.
- **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.
- **Service Zone:** For Complete-Tunnel or Split-Tunnel VAPs, select the Service Zone to be mapped to.
- **Service Schedule:** Customize the service hour of this VAP.

- **Access Control Type:** Configure a list of devices (MAC address) to decide which devices are allowed to associate to the VAP.
  - **Disable:** There is no restriction for client device to access.
  - **MAC ACL Allow List:** Only the client devices (MAC addresses) listed are granted access to the system.
  - **MAC ACL Deny List:** The client devices (MAC addresses) are granted access to the system except for the ones listed in the Deny List.

➤ **Security Settings**



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

➤ **Advanced Wireless Settings**

## Advanced Wireless Settings - 1: Template 1

Profile Name	RF Card A : VAP-1 ▾
RTS Threshold	2346 *(1 - 2346)
Fragment Threshold	2346 *(256 - 2346)
DTIM period	1 *(1 - 15)
Consecutive Dropped Packets	0 *(2 - 50, 0:Disable)
Broadcast SSID	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Wireless Station Isolation	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
WMM	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IAPP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Multicast-to-Unicast Conversion	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
TX STBC	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Multicast/Broadcast Rate	5.5M ▾
Management Frame Rate	5.5M ▾
Receiving RSSI Threshold	-80 *(-95 ~ 0, 0:disable)

- **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.
- **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.
- **TX STBC:** STBC is a pre-transmission encoding done by MIMO transmitter that allows it to improve the signal-to-noise ratio even at a single RF receiver (non-MIMO).
- **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.

#### ➤ **Hotspot 2.0 Settings**

Hotspot 2.0 is also known as WiFi Certified Passpoint initiated by the WiFi Alliance to provide better bandwidth and services for public WiFi subscribers. The HotSpot 2.0 feature is designed only for service providers and their partners. Please consult your service providers or our service team to complete the configuration.

#### ➤ **Firewall Settings**

- **Proxy ARP:** When enabled, AP will reply ARP requests on behalf of downlink stations. The ARP table maintained by the AP will be used as a look up table upon receipt of ARP request from AP uplink. Adversely, without Proxy ARP, ARP request is broadcasted down into the AP's wireless network causing network inefficiencies.

#### ➤ **Linkyfi's Location Engine**

Linkyfi is a platform designed by AVSystem for public Wi-Fi hotspots. Edgecore APs are able to be integrated with the dedicated Linkyfi server for location tracking and traffic analysis.

- **Real Time Location System:** Enable to integrate with the Linkyfi Real Time Location System (RTLS) server for indoor location and real-time navigation.
- **DNS DPI:** Enable to integrate with the Linkyfi DNS DPI server for analysis DNS traffic.

## **g) WDS List**

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, RSSI, TX Bytes, TX Packets, STP and Status.



## WDS List

Peer AP	Band	Channel	Security	TX Power	Link Speed	RSSI	TX Bytes	TX Packets	STP	Status
ECW5211-L-1	ac	165	AES	Level 1	144M	-64	284378	400	Disabled	Active
ECW5211-L-2				Level 1	144M	-64	56378	78	Disabled	

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.

## [h\) Backup Config](#)

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 EWS Controller's memory.

### Backup Config

Delete

<input type="checkbox"/>	Device Type	Version	Size	Backup Time	File Name	Actions
<input type="checkbox"/>	ECW5211-L	1.21.00	39947	2013/02/21 17:55:22	ECW5211-L	Download

Also, automatic **Daily Backup** is available. Configure backup time in 24-hour clock, then it will do backup configuration for the APs on the hour automatically.

## [i\) Firmware](#)

The EWS Controller can store AP's firmware in its' built-in memory. Under the **Firmware** tab page administrator can upload new AP firmware to the EWS 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 EWS Controller memory if desired.

### AP Firmware List

Add... Delete

<input type="checkbox"/>	File Name	Device Type	Version	Size	Actions
--------------------------	-----------	-------------	---------	------	---------

## j) CAPWAP

CAPWAP is a standard interoperable protocol that enables a EWS Controller to manage a collection of wireless access points.

Main > Device Management > Wide Area AP Management > CAPWAP

### CAPWAP Configuration

CAPWAP Status  Enable  Disable

Apply Certificate to APs

Trusted Certificate Authority(CA)

IP Address For Control Channel

IP Netmask For Control Channel

Control Channel IP Range 100.64.144.1 ~ 100.64.145.253

### Access Controller IP List

No.	IP Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>

- **CAPWAP Status:** The configuration status of CAPWAP function. Click **Enable** to turn on the Access EWS Controller to allow CAPWAP supported AP's to automatically add to the managed AP List.
- **Apply Certificate to APs:** This configuration item allows the administrator to select which of the certificates will be used during CAPWAP negotiation between AC and AP. If the certificate selected is invalid, the negotiation will be unsuccessful and the AP will not be automatically added in the managed List.
- **IP Address For Control Channel:** The IP address for AC side to negotiate the CAPWAP tunnel AP over the other side of control channel.
- **IP Netmask For Control Channel:** The netmask size could be automatically/ manually set according to the maximum number of managed APs.
- **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.

## k) Rogue AP Detection

It is designed to detect the non-managed or possibly malicious AP in the deployed environment. It takes the managed APs as sensors to find the non-managed AP even if the AP uses the same SSID with managed AP's. It shows the AP's BSSID, ESSID, Type, Channel, Encryption, and found time.

### General Configuration

Rogue AP Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Apply
Scanning Interval	<input type="text" value="0"/> minutes	
Channel Switching	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Sensor List	0/1	Configure
Trusted APs	0/40	Configure

### Rogue AP List

ESSID

<input type="checkbox"/>	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	Report Time
--------------------------	----	----------------	-------	------	---------	------------	-------------

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page  (Page:1/1) Row per Page:

## l) AP Load Balancing

This is a function to prevent managed APs from overloading. When the system detects the occurrence of APs' associated-client numbers exceeding a predefined threshold 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 allow other available APs to have more chance of being 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.

Wide Area AP Management feature also supports the grouping of various managed APs and perform transmit power management to spread the network load as evenly as possible among APs of the same group.

## WAPM Load Balancing

Load Balancing  Enable  Disable

AP Distance  meter(s)

Interval  minute(s)

Threshold  Number of Clients  clients  Number of Packets

Apply

## Map Cluster Setting

Map

Cluster

Cluster	Device Name	IP Address	RF	Power Level	# of Users	Log
---------	-------------	------------	----	-------------	------------	-----

- **WAPM Load Balancing:** This configuration item enables the administrator to specify the criteria under which AP load balancing feature will be enforced.
- **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.
- **Interval:** This parameter allows the administrator to specify a time interval when the controller will check the loading of each APs in the same group and initiate load balancing if necessary.
- **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.
- **Map:** Select the map to show the clusters and APs on this map.
- **Cluster:** Show the number of the clusters on this map.
  - **Configure:** Entering a page to enable/disable AP Load Balancing function on each cluster.
  - **Create:** Create clusters on current map according to AP distance.
  - **Delete:** Delete clusters on current map.
- **Cluster and Device List:** The scrollable window display all the managed APs sorted by model name with relative information such as Group, Name, IP, Power Level, Loading, etc. The managed APs will have a Group column for indicating which AP cluster it belongs to for AP Load Balancing feature to be enforced. Clear "View" button to see the logs of AP Load Balancing for each AP.

## m) Third Party AP Management

Add a third party AP by selecting THIRDPAP from Device Type. Add to AP List manually by specifying third party AP's IP address, 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	<input type="text" value="3rd Party AP"/> ▾
Device IP	<input type="text" value="192.168.1.1"/> *
Device Name	<input type="text" value="ThirdAP001"/> *
VLAN ID	<input type="text" value="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.

## 2) Switches

**Switches:** This section is used to configure all Switch Management related settings.

### a) Switch List

The EWS Controller is capable of managing the Edgecore switches. Switches under management of the system will be shown on this list.



Switch List

Status

<input type="checkbox"/>	Name	Type	Status	IP address	MAC address	Total allocated/Used/Max supply power [W]	Switch UI
--------------------------	------	------	--------	------------	-------------	---	-----------

The Switch's name will be shown as a hyperlink. Click the hyperlink of each managed switch for further configuration (General Setting, PoE Setting, VLAN Membership Setting, Port Setting, PoE Schedule) on the switch.

Click the hyperlink of the shown Status of each managed AP for detailed status information of the AP (General Setting, PoE Setting, VLAN Membership Setting, Port Setting, PoE Schedule).

- **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.

### b) PoE Schedule Template

The system supports up to a number of PoE Schedule Templates depending on your EWS model.

## PoE Schedule Template

Add template

Template Name	Copy Settings From	Remark	Action
Default	NONE		

Apply

Cancel

The first template is the default template and cannot be deleted. The Template Name may be customized for easy reference (e.g. Switch-Core1).

Click "Configure", illustrated by the pencil icon, to enter settings for the Template. The following can be set on the PoE Schedule Template:

- Power Supply Schedule

### Template Edit - Power supply schedule : Template\_2

	Day	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
<input type="checkbox"/>	Sun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Mon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Tue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Wed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Thu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Fri	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Sat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- Apply to: The band, channel width, transmit power and etc.

## Apply to

Refresh

<input type="checkbox"/>	Port	PoE Mode	Connected Device	<input type="checkbox"/>	Port	PoE Mode	Connected Device
<input type="checkbox"/>	1			<input type="checkbox"/>	13		
<input type="checkbox"/>	2			<input type="checkbox"/>	14		
<input type="checkbox"/>	3			<input type="checkbox"/>	15		
<input type="checkbox"/>	4			<input type="checkbox"/>	16		
<input type="checkbox"/>	5			<input type="checkbox"/>	17		
<input type="checkbox"/>	6			<input type="checkbox"/>	18		
<input type="checkbox"/>	7			<input type="checkbox"/>	19		
<input type="checkbox"/>	8			<input type="checkbox"/>	20		
<input type="checkbox"/>	9			<input type="checkbox"/>	21		
<input type="checkbox"/>	10			<input type="checkbox"/>	22		
<input type="checkbox"/>	11			<input type="checkbox"/>	23		
<input type="checkbox"/>	12			<input type="checkbox"/>	24		

If there is an existing managed switch online and you would like the same settings to be applied to newly added switches, choose from the drop-down list under "Copy Settings From" and click "Apply".

Additional remarks can be added to the Remark section for administrators' reference.

## c) 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.

## Backup Configuration

Delete

<input type="checkbox"/>	Device Type	Size	Backup time	File Name	Action
--------------------------	-------------	------	-------------	-----------	--------



# E. Network

**Network:** This section is used to configure all the network settings.

## 1) NAT

The NAT function supports 3 types of network address translation: DMZ (Demilitarized Zone), Public Accessible Server and IP/Port Forwarding.

### Demilitarized Zone

**DMZ (Demilitarized Zone)**

**WAN Assignment**  
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.

Assign WAN IP automatically

External Interface: WAN1  
External IP Address: 10.30.40.45  
Internal IP Address:   
Remark:

**Static Assignments**

No.	External IP Address	External Interface	Internal IP Address	Remark
1	<input type="text"/>	WAN1 ▾	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	WAN1 ▾	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	WAN1 ▾	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	WAN1 ▾	<input type="text"/>	<input type="text"/>

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.

### Public Accessible Servers

## Public Accessible Server

Enable	No.	External Port	Local Server IP Address	Local Server Port	Type	Remark
<input type="checkbox"/>	1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>

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.

## Port & IP Forwarding

### Port and IP Forwarding

No.	Destination		Translated to Destination		Type	Remark
	IP Address	Port	IP Address	Port		
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>

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**.

## 2) Monitor IP

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	<input type="text"/>
2	http ▾	<input type="text"/>	Create	<input type="text"/>
3	http ▾	<input type="text"/>	Create	<input type="text"/>

## 3) Walled Garden and Walled Garden Ad

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

200 entries can be added to the Walled Garden List.  
40 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
(Total:0/200) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a> Go to Page <input type="text"/> (Page:1/1) Row per Page: <input type="text" value="50"/>		

**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.

The system supports up to 200 Walled Garden entries, and 40 of the 200 can be selected as Walled Garden Advertisements.

### Add Walled Garden List

Domain Name/IP Address/URL: <input type="text"/>	
<b>Walled Garden</b>	<b>Advertisement</b>
Active: <input type="checkbox"/>	Display: <input type="checkbox"/>
Service Zone: All <input type="text"/>	Protocol: http <input type="text"/>
Remark: <input type="text"/>	Topic: <input type="text"/>
	Description: <input type="text"/>

- Click **Add** to add a new entry. Enter the Domain Name/IP Address/URL and select the “Active” checkbox. Click **Apply**, and the items will be added and shown on the list.
- **Display**: Choose **Display** to display advertisement hyperlinks on the login pages, corresponding to Service Zone configuration.

Note that entries selected as Walled Garden Ad must be a URL and cannot be an IP address with prefix. Note that both the checkboxes of walled garden and advertisement check should be checked for enabling walled garden advertisement feature.

## 4) VPN

On this tab, 2 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 iKEv2. For the Site-to-Site VPN, an IPSec tunnel can be used to connect to other IPSec capable device over the Internet.

## Remote VPN IKEv2

Function

Enable  Disable

Allocate IP Address from

IP Address  \* Subnet Mask

Certificate

WISPr

Authentication Options

Auth Option	Auth Database	Postfix	Enable
Server 1	LOCAL	local	<input type="checkbox"/>
Server 2	RADIUS	.	<input type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="checkbox"/>
Server 4	LDAP	ldap	<input type="checkbox"/>
Server 5	POP3	pop3	<input type="checkbox"/>

## Site-to-Site VPN

Local Sites

<input type="checkbox"/>	No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Tunnel Status
--------------------------	-----	-------------------	-----------------	--------------------	--------------------	---------------

Remote Sites

<input type="checkbox"/>	No.	Name	IP Address	Pre-shared Key
--------------------------	-----	------	------------	----------------

## 5) [Proxy Server](#)

The system provides a Built-in Proxy Server and External Proxy Server function. After successful authentication, the clients' will be directed 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 EWS CONTROLLER.

## Web Proxy Settings

Proxy Server

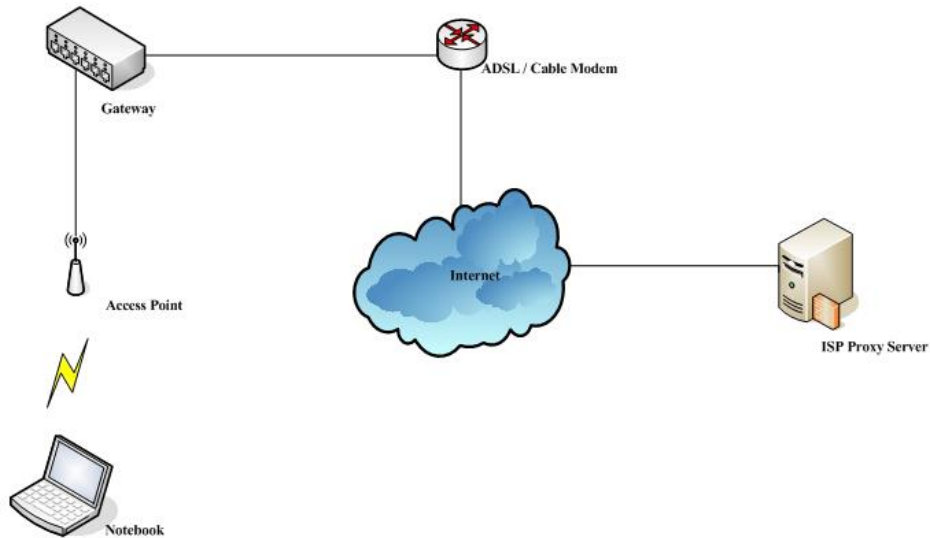
Enable Built-in  Disable Built-in  External

Apply

Cancel

### Using Internet Proxy Server

A built in proxy server in the controller can be **Enabled**, even with a Proxy Server placed outside the LAN environment or in the Internet. For example, the following diagram illustrates how a proxy server of an ISP is used.



Follow the following steps to complete the proxy configuration:

- Step 1.** Log into the system by using the **admin** account.
- Step 2.** **Network >> Proxy Server >> Web Proxy Settings** page.  
Enable the **Built-in Proxy Server**. Click **Apply** to save the settings.

## Web Proxy Settings

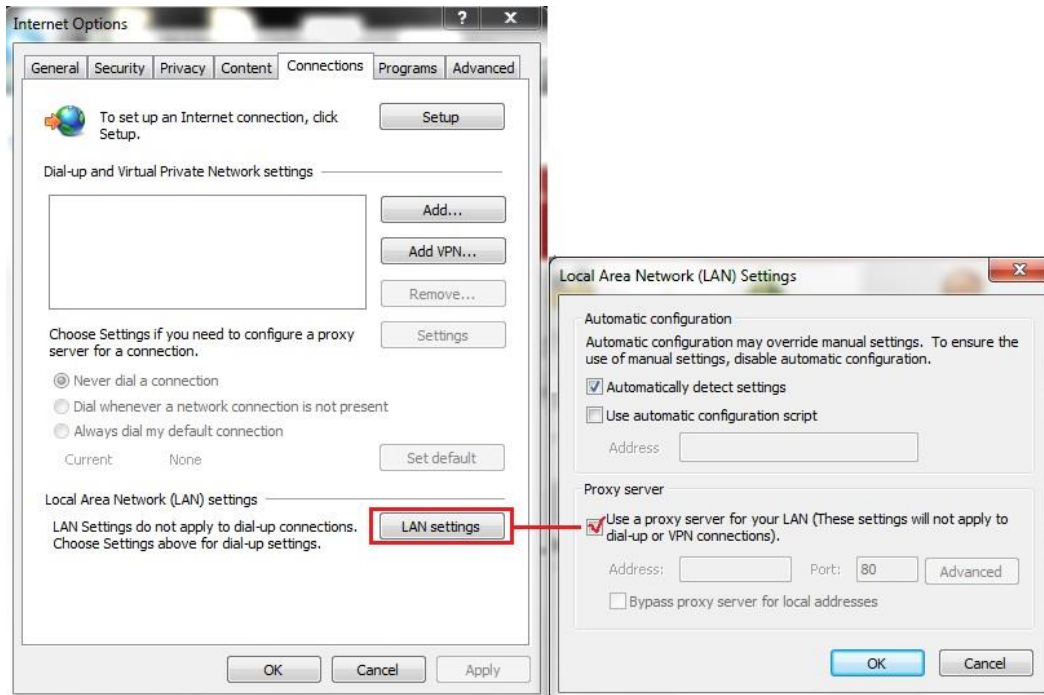
Proxy Server

Enable Built-in  Disable Built-in  External

Apply

Cancel

- Step 3.** Enable Proxy Server Settings in Internet Options on Client Stations.



By enabling the built-in Proxy Server, all traffic is forwarded to the local Proxy Server on the controller.

### Using an External Proxy Server

To specify an External Proxy Server, choose the option “External” and fill in the appropriate IP address of the Proxy Server and the utilized port.

Follow the following steps to complete the proxy configuration:

- Step 1.** Log in to the system by using the *admin* account.
- Step 2.** **Network >> Proxy Server >> Web Proxy Settings.** Select **External** for Proxy Server. Add the IP address and port number of the Proxy server into External Proxy Servers setting. Click **Apply** to save the settings.



- Step 3.** 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.

## 6) Local DNS Record

The administrator could statically assign a Domain Name to IP mappings for all clients connected to the EWS 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  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	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>

## 7) Dynamic Routing

The function supports three dynamic routing protocols: RIP, OSPF and IS-IS.

- **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.



## IS-IS

Function

Enable  Disable

Setup Table

Configuration

Net ID

Router Level

Level 1

Interface	Status	Circuit Type
WAN1	Enabled	Level 1
WAN2	Disabled	Level 1
Default	Enabled	Level 1
SZ1	Disabled	Level 1
SZ2	Disabled	Level 1
SZ3	Disabled	Level 1
SZ4	Disabled	Level 1
SZ5	Disabled	Level 1
SZ6	Disabled	Level 1
SZ7	Disabled	Level 1
SZ8	Disabled	Level 1

- **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.

## OSPF

Function  Enable  Disable

Setup Table

Interface	Status	Area	Stub	Authentication
WAN1	Enabled	<input type="text"/>	<input type="checkbox"/>	None ▾
WAN2	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
Default	Enabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ1	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ2	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ3	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ4	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ5	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ6	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ7	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ8	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾

Advertise as default gateway  
 Advertise Global Policy Route  
 Re-distribute RIP

- 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.
- Redistribute RIP: Check this option to enable using OSPF to distribute routing information acquired via RIP.

- **OSPF v3 Configuration: IPv6 dynamic routing configuration**

## OSPF v3

Function  Enable  Disable

Setup Table

Interface	Status	Area
WAN	Disabled	<input type="text"/>
Default	Enabled	<input type="text"/>
SZ1	Disabled	<input type="text"/>
SZ2	Disabled	<input type="text"/>
SZ3	Disabled	<input type="text"/>
SZ4	Disabled	<input type="text"/>
SZ5	Disabled	<input type="text"/>
SZ6	Disabled	<input type="text"/>
SZ7	Disabled	<input type="text"/>
SZ8	Disabled	<input type="text"/>

Advertise Global Policy Route

- **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.

## RIP

Function  Enable  Disable

Setup Table

	Status	Passive	Version	Authentication
WAN1	Enabled	<input type="checkbox"/>	Both ▾	None ▾
WAN2	Disabled	<input type="checkbox"/>	Both ▾	None ▾
Default	Enabled	<input type="checkbox"/>	Both ▾	None ▾
SZ1	Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ2	Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ3	Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ4	Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ5	Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ6	Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ7	Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ8	Disabled	<input type="checkbox"/>	Both ▾	None ▾

Advertise as default gateway

Advertise Global Policy Route

Re-distribute OSPF

RIP Timer

Update timer:  \* (30~600 seconds)

Timeout timer:  \* (30~600 seconds)

Garbage collect timer:  \* (30~600 seconds)

- **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.
- **Redistribute 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.
  - ◆ **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.
  - ◆ **Garbage Collection Timer:** Specify the time in seconds before erasing invalid route from the routing table.

## 8) DDNS

Before activating this function, you must have your Dynamic DNS hostname registered with a Dynamic DNS provider. EWS 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 EWS 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:** Enable or disable this function.
- **Provider:** 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.

## 9) 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:** Configure this gateway to **Master** or **Slave**. In **Master** mode, you may also need to input the **Slave IP** and **Secret Key**. In **Slave** Mode, input **Master IP** and **Key**.
  - **Master Node:** While configure Master Node, one master could active up to 15 Slave node setting.

**Cross Gateway Roaming**

Mode  Disable  Master Mode  Slave Mode

Status

Slave Nodes Setting	No.	Active	Remote IP Address*	Secret Key*	Remark
	1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

- **Slave Node:** While configuring the Slave Node, enter its master node setting.

**Cross Gateway Roaming**

Mode  Disable  Master Mode  Slave Mode

Status

Master Node Setting

Remote IP Address \*

Secret Key \*

Remark

## F. Utilities

**Utilities:** This section provides functions for modifying accounts, Backup/Restore system, Firmware upgrade, Restart service, Network utilities, and Certificate.

### 1) Administrator Account

This can be used to create, to edit, to remove, and to check administrator account.

The login account for the administrator is "admin". The admin password of the system can be changed here by clicking the admin Name and entering the original password and new password. The default admin password of the system is "admin". The Elementary School's Name field may also be entered for security purposes in case the admin username or password has been forgotten. Noted that Email and Elementary School's Name should be both empty or both filled.

Generate Admin Account

Admin Username	<input type="text"/>	*
Password	<input type="password"/>	*
Confirm Password	<input type="password"/>	*
Email	<input type="text"/>	<input type="button" value="Assign SMTP server"/>
Elementary school's name	<input type="text"/>	

The elementary school's name will identify you, if you forgot your password. Note that, the elementary school's name can not be changed, after apply.

Allocate account to

It also allows the administrator to create other administrator accounts with different permission.

Administrator Accounts

<input type="checkbox"/>	Name	IP Address	MAC Address	Group	Status
<input type="checkbox"/>	admin	10.28.128.188	0A:1F:D4:00:DA:D1	Super Group	Current Page: /Utilities/MlaUser.shtml
<input type="checkbox"/>	admin	10.30.42.168	0A:1F:D4:00:DA:D1	Super Group	Current Page: /SystemConfiguration/ServiceZoneConf.shtml?sz_id=0

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

## General Settings

<b>Password Complexity</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Min Password Length <input type="text" value="2"/> * (2~20)
	Min Password Category <input type="text" value="2"/> * (2~4)
<b>Limit Login Attempts</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Block access after <input type="text" value="5"/> * tries
<b>Password Expiration</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Password expires <input type="text" value="90"/> * day(s) after creation
<b>Password Limits</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Users to choose passwords different from their past <input type="text" value="6"/> * passwords
<b>Access Permission</b>	<input type="button" value="Configure"/>

- **Password Complexity** enables the admin to limit how the passwords the sub-admins use should be formed.

Min password Length sets a limit on the minimum length of a password string;

Min password Category allows 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 (if enabled):** enter 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 (if enabled):** this is a function for admins to decide 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 (if enabled):** it is 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.
- **Sub-admin creation**

## Generate Admin Account

Admin Username	<input type="text"/>	*
Password	<input type="password"/>	*
Confirm Password	<input type="password"/>	*
Email	<input type="text"/>	*
Elementary school's name	<input type="text"/>	*
Allocate account to	<input type="text" value="Super Group"/>	▼

Assign SMTP server

The elementary school's name will identify you, if you forgot your password. Note that, the elementary school's name can not be changed, after apply.

Go to the **Generate** table 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.

Send Password

Username

Elementary school's name

(There are 6 categories a sub-admin can fall into – Super Group, Manager, Operator, On-Demand 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.) Create an account to the list by pressing the Apply button after finishing the settings.



Select Group

Note: Left checkbox means Read-Write, right checkbox means Read-Only.

### Permission Settings

Service Zone	<input type="checkbox"/> <input type="checkbox"/> Select All <input type="checkbox"/> <input type="checkbox"/> Default <input type="checkbox"/> <input type="checkbox"/> SZ1 <input type="checkbox"/> <input type="checkbox"/> SZ2 <input type="checkbox"/> <input type="checkbox"/> SZ3 <input type="checkbox"/> <input type="checkbox"/> SZ4 <input type="checkbox"/> <input type="checkbox"/> SZ5 <input type="checkbox"/> <input type="checkbox"/> SZ6 <input type="checkbox"/> <input type="checkbox"/> SZ7 <input type="checkbox"/> <input type="checkbox"/> SZ8
Map	<input type="checkbox"/> <input type="checkbox"/> Select All <input type="checkbox"/> <input type="checkbox"/> Overview <input type="checkbox"/> <input type="checkbox"/> EL
AP Management	<input type="checkbox"/> <input type="checkbox"/> Select All <input type="checkbox"/> <input type="checkbox"/> Local Area AP Management <input type="checkbox"/> <input type="checkbox"/> Wide Area AP Management

- **The admin list** serves as a list for admins to track the dynamics of each management accounts, i.e., the number of the online admins and the state of each sub-admin.

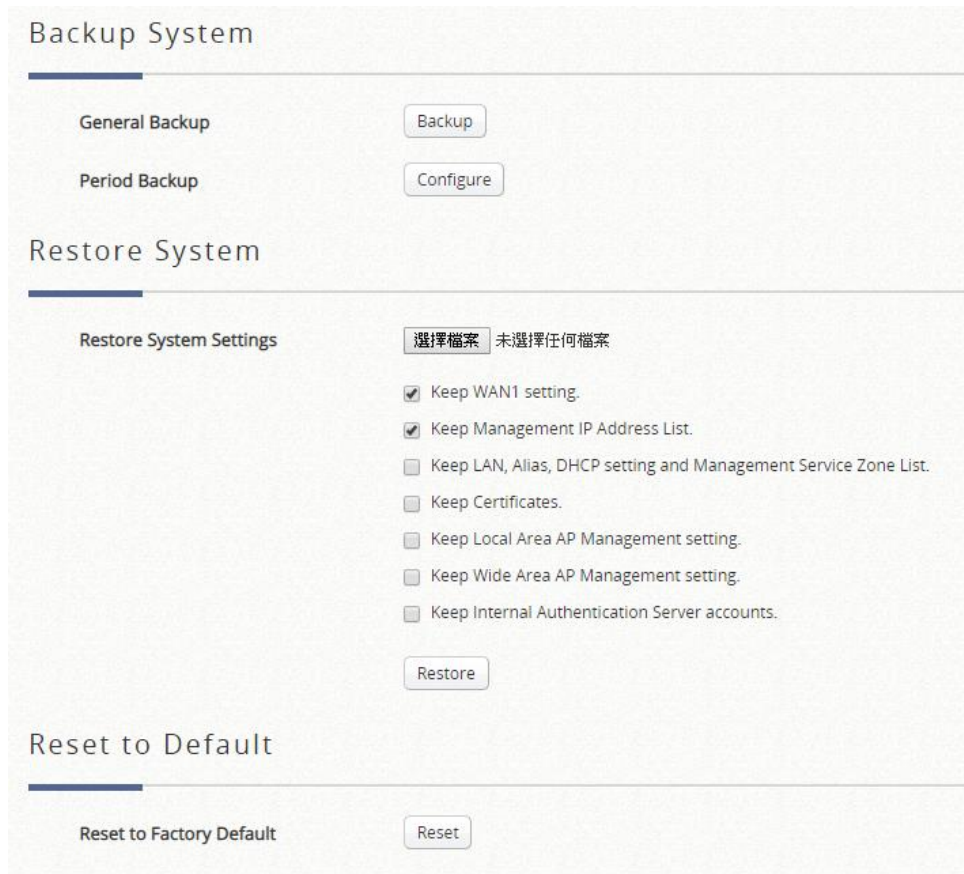
### Administrator Accounts

<input type="checkbox"/>	Name	IP Address	MAC Address	Group	Status
<input type="checkbox"/>	admin	10.28.128.188	0A:1F:D4:00:DA:D1	Super Group	Current Page: <a href="#">/Utilities/MlaUser.shtml</a>
<input type="checkbox"/>	admin	10.30.42.168	0A:1F:D4:00:DA:D1	Super Group	Current Page: <a href="#">/SystemConfiguration/ServiceZoneConf.shtml?sz_id=0</a>

Please note that only the created sub-admins can be deleted. Check the boxes to 'Lock' or 'Unlock' to forbid certain sub-admins to access the management page. Besides, admin can also click the hyperlinks in the 'name' column to edit admins'/ sub-admins' related settings.

## 2) Backup & Restore

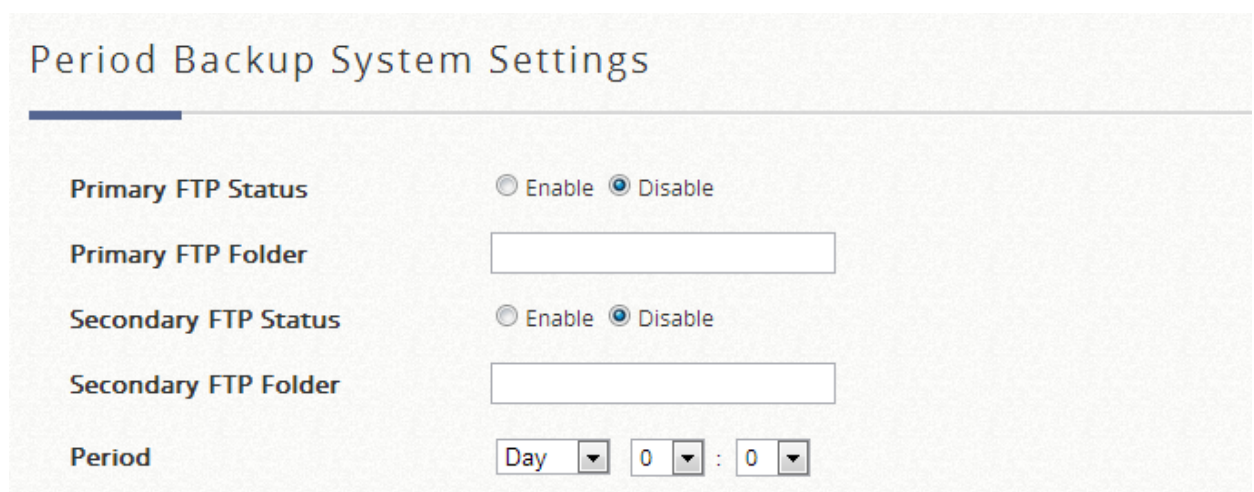
This is used to backup and restore system settings. System factory default can also be restored.



Click the **Backup** button under General Backup to save the current system configurations to a backup file on a local disk of the management console. A backup file will keep the current system settings as well as the local user accounts.

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.

Backup can be done periodically over FTP. Enable this feature by clicking on the **Configure** button under Period Backup.







- **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. The option of “Keep WAN1 setting and Management IP Address List” can be selected to retain WAN1 setting for remote access.
- **Reset to Factory Default:** Click **Reset** to load the factory default settings of the controller.

### 3) Certificates

On this tab, administrators have the ability to manage the system certificate, create Root CA, sign certificates from Root CA, and upload certificate. 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.

Certificate Management

Cert Name	Common Name	Used by
System Certificate 		
Default Certificate	CN=mknhhi.example.com	WEB Server, Built-in RADIUS, CAPWAP
Internal Root CA 		
Internal Root CA	N/A	
Internally Issued Certificate 		
N/A	N/A	
Trusted Certificate Authorities (CA) 		
N/A	N/A	

- **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. Click “Regenerate” button, a new default certificate with a unique CN will be created. To view details of the certificate, click the corresponding "View" button. Click "Get CERT" and "Get Key" to download the certificate and public key onto your local disk.

## System Certificate

Cert Name	Common Name	Operation
Factory Default Certificate		
Factory Default Certificate	CN=gateway.example.com	<a href="#">View</a> <a href="#">Regenerate</a>
Internally Issued Certificate		
N/A	N/A	<a href="#">View</a> <a href="#">Delete</a>
Uploaded Certificate		
N/A	N/A	<a href="#">View</a> <a href="#">Delete</a> <a href="#">Upload Intermediate/Root CA</a> <a href="#">Verify</a>

## Upload System Certificate

Certificate	<a href="#">選擇檔案</a> 未選擇任何檔案
Private Key	<a href="#">選擇檔案</a> 未選擇任何檔案
Intermediate CA	<a href="#">選擇檔案</a> 未選擇任何檔案

[Upload](#)

### Internal Root CA

The administrator can 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.

## Internal Root CA

Cert Name	Common Name	Operation
Internal Root CA		
N/A	N/A	<a href="#">View</a> <a href="#">Delete</a>

## Generate Root CA

Common Name	<input type="text"/>
Email Address	<input type="text"/>
Country Name	<input type="text"/>
State or Province Name	<input type="text"/>
Locality Name	<input type="text"/>
Organization Name	<input type="text"/>
Organization Unit Name	<input type="text"/>
Key Type	<input type="text" value="RSA"/>
Key Length	<input type="text" value="512"/>

[Generate Certificate](#)

## Upload Root CA

Certificate	<input type="text"/>	<a href="#">Browse...</a>
Private Key	<input type="text"/>	<a href="#">Browse...</a>

[Upload Files](#)

A root CA certificate may also be uploaded with a matching Private Key.

- **Internally Issued Certificates**

When an Internal Root CA needs to be created, Internally Issued Certificates can be signed.

**Certificate Information**

Cert Name	Common Name	Operation
Internally Issued Certificate		
N/A	N/A	<a href="#">View</a> <a href="#">Delete</a>

**Use Internal Root CA to generate certificate**

**You must Create Root CA First.**

The generated certificate will be listed and the certificate/key pair can be downloaded with **Get Cert**, **Get key** in **View**.

- **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 and upload a trusted CA certificate from your local disk into the System.

**Trusted Certificate Authorities (CA)**

Cert Name	Common Name	Operation
Certificate Authorities (CA)		
N/A	N/A	<a href="#">View</a> <a href="#">Delete</a>

**Upload Trusted CAs**

Certificate  [Browse...](#)

[Upload Files](#)

## **4) Network Utilities**

Some network utilities such as web-based Ping, Trace Route, and ARP table are supported on the system.

## Network Utilities

Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Sniff <input type="radio"/> IP Discovery		
Ping	<input type="text" value="IP/Domain Name"/>	<input type="button" value="Ping"/>	
Trace Route	<input type="text" value="IP/Domain Name"/>	<input type="button" value="Start"/>	<input type="button" value="Stop"/>
ARPing	<input type="text" value="IP/Domain Name"/>	Interface	<input type="button" value="WAN1"/> <input type="button" value="ARPing"/>
VLAN ID	<input type="text" value="IP/MAC"/>	<input type="button" value="Find"/>	
ARP Table	<input type="button" value="Show"/>		
Status			
Result	<div style="border: 1px solid #ccc; height: 40px;"></div>		

Item	Description
IPv4	<ul style="list-style-type: none"> <li>▪ <b>Ping:</b> It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.</li> <li>▪ <b>Trace Route:</b> It allows administrator to recover the real path of packets from the gateway to a destination using IP address or Host domain name.</li> <li>▪ <b>ARPing:</b> Allows the administrator to send ARP request for a specific IP address or domain name.</li> <li>▪ <b>ARP Table:</b> It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).</li> </ul>
IPv6	<ul style="list-style-type: none"> <li>▪ <b>Ping:</b> It allows administrator to detect a device using IPv6 address or Host domain name to see if it is alive or not.</li> <li>▪ <b>Trace Route 6:</b> It allows administrator to recover the real path of packets from the gateway to a destination using IPv6 address or Host domain name.</li> <li>▪ <b>Neighbor Discovery:</b> The administrator can use this feature to learn about IPv6 Neighbor nodes that are on the same IP segment or domain name.</li> <li>▪ <b>Neighbor Cache:</b> 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.</li> </ul>
Sniff	<p>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 <b>Expression</b> field.</p>

<b>IP Discovery</b>	With this feature, controller can discover the IP address of the APs connected within the same Layer 2 network. Administrator can also modify the IP configuration for the discovered APs.
<b>Status</b>	When the administrator is executing any Network Utilities features, the status of the operation is displayed here.
<b>Result</b>	The operation result is displayed here.

## 5) Restart

Click **Restart** button to restart the system. Please wait for the blinking timer to finish before accessing the system web management interface again.

## 6) System Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click **Browse** to search for the firmware file and click **Apply** for the firmware upgrade. It may 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.

To upgrade the system firmware, click **Browse** button to choose the new firmware file and then click **Apply** button to execute the process. There will be a prompt confirmation message appearing to notify the administrator to restart the system after successful firmware upgrade. (\*\* Firmware upgrade may take up to several minutes, please wait for the confirmation message)

The system must be rebooted before resetting to factory defaults after firmware upgrade.

**Note:** For better maintenance, we strongly recommend you backup system settings before upgrading firmware.

## System Firmware Upgrade

Current Version	3.00.00
Upload New Firmware	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Apply"/>
Upgrade Firmware Via FTP	Anonymous <input checked="" type="radio"/> Yes <input type="radio"/> No
IP Address	<input type="text"/> Port <input type="text"/>
File Name	<input type="text"/> <input type="button" value="Apply"/>

## G. Status

**Status:** Provides information for System Status, Interface Status, Hardware Status, Routing Table, Online Users, Session List, User Logs and set up Notification Configuration.

### 1) System Summary

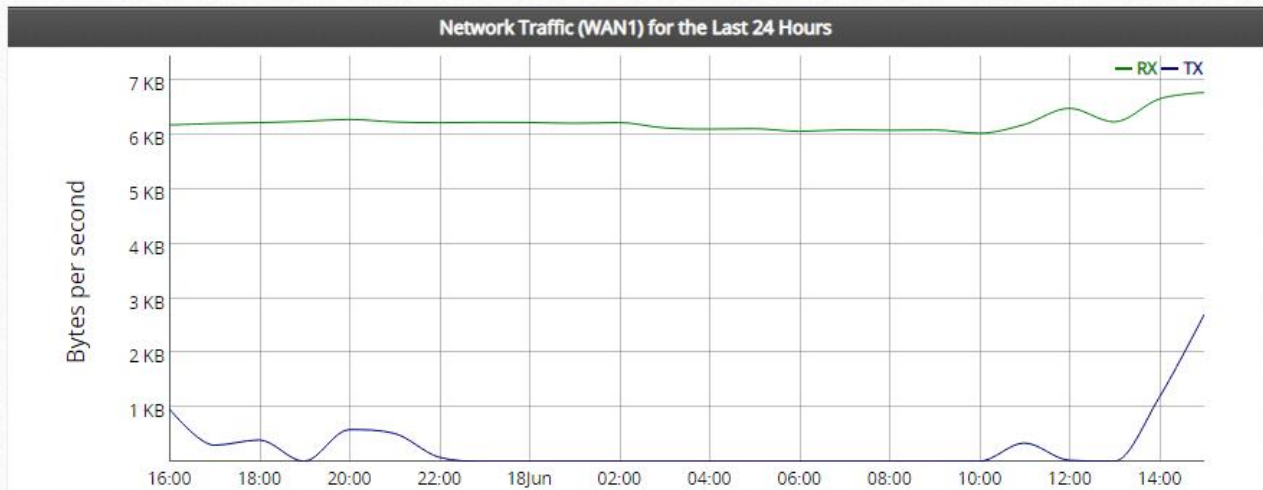
A display of current settings on the system.

An overview of the system is provided here for the administrator's reference.



# System Summary

[See Reports](#)



General			
System Name	EWS101	Firmware Version	3.45.0000
System Up Time	14 days, 23 hours, 27 min	Build Number	1.36-1.9737
System Time	2019/06/18 15:20:58 +0800	NTP Server	ntps1.pads.ufrj.br
Preferred DNS Server	8.8.8.8	Alternate DNS Server	N/A
Proxy Server	Disabled	APM Version	3.45.0000
SNMP	Enabled	Warning of Internet Disconnection	Disabled
Idle Timeout	10min	Traffic Direction for Idle Timeout	Uplink & Downlink
Num of Current Users	0	Num of Maximum Users	400

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	

General			
<b>System Name</b>	The system name. The default name is the model number.	<b>Firmware Version</b>	The present firmware version of EWS CONTROLLER
<b>System Up Time</b>	Displays for how long the system has operated.	<b>Build Number</b>	The current build number.
<b>System Time</b>	The local time is shown as the system time.	<b>NTP Server</b>	The network time server that the system is set to align.
<b>Preferred DNS Server</b>	IP address of the preferred DNS Server.	<b>Alternate DNS Server</b>	IP address of the alternate DNS Server.
<b>Proxy Server</b>	Enabled/Disabled/External	<b>APM Version</b>	The version of AP Management

			Module.
<b>WAN Failover</b>	Enabled/Disabled	<b>Load Balancing</b>	Enabled/Disabled
<b>SNMP</b>	Enabled/Disabled	<b>Warning of Internet Disconnection</b>	Enabled/Disabled
<b>Idle Timeout</b>	The minutes allowed for the users to be inactive before their account expires automatically.	<b>Traffic Direction for Idle Timeout</b>	Uplink/Uplink & Downlink The user's activity inspection may be checked by uplink traffic only or both direction.
<b>Num of Current Users</b>	The number of current online users.	<b>Num of Maximum Users</b>	The number of maximum online users.
<b>Report</b>			
<b>Syslog server 1</b>			The IP address and port number of the external Syslog Server. <b>N/A</b> means that it is not configured.
<b>Syslog server 2</b>			The IP address and port number of the external Syslog Server. <b>N/A</b> means that it is not configured.
<b>User Logs</b>	<b>Retained Days</b>		The maximum number of days for the system to retain the users' information.
	<b>Receiver Email Address (es)</b>		The email address to which the traffic history or user's traffic history information will be sent.

Click "See Reports" for the following available reports, sorted by interface: Network Traffic, CPU Load, CPU Temperature, Memory Usage, Storage Usage, Online Users, Successful Logins, Sessions, DHCP Leases and DNS Queries. The reports can also be customized to your preference by selecting the Time range and Interval. These reports can be sent via email, syslog, or FTP.

## 2) Interface

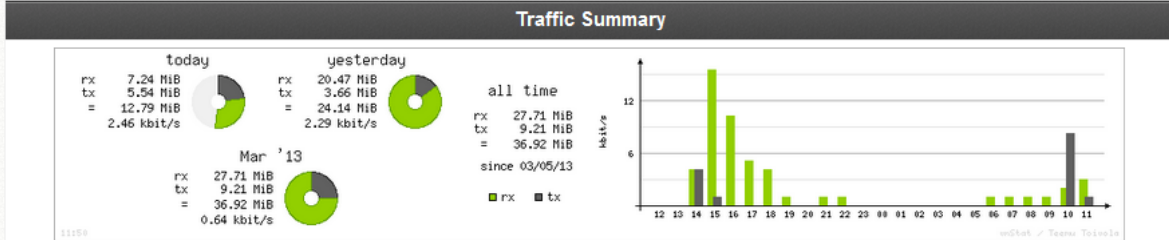
A display of the current settings of all network interfaces. Select Interface from the drop-down menu.

Each service zone represents a virtual system; therefore, the information of the system's network interface is grouped by service zone.

Select Interface **WAN1** ▾

## Network Interface

WAN1			
Mode	STATIC	IP Address	10.29.42.101
MAC Address	00:10:F3:23:D3:54	Subnet Mask	255.255.0.0
IPv6 Address	N/A	IPv6 Prefix	N/A
Auto-Negotiation	On	Speed / Duplex	100Mb/s Full



### Daily Traffic

day	rx	tx	total	avg. rate
03/05/13	20.47 MiB	3.66 MiB	24.14 MiB	2.29 kbit/s
03/06/13	7.24 MiB	5.54 MiB	12.79 MiB	2.46 kbit/s
estimated	14 MiB	10 MiB	24 MiB	

### Monthly Traffic

month	rx	tx	total	avg. rate
Mar '13	27.71 MiB	9.21 MiB	36.92 MiB	0.64 kbit/s
estimated	152 MiB	50 MiB	202 MiB	

### Top 10 Traffic

#	day	rx	tx	total	avg. rate
1	03/05/13	20.47 MiB	3.66 MiB	24.14 MiB	2.29 kbit/s

Item	Description	
<b>Interface (WAN1/WAN2)</b>	<b>Mode</b>	Operating mode of this interface.
	<b>MAC Address</b>	The MAC address of the WAN port.
	<b>IP Address</b>	The IPv4 address of the WAN port.
	<b>Subnet Mask</b>	The Subnet Mask of the WAN port.
	<b>IPv6 Address</b>	The IPv6 address of the selected interface
	<b>IPv6 Prefix</b>	The prefix of IPv6 address
	<b>Auto-Negotiation</b>	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.
	<b>Speed/Duplex</b>	Displays current speed and duplex of the selected interface.
<b>Traffic Summary</b>	Displays daily, monthly and all time graphical summary of the TX and Rx rate for this interface.	
<b>Daily Traffic</b>	Displays traffic information of the day in a table.	
<b>Monthly Traffic</b>	Displays traffic information of the in a table.	

<b>Top 10 Traffic</b>		Shows the top 10 traffic of the day records.
<b>Service Zone – Default, SZ1~SZ8</b>	<b>Mode</b>	The operation mode of the SZ.
	<b>MAC Address</b>	The MAC address of the SZ.
	<b>IP Address</b>	The IP address of the SZ.
	<b>Subnet Mask</b>	The Subnet Mask of the SZ.
	<b>IPv6 Address</b>	The IPv6 address of the SZ
<b>Service Zone – DHCP Scope (Default, SZ1~SZ8)</b>	<b>Status</b>	Enable/disable stands for status of the DHCP server in Default Service Zone
	<b>WINS IP Address</b>	The WINS server IP on DHCP server. <b>N/A</b> means that it is not configured.
	<b>Start IP Address</b>	The start IP address of the DHCP IP range.
	<b>End IP address</b>	The end IP address of the DHCP IP range.
	<b>Lease Time</b>	Minutes of the lease time of the IP address.

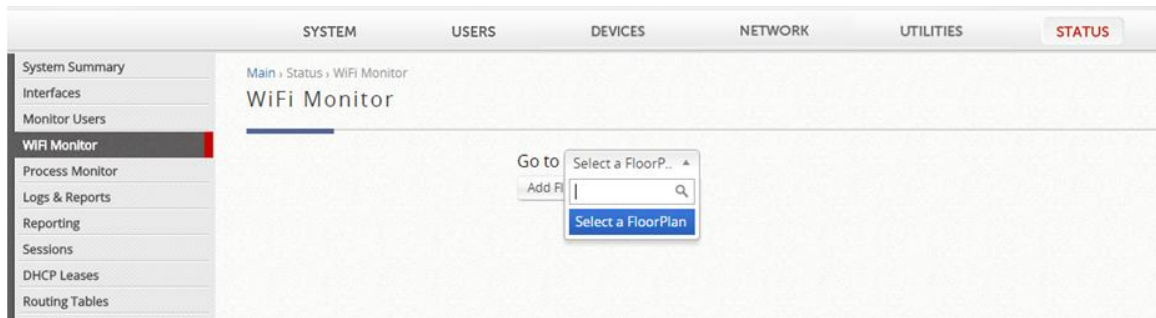
### 3) Monitor Users

All online users/devices will be listed here. The administrator can terminate any user session by clicking the **Kick Out** button. Non-login users will be listed here as well.

- **Online Users:** Successfully authenticated Local Users.
- **Roaming In User:** Roaming Users authenticated at roaming peer controllers (for Cross Gateway Roaming).
- **Roaming Out User:** On-Demand users authenticated at external controllers via RADIUS protocol.
- **Non-Login Local User:** Obtained IP address but has not yet authenticated Local Users.
- **MAC Login Devices:** Disconnected MAC authenticated devices need not be re-plugged physically, and can be MAC authenticated on the MAC Login Devices List
- **Authenticated Users:** The authentication-completed users (via 802.1X, MAC authentication, PPP authentication, or CoA login) whose IP information is unknown to the controller.
- **Smart Login Users:** The On-Demand users within the Smart Login period. The users in this list will be login automatically when accessing the network next time.

### 4) WiFi Monitor

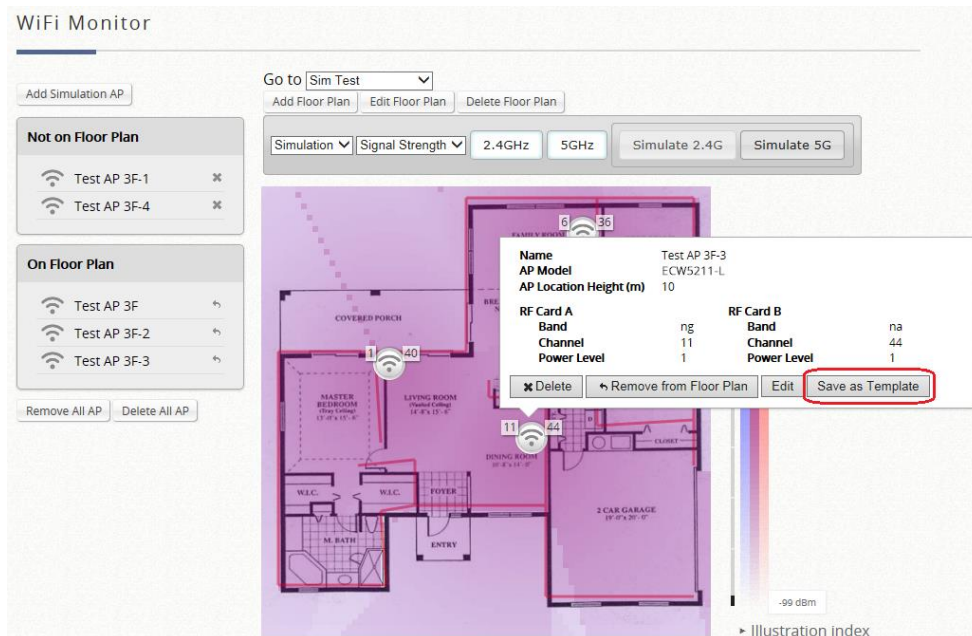
To run the WiFi Monitor, first create a floor plan to start the managed AP monitoring or the simulation and then a 2-D floor plan needs to be uploaded to the EWS Controller. Click the **Add Floor Plan** button to add a floor plan.



### Add Floor Plan

Floor Plan Type	Local ▼	
Floor Plan Name	<input type="text"/>	*
Floor Plan (.jpg)	<input type="button" value="選擇檔案"/> 未選擇任何檔案	* (under 256k, JPG)
Wall (.xml / .osm)	<input type="button" value="選擇檔案"/> 未選擇任何檔案	*
Map Width (m)	<input type="text"/>	* (1~200)
Map Length (m)	<input type="text"/>	* (1~200)
Country Code	EUROPE ▼	
Height of Receiving Device (m)	1 <input type="text"/>	* (1~10)

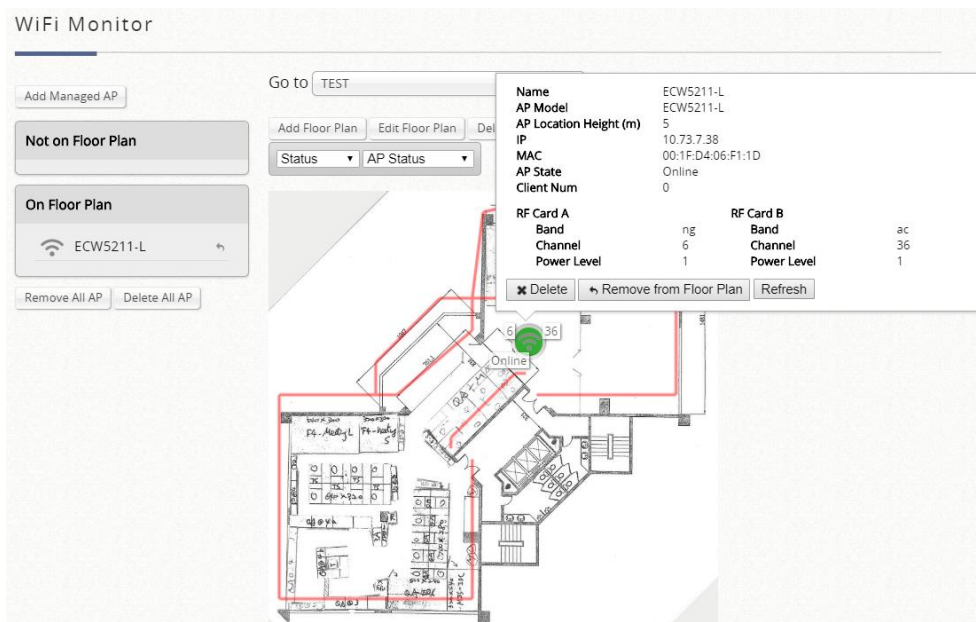
- **Floor Plan Type:** Type of the floor plan. Select “Wide” for monitoring managed APs from Wide Area AP Management. Select “Virtual” for AP simulation.
- **Floor Plan Name:** Self-defined name for Administrator’s reference.
- **Floor Plan:** Select file for floor plan (.jpg format).
- **Wall:** Select file for wall (.xml or .osm 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.



## Virtual Type

Simulation can be done by clicking the **Simulate 2.4G** or the **Simulate 5G** button. If the results are satisfactory, the settings on each AP may be saved as a template to be used to apply to APs in AP Management.

- **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.



## Local & Wide Type

- **AP Status:** Visualize the online/offline status, CPU usage (Wide type only), and memory usage (Wide type only).

- **Statistics:** Show device density, and average traffic rate (Wide type only) for each AP.
- **Coverage:** Similar to Virtual type, showing coverage of each AP in different ways.

## 5) Process Monitor

The Process Monitor is a network utility that shows the active status of process daemons on the gateway. Administrators can choose to **Enable** or **Disable** the Process Monitor by clicking the radio button.

Process Monitor

Process Monitor		
Enable Monitor	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Process Name	Status	ID
apache		11140
proxy		10069
proxy_logout		10085
proxy_fake		10098
cipgwsrv		9271
cipgwlnsrv		9272
dnsmasq		9435
dnsmasq_fake		9176
radiusd	N/A	
snmpd	N/A	
cipgrd	N/A	

## 6) Logs & Reports

This page is used to check the traffic history of the system which includes Logs such as CAPWAP Log, Configuration Change Log, Local Web Log, RADIUS Server Log, System Log and UAMD Log. User logs are summarized in User Events, and the system also keeps a cumulated record of the traffic data generated by each user in the latest calendar month. 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:** The system keeps a cumulated record of the traffic data generated by each Local user in the latest 2 calendar months. Each line in a monthly network usage of local user record consists of 6 fields, System Name, Connection Time Usage, Packets In, Bytes In, Packets Out and Bytes Out.
- **Local Web Log:** This page shows which of the web pages have been accessed on the Controllers built-in web server.

- **On-Demand Billing Report:** This page is 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.

The "Download" button downloads the displayed User Events into a comma separated .txt file, which can be imported into cells (MS Excel).

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.**



- **Alarm:** Error or warning messages for the selected items. An alarm remains on the alarm list until the fault is resolved.
- **Management Events:** Management related logs for the selected items.

## 7) Reporting

EWS CONTROLLER can automatically send various kinds of user and/or system related reports to configured E-mail addresses, SYSLOG Servers, or FTP Server.

Notification Settings Page:

This configuration page allows the selection of log types to send, either to preconfigured E-mail, SYSLOG Servers or FTP Server based on the chosen time Interval.

### ▪ **Sending Logs to E-mail**

The following log types can be sent to E-mail addresses configured in “SMTP Settings”: Monitor IP Report, Users Log, On-Demand Users Log, Trial Users Log, Roaming Out Users Log, Roaming In Users Log, External User Log, Session Log, Firewall Log, Local Area AP Status Change, On-Demand User Billing Report, Wide Area AP Status Change, and Configuration Change Log. The numbers 1 to 5 represent the corresponding E-mail addresses configured in “SMTP Settings”. Click the desired E-mail address profile (1 ~ 5) and select the time interval for sending a report or log.

## Notification Settings

	Receiver E-mail Address(es)						SYSLOG	Primary FTP	Interval	
	1	2	3	4	5	Detail / Test				
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	N/A	N/A	1 Hour ▼	
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
One Time Password Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	N/A	1 Hour ▼	
Online User Limit Notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	N/A	N/A	N/A	
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	N/A	N/A	2 Mins ▼	
On-Demand User Billing Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	N/A	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	N/A	N/A	2 Mins ▼	
Wide Area AP Report										
<input type="checkbox"/> CPU Loading										<input type="checkbox"/> Daily Report
<input type="checkbox"/> Memory Usage										<input type="checkbox"/> Weekly Report
<input type="checkbox"/> Network Delay										<input type="checkbox"/> Monthly Report
<input type="checkbox"/> Network Traffic										
<input type="checkbox"/> Associated Clients										
<input type="checkbox"/> VAP Traffic										
<input type="checkbox"/> WDS Traffic										
Guest Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Social Account Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Guest/Social Account Info Full	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	N/A	N/A	2 Mins ▼	
Local HTTP Web Log							<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
HTTP Web Log							<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	
Configuration Change Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> <input type="radio"/>	N/A	<input type="checkbox"/> <input type="checkbox"/>	1 Hour ▼	

- **Detail:** Clicking this radio button allows the configuration of the E-mail subject for the corresponding log.
- **Send:** Clicking this radio button sends a test log to the selected E-mail address.

### ■ Sending Logs to SYSLOG

The following log types can be sent to external SYSLOG servers configured in “SYSLOG Settings”: Local Users Log, On-Demand Users Log, Trial Users Log, Roaming Out Users Log, Roaming In Users Log, External User Log, Session Log, Firewall Log, Local HTTP Web Log, HTTP Web Log and DHCP Server Log. Click the desired log type and select the time interval for sending log.

## Notification Settings

	Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval		
	1	2	3	4	5				Detail / Test	
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼	
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
One Time Password Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼	
Online User Limit Notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A	
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼	
On-Demand User Billing Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/>	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼	
Wide Area AP Report							N/A	<input type="checkbox"/>	<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report	
							N/A			
Guest Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Social Account Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Guest/Social Account Info Full	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼	
Local HTTP Web Log							N/A	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
HTTP Web Log							N/A	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Configuration Change Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/>	1 Hour ▼	
DHCP Server Log							N/A	<input type="checkbox"/>	N/A	N/A

- **Detail:** Clicking this button allows the configuration of SYSLOG attributes such as Tag, Severity and Facility which will be assigned to the corresponding log to meet the filtering requirements on the SYSLOG Server.

**Note:** The “System Log” option needs to be enabled under SYSLOG Settings in order to send the selected logs to the configured SYSLOG Servers.

- **Sending Logs to FTP**

The following log types can be sent to external FTP servers configured in “FTP Settings”: Local Users Log, On-Demand Users Log, Trial Users Log, Roaming Out Users Log, Roaming In Users Log, External User Log, Session Log, On-Demand Billing Report Log, Wide Area AP Report, Local HTTP Web Log, HTTP Web Log, Configuration Change Log, DHCP Lease Log, System Report and Traffic Report. Click the desired log type and select the time interval for sending log.

## Notification Settings

	Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval									
	1	2	3	4	5				Detail / Test								
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼								
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
One Time Password Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼								
Online User Limit Notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A								
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼								
On-Demand User Billing Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/>	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report								
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼								
Wide Area AP Report	N/A					N/A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Delay <input type="checkbox"/> Network Traffic <input type="checkbox"/> Associated Clients <input type="checkbox"/> VAP Traffic <input type="checkbox"/> WDS Traffic	<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report							
Guest Information									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report
Social Account Information									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report
Guest/Social Account Info Full									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼
Local HTTP Web Log									N/A					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
HTTP Web Log									N/A					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Configuration Change Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/>	1 Hour ▼								
DHCP Server Log	N/A					<input type="checkbox"/>	N/A	N/A	N/A								
DHCP Lease Log	N/A					N/A	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼								
System Report	N/A					N/A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Storage Usage <input type="checkbox"/> Network Traffic <input type="checkbox"/> Online User <input type="checkbox"/> Successful Login <input type="checkbox"/> Session <input type="checkbox"/> DHCP Lease <input type="checkbox"/> DNS Query	<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report							
Traffic Report (Text)									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	<input type="checkbox"/> Service Zone <input type="checkbox"/> VLAN

**Detail:** Clicking this button allows the specification of the FTP server folder where the logs sent will be stored on the FTP server.

**Note:** 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 Settings Page:

The screenshot shows the 'FTP Settings' page. It is divided into two main sections: 'Primary FTP Server' and 'Secondary FTP Server'. Each section contains the following fields and controls:

- Primary FTP Server:**
  - IP Address: [Text Input]
  - Port: [Text Input]
  - Login:  Anonymous  Normal
  - Username: [Text Input]
  - Password: [Text Input]
  - Send Test File: [Send Button]
- Secondary FTP Server:**
  - IP Address: [Text Input]
  - Port: [Text Input]
  - Login:  Anonymous  Normal
  - Send Test File: [Send Button]

- **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.

- **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.

The screenshot shows the 'SMTP Settings' page. It contains the following fields and controls:

- SMTP Server:**
  - Server Address: [Text Input]
  - Port: [Text Input]
- Encryption:**  Disable  TLS  SSL
- Authentication:** [None] (Dropdown)
- Sender E-mail Address:** [Text Input]
- Receiver E-mail Address:**
  - Receiver 1: [Text Input]
  - Receiver 2: [Text Input]
  - Receiver 3: [Text Input]
  - Receiver 4: [Text Input]
  - Receiver 5: [Text Input]
- Send Test E-mail:** [Send Button]

- **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.
  - **SMTP 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**.
    - **NTLMv1** is not currently available for general use.
    - **Plain** and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use a UNIX login and password. Netscape uses **Plain**. Outlook and Outlook express use **Login** as default, although they can be set to use **NTLMv1**.
    - Pegasus uses **CRAM-MD5** or **Login** but which method to be used cannot be configured.
  - **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.
- **SYSLOG Settings:** Allows the configuration of two external SYSLOG servers where selected users logs as well as system logs will be sent to.

SYSLOG settings page:

The screenshot shows the 'SYSLOG Settings' configuration page. At the top, there is a section for 'SYSLOG' with two radio buttons: 'Enabled' (which is selected) and 'Disabled'. Below this, there are two sections for 'SYSLOG Server', labeled 'Server 1' and 'Server 2'. Each server section contains two input fields: 'IP Address' and 'Port'. At the bottom of the page, there is a 'Severity Level' dropdown menu with 'emergency' selected.

- **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.
  - **Severity Level:** The logs more severe than this level will be sent out to the external SYSLOG server.
- **Alarms & Events Settings:** Configure the items to be monitored as Alarm or Management Events. Alarms are error or warning messages for the selected items to be displayed on the Alarms page and Dashboard. An alarm remains on the alarm list until the fault is resolved. Management Events are logs for the selected items to be displayed on the Management Events page. The latest few events will also be listed in Dashboard.

## Alarms & Events Settings

Alarms are error or warning messages for the selected items to be displayed on the Alarms page and Dashboard. An alarm remains on the alarm list until the fault is resolved.  
 Management Events are logs for the selected items to be displayed on the Management Events page. The latest few events will also be listed in Dashboard.

	Alarms	Management Events	Threshold
AP Online/Offline	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP Backup Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP Restore Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP Firmware Upgrade	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP Template Applying	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP High CPU Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
AP High Memory Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
AP High Airtime Utilization	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
Controller High CPU Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
Controller High Memory Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
Controller High Storage Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼

## 8) 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 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Display Mode: ALL ▼

No	Protocol	Source IP	Port	Destination IP	Port	State	Timeout
1	udp	10.29.129.131	137	10.29.255.255	137	UNREPLIED	3
2	udp	10.29.129.87	138	10.29.255.255	138	UNREPLIED	29
3	udp	10.29.129.87	137	10.29.255.255	137	UNREPLIED	23
4	udp	10.29.129.110	17500	255.255.255.255	17500	UNREPLIED	21
5	tcp	10.28.128.188	55026	10.29.42.101	80	TIME_WAIT	119
6	udp	10.29.129.79	137	10.29.255.255	137	UNREPLIED	27

## 9) DHCP Lease

The DHCP IP lease information can be viewed on this page.



- **Statistics of IP Offered**

Valid lease counts of the **Last 10 Minutes, Hours** and **Days** are shown here. The header 1 ~ 10 are the 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 IP Expired**

IP leased to clients that have expired in the **Last 10 Minutes, Hours** and **Days** are shown here. The header 1 ~ 10 are the 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 indicates the expired count in the last 30 minutes/hours/days and so on.

Refresh
Refresh Disable ▾

### 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

	No.	IP Address	MAC Address	Host Name	VLAN	Lease Expires
<input type="checkbox"/>	1	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	3202	2013/03/07 15:23:00

(Total:1) [First](#) [Previous](#) [Next](#) [Last](#)

Go to Page  (Page:1/1)

Row per Page:

## 10) Routing Table

The routing table lists all IPv6 and IPv4 Route rules. The System Route rules are shown here as well. The Policy Route rule has higher priority than the Global Policy route rule, and the System Route rule has the lowest priority.

Global Policy			
Destination	Subnet Mask	Gateway	Interface
Interface			
Destination	Subnet Mask	Gateway	Interface
169.254.0.0	255.255.0.0	0.0.0.0	Default
192.168.0.0	255.255.0.0	0.0.0.0	Default
10.29.0.0	255.255.0.0	0.0.0.0	WAN1
System			
Destination	Subnet Mask	Gateway	Interface
0.0.0.0	0.0.0.0	10.29.0.1	WAN1
Policy 1			
Destination	Subnet Mask	Gateway	Interface
Policy 2			
Destination	Subnet Mask	Gateway	Interface

Clicking either IPv4 or IPv6 will show the routing rules for each policy or interface.

- **Policy 1~n:** Shows the information of the individual Policy from 1 to n.
- **Global Policy:** Shows the information of the Global Policy.
- **System:** Shows the information of the system administration.
  - **Destination:** The destination IP address of the device.
  - **Subnet Mask:** The Subnet Mask IP address of the port.
  - **Gateway:** The Gateway IP address of the port.
  - **Interface:** The choice of interface network, including **WAN1**, **WAN2**, **Default**, or the named **Service Zones** to be applied for the traffic interface.

P/N: V360000020230303