User Manual

EWS Series
Secure WLAN Controller

Copyright

The content 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 Networks Corporation.

Disclaimer

Edgecore Networks Corporation 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 Networks Corporation. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

FCC CAUTION

EWS5202, EWS5206

The equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Table of Contents

Chapter 1. Introduction 9
1.1 EWS Controller Series 9
1.2 EWS Models 11
1.3 Edgecore Solution Overview 11
1.4 Key Terms & Concepts 13
1.5 Recommended Configuration Sequence 16
1.5.1 Common Settings 16
1.5.2 Advanced Settings and Application 16
Chapter 2. WMI & Setup Wizard 18
2.1. Web Management Interface 18
2.2 Running the Wizard 20
Chapter 3. Basic Network Settings 24
3.1. Network Planning 24
3.2. Uplink (WAN side) Configuration 27
3.2.1 WAN Settings 27
3.2.2. Dual Uplink 28
3.2.3. WAN Port Selection for dual WAN1 / WAN2 models 30
3.2.4. WAN Traffic Control 32
3.2.5. Uplink Detection & Failover 32
3.3. Downlink (LAN side) VLAN option 35
3.3.1. Port-Based Service Zone 35
3.3.2. Tag-Based Service Zone 36
Chapter 4. User Authentication Database 37
4.1. Authentication Database Configuration 37
4.2. Built-in Authentication Databases 39
4.2.1. Local User Database 39
4.2.2. On-Demand User Database 42
4.2.3. Guest Authentication 47
4.3. External Authentication Options 52
4.3.1. RADIUS 53
4.3.2. POP3 55
4.3.3. LDAP 56
4.3.4. NT Domain 57
4.3.5. SIP 57
4.3.6. Social Media 59
Chapter 5. Group Attributes & Policy Rules 61
5.1 Overview of Concept 61
5.2 Practical Setups of Group and Policies 63
Chapter 6. Basic Service Zone Configuration 70
6.1 The Concept of Service Zone 70
6.2 Service Zone Setup 70
6.2.1. Tag-based or Port-based Service Zones 70
6.2.2. NAT Mode or Router Mode 73
6.2.3. Service Zone Network Interface 73
6.2.4. DHCP Server options 74
6.2.5. Authentication Options 75
6.2.6. Portal Customization 78
Chapter 7. Basic AP Management 81
7.1. Introduction 81
7.2 Local Area AP Management 83
7.2.1. AP List 83

7.2.2. AP Adding and Configuration Applying 84
7.2.3. Templates Configuration 87
7.2.4. AP Firmware Management 90
7.2.5. WDS Links 90
7.2.6. Rogue AP Scanning 93
7.2.7. AP Load Balancing Feature.. 94
7.3 Wide Area AP Management.. 95
7.3.1. Adding an Access Point.. 96
7.3.2. AP Discovery to find Multiple Access Points 96
7.3.3. AP Configuration with Templates.. 97
7.3.4. AP auto Discovery and Configuration using CAPWAP 98
7.3.5. Tunneled VAP Location Mapping Setup 104
7.3.6. Access Points on Map & AP Grouping....................................105
7.3.7. Rogue AP Scanning 109
7.3.8. AP Load Balancing Feature...110
Chapter 8. Advanced Settings for Network Environment 112
8.1 IPv4 / IPv6 Dual Stack Network 112
8.2 User Access Control 115
8.3 Certification 118
8.3.1. System Certificate 119
8.3.2. Internal Root CA...120
8.3.3. Internally Issued Certificate..121
8.3.4. Trusted Certificate Authorities 121
8.4 Management Access 122
Chapter 9. Utilities for Controller Management................................ 123
9.1 EWS Controller Management 123
9.2 Configuration Backup & Restore 125
9.3 Firmware Upgrade 126
9.4 Restart...127
Chapter 10. Reports and Logs for Monitoring 129
10.1 System Related Status 129
10.1.1. The Dashboard...129
10.1.2. System Summary 130
10.1.3. Network Interface...132
10.1.4. Routing 133
10.1.5. DHCP Server 134
10.2 Client Related Status 135
10.2.1. Online User 135
10.2.2. Associated Non Login Users 136
10.2.3. Cross Gateway Roaming Users..137
10.2.4. On-Demand Roaming Out User 137
10.2.5. Session List 138
10.3 Logs and Reports 139
10.3.1. System Related...139
10.3.2. User Events 140
10.4 Reports & Notification 141
Chapter 11. Hotspot Application 143
11.1 On-Demand Billing Plans 143
11.2 On-Demand Billing Plan Types 144
11.2.1. Usage-time with Expiration Time 144
11.2.2. Usage-time with No Expiration Time..................................146
11.2.3. Hotel Cut-off-time..148

11.2.4. Volume 149
11.2.5. Duration-time with Elapsed Time 151
11.2.6. Duration-time with Cut-off Time 153
11.2.7. Duration-time with Begin-and-End Time 154
11.4 Creating Accounts 155
11.5 User Self Service 158
Chapter 12. PMS Integration 163
12.1 Hotel Room Location Mapping 164
12.2 Micros Opera 166
Chapter 13. Account Roaming 168
13.1 Roaming Related 168
13.2 WISPr for ISP Roaming 168
13.3 Cross Gateway Roaming 170
13.4 Local / On-Demand Account Roaming Out 171
Chapter 14. VPN 174
14.1 Site-to-Site 174
14.2 Remote Client 176
Chapter 15. Platform Dependent Features 178
15.1 High Availability (HA) 178
15.2 WiFi Monitor 180
15.3.1. Add a Floor Plan 180
15.3.2. Simulation AP 182
15.3.3. AP Monitoring on floorplan 184
Appendix A. External Pages 185
Appendix B. Useful Management & Evaluation Tools 199
Appendix C. On-Demand Account Types 201
Appendix D. UI Reference Index 208
I. Main 208
II. Setup Wizard 208
III. Dashboard 209
A. System 209
1) General 210
2) WAN 211
3) IPv6 213
4) LAN Ports 213
5) High Availability 214
6) Service Zones 215
7) Port Location Mapping 219
8) Middleware 223
B. Users 224
1) Groups 224
2) Internal Authentication 225
3) External Authentication 227
4) On-Demand Accounts 228
5) Schedule 229
6) Policies 229
7) Blacklists 230
8) Privilege Lists 231
5) Additional Control 231
C. Access Points 234
1) Local Area AP Management 234
a) Overview 234

b) List 234
c) Adding..235
d) Discovery 235
e) Templates..236
f) Firmware..243
g) Upgrade 244
h) WDS Management 245
i) Rogue AP Detection 246
j) AP Load Balancing 247
2) Wide Area AP Management 248
a) Map 248
b) List 254
c) Discovery...257
d) Adding 258
e) Template 259
f) WDS List..264
g) Backup Config 265
h) Firmware 265
i) CAPWAP 265
j) Rogue AP Detection 267
k) AP Load Balancing 267
l) Third Party AP Management 268
D. Switches..270
1) Switch List 270
2) PoE Schedule Template...270
3) Backup Configuration 272
E. Network...273
1) NAT 273
2) Monitor IP...275
3) Walled Garden and Walled Garden Ad...275
4) VPN 276
5) Proxy Server 277
6) Local DNS Record 280
7) Dynamic Routing 280
8) DDNS...285
9) Client Mobility 285
F. Utilities 287
1) Administrator Account 287
2) Backup & Restore 290
3) Certificates 292
4) Network Utilities 294
5) Restart...296
6) System Upgrade 296
G. Status..297
1) System Summary 297
2) Interface 299
3) Monitor Users...301
4) WiFi Monitor...301
5) Managed AP Simulation 303
6) Process Monitor 305
7) Logs & Reports...305
8) Reporting 307
9) Session List 312

10) DHCP Lease 313
11) Routing Table 315
Appendix E. Advanced Features **.. 316**

Chapter 1. Introduction

1.1 EWS Controller Series

EWS 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 of EWS Controller models to meet network demands with various scale of capacities.

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 EWS Controllers, different users are authenticated based on user role, from there it will define the user's accessible network segments and network portfolio, including accessible time, QoS, routing rules, firewall rules, usage terms and privileges that are collectively known as authorization. Finally, accounting is performed by EWS Controllers periodically while clients are using the network, updating the accounting information for the clients to either the internal user database or an external user database depending on deployment.

Wireless network provisioning is no easy task when deployment of multiple APs is involved. EWS Controllers are equipped with comprehensive AP management features to cover not only Edgecore 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 EWS Controllers. Furthermore, with an interface for 3rd party AP management, EWS Controllers support 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 or hoteliers for example as these are major factors in determining the quality and stability of the network environment as a whole. EWS Controllers address these needs by supporting 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 EWS Controllers. Providing three varieties of NAT function, Walled Garden for accessing certain websites prior to user authentication, Network device monitoring tool, Static DNS translation, Proxy Server, VPN and more. EWS Controllers simplify network deployment by incorporating multiple networking features into one device, avoiding the need to setup external NAT servers, Proxy servers, VPN gateway, and etc., thereby reducing deployment complexity.

Network Maintenance and Network monitoring tasks are made easy with a built in display showing 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 Models

EWS Controller product line includes the following models for targeting network deployment of variable scale.

SMB & Enterprise Controllers
EWS5203

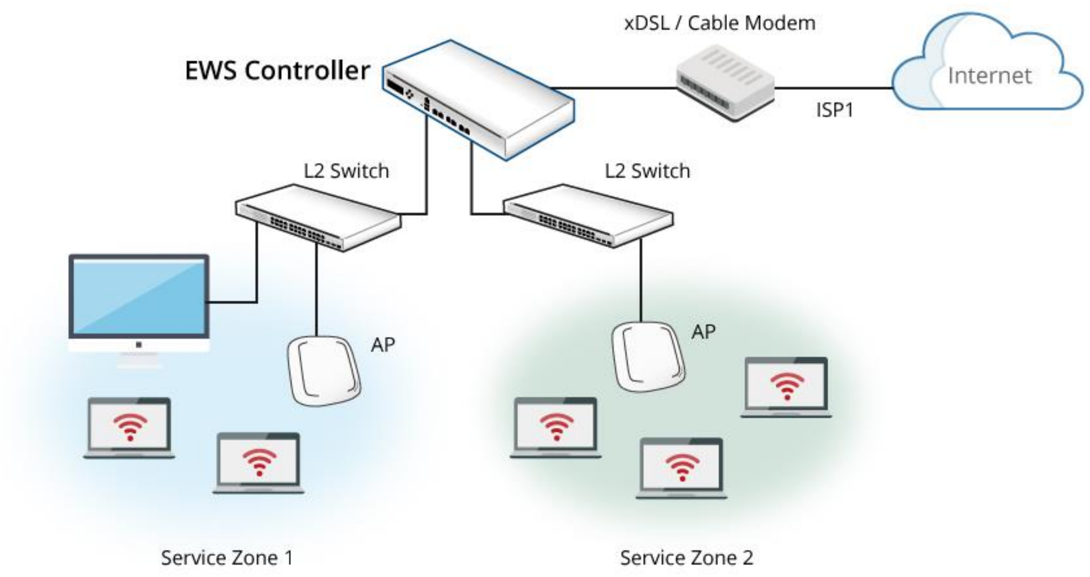
Large Enterprise & Carrier Grade Controllers
EWS5204, EWS5207

Note: As Edgecore may continue to introduce new platforms and/or retire old platforms, please refer to our official website http://www.edge-core.com for the latest product lines.

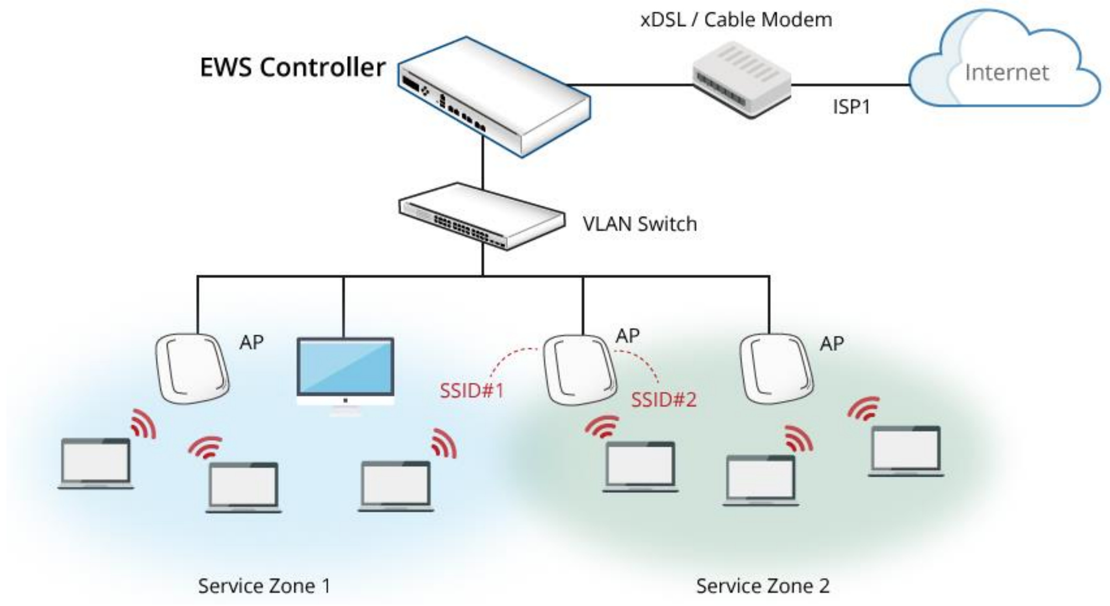
1.3 Edgecore Solution Overview

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

Layer 2 networks have relatively simple network deployment topologies that span physically under the LAN ports of EWS Controllers. Two deployment scenarios are illustrated below.

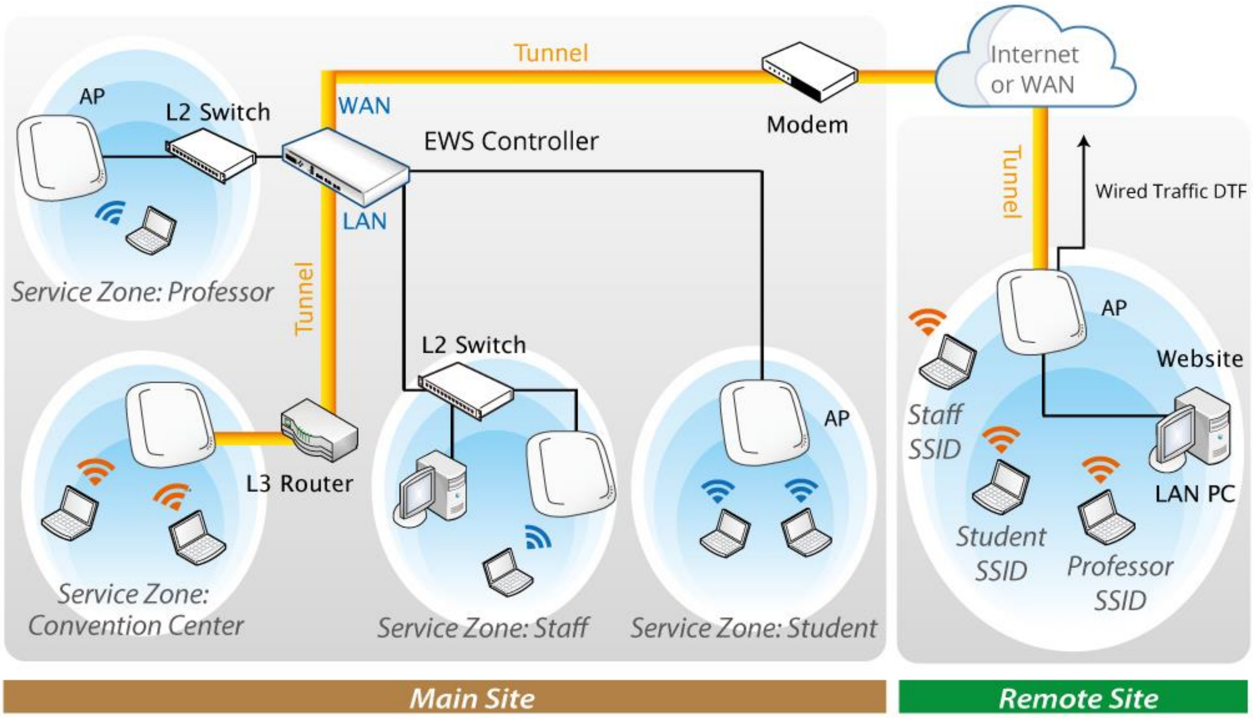

xDSL / Cable Modem
EWS Controller
Internet
ISP1
L2 Switch
L2 Switch
AP
AP
Service Zone 1
Service Zone 2

【Layer 2 Network in Port Based Mode】


xDSL / Cable Modem
EWS Controller
Internet
ISP1
VLAN Switch
AP
AP
AP
SSID#1
SSID#2
Service Zone 1
Service Zone 2

【Layer 2 Network in Tag Based Mode】

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


Tunnel
Internet or WAN
WAN
AP
L2 Switch
EWS Controller
Modem
LAN
Tunnel
Wired Traffic DTF
Service Zone: Professor
Tunnel
AP
L2 Switch
Website
Staff SSID
AP
L3 Router
LAN PC
Student SSID
Professor SSID
Service Zone: Convention Center
Service Zone: Staff
Service Zone: Student
Main Site
Remote Site

【Layer 3 Network with tunnels】

1.4 Key Terms & Concepts

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

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

On-Demand User is a type of user whose account credential is stored in the EWS

Controller's built-in database named "On-Demand". The EWS Controller's "On-Demand" database capacity varies with 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, EWS Controller's On-Demand database can be configured as an external RADIUS database for another EWS Controller for account roaming.

External Authentication Database is a user account database that is not built-in the EWS Controller. Besides Local database and On-Demand database, 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 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, EWS Controller is capable of servicing multiple hotspot franchises with a single device.

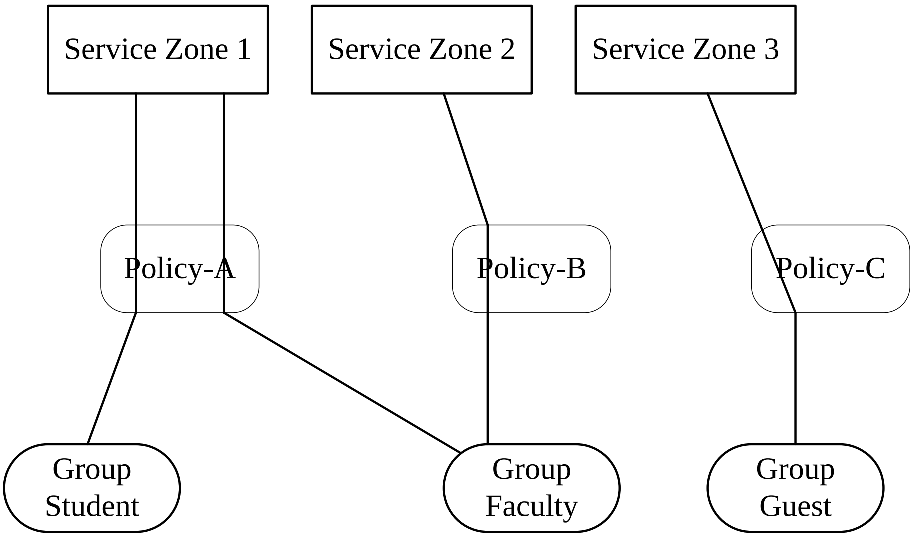
LAN Port Mapping is the correspondence relationship of logical network partitions, i.e. Service Zones to physical LAN ports on the EWS Controller There are two modes of mapping available namely "Port-Based", and "Tag-Based". Port-Based mode statically maps a Service Zone to clients downstream of a physical LAN port. This mode will only service the maximum number of service zones based on the amount of physical LAN ports. Tag-Based mode dynamically maps a client to a service zone based on the VLAN ID tagged on the traffic packet.

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

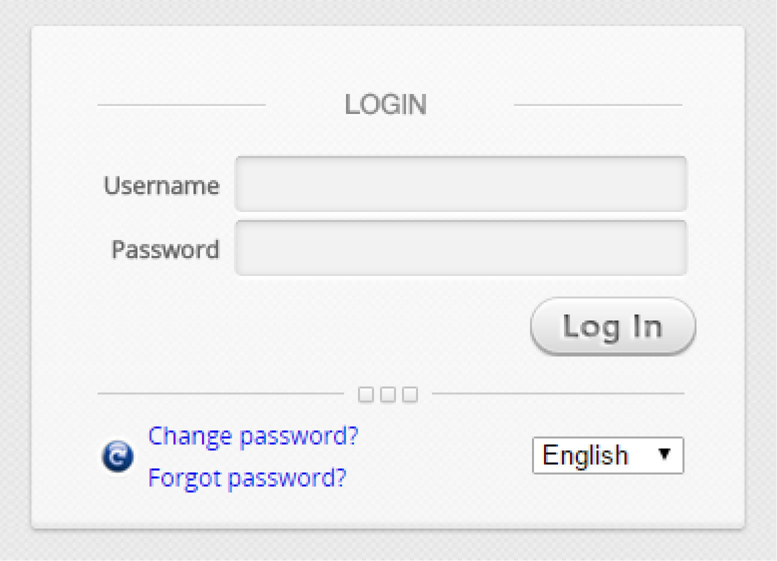
Chapters 8 to **10** discuss about security, system maintenance, and monitoring. These contents are useful once you have successfully configured the necessary functionalities and are for operation usage once your network is up and running.

Customers with needs to fulfill specific applications, integration with 3rd 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**.

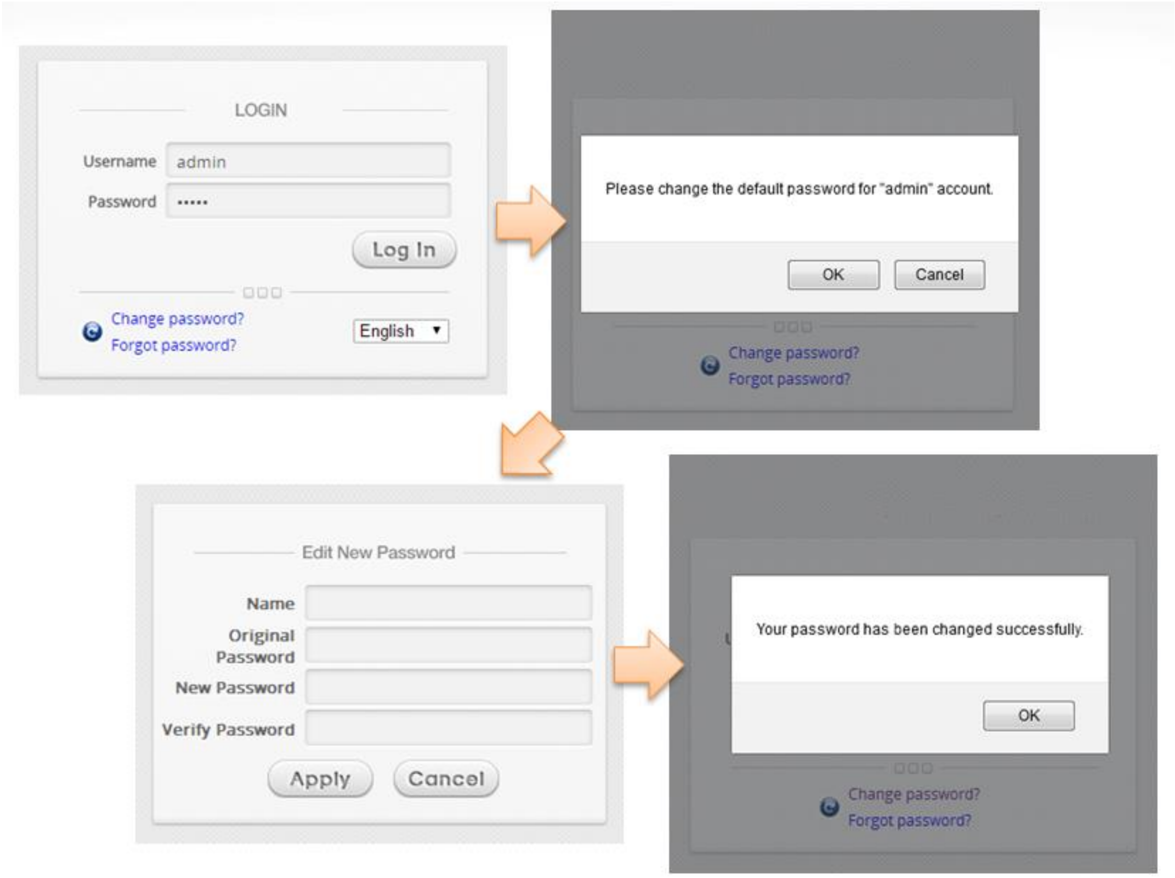


The default administrator account and password is:

- 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.

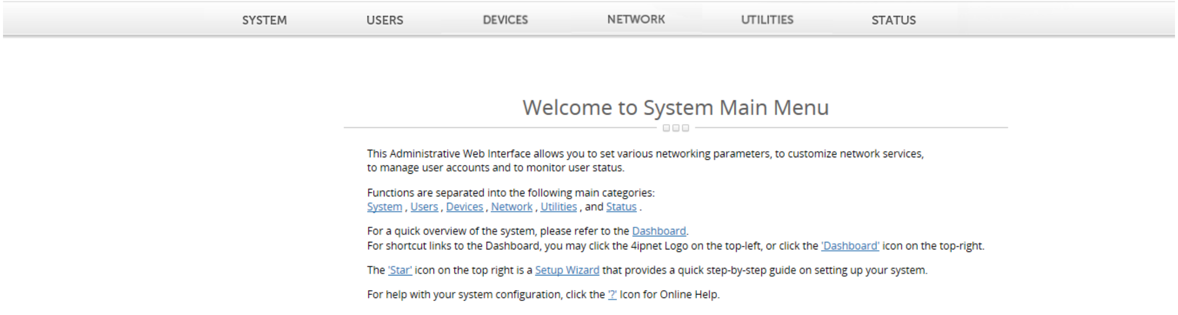
You may refer to part F of Appendix D for details on admin accounts configuration.


LOGIN
Username
admin
Password
•••••
Log In
Change password?
Forgot password?
English
OK
Cancel
Edit New Password
Name
Original Password
New Password
Verify Password
Apply
Cancel
OK

Please change the default password for "admin" account.

Your password has been changed successfully.

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


SYSTEM
USERS
DEVICES
NETWORK
UTILITIES
STATUS

Welcome to System Main Menu

This Administrative Web Interface allows you to set various networking parameters, to customize network services,
to manage user accounts and to monitor user status.

Functions are separated into the following main categories:
System , Users , Devices , Network , Utilities , and Status .

For a quick overview of the system, please refer to the Dashboard.
For shortcut links to the Dashboard, you may click the 4ipnet Logo on the top-left, or click the 'Dashboard' icon on the top-right.

The 'Star' icon on the top right is a Setup Wizard that provides a quick step-by-step guide on setting up your system.

For help with your system configuration, click the '?' Icon for Online Help.

NOTE

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

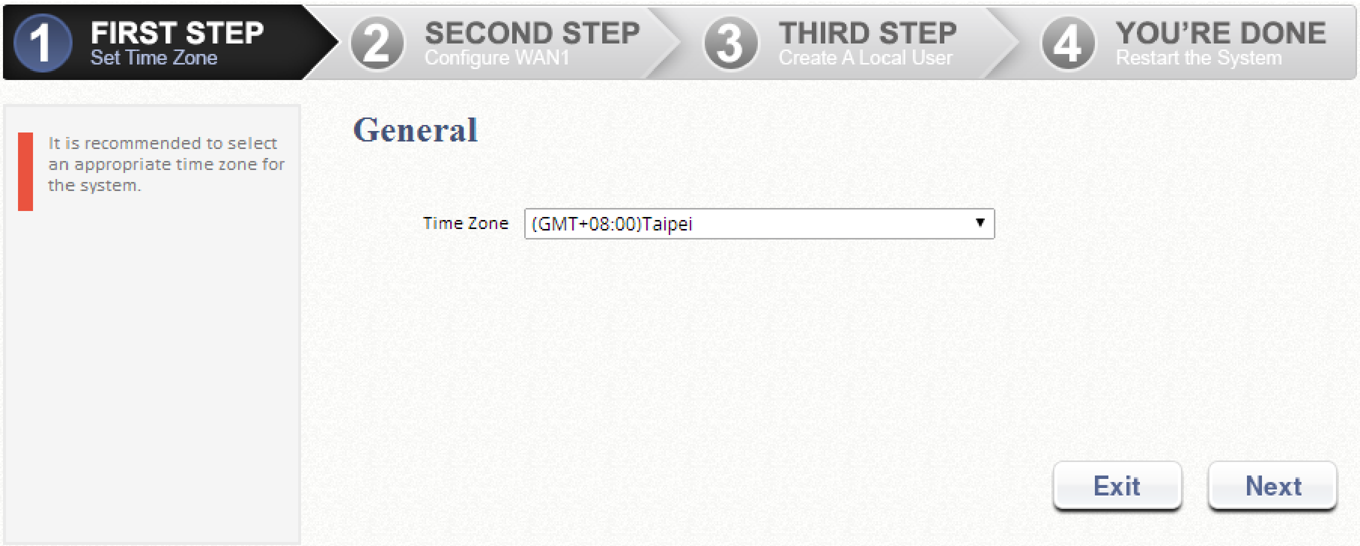
2.2 Running the Wizard

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.

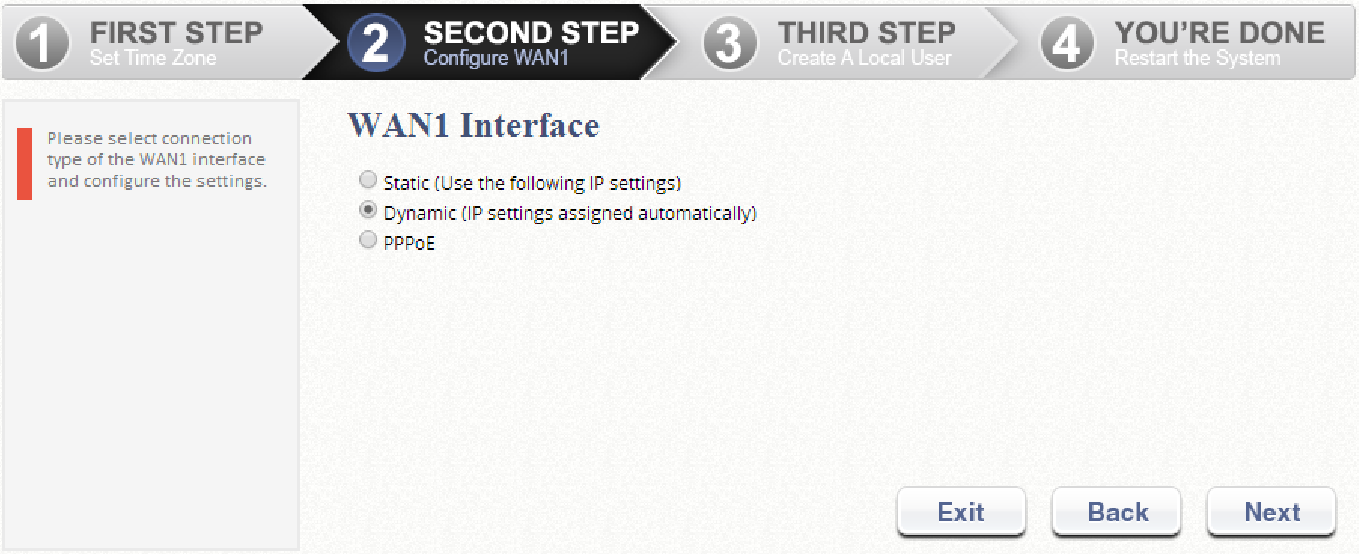

1 FIRST STEP
Set Time Zone
2 SECOND STEP
Configure WAN1
3 THIRD STEP
Create A Local User
4 YOU'RE DONE
Restart the System
General
Exit
Next

It is recommended to select an appropriate time zone for the system.

Time Zone (GMT+08:00)Taipei

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.

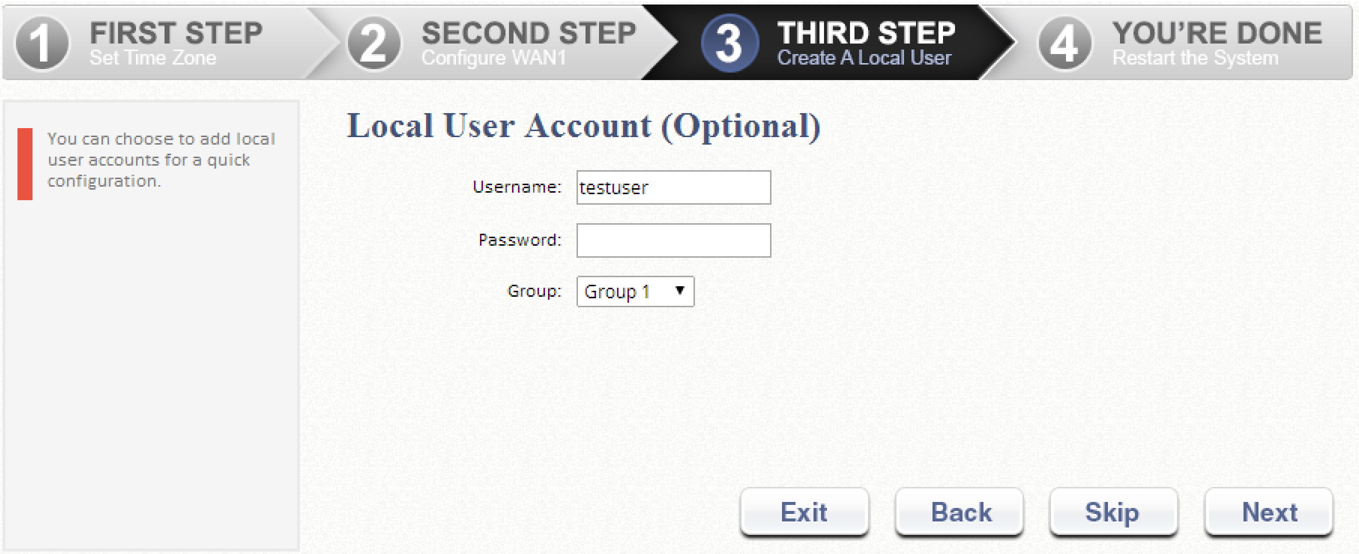
WAN1 Interface

○ 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.

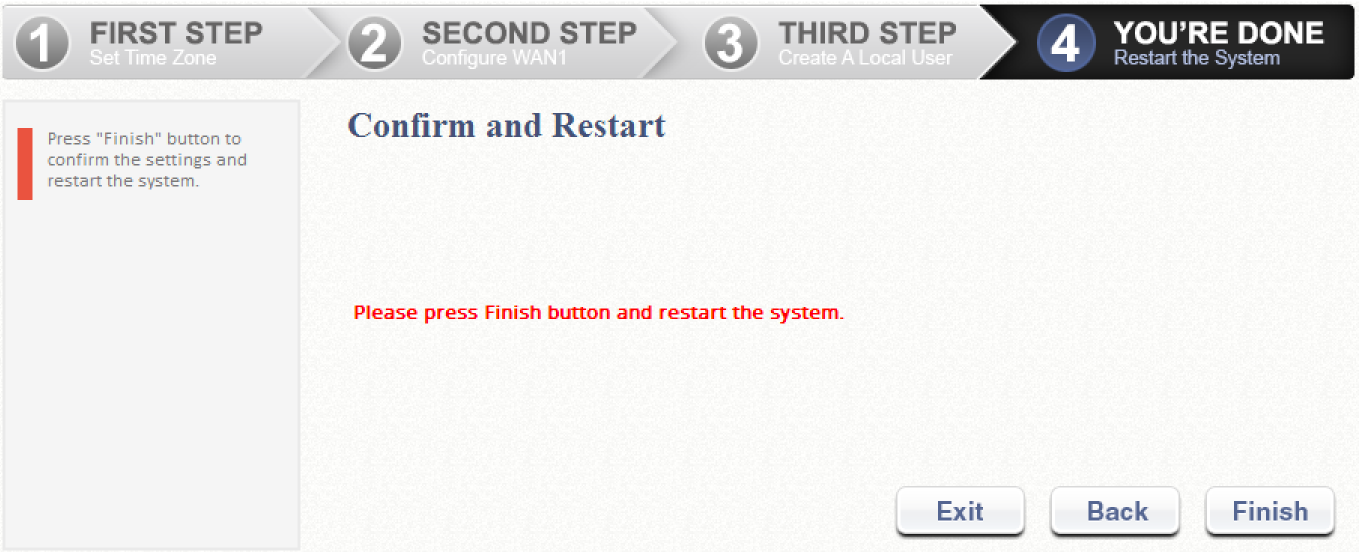
Local User Account (Optional)

Username: testuser
Password:
Group: Group 1

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.



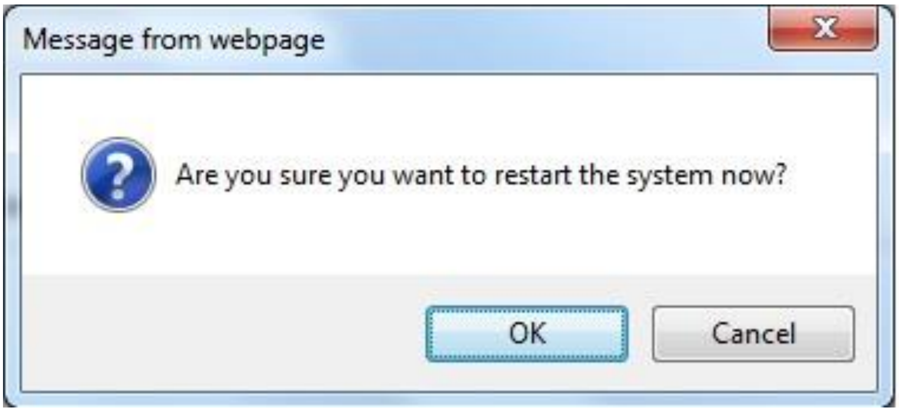
1 FIRST STEP Set Time Zone
2 SECOND STEP Configure WAN1
3 THIRD STEP Create A Local User
4 YOU'RE DONE Restart the System

Press "Finish" button to confirm the settings and restart the system.

Confirm and Restart

Please press Finish button and restart the system.

Exit
Back
Finish

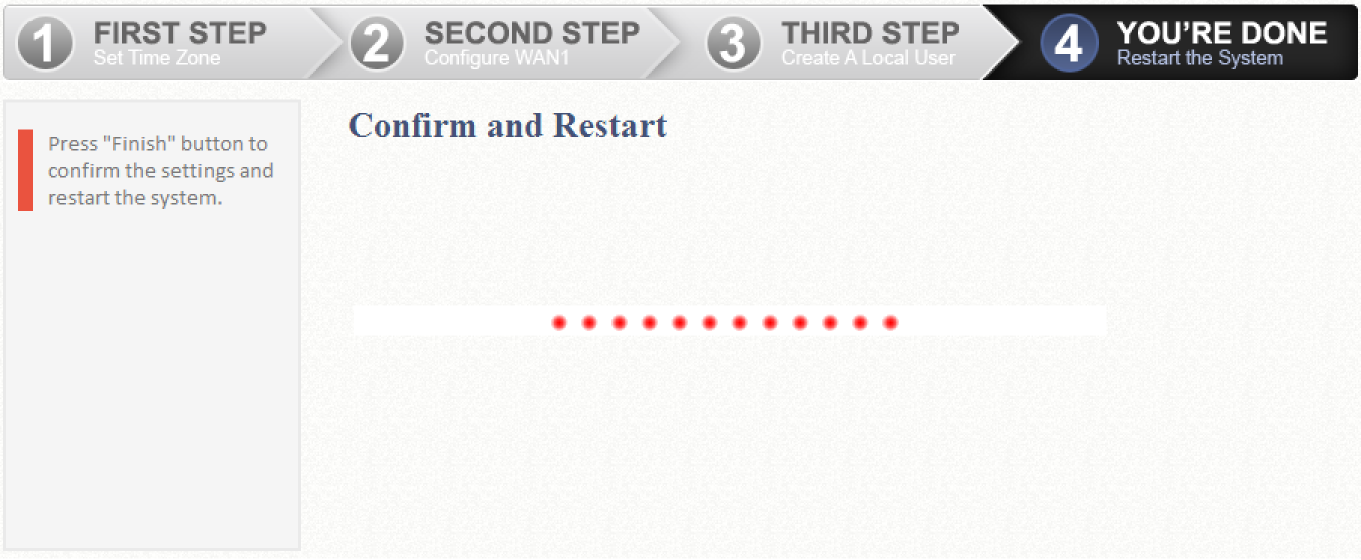


Message from webpage

Are you sure you want to restart the system now?

- 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.

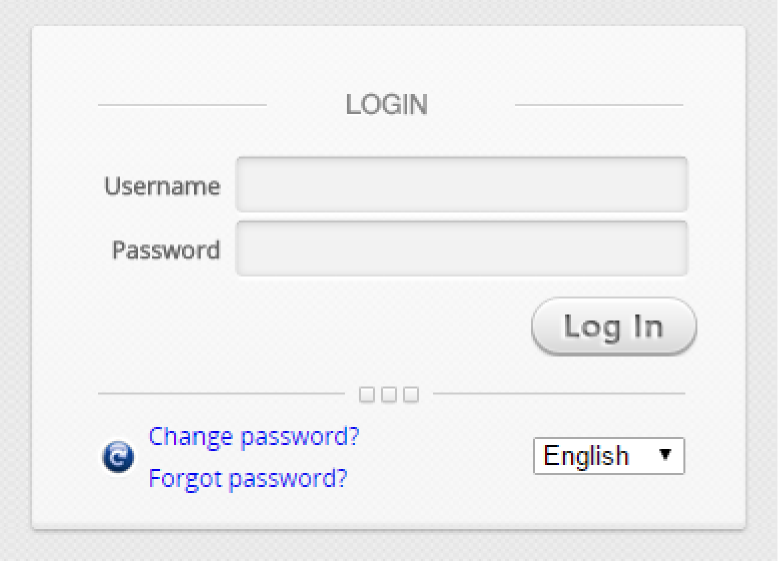

1 FIRST STEP
Set Time Zone
2 SECOND STEP
Configure WAN1
3 THIRD STEP
Create A Local User
4 YOU'RE DONE
Restart the System

Confirm and Restart

Press "Finish" button to confirm the settings and restart the system.

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

Restart process complete.


LOGIN
Username
Password
Log In
Change password?
Forgot password?
English

Chapter 3. Basic Network Settings

3.1. Network Planning

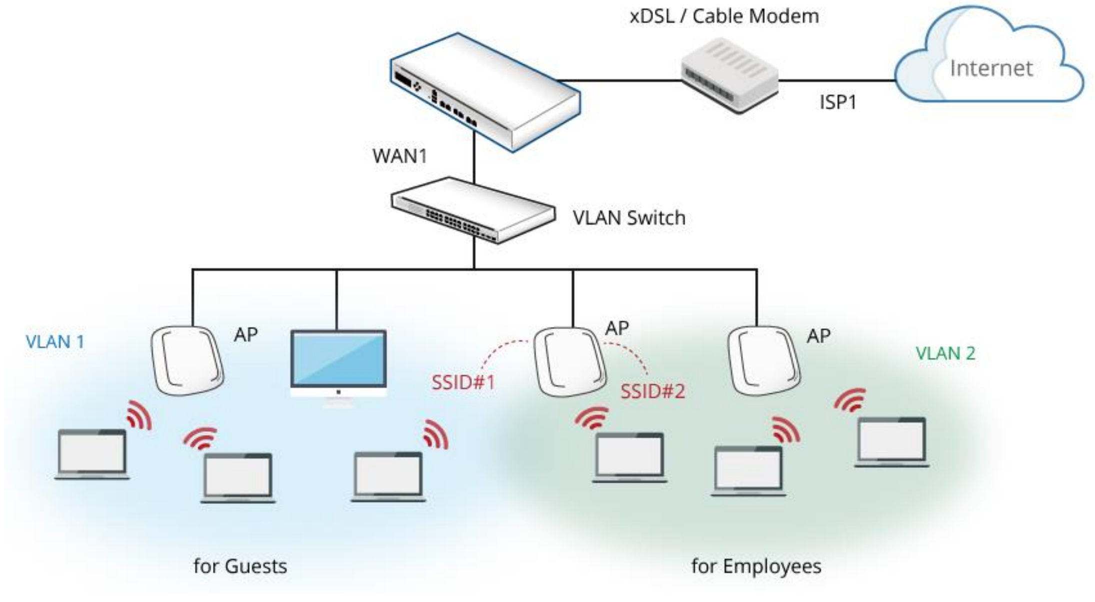
Before installing the EWS Controller, careful network planning is required in order to meet the networking needs with the most efficient utilization of network resources. IT staff of any organization should assess the available network resources at hand, and design a suitable network topology with resiliency,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



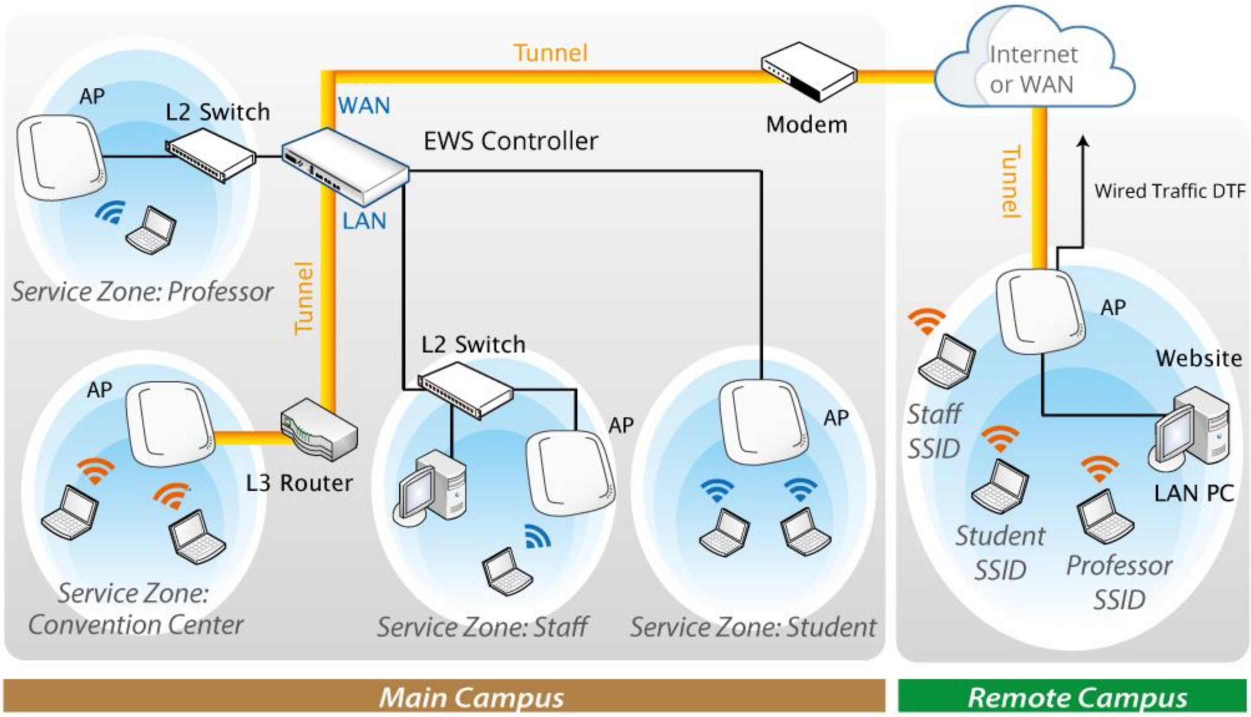
【Graphical Illustration of Layer 2 Topology】

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.


Tunnel
AP
L2 Switch
WAN
EWS Controller
Modem
Internet or WAN
LAN
Tunnel
Wired Traffic DTF
Service Zone: Professor
Tunnel
L2 Switch
AP
AP
Website
AP
AP
L3 Router
Staff SSID
LAN PC
Student SSID
Professor SSID
Service Zone: Convention Center
Service Zone: Staff
Service Zone: Student
Main Campus
Remote Campus

【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.

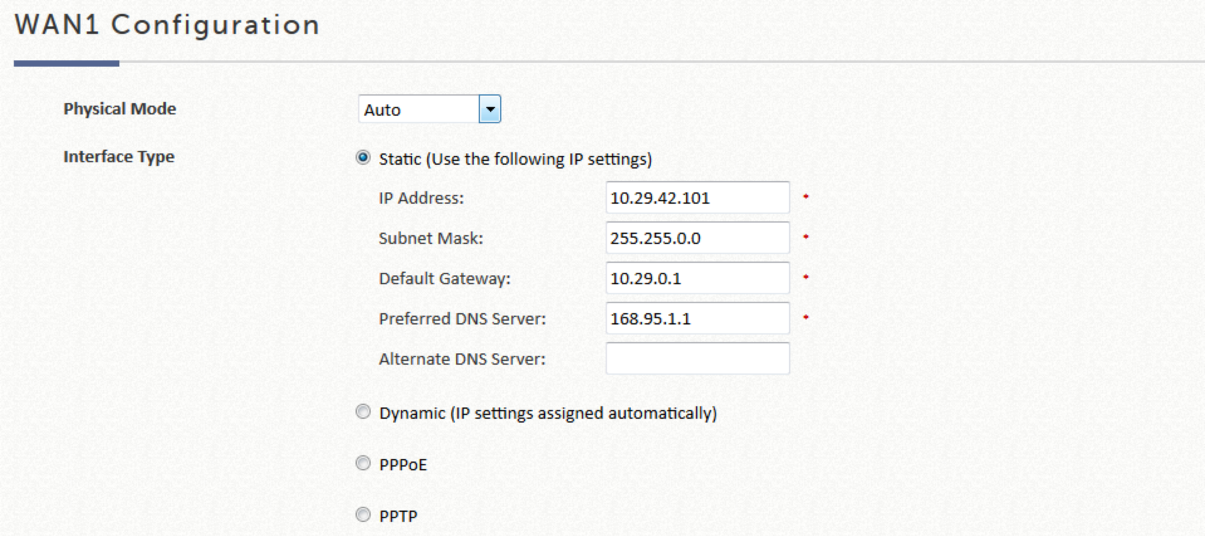
- Locate the aggregation switch close to the network core (e.g. mainframe housing)
- Locate edge switches close to users (e.g. one per floor)
- Remote site’s device (Edgecore AP or Edgecore EWS Controller) uplink should either have a public IP address or an IP address in the same subnet as the main EWS 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.



WAN1 Configuration

Physical Mode: Auto

Interface Type:

● Static (Use the following IP settings)

IP Address: 10.29.42.101 *
Subnet Mask: 255.255.0.0 *
Default Gateway: 10.29.0.1 *
Preferred DNS Server: 168.95.1.1 *
Alternate DNS Server:

○ Dynamic (IP settings assigned automatically)

○ PPPoE

○ 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.

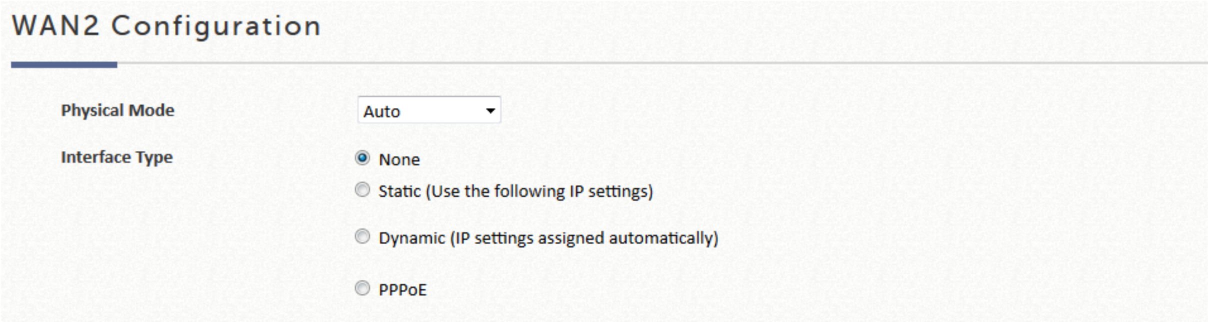
NOTE

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

3.2.2. Dual Uplink

EWS Controllers are designed with 2 WAN ports for load balancing and failover support. WAN2 can be enabled for service once WAN1 connection is established.

If you would like to use a second Internet feed, select one of the three connection types applicable to WAN2 port: **Static, Dynamic,** and **PPPoE**. The Physical Mode of the WAN2 port can be selected.



WAN2 Configuration

Physical Mode: Auto

Interface Type:
● None
○ Static (Use the following IP settings)
○ Dynamic (IP settings assigned automatically)
○ PPPoE

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.

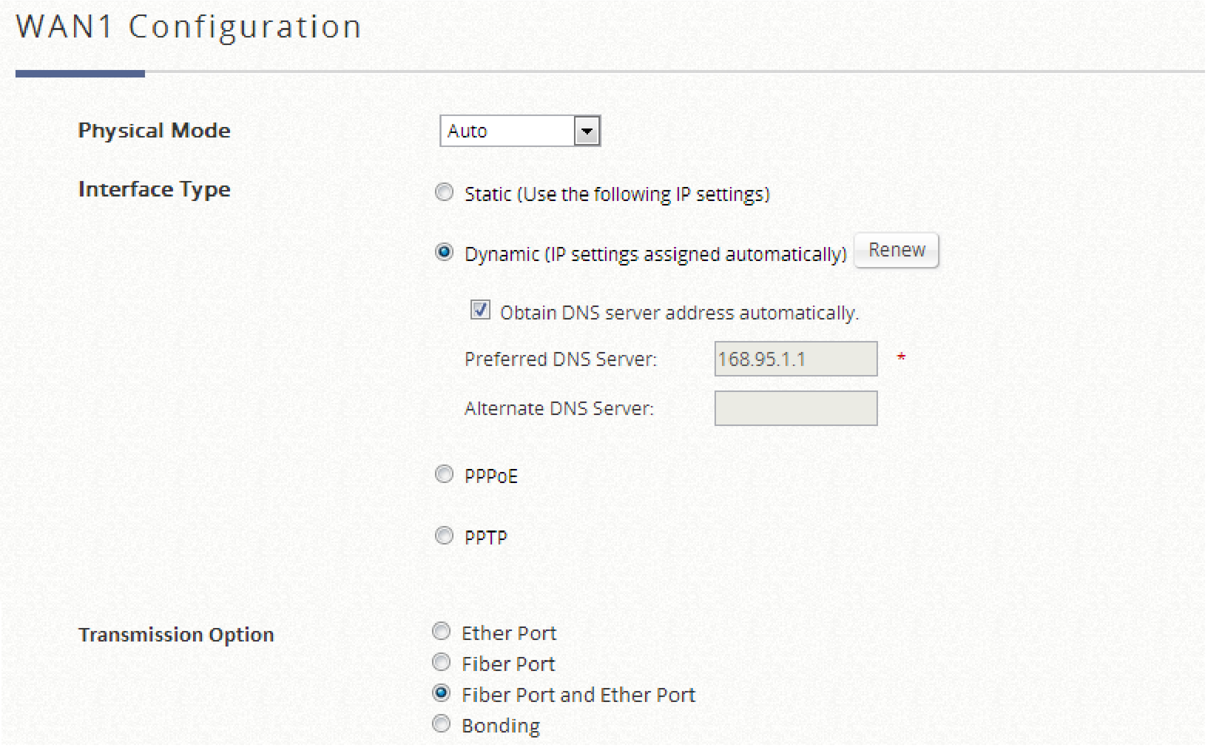
NOTE

1. When in doubt, please consult your ISP provider regarding details of your subscribed uplink service.
2. Please note that WAN load balancing and WAN failover features are only available when WAN2 is configured.

3.2.3. WAN Port Selection for dual WAN1 / WAN2 models

Carrier grade models such as EWS5204 and EWS5207 are designed with a SFP and Ethernet port for both WAN1 and WAN2 respectively. Administrator can further decide which physical port to be deployed as WAN1 or WAN2, Ethernet port, SFP port, Ethernet and SFP port, or both port bonded with aggregated throughput.

Configuration Path: Main Menu >> System >> WAN



WAN1 Configuration

Physical Mode: Auto

Interface Type

○ Static (Use the following IP settings)

● Dynamic (IP settings assigned automatically) Renew

☑ Obtain DNS server address automatically.

Preferred DNS Server: 168.95.1.1 *

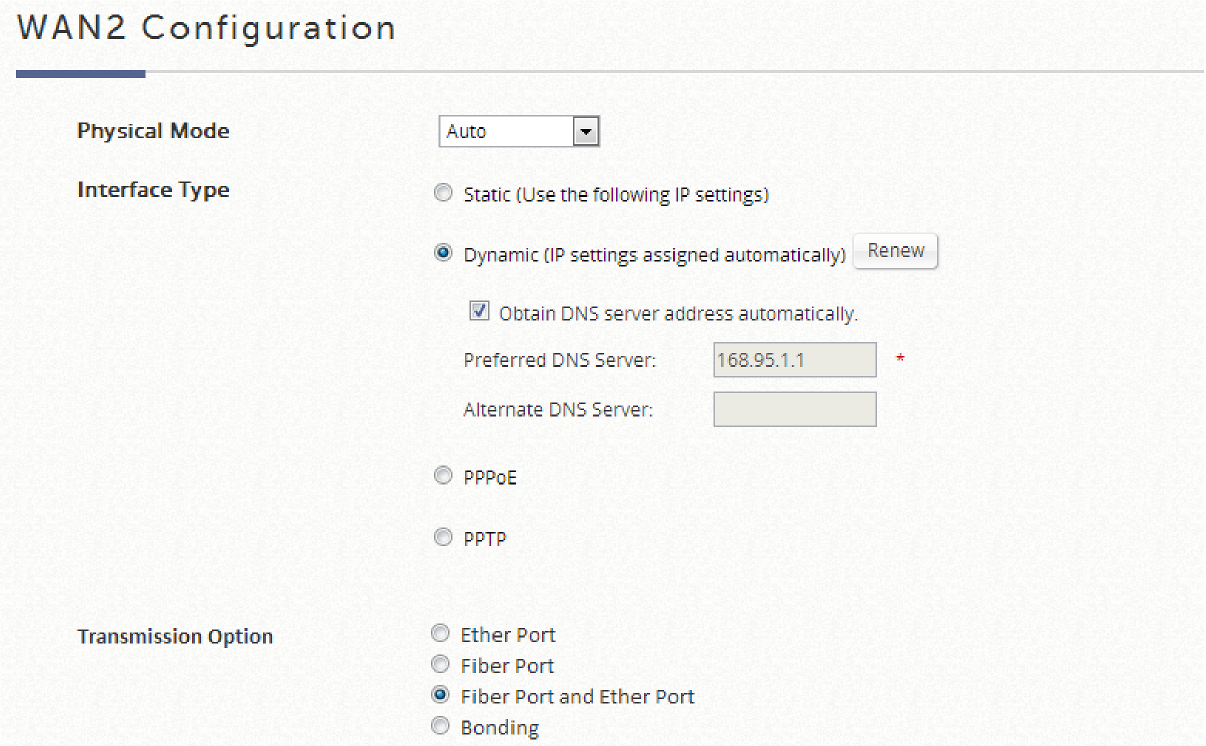
Alternate DNS Server:

○ PPPoE

○ PPTP

Transmission Option

○ Ether Port
○ Fiber Port
● Fiber Port and Ether Port
○ Bonding



WAN2 Configuration

Physical Mode: Auto

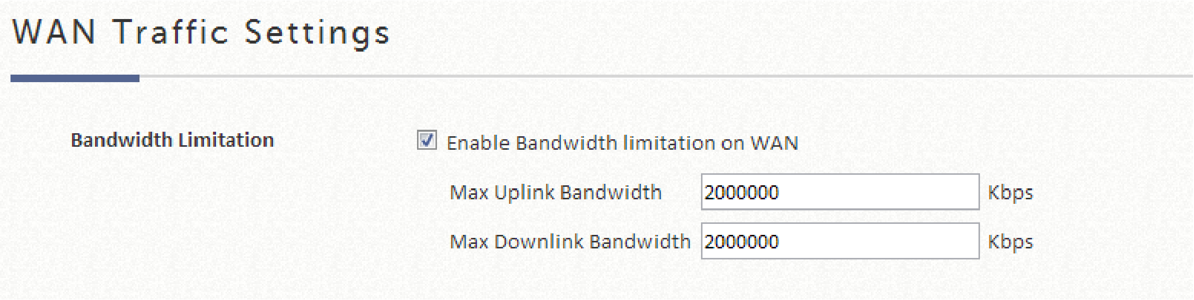
Interface Type:
○ Static (Use the following IP settings)
● Dynamic (IP settings assigned automatically) Renew
☑ Obtain DNS server address automatically.
Preferred DNS Server: 168.95.1.1 *
Alternate DNS Server:
○ PPPoE
○ PPTP

Transmission Option:
○ Ether Port
○ Fiber Port
● Fiber Port and Ether Port
○ Bonding

The deployment options are:

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

3.2.4. WAN Traffic Control


WAN Traffic Settings

Bandwidth Limitation ☑ Enable Bandwidth limitation on WAN

Max Uplink Bandwidth 2000000 Kbps

Max Downlink Bandwidth 2000000 Kbps

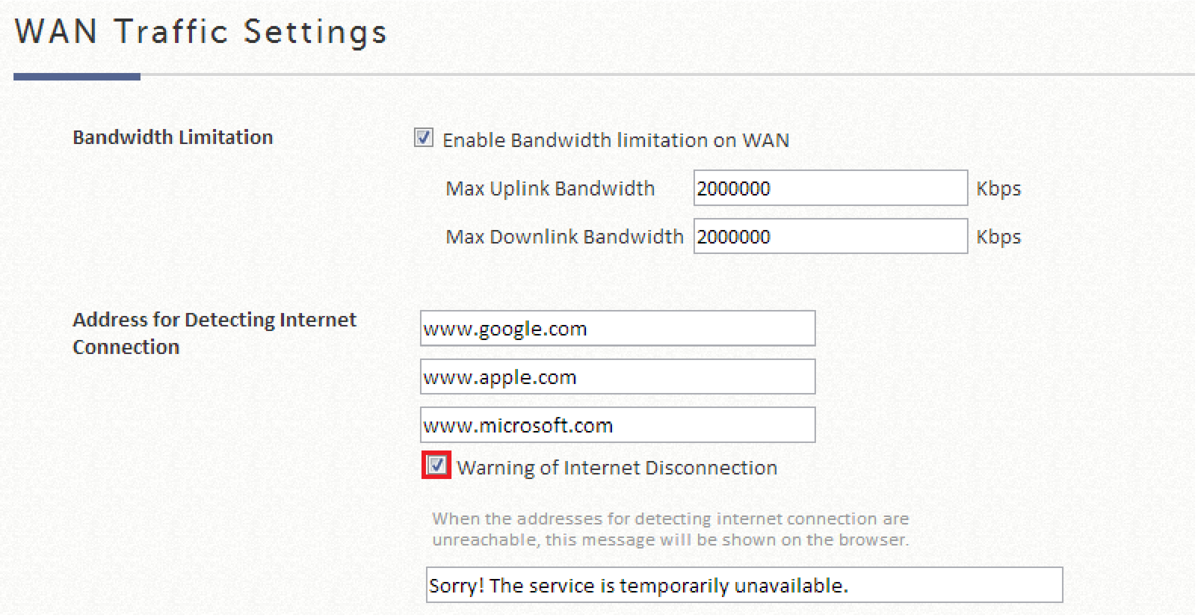
The Uplink and Downlink bandwidth configured here is the combined bandwidth for WAN interface including WAN1 and WAN2. However, please note that the actual bandwidth is still bounded by the network speed of your ISP operator. For instance, when the network speed of your ISP is limited to 1Gbps, the total throughput under such constraint will not be greater than 1Gbps even if you configure 2Gbps on the Controller.

3.2.5. Uplink Detection & Failover

Uplink Detection

When the WAN interface has been configured with a valid uplink connection, administrator may specify up to three outbound sites as detection target for verifying whether the uplink service is alive or down. The controller will periodically check the uplink status.

A field of warning message text may be customized by the administrator which will be displayed on the user’s web browser when all three detection targets fail to respond.



WAN Traffic Settings

Bandwidth Limitation ☑ Enable Bandwidth limitation on WAN

Max Uplink Bandwidth 2000000 Kbps

Max Downlink Bandwidth 2000000 Kbps

Address for Detecting Internet Connection

www.google.com

www.apple.com

www.microsoft.com

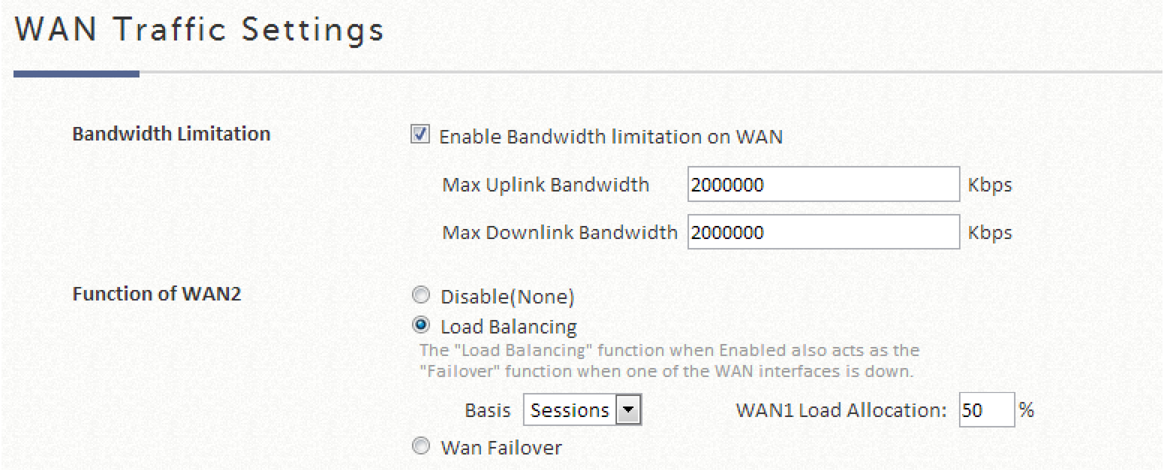
☑ Warning of Internet Disconnection

When the addresses for detecting internet connection are unreachable, this message will be shown on the browser.

Sorry! The service is temporarily unavailable.

Load Balancing

Administrator can spread the system traffic across WAN1 and WAN2 ports based on percentage load, calculated using session, bytes, or packets.



WAN Traffic Settings

Bandwidth Limitation ☑ Enable Bandwidth limitation on WAN

Max Uplink Bandwidth 2000000 Kbps

Max Downlink Bandwidth 2000000 Kbps

Function of WAN2

○ Disable(None)

● Load Balancing

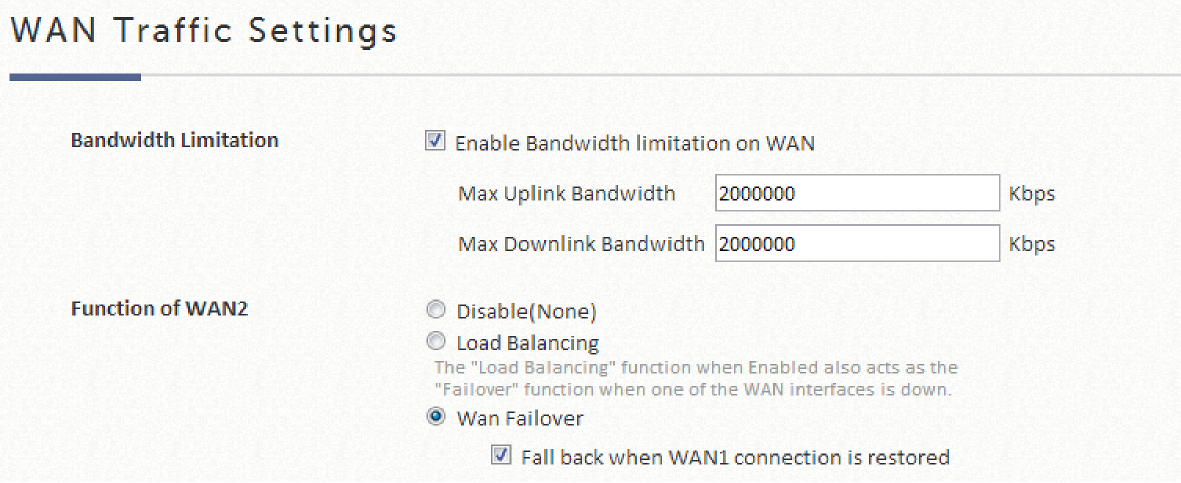
The "Load Balancing" function when Enabled also acts as the "Failover" function when one of the WAN interfaces is down.

Basis Sessions WAN1 Load Allocation: 50 %

○ Wan Failover

WAN Failover

Once enabled, whenever WAN1 is down, WAN2 will service the traffic originally handled by WAN1. If the nested option is selected, service will be returned to WAN1 link if it is up again. This feature is not available to be used concurrently with Load Balancing.



WAN Traffic Settings

Bandwidth Limitation ☑ Enable Bandwidth limitation on WAN

Max Uplink Bandwidth 2000000 Kbps

Max Downlink Bandwidth 2000000 Kbps

Function of WAN2

○ Disable(None)

○ Load Balancing

The "Load Balancing" function when Enabled also acts as the "Failover" function when one of the WAN interfaces is down.

● Wan Failover

☑ Fall back when WAN1 connection is restored

NOTE

1. Please note that WAN Failover feature cannot be enabled concurrently with Load Balancing feature.

3.3. Downlink (LAN side) VLAN option

The Downlink of EWS Controller is basically your managed network deployed for service. There are two types of deployment mode for networks attached to the LAN ports of the EWS Controller: Port-Based mode and Tag-Based mode.

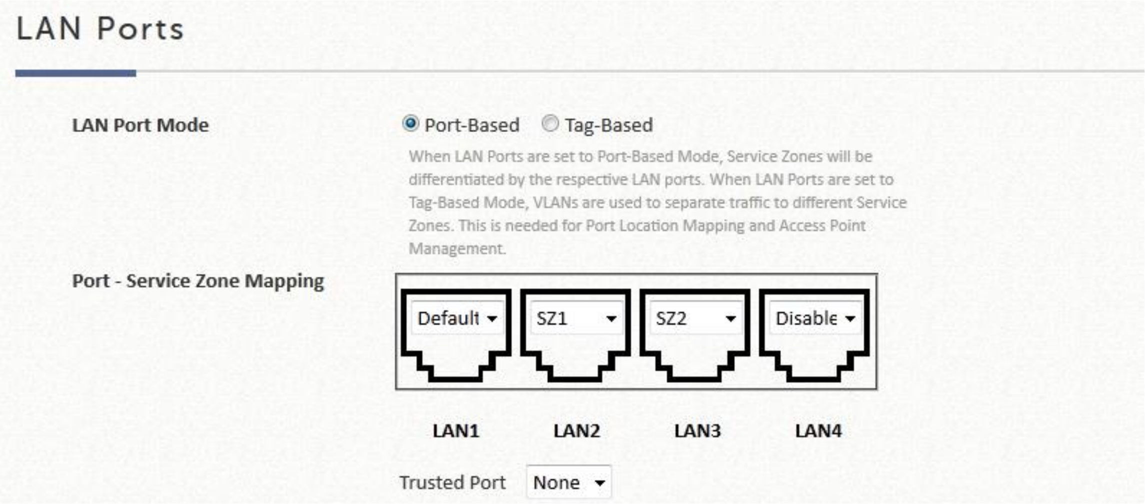
NOTE

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

Configuration Path: Main Menu >> System >> LAN Ports

3.3.1. Port-Based Service Zone

Port-Based mode operates with the principle that each physical LAN port can be mapped to an enabled Service Zone or disabled from providing service. Operating under port based mode therefore means the maximum amount of Service Zones available to actually provide service is determined by the number of LAN ports on the Controller.



LAN Ports

LAN Port Mode ● Port-Based ○ Tag-Based

When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.

Port - Service Zone Mapping

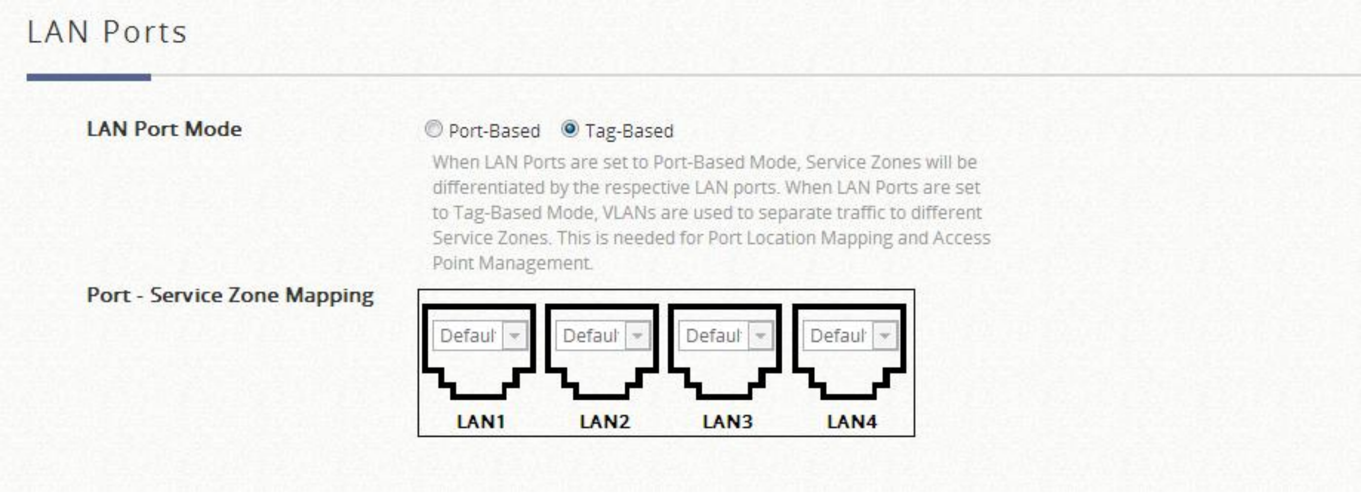
LAN1	LAN2	LAN3	LAN4
Default	SZ1	SZ2	Disable

Trusted Port None

Trusted Port: When a LAN port is selected here, clients under this port will not require authentication regardless of the corresponding Service Zone settings.

3.3.2. Tag-Based Service Zone

Tag-Based operation mode operates under the principle that different Service Zones are identified by VLAN ID. This means that Tag-Based operation allows each physical LAN port to accept traffic for any enabled Service Zones – Traffic handling will be processed internally according to the VLAN ID traffic packets carry.



LAN Ports

LAN Port Mode ○ Port-Based ● Tag-Based

When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.

Port - Service Zone Mapping

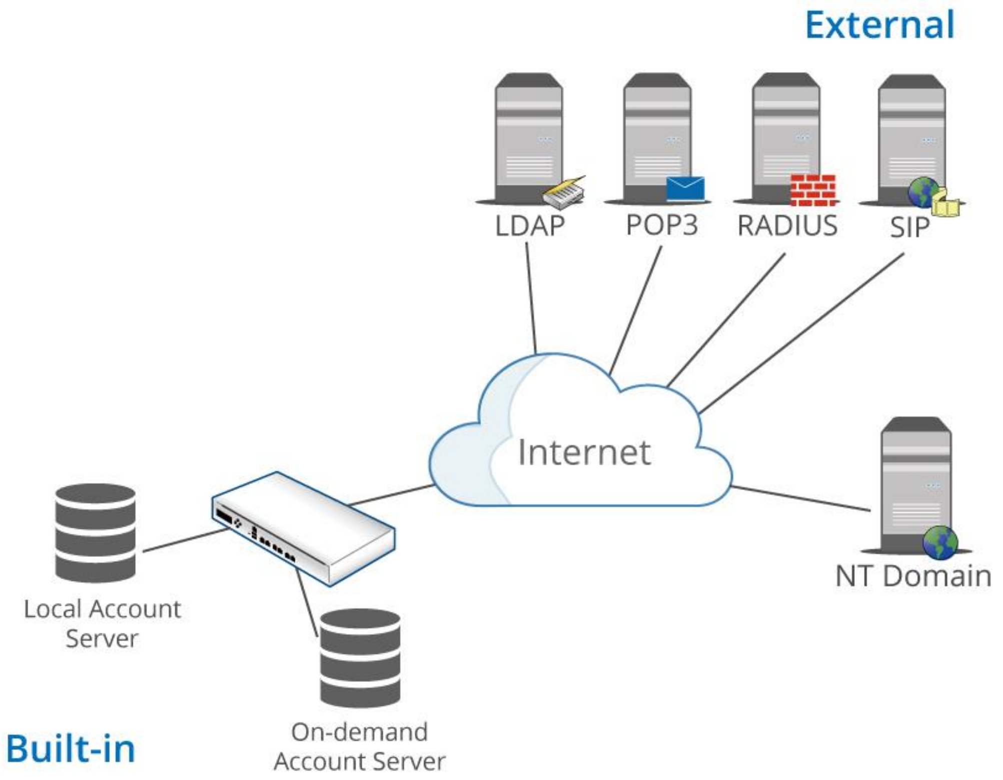
Chapter 4. User Authentication Database

4.1. Authentication Database Configuration

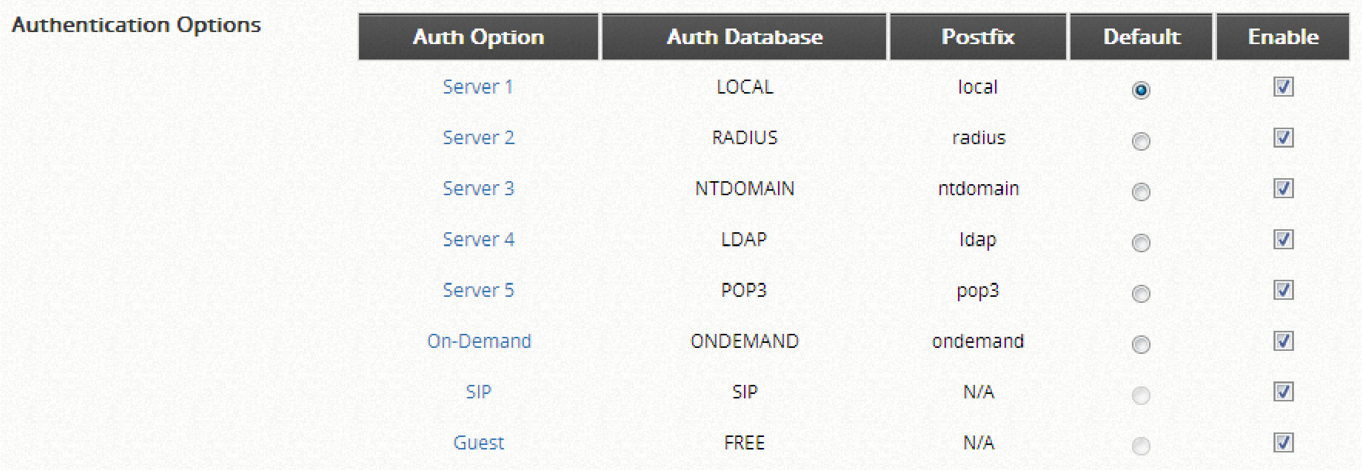
Authentication database is a storage device where users' credentials may be inquired for validity. When a user is associated to an authentication enabled in Service Zone, the EWS controller checks the database to see if the submitted user ID and password combination exists, in order for the user to get network access. 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 (Free) an access option that allows users to access networks with any specified identity token on the login page.

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.**


External
LDAP
POP3
RADIUS
SIP
Internet
NT Domain
Local Account Server
On-demand Account Server
Built-in

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



Authentication Options

Auth Option	Auth Database	Postfix	Default	Enable
Server 1	LOCAL	local	●	☑
Server 2	RADIUS	radius	○	☑
Server 3	NTDOMAIN	ntdomain	○	☑
Server 4	LDAP	ldap	○	☑
Server 5	POP3	pop3	○	☑
On-Demand	ONDEMAND	ondemand	○	☑
SIP	SIP	N/A	○	☑
Guest	FREE	N/A	○	☑

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

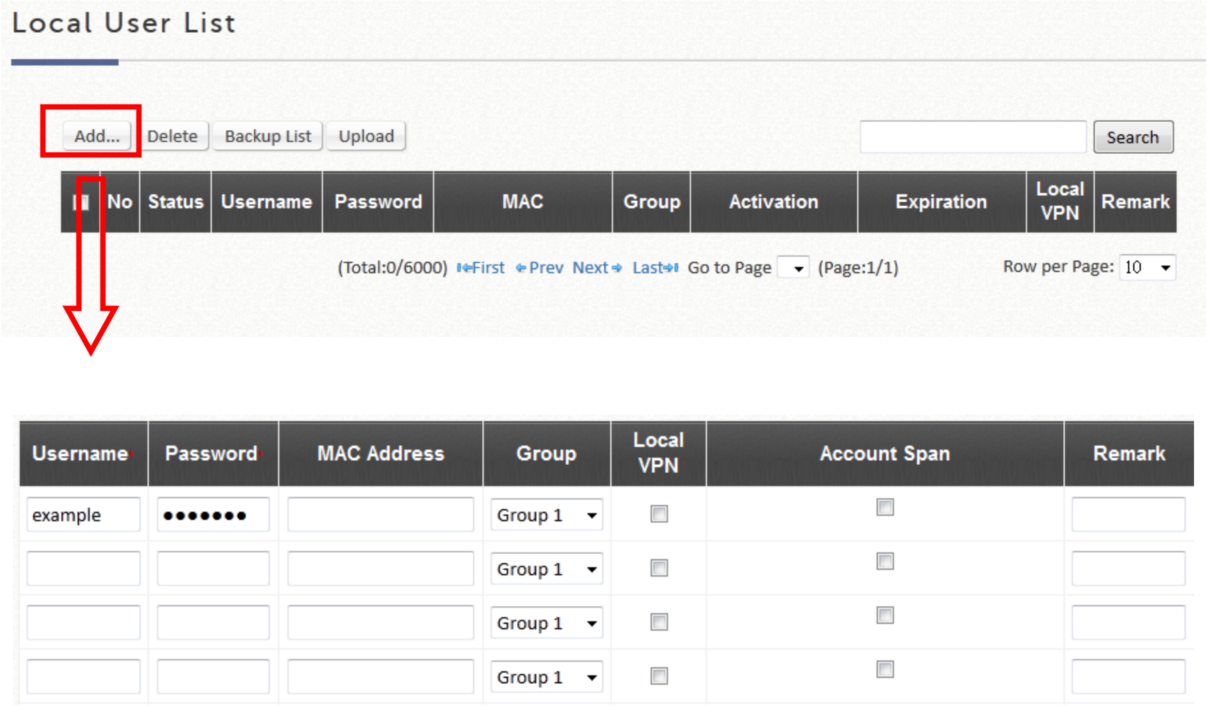
4.2.1. Local User Database

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
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

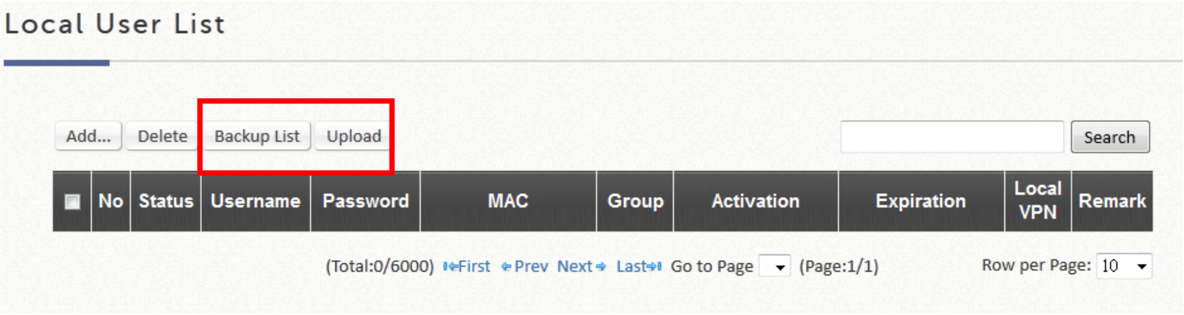
Username	Password	MAC Address	Group	Local VPN	Account Span	Remark
example	•••••••		Group 1	☐	☐	
			Group 1	☐	☐	
			Group 1	☐	☐	
			Group 1	☐	☐	

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 for providing network access to a group of people for a specified amount of time, for instance during a seminar event.

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.

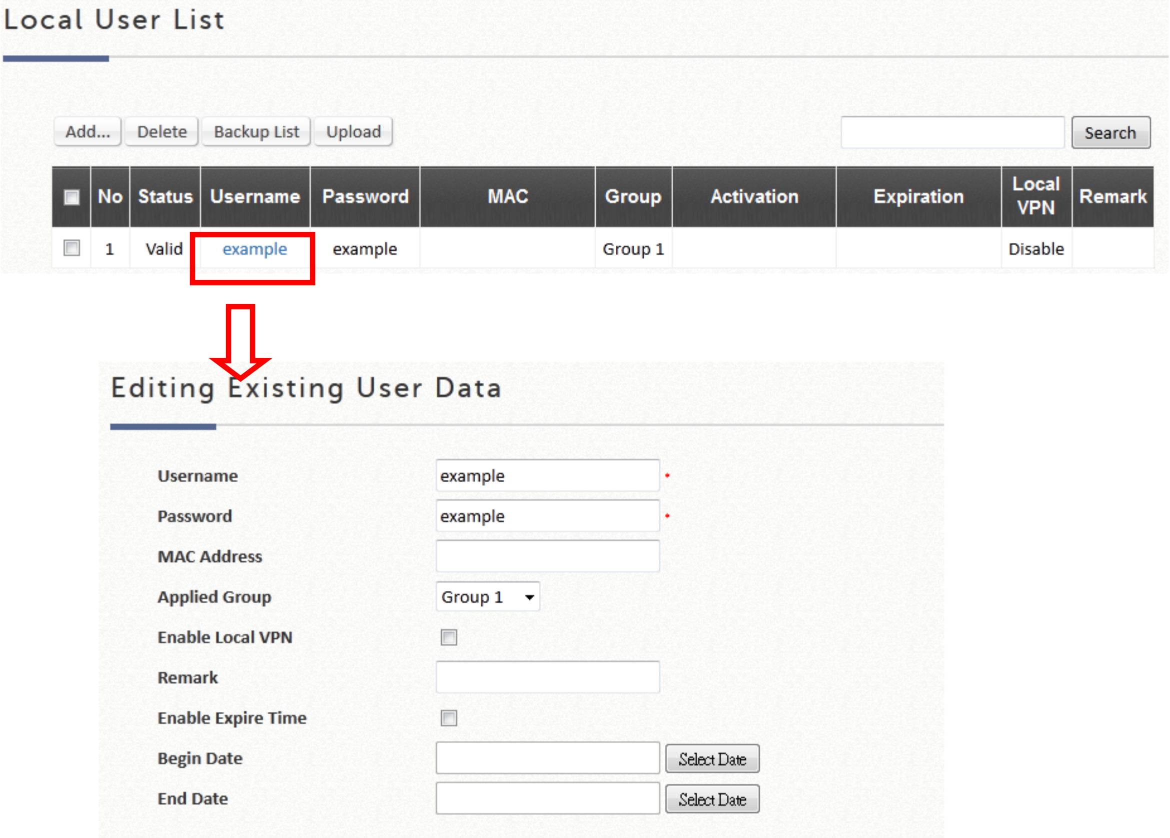

Local User List
Add...
Delete
Backup List
Upload
Search
No
Status
Username
Password
MAC
Group
Activation
Expiration
Local VPN
Remark
(Total:0/6000)
First
Prev
Next
Last
Go to Page
(Page:1/1)
Row per Page: 10

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.

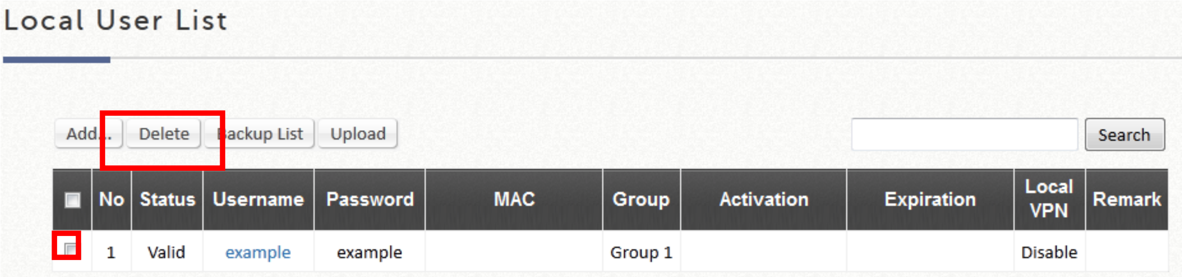

Local User List
Add...
Delete
Backup List
Upload
Search
Editing Existing User Data
Select Date
Select Date

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

Username	example *
Password	example *
MAC Address	
Applied Group	Group 1
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.

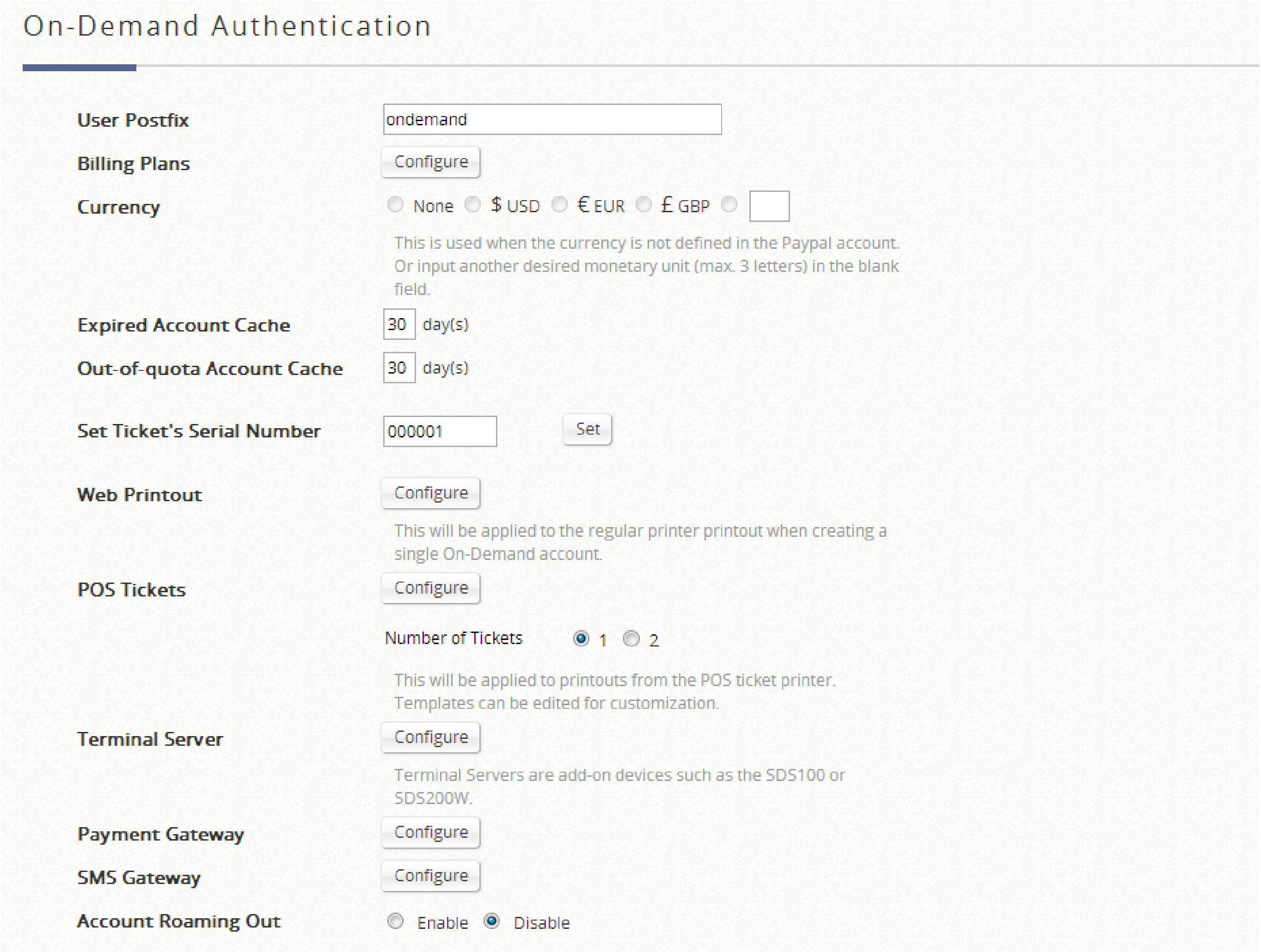


☐	No	Status	Username	Password	MAC	Group	Activation	Expiration	Local VPN	Remark
☐	1	Valid	example	example		Group 1			Disable	

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: ondemand

Billing Plans: Configure

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

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

Expired Account Cache: 30 day(s)

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

Set Ticket's Serial Number: 000001 Set

Web Printout: Configure

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

POS Tickets: Configure

Number of Tickets ● 1 ○ 2

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

Terminal Server: Configure

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

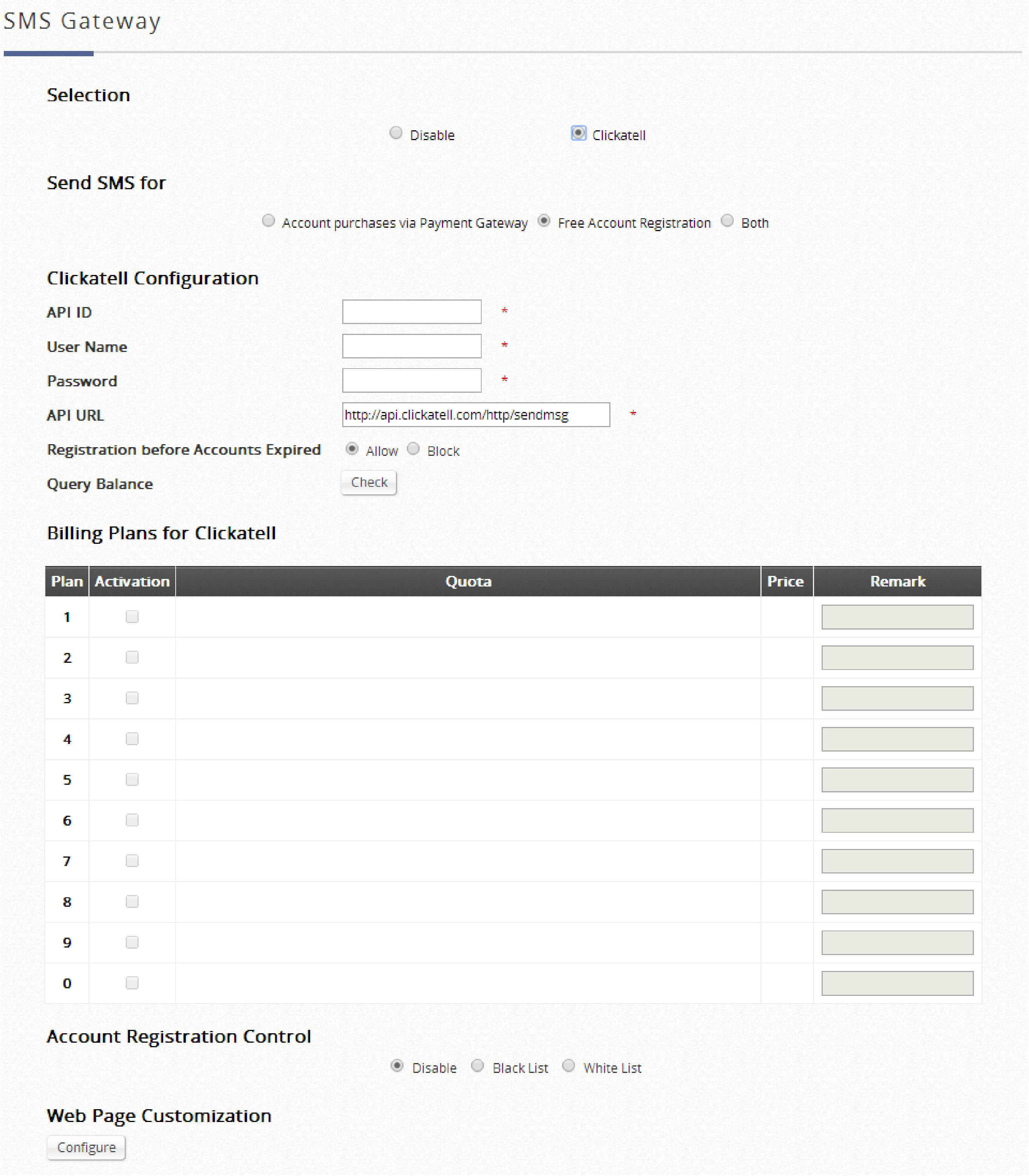
Payment Gateway: Configure

SMS Gateway: Configure

Account Roaming Out: ○ Enable ● 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 Terminal Servers (such as the SDS200W) 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	http://api.clickatell.com/http/sendmsg *
Registration before Accounts Expired	● Allow ○ Block
Query Balance	Check

Billing Plans for Clickatell

Plan	Activation	Quota	Price	Remark
1	☐			
2	☐			
3	☐			
4	☐			
5	☐			
6	☐			
7	☐			
8	☐			
9	☐			
0	☐			

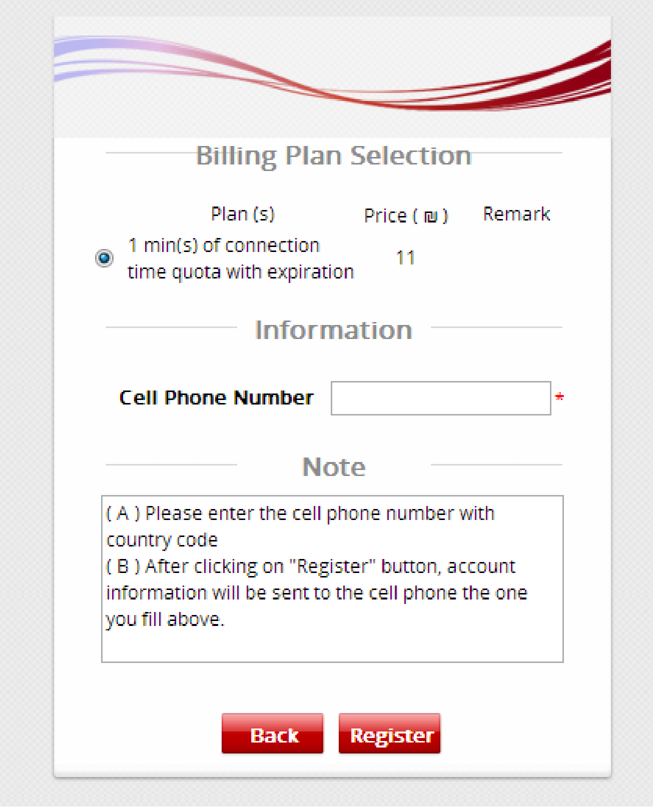
Account Registration Control

● 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:



Billing Plan Selection

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

Information

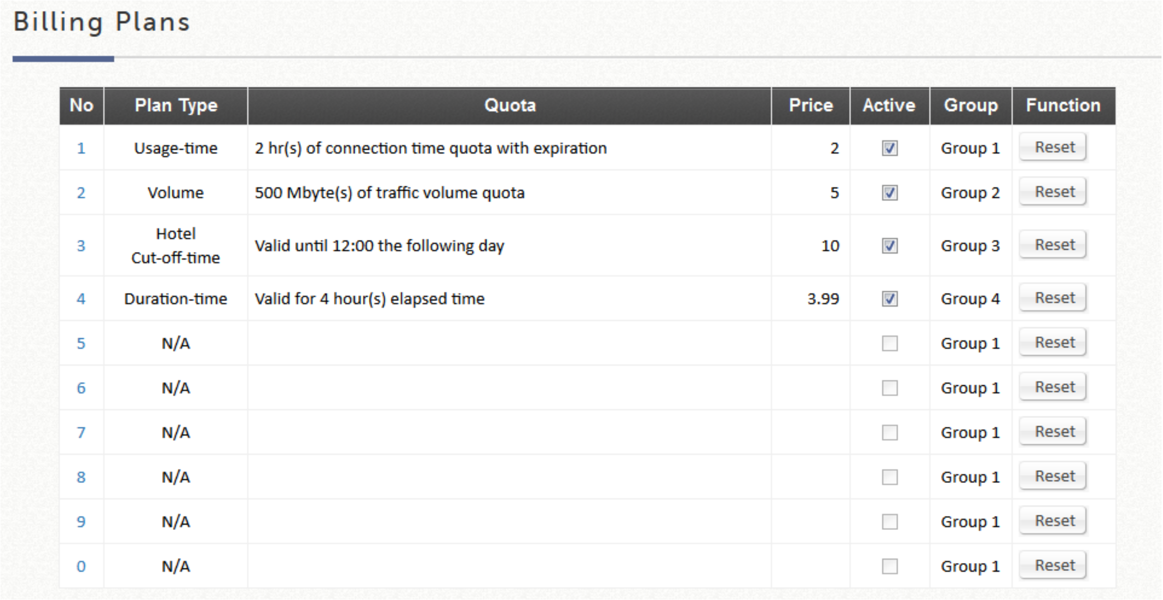
Cell Phone Number ________ *

Note

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

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	☑	Group 1	Reset
2	Volume	500 Mbyte(s) of traffic volume quota	5	☑	Group 2	Reset
3	Hotel Cut-off-time	Valid until 12:00 the following day	10	☑	Group 3	Reset
4	Duration-time	Valid for 4 hour(s) elapsed time	3.99	☑	Group 4	Reset
5	N/A			☐	Group 1	Reset
6	N/A			☐	Group 1	Reset
7	N/A			☐	Group 1	Reset
8	N/A			☐	Group 1	Reset
9	N/A			☐	Group 1	Reset
0	N/A			☐	Group 1	Reset

NOTE

1. For more detailed information on the four major account types, please refer to **Appendix C**.
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.

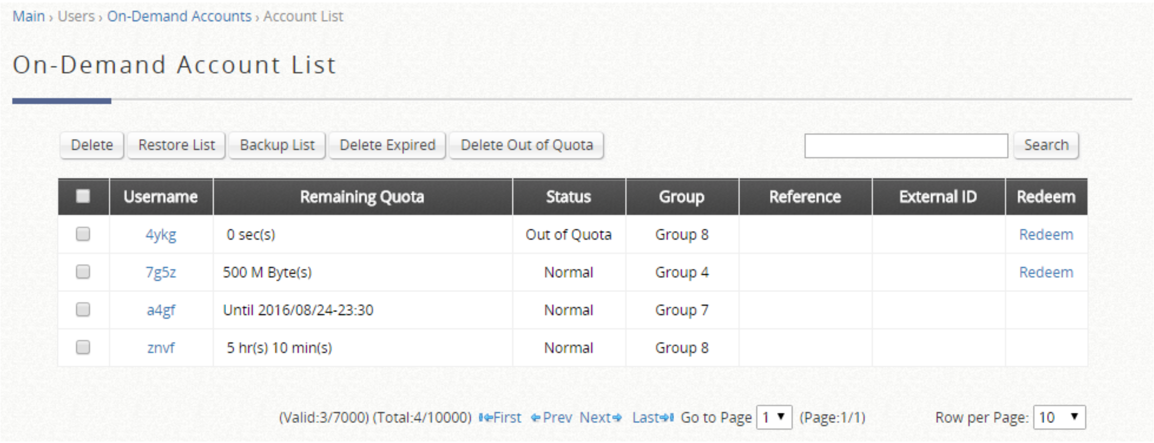
The **On-Demand Accounts List** houses all the existing On-Demand accounts. Each account's status, quota, etc. will be displayed for reference. On-Demand account import, export, deletion and Admin Redeem are also performed on this page.

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

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

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

4.2.3. Guest Authentication

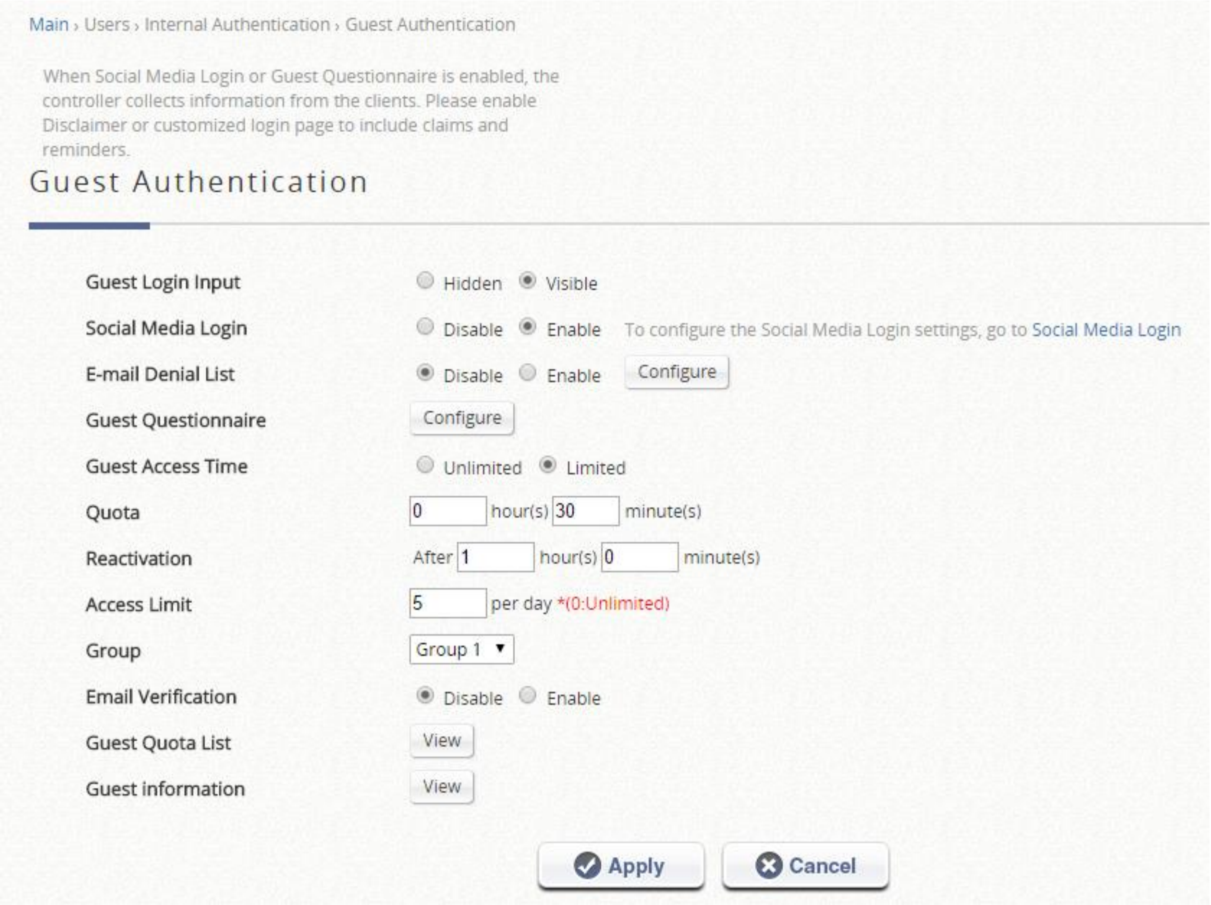
The Guest Authentication Option is not technically a user database, but rather a specially designed option to allow a user to access and surf the network without any user account or password.

This feature allows the user to associate with a particular Service Zone, enter 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.



Main › Users › Internal Authentication › Guest Authentication

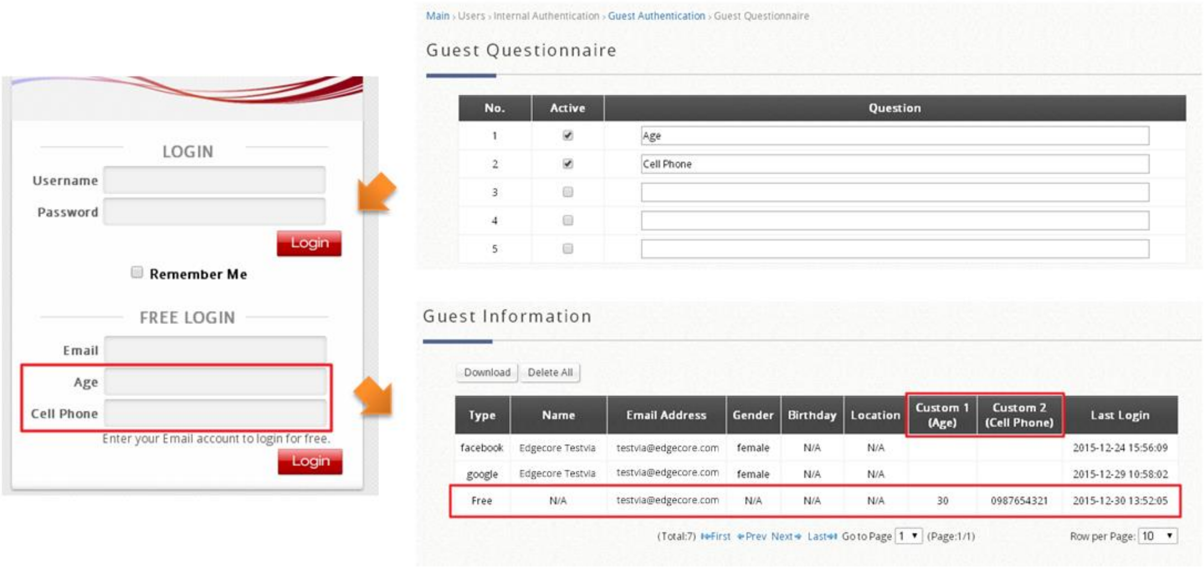
When Social Media Login or Guest Questionnaire is enabled, the controller collects information from the clients. Please enable Disclaimer or customized login page to include claims and reminders.

Guest Authentication

Guest Login Input	○ Hidden ● Visible
Social Media Login	○ Disable ● Enable To configure the Social Media Login settings, go to Social Media Login
E-mail Denial List	● Disable ○ Enable Configure
Guest Questionnaire	Configure
Guest Access Time	○ Unlimited ● Limited
Quota	0 hour(s) 30 minute(s)
Reactivation	After 1 hour(s) 0 minute(s)
Access Limit	5 per day *(0:Unlimited)
Group	Group 1 ▼
Email Verification	● Disable ○ Enable
Guest Quota List	View
Guest information	View

Selecting **Visible** helps administrators enable **Guest Login Input** which allows clients to access internet by entering emails. 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).


LOGIN
Username
Password
Login
Remember Me
FREE LOGIN
Email
Age
Cell Phone
Login
Main › Users › Internal Authentication › Guest Authentication › Guest Questionnaire
Download
Delete All
(Total:7) First Prev Next Last Go to Page 1 (Page:1/1)
Row per Page: 10

☐ Remember Me

Enter your Email account to login for free.

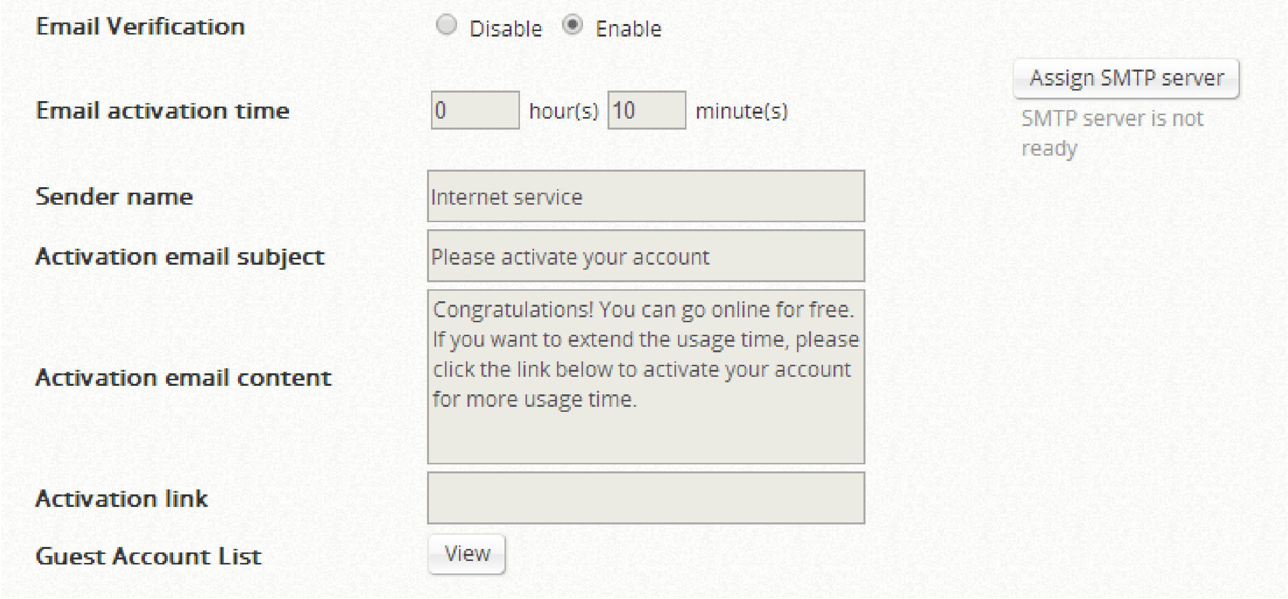
Guest Questionnaire

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

Guest Information

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

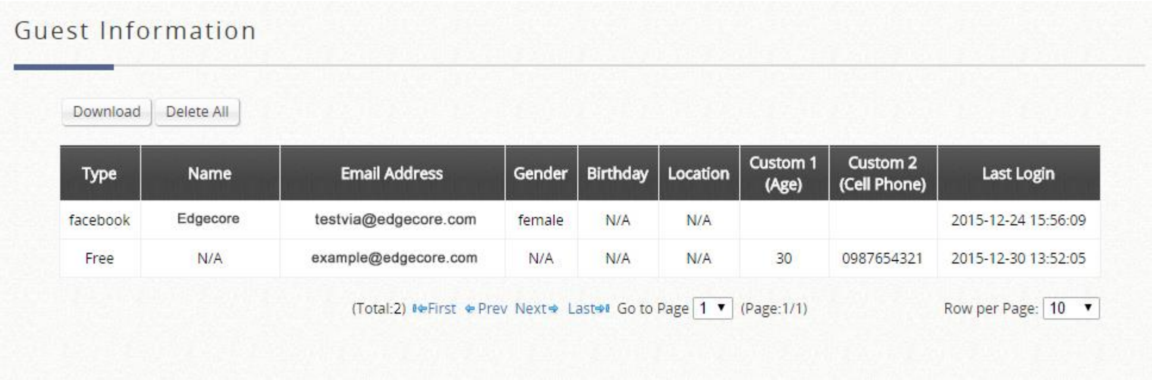
Email verification ensures that the entered email is a valid email address. When this option is enabled, an activation time is allocated to the client. The client then has to activate this account within the activation time to extend his/her usage time by clicking a link in the mail sent by the mail 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	0 hour(s) 10 minute(s)
Sender name	Internet service
Activation email subject	Please activate your account
Activation email content	Congratulations! You can go online for free. If you want to extend the usage time, please click the link below to activate your account for more usage time.
Activation link	
Guest Account List	View

Step2: Setting up Social Media Login profile.

Edgecore EWS Controllers also provide a convenient method for guest authentication; **Social Media Login** enables client to access internet by logging in with their own Social Media Accounts such as Facebook, Google+, and Open ID. The detail configuration can be done with the hyperlink to **Social Media Login** with these application registration IDs or secrets (see 4.3.6 Social Media). Some information of the accounts are available for collection in the **Guest Information** list for administrators' further analysis or marketing purposes. Account names, account emails, gender, birthdays, and location on the Social Media Account List are downloadable for administrators' data manipulation (if Social Medias permit to provide). Guest Questionnaire answer sheets are displayed over following custom columns as well.



Guest Information

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

(Total:2) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 10

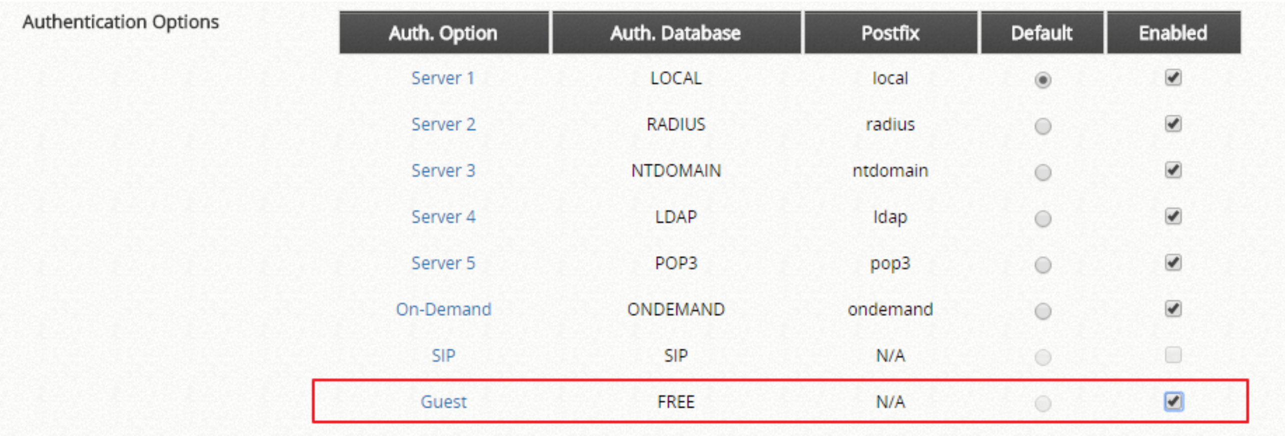
Administrators are able to download the collected guest information by clicking “Download” button, besides, a ”Delete All” button is available for deleting all the stored data. Administrator can delete all entries after export to keep the list up-to-date.

NOTE

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

Step3: 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.



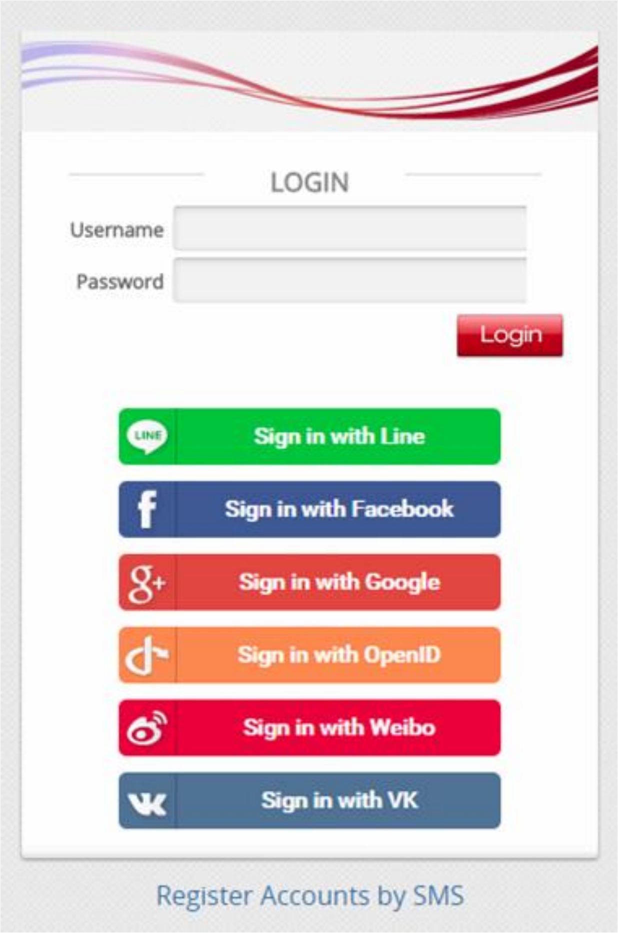
Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	●	☑
Server 2	RADIUS	radius	○	☑
Server 3	NTDOMAIN	ntdomain	○	☑
Server 4	LDAP	ldap	○	☑
Server 5	POP3	pop3	○	☑
On-Demand	ONDEMAND	ondemand	○	☑
SIP	SIP	N/A	○	☐
Guest	FREE	N/A	○	☑

Consequently, after going through configurations from STEP 1 to STEP 3, end users will see that the an additional section for guest access will show on the Service Zone’s login page.

By typing an email address and click login or by clicking Social Media Login button, 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.


LOGIN
Username
Password
Login
Sign in with Line
Sign in with Facebook
Sign in with Google
Sign in with OpenID
Sign in with Weibo
Sign in with VK
Register Accounts by SMS

4.3. External Authentication Options

Most organizations have already established a centralized user account servers. Consequently, 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.

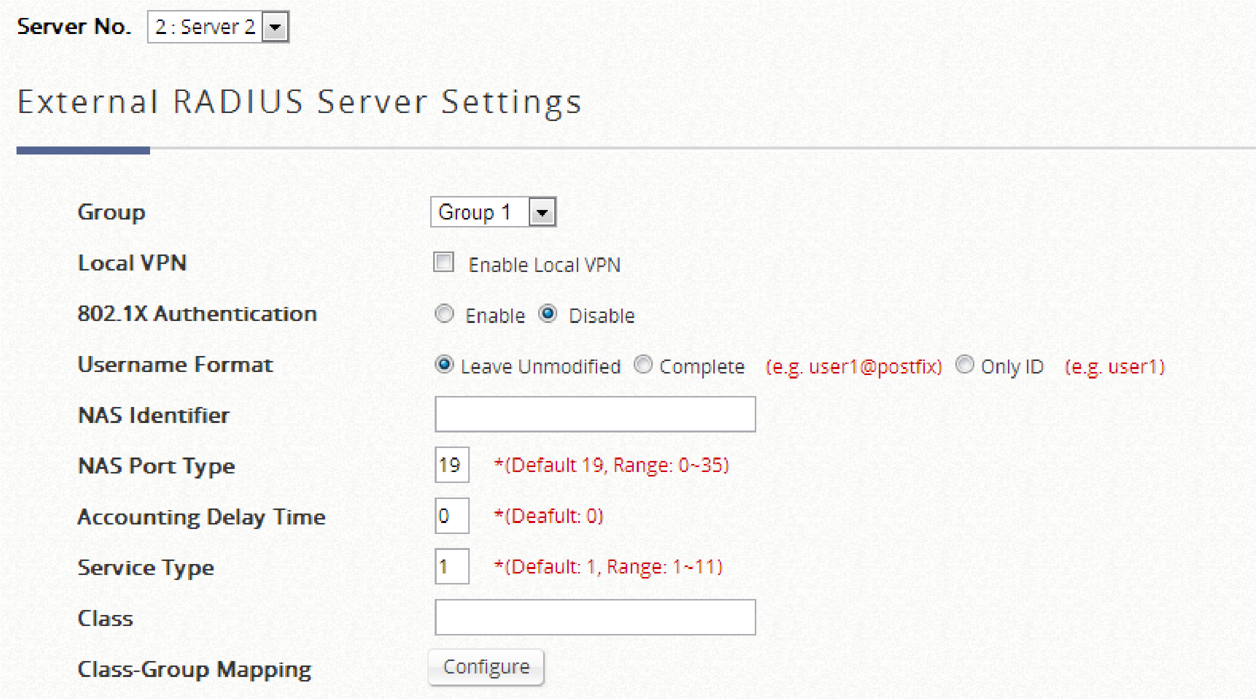
NOTE

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



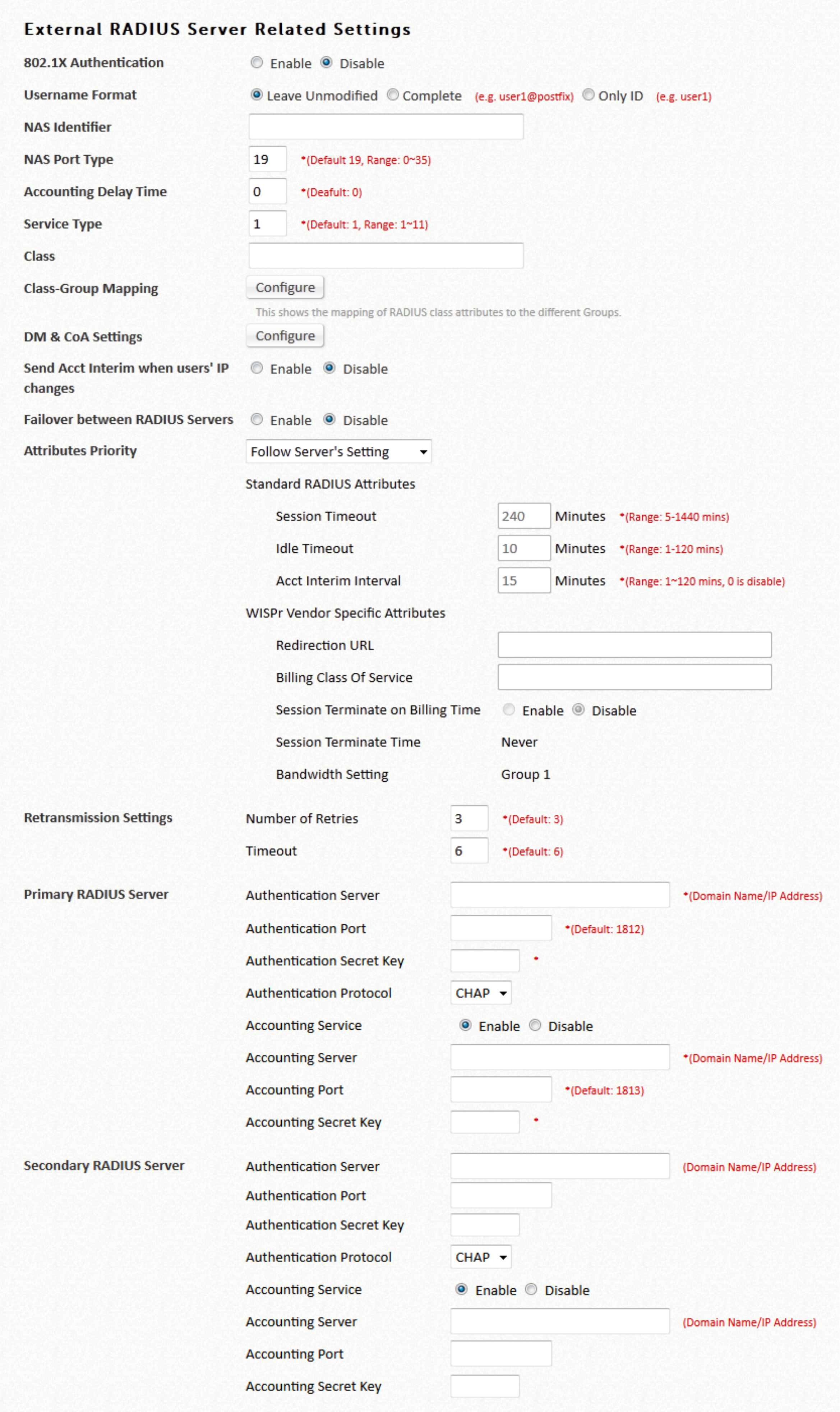
Server No. 2 : Server 2

External RADIUS Server Settings

Group	Group 1
Local VPN	☐ Enable Local VPN
802.1X Authentication	○ Enable ● Disable
Username Format	● Leave Unmodified ○ Complete (e.g. user1@postfix) ○ Only ID (e.g. user1)
NAS Identifier	
NAS Port Type	19 *(Default 19, Range: 0~35)
Accounting Delay Time	0 *(Deafult: 0)
Service Type	1 *(Default: 1, Range: 1~11)
Class	
Class-Group Mapping	Configure

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 19 *(Default 19, Range: 0~35)

Accounting Delay Time 0 *(Deafult: 0)

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

Class

Class-Group Mapping Configure

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

DM & CoA Settings Configure

Send Acct Interim when users' IP changes ○ Enable ● Disable

Failover between RADIUS Servers ○ Enable ● Disable

Attributes Priority Follow Server's Setting

Standard RADIUS Attributes

- Session Timeout 240 Minutes *(Range: 5-1440 mins)
- Idle Timeout 10 Minutes *(Range: 1-120 mins)
- Acct Interim Interval 15 Minutes *(Range: 1~120 mins, 0 is disable)

WISPr Vendor Specific Attributes

- Redirection URL
- Billing Class Of Service
- Session Terminate on Billing Time ○ Enable ● Disable
- Session Terminate Time Never
- Bandwidth Setting Group 1

Retransmission Settings

- Number of Retries 3 *(Default: 3)
- Timeout 6 *(Default: 6)

Primary RADIUS Server

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

Secondary RADIUS Server

- Authentication Server (Domain Name/IP Address)
- Authentication Port
- Authentication Secret Key
- Authentication Protocol CHAP
- Accounting Service ● Enable ○ Disable
- Accounting Server (Domain Name/IP Address)
- Accounting Port
- Accounting Secret Key

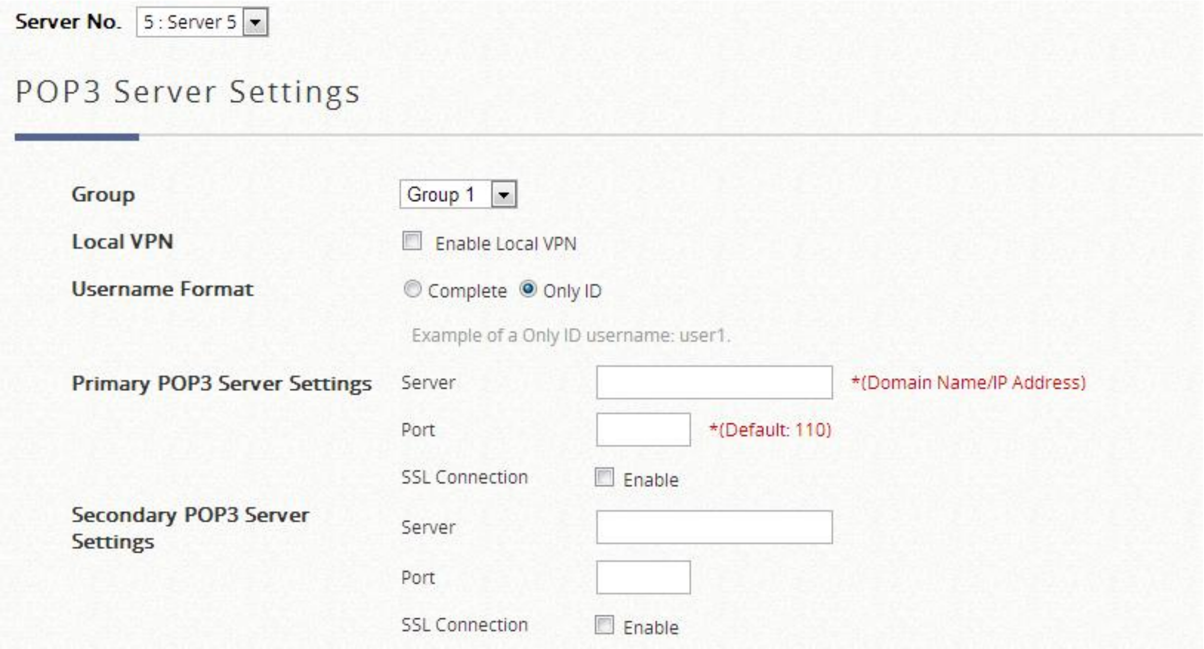
Another important setting field is the **Class-Group Mapping** on the page. It is a translation setting which maps RADIUS classes to different groups on the EWS controller, enabling different RADIUS accounts to be incorporated into different Groups.

4.3.2. POP3

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

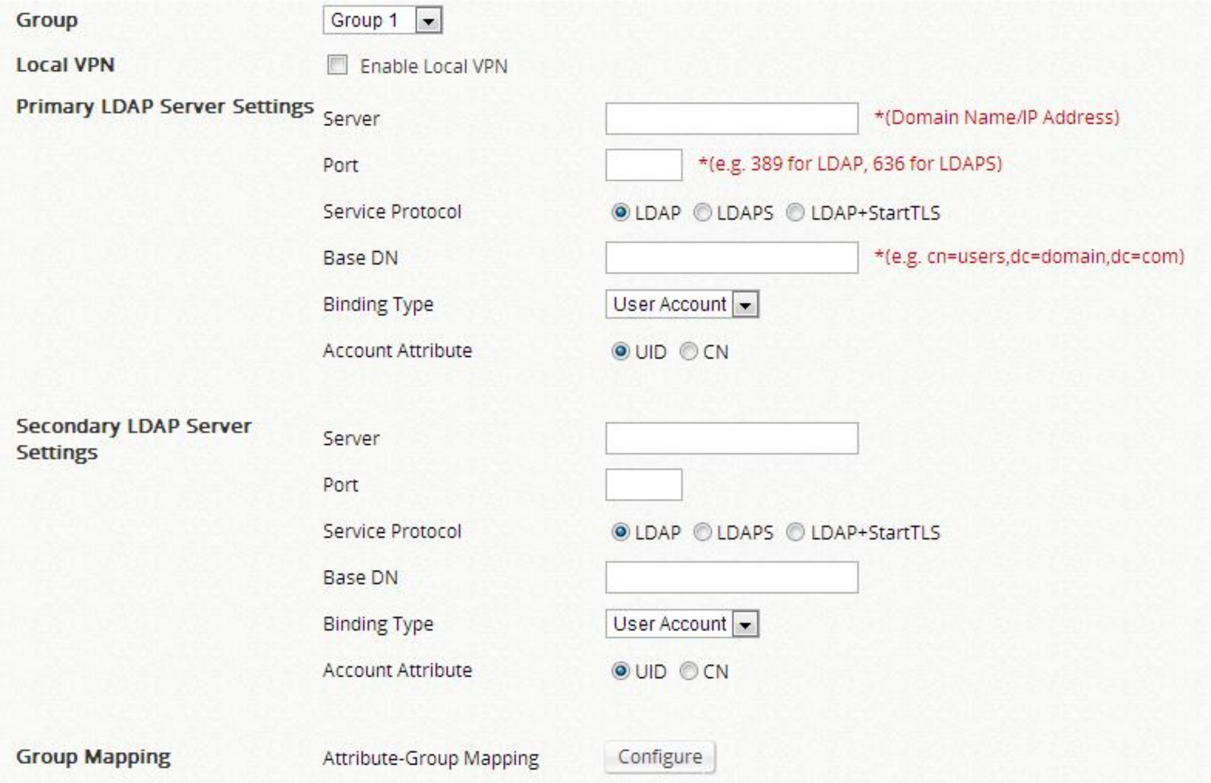
4.3.3. LDAP

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

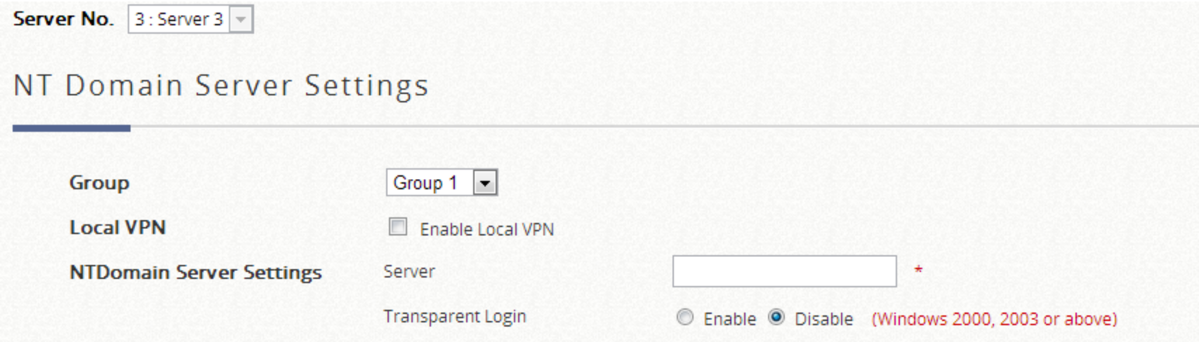


Group	Group 1 ▾	
Local VPN	☐ Enable Local VPN	
Primary LDAP Server Settings	Server	*(Domain Name/IP Address)
	Port	*(e.g. 389 for LDAP, 636 for LDAPS)
	Service Protocol	● LDAP ○ LDAPS ○ LDAP+StartTLS
	Base DN	*(e.g. cn=users,dc=domain,dc=com)
	Binding Type	User Account ▾
	Account Attribute	● UID ○ CN
Secondary LDAP Server Settings	Server	
	Port	
	Service Protocol	● LDAP ○ LDAPS ○ LDAP+StartTLS
	Base DN	
	Binding Type	User Account ▾
	Account Attribute	● UID ○ CN
Group Mapping	Attribute-Group Mapping	Configure

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. EWS controllers support SIP authentication as well as the use of SIP phones. In addition to an EWS controller, admin has to set up other devices as to making successful SIP phone calls. This includes: A valid SIP Registrar, SIP phones.

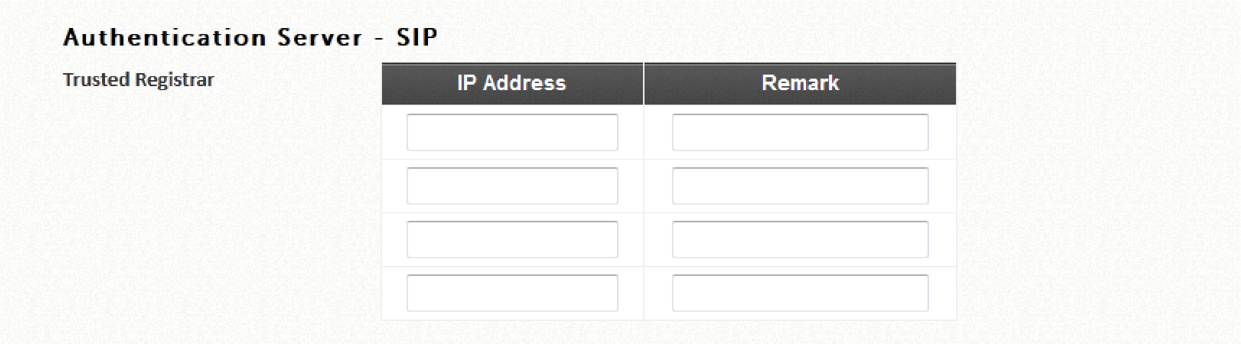
(1) A user is making a call through a SIP-based phone (e.g. #301 --> #303).

(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.

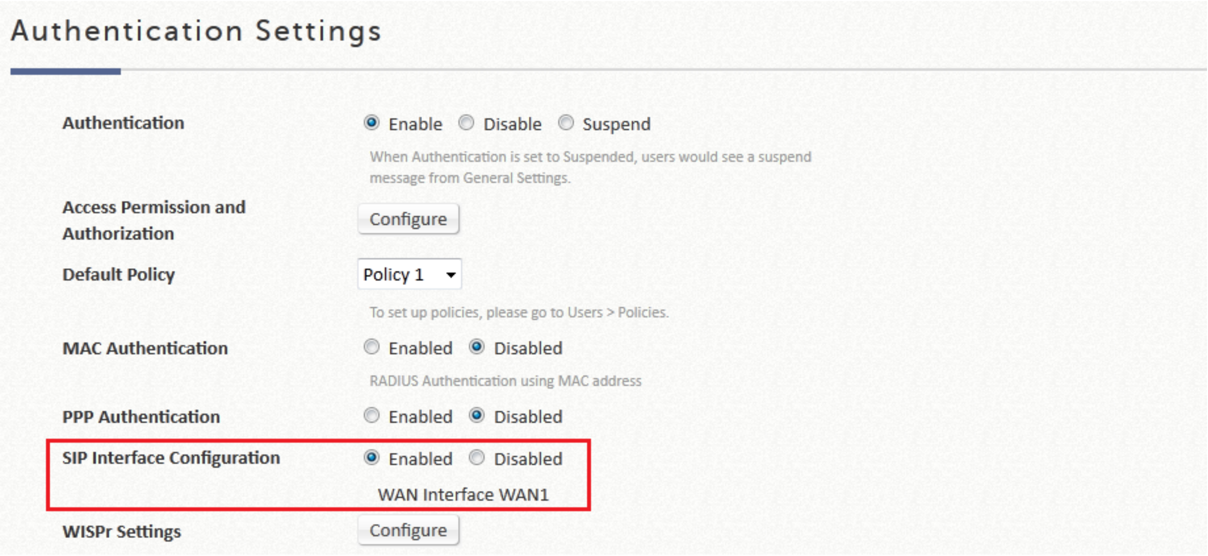


Authentication Server - SIP

Trusted Registrar

IP Address	Remark

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

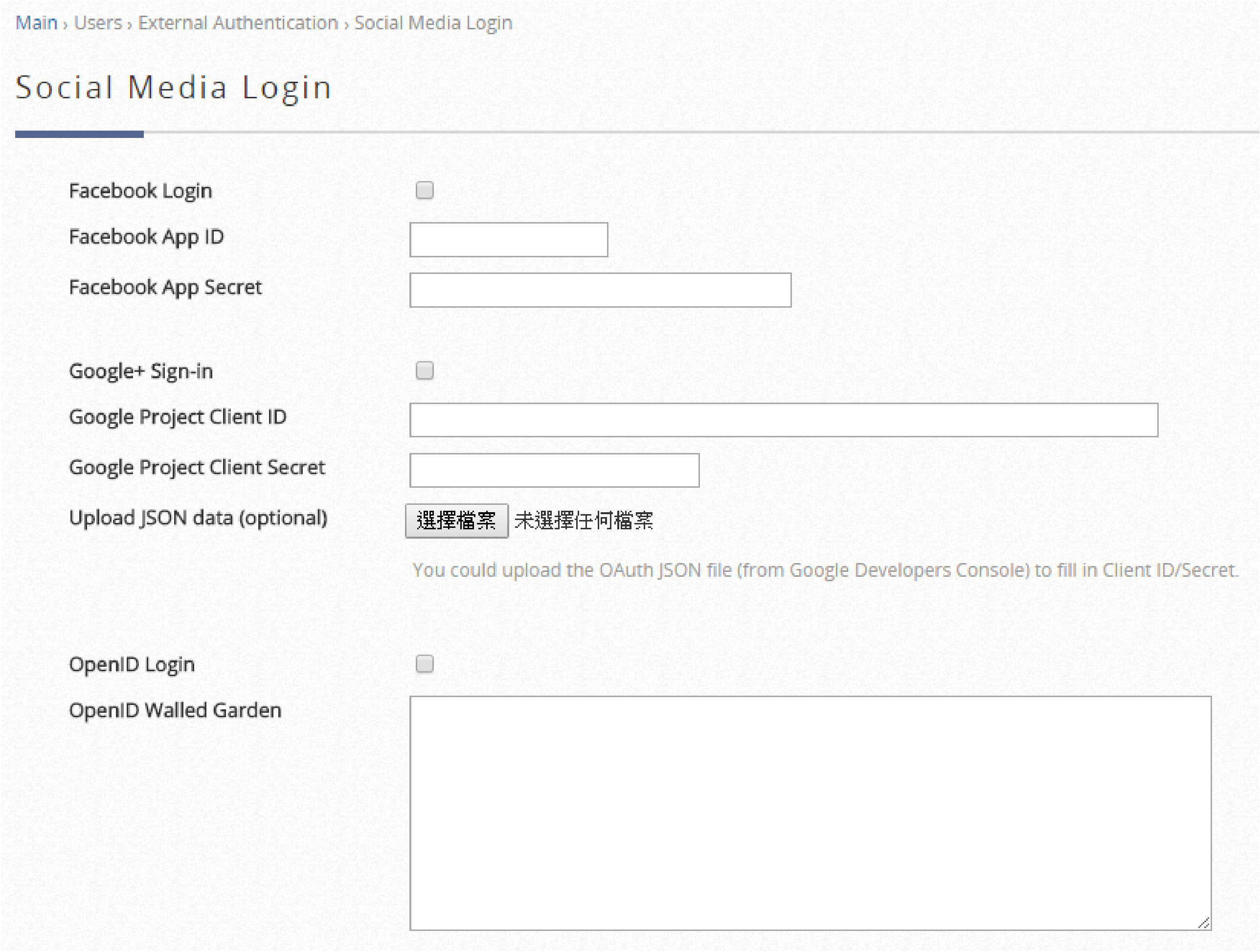


Authentication Settings

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 WAN Interface WAN1
WISPr Settings	Configure

4.3.6. Social Media

Social Media Login allows Wi-Fi users to access internet without going through a tedious account registration process. EWS Controller supports several kinds of social media accounts such as Facebook, Google+ and Open ID. All administrators have to do is to apply the corresponding ID and secret.



Main › Users › External Authentication › Social Media Login

Social Media Login

Facebook Login	☐
Facebook App ID	
Facebook App Secret	
Google+ Sign-in	☐
Google Project Client ID	
Google Project Client Secret	
Upload JSON data (optional)	選擇檔案 未選擇任何檔案 You could upload the OAuth JSON file (from Google Developers Console) to fill in Client ID/Secret.
OpenID Login	☐
OpenID Walled Garden	

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

- Facebook: visit the website at Facebook developers site (https://developers.facebook.com/) and apply for “Facebook Login” APP to get the app ID and app secret.
- Google+: visit the website at Google Developers Console (https://console.developers.google.com/) and apply for “Google+ API” to get the client ID and secret.
- Open ID: the login path must be traversed and added into OpenID Walled Garden and the redirection target depends on OpenID provider.

Chapter 5. Group Attributes & Policy Rules

All 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 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, EWS controllers also offer Group assignment per account for RADIUS and LDAP option via Class-Group Mapping and Attribute-Group Mapping respectively.

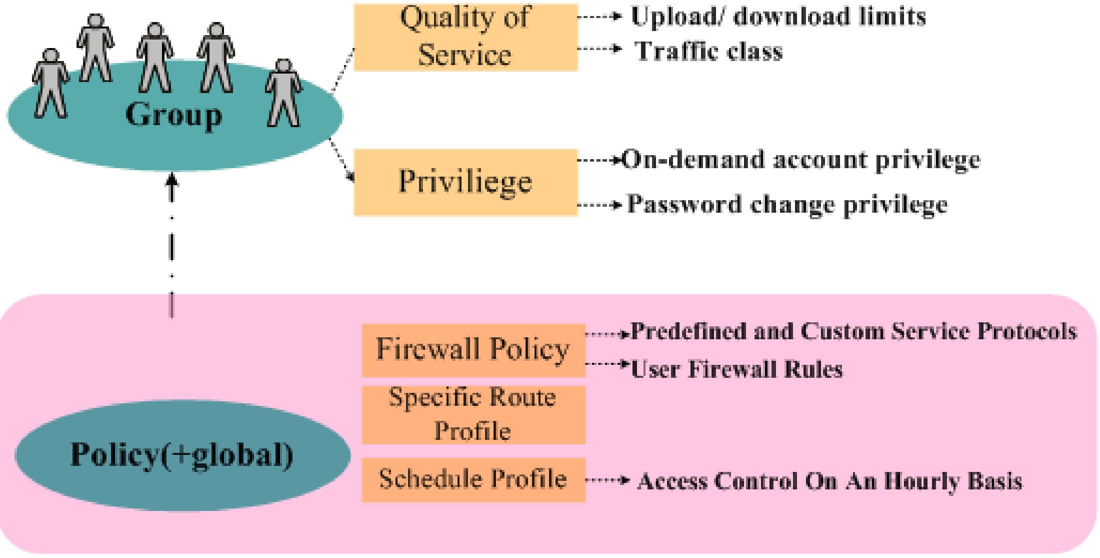
In each Group profile, there are several attributes that can be defined by administrator:

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 privileg*e 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.

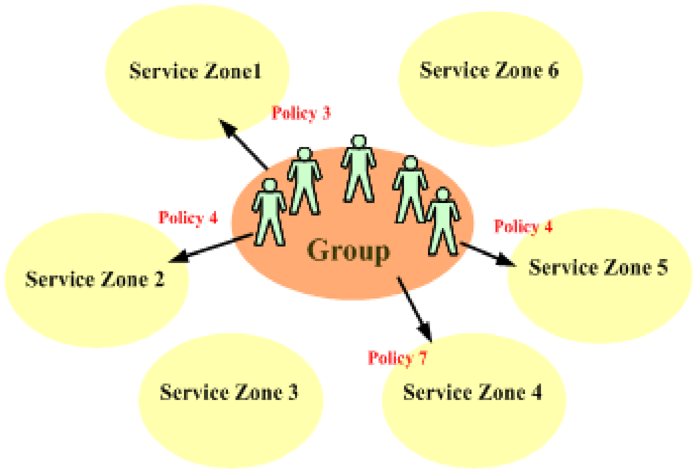
- **Policy**

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.

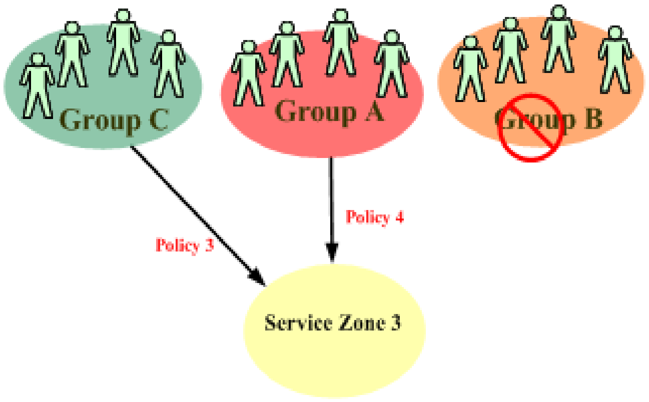
- **Relationship Between Group, Policy, and Service Zones**


Group
Quality of Service
Upload/ download limits
Traffic class
Privilege
On-demand account privilege
Password change privilege
Policy(+global)
Firewall Policy
Predefined and Custom Service Protocols
User Firewall Rules
Specific Route Profile
Schedule Profile
Access Control On An Hourly Basis

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:


Service Zone1
Service Zone 6
Policy 3
Policy 4
Group
Policy 4
Service Zone 2
Service Zone 5
Policy 7
Service Zone 3
Service Zone 4

*Admin can impose a group with different policies in different service zones


Group C
Group A
Group B
Policy 3
Policy 4
Service Zone 3

*One service zone can allow many groups to come in (association) with different policies enforced on each one

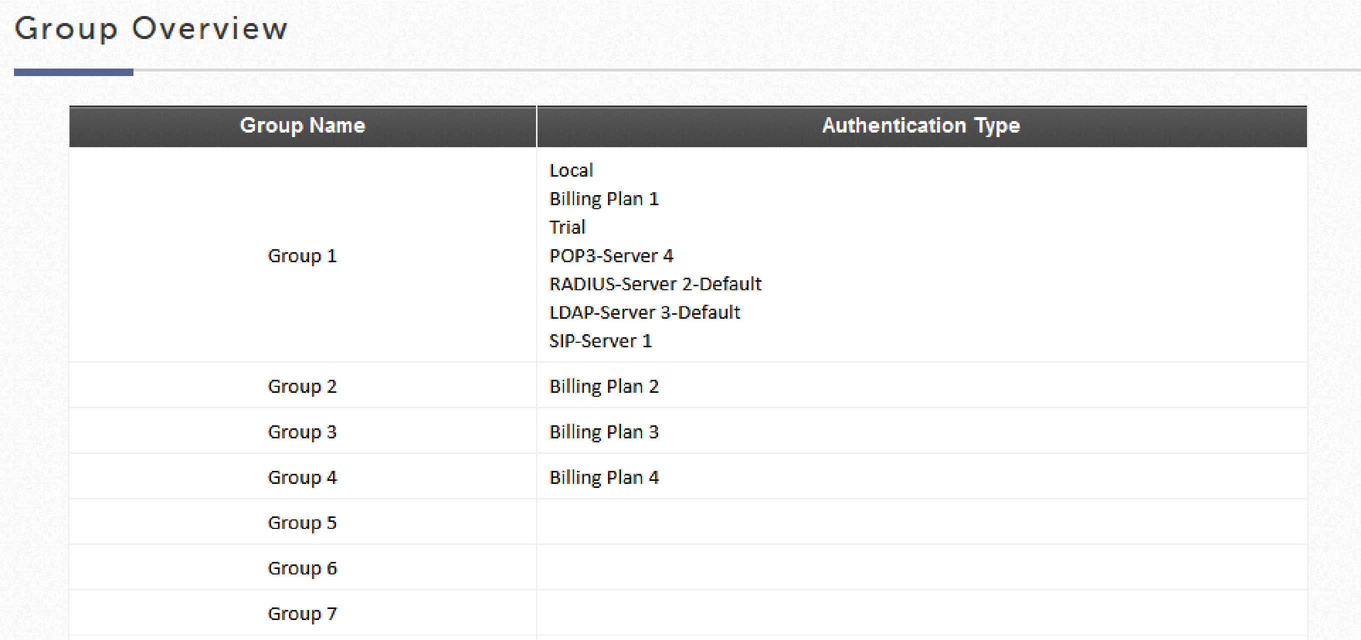
5.2 Practical Setups of Group and Policies

This section demonstrates with screenshots on how to practically set up the groups and policies on the WMI of the 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

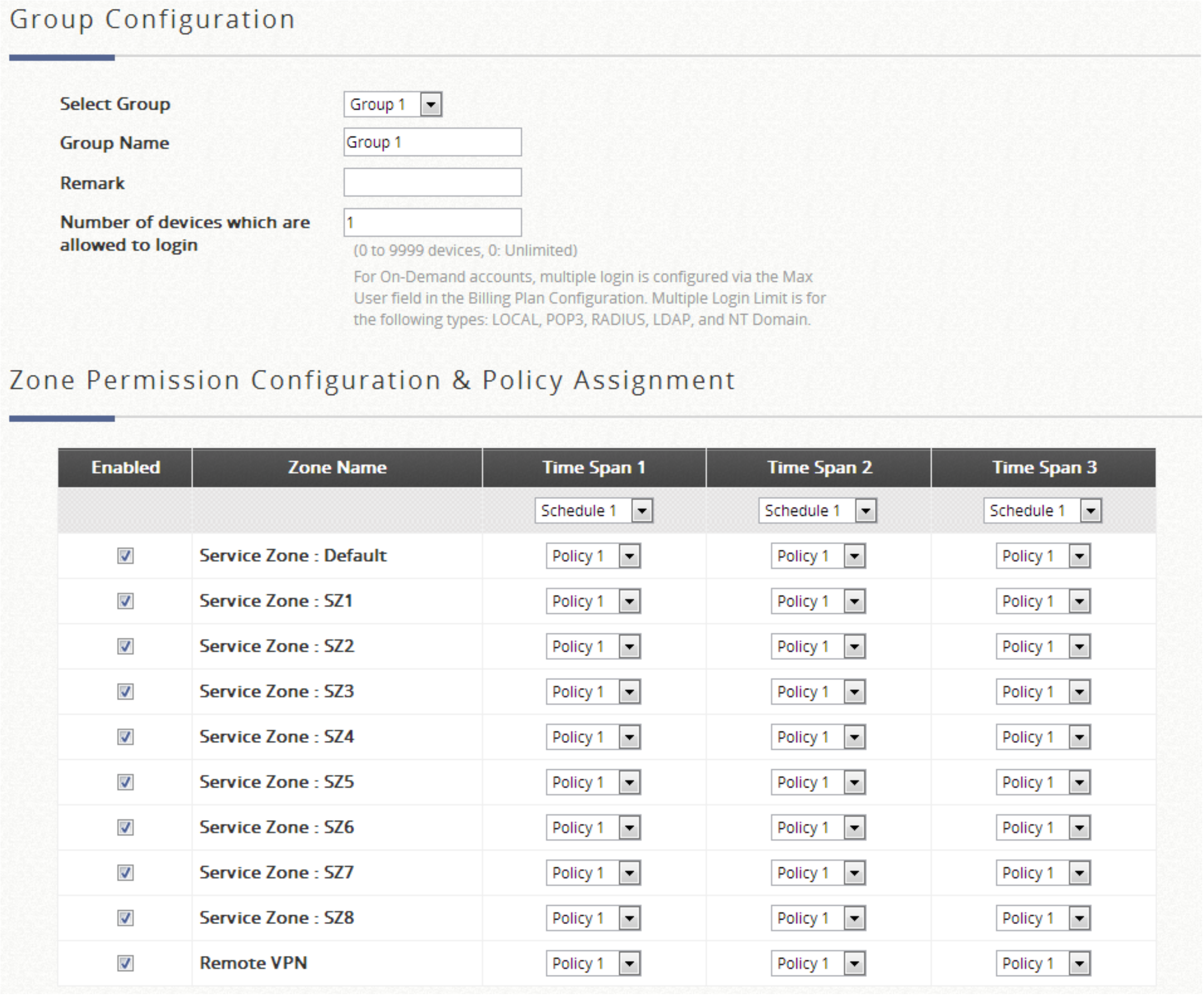
Group Name	Authentication Type
Group 1	Local Billing Plan 1 Trial POP3-Server 4 RADIUS-Server 2-Default LDAP-Server 3-Default SIP-Server 1
Group 2	Billing Plan 2
Group 3	Billing Plan 3
Group 4	Billing Plan 4
Group 5	
Group 6	
Group 7	

- **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.



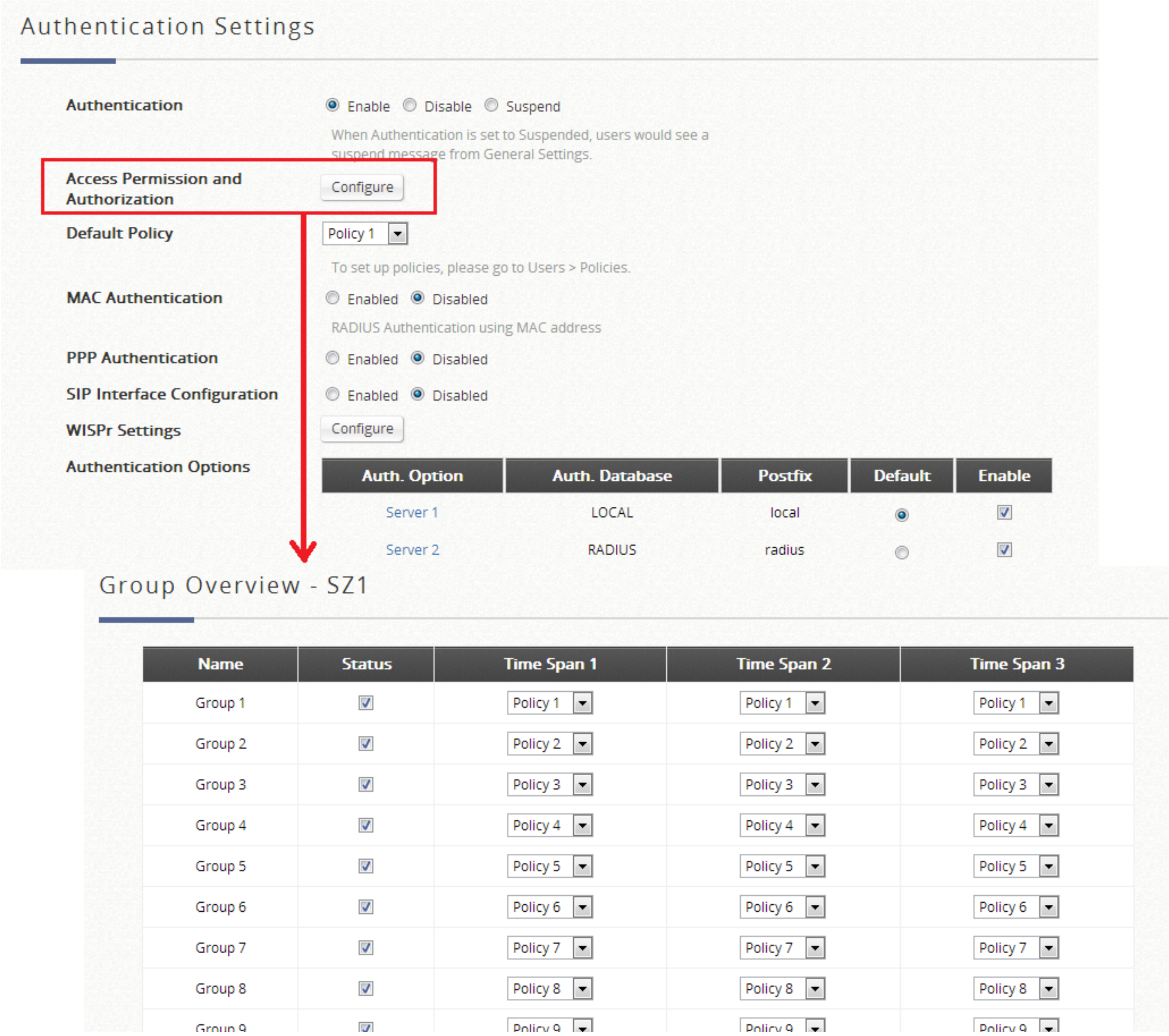
Group Configuration

Select Group	Group 1
Group Name	Group 1
Remark	
Number of devices which are allowed to login	1 (0 to 9999 devices, 0: Unlimited) For On-Demand accounts, multiple login is configured via the Max User field in the Billing Plan Configuration. Multiple Login Limit is for the following types: LOCAL, POP3, RADIUS, LDAP, and NT Domain.

Zone Permission Configuration & Policy Assignment

Enabled	Zone Name	Time Span 1	Time Span 2	Time Span 3
		Schedule 1	Schedule 1	Schedule 1
☑	Service Zone : Default	Policy 1	Policy 1	Policy 1
☑	Service Zone : SZ1	Policy 1	Policy 1	Policy 1
☑	Service Zone : SZ2	Policy 1	Policy 1	Policy 1
☑	Service Zone : SZ3	Policy 1	Policy 1	Policy 1
☑	Service Zone : SZ4	Policy 1	Policy 1	Policy 1
☑	Service Zone : SZ5	Policy 1	Policy 1	Policy 1
☑	Service Zone : SZ6	Policy 1	Policy 1	Policy 1
☑	Service Zone : SZ7	Policy 1	Policy 1	Policy 1
☑	Service Zone : SZ8	Policy 1	Policy 1	Policy 1
☑	Remote VPN	Policy 1	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	●	☑
Server 2	RADIUS	radius	○	☑

Group Overview - SZ1

Name	Status	Time Span 1	Time Span 2	Time Span 3
Group 1	☑	Policy 1	Policy 1	Policy 1
Group 2	☑	Policy 2	Policy 2	Policy 2
Group 3	☑	Policy 3	Policy 3	Policy 3
Group 4	☑	Policy 4	Policy 4	Policy 4
Group 5	☑	Policy 5	Policy 5	Policy 5
Group 6	☑	Policy 6	Policy 6	Policy 6
Group 7	☑	Policy 7	Policy 7	Policy 7
Group 8	☑	Policy 8	Policy 8	Policy 8
Group 9	☑	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.

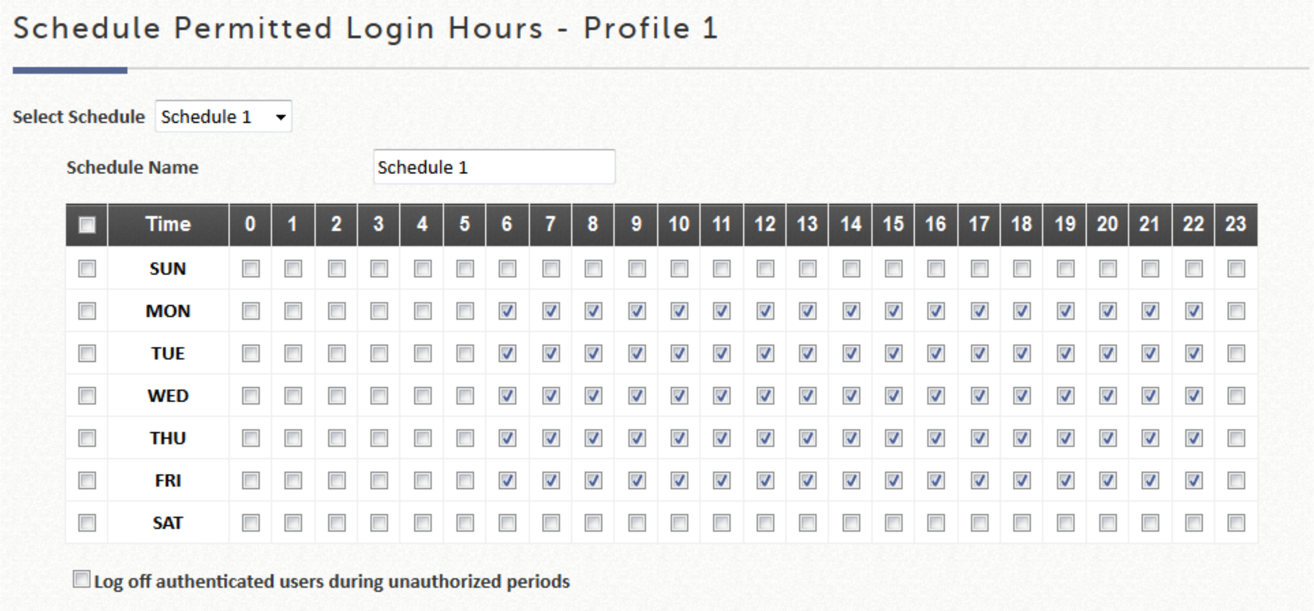
5. *Specific Route Profile is* where the administrator may statically assign routing nodes to forward traffic to a certain destination.
6. *IPv6 traffic class and 802.1p mapping* (for global policy only) - to map IPv6 traffic class to 802.1p when IPv6 traffic is being forwarded into VLAN IPv4 networks.

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 1

Schedule Name: Schedule 1

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

☐ Log off authenticated users during unauthorized periods

Defined Schedules are then applied in Group Configuration.

- **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)

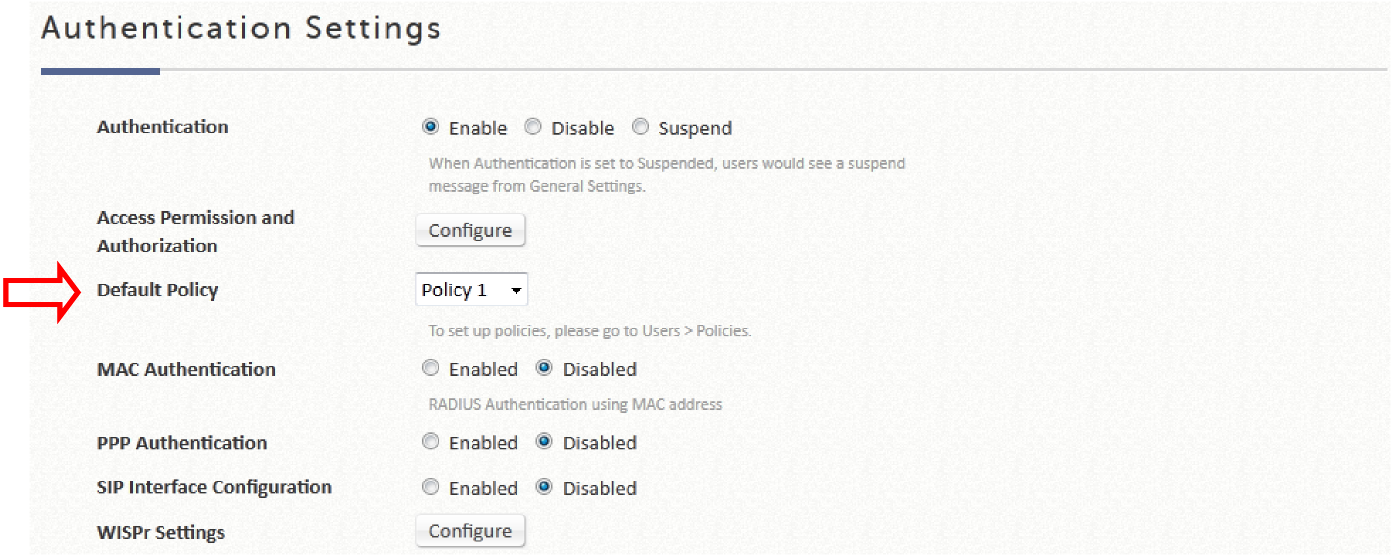
- On-Demand accounts may be assigned a Group per account individually upon creation.

- 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

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

The Policy enforcement priority is as follows:

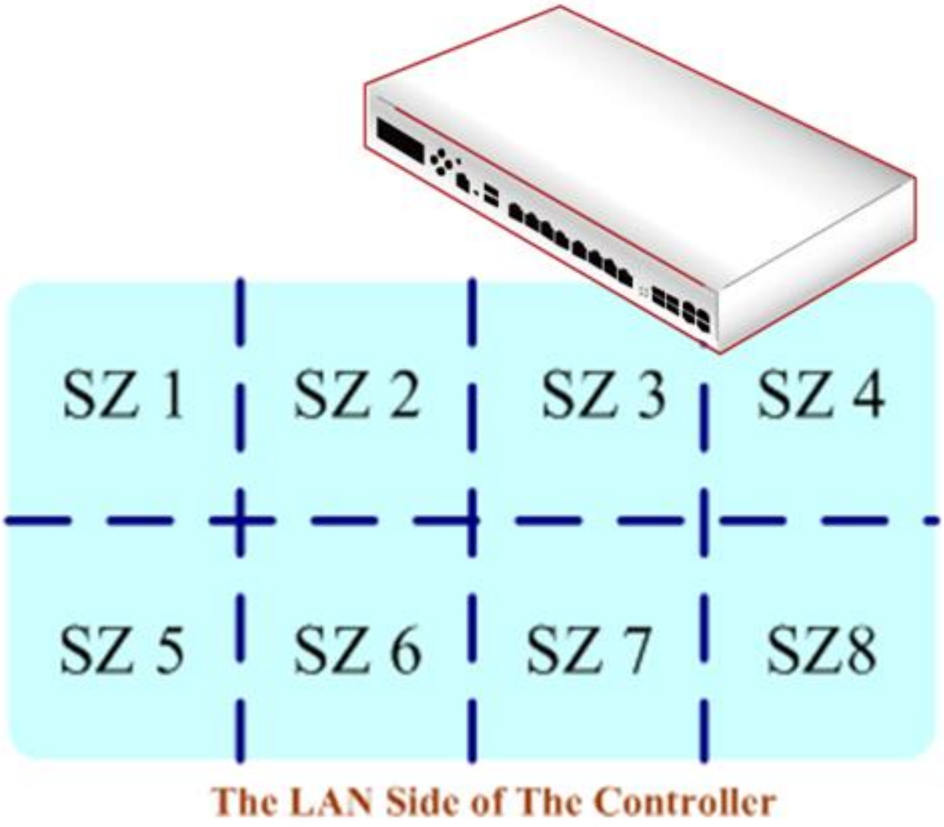
Group-Service Zone Mapping > Service Zone default Policy > Global Policy

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

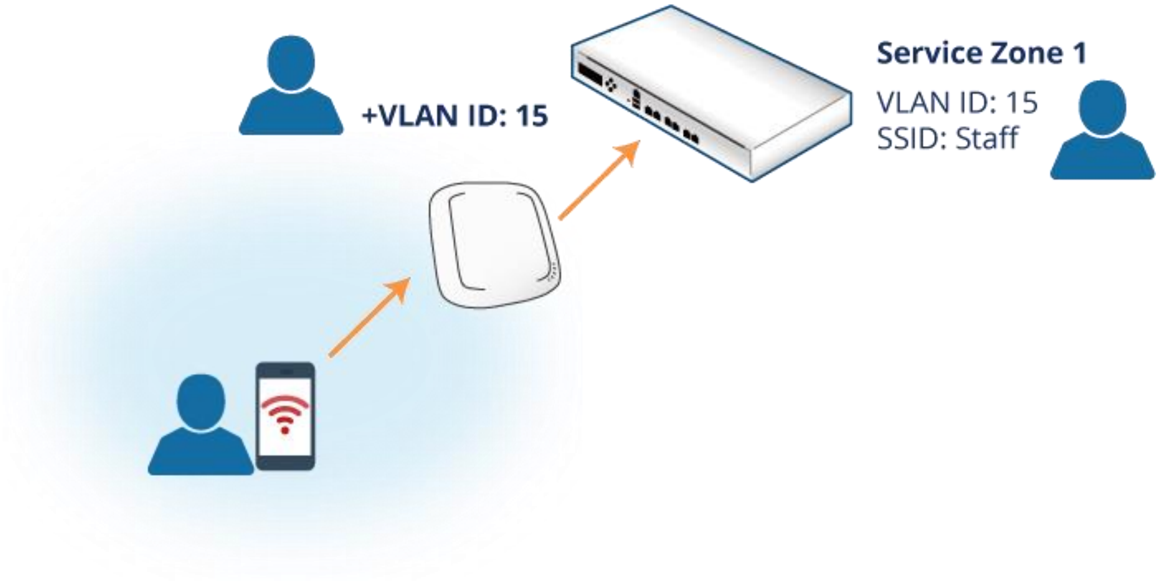


6.2 Service Zone Setup

6.2.1. Tag-based or Port-based Service Zones

EWS controllers offer two modes of physical LAN port to service zone mappings, namely port-based mode and tag-based mode. Intuitively as the name suggests, Port-based mode means that each LAN port services one or none Service Zones, so the maximum number of service zones is equivalent to the number of LAN ports on a EWS controller.

On the contrary, Tag-based service zones are not limited by the number of ports, for they are specified by the VLAN tag ID pre-defined by the admin, regardless of which LAN port. A simple concept is displayed in the picture below.

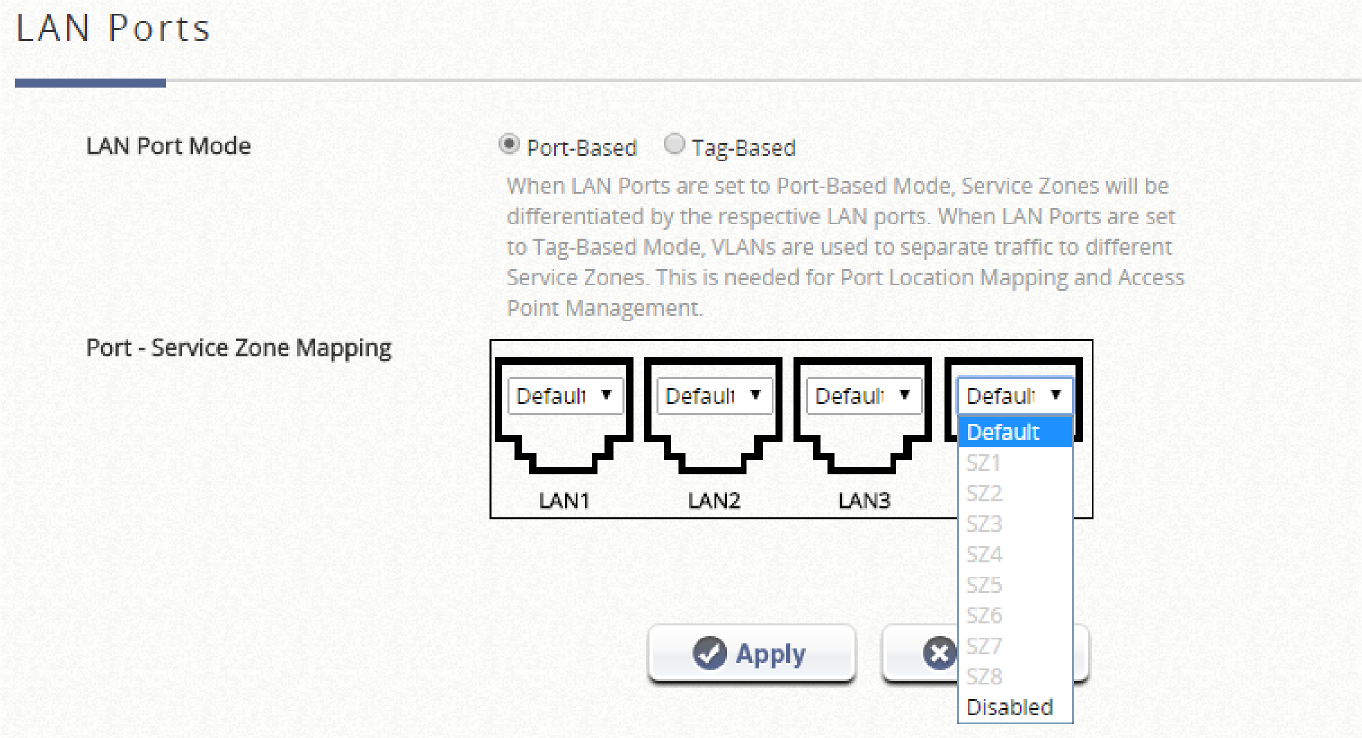


As the figure depicts, a staff of a firm is associated with a certain SSID broadcast by an access point. This SSID belongs to, let’s say, VAP with VLAN ID 15. Therefore the AP’s traffic when forwarded back to the Controller will be mapped to Service Zone 1 with configurations set for staff access.

Configuration Mapping

Configuration Path: Main Menu >> System >> LAN Ports

Admin can change the type of service zones. There are some grayed-out service zones because they have been disabled. Therefore, admin should first go to ‘System > Service Zones > Configure’ to enable the needed service zones.



LAN Ports

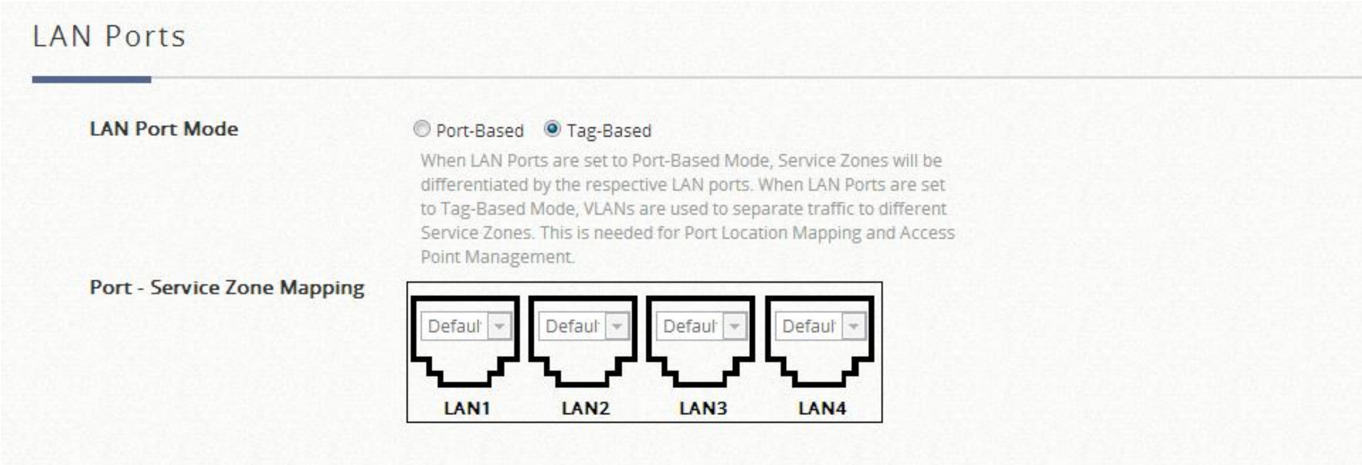
LAN Port Mode ● Port-Based ○ Tag-Based

When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.

Port - Service Zone Mapping

Default
Default
Default
Default
Default
SZ1
SZ2
SZ3
SZ4
SZ5
SZ6
SZ7
SZ8
Disabled
LAN1
LAN2
LAN3
Apply

If the setting is change to **Tag-based,** the correspondence of service zones and ports will be grayed out. Each Service Zone will need to be assigned a unique VLAN ID, ranging from 1 to 4096.



LAN Ports

LAN Port Mode ○ Port-Based ● Tag-Based

When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.

Port - Service Zone Mapping

Defaul
Defaul
Defaul
Defaul
LAN1
LAN2
LAN3
LAN4

Note that the Default Service Zone is designed to be tag-less to manage Local Access Points and process untagged traffic.

6.2.2. 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.

6.2.3. 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 when the system is set to Tag-based mode: **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.

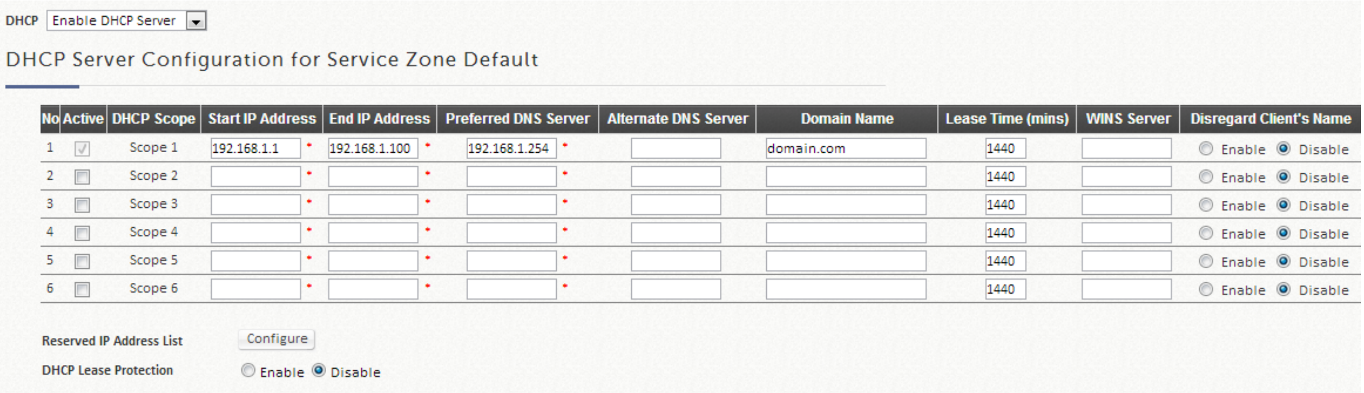
- Clients Isolation: All clients on the same Layer 2 network are isolated from one another in this Service Zone.
- None: No isolation will be applied to clients in this Service Zone.

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.

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



DHCP: Enable DHCP Server

DHCP Server Configuration for Service Zone Default

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

Reserved IP Address List: Configure

DHCP Lease Protection: ○ Enable ● Disable

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.

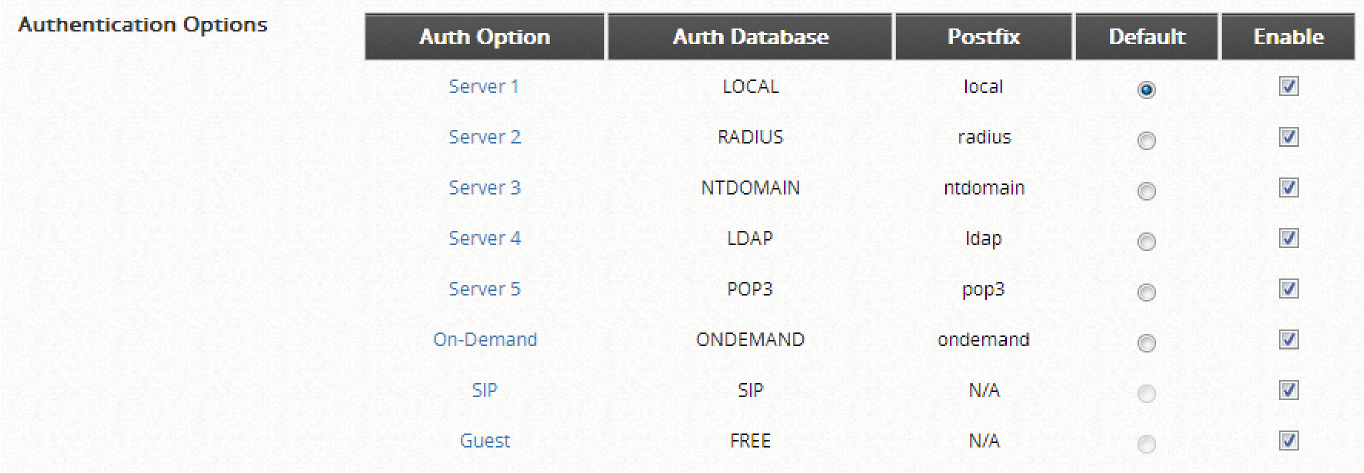
6.2.5. Authentication Options

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.

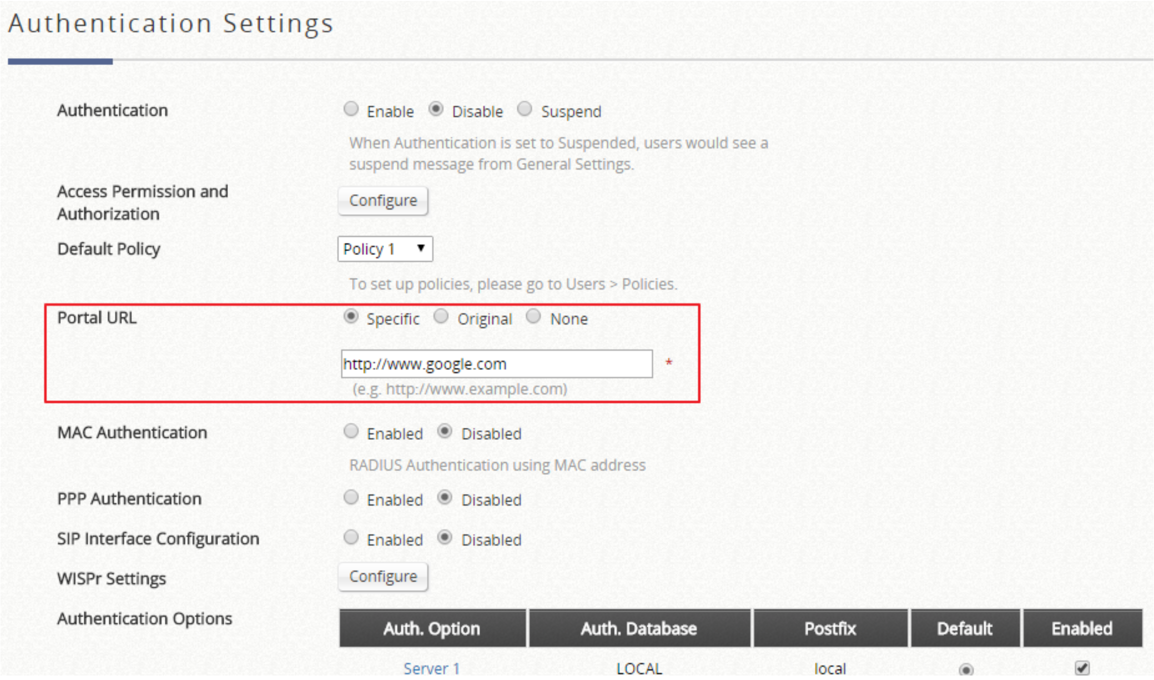


Authentication Options

Auth Option	Auth Database	Postfix	Default	Enable
Server 1	LOCAL	local	●	☑
Server 2	RADIUS	radius	○	☑
Server 3	NTDOMAIN	ntdomain	○	☑
Server 4	LDAP	ldap	○	☑
Server 5	POP3	pop3	○	☑
On-Demand	ONDEMAND	ondemand	○	☑
SIP	SIP	N/A	○	☑
Guest	FREE	N/A	○	☑

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: Configure

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

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

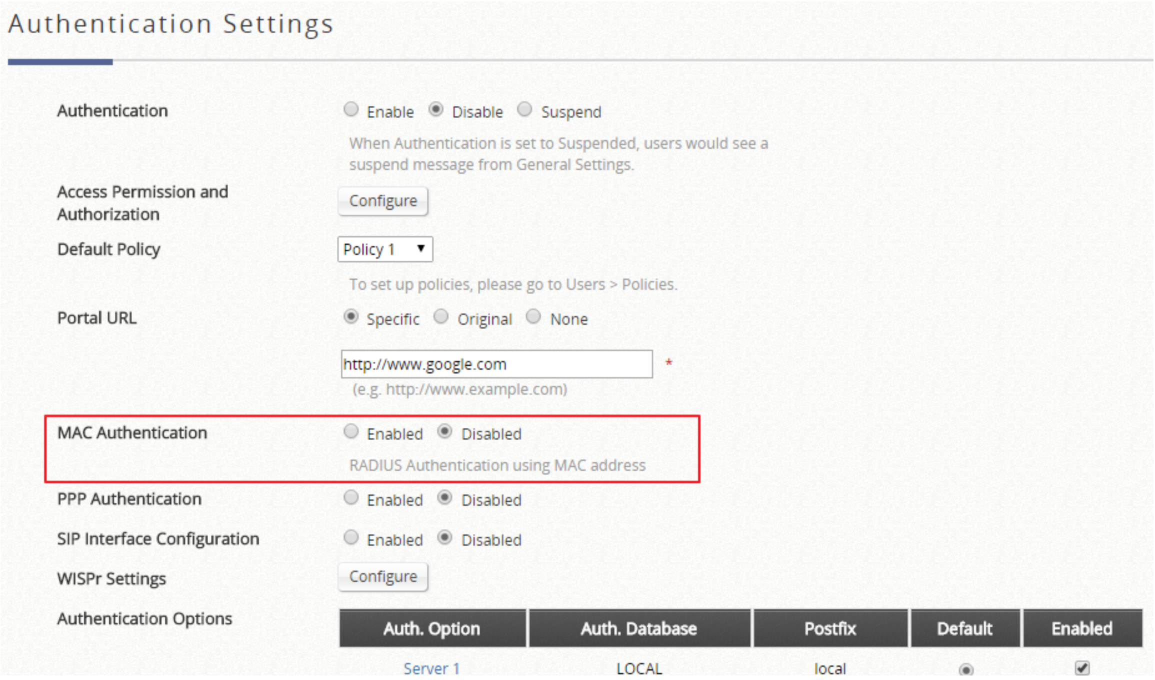
WISPr Settings: Configure

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	●	☑

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
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

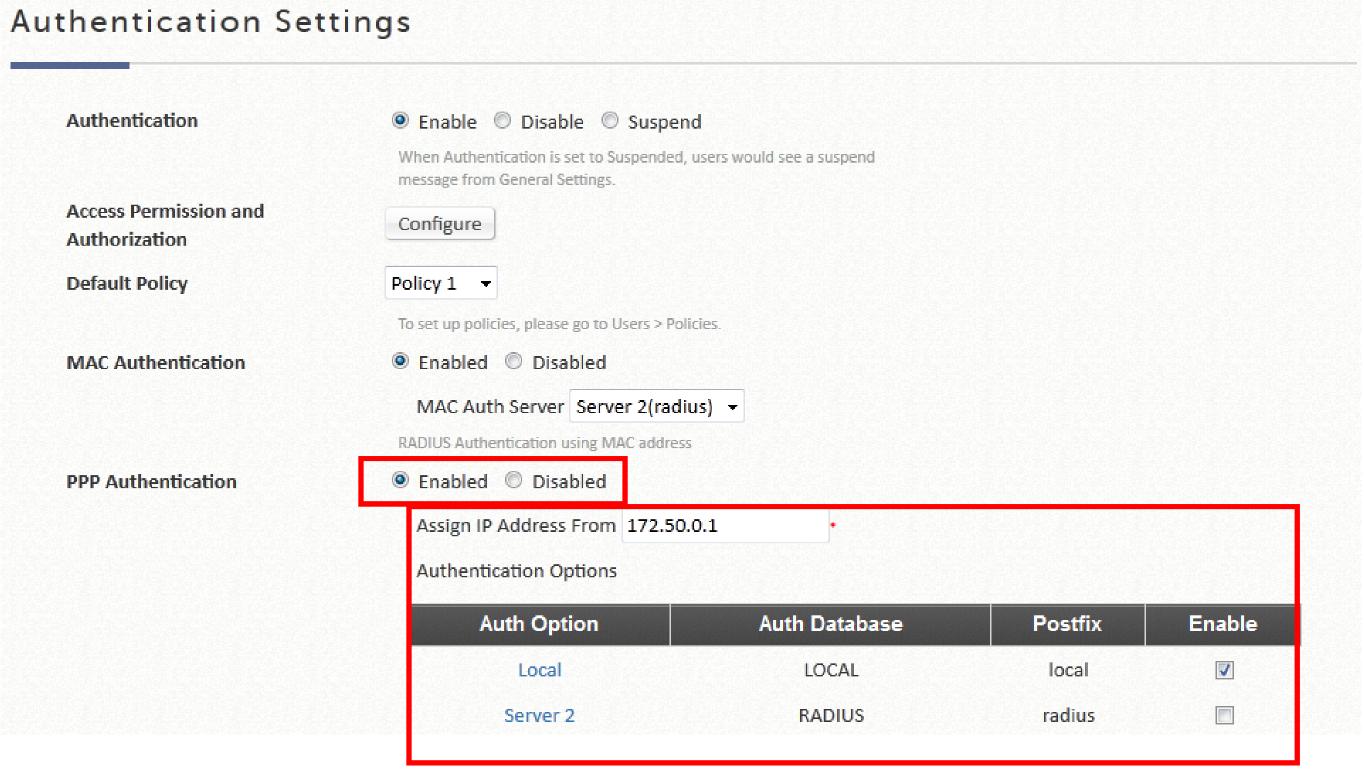
WISPr Settings

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	●	☑

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 Configure

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

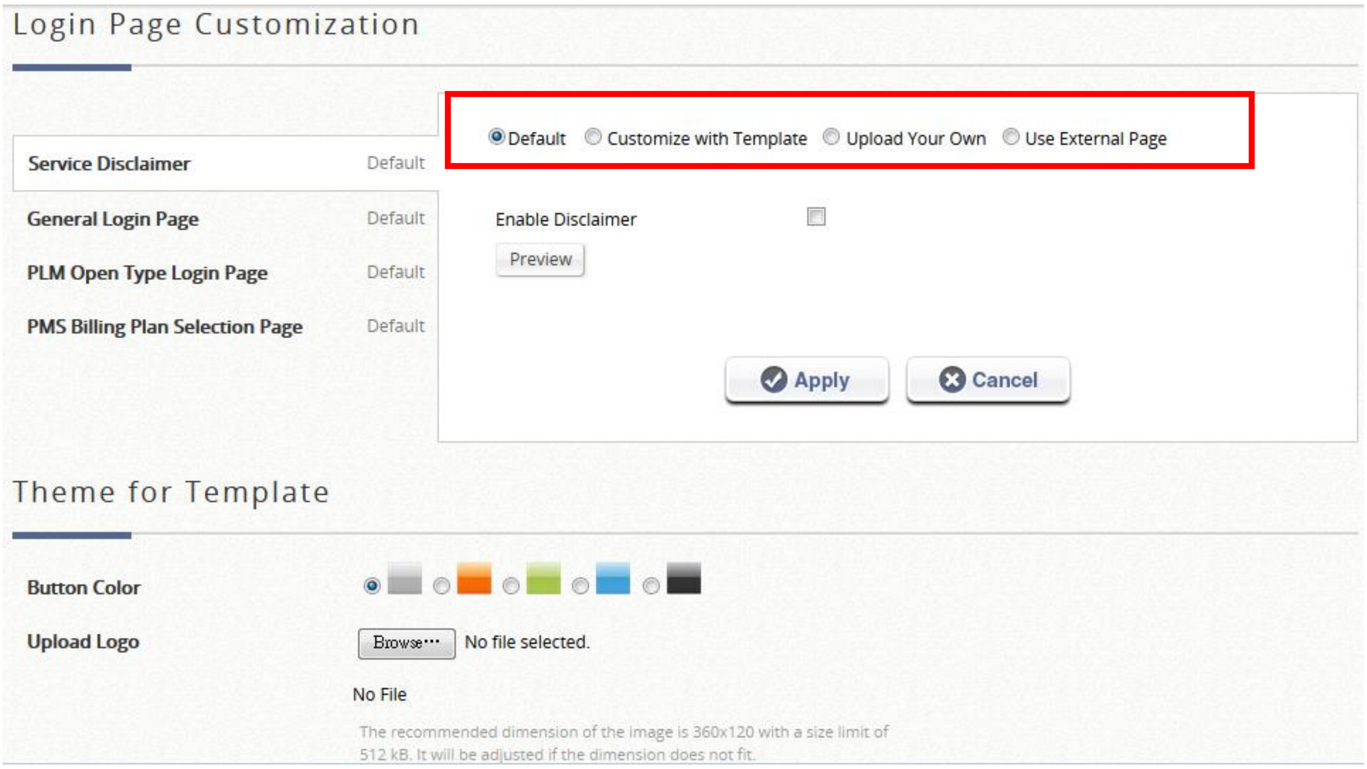
Auth Option	Auth Database	Postfix	Enable
Local	LOCAL	local	☑
Server 2	RADIUS	radius	☐

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.

6.2.6. 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
General Login Page	Default
PLM Open Type Login Page	Default
PMS Billing Plan Selection Page	Default

● Default ○ Customize with Template ○ Upload Your Own ○ Use External Page

Enable Disclaimer ☐

Theme for Template

Button Color ● ○ ○ ○ ○

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

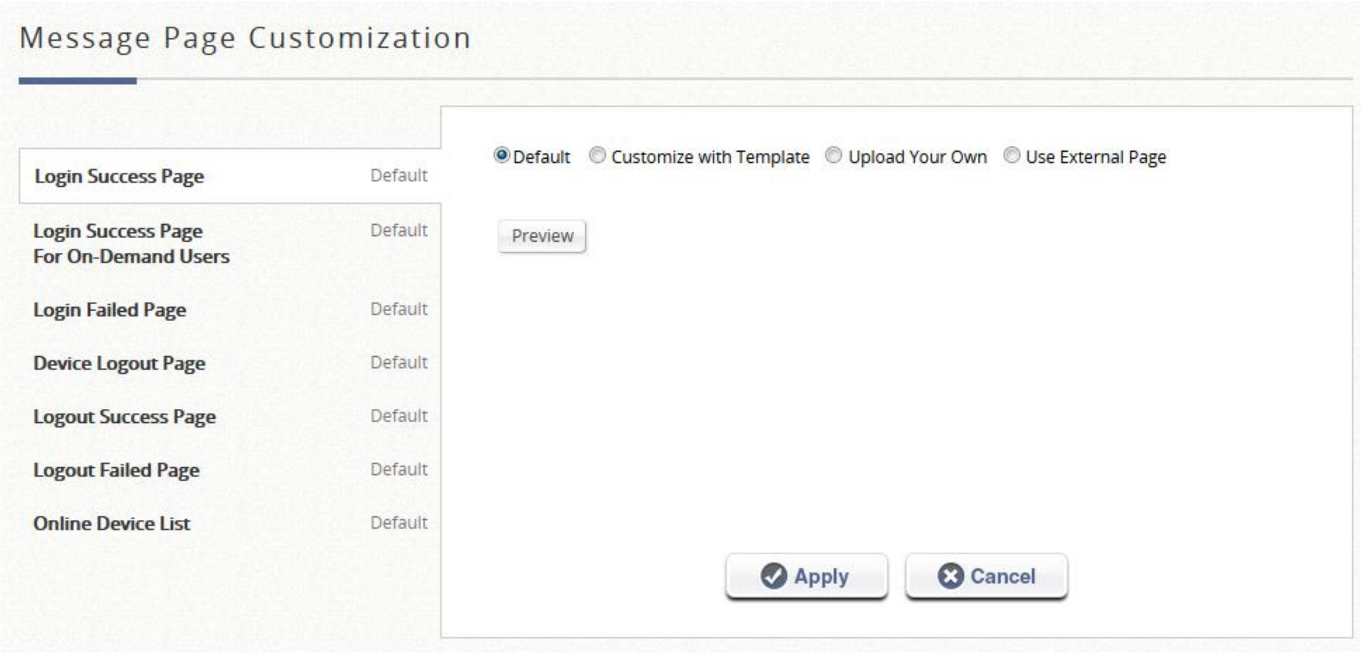
Default: The gateway has a standard Default Login Page with the logo and Administrators can choose to enable a Service Disclaimer if needed.

Customize with Template: For this option, a template is prepared for the administrator's easy customization. The general layout has been set for the administrator but the contents can be customized to his preference. A color theme and a logo can be uploaded, and contents field such as Service Disclaimer, text colors can entered within the template presentation layout.

Upload Your Own: The Administrator has the option to upload a html file as the Login Page. The "Download HTML Sample File" gives administrators a sample HTML code to edit from. Once this sample HTML code is downloaded, open the file with any browser, right click and select "View Page Source". You may edit the HTML code with any text editor as long as the file is saved in .html format.

Use External Page: The Login Page can be a defined external URL. This option requires extensive knowledge of URL parameter utilization that works together with the Message Pages and should be organized carefully. For more details on External Login Page customization, please refer to Appendix A of the User Manual.

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

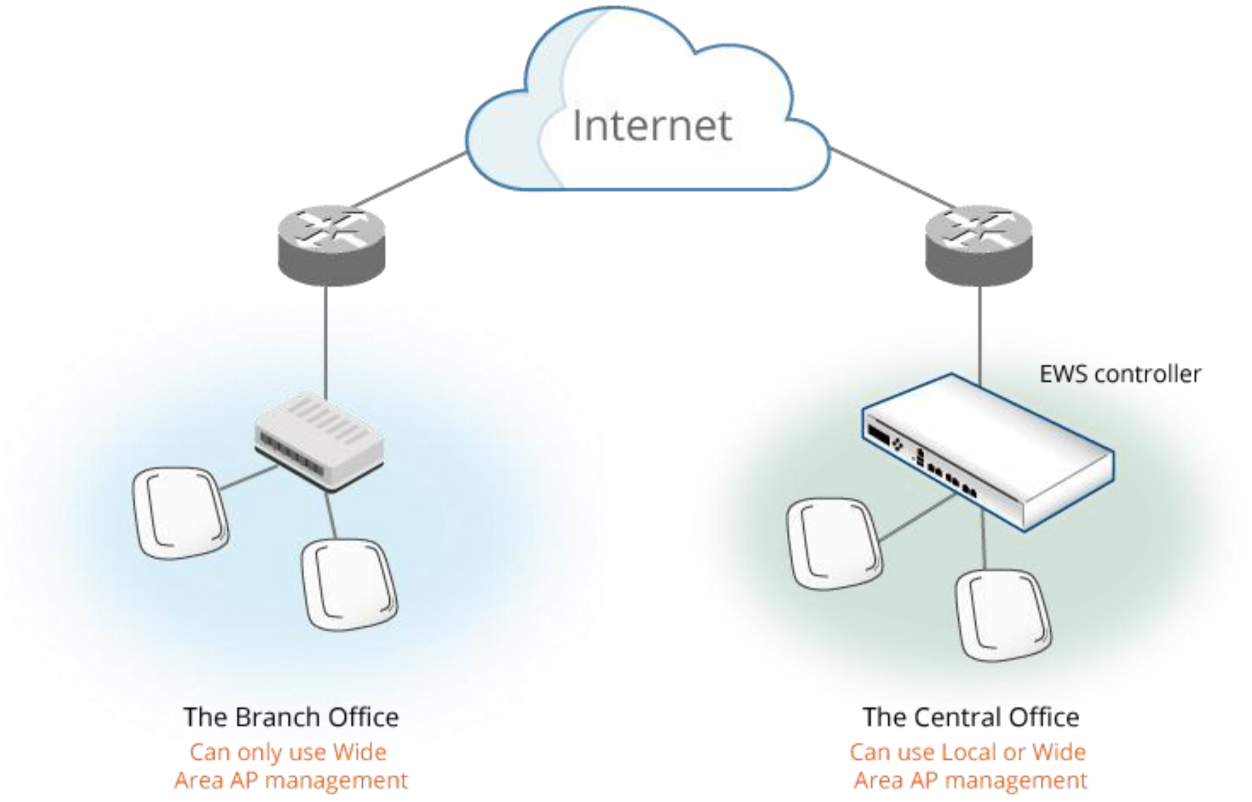
Login Success Page	Default
Login Success Page For On-Demand Users	Default
Login Failed Page	Default
Device Logout Page	Default
Logout Success Page	Default
Logout Failed Page	Default
Online Device List	Default

● Default ○ Customize with Template ○ Upload Your Own ○ Use External Page

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, and the LAN-side AP management '**Local Area AP Management.**' Below illustrates the concept of these two types of management.


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

【Illustration of Wide Area and Local AP Management】

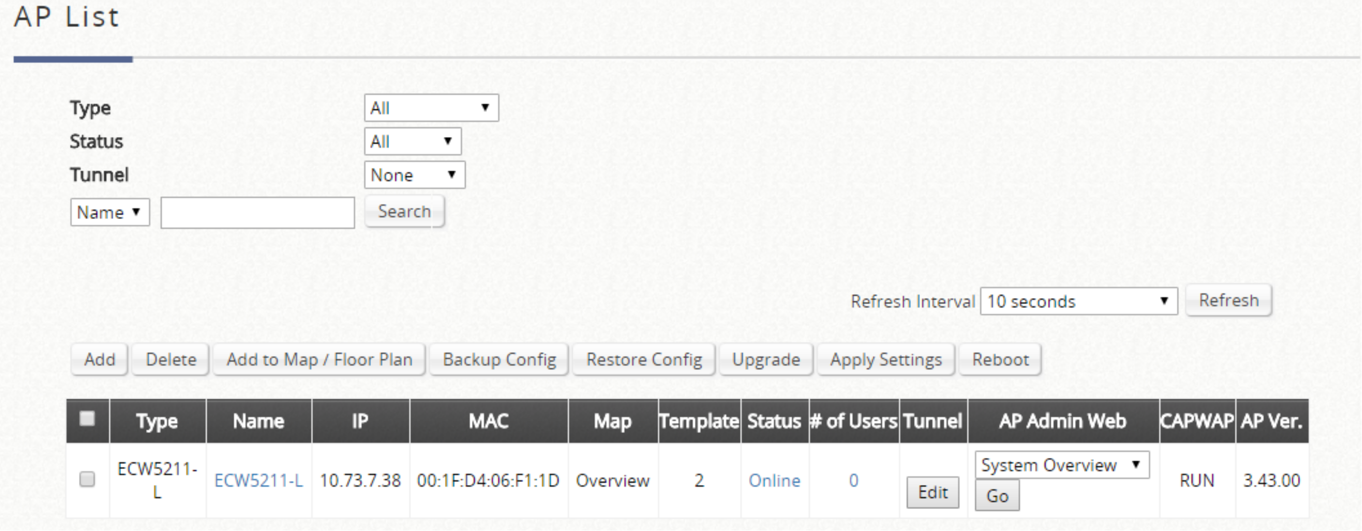
EWS models have different manageability with Edgecore access points, i.e., admin should make sure what AP models your EWS controller supports.

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

Main Menu >> Devices >> Local Area AP Management >> Overview.

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

Main Menu >> Devices >> Wide Area AP Management >> Overview.



Type: All
Status: All
Tunnel: None
Name:
Refresh Interval: 10 seconds

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

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

Under Local Area AP Management, there are up to 8 templates available for each AP model containing configuration attributes primarily on wireless band, data rate, transmit power, data rate, etc. They may be applied to manage APs automatically or manually, avoiding the process of tedious one by one AP configuration.

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. In the tag-based mode, the AP addresses are given by the DHCP server in the default service zone; while in the port-based one, an AP will be allocated an IP address by the DHCP server in its affiliated service zone.

7.2 Local Area AP Management

Configuration path: Main Menu >> Devices >> Local Area AP Management

This section handles the management of access points on the LAN side of your EWS controller. It starts with a methodology of adding access points to the AP management list of a controller, all the way to the utilities that can be applied on the controller to its managed AP's.

7.2.1 AP List

Configuration path: Main Menu >> Devices >> Local Area AP Management >> AP List

All of the supported APs under management of the system will be shown in the list. Check the checkbox for the desired AP Types and click "Apply" to display on the AP List. A search can be performed based on AP Name, IP Address, MAC Address, and Channel by selecting from the drop-down list. The AP's name will be shown as a hyperlink. Click the hyperlink of each managed AP to further configure (General Setting, LAN Setting, Wireless LAN, Layer 2 Firewall) the AP. Click the hyperlink of the shown Status of each managed AP for detailed status information of the AP (System Status, Service Zone Status, Wireless Status, Access Control Status, and Associated Client Status).

Administrators may filter the AP List by selecting the desired AP Models. Check the AP Models under AP Type and click "Apply" to apply the filter.

To add an AP or multiple APs, click the "Add" button. This is elaborated in Section 7.2.2 AP Adding and Discovery.

Options such as Enabling or Disabling an AP, applying Templates and Service Zones can be done by checking the checkboxes on the left of the AP List and clicking the respective buttons. Details on AP Templates configuration are elaborated in Section 7.2.3 Templates Configuration. For monitoring, there is a refresh interval option to allow administrator realize what the exact status of each managed AP.

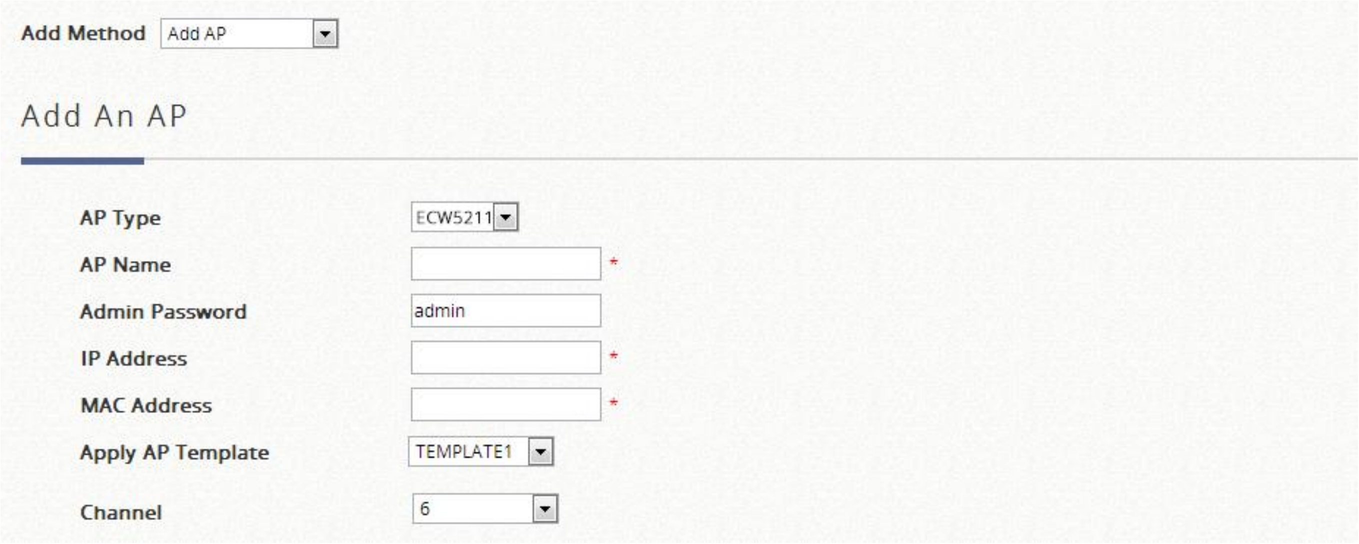
Note that not all firmware versions are fully compatible with EWS's AP Management feature. Check for compatibility under the "Status" column.

7.2.2 AP Adding and Configuration Applying

Configuration path: Main Menu >> Devices >> Local Area AP Management >> AP List >> Add

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

To add an AP, specify an AP Name and enter its IP and MAC address. These rows with red asterisks are mandatory information that needs to be provided. After filling in all the fields, click **Apply** at the bottom of the page to add the AP (to add an AP, it doesn't necessarily have to be online). Check the **AP List** to confirm the adding.



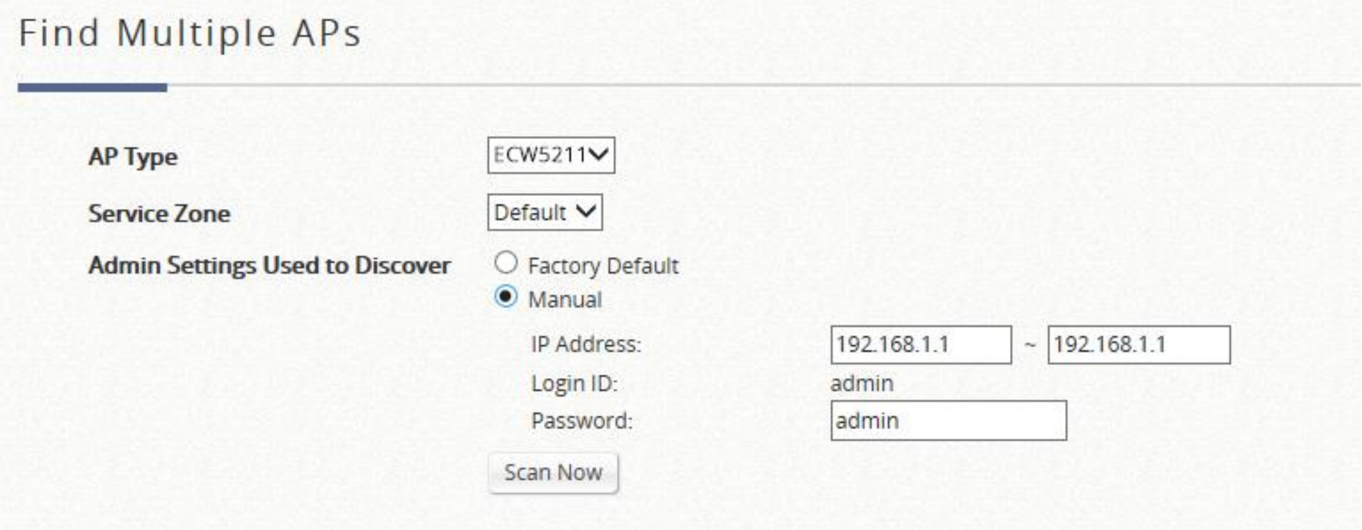
Add Method: Add AP

Add An AP

AP Type	ECW5211
AP Name	*
Admin Password	admin
IP Address	*
MAC Address	*
Apply AP Template	TEMPLATE1
Channel	6

To Add APs in batches, the admin scans an IP address range and collectively discover the AP's of the same type, either by

1. 'Factory Default' scanning – used if the administrator has not changed any of the configuration on their AP's. And there is no need to fill in any fields. Just click **Scan Now**
2. 'Manual' scanning**-** used if the IP addresses of the AP's have been changed to those other than 192.168.1.1. Type in the range of the IP addresses you would like to scan through and click **Scan Now**.



AP Type: ECW5211
Service Zone: Default
Admin Settings Used to Discover: ○ Factory Default ● Manual
IP Address: 192.168.1.1 ~ 192.168.1.1
Login ID: admin
Password: admin

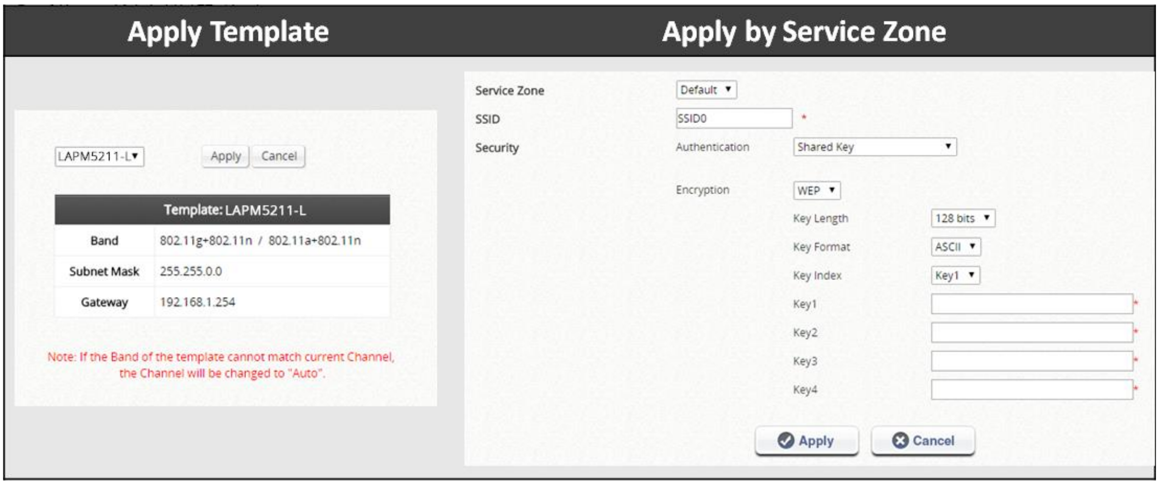
The **Discovery Results** Table will then display all the AP's found currently alive. After finding the AP, admin can further set up the template to be applied and the operating channel, and furthermore put the AP under a specific service zone you have enabled.

NOTE

1. It might take some time for the controller to discover AP's. Please wait for a moment until the AP you are scanning for is displayed on the **Discovery Results** list.
2. Note that the **Background** above the discovery list could be enabled to scan the wireless environment every fixed period of time based on admin's setting. Click **Configure** to set up the function.

Subsequent modifications to AP configurations are possible via the hyperlink under the AP Name. Click one of the AP Names to access its settings page, including **General Settings, LAN Interface Settings and Wireless Interface Settings**.
There is also a row of buttons indicating **Reboot, Enable, Disable, Delete, Apply template, Apply by Service Zone, and Reset to Default**, which are quite intuitive in terms of the names for changing the content of the AP list. Choose one or more AP's in advance and perform one of the functions.

Applying template is designed for initializing the AP configuration such as fundamental wireless parameters which administrators have already prepared in advance. Edgecore's Local Area AP Management function provides another option for applying settings, namely the **Applying by Service Zone** feature, whenever administrators would like to revise VAP configuration such as SSID name and wireless security pre-shared keys after a period of practical usage. Simply confirm whether a VAP is mapped to the selected Service Zone.



LAPM5211-L

Template: LAPM5211-L	
Band	802.11g+802.11n / 802.11a+802.11n
Subnet Mask	255.255.0.0
Gateway	192.168.1.254

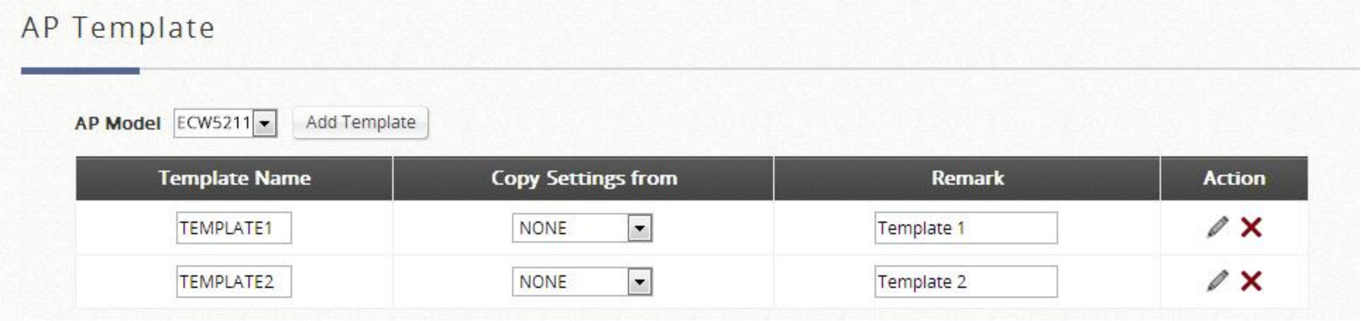
Note: If the Band of the template cannot match current Channel, the Channel will be changed to "Auto".

Service Zone: Default
SSID: SSID0 *
Security: Authentication: Shared Key
Encryption: WEP
Key Length: 128 bits
Key Format: ASCII
Key Index: Key1
Key1: *
Key2: *
Key3: *
Key4: *

7.2.3 Templates Configuration

Configuration path: Main Menu >> Devices >> Local Area AP Management >> Templates

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

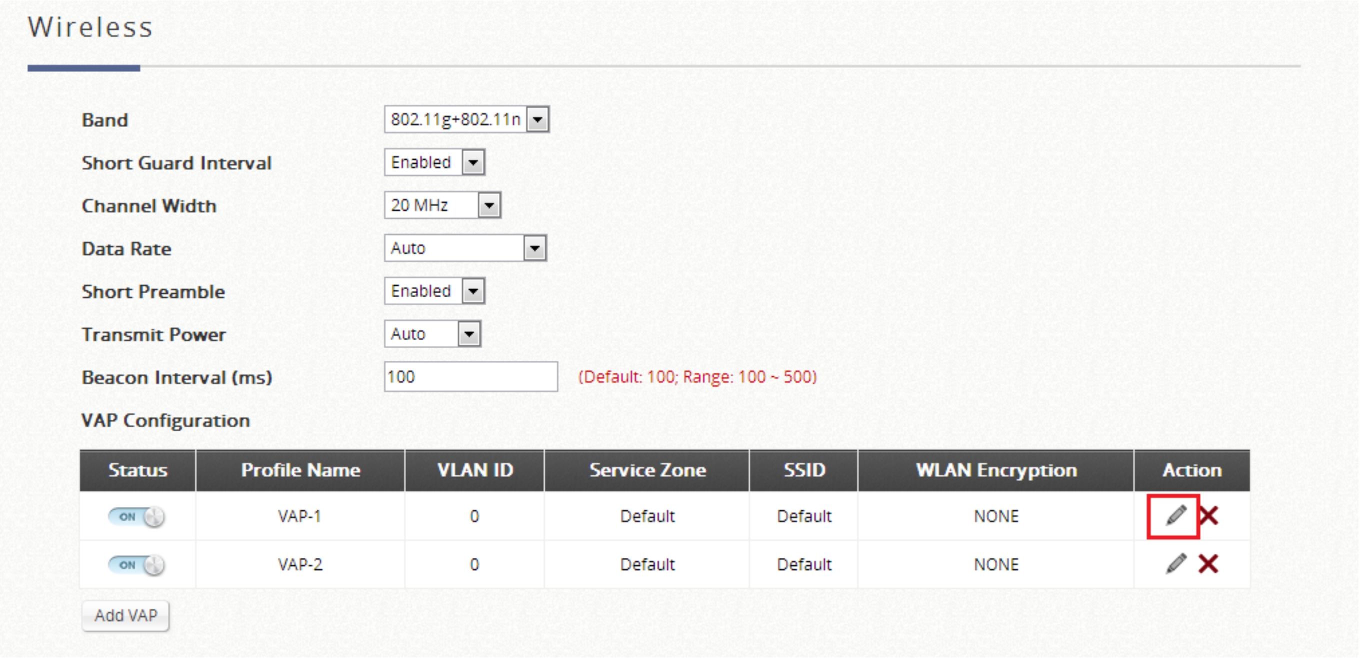


AP Template

AP Model ECW5211 Add Template

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

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



Wireless

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

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

Add VAP

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

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

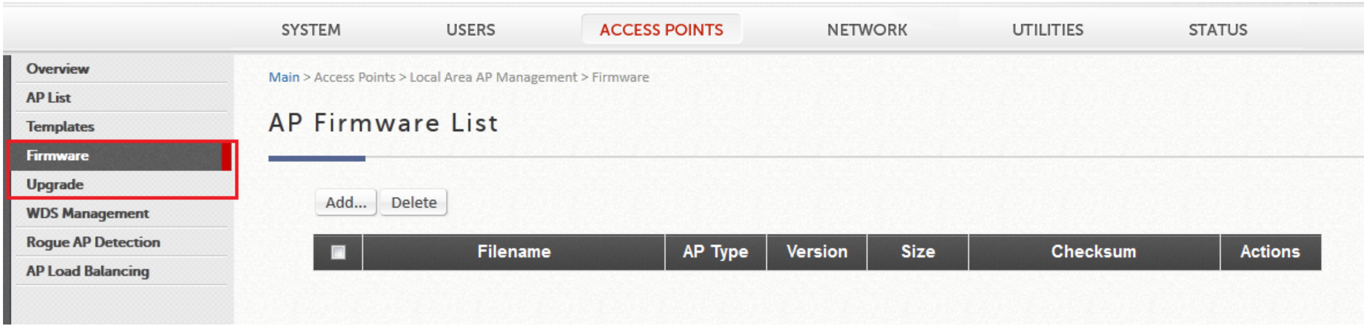
WEP: When Authentication is Open System or Share Key, WEP will be enabled.
WPA: When Authentication is WPA, WPA-PSK or WPA-RADIUS will be the options of WPA. For WPA-PSK, Passphrase or HEX can be selected.
WPA2: When Authentication is WPA, WPA-PSK or WPA-RADIUS will be the options of WPA. For WPA-PSK,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

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

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

7.2.4. AP Firmware Management

Firmware upgrade matters because much of the software enhancements are released periodically for enhanced standards / features. Edgecore offers an easy firmware upgrade process from the controller’s AP management interface, allowing the administrator to upgrade multiple AP devices at once.


SYSTEM
USERS
ACCESS POINTS
NETWORK
UTILITIES
STATUS
Overview
AP List
Templates
Firmware
Upgrade
WDS Management
Rogue AP Detection
AP Load Balancing
Main > Access Points > Local Area AP Management > Firmware
AP Firmware List
Add...
Delete
Filename
AP Type
Version
Size
Checksum
Actions

1. First add a firmware and select the firmware file at Devices >> Local Area AP Management >> Firmware and click **Upload** next to the row to store the AP firmware within the Controller.
2. Upgrade the necessary AP’s by going to Devices >> Local Area AP Management >> Upgrade, select the AP’s you would like to import the version to. When done with the selection, click **Upgrade** at the bottom of the page.

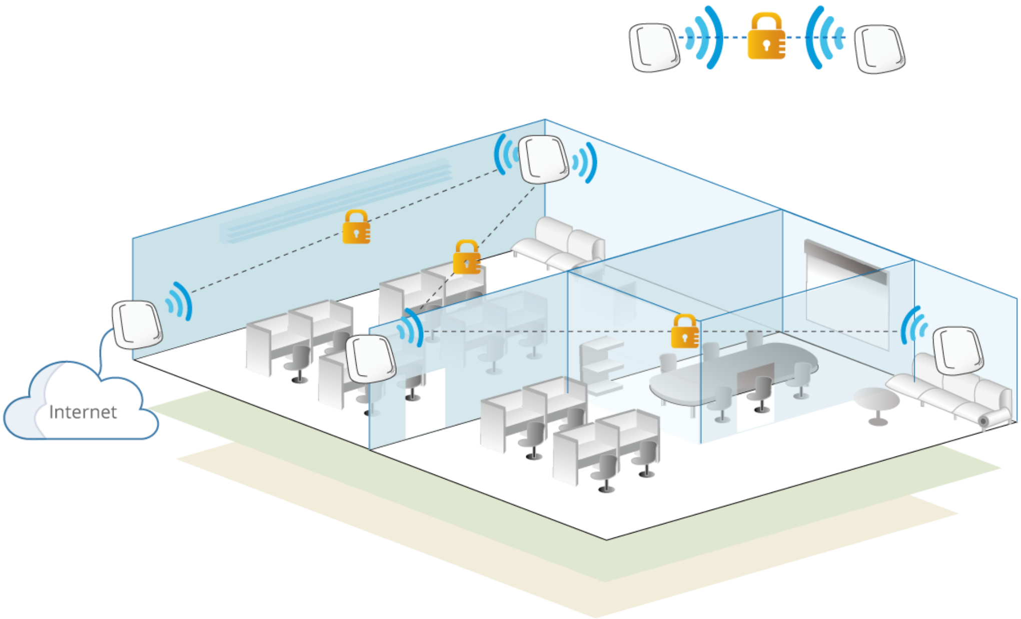
NOTE

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

7.2.5 WDS Links

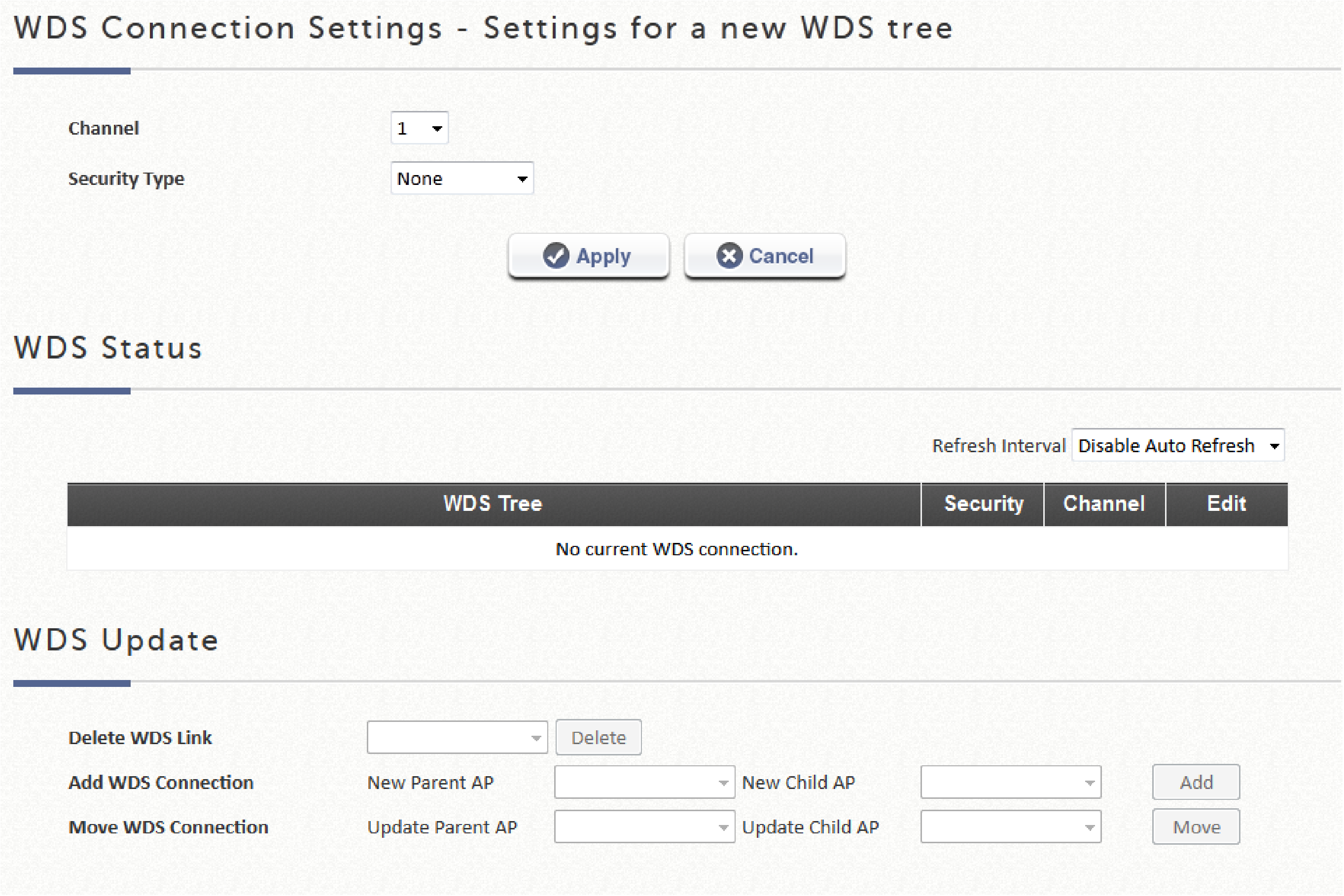
Configuration path: Main Menu >> Devices >> Local Area AP Management >> WDS Management

WDS is the acronym for Wireless Distribution System, a function for extending the wireless coverage of the network with additional APs.



【A simple concept diagram illustrating WDS connection】

The WDS management function helps administrators plan and setup a "Tree" structure of WDS network with managed APs.



WDS Connection Settings - Settings for a new WDS tree

Channel: 1

Security Type: None

Apply
Cancel

WDS Status

Refresh Interval: Disable Auto Refresh

WDS Tree	Security	Channel	Edit
No current WDS connection.			

WDS Update

Delete WDS Link
Delete
Add WDS Connection
New Parent AP
New Child AP
Add
Move WDS Connection
Update Parent AP
Update Child AP
Move

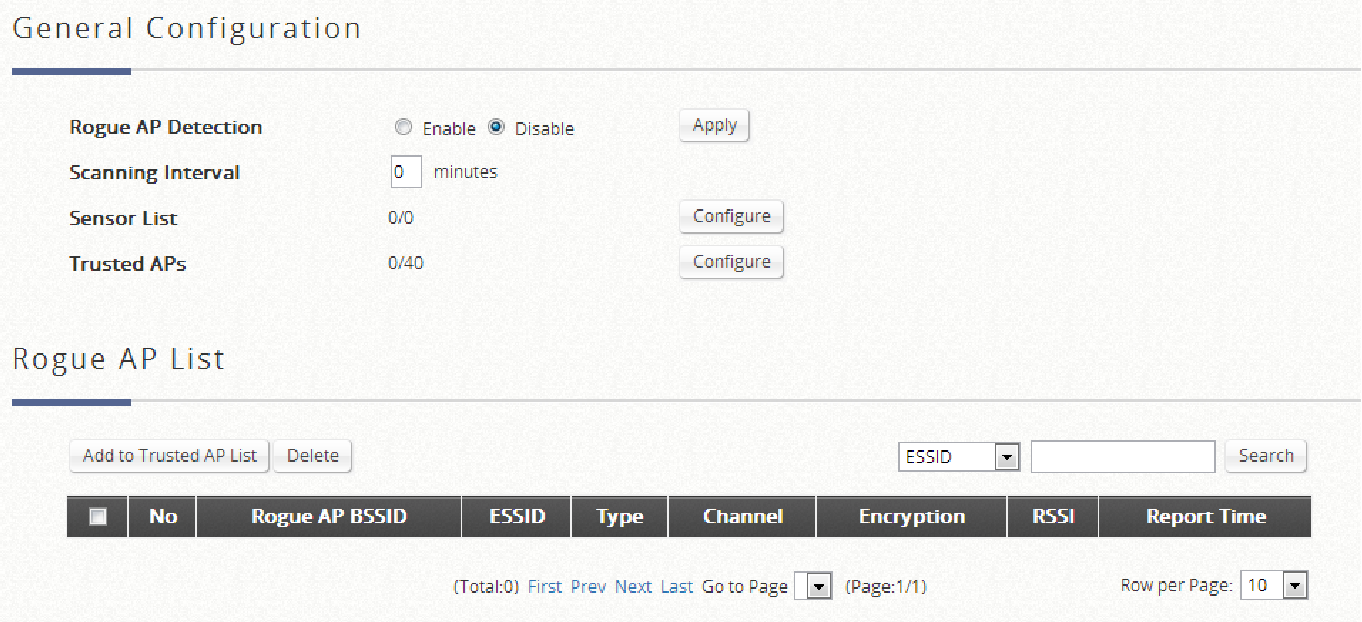
WDS Connection Settings: Determine the Channel and Security Type for the APs deployed in the WDS network tree.

WDS Status: Shows the added APs in the WDS Tree with Security and Channel settings. More than one WDS Tree can be set up in your network. Click "Edit" to change the WDS connection settings for the associated WDS Tree. This list can be set to refresh automatically at fixed intervals (10s, 20s, 30s, 40s, 50s, 60s).

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

7.2.6 Rogue AP Scanning

Rogue AP detection is another essential way of protecting your network environment. Local AP Management supports the detection of non-authorized access points present in the vicinity.
Non-authorized access points pose a possible problem in terms of wireless interference. Go to Main Menu >> Devices >> Enter Local Area AP Management >> Rogue AP Detection to set up the function. Admin should 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.



General Configuration

Rogue AP Detection	○ Enable ● Disable	Apply
Scanning Interval	0 minutes	
Sensor List	0/0	Configure
Trusted APs	0/40	Configure

Rogue AP List

☐	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	RSSI	Report Time

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

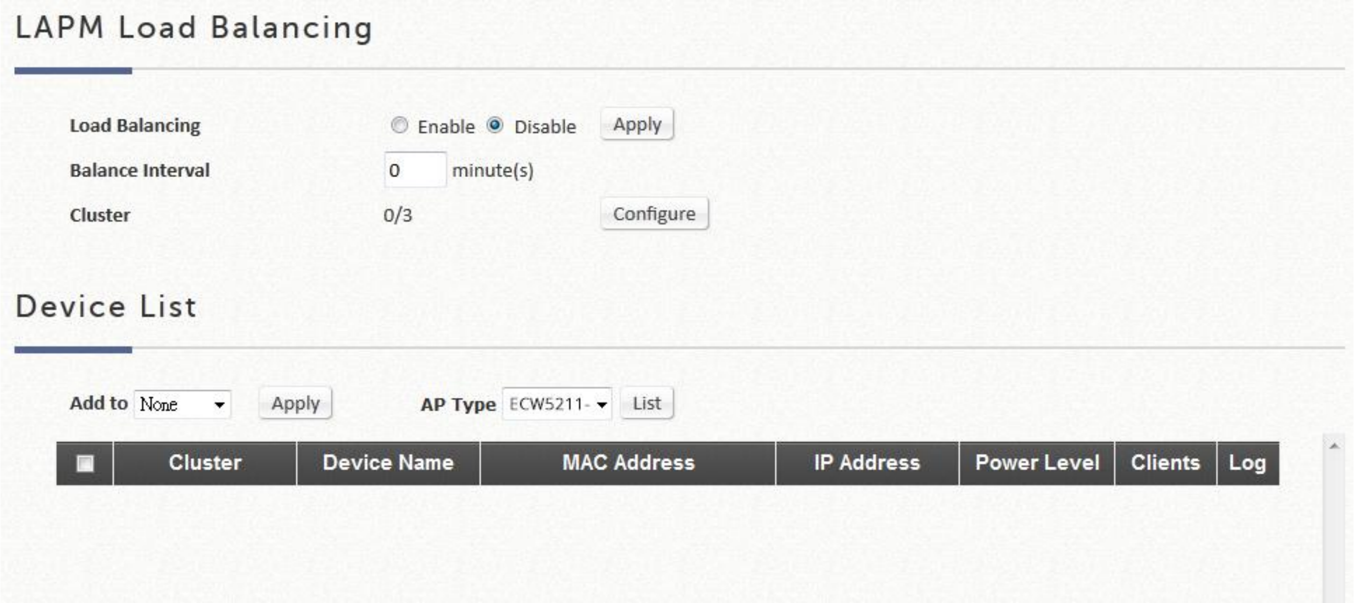
Discovered access points are temporarily put in the Rogue AP list. Click one of the hyperlinked BSSID's to see its detailed information. However, if admin recognized some of the listed APs as trusted, just check the checkboxes before the BSSID column and then click **Add to Trusted AP List.** This action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

7.2.7 AP Load Balancing Feature

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

Local 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.

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 threshold.


LAPM Load Balancing

Load Balancing ○ Enable ● Disable

Balance Interval 0 minute(s)

Cluster 0/3

Device List

Add to None

AP Type ECW5211-

☐	Cluster	Device Name	MAC Address	IP Address	Power Level	Clients	Log

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

7.3 Wide Area AP Management

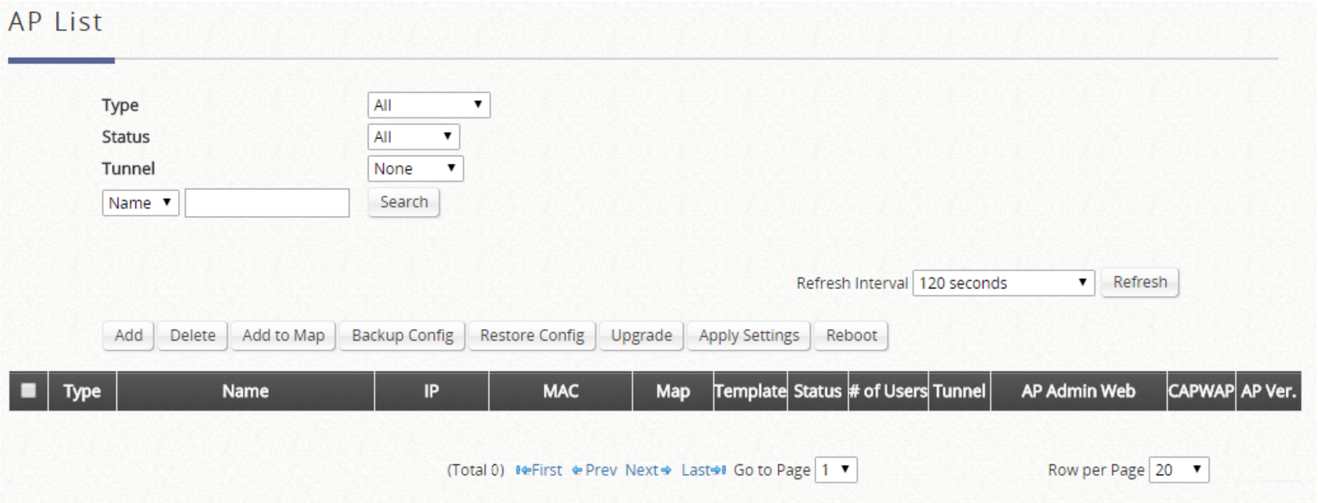
Configuration path: Main Menu >> Devices >> Wide Area AP Management

This section goes on to explain how to centrally manage the access points on the WAN from an 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 3rd 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: All
Status: All
Tunnel: None
Name

Refresh Interval: 120 seconds

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

(Total 0) First Prev Next Last Go to Page 1

Row per Page 20

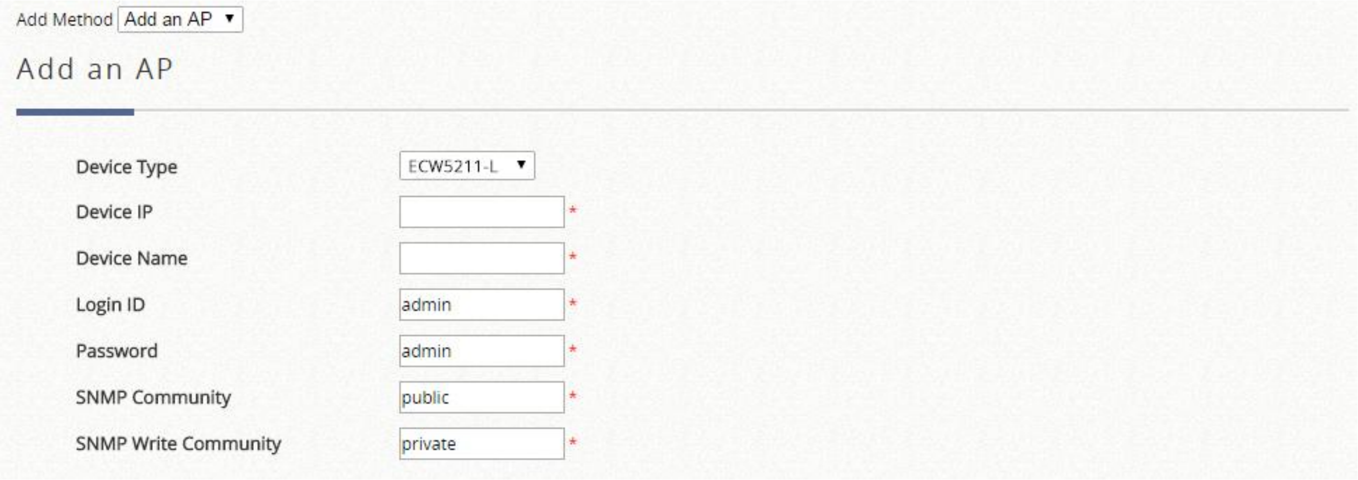
NOTE

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

7.3.1. 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 ▼

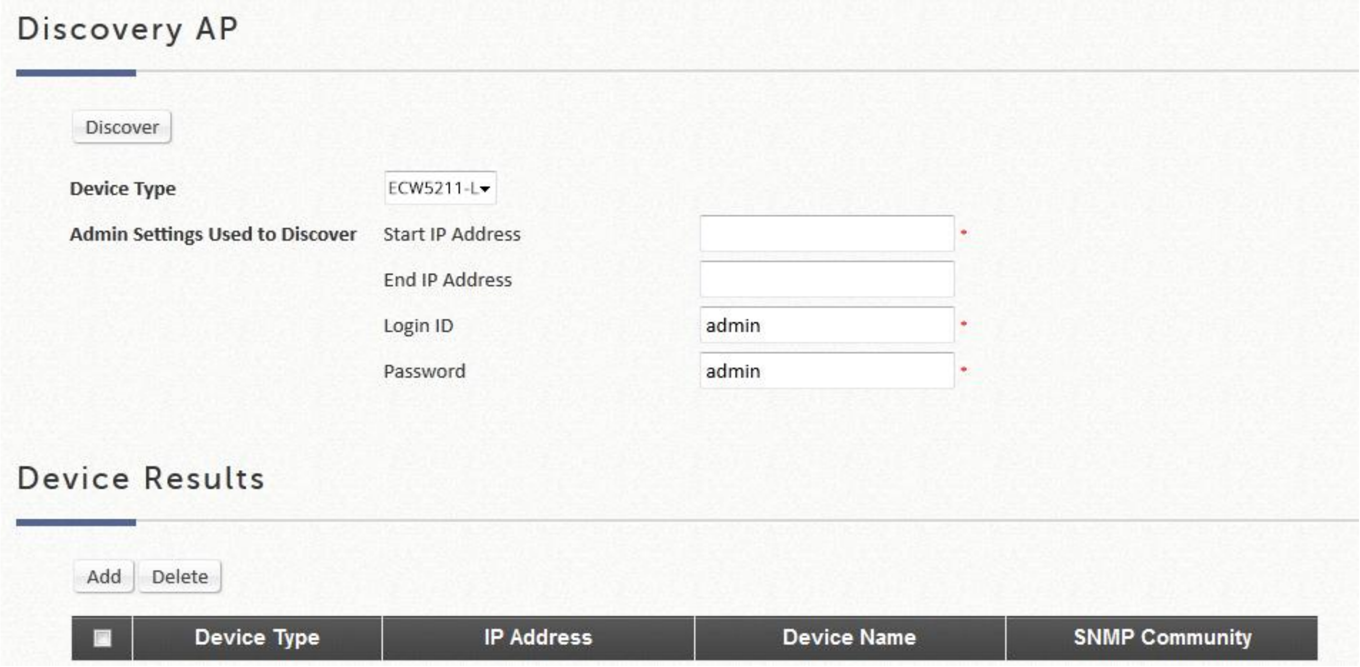
Add an AP

Device Type	ECW5211-L ▼
Device IP	*
Device Name	*
Login ID	admin *
Password	admin *
SNMP Community	public *
SNMP Write Community	private *

7.3.2. 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, then click “Discover”. After the discovery process, newly found AP’s will be listed under Device Results where the administrator can specify the individual APs Device Name and SNMP Community string. Select and click the Add button and the discovered APs will be added into List.



Discovery AP

Device Type: ECW5211-L

Admin Settings Used to Discover
Start IP Address:
End IP Address:
Login ID: admin
Password: admin

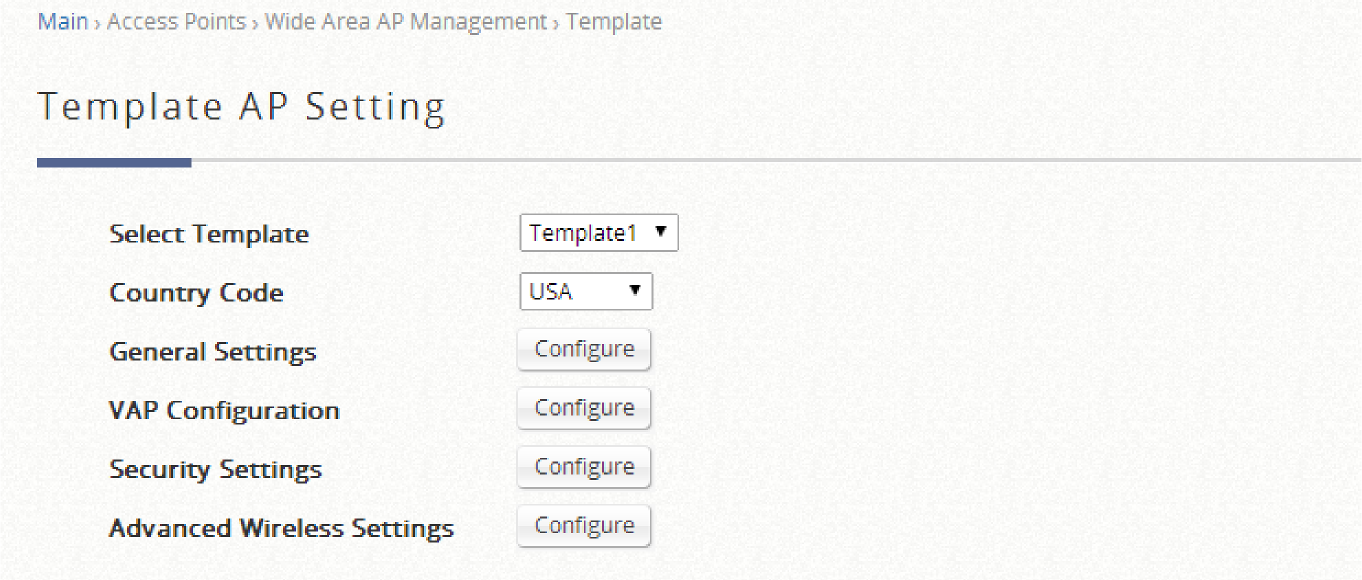
Device Results

☐	Device Type	IP Address	Device Name	SNMP Community

7.3.3 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



Main › Access Points › Wide Area AP Management › Template

Template AP Setting

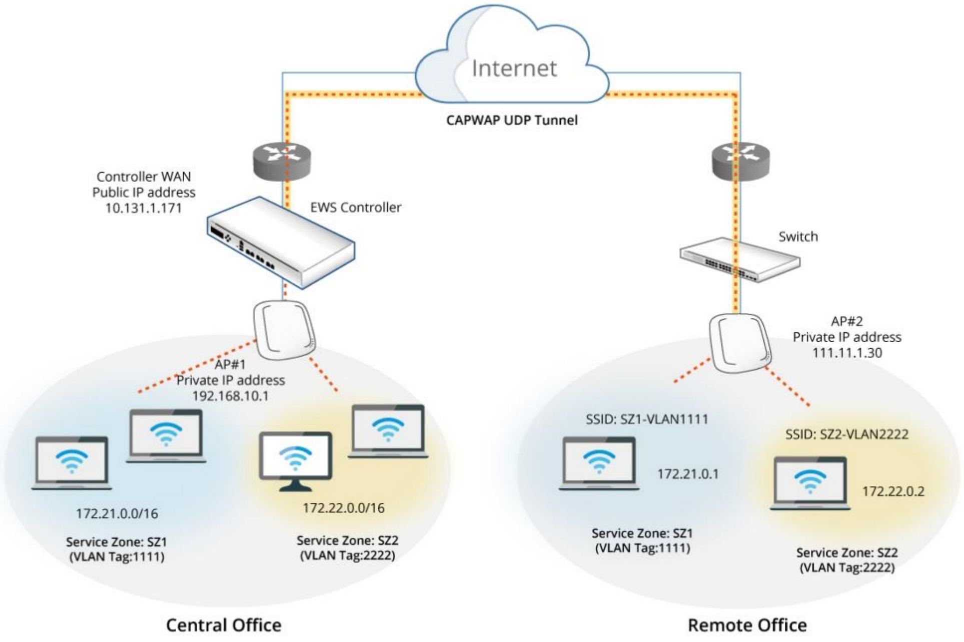
Select Template: Template1
Country Code: USA
General Settings
VAP Configuration
Security Settings
Advanced Wireless Settings

Up to 3 Templates are available and all functions configurable for wireless on the access point can be configured from the template.

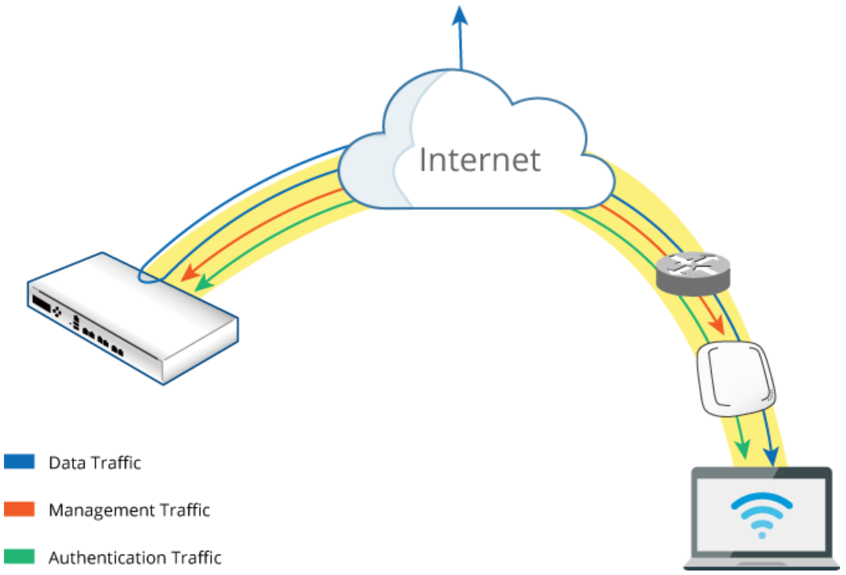
General Settings on the Access Point include basic wireless settings such as the Band, Channel, Transmit Power, Transmit Rates and etc. **VAP Settings** allows the administrator to enable/disable a VAP, designate an ESSID, and assign VLAN ID with/ without corresponding tunnel if needed. Configure **Security Settings**, such as WEP, 802.1X, WPA-Personal, 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.

7.3.4 AP auto Discovery and Configuration using CAPWAP

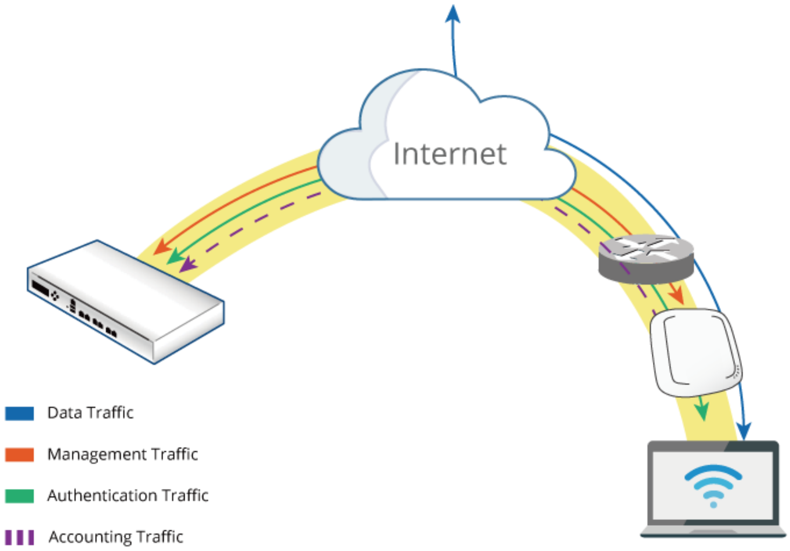
CAPWAP is a standard interoperable protocol that enables an EWS Controller to manage a collection of wireless access points. Two tunneling options are available: complete tunnel and split tunnel.


Internet
CAPWAP UDP Tunnel
Controller WAN
Public IP address
10.131.1.171
EWS Controller
Switch
AP#1
Private IP address
192.168.10.1
AP#2
Private IP address
111.11.1.30
SSID: SZ1-VLAN1111
SSID: SZ2-VLAN2222
172.21.0.0/16
172.22.0.0/16
172.21.0.1
172.22.0.2
Service Zone: SZ1
(VLAN Tag:1111)
Service Zone: SZ2
(VLAN Tag:2222)
Service Zone: SZ1
(VLAN Tag:1111)
Service Zone: SZ2
(VLAN Tag:2222)
Central Office
Remote Office

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 EWS Controller to fully support centralized AP management and user management.


Internet
Data Traffic
Management Traffic
Authentication Traffic

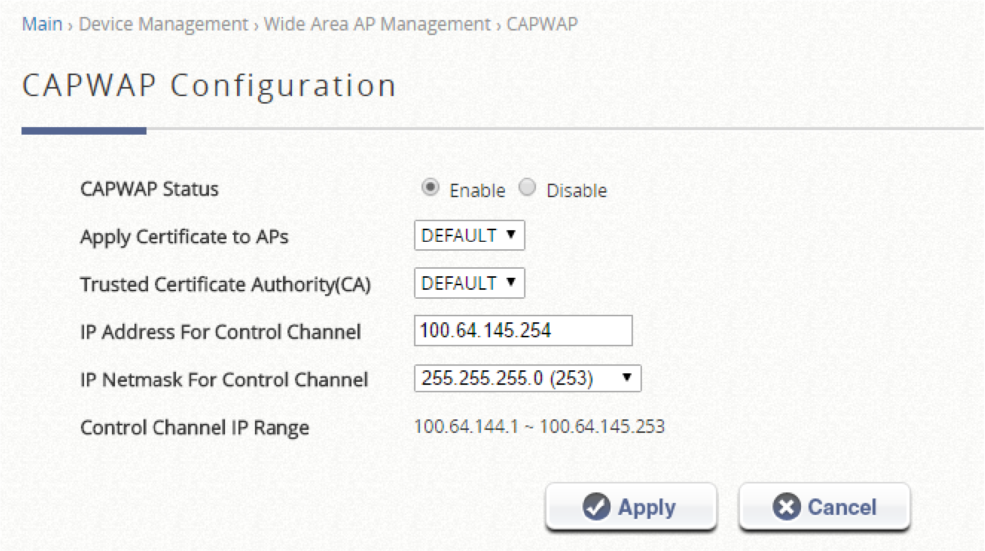
For **Split tunnel,** only user authentication related traffic will be directed back to the controller. For authenticated users, data traffic will go to the Internet through the local network directly. The user data can be transmitted with a shorter path and the network load of the controller can also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


Internet
Data Traffic
Management Traffic
Authentication Traffic
Accounting Traffic

Configuration Steps:

1. On the EWS controller: Enable CAPWAP from Main Menu >> Devices >> Wide Area AP Management >> CAPWAP

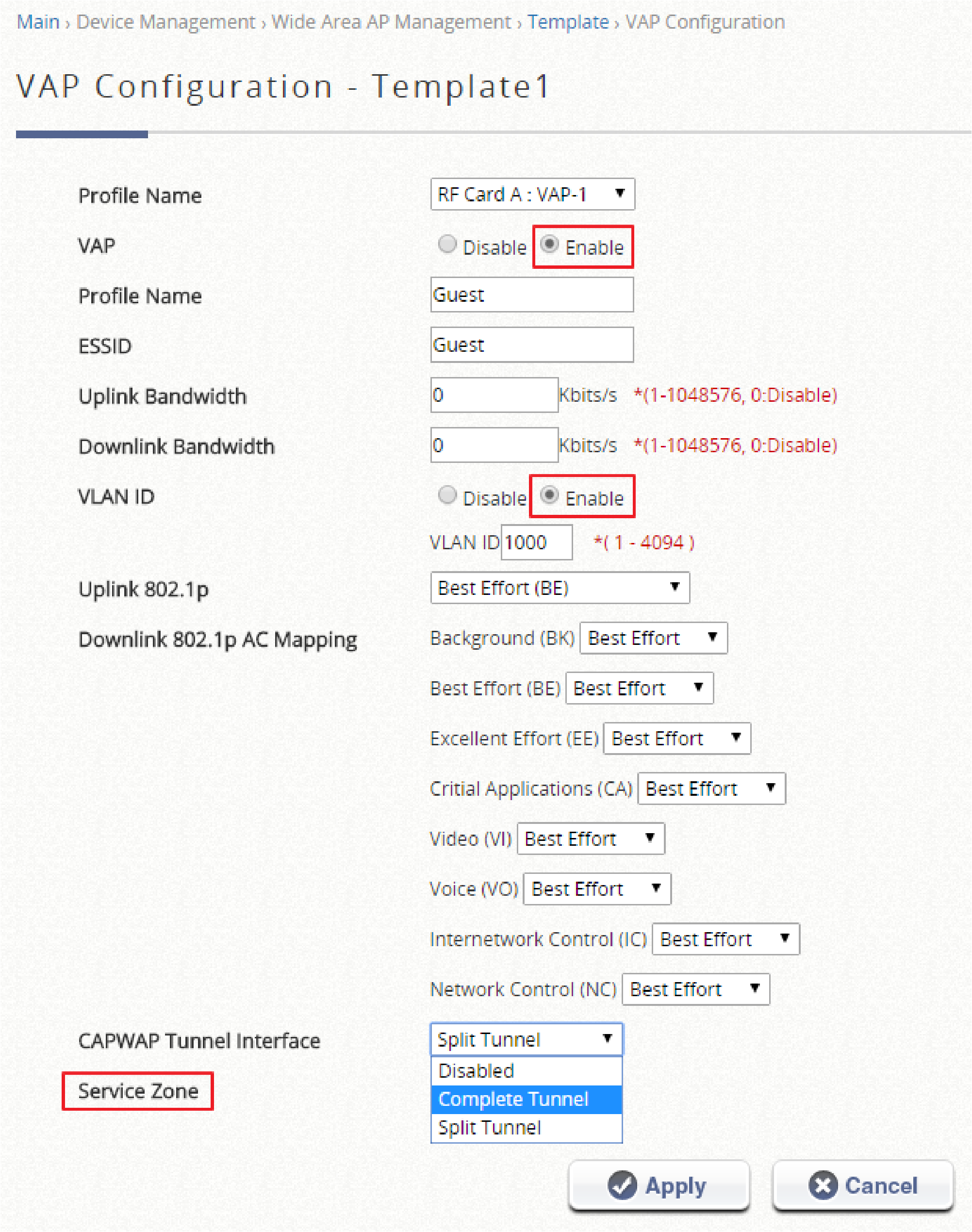
2. Make sure that the Controllers' CAPWAP settings uses a security certificate that is issued by the same CA. For information on Certificate management on the controller please refer to the subsequent chapter in this guide.



CAPWAP Status: ● Enable ○ 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.



Main › Device Management › Wide Area AP Management › Template › VAP Configuration

VAP Configuration - Template1

Profile Name RF Card A : VAP-1
VAP ○ Disable ● Enable
Profile Name Guest
ESSID Guest
Uplink Bandwidth 0 Kbits/s *(1-1048576, 0:Disable)
Downlink Bandwidth 0 Kbits/s *(1-1048576, 0:Disable)
VLAN ID ○ Disable ● Enable
VLAN ID 1000 *(1 - 4094)
Uplink 802.1p Best Effort (BE)
Downlink 802.1p AC Mapping
Background (BK) Best Effort
Best Effort (BE) Best Effort
Excellent Effort (EE) Best Effort
Critial Applications (CA) Best Effort
Video (VI) Best Effort
Voice (VO) Best Effort
Internetwork Control (IC) Best Effort
Network Control (NC) Best Effort
CAPWAP Tunnel Interface Split Tunnel
Service Zone

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 EWS controller it is trying to connect.

(3) **Broadcast Discovery**

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

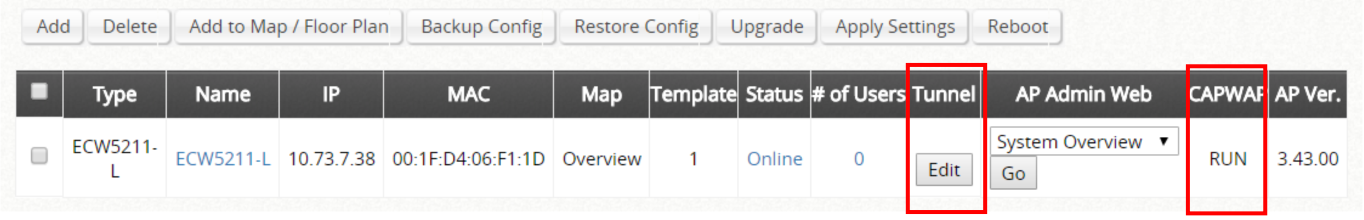
Multicast discovery works by sending a multicast discover packet to the network in hopes of the correct controller responding to it. This function should go with a proper setup on the routing paths of the AP. Please make sure you enable it with the related settings in place.

(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 EWS controller you want this AP to join to.

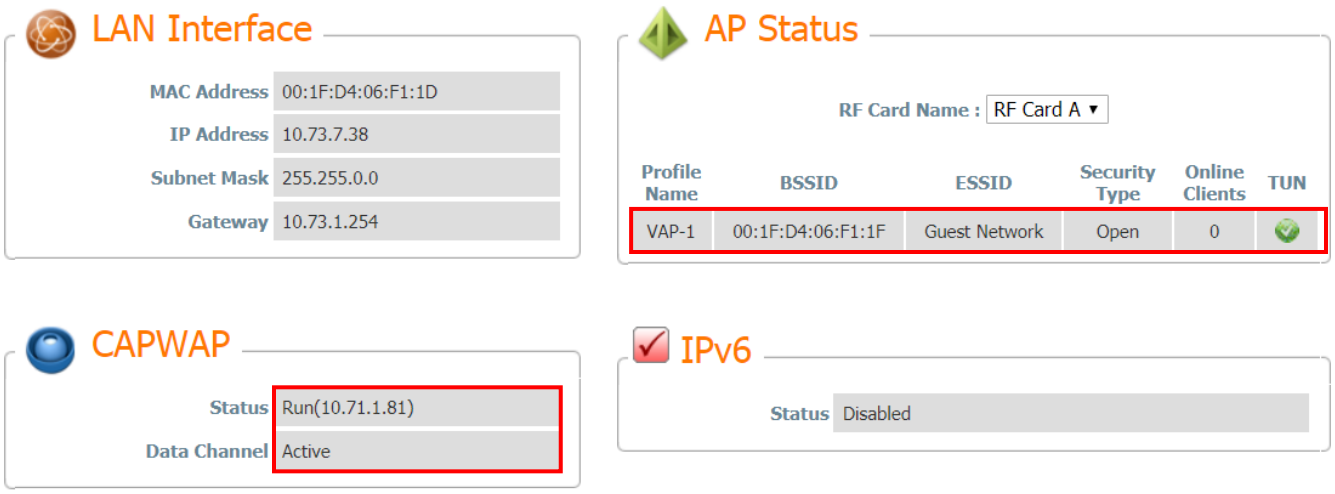
Successful CAPWAP joining will lead to the AP being listed in the managed AP list, as illustrated below:

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.



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

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	✓

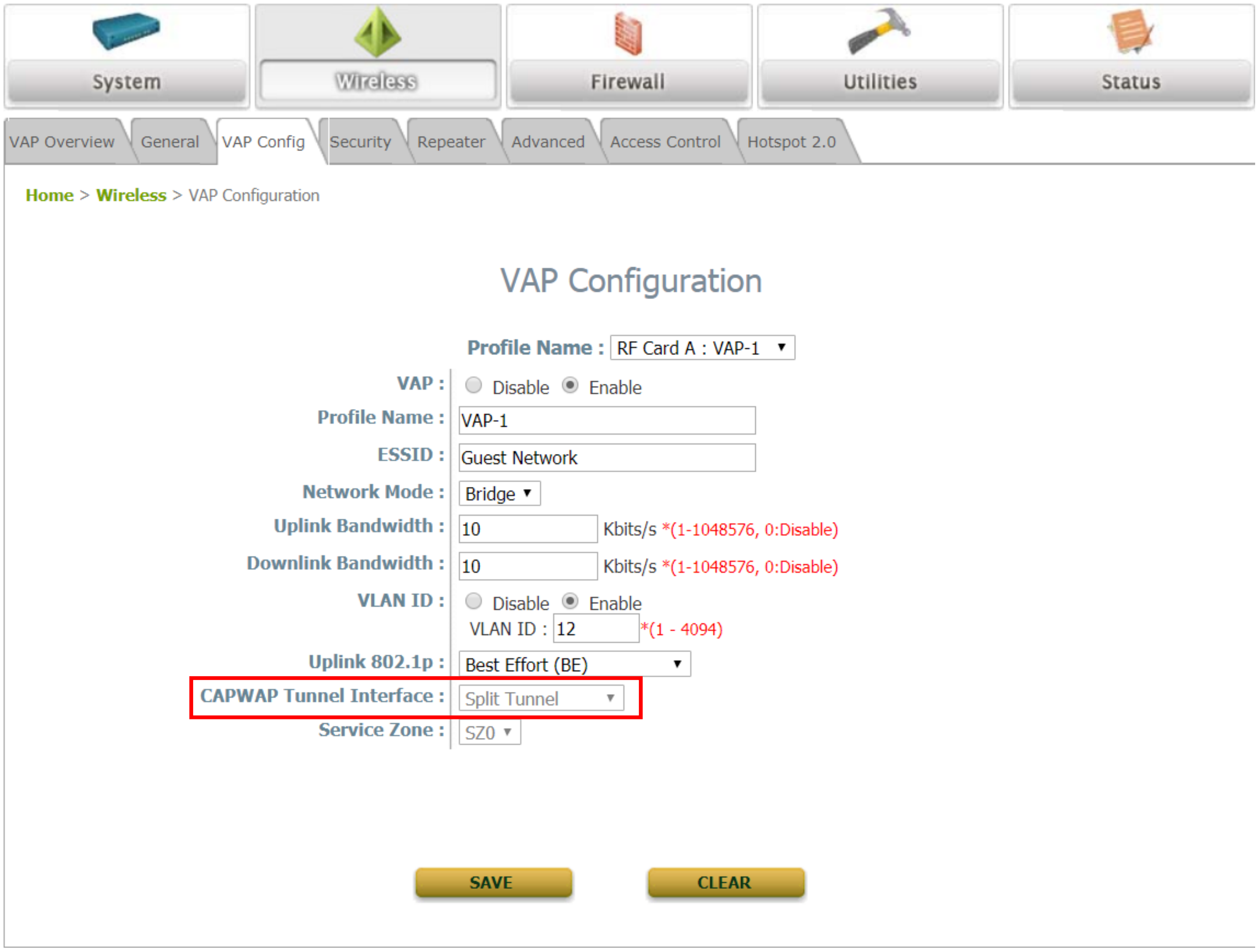
CAPWAP

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
SAVE
CLEAR

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 ▾

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.

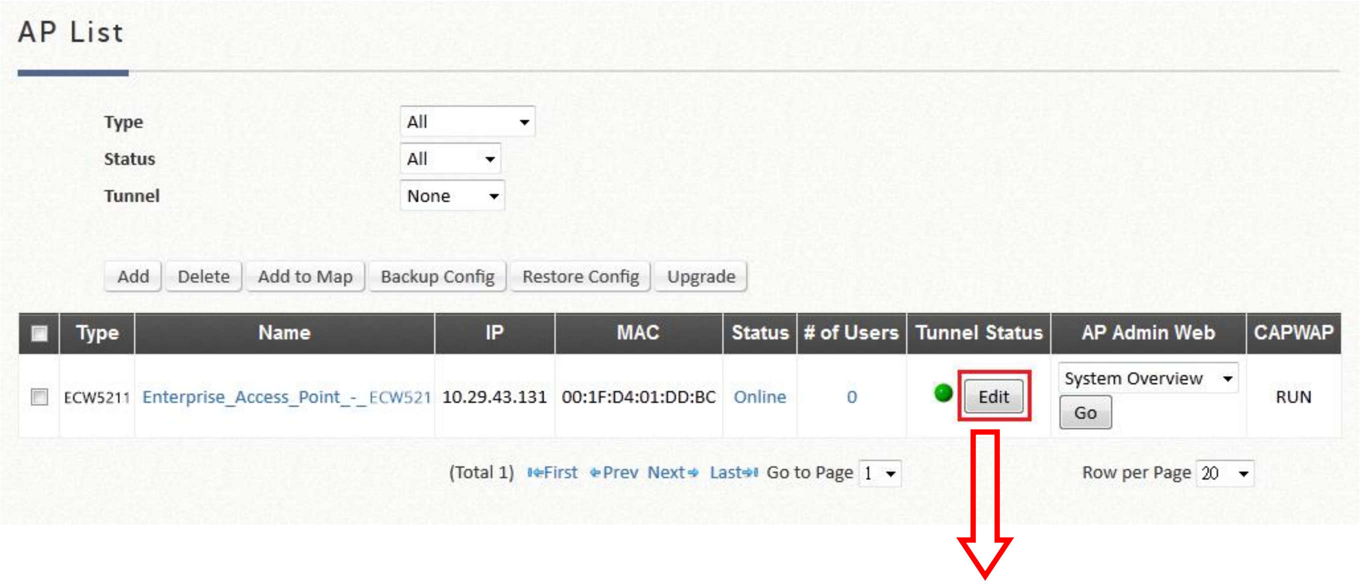
The EWS Controller would automatically identify AP model and update the firmware if necessary and restart the AP. Ensure that the firmware image file is uploaded to the Controller (Main Menu > Devices > WAPM > Firmware), and enable "Automatic Upgrade" (Main Menu > Devices > WAPM > Upgrade).

7.3.5 Tunneled 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.



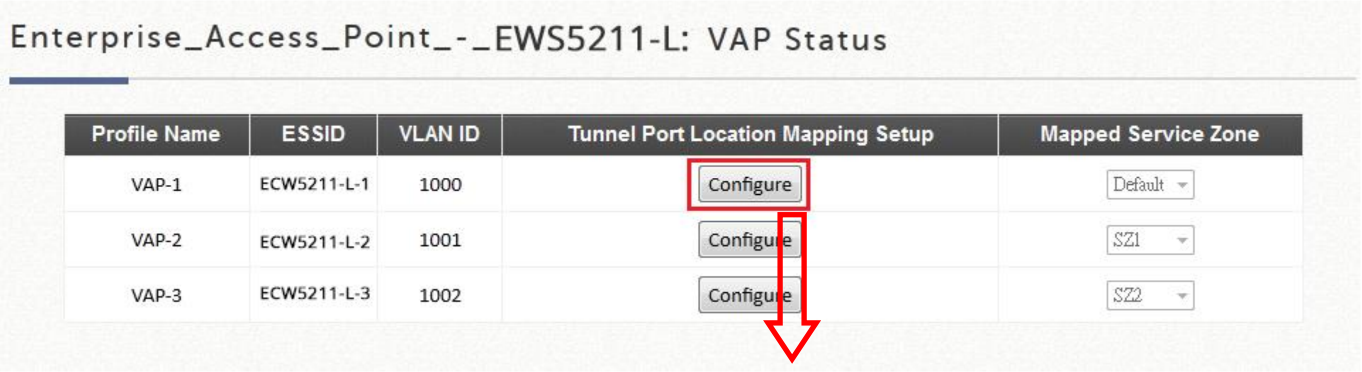
AP List

Type: All
Status: All
Tunnel: None

☐	Type	Name	IP	MAC	Status	# of Users	Tunnel Status	AP Admin Web	CAPWAP
☐	ECW5211	Enterprise_Access_Point_-_ECW521	10.29.43.131	00:1F:D4:01:DD:BC	Online	0	● Edit	System Overview Go	RUN

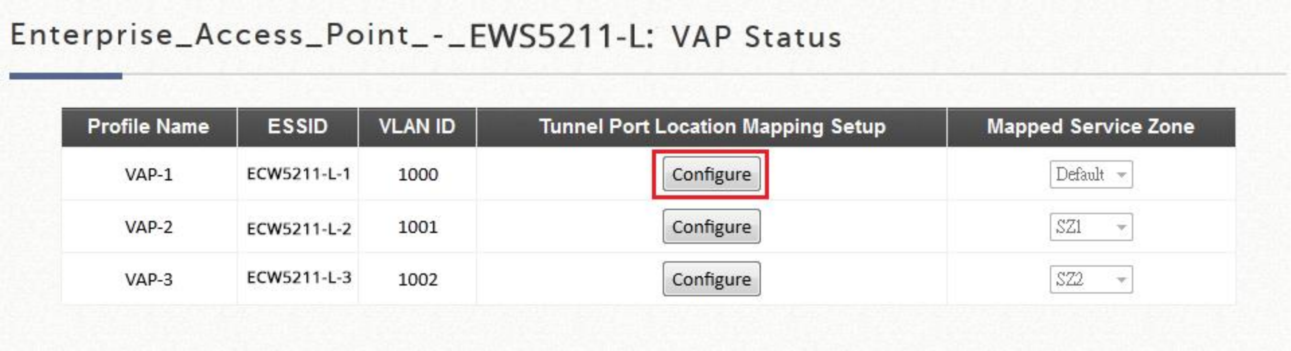
(Total 1) First Prev Next Last Go to Page 1

Row per Page 20



Enterprise_Access_Point_-_EWS5211-L: VAP Status

Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
VAP-1	ECW5211-L-1	1000	Configure	Default
VAP-2	ECW5211-L-2	1001	Configure	SZ1
VAP-3	ECW5211-L-3	1002	Configure	SZ2



Enterprise_Access_Point_-_EWS5211-L: VAP Status

Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
VAP-1	ECW5211-L-1	1000	Configure	Default
VAP-2	ECW5211-L-2	1001	Configure	SZ1
VAP-3	ECW5211-L-3	1002	Configure	SZ2

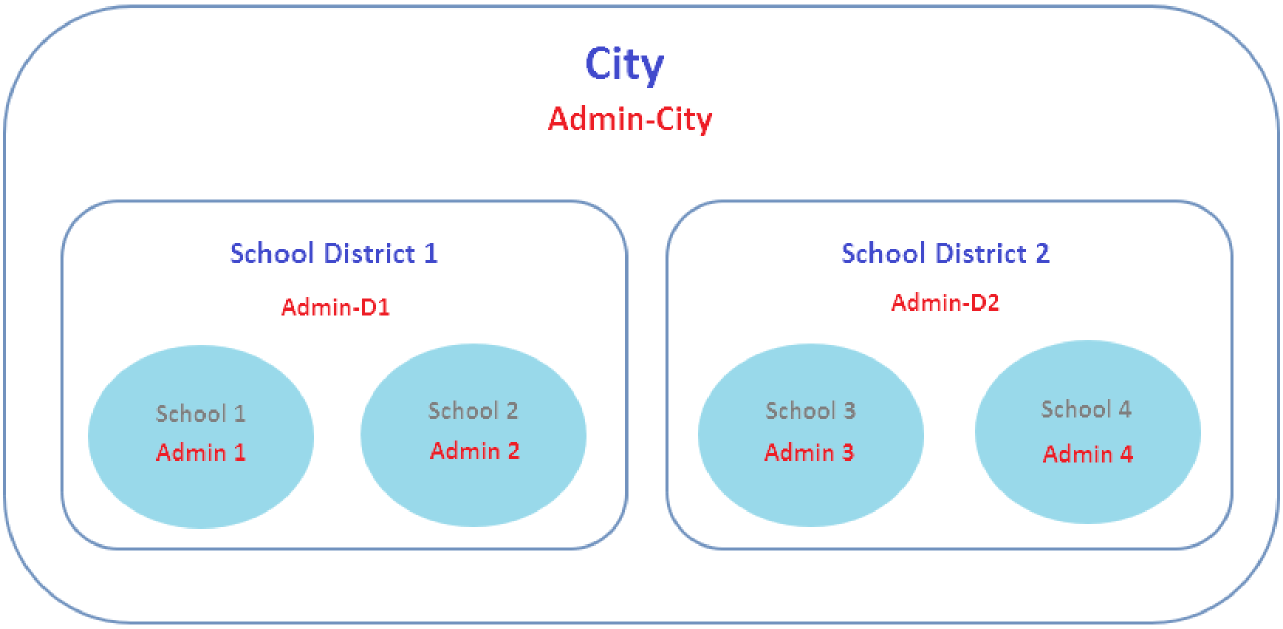
Once the VAP tunneled back, complete tunnel or split tunnel, has been configured with PLM (Port Location Mapping), remote sites may also benefit from the PMS system or other centrally managed hotspot operations which require location attributes or information.

7.3.6 Access Points on Map & 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.

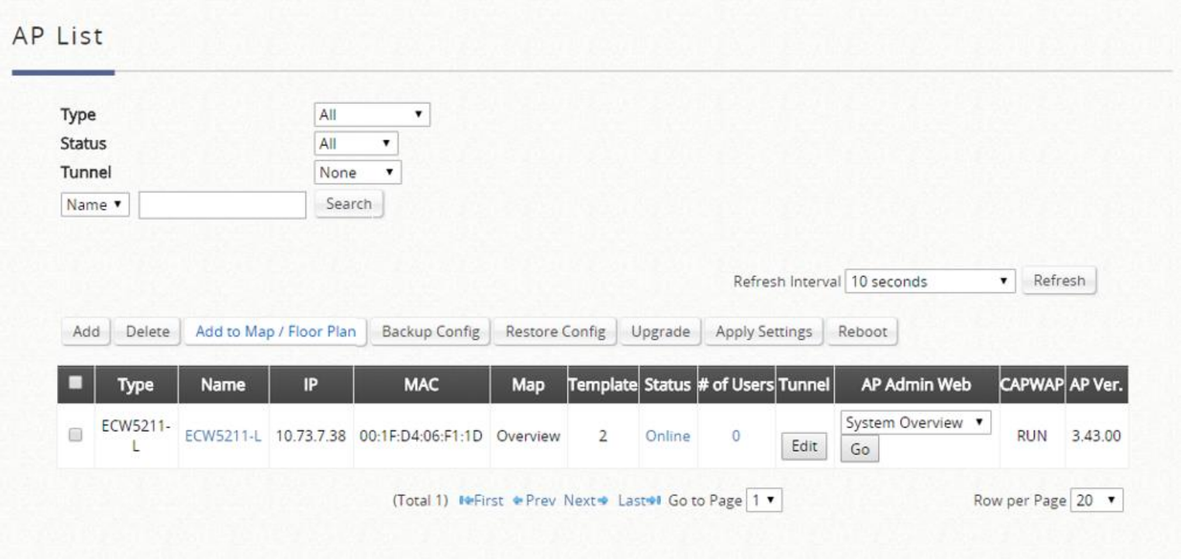
AP grouping allows different levels of administrators to manage APs by different AP group. An AP Group can include multiple maps and AP templates. On the other hand, a map can be included by different AP groups. You may assign different administrator groups to have different read/write permission for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


City
Admin-City
School District 1
Admin-D1
School 1
Admin 1
School 2
Admin 2
School District 2
Admin-D2
School 3
Admin 3
School 4
Admin 4

【A simple concept diagram illustrating AP Grouping】

EWS 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)



AP List

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

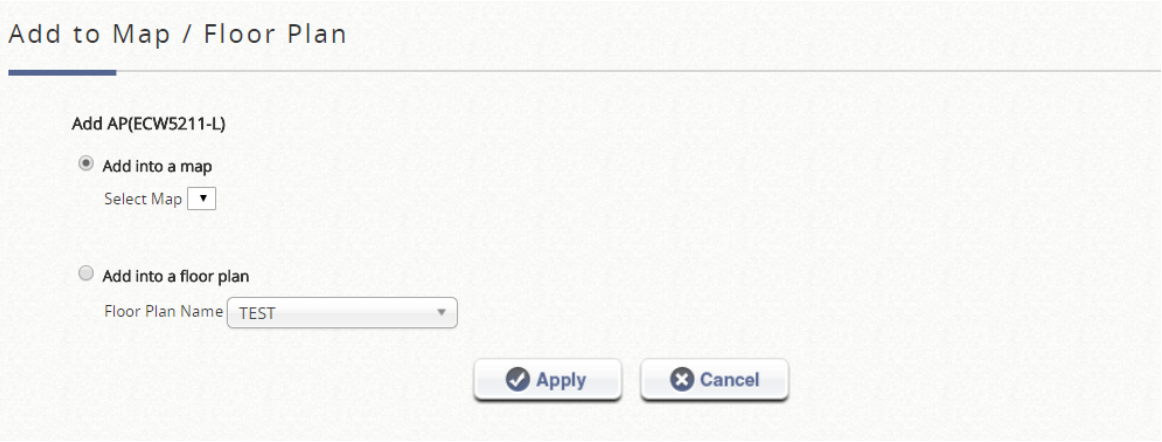
Refresh Interval: 10 seconds Refresh

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

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

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

3. Go back to the List page, choose the AP, and then click the **Add to Map** button, and choose the desired map.



Add to Map / Floor Plan

Add AP(ECW5211-L)

● Add into a map
Select Map

○ Add into a floor plan
Floor Plan Name: TEST

Apply
Cancel

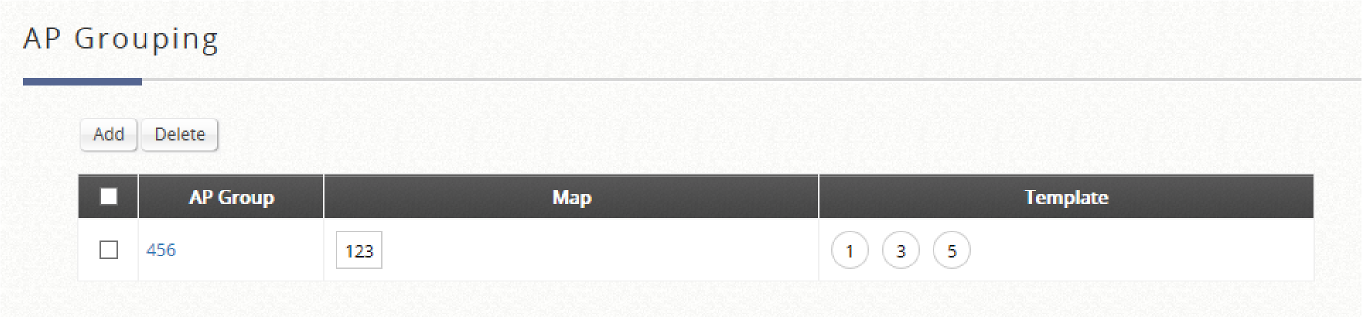
After the settings, admin should be able to see an icon of the AP on the selected map.

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

NOTE

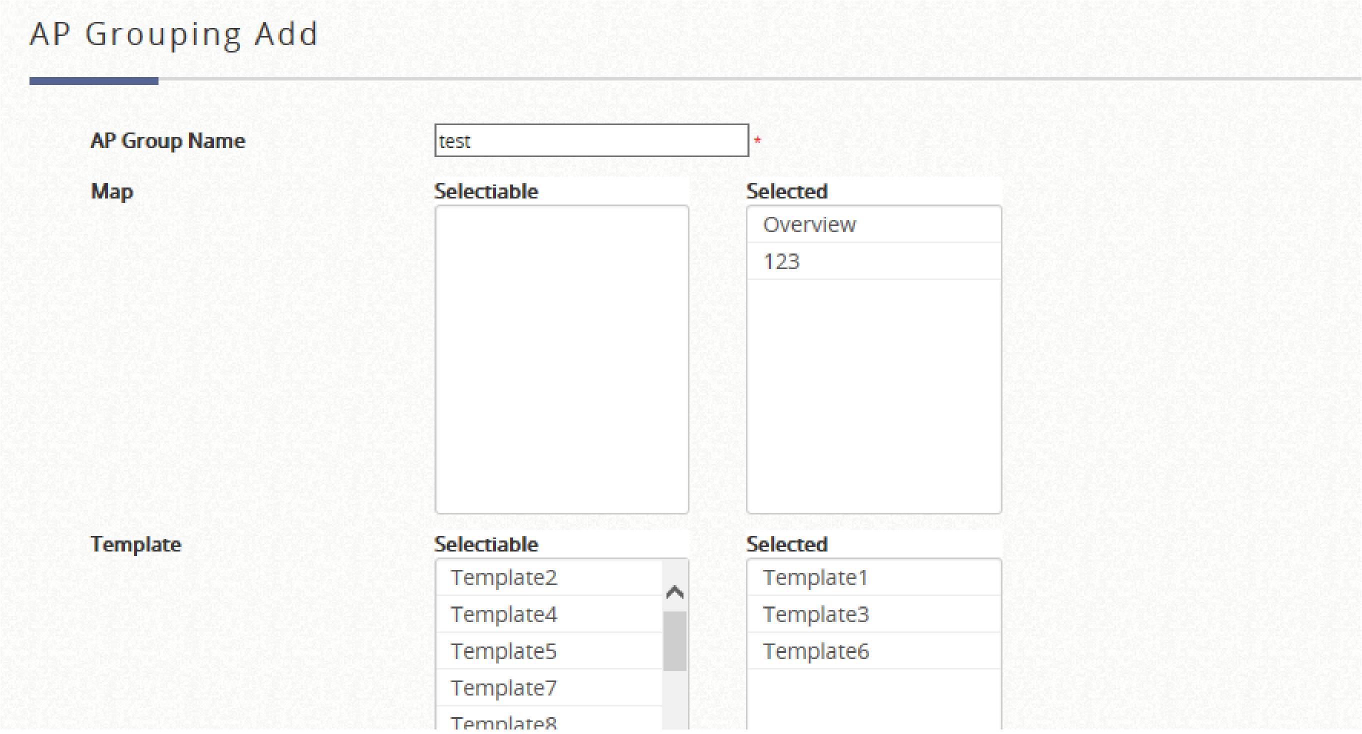
1. The button **Show Coverage** on the main page of **Map** indicates the wireless coverage on the map for the deployment's use. There's also a tool on the bottom of the page for admin to calculate the distance between two APs.

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



☐	AP Group	Map	Template
☐	456	123	① ③ ⑤

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

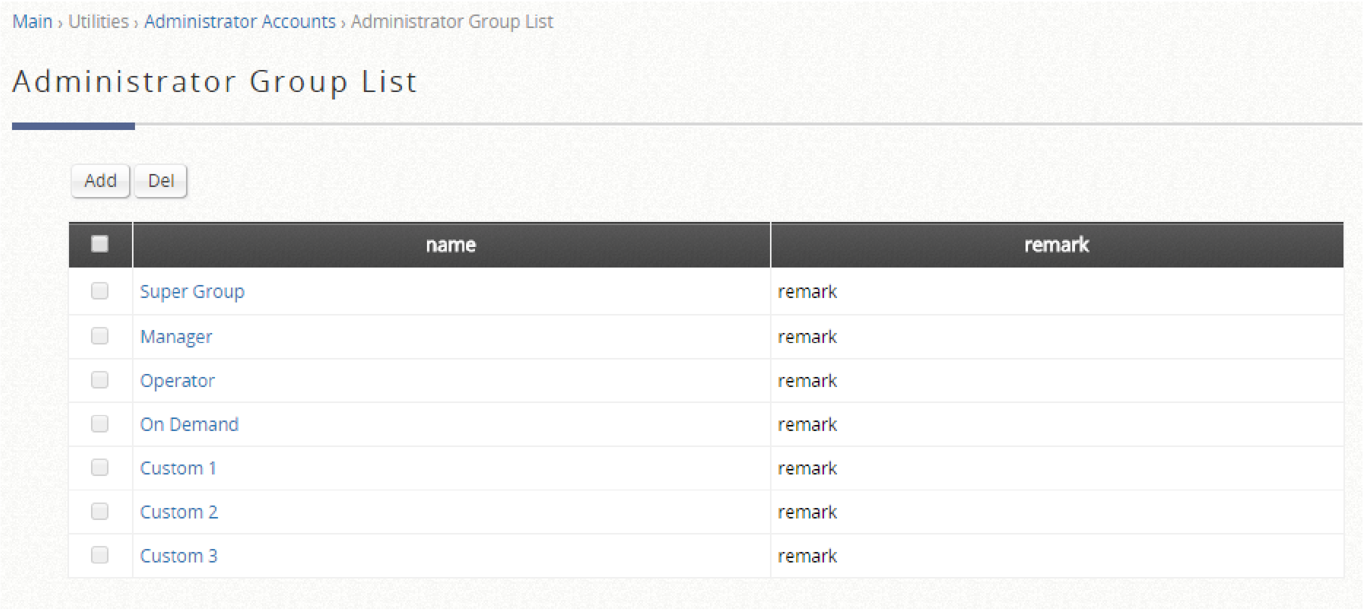


AP Group Name: test *

Map
Selectiable:
Selected: Overview, 123

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

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

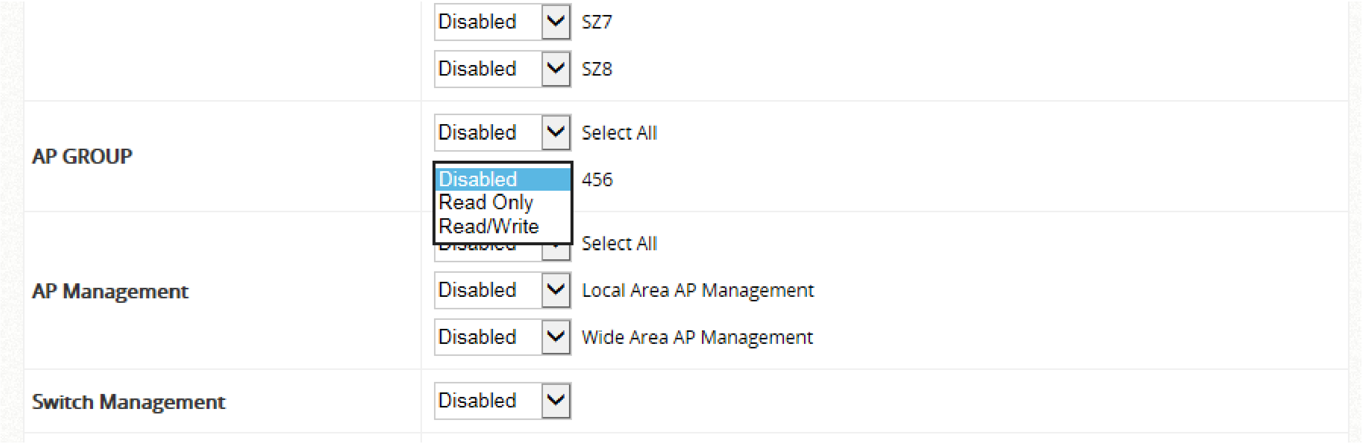


Main › Utilities › Administrator Accounts › Administrator Group List

Administrator Group List

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

Assigning permission to an AP group.

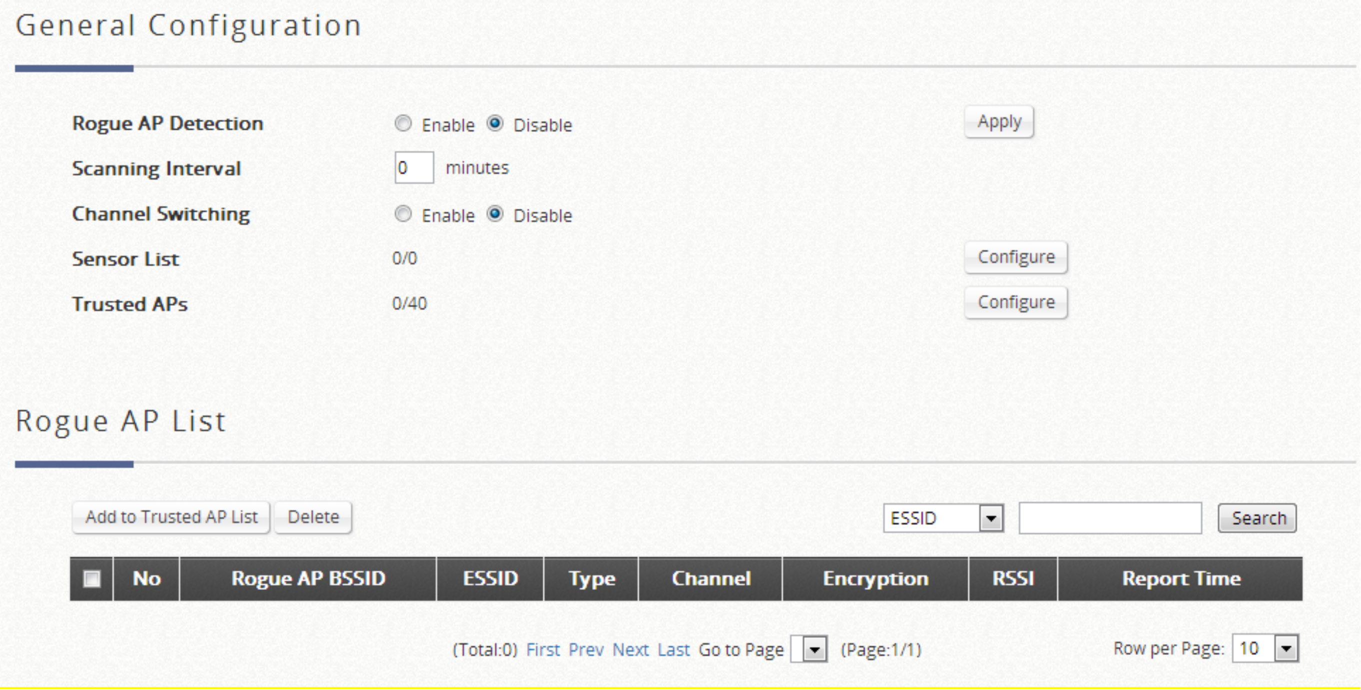


	Disabled	SZ7
	Disabled	SZ8
AP GROUP	Disabled	Select All
	Disabled	456
AP Management	Disabled	Select All
	Disabled	Local Area AP Management
	Disabled	Wide Area AP Management
Switch Management	Disabled	

7.3.7 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.



General Configuration

Rogue AP Detection ○ Enable ● Disable
Scanning Interval 0 minutes
Channel Switching ○ Enable ● Disable
Sensor List 0/0
Trusted APs 0/40

Rogue AP List

☐	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	RSSI	Report Time

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

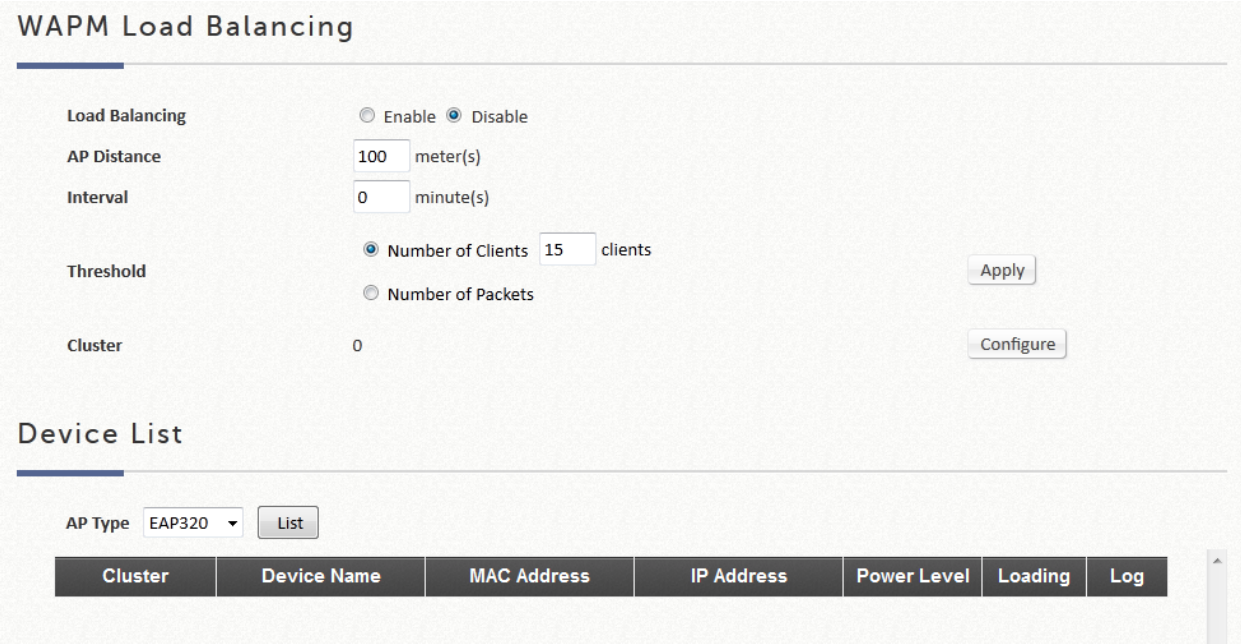
The discovered access points are temporarily put in the Rogue AP list. Click on one of the hyperlinked BSSID's to see its detailed information. However, if admin recognizes some of the listed APs as trusted, just check the checkboxes before the BSSID column and then click **Add to Trusted AP List.**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

7.3.8 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 exceeding a predefined threshold at circumstances and other APs in the same group are still below the threshold, the balancing function will be activated to decrease the overloading APs' transmit power and increase other available APs' transmit power; this would increase chances for other available APs to be associated. The system can divide the managed APs into groups; define the group threshold, and a time interval which will trigger the AP load balancing.

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.

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.


WAPM Load Balancing

Load Balancing ○ Enable ● Disable
AP Distance 100 meter(s)
Interval 0 minute(s)
Threshold ● Number of Clients 15 clients
○ Number of Packets
Cluster 0

Device List

AP Type EAP320

Cluster	Device Name	MAC Address	IP Address	Power Level	Loading	Log

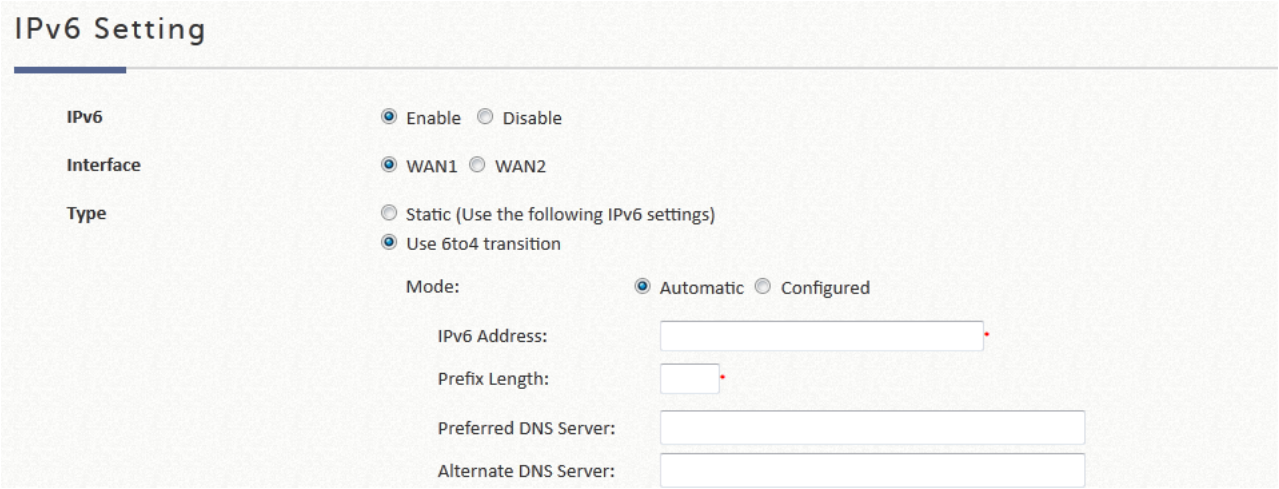
These are automatically calculated by the Controller via the distance attributes of each of the managed AP profile.

Chapter 8. Advanced Settings for Network Environment

8.1 IPv4 / IPv6 Dual Stack Network

Configuration Path: Main Menu >> System >> IPv6

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

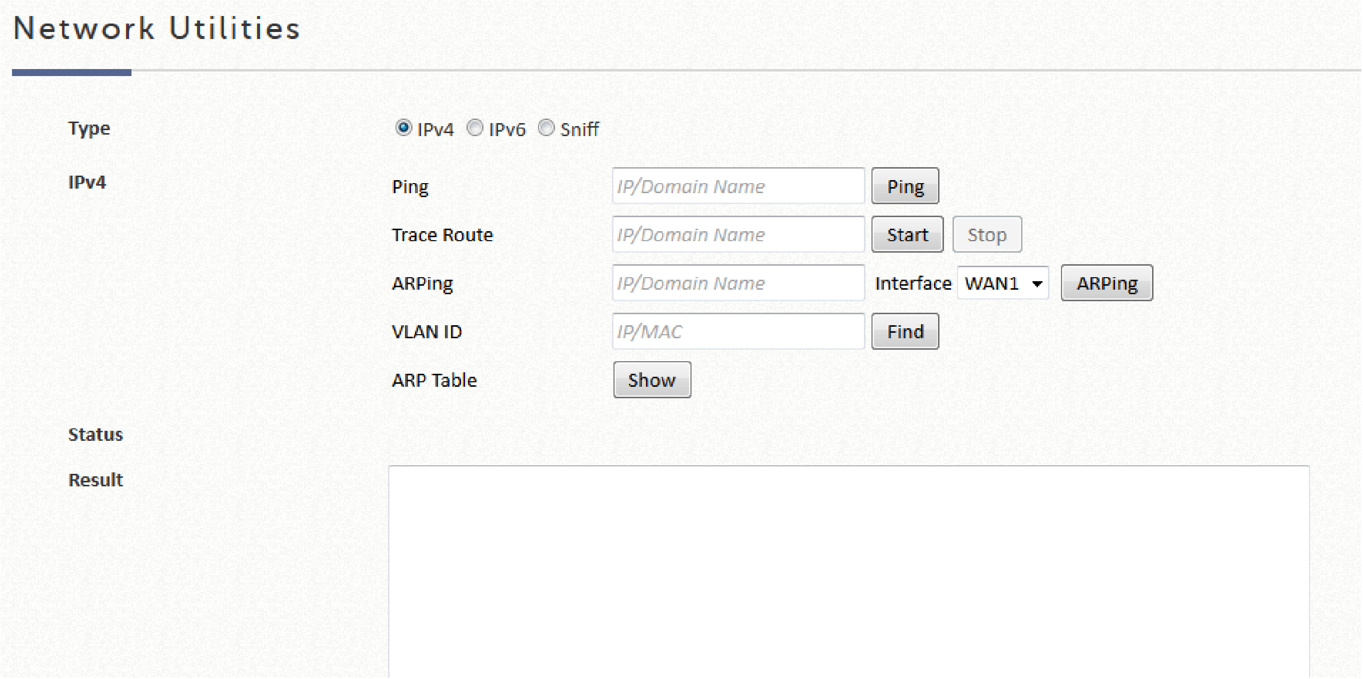
IPv6 ● Enable ○ Disable
Interface ● WAN1 ○ WAN2
Type ○ Static (Use the following IPv6 settings)
● Use 6to4 transition
Mode: ● Automatic ○ Configured
IPv6 Address:
Prefix Length:
Preferred DNS Server:
Alternate DNS Server:

- **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: ● IPv4 ○ IPv6 ○ Sniff

IPv4

Ping
IP/Domain Name
Ping
Trace Route
IP/Domain Name
Start
Stop
ARPing
IP/Domain Name
Interface
WAN1
ARPing
VLAN ID
IP/MAC
Find
ARP Table
Show
Status
Result

Item	Description
IPv4	▪ **Ping:** It allows administrator to detect a device using IP address or Host domain name to see if it is responding. ▪ **Trace Route:** It allows administrator to recover the real path of packets from the gateway to a destination using IP address or Host domain name. ▪ **ARPing:** Allows administrator to send ARP request for a specific IP address or domain name. ▪ **ARP Table:** It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).
IPv6	▪ **Ping:** It allows administrator to detect a device using IPv6 address or Host domain name to see if it is responding. ▪ **Trace Route 6:** It allows administrator to recover the real path of packets from the gateway to a destination using IPv6 address or Host domain name. ▪ **Neighbor Discovery:** The administrator can use this feature to learn about IPv6 Neighbor nodes that are on the same IP segment or domain name. ▪ **Neighbor Cache:** a node 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.
Sniff	With this feature the administrator can listen for packets from selected Interfaces. The administrator can further filter the types of packets to capture by using tcpdump commands under the **Expression** field.

Status	When the administrator is executing any Network Utilities features, the status of the operation is displayed here.
Result	The operation result is displayed here.

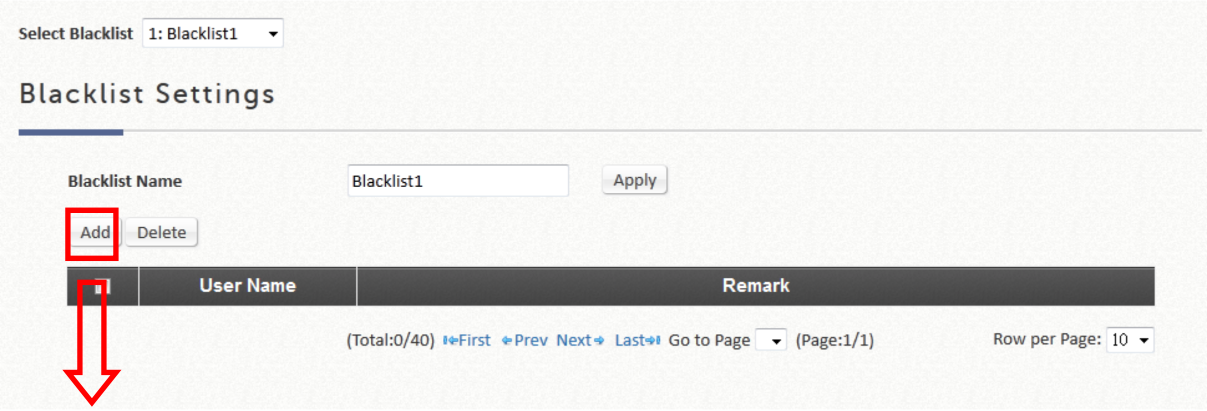
8.2 User Access Control

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.

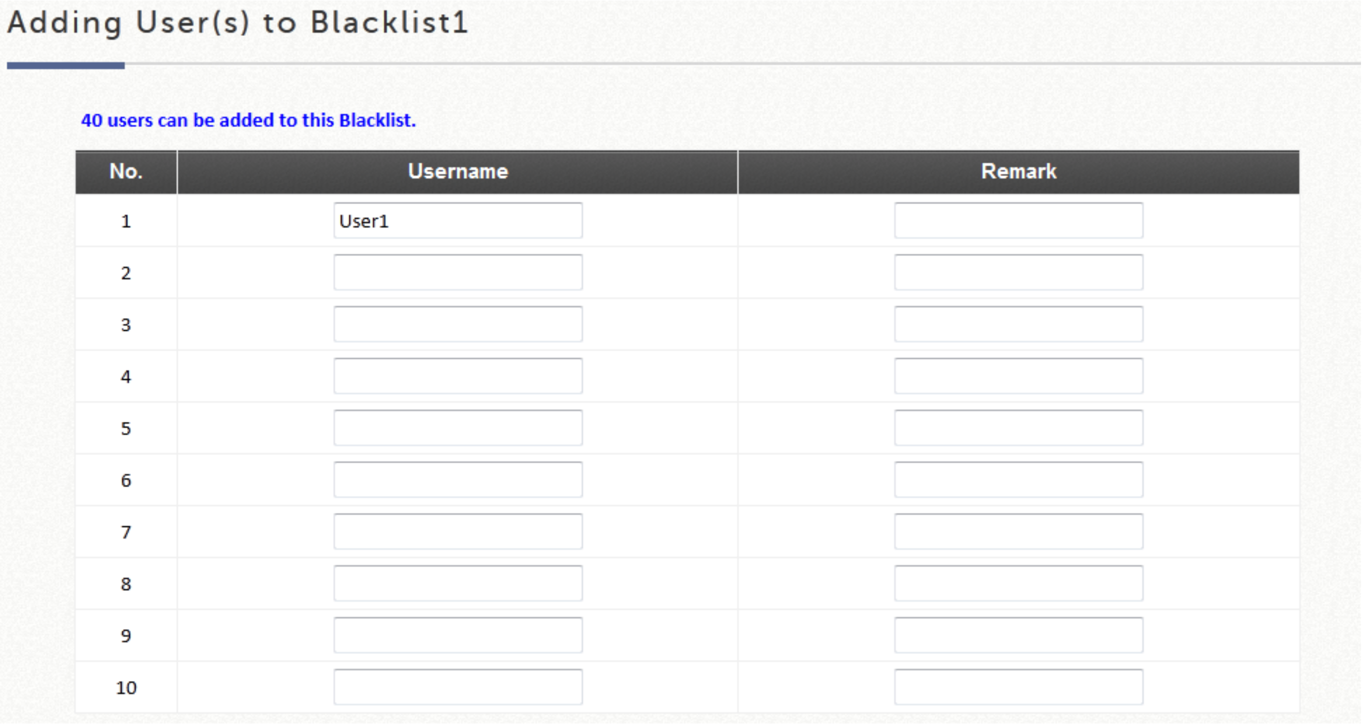

Select Blacklist: 1: Blacklist1

Blacklist Settings

Blacklist Name: Blacklist1

☐	User Name	Remark

(Total:0/40) First Prev Next Last Go to Page (Page:1/1) Row per Page: 10



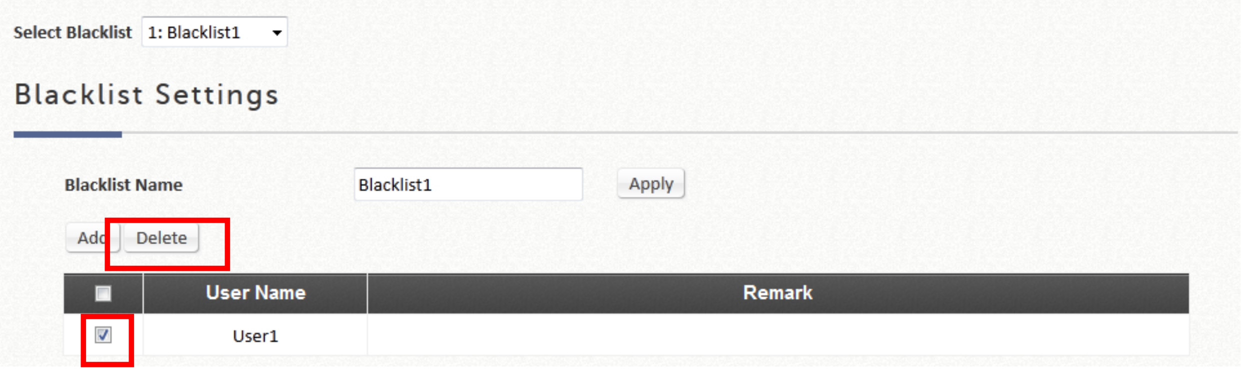
Adding User(s) to Blacklist1

40 users can be added to this Blacklist.

No.	Username	Remark
1	User1	
2		
3		
4		
5		
6		
7		
8		
9		
10		

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.



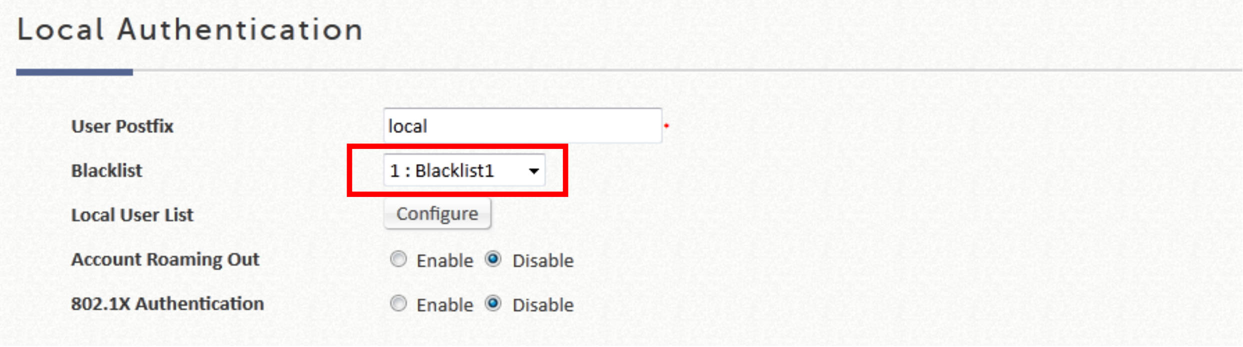
Select Blacklist: 1: Blacklist1

Blacklist Settings

Blacklist Name: Blacklist1

☐	User Name	Remark
☑	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

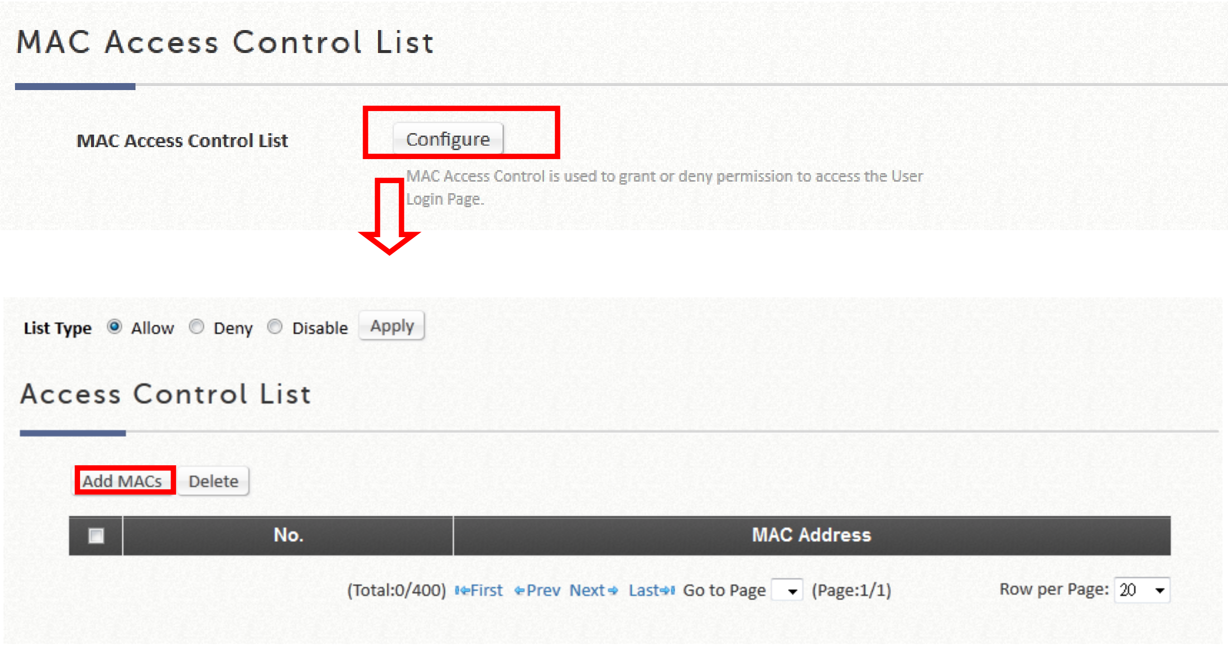
Account Roaming Out: ○ Enable ● Disable

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
Access Control List
Add MACs
Delete

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

List Type ● Allow ○ Deny ○ Disable Apply

☐	No.	MAC Address

(Total:0/400) First Prev Next Last Go to Page (Page:1/1) Row per Page: 20

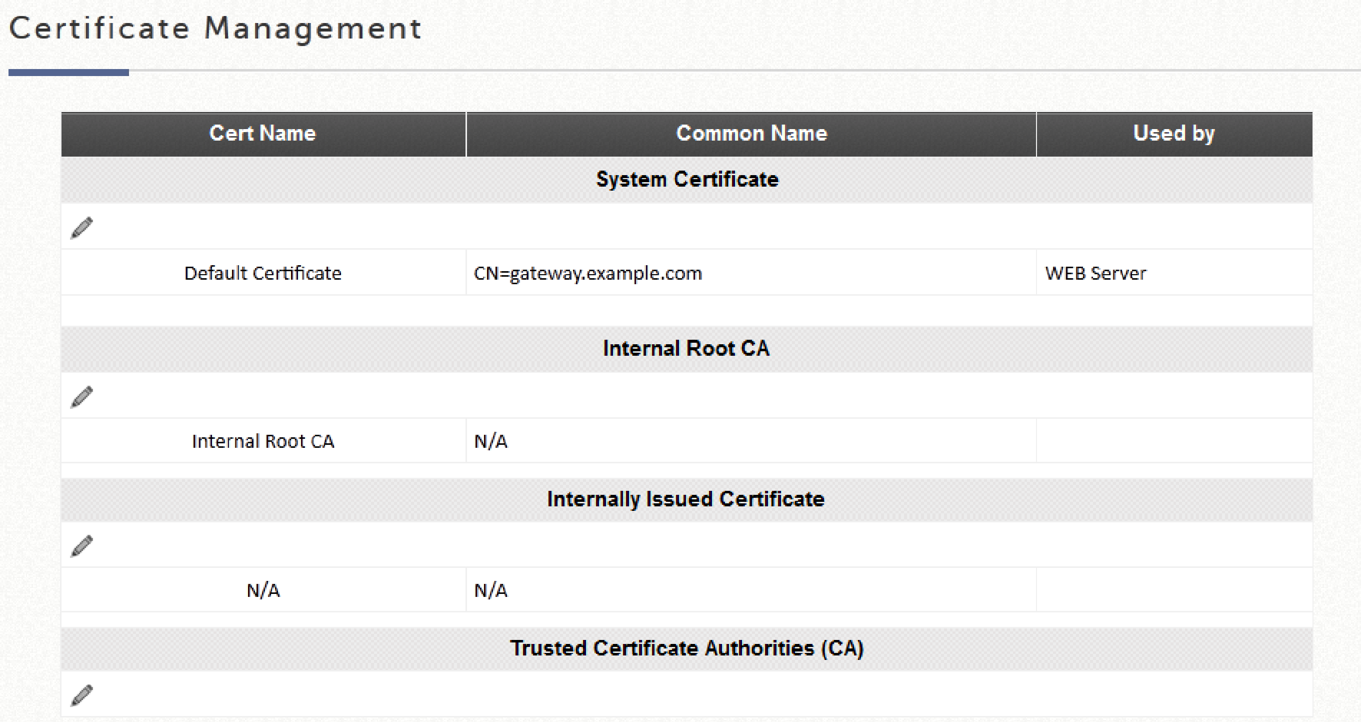
NOTE

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.



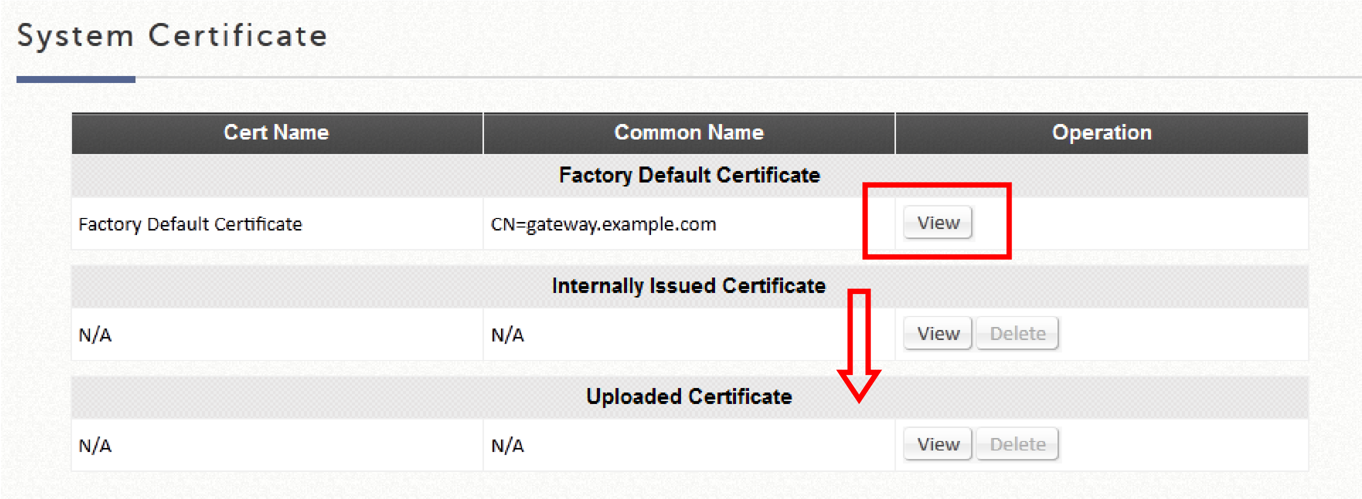
Certificate Management

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

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

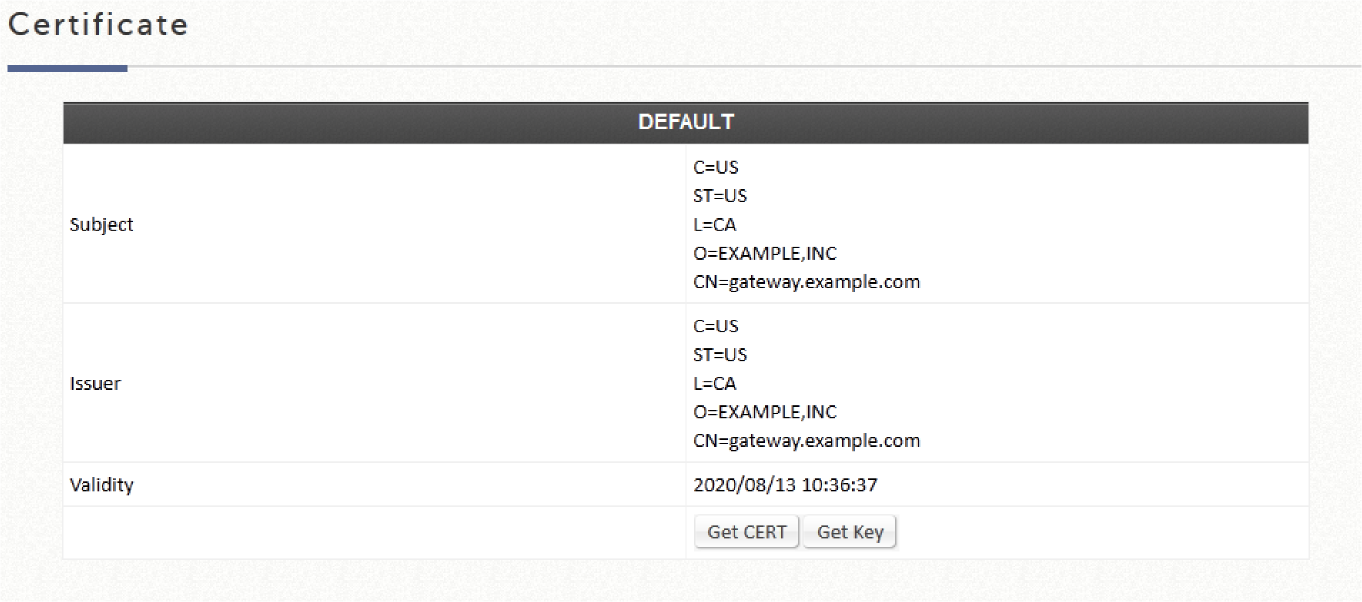
8.3.1. System Certificate

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. 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	View
Internally Issued Certificate		
N/A	N/A	View Delete
Uploaded Certificate		
N/A	N/A	View Delete

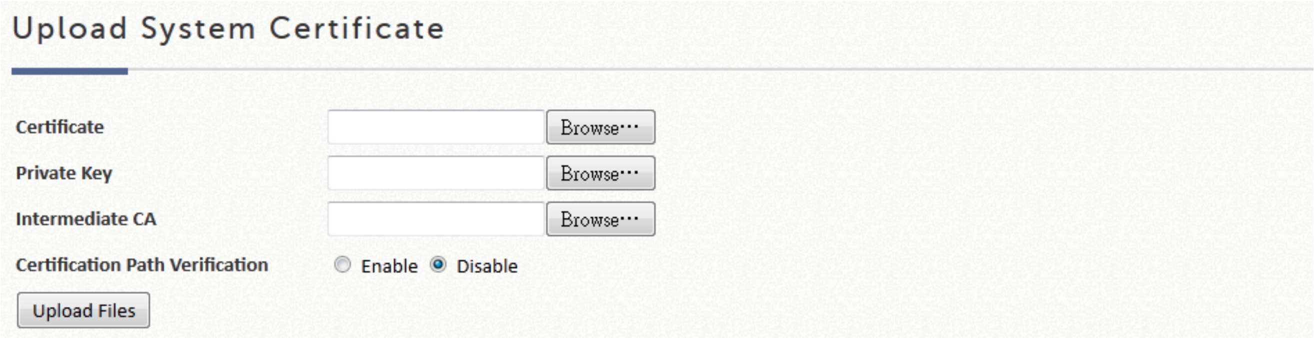


Certificate

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
	Get CERT Get Key

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.

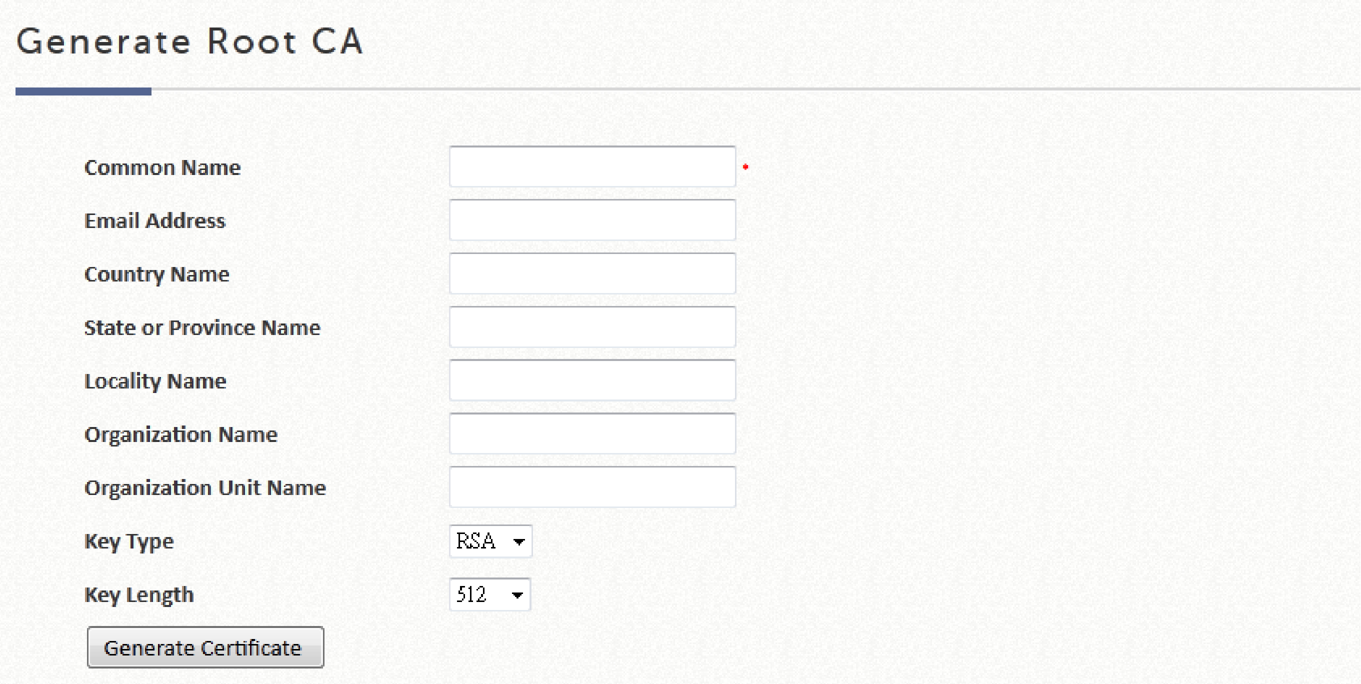


Upload System Certificate

Certificate	Browse…
Private Key	Browse…
Intermediate CA	Browse…
Certification Path Verification	○ Enable ● Disable

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.

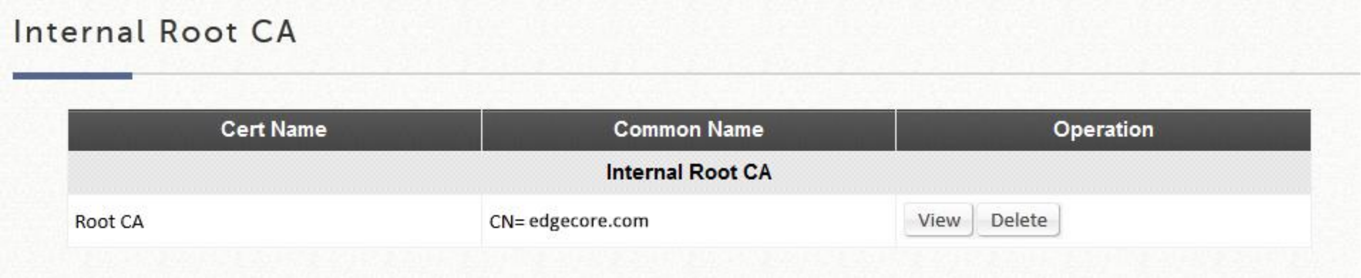


Generate Root CA

Common Name	*
Email Address	
Country Name	
State or Province Name	
Locality Name	
Organization Name	
Organization Unit Name	
Key Type	RSA
Key Length	512

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.



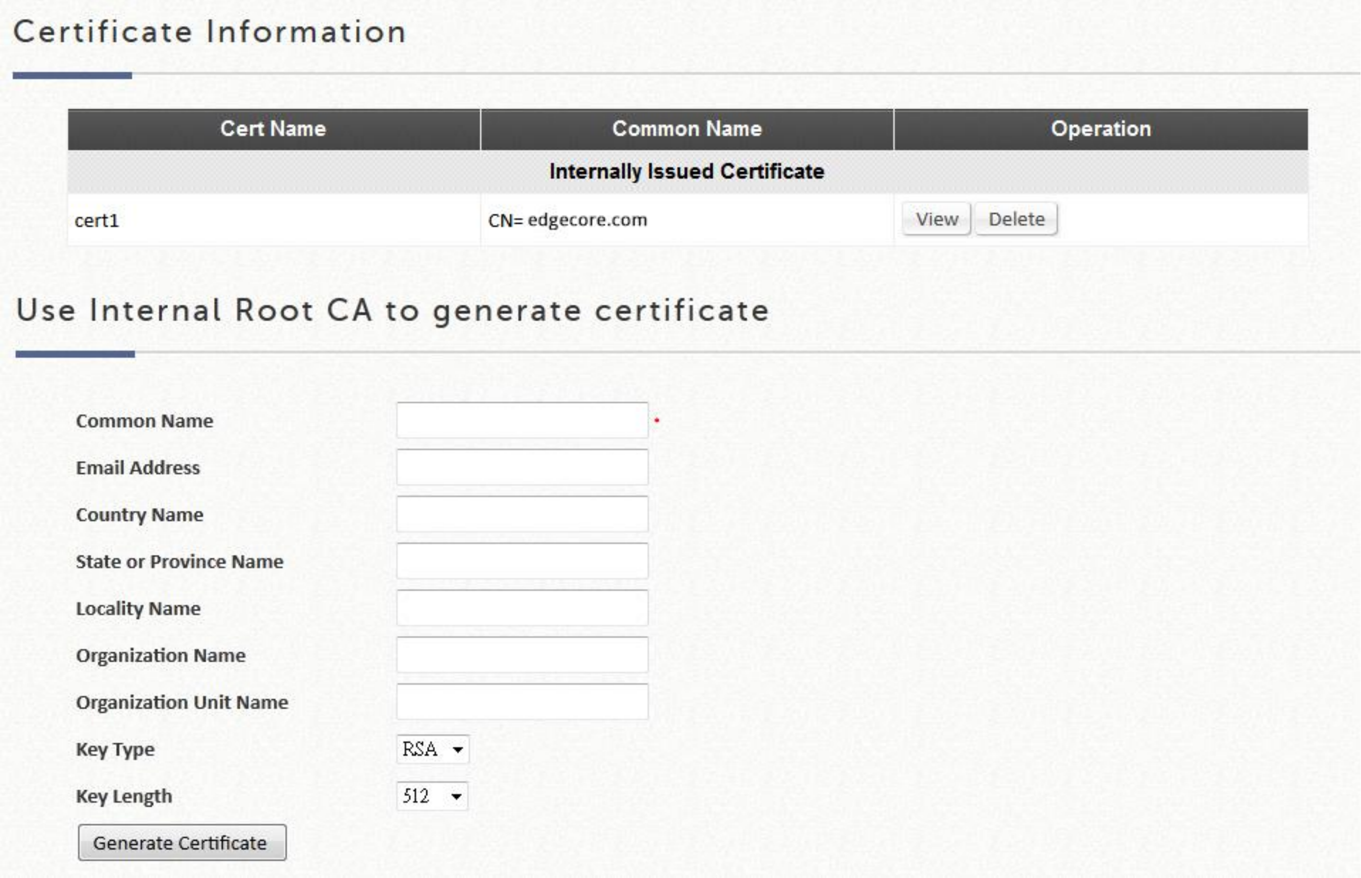
Internal Root CA

Cert Name	Common Name	Operation
Internal Root CA		
Root CA	CN= edgecore.com	View Delete

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

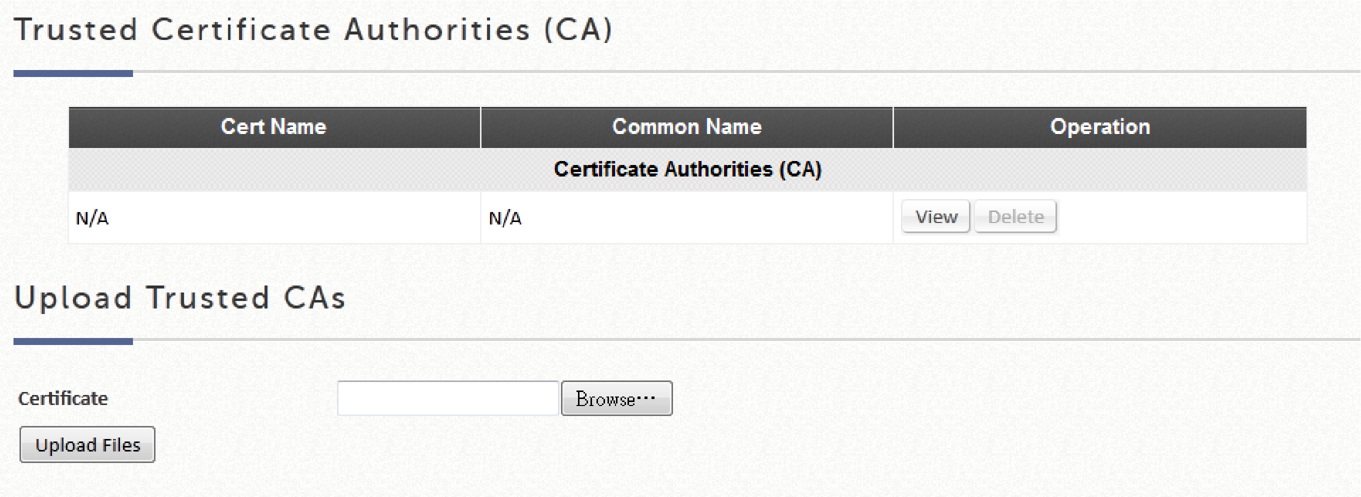
Cert Name	Common Name	Operation
Internally Issued Certificate		
cert1	CN= edgecore.com	View Delete

Use Internal Root CA to generate certificate

Common Name	*
Email Address	
Country Name	
State or Province Name	
Locality Name	
Organization Name	
Organization Unit Name	
Key Type	RSA
Key Length	512

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	View Delete

Upload Trusted CAs

8.4 Management Access

Configuration path: Main Menu >> System >> General >> Management IP Address

On the EWS 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

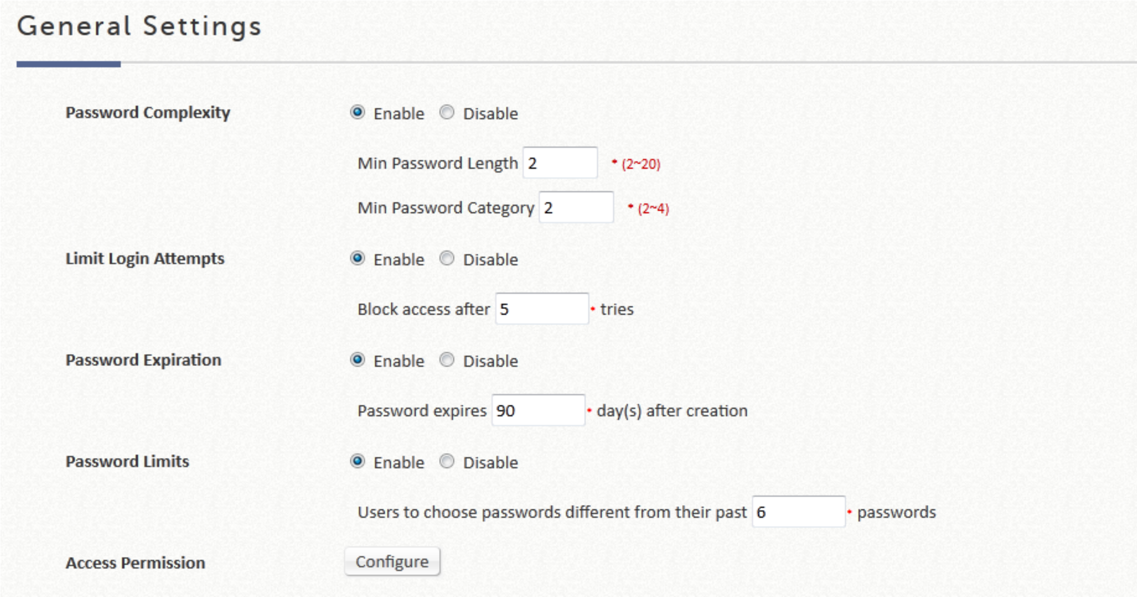
Configuration path: Main Menu >> Utilities >> Administrator Account

The EWS controller’s root management account is the “admin” account with full access, modification and application privilege and authority. There are however, 2nd 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

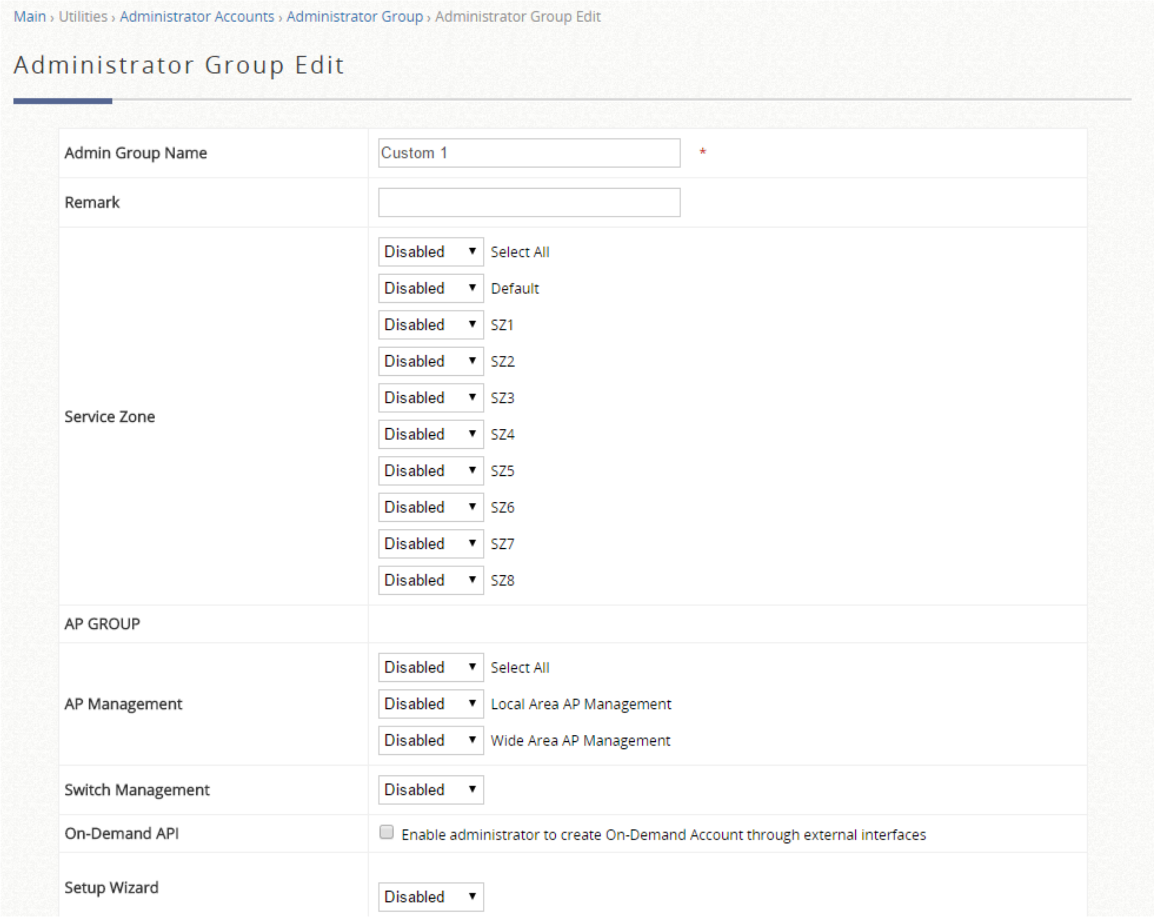


General Settings

Password Complexity	● Enable ○ Disable
	Min Password Length 2 * (2~20)
	Min Password Category 2 * (2~4)
Limit Login Attempts	● Enable ○ Disable
	Block access after 5 * tries
Password Expiration	● Enable ○ Disable
	Password expires 90 * day(s) after creation
Password Limits	● Enable ○ Disable
	Users to choose passwords different from their past 6 * passwords
Access Permission	Configure

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



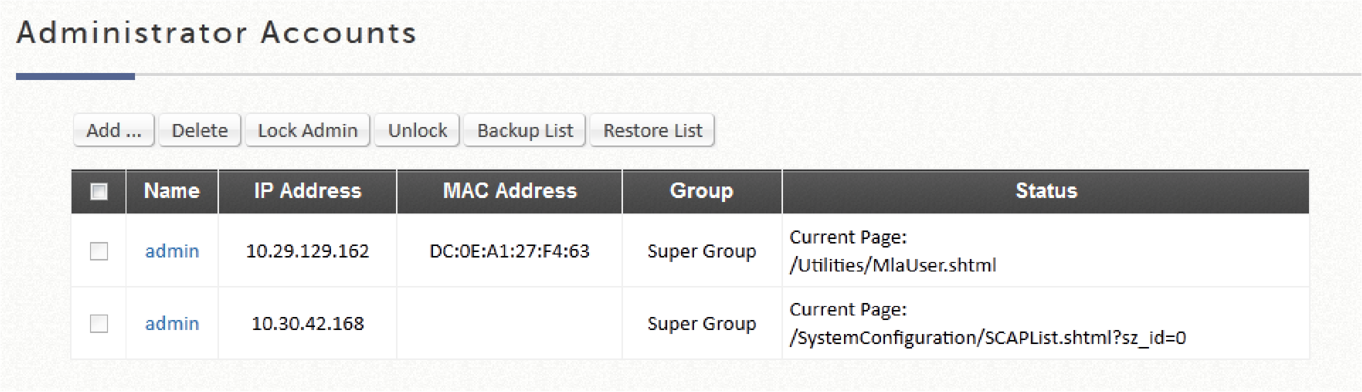
Main › Utilities › Administrator Accounts › Administrator Group › Administrator Group Edit

Administrator Group Edit

Admin Group Name	Custom 1 *
Remark	
Service Zone	Disabled ▾ Select All Disabled ▾ Default Disabled ▾ SZ1 Disabled ▾ SZ2 Disabled ▾ SZ3 Disabled ▾ SZ4 Disabled ▾ SZ5 Disabled ▾ SZ6 Disabled ▾ SZ7 Disabled ▾ SZ8
AP GROUP	
AP Management	Disabled ▾ Select All Disabled ▾ Local Area AP Management Disabled ▾ Wide Area AP Management
Switch Management	Disabled ▾
On-Demand API	☐ 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.



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

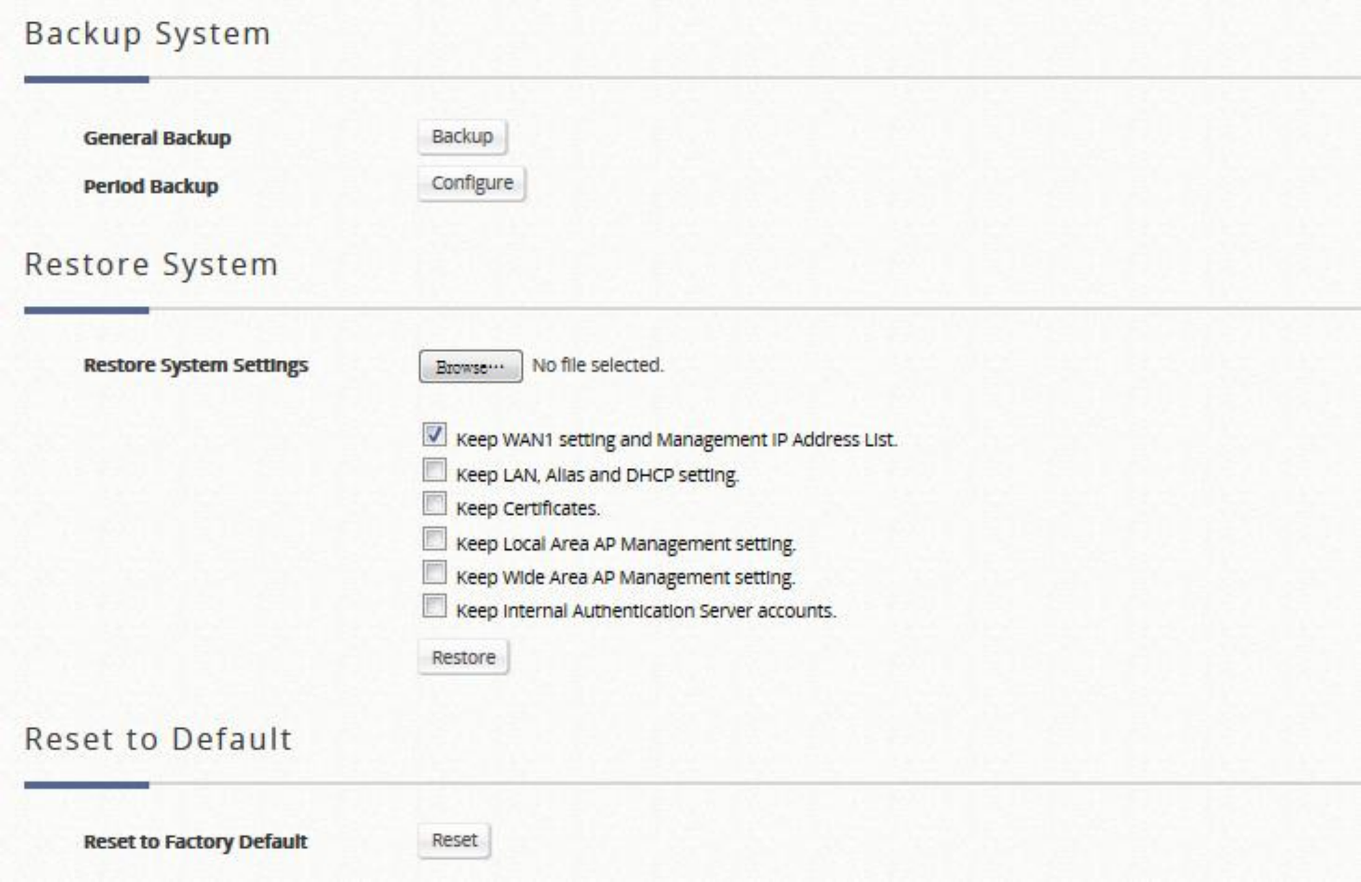
NOTE

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.



Backup System

General Backup

Period Backup

Restore System

Restore System Settings — No file selected.

☑ Keep WAN1 setting and Management IP Address List.
☐ Keep LAN, Alias and DHCP setting.
☐ Keep Certificates.
☐ Keep Local Area AP Management setting.
☐ Keep Wide Area AP Management setting.
☐ Keep Internal Authentication Server accounts.

Reset to Default

Reset to Factory Default

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.

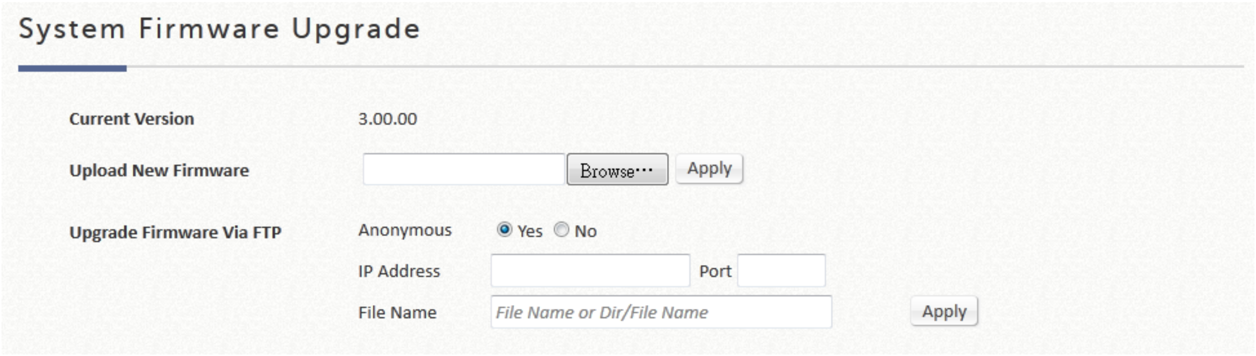
9.3 Firmware Upgrade

Configuration path: Main Menu >> Utilities >> System Upgrade

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

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.


System Firmware Upgrade

Current Version 3.00.00

Upload New Firmware

Upgrade Firmware Via FTP

Anonymous ● Yes ○ No

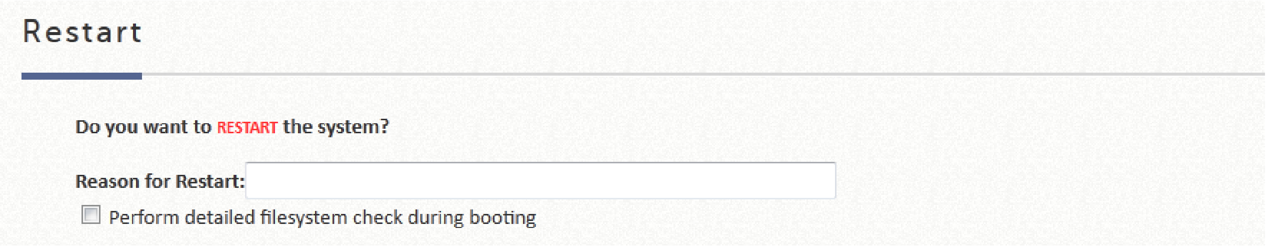
NOTE

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

Do you want to RESTART the system?

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.

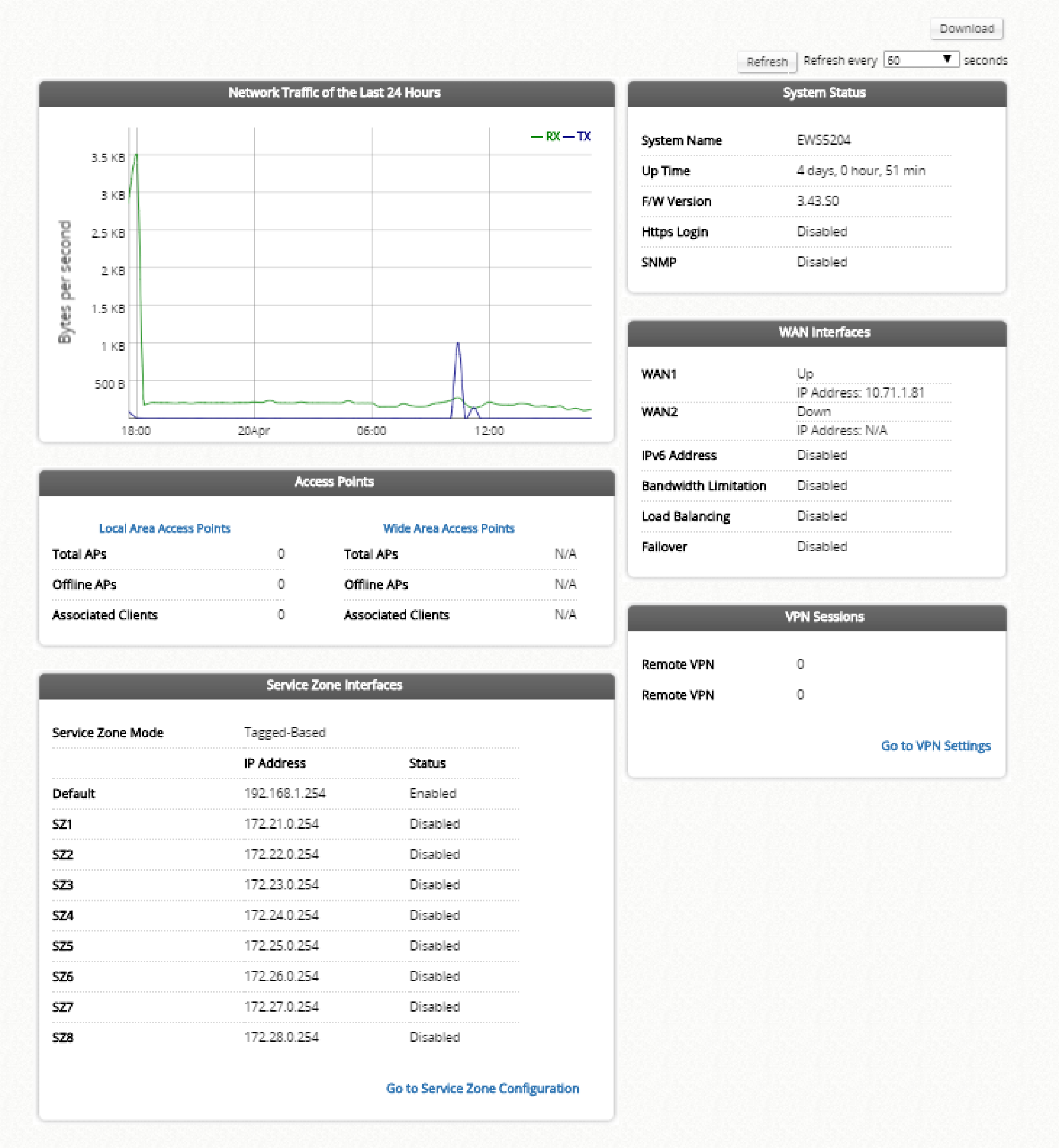
Chapter 10. Reports and Logs for Monitoring

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


Download
Refresh
Refresh every 60 ▼ seconds
Network Traffic of the Last 24 Hours
— RX — TX
3.5 KB
3 KB
2.5 KB
2 KB
1.5 KB
1 KB
500 B
Bytes per second
18:00
20Apr
06:00
12:00

System Status

System Name	EWS5204
Up Time	4 days, 0 hour, 51 min
F/W Version	3.43.50
Https Login	Disabled
SNMP	Disabled

WAN Interfaces

WAN1	Up IP Address: 10.71.1.81
WAN2	Down IP Address: N/A
IPv6 Address	Disabled
Bandwidth Limitation	Disabled
Load Balancing	Disabled
Failover	Disabled

VPN Sessions

Remote VPN	0
Remote VPN	0

Go to VPN Settings

Access Points

Local Area Access Points		Wide Area Access Points	
Total APs	0	Total APs	N/A
Offline APs	0	Offline APs	N/A
Associated Clients	0	Associated Clients	N/A

Service Zone Interfaces

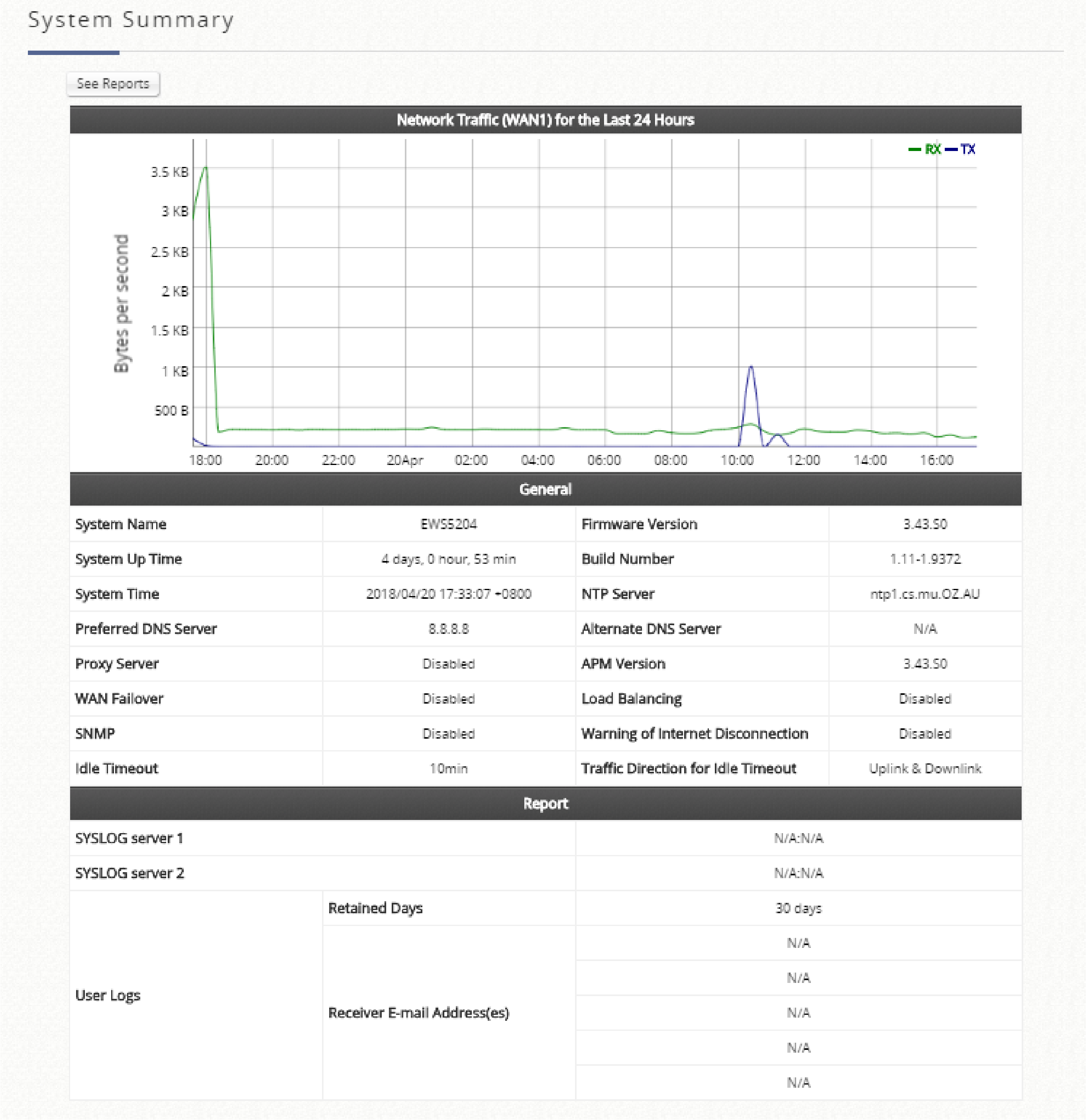
Service Zone Mode	Tagged-Based	
	IP Address	Status
Default	192.168.1.254	Enabled
SZ1	172.21.0.254	Disabled
SZ2	172.22.0.254	Disabled
SZ3	172.23.0.254	Disabled
SZ4	172.24.0.254	Disabled
SZ5	172.25.0.254	Disabled
SZ6	172.26.0.254	Disabled
SZ7	172.27.0.254	Disabled
SZ8	172.28.0.254	Disabled

Go to Service Zone Configuration

10.1.2 System Summary

Configuration path: Main Menu >> Status >> System Summary

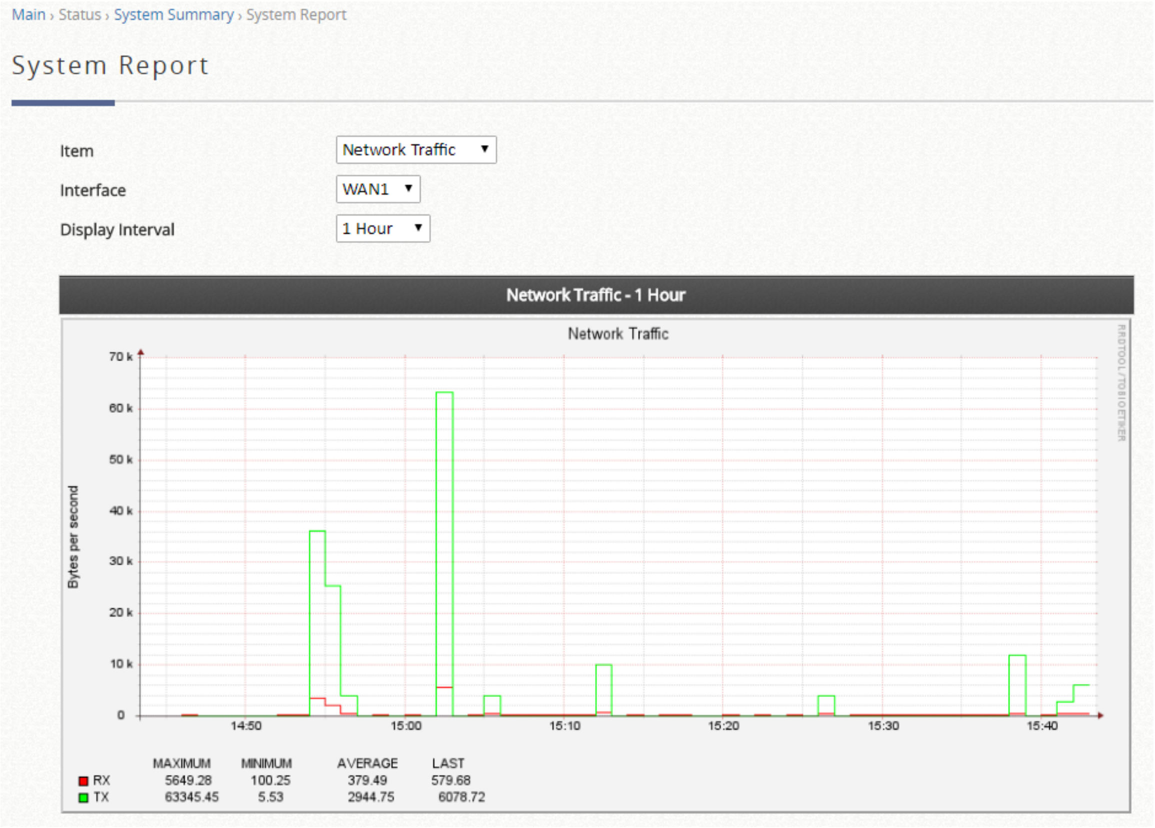
The system status page displays a table of contents including system firmware version, report servers configured, WAN optional settings, User log profile, system time and session control settings. This overview is designed for main configuration items. For detailed status, please proceed to corresponding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


System Summary
See Reports
Network Traffic (WAN1) for the Last 24 Hours
RX
TX
Bytes per second
3.5 KB
3 KB
2.5 KB
2 KB
1.5 KB
1 KB
500 B
18:00
20:00
22:00
20Apr
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00

General			
System Name	EWS5204	Firmware Version	3.43.50
System Up Time	4 days, 0 hour, 53 min	Build Number	1.11-1.9372
System Time	2018/04/20 17:33:07 +0800	NTP Server	ntp1.cs.mu.OZ.AU
Preferred DNS Server	8.8.8.8	Alternate DNS Server	N/A
Proxy Server	Disabled	APM Version	3.43.50
WAN Failover	Disabled	Load Balancing	Disabled
SNMP	Disabled	Warning of Internet Disconnection	Disabled
Idle Timeout	10min	Traffic Direction for Idle Timeout	Uplink & Downlink

Report		
SYSLOG server 1		N/A:N/A
SYSLOG server 2		N/A:N/A
User Logs	Retained Days	30 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
		N/A
		N/A

A selection of Reports is available when the “See Reports” button is clicked. These reports can be sorted based on interface and intervals.



Main › Status › System Summary › System Report

System Report

Item: Network Traffic
Interface: WAN1
Display Interval: 1 Hour

Network Traffic - 1 Hour

Network Traffic
Bytes per second
70 k
60 k
50 k
40 k
30 k
20 k
10 k
0
14:50
15:00
15:10
15:20
15:30
15:40
RRDTOOL / TOBI OETIKER

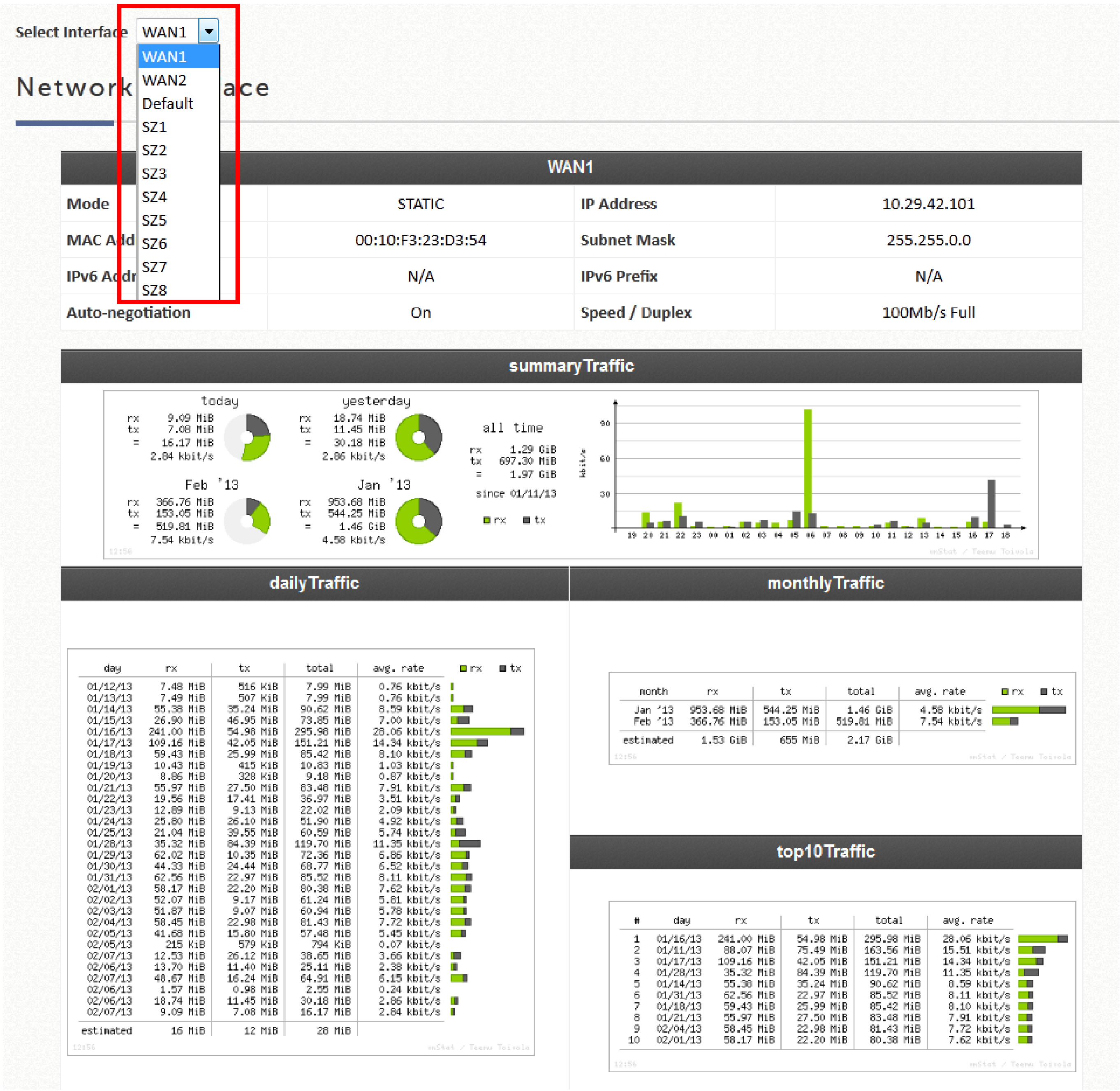
	MAXIMUM	MINIMUM	AVERAGE	LAST
🟥 RX	5649.28	100.25	379.49	579.68
🟩 TX	63345.45	5.53	2944.75	6078.72

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.



WAN1			
Mode	STATIC	IP Address	10.29.42.101
MAC Add	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	yesterday
rx	9.09 MiB	18.74 MiB
tx	7.08 MiB	11.45 MiB
=	16.17 MiB	30.18 MiB
	2.84 kbit/s	2.86 kbit/s

	Feb '13	Jan '13
rx	366.76 MiB	953.68 MiB
tx	153.05 MiB	544.25 MiB
=	519.81 MiB	1.46 GiB
	7.54 kbit/s	4.58 kbit/s

all time
rx 1.29 GiB
tx 697.30 MiB
= 1.97 GiB
since 01/11/13

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	151.21 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	26.10 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	80.38 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
02/06/13	13.70 MiB	11.40 MiB	25.11 MiB	2.38 kbit/s
02/07/13	48.67 MiB	16.24 MiB	64.91 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	01/16/13	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	151.21 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	80.38 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.

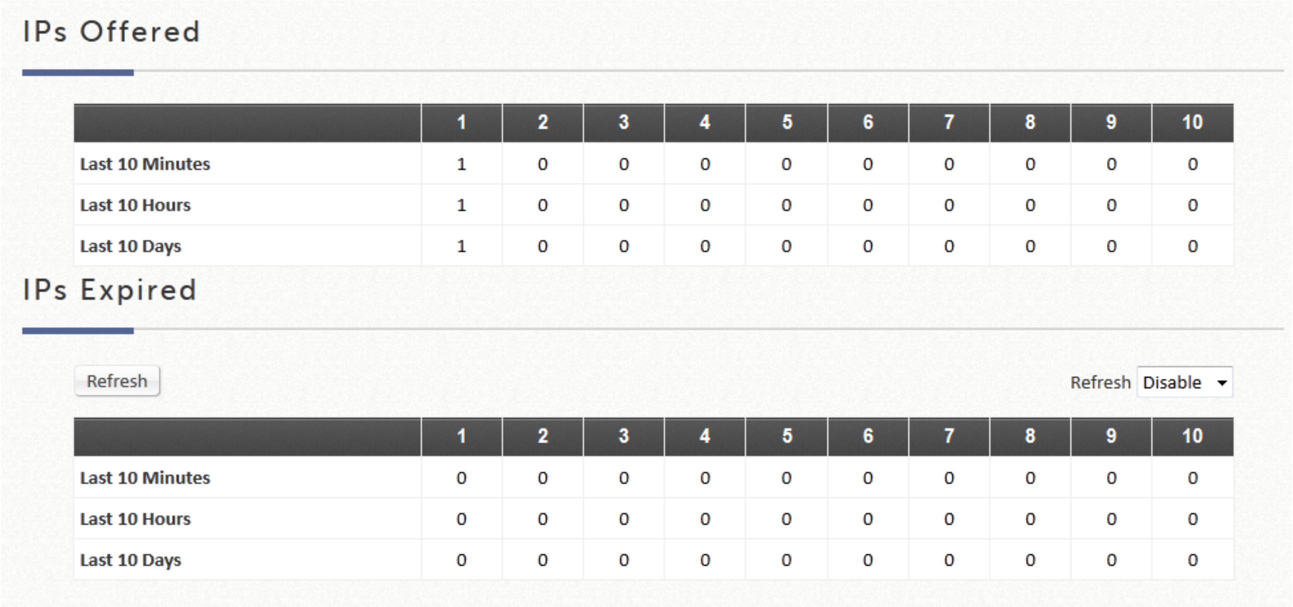
10.1.5 DHCP Server

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

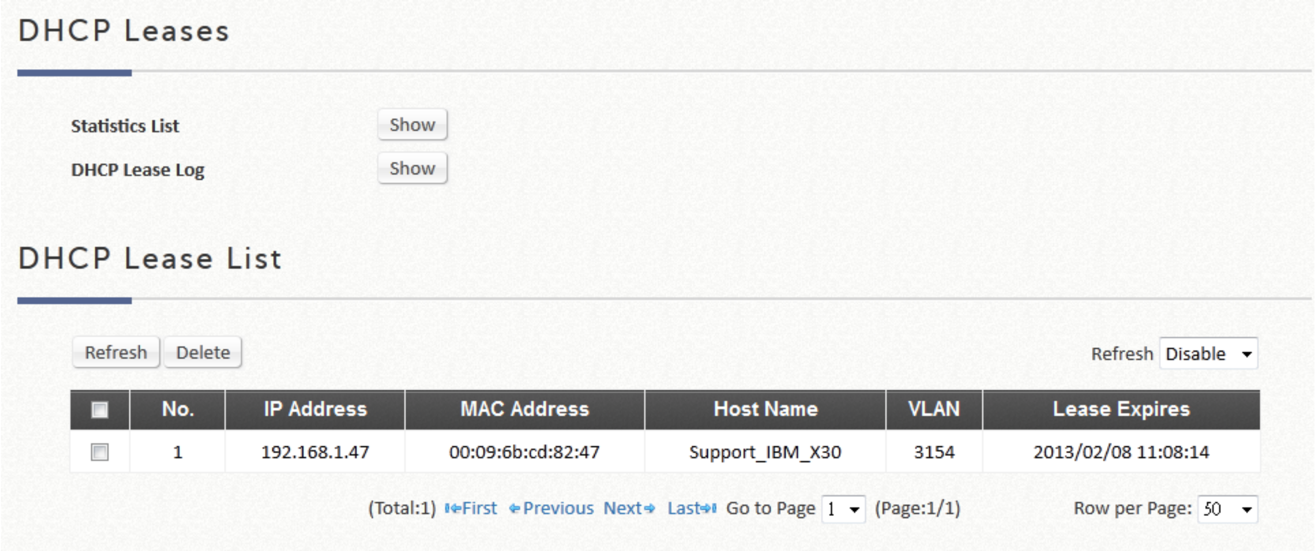
IPs Expired

Refresh: 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

DHCP Lease List

Refresh: Disable

☐	No.	IP Address	MAC Address	Host Name	VLAN	Lease Expires
☐	1	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	3154	2013/02/08 11:08:14

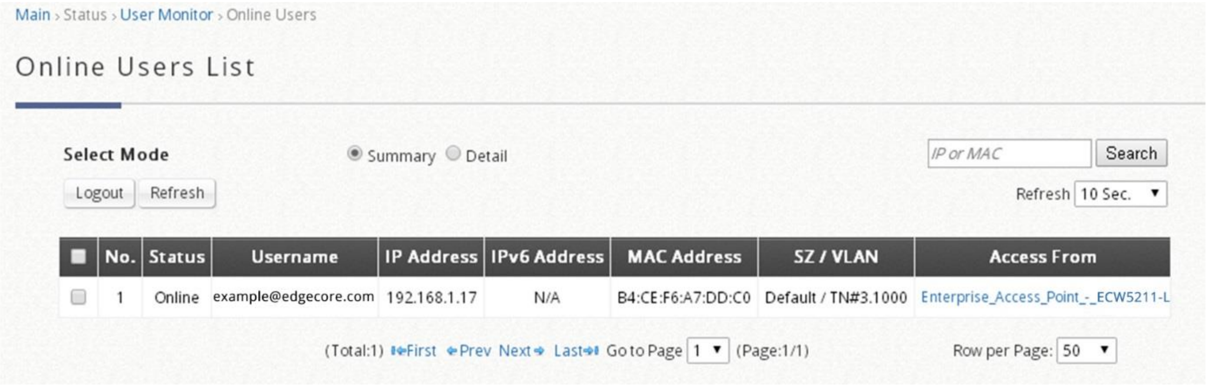
(Total:1) First Previous Next Last Go to Page 1 (Page:1/1) Row per Page: 50

10.2 Client Related Status

10.2.1 Online User

Configuration 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.


Main › Status › User Monitor › Online Users
Online Users List
Select Mode
Logout
Refresh
IP or MAC
Search
(Total:1) First Prev Next Last Go to Page
(Page:1/1)

● Summary ○ Detail

Refresh 10 Sec.

☐	No.	Status	Username	IP Address	IPv6 Address	MAC Address	SZ / VLAN	Access From
☐	1	Online	example@edgecore.com	192.168.1.17	N/A	B4:CE:F6:A7:DD:C0	Default / TN#3.1000	Enterprise_Access_Point_-_ECW5211-L

Go to Page 1

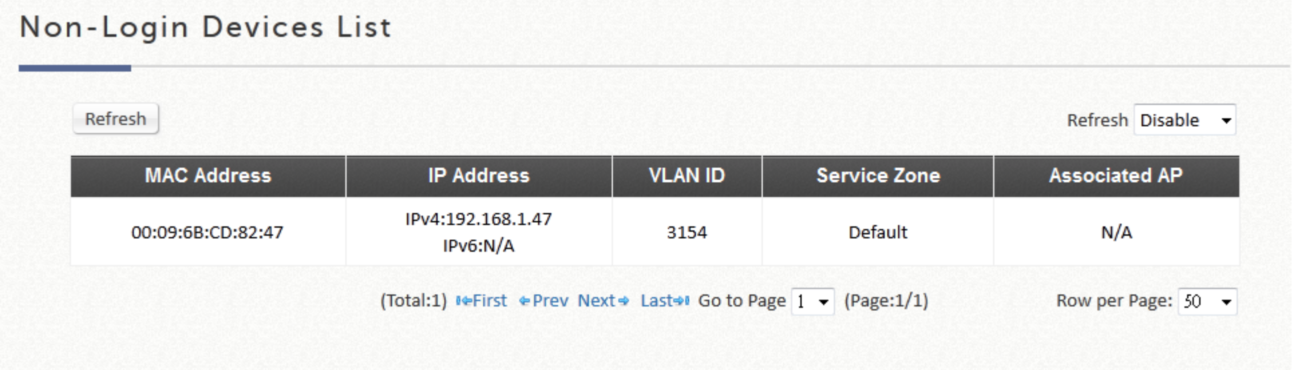
Row per Page: 50

There are 2 modes to select from. Select ‘Detail’ to display more information, such as Pkts In/Out, Bytes In/Out and etc. Administrators can force out a specific online user by clicking ***Kick Out*** and check the user access AP status by clicking the hyperlink of the AP name for **Access From**. A “Search” tool is available for searching IP or MAC address of specific online user. Click ***Refresh*** to update the current users list or you can select the time interval for automatic refresh from the drop-down box in the lower right corner of this page.

10.2.2 Associated Non Login Users

Configuration 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.


Refresh
(Total:1) First Prev Next Last Go to Page 1 (Page:1/1)

Non-Login Devices List

Refresh Disable

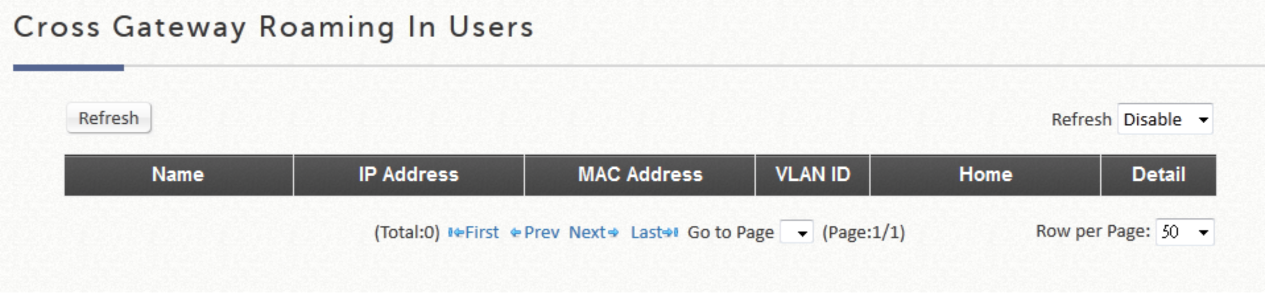
MAC Address	IP Address	VLAN ID	Service Zone	Associated AP
00:09:6B:CD:82:47	IPv4:192.168.1.47 IPv6:N/A	3154	Default	N/A

Row per Page: 50

10.2.3 Cross Gateway Roaming Users

Configuration 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.


Refresh
(Total:0) First Prev Next Last Go to Page (Page:1/1)

Cross Gateway Roaming In Users

Refresh Disable

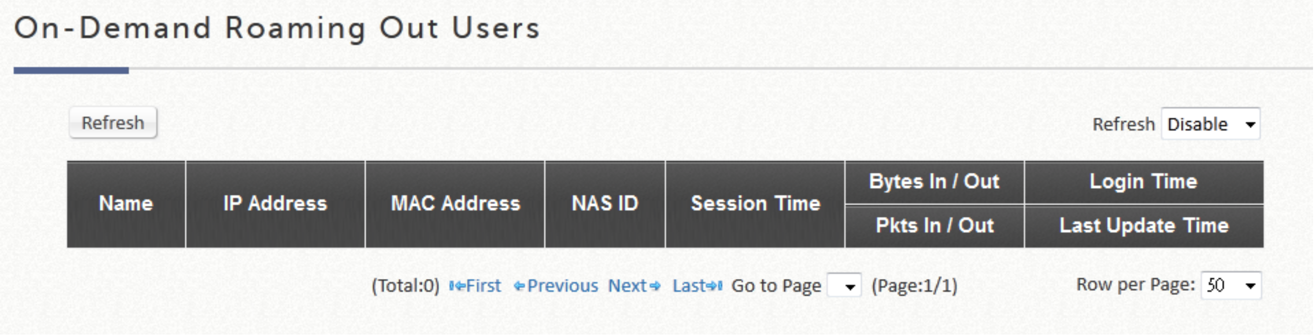
Name	IP Address	MAC Address	VLAN ID	Home	Detail

Row per Page: 50

10.2.4 On-Demand Roaming Out User

Configuration 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

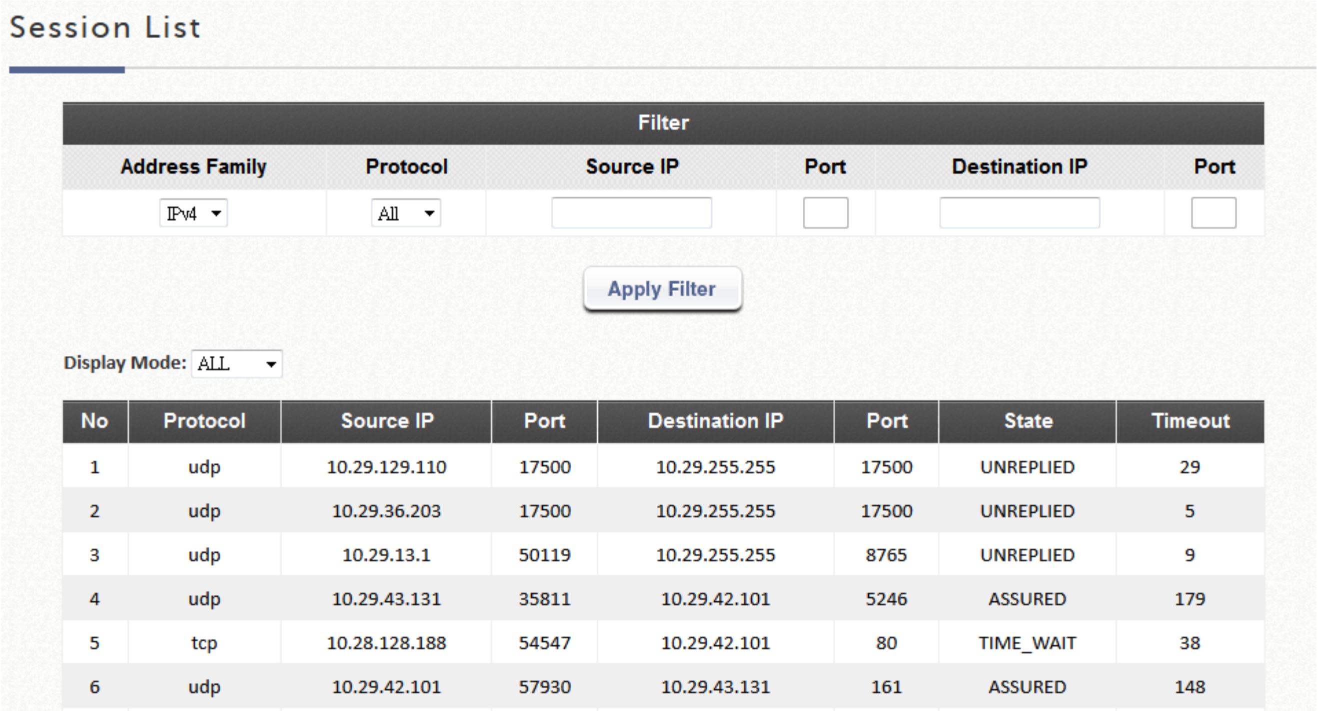
Name	IP Address	MAC Address	NAS ID	Session Time	Bytes In / Out	Login Time
					Pkts In / Out	Last Update Time

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

10.2.5 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

Address Family	Protocol	Source IP	Port	Destination IP	Port
IPv4	All				

Filter
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.

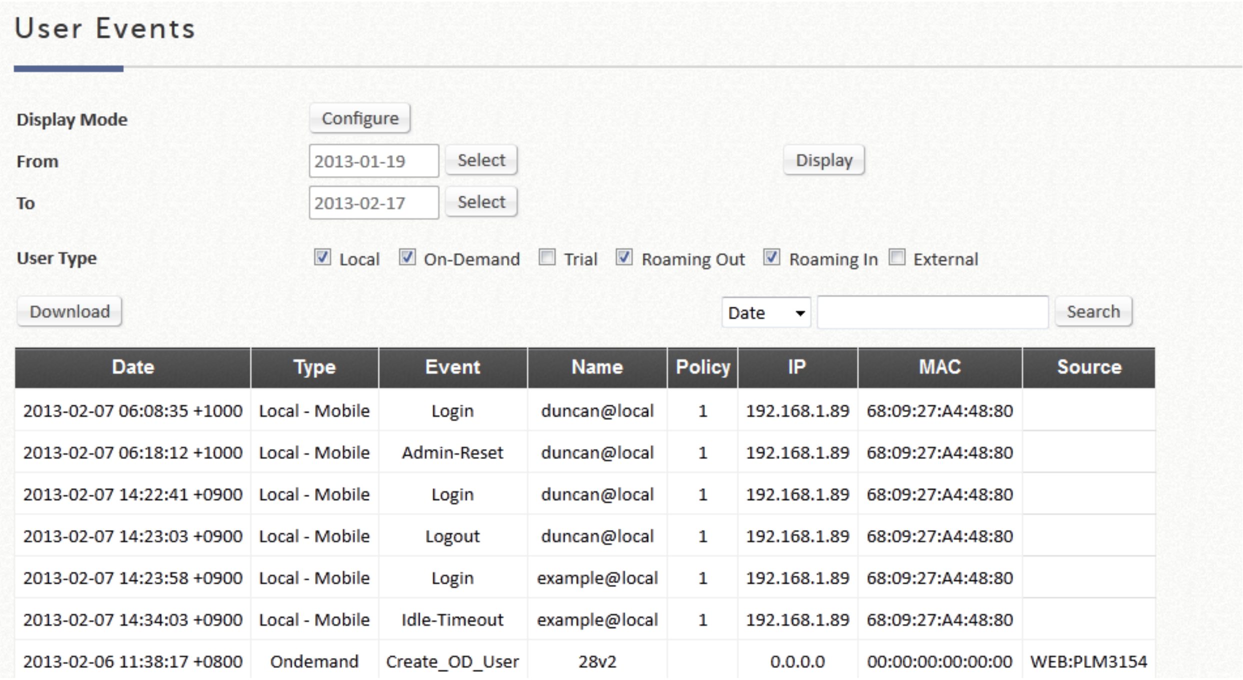
- **CAPWAP Log:** This page shows the CAPWAP message communicated between the Controller and CAPWAP enabled APs.
- **Configuration Change Log:** This page shows the account, and IP of the person that has made changes to Controllers WMI configurations.
- **Local Monthly Usage:** This page shows the aggregated 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.

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, 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.



Display Mode
From 2013-01-19
To 2013-02-17
User Type ☑ Local ☑ On-Demand ☐ Trial ☑ Roaming Out ☑ Roaming In ☐ External

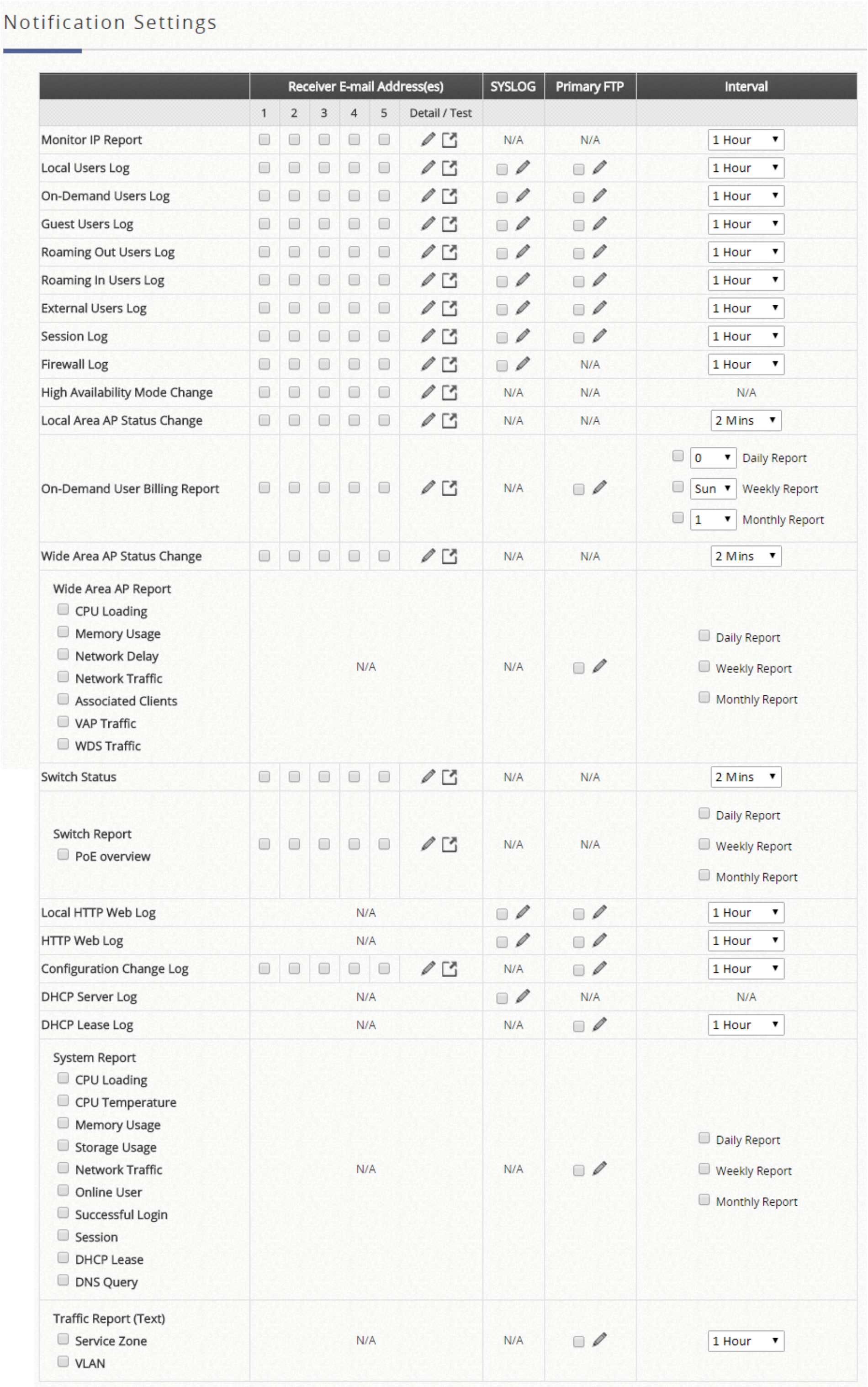
Date	Type	Event	Name	Policy	IP	MAC	Source
2013-02-07 06:08:35 +1000	Local - Mobile	Login	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 06:18:12 +1000	Local - Mobile	Admin-Reset	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:22:41 +0900	Local - Mobile	Login	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:23:03 +0900	Local - Mobile	Logout	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:23:58 +0900	Local - Mobile	Login	example@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:34:03 +0900	Local - Mobile	Idle-Timeout	example@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-06 11:38:17 +0800	Ondemand	Create_OD_User	28v2		0.0.0.0	00:00:00:00:00:00	WEB:PLM3154

Note that different User Types contain different user information. Categories will be left blank if inapplicable to the User Type.

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	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	1 Hour ▾
Local Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
On-Demand Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Guest Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Roaming Out Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Roaming In Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
External Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Session Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Firewall Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	N/A	1 Hour ▾
High Availability Mode Change	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	N/A
Local Area AP Status Change	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	2 Mins ▾
On-Demand User Billing Report	☐	☐	☐	☐	☐	✎ ↗	N/A	☐ ✎	☐ 0 ▾ Daily Report ☐ Sun ▾ Weekly Report ☐ 1 ▾ Monthly Report
Wide Area AP Status Change	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	2 Mins ▾
Wide Area AP Report ☐ CPU Loading ☐ Memory Usage ☐ Network Delay ☐ Network Traffic ☐ Associated Clients ☐ VAP Traffic ☐ WDS Traffic	N/A						N/A	☐ ✎	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Switch Status	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	2 Mins ▾
Switch Report ☐ PoE overview	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Local HTTP Web Log	N/A						☐ ✎	☐ ✎	1 Hour ▾
HTTP Web Log	N/A						☐ ✎	☐ ✎	1 Hour ▾
Configuration Change Log	☐	☐	☐	☐	☐	✎ ↗	N/A	☐ ✎	1 Hour ▾
DHCP Server Log	N/A						☐ ✎	N/A	N/A
DHCP Lease Log	N/A						N/A	☐ ✎	1 Hour ▾
System Report ☐ CPU Loading ☐ CPU Temperature ☐ Memory Usage ☐ Storage Usage ☐ Network Traffic ☐ Online User ☐ Successful Login ☐ Session ☐ DHCP Lease ☐ DNS Query	N/A						N/A	☐ ✎	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Traffic Report (Text) ☐ Service Zone ☐ VLAN	N/A						N/A	☐ ✎	1 Hour ▾

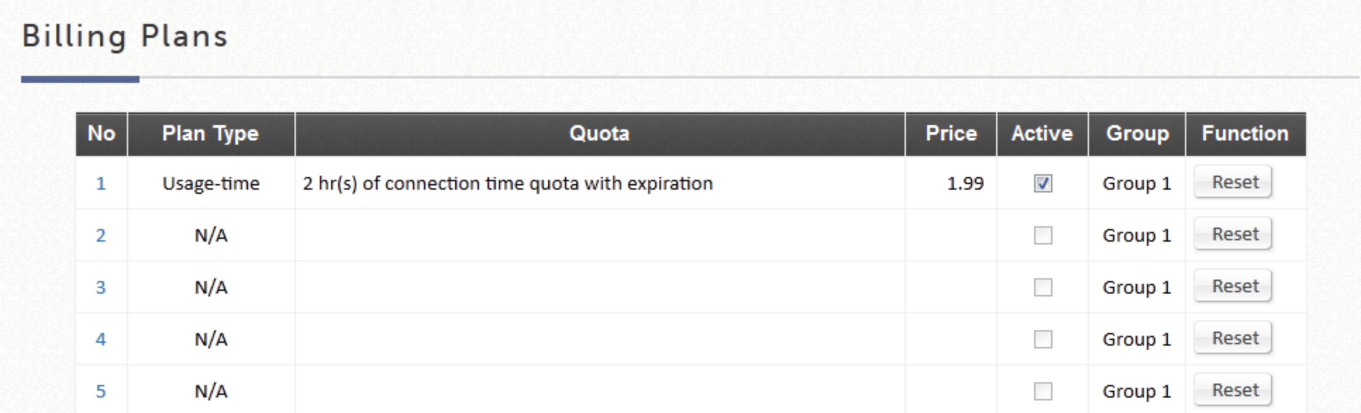
- **SMTP Settings:** Allows the configuration of 5 recipient E-mail addresses and necessary mail server settings where various user related logs will be sent to.
- **SYSLOG Settings:** Allows the configuration of two external SYSLOG servers where selected users logs as well as system logs will be sent 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, FTP) on customizable time intervals.

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	☑	Group 1	Reset
2	N/A			☐	Group 1	Reset
3	N/A			☐	Group 1	Reset
4	N/A			☐	Group 1	Reset
5	N/A			☐	Group 1	Reset

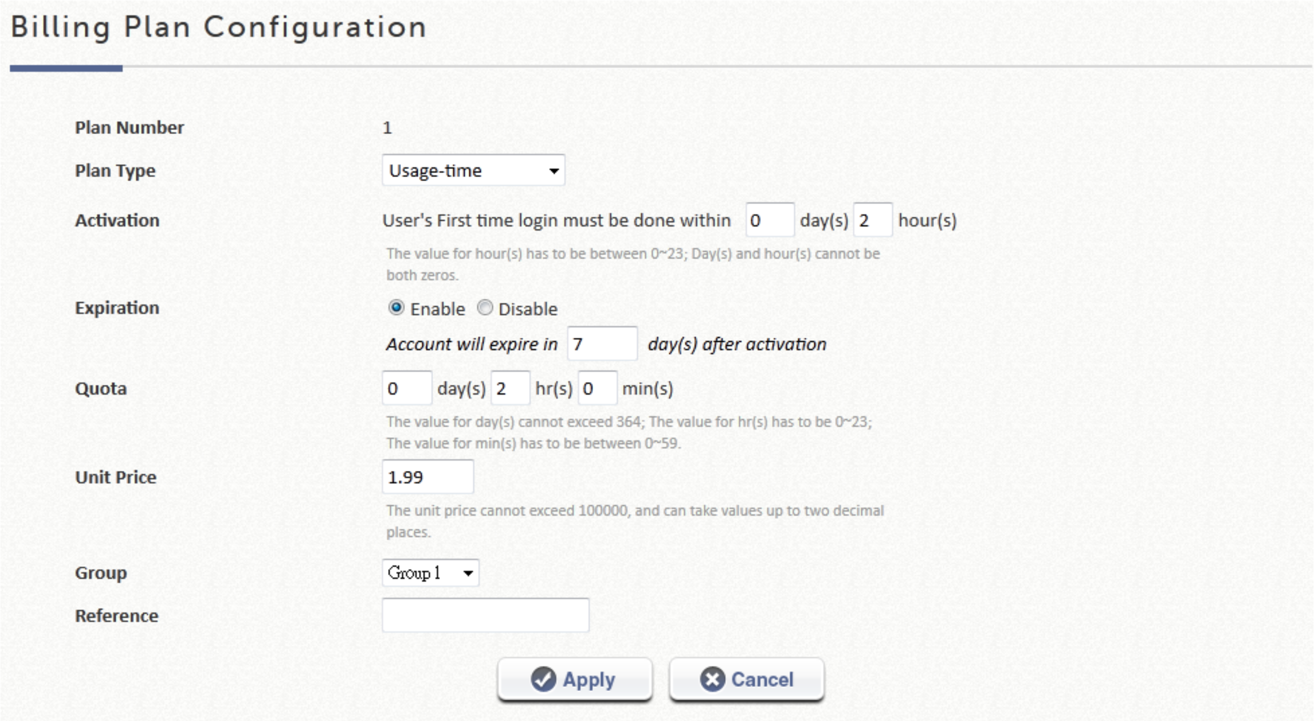
- **Plan:** The number of the selected Billing Plan profile.
- **Plan Type:** The account type chosen for this plan. Different account types have different properties. A suitable account type should be selected that will best meet guest usage requirements.
- **Quota:** The usage terms on how much or 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 count down to Expiration Time is continuous regardless of logging in or out. Account expires when ***Valid Period*** has been used up or quota depleted.

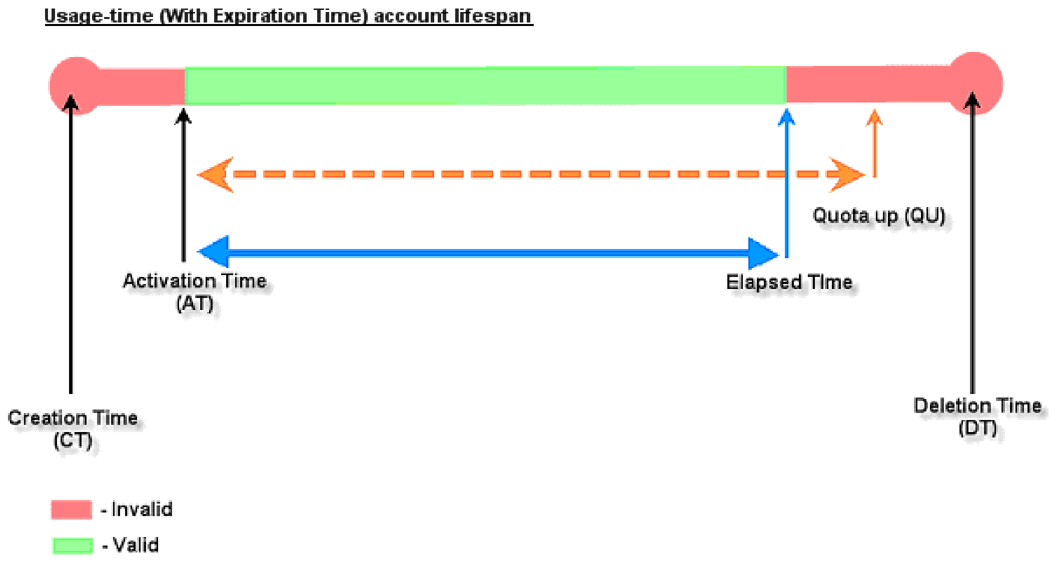
- **Quota** is the total period of time (xx *days* yy *hrs* zz *mins*), during which On-Demand users are allowed to access the network. The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeeming.
- **Account Activation** is the time period for which the user must execute a first login. 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.



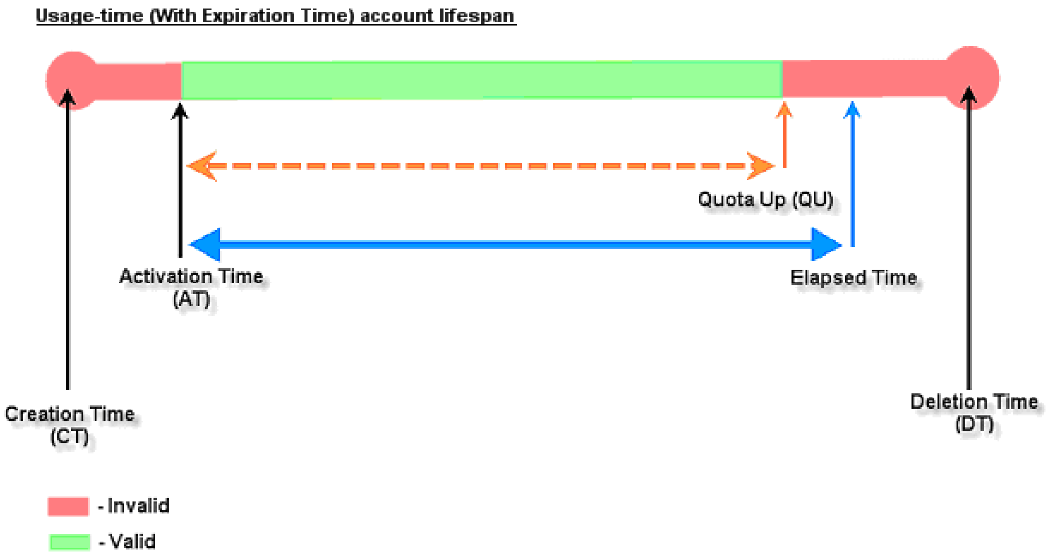
Billing Plan Configuration

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	

Apply
Cancel



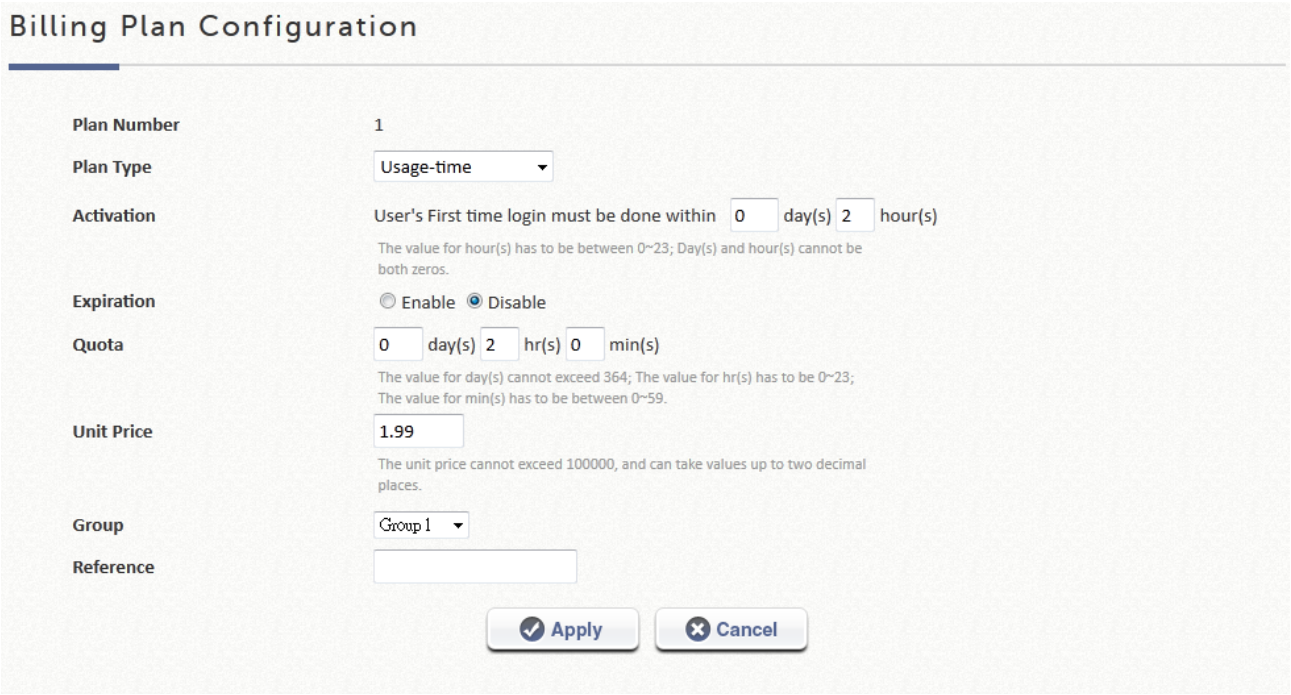
Usage-time (With Expiration Time) account lifespan
Quota up (QU)
Activation Time (AT)
Elapsed Time
Creation Time (CT)
Deletion Time (DT)
- Invalid
- Valid


Usage-time (With Expiration Time) account lifespan
Quota Up (QU)
Activation Time (AT)
Elapsed Time
Creation Time (CT)
Deletion Time (DT)
- Invalid
- Valid

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.

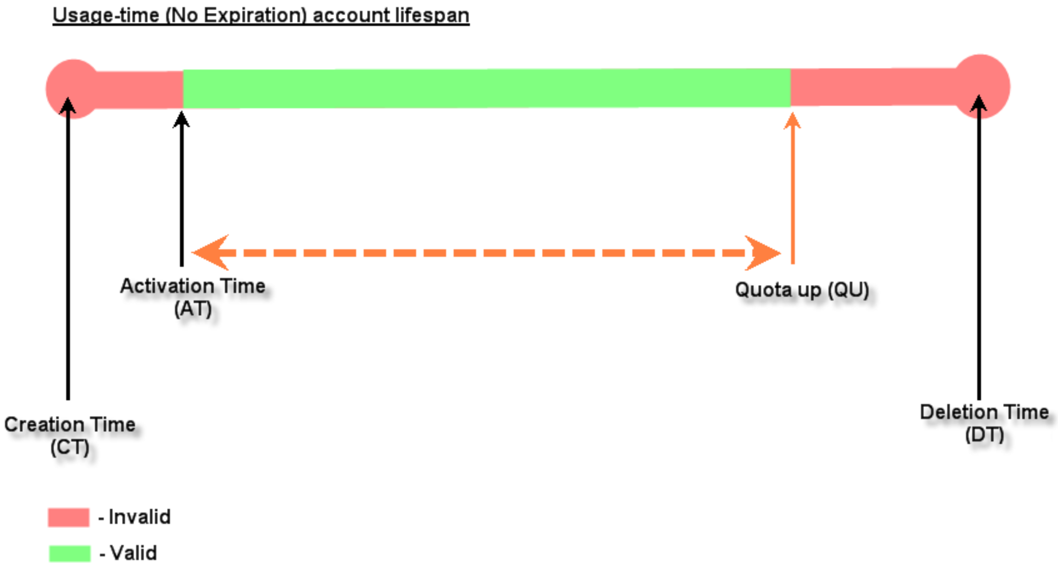
- **Quota** is the total period of time (xx *days* yy *hrs* zz *mins*), during which On-Demand users are allowed to access the network. The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeem.
- **Account Activation** is the time period for which the user must execute a first login. 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) The value for hour(s) has to be between 0~23; Day(s) and hour(s) cannot be both zeros.
Expiration	○ Enable ● Disable
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	

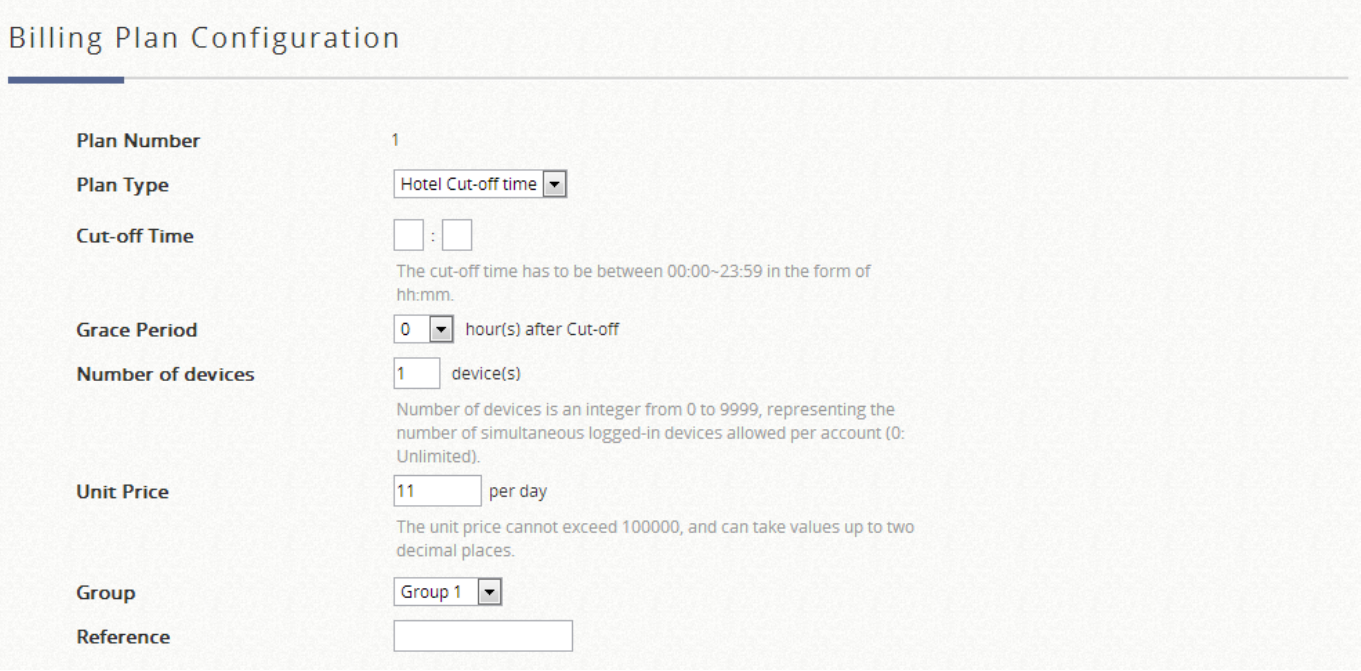
Apply
Cancel



Usage-time (No Expiration) account lifespan
Activation Time (AT)
Quota up (QU)
Creation Time (CT)
Deletion Time (DT)
🟥 - Invalid
🟩 - Valid

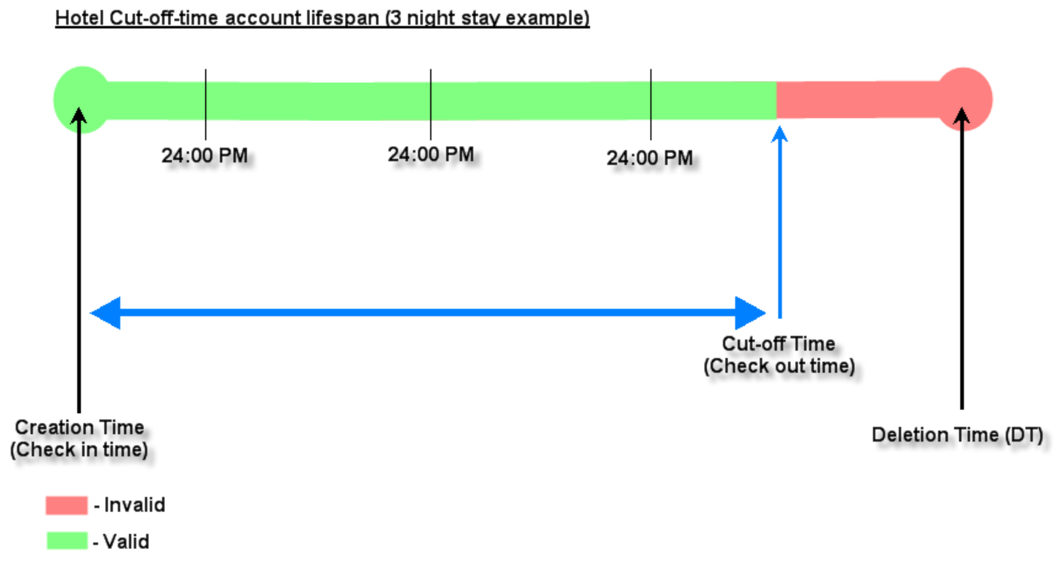
11.2.3. Hotel Cut-off-time

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.



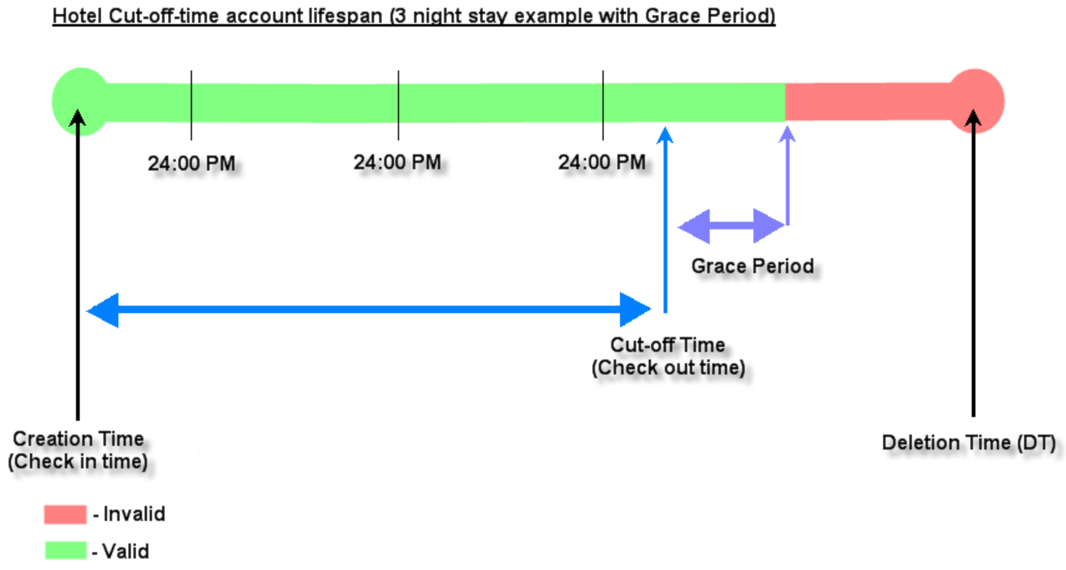
Billing Plan Configuration

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



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

24:00 PM
24:00 PM
24:00 PM
Cut-off Time
(Check out time)
Creation Time
(Check in time)
Deletion Time (DT)
- Invalid
- Valid



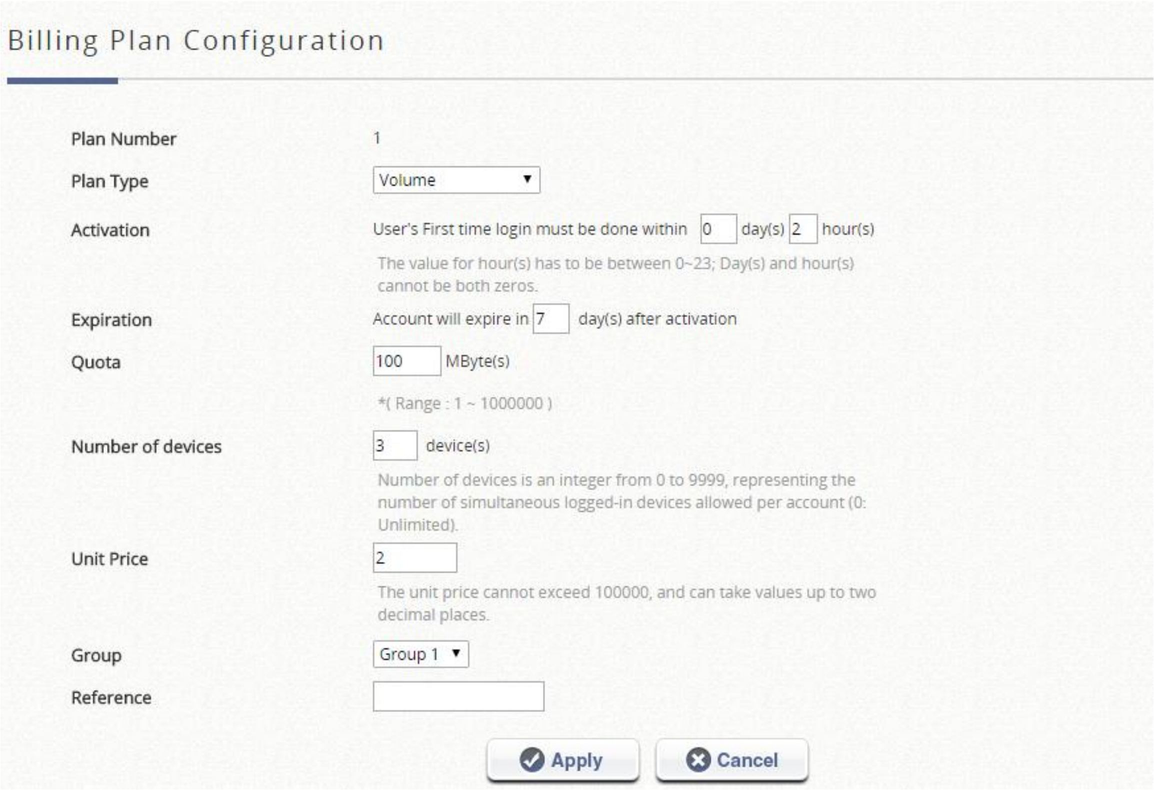
Hotel Cut-off-time account lifespan (3 night stay example with Grace Period)

24:00 PM
24:00 PM
24:00 PM
Grace Period
Cut-off Time
(Check out time)
Creation Time
(Check in time)
Deletion Time (DT)
- Invalid
- Valid

11.2.4. Volume

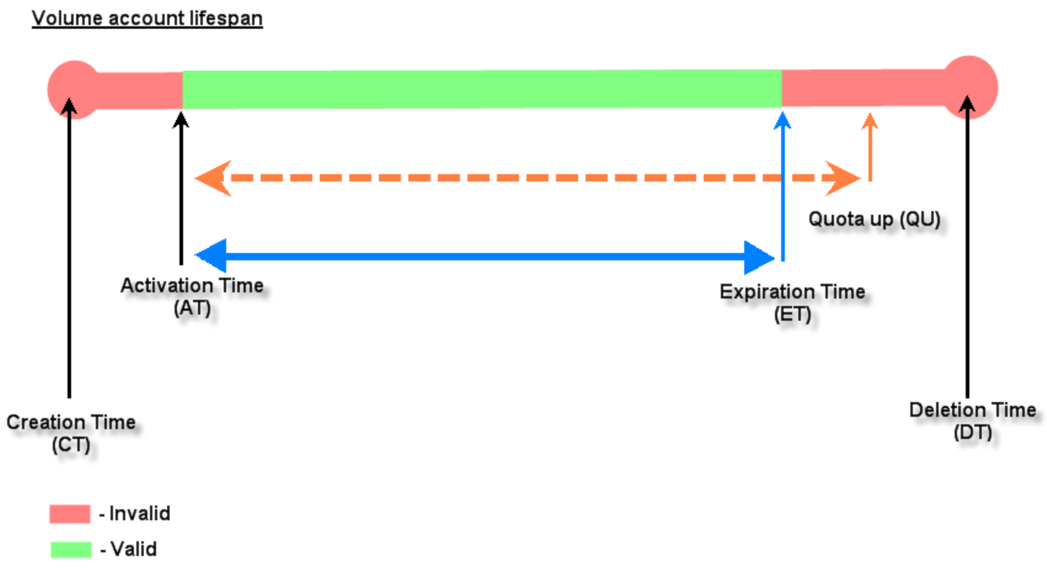
Users can access internet as long as account is valid with remaining quota (traffic volume). Account expires when *Valid Period* is used up or quota is depleted. This is ideal for small quantity applications such as sending/receiving mail, transferring a file etc. Count down of Valid Period is continuous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

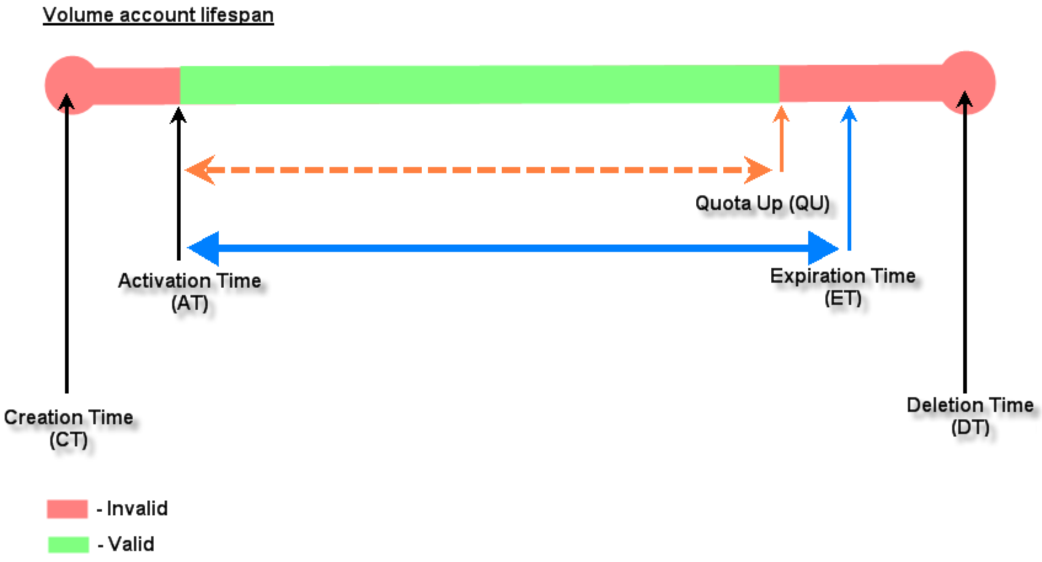
- **Account Activation** is the time period for which the user must execute a first login. Failure to do so in the time period set in Account Activation will result in account expiration.
- **Expiration** is the valid time period for using. After this time period, the account expires even with quota 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 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	Account will expire in 7 day(s) after activation
Quota	100 MByte(s) *(Range : 1 ~ 1000000)
Number of devices	3 device(s) Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).
Unit Price	2 The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 1
Reference	


Volume account lifespan
Quota up (QU)
Activation Time (AT)
Expiration Time (ET)
Creation Time (CT)
Deletion Time (DT)
- Invalid
- Valid

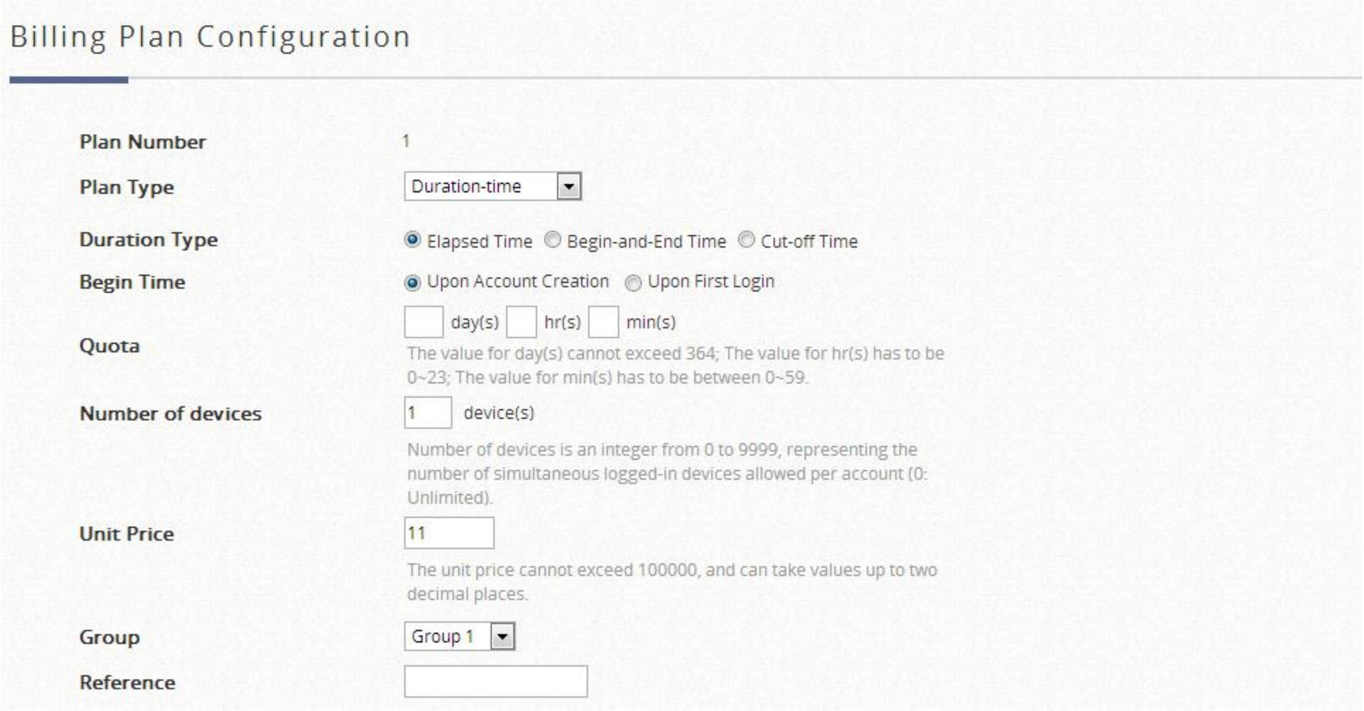

Volume account lifespan
Quota Up (QU)
Activation Time (AT)
Expiration Time (ET)
Creation Time (CT)
Deletion Time (DT)
- Invalid
- Valid

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.

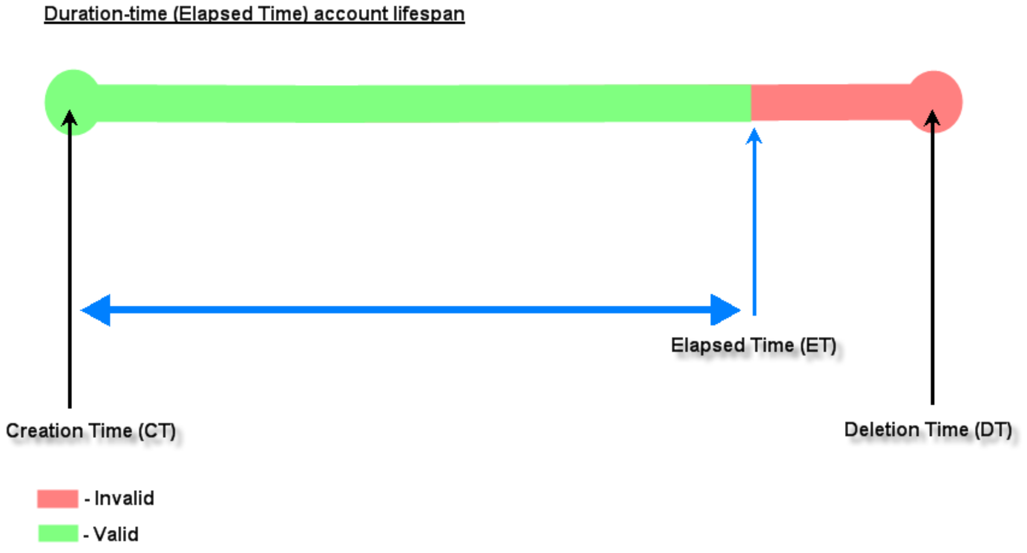
- **Begin Time** is the time that the account will be activated for use. It is set to account creation time.

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



Billing Plan Configuration

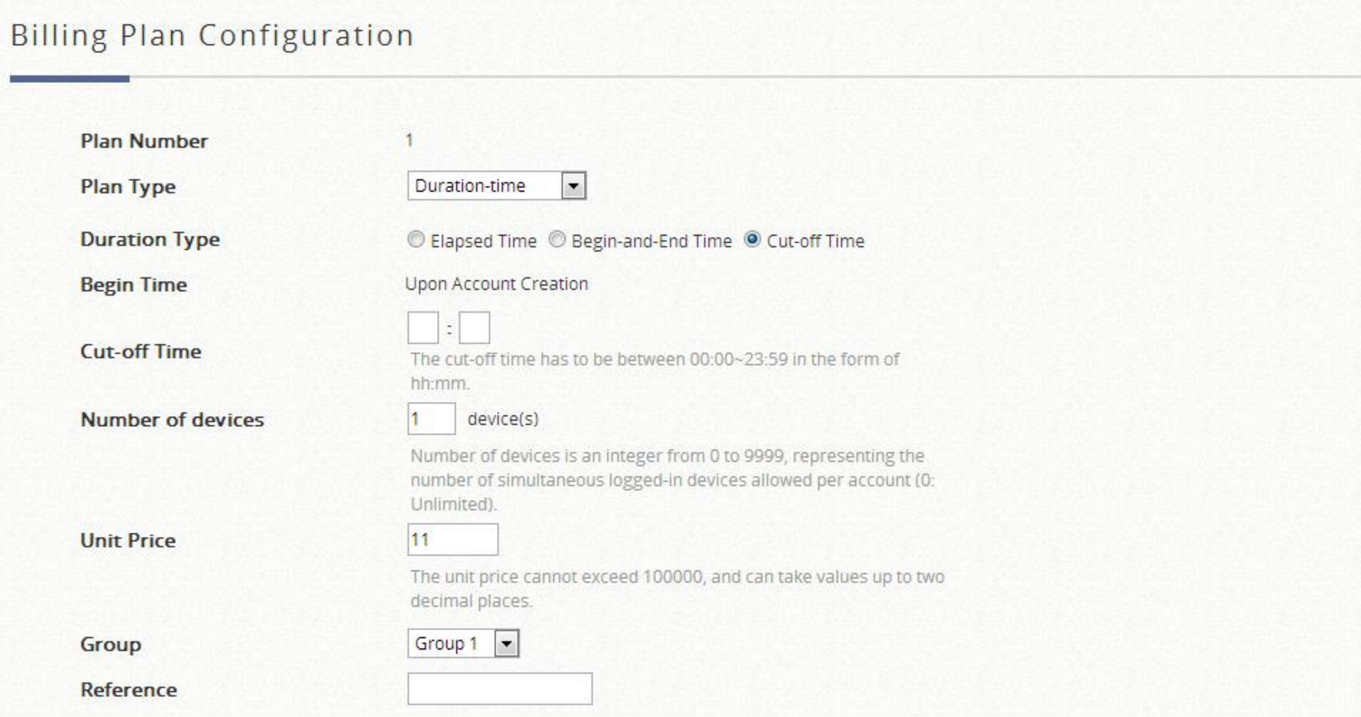
Plan Number	1
Plan Type	Duration-time
Duration Type	● Elapsed Time ○ Begin-and-End Time ○ Cut-off Time
Begin Time	● Upon Account Creation ○ Upon First Login
Quota	day(s) hr(s) min(s) The value for day(s) cannot exceed 364; The value for hr(s) has to be 0~23; The value for min(s) has to be between 0~59.
Number of devices	1 device(s) Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).
Unit Price	11 The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 1
Reference	


Duration-time (Elapsed Time) account lifespan
Elapsed Time (ET)
Creation Time (CT)
Deletion Time (DT)
🟥 - Invalid
🟩 - Valid

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.

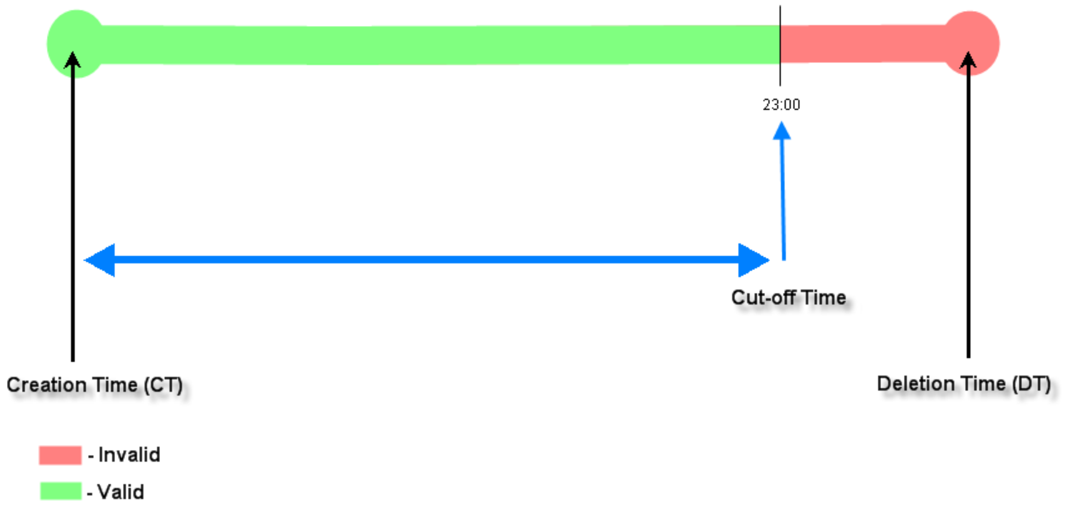
- **Begin Time** is the time that the account will be activated for use. It is set to account creation time.
- **Cut-off Time** is the clock time when the account will expire.
- **Number of Devices** is to define the number of allowed simultaneous logged in devices per account.
- **Price** is the unit 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	○ Elapsed Time ○ Begin-and-End Time ● Cut-off Time
Begin Time	Upon Account Creation
Cut-off Time	: The cut-off time has to be between 00:00~23:59 in the form of hh:mm.
Number of devices	1 device(s) Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).
Unit Price	11 The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 1
Reference	

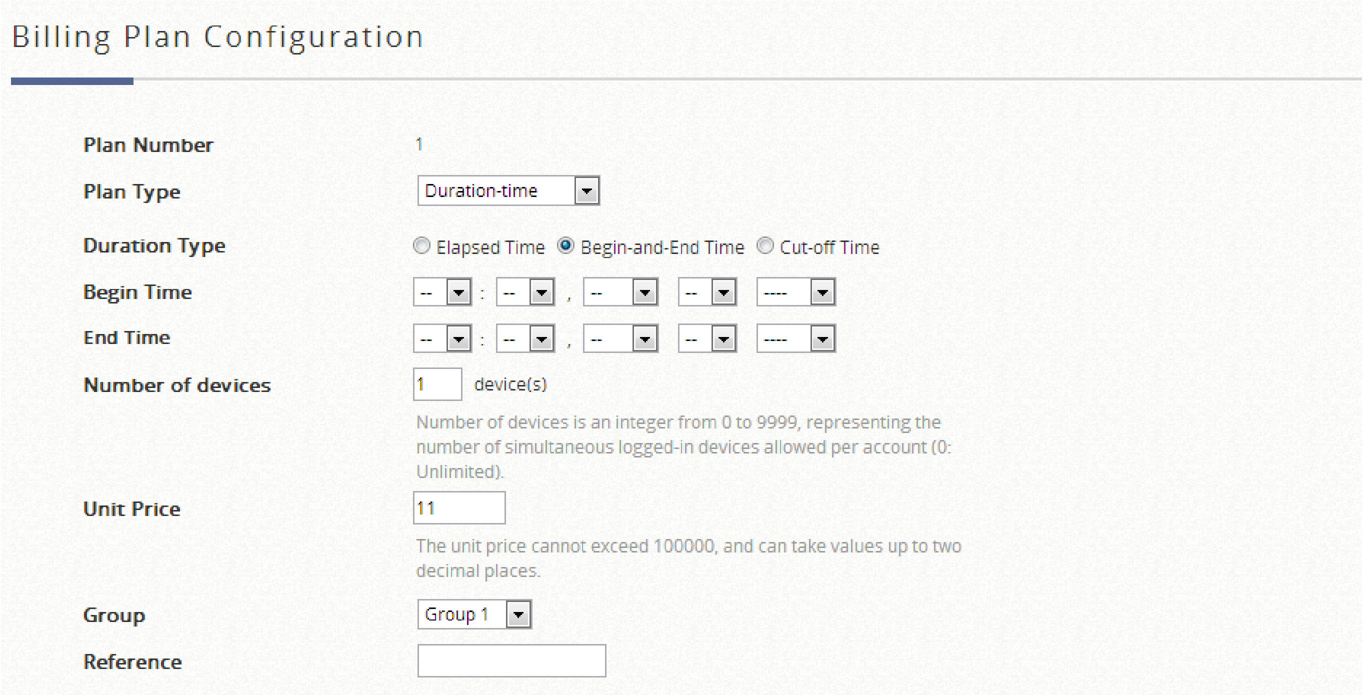
Duration-time (Cut-off Time) account lifespan (exapmle showing Cut-off on 23:00)



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

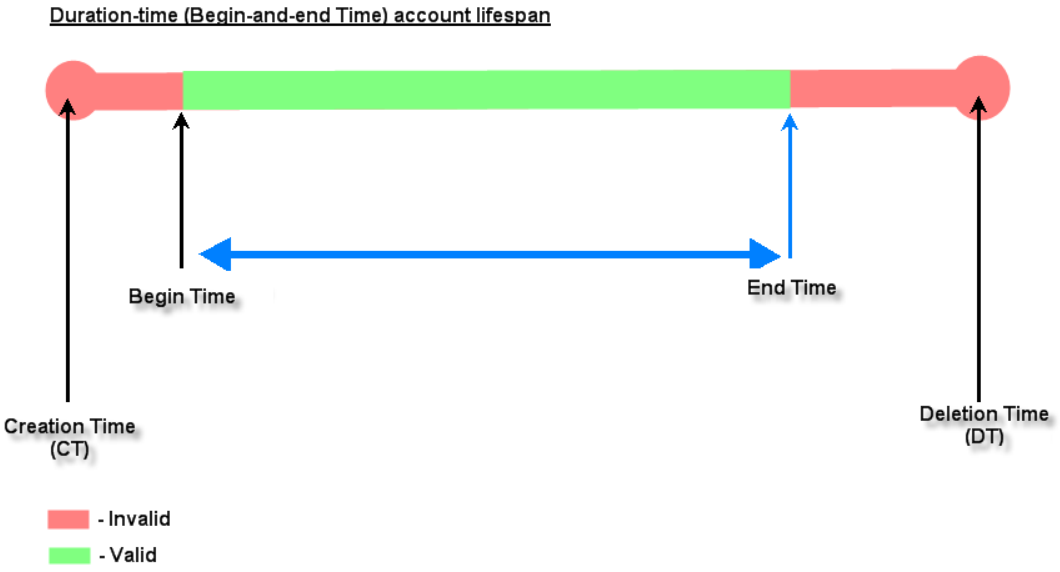
The *Begin Time* and *End Time* of the account are defined explicitly. Count down begins immediately after account activation and expires when the *End Time* has been reached. This is ideal for providing internet service throughout a specific period of time. For example during exhibition events or large conventions 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

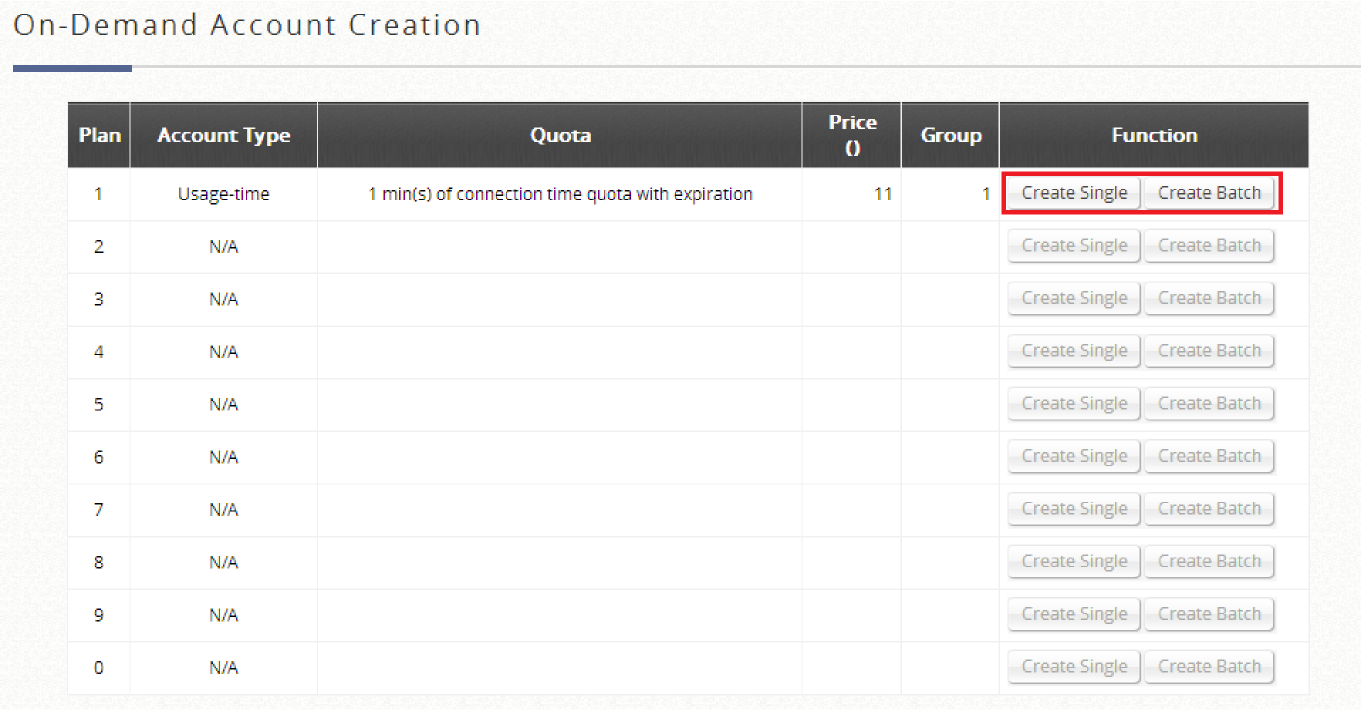
Plan Number	1
Plan Type	Duration-time
Duration Type	○ Elapsed Time ● Begin-and-End Time ○ Cut-off Time
Begin Time	-- : -- , -- -- ----
End Time	-- : -- , -- -- ----
Number of devices	1 device(s) Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices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


Duration-time (Begin-and-end Time) account lifespan
Begin Time
End Time
Creation Time
(CT)
Deletion Time
(DT)
- Invalid
- Valid

11.4 Creating Accounts

Configuration path: Main Menu >> Users >> On-Demand Accounts >> Accounts Creation

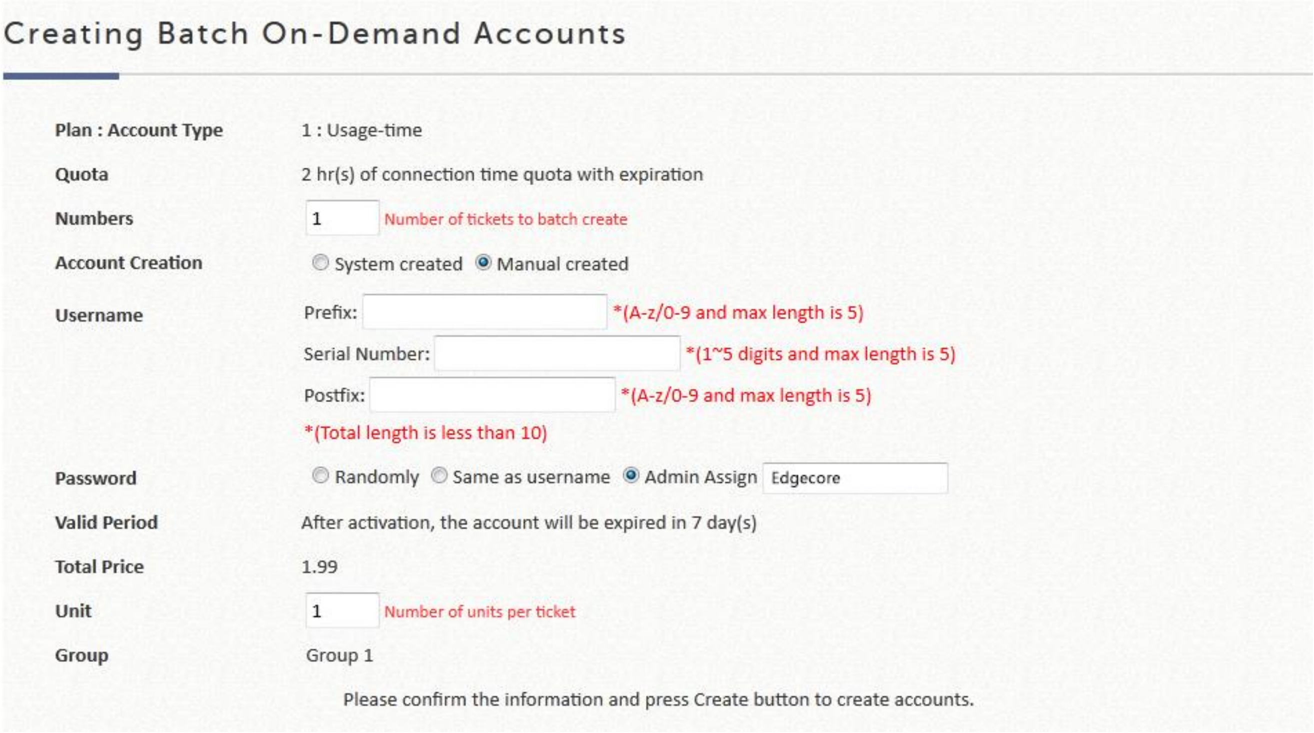
Administrators have the option of creating single accounts or batch accounts. For potential hotspot operators who may wish to pre-generate guest accounts for sale, On-Demand feature has a batch create functionality which allows the administrator or operator with access authority to On-Demand page, to create multiple accounts for an enabled billing plan in batch, and send them to a printer for generating physical tickets 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).



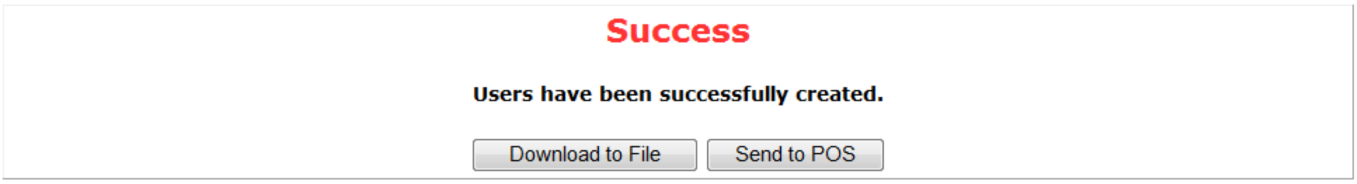
Creating Batch On-Demand Accounts

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

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

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.

11.5 User Self Service

Credit Card via External Payment Gateway

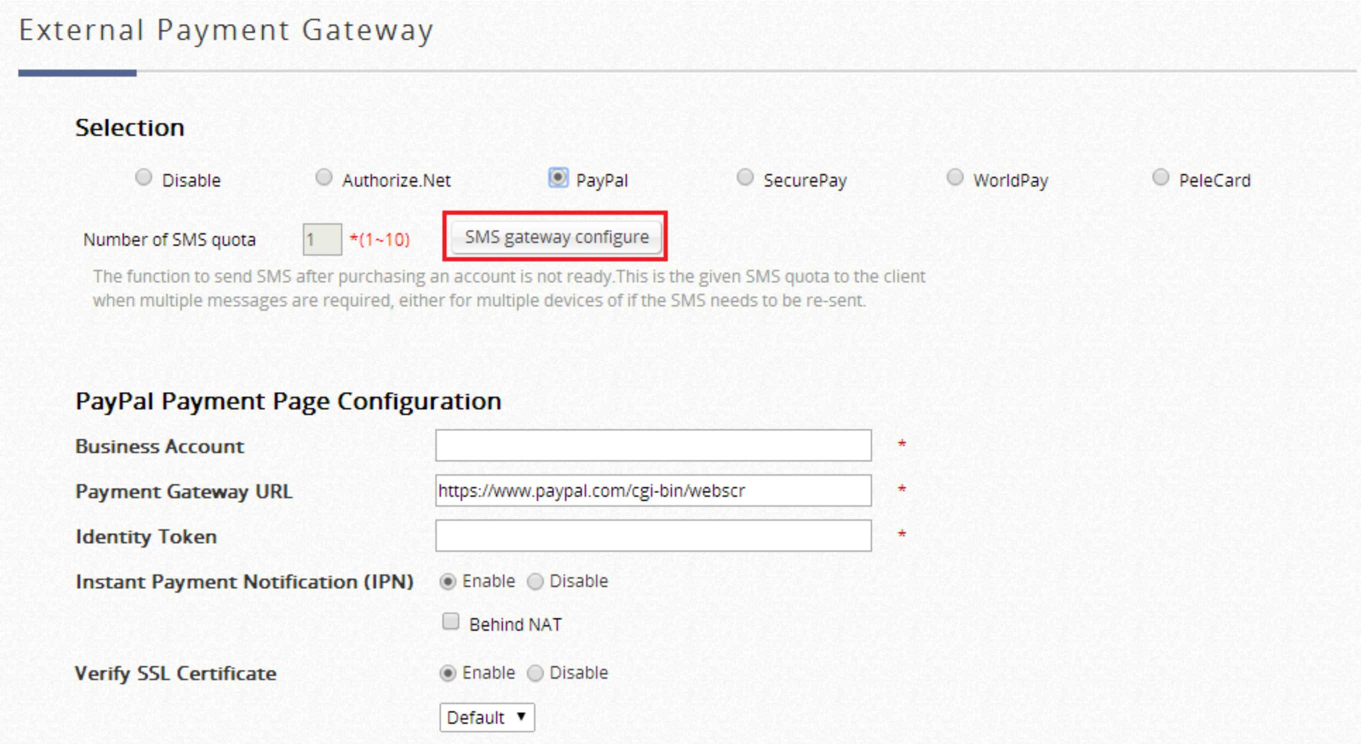
Configuration path: Main Menu >> Users >> Authentication >> On-Demand User >> External Payment Gateway

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

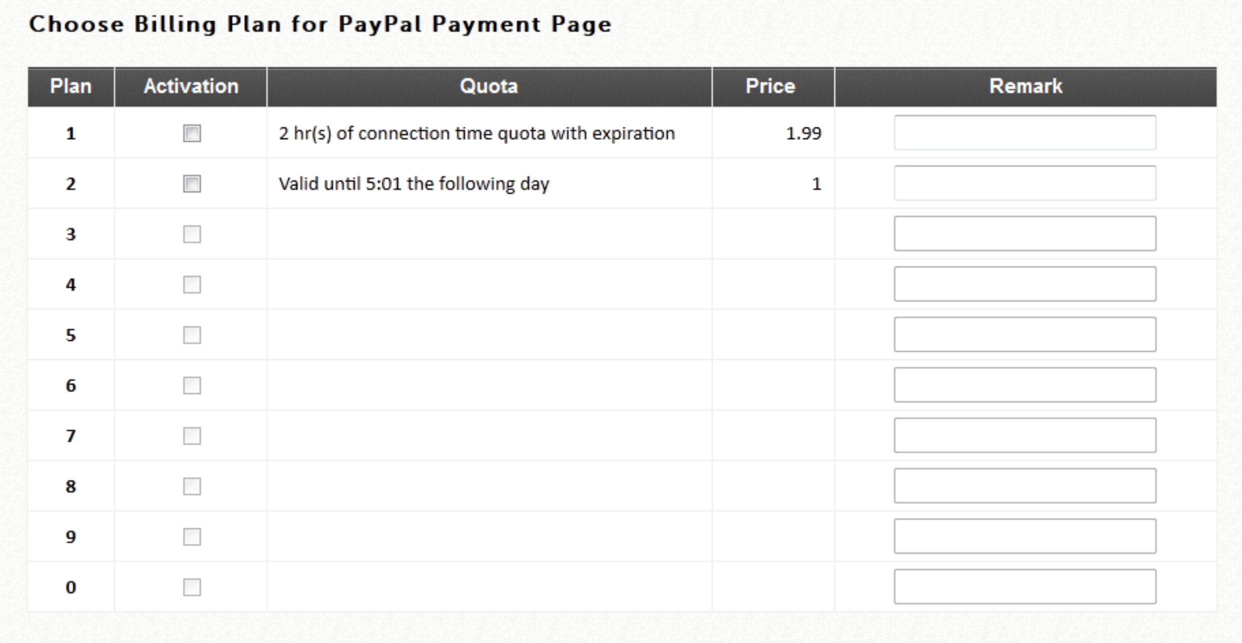
Number of SMS quota: 1 *(1~10)

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

PayPal Payment Page Configuration

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

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



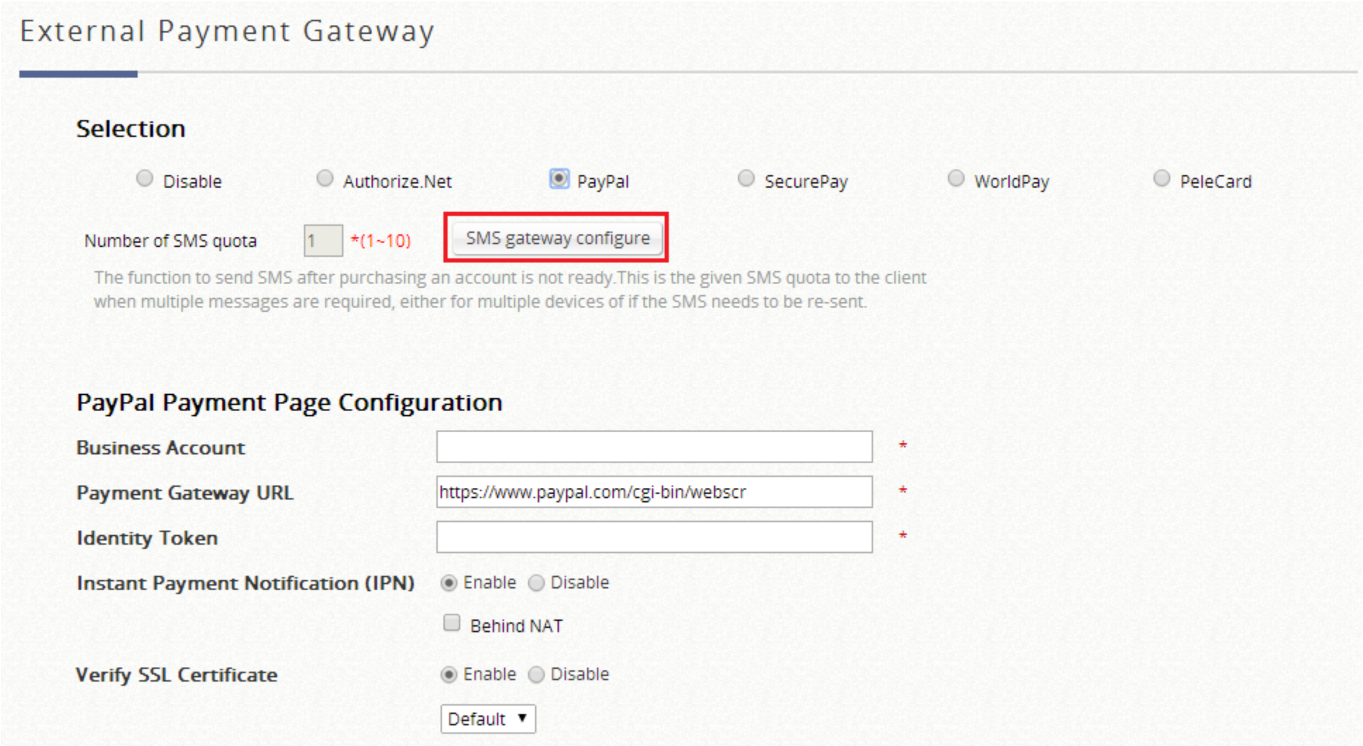
Choose Billing Plan for PayPal Payment Page

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

The service disclaimer can be customized by configuring Web Page Customization.

After the configuration of your external payment gateway, the login page will be shown with a hyperlink which guides the end user step by step to purchase an account with a valid credit card.

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



External Payment Gateway

Selection

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

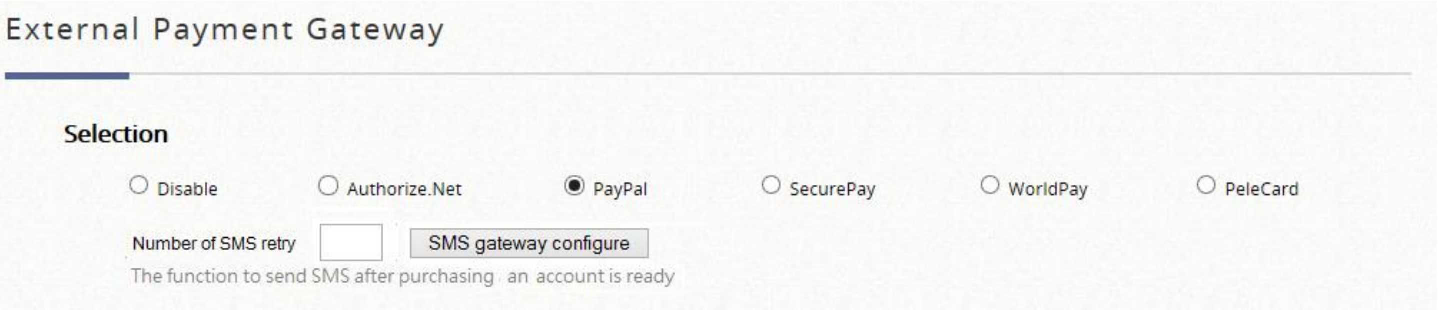
Number of SMS quota: 1 *(1~10) SMS gateway configure

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

PayPal Payment Page Configuration

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

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



External Payment Gateway

Selection

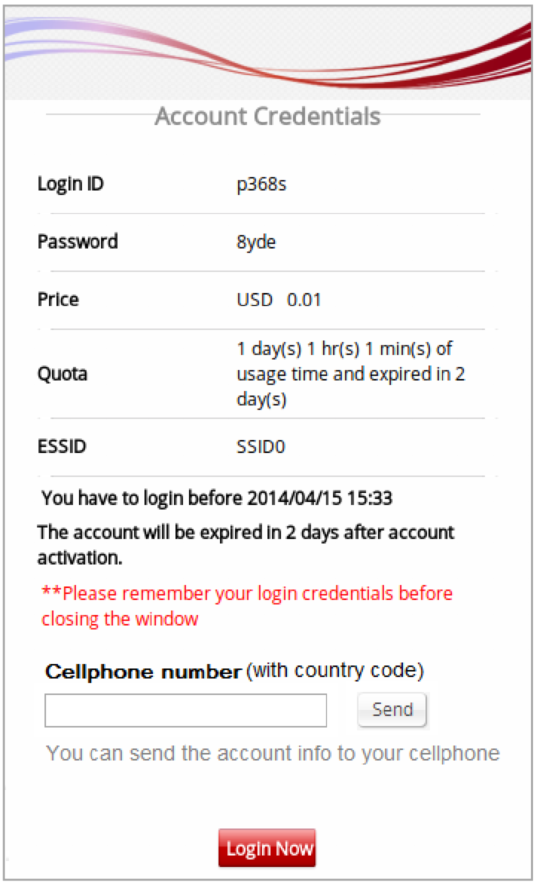
○ Disable ○ Authorize.Net ● PayPal ○ SecurePay ○ WorldPay ○ PeleCard

Number of SMS retry 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:



Account Credentials

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

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

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

**Please remember your login credentials before closing the window

Cellphone number (with country code)

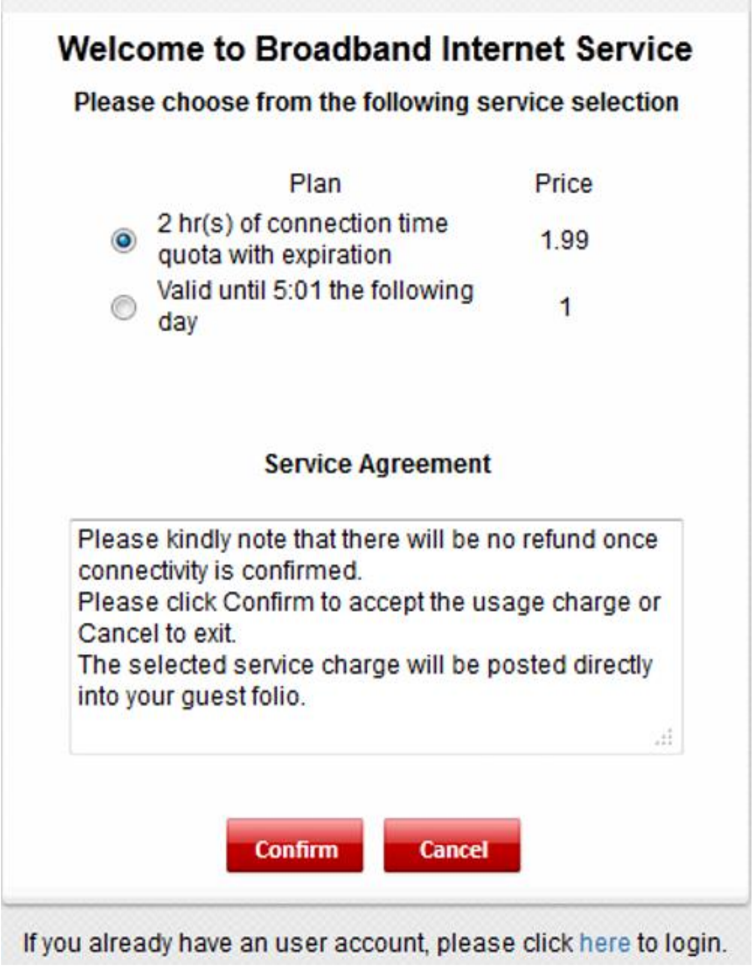
You can send the account info to your cellphone

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	Price
●	2 hr(s) of connection time quota with expiration	1.99
○	Valid until 5:01 the following day	1

Service Agreement

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

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.

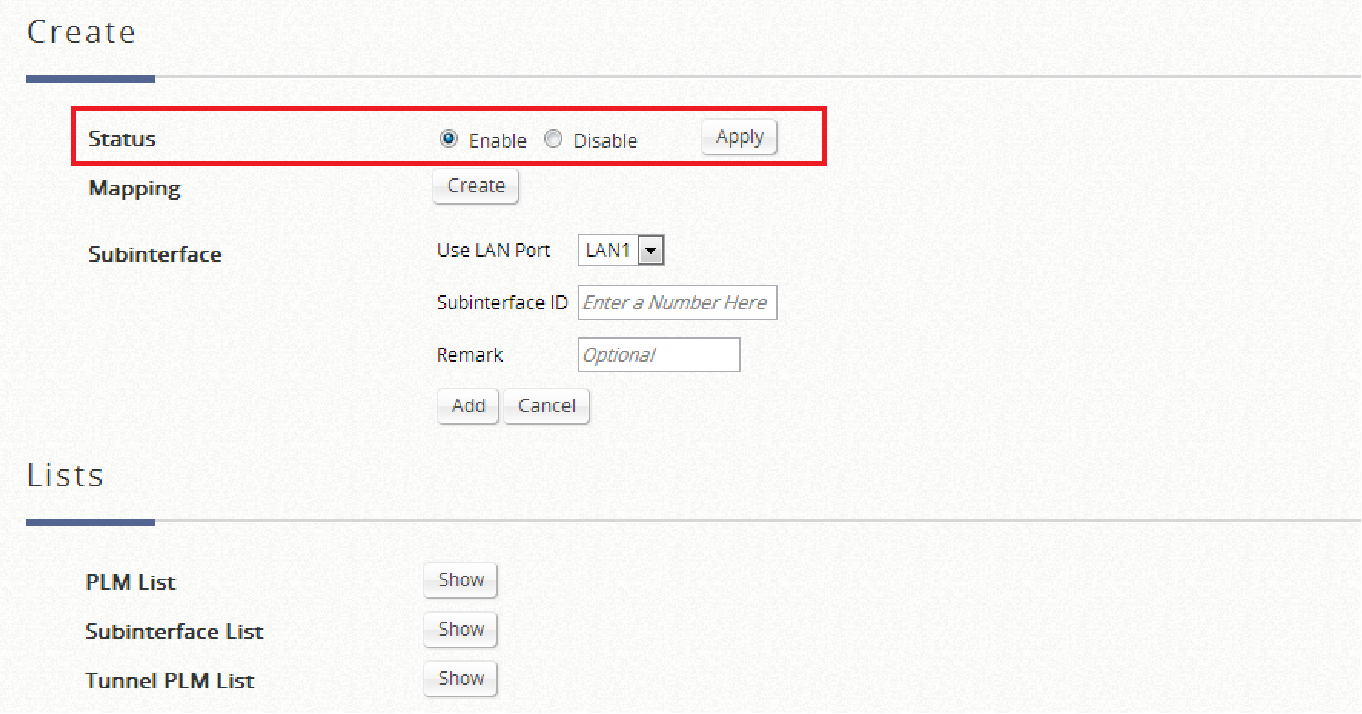
NOTE

1. EWS Controllers default support Micros PMS interface and NetRetriever middleware interface, 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.


Create
Status
● Enable ○ Disable
Apply
Mapping
Create
Subinterface
Use LAN Port
LAN1
Subinterface ID
Enter a Number Here
Remark
Optional
Add
Cancel
Lists
PLM List
Show
Subinterface List
Show
Tunnel PLM List
Show

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

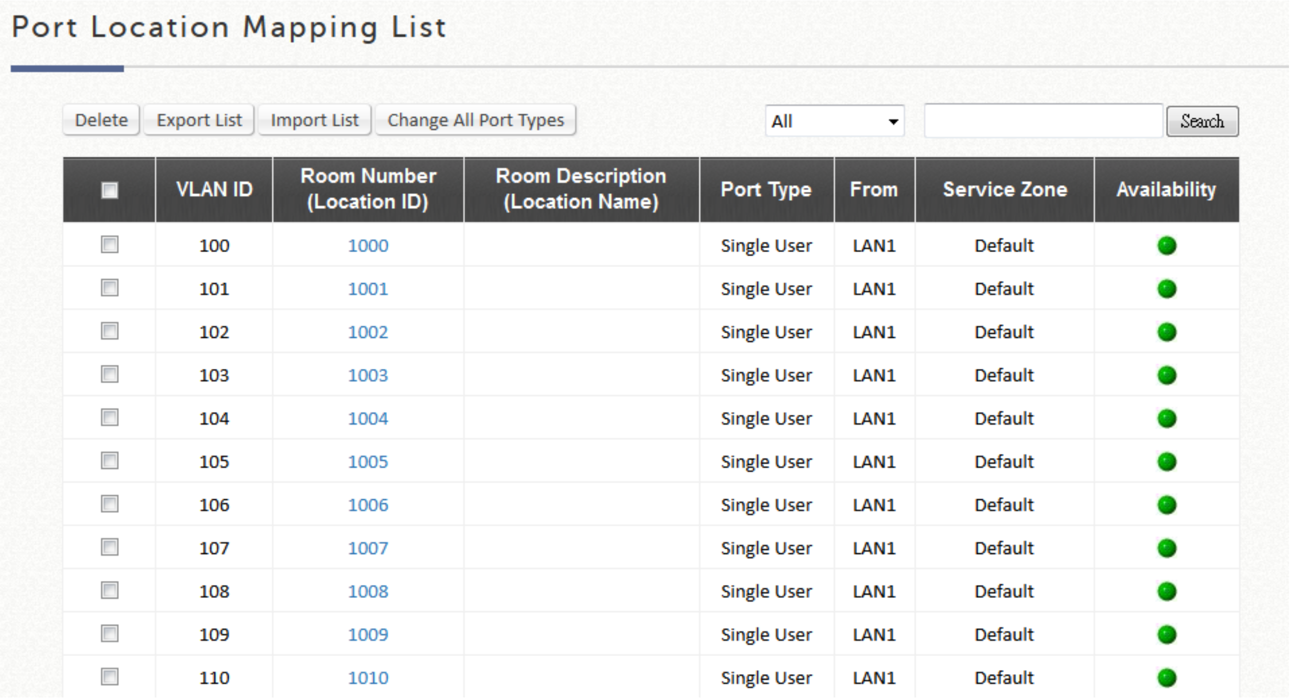
tries to access internet, it will pop up a Blocking message to notify the user.

- **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.

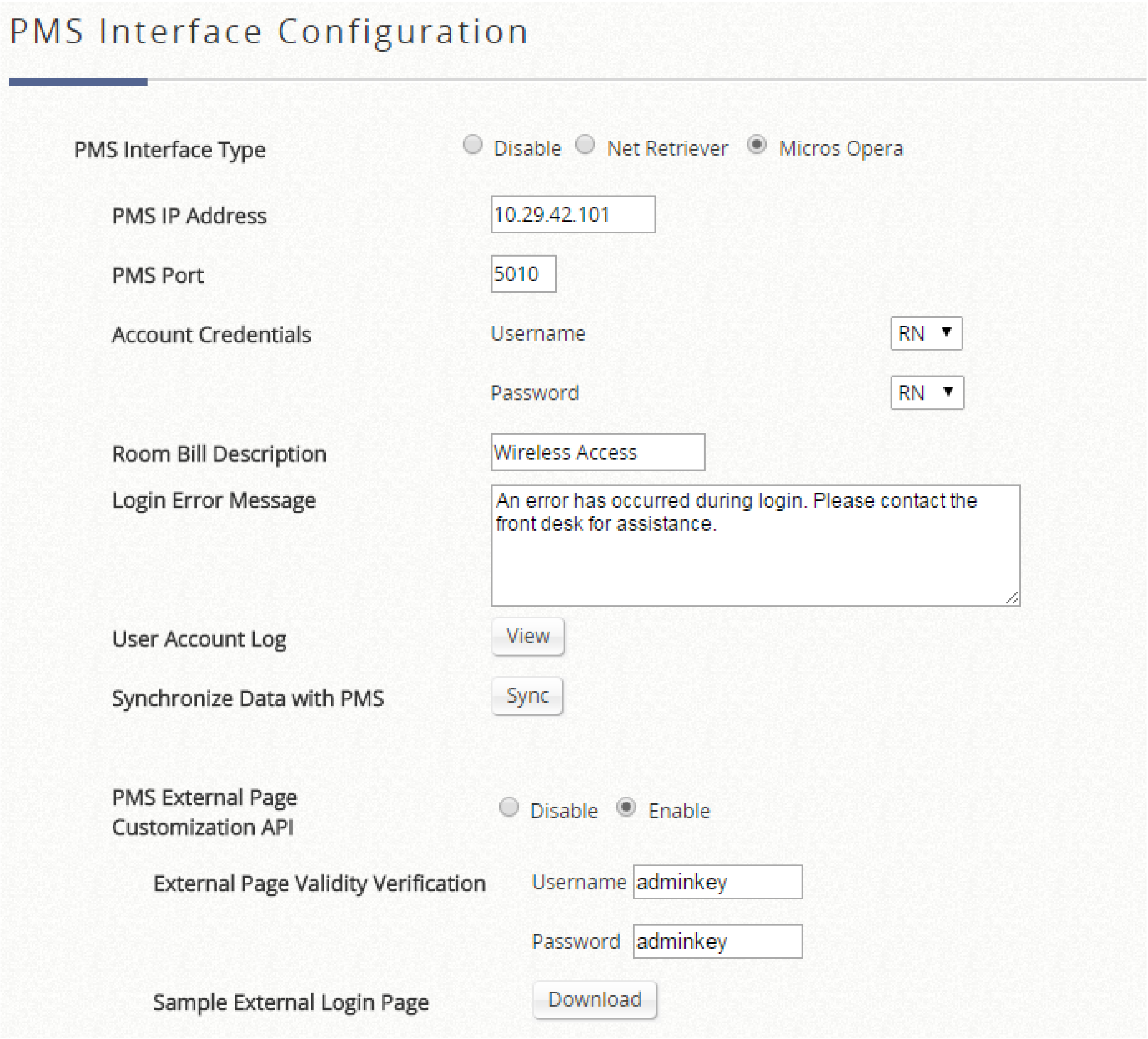


☐	VLAN ID	Room Number (Location ID)	Room Description (Location Name)	Port Type	From	Service Zone	Availability
☐	100	1000		Single User	LAN1	Default	●
☐	101	1001		Single User	LAN1	Default	●
☐	102	1002		Single User	LAN1	Default	●
☐	103	1003		Single User	LAN1	Default	●
☐	104	1004		Single User	LAN1	Default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

12.2 Micros Opera

Configuration path: Main Menu >> Users >> Middleware >> Micros Opera

In the Middleware tab page of Users category, administrator may choose to select the interfacing protocol that is compatible with their site's hospitality management system or PMS system.



PMS Interface Configuration

PMS Interface Type ○ Disable ○ Net Retriever ● Micros Opera

PMS IP Address 10.29.42.101

PMS Port 5010

Account Credentials
Username RN ▼
Password RN ▼

Room Bill Description Wireless Access

Login Error Message An error has occurred during login. Please contact the front desk for assistance.

User Account Log View

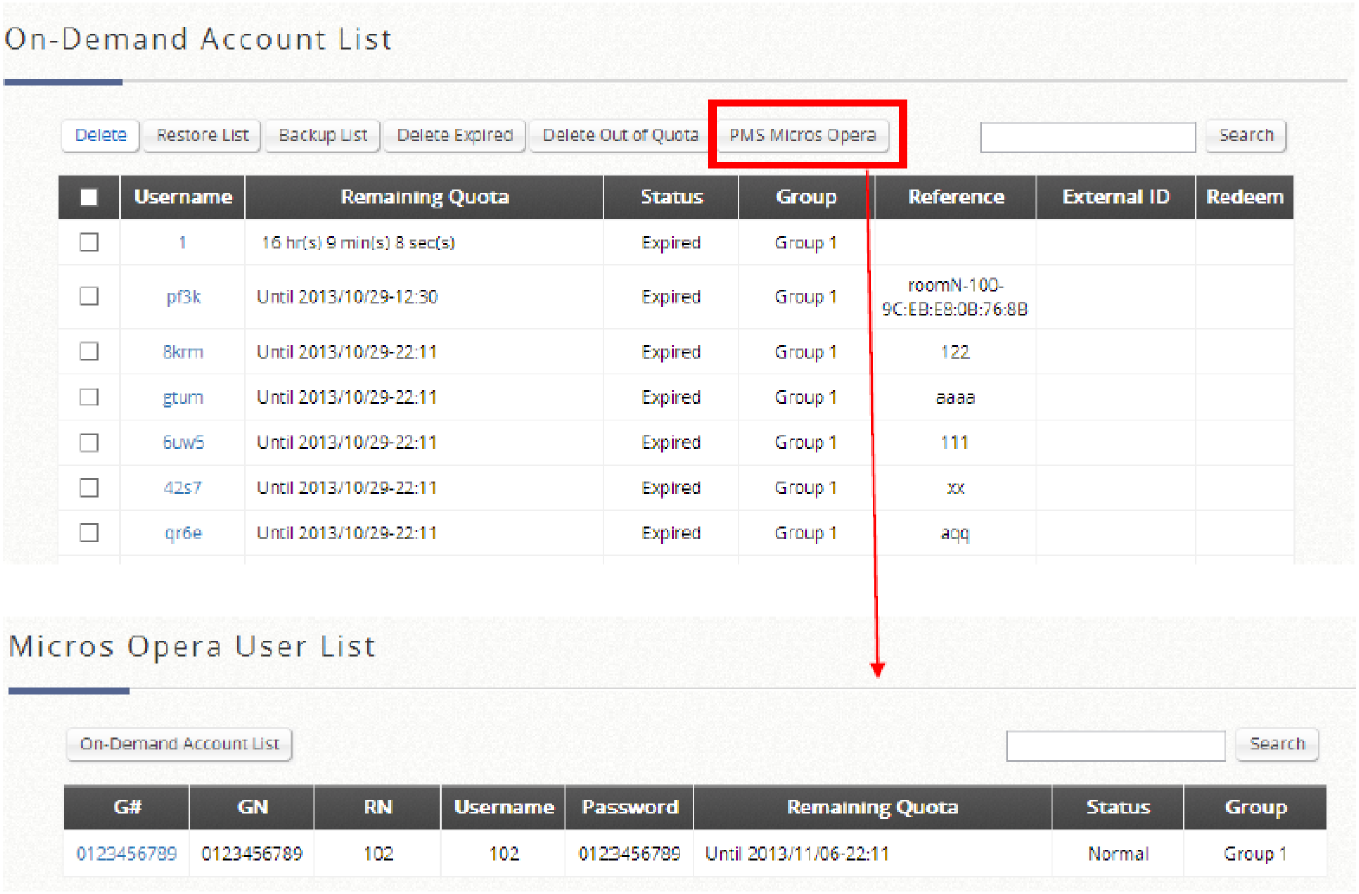
Synchronize Data with PMS Sync

PMS External Page Customization API ○ Disable ● Enable

External Page Validity Verification
Username adminkey
Password adminkey

Sample External Login Page Download

Fill in the Micros 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) or G# (Guest Number) to designate the Micros 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

Delete
Restore List
Backup List
Delete Expired
Delete Out of Quota
PMS Micros Opera
Search

☐	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
☐	1	16 hr(s) 9 min(s) 8 sec(s)	Expired	Group 1			
☐	pf3k	Until 2013/10/29-12:30	Expired	Group 1	roomN-100-9C:EB:E8:0B:76:8B		
☐	8krm	Until 2013/10/29-22:11	Expired	Group 1	122		
☐	gtum	Until 2013/10/29-22:11	Expired	Group 1	aaaa		
☐	6uw5	Until 2013/10/29-22:11	Expired	Group 1	111		
☐	42s7	Until 2013/10/29-22:11	Expired	Group 1	xx		
☐	qr6e	Until 2013/10/29-22:11	Expired	Group 1	aqq		

Micros Opera User List

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

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.

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.

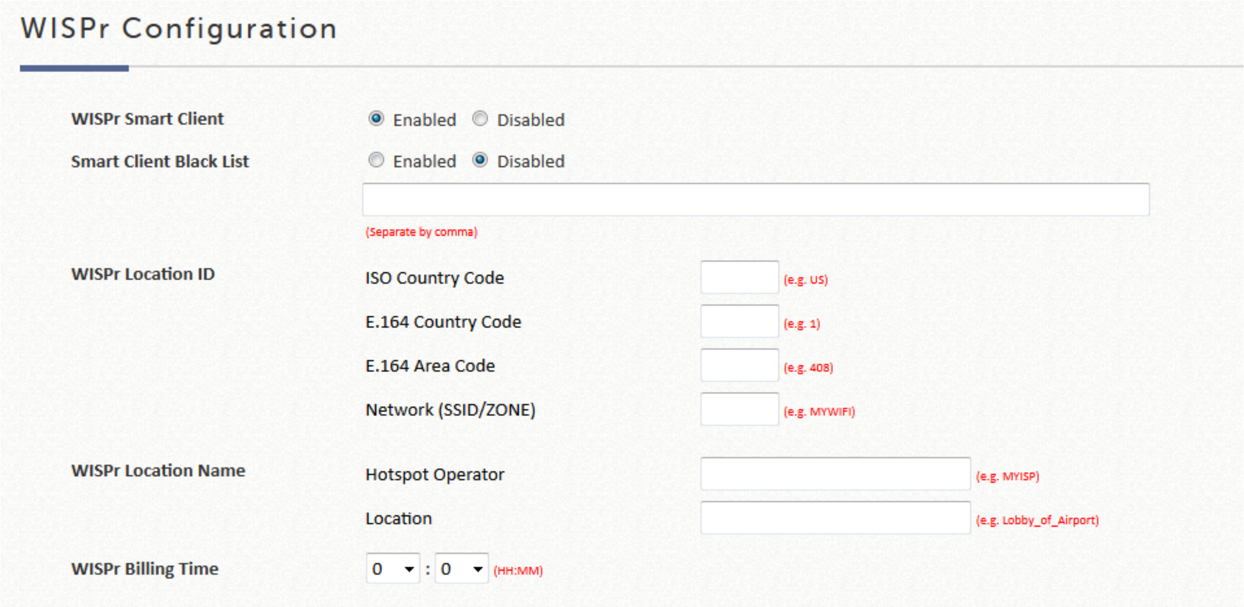
For more in depth support regarding compatibility and technical evaluation on your telecom operator, please contact Edgecore support team.

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

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

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

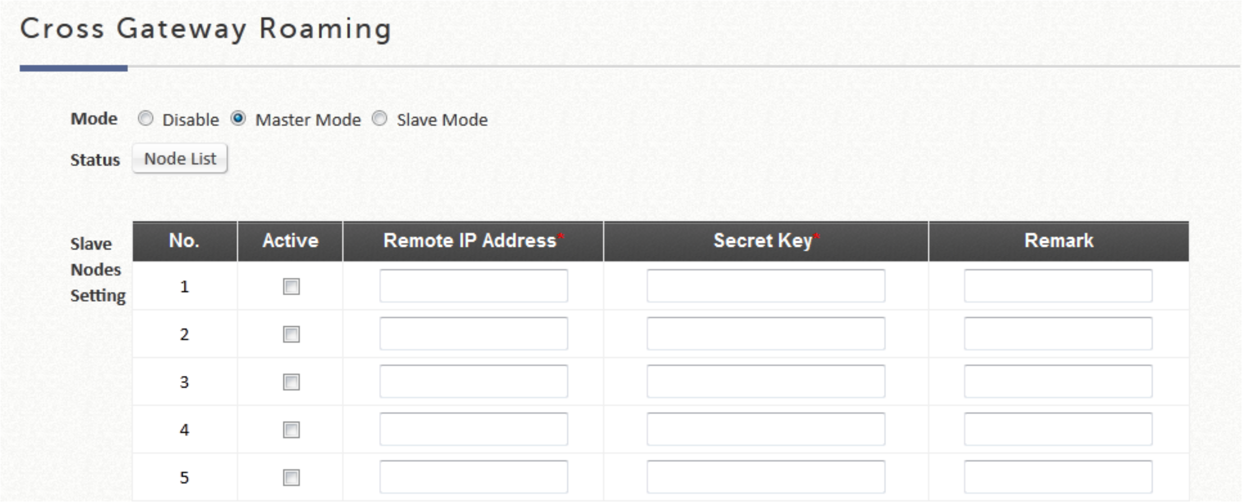
Cross Gateway roaming feature enables an end user to seamlessly move around large network deployment where there are multiple Controllers in service. Normally when a user moves from edge AP to another edge AP that is managed by another Controller, the user would experience network disconnection and would 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

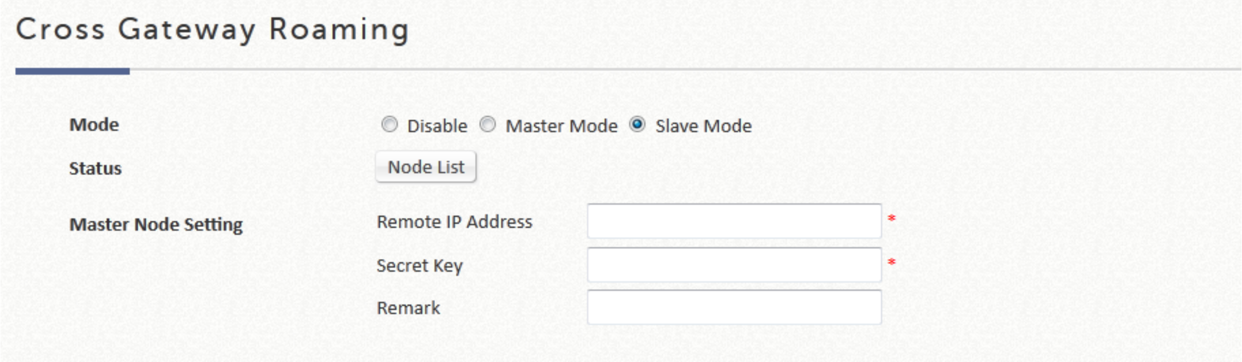
Mode ○ Disable ● Master Mode ○ Slave Mode

Status Node List

Slave Nodes Setting

No.	Active	Remote IP Address*	Secret Key*	Remark
1	☐			
2	☐			
3	☐			
4	☐			
5	☐			

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



Cross Gateway Roaming

Mode ○ Disable ○ Master Mode ● Slave Mode

Status Node List

Master Node Setting

Remote IP Address *

Secret Key *

Remark

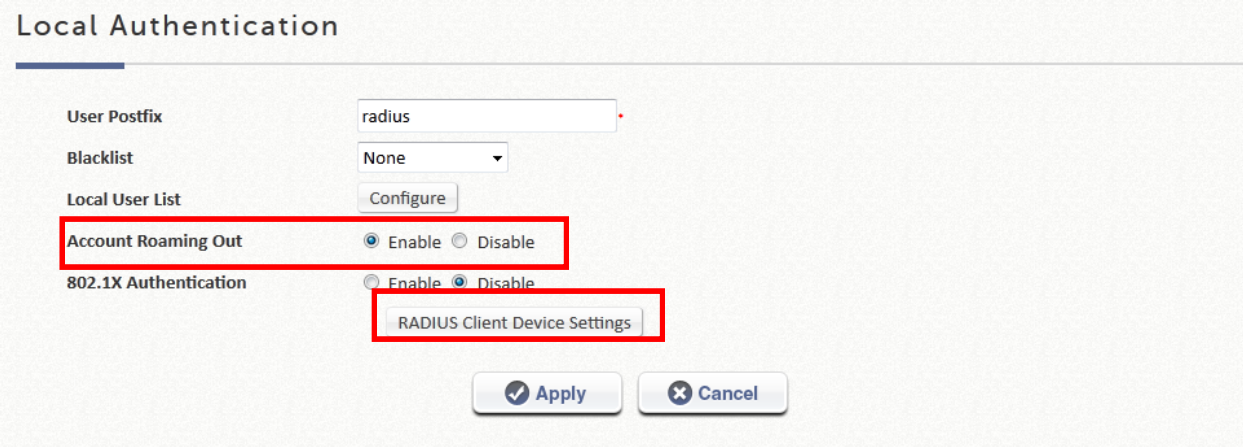
13.4 Local / On-Demand Account Roaming Out

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

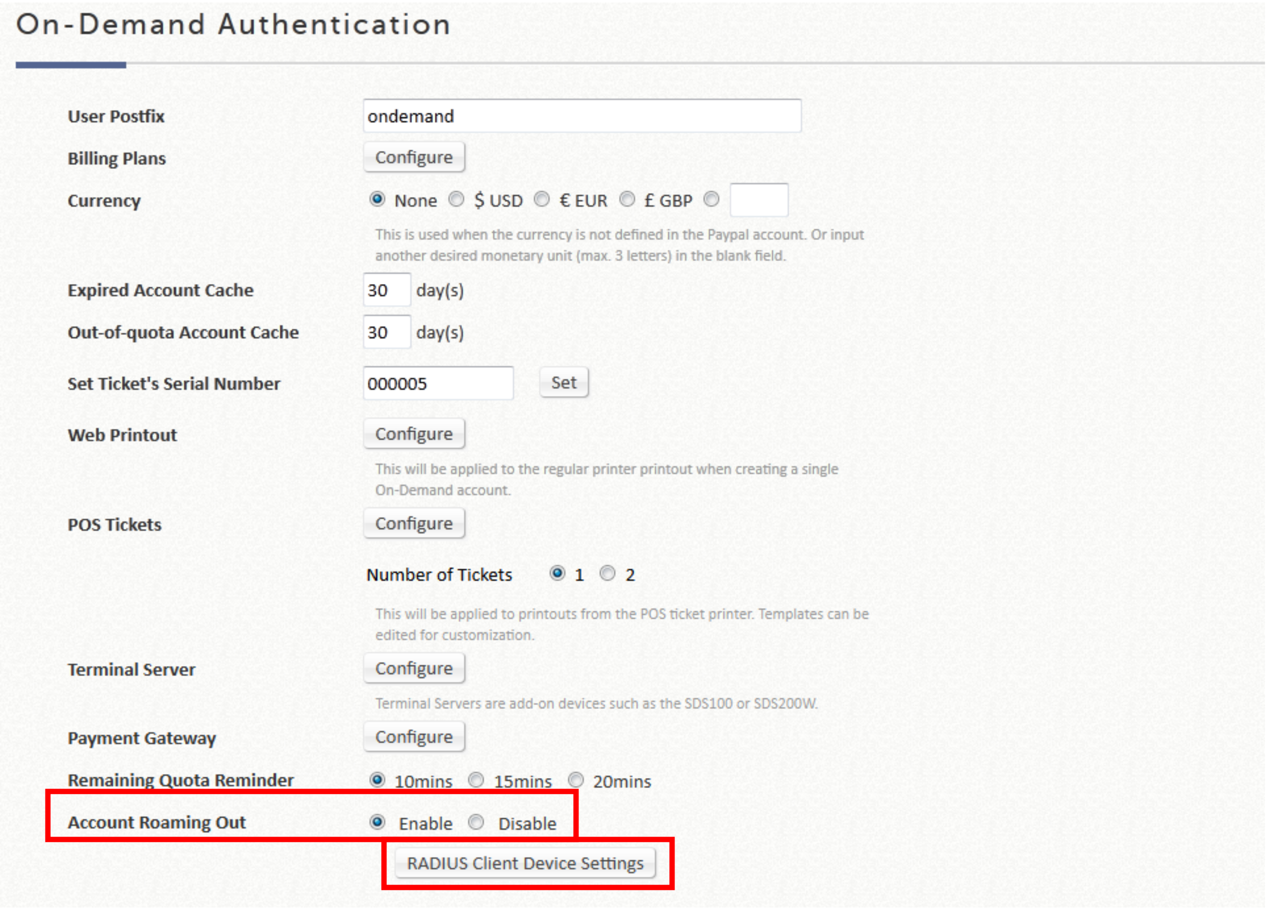
Blacklist: None

Local User List: Configure

Account Roaming Out: ● Enable ○ Disable

802.1X Authentication: ○ Enable ● Disable

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)

Set Ticket's Serial Number: 000005 Set

Web Printout: Configure

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

POS Tickets: Configure

Number of Tickets: ● 1 ○ 2

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

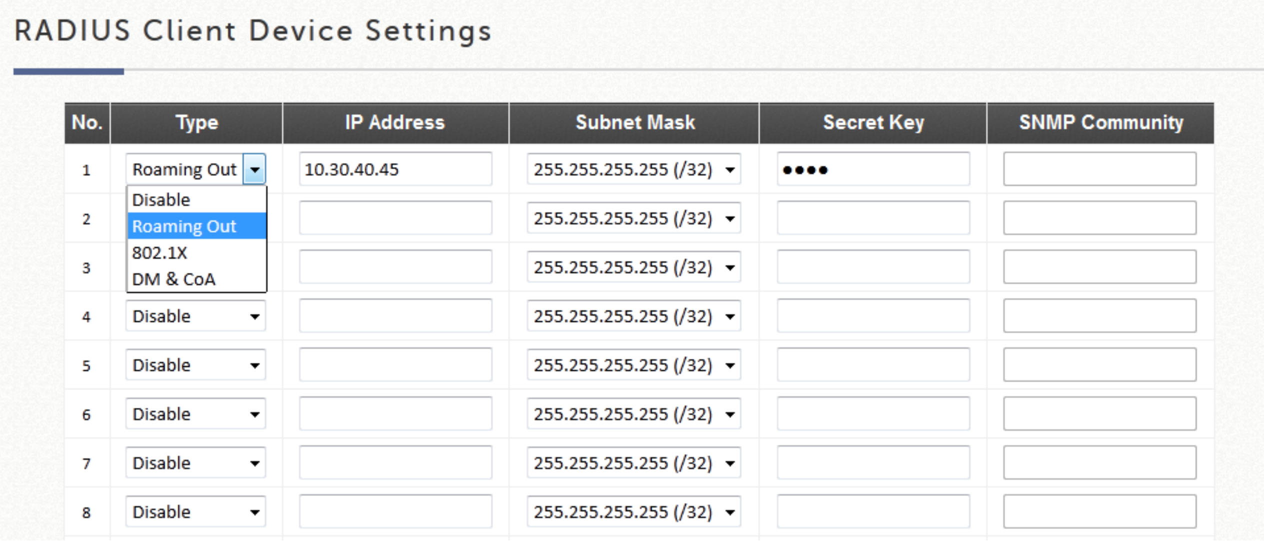
Terminal Server: Configure

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

Payment Gateway: Configure

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

Account Roaming Out: ● Enable ○ Disable


RADIUS Client Device Settings

No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	Roaming Out	10.30.40.45	255.255.255.255 (/32)	••••	
2			255.255.255.255 (/32)		
3			255.255.255.255 (/32)		
4	Disable		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

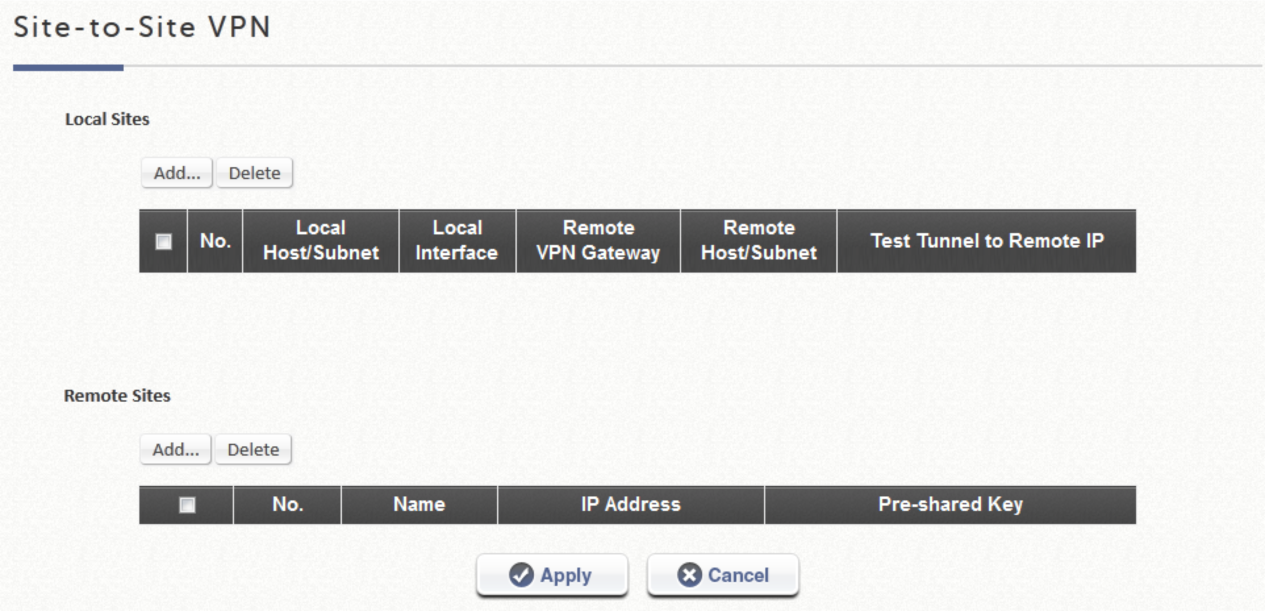
1. Please make sure that the user database postfixes are configured without conflicting with one another over the two Controllers.

Chapter 14. VPN

14.1 Site-to-Site

Configuration path: Main Menu >> Network >> VPN >> Site-to-Site 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

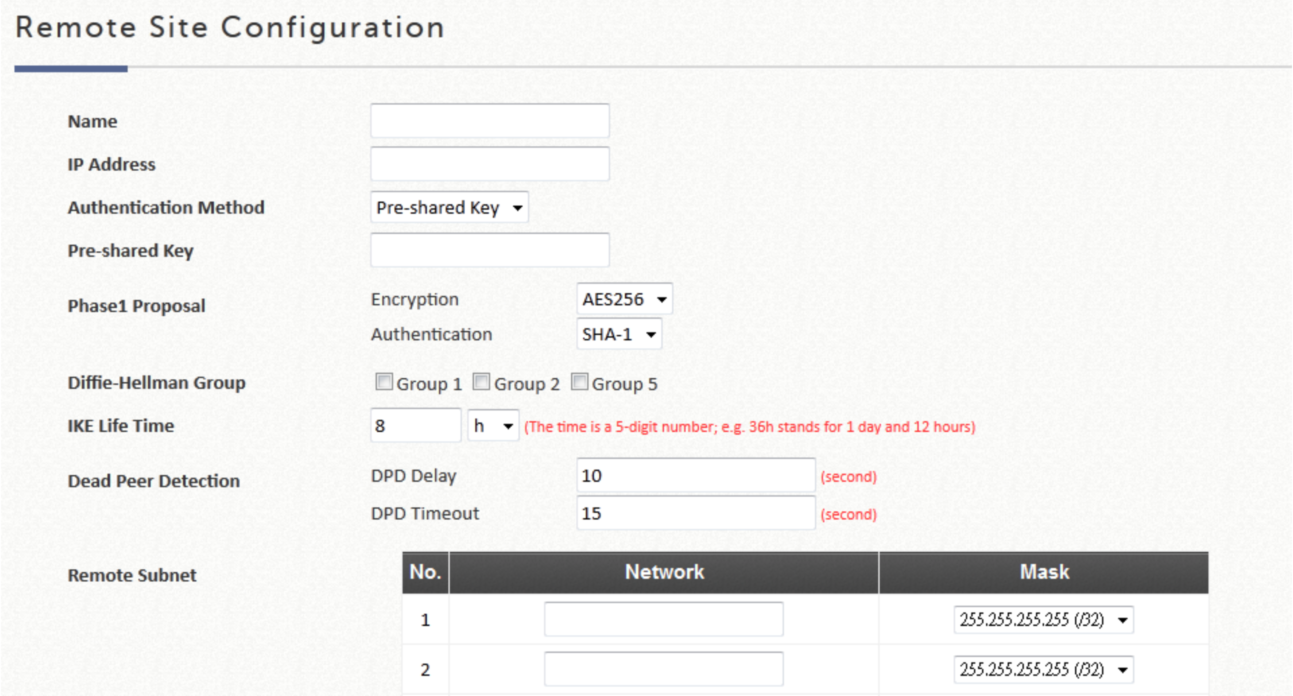
Local Sites

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

Remote Sites

☐	No.	Name	IP Address	Pre-shared Key

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

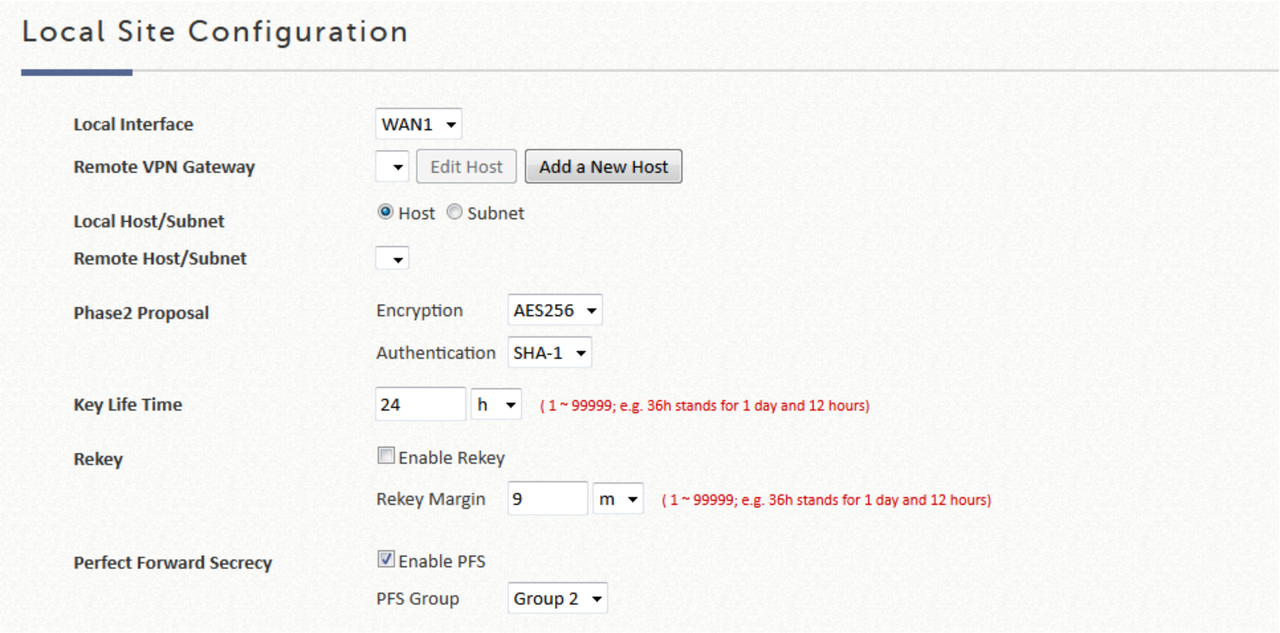
Remote Subnet

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

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	WAN1
Remote VPN Gateway	Edit Host / Add a New Host
Local Host/Subnet	● Host ○ Subnet
Remote Host/Subnet	
Phase2 Proposal	Encryption: AES256 Authentication: SHA-1
Key Life Time	24 h (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)
Rekey	☐ Enable Rekey Rekey Margin: 9 m (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)
Perfect Forward Secrecy	☑ Enable PFS PFS Group: Group 2

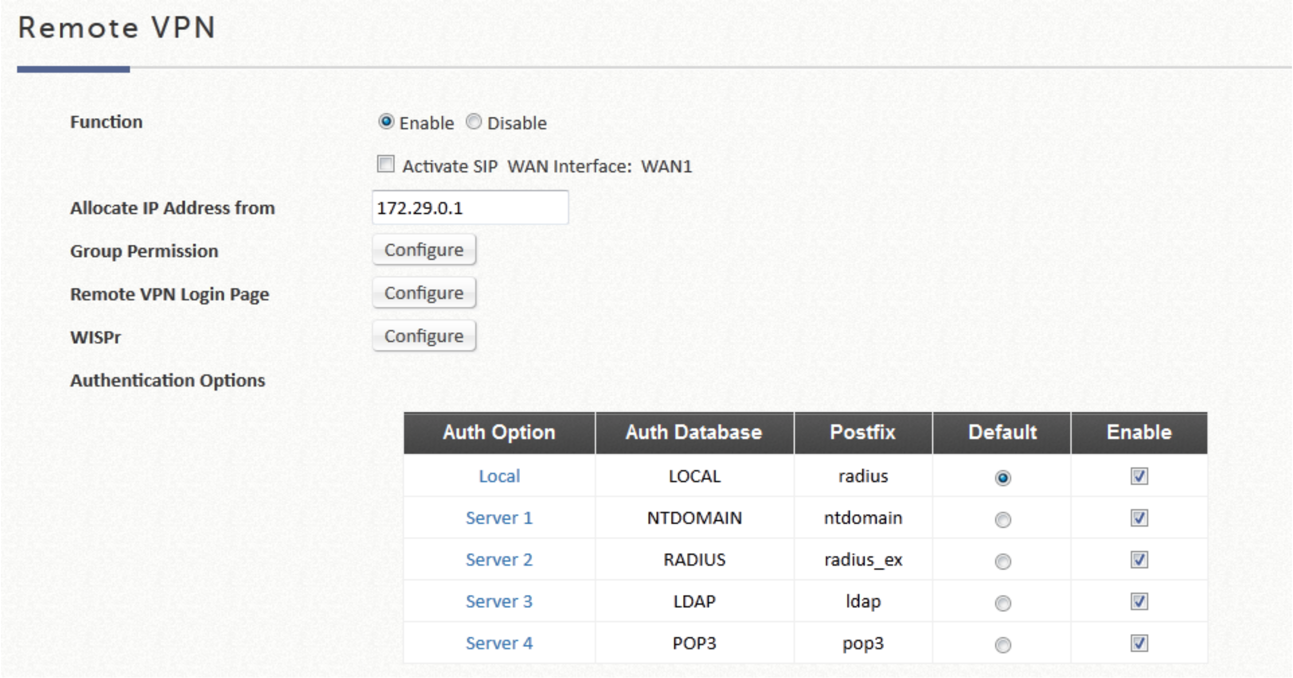
NOTE

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

14.2 Remote Client

Configuration path: Main Menu >> Network >> VPN >> Remote 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. Policy can also be applied and users are controlled by system to access the network.



Remote VPN

Function: ● Enable ○ Disable

☐ Activate SIP WAN Interface: WAN1

Allocate IP Address from: 172.29.0.1

Group Permission: Configure

Remote VPN Login Page: Configure

WISPr: Configure

Authentication Options

Auth Option	Auth Database	Postfix	Default	Enable
Local	LOCAL	radius	●	☑
Server 1	NTDOMAIN	ntdomain	○	☑
Server 2	RADIUS	radius_ex	○	☑
Server 3	LDAP	ldap	○	☑
Server 4	POP3	pop3	○	☑

All settings are similar to the settings in a Service Zone. Remote VPN can also be setup with a **SIP WAN Interface**, **Authentication Options**, **Group Permission**, **Applied Policy** and customizable Login Page.

After Remote VPN is enabled, when users browse the home page with the WAN IP, they will get to the Remote VPN login page. Input the enabled authentication options username and password, and the user will login successfully to the system.

NOTE

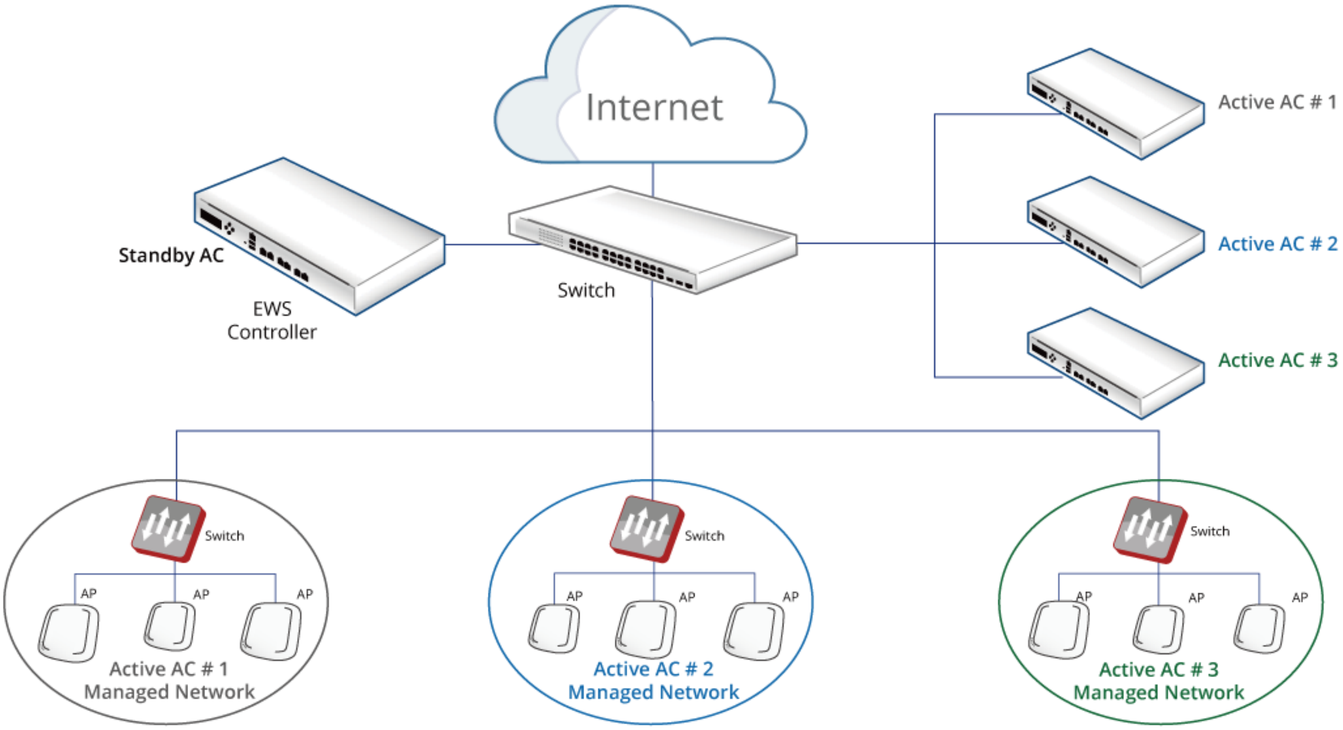
1. After Remote VPN is enabled, the default home page will be the Remove VPN login page. If you want to access the WMI of EWS Controller, please input “login.shtml” after the WAN IP. For example, : “http://192.168.X.X/login.shtml”

Chapter 15. Platform Dependent Features

15.1 High Availability (HA)

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

Configuration path: Main Menu >> System >> High Availability


Internet
Active AC # 1
Active AC # 2
Active AC # 3
Standby AC
EWS
Controller
Switch
Switch
AP
AP
AP
Active AC # 1
Managed Network
Switch
AP
AP
AP
Active AC # 2
Managed Network
Switch
AP
AP
AP
Active AC # 3
Managed Network

Feature Description:

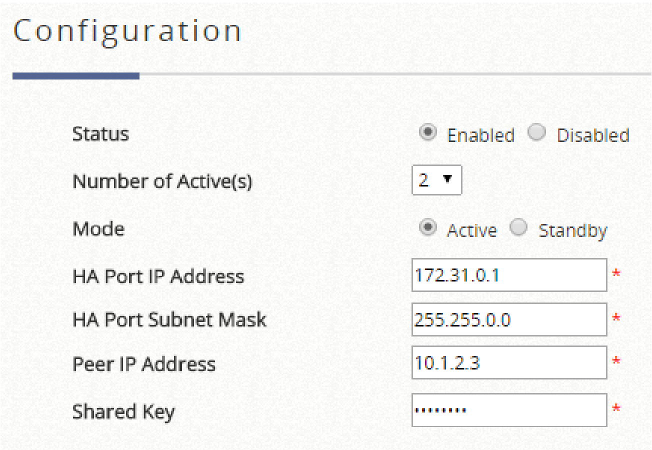
1. Edgecore HA feature is a software determined feature which can be Enabled or Disabled.

   Software determined Ethernet role:

   - When enabled, LAN1 port will become the dedicated HA port.

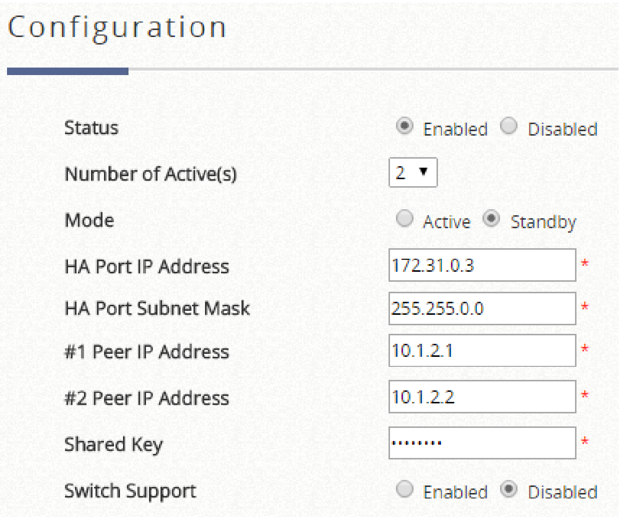
- When disabled, LAN1 remain its normal function as LAN port.

2. The Web UI has a configuration item to designate this AC as either “Active” or “Standby” when HA feature is enabled.
3. All HA configuration are manually applied. This includes AC role as an Active or Standby as well as the HA pair restoration after an AC goes down.



Configuration

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



Configuration

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

4. HA link once established synchronizes all system configurations, user databases, user online status, system resource status, managed AP profile from the Active AC to the Standby AC.
5. There is a HA link monitoring mechanism by the standby AC when HA links have been established. This link monitoring module checks the status of the Active ACs. During an event when an Active AC is not responding, this module will regard this AC as no longer providing service and take over network service.
6. Local APM managed APs will experience little network interruption as they are L2 devices. Clients associated to locally managed AP will experience the same scenario (little or no network interruption) as wired clients during service switchover.
7. Wide Area managed APs (manually or via CAPWAP) over L3 device with tunnels established will be able to resume service within 5 min max (approximation) after service switchover with full AP management capacity.
8. HA Status Changes Email Notification can be configured Status > Reporting > Notification Settings > High Availability Mode Change. For HA N+1, the email will

be sent by new Active AC when it replaces to provide service; besides, there is a Standby-AC-is-DOWN email will be sent from Active AC(s) when there is no Standby AC detected when HA is already enabled.

9. HA feature can only be enabled for up to 3 ACs of the same brand and same FW version and build number.

15.2 WiFi Monitor

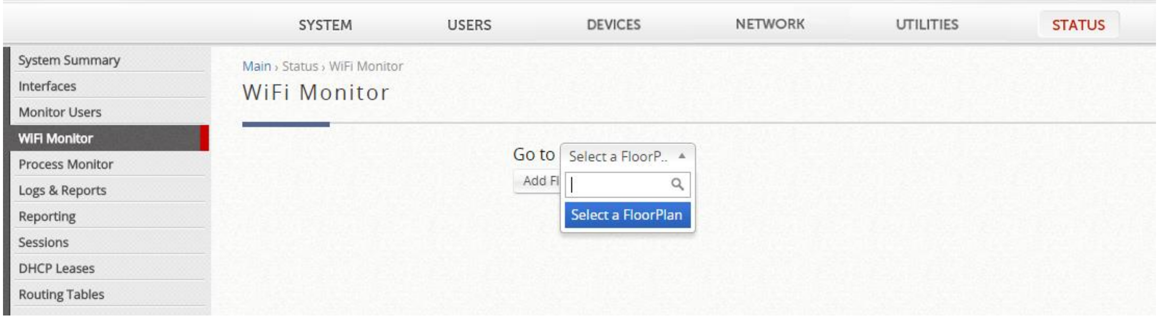
WiFi Monitor allows the administrator to simulate WiFi signal coverage of Access Points; be it a virtual area or a real managed APs signal coverage. It also monitors AP statuses and statistic information of the managed APs.

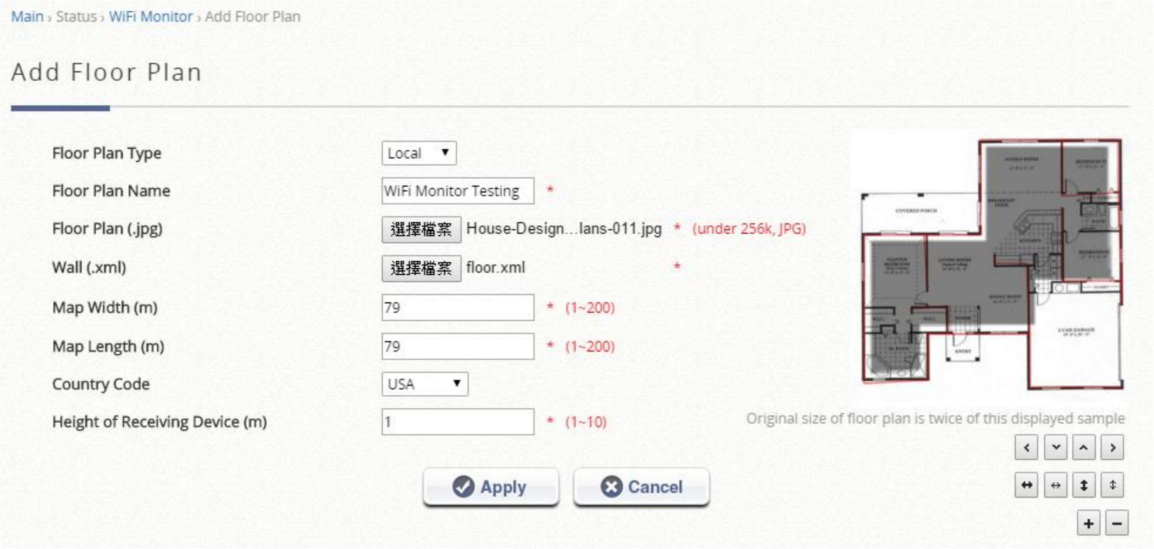
This is designed to help administrators with network survey, planning and performance enhancement during the initial installation stage, and also monitoring managed APs in an existing deployment.

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

15.3.1. Add a Floor Plan

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


SYSTEM
USERS
DEVICES
NETWORK
UTILITIES
STATUS
System Summary
Interfaces
Monitor Users
WiFi Monitor
Process Monitor
Logs & Reports
Reporting
Sessions
DHCP Leases
Routing Tables
Main › Status › WiFi Monitor
WiFi Monitor
Go to
Select a FloorP..
Add Fl
Select a FloorPlan



Main › Status › WiFi Monitor › Add Floor Plan

Add Floor Plan

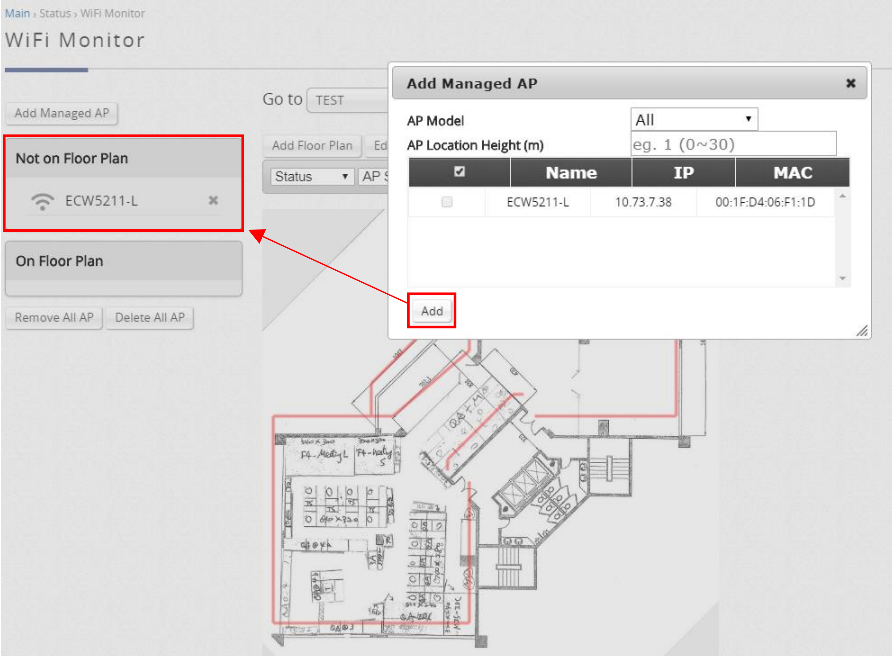
Floor Plan Type	Local
Floor Plan Name	WiFi Monitor Testing *
Floor Plan (.jpg)	選擇檔案 House-Design...lans-011.jpg * (under 256k, JPG)
Wall (.xml)	選擇檔案 floor.xml *
Map Width (m)	79 * (1~200)
Map Length (m)	79 * (1~200)
Country Code	USA
Height of Receiving Device (m)	1 * (1~10)

Original size of floor plan is twice of this displayed sample

Apply
Cancel
+
−

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

Access Points here are linked to APs managed by the 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

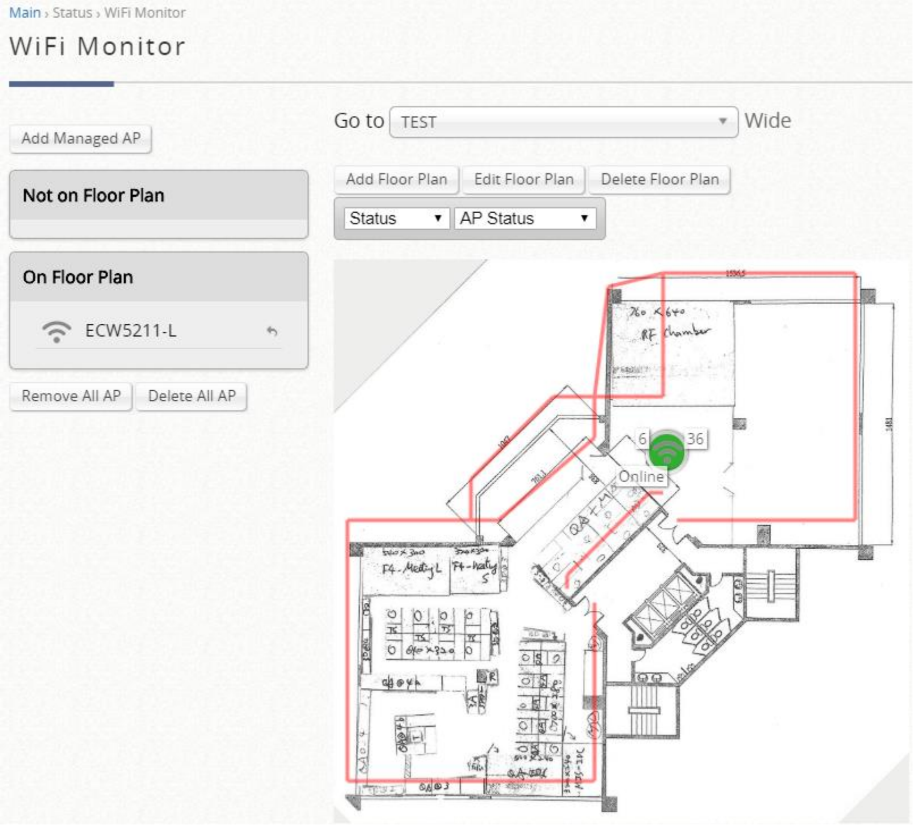
Add Managed AP
Not on Floor Plan
ECW5211-L
On Floor Plan
Remove All AP
Delete All AP
Go to TEST
Add Floor Plan
Status
Add

Add Managed AP

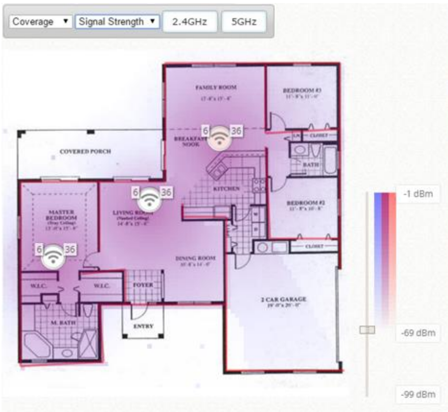
AP Model	All
AP Location Height (m)	eg. 1 (0~30)

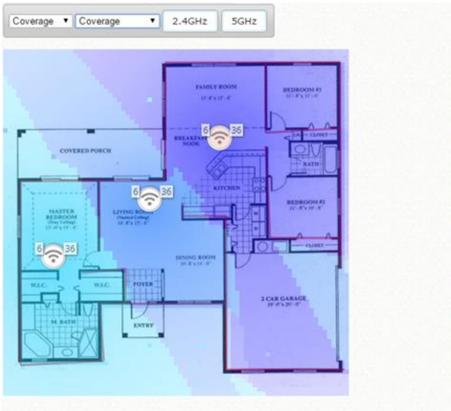
☑	Name	IP	MAC
☐	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D

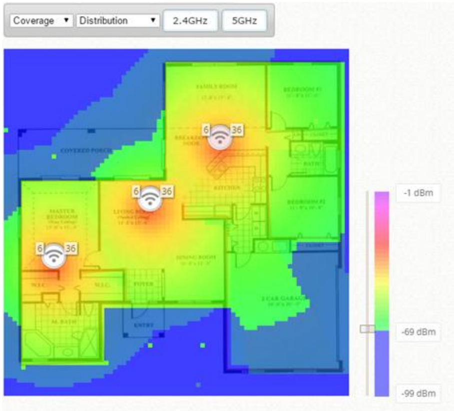
Once these managed APs are created, simply drag and drop these APs onto the floor plan. 2.4GHz is indicated blue and 5GHz is indicated red for signal strength (hence purple when both bands are overlapping).


Main › Status › WiFi Monitor
WiFi Monitor
Add Managed AP
Go to
TEST
Wide
Not on Floor Plan
Add Floor Plan
Edit Floor Plan
Delete Floor Plan
Status
AP Status
On Floor Plan
ECW5211-L
Remove All AP
Delete All AP
6
36
Online

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


Coverage
Signal Strength
2.4GHz
5GHz
6
36
-1 dBm
-69 dBm
-99 dBm

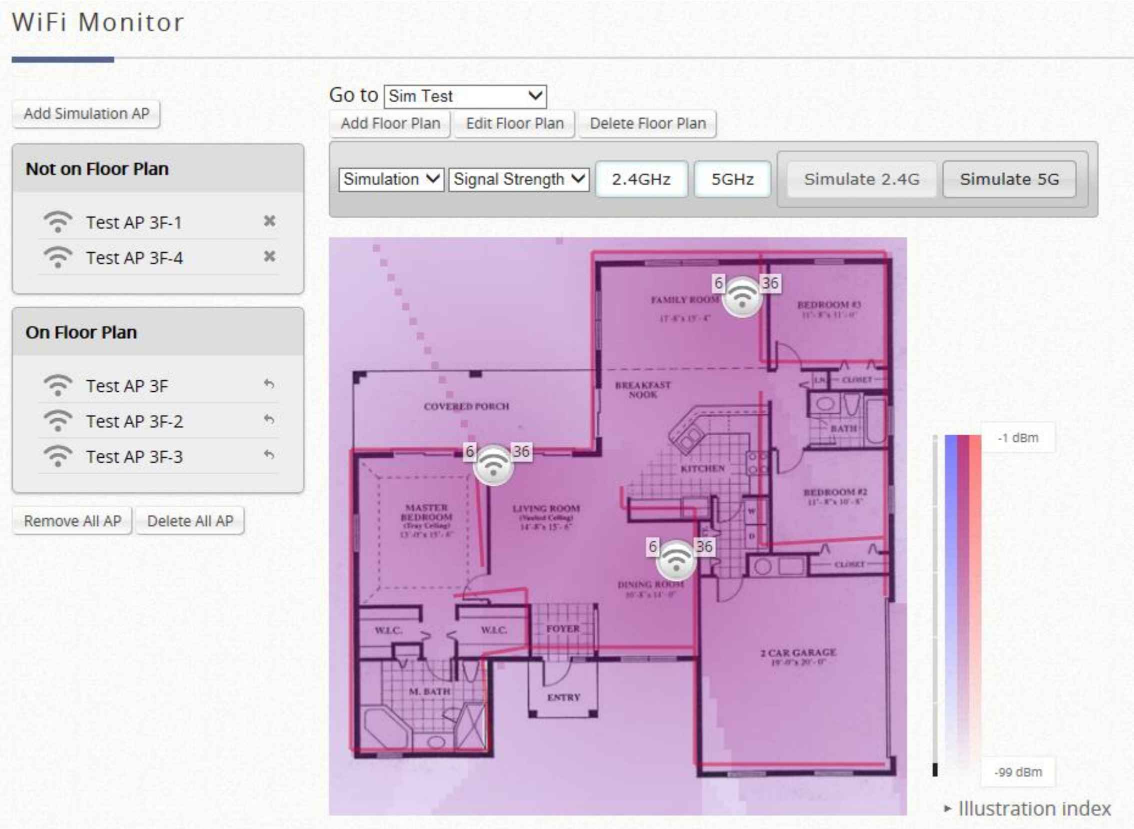

Coverage
Coverage
2.4GHz
5GHz
6
36


Coverage
Distribution
2.4GHz
5GHz
6
36
-1 dBm
-69 dBm
-99 dBm

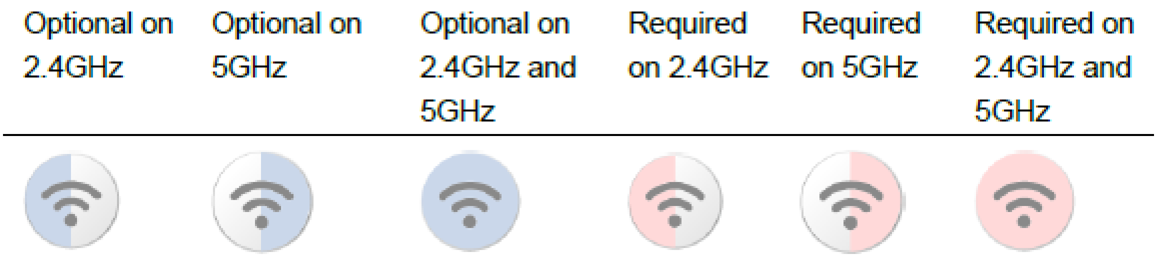
15.3.2. Simulation AP

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.

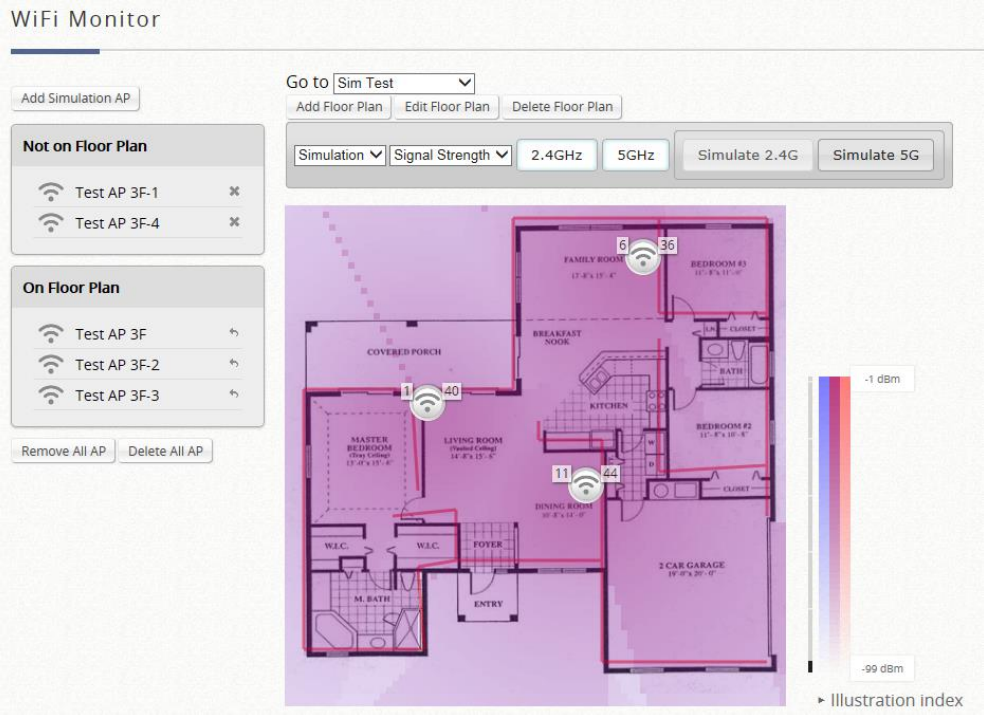
With the floor plan and partitions in place, simulation APs can now be added to the floor plan for simulation as shown below.

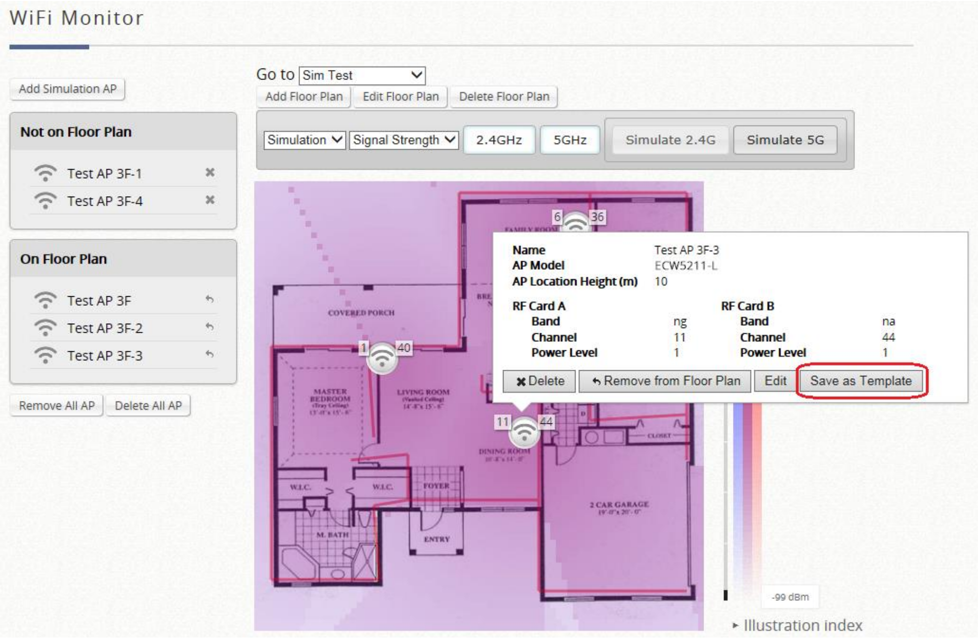

WiFi Monitor
Add Simulation AP
Not on Floor Plan
Test AP 3F-1
Test AP 3F-4
On Floor Plan
Test AP 3F
Test AP 3F-2
Test AP 3F-3
Remove All AP
Delete All AP
Go to Sim Test
Add Floor Plan
Edit Floor Plan
Delete Floor Plan
Simulation
Signal Strength
2.4GHz
5GHz
Simulate 2.4G
Simulate 5G
6
36
-1 dBm
-99 dBm
Illustration index

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


Optional on 2.4GHz
Optional on 5GHz
Optional on 2.4GHz and 5GHz
Required on 2.4GHz
Required on 5GHz
Required on 2.4GHz and 5GHz

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


WiFi Monitor
Add Simulation AP
Not on Floor Plan
Test AP 3F-1
Test AP 3F-4
On Floor Plan
Test AP 3F
Test AP 3F-2
Test AP 3F-3
Remove All AP
Delete All AP
Go to Sim Test
Add Floor Plan
Edit Floor Plan
Delete Floor Plan
Simulation
Signal Strength
2.4GHz
5GHz
Simulate 2.4G
Simulate 5G
6
36
1
40
11
44
FAMILY ROOM
BEDROOM #3
BREAKFAST NOOK
COVERED PORCH
CLOSET
BATH
KITCHEN
BEDROOM #2
MASTER BEDROOM
LIVING ROOM
DINING ROOM
W.I.C.
W.I.C.
FOYER
2 CAR GARAGE
M. BATH
ENTRY
-1 dBm
-99 dBm
▸ Illustration index


WiFi Monitor
Add Simulation AP
Not on Floor Plan
Test AP 3F-1
Test AP 3F-4
On Floor Plan
Test AP 3F
Test AP 3F-2
Test AP 3F-3
Remove All AP
Delete All AP
Go to Sim Test
Add Floor Plan
Edit Floor Plan
Delete Floor Plan
Simulation
Signal Strength
2.4GHz
5GHz
Simulate 2.4G
Simulate 5G
6
36
1
40
11
44
COVERED PORCH
MASTER BEDROOM
LIVING ROOM
DINING ROOM
W.I.C.
W.I.C.
FOYER
2 CAR GARAGE
M. BATH
ENTRY
CLOSET
-99 dBm
▸ Illustration index
✖ Delete
↰ Remove from Floor Plan
Edit
Save as Template

Name Test AP 3F-3
AP Model ECW5211-L
AP Location Height (m) 10

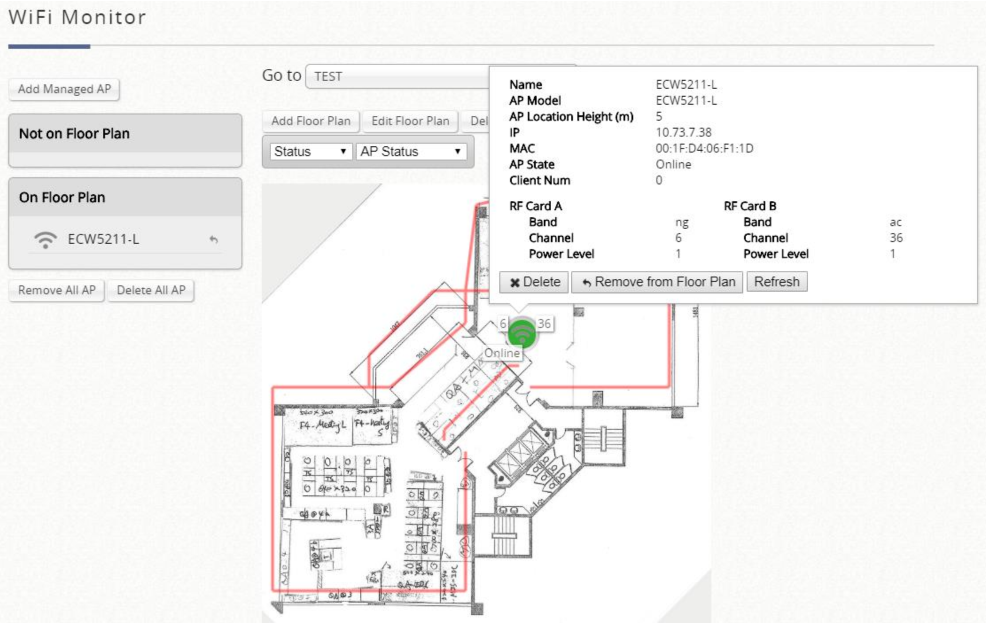
RF Card A		**RF Card B**	
Band	ng	**Band**	na
Channel	11	**Channel**	44
Power Level	1	**Power Level**	1

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

15.3.3. 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
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
Delete
Remove from Floor Plan
Refresh
6
36
Online

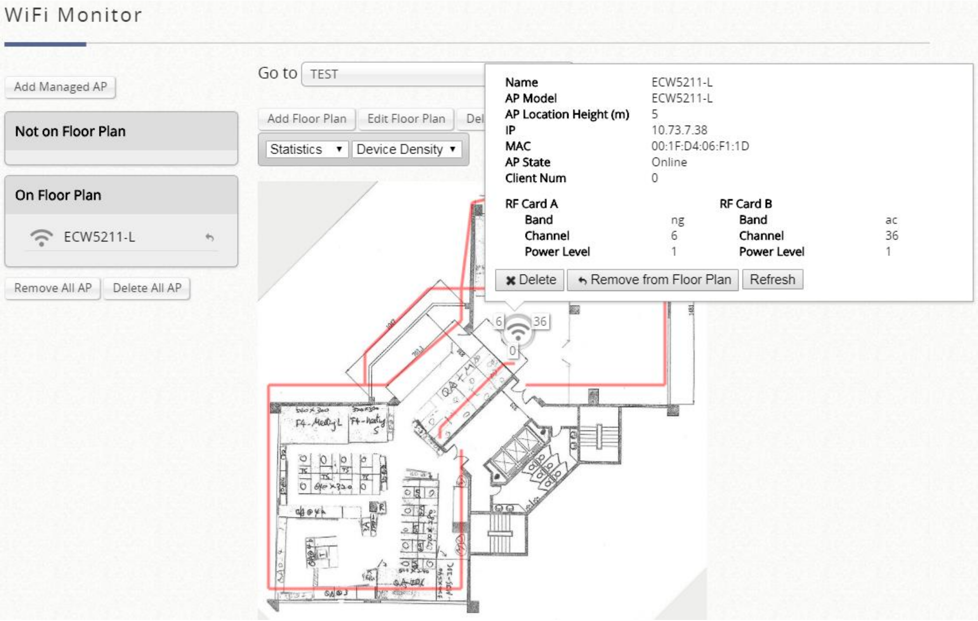
Go to TEST

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

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
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
Delete
Remove from Floor Plan
Refresh
6
36
0

Go to TEST

Statistics ▾ Device Density ▾

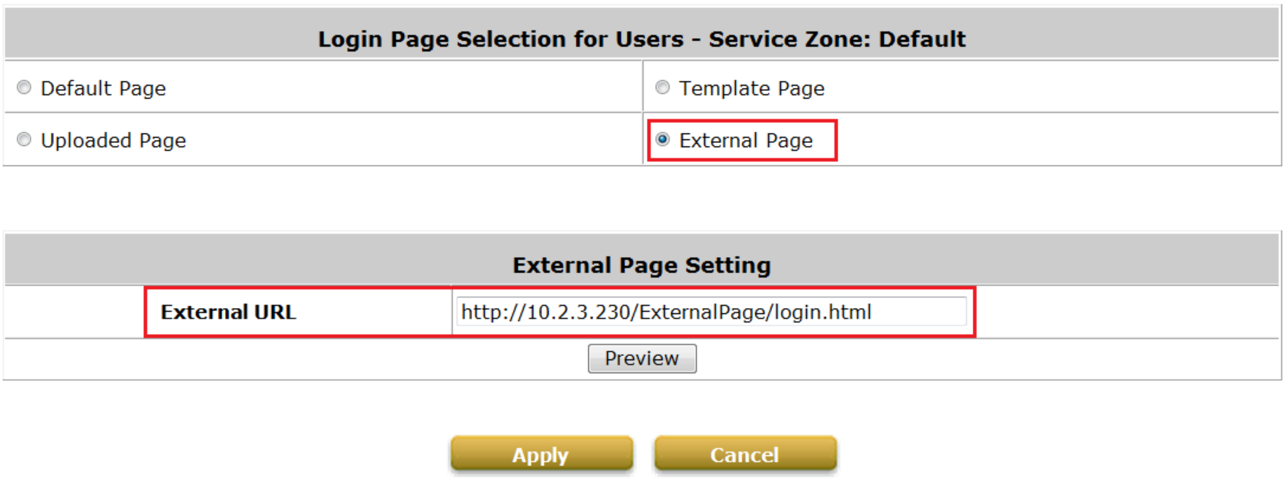
Name	ECW5211-L
AP Model	ECW5211-L
AP Location Height (m)	5
IP	10.73.7.38
MAC	00:1F:D4:06:F1:1D
AP State	Online
Client Num	0

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

Appendix A. 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.



Login Page Selection for Users - Service Zone: Default

○ Default Page	○ Template Page
○ Uploaded Page	● External Page

External Page Setting

External URL: http://10.2.3.230/ExternalPage/login.html

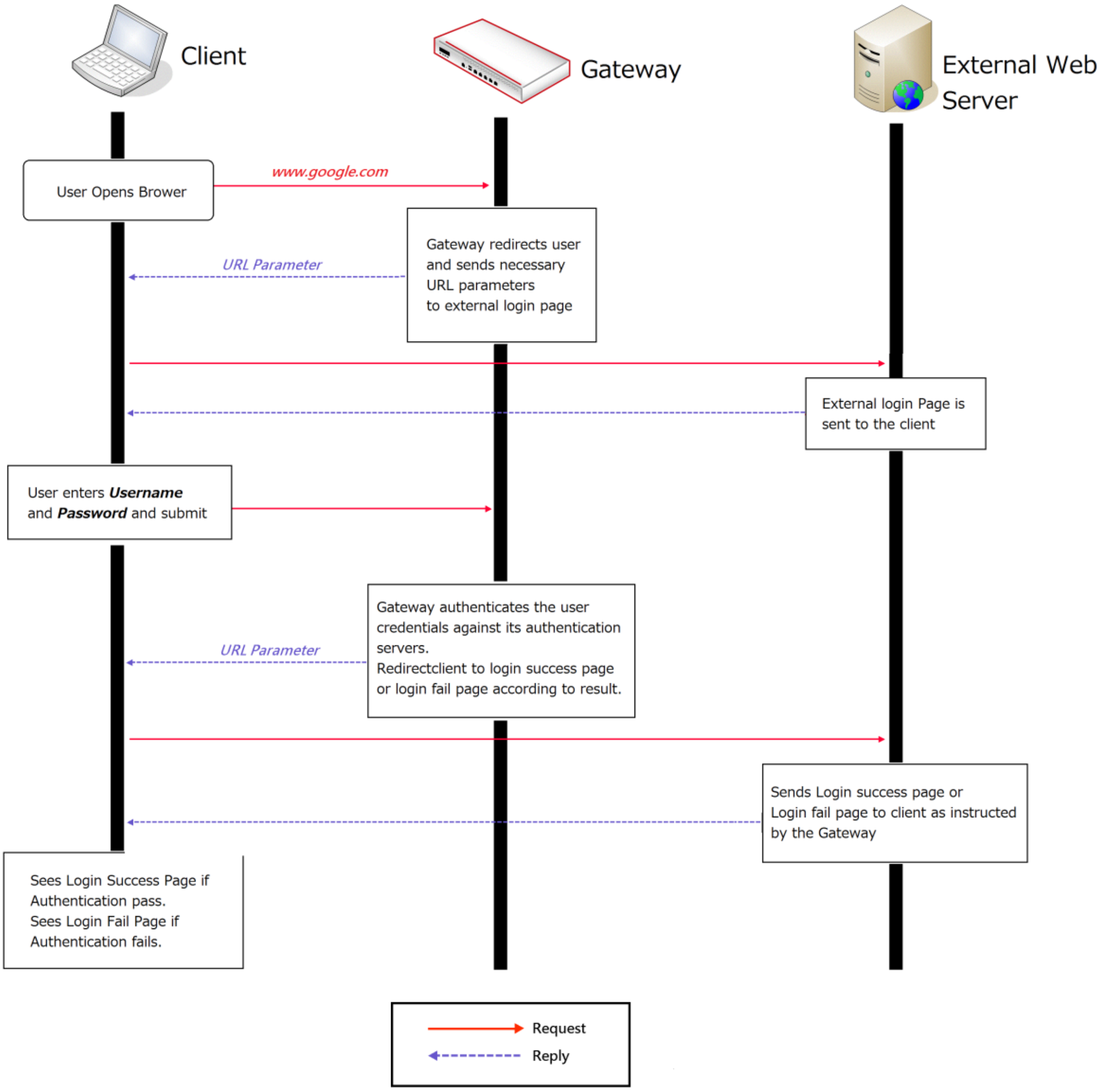
Main Menu>System>Service Zone>Service Zone Configuration>Login Page

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.

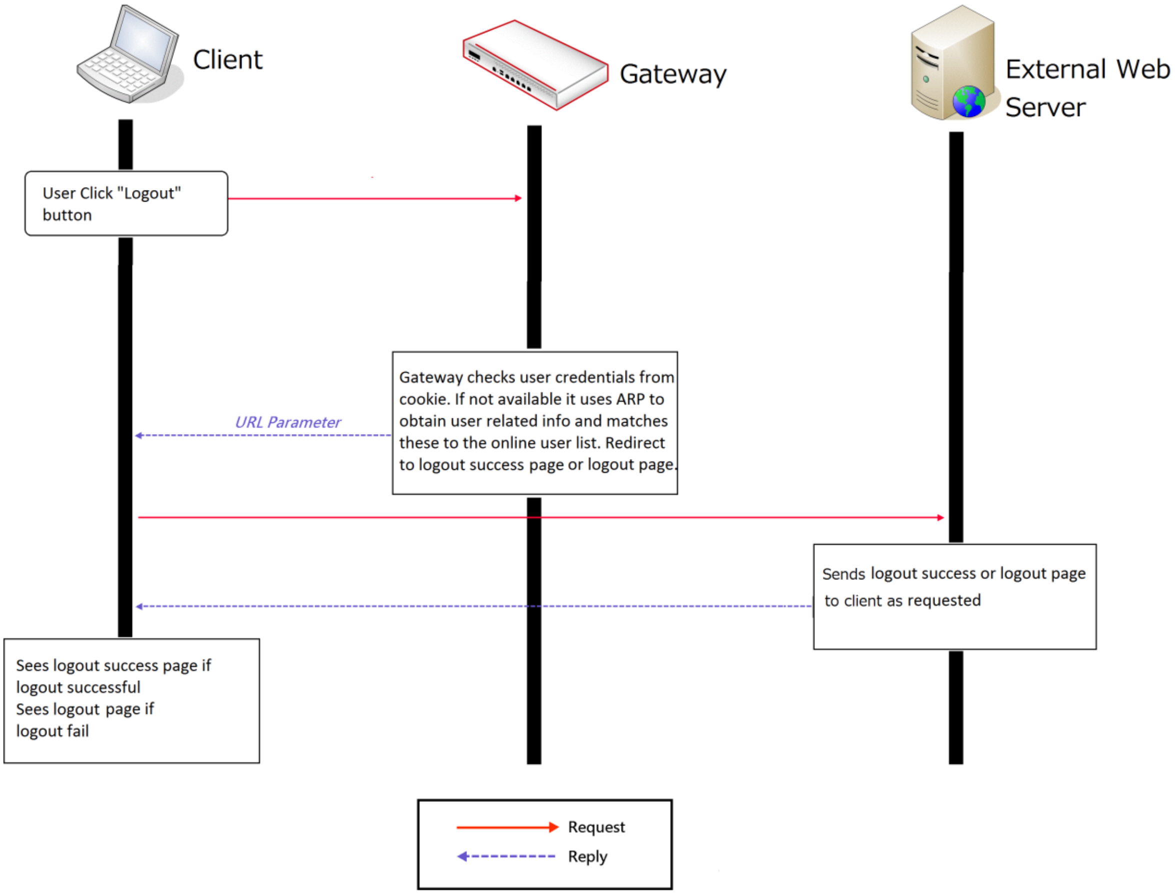
Therefore it is important that your external pages are designed by someone with good knowledge of URL parameter utilization.

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

Login:


Client
Gateway
External Web Server
User Opens Brower
www.google.com
Gateway redirects user and sends necessary URL parameters to external login page
URL Parameter
External login Page is sent to the client
User enters *Username* and *Password* and submit
Gateway authenticates the user credentials against its authentication servers.
Redirectclient to login success page or login fail page according to result.
URL Parameter
Sends Login success page or Login fail page to client as instructed by the Gateway
Sees Login Success Page if Authentication pass.
Sees Login Fail Page if Authentication fails.
Request
Reply

Logout:


Client
Gateway
External Web Server
User Click "Logout" button
URL Parameter
Gateway checks user credentials from cookie. If not available it uses ARP to obtain user related info and matches these to the online user list. Redirect to logout success page or logout page.
Sends logout success or logout page to client as requested
Sees logout success page if logout successful
Sees logout page if logout fail
Request
Reply

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.

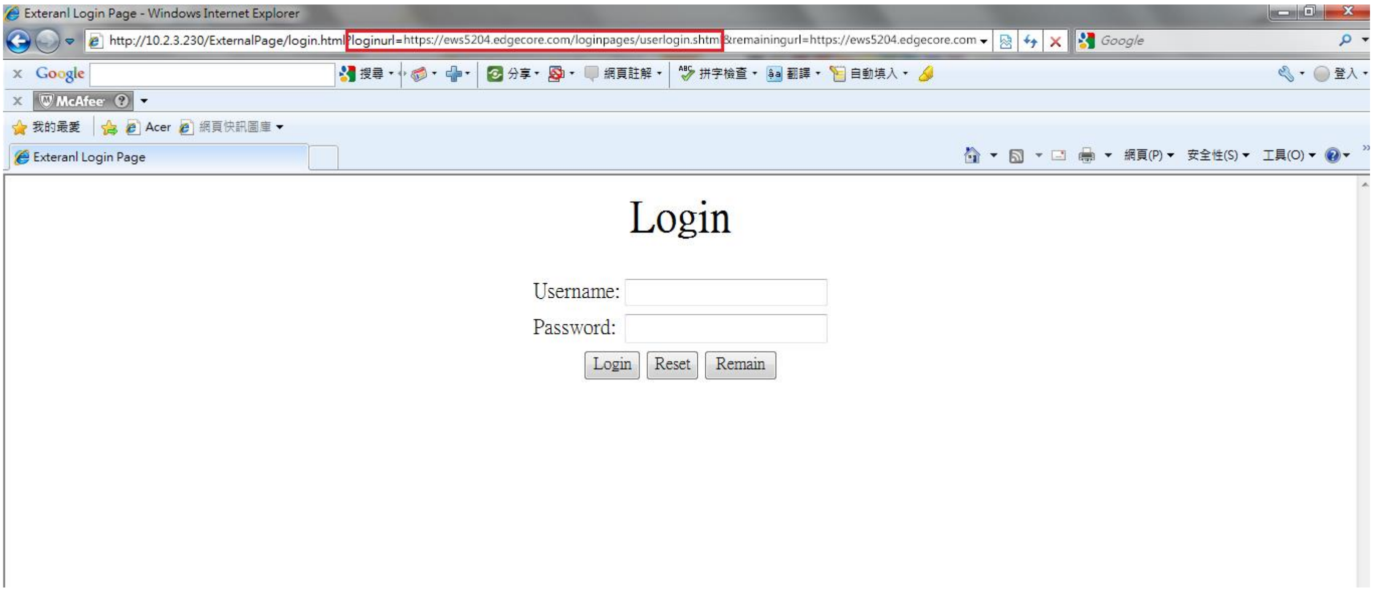
You will need to parse the required parameters in your html code. The following HTML code segment is an example of parsing *loginurl* parameter with a self defined javascript function:

```
<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:



Exteranl Login Page - Windows Internet Explorer

http://10.2.3.230/ExternalPage/login.html?loginurl=https://ews5204.edgecore.com/loginpages/userlogin.shtm&remainingurl=https://ews5204.edgecore.com

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
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, include: client IP address, MAC address, date, and return URL.

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	RADUIS 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)
session	String	Encrypted session information

3. External Error Page Variables:

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

	User of this device (the MAC address) is not allowed to use this account.<BR>Please contact your network administrator. Sorry, the external authentication server is currently unreachable. <BR>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)	
vlanid	Integer (1~4094)	VLAN ID
client_ip	IP format	Client IP address
gwip	IP format	Gateway activated IP address
original_uid	String	Original User ID

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 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
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
session	String	Encrypted session information

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

This page 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
session	Optional	String	Encoded string which contains some information of this session, 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: Sorry, this feature is available for On-Demand user only. Sorry, this username: XXX is not found.	Error messages

	Sorry, this username: XXX is out of quota. Sorry, this username: XXX is expired. Sorry, this username: XXX is redeemed.	
Value	Integer (Sec. Or Byte) or error no. -1: Account not found. -2: Out of quota. -3: Expired. -4: Redeemed.	Remaining quota, if user is time type, the value is remaining seconds, if user is volume type, the value remaining bytes.
Uname	String	User name
Type	String, includes: TIME: Time type DATA: Volume type CUTOFF: Cut-off type	On-Demand user billing type

4. Change Password

Path:

(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	String, including: Change password successfully User password is incorrect Invalid password format	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
Uid	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 alternative variables: (username, user, account)	Required	String	Redeem user ID
mypassword alternative variables (passwd, password, pass)	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 can not be found from the database. Redeem user name can not 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.	Result and error messages

	Maximum allowable time has exceeded. Maximum allowable memory space has exceeded. Wrong postfix please check it. This account is expired.	

6. On-Demand Account Creation

Path:

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

Input:

Field	Required	Value	Description
buttonNo	Required	Integer (1~10)	Billing Plan No.
random	Optional	Integer	A random number, this number is to prevent quick-click issue in IE 6.0.
ret_url	Optional	String (URL encoded)	Return URL.

Output:

If no ret_url is presented, the client would be led to a ticket page in our UI style. If ret_url is presented, client would return to ret_url and receive the result containing created On-Demand account information.

Field	Value	Description
Result	String, the format is: (separated by ',') username, password, expiretime, usage, price, duration, serial number	If ret_url is presented, the client would return to ret_url page and carry the result valuable. expiretime is account expiration time which is a Linux time stamp, and duration is account duration time and the unit is 'day', serial number is account s/n.

Appendix B. 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 C. 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.

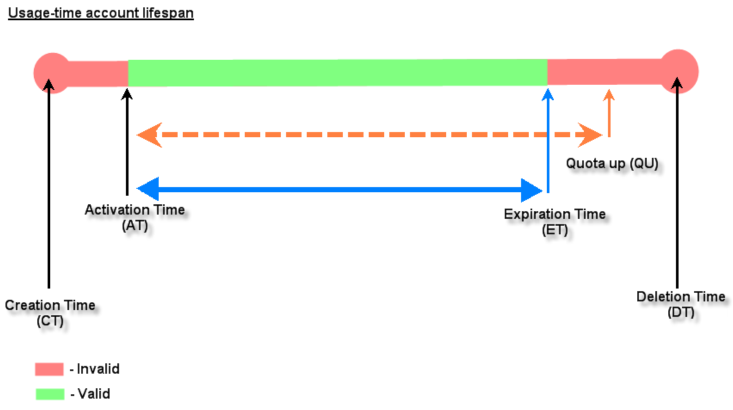
- **Hotel Cut-off** (Buy the time interval for a valid account)
- **Duration-time** (Buy the time interval for a valid account)

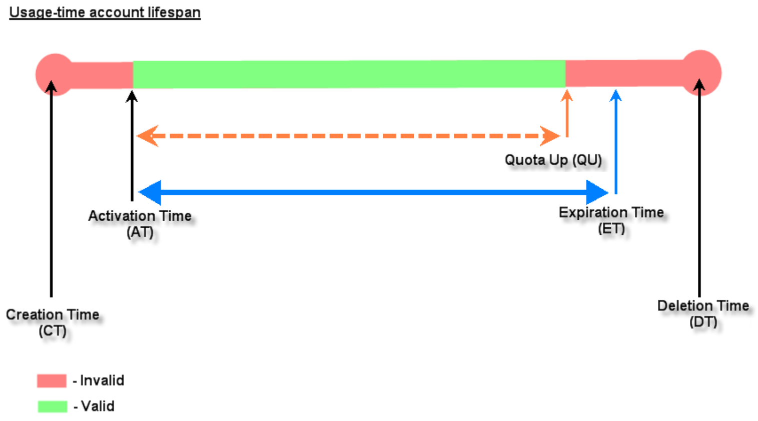
Define the time interval for usage. Count down begins when account activated and expires when the expiration time/date reached.

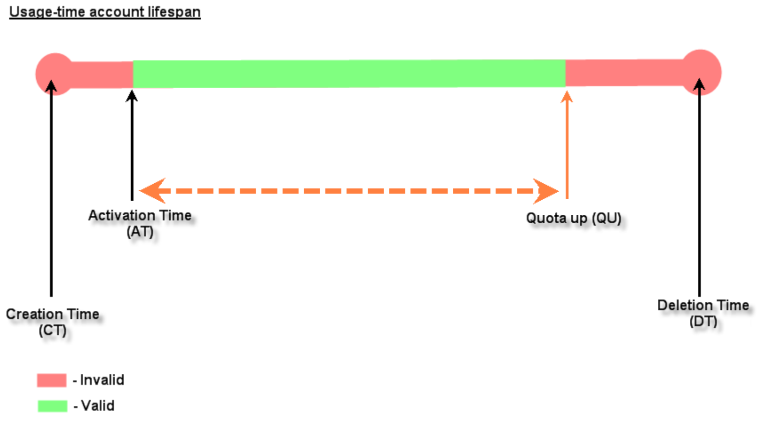
Usage-time

- 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.

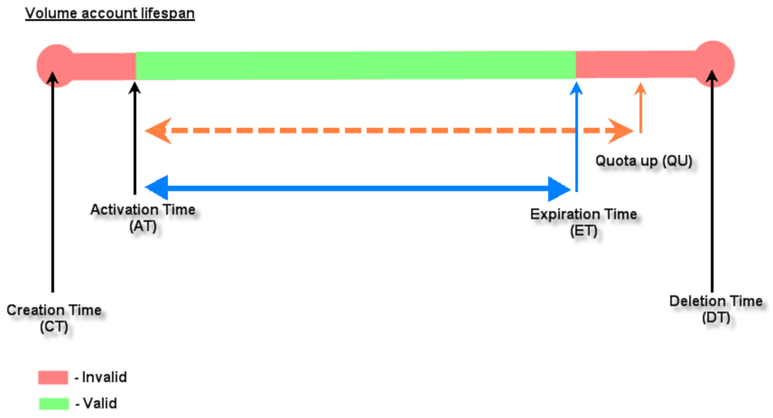

Usage-time account lifespan
Quota up (QU)
Activation Time (AT)
Expiration Time (ET)
Creation Time (CT)
Deletion Time (DT)
🟥 - Invalid
🟩 - Valid

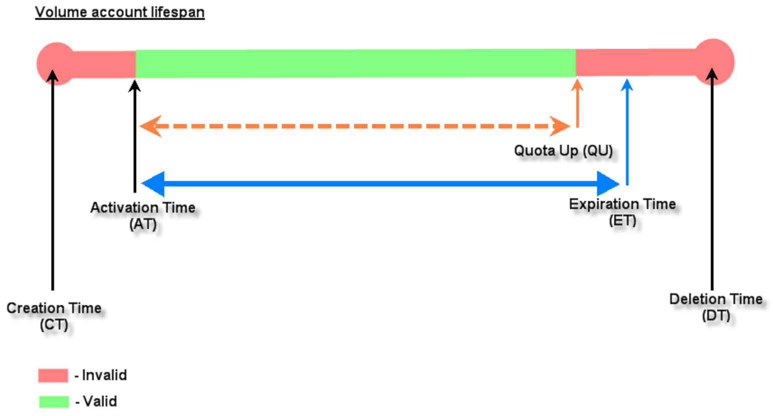

Usage-time account lifespan
Quota Up (QU)
Activation Time (AT)
Expiration Time (ET)
Creation Time (CT)
Deletion Time (DT)
🟥 - Invalid
🟩 - Valid


Usage-time account lifespan
Activation Time (AT)
Quota up (QU)
Creation Time (CT)
Deletion Time (DT)
🟥 - Invalid
🟩 - Valid

Volume

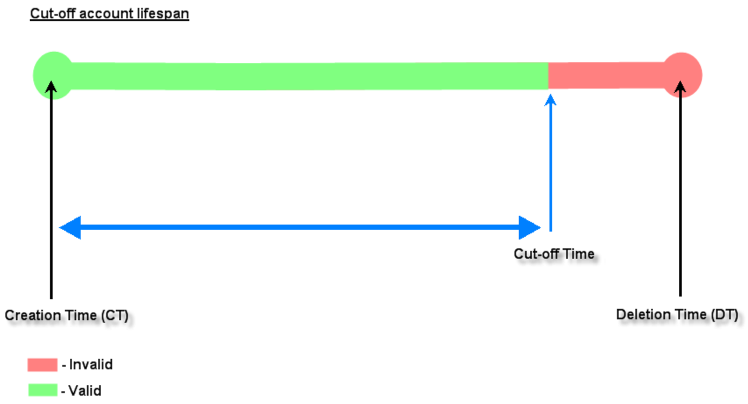
- Users can access internet as long as account is valid with remaining quota and need to activate the purchased account within a given time period by logging in.
- Account expires when *Valid Period* is used up or quota is depleted.

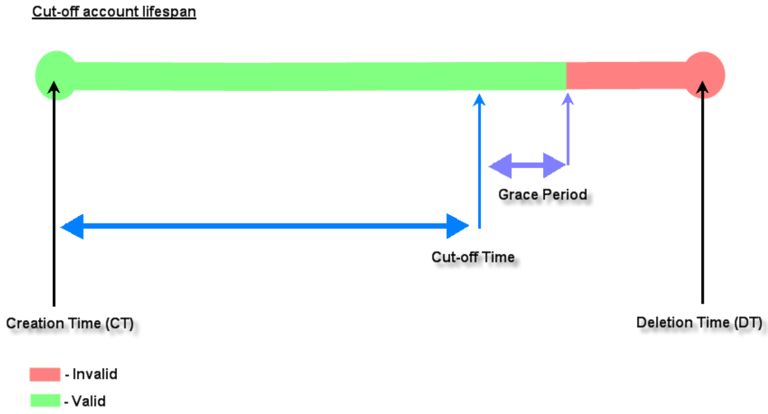

Volume account lifespan
Quota up (QU)
Activation Time (AT)
Expiration Time (ET)
Creation Time (CT)
Deletion Time (DT)
- Invalid
- Valid


Volume account lifespan
Quota Up (QU)
Activation Time (AT)
Expiration Time (ET)
Creation Time (CT)
Deletion Time (DT)
- Invalid
- Valid

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.


Cut-off account lifespan
Cut-off Time
Creation Time (CT)
Deletion Time (DT)
- Invalid
- Valid


Cut-off account lifespan
Grace Period
Cut-off Time
Creation Time (CT)
Deletion Time (DT)
- Invalid
- Valid

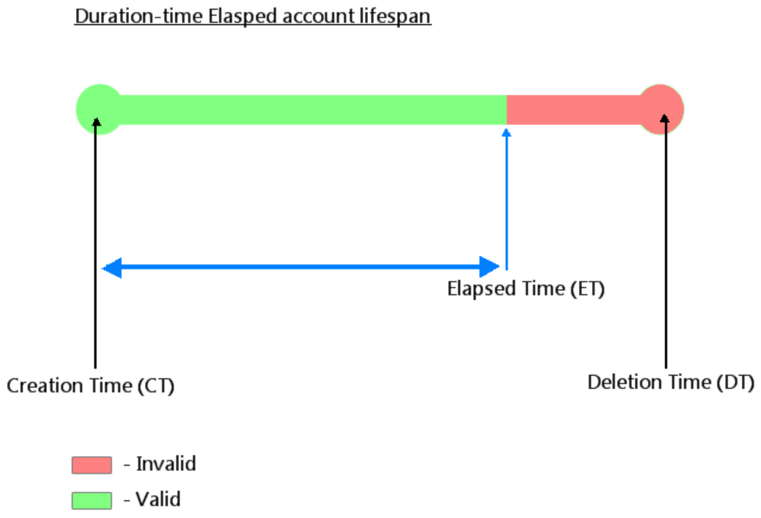
Duration Time

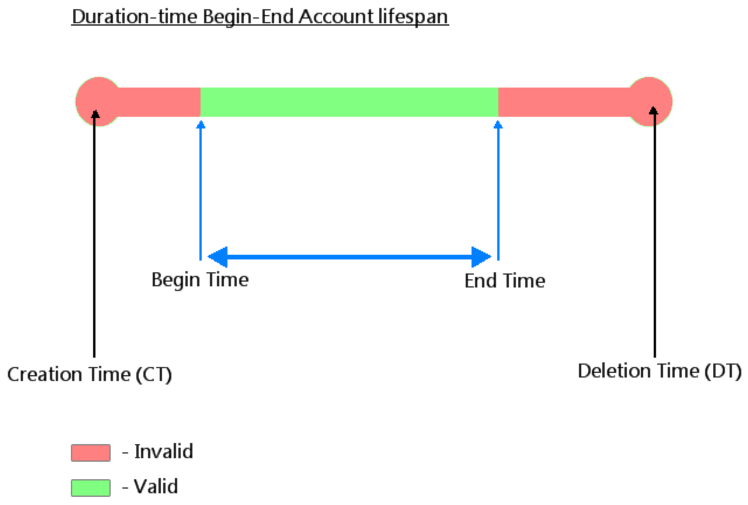
- Users can access internet while account is within valid time interval. Count down begins once account activates and expires when *Expiration Time* is reached.

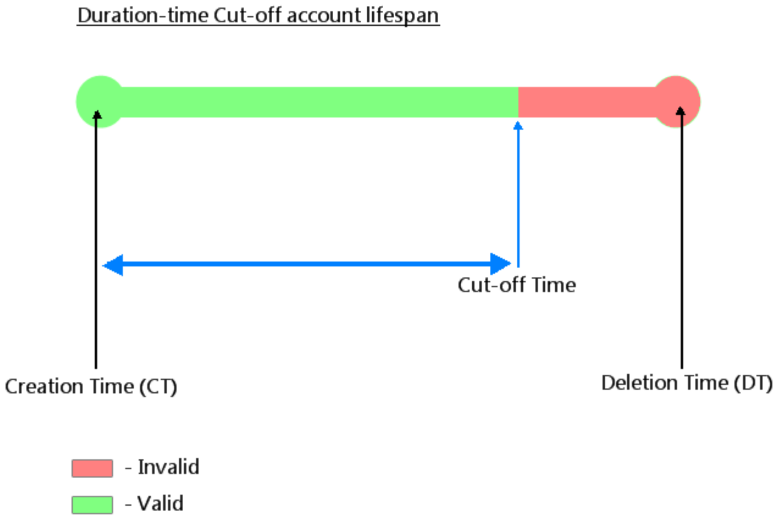
- Duration-time accounts can be further classified into:
  - ☐ **Elapsed Time**
    - Relative to *Activation Time* which is the account creation time. Account expires when the *Expiration Time* has been reached.
  - ☐ **Begin-End Time**
    - Define explicitly the *Begin Time* and *End Time* of the 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.

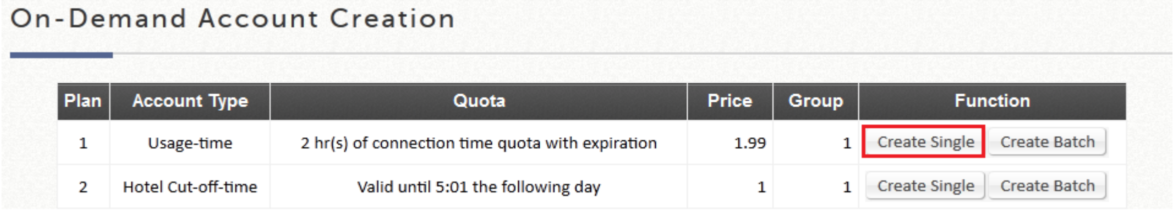

Duration-time Elasped account lifespan
Elapsed Time (ET)
Creation Time (CT)
Deletion Time (DT)
🟥 - Invalid
🟩 - Valid


Duration-time Begin-End Account lifespan
Begin Time
End Time
Creation Time (CT)
Deletion Time (DT)
🟥 - Invalid
🟩 - Valid


Duration-time Cut-off account lifespan
Cut-off Time
Creation Time (CT)
Deletion Time (DT)
🟥 - Invalid
🟩 - Valid

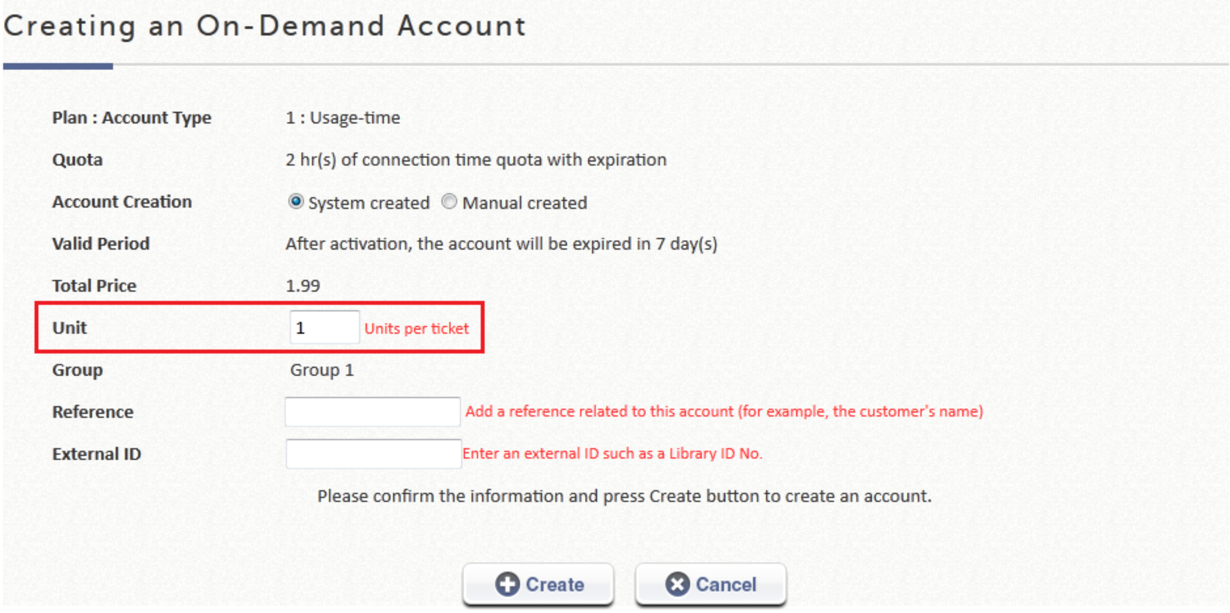
NOTE

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	Create Single Create Batch
2	Hotel Cut-off-time	Valid until 5:01 the following day	1	1	Create Single 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 1 Units per ticket

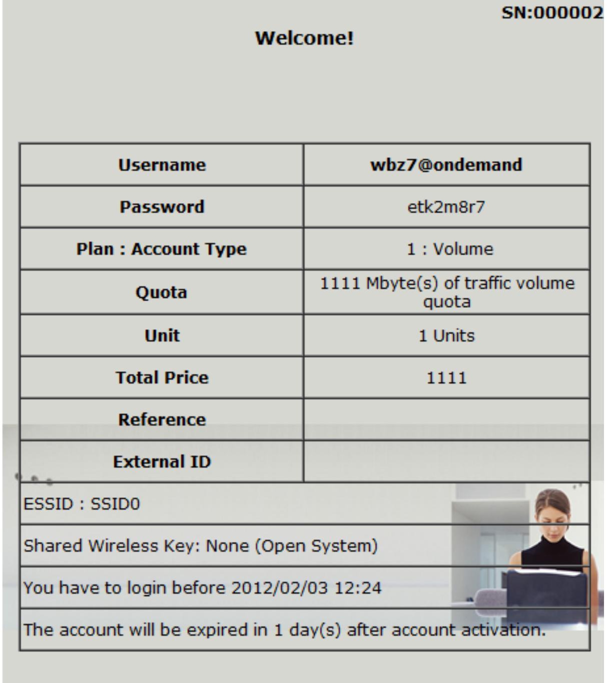
Group Group 1

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:000002

Welcome!

Username	**wbz7@ondemand**
Password	etk2m8r7
Plan : Account Type	1 : Volume
Quota	1111 Mbyte(s) of traffic volume quota
Unit	1 Units
Total Price	1111
Reference	
External ID	

ESSID : SSID0

Shared Wireless Key: None (Open System)

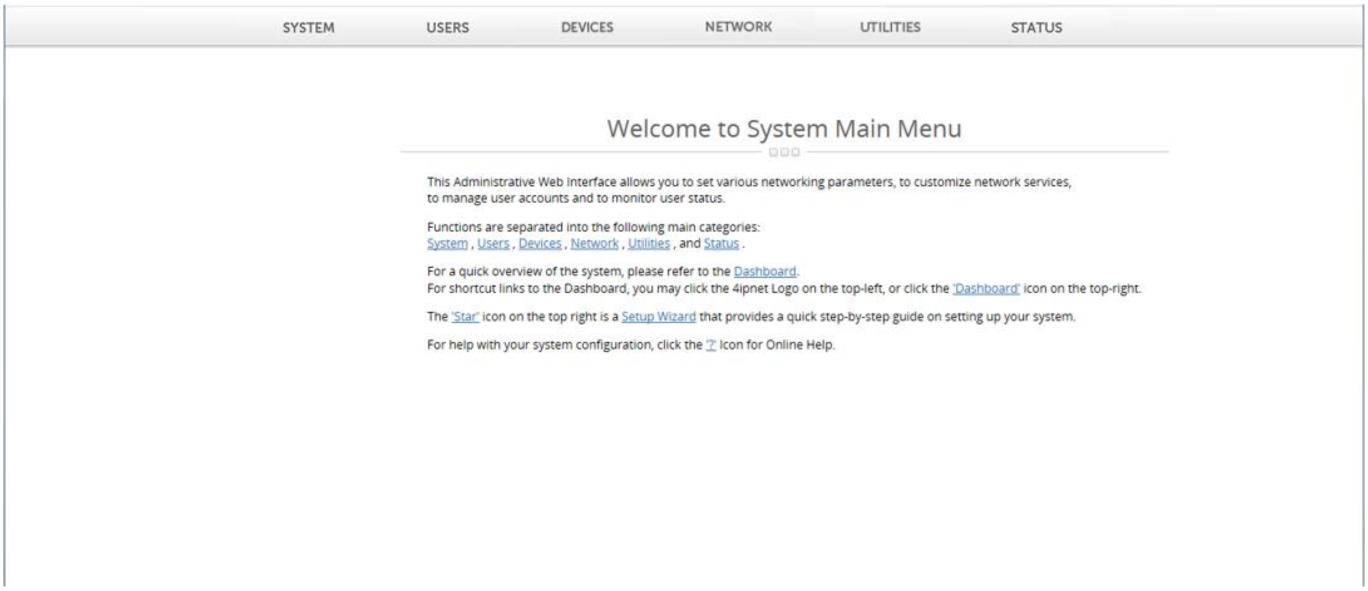
You have to login before 2012/02/03 12:24

The account will be expired in 1 day(s) after account activation.

Appendix D. UI Reference Index

I. Main

Main Menu is the link that leads to all the configuration pages in the Web Management Interface. A screenshot of the main menu is captured below, the iconic button on the top row will redirect to configuration pages relating to its category.


SYSTEM
USERS
DEVICES
NETWORK
UTILITIES
STATUS

Welcome to System Main Menu

This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.

Functions are separated into the following main categories:
System , Users , Devices , Network , Utilities , and Status .

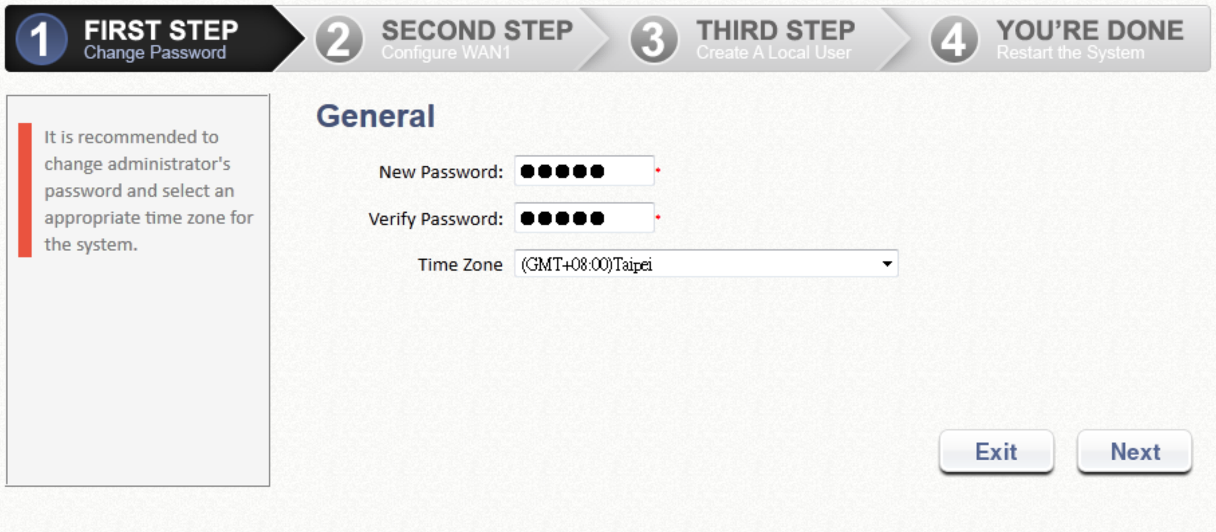
For a quick overview of the system, please refer to the Dashboard.
For shortcut links to the Dashboard, you may click the 4ipnet Logo on the top-left, or click the 'Dashboard' icon on the top-right.

The 'Star' icon on the top right is a Setup Wizard that provides a quick step-by-step guide on setting up your system.

For help with your system configuration, click the '?' Icon for Online Help.

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.


1 FIRST STEP
Change Password
2 SECOND STEP
Configure WAN1
3 THIRD STEP
Create A Local User
4 YOU'RE DONE
Restart the System
Exit
Next

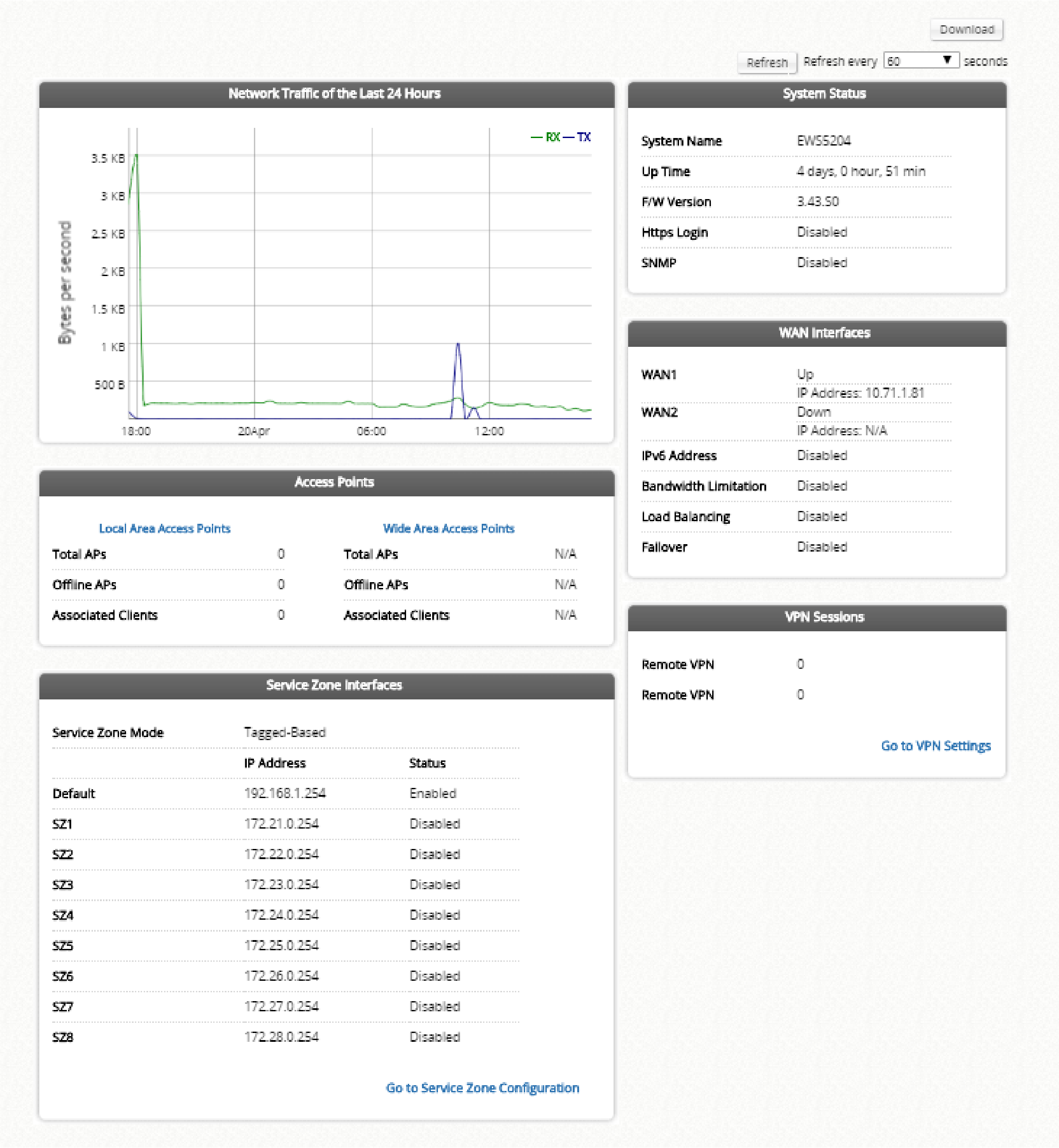
It is recommended to change administrator's password and select an appropriate time zone for the system.

General

New Password: ●●●●●
Verify Password: ●●●●●
Time Zone (GMT+08:00)Taipei

III. 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.


Download
Refresh
Refresh every
60
seconds
Network Traffic of the Last 24 Hours
RX
TX
Bytes per second
3.5 KB
3 KB
2.5 KB
2 KB
1.5 KB
1 KB
500 B
18:00
20Apr
06:00
12:00
Go to VPN Settings
Go to Service Zone Configuration

System Status

System Name	EWS5204
Up Time	4 days, 0 hour, 51 min
F/W Version	3.43.50
Https Login	Disabled
SNMP	Disabled

WAN Interfaces

WAN1	Up IP Address: 10.71.1.81
WAN2	Down IP Address: N/A
IPv6 Address	Disabled
Bandwidth Limitation	Disabled
Load Balancing	Disabled
Failover	Disabled

Access Points

Local Area Access Points		Wide Area Access Points	
Total APs	0	Total APs	N/A
Offline APs	0	Offline APs	N/A
Associated Clients	0	Associated Clients	N/A

VPN Sessions

Remote VPN	0
Remote VPN	0

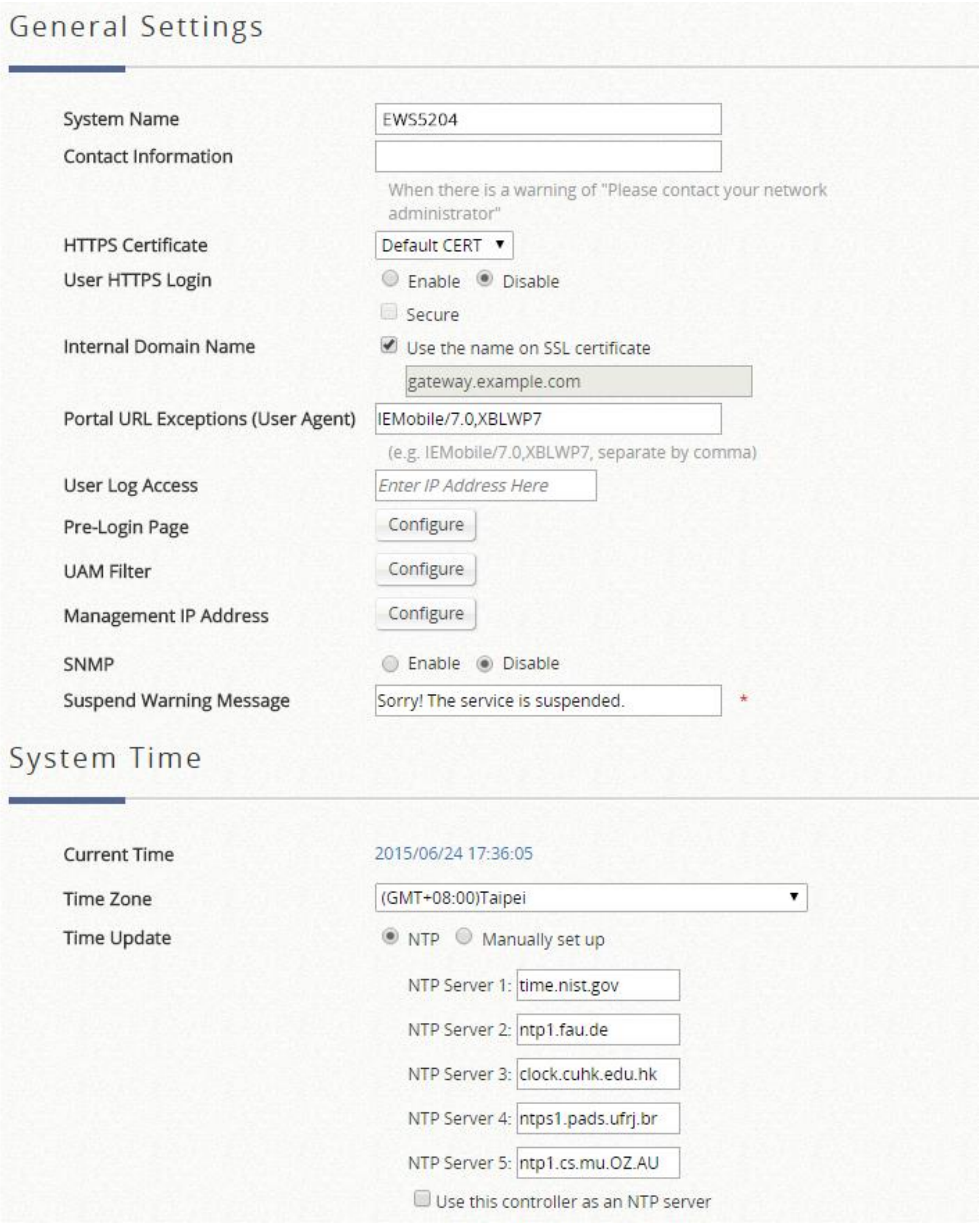
Service Zone Interfaces

Service Zone Mode	Tagged-Based	
	IP Address	Status
Default	192.168.1.254	Enabled
SZ1	172.21.0.254	Disabled
SZ2	172.22.0.254	Disabled
SZ3	172.23.0.254	Disabled
SZ4	172.24.0.254	Disabled
SZ5	172.25.0.254	Disabled
SZ6	172.26.0.254	Disabled
SZ7	172.27.0.254	Disabled
SZ8	172.28.0.254	Disabled

A. System

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

1) General



General Settings

System Name: EWS5204
Contact Information:
When there is a warning of "Please contact your network administrator"
HTTPS Certificate: Default CERT ▼
User HTTPS Login: ○ Enable ● Disable
☐ Secure
Internal Domain Name: ☑ Use the name on SSL certificate
gateway.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*
Pre-Login Page: Configure
UAM Filter: Configure
Management IP Address: Configure
SNMP: ○ Enable ● Disable
Suspend Warning Message: Sorry! The service is suspended. *

System Time

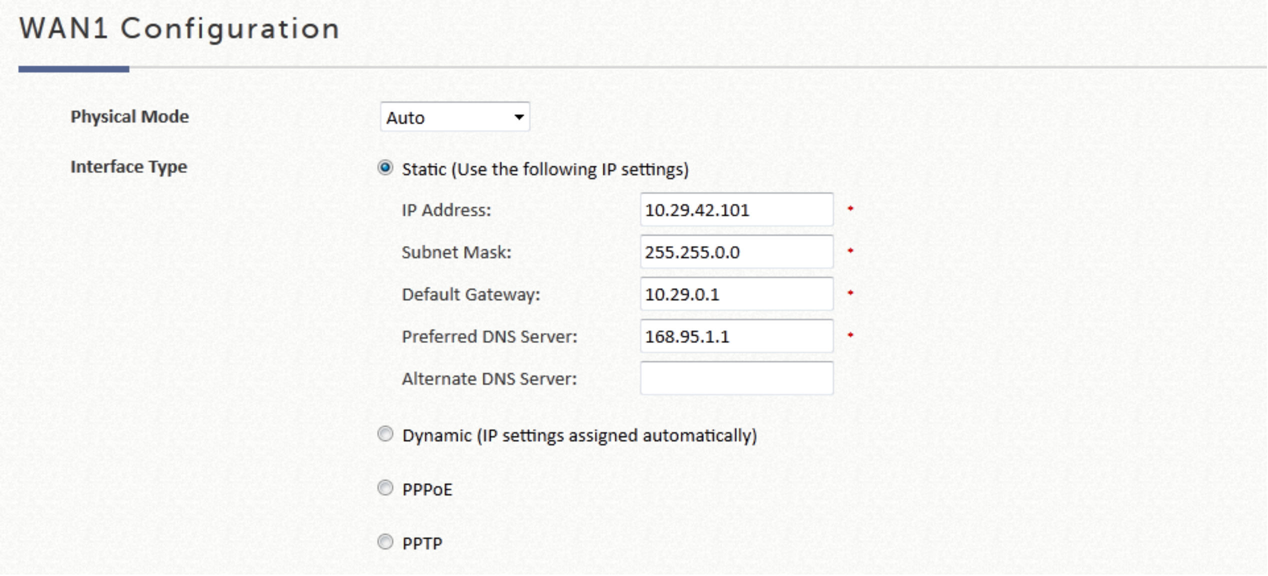
Current Time: 2015/06/24 17:36:05
Time Zone: (GMT+08:00)Taipei ▼
Time Update: ● NTP ○ Manually set up
NTP Server 1: time.nist.gov
NTP Server 2: ntp1.fau.de
NTP Server 3: clock.cuhk.edu.hk
NTP Server 4: ntps1.pads.ufrj.br
NTP Server 5: ntp1.cs.mu.OZ.AU
☐ Use this controller as an NTP server

- **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 uploaded and selected here as site safety verification.
- **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.
- **Internal Domain Name:** A self designated domain name. Ideal for accessing the Controller

instead of remembering the IP address of the LAN interfaces. Certificate’s name may also be used.

- **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:** The reserved IP address of the administrator may be entered here. Once configured, user logs can only be accessed via the entered IP.
- **Pre-Login Page:** A HTML customizable pre-portal page before landing the Login Page.
- **UAM Filter:** The Universal Access Method 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. You may enable remote access from this page. If administrators would like to type a specific IP address, there is not necessary to type the segment.
- **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.

2) WAN



WAN1 Configuration

Physical Mode: Auto

Interface Type:

● Static (Use the following IP settings)

IP Address: 10.29.42.101 *

Subnet Mask: 255.255.0.0 *

Default Gateway: 10.29.0.1 *

Preferred DNS Server: 168.95.1.1 *

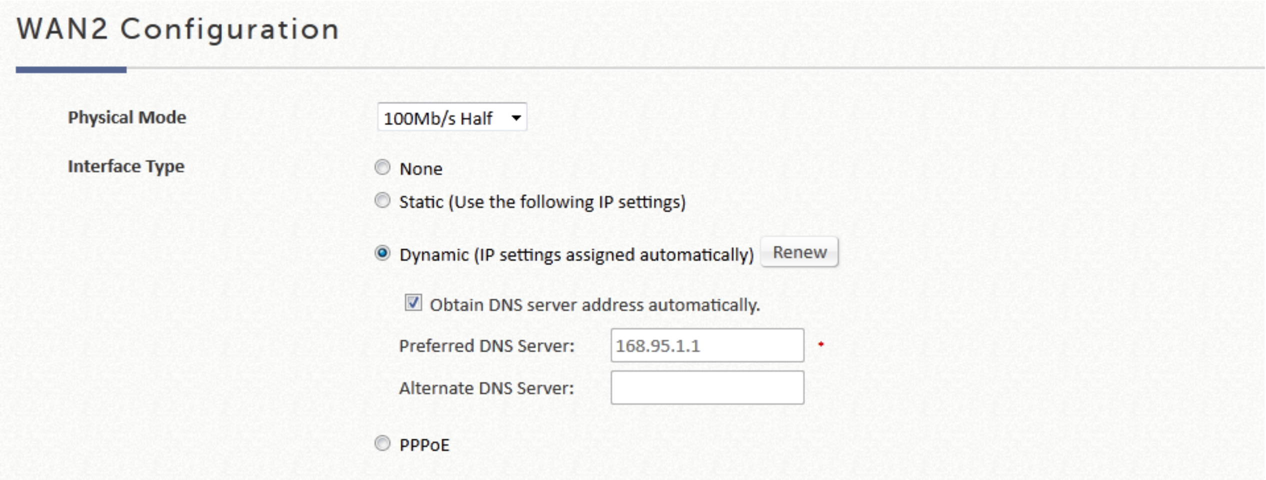
Alternate DNS Server:

○ Dynamic (IP settings assigned automatically)

○ PPPoE

○ PPTP

- **Physical Mode:** Select the mode (Auto/1000Mbps Full/100Mbps Full/100Mbps Half) based on your WAN connection
- **Static:** This option enables the administrator to configure a static IP address on the WAN interface. Applicable if your subscribed internet package comes with a static IP address.
- **Dynamic:** This option enables the WAN interface to be assigned with an IP address automatically by upstream DHCP server.
- **PPPoE:** This is the option of connecting WAN interface to your ISP network via PPP protocol, please select this option if your subscribed network service uses PPP.
- **PPTP:** This is the option of connecting WAN interface to your ISP network via PPP tunneling protocol, please select this option if your subscribed network service uses PPP tunneling.
- **WAN1 Interface Type:** This section enables the selection of actual Port to be deployed as WAN1 servicing port.

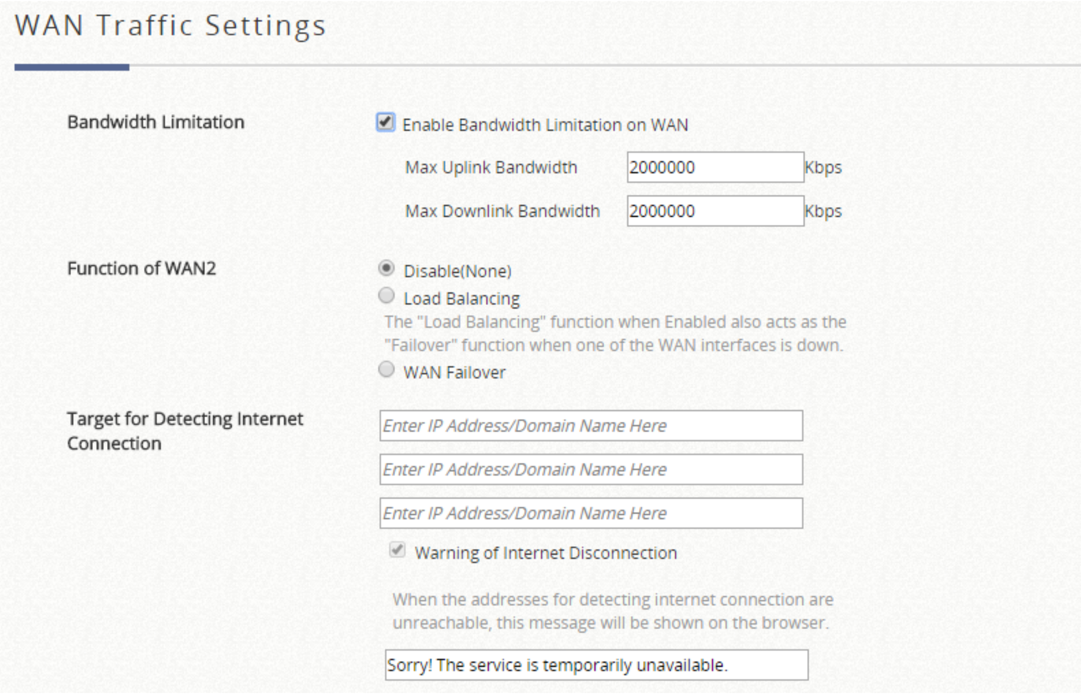


WAN2 Configuration

Physical Mode: 100Mb/s Half

Interface Type:
○ None
○ Static (Use the following IP settings)
● Dynamic (IP settings assigned automatically) Renew
☑ Obtain DNS server address automatically.
Preferred DNS Server: 168.95.1.1 *
Alternate DNS Server:
○ PPPoE

- **Physical Mode**: Select the mode (Auto/1000Mbps Full/100Mbps Full/100Mbps Half) based on your WAN connection
- **None:** Disable the WAN2 interface from providing service.
- **Static:** This option enables the administrator to configure a static IP address on the WAN interface. Applicable if your subscribed internet package comes with a static IP address.
- **Dynamic:** This option enables the WAN interface to be assigned with an IP address automatically by upstream DHCP server.
- **PPPoE:** This is the option of connecting WAN interface to your ISP network via PPP protocol, please select this option if your subscribed network service uses PPP.
- **WAN2 Interface Type:** This section enables the selection of actual Port to be deployed as WAN2 servicing port.



WAN Traffic Settings

Bandwidth Limitation: ☑ Enable Bandwidth Limitation on WAN
Max Uplink Bandwidth: 2000000 Kbps
Max Downlink Bandwidth: 2000000 Kbps

Function of WAN2:
● Disable(None)
○ Load Balancing
The "Load Balancing" function when Enabled also acts as the "Failover" function when one of the WAN interfaces is down.
○ WAN Failover

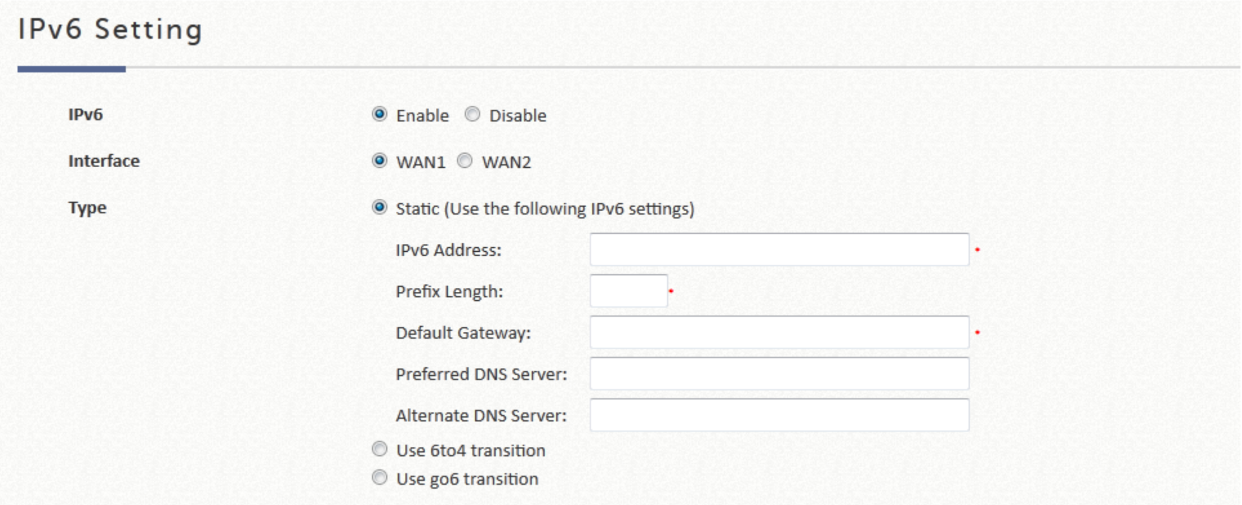
Target for Detecting Internet Connection:
Enter IP Address/Domain Name Here
Enter IP Address/Domain Name Here
Enter IP Address/Domain Name Here
☑ Warning of Internet Disconnection
When the addresses for detecting internet connection are unreachable, this message will be shown on the browser.
Sorry! The service is temporarily unavailable.

- **Available Bandwidth on WAN Interface:** This section of the configuration page allows the administrator to specify uplink and downlink limitations to be enforced on the servicing WAN interface.
- **Function of WAN2:** The WAN2 connection can be activated for Load Balancing or WAN Failover

when WAN2 is enabled.

- **Address for Detecting Internet Connection:** This section of the configuration page enables the administrator to specify external targets to check for uplink status. WAN Failover or WAN Load Balancing may be selected to be enabled along with a customizable disconnection message to the end user.

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:

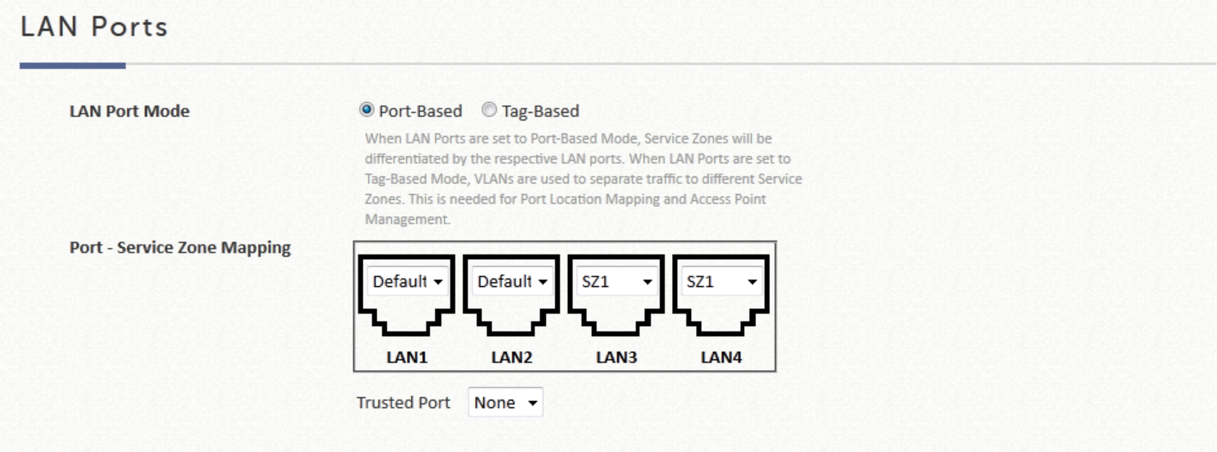
○ Use 6to4 transition

○ 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.
- **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.
- **go6:** go6 is a platform that connects the world to the new Internet with IPv6 products, community and services. You may choose this connection option if you have a registered account.

4) LAN Ports

A "Service Zone" in the system, by default, contains wired and wireless coverage areas in the organization. When "Port-Based" mode is enabled, each physical LAN port can be set individually to map to a specific Service Zone for later use. By contrast, under "Tag-Based" mode, Service Zones will be distinguished by VLAN tagging, instead of physical LAN ports.



LAN Ports

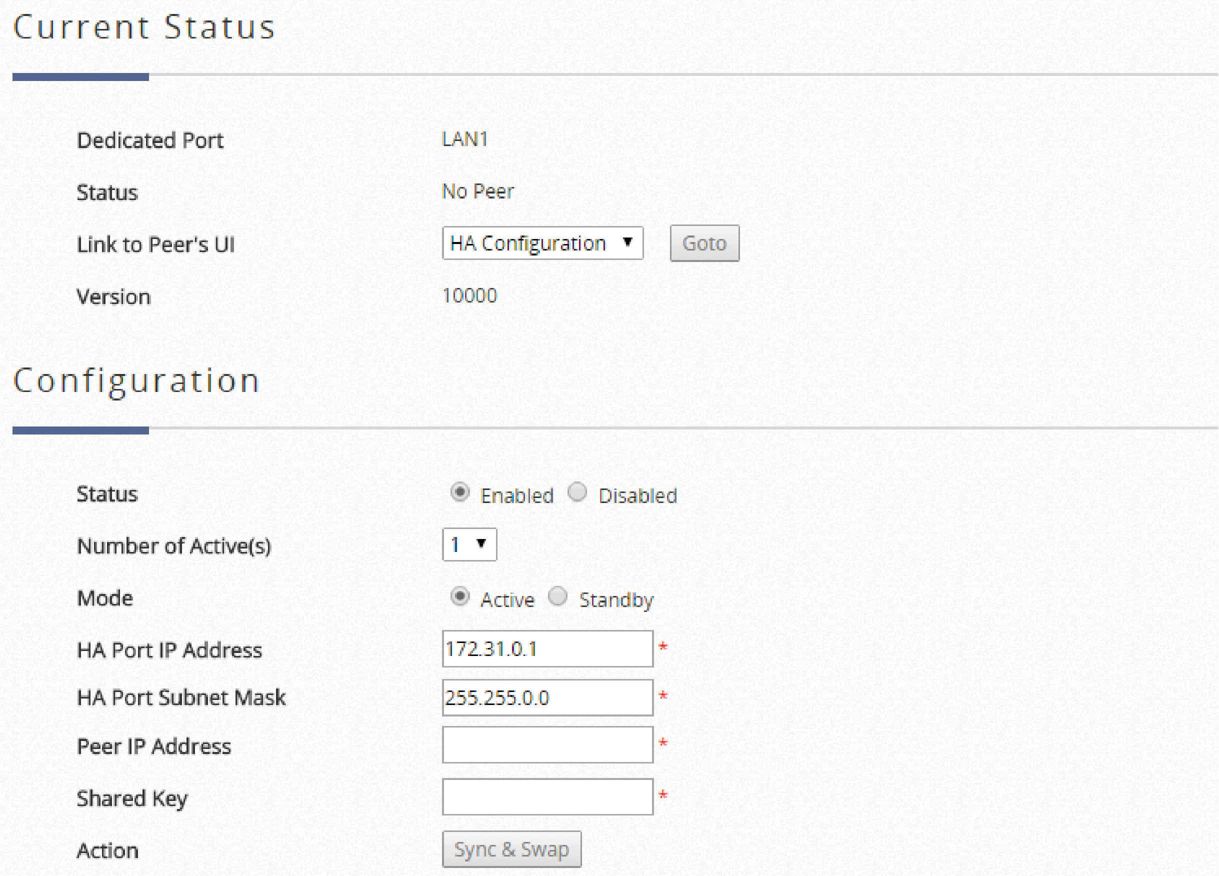
LAN Port Mode: ● Port-Based ○ Tag-Based

When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.

Port - Service Zone Mapping: LAN1 Default, LAN2 Default, LAN3 SZ1, LAN4 SZ1

Trusted Port: None

5) High Availability



Current Status

Dedicated Port: LAN1

Status: No Peer

Link to Peer's UI: HA Configuration

Version: 10000

Configuration

Status: ● Enabled ○ Disabled

Number of Active(s): 1

Mode: ● Active ○ Standby

HA Port IP Address: 172.31.0.1 *

HA Port Subnet Mask: 255.255.0.0 *

Peer IP Address: *

Shared Key: *

Action:

- **Status:** This feature can be turn on or off here.
- **Number of Active(s):** Selecting up to 3 Actives for N+1 HA
- **Mode:** The role of this particular controller must be determined here manually.
- **HA Port IP Address:** The IP address configured for the dedicated HA port. Should make sure that all controller’s HA port IP are under the same subnet.
- **HA Port Subnet Mask:** The subnet mask for HA communication.
- **Peer IP Address:** Fill in the IP address of the peer Controller’s HA port.
- **Shared Key:** Enter a secret string on both of the controller. The Shared Key must be the same for a successful HA connection.
- **Switch Support:** when HA N+1, N=2 or 3, Edgecore SW1024 is highly recommended since the related LAN port and VLAN ID can automatically be modified when HA is happening. If admin would like to set port1, port 4 and port 2 on SW1024 for #1 Active AC with VLAN 101, 41, 42,

respectively, please enter 1,4,2 on #1 Active Related Port(s) and type 101, 41, 42 on #1 Active LAN Port VLAN ID(s).

- **Action:** This function may be triggered on the primary controller, switching service to the secondary controller manually. (available on 1+1 HA only)
- **Dedicated Port:** Currently LAN1 for all Controller models.
- **Status:** Reflects the current status of the HA link.
- **Version:** Shows the HA feature revision.

6) Service Zones

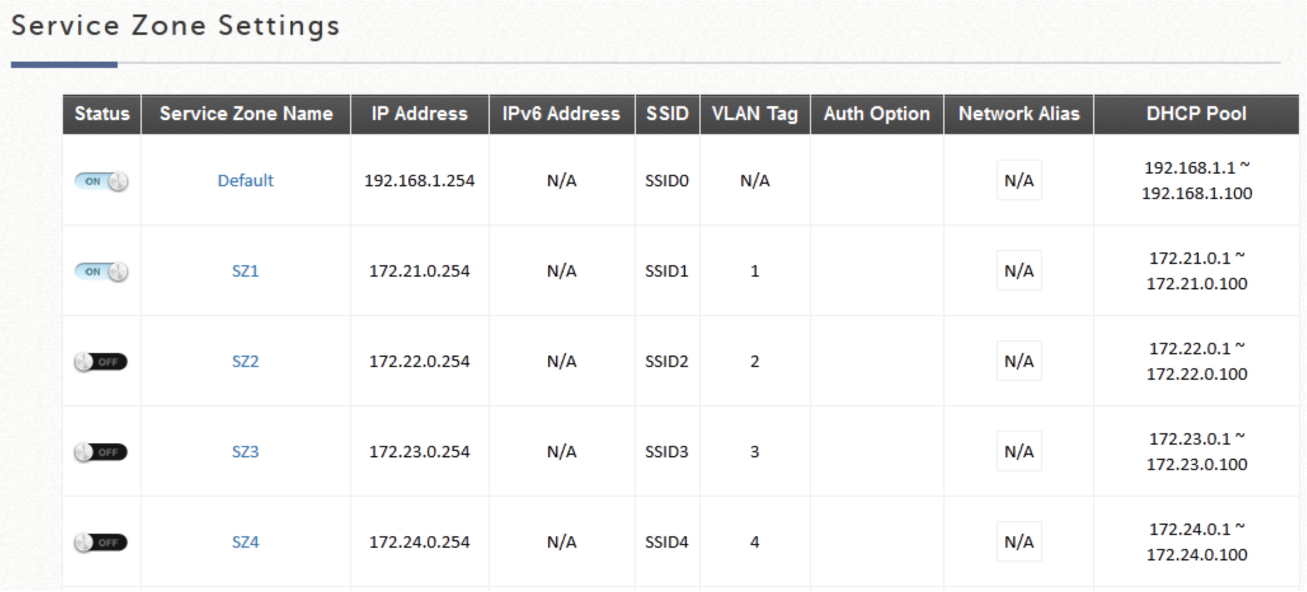
The table will list the Service Zones and related settings.

DHCP Server: The system supports three types of DHCP modes; **Disable Built-in DHCP Server**, **Enable Built-in DHCP server**, and **Enable DHCP relay**. Select **Disable Built-in DHCP Server** to disable the built-in DHCP server when clients are assigned static IP addresses. Select **Enable Built-in DHCP Server** to enable the built-in DHCP server. When the built-in DHCP server is chosen, the system will act as a DHCP server and assign IP addresses to its clients. Select **Enable DHCP Relay** when a service zone is connected to an external DHCP server. When Enable DHCP Relay is chosen, the IP addresses 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.

Assigned IP Address for AP Management: Under port-based service zone, each service zone can designate an IP segment for IP address assignment to the managed AP when the newly discovered AP is added into the service zone. Under tag-based service zone, only default service zone will designate an IP segment for IP address assignment to the managed AP when the newly discovered AP is added into the selected service zones.

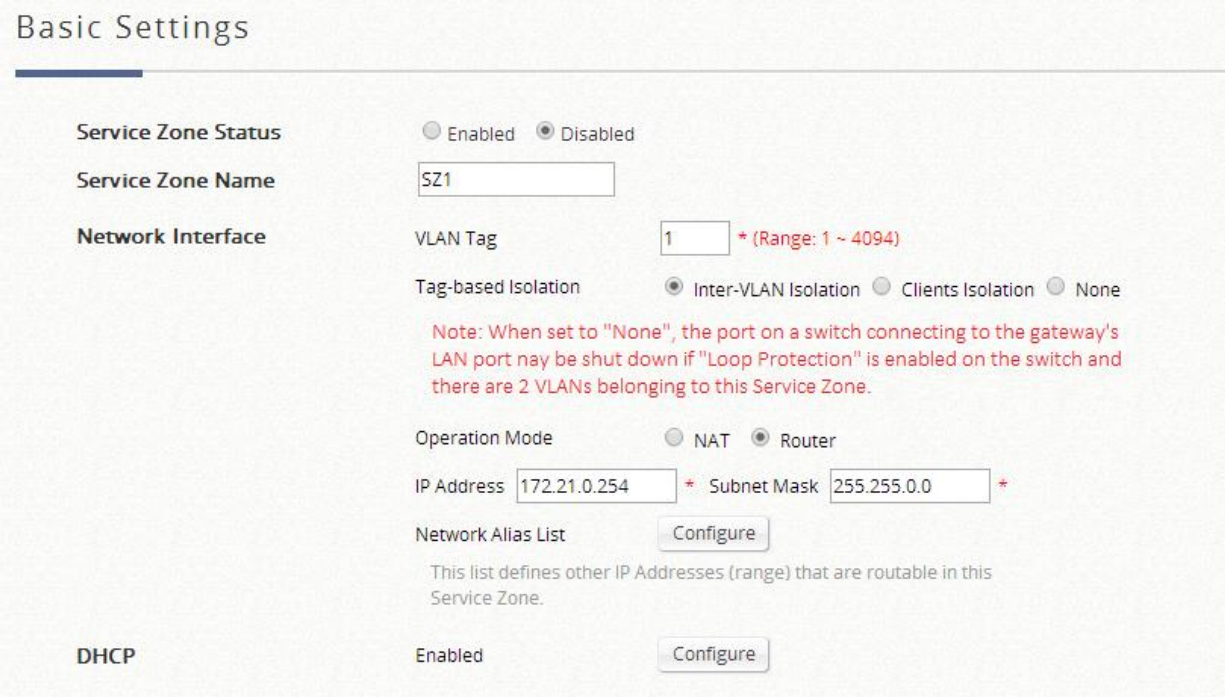
SIP Interface Configuration: The system provides **SIP** proxy that helps SIP clients (devices or soft clients) pass through NAT. After enabling SIP proxy server, all SIP traffic can pass through NAT with a selective but fixed WAN interface.

Authentication Settings: The system supports several authentication databases that are **Local**, **POP3**, **RADIUS**, **LDAP**, and **NT Domain** and provides up to four authentication options and one **On-Demand User** authentication option and one **SIP** authentication option.



Service Zone Settings

Status	Service Zone Name	IP Address	IPv6 Address	SSID	VLAN Tag	Auth Option	Network Alias	DHCP Pool
ON	Default	192.168.1.254	N/A	SSID0	N/A		N/A	192.168.1.1 ~ 192.168.1.100
ON	SZ1	172.21.0.254	N/A	SSID1	1		N/A	172.21.0.1 ~ 172.21.0.100
OFF	SZ2	172.22.0.254	N/A	SSID2	2		N/A	172.22.0.1 ~ 172.22.0.100
OFF	SZ3	172.23.0.254	N/A	SSID3	3		N/A	172.23.0.1 ~ 172.23.0.100
OFF	SZ4	172.24.0.254	N/A	SSID4	4		N/A	172.24.0.1 ~ 172.24.0.100



Basic Settings

Service Zone Status ○ Enabled ● Disabled

Service Zone Name SZ1

Network Interface

VLAN Tag 1 * (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 nay 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

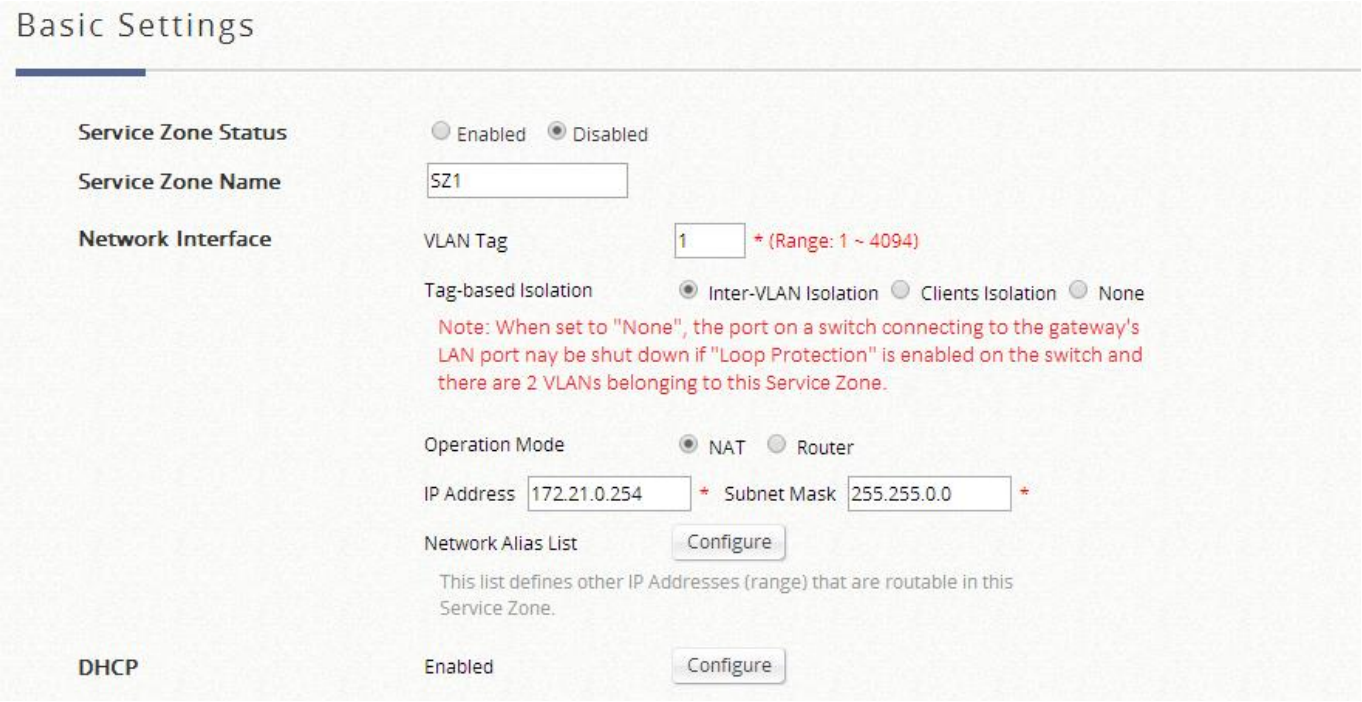
IP Address 172.21.0.254 * Subnet Mask 255.255.0.0 *

Network Alias List Configure

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

DHCP Enabled Configure

Router Mode



Basic Settings

Service Zone Status ○ Enabled ● Disabled

Service Zone Name SZ1

Network Interface

VLAN Tag 1 * (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 nay 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 172.21.0.254 * Subnet Mask 255.255.0.0 *

Network Alias List Configure

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

DHCP Enabled Configure

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 (Tag Base Only):** The VLAN tag number that is mapped to the Service Zone.
    - **Tag-Based LAN Port Isolation:** Administrators can choose different isolation options in each Service Zone when in Tag-based mode. In Port-based mode, administrators have 3 options: Disabled, Authentication Required, and Enable.

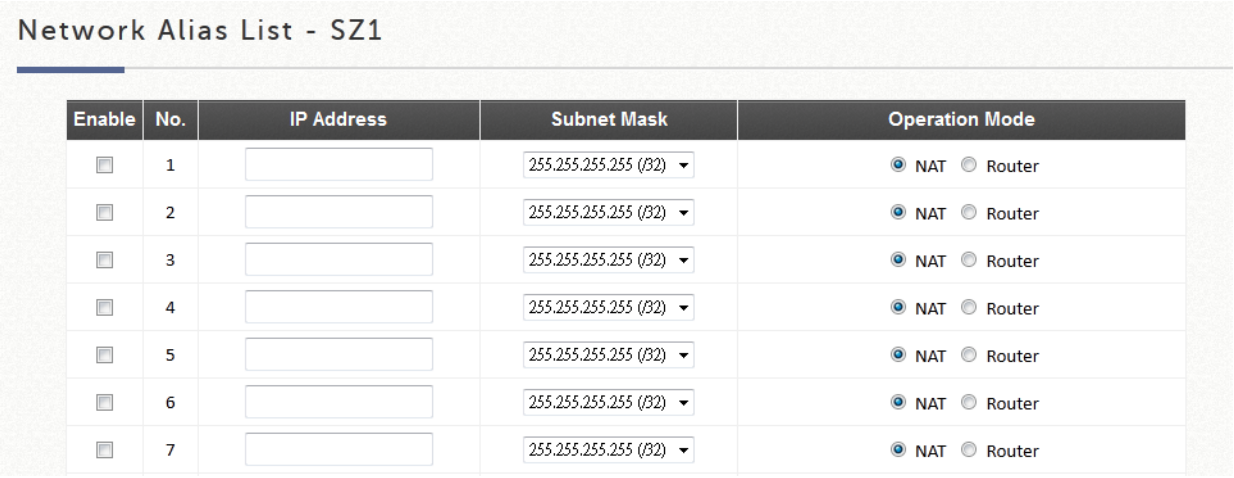
Inter LAN Port Isolation: Select ***Enable*** or ***Disable***. When the option is "Enabled", clients under different LAN ports cannot ping each other. When the option is "Disabled", clients under different LAN ports can ping each other.

Trusted Ports (Port Based): Clients under this port will not require authentication regardless of the corresponding Service Zone settings.

Inter-VLAN Isolation (Tag Based): 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 (Tag Based): When this option is selected, unicast transmission is prevented between any clients in the same Layer 2 subnet.

- **Operation Mode:** Contain **NAT** mode and **Router** mode. When NAT mode is chosen, service zone runs in NAT mode. When Router mode is chosen this service zone runs in Router mode.
- **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 (When IPv6 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.

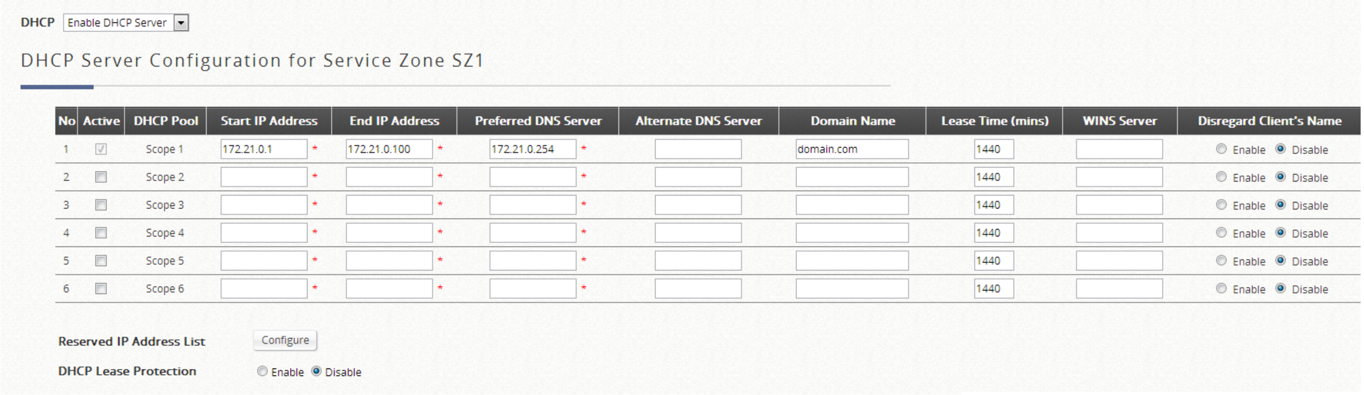


Network Alias List - SZ1

Enable	No.	IP Address	Subnet Mask	Operation Mode
☐	1		255.255.255.255 (/32)	● NAT ○ Router
☐	2		255.255.255.255 (/32)	● NAT ○ Router
☐	3		255.255.255.255 (/32)	● NAT ○ Router
☐	4		255.255.255.255 (/32)	● NAT ○ Router
☐	5		255.255.255.255 (/32)	● NAT ○ Router
☐	6		255.255.255.255 (/32)	● NAT ○ Router
☐	7		255.255.255.255 (/32)	● NAT ○ 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	☑	Scope 1	172.21.0.1 *	172.21.0.100 *	172.21.0.254 *		domain.com	1440		○ Enable ● Disable
2	☐	Scope 2	*	*	*			1440		○ Enable ● Disable
3	☐	Scope 3	*	*	*			1440		○ Enable ● Disable
4	☐	Scope 4	*	*	*			1440		○ Enable ● Disable
5	☐	Scope 5	*	*	*			1440		○ Enable ● Disable
6	☐	Scope 6	*	*	*			1440		○ Enable ● Disable

Reserved IP Address List: Configure

DHCP Lease Protection: ○ Enable ● Disable

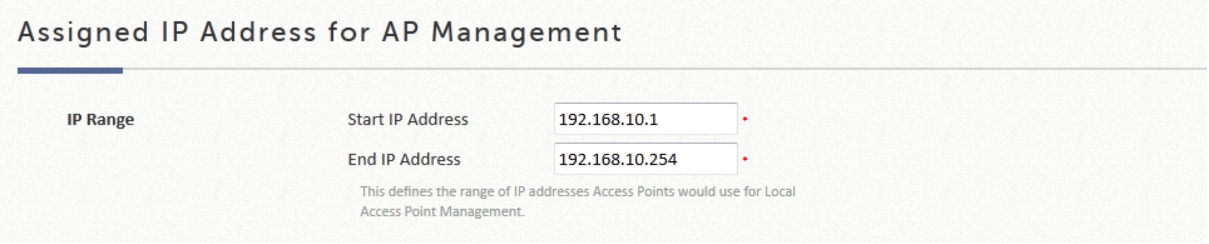
Item	Description
DHCP Server Scope 1	
Start IP Address / End IP Address	A range of IP addresses that are built in DHCP server will be assigned to clients. Note: please change the Management IP Address List accordingly (at *System Configuration >> System Information >> Management IP Address List*) to 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.
DHCP Server Scope 2	
Enable/Disable	When Enabled, an additional DHCP server can be configured to assign IP address to clients associated to the alias IP of this Service Zone. The configurable fields are the same as DHCP Server Scope 1.

Reserved IP Address List: Each service zone can reserve specific IP addresses from predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. Click the **Configure** button to edit the Reserved IP List.

The administrator can reserve a list of specific IP addresses for special device with certain MAC address. Fill a set of IP address and MAC address as reserve, additional information can be entered in the Description field. Click ***Apply*** to activate your settings.

DHCP Lease Protection: When "Enabled", whenever the Service Zone's built-in DHCP server receives a DHCP request, it will automatically bind the MAC address with an IP address permanently. This means that once all the IP addresses have been assigned, it will be bound with the MAC address that first acquired this IP. Subsequent devices with new MAC address will be unable to acquire an IP address. When "Disabled" DHCP server will operate as usual, assigning available IP addresses upon DHCP request.

- **Assigned IP Address for AP Management (Default Zone):** When LAN ports are in Port-Based Mode, each Service Zone can designate an IP segment for IP address assignment to the managed AP when the newly discovered AP is added into the service zone. When LAN ports are in Tagged-Based mode, only the Default Service Zone will designate an IP segment for IP address assignment to the managed AP when the newly discovered AP is added into the selected Service Zones.



Assigned IP Address for AP Management

IP Range

Start IP Address: 192.168.10.1

End IP Address: 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, FREE, SIP, LDAP, NT Domain, and POP3. All authentication option can be enabled and applied concurrently. This is to be emphasized in the next section “Users”.

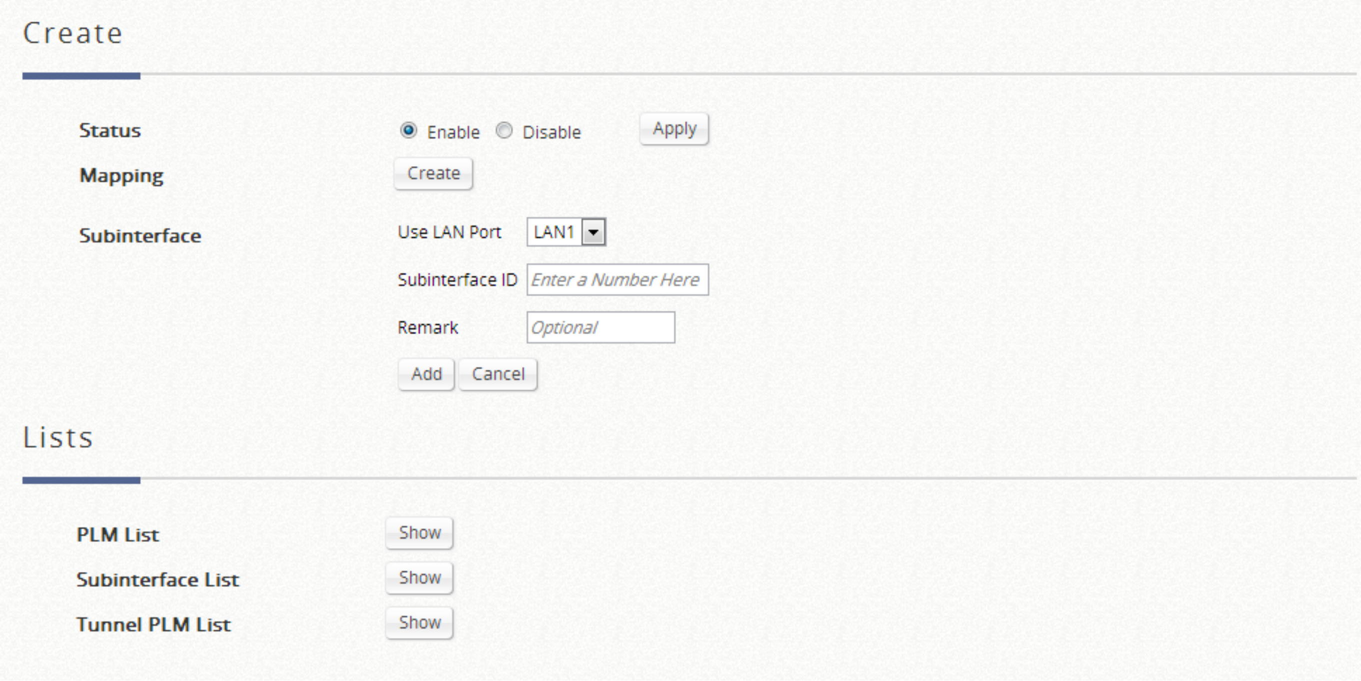
- **Page Customization:** Each Service Zone can be configured to have unique Login Pages or Message Pages. There are 3 types of Login Pages: The General Login Page, Port Location Mapping Login Page (Free Access), and Port Location Mapping Login Page (Paid Access). These pages are fully customizable to 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, Logout Page, Logout Succeeded Page, and Logout Fail Page.

- **Managed AP(s):** APs 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.

7) Port Location Mapping

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 least one or more On-Demand Billing Plans are created, allowing the user to choose a desired plan to pay for their internet access.


Create

Status ● Enable ○ Disable Apply

Mapping Create

Subinterface Use LAN Port LAN1

Subinterface ID Enter a Number Here

Remark Optional

Add Cancel

Lists

PLM List Show

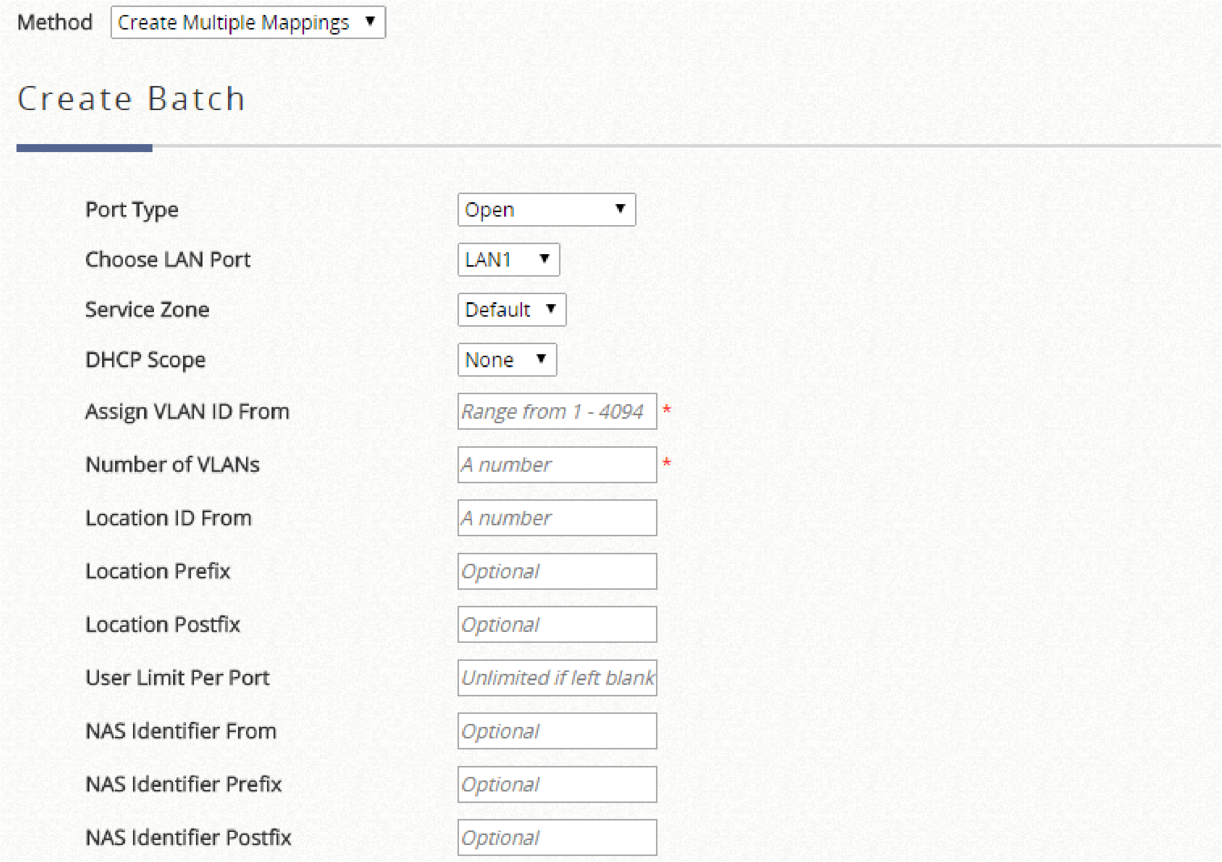
Subinterface List Show

Tunnel PLM List Show

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**.

- **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. 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.

➢ Port Location Mapping Setup – Create Batch



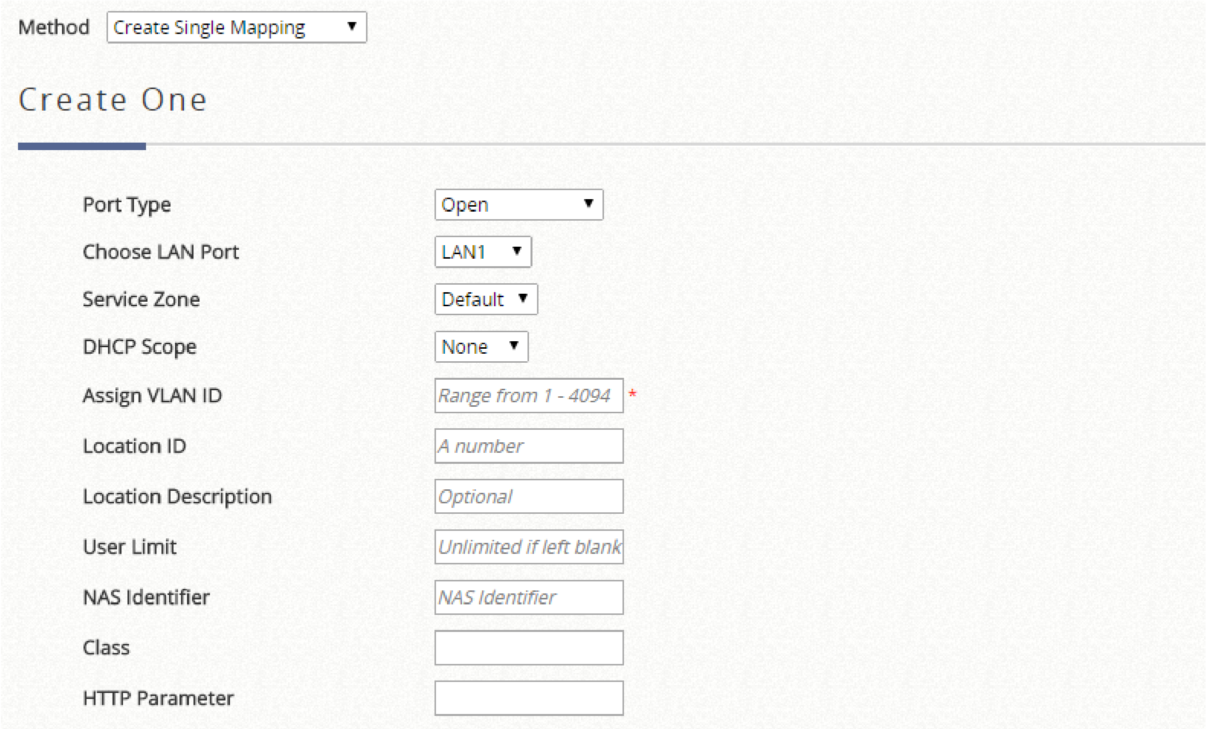
Method: Create Multiple Mappings

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

➢ **Port Location Mapping Setup – Create One**



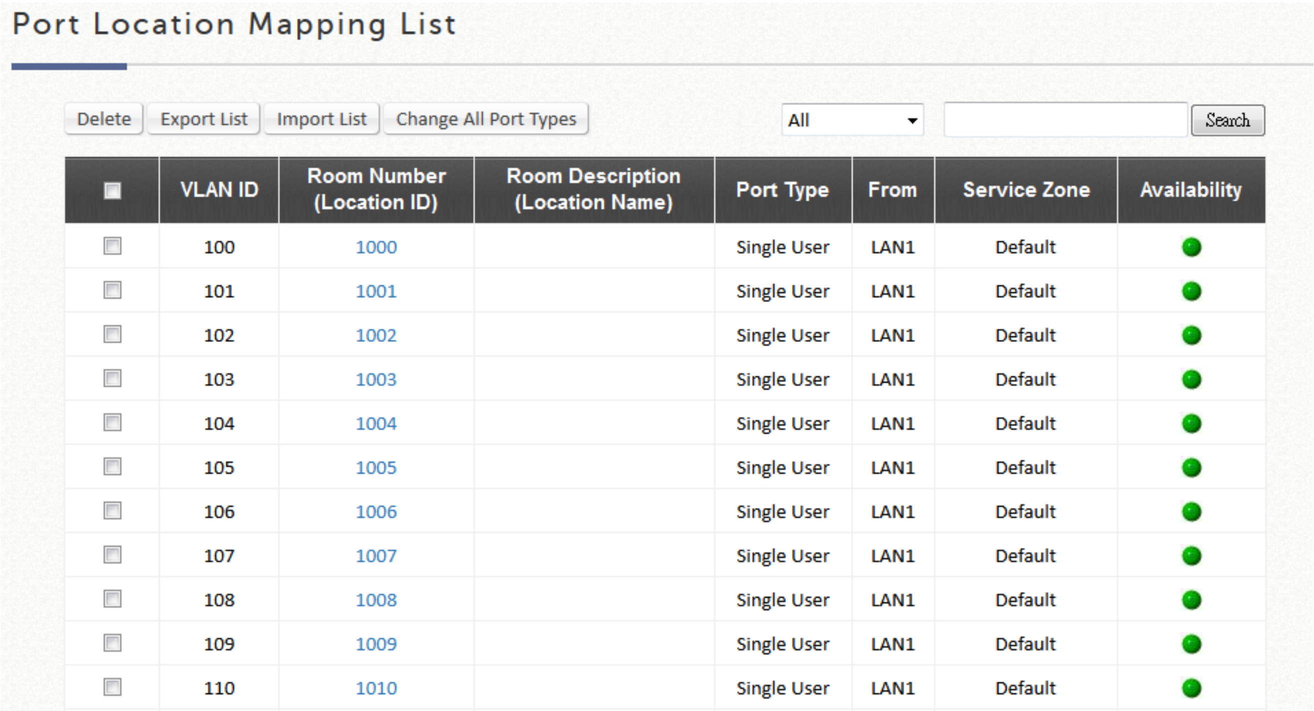
Method: Create Single Mapping

Create One

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 Scope to use from corresponding Service Zone.
- **Assign VLAN ID:** The starting VLAN ID.
- **Location ID:** A numeric identification number (or typically the room number).
- **Location Description:** Optional description for reference.
- **User Limit:** Maximum number of users in batch on corresponding port
- **NAS Identifier:** An optional parameter for RADIUS attribute.
- **Class:** An optional parameter for RADIUS attribute.
- **HTTP Parameter:** Used only when an External Login Page is configured and additional HTTP parameters are required.

➢ **Port Location Mapping List**

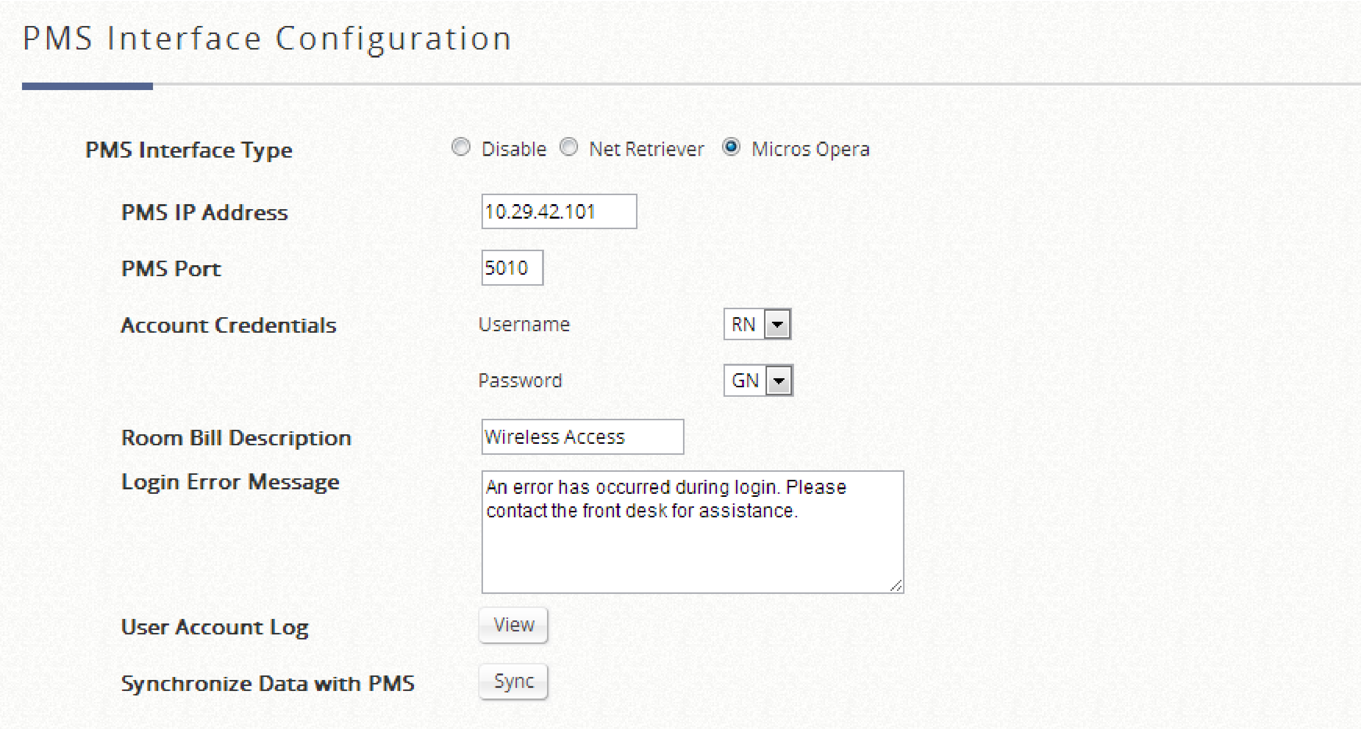


☐	VLAN ID	Room Number (Location ID)	Room Description (Location Name)	Port Type	From	Service Zone	Availability
☐	100	1000		Single User	LAN1	Default	●
☐	101	1001		Single User	LAN1	Default	●
☐	102	1002		Single User	LAN1	Default	●
☐	103	1003		Single User	LAN1	Default	●
☐	104	1004		Single User	LAN1	Default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

- **Import/Export List:** For backing up and restoring the Port Location Mapping List
- **Change All Port Type:** To configure Port Type for all rooms: Free, Block, Single User, Multiple User.

8) Middleware

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



PMS Interface Type: ○ Disable ○ Net Retriever ● Micros Opera
PMS IP Address: 10.29.42.101
PMS Port: 5010
Account Credentials: Username RN; Password GN
Room Bill Description: Wireless Access
Login Error Message: An error has occurred during login. Please contact the front desk for assistance.
User Account Log
Synchronize Data with PMS

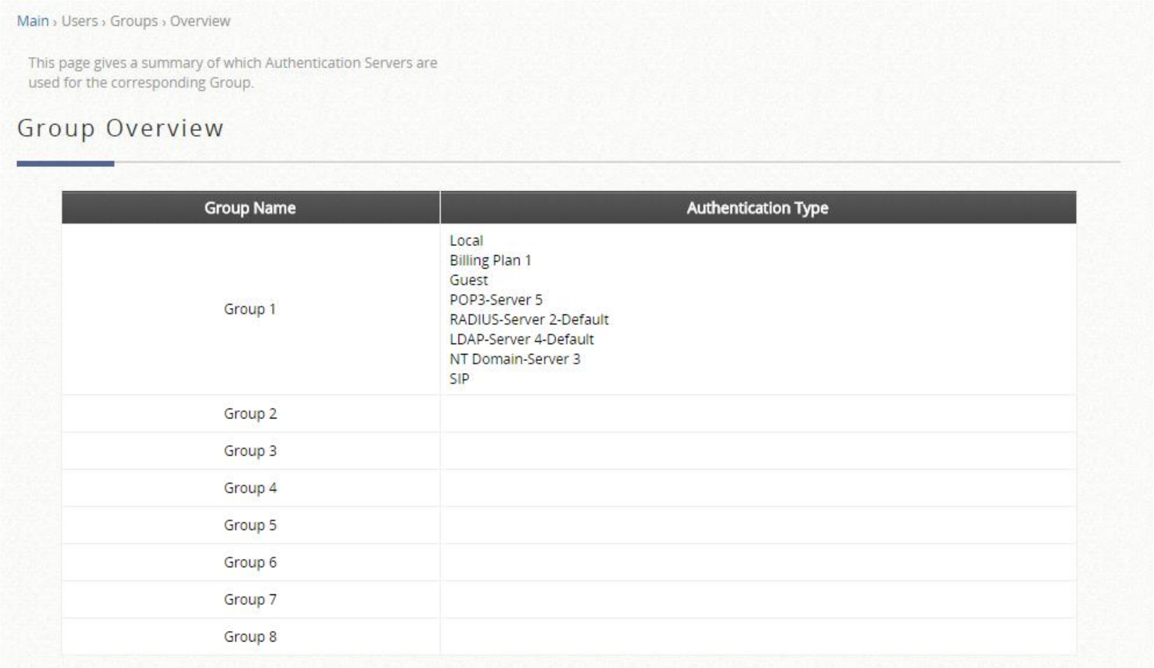
- **Micros Opera Setup:** Enter the PMS IP and PMS Port for Middleware connection.
- **PMS IP:** Enter the IP used by the Micros Fidelio PMS.
- **PMS Port:** Enter the Port used by the Micros Fidelio PMS.
- **Account Credentials:** Administrators may define User Account credentials using a combination of RN (Room number), GN (Guest Name), G# (Guest Number) or G+ (Profile Name) to designate the Micros protocol parameter for carrying the username and password information.
- **Room Bill Description:** The entered description will appear on Room Bills via PMS integration.
- **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.

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.



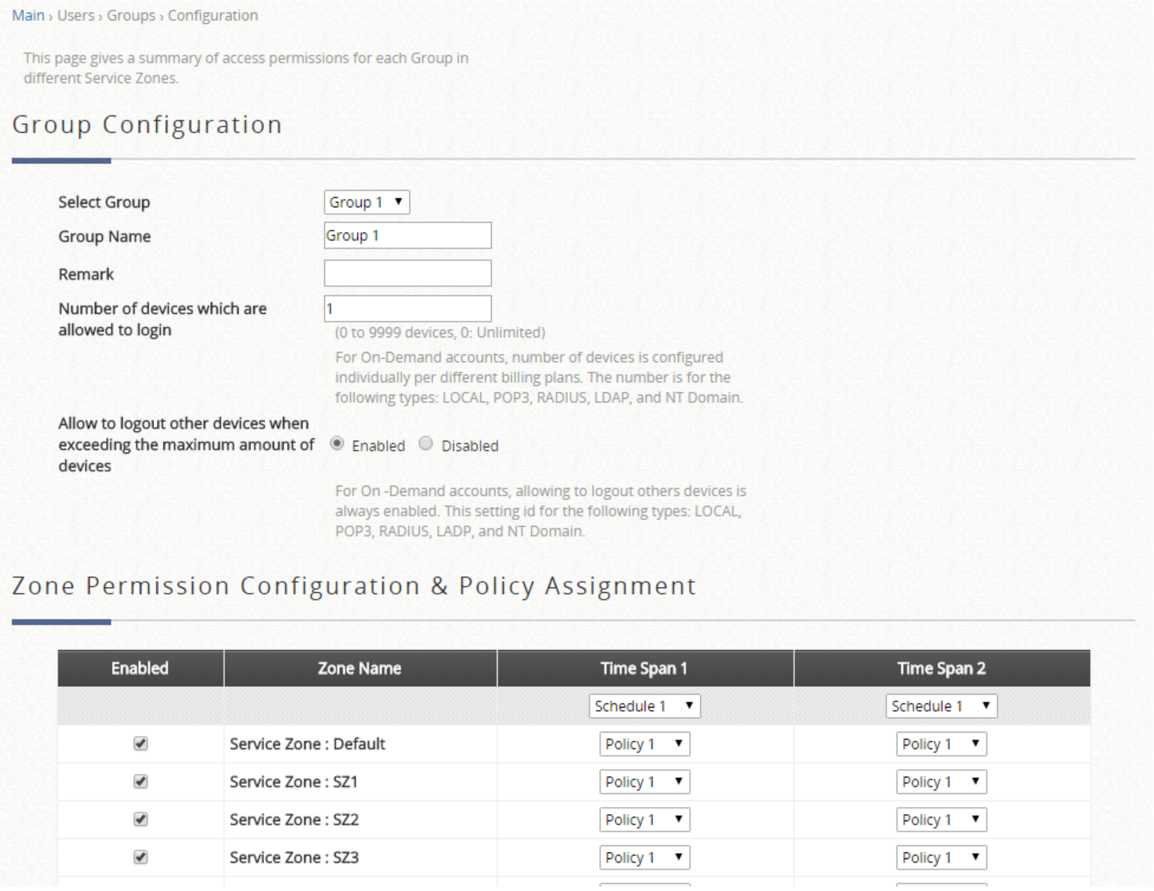
Main › Users › Groups › Overview

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 Guest 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.



Main › Users › Groups › Configuration

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

Group Configuration

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

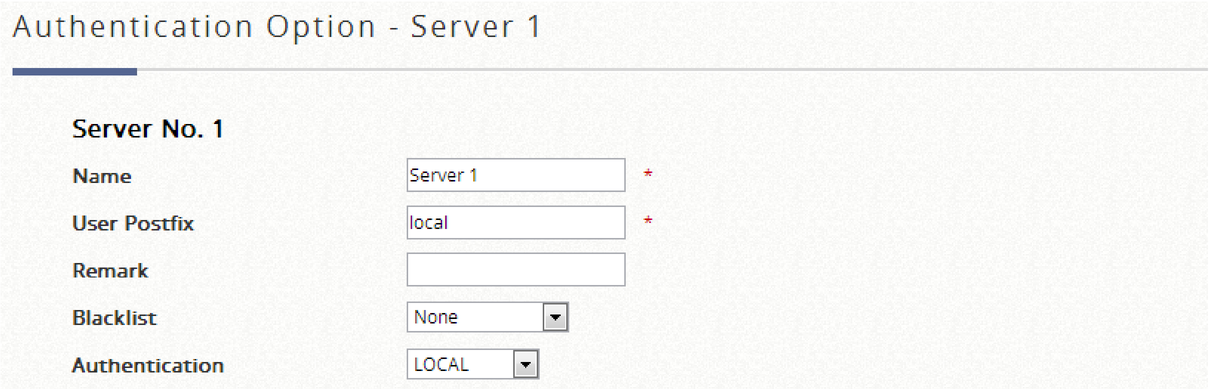
Zone Permission Configuration & Policy Assignment

Enabled	Zone Name	Time Span 1	Time Span 2
		Schedule 1 ▼	Schedule 1 ▼
☑	Service Zone : Default	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ1	Policy 1 ▼	Policy 1 ▼
☑	Service Zone : SZ2	Policy 1 ▼	Policy 1 ▼
☑	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”.

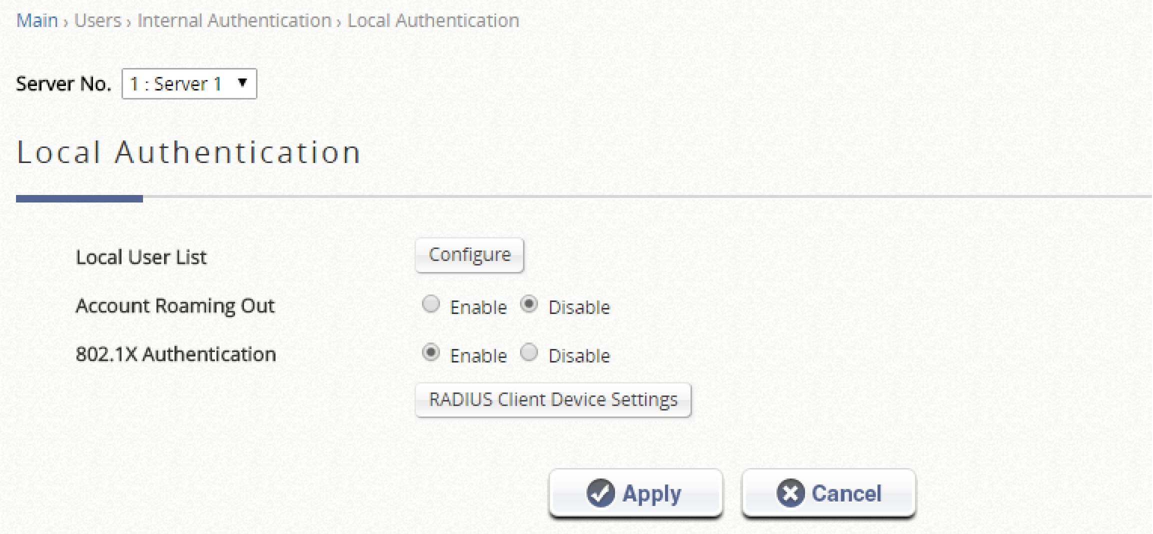


Authentication Option - Server 1

Server No. 1

Name	Server 1 *
User Postfix	local *
Remark	
Blacklist	None ▼
Authentication	LOCAL ▼

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.



Main › Users › Internal Authentication › Local Authentication

Server No. 1 : Server 1

Local Authentication

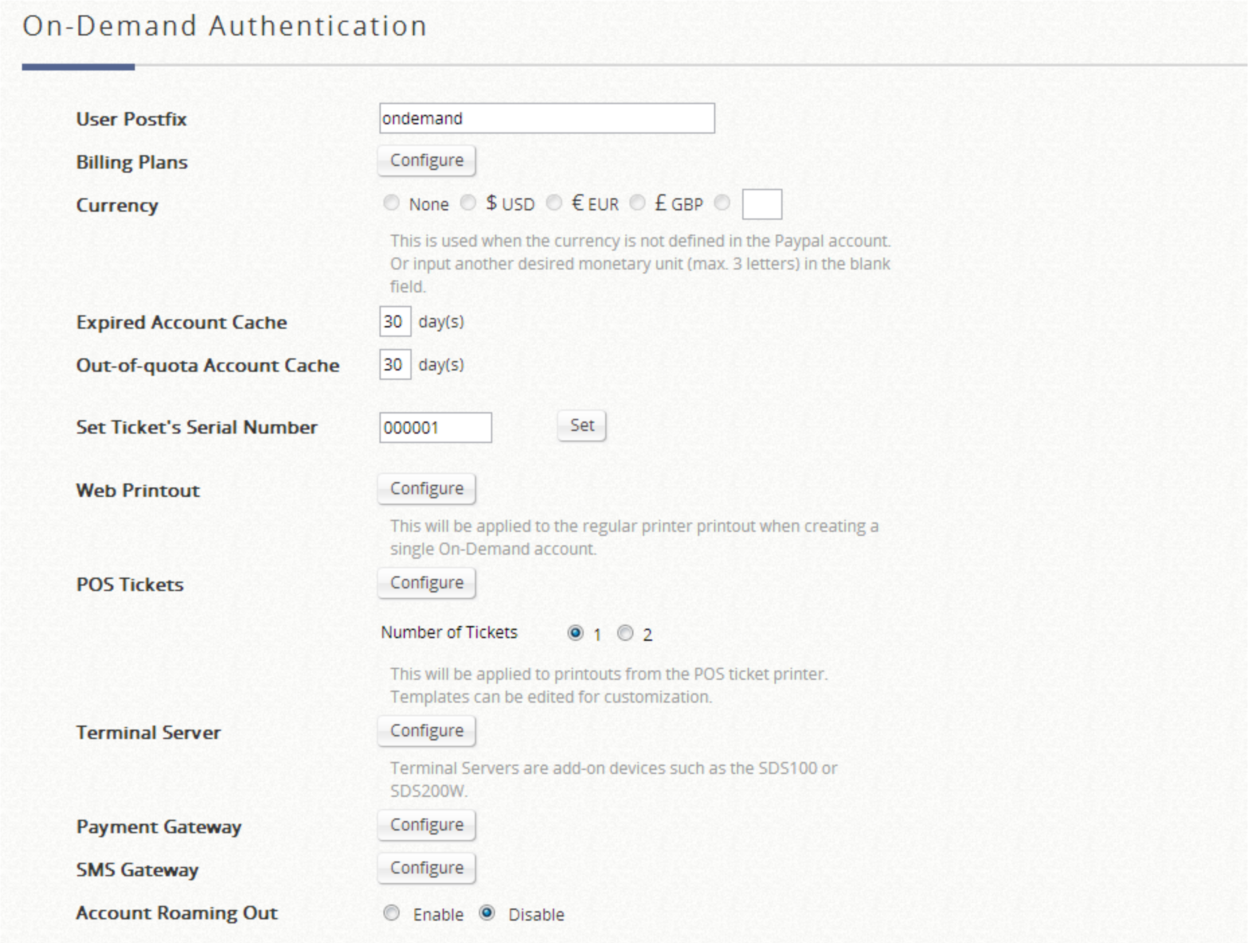
Local User List: Configure

Account Roaming Out: ○ Enable ● Disable

802.1X Authentication: ● Enable ○ Disable

RADIUS Client Device Settings

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: ondemand

Billing Plans: Configure

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

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

Expired Account Cache: 30 day(s)

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

Set Ticket's Serial Number: 000001 Set

Web Printout: Configure

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

POS Tickets: Configure

Number of Tickets ● 1 ○ 2

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

Terminal Server: Configure

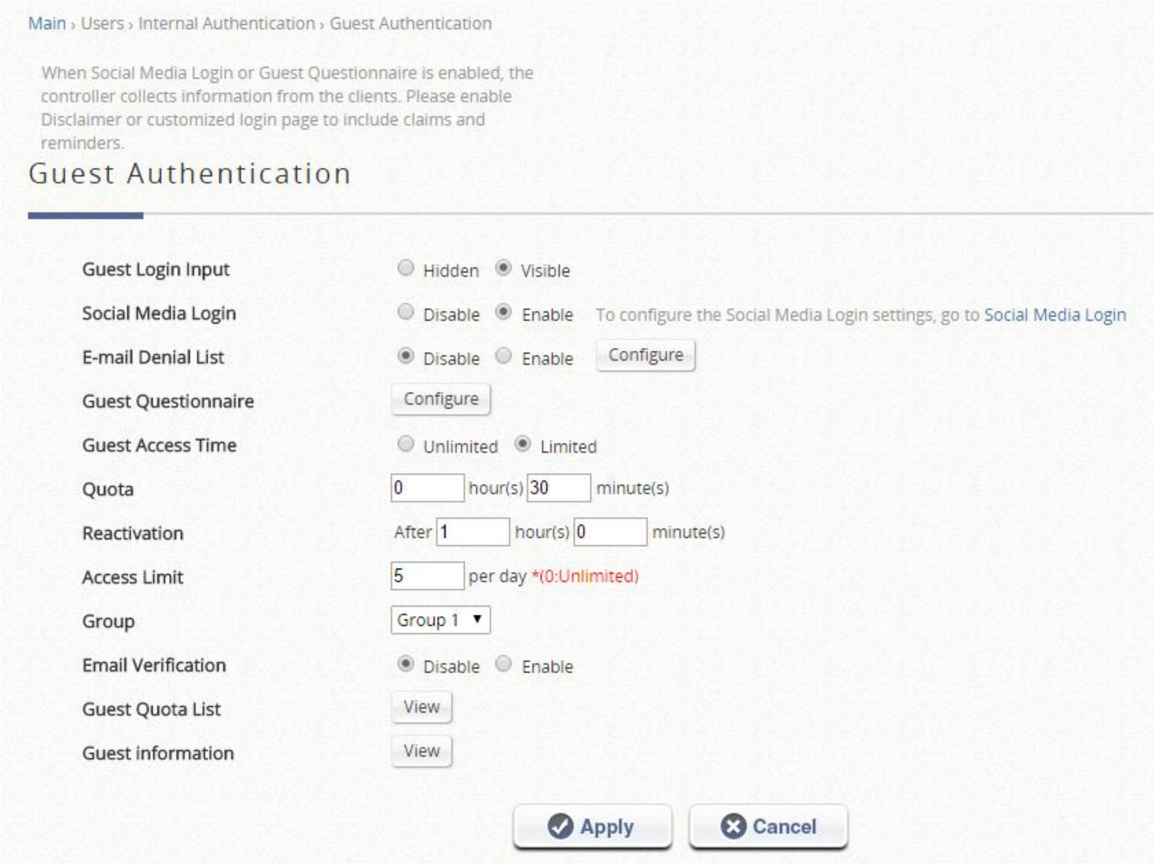
Terminal Servers are add-on devices such as the SDS100 or SDS200W.

Payment Gateway: Configure

SMS Gateway: Configure

Account Roaming Out: ○ Enable ● Disable

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 accounts can have limited or limited access time, and guest users can be bound to a User Group to apply Policies.



Main › Users › Internal Authentication › Guest Authentication

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

Guest Authentication

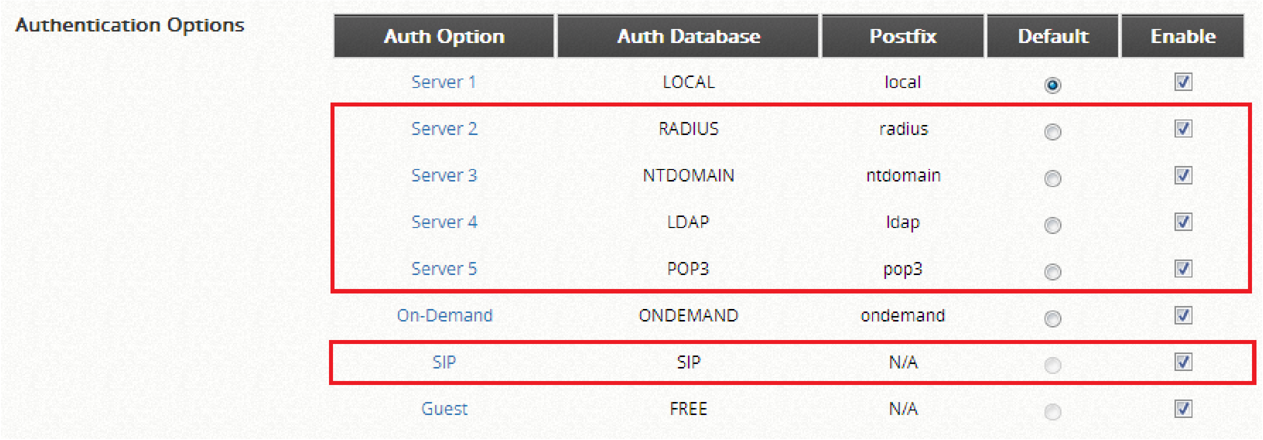
Guest Login Input	○ Hidden ● Visible
Social Media Login	○ Disable ● Enable To configure the Social Media Login settings, go to Social Media Login
E-mail Denial List	● Disable ○ Enable Configure
Guest Questionnaire	Configure
Guest Access Time	○ Unlimited ● Limited
Quota	0 hour(s) 30 minute(s)
Reactivation	After 1 hour(s) 0 minute(s)
Access Limit	5 per day *(0:Unlimited)
Group	Group 1 ▼
Email Verification	● Disable ○ Enable
Guest Quota List	View
Guest information	View

By enabling the “Email Denial List”, some guest email addresses which are disclaimed by certain email domain names would be blocked from internet access. By enabling “Email Verification”, limited free access is provided when an activation link sent by email is clicked by the user.

By enabling “ Social Media Login” and entering the Social Media ID and secret registered from Social Media Sites, guest users could directly login with their already own social media accounts. Selected guest information would be collected from Social Media sites and displayed in Guest Information page.

3) External Authentication

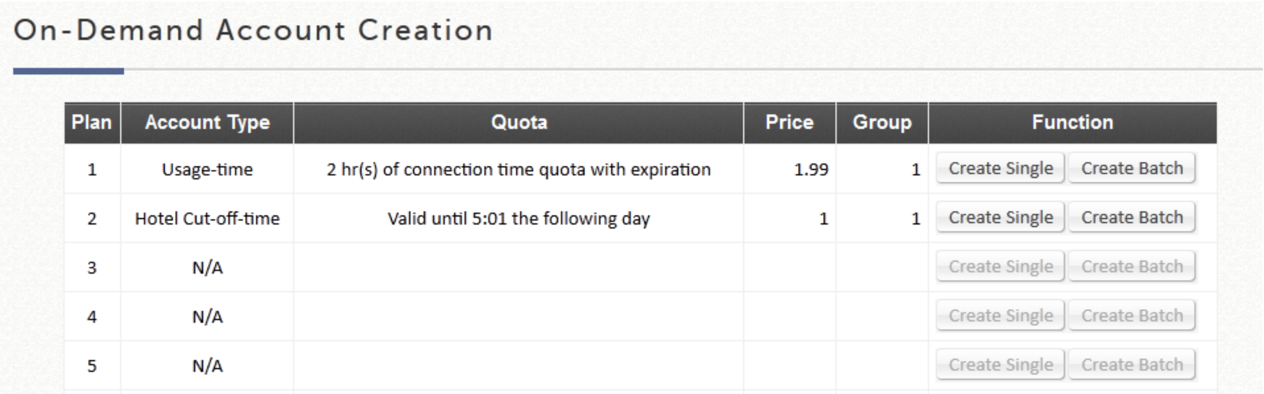
Up to 5 External Authentication servers can be set up and enabled concurrently to facilitate existing user account databases on your network. External Authentication options include RADIUS, POP3, LDAP, NT Domain, and SIP.



Authentication Options

Auth Option	Auth Database	Postfix	Default	Enable
Server 1	LOCAL	local	●	☑
Server 2	RADIUS	radius	○	☑
Server 3	NTDOMAIN	ntdomain	○	☑
Server 4	LDAP	ldap	○	☑
Server 5	POP3	pop3	○	☑
On-Demand	ONDEMAND	ondemand	○	☑
SIP	SIP	N/A	○	☑
Guest	FREE	N/A	○	☑

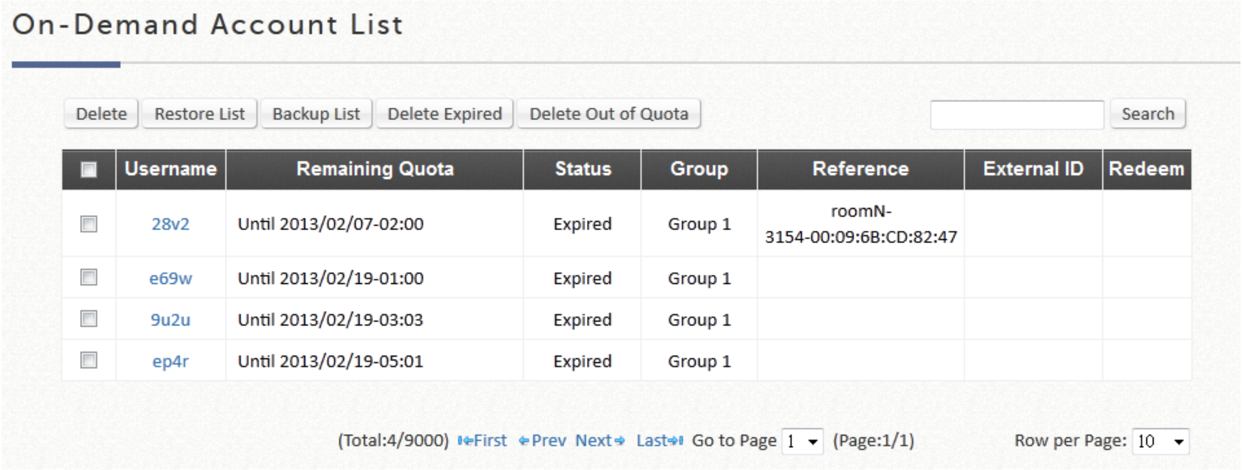
4) On-Demand Accounts



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	Create Single Create Batch
2	Hotel Cut-off-time	Valid until 5:01 the following day	1	1	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

- **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. (eg. Prefix = ABC, Postfix = DEF, Serial Number 0001.)



On-Demand Account List

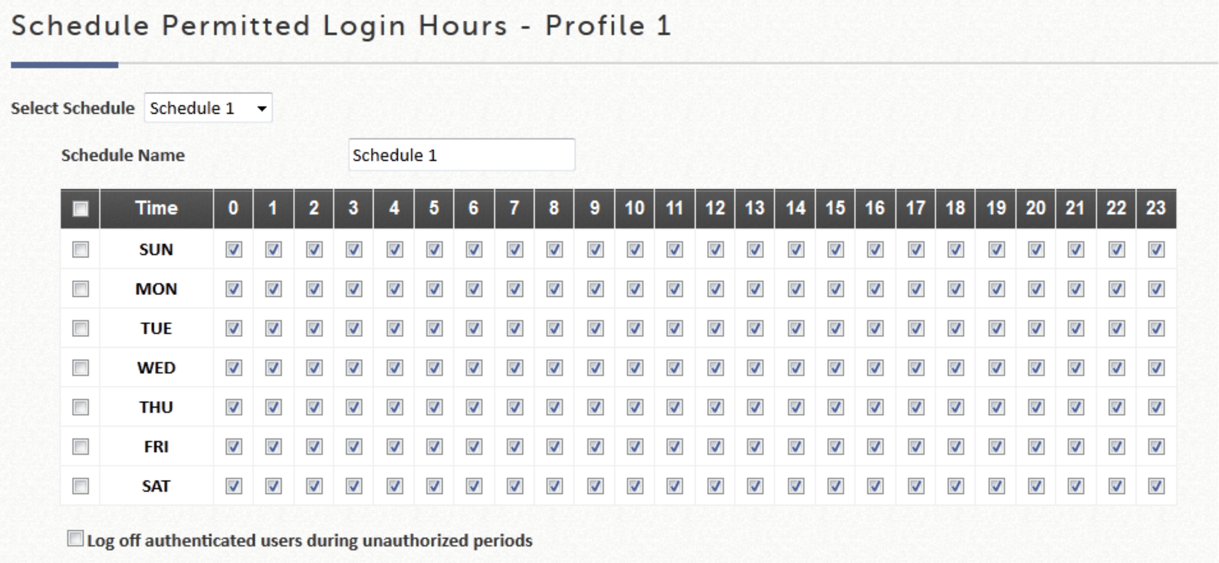
☐	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
☐	28v2	Until 2013/02/07-02:00	Expired	Group 1	roomN-3154-00:09:6B:CD:82:47		
☐	e69w	Until 2013/02/19-01:00	Expired	Group 1			
☐	9u2u	Until 2013/02/19-03:03	Expired	Group 1			
☐	ep4r	Until 2013/02/19-05:01	Expired	Group 1			

(Total:4/9000) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 10

- **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 1

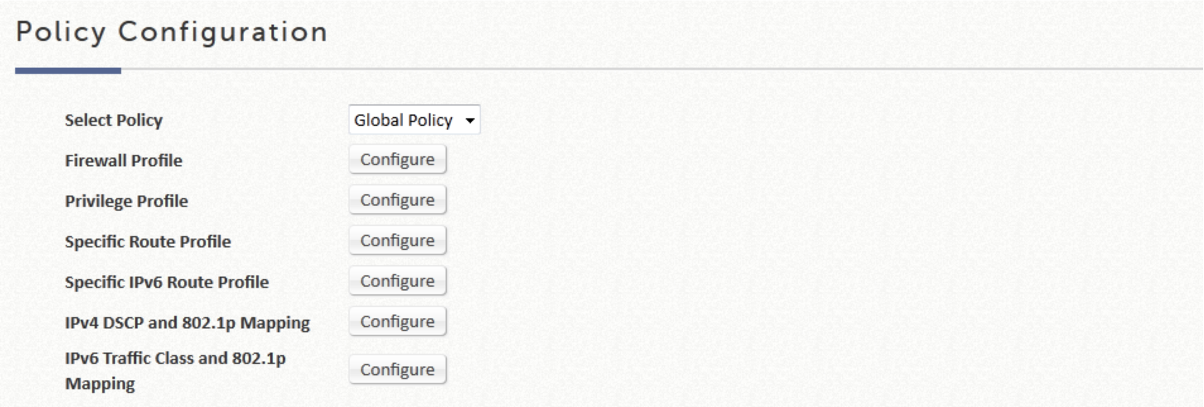
Schedule Name: Schedule 1

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

☐ Log off authenticated users during unauthorized periods

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.



Policy Configuration

Select Policy	Global Policy
Firewall Profile	Configure
Privilege Profile	Configure
Specific Route Profile	Configure
Specific IPv6 Route Profile	Configure
IPv4 DSCP and 802.1p Mapping	Configure
IPv6 Traffic Class and 802.1p Mapping	Configure

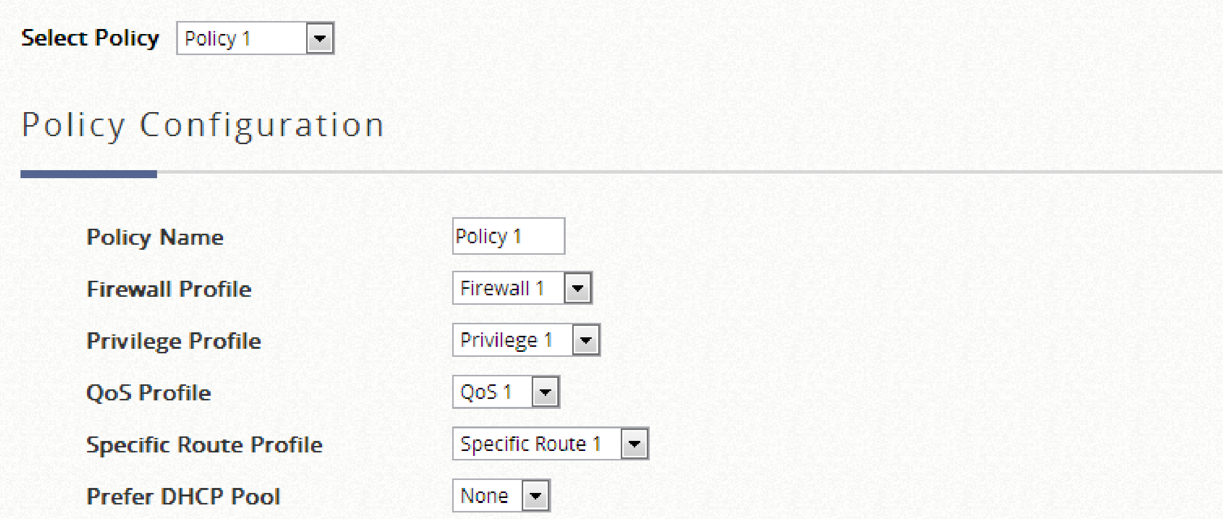
Each policy consists of **Firewall Profile**, **Specific Route Profile**, **Schedule Profile** and **Maximum Concurrent Sessions** management as well. Policies can be defined in the Policy tab. The administrator can select one of the defined policies to apply it to groups within a certain Service Zone. 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.
- **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.
- **Privilege Profile:** User generated session number limit may be configured here. Please adjust this attribute carefully based on your network usage
- **IPv4 DSCP and 802.1p Mapping:** 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:** 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

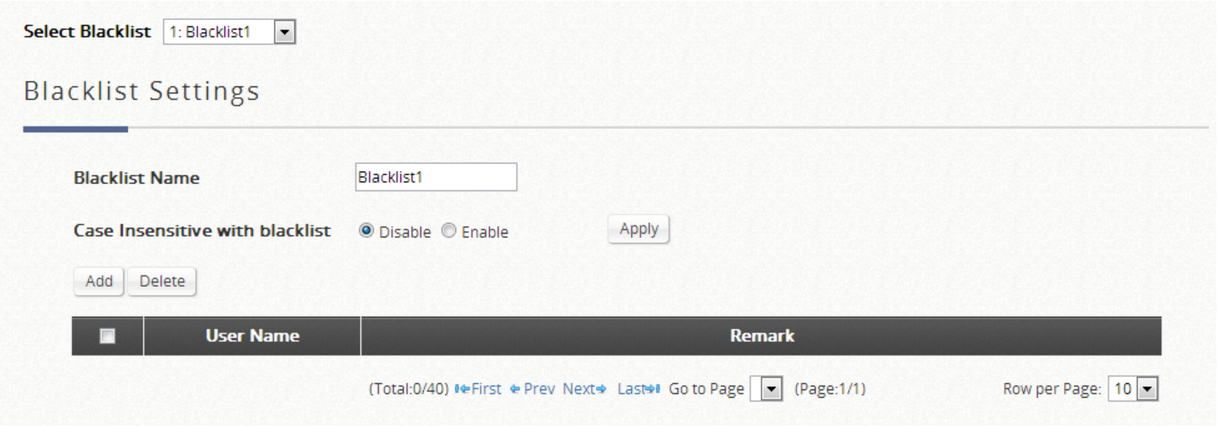
Policy Configuration

Policy Name	Policy 1
Firewall Profile	Firewall 1
Privilege Profile	Privilege 1
QoS Profile	QoS 1
Specific Route Profile	Specific Route 1
Prefer DHCP Pool	None

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

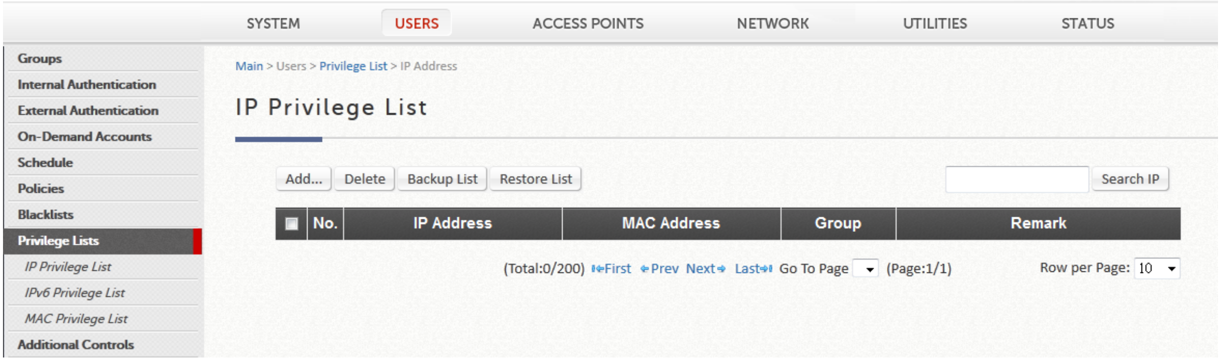
Blacklist Name	Blacklist1
Case Insensitive with blacklist	● Disable ○ Enable

☐	User Name	Remark

(Total:0/40) First Prev Next Last Go to Page (Page:1/1) Row per Page: 10

8) Privilege Lists

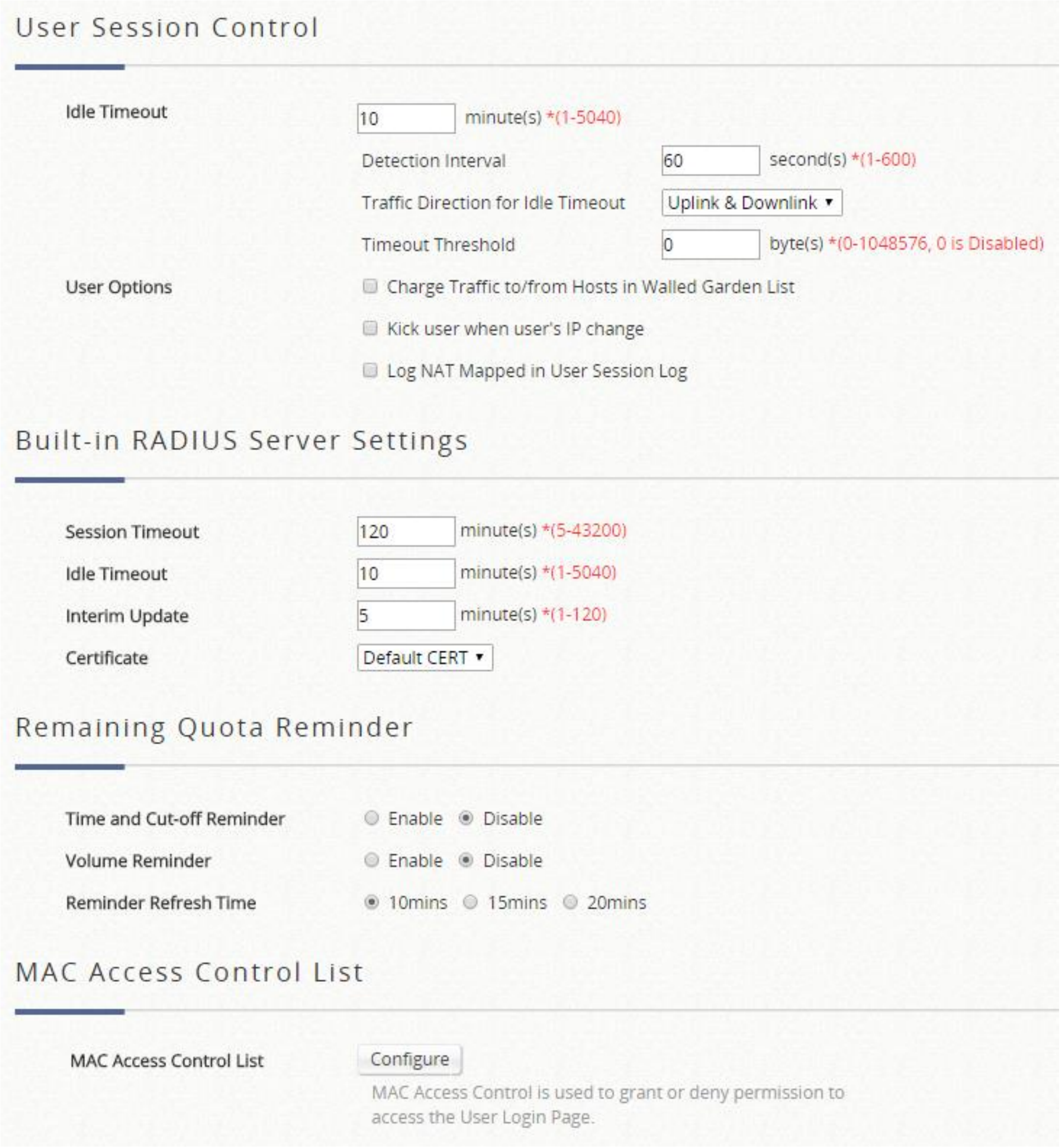
The Privilege function supports three types of privilege list based on IP address, MAC address and IPv6 address. Devices specified in the list require NO authentication to access the network. Note that a User Group can be assigned to Devices on the IP Privilege List but not on the MAC Privilege List.


SYSTEM
USERS
ACCESS POINTS
NETWORK
UTILITIES
STATUS
Groups
Internal Authentication
External Authentication
On-Demand Accounts
Schedule
Policies
Blacklists
Privilege Lists
IP Privilege List
IPv6 Privilege List
MAC Privilege List
Additional Controls
Main > Users > Privilege List > IP Address
IP Privilege List
Add...
Delete
Backup List
Restore List
Search IP
No.
IP Address
MAC Address
Group
Remark
(Total:0/200) First Prev Next Last Go To Page (Page:1/1)
Row per Page: 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.

5) 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: 10 minute(s) *(1-5040)
Detection Interval: 60 second(s) *(1-600)
Traffic Direction for Idle Timeout: Uplink & Downlink
Timeout Threshold: 0 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: 120 minute(s) *(5-43200)
Idle Timeout: 10 minute(s) *(1-5040)
Interim Update: 5 minute(s) *(1-120)
Certificate: Default CERT

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

Built in RADIUS Server Settings

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

Remaining Quota Reminder

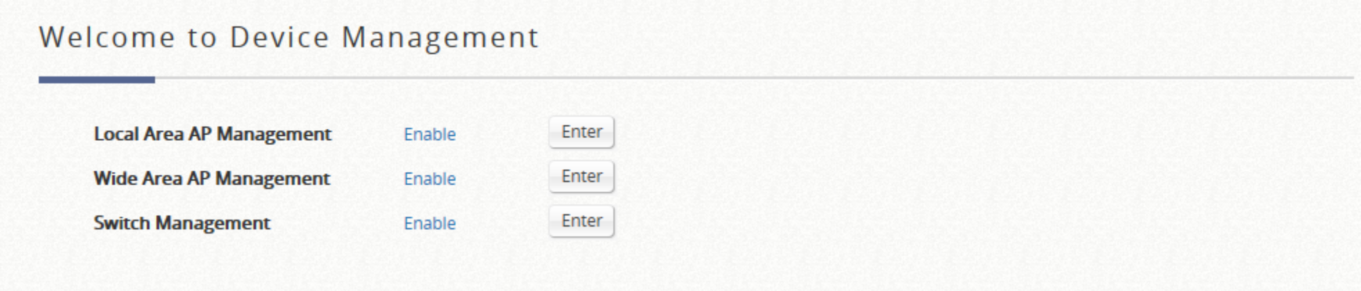
- **Time and Cut-off reminder:** This is the option for the system to display a warning message to On-Demand users that their time based account quota is about to run out.
- **Volume Reminder:** This is the option for the system to display a warning message to On-Demand users that their volume based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

MAC Access Control List

- **MAC ACL:** The administrator may configure restraining measures to MAC address, either MAC allow or deny list.

C. Access Points

Access Points: This section is used to manage the APs. Besides showing the various attributes of APs, there are different functions provided for various configurations.


Welcome to Device Management

Local Area AP Management	Enable	Enter
Wide Area AP Management	Enable	Enter
Switch Management	Enable	Enter

1) Local Area AP Management

a) Overview

A summary is used to list the basic information of each AP type. It includes: number of AP, number Online, number Offline, and total number of associated clients in each AP type.

All of the supported APs under management of the system will be shown in the table and listed by AP type.

Select any AP by checking the checkbox and then click the button below to ***Reboot***, ***Enable***, ***Disable, Delete, Apply Template*** and ***Apply Service Zone*** (Tag-Based) the selected AP if desired.

b) List

A list is used to show the information of each managed AP, including Type, Name, IP Address, MAC Address, and online Status. Functions in this section also include the operations such as reboot, enable, disable, delete, apply a new template, apply by service zone and other configuration.

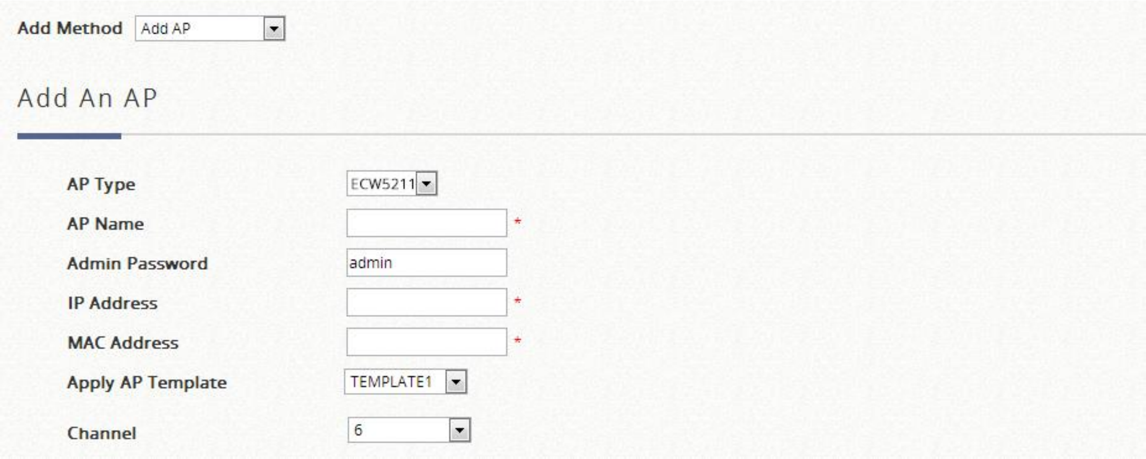
All of the supported APs under management of the system will be shown in the list. The administrator can add supported APs from the **Discovery** or the **Adding** tabs. After APs are added, this list will show the current managed APs including AP type, AP name, IP Address, MAC Address, Service Zone and Status. The administrator can then perform reboot, enable, disable, delete the managed APs, or apply template or apply service zone to them by checking the check box in front of each individual AP or selecting all the APs together by checking the top check box.

Select any AP by checking the checkbox on the list and then click the buttons to ***Reboot***, ***Enable***, ***Disable, Delete, Apply Template*** and ***Reset to Default*** to the selected AP if desired.

c) Adding

The Adding function is used to manually set up an AP via filling in the required information for that AP. The system provides templates that can be used to simplify the AP configuration.

The administrator can add supported APs into the **List** table manually by clicking “Add” and selecting “Add AP”. The system will attempt to configure the AP with the value specified. After processing, the AP's status will display "online" or "offline" on the AP List.


Add Method: Add AP

Add An AP

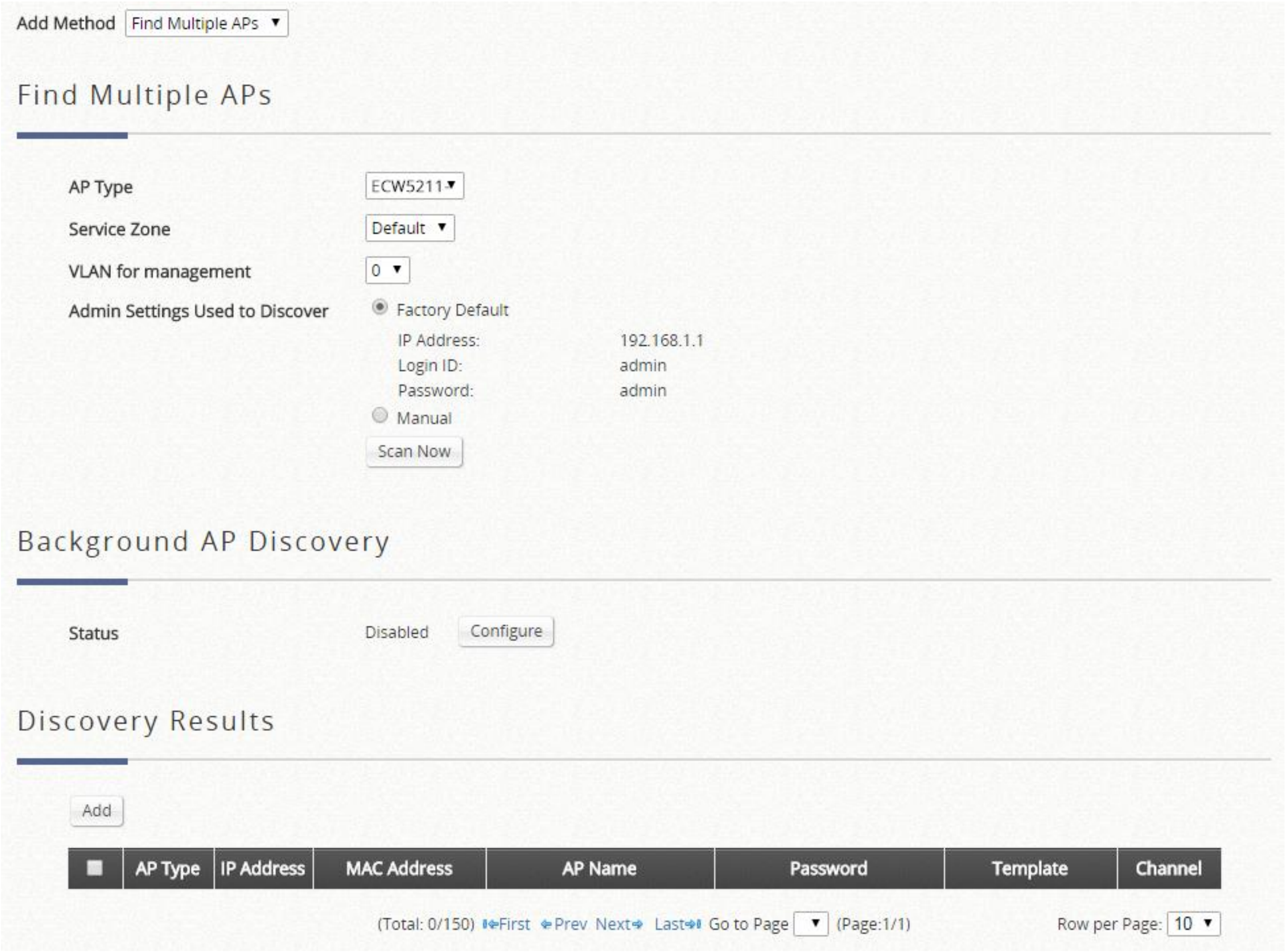
AP Type	ECW5211
AP Name	*
Admin Password	admin
IP Address	*
MAC Address	*
Apply AP Template	TEMPLATE1
Channel	6

- **AP Type**: The model type of the AP for adding to the List.
- **AP Name:** Mnemonic name of the specific AP.
- **Admin Password:** Password required for this AP.
- **IP Address:** IP address of the specified AP.
- **MAC Address:** MAC address of the specific AP.
- **Apply AP Template:** Select the AP Template to be applied to this added AP.
- **Channel:** The selected channel will be applied to the added AP.

d) Discovery

This Discovery function is to manually or automatically detect the supported types of APs when connected to the LAN ports and automatically assign a unique IP address to each AP discovered. Click “Add” from the AP List and select “Find Multiple APs”.

When **Background AP Discovery** function is enabled, the system will scan once every 10 minutes or according to the time set by the administrator. If any AP is discovered and **Auto Adding AP to the List** is enabled, it will be assigned an available IP from the starting IP address set in checked Service Zone profile and applied with the selected template. You can also set the channel the AP would use.



Add Method: Find Multiple APs

Find Multiple APs

AP Type: ECW5211
Service Zone: Default
VLAN for management: 0
Admin Settings Used to Discover: ● Factory Default
IP Address: 192.168.1.1
Login ID: admin
Password: admin
○ Manual

Background AP Discovery

Status: Disabled

Discovery Results

■	AP Type	IP Address	MAC Address	AP Name	Password	Template	Channel

(Total: 0/150) First Prev Next Last Go to Page (Page:1/1) Row per Page: 10

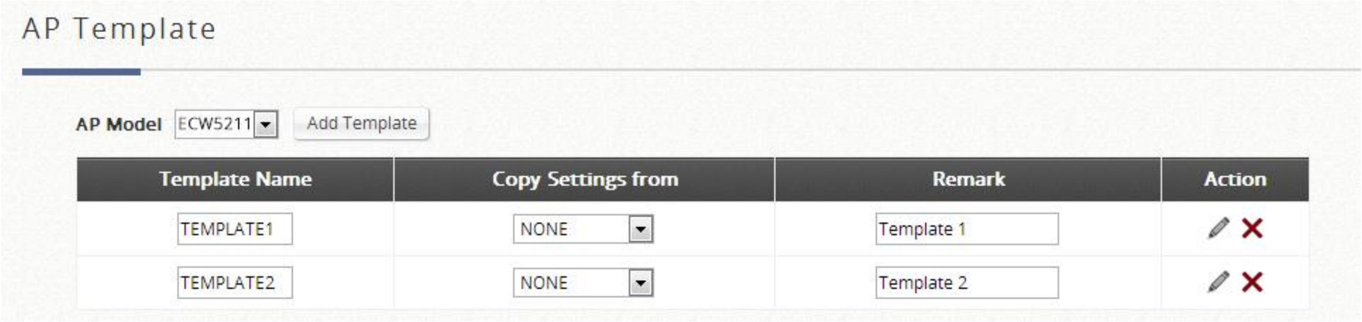
- **AP Type:** Select the AP model name which you like for the system to find.
- **Service Zone:** Select the Service Zone for which the device connected AP is to be managed in**.**
- **VLAN for management:** Set VLAN for management for the discovered AP.
- **Admin Settings Used to Discover:** Select factory default if the connected AP’s interface and management credentials have not been changed. Otherwise, choose manual and specify the IP range and management settings accordingly. The administrator may stop the controller from scanning at any time during the discovery process.
- **Background AP Discovery:** When configured, the system will periodically scan the configured IP range for newly connected AP devices and automatically display the discovery results.
- **Discovery Results:** Shows the AP devices detected that match the discovery criteria configured above.

e) Templates

The AP setting templates can be defined. Up to 8 templates can be edited, saved, and used in "Adding" and "Discovery" sections.

Templates by AP Model

The system supports up to eight templates which include configurations of APs. The administrator can configure the setting together in the template instead of logging the AP management interface to set the configurations one by one. Select the **AP type**, and then click ***Edit*** icon to enter the **Template Editing** page.

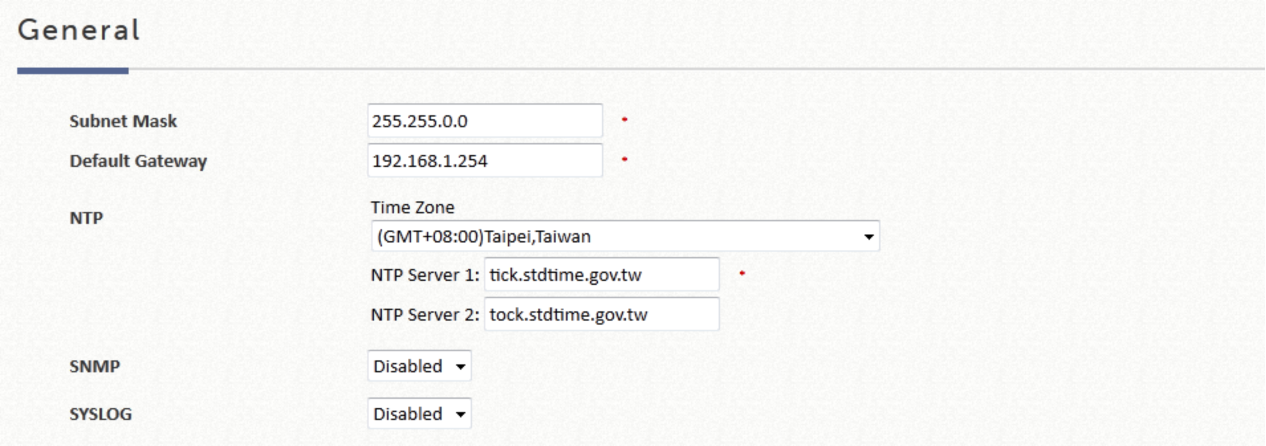


AP Template

AP Model ECW5211 Add Template

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

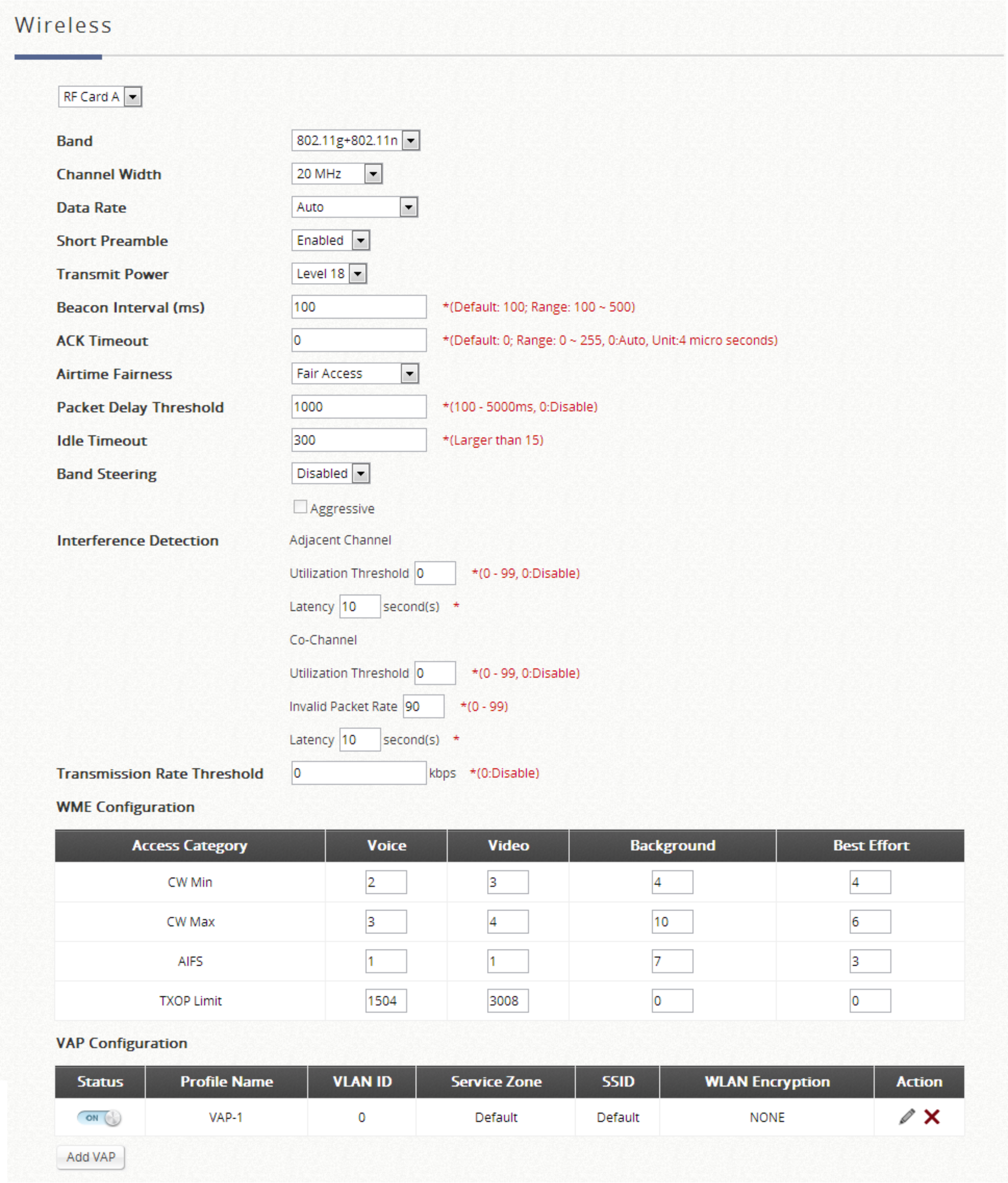
- **Template Editing**: The administrator can set the template configuration manually or copy the configurations from a specific existing managed AP by **Copy Settings From** option. Click ***Configure*** button to have detailed configurations.
  - **Name**: The name shown for this particular template.
  - **Copy Settings From**: Select a pre-configured existing AP and click ***Apply*** to save its settings as the template settings.
  - **Remark:** The remark or additional information for this template profile.
  - **Action:** Click Edit depicted by a pencil icon to enter configurations or click the red cross to delete template



General

Subnet Mask	255.255.0.0 *
Default Gateway	192.168.1.254 *
NTP	Time Zone (GMT+08:00)Taipei,Taiwan NTP Server 1: tick.stdtime.gov.tw * NTP Server 2: tock.stdtime.gov.tw
SNMP	Disabled
SYSLOG	Disabled

- **General:** In this section, revise the **Subnet Mask** and **Default Gateway** here if desired. Configure the **NTP Servers** and **Time Zone**. In addition, administrator can enable **SYSLOG** server to receive the log from AP and enable **SNMP** read/write ability.



Wireless

RF Card A

Band: 802.11g+802.11n

Channel Width: 20 MHz

Data Rate: Auto

Short Preamble: Enabled

Transmit Power: Level 18

Beacon Interval (ms): 100 *(Default: 100; Range: 100 ~ 500)

ACK Timeout: 0 *(Default: 0; Range: 0 ~ 255, 0:Auto, Unit:4 micro seconds)

Airtime Fairness: Fair Access

Packet Delay Threshold: 1000 *(100 - 5000ms, 0:Disable)

Idle Timeout: 300 *(Larger than 15)

Band Steering: Disabled

☐ Aggressive

Interference Detection: Adjacent Channel

Utilization Threshold 0 *(0 - 99, 0:Disable)

Latency 10 second(s) *

Co-Channel

Utilization Threshold 0 *(0 - 99, 0:Disable)

Invalid Packet Rate 90 *(0 - 99)

Latency 10 second(s) *

Transmission Rate Threshold: 0 kbps *(0:Disable)

WME Configuration

Access Category	Voice	Video	Background	Best Effort
CW Min	2	3	4	4
CW Max	3	4	10	6
AIFS	1	1	7	3
TXOP Limit	1504	3008	0	0

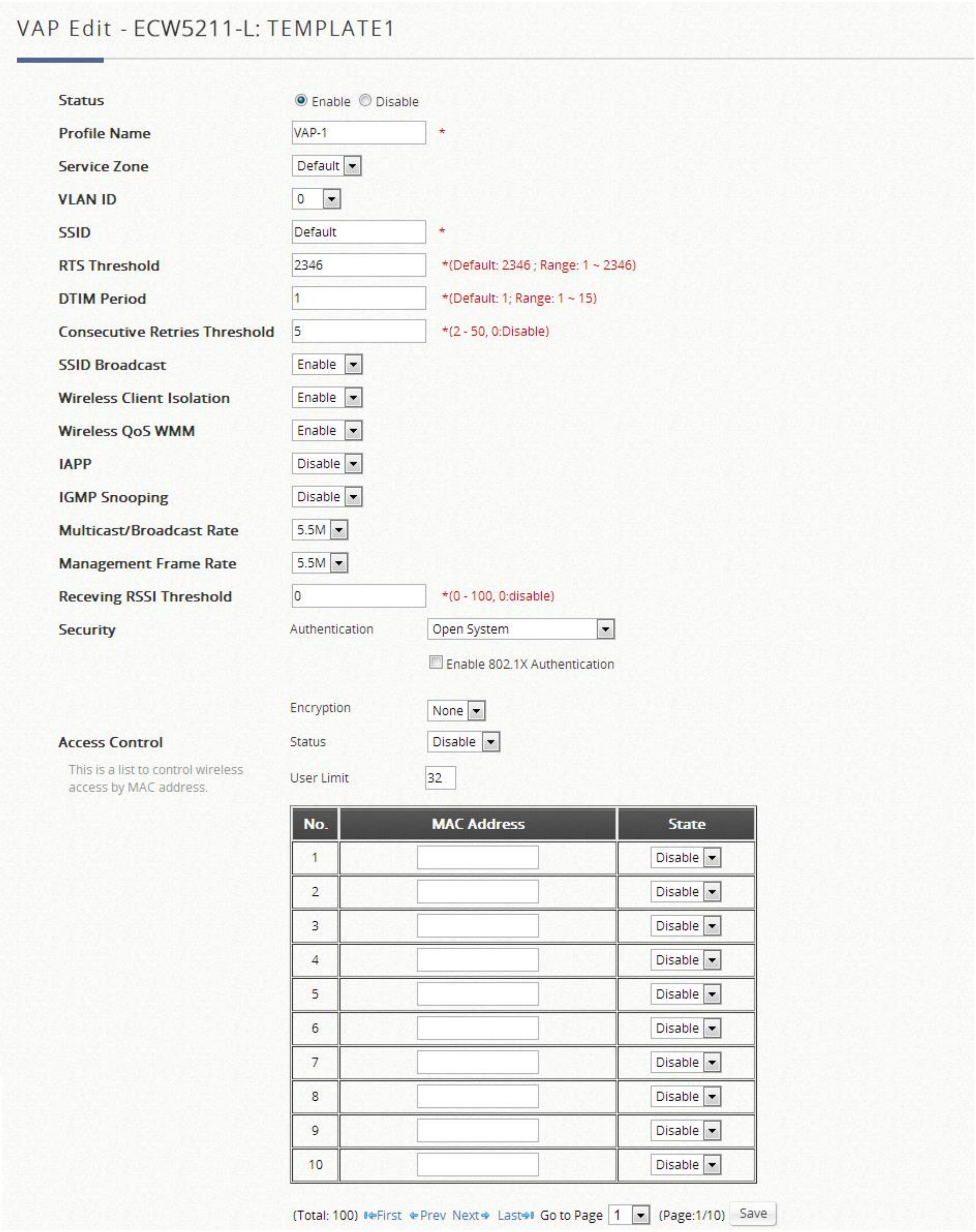
VAP Configuration

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

Add VAP

- **Wireless:**
  - **SSID Broadcast:** Select this option to enable the AP's SSID to broadcast in your network. It is suggested to disable SSID broadcast feature when you have an authentication disabled network intended for private use.
  - **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**.

- **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.
- **Data Rate:** The default is set to **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to allow the Access Point to automatically use the fastest rate possible. For 802.11n the selectable data rates range from MCS0 to MCS15.
- **Transmit Power:** On select AP models, the signal strength transmitted from the system can be selected by Levels. Each level signifies a decrement of 1 dBm from the highest power. **Level 1** is the actual highest power, **Level 2** is the highest power minus 1 dBm, so on and so forth.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal is transmitted between the access point and the wireless network.
- **ACK Timeout:** The time interval for waiting for the “acknowledgement (ACK) frame”. If the ACK is not received within the interval then the packet will be re-transmitted. Higher ACK Timeout interval will decrease the packet lost, but the throughput will be decreased/worsened.
- **Airtime Fairness:** When set to “Fair Access”, this feature ensures all devices with different band compatibilities have the same air time. When set to “Preferred Access”, N clients are prioritized. This feature is ideal for networks with devices supporting different bands.
- **Packet Delay Threshold (ms):** This is the Tx Queue flushing mechanism, which purpose is to drop packets and immediately process others if the queue has been processed for more than x milliseconds. This is disabled by default (=0).
- **Idle Timeout (s):** Clients disconnects when inactivity reaches the configured amount of time in seconds, where default = 300s.
- **Band Steering:** When enabled, clients with 5GHz connectivity will be steered towards the 5GHz band to reduce congestion in the 2.4GHz band. This is applicable only when the AP is set to 2.4GHz and 5GHz on the 2 RF Cards. When “Aggressive” is checked, clients with 5GHz connectivity are forced to connect to the 5GHz band.
- **Interference Detection:** When utilization of the current channel reaches the configured threshold (in %), the AP switches to a different Channel.
- **Transmission Rate Threshold:** The associated client will be kicked when transmission rate is lower than the configured threshold. This ensures high connection speed for all associated clients.
- **WME Configuration:** Access priority can be configured using with different parameters. CW Min: Contention Window Minimum, CW Max: Contention Window Maximum, AIFS: Arbitration Inter Frame Spacing, TXOP Limit: Transmission Opportunity Limit.
- **VAP Configuration:** Enable/Disable VAP under the ‘Status’ column. Configuration of VAPs can be done by clicking the edit icon under ‘Action’.



VAP Edit - ECW5211-L: TEMPLATE1

Status	● Enable ○ Disable
Profile Name	VAP-1 *
Service Zone	Default
VLAN ID	0
SSID	Default *
RTS Threshold	2346 *(Default: 2346 ; Range: 1 ~ 2346)
DTIM Period	1 *(Default: 1; Range: 1 ~ 15)
Consecutive Retries Threshold	5 *(2 - 50, 0:Disable)
SSID Broadcast	Enable
Wireless Client Isolation	Enable
Wireless QoS WMM	Enable
IAPP	Disable
IGMP Snooping	Disable
Multicast/Broadcast Rate	5.5M
Management Frame Rate	5.5M
Receving RSSI Threshold	0 *(0 - 100, 0:disable)
Security	Authentication: Open System ☐ Enable 802.1X Authentication Encryption: None
Access Control This is a list to control wireless access by MAC address.	Status: Disable User Limit: 32

No.	MAC Address	State
1		Disable
2		Disable
3		Disable
4		Disable
5		Disable
6		Disable
7		Disable
8		Disable
9		Disable
10		Disable

(Total: 100) First Prev Next Last Go to Page 1 (Page:1/10) Save

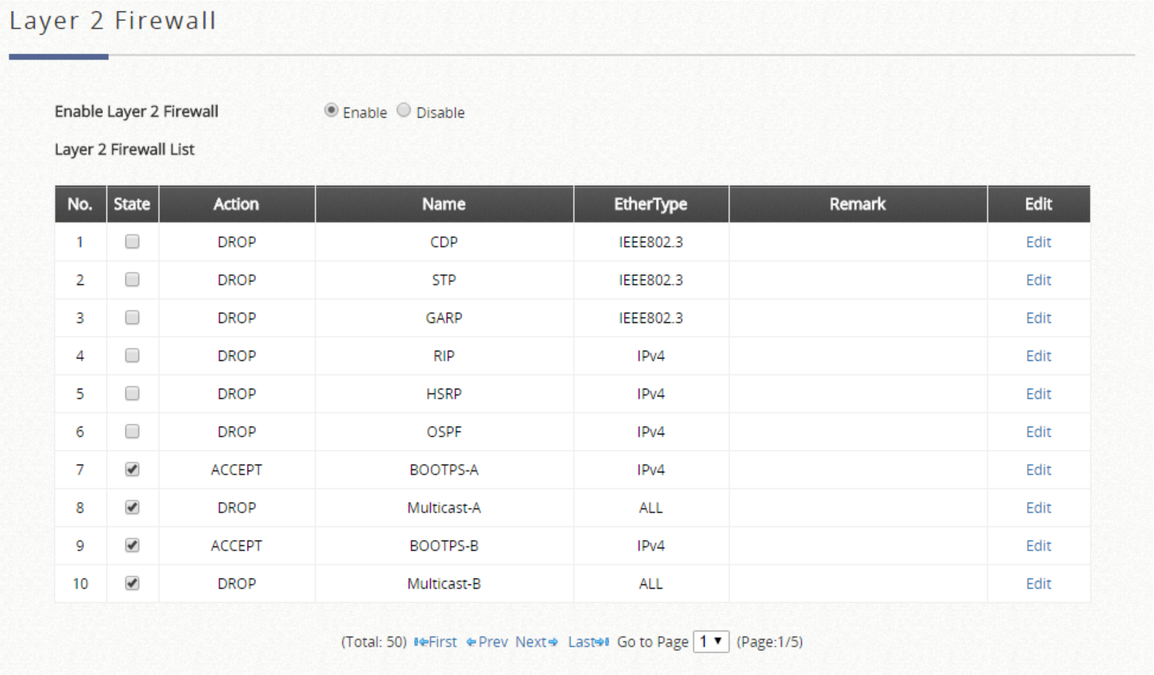
- **Status:** VAP can be Enabled or Disabled here
- **Profile Name:** The profile name of a specific RF card and its VAP for identity / management purposes.
- **Service Zone:** Select the mapping Service Zone for the VAP from the drop-down list
- **VLAN ID:** Select the VLAN ID for this VAP
- **SSID:** The SSID 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.
- **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.
- **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 fails 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.
- **SSID Broadcast:** 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 Client Isolation:** By enabling this function, all stations associated with the system are isolated and can only communicate with the system.
- **Wireless QoS WMM:** Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.
- **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.
- **IGMP Snooping:** When IGMP snooping is enabled, IGMP packets are transferred via the Access Point’s network interface and the IP multicast host. Registration information is recorded and sorted into multicast groups. The internal switch can then intelligently forward traffic only to those ports that request multicast traffic. Adversely, without IGMP snooping, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.
- **Multicast/Broadcast Rate:** Bandwidth configuration for multicast/broadcast packets. If your wireless clients require a larger or smaller bandwidth for sending multicast/ broadcast packets, the administrator can customize the Access Point’s multicast/ broadcast bandwidth here.

- **Management Frame Rate:** This feature controls the bandwidth for Management Frames. The higher the rate it, the shorter range the transmission covers.
- **Receiving RSSI Threshold:** To keep connected stations with high connection speeds, the station is kicked out when its receiving sensitivity is lower than the threshold.
- **Security:** The Access Point supports various wireless authentication and data encryption methods in each VAP profile. With this, the administrator can provide different service levels to clients. The security type includes Open, WEP, 802.1X, WPA-Personal, and WPA-Enterprise.
- **Access Control:** The administrator can restrict the wireless access of client devices based on their MAC addresses.
    - Disable Access Control: When Disable is selected, there is no restriction for client devices to access the system.
    - MAC ACL Allow List: When selecting MAC ACL Allow List, only the client devices (identified by their MAC addresses) listed in the Allow List (“allowed MAC addresses”)are granted access to the system. The administrator can temporarily block any allowed MAC address by checking Disable, until the administrator re-Enables the listed MAC.
    - MAC ACL Deny List: When selecting MAC ACL Deny List, all client devices are granted access to the system except those listed in the Deny List (“denied MAC addresses”).

      The administrator can allow any denied MAC address to connect to the system temporarily by checking Disable.

The Wireless Setting for RF Card B is available for dual Radio Access Points. Configuration parameters may differ on select AP Models.

- **Layer 2 Firewall:**



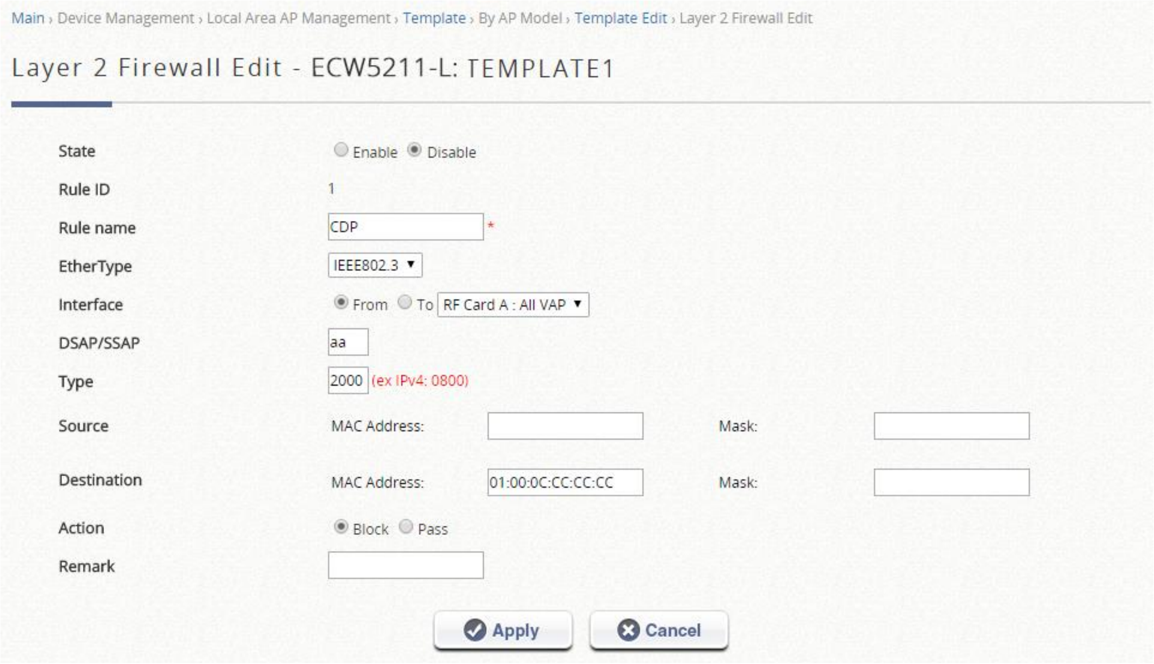
Layer 2 Firewall

Enable Layer 2 Firewall ● Enable ○ Disable

Layer 2 Firewall List

No.	State	Action	Name	EtherType	Remark	Edit
1	☐	DROP	CDP	IEEE802.3		Edit
2	☐	DROP	STP	IEEE802.3		Edit
3	☐	DROP	GARP	IEEE802.3		Edit
4	☐	DROP	RIP	IPv4		Edit
5	☐	DROP	HSRP	IPv4		Edit
6	☐	DROP	OSPF	IPv4		Edit
7	☑	ACCEPT	BOOTPS-A	IPv4		Edit
8	☑	DROP	Multicast-A	ALL		Edit
9	☑	ACCEPT	BOOTPS-B	IPv4		Edit
10	☑	DROP	Multicast-B	ALL		Edit

(Total: 50) First Prev Next Last Go to Page 1 (Page:1/5)



Main › Device Management › Local Area AP Management › Template › By AP Model › Template Edit › Layer 2 Firewall Edit

Layer 2 Firewall Edit - ECW5211-L: TEMPLATE1

State	○ Enable ● Disable		
Rule ID	1		
Rule name	CDP *		
EtherType	IEEE802.3 ▼		
Interface	● From ○ To RF Card A : All VAP ▼		
DSAP/SSAP	aa		
Type	2000 (ex IPv4: 0800)		
Source	MAC Address:		Mask:
Destination	MAC Address:	01:00:0C:CC:CC:CC	Mask:
Action	● Block ○ Pass		
Remark			

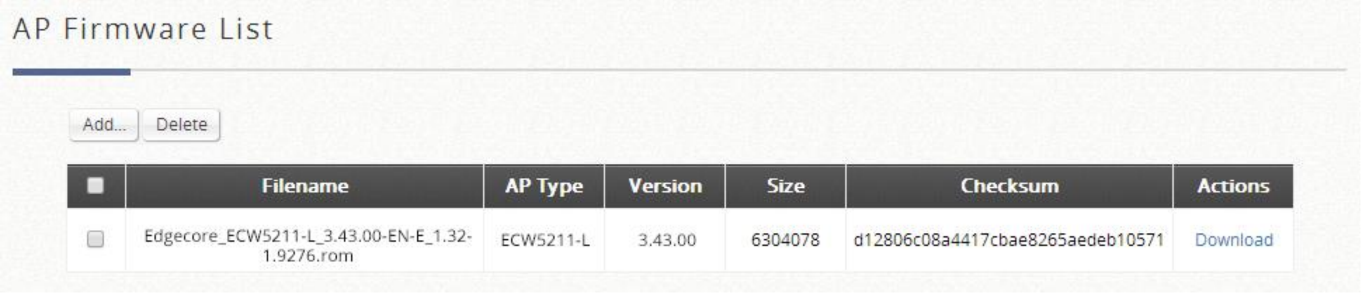
- **State:** Enable or Disable the respective rules
- **Rule:** The numbering of this specific rule will decide its priority among available firewall rules in the table.
- **Rule name:** The rule name can be specified here.
- **EtherType:** The drop-down list will provide the available types of traffics subject to this rule.
- **Interface:** This indicates inbound/outbound direction with desired interfaces.
- **DSAP/SSAP (**when EtherType is IEEE 802.3)**:** The value can be further specified for the fields in 802.2 LLC frame header.
- **Type** (when EtherType is IEEE 802.3)**:** The field can be used to indicate the type of encapsulated traffic.
- **Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.
- **Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.
- **Action:** The rule can be chosen to be **Block** or **Pass**
- **Remark:** Notes of this rule can be specified here.

f) Firmware

The Firmware function provides the tools to see the AP firmware version and upload new AP firmware into the system.

The system supports the firmware management of APs to upload new firmware, delete the existing firmware, and download the firmware to managed APs. Note that the AP's firmware version must be one that has been integrated.

Firmware Upload displays the current version of the AP's firmware. New firmware can be uploaded here to update the current firmware. To upload, first click ***Add***, and then ***Browse*** to select the file and then click ***Upload***.



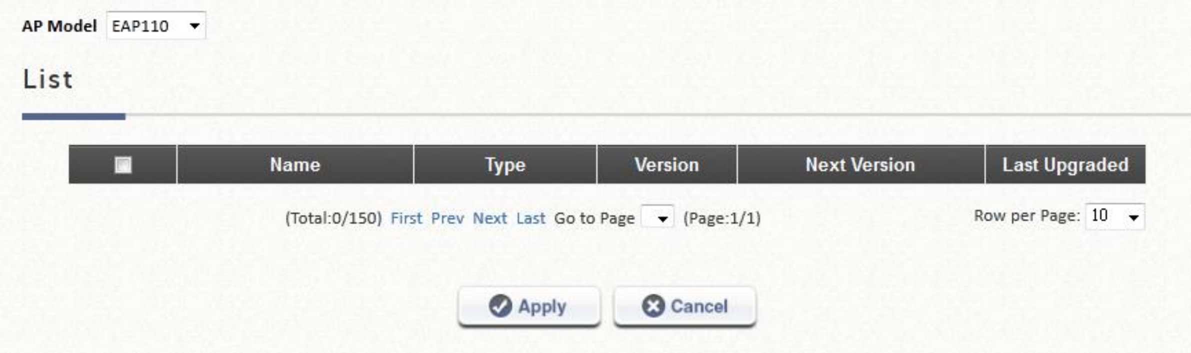
☐	Filename	AP Type	Version	Size	Checksum	Actions
☐	Edgecore_ECW5211-L_3.43.00-EN-E_1.32-1.9276.rom	ECW5211-L	3.43.00	6304078	d12806c08a4417cbae8265aedeb10571	Download

- **AP Firmware List:** The uploaded firmware will be listed here.
- **File Name:** The name of the AP firmware that has been uploaded.
- **AP Type:** The AP Type for the firmware
- **Version:** The version of the firmware
- **Size:** The file size of the firmware
- **Checksum:** The automatically detected security identification of the firmware.
- **Download:** Click ***Download*** to save the selected firmware to a local disk.
- **Delete:** Click ***Delete*** to delete the selected firmware from the system.

g) Upgrade

The Upgrade function allows administrators to upgrade the AP firmware using the firmware files stored in the system.

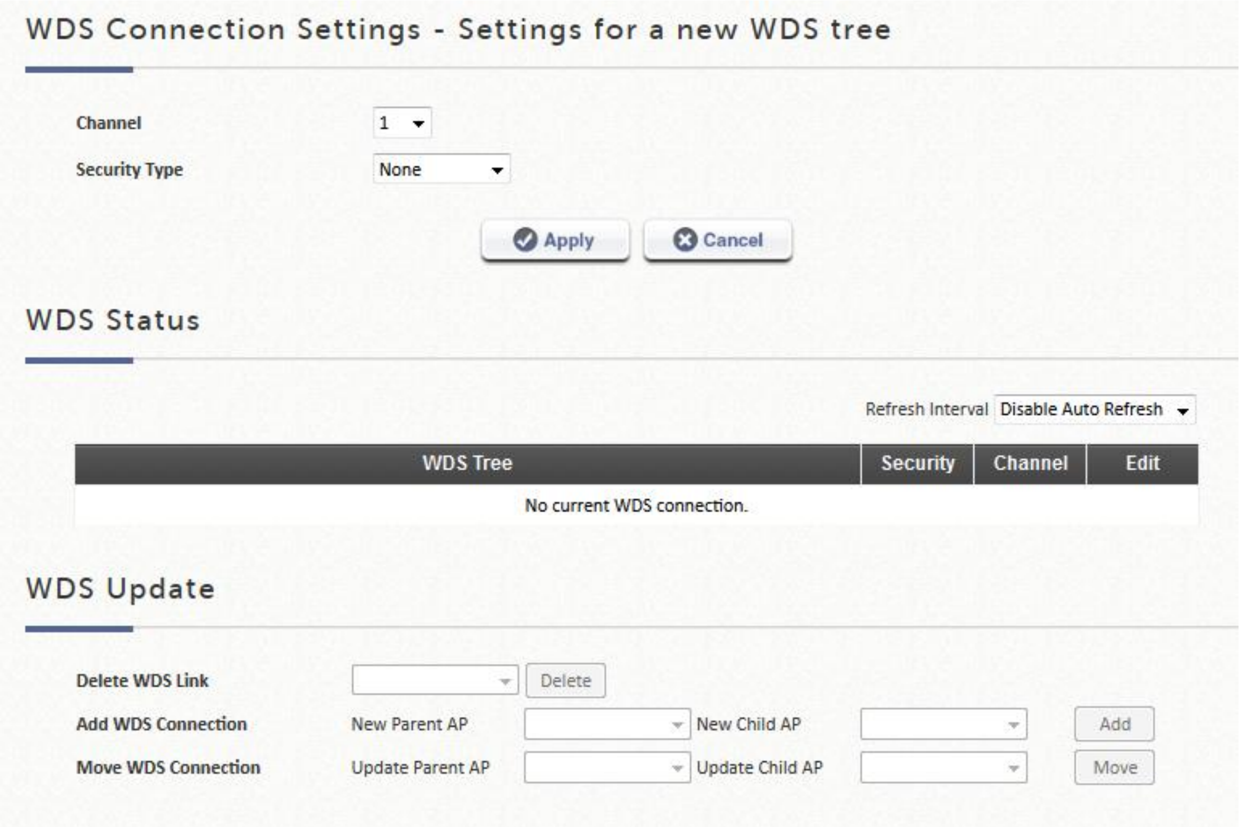
The administrator can upgrade the firmware of selected APs individually or at the same time by checking the check box of the APs in Selection column. Note that both the version before upgrade and the next version must be ones that have been integrated with the system.



☐	Name	Type	Version	Next Version	Last Upgraded

h) WDS Management

WDS (Wireless Distribution System) is a function used to connect APs (access points) wirelessly. The WDS management function of the system can help administrators to setup a "Tree" structure of WDS network.



WDS Connection Settings - Settings for a new WDS tree

Channel: 1
Security Type: None

WDS Status

Refresh Interval: Disable Auto Refresh

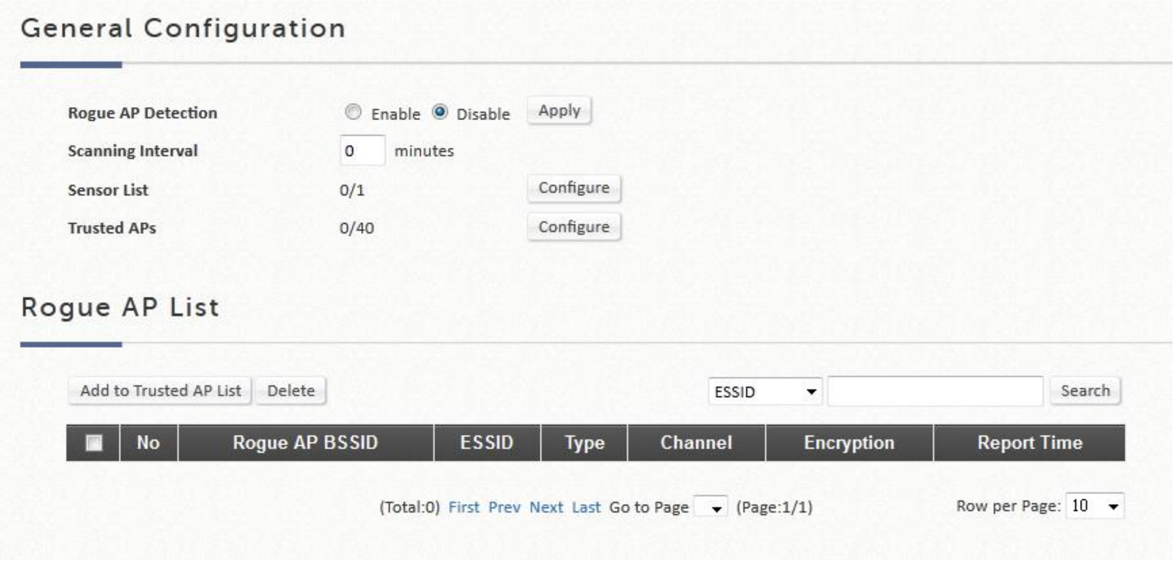
WDS Tree	Security	Channel	Edit
No current WDS connection.			

WDS Update

- **WDS Status:** Status shows the added APs in the WDS Tree with the Security and Channel settings. The WDS could be set up for more than one tree. Click ***Edit*** to change the **WDS connection settings** for the associated WDS Tree.
- **WDS Update:** Update the WDS connection with the following operations.
  - ***Add***: Add a new WDS connection with a Child AP not in the WDS and a Parent AP from the AP List. A new WDS Tree will be added if the selected Parent AP is not in any of the current WDS Trees. Click ***Edit*** to change the **WDS connection settings** for the new added WDS Tree.
  - ***Move***: Update a WDS connection with a Child AP from WDS and a Parent AP which could be connected by WDS, and the previous WDS connection of the Child AP to the previous Parent AP will be deleted.
  - ***Delete***: All the WDS connections of the selected AP will be deleted including the WDS connections to its Child APs, and the Child APs without wired connection will become unreachable.

i) 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 report time.



General Configuration

Rogue AP Detection ○ Enable ● Disable

Scanning Interval 0 minutes
Sensor List 0/1

Trusted APs 0/40

Rogue AP List

☐	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: 10

- **General Config:** This configuration item contains the switch for turning on features within this tab page. i.e. ***Rogue AP Detection*** as well as an optional “Channel Switching” feature.
- **Sensor List Config:** This configuration item contains a listing of all currently managed APs under Wide Area AP Management. Administrator may select one or more APs as sensors to scan for rogue AP.
- **Trusted AP Config:** This configuration item allows the administrator to maintain a list of detected rogue APs and remark them as trusted AP.
- **Rogue AP List:** This window lists all the detected Rogue AP. Each rogue AP will be presented with relevant information such as its BSSID, Channel, Encryption, Report Time etc. From the radio buttons at the bottom of the window, the selected Rogue AP on this list can be added into the trusted list or deleted if it can be ignored.

- **General Configuration**

  - **Scanning Interval:** The unit for this field is minute. Enter 0 to disable “Rogue AP Detection”. To enable “Rogue AP Detection”, please enter an integer ranging from 1 ~ 999 as the detection interval.

- **Sensor List Config**

  - **AP Type:** The drop down menu will contain the manageable model type for selection. The managed APs of the selected model type will be listed in the scroll window below.

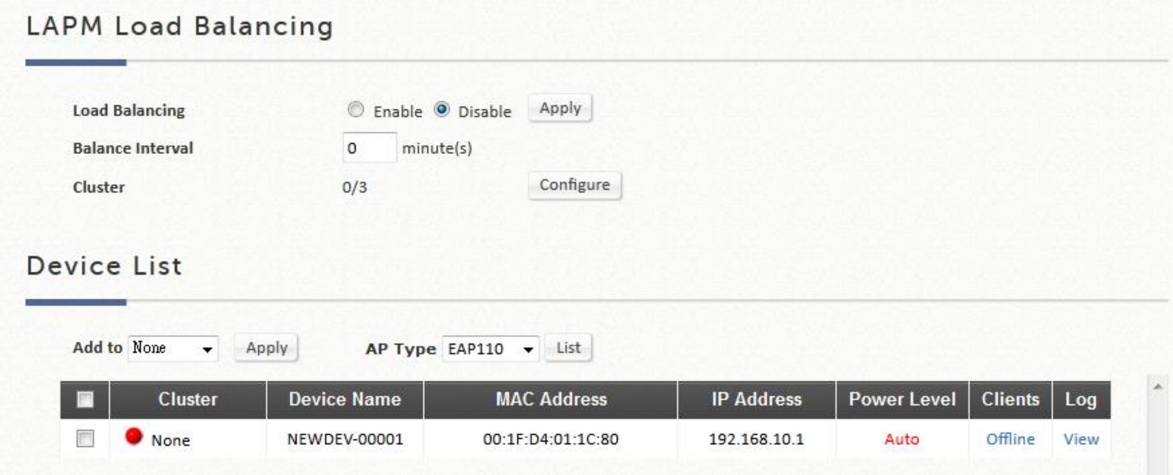
Administrator can check on one or more of the listed AP and click apply button at the bottom to designate these

APs as scanners.

- **Trusted AP Config**
  - **BSSID:** Administrator can statically assign the BSSID of a known trusted AP in this list. If an AP is entered into this list but not managed yet is present in the environment, it will not show up in the Rogue AP device list.
  - **Remark:** Administrator can type in a string of additional information that relates to the trusted AP on the list.

j) 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 the time interval which will trigger the AP load balancing.



Load Balancing ○ Enable ● Disable

Balance Interval 0 minute(s)

Cluster 0/3

Add to None

AP Type EAP110

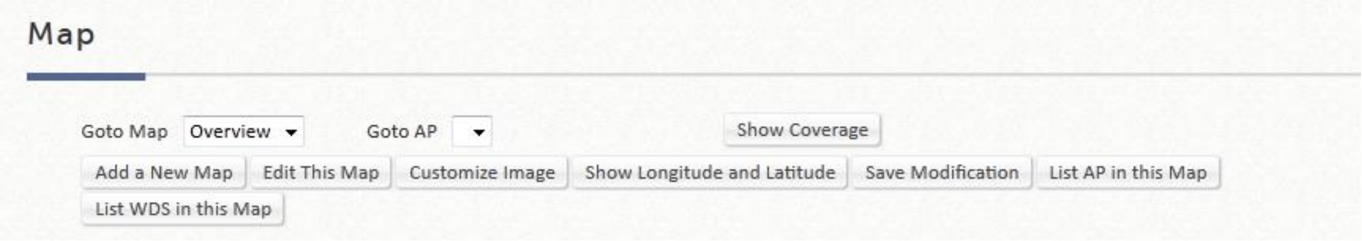
☐	Cluster	Device Name	MAC Address	IP Address	Power Level	Clients	Log
☐	● None	NEWDEV-00001	00:1F:D4:01:1C:80	192.168.10.1	Auto	Offline	View

- **Load Balancing:** This configuration item enables the administrator to specify the criteria under which AP load balancing feature will be enforced.
- **Balance Interval:** The administrator specifies the time interval for which the system synchronizes the number of clients within the cluster.
- **Cluster:** This item when entered to its configuration page will display all the current AP groups and their status info.
- **Device List:** The scrollable window displays all the managed APs sorted by model name with relative information such as Group, Name, MAC, IP, Power Lv, Loading, etc. The managed APs will have a Group column for indicating which AP group it belongs to for AP Load Balancing feature to be enforced.

2) Wide Area AP Management

a) Map

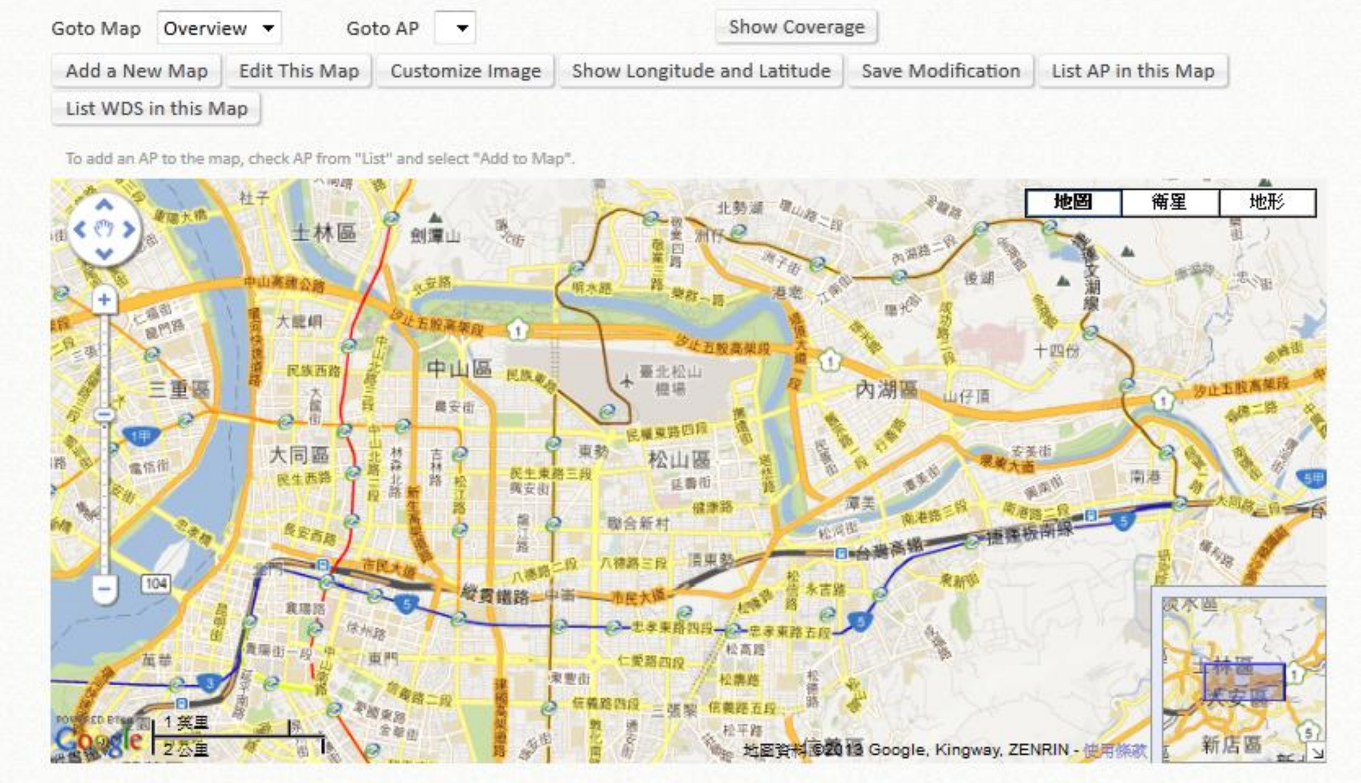
Map shows the managed APs and their WDS links on Google Maps. It is a utility for wireless network planning and management.



- **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.
- **Show Coverage:** This button once pressed will display the signal coverage of all the APs on the map according to the coverage radius set in each AP's profile under **List** tab page.
- **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.
- **Save Modification:** This function is for saving the changes made to the map and overwriting the maps' profile attributes. For instance if you have altered or panned the original map, clicking this button will save the changes made.
- **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.
- **Delete this Map:** Delete the current map profile.
- **Add a New Map:** Click to add a new map profile.
- **Edit this Map:** Click to modify the current map's attribute settings.
- **Customize Image:** Administrator can upload desired images for each AP model that will be used as AP markers on the MAP.

The Map tab page is implemented with Google Map API version2 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:


Goto Map
Overview
Goto AP
Show Coverage
Add a New Map
Edit This Map
Customize Image
Show Longitude and Latitude
Save Modification
List AP in this Map
List WDS in this Map
地圖
衛星
地形
士林區
中山區
大同區
松山區
內湖區
三重區
萬華
南港
新店區
1 英里
2 公里
©2013 Google, Kingway, ZENRIN

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

Procedure to create a Map:

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

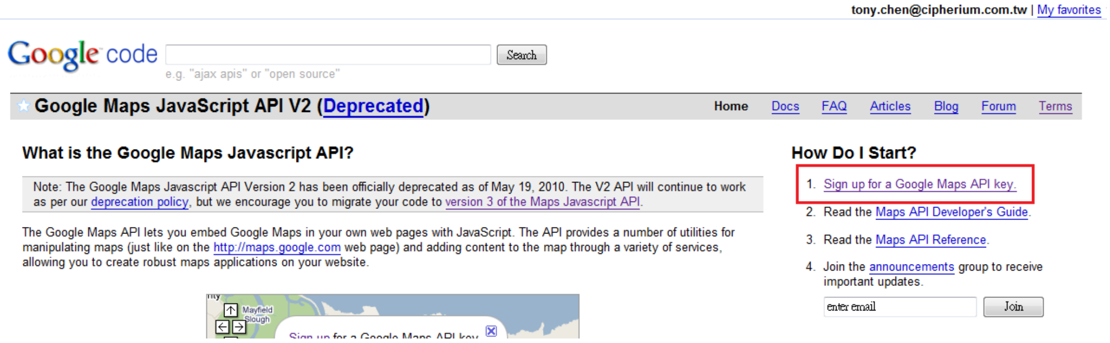
Step 2: Apply for a Google Maps Registration key.

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 v2 key. For more detail, please follow the instructions from Google at https://developers.google.com/maps/documentation/javascript/v2/introduction to obtain such Maps API v2 key and provide the key info into the field of "**Google Maps Registration Key"** under **Map Configuration page.**


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

Google Maps JavaScript API V2 (Deprecated)

What is the Google Maps Javascript API?

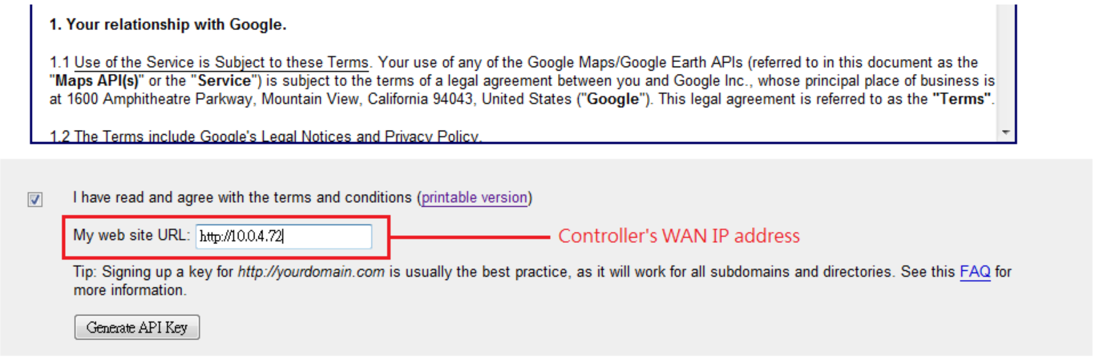
Note: The Google Maps Javascript API Version 2 has been officially deprecated as of May 19, 2010. The V2 API will continue to work as per our deprecation policy, but we encourage you to migrate your code to version 3 of the Maps Javascript API.

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

How Do I Start?

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

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



1. Your relationship with Google.

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

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

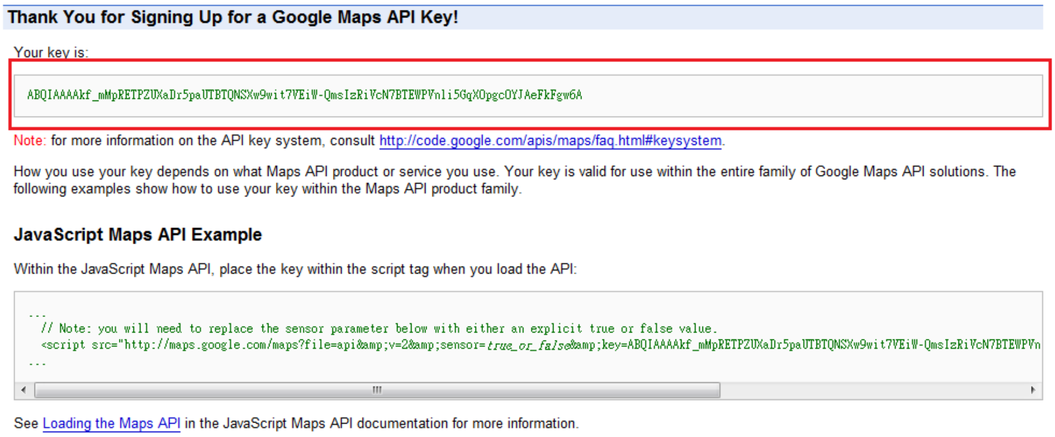
☑ I have read and agree with the terms and conditions (printable version)

My web site URL: http://10.0.4.72

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_mMpRETPZUXaDr5paUTBTQNSXw9wit7VEiW-QmsIzRiVcN7BTEWPVnli5GqXOpgcOYJAeFkFgw6A
```

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

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

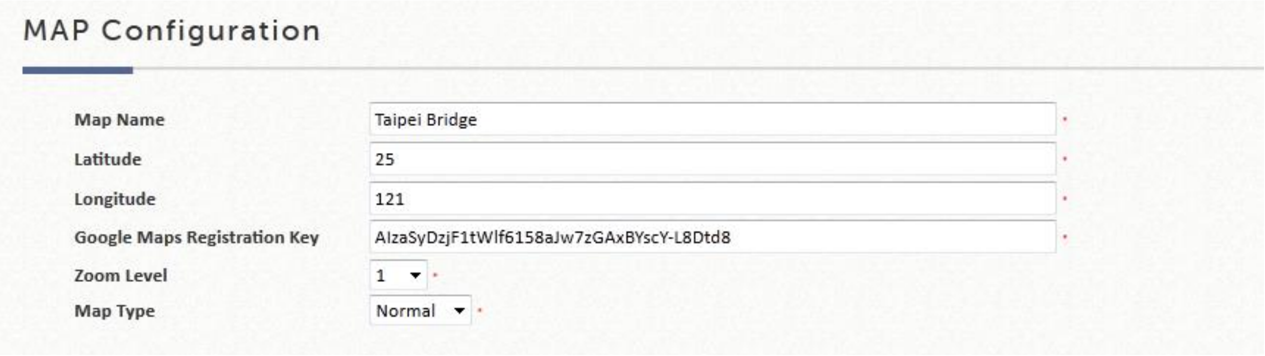
JavaScript Maps API Example

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

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

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

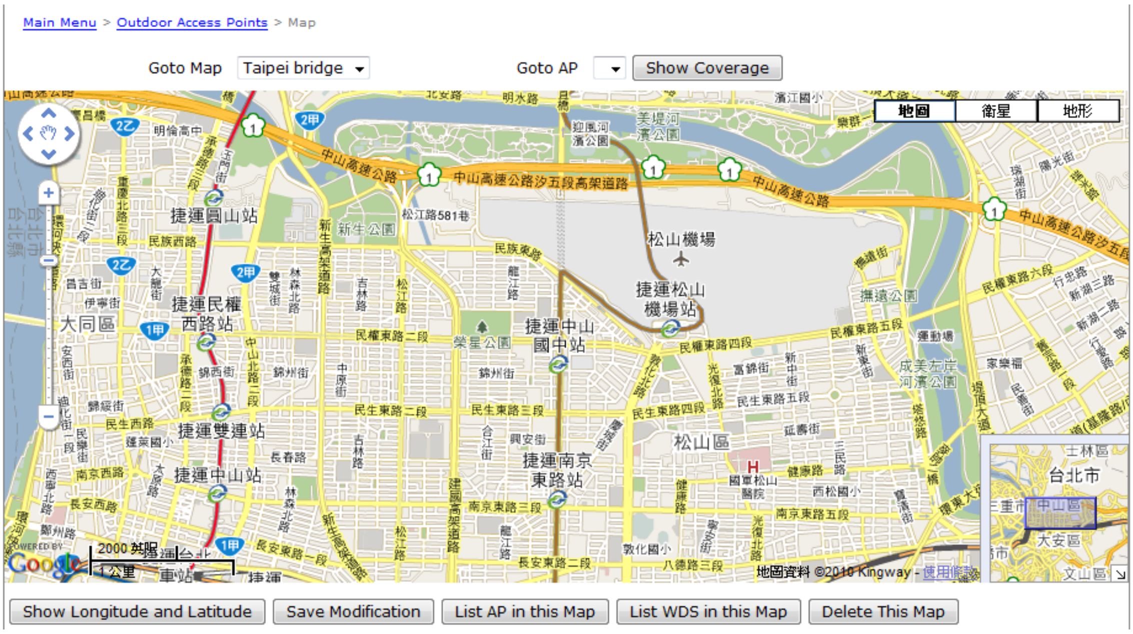
Now, return to the **Map** tab page in EWS Controller’s WMI and Scroll down to the bottom of the page, click on the **Add a New Map** button.



MAP Configuration

Map Name	Taipei Bridge
Latitude	25
Longitude	121
Google Maps Registration Key	AIzaSyDzjF1tWlf6158aJw7zGAxBYscY-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.



Main Menu > Outdoor Access Points > Map

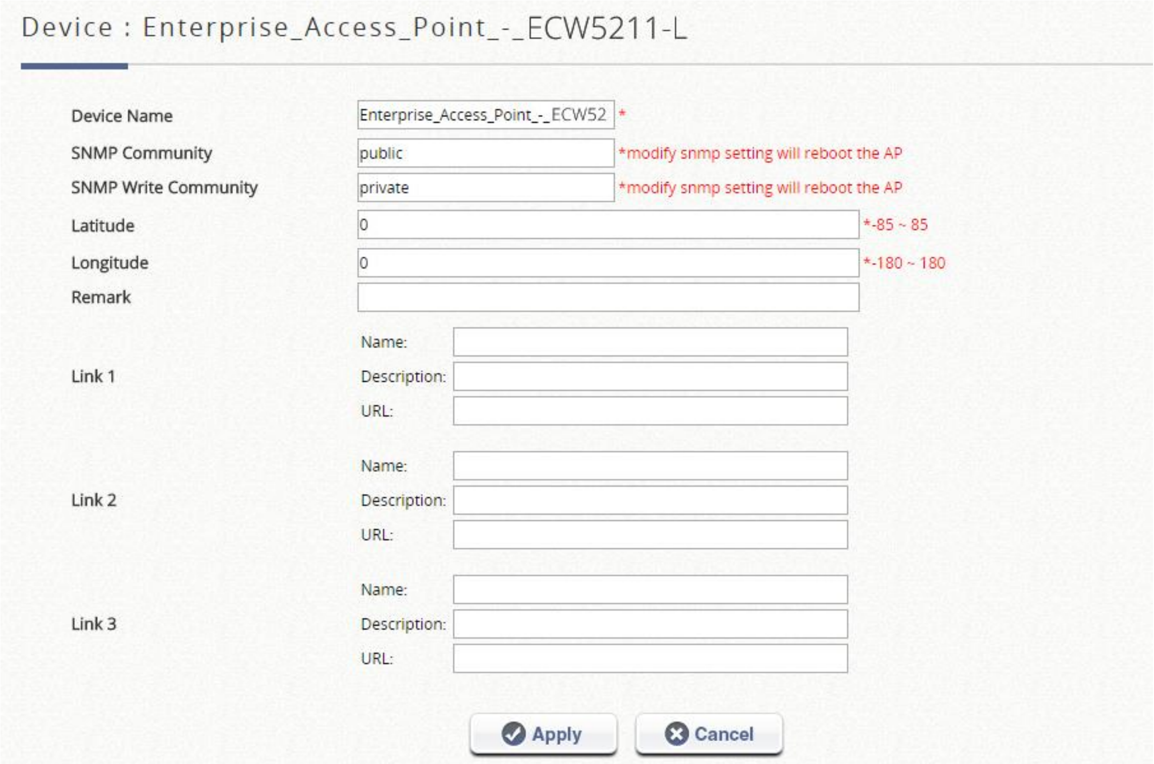
Goto Map: Taipei bridge

Goto AP
Show Coverage
地圖
衛星
地形
松山機場
捷運松山機場站
大同區
松山區
台北市
Show Longitude and Latitude
Save Modification
List AP in this Map
List WDS in this Map
Delete This Map

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.



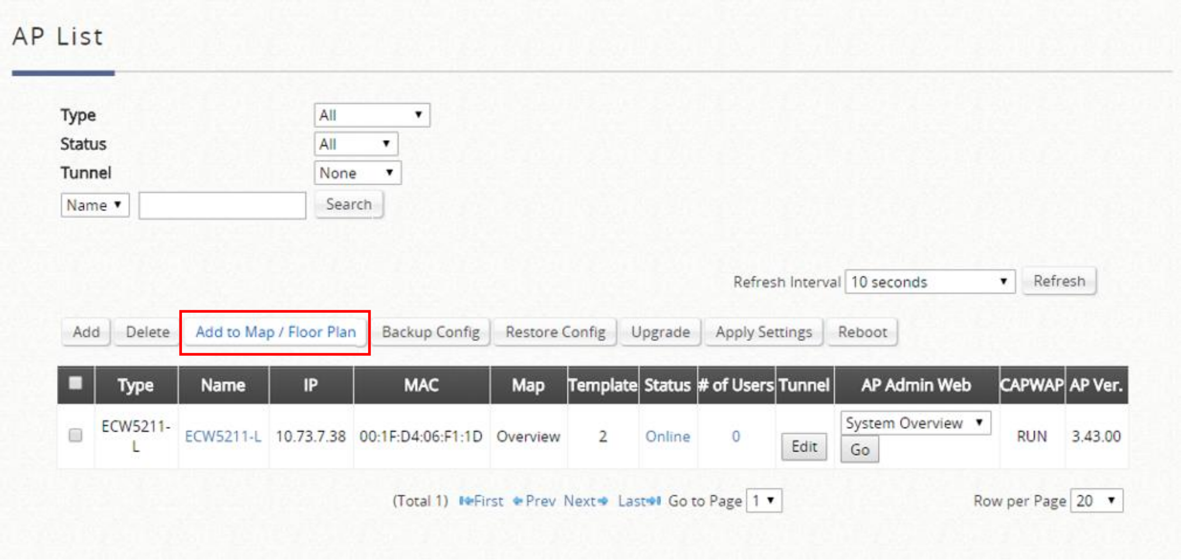
Device : Enterprise_Access_Point_-_ECW5211-L

Device Name	Enterprise_Access_Point_-_ECW52 *
SNMP Community	public *modify snmp setting will reboot the AP
SNMP Write Community	private *modify snmp setting will reboot the AP
Latitude	0 *-85 ~ 85
Longitude	0 *-180 ~ 180
Remark	
Link 1	Name: Description: URL:
Link 2	Name: Description: URL:
Link 3	Name: Description: URL:

Apply
Cancel

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

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



AP List

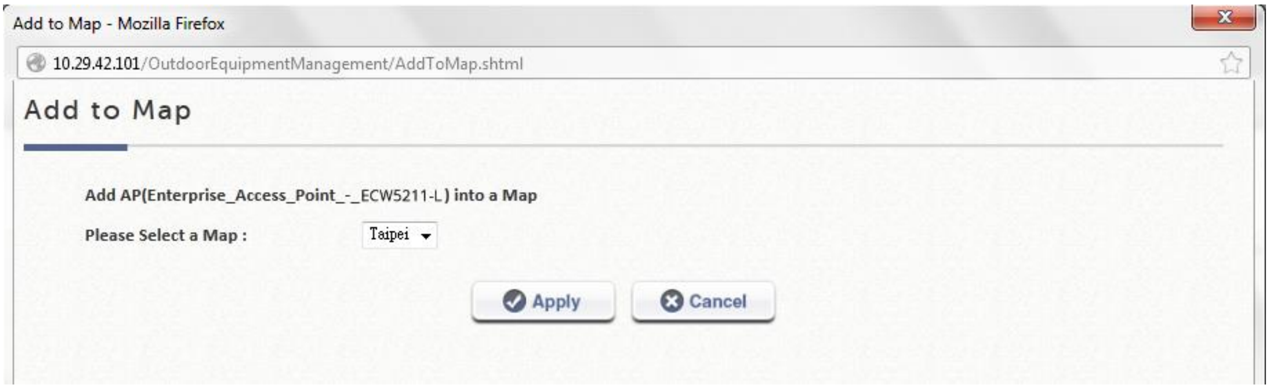
Type: All
Status: All
Tunnel: None

Name ▾
Search
Refresh Interval 10 seconds ▾
Refresh
Add
Delete
Add to Map / Floor Plan
Backup Config
Restore Config
Upgrade
Apply Settings
Reboot

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

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

⇩


Add to Map - Mozilla Firefox
10.29.42.101/OutdoorEquipmentManagement/AddToMap.shtml

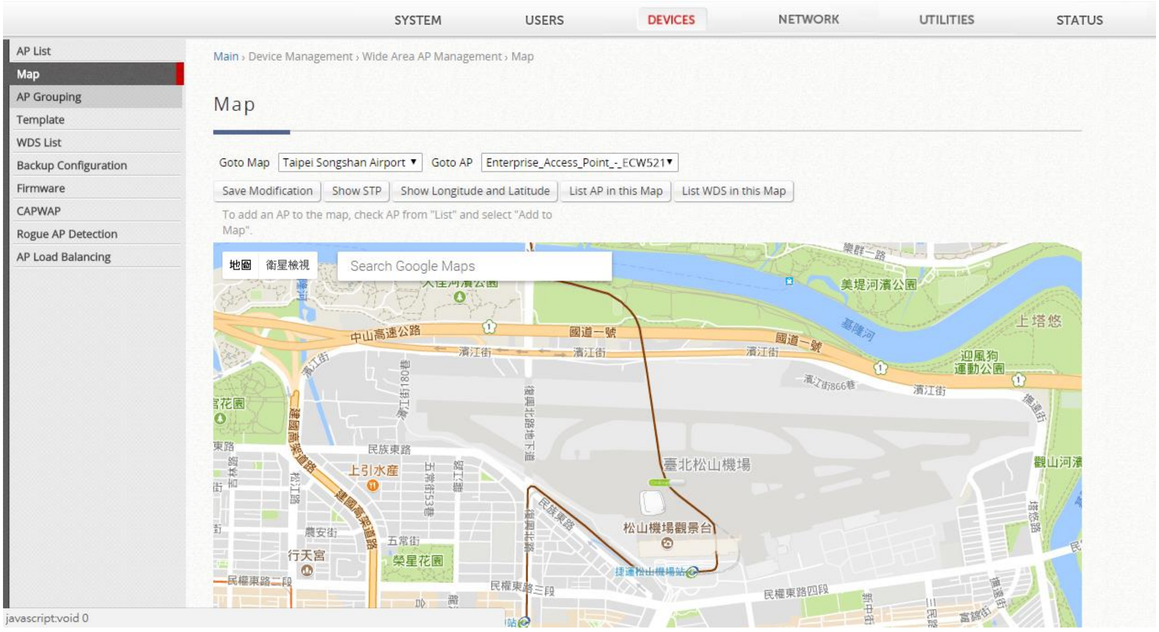
Add to Map

Add AP(Enterprise_Access_Point_-_ECW5211-L) into a Map

Please Select a Map : Taipei

Apply
Cancel

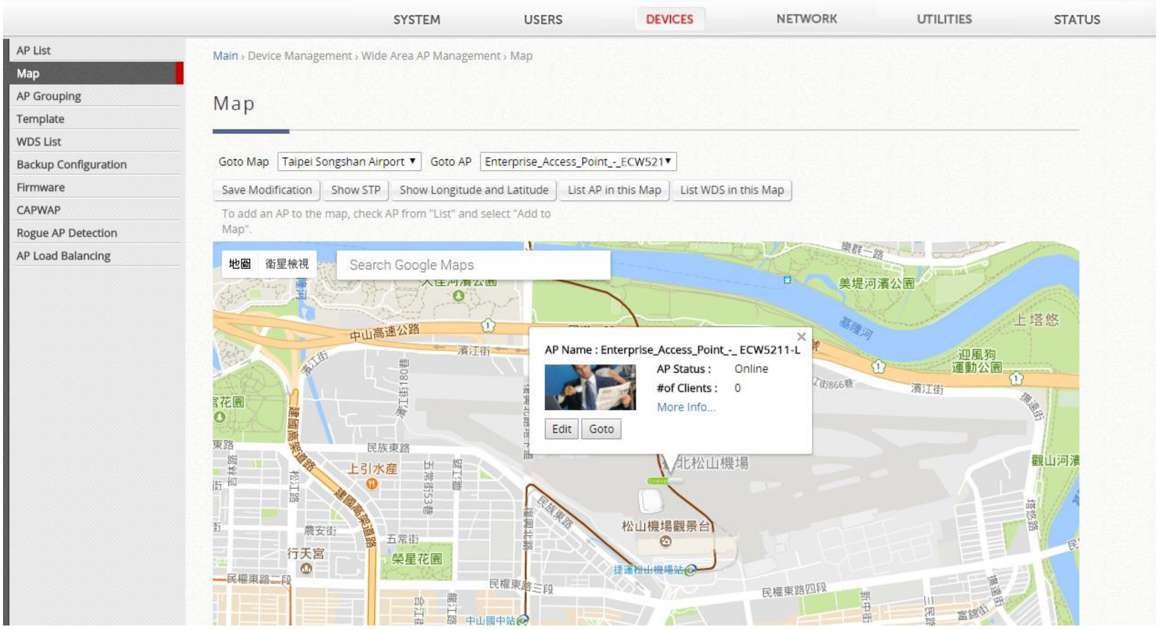
The selected APs will show up as marker images on the map at the physical coordinates configured, as shown below.


SYSTEM
USERS
DEVICES
NETWORK
UTILITIES
STATUS
AP List
Map
AP Grouping
Template
WDS List
Backup Configuration
Firmware
CAPWAP
Rogue AP Detection
AP Load Balancing
Main › Device Management › Wide Area AP Management › Map
Map
Save Modification
Show STP
Show Longitude and Latitude
List AP in this Map
List WDS in this Map
地圖
衛星檢視
Search Google Maps
臺北松山機場
松山機場觀景台
javascript:void 0

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

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

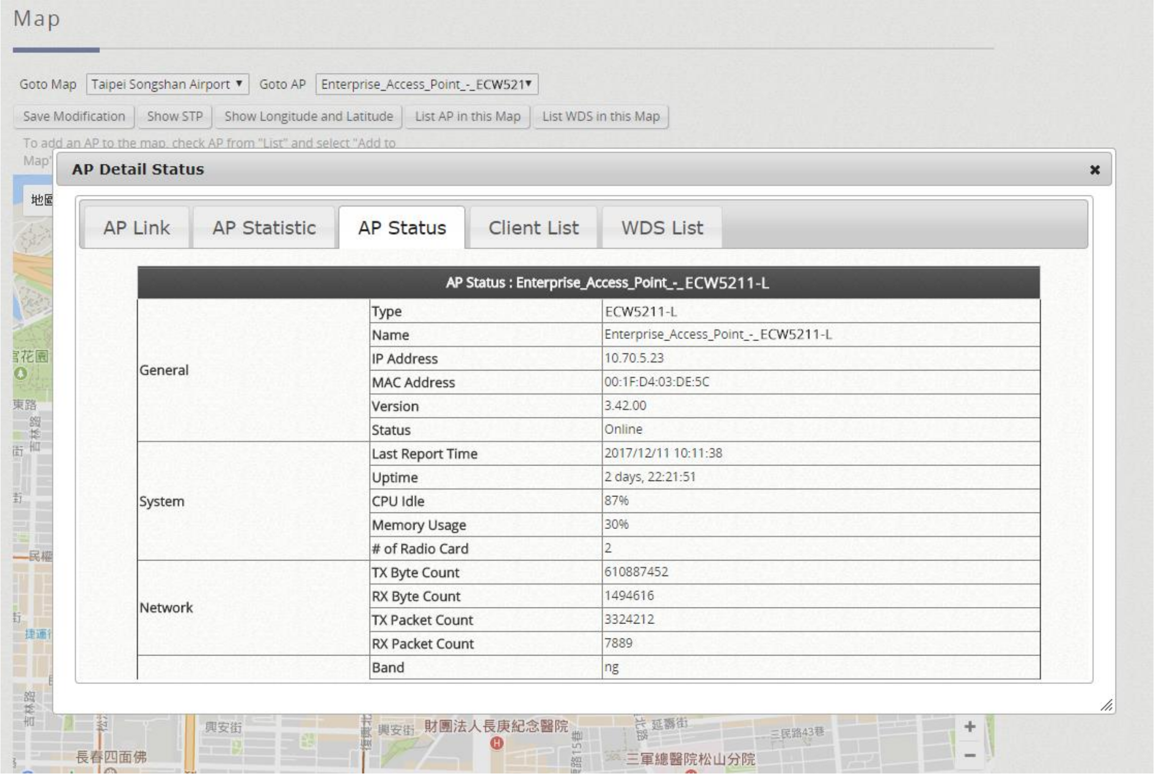
Administrators are able to click on the AP icon to see the dialogue box for additional information or links that you have configured. Besides, administrators can click the **more info** link for information on **AP Link**, **AP Statistic**, **AP Status**, **Client List**, **WDS List** and **Links** related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


SYSTEM
USERS
DEVICES
NETWORK
UTILITIES
STATUS
AP List
Map
AP Grouping
Template
WDS List
Backup Configuration
Firmware
CAPWAP
Rogue AP Detection
AP Load Balancing
Main › Device Management › Wide Area AP Management › Map
Map
Save Modification
Show STP
Show Longitude and Latitude
List AP in this Map
List WDS in this Map
地圖
衛星檢視
Search Google Maps
More Info...
Edit
Goto

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

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

AP Name : Enterprise_Access_Point_-_ECW5211-L
AP Status : Online
#of Clients : 0


Map
Save Modification
Show STP
Show Longitude and Latitude
List AP in this Map
List WDS in this Map
AP Detail Status
AP Link
AP Statistic
AP Status
Client List
WDS List

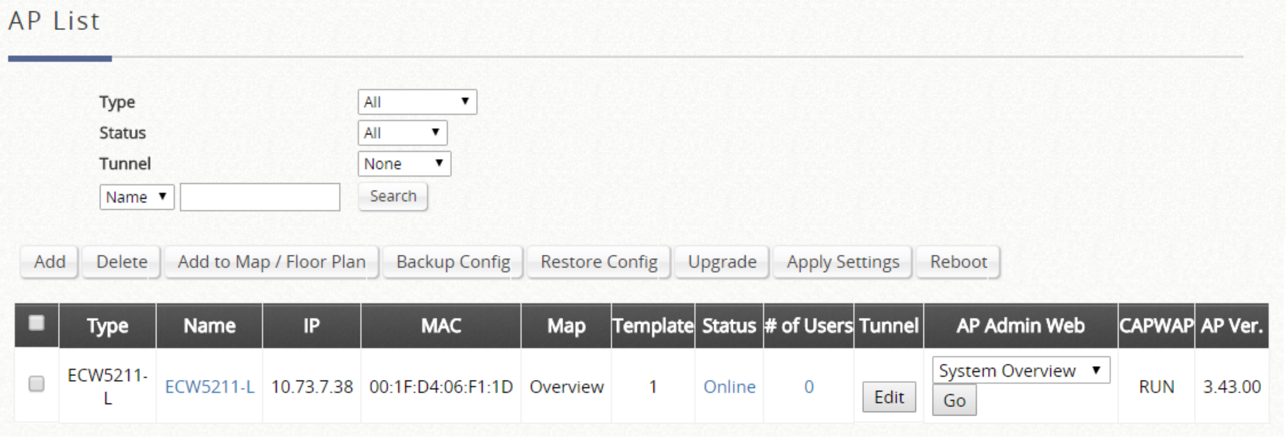
Goto Map: Taipei Songshan Airport
Goto AP: Enterprise_Access_Point_-_ECW521

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

b) 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.

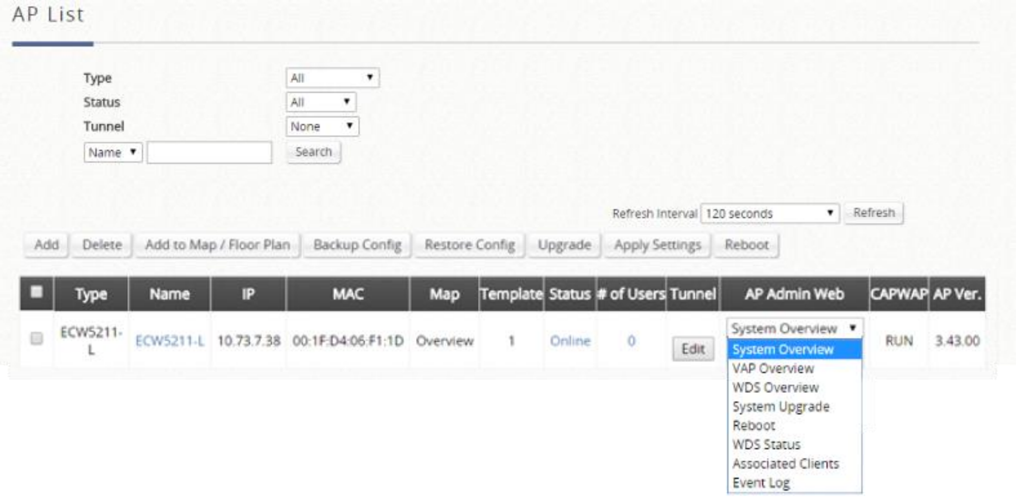

AP List
Search
Add
Delete
Add to Map / Floor Plan
Backup Config
Restore Config
Upgrade
Apply Settings
Reboot
Edit
Go

Type: All
Status: All
Tunnel: None
Name

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

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.


AP List
Search
Refresh
Add
Delete
Add to Map / Floor Plan
Backup Config
Restore Config
Upgrade
Apply Settings
Reboot
Edit
System Overview
System Overview
VAP Overview
WDS Overview
System Upgrade
Reboot
WDS Status
Associated Clients
Event Log

Type: All
Status: All
Tunnel: None
Name
Refresh Interval: 120 seconds

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

The drop down list on the column header is for specifying which WMI page to go to.

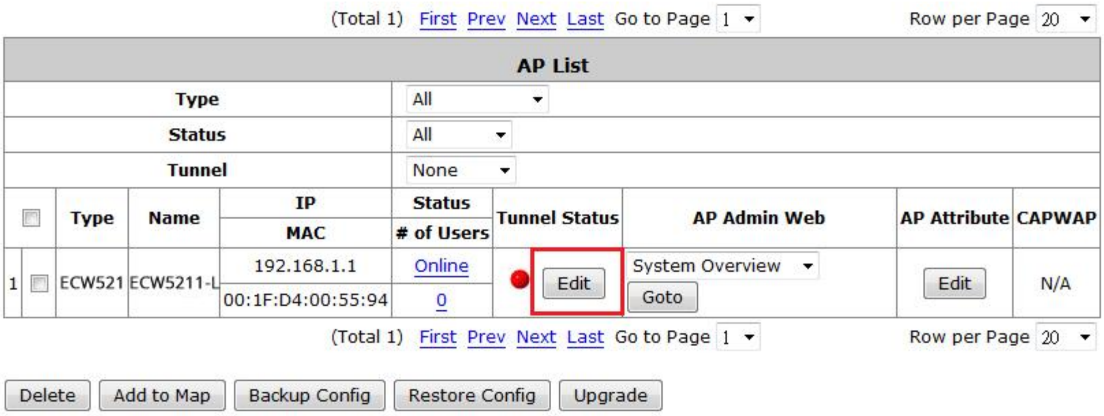
- **Edit (AP Name):** Click this button to enter the AP’s attribute editing page where administrator can specify the Device Name and SNMP community. If the AP is to be marked on a map, this page also allows administrator to configure the geographical location, coverage, related links and customize marker or icon images that will be displayed on the map.
- **Edit (Tunnel Status):** This function is used with Port Location Mapping on the EWS Controller for setting up a secure tunnel between the Controller and the listed AP. Once the tunnel has been established, the AP can be seen as logically connected under the EWS Controllers managed network with specific VLAN tags and can be applied as a Service Zone.
- **Delete:** Remove the checked AP from the List.

- **Add to Map:** Clicking this button will open a popup window. Administrator can Mark the selected APs on the Map chosen from the drop down list. If no map profile has been configured, there will be no available map 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 memory. 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 memory.
- **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.

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 AP and Controller.

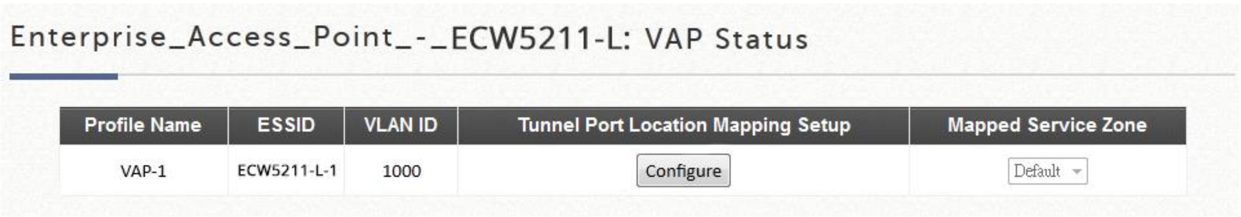
Go to: ***Main >> Access Points >> Wide Area AP Management >> List***.



Type	All
Status	All
Tunnel	None

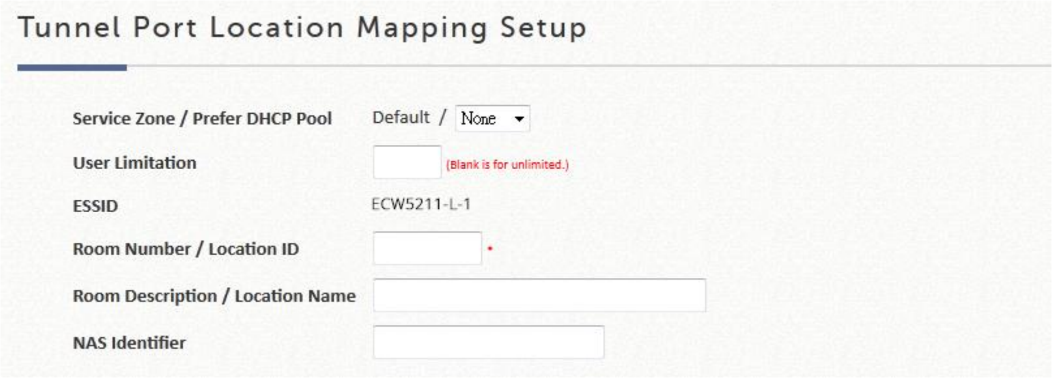
	☐	Type	Name	IP MAC	Status # of Users	Tunnel Status	AP Admin Web	AP Attribute	CAPWAP
1	☐	ECW521	ECW5211-L	192.168.1.1 00:1F:D4:00:55:94	Online 0	● Edit	System Overview Goto	Edit	N/A

⇩



Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
VAP-1	ECW5211-L-1	1000	Configure	Default

⇩



Tunnel Port Location Mapping Setup

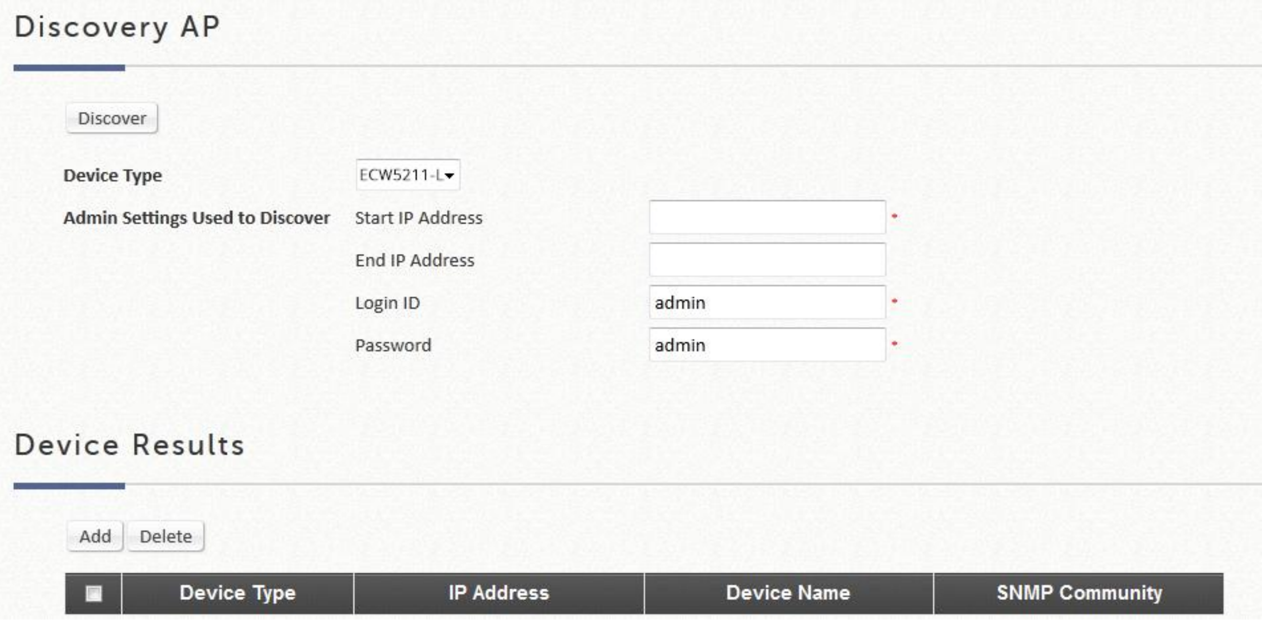
Service Zone / Prefer DHCP Pool	Default / None
User Limitation	(Blank is for unlimited.)
ESSID	ECW5211-L-1
Room Number / Location ID	*
Room Description / Location Name	
NAS Identifier	

- **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.

c) 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.



Discovery AP

Device Type: ECW5211-L

Admin Settings Used to Discover
Start IP Address:
End IP Address:
Login ID: admin
Password: admin

Device Results

☐	Device Type	IP Address	Device Name	SNMP Community

- **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:** The discovery new APs will be listed here. The administrator can click ***Add*** to register the APs to the List for management.

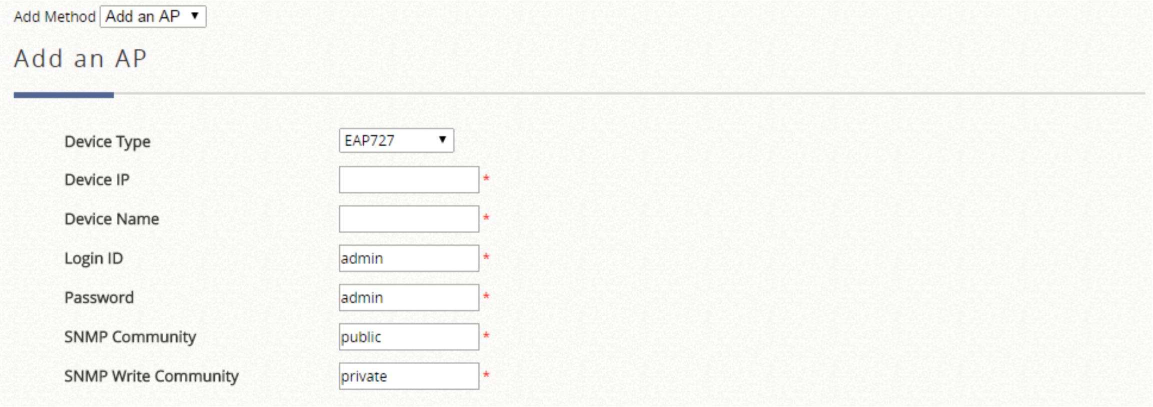
When the discovery process is complete, the APs found will be listed under the **Device Results** table. Here the administrator can specify the individual AP's **Device Name** and SNMP **Community** string. Click the Add button and the discovered APs will be added into **List**.

d) 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.



Add Method: Add an AP

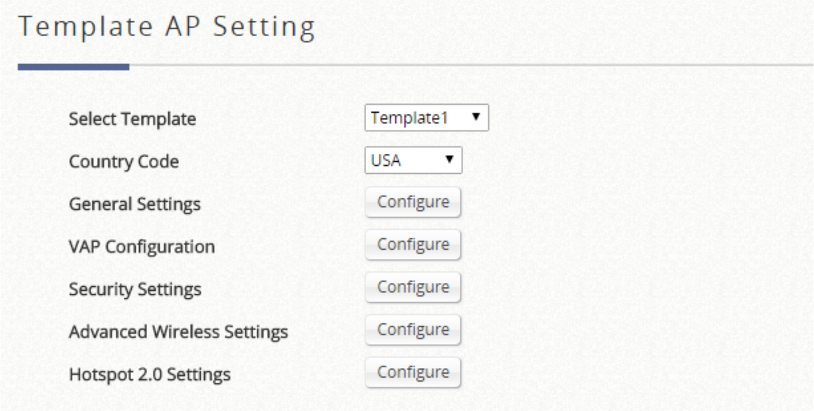
Add an AP

Device Type	EAP727
Device IP	*
Device Name	*
Login ID	admin *
Password	admin *
SNMP Community	public *
SNMP Write Community	private *

- ➢ **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.

e) Template

Configuration with templates is supported on selectable AP Models.

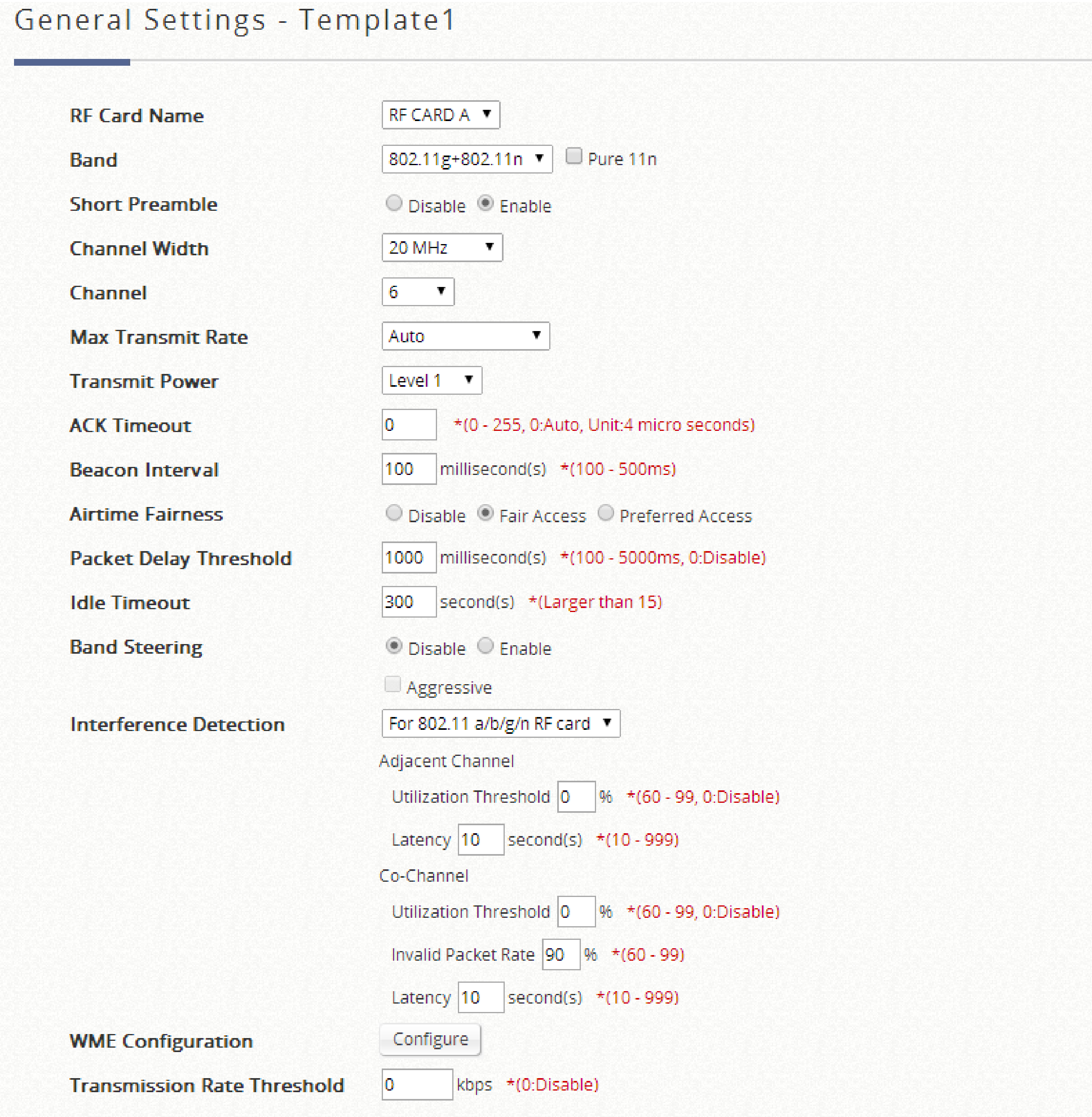


Template AP Setting

Select Template	Template1
Country Code	USA
General Settings	Configure
VAP Configuration	Configure
Security Settings	Configure
Advanced Wireless Settings	Configure
Hotspot 2.0 Settings	Configure

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**



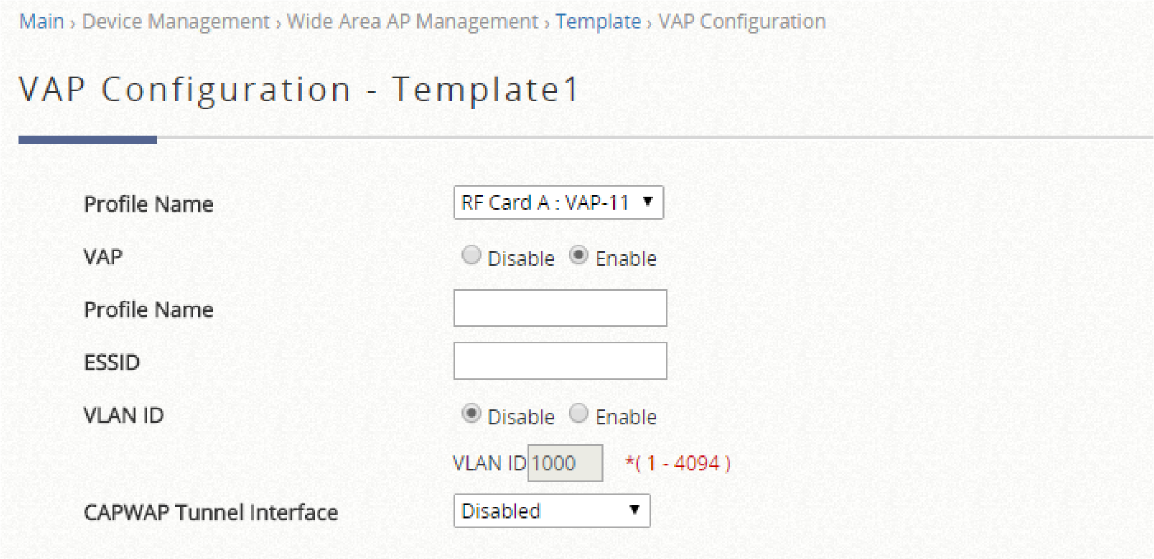
General Settings - Template1

RF Card Name: RF CARD A
Band: 802.11g+802.11n ☐ Pure 11n
Short Preamble: ○ Disable ● Enable
Channel Width: 20 MHz
Channel: 6
Max Transmit Rate: Auto
Transmit Power: Level 1
ACK Timeout: 0 *(0 - 255, 0:Auto, Unit:4 micro seconds)
Beacon Interval: 100 millisecond(s) *(100 - 500ms)
Airtime Fairness: ○ Disable ● Fair Access ○ Preferred Access
Packet Delay Threshold: 1000 millisecond(s) *(100 - 5000ms, 0:Disable)
Idle Timeout: 300 second(s) *(Larger than 15)
Band Steering: ● Disable ○ Enable
☐ Aggressive
Interference Detection: For 802.11 a/b/g/n RF card
Adjacent Channel
Utilization Threshold 0 % *(60 - 99, 0:Disable)
Latency 10 second(s) *(10 - 999)
Co-Channel
Utilization Threshold 0 % *(60 - 99, 0:Disable)
Invalid Packet Rate 90 % *(60 - 99)
Latency 10 second(s) *(10 - 999)
WME Configuration: Configure
Transmission Rate Threshold: 0 kbps *(0:Disable)

- **RF Card Name:** Select an RF Card for your AP.
- **Band:** Depending on the AP model template you are editing, there are different modes to select, **802.11a, 802.11b**, **802.11g, 802.11a+802.11n, 802.11b+802.11g**, **802.11g+802.11n** and **802.11ac**.
- **Short Preamble:** The short preamble with a 56-bit synchronization field can improve WLAN transmission efficiency. Select *Enable* to use Short Preamble or *Disable* to use Long Preamble with a 128-bit synchronization field.
- **Channel Width (802.11g+n, 802.11a+n and 802.11ac only):** Choose between 20MHz, 40MHz or Auto. Doubling channel bandwidth to 40 MHz is supported to enhance throughput. 80MHz is available for selection in 802.11ac mode.

- **Channel:** Select the appropriate *channel* from the drop-down menu to correspond with your network settings.
- **Max Transmit Rate:** The default is set to **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to allow the Access Point to automatically use the fastest rate possible. For 802.11n the selectable data rates range from MCS0 to MCS15, and for 802.11ac, select data rates up to MCS9.
- **Transmit Power:** On select AP models, the signal strength transmitted from the system can be selected by Levels. Each level signifies a decrement of 1 dBm from the highest power. **Level 1** is the actual highest power, **Level 2** is the highest power minus 1 dBm, so on and so forth.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal is transmitted between the access point and the wireless network.
- **ACK Timeout:** The time interval for waiting for the “acknowledgement (ACK) frame”. If the ACK is not received within the interval then the packet will be re-transmitted. Higher ACK Timeout interval will decrease the packet lost, but the throughput will be decreased/worsened.
- **Airtime Fairness:** When set to “Fair Access”, this feature ensures all devices with different band compatibilities have the same air time. When set to “Preferred Access”, N clients are prioritized. This feature is ideal for networks with devices supporting different bands.
- **Packet Delay Threshold (ms):** This is the Tx Queue flushing mechanism, which purpose is to drop packets and immediately process others if the queue has been processed for more than x milliseconds. This is disabled by default (=0).
- **Idle Timeout (s):** Clients disconnects when inactivity reaches the configured amount of time in seconds, where default = 300s.
- **Band Steering:** When enabled, clients with 5GHz connectivity will be steered towards the 5GHz band to reduce congestion in the 2.4GHz band. This is applicable only when the AP is set to 2.4GHz and 5GHz on the 2 RF Cards. When “Aggressive” is checked, clients with 5GHz connectivity are forced to connect to the 5GHz band.
- **Interference Detection:** When utilization of the current channel reaches the configured threshold (in %), the AP switches to a different Channel.
- **Transmission Rate Threshold:** The associated client will be kicked when transmission rate is lower than the configured threshold. This ensures high connection speed for all associated clients.
- **WME Configuration:** Access priority can be configured using with different parameters. CW Min: Contention Window Minimum, CW Max: Contention Window Maximum, AIFS: Arbitration Inter Frame Spacing, TXOP Limit: Transmission Opportunity Limit.

➢ VAP Configuration



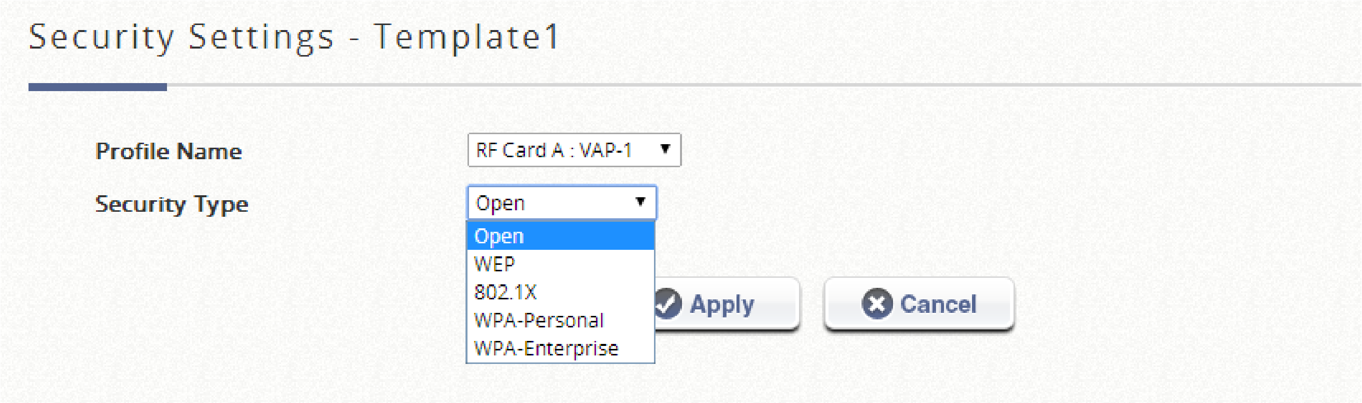
Main › Device Management › Wide Area AP Management › Template › VAP Configuration

VAP Configuration - Template1

Profile Name	RF Card A : VAP-11 ▼
VAP	○ Disable ● Enable
Profile Name	
ESSID	
VLAN ID	● Disable ○ Enable VLAN ID 1000 *(1 - 4094)
CAPWAP Tunnel Interface	Disabled ▼

- **VAP: *Enable*** or ***Disable*** this VAP.
- **Profile Name:** The profile name of a specific RF card and its VAP for identity / management purposes.
- **ESSID:** ESSID (Extended Service Set ID) serves as an identifier for clients to associate with the specific VAP. It can be coupled with different service levels like a variety of wireless security types.
- **VLAN ID:** The Edgecore Access Point supports tagged VLANs (virtual LANs). To enable VLAN function, each VAP shall be given a unique VLAN ID with valid values ranging from 1 to 4094. Once VLAN is Enabled, QoS is supported on the VAP.
- **CAPWAP Tunnel Interface:** Select dropdown to designate traffic for the VAP to pass through CAPWAP Tunnel established between the AP and the controller. When CAPWAP Tunnel Interface is “Complete” or “Split Tunnel”, you may then select the Service Zone to be mapped to this VAP.

➢ **Security Settings**

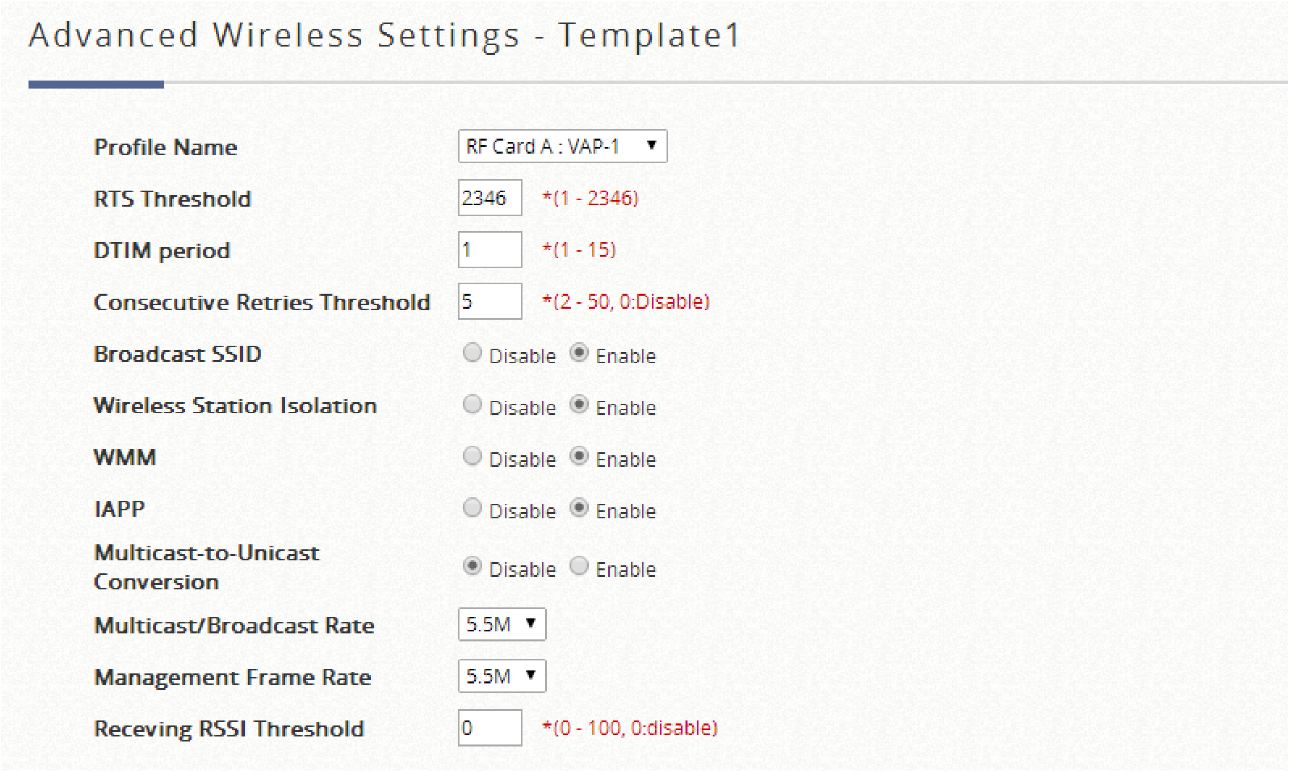


Security Settings - Template1

Profile Name	RF Card A : VAP-1 ▼
Security Type	Open ▼

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

- **Advanced Wireless Settings**



Advanced Wireless Settings - Template1

Profile Name	RF Card A : VAP-1 ▼	
RTS Threshold	2346	*(1 - 2346)
DTIM period	1	*(1 - 15)
Consecutive Retries Threshold	5	*(2 - 50, 0:Disable)
Broadcast SSID	○ Disable ● Enable	
Wireless Station Isolation	○ Disable ● Enable	
WMM	○ Disable ● Enable	
IAPP	○ Disable ● Enable	
Multicast-to-Unicast Conversion	● Disable ○ Enable	
Multicast/Broadcast Rate	5.5M ▼	
Management Frame Rate	5.5M ▼	
Receving RSSI Threshold	0	*(0 - 100, 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.
- **WMM:** The default is *Disable.* Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes

wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.

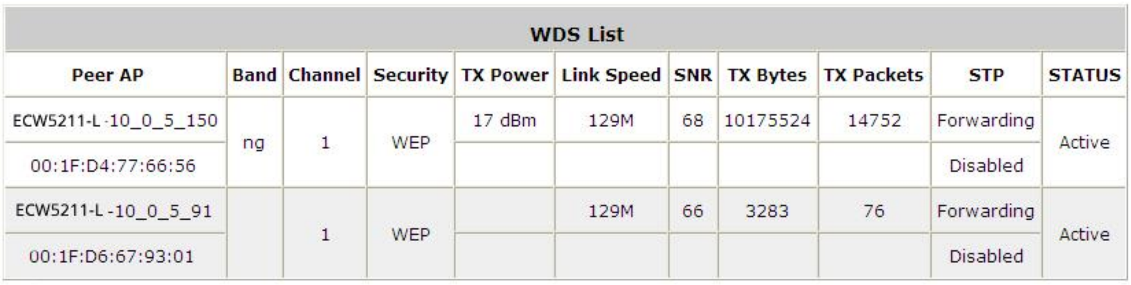
<To receive the benefits of WMM QoS>

- The application must support WMM.
- WMM shall be enabled on the Access Point.
- WMM shall be enabled in the wireless adapter on client's computer.

- **IAPP:** IAPP (Inter Access Point Protocol) is a protocol by which access points share information about the stations connected to them. When this function is enabled, the system will automatically broadcast information of associated wireless stations to its peer access points. This will help wireless stations roam smoothly among IAPP-enabled access points in the same wireless LAN.
- **Multicast-to-Unicast Conversion:** When Multicast-to-Unicast Conversion is enabled, the Access Point intelligently forwards traffic only to those ports that request multicast traffic. Adversely, when disabled, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.
- **Multicast/Broadcast Rate:** Bandwidth configuration for multicast/broadcast packets. If your wireless clients require a larger or smaller bandwidth for sending multicast/ broadcast packets, the administrator can customize the Access Point's multicast/ broadcast bandwidth here.
- **Management Frame Rate:** This feature controls the bandwidth for Management Frames. The higher the rate it, the shorter range the transmission covers
- **Receiving RSSI Threshold:** To ensure connected stations have quality connection speeds, a station will not be able to associate to the network unless its receiving sensitivity meets the configured threshold.

f) 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, SNR, TX Bytes, TX Packets, STP and Status.



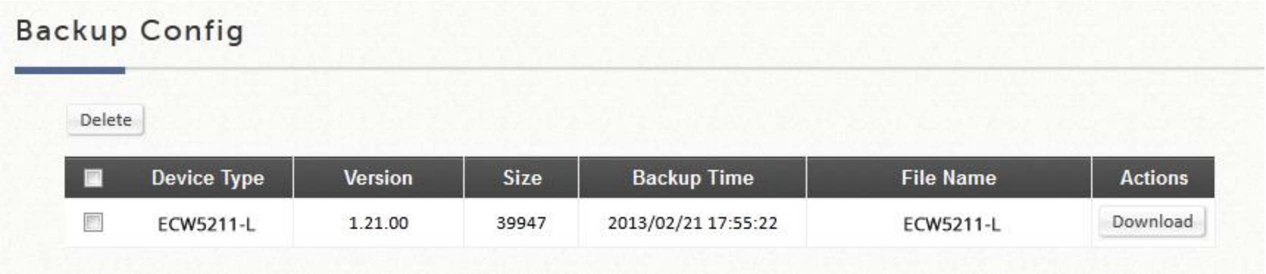
WDS List

Peer AP	Band	Channel	Security	TX Power	Link Speed	SNR	TX Bytes	TX Packets	STP	STATUS
ECW5211-L-10_0_5_150	ng	1	WEP	17 dBm	129M	68	10175524	14752	Forwarding	Active
00:1F:D4:77:66:56									Disabled	
ECW5211-L-10_0_5_91		1	WEP		129M	66	3283	76	Forwarding	Active
00:1F:D6:67:93:01									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.

g) Backup Config

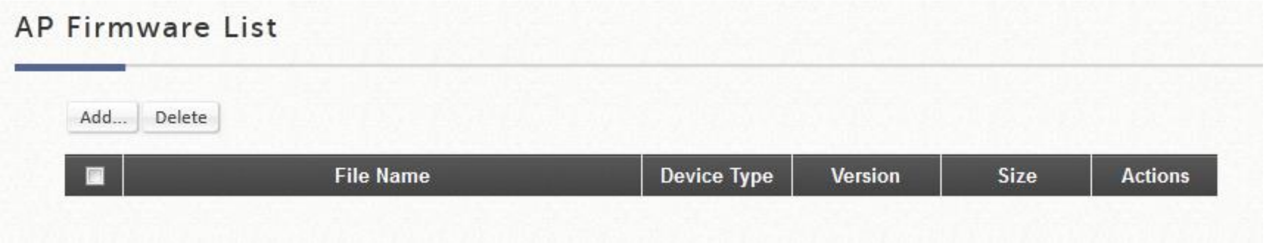
Backed up Config files can be used to restore an AP's settings in **List**. When administrator backs up an AP's configuration settings, all the backup files are listed on the **Backup Config** tab page and can be downloaded to a local storage device or deleted from EWS Controller's memory.



☐	Device Type	Version	Size	Backup Time	File Name	Actions
☐	ECW5211-L	1.21.00	39947	2013/02/21 17:55:22	ECW5211-L	Download

h) Firmware

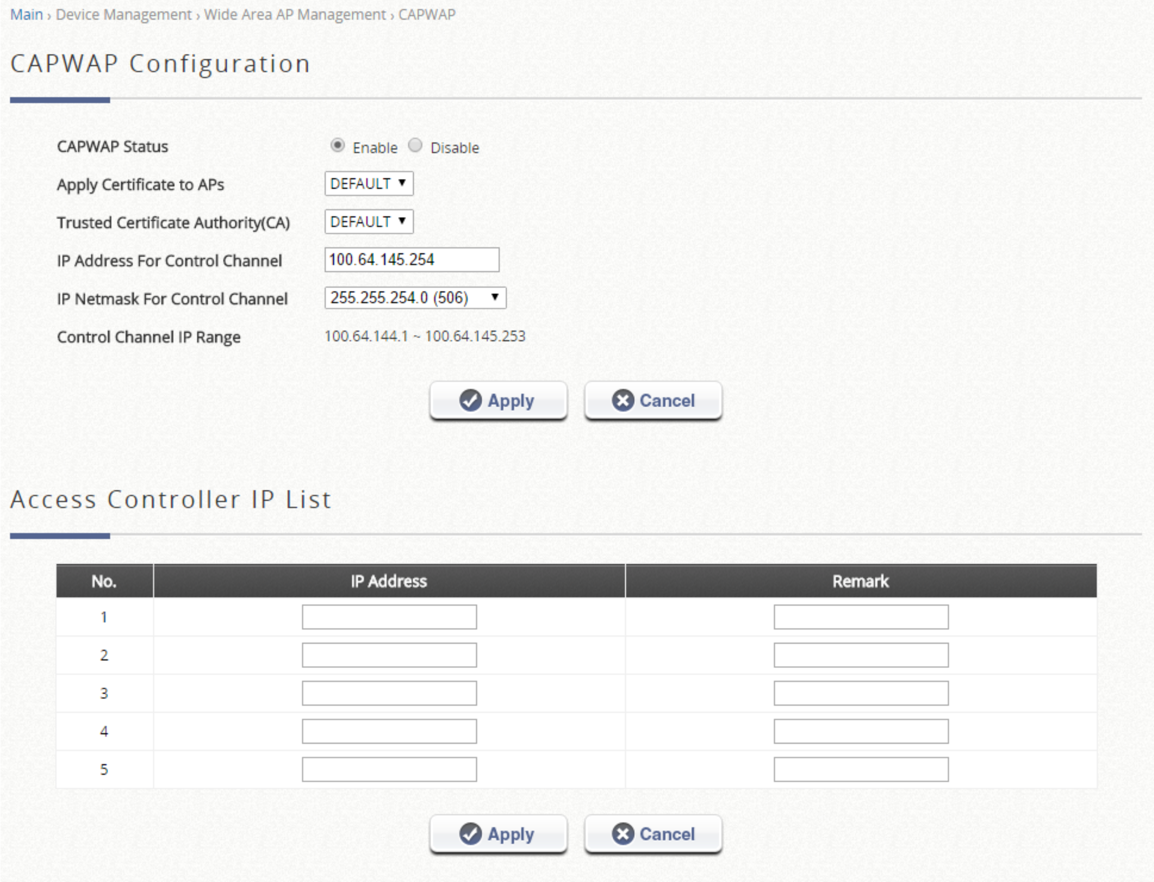
The EWS Controller can store AP's firmware in its' built-in memory. Under the **Firmware** tab page administrator can upload new AP firmware to the EWS Controller's memory allowing for easy remote AP upgrade and restore operations from the AP **List** page. The AP firmware listed under this page can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



☐	File Name	Device Type	Version	Size	Actions

i) 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	DEFAULT
Trusted Certificate Authority(CA)	DEFAULT
IP Address For Control Channel	100.64.145.254
IP Netmask For Control Channel	255.255.254.0 (506)
Control Channel IP Range	100.64.144.1 ~ 100.64.145.253

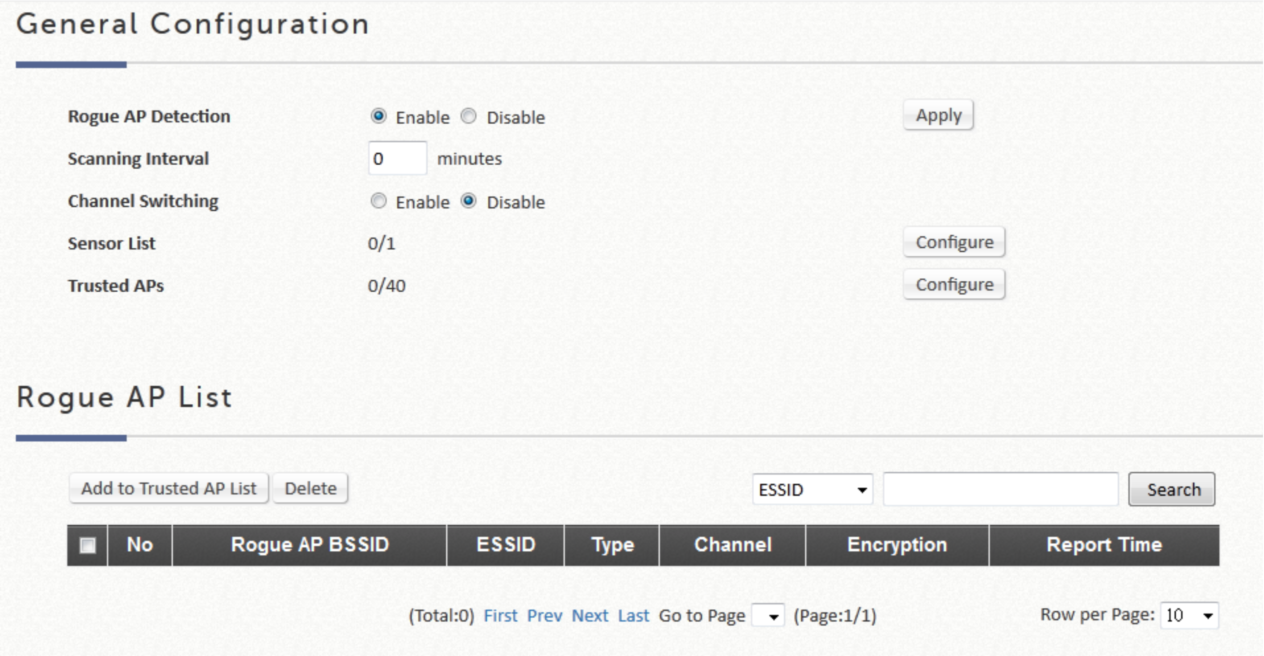
Access Controller IP List

No.	IP Address	Remark
1		
2		
3		
4		
5		

- **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.
- **Trusted Certificate Authority (CA):** This configuration item allows the administrator to select a Trust CA to validate the certificate used for CAPWAP.
- **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.

j) 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 ● Enable ○ Disable
Scanning Interval 0 minutes
Channel Switching ○ Enable ● Disable
Sensor List 0/1
Trusted APs 0/40

Rogue AP List

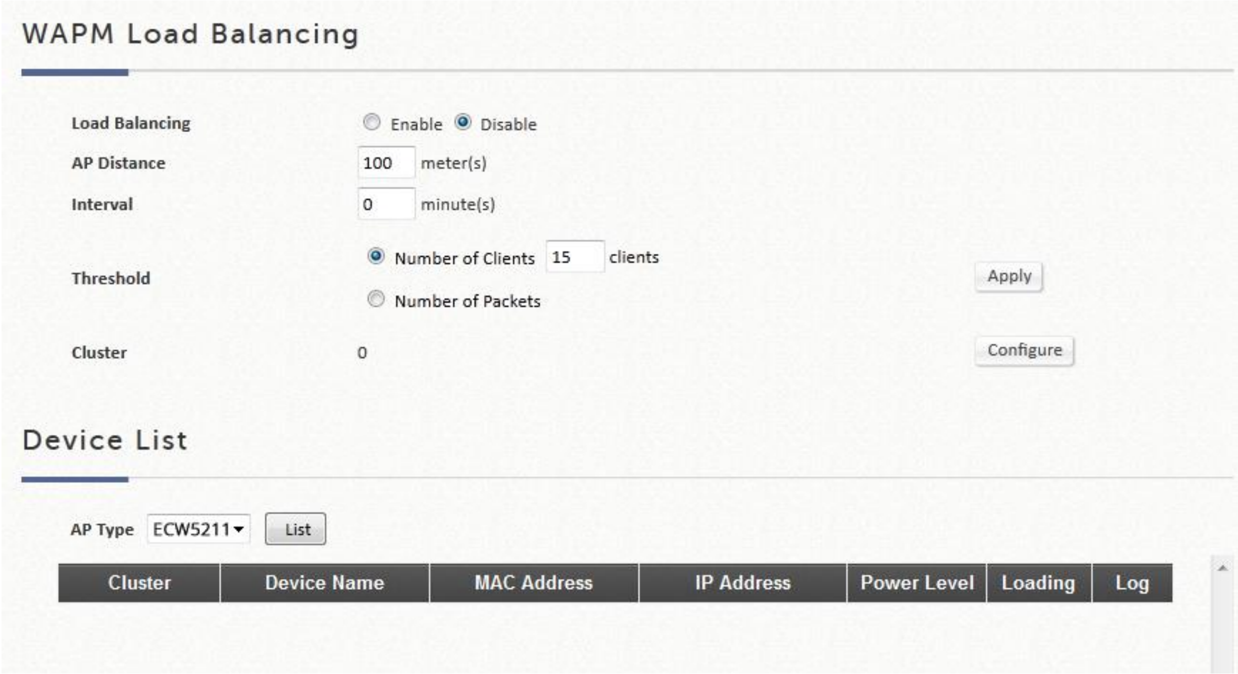
☐	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	Report Time

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

k) 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 100 meter(s)

Interval 0 minute(s)

Threshold ● Number of Clients 15 clients
○ Number of Packets

Cluster 0

Device List

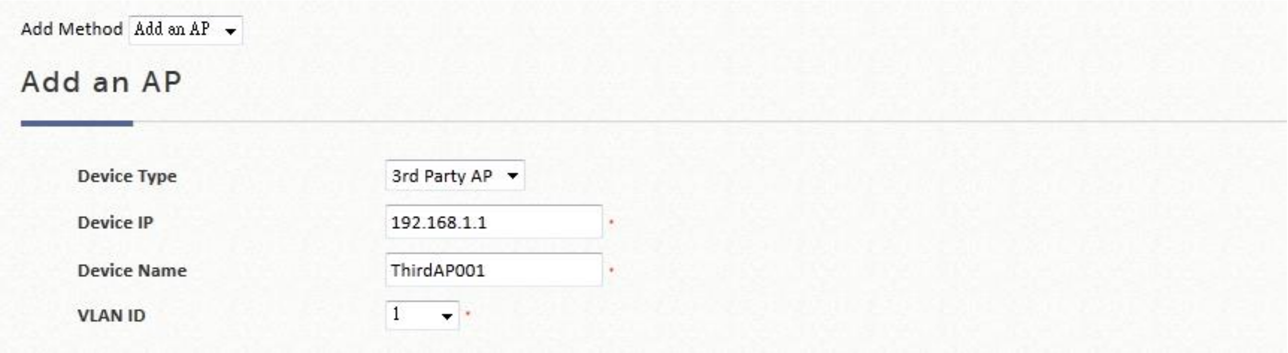
AP Type ECW5211

Cluster	Device Name	MAC Address	IP Address	Power Level	Loading	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.
- **Cluster:** This item when entered to its configuration page will display all the current AP groups and their status info.
- **Device List:** The scrollable window display all the managed APs sorted by model name with relative information such as Group, Name, MAC, IP, Power Lv, Loading, etc. The managed APs will have a Group column for indicating which AP group it belongs to for AP Load Balancing feature to be enforced.

I) Third Party AP Management

Add a third party AP by selecting THIRDAP 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: 3rd Party AP

Device IP: 192.168.1.1 *

Device Name: ThirdAP001 *

VLAN ID: 1 *

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

Manage this third party AP from the Type Lists. Edit its AP Attribute and Administration from the column.

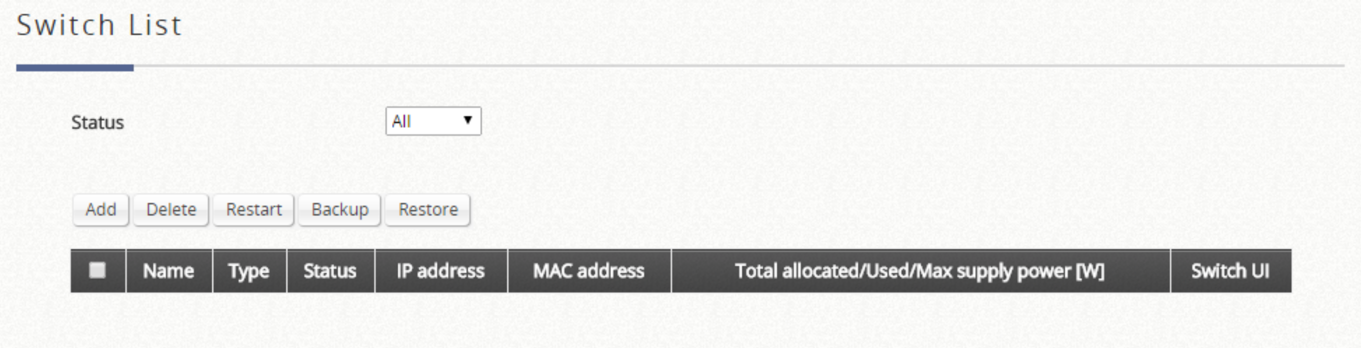
Go to Map icon. The added third party AP could also be placed on Google Map features and all map functions.

D. Switches

Switches: This section is used to configure all Switch Management related settings.

1) Switch List

The EWS Controller is capable of managing the Edgecore SW1024 switch. Switches under management of the system will be shown on this list.



■	Name	Type	Status	IP address	MAC address	Total allocated/Used/Max supply power [W]	Switch UI

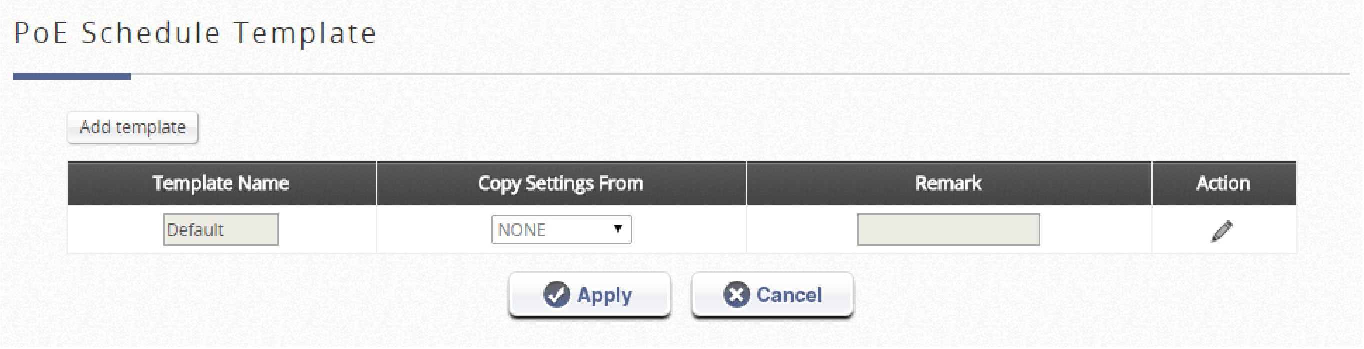
The Switch's name will be shown as a hyperlink. Click the hyperlink of each managed SW1024 for further configuration (General Setting, PoE Setting, VLAN Membership Setting, Port Setting, Poe Schedule) on the switch.

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.

2) PoE Schedule Template

The system supports up to a number of PoE Schedule Templates depending on your EWS model.



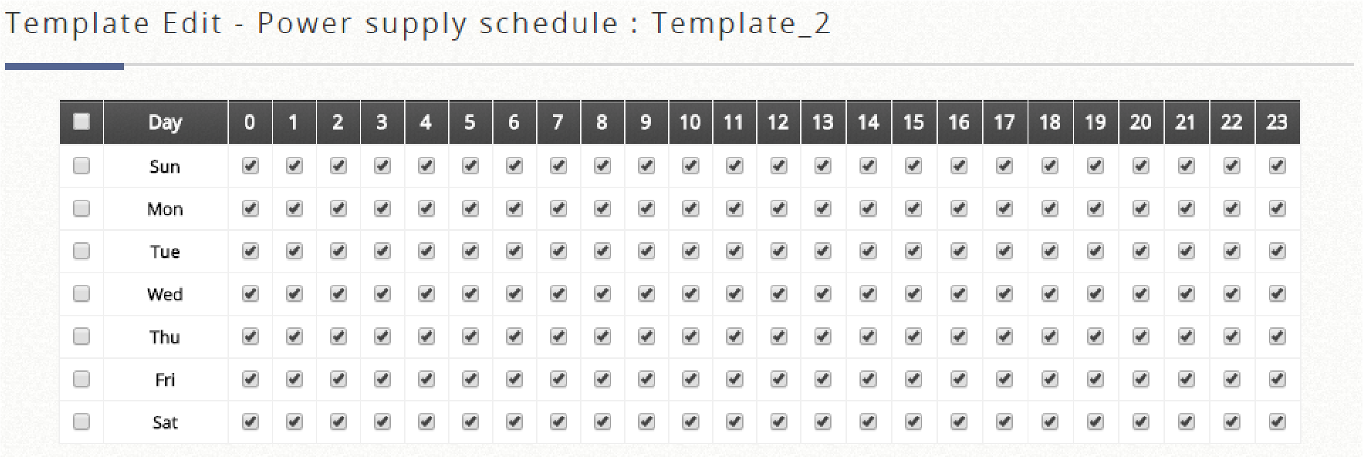
PoE Schedule Template

Template Name	Copy Settings From	Remark	Action
Default	NONE ▾		✎

The first template is the default template and cannot be deleted. The Template Name may be customized for easy reference (eg. 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:

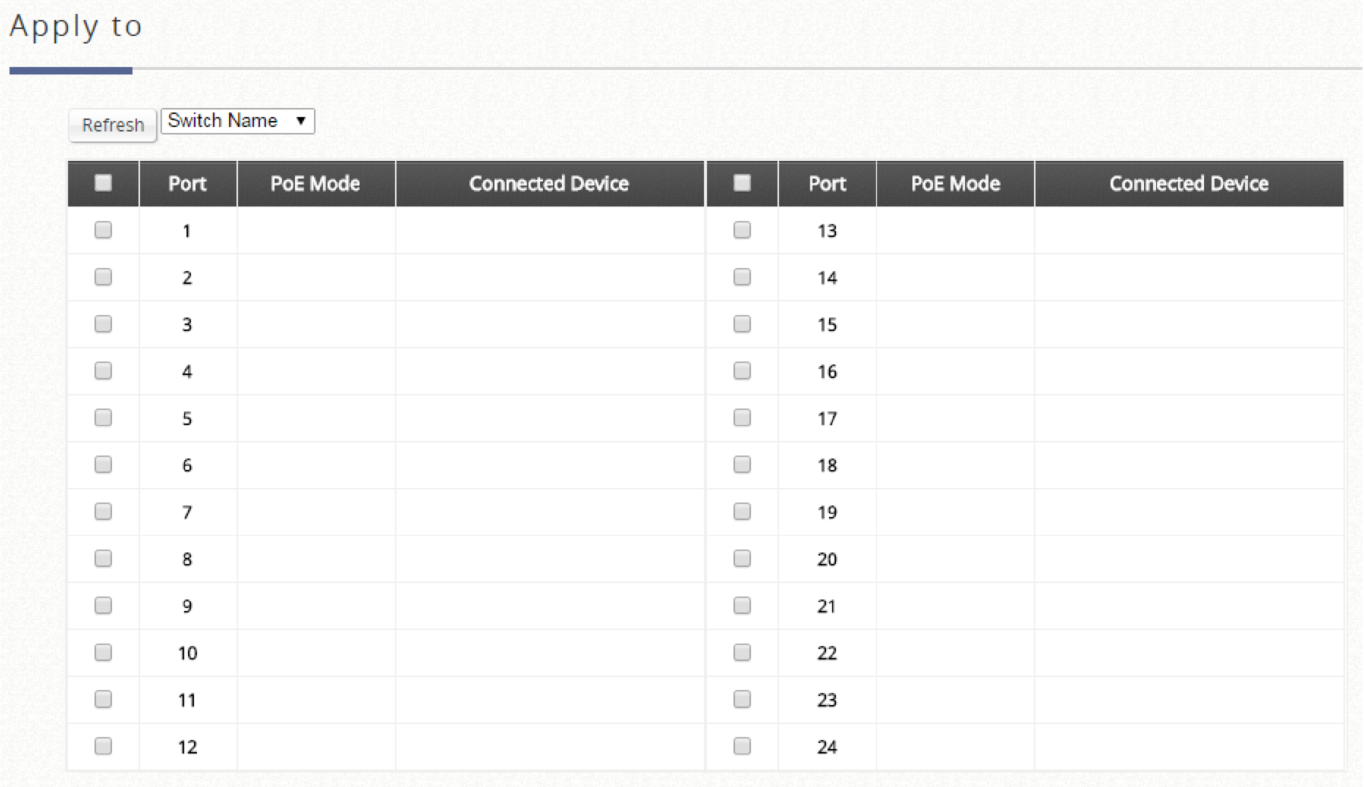
- Power Supply Schedule



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
☐	Sun	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	Mon	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	Tue	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	Wed	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	Thu	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	Fri	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	Sat	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

- Apply to: The band, channel width, transmit power and etc.



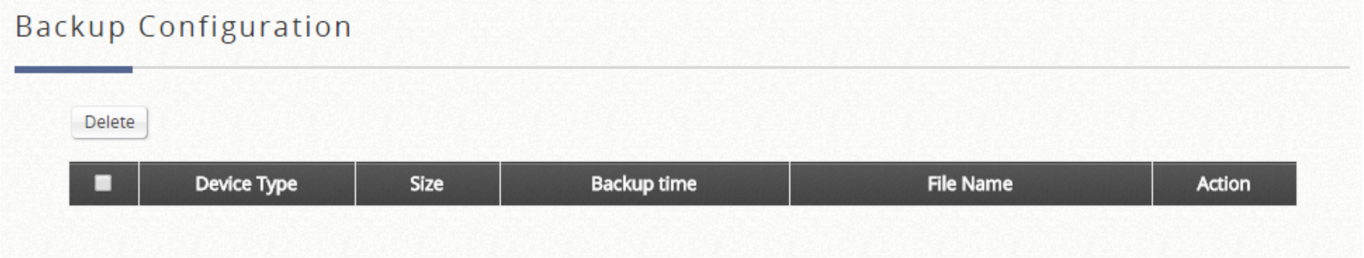
☐	Port	PoE Mode	Connected Device	☐	Port	PoE Mode	Connected Device
☐	1			☐	13		
☐	2			☐	14		
☐	3			☐	15		
☐	4			☐	16		
☐	5			☐	17		
☐	6			☐	18		
☐	7			☐	19		
☐	8			☐	20		
☐	9			☐	21		
☐	10			☐	22		
☐	11			☐	23		
☐	12			☐	24		

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.

3) Backup Configuration

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



☐	Device Type	Size	Backup time	File Name	Action

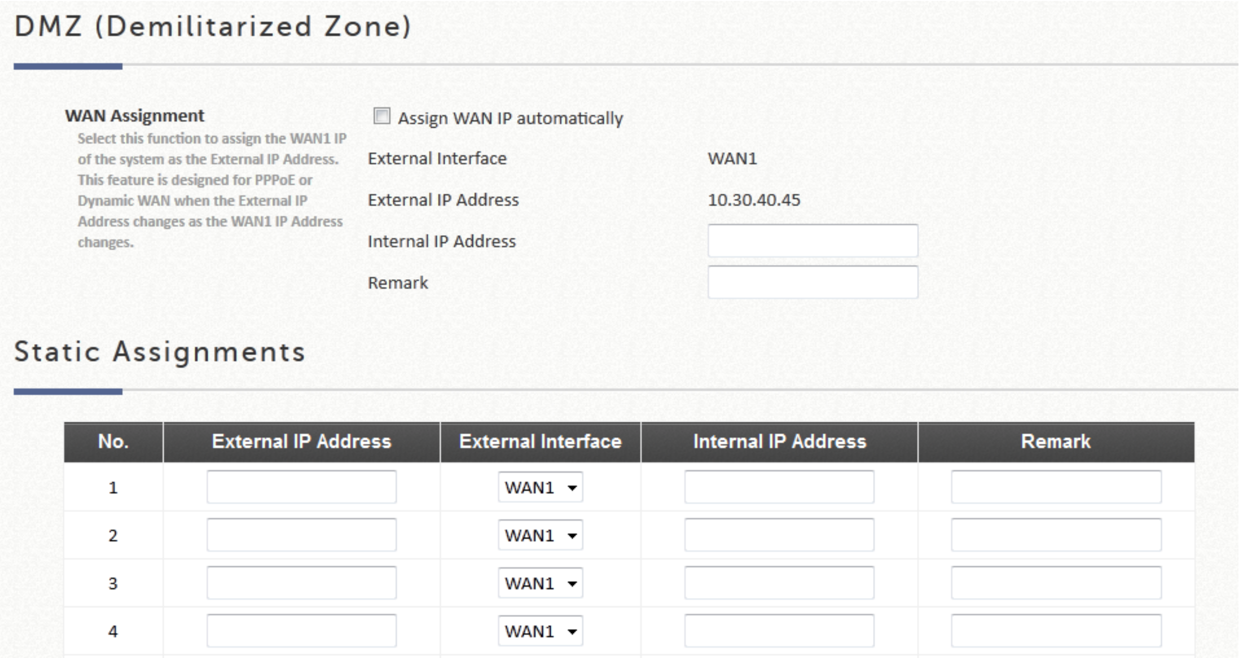
E. Network

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

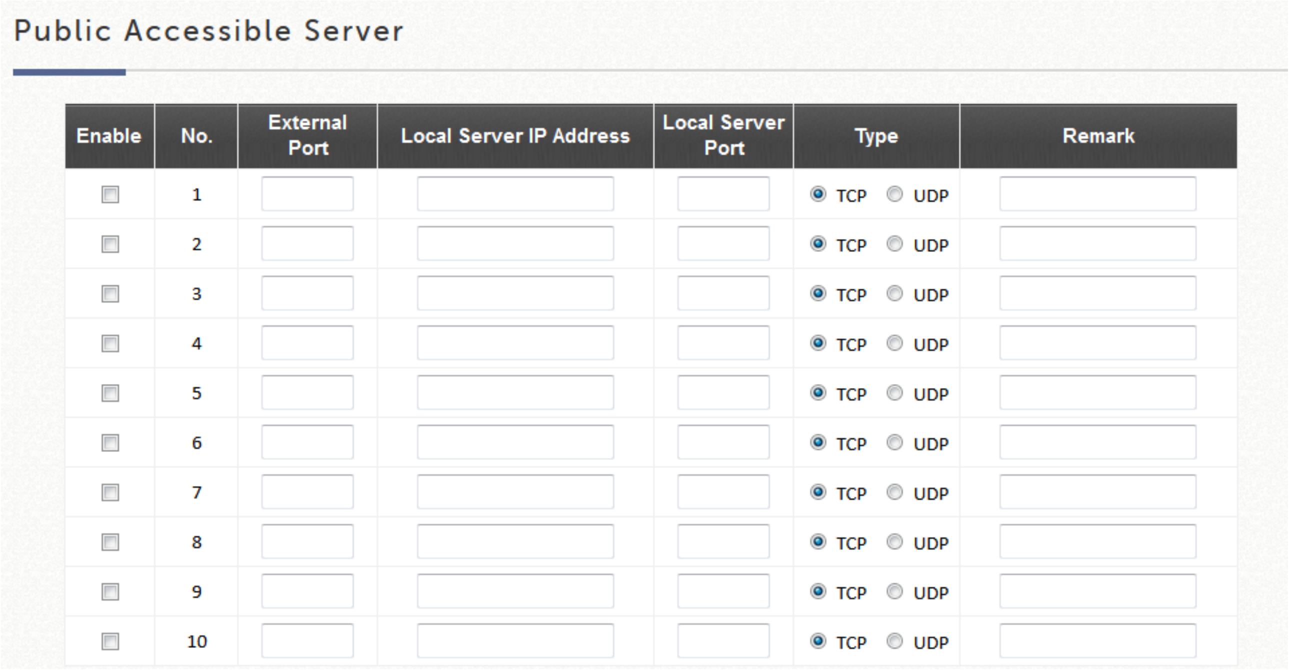
External Interface	WAN1
External IP Address	10.30.40.45
Internal IP Address	
Remark	

Static Assignments

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

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

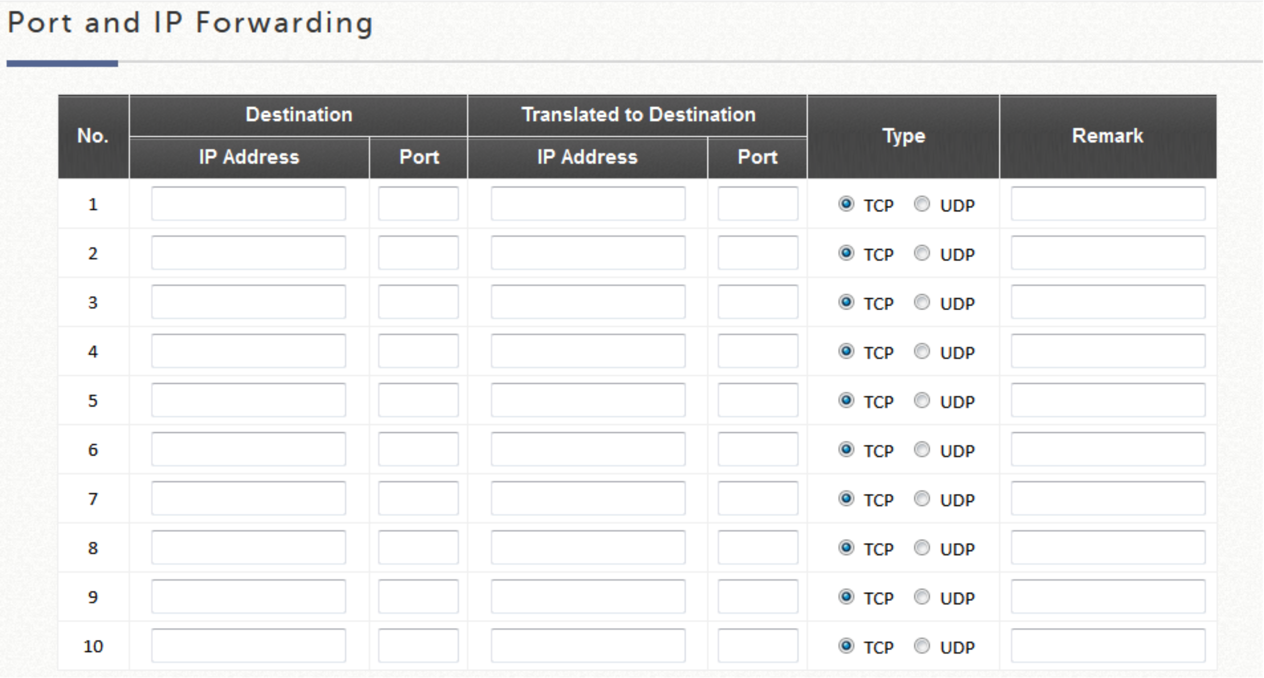


Public Accessible Server

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

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



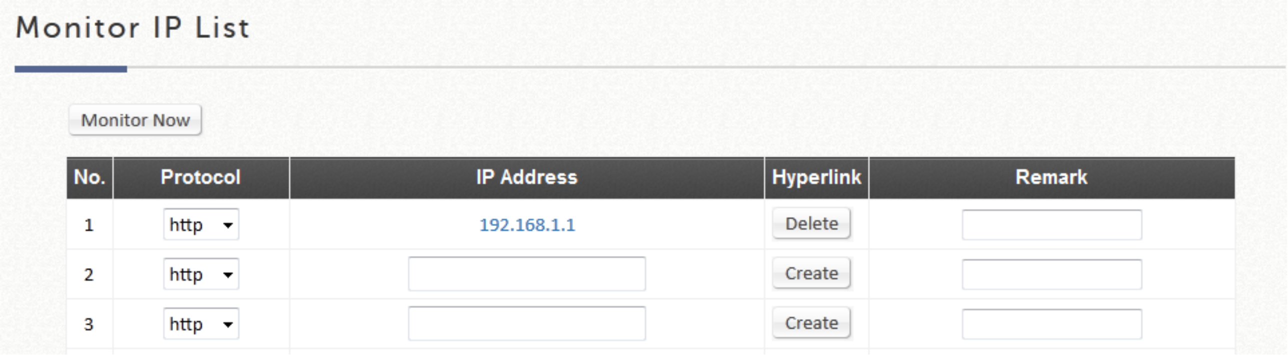
Port and IP Forwarding

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

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

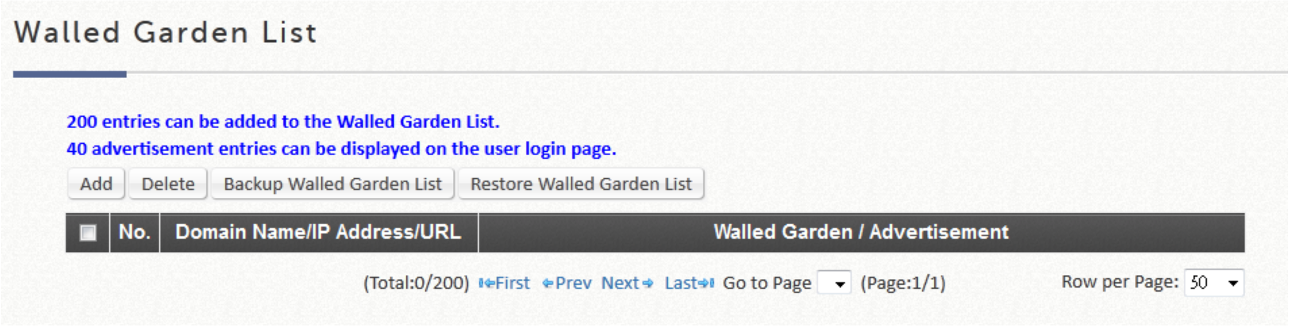
Multiple IP addresses can be defined in the Monitor IP function. System can monitor these IP based network devices and periodically report online status via email based on a configurable interval. These monitored devices can be accessed via HTTP or HTTPS connection. The management interface of the monitored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



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

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

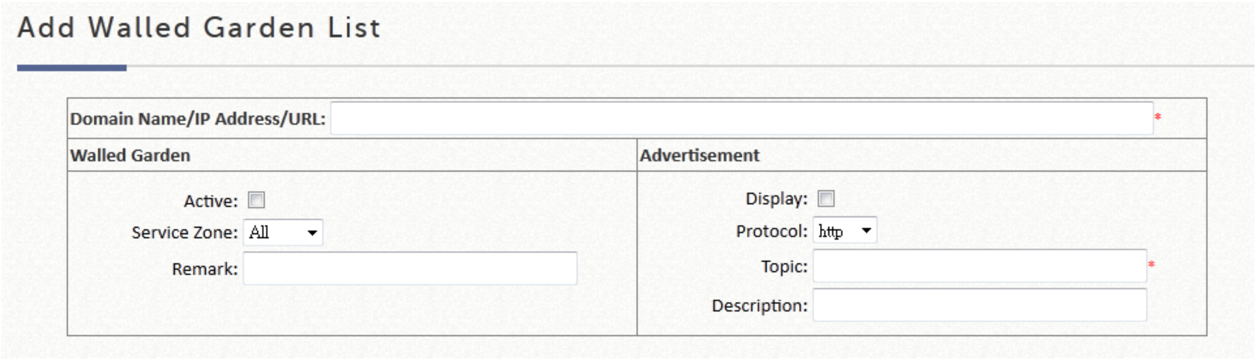
200 entries can be added to the Walled Garden List.
40 advertisement entries can be displayed on the user login page.

☐	No.	Domain Name/IP Address/URL	Walled Garden / Advertisement

(Total:0/200) First Prev Next Last Go to Page (Page:1/1) Row per Page: 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: *

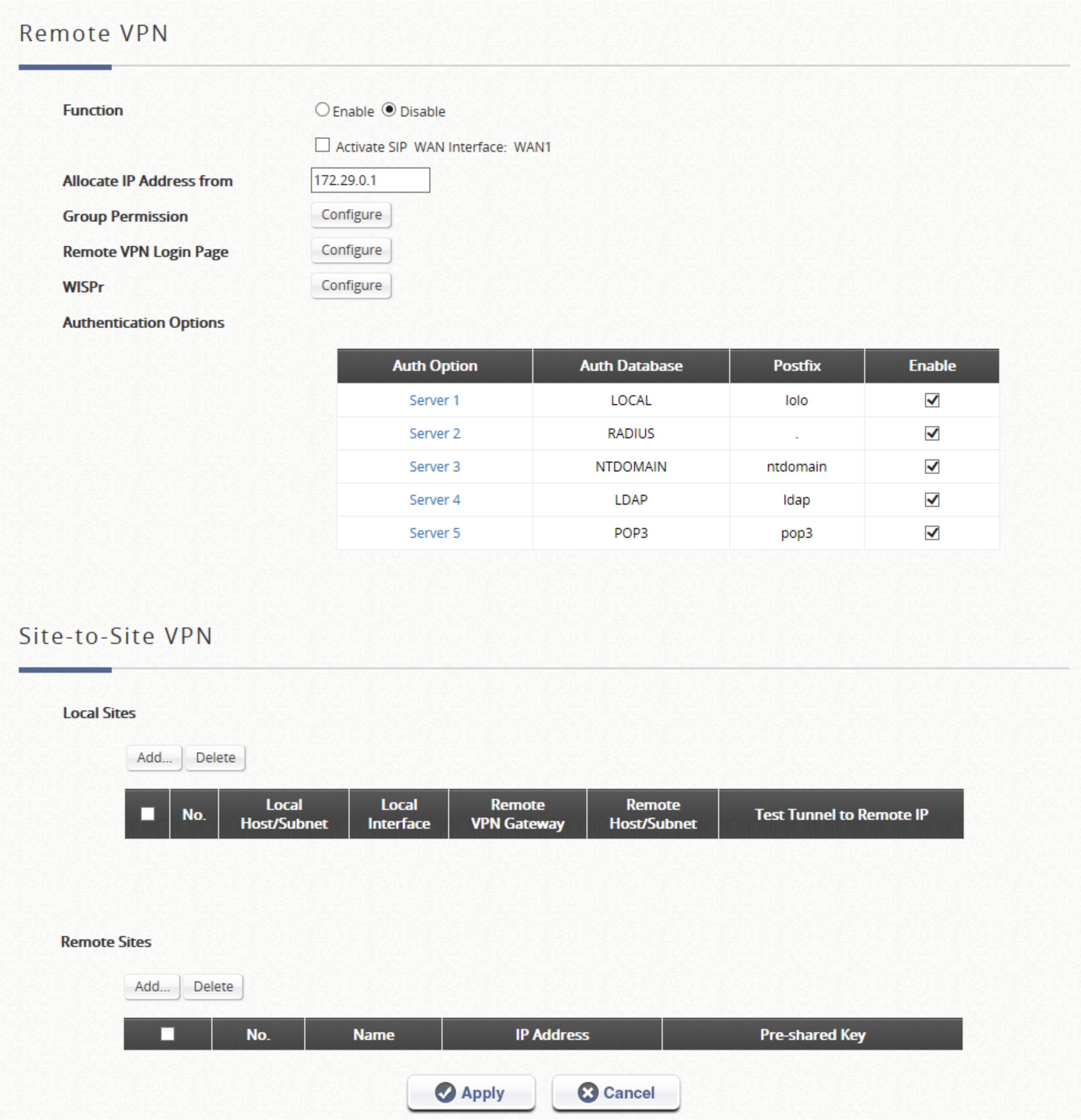
Walled Garden	Advertisement
Active: ☐	Display: ☐
Service Zone: All	Protocol: http
Remark:	Topic: *
	Description:

- 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 PPTP. For the Site-to-Site VPN, an IPSec tunnel can be used to connect to other IPSec capable device over the Internet.



Remote VPN

Function ○ Enable ● Disable

☐ Activate SIP WAN Interface: WAN1

Allocate IP Address from 172.29.0.1

Group Permission Configure

Remote VPN Login Page Configure

WISPr Configure

Authentication Options

Auth Option	Auth Database	Postfix	Enable
Server 1	LOCAL	lolo	☑
Server 2	RADIUS	.	☑
Server 3	NTDOMAIN	ntdomain	☑
Server 4	LDAP	ldap	☑
Server 5	POP3	pop3	☑

Site-to-Site VPN

Local Sites

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

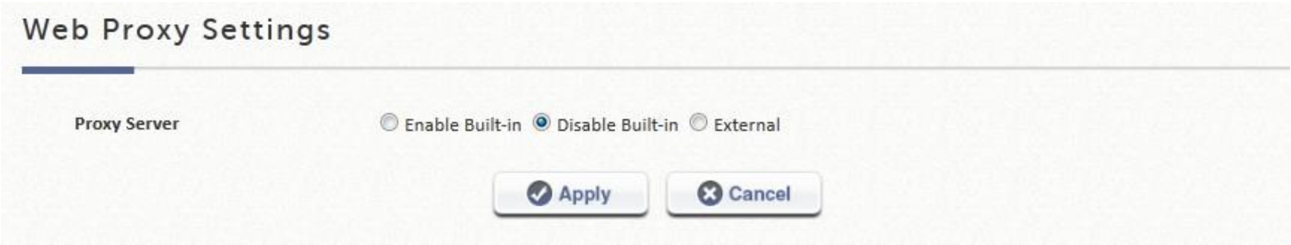
Remote Sites

☐	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.

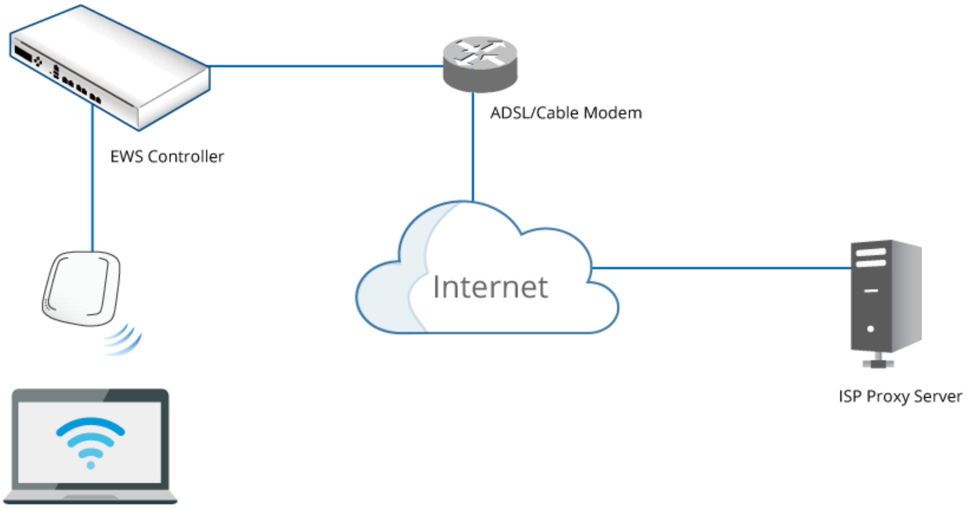


Web Proxy Settings

Proxy Server ○ Enable Built-in ● Disable Built-in ○ External

- **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.

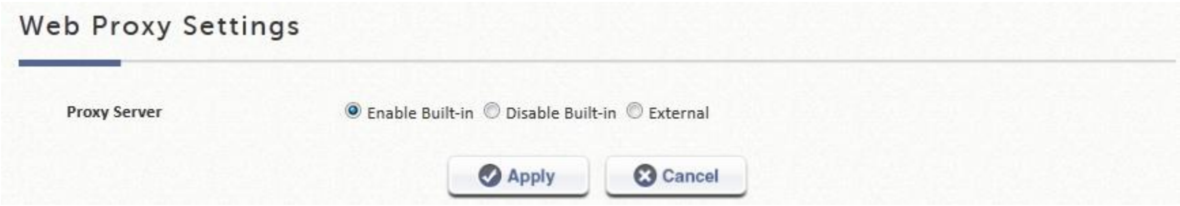


Follow the following steps to complete the proxy configuration:

Step 1. Log into the system by using the ***admin*** account.

Step 2. ***Network >> Proxy Server >> Web Proxy Settings*** page.

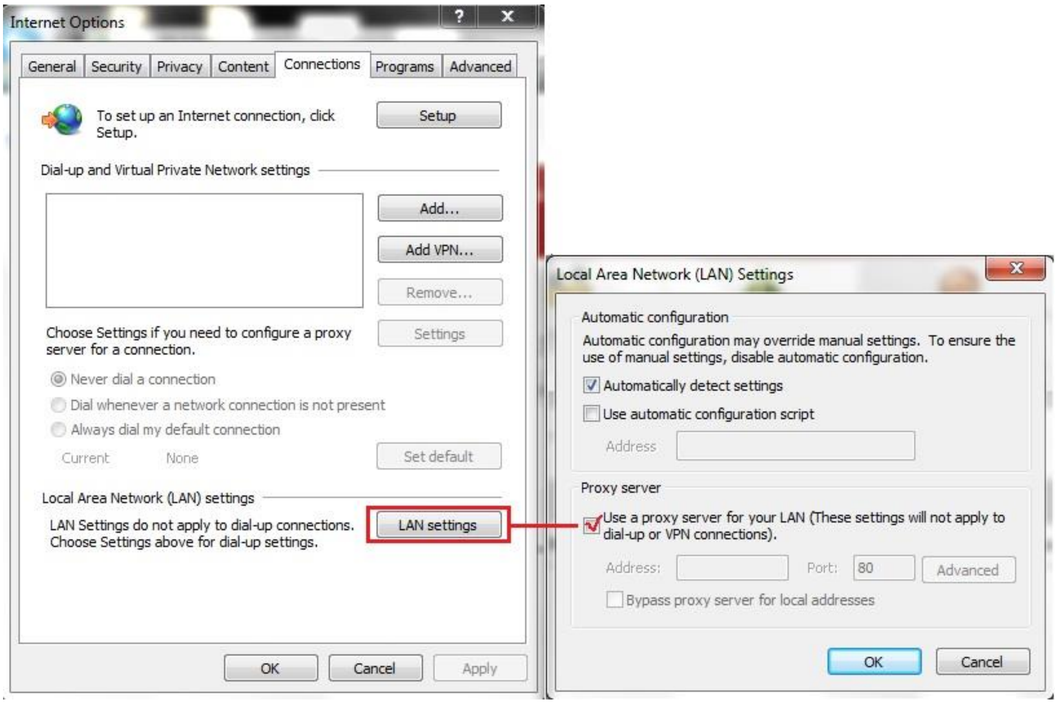
Enable the ***Built-in Proxy Server***. Click ***Apply*** to save the settings.



Web Proxy Settings

Proxy Server ● Enable Built-in ○ Disable Built-in ○ External

Step 3. Enable Proxy Server Settings in Internet Options on Client Stations.


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
To set up an Internet connection, click Setup.
Setup
Dial-up and Virtual Private Network settings
Add...
Add VPN...
Remove...
Choose Settings if you need to configure a proxy server for a connection.
Settings
Never dial a connection
Dial whenever a network connection is not present
Always dial my default connection
Current
None
Set default
Local Area Network (LAN) settings
LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.
LAN settings
OK
Cancel
Apply
Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Address
Proxy server
Address:
Advanced
Bypass proxy server for local addresses
OK
Cancel

☑ Automatically detect settings

☐ Use automatic configuration script

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Port: 80

By enabling the built-in Proxy Server, all traffic is forwarded to the local Proxy Server on the controller.

Using an External Proxy Server

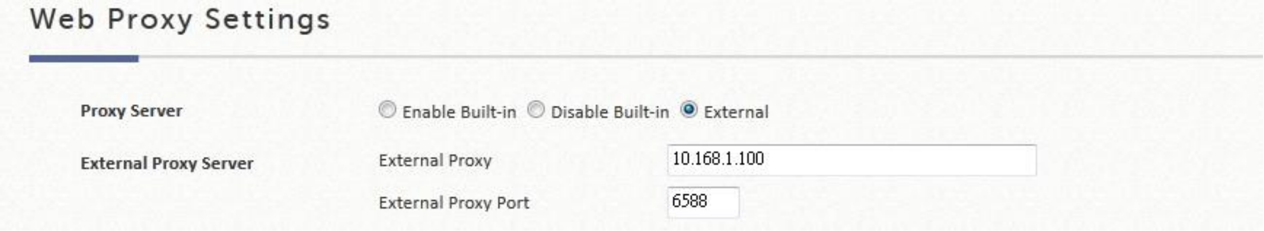
To specify an External Proxy Server, choose the option “External” and fill in the appropriate IP address of the Proxy Server and the utilized port.

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.


Web Proxy Settings

Proxy Server: ○ Enable Built-in ○ Disable Built-in ● External

External Proxy Server

External Proxy: 10.168.1.100

External Proxy Port: 6588

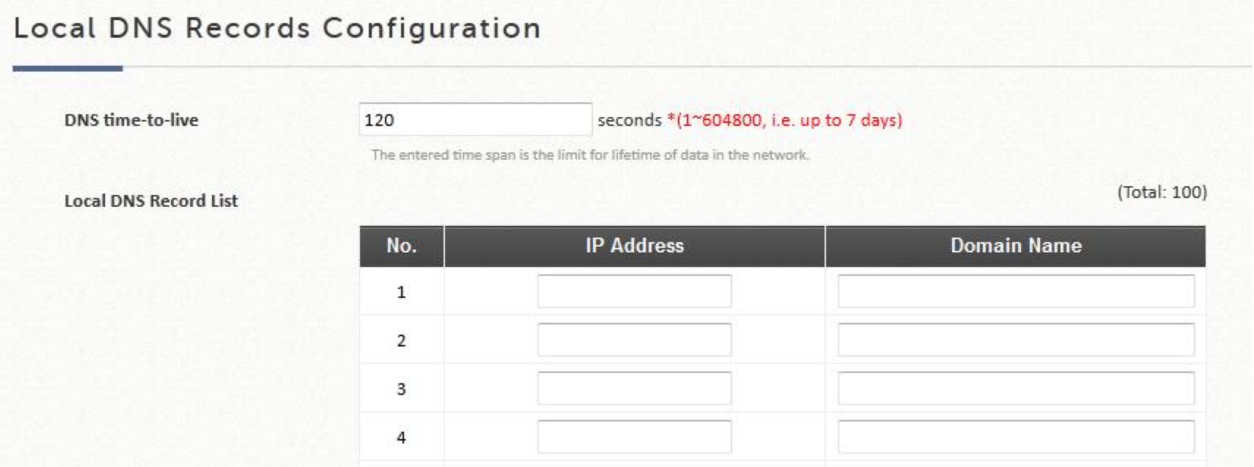
Step 3. Enable Proxy Server Settings in Internet Options on Client Stations.

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: 120 seconds *(1~604800, i.e. up to 7 days)

The entered time span is the limit for lifetime of data in the network.

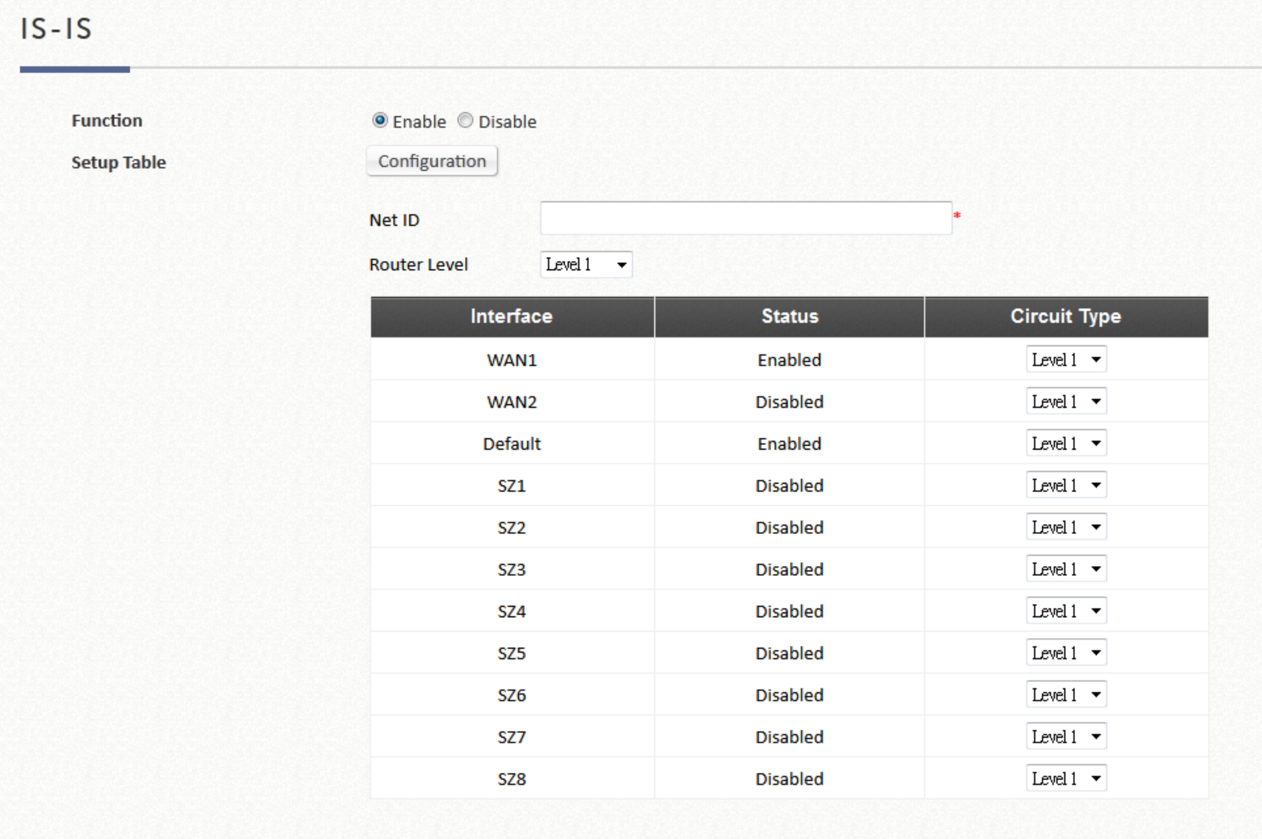
Local DNS Record List (Total: 100)

No.	IP Address	Domain Name
1		
2		
3		
4		

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.



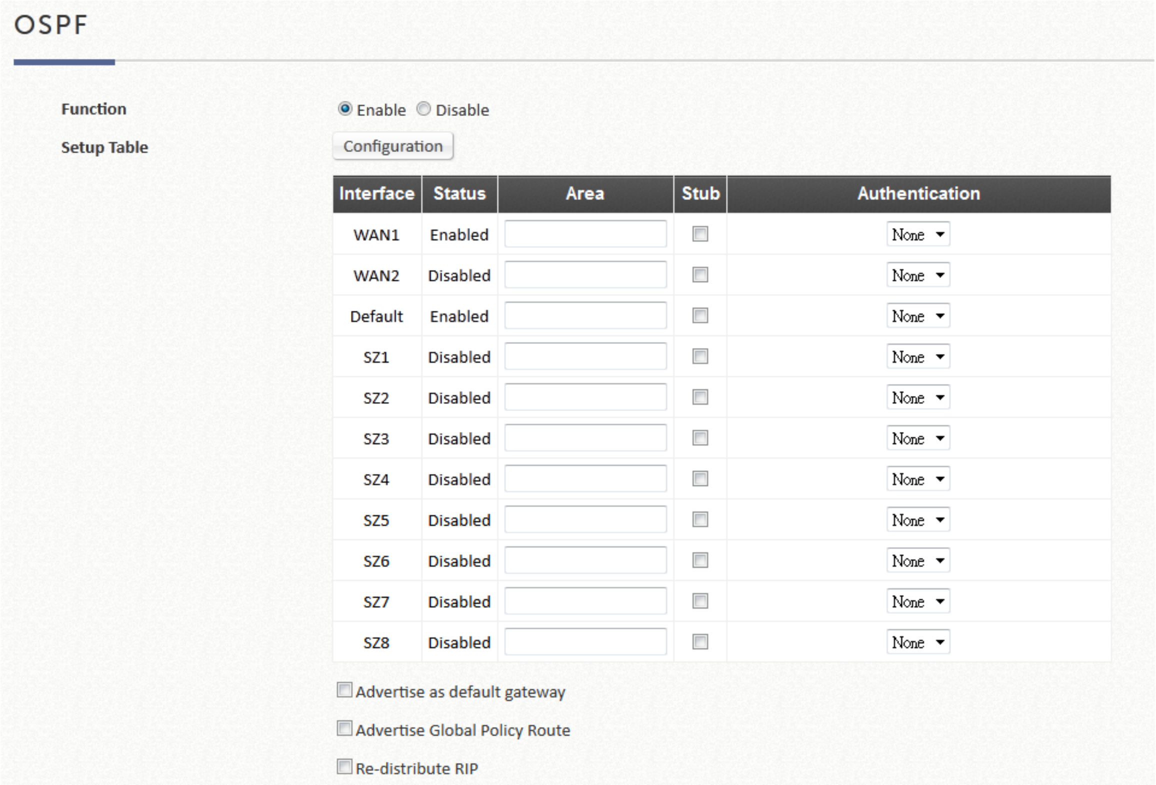
IS-IS

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		☐	None
WAN2	Disabled		☐	None
Default	Enabled		☐	None
SZ1	Disabled		☐	None
SZ2	Disabled		☐	None
SZ3	Disabled		☐	None
SZ4	Disabled		☐	None
SZ5	Disabled		☐	None
SZ6	Disabled		☐	None
SZ7	Disabled		☐	None
SZ8	Disabled		☐	None

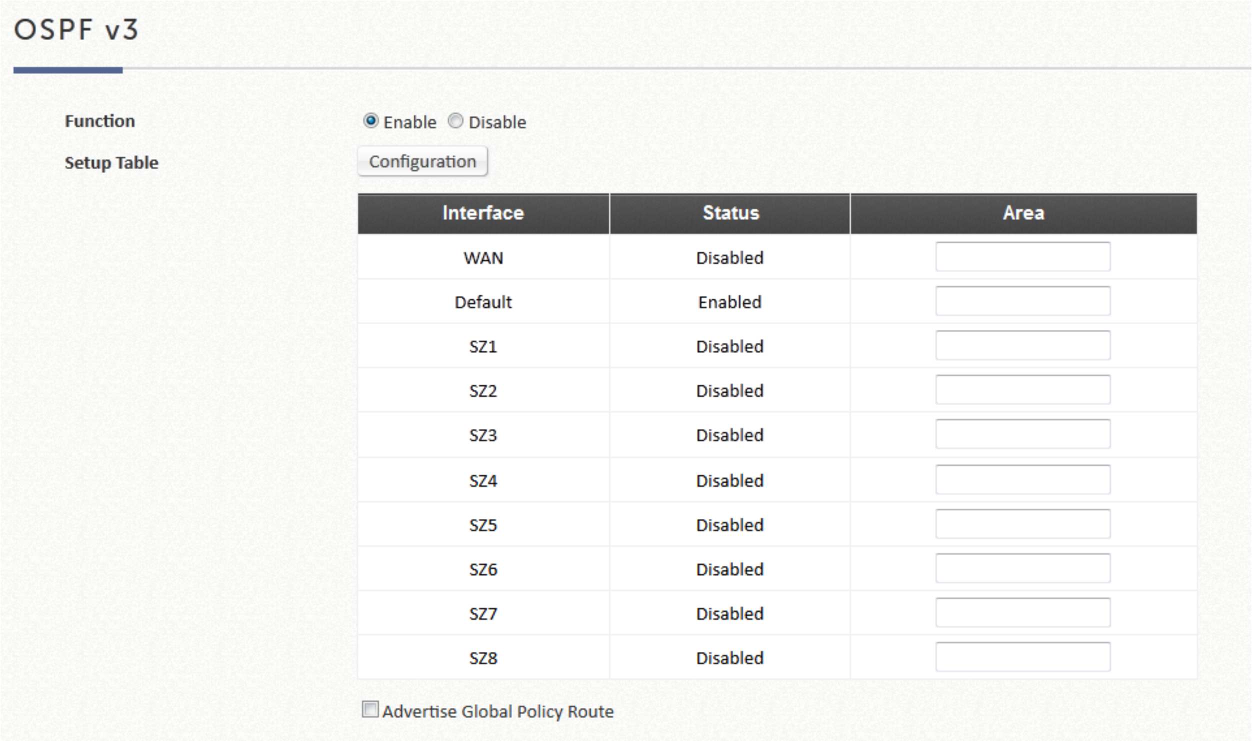
☐ Advertise as default gateway

☐ 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

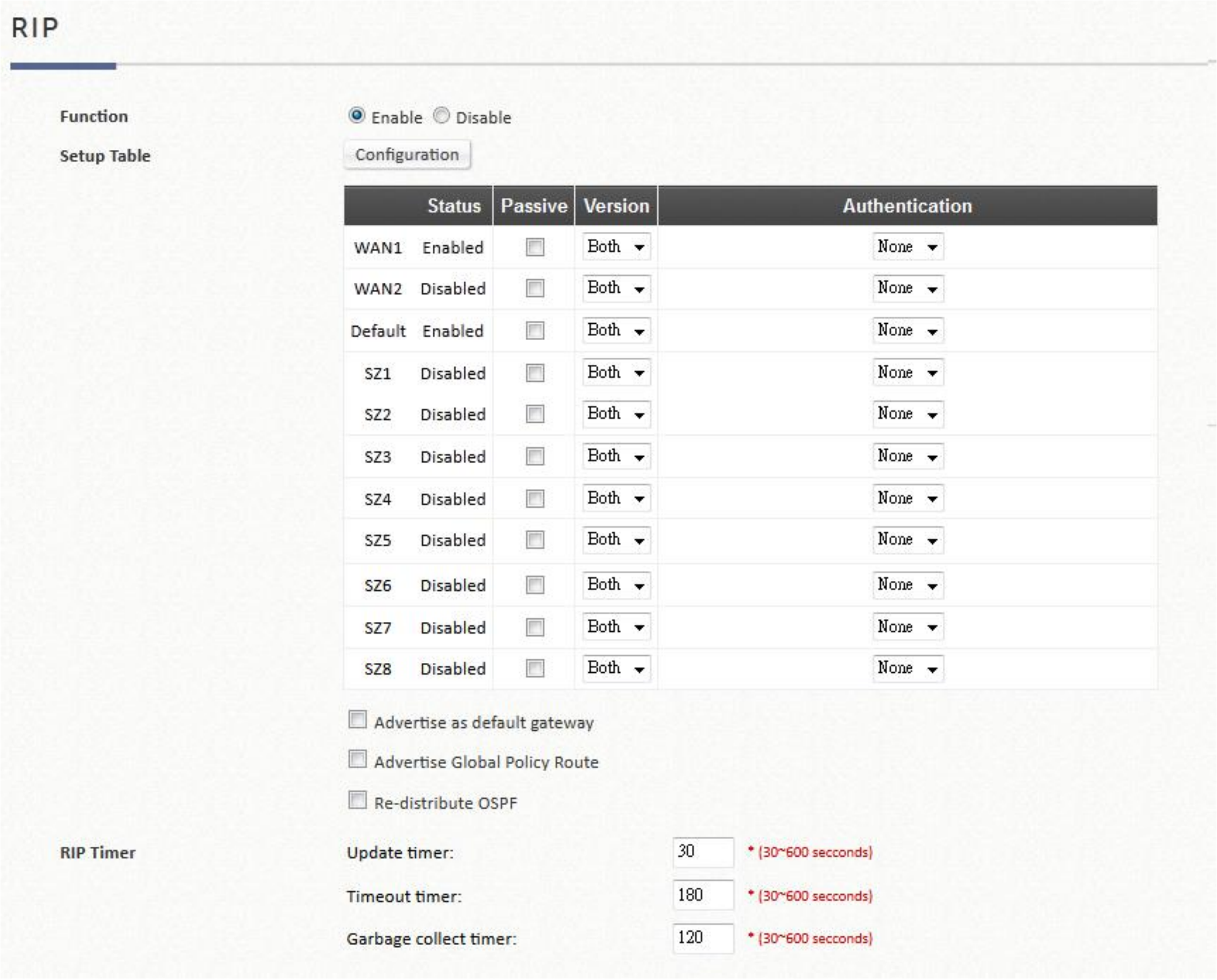
Function ● Enable ○ Disable

Setup Table

Interface	Status	Area
WAN	Disabled	
Default	Enabled	
SZ1	Disabled	
SZ2	Disabled	
SZ3	Disabled	
SZ4	Disabled	
SZ5	Disabled	
SZ6	Disabled	
SZ7	Disabled	
SZ8	Disabled	

☐ 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 Configuration

	Status	Passive	Version	Authentication
WAN1	Enabled	☐	Both	None
WAN2	Disabled	☐	Both	None
Default	Enabled	☐	Both	None
SZ1	Disabled	☐	Both	None
SZ2	Disabled	☐	Both	None
SZ3	Disabled	☐	Both	None
SZ4	Disabled	☐	Both	None
SZ5	Disabled	☐	Both	None
SZ6	Disabled	☐	Both	None
SZ7	Disabled	☐	Both	None
SZ8	Disabled	☐	Both	None

☐ Advertise as default gateway

☐ Advertise Global Policy Route

☐ Re-distribute OSPF

RIP Timer

Update timer: 30 * (30~600 secconds)

Timeout timer: 180 * (30~600 secconds)

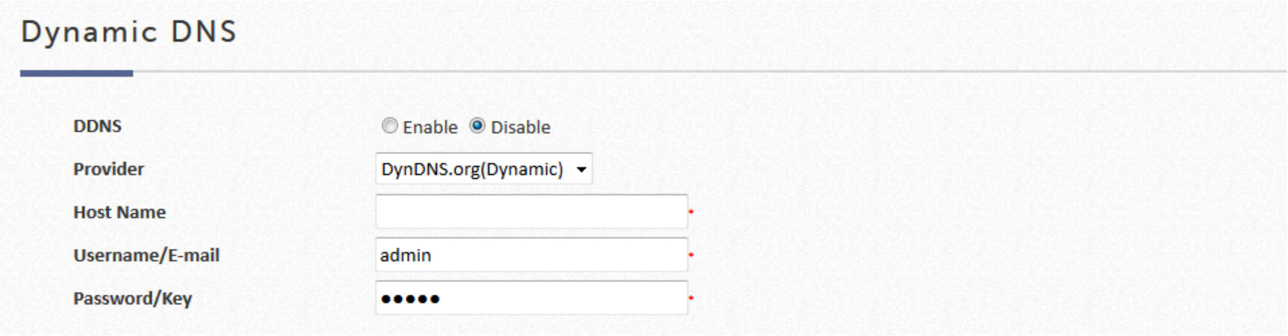
Garbage collect timer: 120 * (30~600 secconds)

- 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

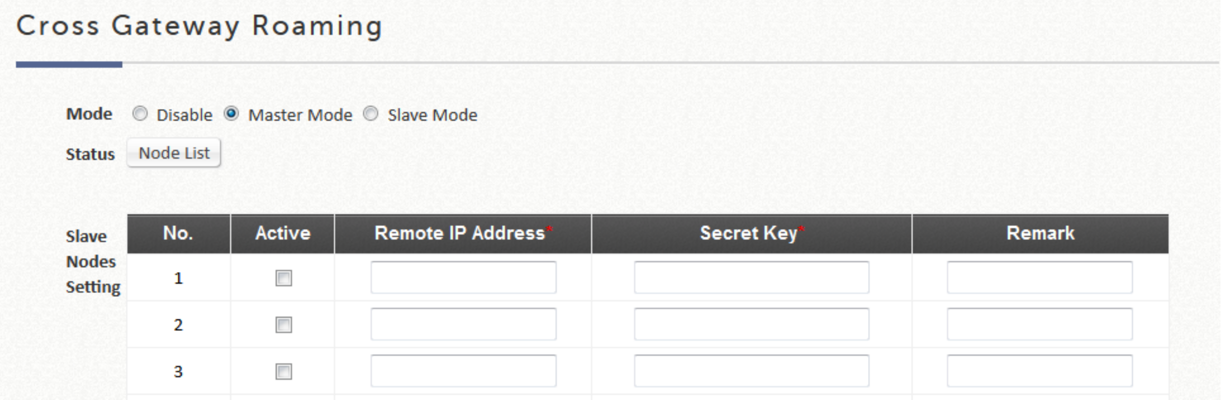
Username/E-mail admin

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

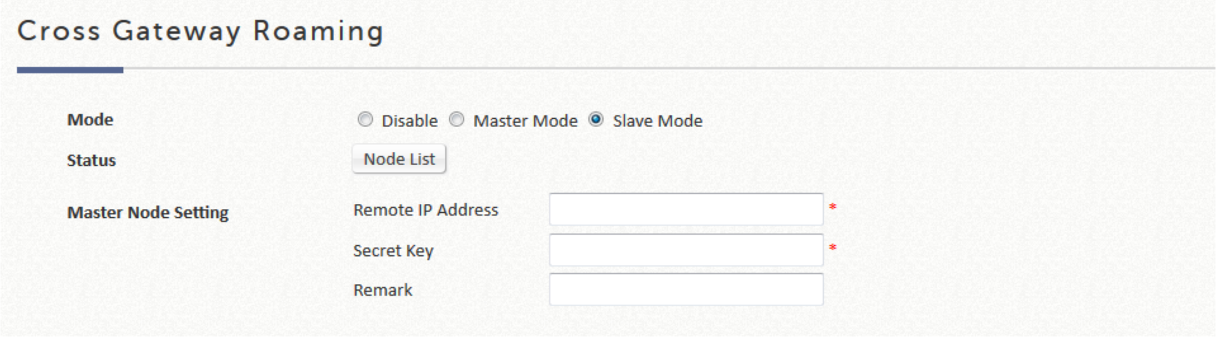
Mode ○ Disable ● Master Mode ○ Slave Mode

Status

Slave Nodes Setting

No.	Active	Remote IP Address*	Secret Key*	Remark
1	☐			
2	☐			
3	☐			

- **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

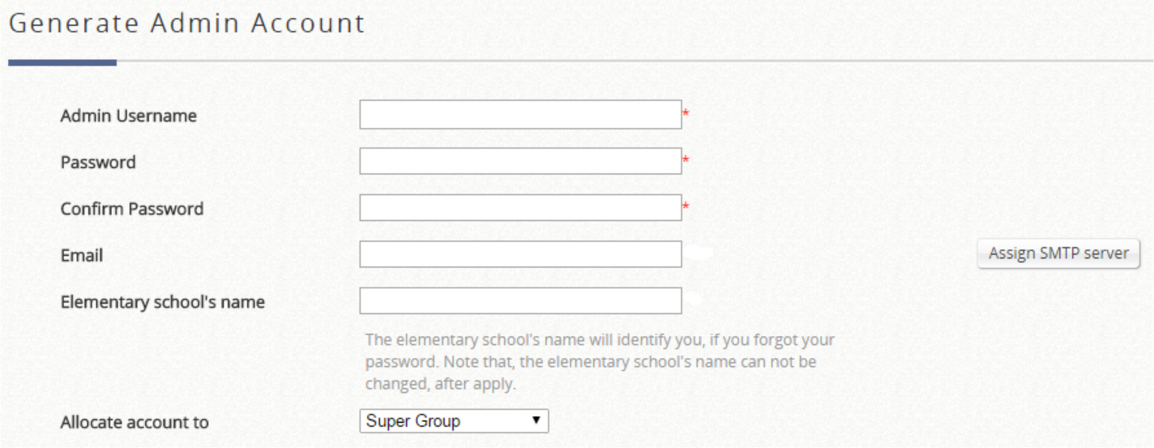
F. Utilities

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.

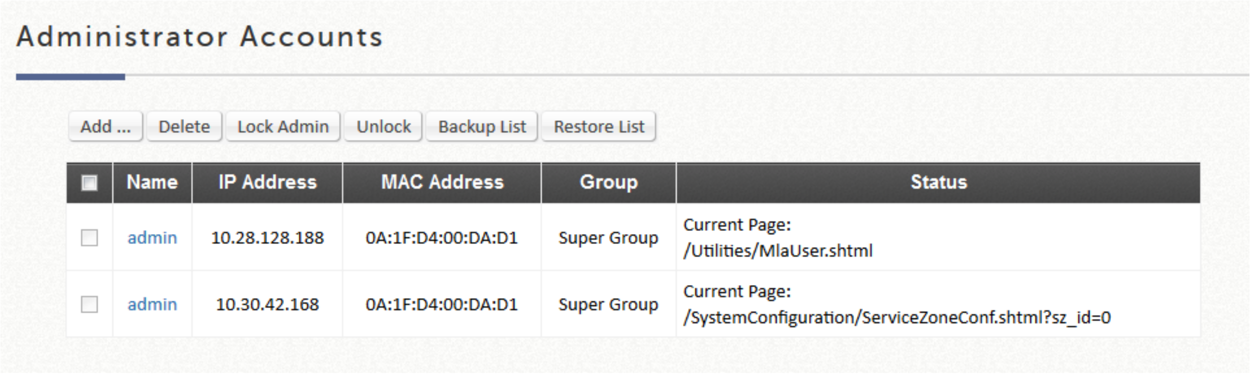

Generate Admin Account

Admin Username *
Password *
Confirm Password *
Email
Elementary school's name

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.

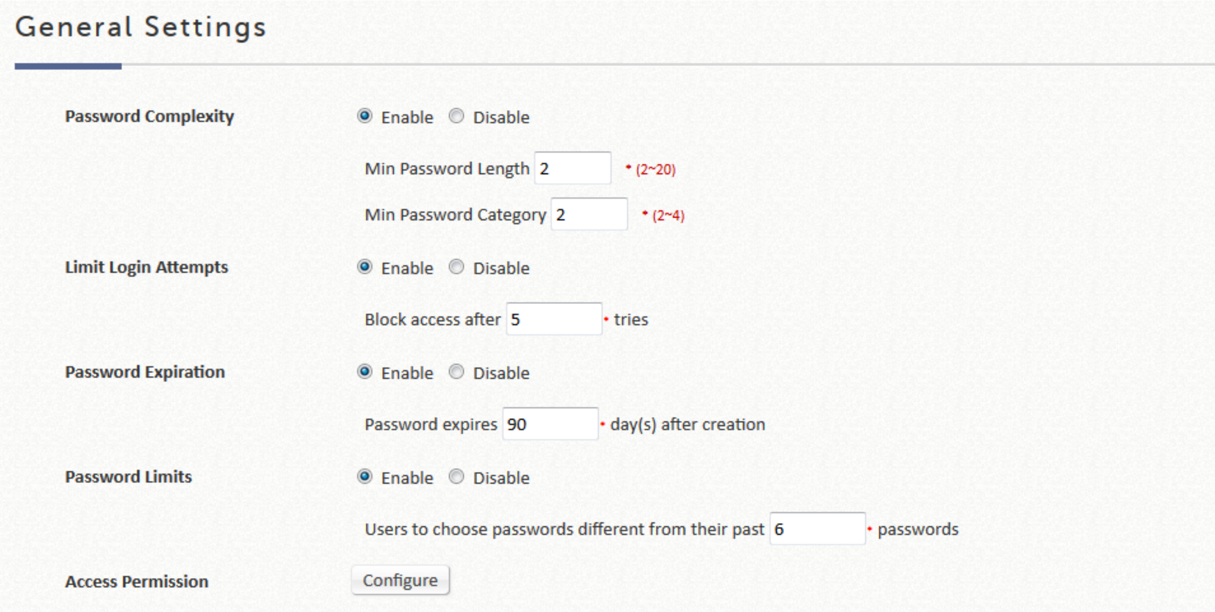
Allocate account to: Super Group

It also allows the administrator to create other administrator accounts with different permission.


Administrator Accounts

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

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

Password Complexity ● Enable ○ Disable
Min Password Length 2 * (2~20)
Min Password Category 2 * (2~4)

Limit Login Attempts ● Enable ○ Disable
Block access after 5 * tries

Password Expiration ● Enable ○ Disable
Password expires 90 * day(s) after creation

Password Limits ● Enable ○ Disable
Users to choose passwords different from their past 6 * passwords

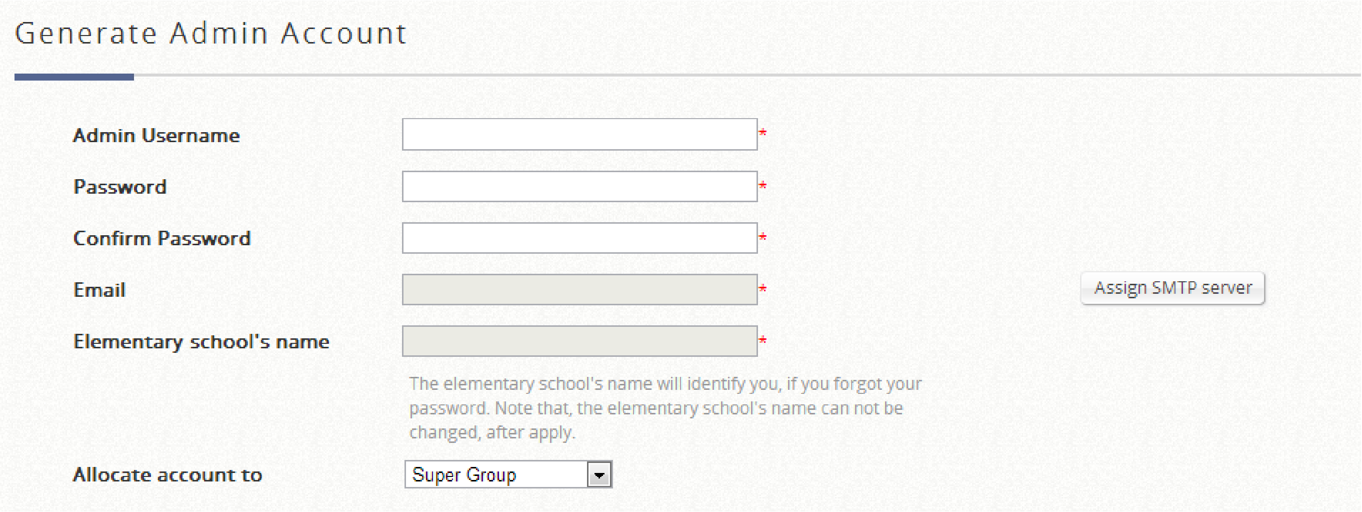
Access Permission

- **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**

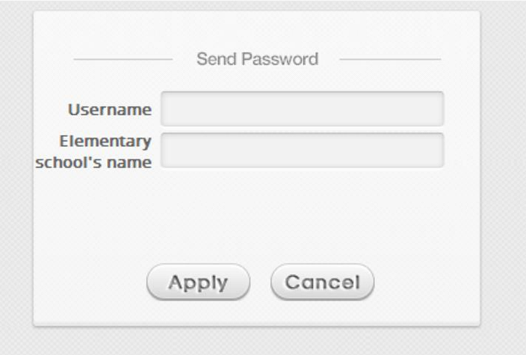


Generate Admin Account

Admin Username	*
Password	*
Confirm Password	*
Email	*
Elementary school's name	*
Allocate account to	Super Group

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.

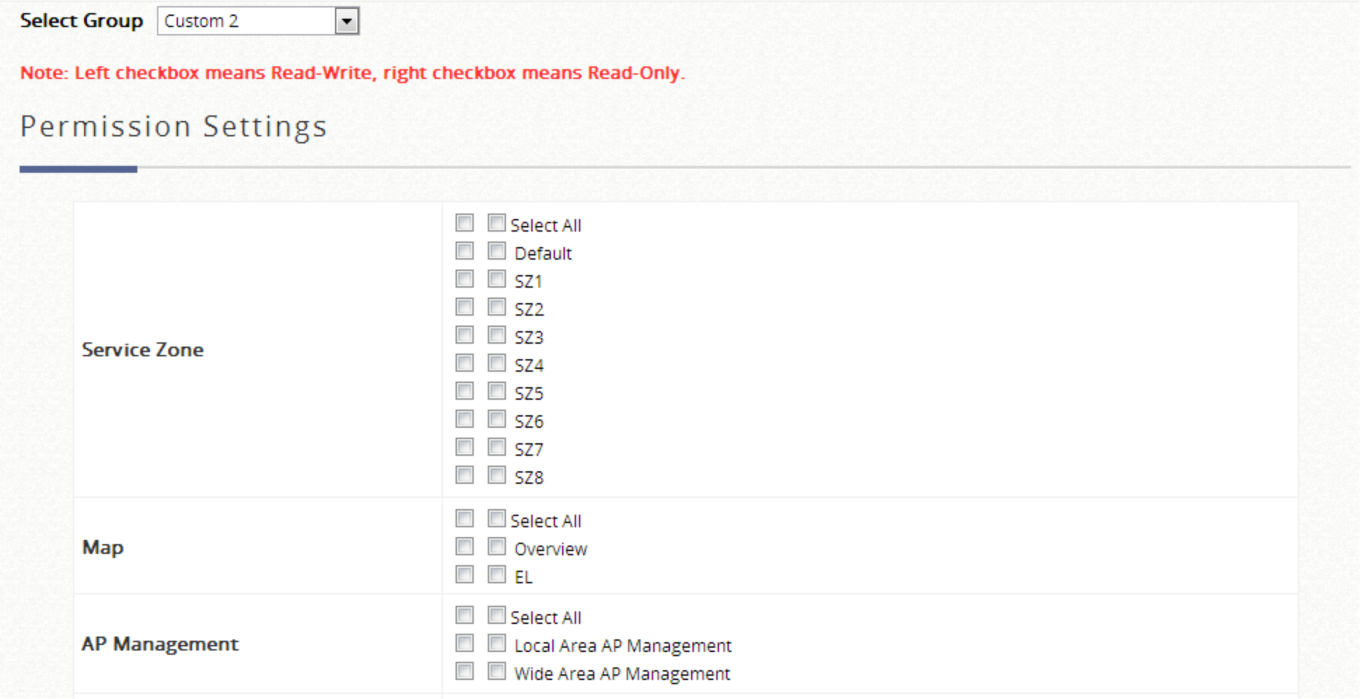
Go to the **Generate** table to create a sub-admin and define his/her authority limits. In case the administrator forgets his/her password, by entering both email and the Elementary School Name, the account credential will be email to the assigned email address. Note that an SMTP Server needs to be setup 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, OnDemand Manager, Custom1, Custom2, and Custom3. Click configure at the right of the drop-down list to see and modify the differences. Be aware that the authority limits of ‘Super Group’ are unchangeable.) Create an account to the list by pressing the Apply button after finishing the settings.



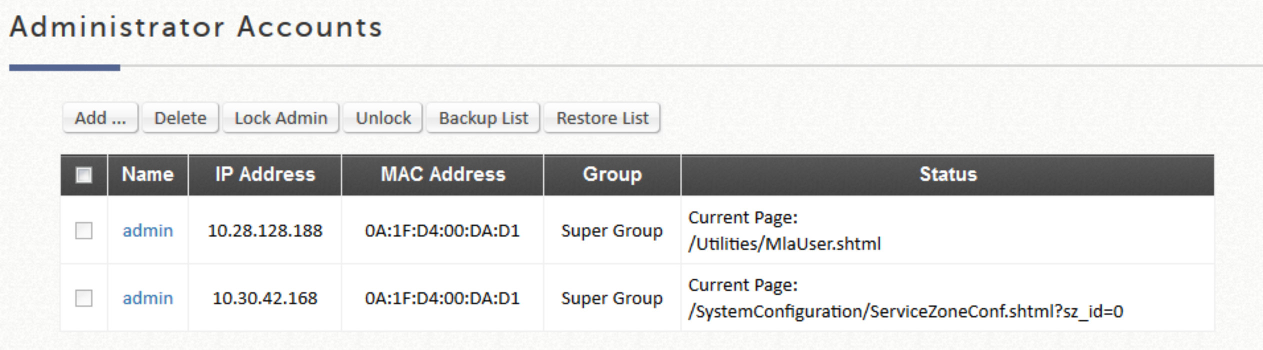
Select Group Custom 2

Note: Left checkbox means Read-Write, right checkbox means Read-Only.

Permission Settings

Service Zone	☐ ☐ Select All ☐ ☐ Default ☐ ☐ SZ1 ☐ ☐ SZ2 ☐ ☐ SZ3 ☐ ☐ SZ4 ☐ ☐ SZ5 ☐ ☐ SZ6 ☐ ☐ SZ7 ☐ ☐ SZ8
Map	☐ ☐ Select All ☐ ☐ Overview ☐ ☐ EL
AP Management	☐ ☐ Select All ☐ ☐ Local Area AP Management ☐ ☐ 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.



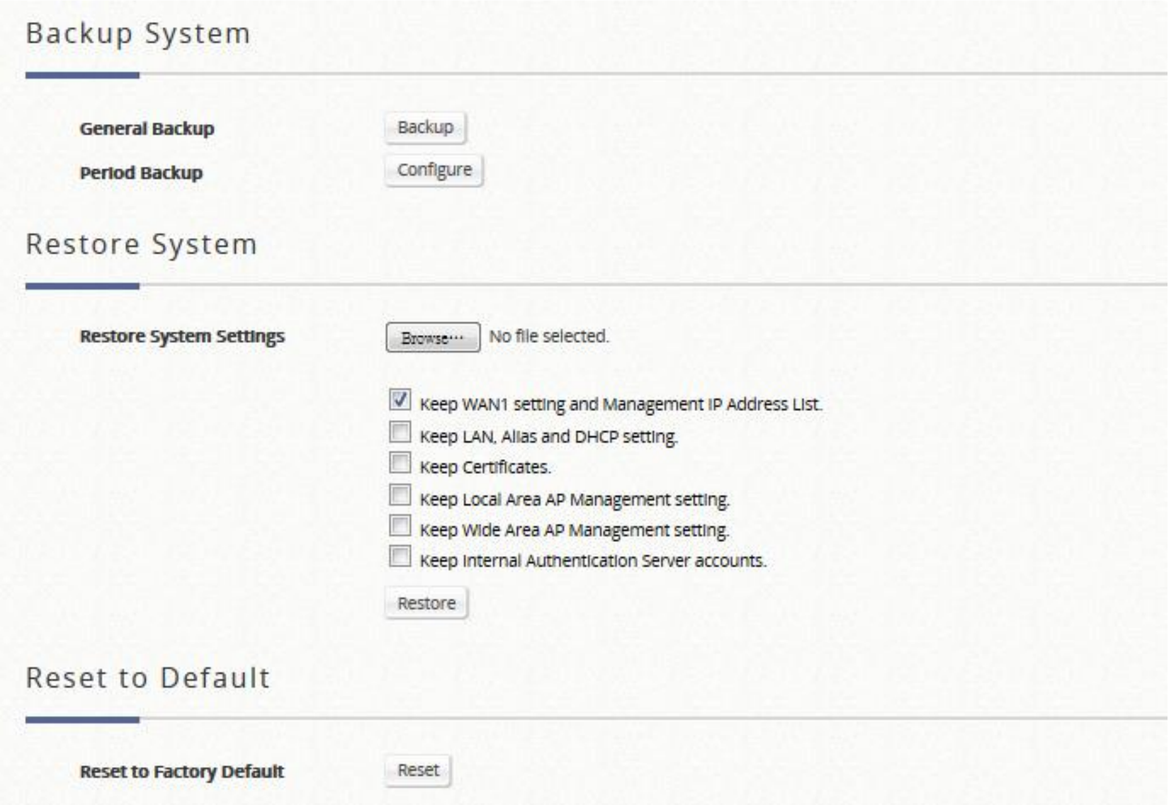
Administrator Accounts

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

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.



Backup System

General Backup

Period Backup

Restore System

Restore System Settings No file selected.

☑ Keep WAN1 setting and Management IP Address List.
☐ Keep LAN, Alias and DHCP setting.
☐ Keep Certificates.
☐ Keep Local Area AP Management setting.
☐ Keep Wide Area AP Management setting.
☐ Keep Internal Authentication Server accounts.

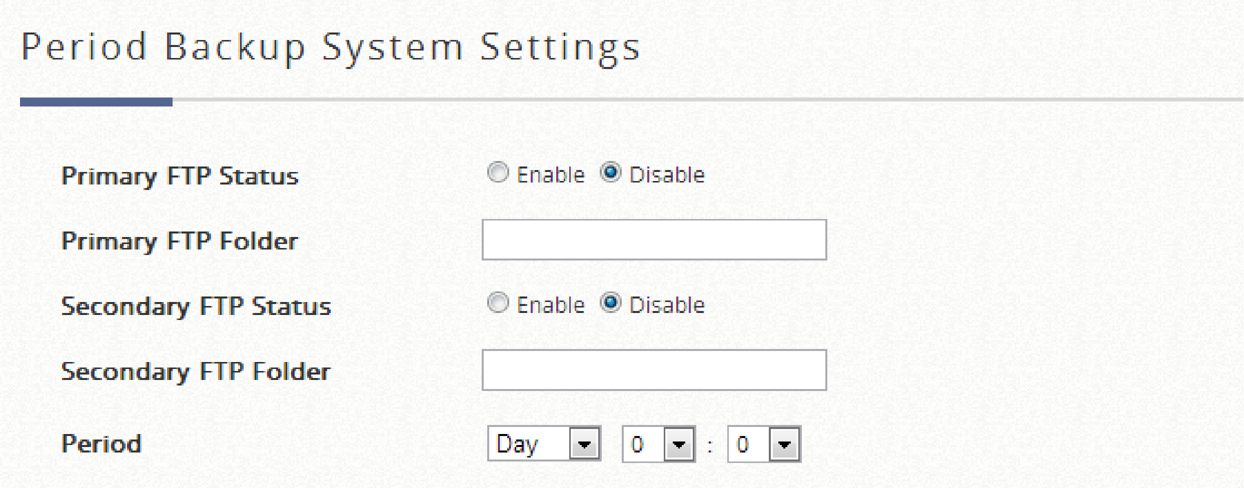
Reset to Default

Reset to Factory Default

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.



Period Backup System Settings

Primary FTP Status ○ Enable ● Disable

Primary FTP Folder

Secondary FTP Status ○ Enable ● Disable

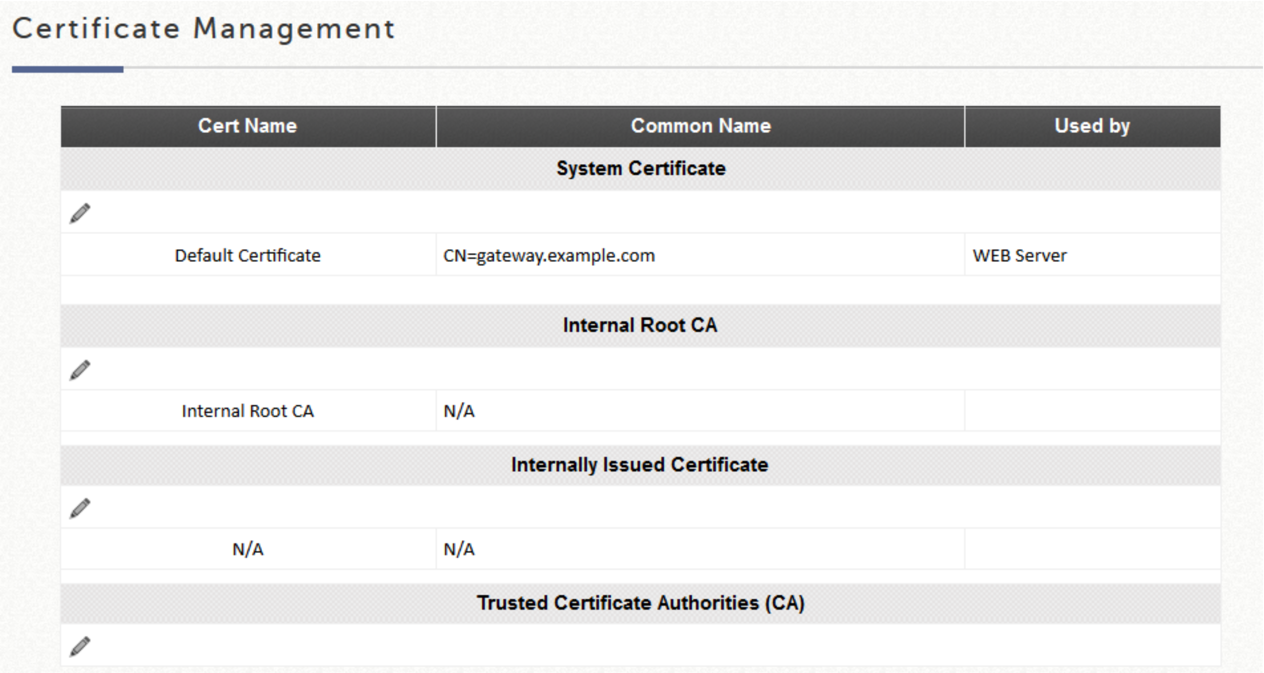
Secondary FTP Folder

Period Day 0 : 0

- **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.

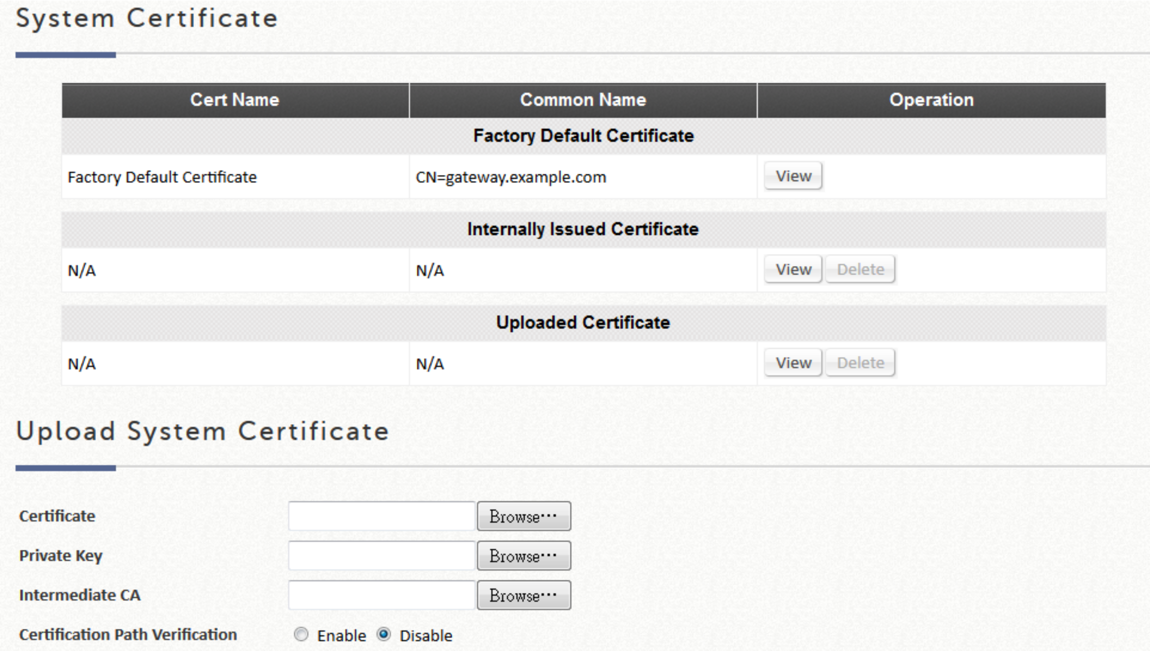


Certificate Management

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

- **System Certificate**

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



System Certificate

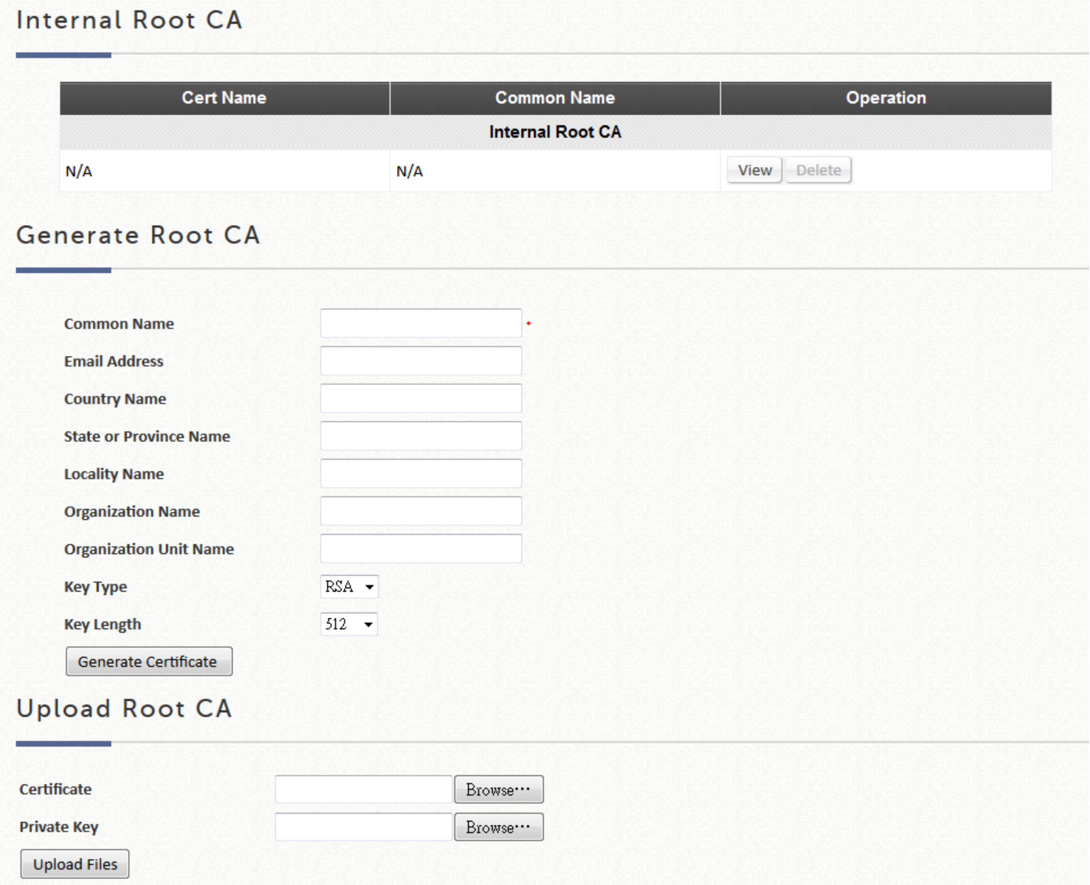
Cert Name	Common Name	Operation
Factory Default Certificate		
Factory Default Certificate	CN=gateway.example.com	View
Internally Issued Certificate		
N/A	N/A	View Delete
Uploaded Certificate		
N/A	N/A	View Delete

Upload System Certificate

Certificate	Browse…
Private Key	Browse…
Intermediate CA	Browse…
Certification Path Verification	○ Enable ● Disable

- **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	View Delete

Generate Root CA

Common Name	*
Email Address	
Country Name	
State or Province Name	
Locality Name	
Organization Name	
Organization Unit Name	
Key Type	RSA
Key Length	512

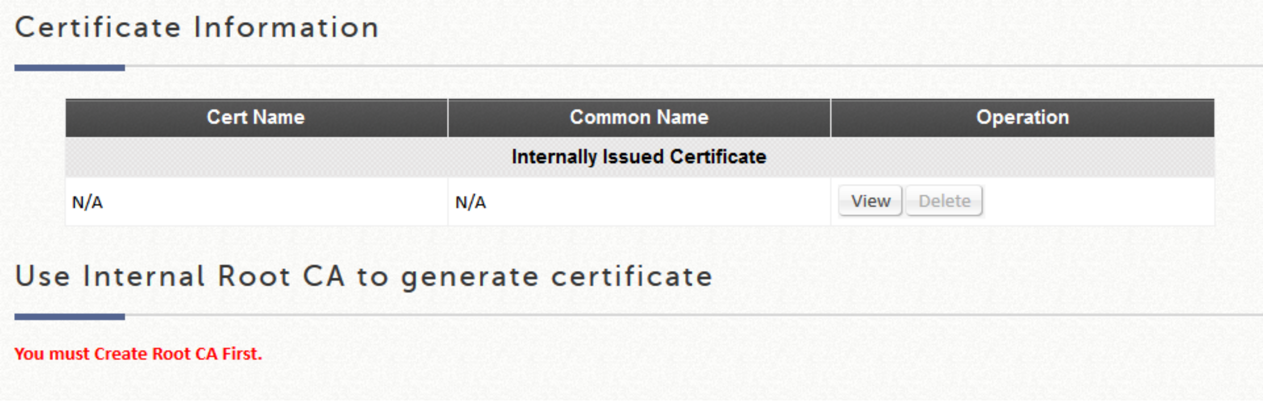
Upload Root CA

Certificate	Browse…
Private Key	Browse…

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	View Delete

Use Internal Root CA to generate certificate

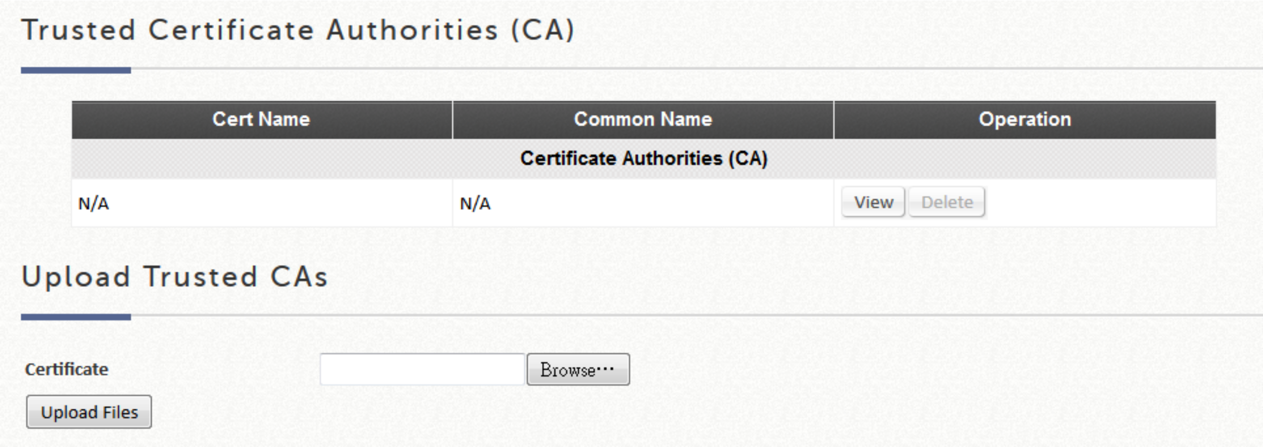
You must Create Root CA First.

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.



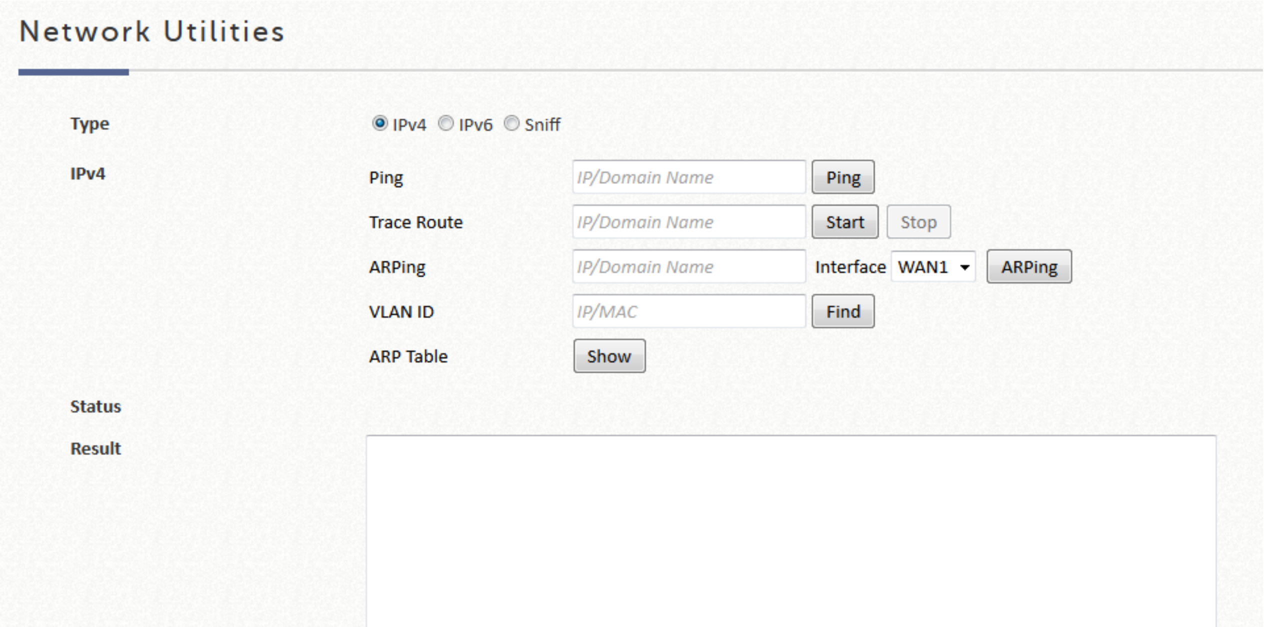
Trusted Certificate Authorities (CA)

Cert Name	Common Name	Operation
Certificate Authorities (CA)		
N/A	N/A	View Delete

Upload Trusted CAs

4) Network Utilities

Some network utilities such as web-based Ping, Trace Route, and ARP table are supported on the system.



Network Utilities

Type ● IPv4 ○ IPv6 ○ Sniff

IPv4

Ping IP/Domain Name Ping

Trace Route IP/Domain Name Start Stop

ARPing IP/Domain Name Interface WAN1 ARPing

VLAN ID IP/MAC Find

ARP Table Show

Status

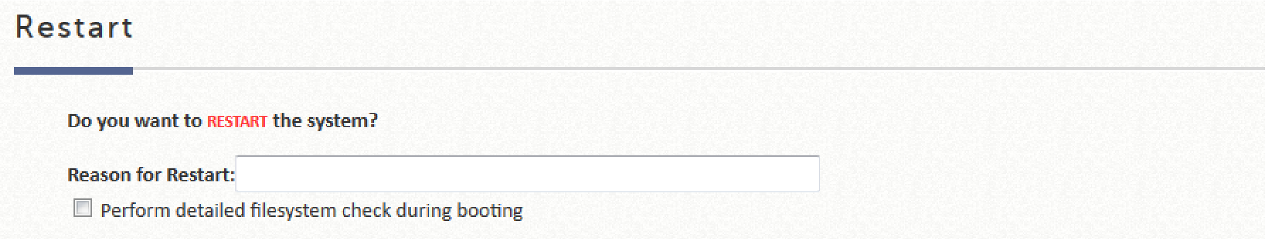
Result

Item	Description
IPv4	▪ **Ping:** It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not. ▪ **Trace Route:** It allows administrator to recover the real path of packets from the gateway to a destination using IP address or Host domain name. ▪ **ARPing:** Allows the administrator to send ARP request for a specific IP address or domain name. ▪ **ARP Table:** It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).
IPv6	▪ **Ping:** It allows administrator to detect a device using IPv6 address or Host domain name to see if it is alive or not. ▪ **Trace Route 6:** It allows administrator to recover the real path of packets from the gateway to a destination using IPv6 address or Host domain name. ▪ **Neighbor Discovery:** The administrator can use this feature to learn about IPv6 Neighbor nodes that are on the same IP segment or domain name. ▪ **Neighbor Cache:** a node that manages the information about its neighbors in the Neighbor Cache. This feature allows the administrator to view the information stored on system’s neighbor cache.

Sniff	With this feature the administrator can listen for packets from selected Interfaces. The administrator can further filter the types of packets to capture by using tcpdump commands under the **Expression** field.
Status	When the administrator is executing any Network Utilities features, the status of the operation is displayed here.
Result	The operation result is displayed here.

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.


Restart

Do you want to RESTART the system?

Reason for Restart:

☐ Perform detailed filesystem check during booting

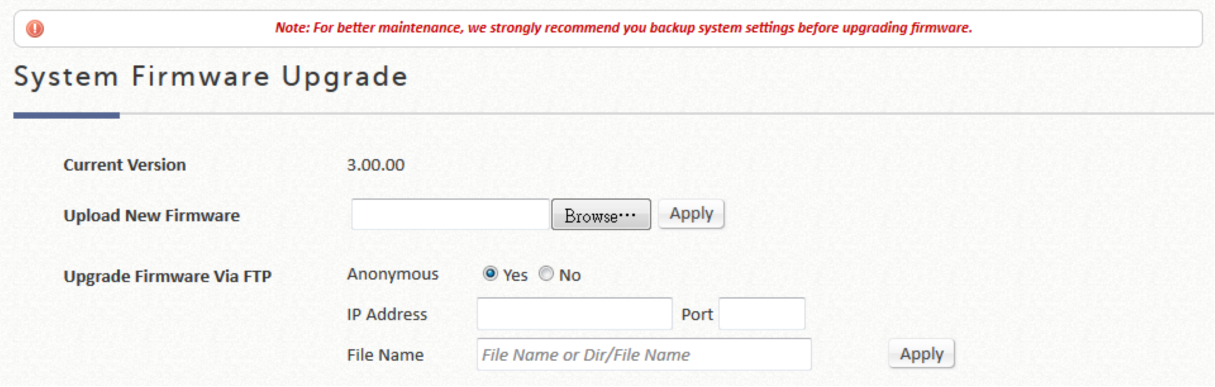
6) System Upgrade

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
Browse…
Apply
Upgrade Firmware Via FTP
Anonymous
● Yes ○ No
IP Address
Port
File Name
File Name or Dir/File Name
Apply

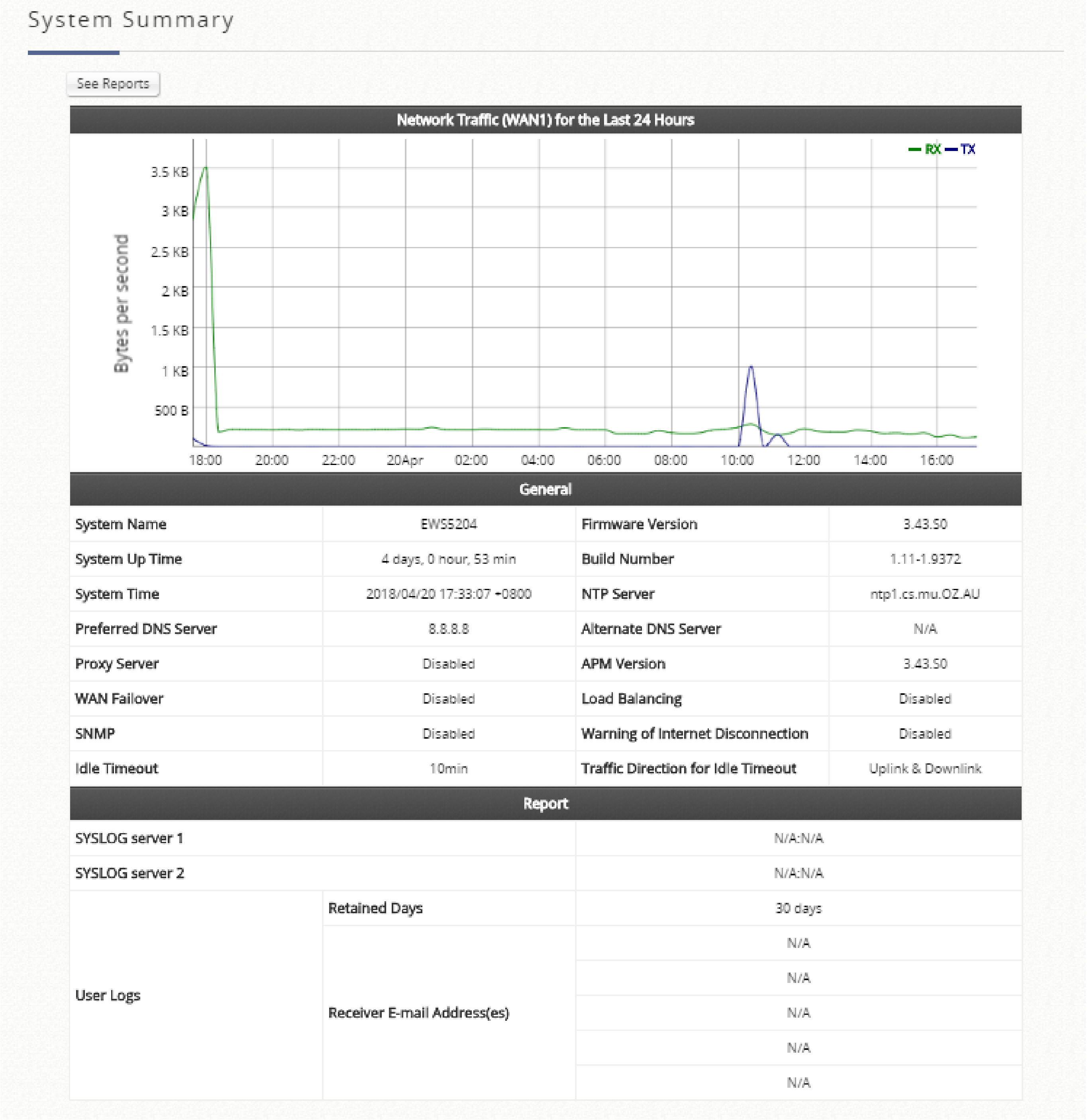
G. Status

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

Network Traffic (WAN1) for the Last 24 Hours

General

System Name	EWS5204	Firmware Version	3.43.50
System Up Time	4 days, 0 hour, 53 min	Build Number	1.11-1.9372
System Time	2018/04/20 17:33:07 +0800	NTP Server	ntp1.cs.mu.OZ.AU
Preferred DNS Server	8.8.8.8	Alternate DNS Server	N/A
Proxy Server	Disabled	APM Version	3.43.50
WAN Failover	Disabled	Load Balancing	Disabled
SNMP	Disabled	Warning of Internet Disconnection	Disabled
Idle Timeout	10min	Traffic Direction for Idle Timeout	Uplink & Downlink

Report

SYSLOG server 1		N/A:N/A
SYSLOG server 2		N/A:N/A
User Logs	Retained Days	30 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
		N/A
		N/A

General			
System Name	The system name. The default name is the model number.	**Firmware Version**	The present firmware version of EWS CONTROLLER
System Up Time	Displays for how long the system has operated.	**Build Number**	The current build number.
System Time	The local time is shown as the system time.	**NTP Server**	The network time server that the system is set to align.
Preferred DNS Server	IP address of the preferred DNS Server.	**Alternate DNS Server**	IP address of the alternate DNS Server.
Proxy Server	Enabled/disabled displays if the	**Start Page URL**	The preset URL upon users' initial

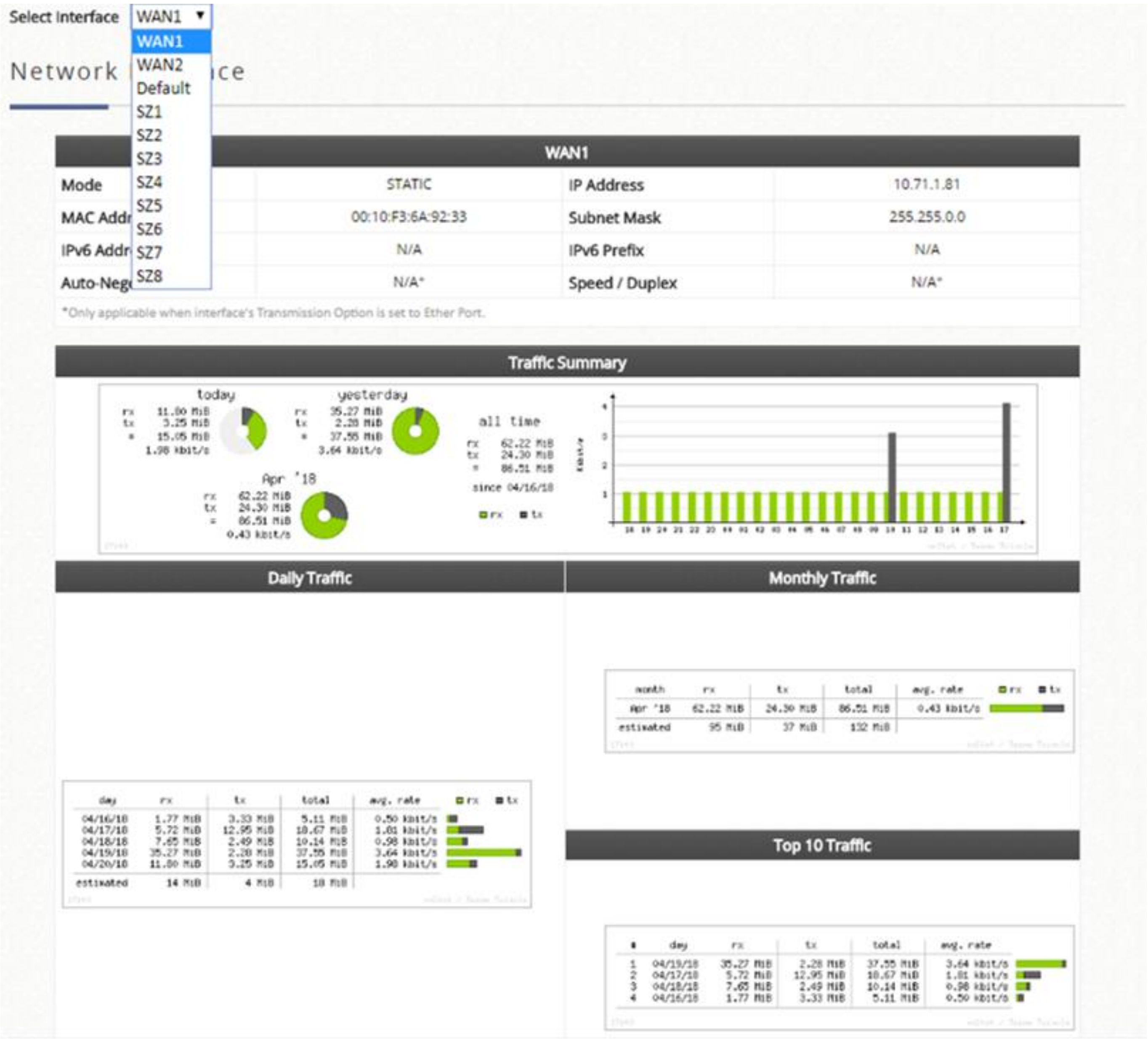
	system is currently using the proxy server.		successful login.
WAN Failover	Enabled/Disabled	**Load Balancing**	Enabled/Disabled
SNMP	Enabled/Disabled	**Warning of Internet Disconnection**	Enabled/Disabled
Idle Timeout	The minutes allowed for the users to be inactive before their account expires automatically.	**Multiple Login**	Enabled/Disabled
Report			
Syslog server 1			The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Syslog server 2			The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
User Logs	**Retained Days**		The maximum number of days for the system to retain the users' information.
	Receiver Email Address (es)		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 (available on EWS models): 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
WAN1
WAN2
Default
SZ1
SZ2
SZ3
SZ4
SZ5
SZ6
SZ7
SZ8
Network
ce
Traffic Summary
today
yesterday
all time
Apr '18
since 04/16/18
rx
tx
Daily Traffic
Monthly Traffic
Top 10 Traffic

WAN1			
Mode	STATIC	IP Address	10.71.1.81
MAC Addr	00:10:F3:6A:92:33	Subnet Mask	255.255.0.0
IPv6 Addr	N/A	IPv6 Prefix	N/A
Auto-Neg	N/A*	Speed / Duplex	N/A*

*Only applicable when interface's Transmission Option is set to Ether Port.

day	rx	tx	total	avg. rate
04/16/18	1.77 MiB	3.33 MiB	5.11 MiB	0.50 kbit/s
04/17/18	5.72 MiB	12.95 MiB	18.67 MiB	1.81 kbit/s
04/18/18	7.65 MiB	2.49 MiB	10.14 MiB	0.98 kbit/s
04/19/18	35.27 MiB	2.28 MiB	37.55 MiB	3.64 kbit/s
04/20/18	11.80 MiB	3.25 MiB	15.05 MiB	1.98 kbit/s
estimated	14 MiB	4 MiB	18 MiB	

month	rx	tx	total	avg. rate
Apr '18	62.22 MiB	24.30 MiB	86.51 MiB	0.43 kbit/s
estimated	95 MiB	37 MiB	132 MiB	

#	day	rx	tx	total	avg. rate
1	04/19/18	35.27 MiB	2.28 MiB	37.55 MiB	3.64 kbit/s
2	04/17/18	5.72 MiB	12.95 MiB	18.67 MiB	1.81 kbit/s
3	04/18/18	7.65 MiB	2.49 MiB	10.14 MiB	0.98 kbit/s
4	04/16/18	1.77 MiB	3.33 MiB	5.11 MiB	0.50 kbit/s

Item		**Description**
Interface (WAN1)	**Mode**	Operating mode of this interface.
	MAC Address	The MAC address of the WAN1 port.
	IP Address	The IPv4 address of the WAN1 port.
	Subnet Mask	The Subnet Mask of the WAN1 port.
	IPv6 Address	The IPv6 address of the selected interface
	IPv6 Prefix	The prefix of IPv6 address
	Auto-Negotiation	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.
	Speed/Duplex	Displays current speed and duplex of the selected interface.
Traffic Summary		Displays daily, monthly and all time graphical summary of the TX and Rx rate for this interface.

Daily Traffic		Displays traffic information of the day in a table.
Monthly Traffic		Displays traffic information of the in a table.
Top 10 Traffic		Shows the top 10 traffic of the day records.
Service Zone – Default, SZ1~SZ8	**Mode**	The operation mode of the SZ.
	MAC Address	The MAC address of the SZ.
	IP Address	The IP address of the SZ.
	Subnet Mask	The Subnet Mask of the SZ.
	IPv6 Address	The IPv6 address of the SZ
Service Zone – DHCP Scope (Default, SZ1~SZ8)	**Status**	Enable/disable stands for status of the DHCP server in Default Service Zone
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.

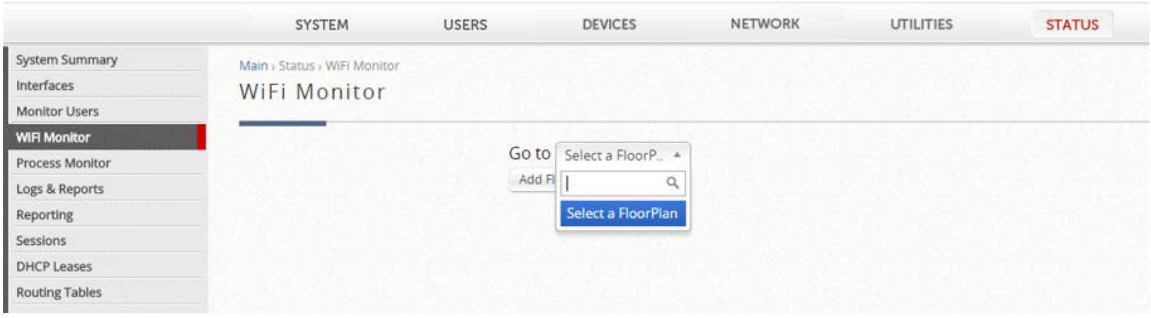
3) Monitor Users

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.
- **Cross Gateway Roaming In User:** Roaming Users authenticated at roaming peer controllers.
- **On-Demand 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

4) WiFi Monitor

To run the WiFi Monitor, first create a floor plan to start 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.


SYSTEM
USERS
DEVICES
NETWORK
UTILITIES
STATUS
System Summary
Interfaces
Monitor Users
WiFi Monitor
Process Monitor
Logs & Reports
Reporting
Sessions
DHCP Leases
Routing Tables

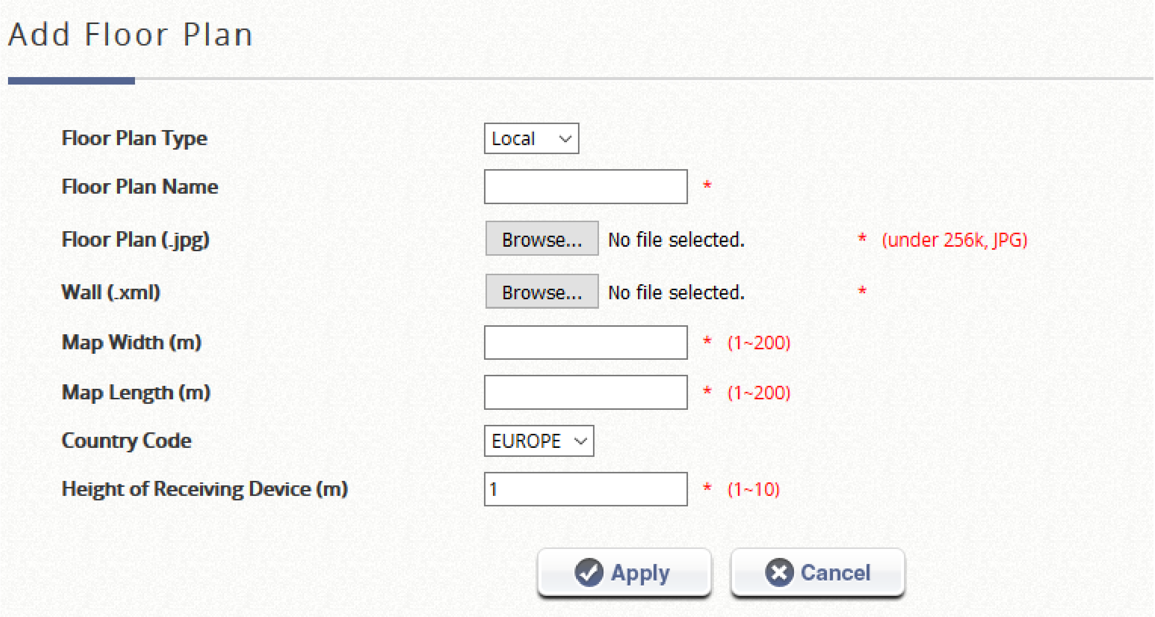
Main › Status › WiFi Monitor

WiFi Monitor

Go to Select a FloorP..

Add Fl

Select a FloorPlan

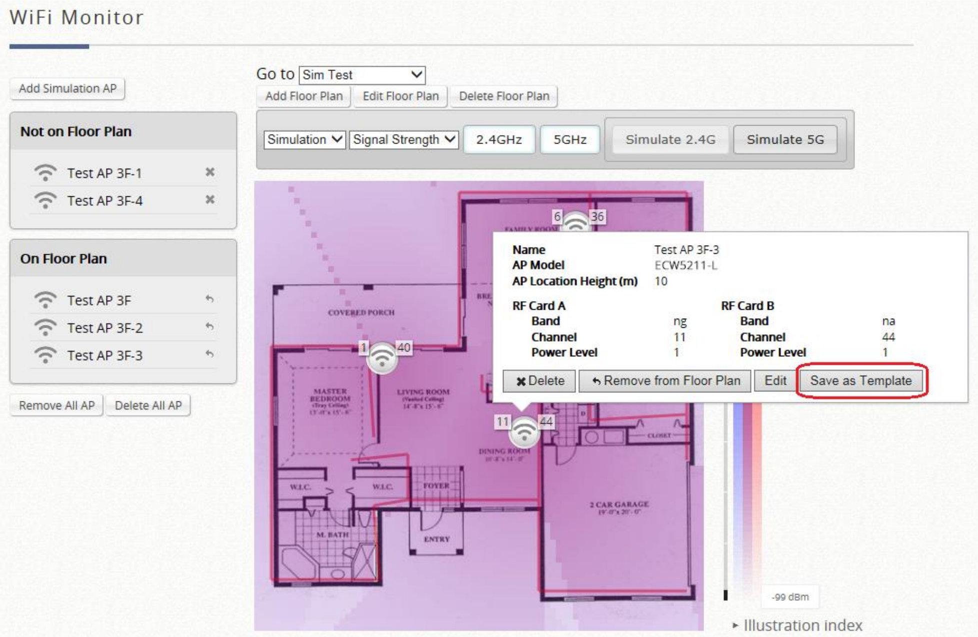


Add Floor Plan

Floor Plan Type	Local	
Floor Plan Name		*
Floor Plan (.jpg)	Browse... No file selected.	* (under 256k, JPG)
Wall (.xml)	Browse... No file selected.	*
Map Width (m)		* (1~200)
Map Length (m)		* (1~200)
Country Code	EUROPE	
Height of Receiving Device (m)	1	* (1~10)

Apply
Cancel

- **Floor Plan Name:** Self-defined name for Administrator’s reference.
- **Floor Plan:** Select file for floor plan (.jpg format).
- **Wall:** Select file for wall (.xml format).
- **Map Width:** Actual width of floor plan.
- **Map Length:** Actual length of floor plan.
- **Country Code:** Select the country code (EU/US). This will determine the max output power of access points
- **Height of Receiving Device (m):** The assumed average height of receiving client devices.


WiFi Monitor
Add Simulation AP
Go to Sim Test
Add Floor Plan
Edit Floor Plan
Delete Floor Plan
Not on Floor Plan
Test AP 3F-1
Test AP 3F-4
On Floor Plan
Test AP 3F
Test AP 3F-2
Test AP 3F-3
Remove All AP
Delete All AP
Simulation
Signal Strength
2.4GHz
5GHz
Simulate 2.4G
Simulate 5G
Delete
Remove from Floor Plan
Edit
Save as Template
-99 dBm
Illustration index

Name	Test AP 3F-3		
AP Model	ECW5211-L		
AP Location Height (m)	10		
RF Card A		RF Card B	
Band	ng	Band	na
Channel	11	Channel	44
Power Level	1	Power Level	1

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.

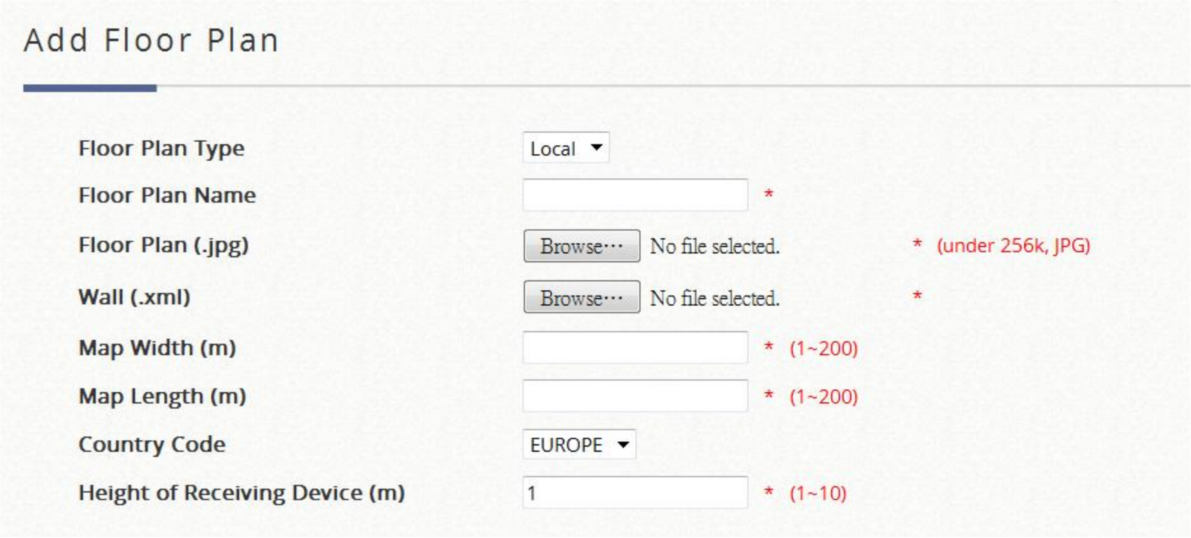
Signal Strength: The darker the color, the stronger the signal strength is.

Coverage: Different colors depict the different coverage area of each AP.

Distribution: Use different colors to illustrate the strength of signals.

5) Managed AP Simulation

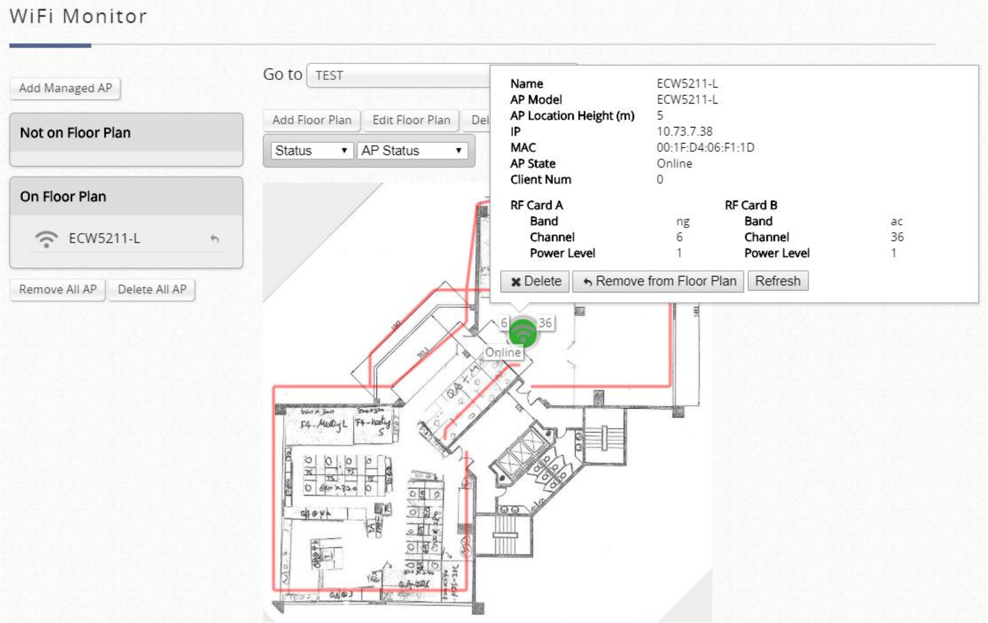
Managed AP Simulation allows administrators to upload a 2-D floor plan for a visualization report of managed APs. Click the ***Add Floor Plan*** button to first add a floor plan.



Add Floor Plan

Floor Plan Type	Local ▾
Floor Plan Name	*
Floor Plan (.jpg)	Browse… No file selected. * (under 256k, JPG)
Wall (.xml)	Browse… No file selected. *
Map Width (m)	* (1~200)
Map Length (m)	* (1~200)
Country Code	EUROPE ▾
Height of Receiving Device (m)	1 * (1~10)

- **Floor Plan Type:** Determine if floor plan will be used for Local Area Managed APs or Wide Area Managed APs.
- **Floor Plan Name:** Self-defined name for Administrator’s reference.
- **Floor Plan:** Select file for floor plan (.jpg format).
- **Wall:** Select file for wall (.xml format).
- **Map Width:** Actual width of floor plan.
- **Map Length:** Actual length of floor plan.
- **Country Code:** Select the country code (EU/US). This will determine the max output power of access points
- **Height of Receiving Device (m):** The assumed average height of receiving client devices.



WiFi Monitor

Go to TEST

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

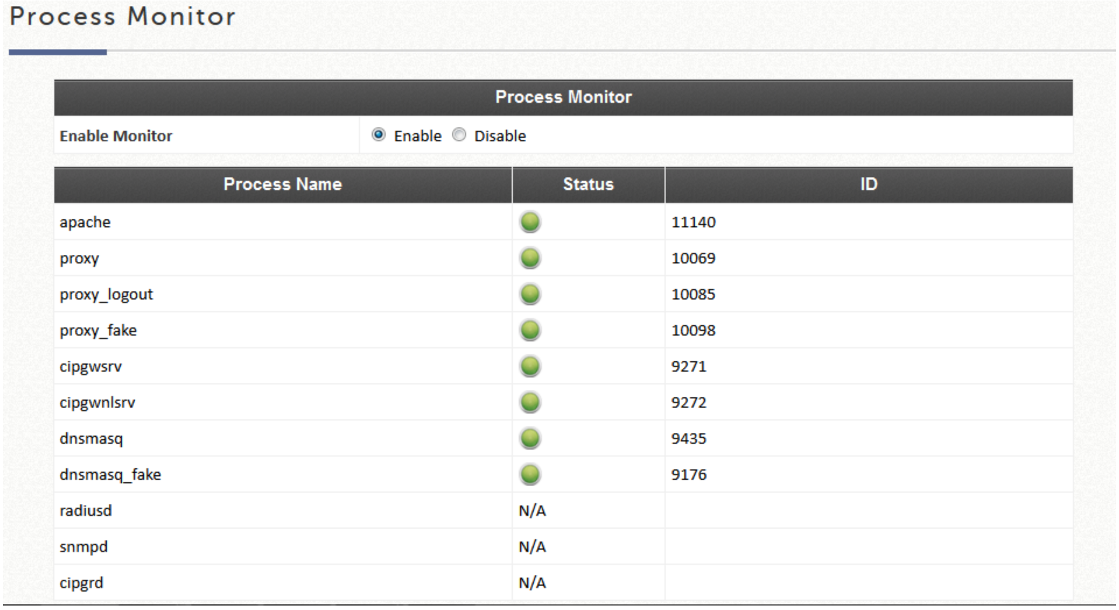
RF Card A		RF Card B	
Band	ng	Band	ac
Channel	6	Channel	36
Power Level	1	Power Level	1

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
Delete
Remove from Floor Plan
Refresh
6
36
Online

Managed APs can then be added using the **Add Managed AP** button.

6) 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	● Enable ○ Disable

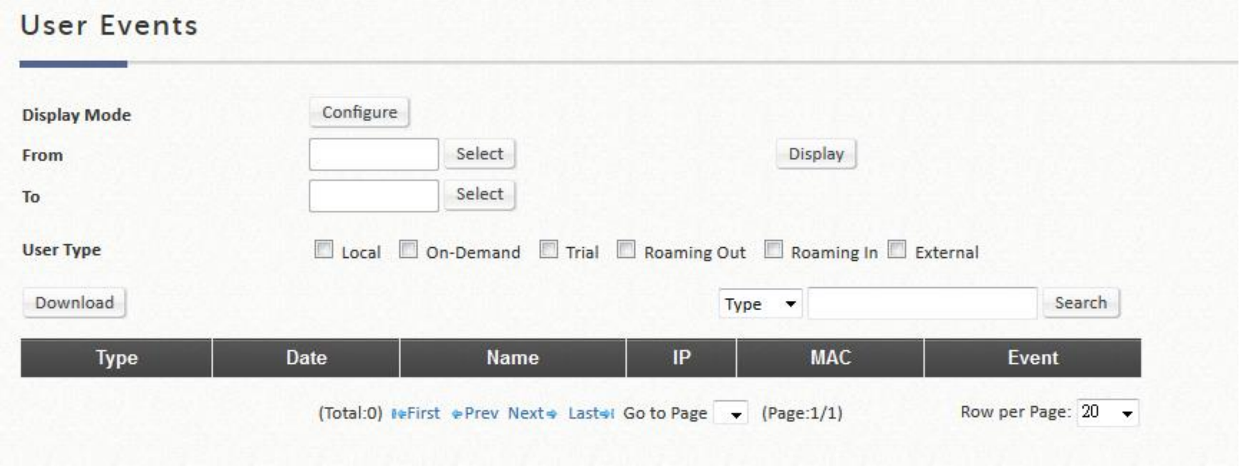
Process Name	Status	ID
apache	●	11140
proxy	●	10069
proxy_logout	●	10085
proxy_fake	●	10098
cipgwsrv	●	9271
cipgwnlsrv	●	9272
dnsmasq	●	9435
dnsmasq_fake	●	9176
radiusd	N/A	
snmpd	N/A	
cipgrd	N/A	

7) 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.


User Events
Display Mode
Configure
From
Select
Display
To
Select
User Type
☐ Local ☐ On-Demand ☐ Trial ☐ Roaming Out ☐ Roaming In ☐ External
Download
Type
Search
Type
Date
Name
IP
MAC
Event
(Total:0) First Prev Next Last Go to Page (Page:1/1)
Row per Page: 20

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**.

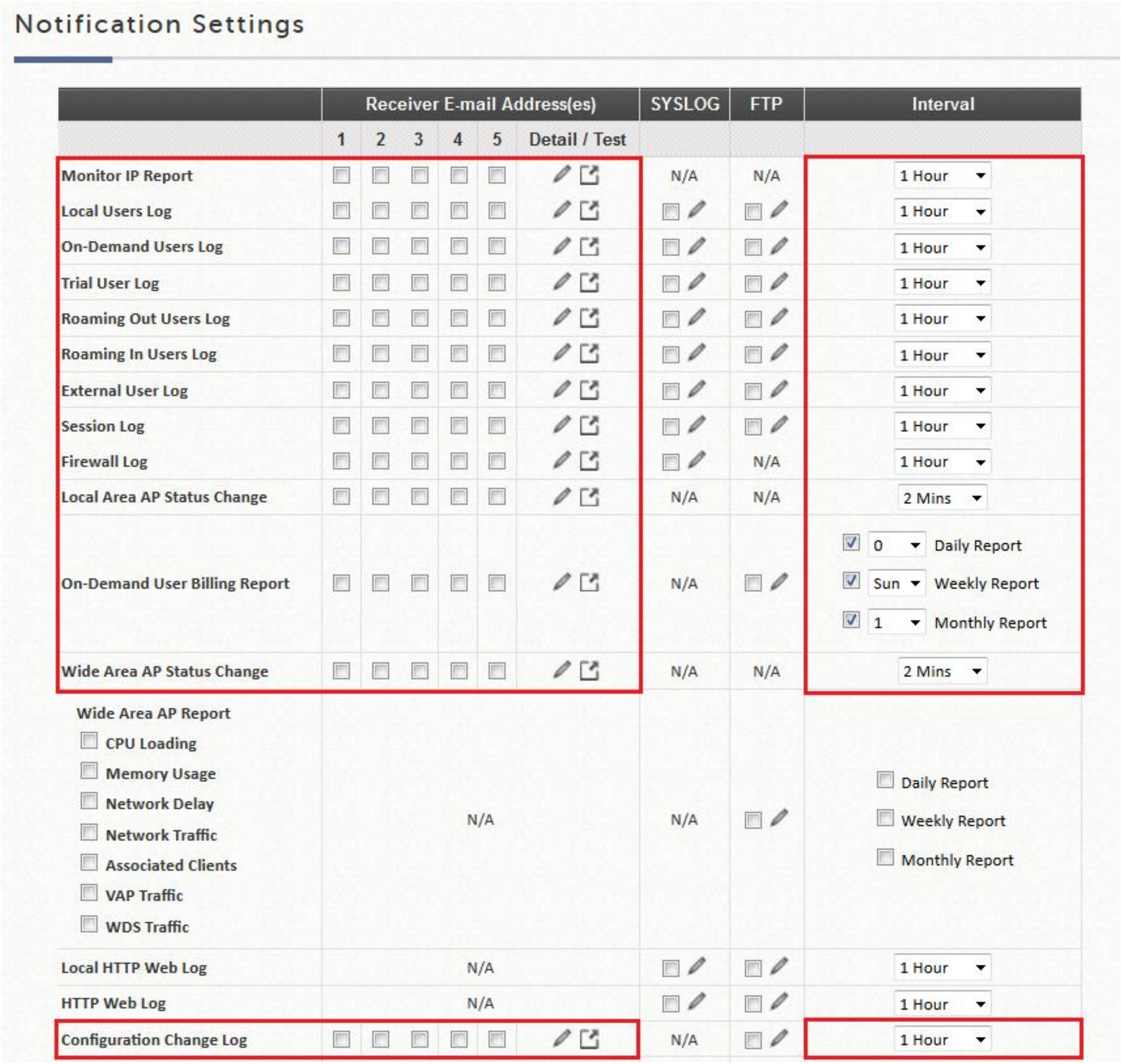
8) Reporting

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.



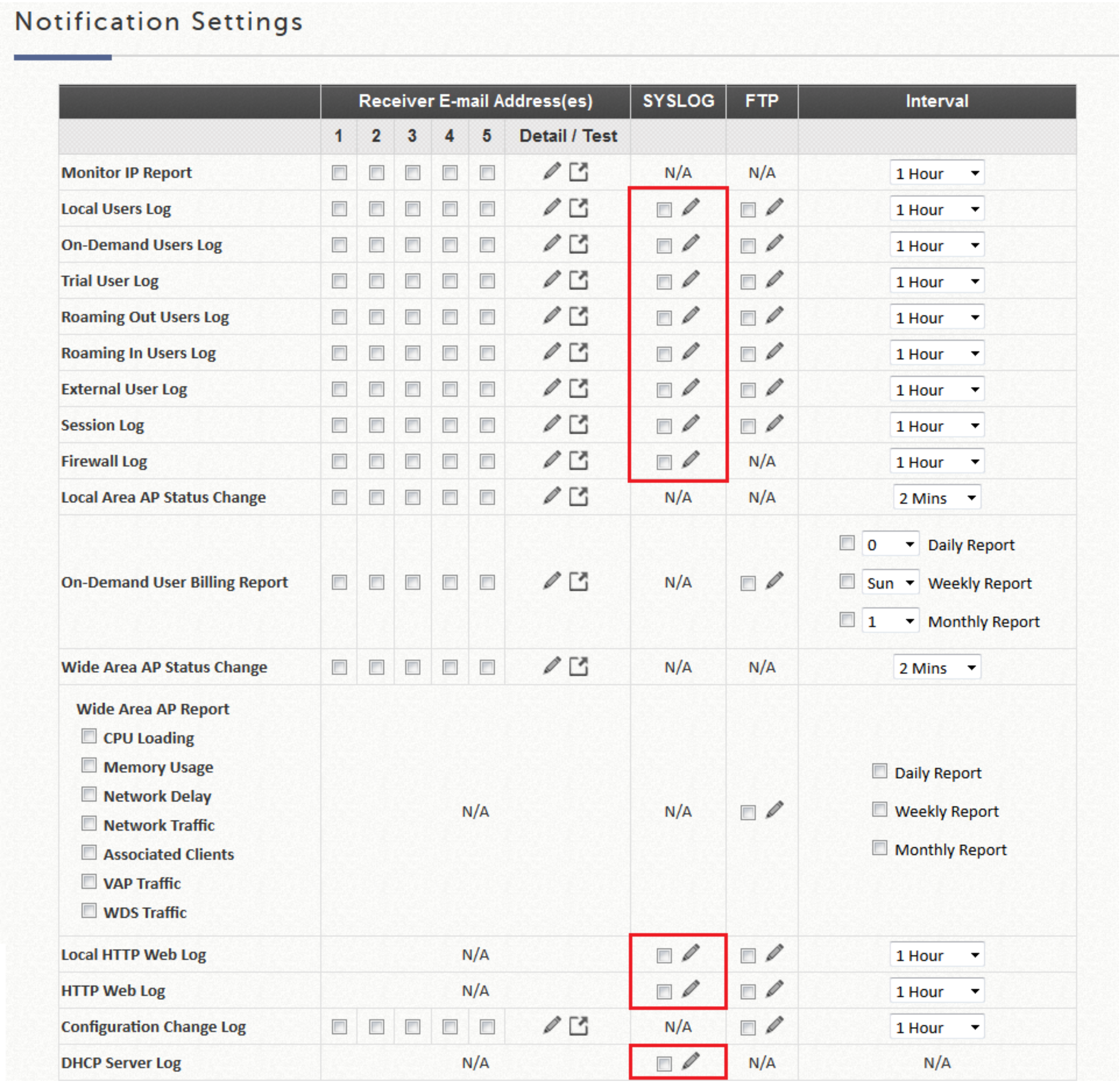
Notification Settings

	Receiver E-mail Address(es)						SYSLOG	FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	1 Hour ▾
Local Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
On-Demand Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Trial User Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Roaming Out Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Roaming In Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
External User Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Session Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Firewall Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	N/A	1 Hour ▾
Local Area AP Status Change	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	2 Mins ▾
On-Demand User Billing Report	☐	☐	☐	☐	☐	✎ ↗	N/A	☐ ✎	☑ 0 ▾ Daily Report ☑ Sun ▾ Weekly Report ☑ 1 ▾ Monthly Report
Wide Area AP Status Change	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	2 Mins ▾
Wide Area AP Report ☐ CPU Loading ☐ Memory Usage ☐ Network Delay ☐ Network Traffic ☐ Associated Clients ☐ VAP Traffic ☐ WDS Traffic	N/A						N/A	☐ ✎	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Local HTTP Web Log	N/A						☐ ✎	☐ ✎	1 Hour ▾
HTTP Web Log	N/A						☐ ✎	☐ ✎	1 Hour ▾
Configuration Change Log	☐	☐	☐	☐	☐	✎ ↗	N/A	☐ ✎	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

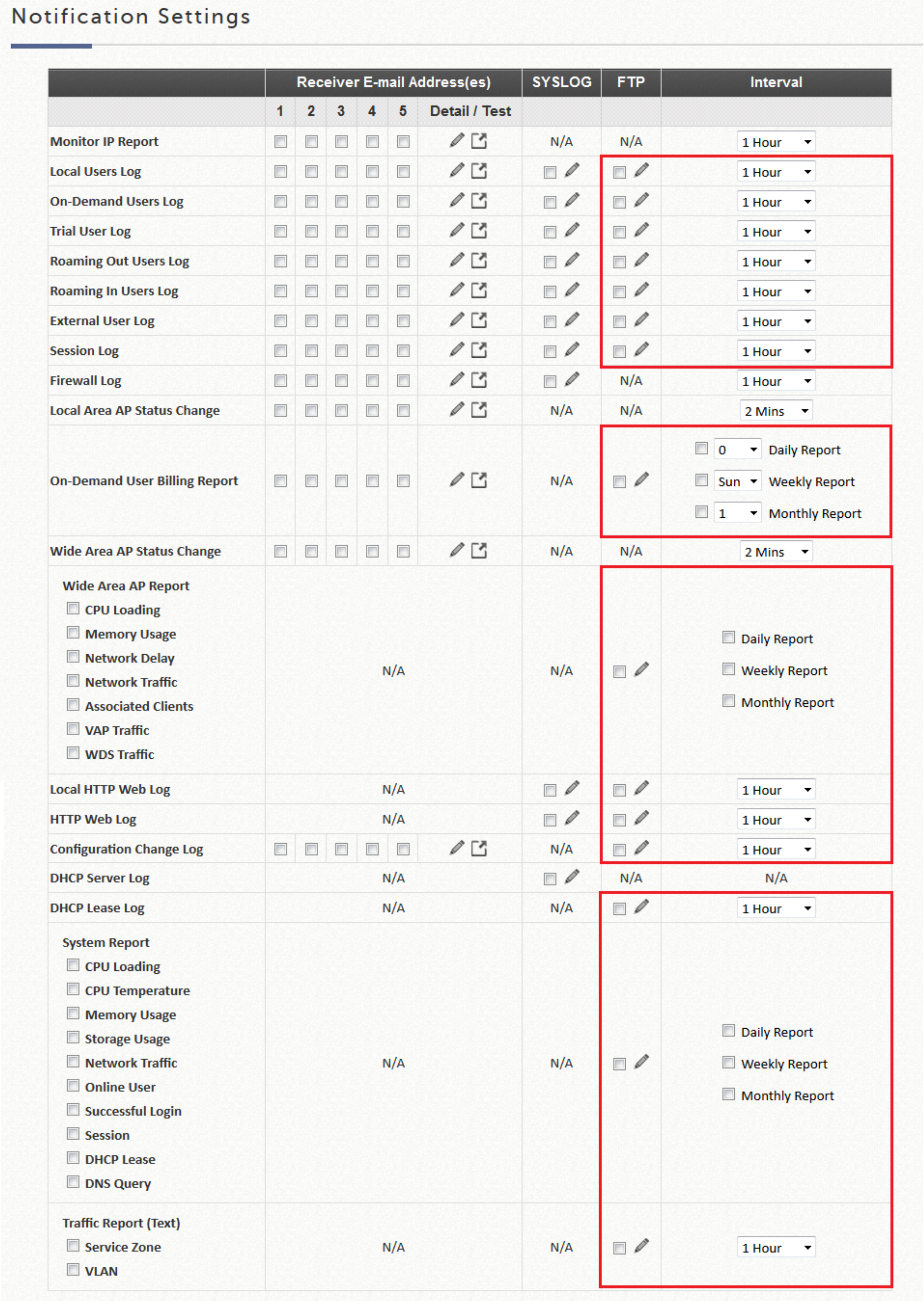
	Receiver E-mail Address(es)						SYSLOG	FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	1 Hour ▾
Local Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
On-Demand Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Trial User Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Roaming Out Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Roaming In Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
External User Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Session Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Firewall Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	N/A	1 Hour ▾
Local Area AP Status Change	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	2 Mins ▾
On-Demand User Billing Report	☐	☐	☐	☐	☐	✎ ↗	N/A	☐ ✎	☐ 0 ▾ Daily Report ☐ Sun ▾ Weekly Report ☐ 1 ▾ Monthly Report
Wide Area AP Status Change	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	2 Mins ▾
Wide Area AP Report ☐ CPU Loading ☐ Memory Usage ☐ Network Delay ☐ Network Traffic ☐ Associated Clients ☐ VAP Traffic ☐ WDS Traffic	N/A						N/A	☐ ✎	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Local HTTP Web Log	N/A						☐ ✎	☐ ✎	1 Hour ▾
HTTP Web Log	N/A						☐ ✎	☐ ✎	1 Hour ▾
Configuration Change Log	☐	☐	☐	☐	☐	✎ ↗	N/A	☐ ✎	1 Hour ▾
DHCP Server Log	N/A						☐ ✎	N/A	N/A

- **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	FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	1 Hour ▾
Local Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
On-Demand Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Trial User Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Roaming Out Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Roaming In Users Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
External User Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Session Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	☐ ✎	1 Hour ▾
Firewall Log	☐	☐	☐	☐	☐	✎ ↗	☐ ✎	N/A	1 Hour ▾
Local Area AP Status Change	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	2 Mins ▾
On-Demand User Billing Report	☐	☐	☐	☐	☐	✎ ↗	N/A	☐ ✎	☐ 0 ▾ Daily Report ☐ Sun ▾ Weekly Report ☐ 1 ▾ Monthly Report
Wide Area AP Status Change	☐	☐	☐	☐	☐	✎ ↗	N/A	N/A	2 Mins ▾
Wide Area AP Report ☐ CPU Loading ☐ Memory Usage ☐ Network Delay ☐ Network Traffic ☐ Associated Clients ☐ VAP Traffic ☐ WDS Traffic	N/A						N/A	☐ ✎	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Local HTTP Web Log	N/A						☐ ✎	☐ ✎	1 Hour ▾
HTTP Web Log	N/A						☐ ✎	☐ ✎	1 Hour ▾
Configuration Change Log	☐	☐	☐	☐	☐	✎ ↗	N/A	☐ ✎	1 Hour ▾
DHCP Server Log	N/A						☐ ✎	N/A	N/A
DHCP Lease Log	N/A						N/A	☐ ✎	1 Hour ▾
System Report ☐ CPU Loading ☐ CPU Temperature ☐ Memory Usage ☐ Storage Usage ☐ Network Traffic ☐ Online User ☐ Successful Login ☐ Session ☐ DHCP Lease ☐ DNS Query	N/A						N/A	☐ ✎	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Traffic Report (Text) ☐ Service Zone ☐ VLAN	N/A						N/A	☐ ✎	1 Hour ▾

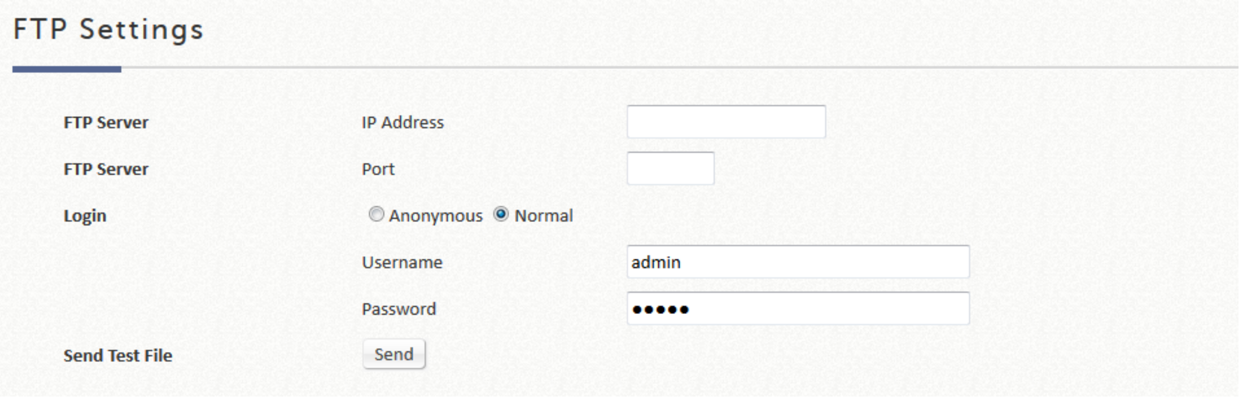
Detail: Clicking this button allows the specification of the FTP server folder where the logs sent will be stored on the

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:

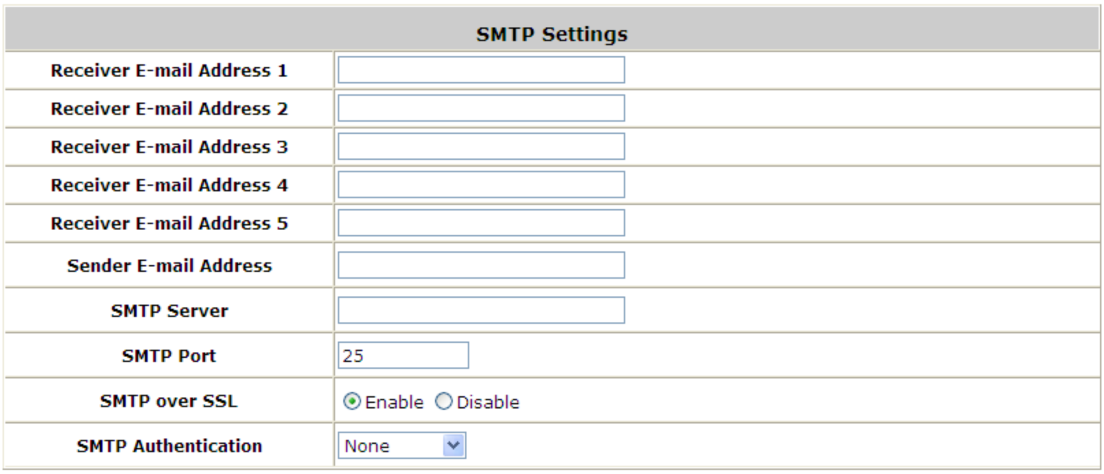


FTP Settings

FTP Server	IP Address	
FTP Server	Port	
Login	○ Anonymous ● Normal	
	Username	admin
	Password	•••••
Send Test File	Send	

- **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.



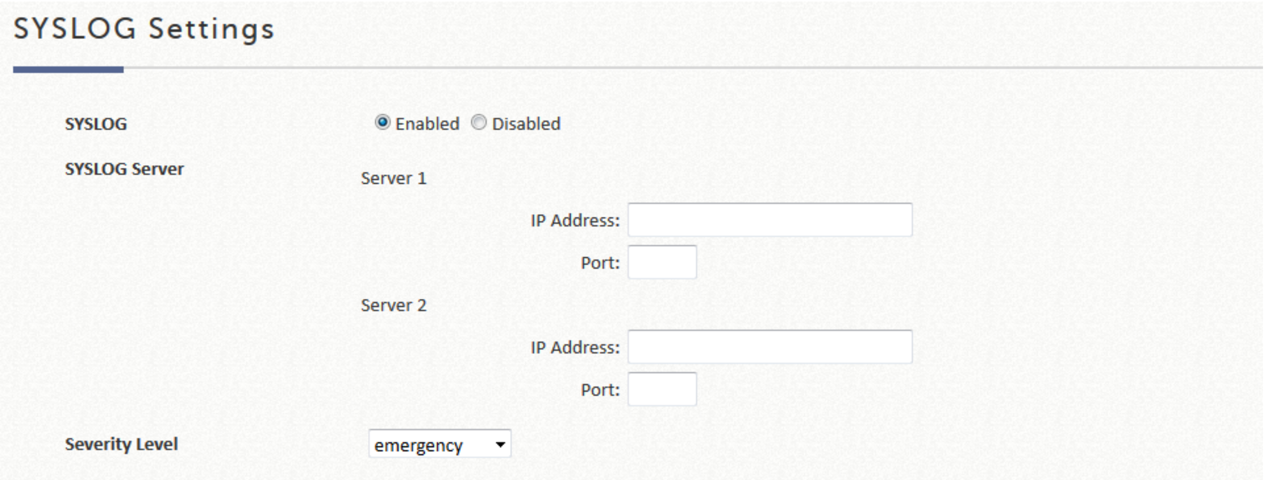
SMTP Settings	
Receiver E-mail Address 1	
Receiver E-mail Address 2	
Receiver E-mail Address 3	
Receiver E-mail Address 4	
Receiver E-mail Address 5	
Sender E-mail Address	
SMTP Server	
SMTP Port	25
SMTP over SSL	● Enable ○ Disable
SMTP Authentication	None

- **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 can not 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:



SYSLOG Settings

SYSLOG ● Enabled ○ Disabled

SYSLOG Server

Server 1

IP Address:

Port:

Server 2

IP Address:

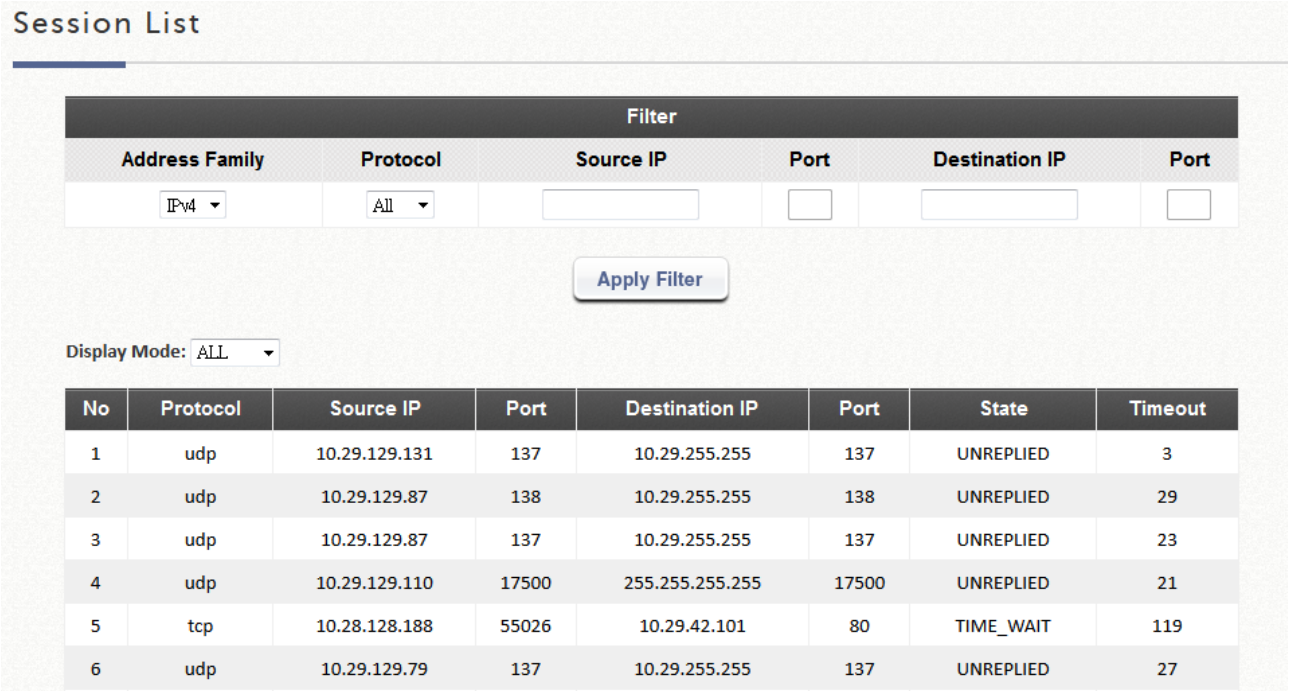
Port:

Severity Level emergency

- **SYSLOG Destinations:** Up to two external SYSLOG servers may be configured. Please enter the IP address and port number of the external SYSLOG server here.
- **System Log:** This controls the enabling/disabling of the SYSLOG logging feature. When enabled, the selected logs from "Notification Settings" will be sent to the SYSLOG server configured above. However, when disabled, no logs will be sent to the SYSLOG server configured above.

9) 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				

Display Mode: ALL

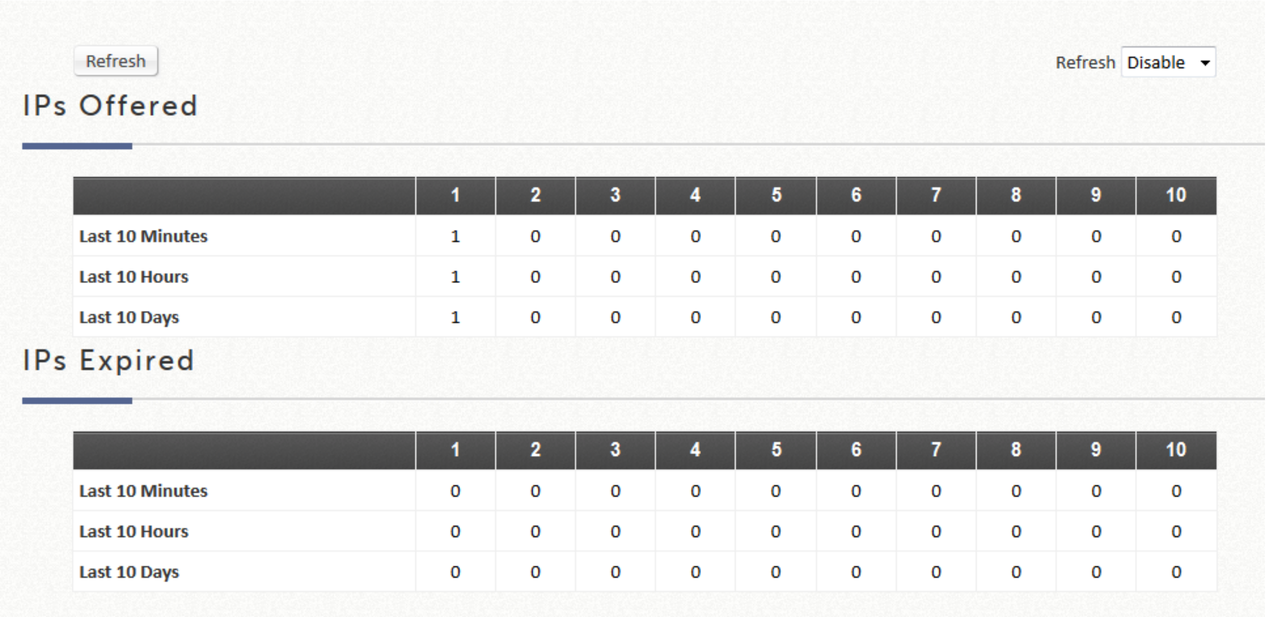
No	Protocol	Source IP	Port	Destination IP	Port	State	Timeout
1	udp	10.29.129.131	137	10.29.255.255	137	UNREPLIED	3
2	udp	10.29.129.87	138	10.29.255.255	138	UNREPLIED	29
3	udp	10.29.129.87	137	10.29.255.255	137	UNREPLIED	23
4	udp	10.29.129.110	17500	255.255.255.255	17500	UNREPLIED	21
5	tcp	10.28.128.188	55026	10.29.42.101	80	TIME_WAIT	119
6	udp	10.29.129.79	137	10.29.255.255	137	UNREPLIED	27

10) 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.



IPs Offered

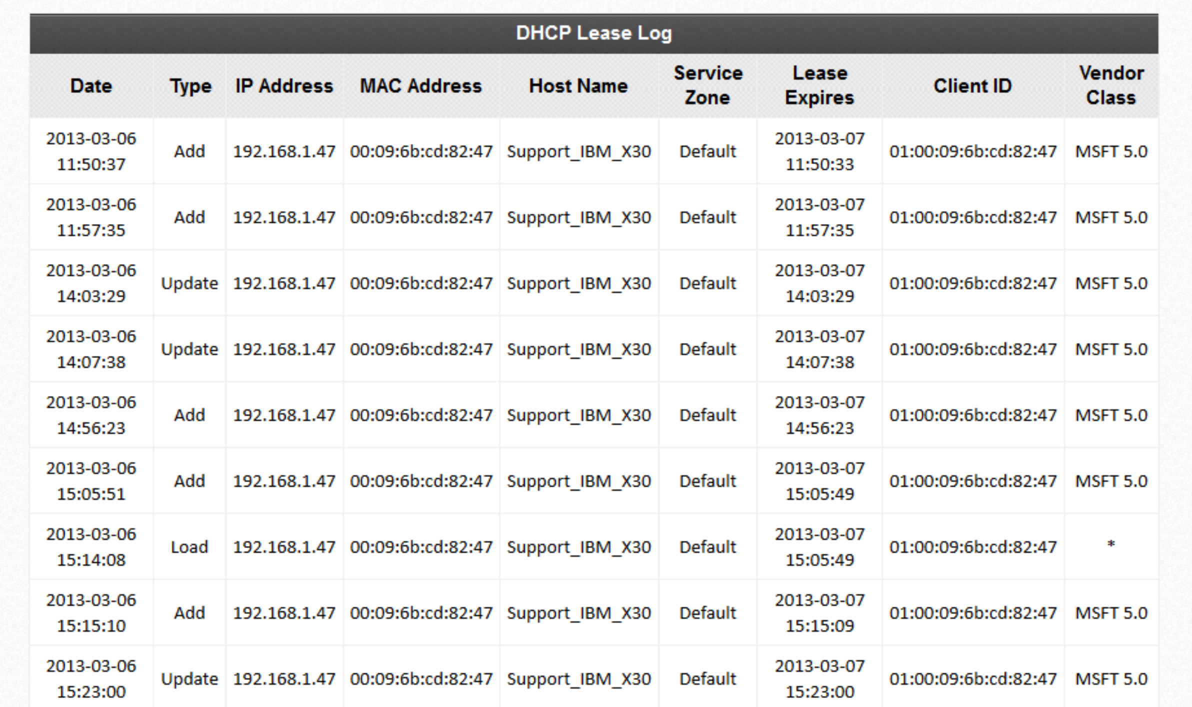
	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	1	0	0	0	0	0	0	0	0	0
Last 10 Hours	1	0	0	0	0	0	0	0	0	0
Last 10 Days	1	0	0	0	0	0	0	0	0	0

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.

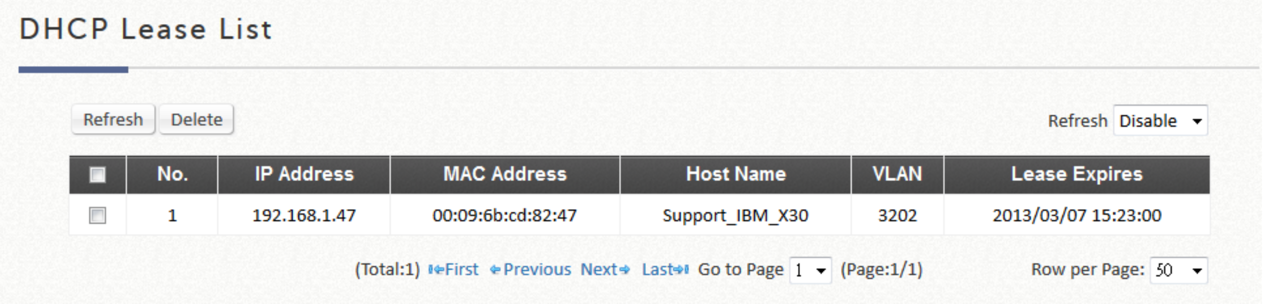


DHCP Lease Log

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.



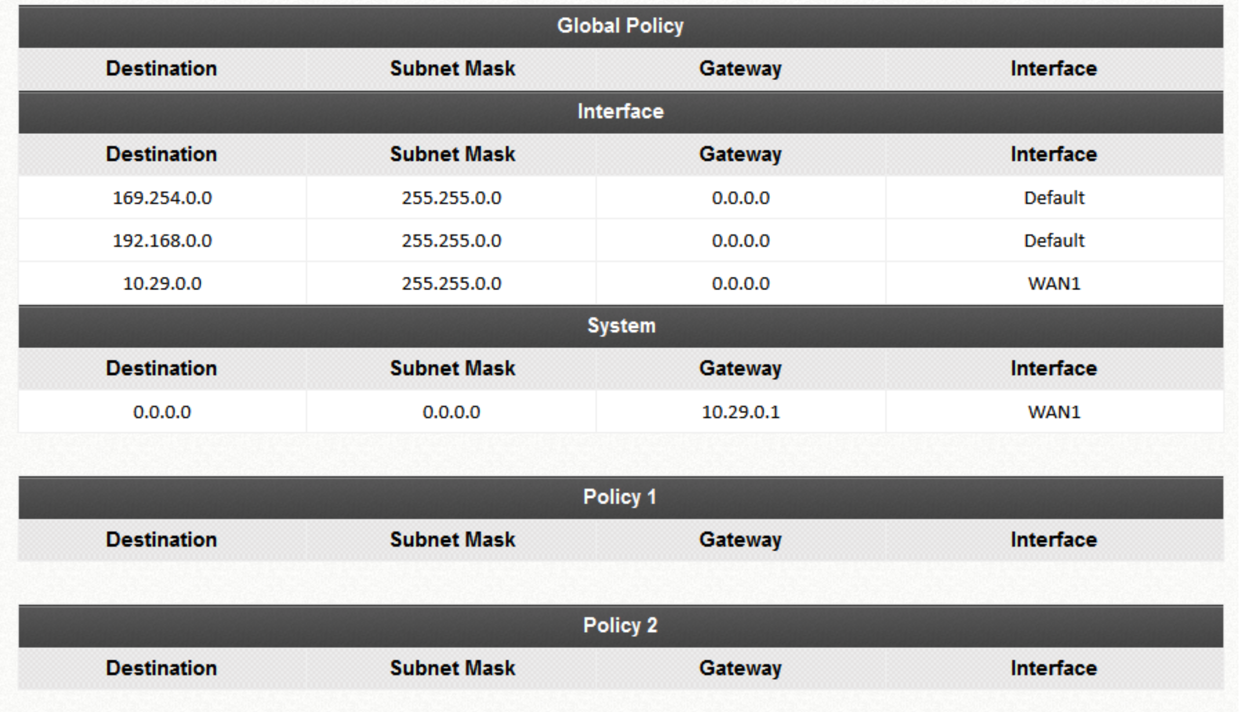
Refresh Disable

☐	No.	IP Address	MAC Address	Host Name	VLAN	Lease Expires
☐	1	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	3202	2013/03/07 15:23:00

(Total:1) Go to Page 1 (Page:1/1) Row per Page: 50

11) 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.

Appendix E. Advanced Features

1. RADIUS authentication for equipment administration and configuration

The system allows administrators to log in by authenticating against a back-end RADIUS server. Configuration steps:

1. Enable an external RADIUS server for administrators' authentication.
2. Add a new administrative account on the RADIUS server.
3. Log into the WMI with the new RADIUS account.

2. Automatic and continuous RF scanning for detection of rogue APs and interferences

Rogue APs and radio interferences can be identified by the system (Controller and Sensor APs). Configuration steps:

Rogue APs:

1. Configure third-party APs to act as Rogue APs.
2. Enable "Rogue AP Detection" and set "Scanning Interval" (Main Menu > Devices > WAPM > Rogue AP Detection >> General Configuration).
3. Enable one or more managed, legitimate APs to act as "Sensors" (Main Menu > Devices > WAPM >> Rogue AP Detection > General Configuration >> Sensor List) to scan for Rogue APs.
4. Once Rogue APs are detected (when any BSSID which is not under management is found, this AP will be regarded as a Rogue AP), each Rogue AP will be presented with relevant information in the "Rogue AP List".
5. Manually select any of the APs on this list, if they are legitimate, to add into the "Trusted AP List".

Radio Interferences:

Enable "Interference Detection" by setting "Utilization Threshold" of the existing APs (AP WMI: Home > Wireless > General).

3. Operator authentication through local base and through RADIUS

Rogue APs and radio interferences can be identified by the system (Controller and Sensor APs). Configuration steps:

1. Log in with the default administrative account (Username = admin).
2. Enable an external RADIUS server for administrators' authentication.
3. Add a new operator account (Username = operator1) on the RADIUS server.
4. Enter the WMI in a second administrative PC.
5. Log into the WMI with the new RADIUS account (Username = operator1).

4. System dashboard page allows for customization

The system Dashboard page allows for page customization to include system alarms and performance statistics. Configuration steps:

1. Go to the system Dashboard page (Main Menu > Status >> System Summary).
2. Add and remove the items of system alarms or performance

5. Equipment visualization by device type

The system provides visualization of client devices by the device type:

1. Go to "User Events" page (Main Menu > Status > Logs and Reports > User Events).
2. The table includes user event entries which has "Device Type" as the default column.

6. System allows to import an "Access Control" list file of APs

The system Dashboard page allows for page customization to include system alarms and performance statistics. Configuration steps:

1. Go to "WAPM AP List" page (Main Menu > Devices > WAPM > AP List).
2. Click on "Import" to import an "Access Control" file (containing MAC address and Serial Number of all APs to be installed).

7. Generate more reports on the managed APs

The system provides reports that contain the following information: Name of AP; Location; Availability; Traffic Transmitted and Received by Radio; Access points classified by traffic volume; Access points classified by number of customers; Maximum number of clients; Average customer; Average AP usage (traffic); Peak AP usage (traffic); Total session time; Configuration steps:

1. Go to "WAPM Overview" page (Main Menu > Devices > WAPM >> Overview).
2. Click on "Customize Monitored Items" on the AP List, and select the items from the available items.
3. Click on "Generate Report" to export the information on Overview page and save it as a file.

8. Report AP failures

Failures of managed APs can be reported to administrators by email. Configuration steps: Check the settings "Receiver E-mail Address(es)" for the "Wide Area AP Status Change Offline" log and set the "Interval" in "Notification Settings" (Main Menu > Status > Reporting >> Notification Settings).

9. Current associated clients report and SSID statistics

The system provides the information about associated clients and SSID statistics of managed APs. Configuration steps:

1. Go to "WAPM AP List" (Main Menu > Devices > WAPM >> AP List).
2. Click on "Customize Monitored Items" on the AP List, and select "Client" and "SSID" from the available items.
3. Click on the "Client" number of an AP on the AP List to view the information of clients that are associated to the AP.
4. Click on the "SSID" name of an AP on the AP List to view the information of SSID.
5. Click on "Generate Report" to export the information on the AP List and save it as a file.

10. SNR reporting on the APs

The system Dashboard page allows for page customization to include system alarms and performance statistics. Configuration steps:

1. Go to WAPM AP List (Main Menu > Devices > WAPM >> AP List).
2. Click on the "Client" number of an AP on the AP List to view the SNR information of clients that are associated to the AP.