

Application Scenario Guide

Enterprise

Release: July 2017

Release Version: R1

TABLE OF CONTENT

1	INTRODUCTION.....	2
2	PROJECT REQUIREMENTS	2
2.1	FEATURE REQUIREMENTS:	2
3	PROPOSED SOLUTION	3
3.1	BOM:	3
3.2	NETWORK TOPOLOGY:.....	3
3.3	EXPECTED RESULTS:.....	3
3.3.1	<i>Captive Portal with Company Logo</i>	3
3.3.2	<i>Staff and Guest connect to the same SSID</i>	4
4	CONFIGURATION	9
4.1	CONFIGURATION CHECKLIST	9
4.2	SYSTEM – INITIAL ACCESS BROWSER-BASED GUI	10
4.3	SYSTEM – WAN & LAN INTERFACE CONFIGURATION.....	11
4.4	SYSTEM - MANAGEMENT IP ADDRESS LIST	12
4.5	UTILITIES - ADMIN PASSWORD RECOVERY.....	13
4.6	SYSTEM - SERVICE ZONES CONFIGURATION.....	14
4.7	SYSTEM - SERVICE ZONE – CAPTIVE PORTAL CUSTOMIZATION.....	17
4.8	USERS - LOCAL ACCOUNTS	19
4.9	USERS – GUEST AUTHENTICATION.....	21
4.10	USERS – USER POLICIES CONFIGURATION.....	22
4.10.1	<i>Guest Users → Policy 1 profile configuration</i>	22
4.9.1	<i>Staff Users → Policy 2 profile configuration</i>	24
4.10	USERS – USER GROUPS CONFIGURATION.....	27
4.11	USE WAPM ON EWS TO MANAGE ECW	29
4.11.1	<i>Edit WAPM Templates</i>	29
4.11.2	<i>Establish CAPWAP Tunnel from AP to EWS</i>	32
4.11.3	<i>Applying the template</i>	34
4.12	1+1 HIGH AVAILABILITY	36
4.12.1	<i>Configure EWS#1 HA</i>	36
4.12.2	<i>Configure EWS#2</i>	36
4.12.3	<i>Confirm HA status of both EWS</i>	37
4.13	REPORTING	37
4.13.1	<i>Notification</i>	37
4.13.2	<i>FTP Setting</i>	38
4.13.3	<i>SMTP Setting</i>	39
4.13.4	<i>Syslog Setting</i>	39

1 Introduction

In this Application Scenario Guideline we will illustrate an actual Enterprise deployment, including its requirements and the corresponding solution and configurations.

The purpose of this guideline is to provide step-by-step configuration instructions that may also be applied to other enterprise deployments.

2 Project Requirements

2.1 Deployment Requirements:



Enterprise Building Wi-Fi
<ul style="list-style-type: none">- Wall or ceiling mounted- Dual-band 2x2 MIMO Technique- Coverage is the top priority- External antenna- Extra LAN port with PoE downlink capability
Network Gateway-Controller
<ul style="list-style-type: none">- Estimated 3500 concurrent users- Centralized manage 1200 APs- Standby unit for service redundancy

2.2 Feature Requirements:

Wi-Fi Features
<ul style="list-style-type: none">- Customizable Captive Portal (Login Page) for guest to submit credentials- User Authentication for granting Wi-Fi access- SSID with WPA2-Enterprise security (802.1x Transparent Login)- Multiple concurrent devices login limit via the same account- Centralized Management for APs at each site- Built-in DHCP server in solution to allocate IP addresses to all users
Administrator Features
<ul style="list-style-type: none">- 1+1 High Availability to maintain network service- Periodic Usage Reports to track- GUI permission for Staff only- Websites access limitation for Staff users

3 Proposed Solution

3.1 Recommended Edgecore Models:

ECW	EWS
	
<ul style="list-style-type: none"> - 802.11ac wave 2 Dual-band - 2x2 MIMO - Internal antennas in 2.4GHz/5GHz, 2dBi/2dBi, 3 dBi (BLE) - Output power 2.4GHz/5GHz, 18dBm/19 dBm 	<ul style="list-style-type: none"> - 5000 recommended concurrent users - 1200 APs managed - High Availability 1+1 - Power Redundancy

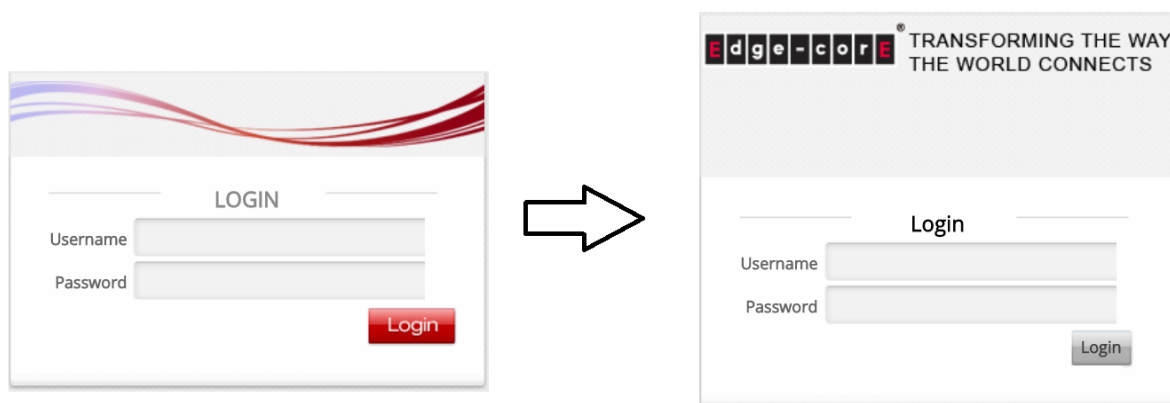
Location	Area	AP Model	QTY
Factory	500m ² x 40 sties	ECW	400
Office	300m ² x 40 floors x 2 buildings	ECW	800

3.2 Network Topology:

3.3 Expected Results:

3.3.1 Captive Portal with Company Logo

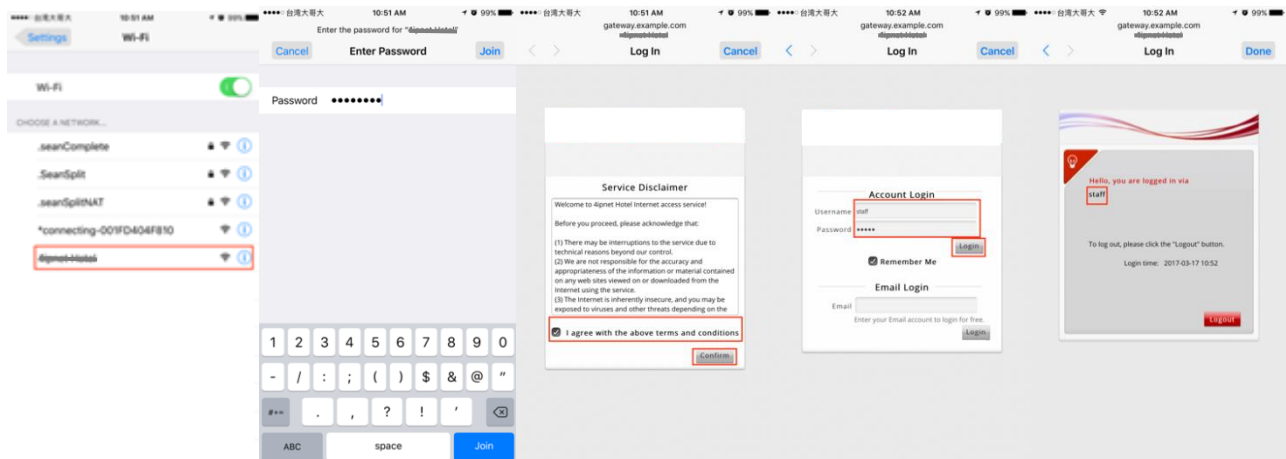
The customizable Login Page allows MIS administrators to easily change the logo on the top with their most current advertisement images.



3.3.2 Staff and Guest connect to the same SSID

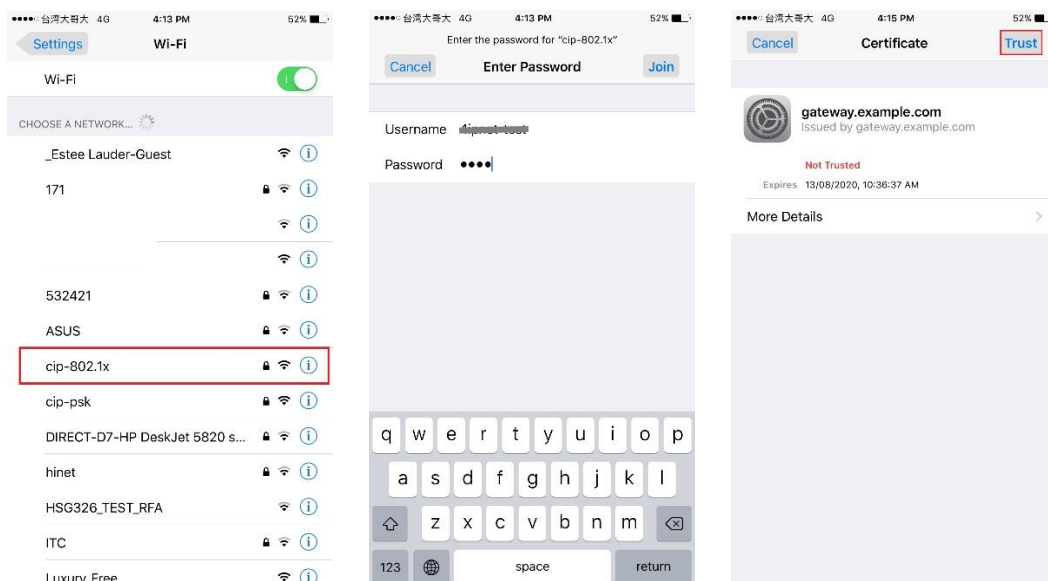
User Login Flow (UAM) – Staff/Guest account

After connecting to the SSID, a Service Disclaimer page will pop up. The user will need to tick the checkbox and click on the Confirm button move on to the Login Page. Enter staff/staff for the username/password or complete the E-mail field and click Login. The Login Success Page will show up after.



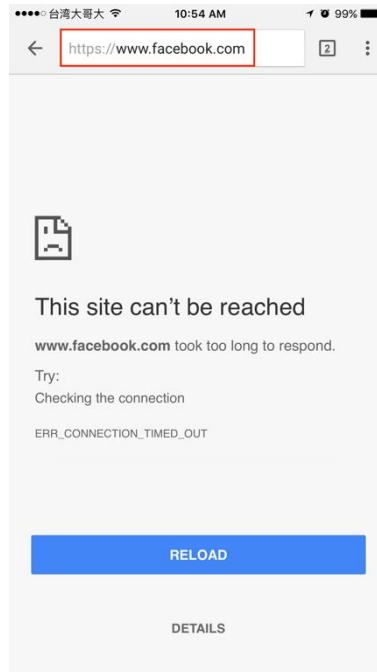
User Login Flow (WPA2-Enterprise) – Staff account

Client devices associated with the SSID and enter the account username/password to authentication. Once the profile been build and trust, the device could auto transparent connect to the same SSID, simplify the user login flow.



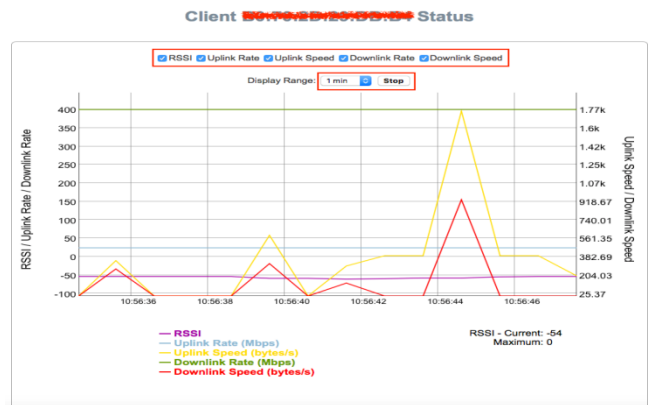
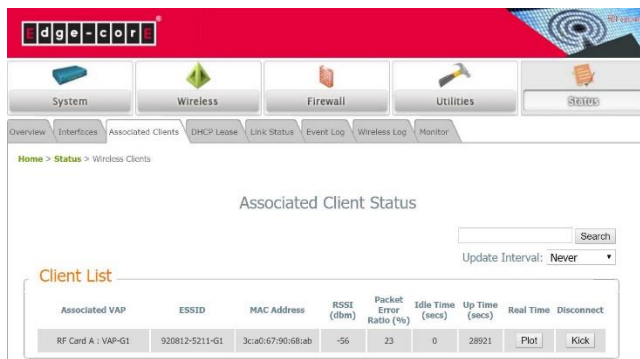
Facebook access blocked for Staff accounts

The Staff Users belong to Staff Group with specific Firewall Rule for blocking their traffics to Facebook website. So, after Staff users have successfully logged in, they cannot reach to www.facebook.com.



Real time and daily network usage reports

When the user successfully associates to the SSID, AP's Associated Clients List will display each of their connection details. By clicking Plot button, administrator may check the real-time plotting diagram about user traffics. By clicking Kick button, administrator may manually disconnect this user.



Before user successfully logged in, administrator may observe them on EWS's *Non-Login Devices*. After user successfully logged in by their accounts, EWS's *Online Users List* will have their real-time information.



Last, the administrator may go to *User Events* for granting the statistics about each kind of users' usage information by selecting the correct parameters.

The screenshot shows the 'User Events' page. The configuration section includes a 'From' date dropdown set to '2017-03-17', a 'To' date dropdown set to '2017-03-17', and a 'User Type' section with radio buttons for 'Local', 'On-Demand', 'Guest', 'Roaming Out', 'Roaming In', and 'External'. A 'Display' button is also present. Below the configuration is a table with the following data:

Type	Date	Name	IP	MAC	Vlan ID	Event	Group	Policy	Max Download	Max Upload	Req Download	Req Upload	Packets In	Packets out
Local - Mobile	2017-03-17 10:52:16 +0800	staff@local	192.168.1.158	08:00:27:00:00:00	0	Login	Staff	2	Unlimited	Unlimited	Unlimited	Unlimited	0	0
Local - Mobile	2017-03-17 10:57:10 +0800	staff@local	192.168.1.158	08:00:27:00:00:00	0	Logout	Staff	2					12789	12193
Guest - Mobile	2017-03-17 10:58:21 +0800	suppppp@suppppppp	192.168.1.158	08:00:27:00:00:00	0	Login	Guest	1	1mbit	1mbit	512kbit	512kbit	0	0
Guest - Mobile	2017-03-17 11:01:12 +0800	suppppp@suppppppp	192.168.1.158	08:00:27:00:00:00	0	Logout	Guest	1					16674	11547

The administrator could monitor the *System Report* to confirm status of each items.

The screenshot shows the 'System Report' page. The configuration section includes a dropdown for 'Item' set to 'Network Traffic', a dropdown for 'Interface' set to 'WAN1', and a dropdown for 'Display Interval' set to '1 Week'. Below the configuration is a line graph titled 'Network Traffic' showing 'Bytes per second' on the y-axis (0 to 140 KB) and time on the x-axis (24 Jun to 29 Jun). The graph shows two lines: RX (green) and TX (blue).

GUI permission only for Staff Users

Check the appropriate SZs and the preferred IP Addresses to allow access permission.

The screenshot shows the Management Service configuration page. At the top, there are tabs for SYSTEM, USERS, DEVICES, NETWORK, UTILITIES, and STATUS. The left sidebar lists various configuration options like General, WAN, IPv6, LAN Ports, Service Zones, Port Location Mapping, and PMS Interface. The main content area is titled 'Management Service' and includes sections for enabling services, a list of service zones, and a list of IP addresses.

Management Service

SSH Service Enable Disable
Telnet Service Enable Disable

Enable/Disable SSH or Telnet for troubleshooting purposes

Management Service Zone List Allowed IPs in configured SZs to access the EWS's WMI

Active	Status	Service Zone	IP Address/Segment
<input checked="" type="checkbox"/>		Default	192.168.1.254/255.255.255.0
<input type="checkbox"/>		SZ1-Public	172.21.0.254/255.255.0.0
<input type="checkbox"/>		SZ2	172.22.0.254/255.255.0.0
<input type="checkbox"/>		SZ3	172.23.0.254/255.255.0.0
<input type="checkbox"/>		SZ4	172.24.0.254/255.255.0.0
<input type="checkbox"/>		SZ5	172.25.0.254/255.255.0.0
<input type="checkbox"/>		SZ6	172.26.0.254/255.255.0.0
<input type="checkbox"/>		SZ7	172.27.0.254/255.255.0.0
<input type="checkbox"/>		SZ8	172.28.0.254/255.255.0.0

Example: PC connected to LAN Port to receive an IP of 192.168.X.X

Example: Clients connected to SZ1-Public with an IP of 172.21.0.X **cannot** enter the EWS's WMI because it is unchecked.

Management IP Address List Allowed specific IPs & Segments on both LAN/WAN sides

No.	Active	IP Address/Segment
1	<input checked="" type="checkbox"/>	0.0.0.0/0.0.0.0
2	<input type="checkbox"/>	

Example: Allows all IPs (0.0.0.0/0.0.0.0) to connect to the EWS's WMI

4 Configuration

4.1 Configuration Checklist

Items	Configuration paths	Done
3.1 Configuration Checklist		
3.2 Initial Access Browser-based GUI	- <i>Connect admin PC and open a browser</i>	<input type="checkbox"/>
3.3 WAN & LAN Interface Configuration	- <i>System > WAN</i> - <i>System > LAN</i>	<input type="checkbox"/> <input type="checkbox"/>
3.4 Management IP Address List	- <i>System > General > Management IP Address List</i>	<input type="checkbox"/>
3.5 Admin Password Recovery	- <i>Utilities > Administrator Accounts</i>	<input type="checkbox"/>
3.6 Service Zone Configuration	- <i>System > Service Zones</i>	<input type="checkbox"/>
3.7 Service Zone Captive Portal Customization	- <i>System > Service Zones > Service Zone Configuration > Login Page Customization</i>	<input type="checkbox"/>
3.8 Local Accounts	- <i>Users > Internal Authentication > Local</i>	<input type="checkbox"/>
3.9 Guest Authentication	- <i>Users > Internal Authentication > Guest</i>	<input type="checkbox"/>
3.10 User Policies Configuration	- <i>Users > Policies Firewall</i> - <i>Users > Policies > Privilege</i> - <i>Users > Policies > QoS</i>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3.11 User Group Configuration	- <i>Users > Groups > Configuration</i>	<input type="checkbox"/>
3.12 Add APs into Management	- <i>Devices > WAPM > Enable CAPWAP</i> - <i>Devices > WAPM > Template</i>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

- *Devices > WAPM > AP List*
- *Establish CAPWAP Tunnel from AP to EWS*

3.13 1+1 High Availability - *System > High Availability*

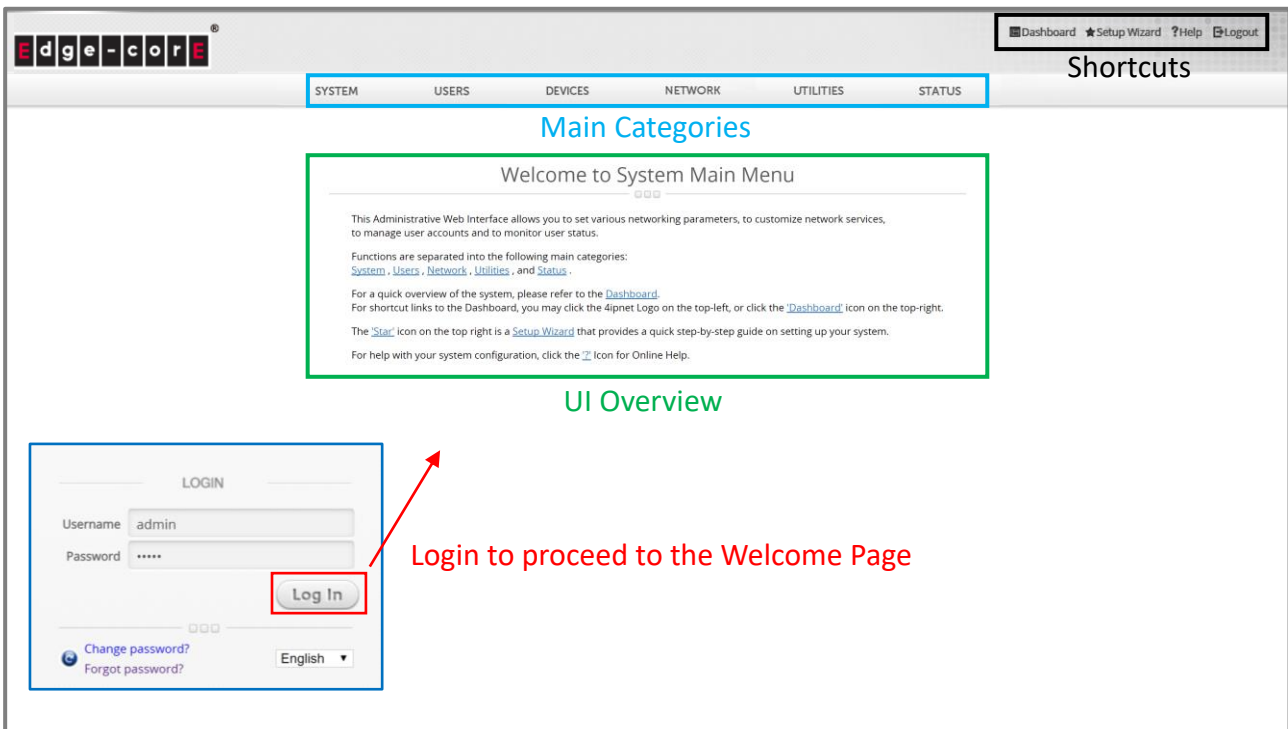
- *Status > Reporting > Notification*
- *Status > Reporting > FTP Setting*

3.14 Reporting - *Status > Reporting > SMTP Setting*

- *Status > Reporting > Syslog Setting*

4.2 System – Initial Access Browser-based GUI

Connect your PC to the EWS’s LAN port, then access the EWS’s Web Management Interface (WMI) by entering 192.168.1.254 in your web browser. Login to the EWS using the Default Username/Password: *admin/admin*.



Note: first time login will require changing the password.

4.3 System – WAN & LAN Interface Configuration

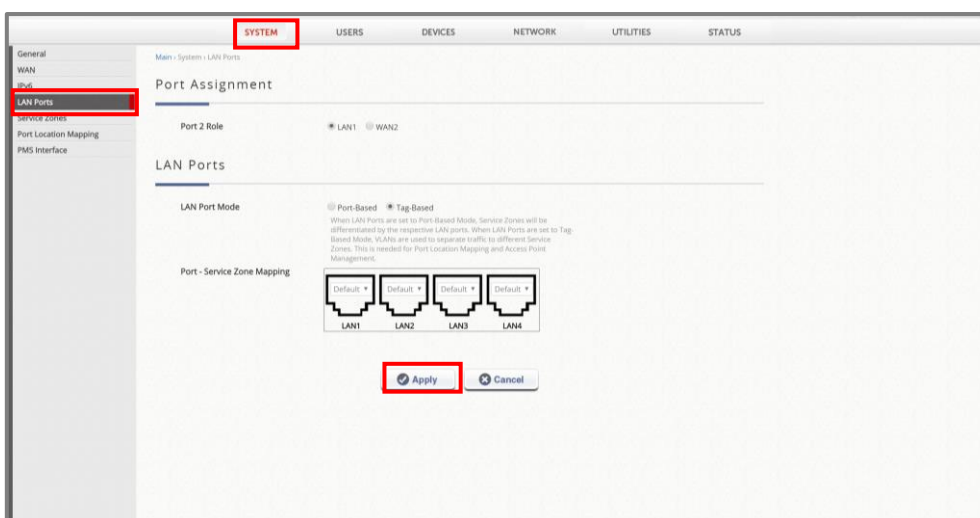
Go to **System > WAN** to configure the WAN1 Interface Type as “Static” with required details. Here we set the IP Address as 10.201.5.66/255.255.0.0 with **Default Gateway** 10.201.1.254.



Go to **Status > Interfaces > WAN1** to verify WAN1 IP Address.

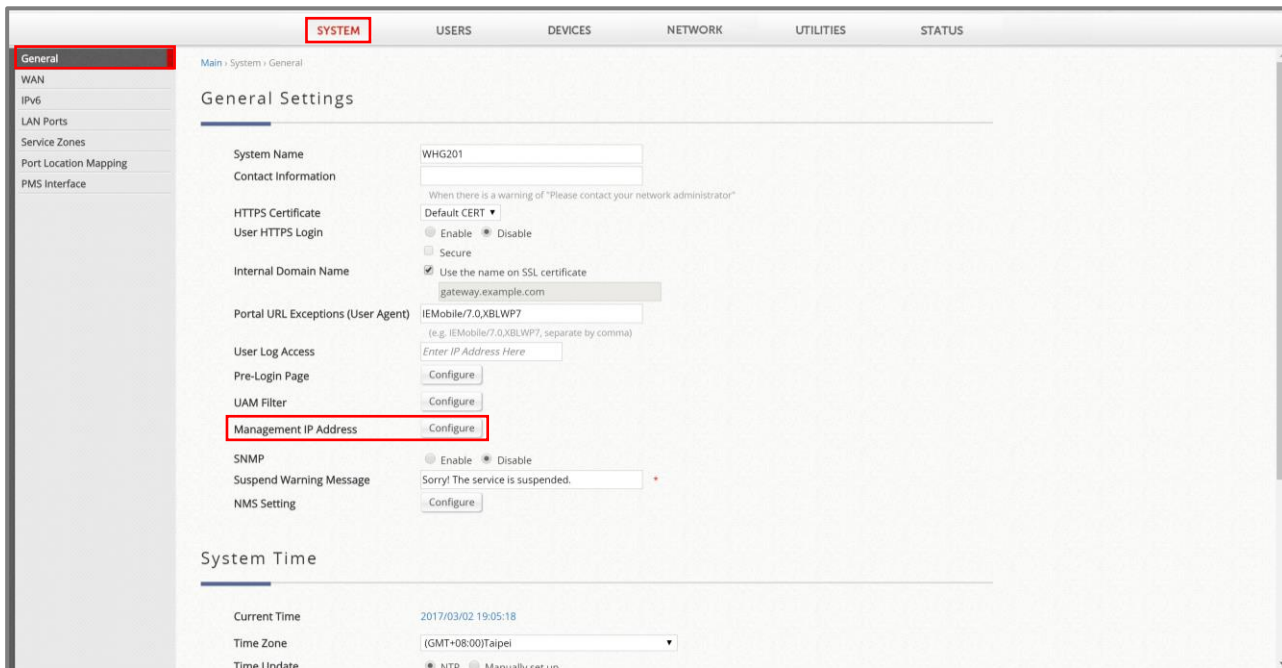


Go to **System > LAN Ports** to select “Tag-Based” as the LAN Port Mode and click on Apply.

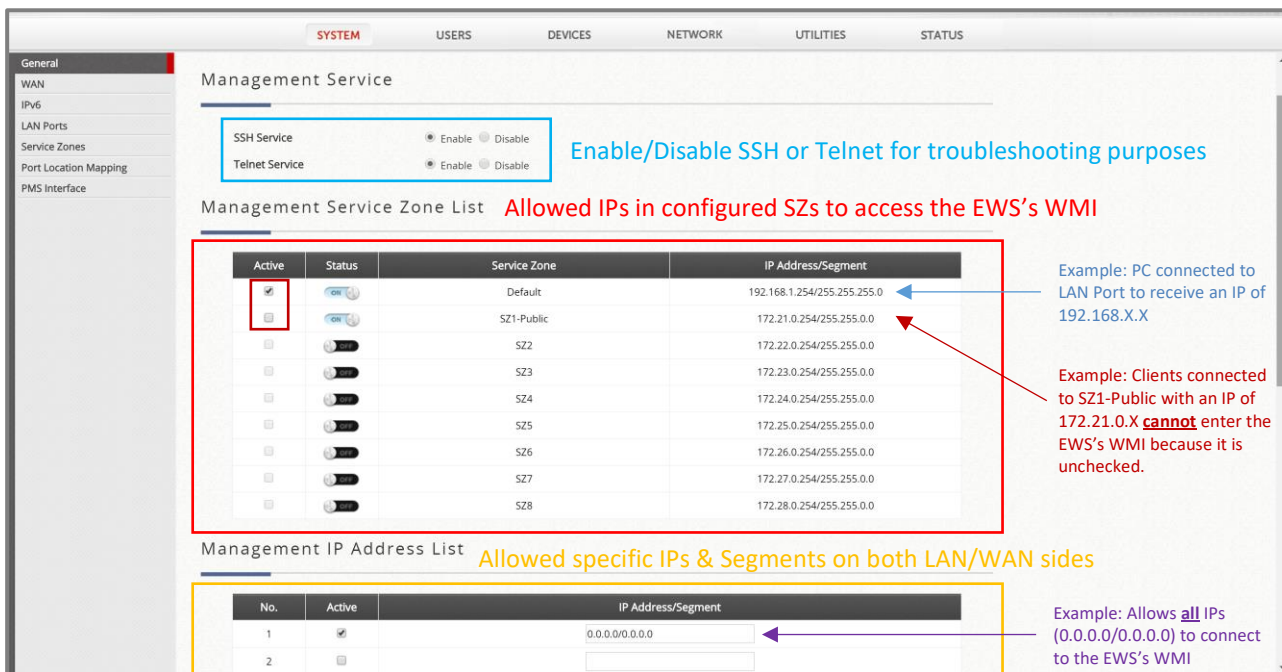


4.4 System - Management IP Address List

Go to *System > General > Management IP Address List* and click the *Configure* button beside *Management IP Address*.



Check the appropriate SZs and configure the preferred IP Addresses to allow access to the Web Management Interface.



Note: Unchecking all options and disabling the SSH/Telnet Service will result in being locked out of the EWS. Please be cautious when configuring the Management IP List.

4.5 Utilities - Admin Password Recovery

Go to *Utilities > Administrator Accounts* and click the “admin” Name to configure password recovery.

The screenshot shows the 'General Settings' page for Administrator Accounts. The 'UTILITIES' tab is selected. The page includes sections for Password Complexity, Limit Login Attempts, Password Expiration, Password Limits, and Access Permission. Below these settings is a table of Administrator Accounts with columns for Name, IP Address, MAC Address, Group, and Status. The 'admin' account is highlighted. A blue text annotation at the bottom of the screenshot reads: 'Click Administrator Account Name to setup an email account for password recovery/reset'.

Name	IP Address	MAC Address	Group	Status
admin	192.168.1.99	00-E0-4C-60-EB-78	Super Group	Current Page: Main > Utilities > Administrator Accounts

Apply the configured *Email* and *Security Answer* before setting up the SMTP server.

The screenshot shows the 'Admin Editing and Password Safety Setting' page for the 'admin' account. The page includes fields for Name, Original Password, New Password, Verify Password, Email, and Elementary school's name. The 'Email' field is highlighted with a red box, and a blue text annotation next to it reads: 'Email Address for Password Recovery'. The 'Elementary school's name' field is also highlighted with a red box, and a blue text annotation next to it reads: 'Security Answer for Password Recovery (1-time setup)'. A blue button labeled 'Assign SMTP server...' is also visible, with a blue text annotation next to it: 'Click to setup a SMTP server'. The page includes 'Apply' and 'Cancel' buttons at the bottom.

Setup *SMTP Server* to allow EWS to send Password Recovery Email to administrator.

Each email domain uses specific SMTP Server Address/Port and Encryption. This example uses a Gmail account.

Main IT Administrator Account Credentials

4.6 System - Service Zones Configuration

Go to *System > Service Zones* and confirm WAN Subnet and *Default Service Zone* IP Address are in different subnets. Take below as example,

WAN1 = 10.201.5.66 / Subnet = 255.255.0.0

LAN/Default SZ = 192.168.1.254 / Subnet = 255.255.0.0

Status	Service Zone Name	IP Address	IPv6 Address	VLAN Tag	Default Auth. Option	Network Alias	DHCP Pool
ON	Default	192.168.1.254	N/A	N/A	Server 1	N/A	192.168.1.1 ~ 192.168.1.100
OFF	SZ1	172.21.0.254	N/A	1	Server 1	N/A	172.21.0.1 ~ 172.21.0.100
OFF	SZ2	172.22.0.254	N/A	2	Server 1	N/A	172.22.0.1 ~ 172.22.0.100
OFF	SZ3	172.23.0.254	N/A	3	Server 1	N/A	172.23.0.1 ~ 172.23.0.100
OFF	SZ4	172.24.0.254	N/A	4	Server 1	N/A	172.24.0.1 ~ 172.24.0.100
OFF	SZ5	172.25.0.254	N/A	5	Server 1	N/A	172.25.0.1 ~ 172.25.0.100
OFF	SZ6	172.26.0.254	N/A	6	Server 1	N/A	172.26.0.1 ~ 172.26.0.100
OFF	SZ7	172.27.0.254	N/A	7	Server 1	N/A	172.27.0.1 ~ 172.27.0.100
OFF	SZ8	172.28.0.254	N/A	8	Server 1	N/A	172.28.0.1 ~ 172.28.0.100

Click Service Zone Name to configure each SZ

Click *Default Service Zone*, and administrators are able to enable the Service Zone Status and configure the basic network settings, including *Service Zone IP address, DHCP scope, and preferred DNS server, etc.*

SYSTEM USERS DEVICES NETWORK UTILITIES STATUS

Main > System > Service Zone > Service Zone Configuration

Basic Settings

Service Zone Status: Enabled

Service Zone Name: Default

Network Interface: Tag-based Isolation Inter-VLAN Isolation Clients Isolation None

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

Operation Mode: NAT Router

IP Address: 192.168.1.254 * Subnet Mask: 255.255.0.0 *

Network Alias List:

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

DHCP: Disabled

SYSTEM USERS DEVICES NETWORK UTILITIES STATUS

Main > System > Service Zone > Service Zone Configuration > DHCP Configuration

DHCP:

DHCP Server Configuration for Service Zone Default

No	Active	DHCP Pool	Start IP Address	End IP Address	Preferred DNS Server	Alternate DNS Server	Domain Name
1	<input checked="" type="checkbox"/>	Scope 1	192.168.1.2 *	192.168.1.200 *	192.168.1.254 *		domain.com
2	<input type="checkbox"/>	Scope 2					
3	<input type="checkbox"/>	Scope 3					
4	<input type="checkbox"/>	Scope 4					
5	<input type="checkbox"/>	Scope 5					
6	<input type="checkbox"/>	Scope 6					

Next, Configuring *Authentication Settings* is another important session, which administrators can enable *Guest Authentication* Database to allow self-registration users.

Authentication Settings

Authentication: Enable Disable Suspend **Enable/Disable Authentication on this Service Zone**
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
 Portal URL opens specified URL after user is authenticated
(e.g. http://www.example.com)

MAC Authentication: Enabled Disabled
RADIUS Authentication using MAC address

PPP Authentication: Enabled Disabled

SIP Interface Configuration: Enabled Disabled

WISPr Settings:

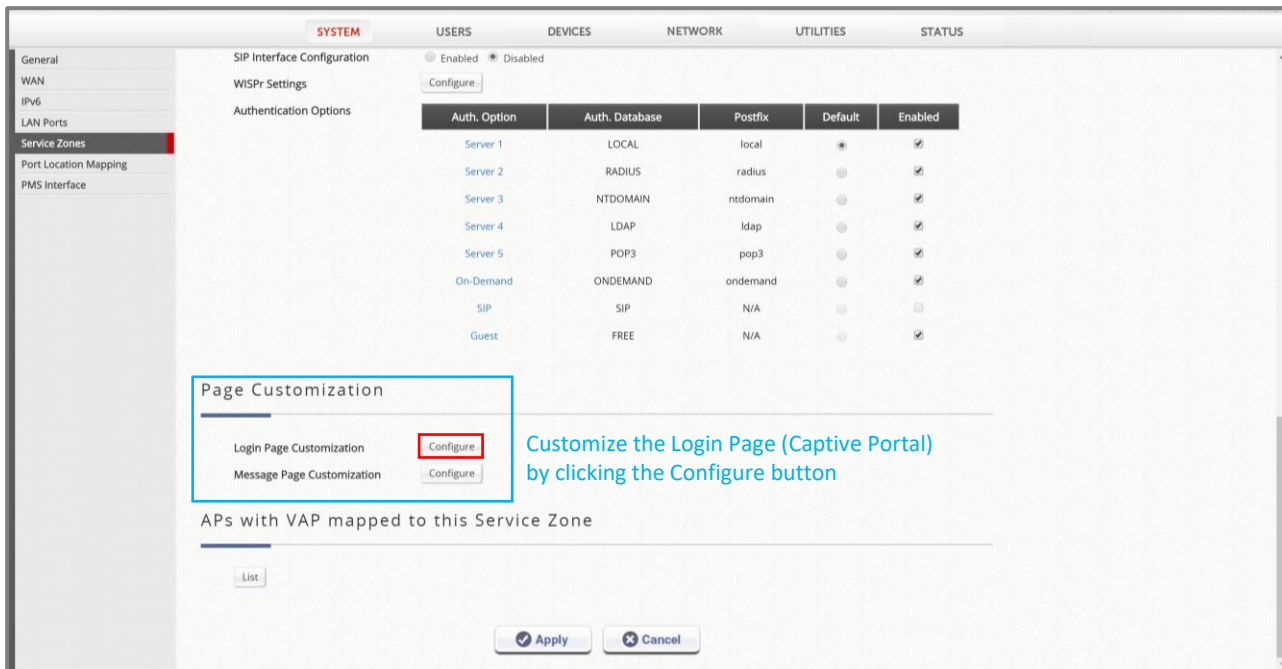
Authentication Options:

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

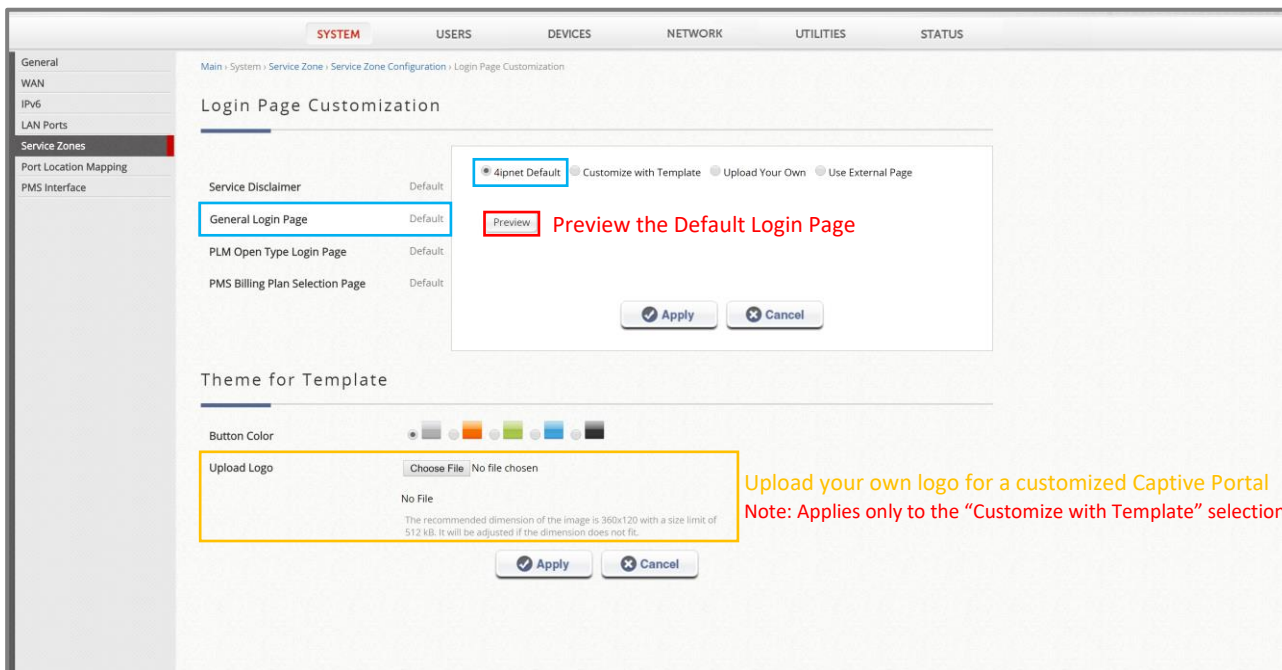
Confirm Authentication Databases allowed in this Service Zone

4.7 System - Service Zone – Captive Portal Customization

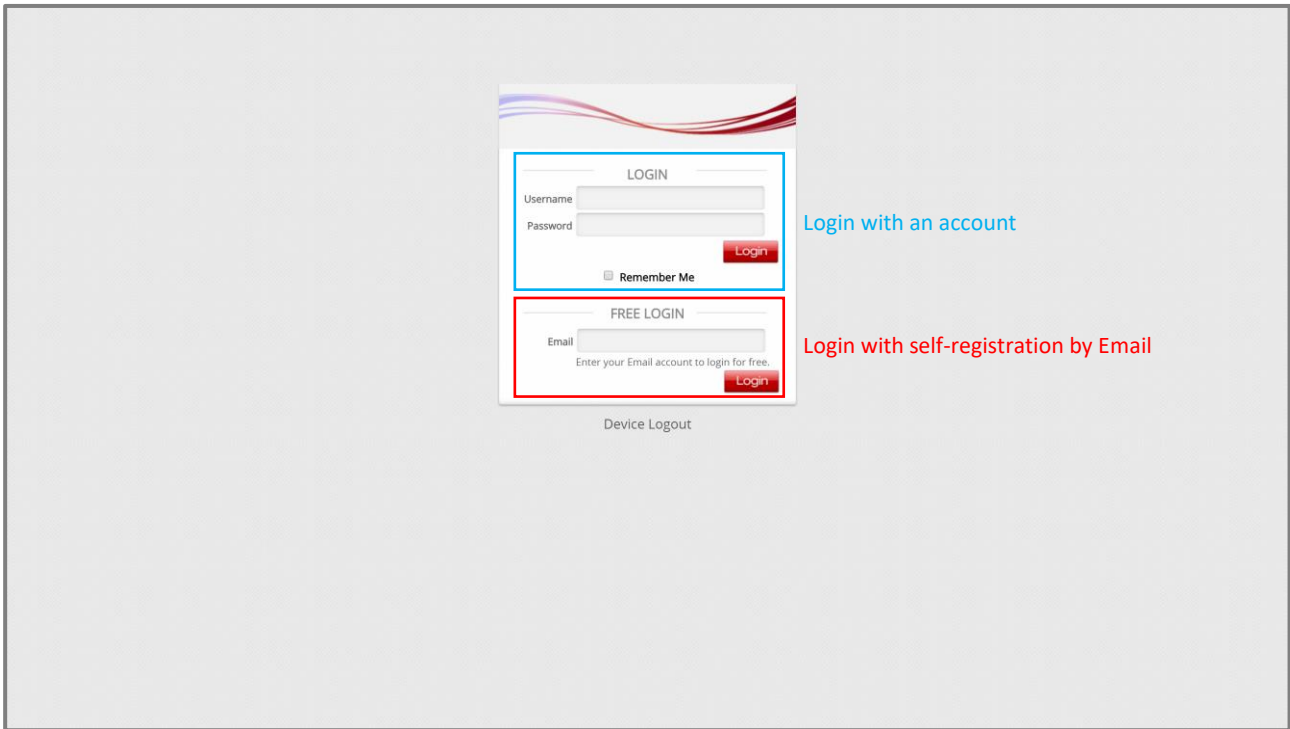
Go to *System > Service Zones > Service Zone Configuration > Login Page Customization* Click “Configure” button to start customizing different Login Page. On the other hand, *Message Page Customization* will provide customizations to message pages such as the login success page.



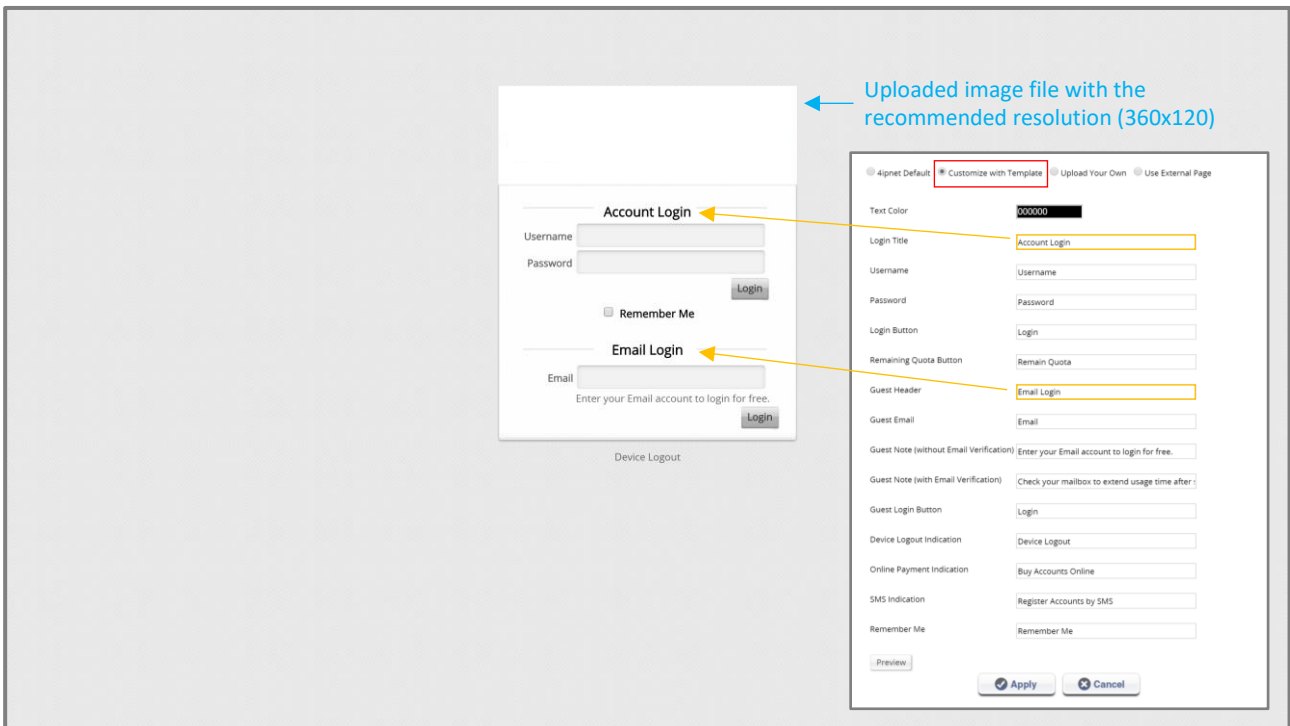
Each page has 4 different types of customization, *Default, Customize with Template, Upload Your Own, and Use External Page.*



Preview *General Login Page* in *Default* mode.

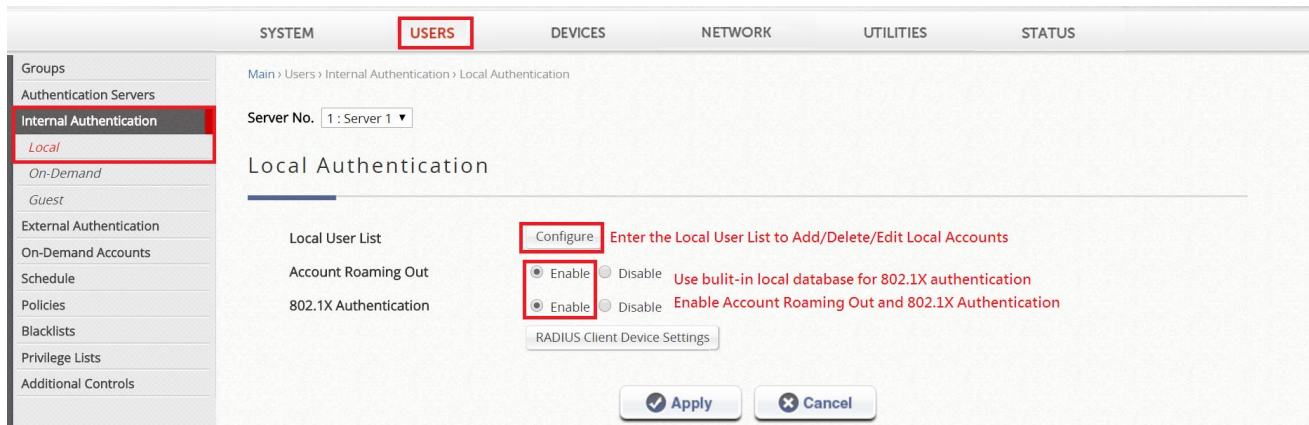


Preview *General Login Page* in *Customize with Template* mode with an uploaded logo and customized text.

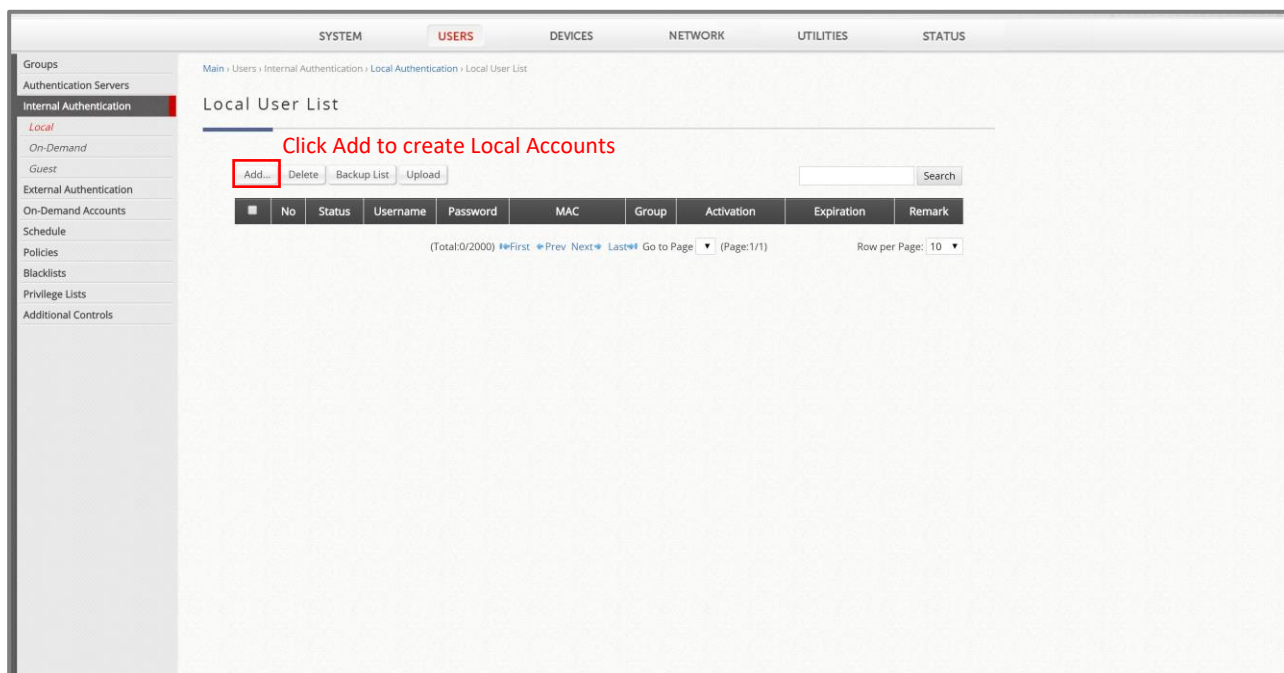


4.8 Users - Local Accounts

Go to *Users > Internal Authentication > Local* to create accounts using the Local Database.



Click *Add* to create a single or multiple accounts at once.



Enter user account credentials and Apply. (in this example, we use *staff/staff*)

10000 users can be added to this local user list.

Username	Password	MAC Address	Group	Account Span	Remark
staff	staff		Staff		
			Guest		
			Guest		
			Guest		
			Guest		
			Guest		
			Guest		
			Guest		
			Guest		
			Guest		
			Guest		
			Guest		

Apply Cancel

Created accounts can be viewed on the *Local User List*.

Local User List

No	Status	Username	Password	MAC	Group	Activation	Expiration	Remark
1	Valid	staff	staff		Staff			

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

User List available for Add/Delete/Edit/Backup/Restore

4.9 Users – Guest Authentication

Administrator expects that Guest users are authenticated by submitting their Email addresses for granting free Wi-Fi Internet access for 24 hours with limited speed and sessions, which can be achieved by Guest Authentication on EWS controller.

This paragraph will illustrate the configuration steps for Guest Authentication.

Go to *Users > Internal Authentication > Guest Authentication*, select the radio box to make Guest Login Input to be *visible*, which is the column for users to enter their Email address. Select *Limited* radio box to set up limited *Guest Access Time*, and then the further configurations will be visible. Please assign 24 hours 0 minutes as *Quota*; 1 minute for *Access Limit*. Last, assign this Guest Authentication to *Guest Group* for User Policy enforcement.

The screenshot shows the configuration page for Guest Authentication in the EWS controller. The page is titled "Guest Authentication" and is part of the "USERS" section. The left sidebar shows the navigation menu with "Internal Authentication" selected. The main content area displays the following configuration options:

- Group: Guest
- Guest Information: View
- Guest Questionnaire: Configure
- Guest Access Time: Unlimited Limited
- Quota: 24 hour(s) 00 minute(s)
- Reactivation: After 0 hour(s) 1 minute(s)
- Access Limit: 0 per day *(0:Unlimited)
- Email Verification: Disable Enable
- Guest Quota List: View
- E-mail Denial List: Disable Enable

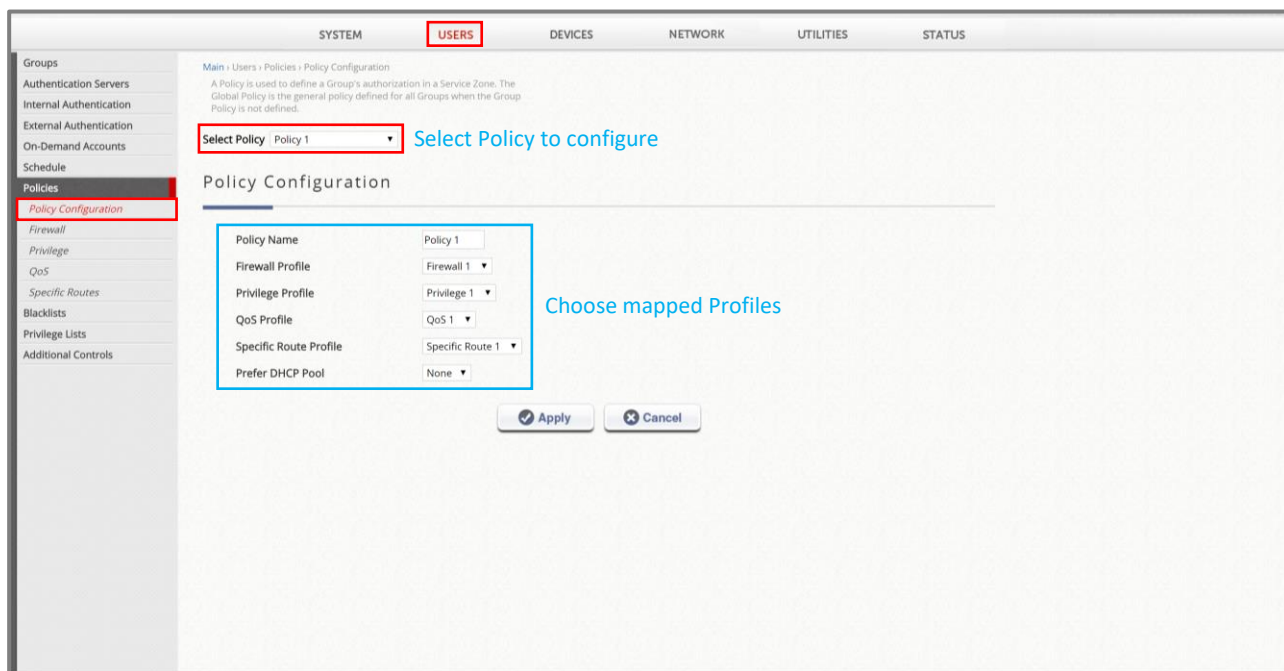
At the bottom of the page, there are "Apply" and "Cancel" buttons.

4.10 Users – User Policies Configuration

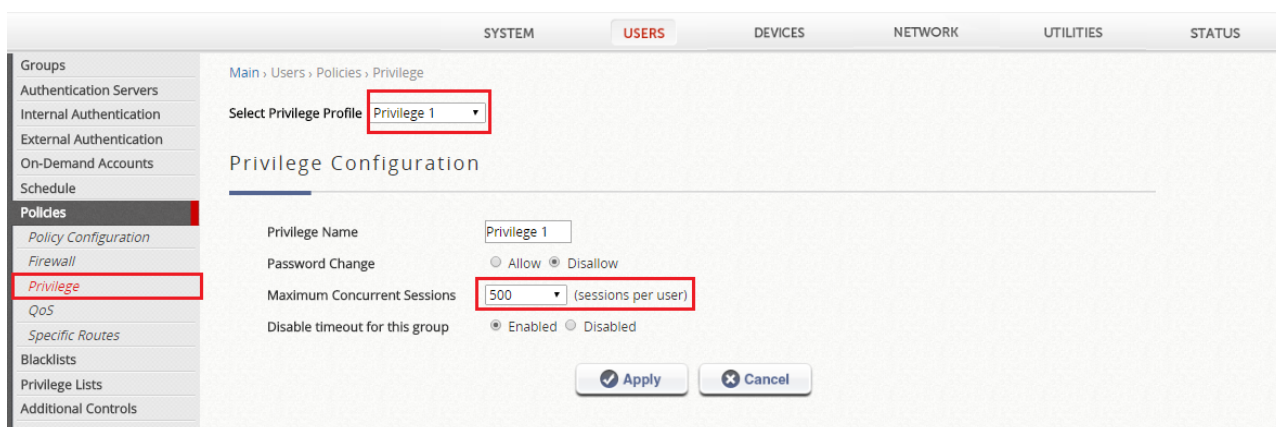
Administrator is going to enforce *Policy 1* on Guest users with limited 500 *Maximum Concurrent Sessions* & *QoS bandwidth* control; and *Policy 2* on Staff users with *Firewall Rule* to block Facebook access & *Unlimited Maximum Concurrent Sessions*.

4.10.1 Guest Users → Policy 1 profile configuration

Configure and select *Privilege Profile*, and *QoS Profile* to create Policy 1.



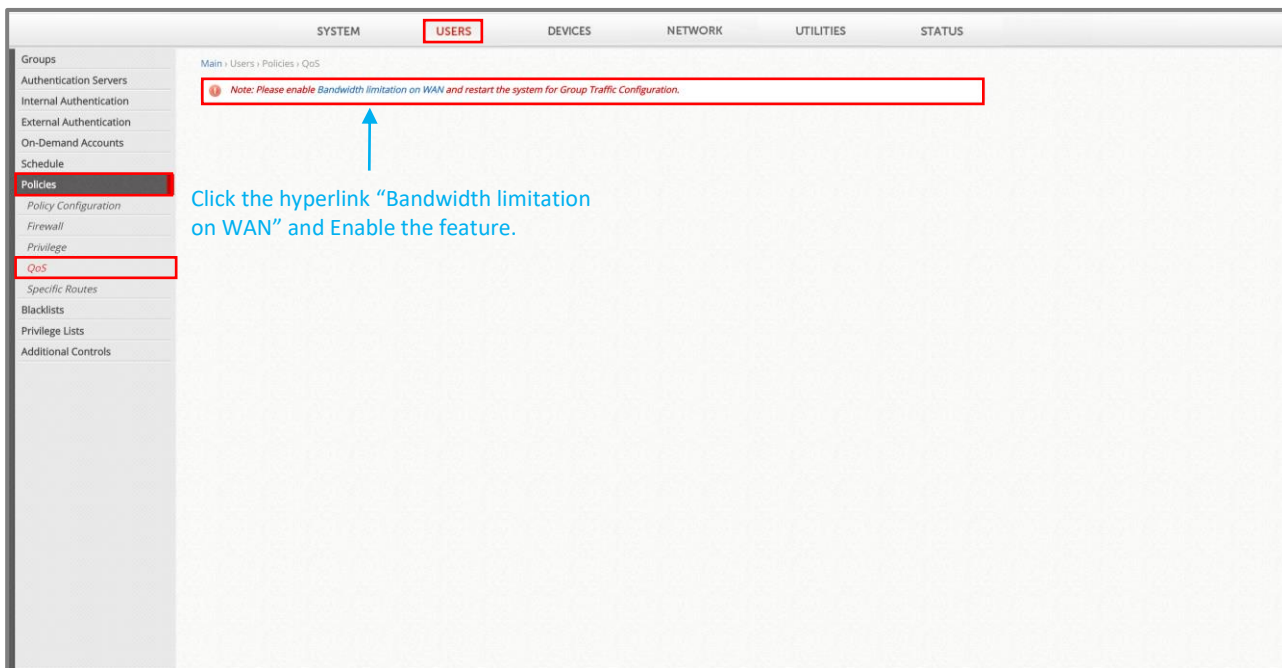
Go to *Users > Policies > Privilege 1* to check if the *Maximum Concurrent Session* is 500 as the default value.



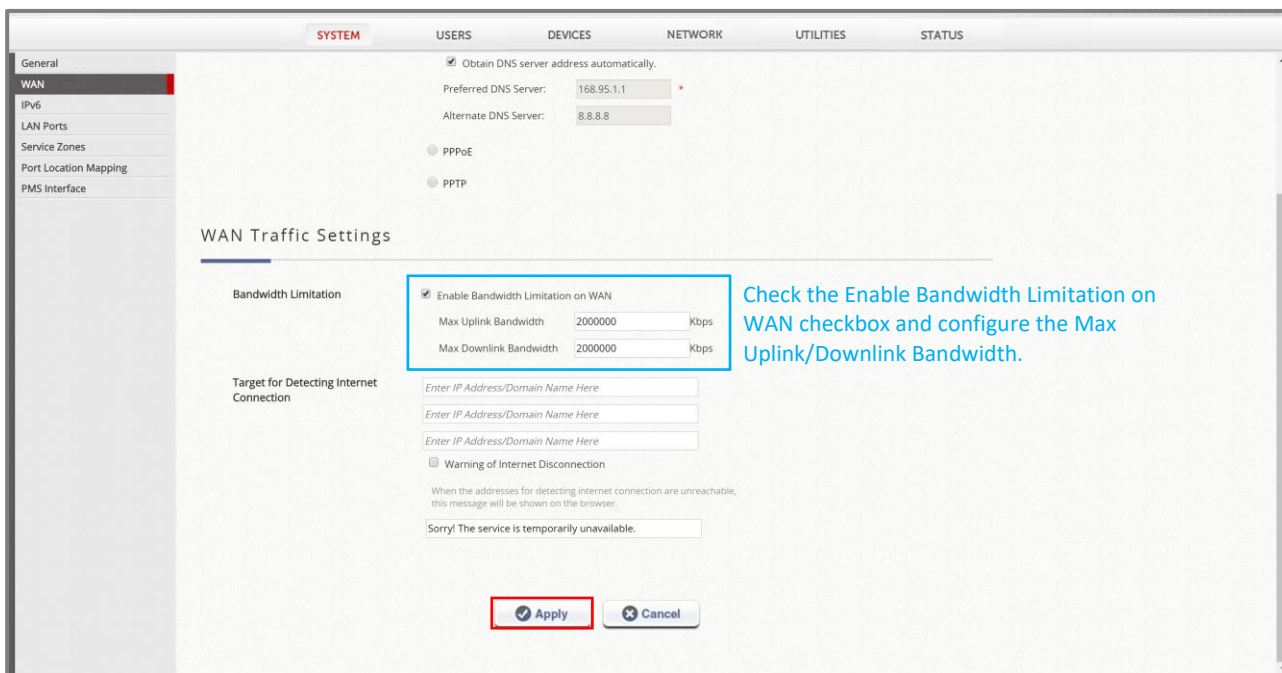
Go to *Users > Policies > QoS* to configure each Group/User's bandwidth.

In order to configure the QoS Bandwidth Control, *Bandwidth Limitation on WAN*

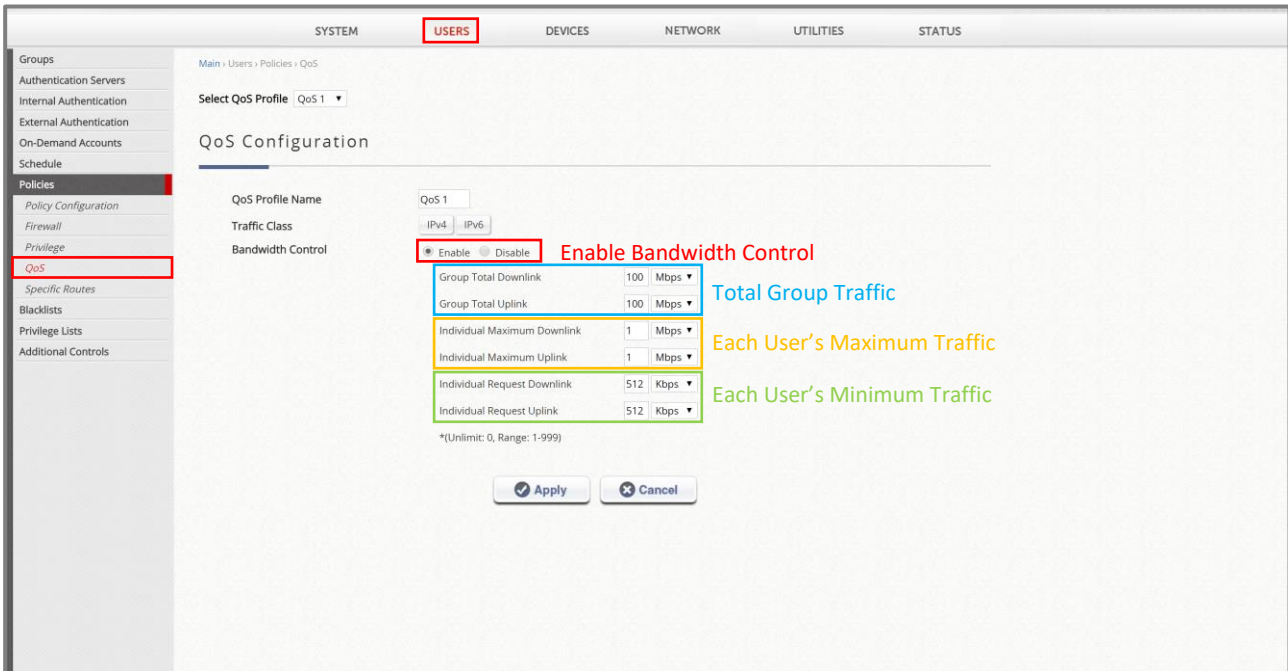
must be enabled. Click the hyperlink to access the WAN configuration page.



Please check the *Bandwidth Limitation* at WAN checkbox, Apply and restart the EWS to activate the changes.

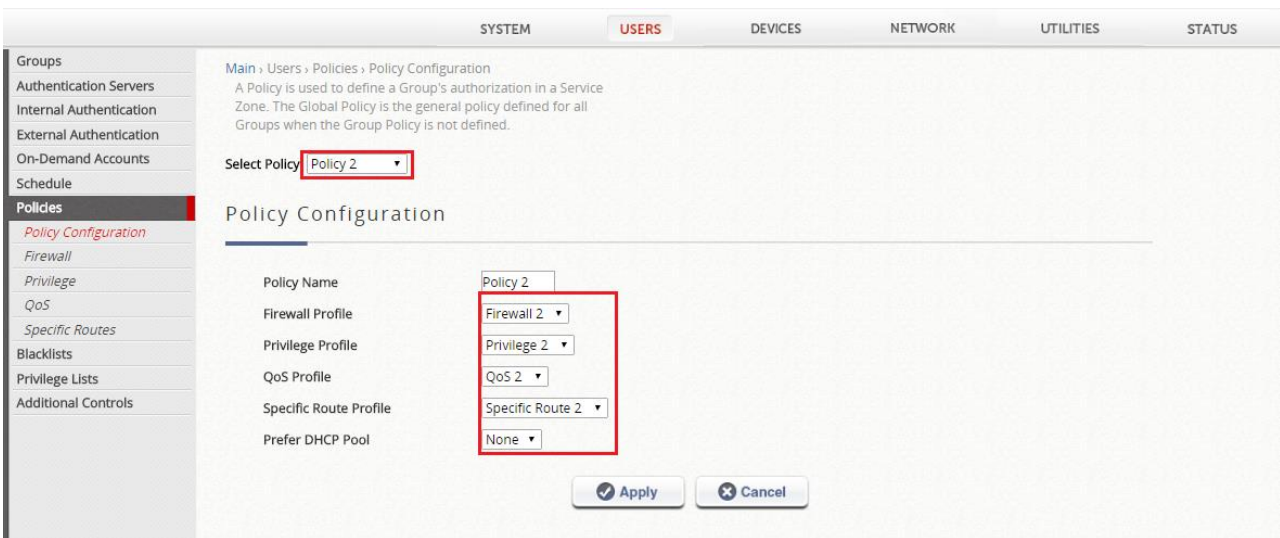


After the EWS has restarted, go to *Users > Policies > QoS* to configure the QoS 1 Profile as shown below.

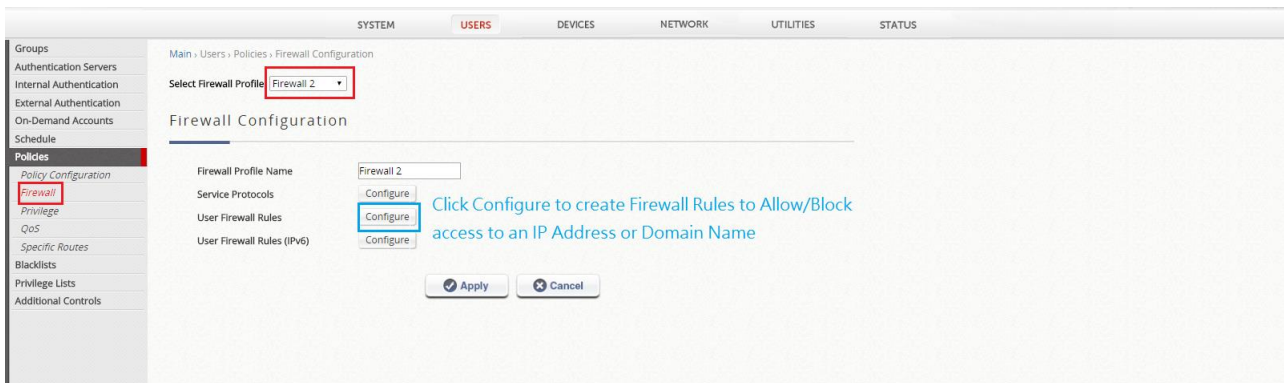


4.10.2 Staff Users → Policy 2 profile configuration

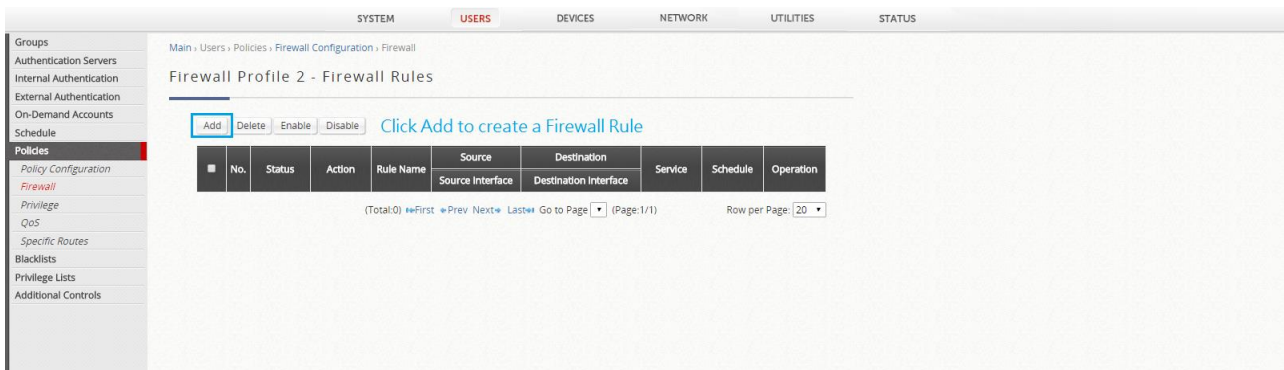
Go to *Users > Policies > Policy 2* profile to check each of the profile numbers.



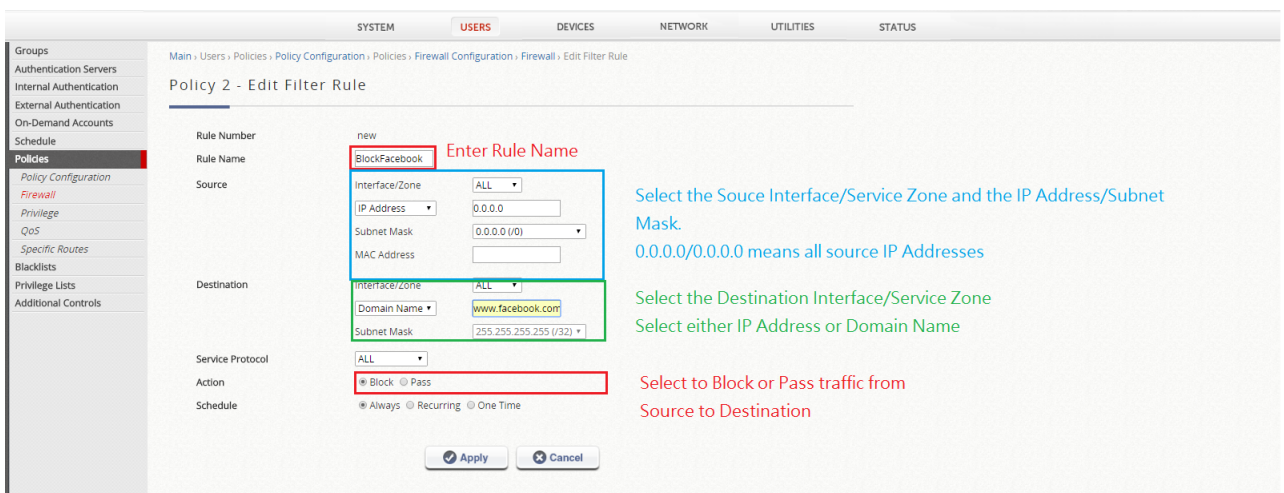
Go to **Users > Firewall** and select Firewall 2 to configure **User Firewall Rules** to block a user's access to an IP Address or Web Domain.



Click the **Add** button to create a new **Firewall Rule**.



Configure a new Firewall Rule (BlockFacebook) with preferred **Source and Destination**.



Check the checkbox and click the Enable button to **Activate & Enable** the **Firewall Rule**.

SYSTEM **USERS** DEVICES NETWORK UTILITIES STATUS

Main > Users > Policies > Firewall Configuration > Firewall

Firewall Profile 2 - Firewall Rules

Add Delete **Enable** Disable *Check the Firewall Rule & click Enable*

No.	Status	Action	Rule Name	Source		Destination		Service	Schedule	Operation
				Source Interface	Destination Interface					
1	Disabled	Block	BlockFacebook	ANY	www.facebook.com	ALL	always	Move		
				ALL	ALL					

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

Go to *Users > Policies > Privilege 2* to configure the *Maximum Concurrent Sessions* of each user under this Policy. (Default = 500)

SYSTEM **USERS** DEVICES NETWORK UTILITIES STATUS

Main > Users > Policies > Privilege

Select Privilege Profile: Privilege 2

Privilege Configuration

Privilege Name: Privilege 2

Password Change: Allow Disallow

Maximum Concurrent Sessions: **Unlimited** sessions per user *Configure preferred value for Maximum Concurrent Sessions*

Disable timeout for this group: Enabled Disabled

4.11 Users – User Groups Configuration

Go to *Users > Groups > Configuration* and select *Group 1* to configure the Group parameters, Service Zones Group 1 is allowed access to and the Policy Profile applied when an account in this group connects to the specified Service Zone.

Here we rename the Group Name of Group1 as Guest, with 2 for Number of devices which are allowed to login, and assign Policy 1 for Default Service Zone.

The screenshot shows the 'Group Configuration' page for 'Group 1'. The 'Configuration' tab is selected in the left sidebar. The main content area has the following fields:

- Select Group: Guest (dropdown)
- Group Name: Guest (text input)
- Remark: (empty text input)
- Number of devices which are allowed to login: 2 (text input)
- Allow to logout other devices when exceeding the maximum amount of devices: Enabled (radio button selected)

Below these fields is a section titled 'Zone Permission Configuration & Policy Assignment' with a table:

Enabled	Zone Name	Time Span 1	Time Span 2
<input checked="" type="checkbox"/>	Service Zone : Default	Schedule 1	Schedule 1
<input checked="" type="checkbox"/>	Service Zone : SZ1	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ2	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ3	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ4	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ5	Policy 1	Policy 1

Here we select and rename Group 2 as Staff, with unlimited Number of devices which are allowed to login, and assign Policy 2 for Default Service Zone.

The screenshot shows the 'Group Configuration' page for 'Group 2'. The 'Configuration' tab is selected in the left sidebar. The main content area has the following fields:

- Select Group: Staff (dropdown)
- Group Name: Staff (text input)
- Remark: (empty text input)
- Number of devices which are allowed to login: 0 (text input)
- Allow to logout other devices when exceeding the maximum amount of devices: Enabled (radio button selected)

Below these fields is a section titled 'Zone Permission Configuration & Policy Assignment' with a table:

Enabled	Zone Name	Time Span 1	Time Span 2
<input checked="" type="checkbox"/>	Service Zone : Default	Schedule 2	Schedule 2
<input checked="" type="checkbox"/>	Service Zone : SZ1	Policy 2	Policy 2
<input checked="" type="checkbox"/>	Service Zone : SZ2	Policy 2	Policy 2
<input checked="" type="checkbox"/>	Service Zone : SZ3	Policy 2	Policy 2
<input checked="" type="checkbox"/>	Service Zone : SZ4	Policy 2	Policy 2
<input checked="" type="checkbox"/>	Service Zone : SZ5	Policy 2	Policy 2

Go to *Users > Groups > Overview* to check if the authentication and group relationship are correctly mapping here.

SYSTEM **USERS** DEVICES NETWORK UTILITIES STATUS

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
Guest	Billing Plan 1 Billing Plan 2 Guest POP3-Server 5 RADIUS-Server 2-Default LDAP-Server 4-Default NT Domain-Server 3 SIP
Staff	Local
Group 3	
Group 4	
Group 5	
Group 6	
Group 7	
Group 8	

Guest Group is the Default Group for all Authentication Types including the Guest Authentication

Staff Group has been selected as the Staff Local User Account: staff

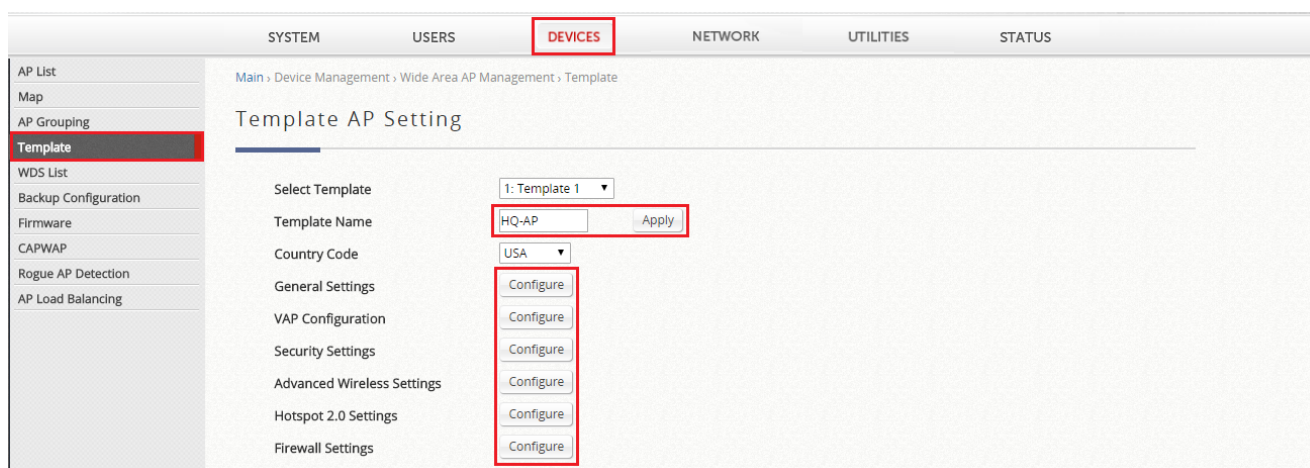
4.12 Use WAPM on EWS to manage ECW

Go to *Devices*, Enable *Wide Area AP Management* and click Enter to configure WAPM.



4.12.1 Edit WAPM Templates

Go to *Devices > Wide Area AP Management > Template*, rename the Template Name then apply, configure each item.



General Settings

Select each card and check if the parameters are able to fit the network. After edit, click the Apply to save the configuration.

General Settings - 1: Template 1

RF Card Name: RF CARD A (Select and edit RF CARD A (2.4G), RF CARD B (5G))

Band: 802.11g-802.11n (Pure 11n)

Short Preamble: Disable Enable

Short Guard Interval: 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) *(60 - 60000)

Band Steering: Disable Enable

Aggressive

Confirm the setting are suit for network

VAP Configuration

VAP Configuration - 1: Template 1

Profile Name: RF Card A : VAP-1 (Select Profile of VAP)

VAP: Enable (Select to enable this VAP)

Profile Name: (Assign a Profile Name)

ESSID: (Assign a SSID)

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

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

VLAN ID: Disable Enable

VLAN ID: 1000 *(1 - 4094)

Uplink 802.1p: Best Effort (BE)

CAPWAP Tunnel Interface: Complete Tunnel (Select Complete Tunnel and Service Zone, and the VLAN ID will auto-change)

Service Zone: n26

Apply Cancel

We can use same procedure to configure other VAP.

Security Configuration

The screenshot shows the 'Security Settings - 1: Template 1' configuration page. The breadcrumb trail is 'Main > Device Management > Wide Area AP Management > Template > Security Settings'. The left sidebar contains a menu with 'Template' selected. The main content area has two dropdown menus: 'Profile Name' set to 'RF Card A : VAP-1' and 'Security Type' set to 'Open'. A red note says 'Select the Profile and choose the Security Type'. At the bottom are 'Apply' and 'Cancel' buttons.

If you would like to use 802.1x authentication, please select WPA-Enterprise.

Advanced Wireless Configuration

The screenshot shows the 'Advanced Wireless Settings - 1: Template 1' configuration page. The breadcrumb trail is 'Main > Device Management > Wide Area AP Management > Template > Advanced Wireless Settings'. The left sidebar contains a menu with 'Template' selected. The main content area lists various settings: Profile Name (RF Card A : VAP-1), RTS Threshold (2346), Fragment Threshold (2346), DTIM period (1), Consecutive Retries Threshold (5), Broadcast SSID (radio buttons for Disable and Enable, with 'Enable' selected), Wireless Station Isolation (radio buttons for Disable and Enable, with 'Enable' selected), WMM (radio buttons for Disable and Enable, with 'Enable' selected), IAPP (radio buttons for Disable and Enable, with 'Enable' selected), Multicast-to-Unicast Conversion (radio buttons for Disable and Enable, with 'Disable' selected), TX STBC (radio buttons for Disable and Enable, with 'Enable' selected), Multicast/Broadcast Rate (5.5M), Management Frame Rate (5.5M), and Receiving RSSI Threshold (-80). Red notes provide instructions for the Broadcast SSID and Wireless Station Isolation settings. At the bottom are 'Apply' and 'Cancel' buttons.

4.12.2 Establish CAPWAP Tunnel from AP to EWS

Enable CAPWAP in EWS

Go to *Devices > WAPM > CAPWAP*

SYSTEM USERS **DEVICES** NETWORK UTILITIES STATUS

Main > Device Management > Wide Area AP Management > CAPWAP

CAPWAP Configuration

CAPWAP Status Enable Disable

Apply Certificate to APs DEFAULT ▾

IP Address For Control Channel 100.64.144.254

IP Netmask For Control Channel 255.255.255.128 (125) ▾

Control Channel IP Range 100.64.144.1 ~ 100.64.144.253

Go to *AP > System > CAPWAP*, and edit CAPWAP Configuration then apply and reboot. Please make sure AP's uplink could reach AC, otherwise the CAPWAP tunnel cannot build.

System Wireless Firewall Utilities Status

General Network Interface Port Management **CAPWAP** IPv6 Operating Mode

Home > System > CAPWAP Configuration

CAPWAP Configuration

CAPWAP : Disable Enable Enable CAPWAP

Certificate Date Check : Disable Enable Manage Certificates

DNS SRV Discovery : Disable Enable

DHCP Option Discovery : Disable Enable

Broadcast Discovery : Disable Enable

Multicast Discovery : Disable Enable

Static Discovery : Disable Enable Enable Static Discovery

Pri.	AC Address	Remark
1	10.201.5.117	Fill in WAN IP of AC
2		
3		
4		
5		

After Reboot, the AP would auto connect to EWS, the overview page could confirm the status of CAPWAP. Also, could monitor this at AP List from EWS.

The screenshot displays a network management dashboard with the following sections:

- System Overview**
 - System**

System Name	TS-Joyce
Firmware Version	3.42.10
Build Number	1.36.2.6-1.8992.2.7
Location	Taipei, Taiwan
Site	EN-A
Device Time	2017/07/03 16:33:56
System Up Time	0 days, 12:33:37
CPU/RAM Usage	48.08% / 30.62% <input type="button" value="Plot"/>
Operating Mode	AP
 - Radio Status**

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:1F:D4:04:F8:0A	802.11g+n	11	28 dBm
RF Card B	00:1F:D4:04:F8:0B	802.11ac	36	17 dBm
 - LAN Interface**

MAC Address	00:1F:D4:04:F8:08
IP Address	192.168.5.246
Subnet Mask	255.255.255.0
Gateway	192.168.5.252
 - AP Status**

RF Card Name:

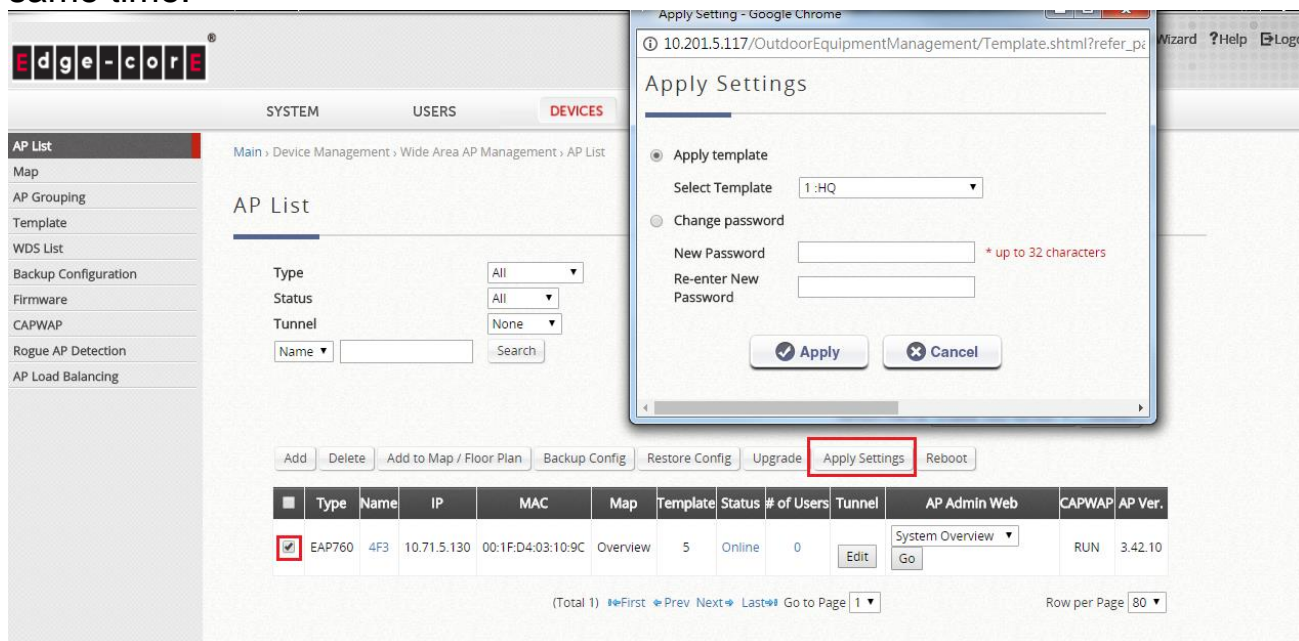
Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	00:1F:D4:04:F8:0A	cip-802.1x	WPA-Enter...	1	<input type="button" value="x"/>
 - CAPWAP**

Status	Run(10.201.5.117)
Data Channel	Active
 - IPv6**

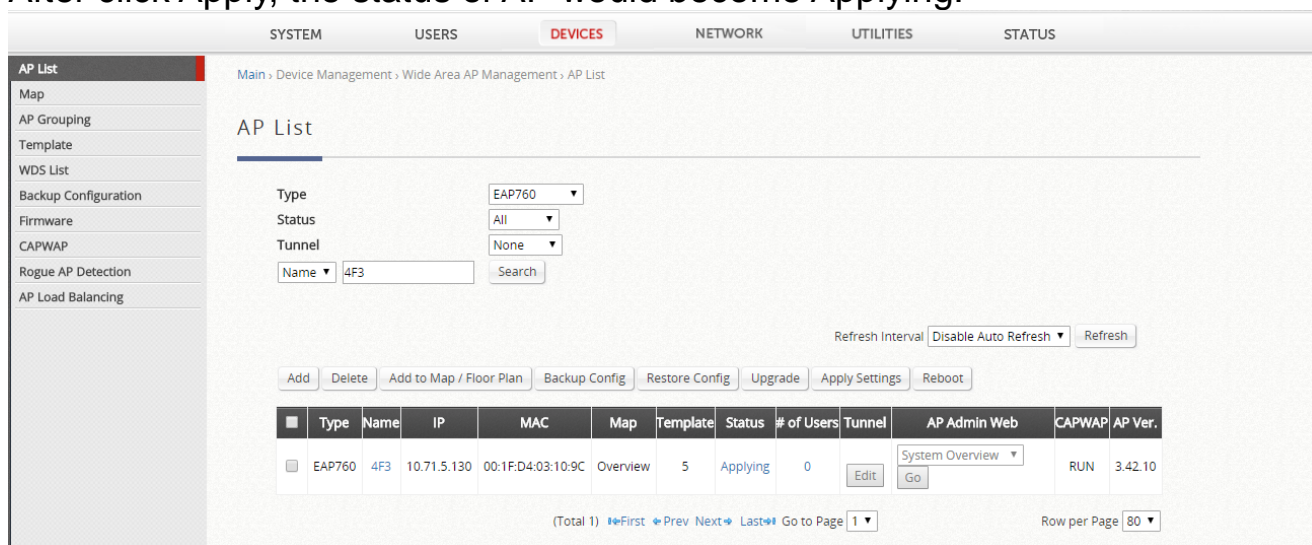
Status:

4.12.3 Applying the template

Select the APs and click Applying template to configure multiple APs at the same time.



After click Apply, the status of AP would become Applying.



When AP successfully been applied, the status would become online and you can click Go button to access the web page of AP.

SYSTEM USERS **DEVICES** NETWORK UTILITIES STATUS

Main > Device Management > Wide Area AP Management > AP List

AP List

Type: EAP760
 Status: All
 Tunnel: None

Name: Search

Refresh Interval: Disable Auto Refresh Refresh

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

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.
EAP760	4F3	10.71.5.130	00:1F:D4:03:10:9C	Overview	1	Online	0		System Overview	RUN	3.42.10

(Total 1) First Prev Next Last Go to Page 1 Row per Page 80

System Wireless Firewall Utilities Status

Overview Interfaces Associated Clients Link Status Event Log Monitor

Home > Status > System Overview

System Overview

System

System Name: 4F3
 Firmware Version: 3.42.10
 Build Number: 1.36.2.6-1.8992.2.7
 Location: EN-A
 Site: EN-A
 Device Time: 2017/06/30 01:20:32
 System Up Time: 0 days, 0:13:41
 CPU/RAM Usage: 1.96% / 29.15% Plot
 Operating Mode: AP

Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:1F:D4:03:10:9E	802.11g+n	6	28 dBm
RF Card B	00:1F:D4:03:10:9F	802.11ac	36	17 dBm

LAN Interface

MAC Address: 00:1F:D4:03:10:9C
 IP Address: 192.168.5.247
 Subnet Mask: 255.255.255.0
 Gateway: 192.168.5.252

AP Status

RF Card Name: RF Card A

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	00:1F:D4:03:10:9E	apricot	Open	0	<input checked="" type="checkbox"/>

If SSID contain tunnel (it must be configure with template), would show green check icon

IPv6
 Status: Disabled

CAPWAP

Status: Run(10.201.5.117)
 Data Channel: Active

4.13 1+1 High Availability for Service Redundancy

4.13.1 Configure EWS#1 HA

First, we need to check System time, go to **SYSTEM > General > System**, and use the main EWS as NTP server.

The screenshot shows the 'System Time' configuration page. The 'SYSTEM' tab is selected. The left sidebar has 'General' selected. The main content area shows the following configuration:

- Current Time: 2017/06/30 10:19:17
- 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

Buttons for 'Apply' and 'Cancel' are visible at the bottom.

Go to **SYSTEM > High Availability**, and Enable the High Availability at EWS#1 After Apply then reboot.

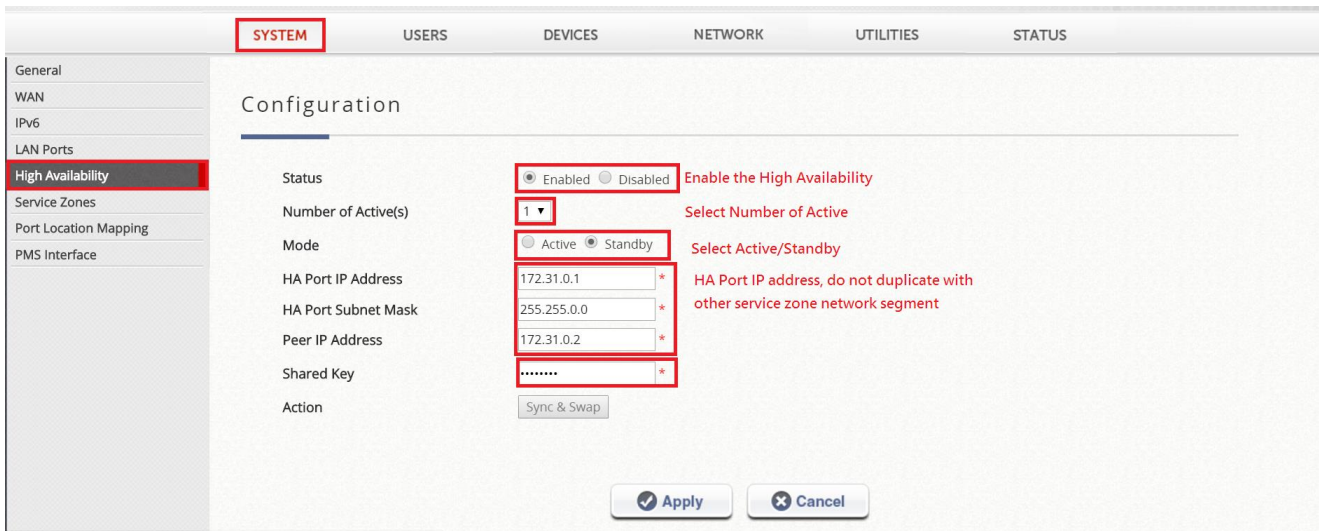
The screenshot shows the 'High Availability' configuration page. The 'SYSTEM' tab is selected. The left sidebar has 'High Availability' selected. The main content area shows the following configuration:

- 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: 172.31.0.2
- Shared Key:
- Action: Sync & Swap

Buttons for 'Apply' and 'Cancel' are visible at the bottom.

4.13.2 Configure EWS#2

Please make sure EWS#1 boot up successfully before configuring EWS#2. Same as EWS#1, go to **SYSTEM > High Availability**, enable *High Availability* and select *Standby*. After click *Apply*, before reboot, **make sure the LAN1 port of both EWS are directly connect.**



4.13.3 Confirm HA status of both EWS

Click "Goto" to access the standby page.



4.14 Reporting

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

4.14.1 Notification

Go to **STATUS > Reporting > Notification**, click the check box and select the interval

		Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
		1	2	3	4	5	Detail / Test			
Monitor IP Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A

4.14.2 FTP Setting

Go to **STATUS > Reporting > FTP Setting**, configure the FTP Settings. After configure, you can click test to confirm it.

		Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
		1	2	3	4	5	Detail / Test			
Monitor IP Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A

		Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
		1	2	3	4	5	Detail / Test			
Monitor IP Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A

		Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
		1	2	3	4	5	Detail / Test			
Monitor IP Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A

		Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
		1	2	3	4	5	Detail / Test			
Monitor IP Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A

		Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
		1	2	3	4	5	Detail / Test			
Monitor IP Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A

		Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
		1	2	3	4	5	Detail / Test			
Monitor IP Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A

		Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
		1	2	3	4	5	Detail / Test			
Monitor IP Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A

		Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
		1	2	3	4	5	Detail / Test			
Monitor IP Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/> </									

4.14.3 SMTP Setting

Go to *STATUS > Reporting > SMTP Setting*, configure the SMTP Settings.

System Summary
Interfaces
Monitor Users
WiFi Monitor
Process Monitor
Logs & Reports
Reporting
Notification Settings
FTP Settings
SMTP Settings
Syslog Settings
Sessions
DHCP Leases
Routing Tables

Main > Status > Reporting > SMTP Settings

SMTP Settings

SMTP Server: Server Address: 10.2.4.25, Port: 25

Encryption: Disable TLS SSL

Authentication: Login (dropdown), Account Name: admin, Password: masked

Sender E-mail Address: controller@example.com

Receiver E-mail Address:
Receiver 1: admin@example.com
Receiver 2: manager@example.com
Receiver 3:
Receiver 4:
Receiver 5:

System Summary
Interfaces
Monitor Users
WiFi Monitor
Process Monitor
Logs & Reports
Reporting
Notification Settings
FTP Settings
SMTP Settings
Syslog Settings
Sessions
DHCP Leases
Routing Tables

Main > Status > Reporting > Notification Settings

Notification Settings

Select Receiver Click test to confirm the Notification e-mail could receive

	Receiver E-mail Address(es)					Detail / Test	SYSLOG	Primary FTP	Interval
	1	2	3	4	5				
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A	N/A	1 Hour
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A	N/A	N/A	N/A
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A	N/A	2 Mins

Select the sending interval

4.14.4 Syslog Setting

System Summary
Interfaces
Monitor Users
WiFi Monitor
Process Monitor
Logs & Reports
Reporting
Notification Settings
FTP Settings
SMTP Settings
Syslog Settings
Sessions
DHCP Leases
Routing Tables

Main > Status > Reporting > SYSLOG Settings

SYSLOG Settings

SYSLOG: Enabled Disabled Enable SYSLOG function

SYSLOG Server:
Server 1: IP Address: 10.2.30.30, Port: 514
Server 2: IP Address: , Port:

Severity Level: emergency Select Severity Level

Apply Cancel

- System Summary
- Interfaces
- Monitor Users
- WiFi Monitor
- Process Monitor
- Logs & Reports
- Reporting**
- Notification Settings
- FTP Settings
- SMTP Settings
- Syslog Settings
- Sessions
- DHCP Leases
- Routing Tables

Main > Status > Reporting > Notification Settings > Local Users Log SYSLOG Settings

Local Users Log SYSLOG Settings

Tag	<input type="text" value="local"/>	Determine the Tag, Serverity and Facility
Severity	<input type="text" value="informational"/>	
Facility	<input type="text" value="local 0"/>	

Notification Settings

Click pencil to edit the information of Local Users Log

	Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval
	1	2	3	4	5			
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A	N/A	1 Hour ▾
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Hour ▾
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▾