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 Captive Portal with Company Logo....3
3.3.2 Staff and Guest connect to the same SSID....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 Guest Users → Policy 1 profile configuration....22
4.9.1 Staff Users → Policy 2 profile configuration....24
4.10 USERS – USER GROUPS CONFIGURATION....27
4.11 USE WAPM ON EWS TO MANAGE ECW....29
4.11.1 Edit WAPM Templates....29
4.11.2 Establish CAPWAP Tunnel from AP to EWS....32
4.11.3 Applying the template....34
4.12 1+1 HIGH AVAILABILITY....36
4.12.1 Configure EWS#1 HA....36
4.12.2 Configure EWS#2....36
4.12.3 Confirm HA status of both EWS....37
4.13 REPORTING....37
4.13.1 Notification....37
4.13.2 FTP Setting....38
4.13.3 SMTP Setting....39
4.13.4 Syslog Setting....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
- 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
- Estimated 3500 concurrent users - Centralized manage 1200 APs - Standby unit for service redundancy

2.2 Feature Requirements:

Wi-Fi Features
- 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
- 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
- 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	- 5000 recommended concurrent users - 1200 APs managed - High Availability 1+1 - Power Redundancy

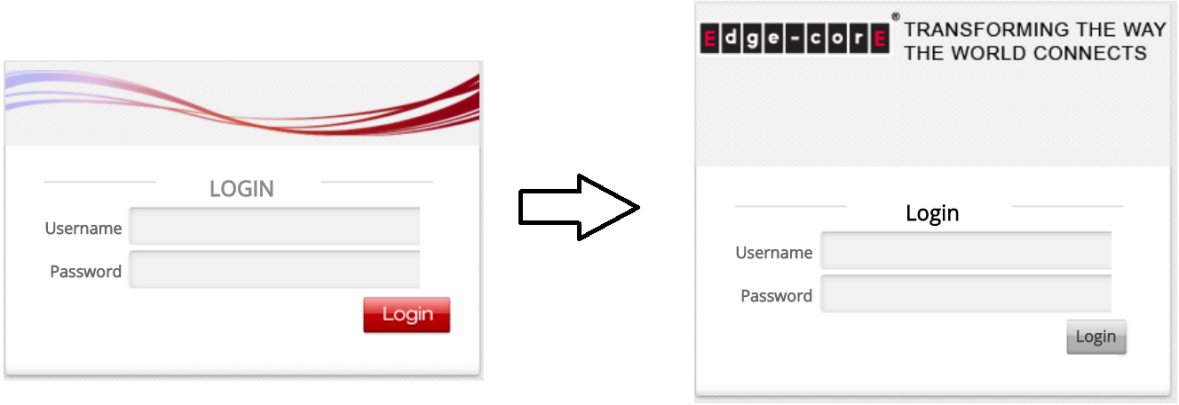
Location	Area	AP Model	QTY
Factory	500m^2 x 40 sties	ECW	400
Office	300m^2 x 40 floors x 2 buildings	ECW	800

3.2 Network Topology:

3.3 Expected Results:

3.3.1 Captive Portal with Company Logo

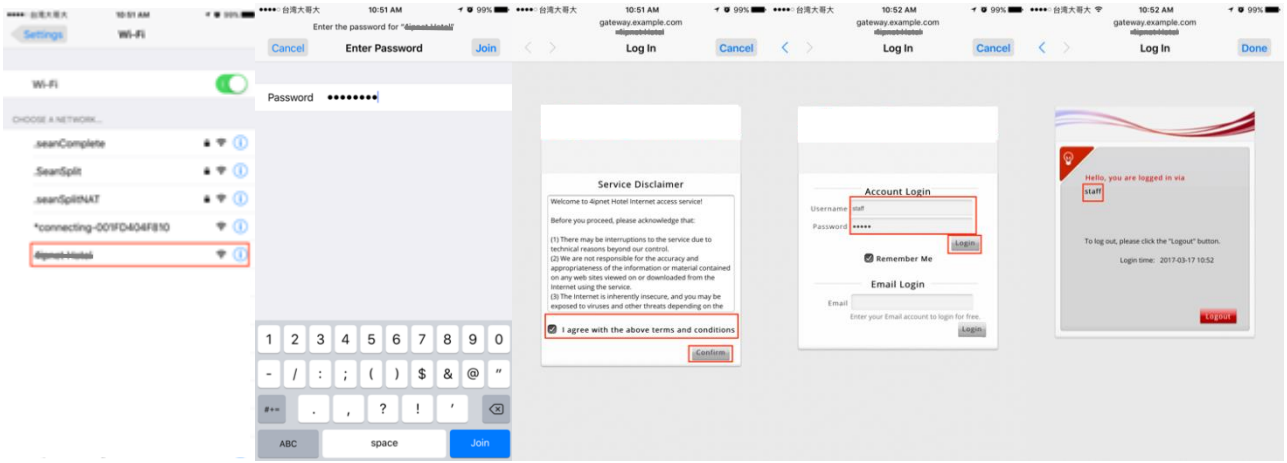
The customizable Login Page allows MIS administrators to easily change the logo on the top with their most current advertisement images.



3.3.2 Staff and Guest connect to the same SSID

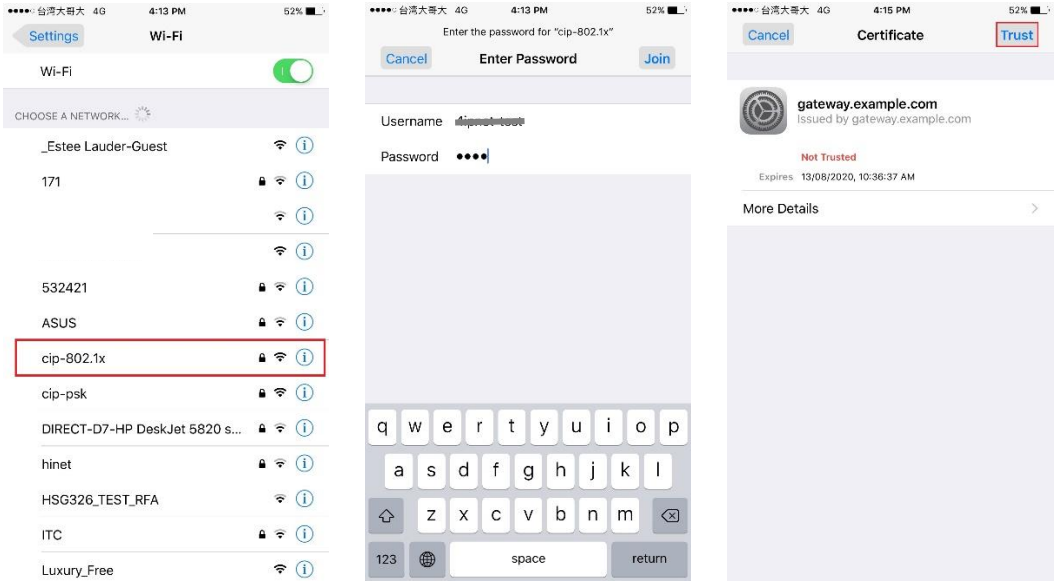
User Login Flow (UAM) – Staff/Guest account

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.



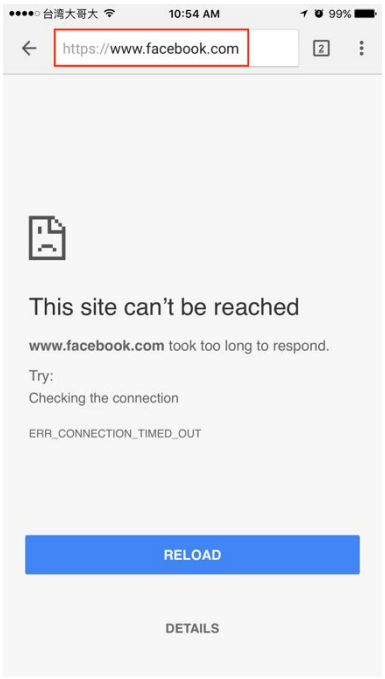
User Login Flow (WPA2-Enterprise) – Staff account

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.



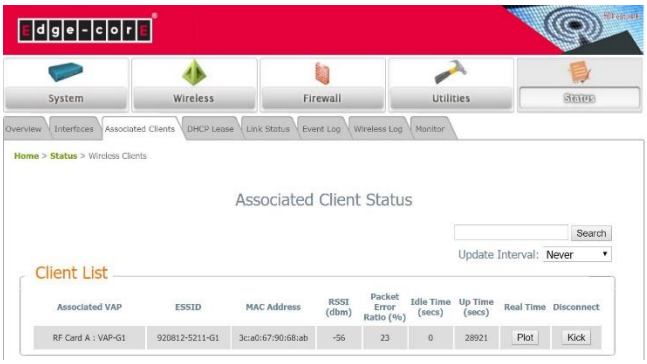
Facebook access blocked for Staff accounts

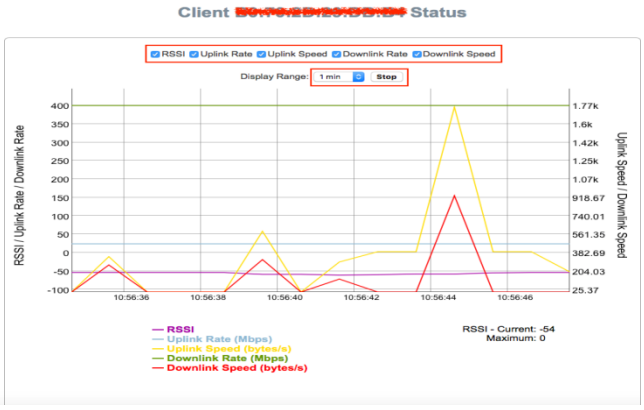
The Staff Users belong to Staff Group with specific Firewall Rule for blocking their traffics to Facebook website. So, after Staff users have successfully logged in, they cannot reach to www.facebook.com.



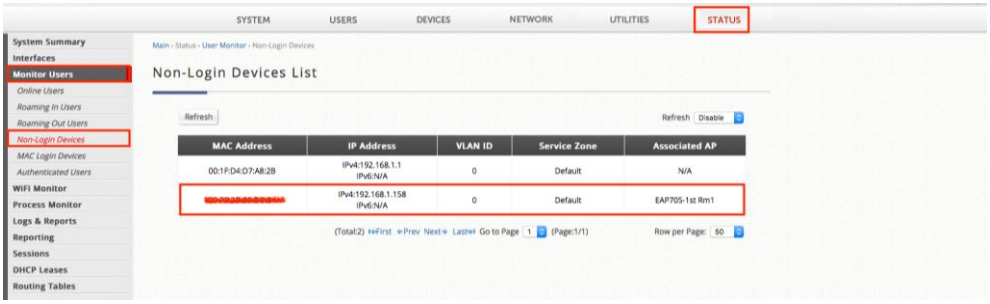
Real time and daily network usage reports

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.

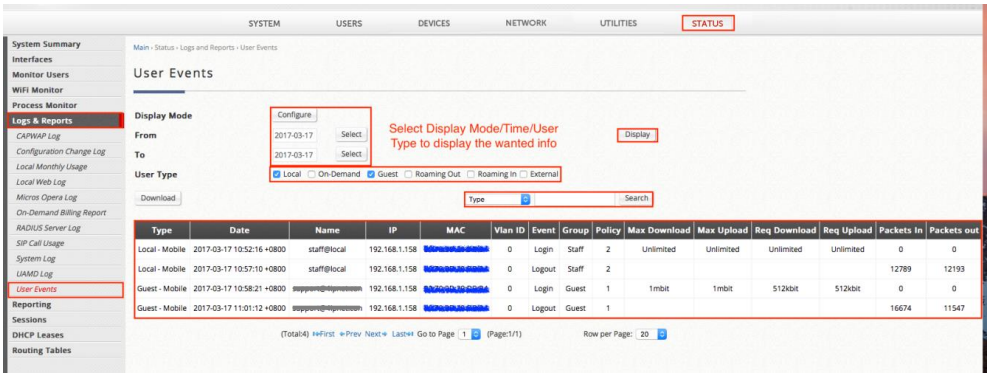




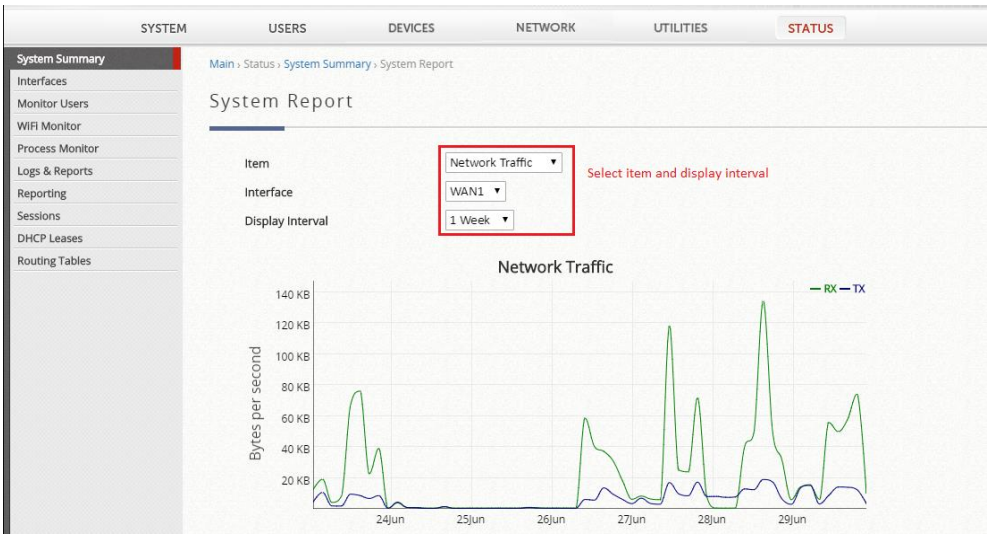
Before user successfully logged in, administrator may observe them on EWS's *Non-Login Devices*. After user successfully logged in by their accounts, EWS's *Online Users List* will have their real-time information.



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

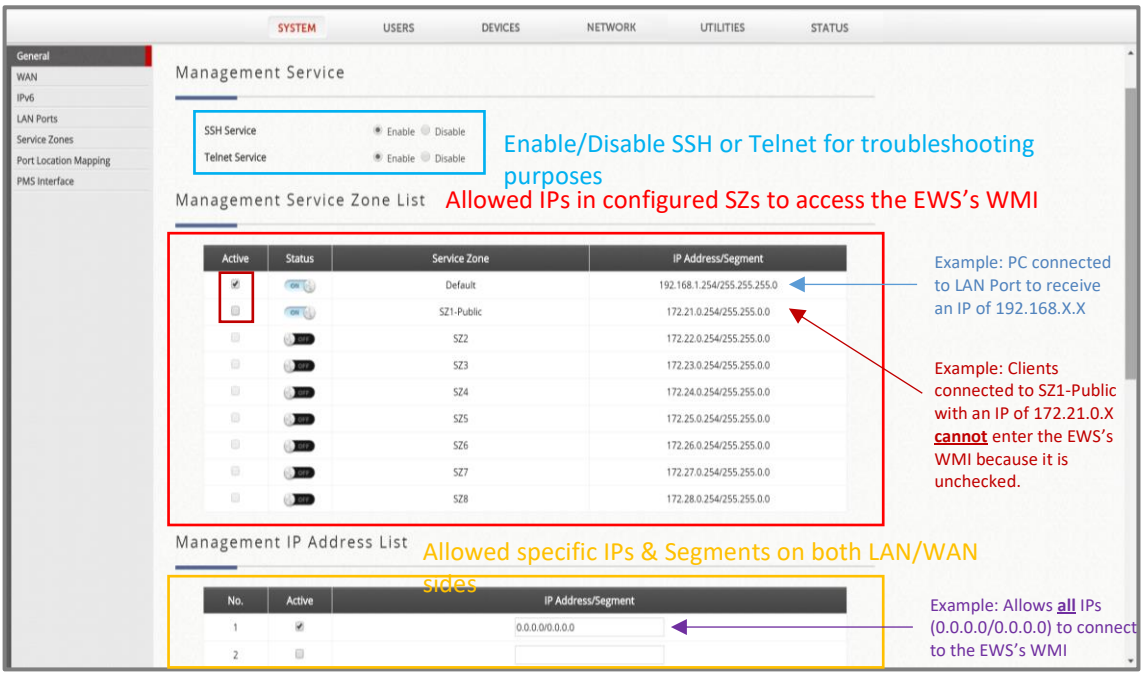


The administrator could monitor the *System Report* to confirm status of each items.



GUI permission only for Staff Users

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



4 Configuration

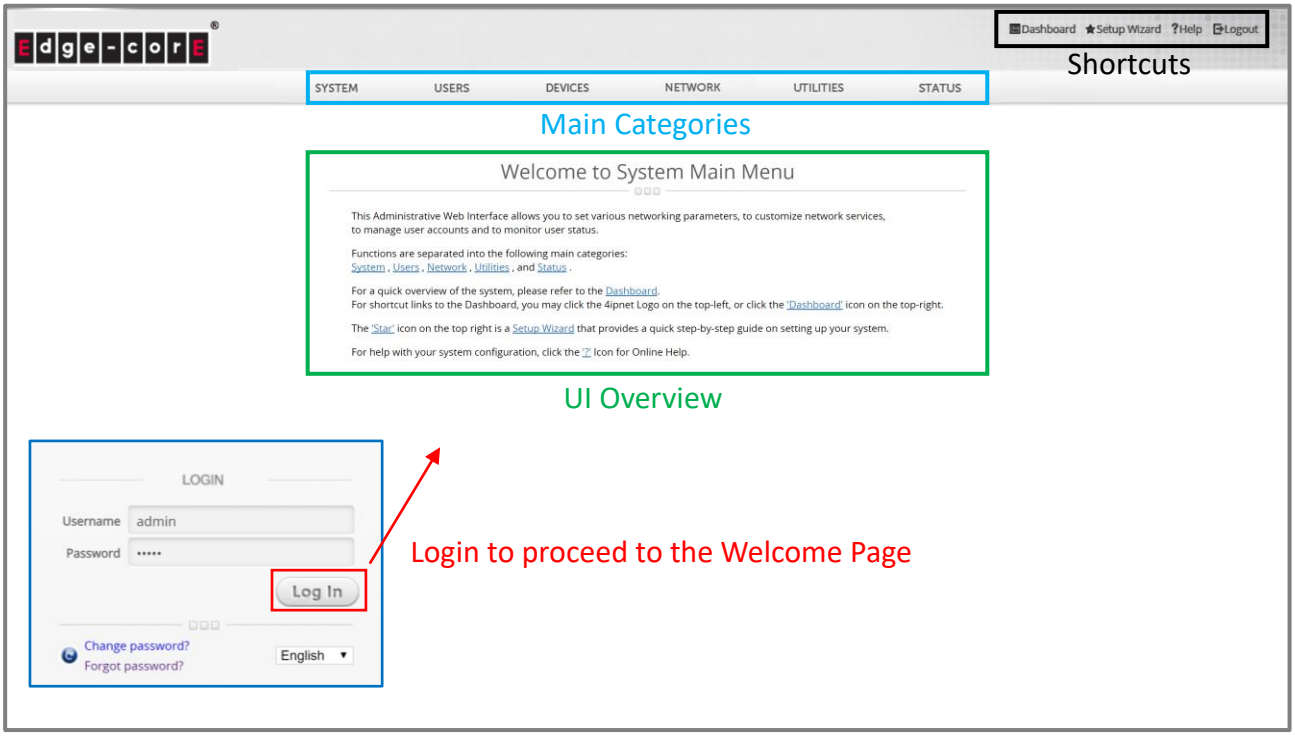
4.1 Configuration Checklist

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

	- Devices > WAPM › AP List *- Establish CAPWAP Tunnel from AP to EWS*	☐
3.13 1+1 High Availability	*- System > High Availability*	☐
3.14 Reporting	*- Status > Reporting › Notification* *- Status > Reporting › FTP Setting* *- Status > Reporting › SMTP Setting* *- Status > Reporting › Syslog Setting*	☐ ☐ ☐ ☐

4.2 System – Initial Access Browser-based GUI

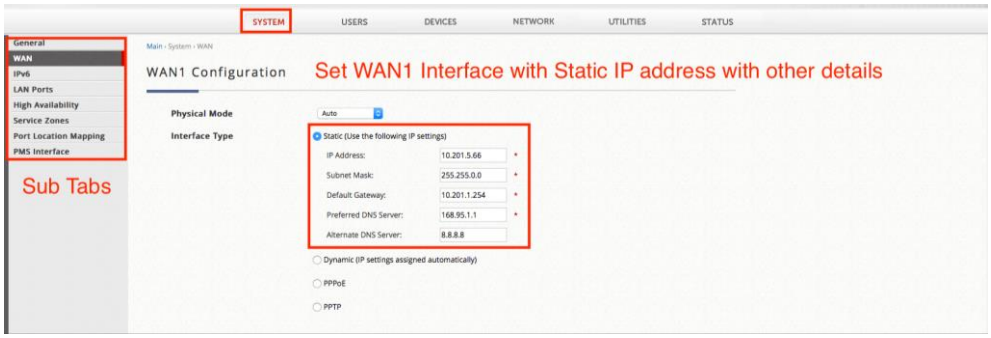
Connect your PC to the EWS's LAN port, then access the EWS's Web Management Interface (WMI) by entering 192.168.1.254 in your web browser. Login to the EWS using the Default Username/Password: *admin/admin*.



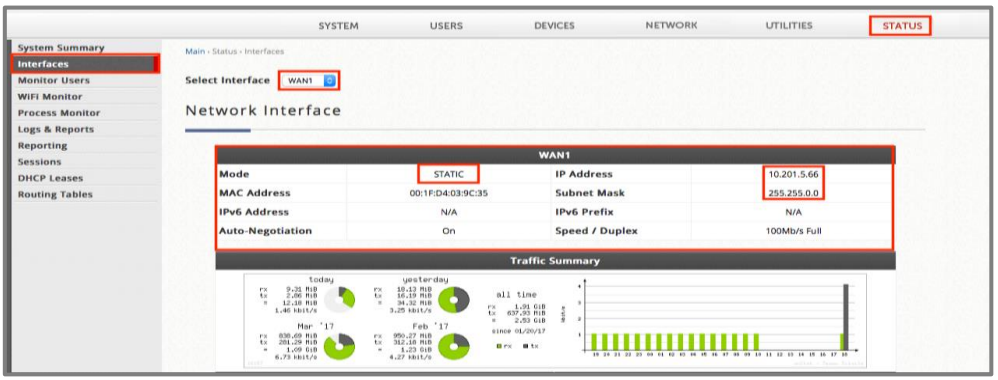
Note: first time login will require changing the password.

4.3 System – WAN & LAN Interface Configuration

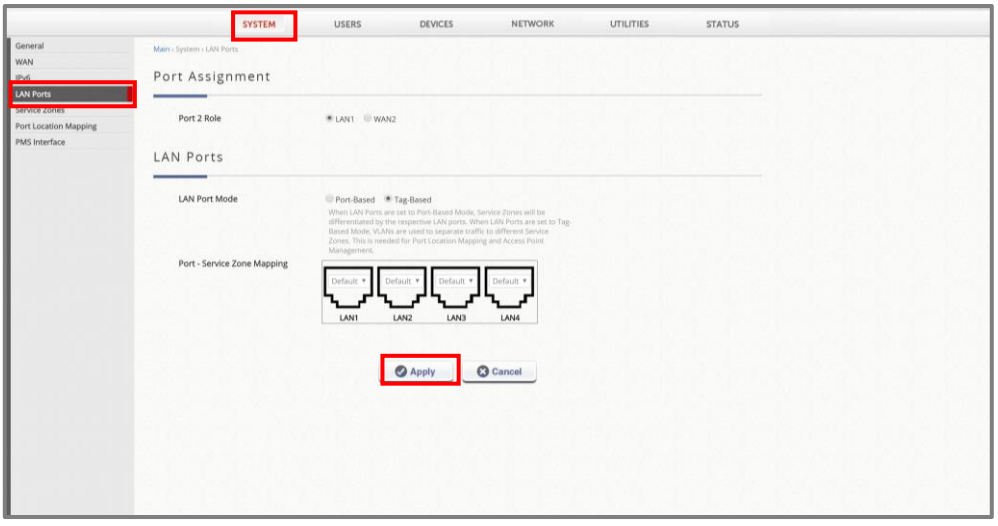
Go to *System > WAN* to configure the WAN1 Interface Type as "*Static*" with required details. Here we set the IP Address as 10.201.5.66/255.255.0.0 with *Default Gateway* 10.201.1.254.



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

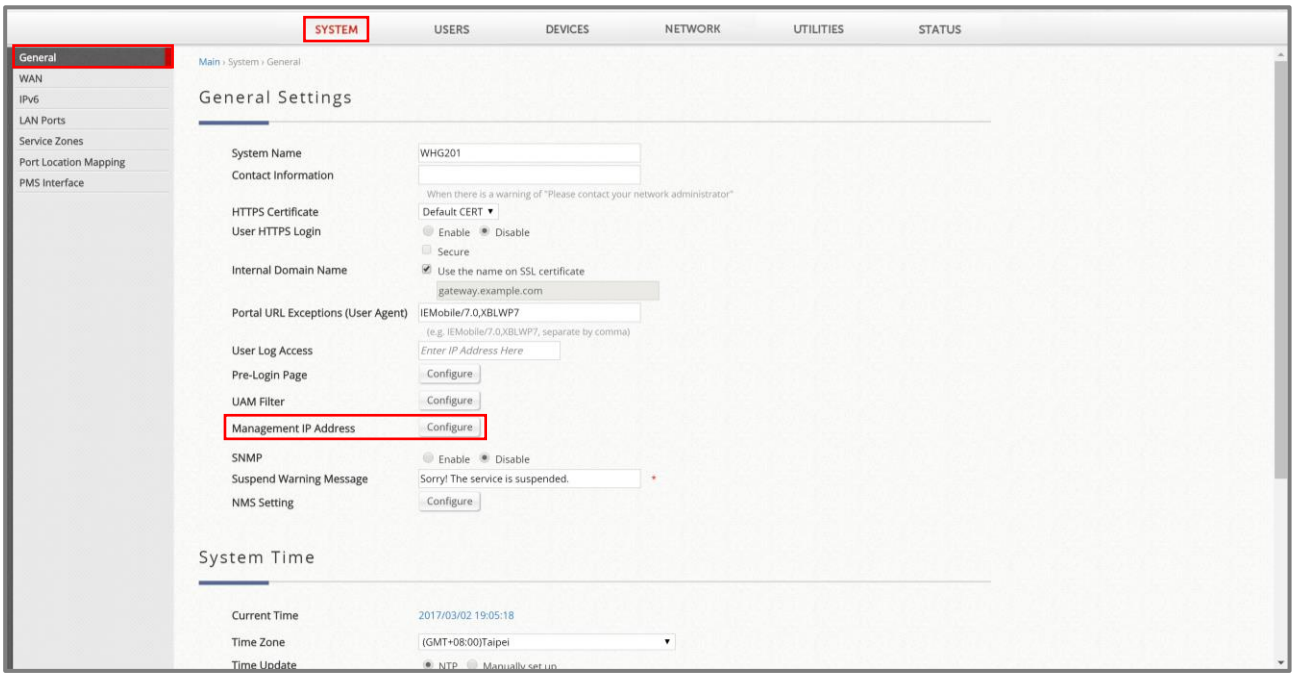


Go to *System > LAN Ports* to select "Tag-Based" as the *LAN Port Mode* and click on Apply.

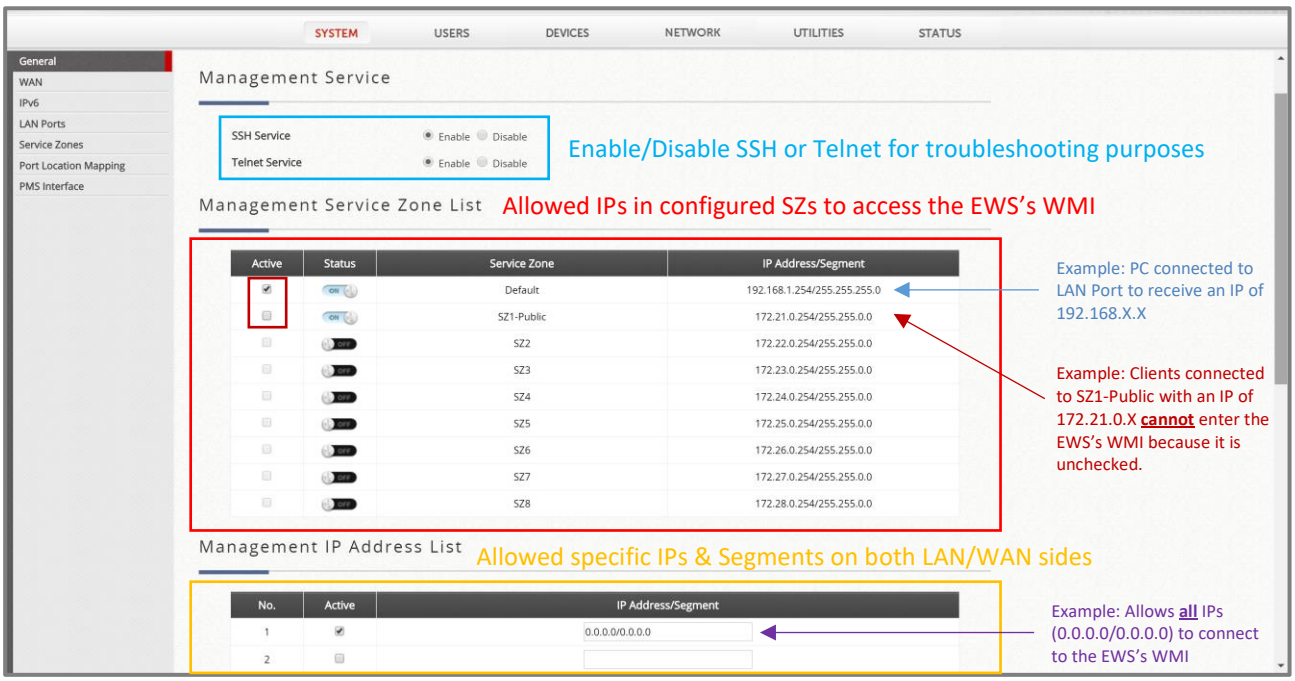


4.4 System - Management IP Address List

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



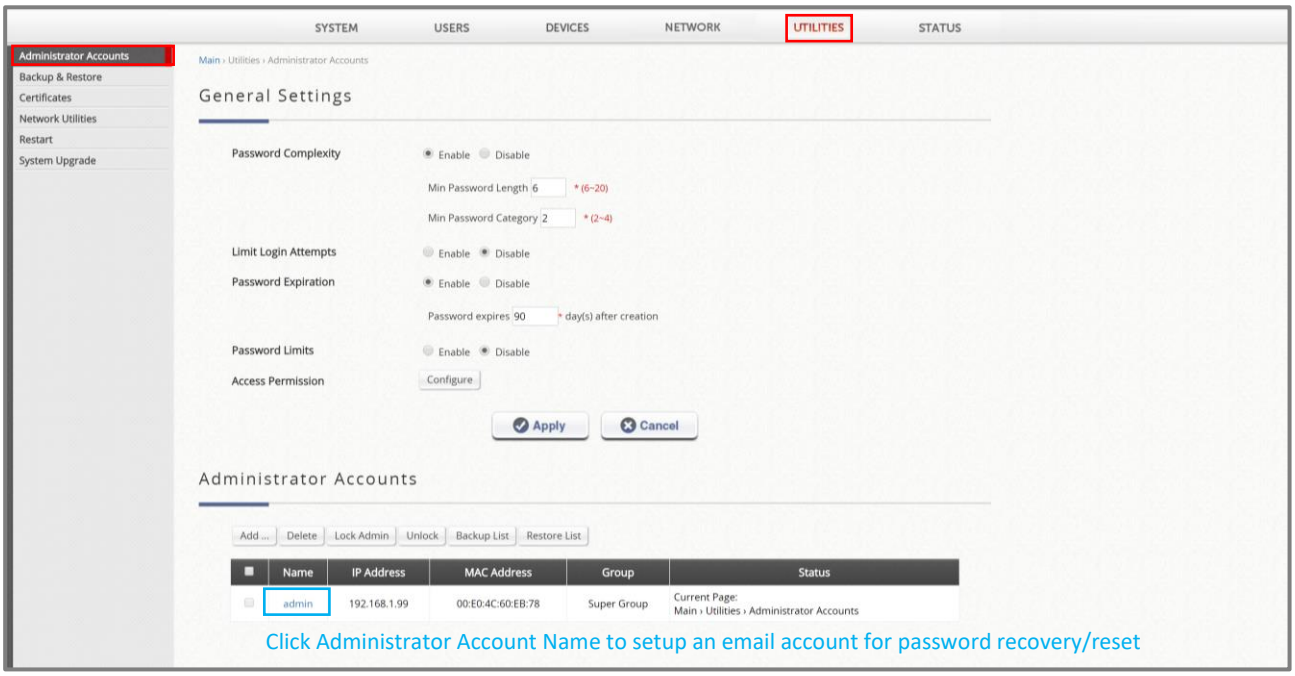
Check the appropriate SZs and configure the preferred IP Addresses to allow access to the Web Management Interface.



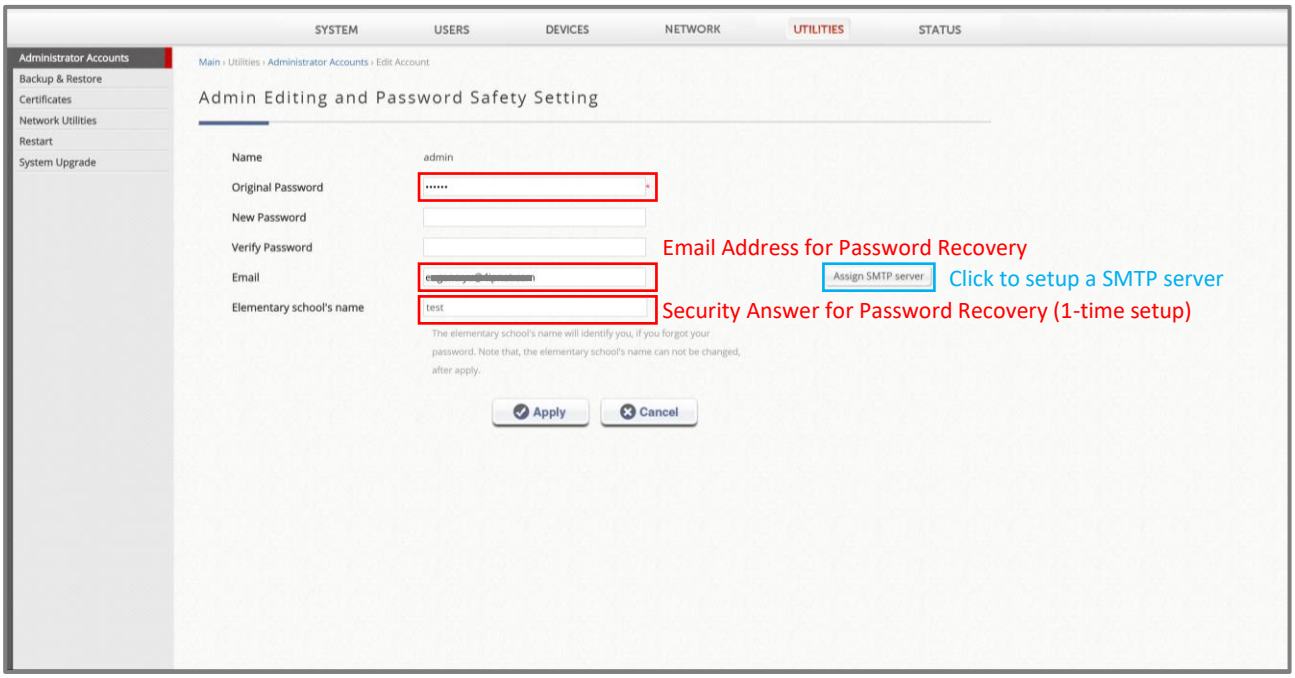
Note: Unchecking all options and disabling the SSH/Telnet Service will result in being locked out of the EWS. Please be cautious when configuring the Management IP List.

4.5 Utilities - Admin Password Recovery

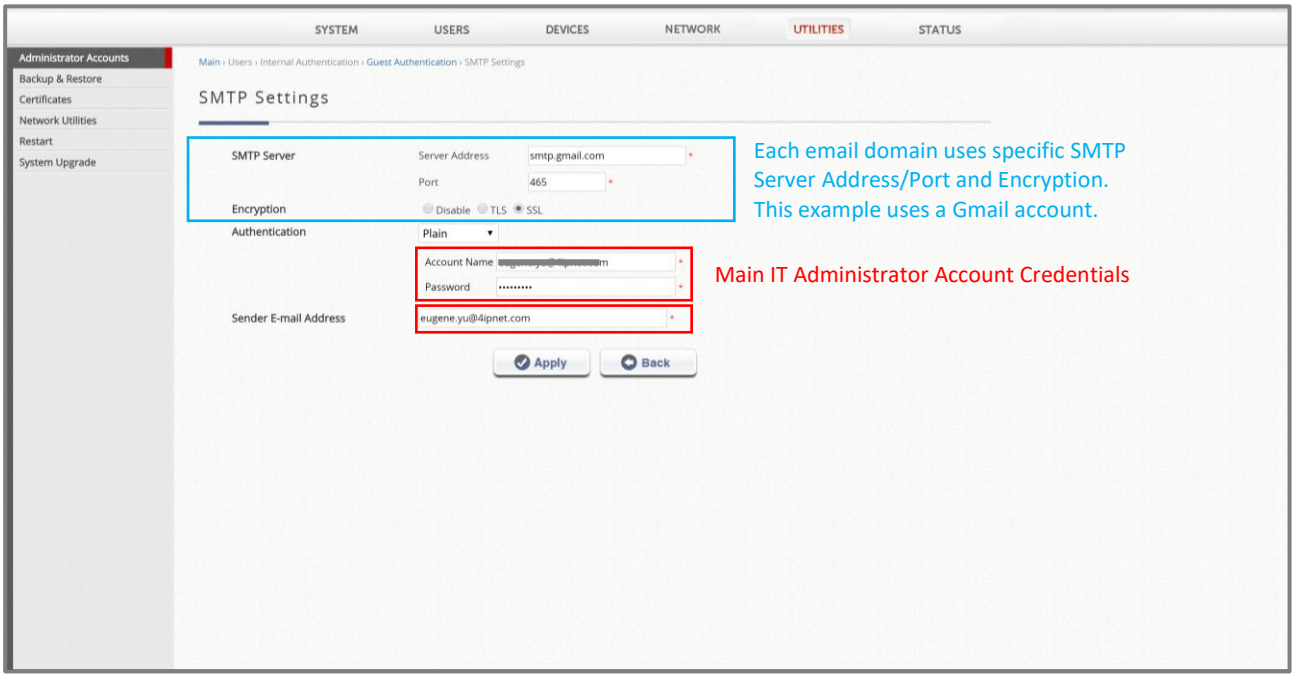
Go to *Utilities > Administrator Accounts* and click the "*admin*" Name to configure password recovery.



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



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

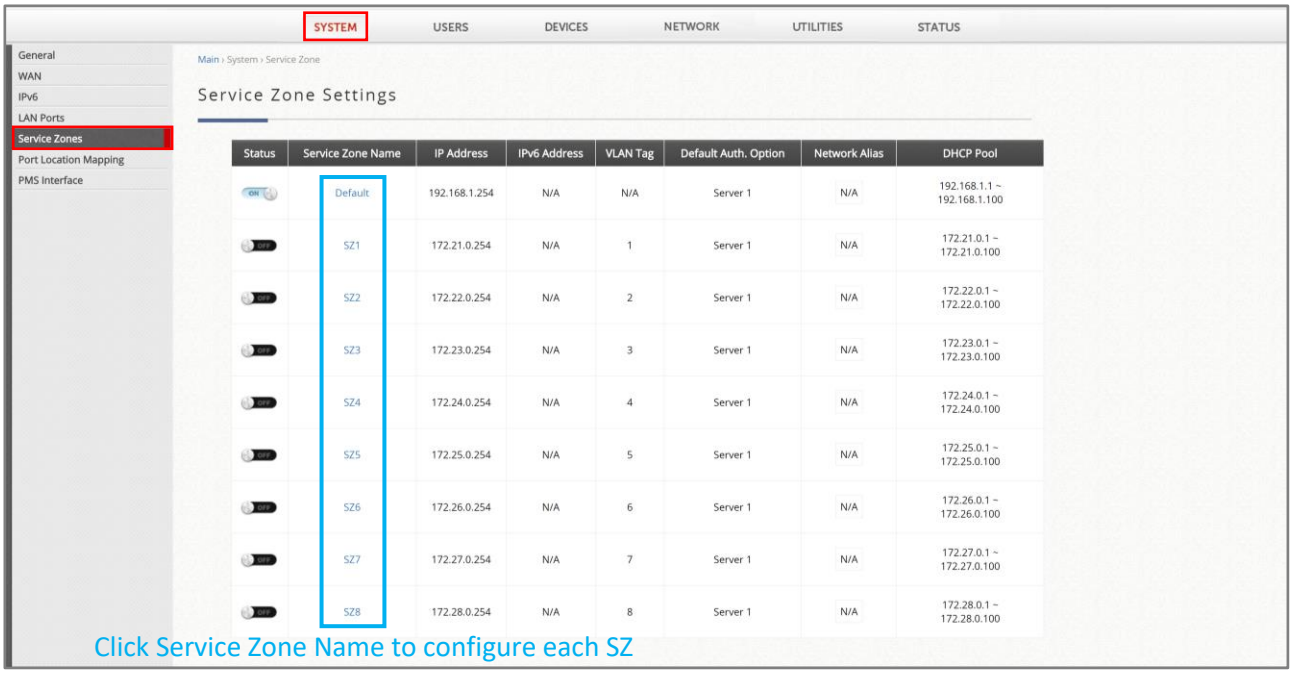


4.6 System - Service Zones Configuration

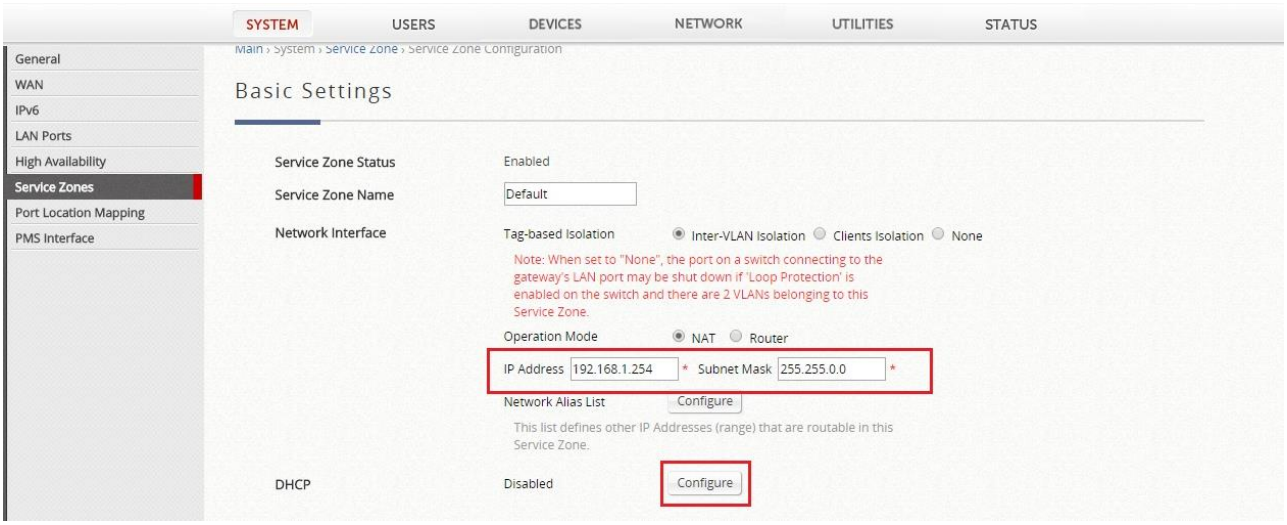
Go to *System > Service Zones* and confirm WAN Subnet and *Default Service Zone* IP Address are in different subnets. Take below as example,

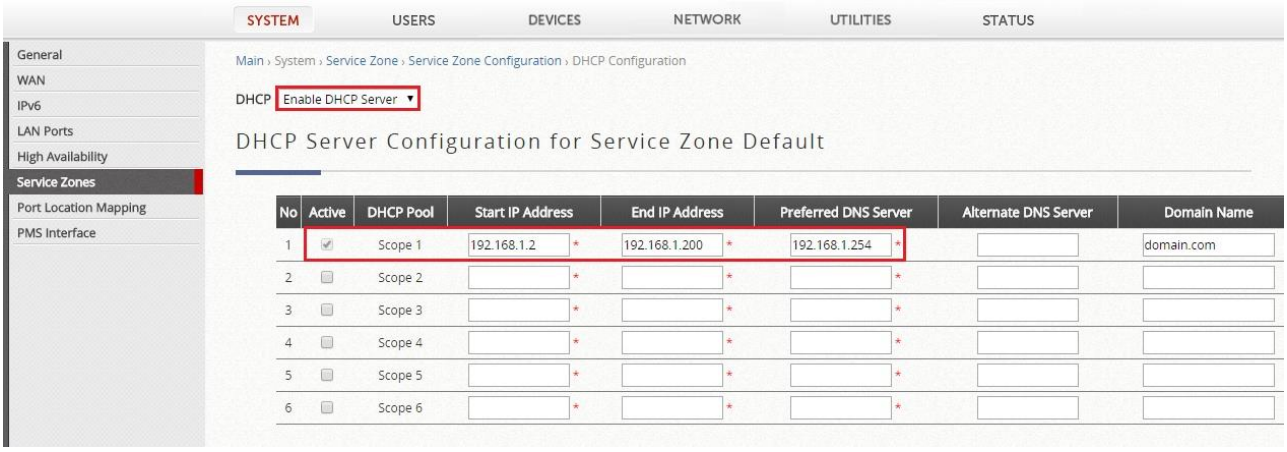
WAN1 = 10.201.5.66 / Subnet = 255.255.0.0

LAN/Default SZ = 192.168.1.254 / Subnet = 255.255.0.0

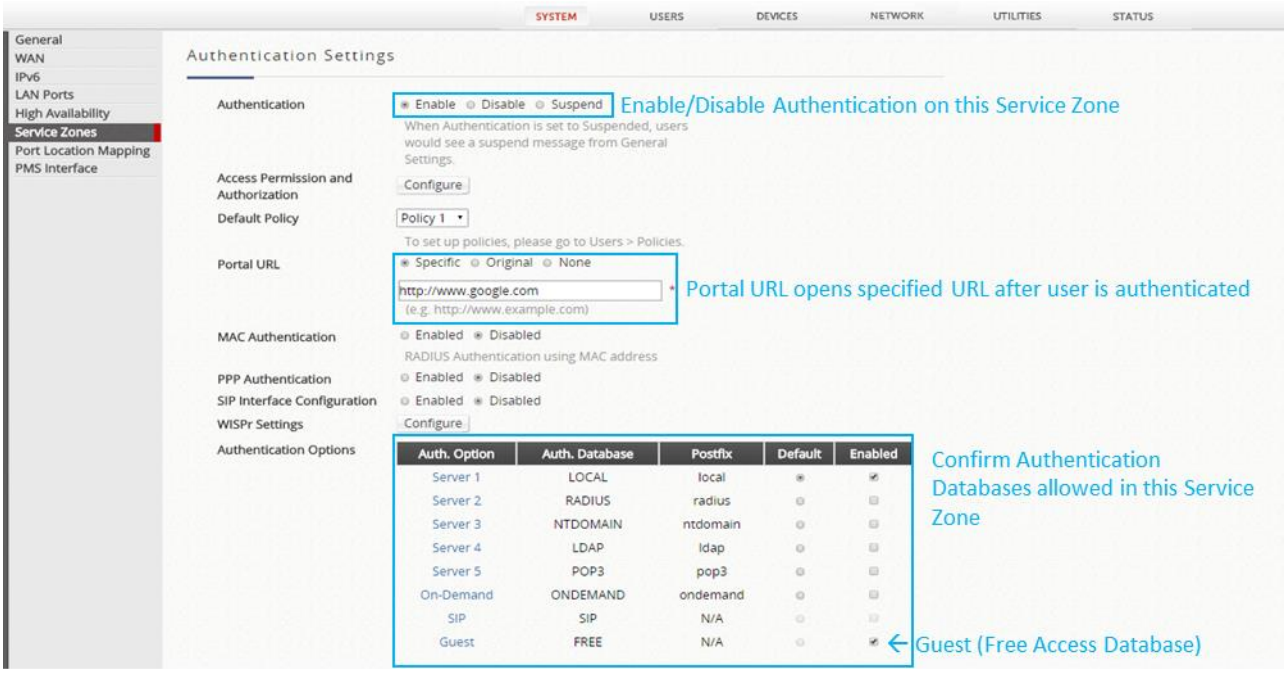


Click *Default Service Zone*, and administrators are able to enable the Service Zone Status and configure the basic network settings, including *Service Zone IP address, DHCP scope*, and *preferred DNS server,* etc.



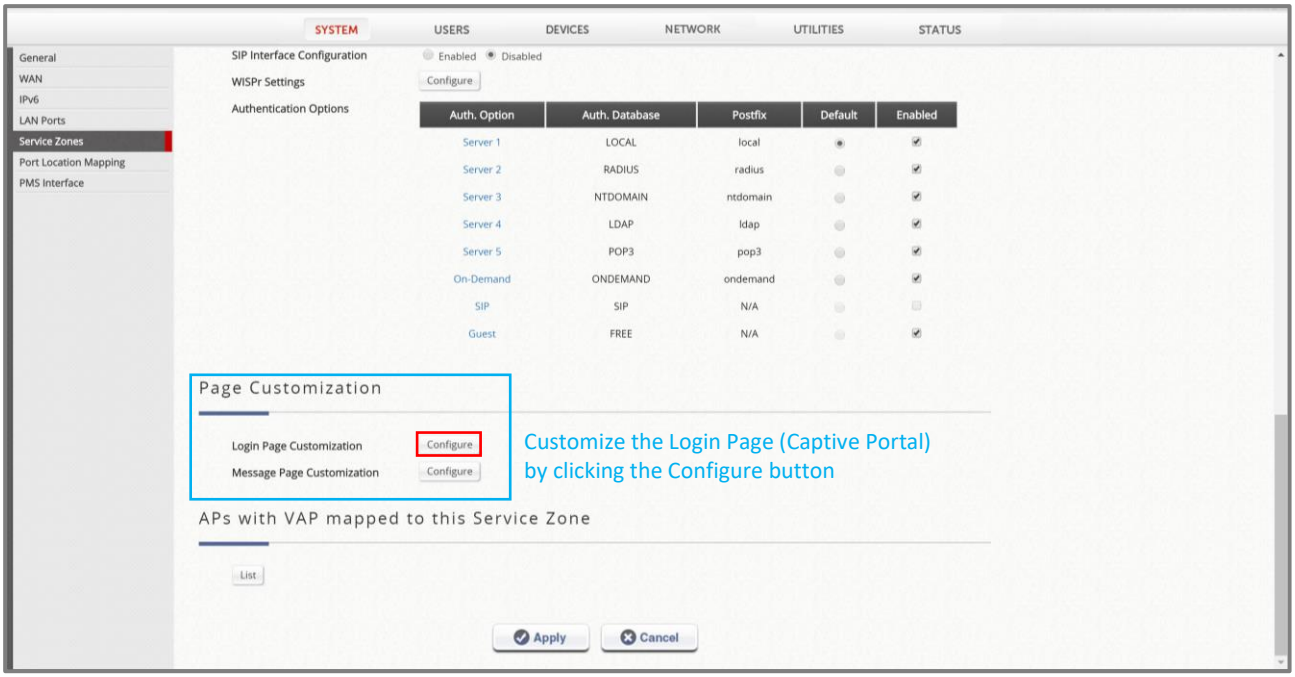


Next, Configuring *Authentication Settings* is another important session, which administrators can enable *Guest Authentication* Database to allow self-registration users.

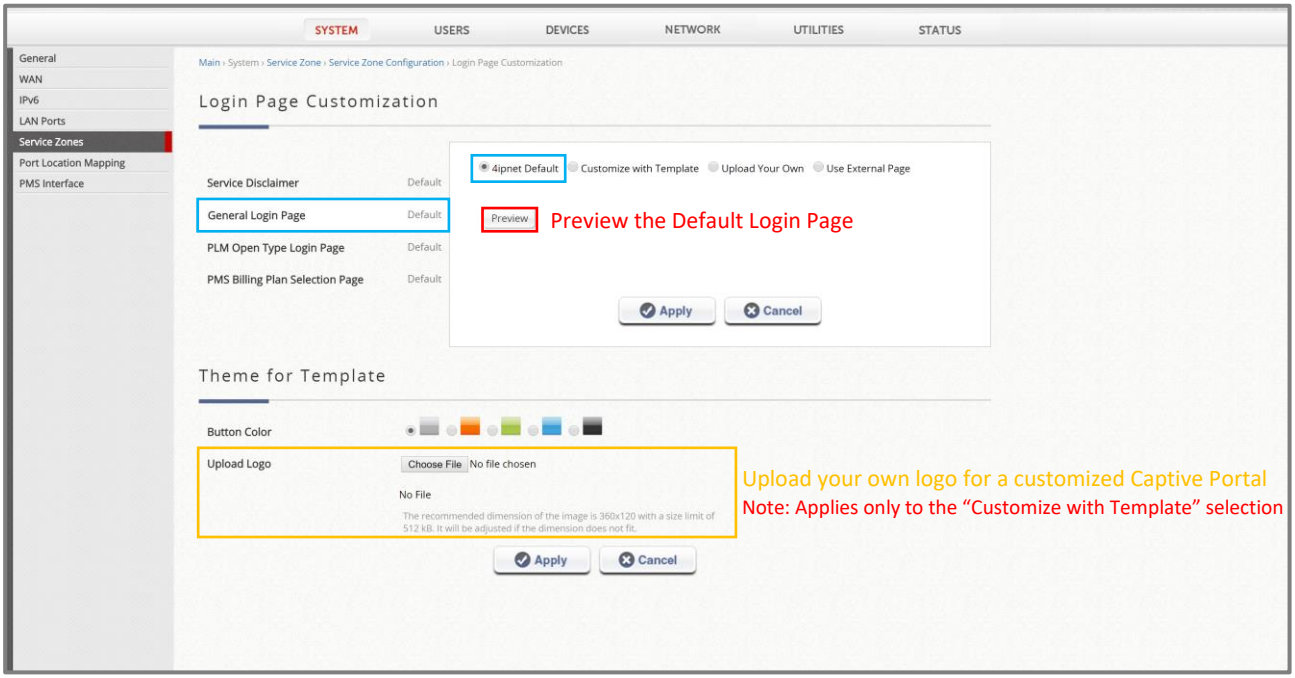


4.7 System - Service Zone – Captive Portal Customization

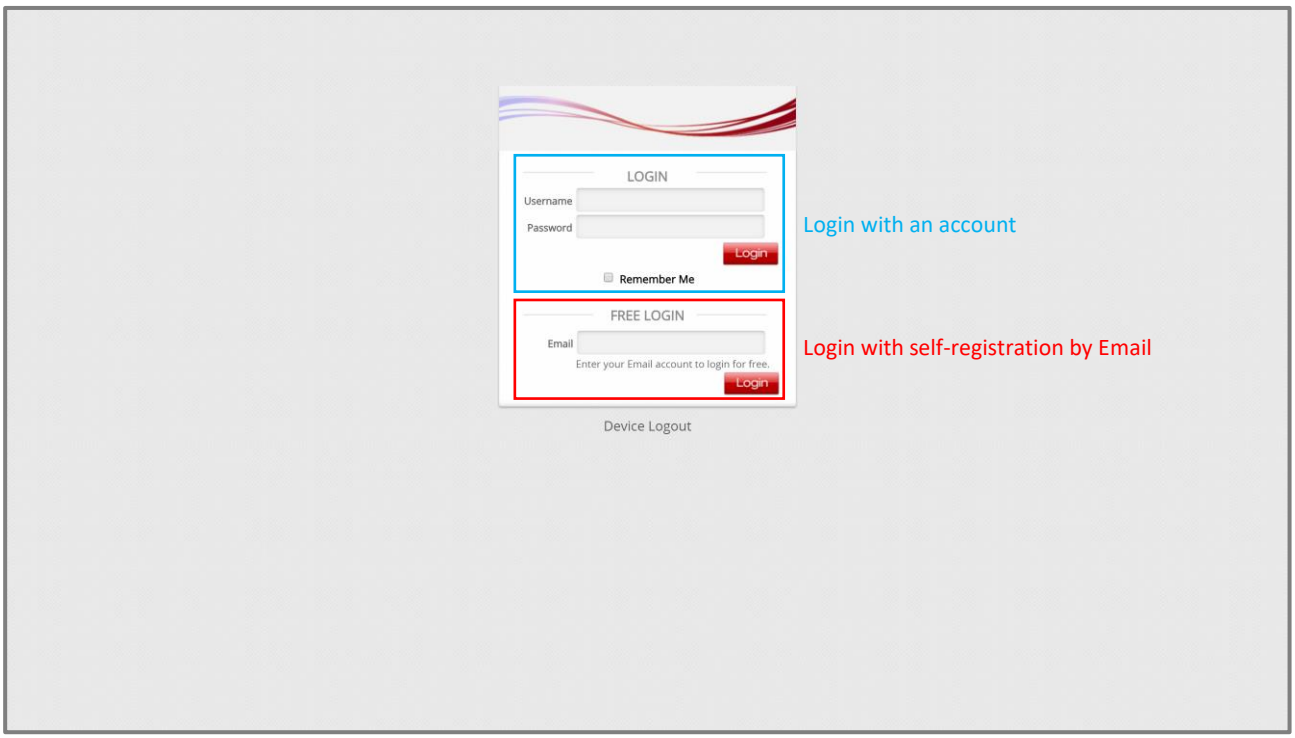
Go to *System > Service Zones > Service Zone Configuration › Login Page Customization* Click "*Configure*" button to start customizing different Login Page. On the other hand, *Message Page Customization* will provide customizations to message pages such as the login success page.



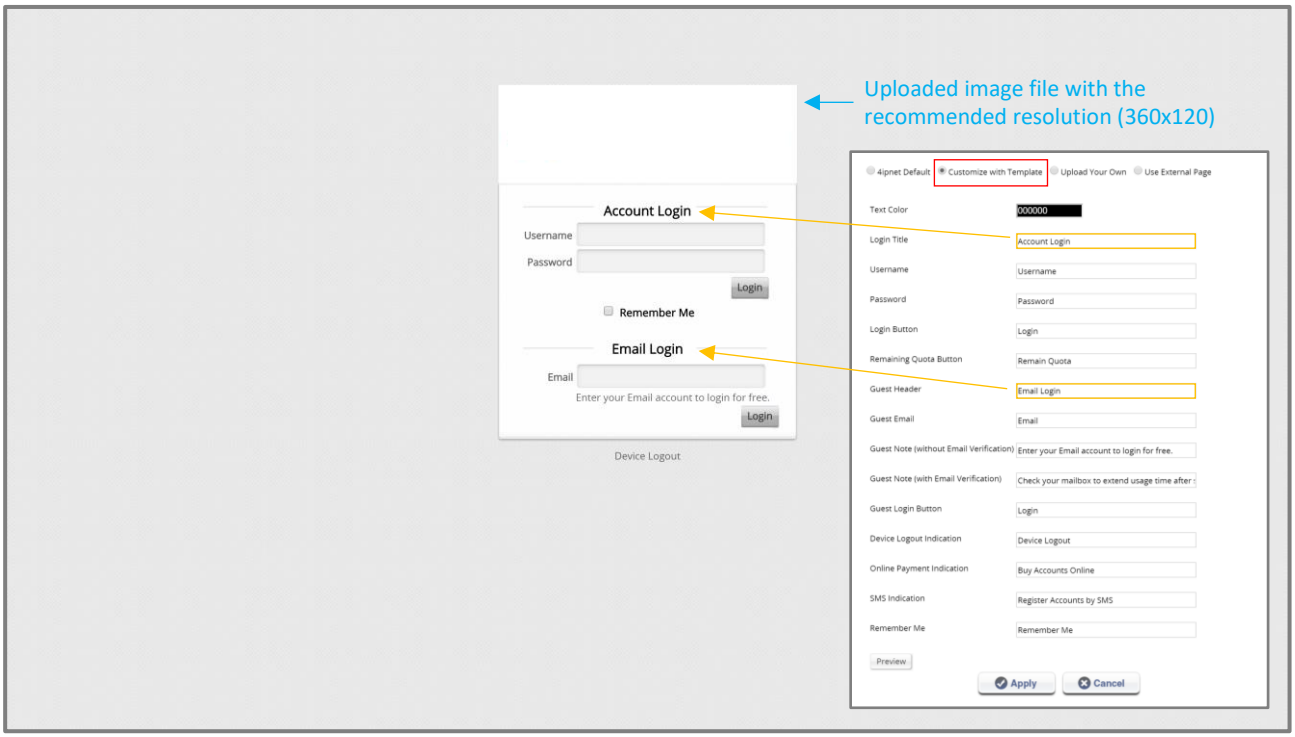
Each page has 4 different types of customization, *Default, Customize with Template, Upload Your Own,* and *Use External Page*.



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

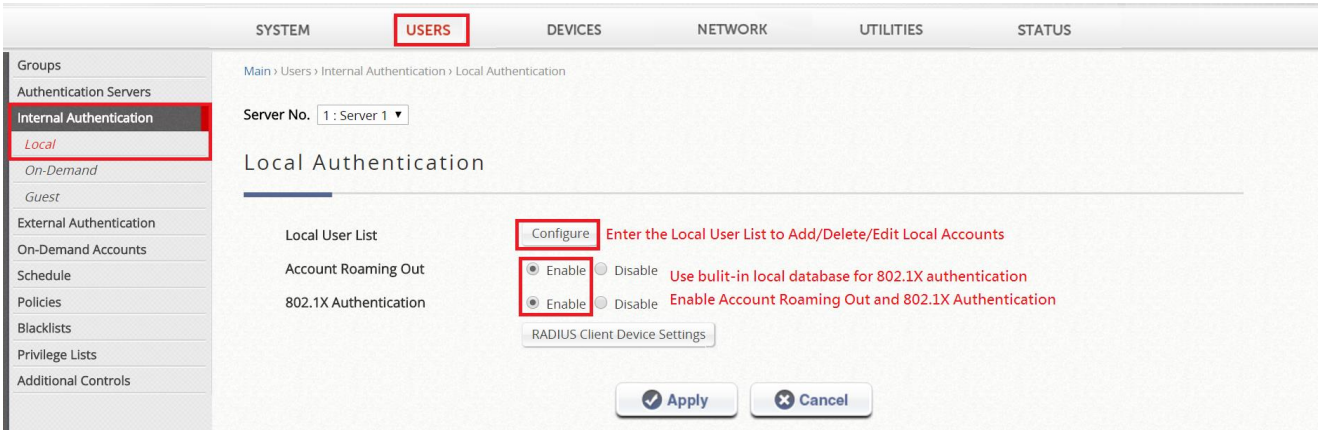


Preview General Login Page in *Customize with Template* mode with an uploaded logo and customized text.

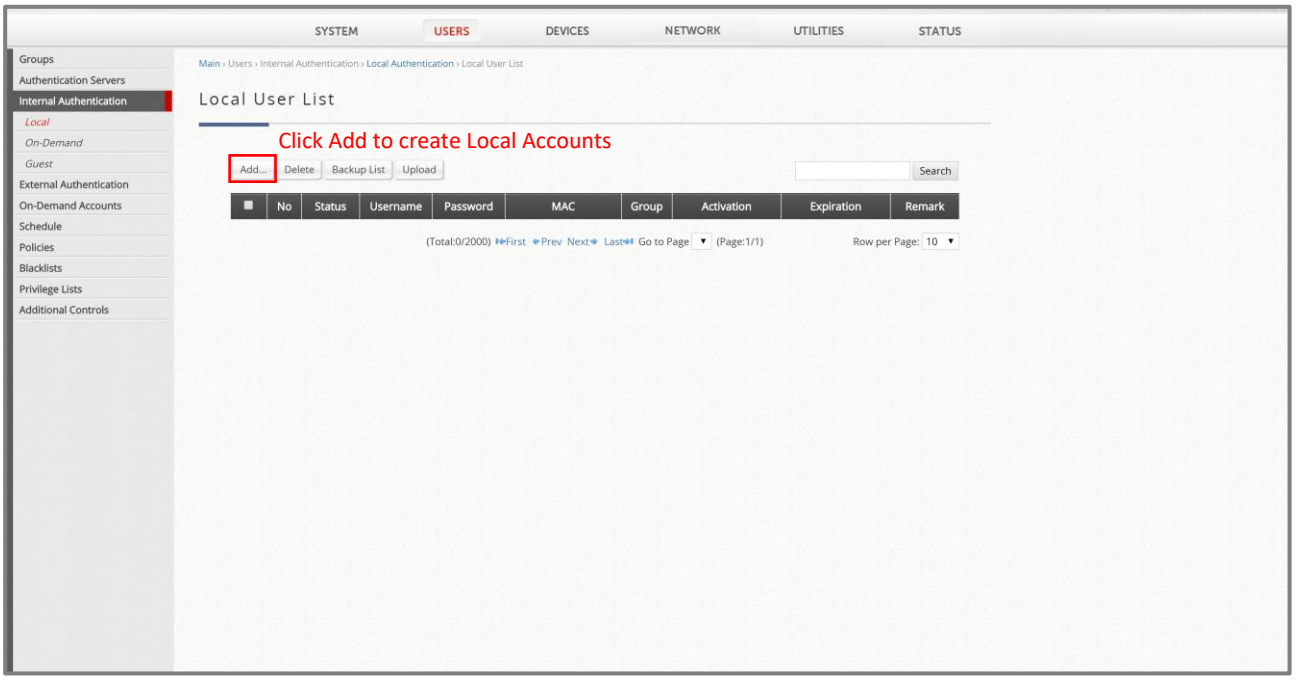


4.8 Users - Local Accounts

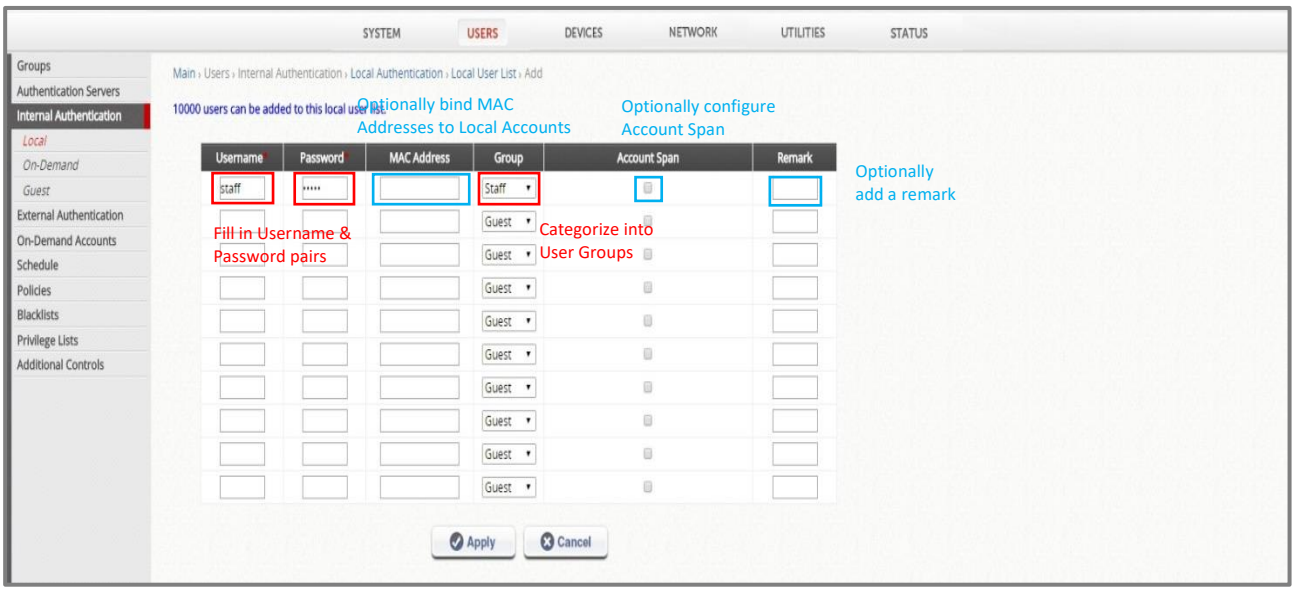
Go to *Users > Internal Authentication > Local* to create accounts using the Local Database.



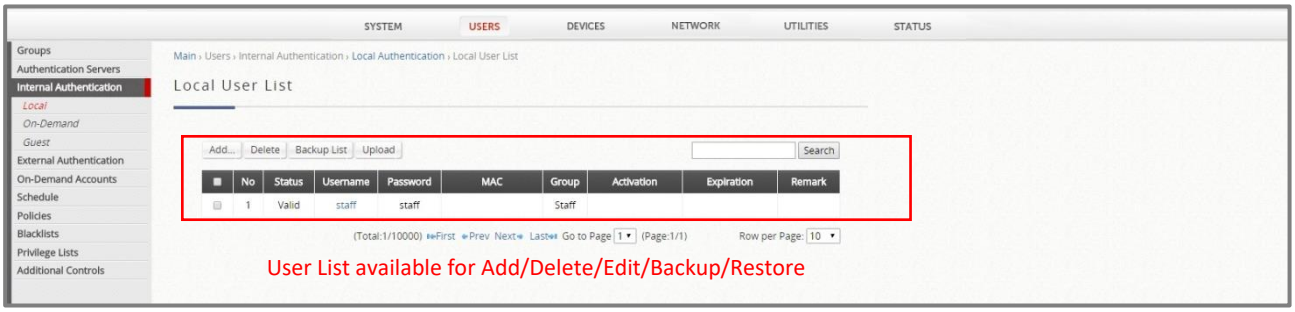
Click *Add* to create a single or multiple accounts at once.



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



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

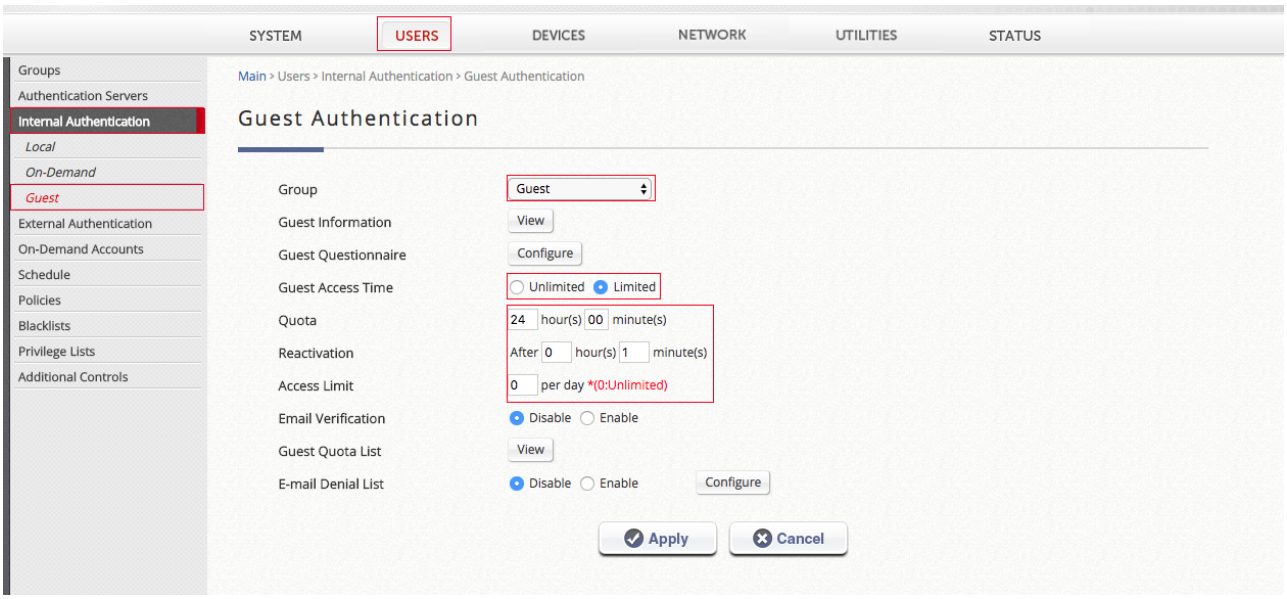


4.9 Users – Guest Authentication

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.

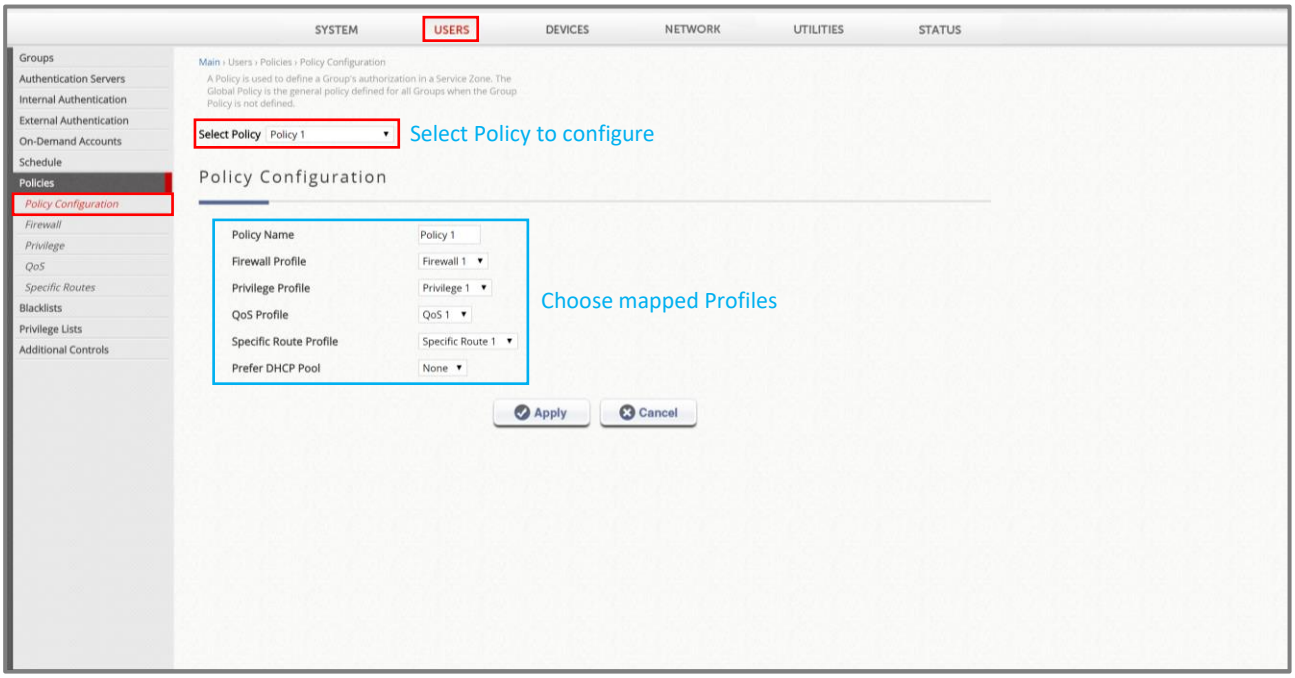


4.10 Users – User Policies Configuration

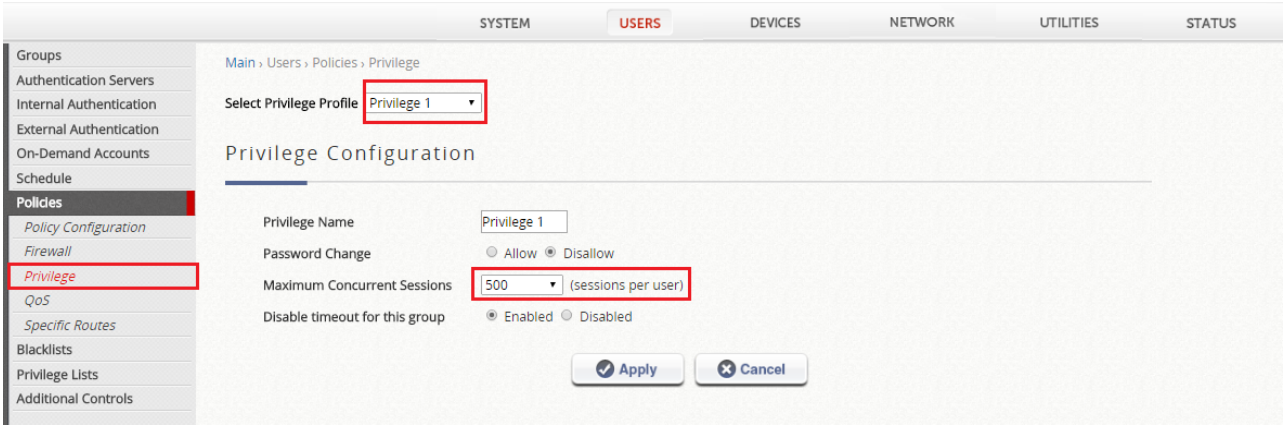
Administrator is going to enforce *Policy 1* on Guest users with limited 500 *Maximum Concurrent Sessions* & *QoS bandwidth* control; and *Policy 2* on Staff users with *Firewall Rule* to block Facebook access & *Unlimited Maximum Concurrent Sessions*.

4.10.1 Guest Users → Policy 1 profile configuration

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



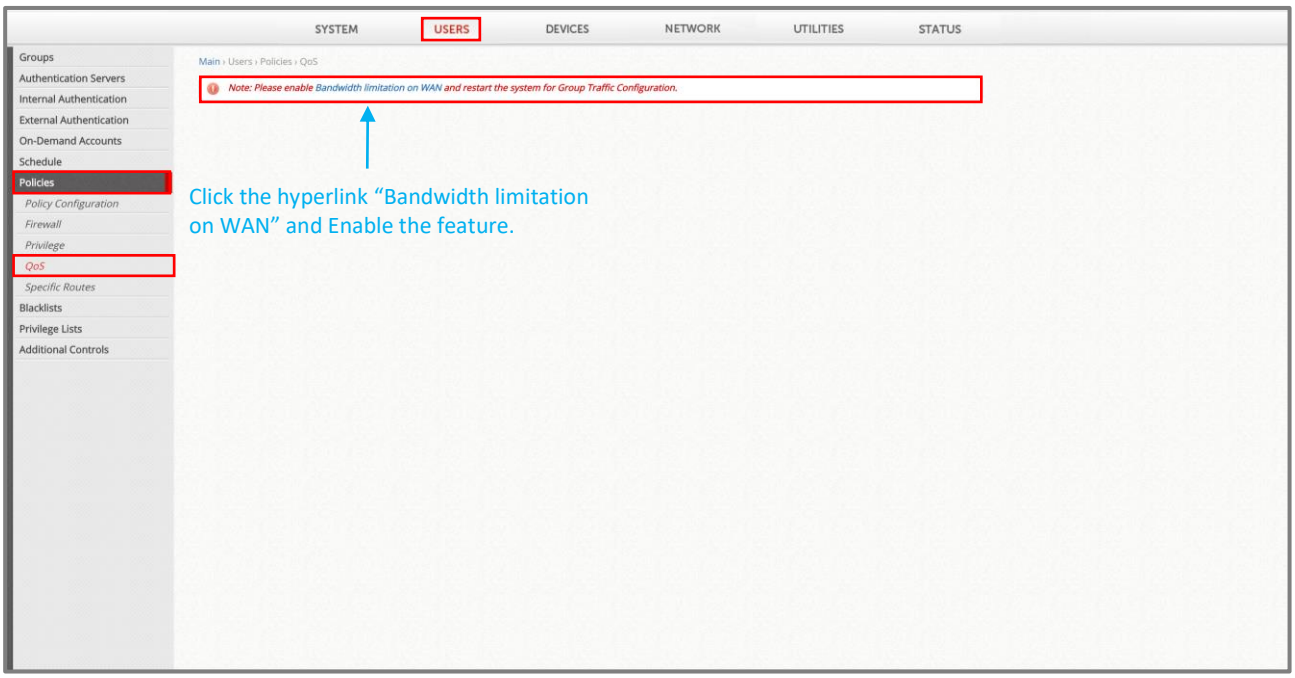
Go to *Users > Policies > Privilege 1* to check if the *Maximum Concurrent Session* is 500 as the default value.



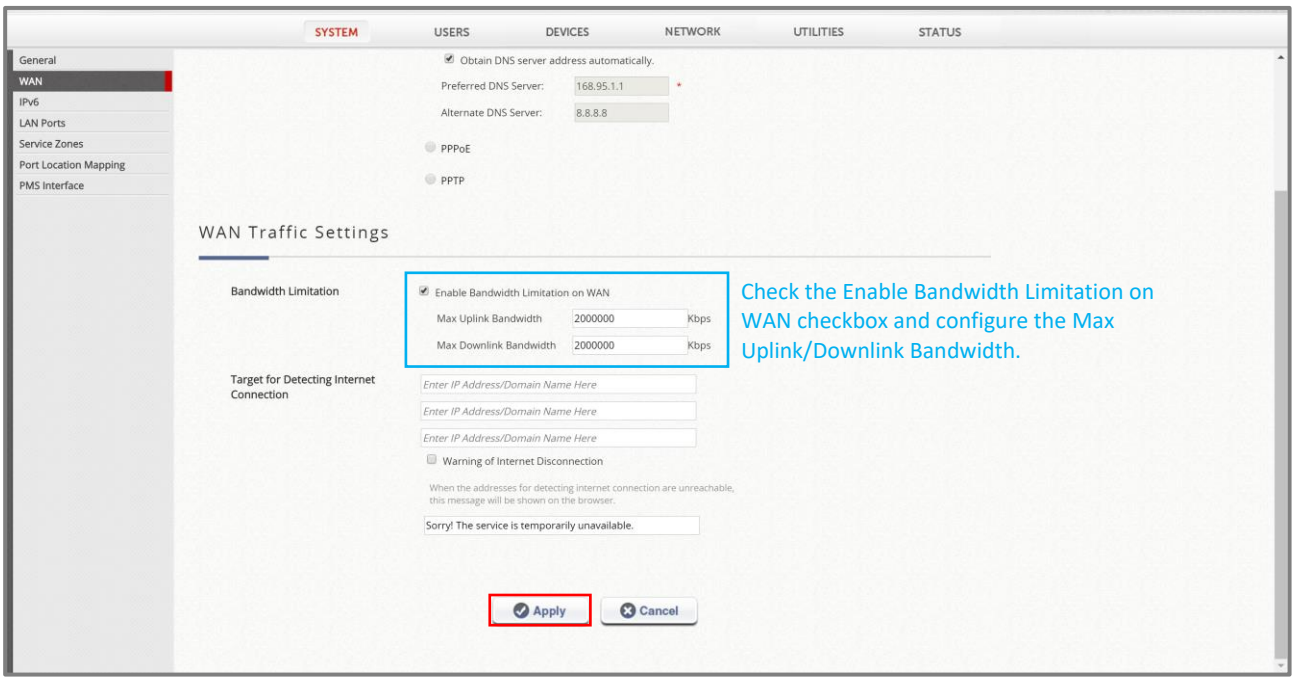
Go to *Users > Policies > QoS* to configure each Group/User's bandwidth.

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

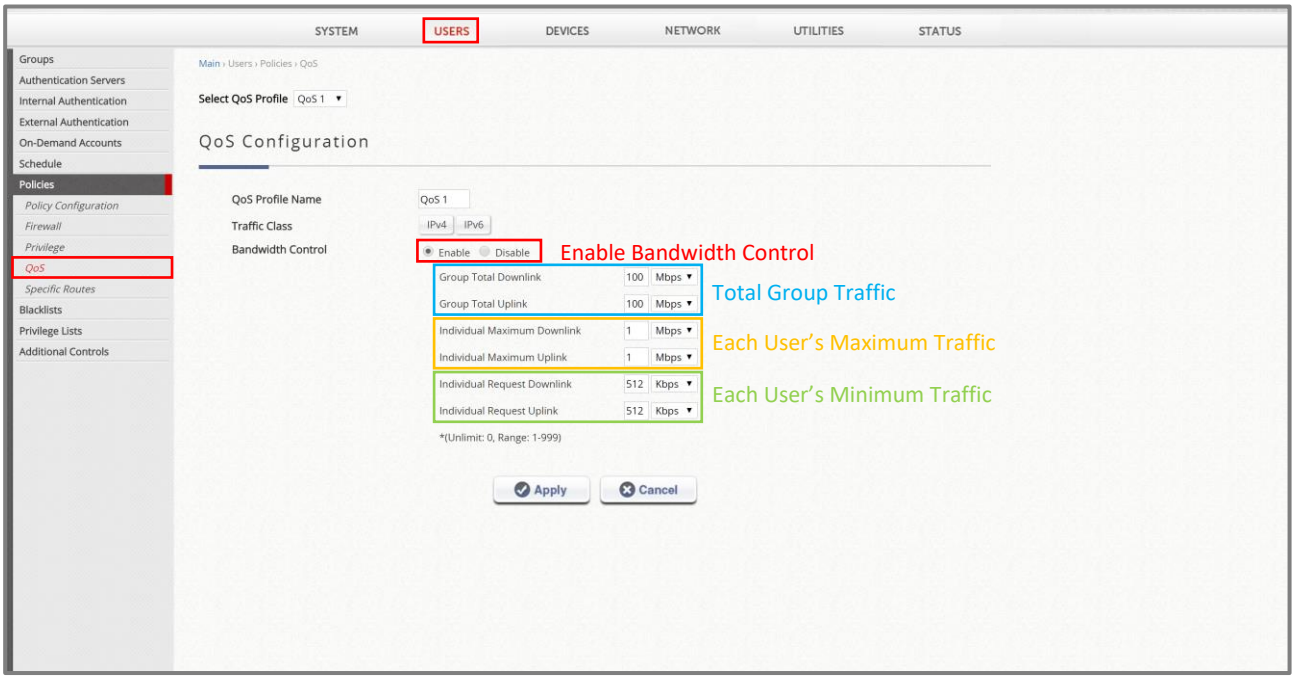
must be enabled. Click the hyperlink to access the WAN configuration page.



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

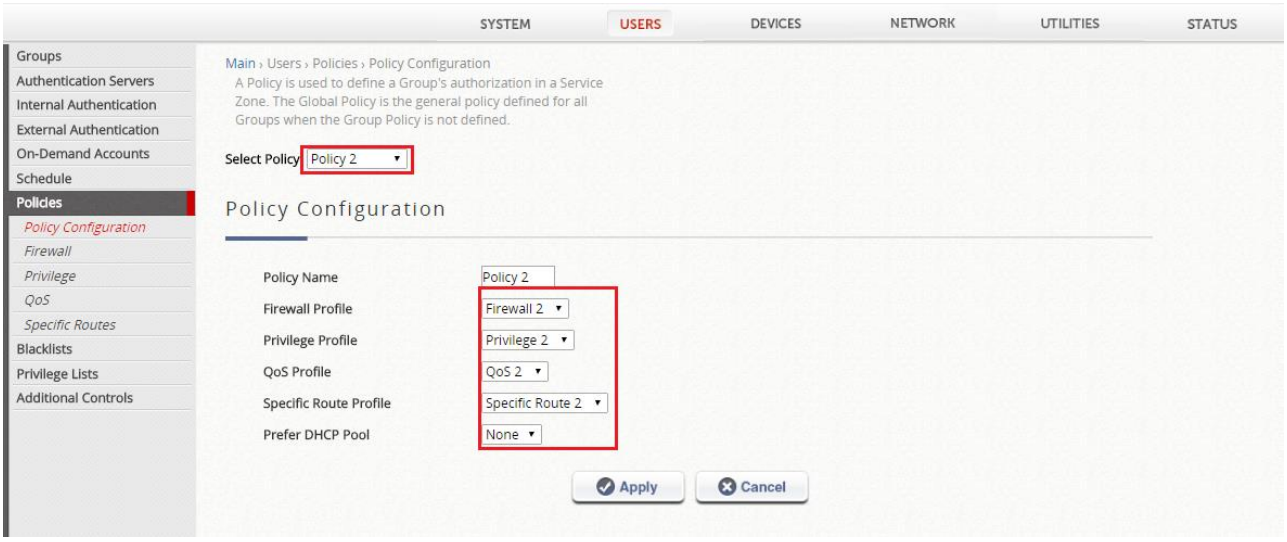


After the EWS has restarted, go to *Users > Policies > QoS* to configure the QoS 1 Profile as shown below.



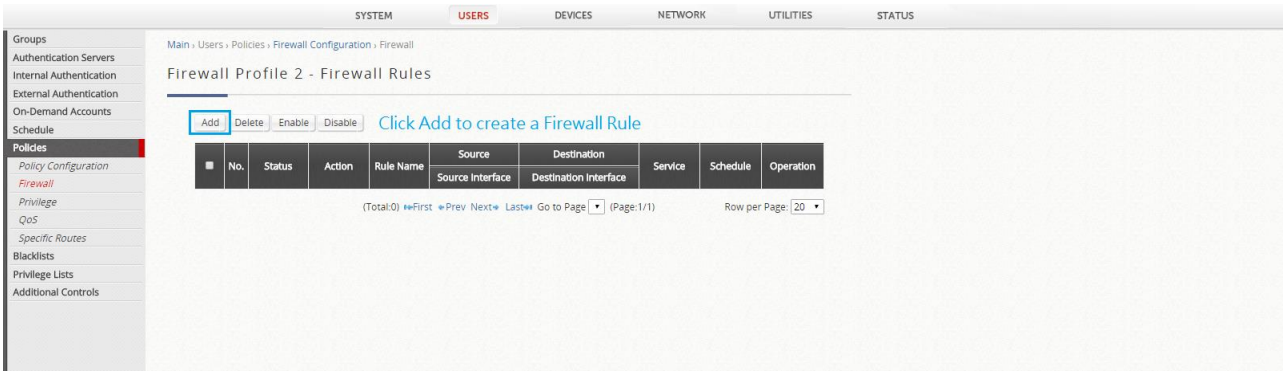
4.10.2 Staff Users → Policy 2 profile configuration

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

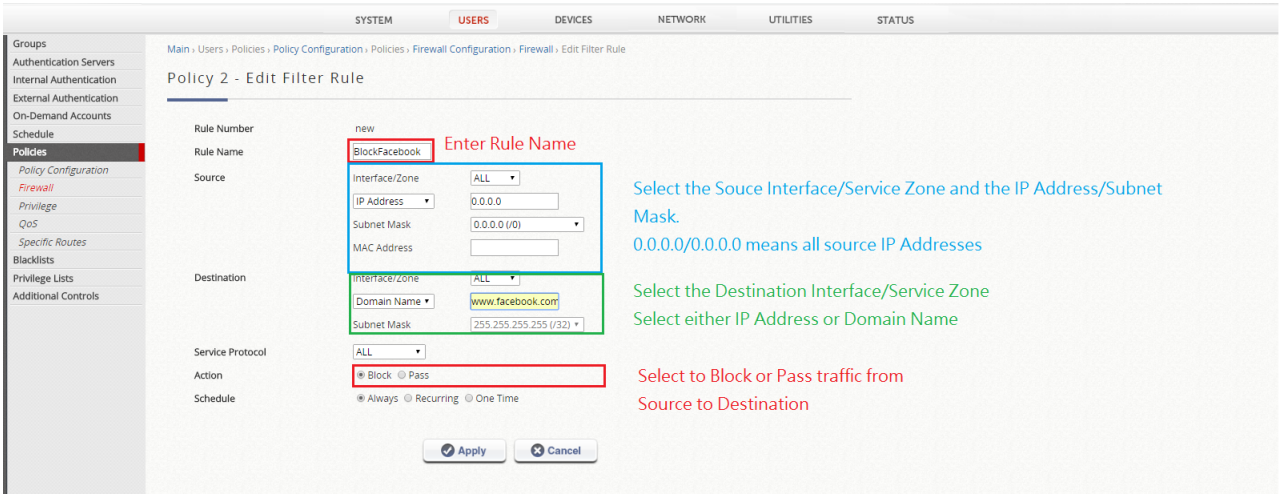


Go to *Users > Firewall* and select Firewall 2 to configure *User Firewall Rules* to block a user's access to an IP Address or Web Domain.

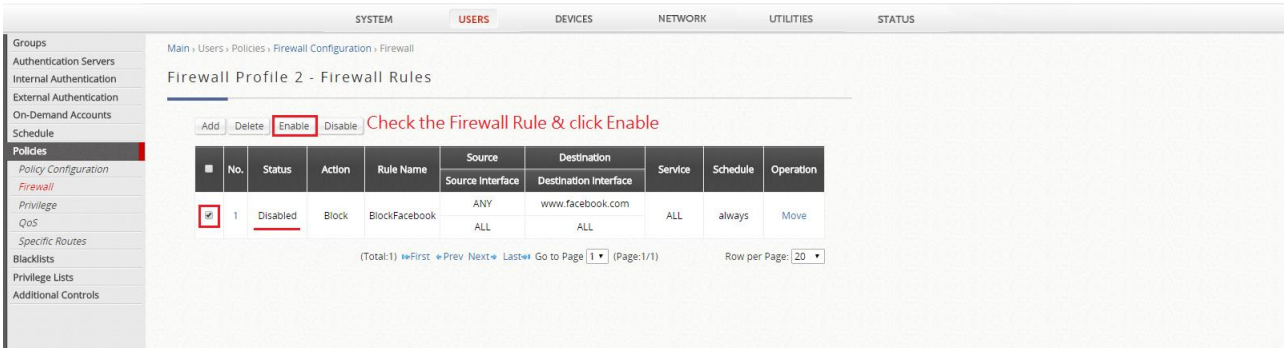
Click the *Add* button to create a new *Firewall Rule*.



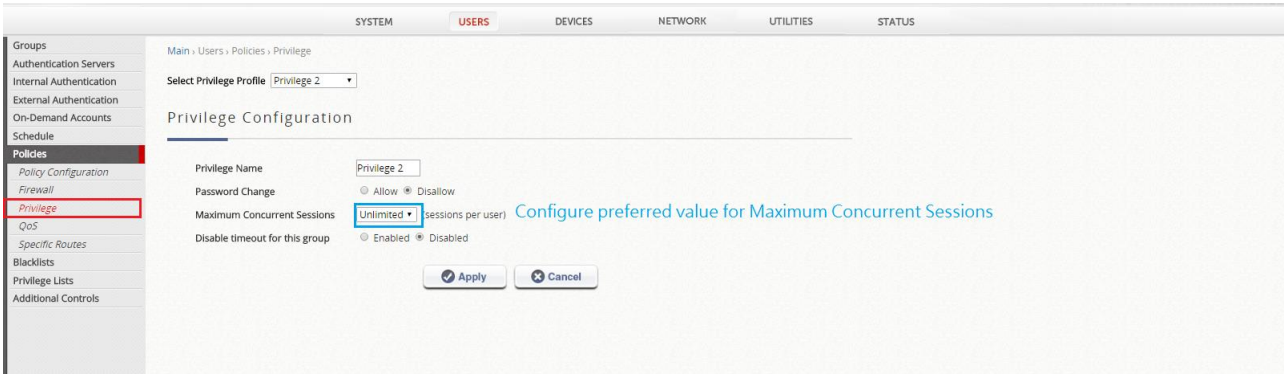
Configure a new Firewall Rule (BlockFacebook) with preferred *Source and Destination*.



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



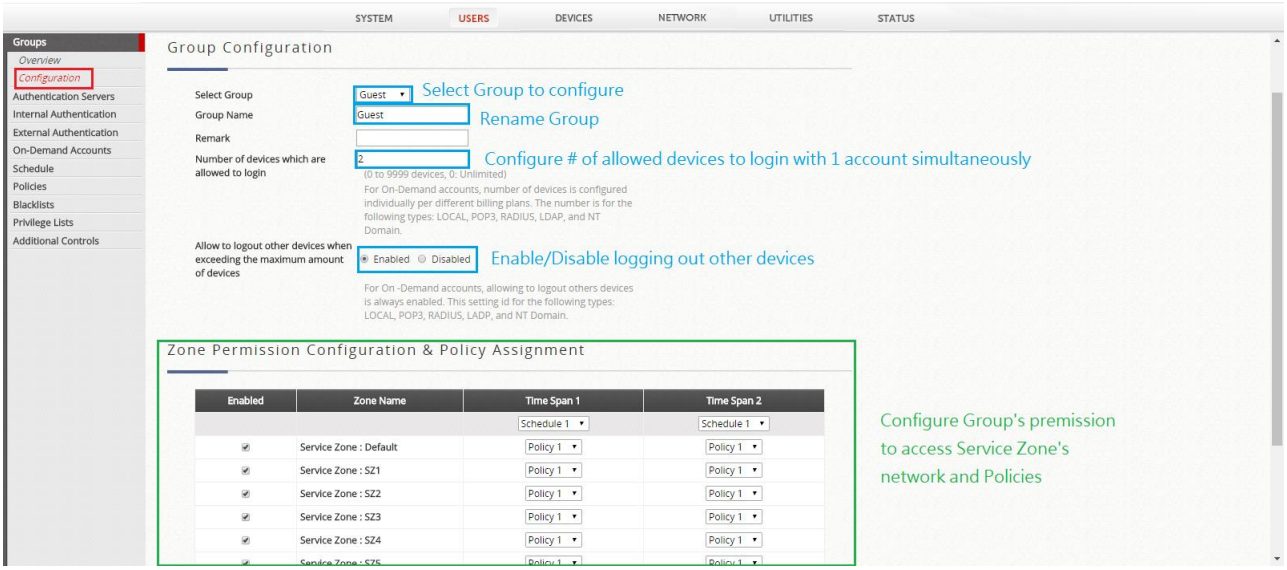
Go to *Users > Policies > Privilege 2* to configure the *Maximum Concurrent Sessions* of each user under this Policy. (Default = 500)



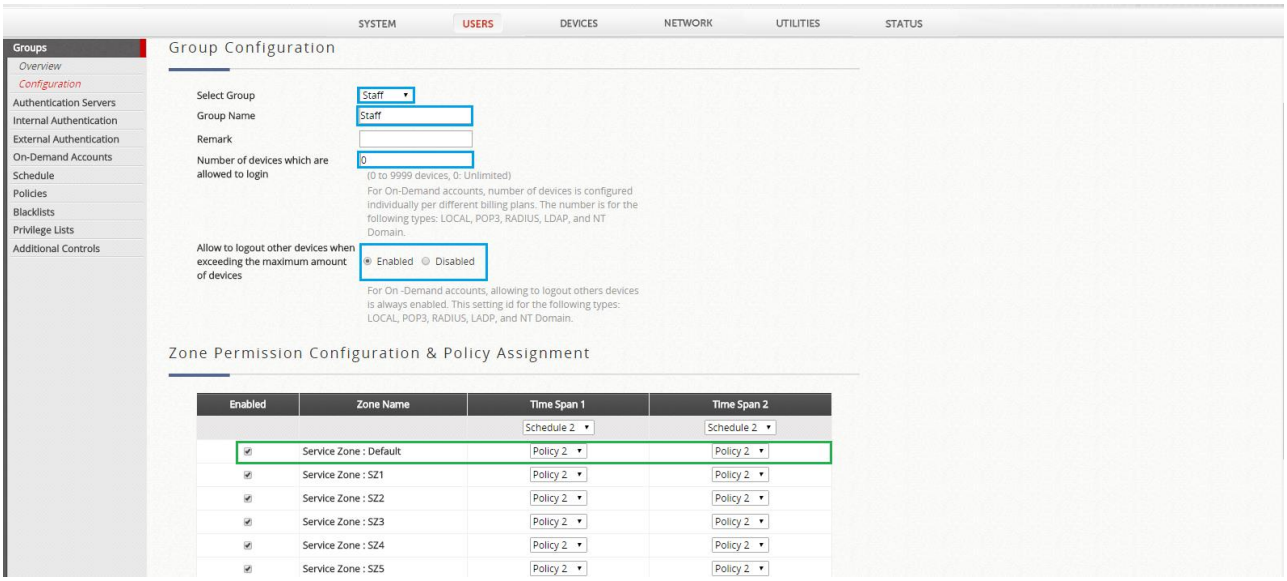
4.11 Users – User Groups Configuration

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.

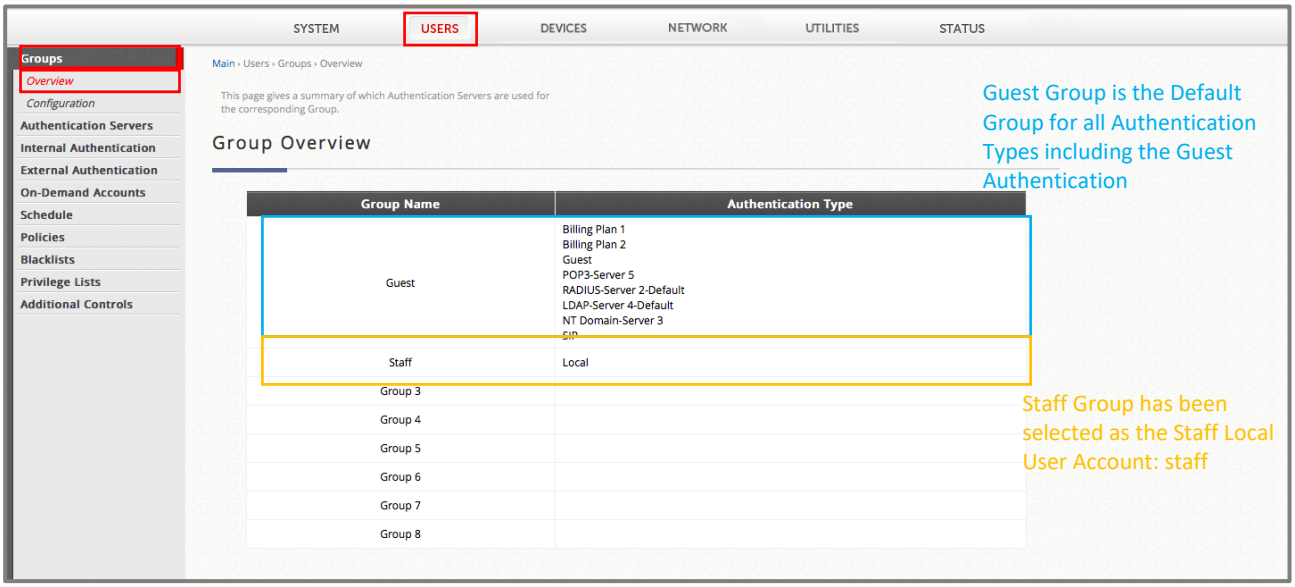
Here we rename the Group Name of Group1 as Guest, with 2 for Number of devices which are allowed to login, and assign Policy 1 for Default Service Zone.



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.



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

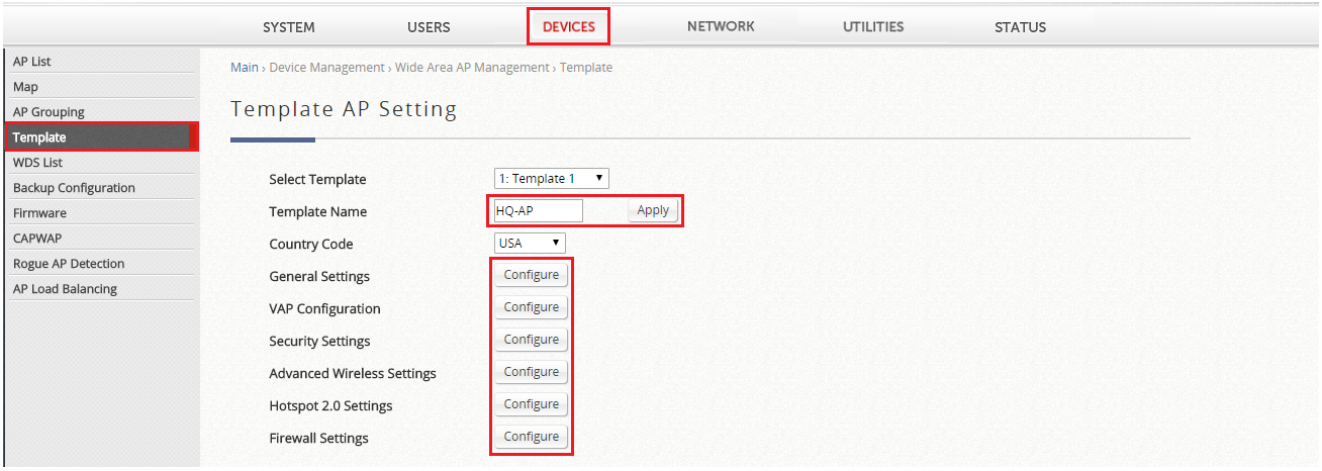

SYSTEM
USERS
DEVICES
NETWORK
UTILITIES
STATUS
Groups
Overview
Configuration
Authentication Servers
Internal Authentication
External Authentication
On-Demand Accounts
Schedule
Policies
Blacklists
Privilege Lists
Additional Controls
Main › Users › Groups › Overview
This page gives a summary of which Authentication 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.

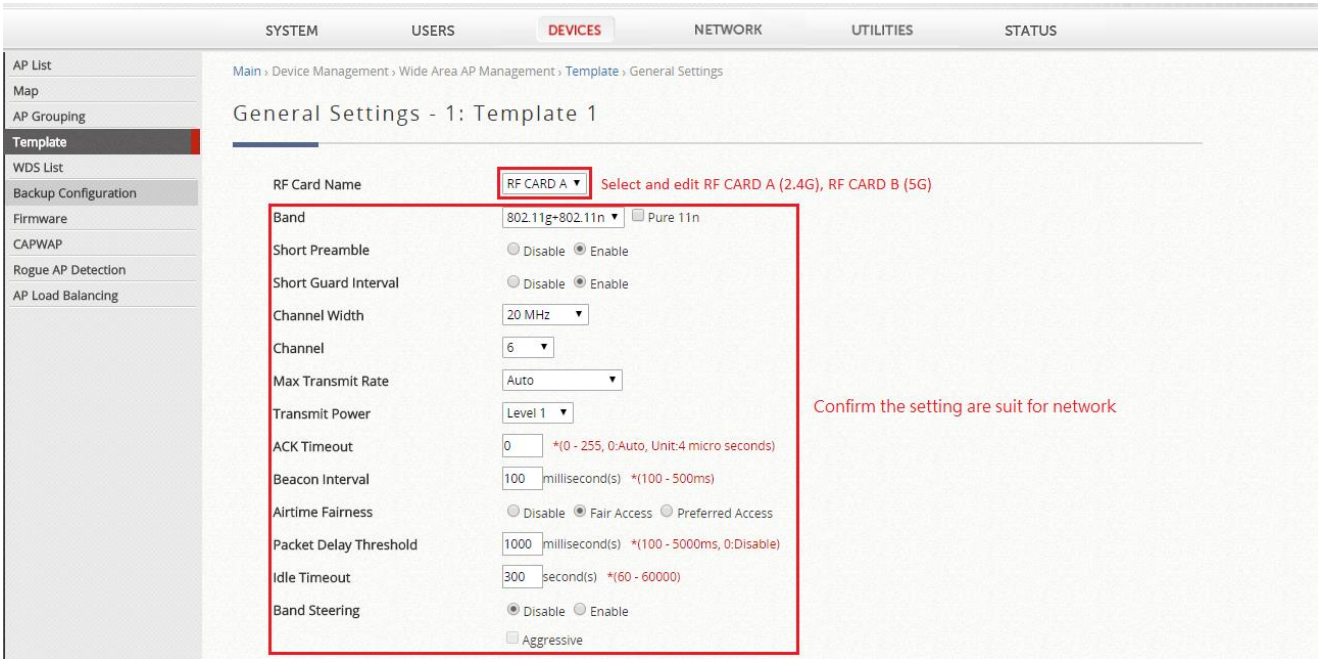
4.12.1 Edit WAPM Templates

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

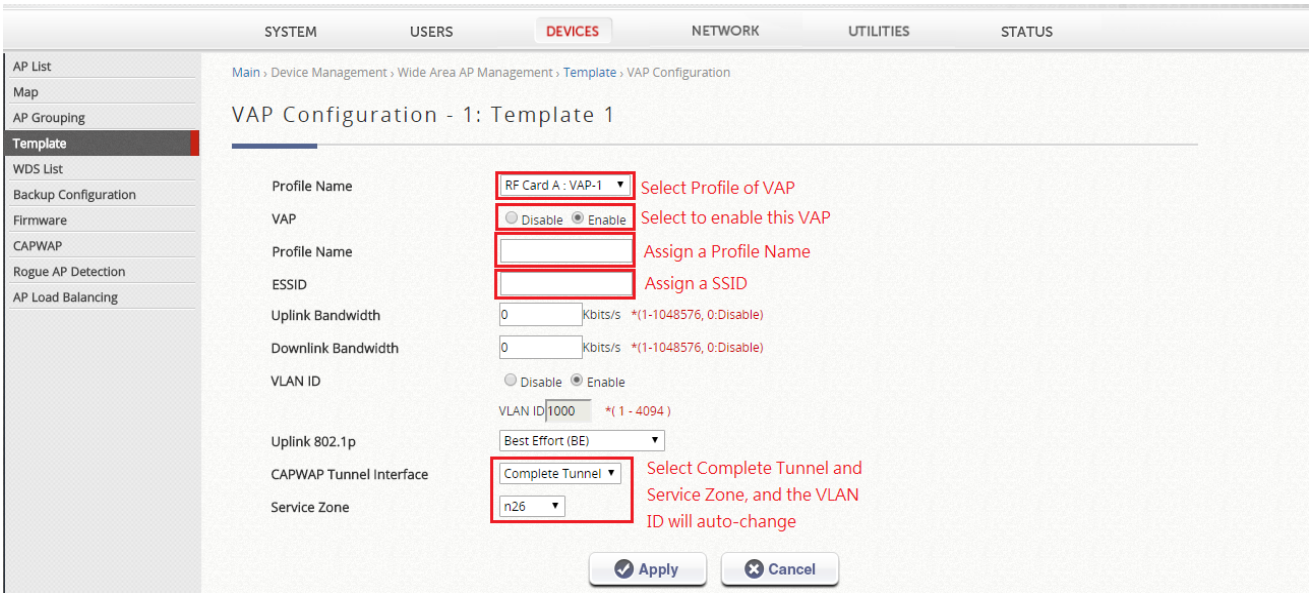


General Settings

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

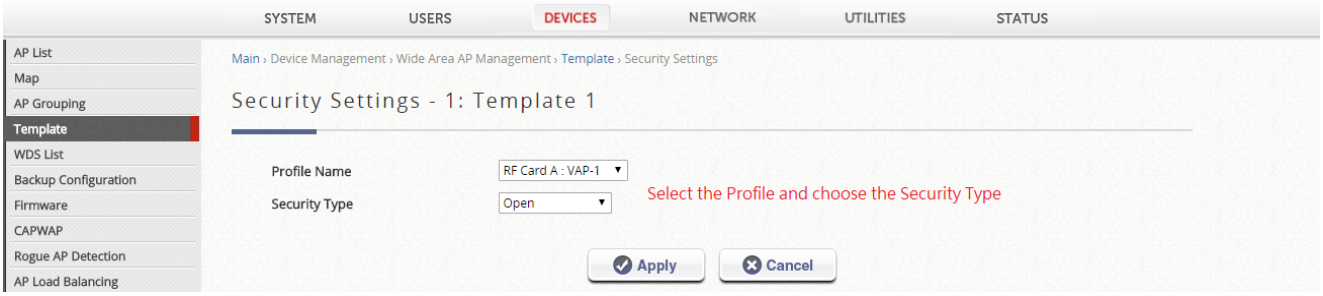


VAP Configuration



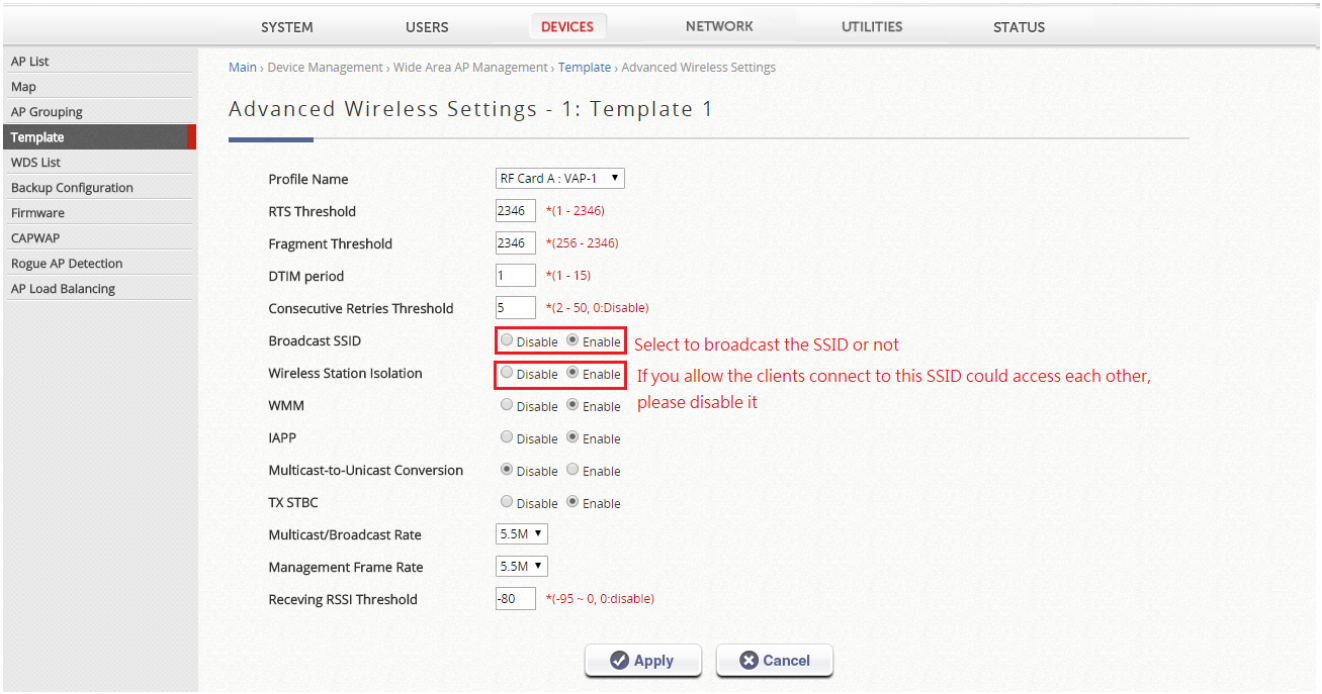
We can use same procedure to configure other VAP.

Security Configuration



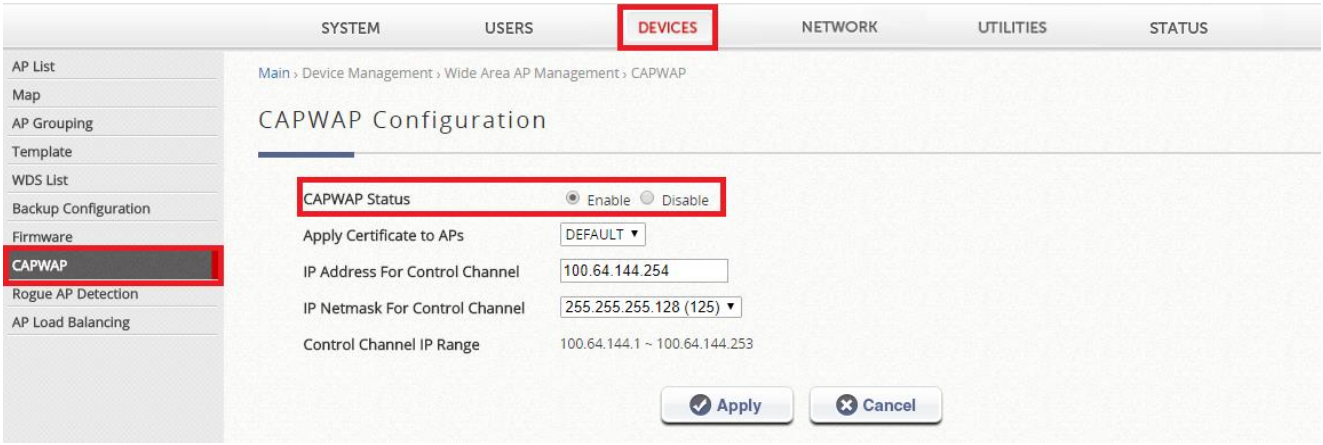
If you would like to use 802.1x authentication, please select WPA-Enterprise.

Advanced Wireless Configuration

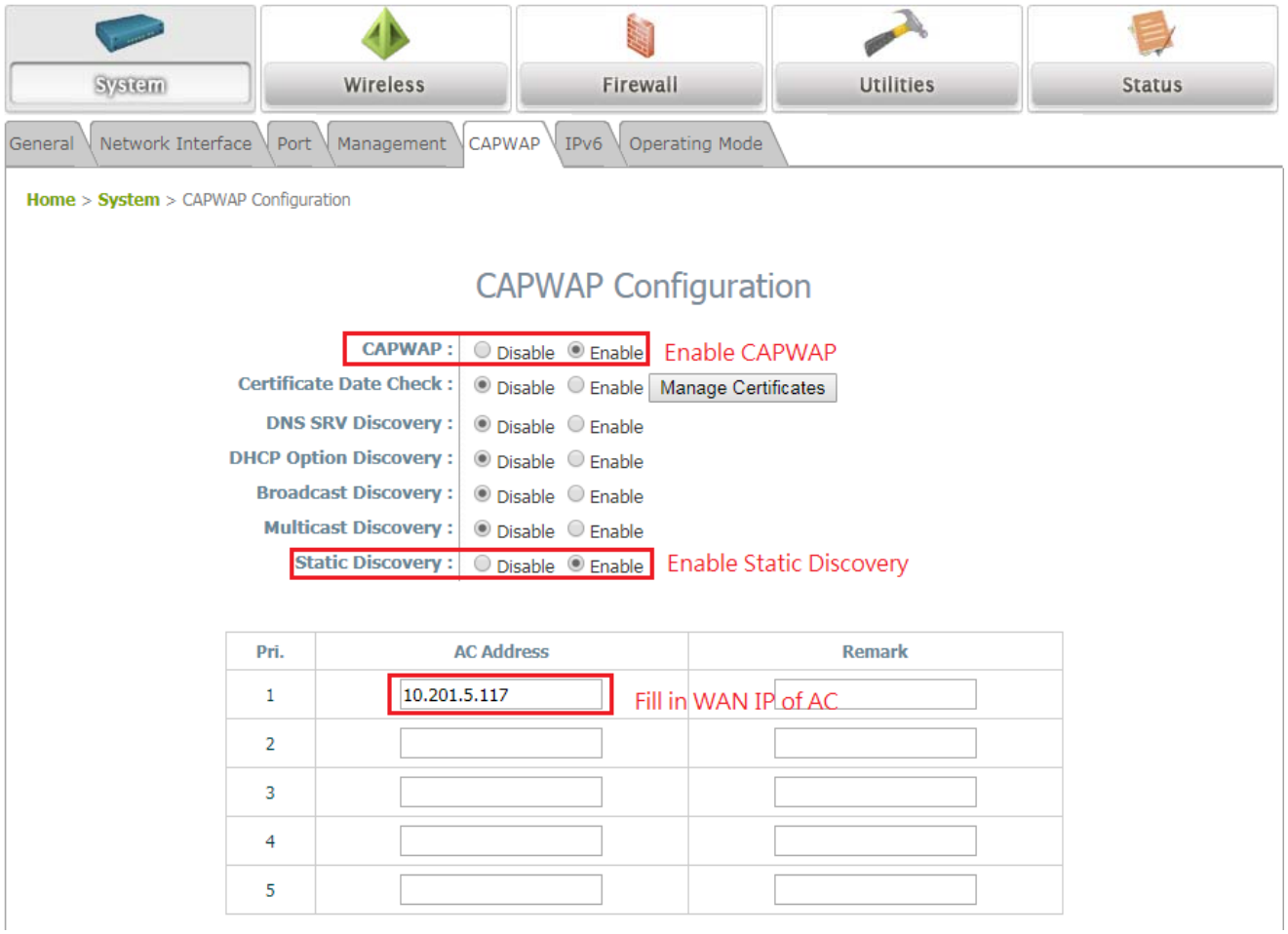


4.12.2 Establish CAPWAP Tunnel from AP to EWS

Enable CAPWAP in EWS
Go to *Devices > WAPM > CAPWAP*



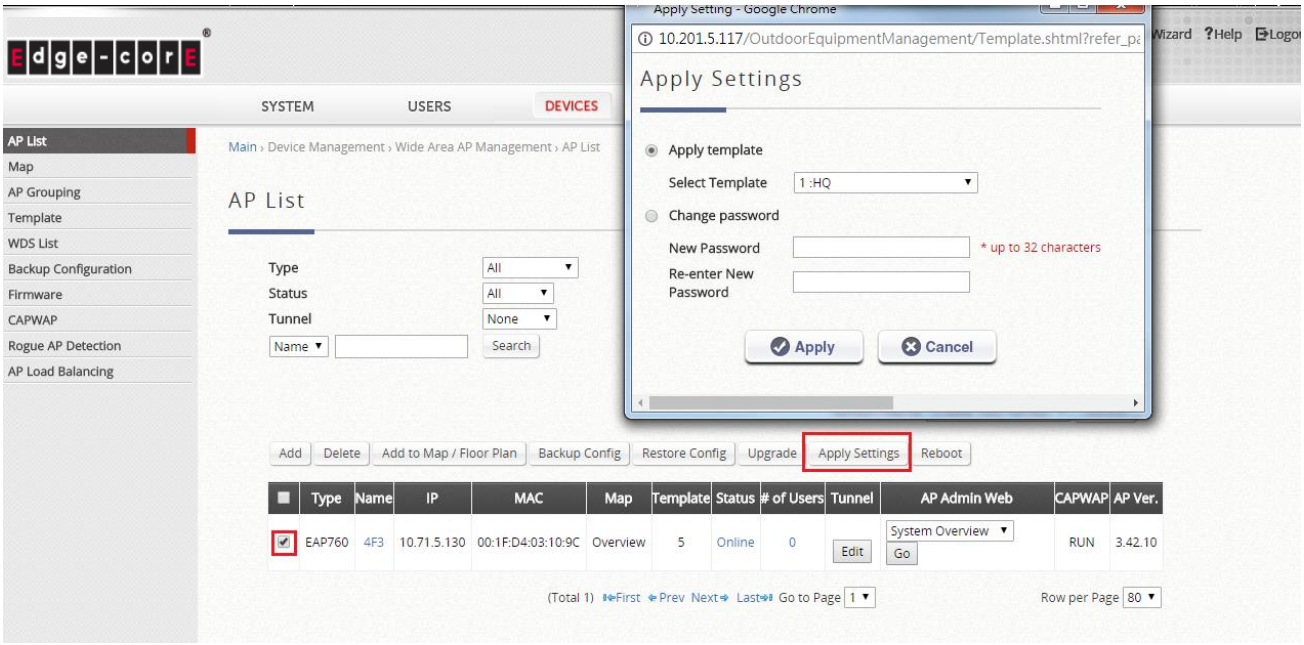
Go to *AP > System › CAPWAP*, and edit CAPWAP Configuration then apply and reboot. Please make sure AP's uplink could reach AC, otherwise the CAPWAP tunnel cannot build.



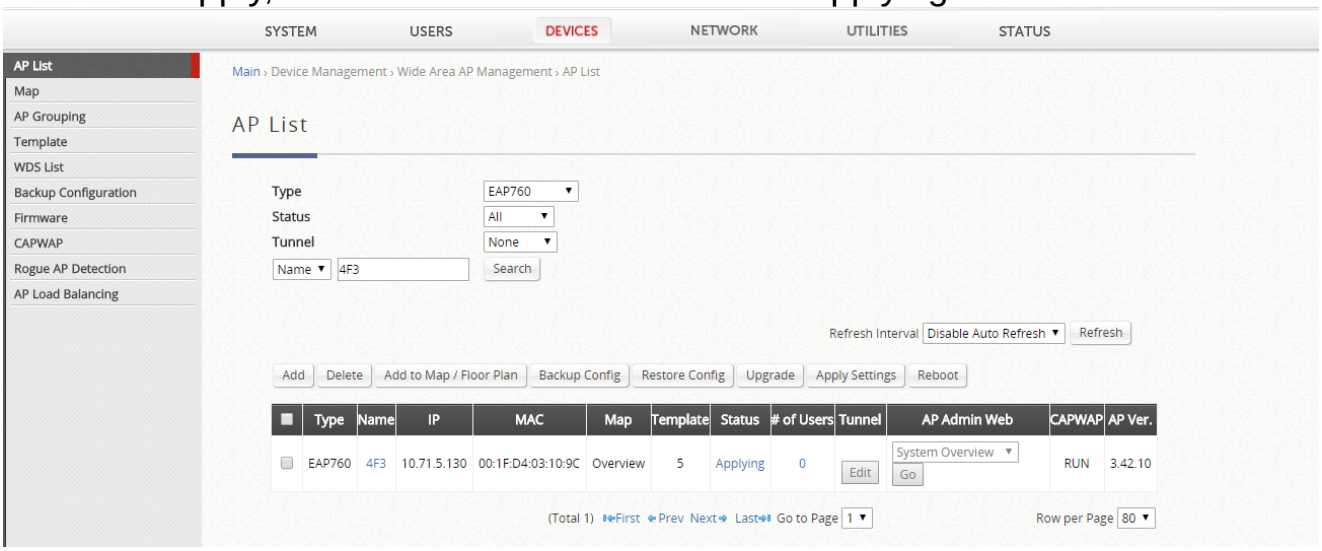
After Reboot, the AP would auto connect to EWS, the overview page could confirm the status of CAPWAP. Also, could monitor this at AP List from EWS.

4.12.3 Applying the template

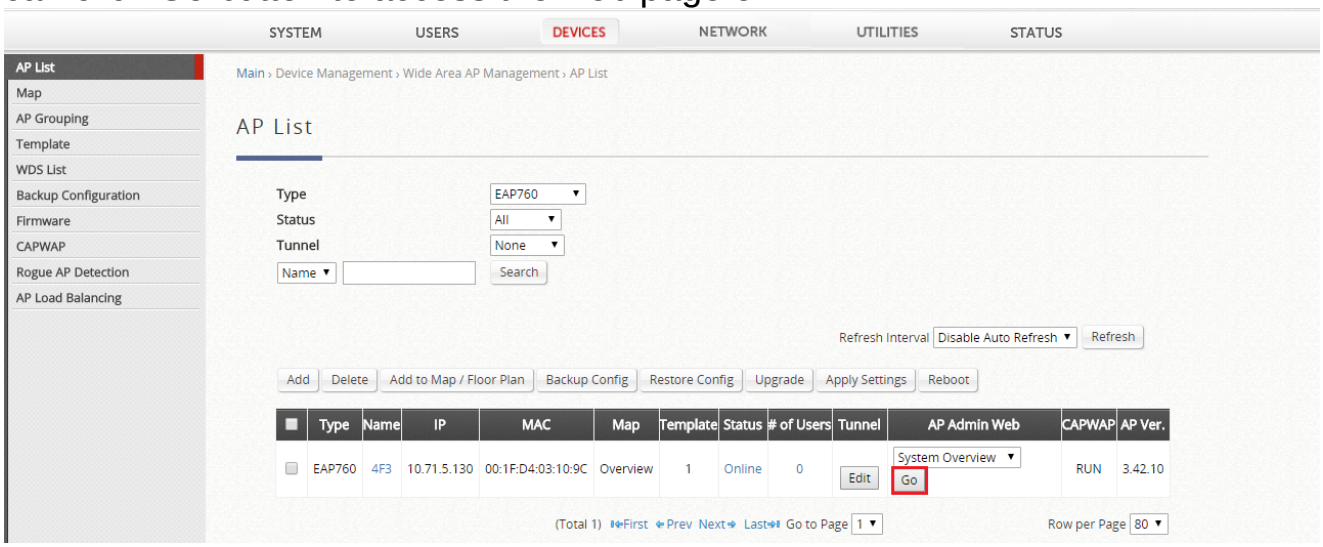
Select the APs and click Applying template to configure multiple APs at the same time.

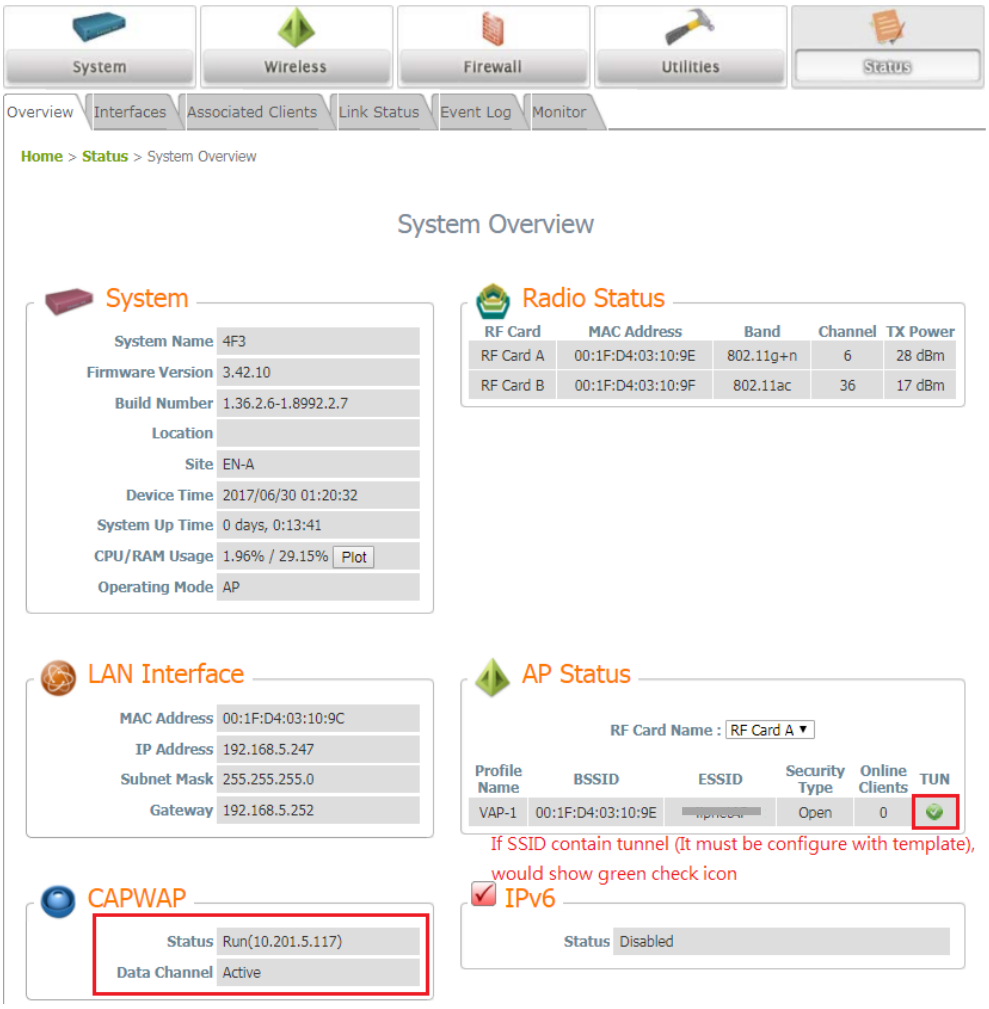


After click Apply, the status of AP would become Applying.



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



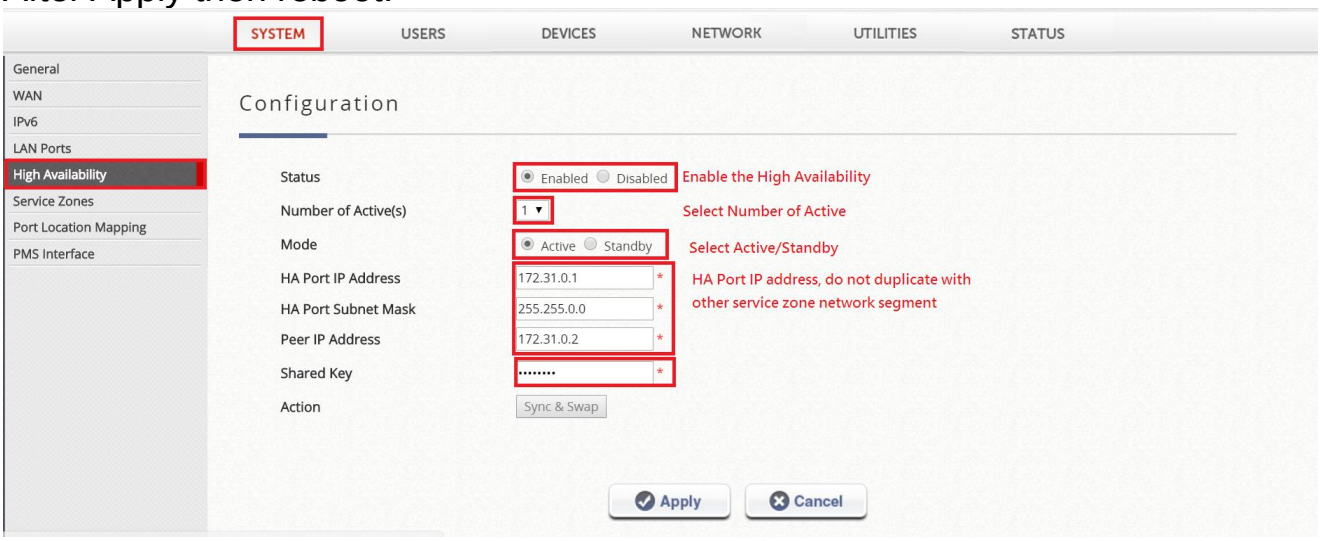


4.13 1+1 High Availability for Service Redundancy

4.13.1 Configure EWS#1 HA

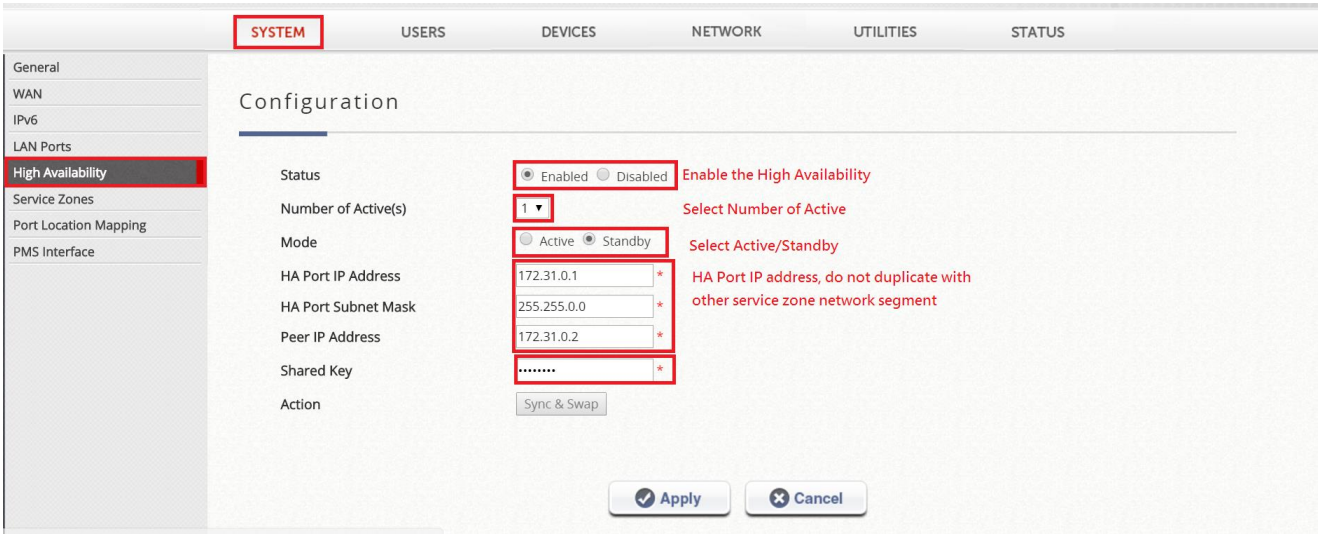
First, we need to check System time, go to *SYSTEM > General > System*, and use the main EWS as NTP server.

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



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

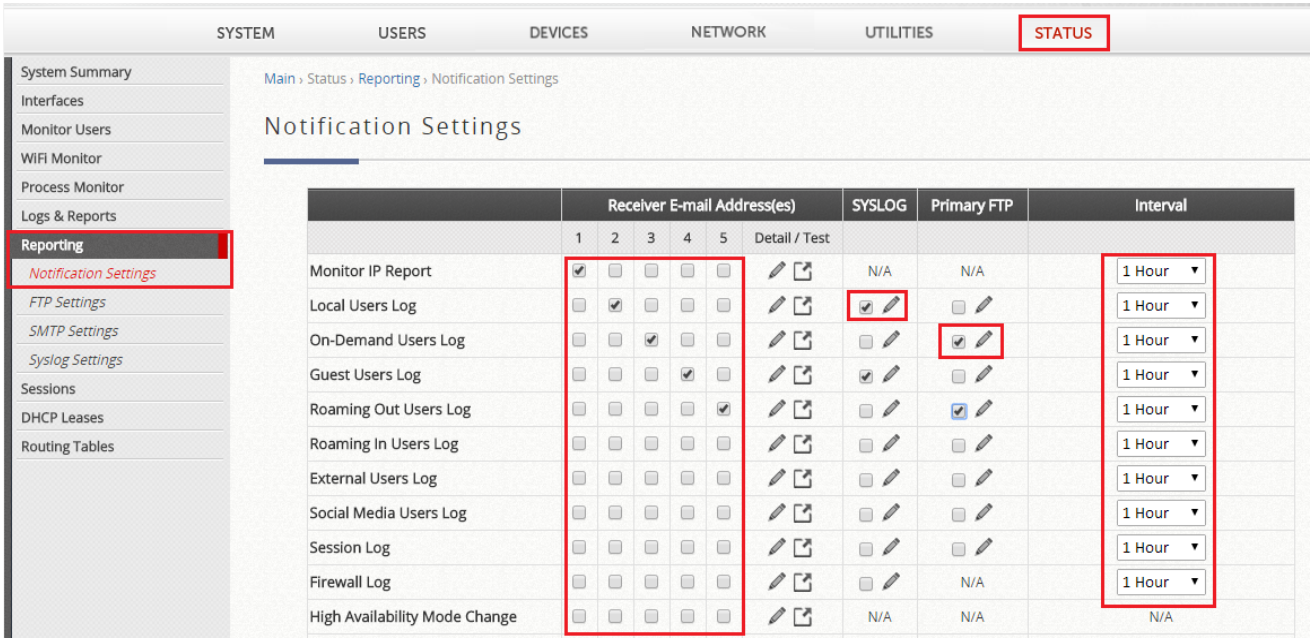
Click “Goto” to access the standby page.

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.

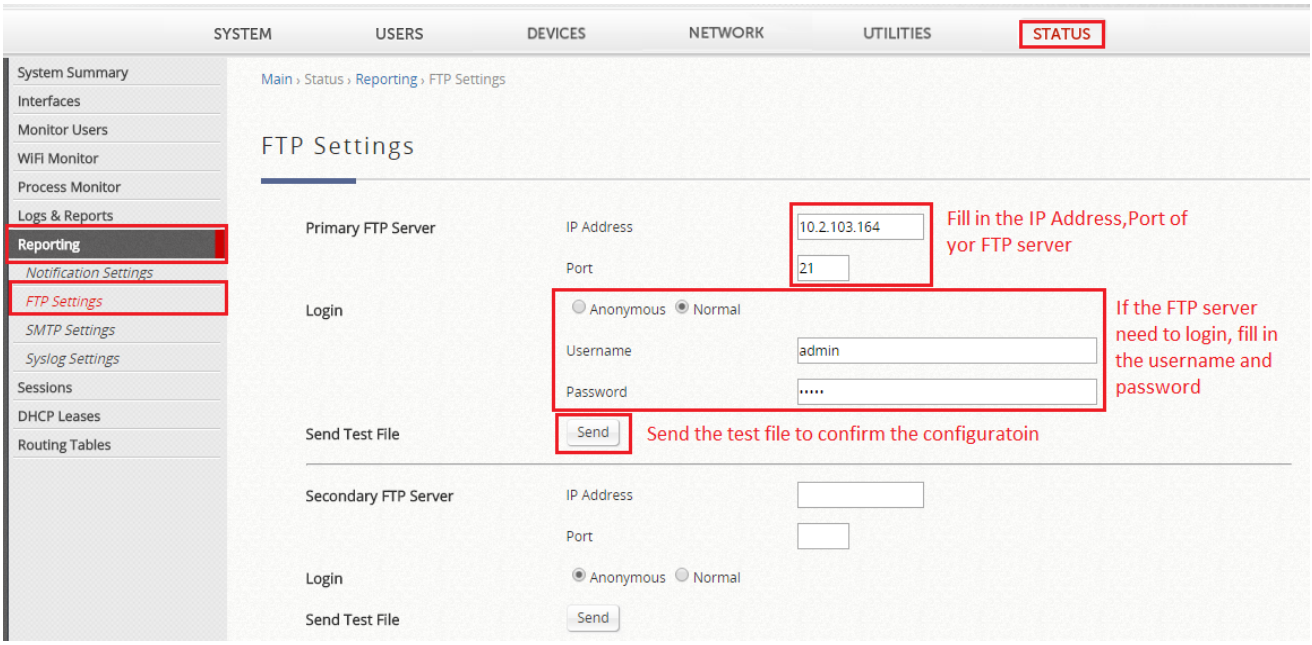
4.14.1 Notification

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



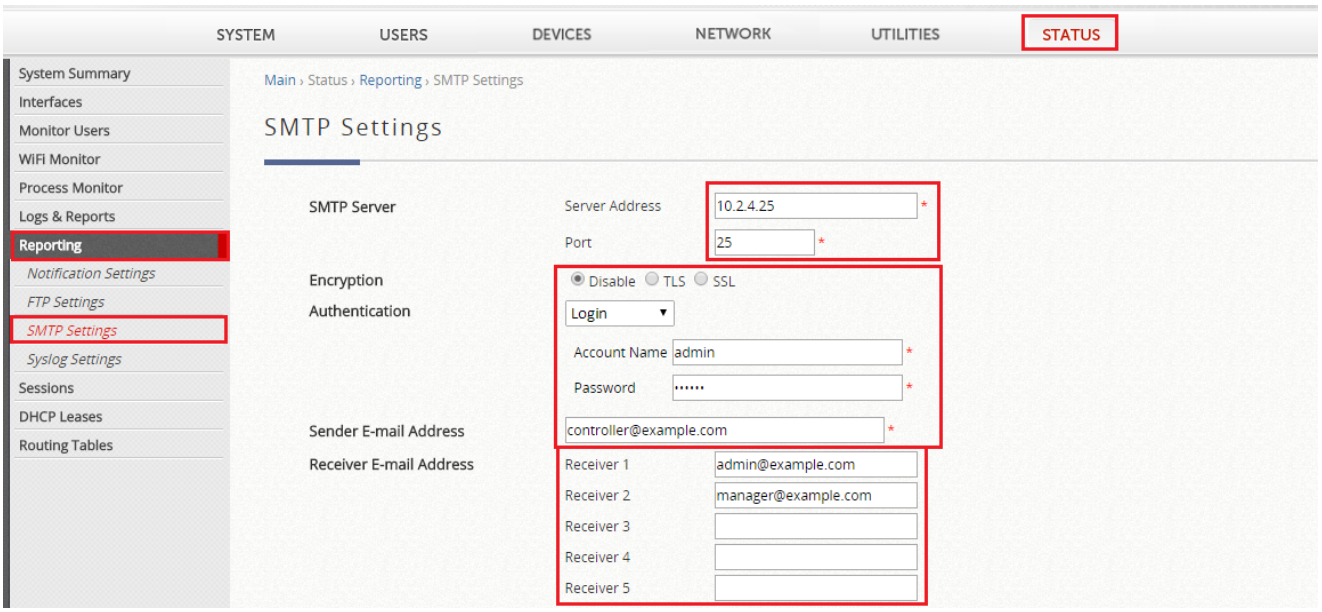
4.14.2 FTP Setting

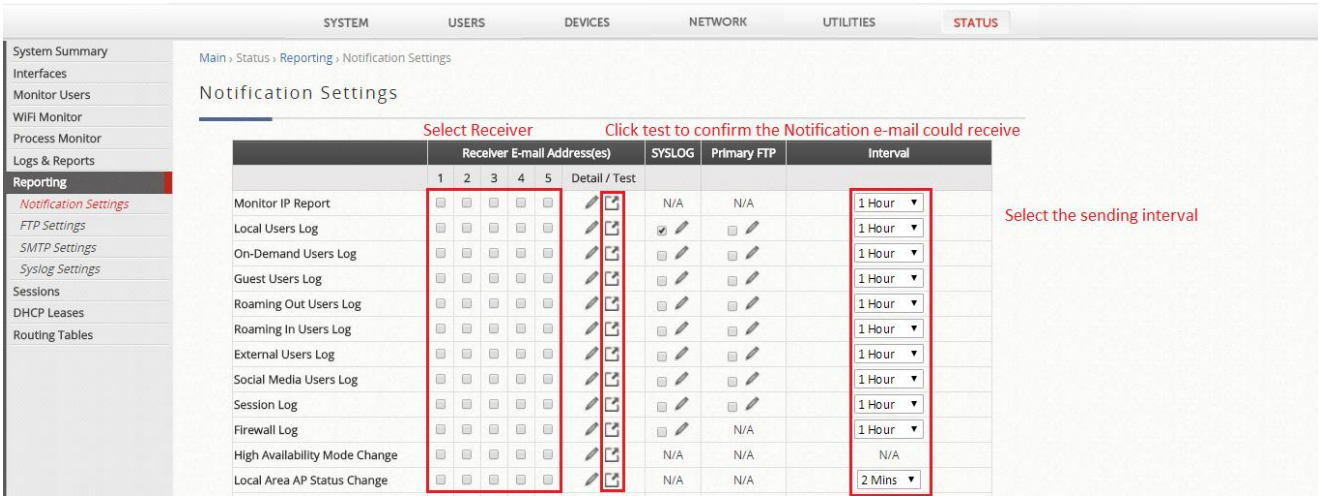
Go to *STATUS > Reporting > FTP Setting*, configure the FTP Settings. After configure, you can click test to confirm it.



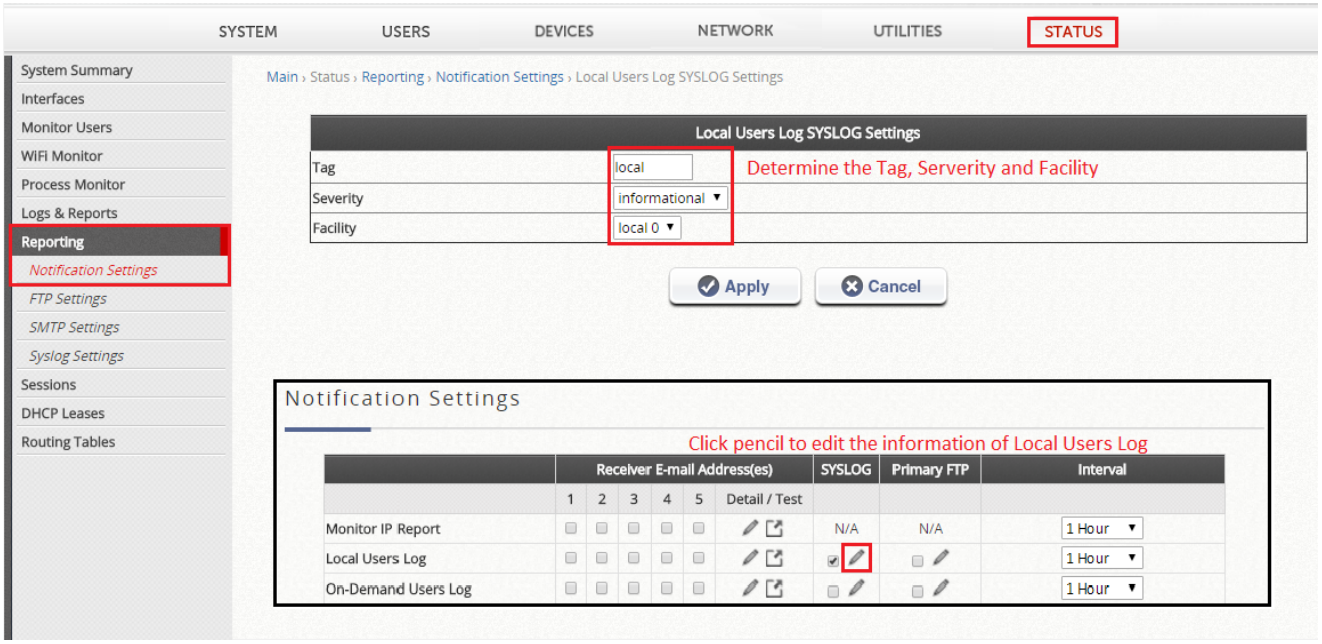
4.14.3 SMTP Setting

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





4.14.4 Syslog Setting


SYSTEM
USERS
DEVICES
NETWORK
UTILITIES
STATUS
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
local
Severity
informational
Facility
local 0
Determine the Tag, Serverity and Facility
Apply
Cancel
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
Detail / Test
Monitor IP Report
N/A
N/A
1 Hour
Local Users Log
1 Hour
On-Demand Users Log
1 Hour