Technical Guide

Basic Configurations

Released: 2018-08-02

Table of Contents

1 Introduction

This guide will provide the basic configurations to quickly set up your own managed network. The guide highlights the minimum steps required for a wired or wireless network in each of the EWS controller's features; Service Zones, Authentication, Page Customization and User Policy Management and AP Management.

An introduction to Edgecore's Wide Area AP Management (WAPM) will include a comprehensive guideline to manage a remote Edgecore Access Point (AP) by establishing a CAPWAP Tunnel between the EWS and AP.

1.1 Pre-condition

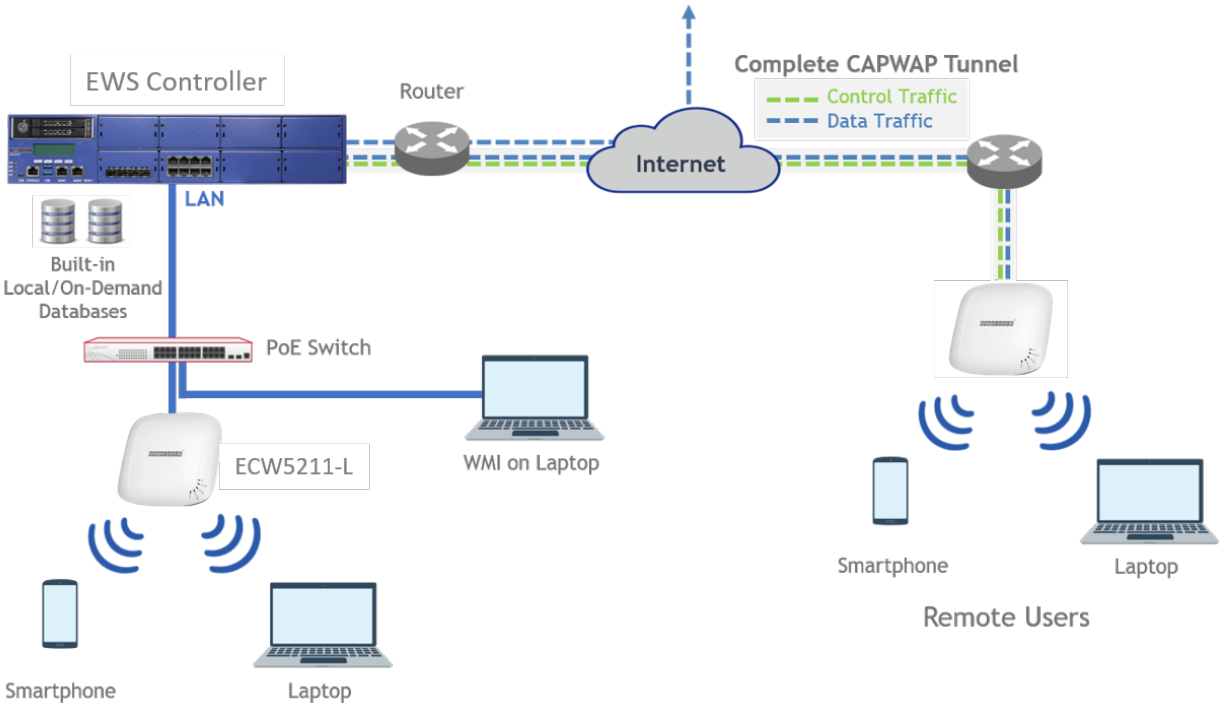
a. Edgecore EWS controller is installed at the central site with uplink connected to WAN.

b. Edgecore AP is deployed locally under the layer 2 network or through the Layer 3 network at a remote site with internet connection at the uplink interface.

c. Confirm UDP ports 5246 & 5247 are open for connections between the EWS and AP.

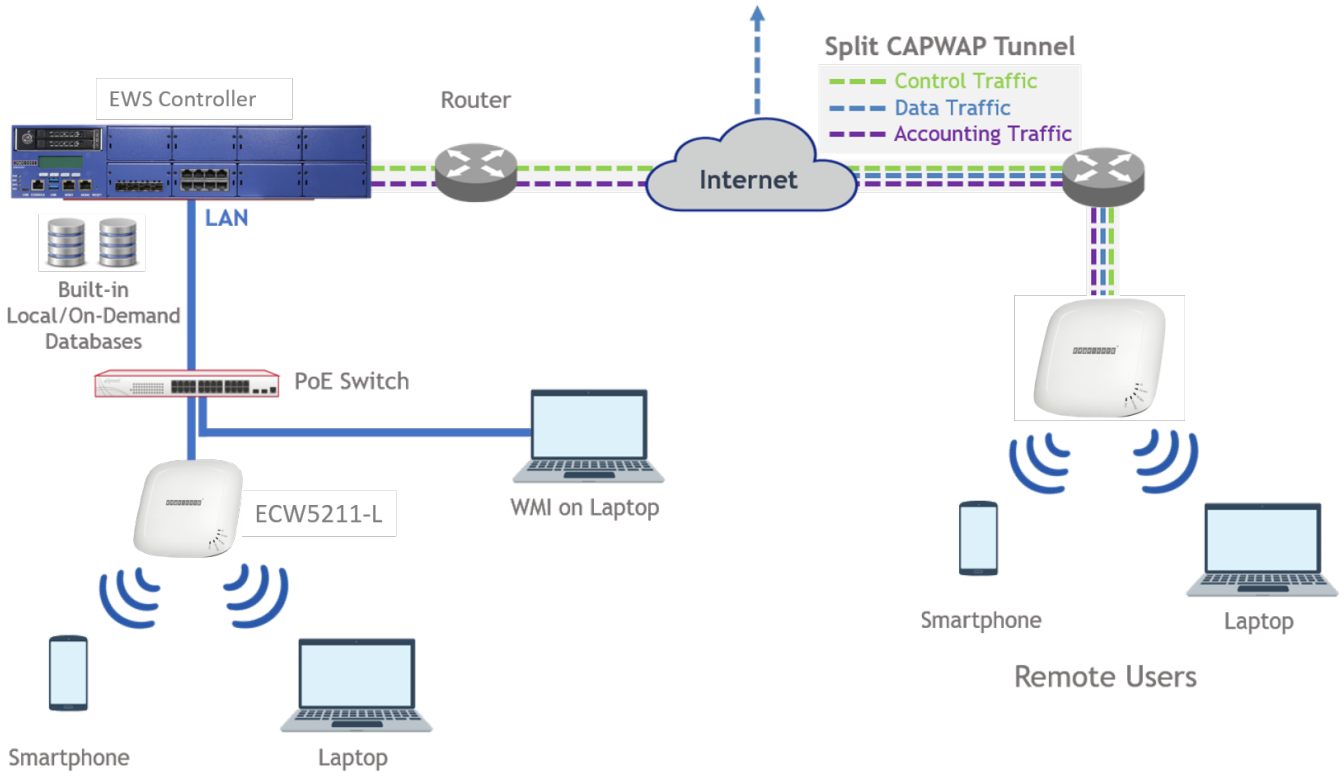
※ *EWS's WAN interface and AP's uplink interface can be connected to the same switch to simulate a scenario like deploying the AP at a remote location over the layer 3 network.*

1.2 Complete Tunnel Network Topology



※ *Remote users connected to an SSID with Complete Tunnel can be authenticated by the EWS and enforced by the EWS's user policies. All data are routed back to the EWS Controller.*

1.3 Split Tunnel Network Topology



※ *Remote users connected to an SSID with Split Tunnel can be authenticated by the EWS Controller and user data will be routed locally.*

2 Configuration Flow Guideline

Below is a one-page step by step guideline for first time users in configuring the EWS.

EWS Configuration Flow			
Steps	**User Interface**	**Configuration Options**	**Description**
1. System General WAN LAN Ports	General WAN Configuration LAN Ports	System Name, Time Static, Dynamic, PPPoE, PPTP Bandwidth Limitation Management IP List	Configure system settings and WAN settings for internet connection Choose LAN Port mode. Configure allowed IPs to access the WMI
2. Utilities Administrator Accounts	Admin Editing Password Safety	Administrator Email Security Answer SMTP Server	Configure administrator's account to enable password recovery.
3.1 System Service Zone (SZ)	Service Zone Settings	AP IP Management NAT/Router, IP Address, DHCP Authentication Options	Configure up to 8 Service Zones for managing separate networks.
3.2 System Service Zone → Page Customization	Service Zone Configuration	Login Page Customization Message Page Customization Default Template Upload External	Personalize Captive Portal's appearance using built-in customization methods.
4.1 Users Internal Auth. → Local	Local User List	Username Password Group	Create long-term accounts. Ex. Staff, Employees.
4.2.1 Users Internal Auth. → On-Demand	On-Demand Billing Plans	Plan Type Quota (Time/Volume) Price Group	Configure short-term account plans. Ex. Hotel Guests, Students. 4 Plan Types: Usage Time, Volume, Hotel Cut-off Time, Duration Time
4.2.2 Users On-Demand Accounts → Account Creation	On-Demand Account Creation	Create Single Create Batch	Create On-Demand accounts through a central Web Management Interface or a Edgecore WTG Hotspot Ticketing System
5. Users Policies → Policy Configuration	Policy Configuration	Policy Name Firewall Profile Privilege Profile QoS Profile Specific Route Profile	Configure User Group's enforced policy profiles. Block Websites, Limit User Bandwidth & Gateway Routing.
6. Users Groups	Group Configuration	User Roles User Authentication Database Groups → Policies	Plan & categorize the types of users Make 1-to-1 mapping to User Groups and Policies.
7. Devices Local Area AP Management (L2) or Wide Area AP Management (L2/L3) → Template → AP List	LAPM/ WAPM Template AP List Add a single AP Discover Multiple APs CAPWAP	WAPM Template Template Settings General Settings VAP Configurations Security Settings CAPWAP: Complete/Split Tunnel	LAPM for L2 Networks WAPM for L2/L3 Networks Configure generic Templates Monitor & apply AP settings through a centralized interface. Configure CAPWAP for Remote AP/User Management
8. Client Login User Flow Online Users User Events On-Demand Accounts List	Online Users List User Events On-Demand Accounts List	Summary/Detail view To-From Time Periods Authentication Type Remaining Quota	Monitor online users View recorded user events log

3 Configuration Steps

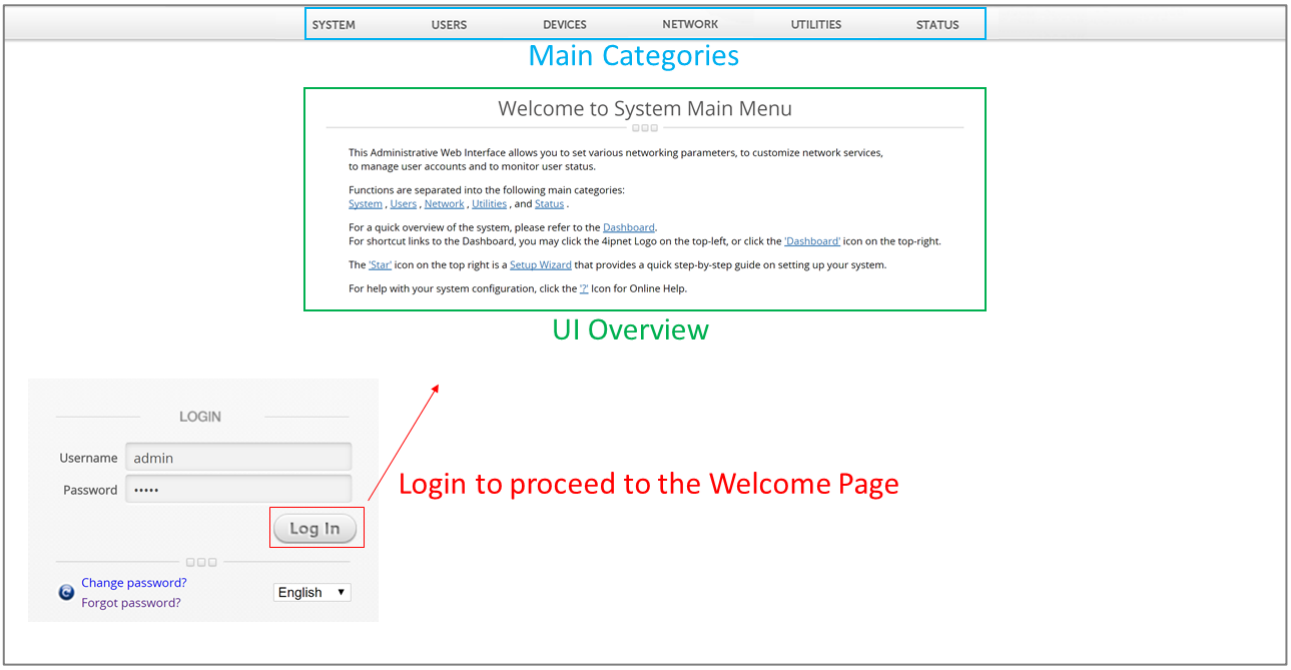
3.0 System - Initial Login

a. Connect your PC to the EWS's LAN port.

b. Access into EWS's Web Management Interface (WMI) by entering 192.168.1.254 in your Web Browser.

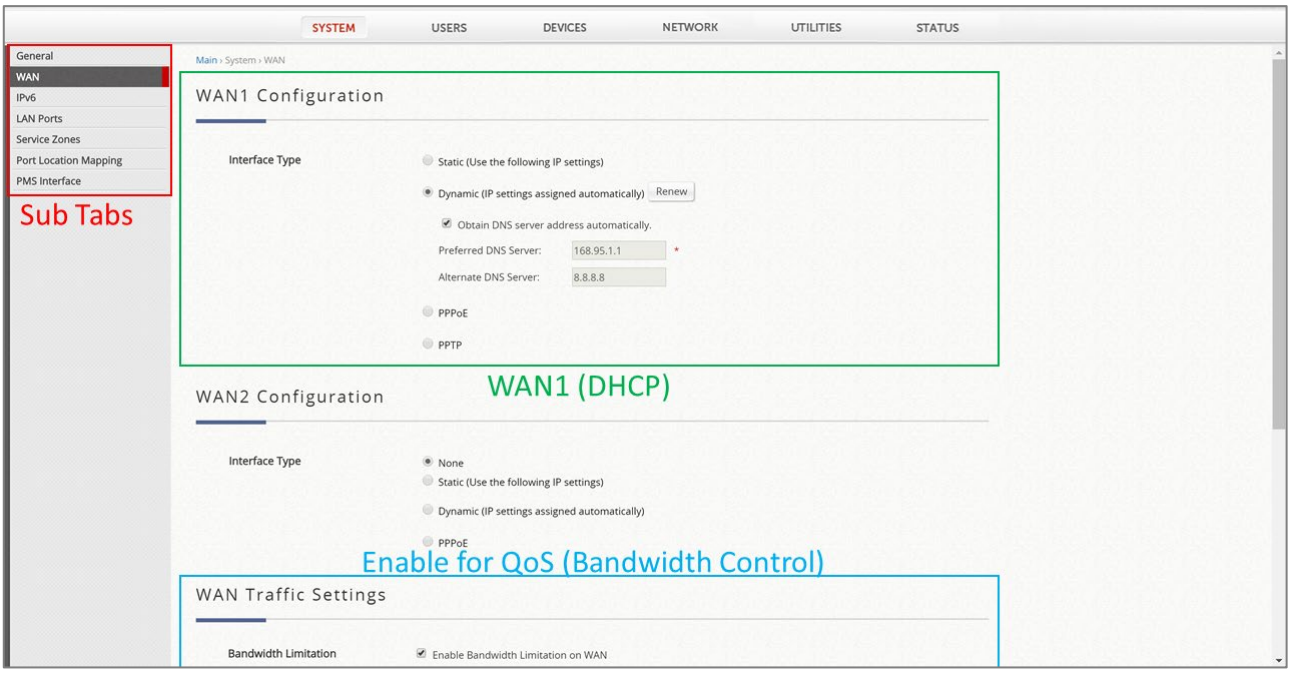
c. Login to the EWS using the Default Username/Password: admin/admin.

※ *Note: First time logging into the EWS will require changing the password.*

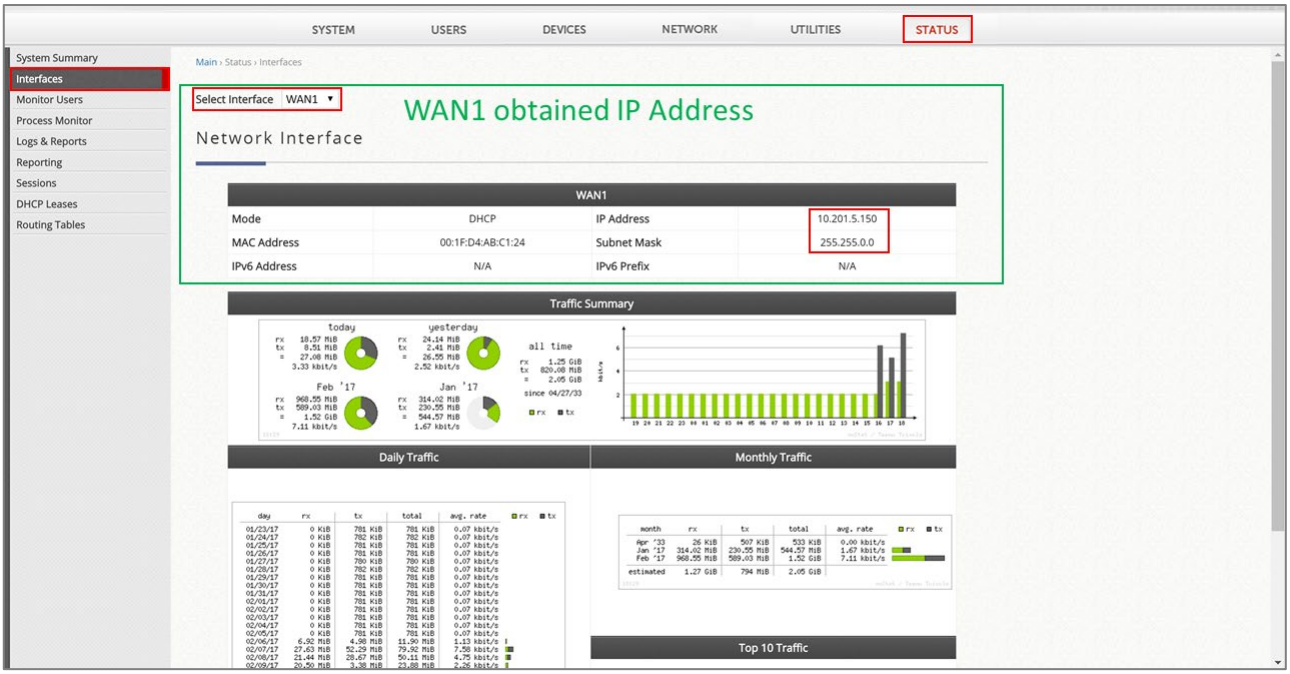


3.1 System - WAN & LAN Interface Configuration

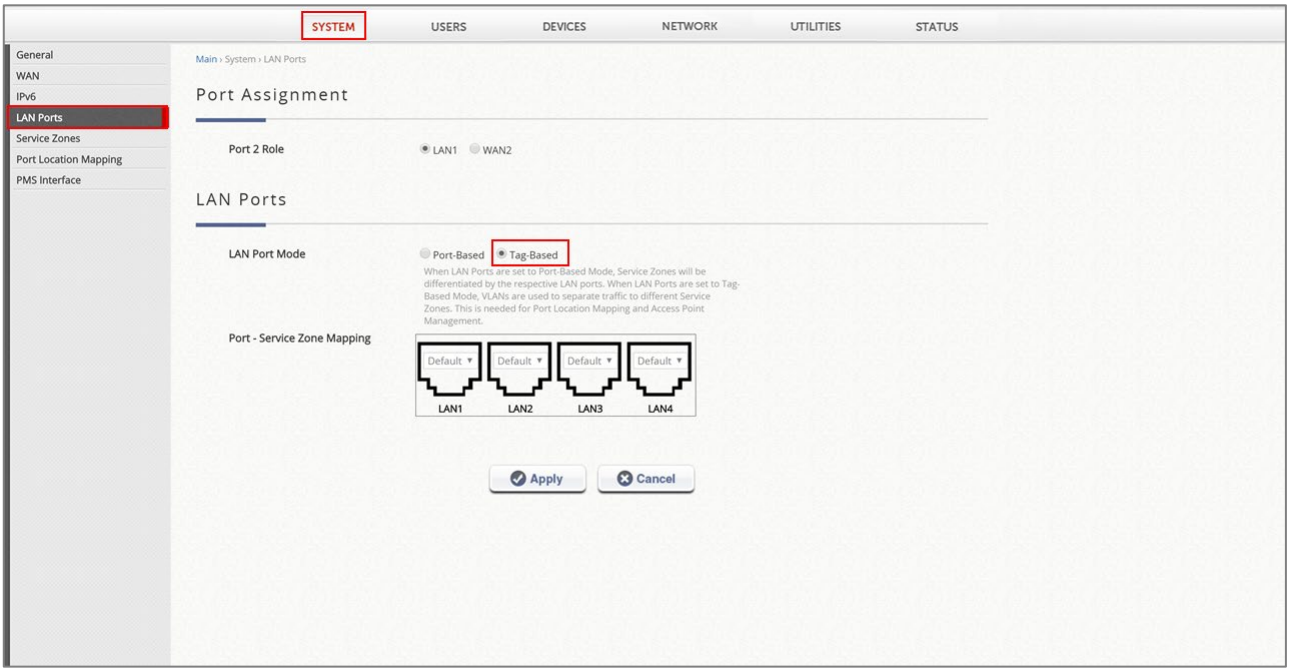
a. Go to System → WAN to configure the WAN1 Interface Type as "Dynamic".



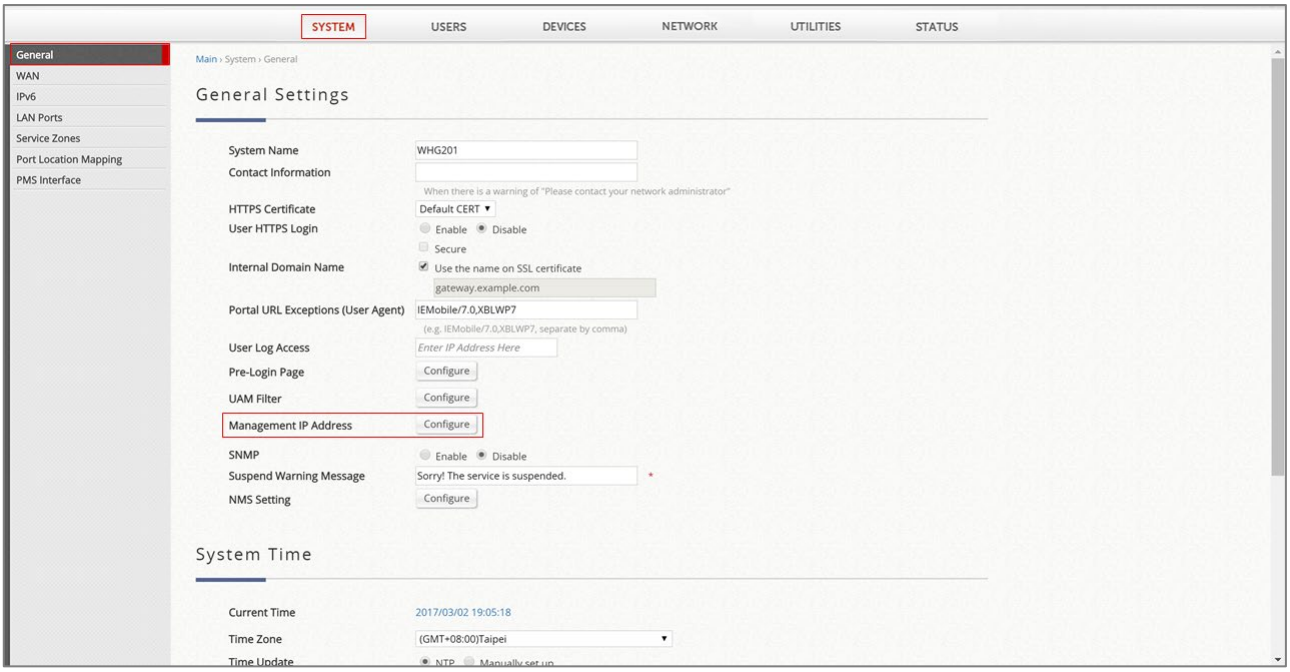
b. Go to Status → Interfaces → WAN1 to verify WAN1 IP Address.



c. Go to System → LAN Ports to select “Tag-Based” as the LAN Port Mode and Apply.

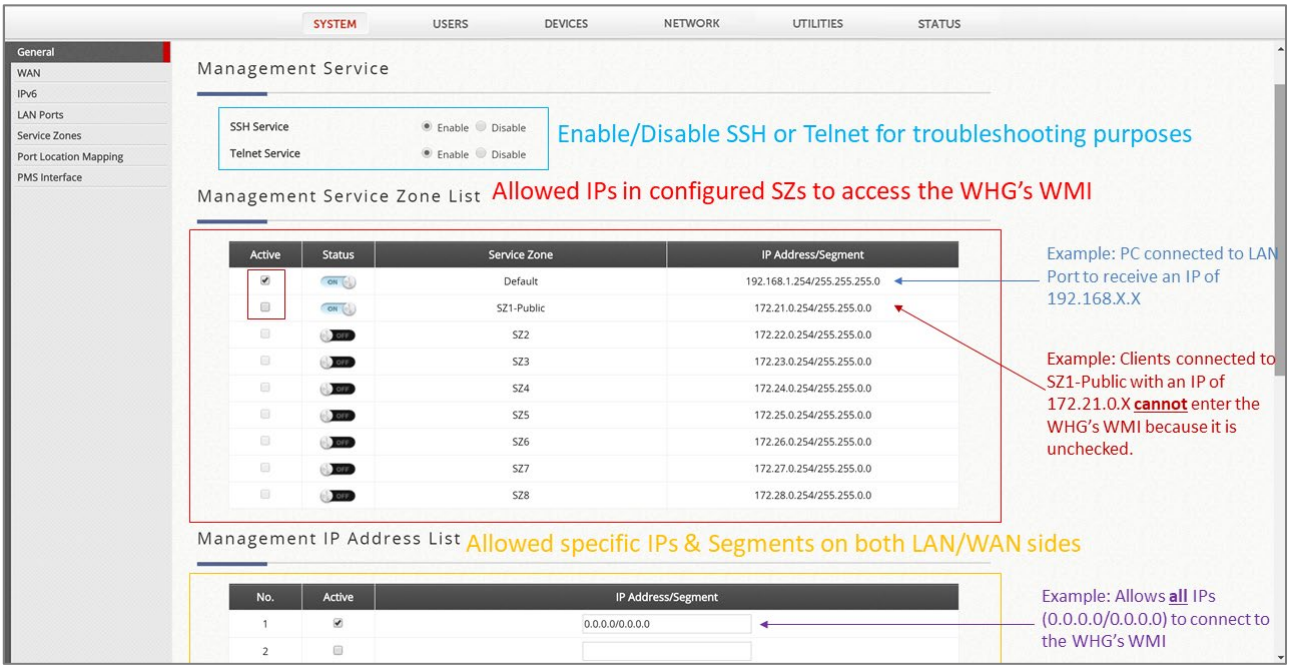


d. Go to System → General and click the Configure button beside Management IP Address.



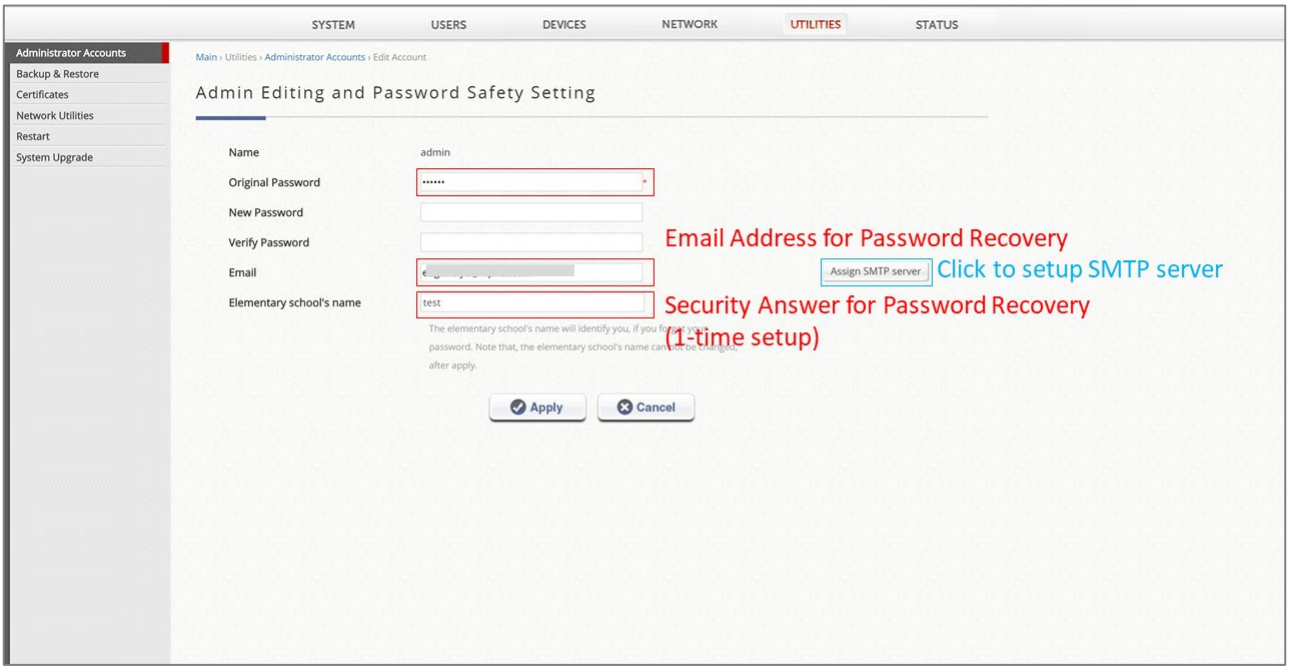
e. Check the appropriate SZs and configure the preferred IP Addresses to allow access to the Web Management Interface.

※ *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.*

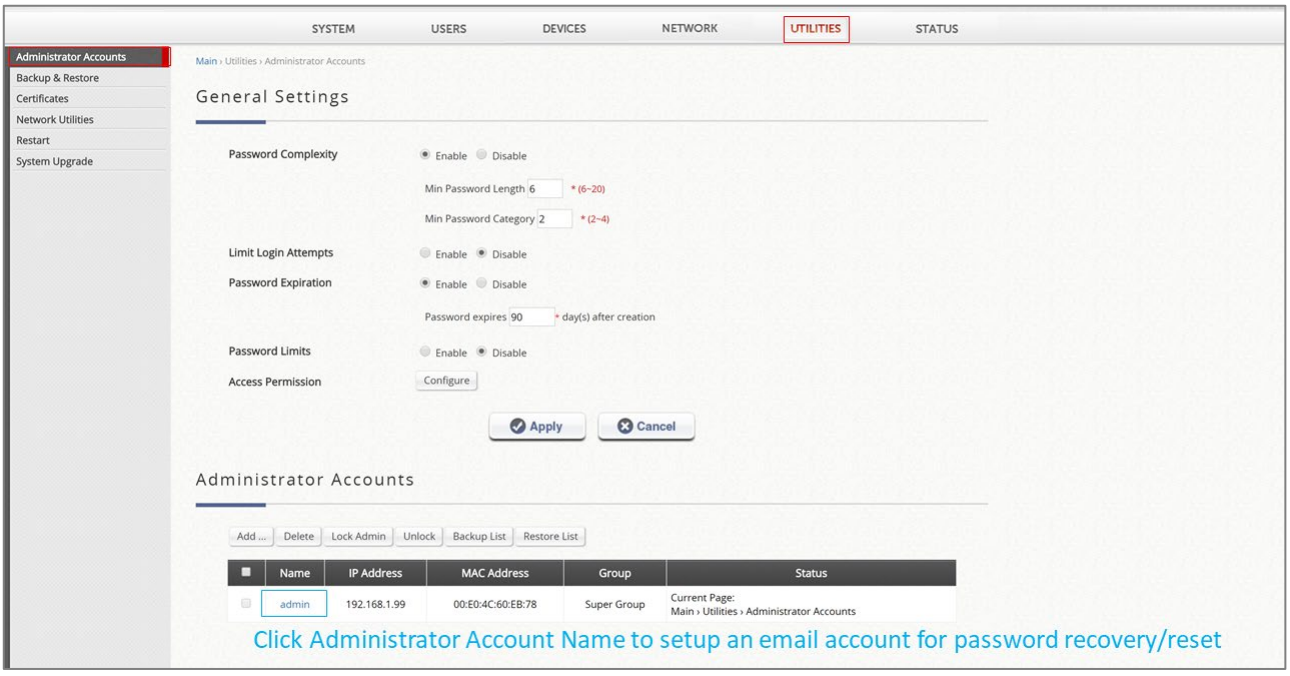


3.2 Utilities - Admin Password Recovery

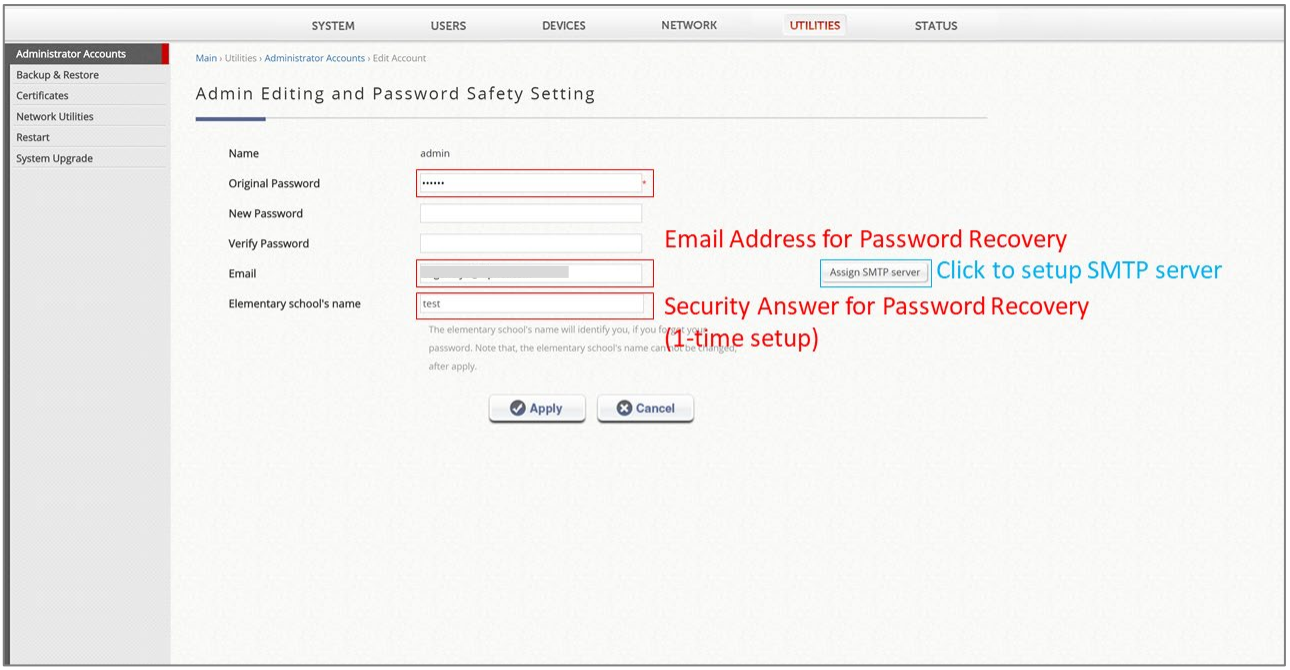
a. Go to Utilities → Administrator Accounts and click the “admin” Name to configure password recovery.



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



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



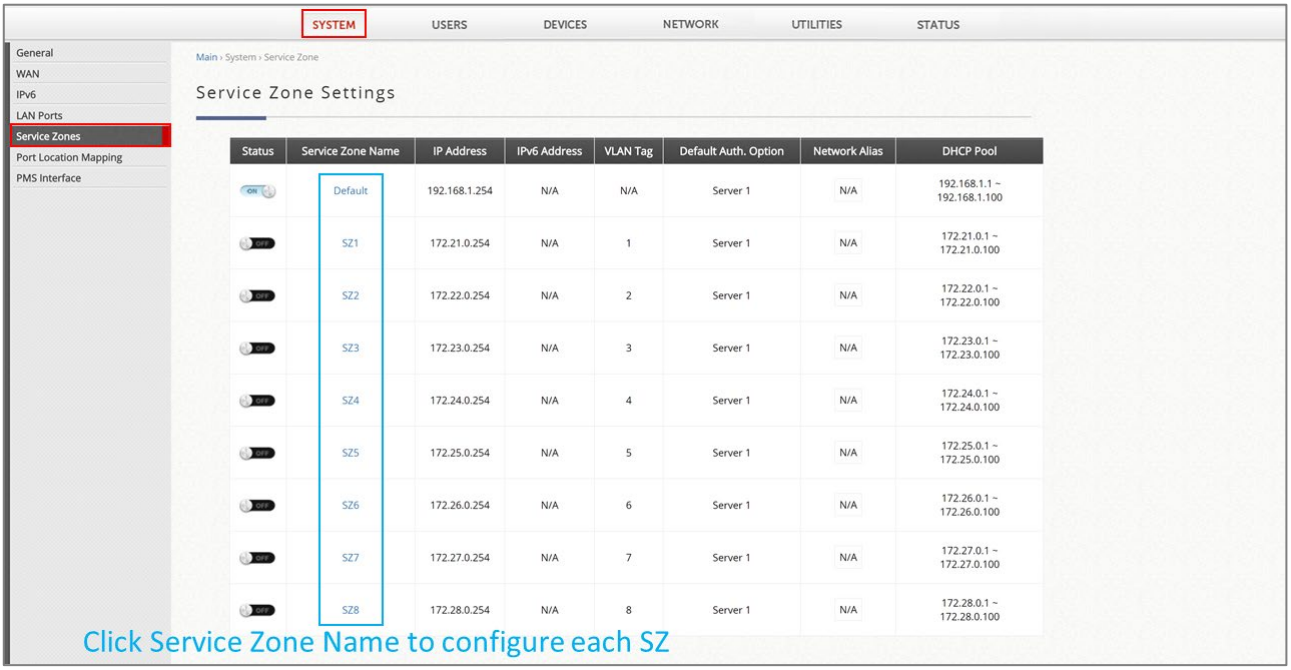
3.3 System

3.3.1 System - Service Zones Configuration

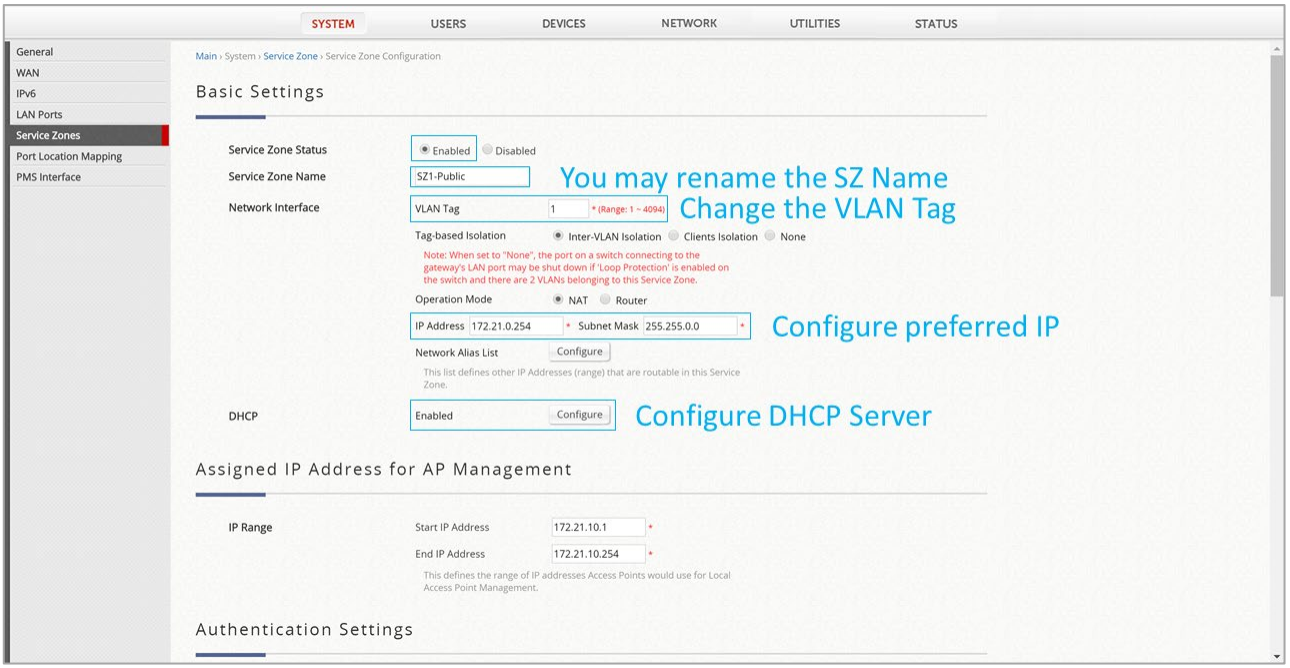
a. Go to System → Service Zones and confirm WAN Subnet and Default Service Zone IP Address are in different subnets.

Example: WAN1 IP = 10.201.5.150 / Subnet = 255.255.255.0

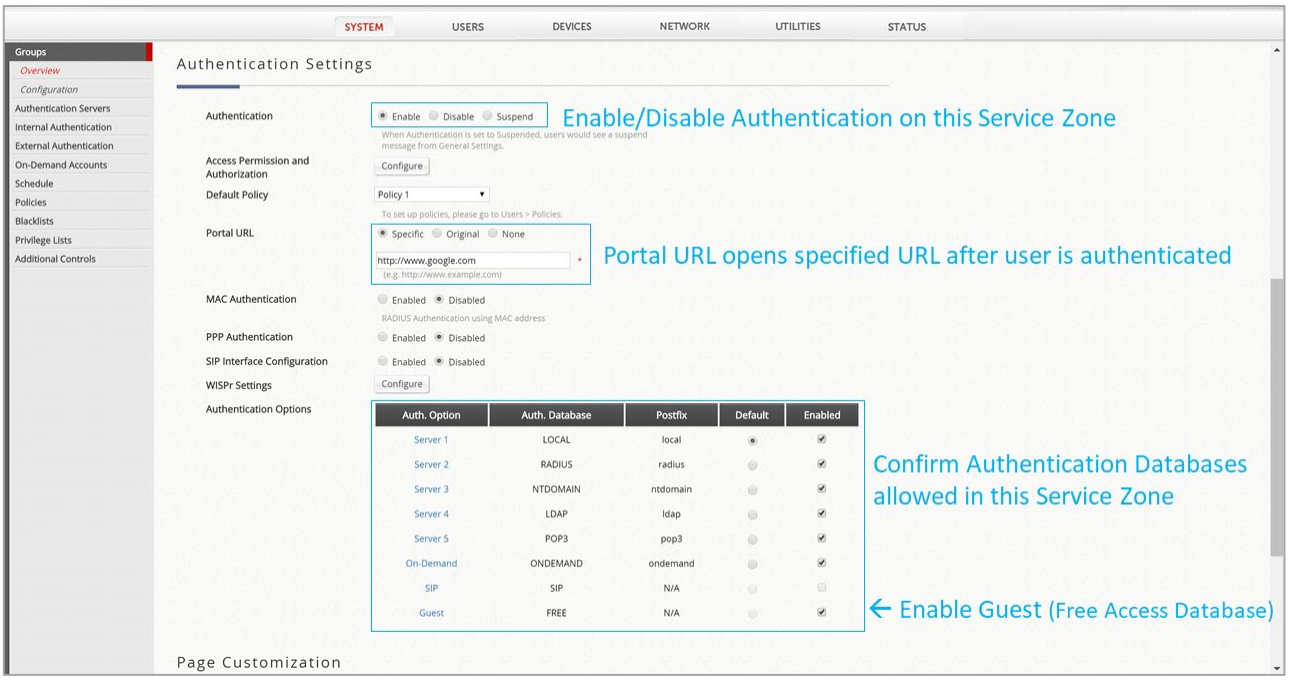
Default SZ IP = 192.168.1.254 / Subnet = 255.255.0.0



b. Click SZ1, Enable the Service Zone and configure the basic network settings.

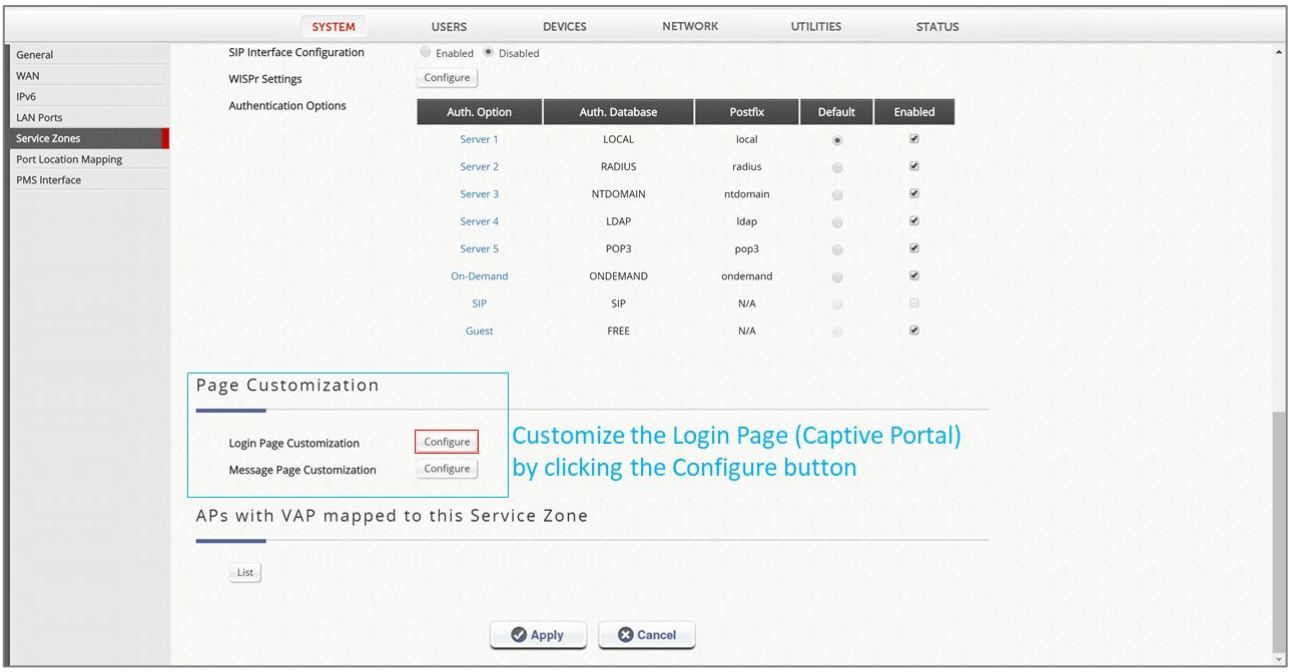


c. Configure Authentication Settings. Enable Guest Free Auth. Database to allow self-registration users.

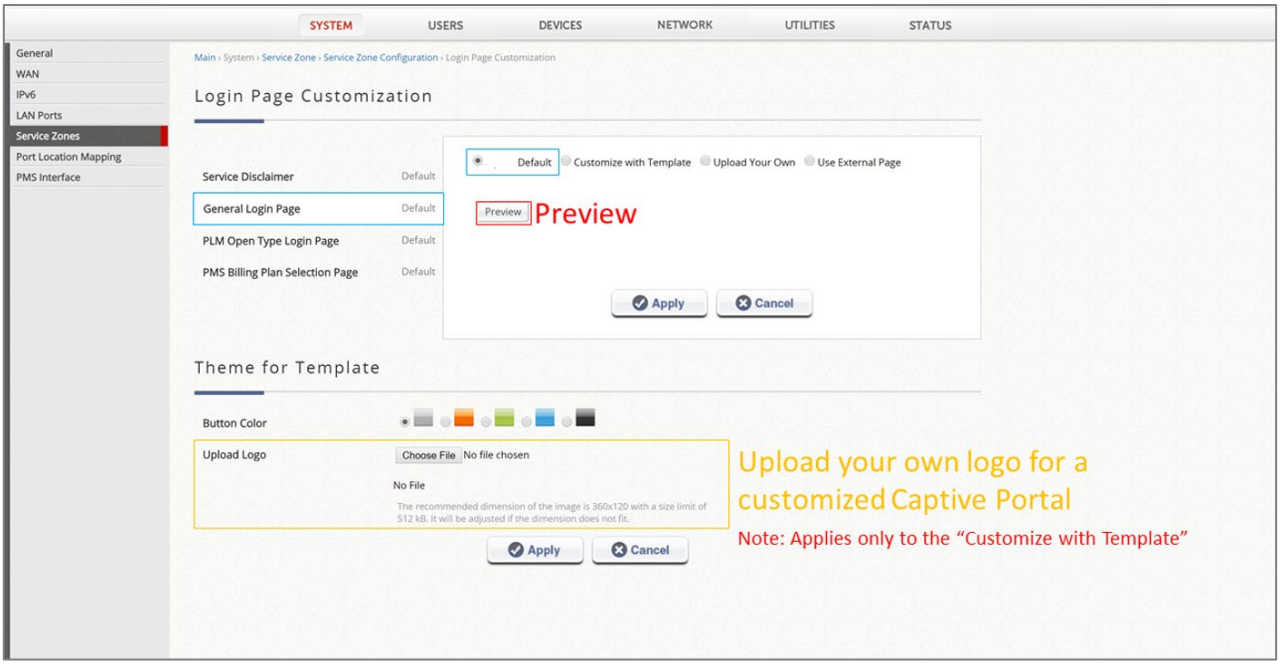


3.3.2 System - Service Zone – Captive Portal Customization

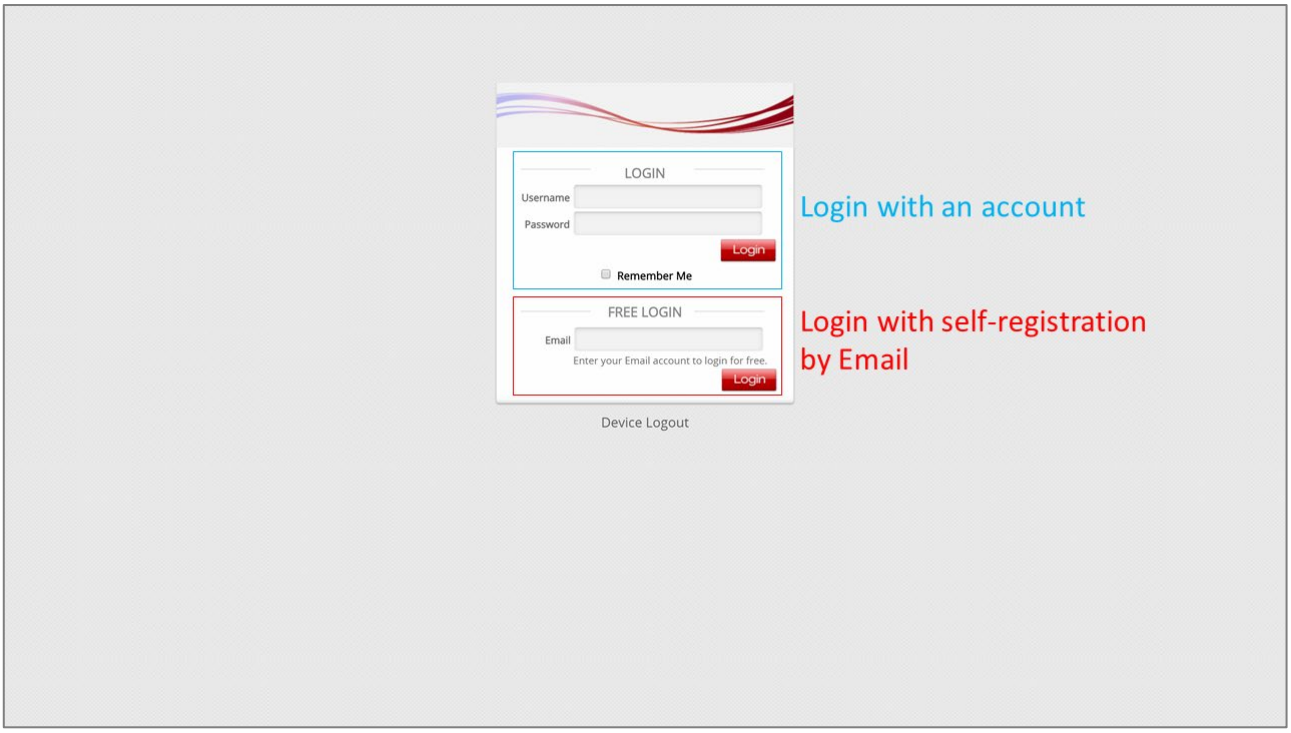
a. Click configure to customize different Login Page Customization. Message Page Customization will provide customizations to message pages such as the login success page.



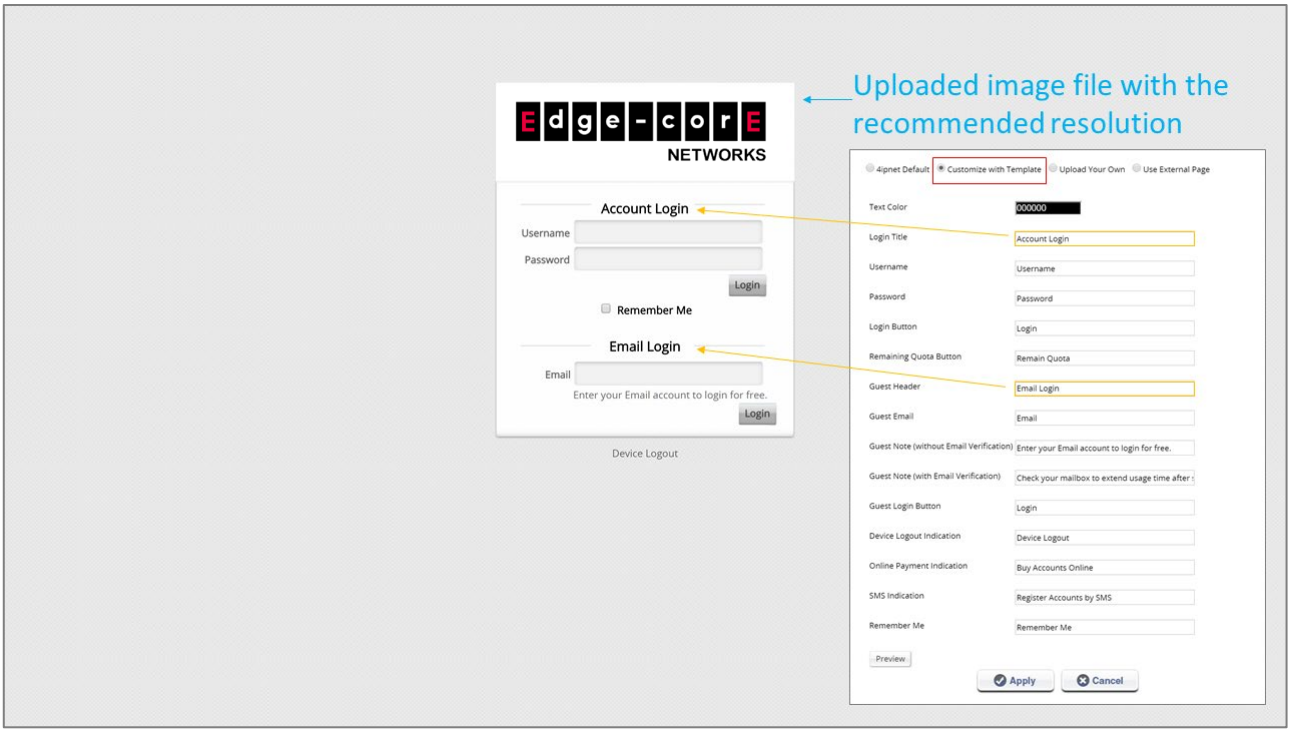
b. Click configure to customize different Login Page Customization. Message Page Customization will provide customizations to message pages such as the login success page.



c. Preview General Login Page in Default mode.



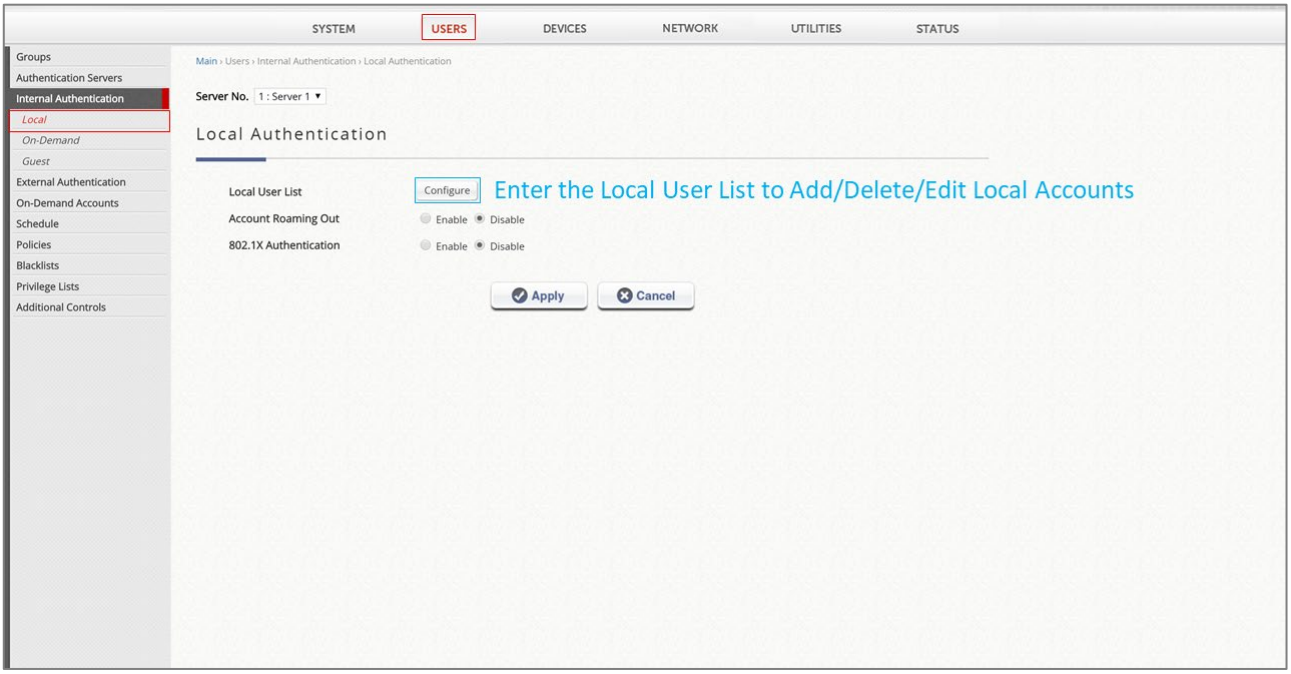
d. Preview General Login Page in Customize with Template selection with an uploaded logo and customized text.



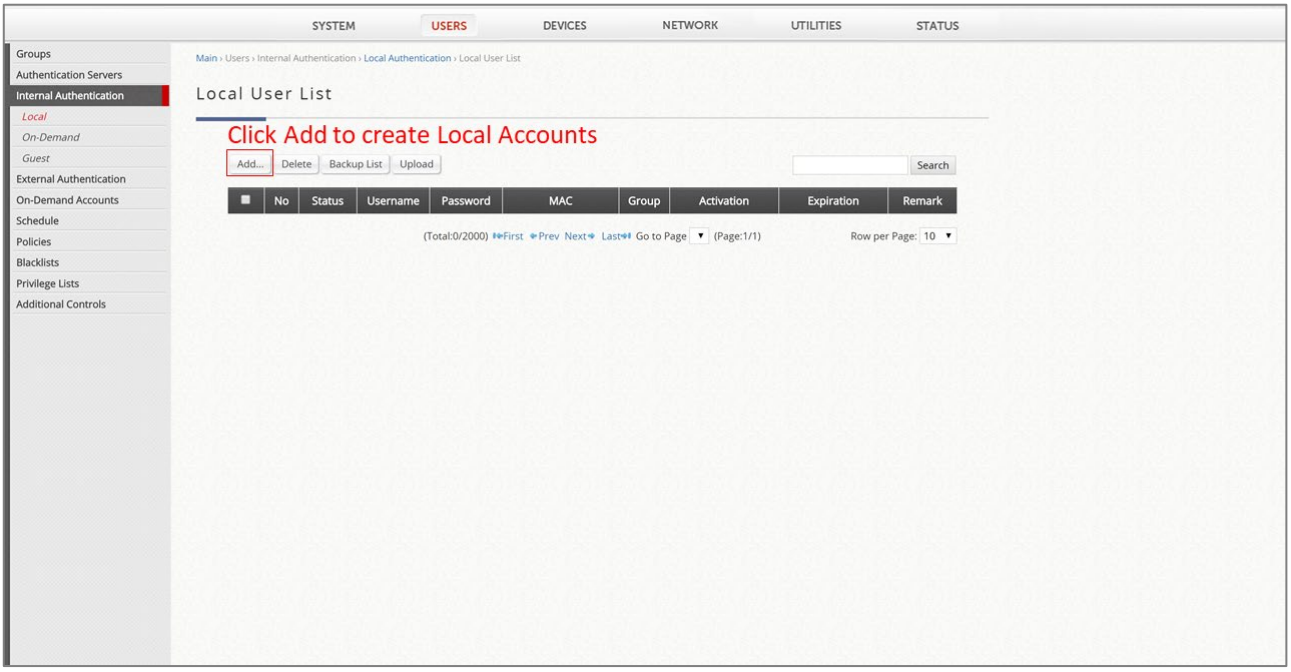
3.4 Users

3.4.1 Users - Local Accounts

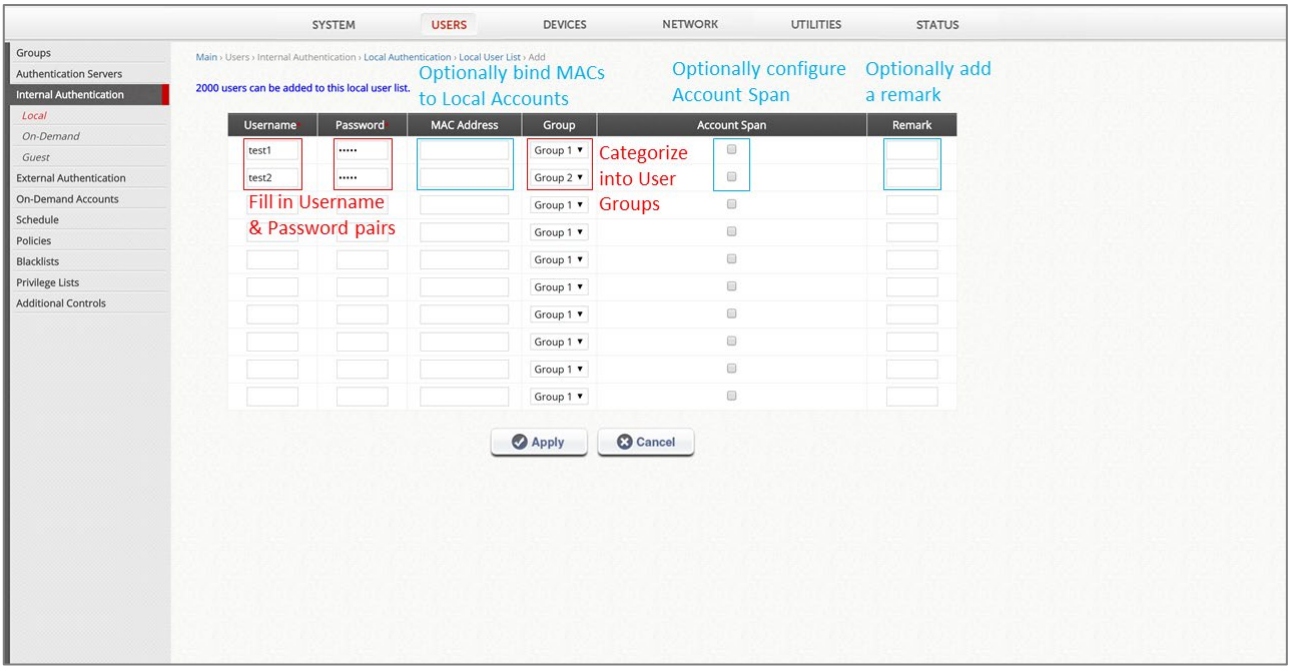
a. Go to Users → Internal Authentication, Local to create accounts using the Local Database.



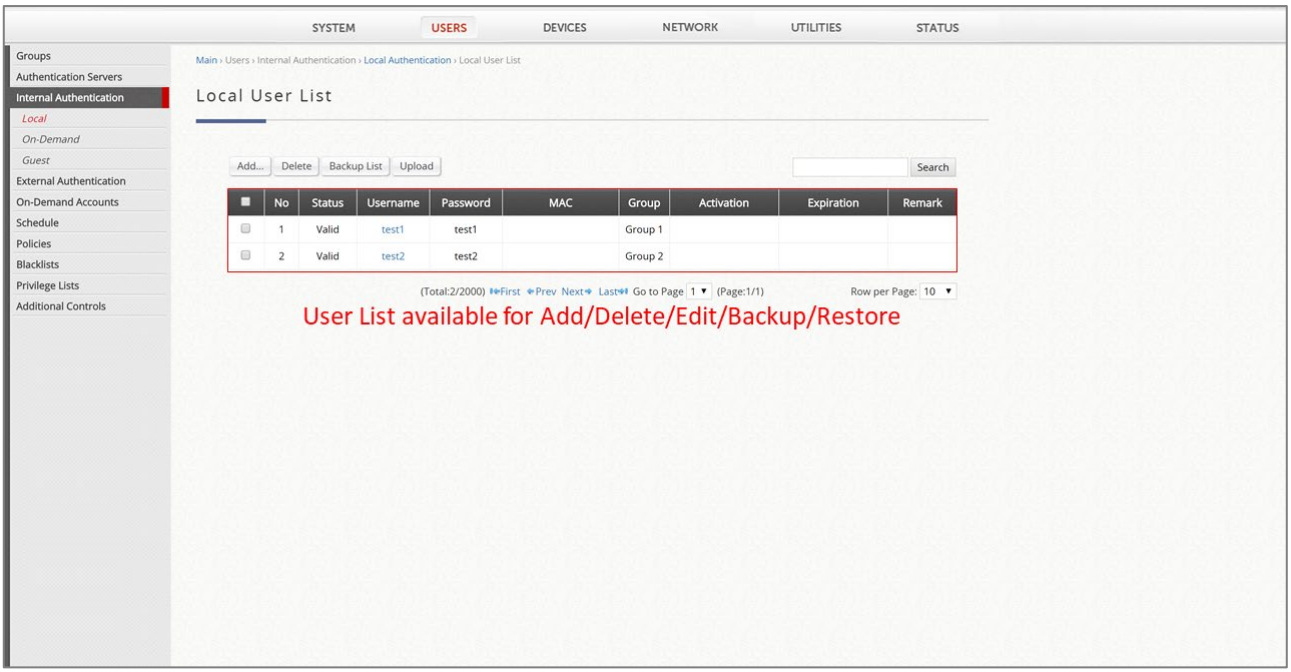
b. Click Add to create single or multiple accounts at once.



c. Enter user account credentials and Apply. (Ex. test1/test1 and test2/test2)

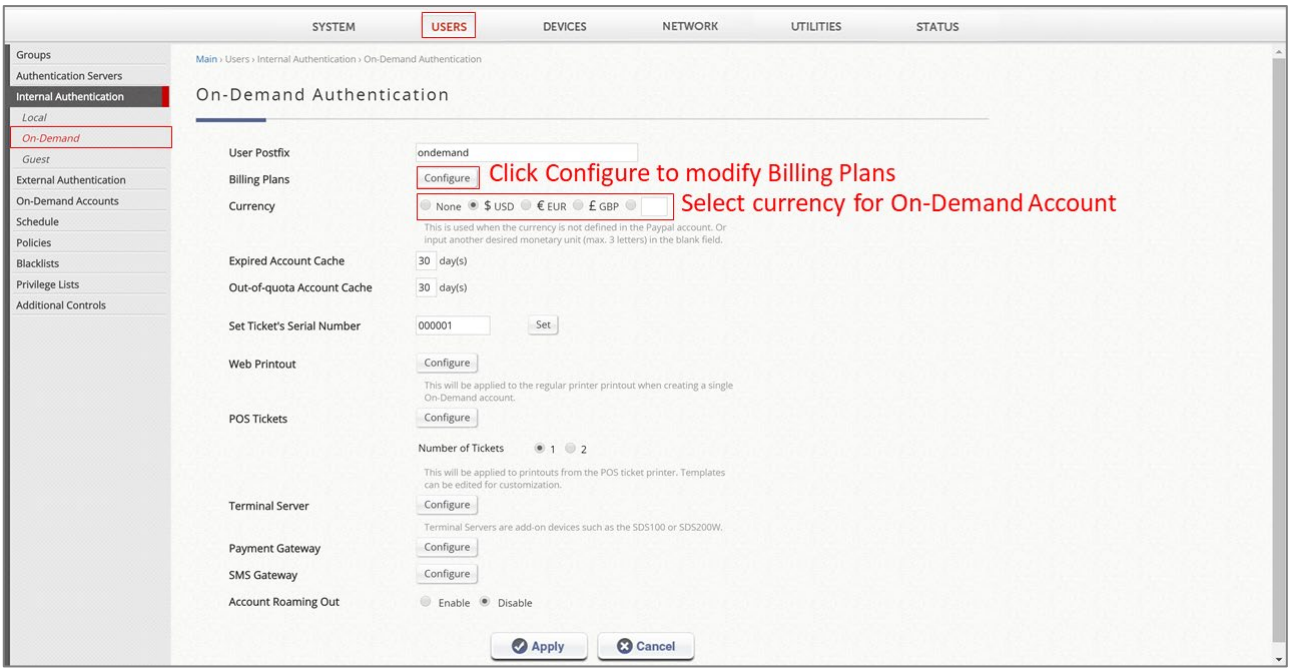


d. Created accounts can be viewed on the Local User List.

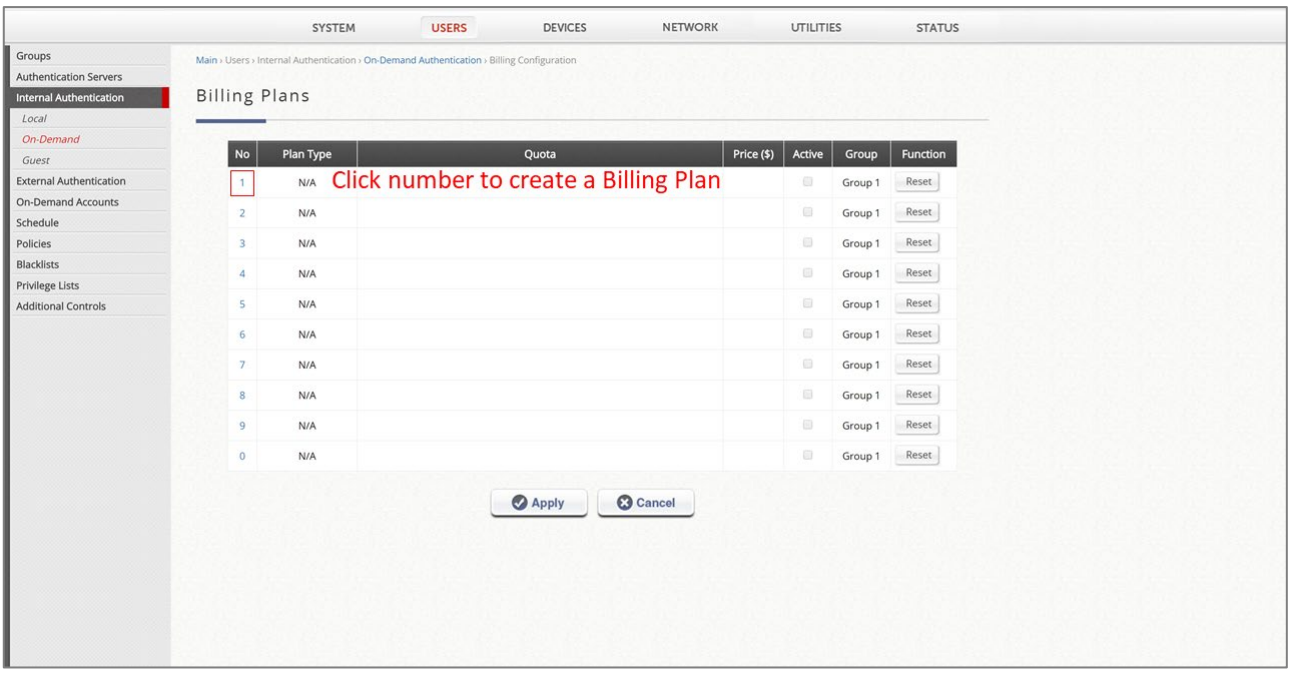


3.4.2 Users - On-Demand Accounts

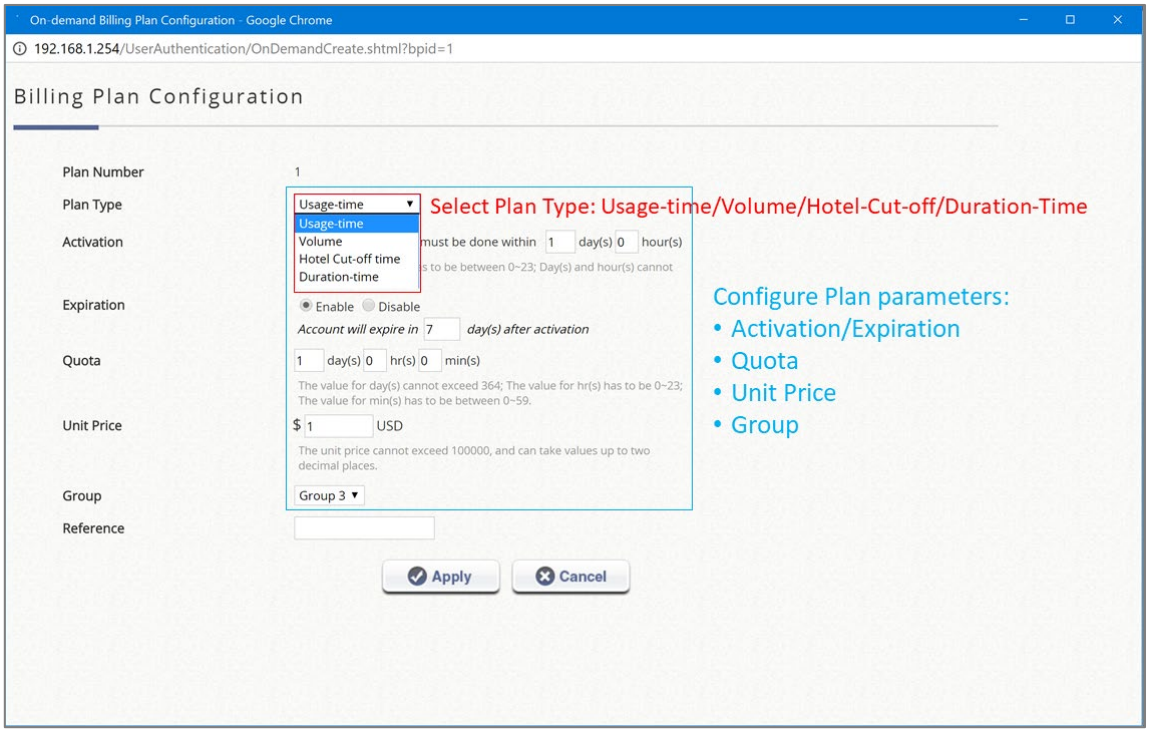
a. Go to Users → Internal Authentication → On-Demand and click Billing Plan's Configure button to modify Billing Plans



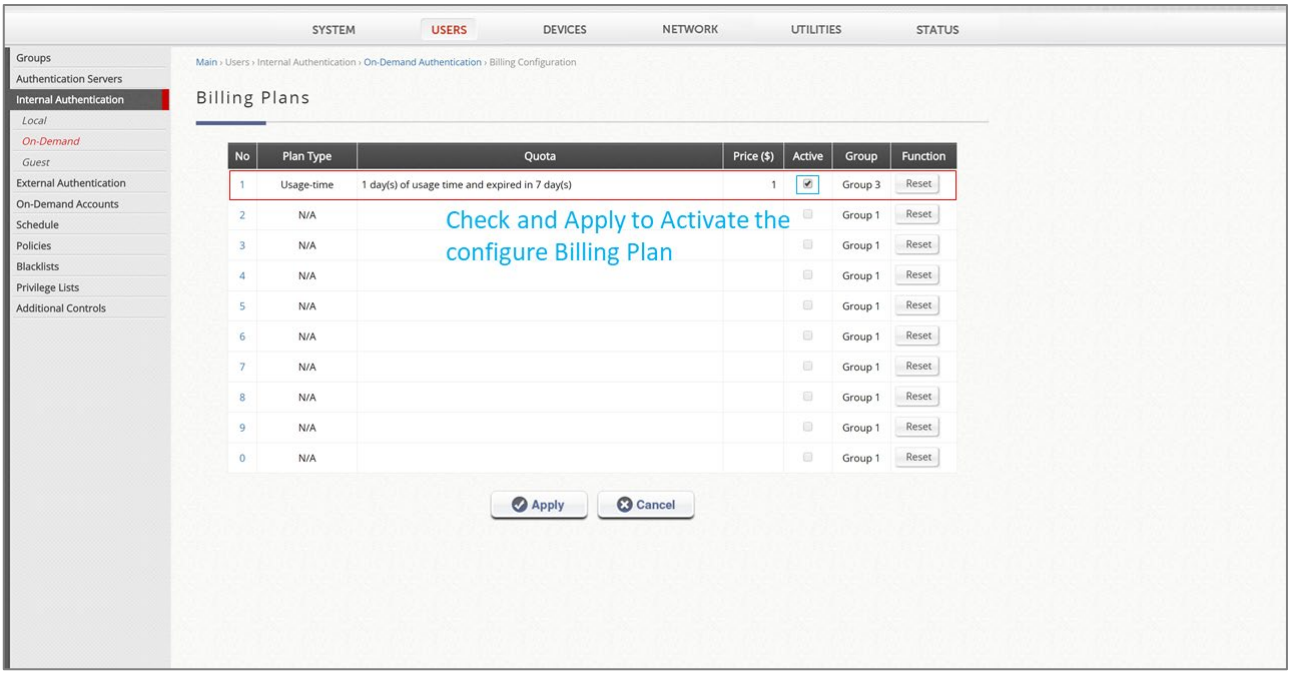
b. Click the Billing Plan number to create a billing plan.



c. Choose a Plan Type and configure the Plan parameters to achieve a complete User Management: Activation, Expiration, Quota, Unit Price and Group.

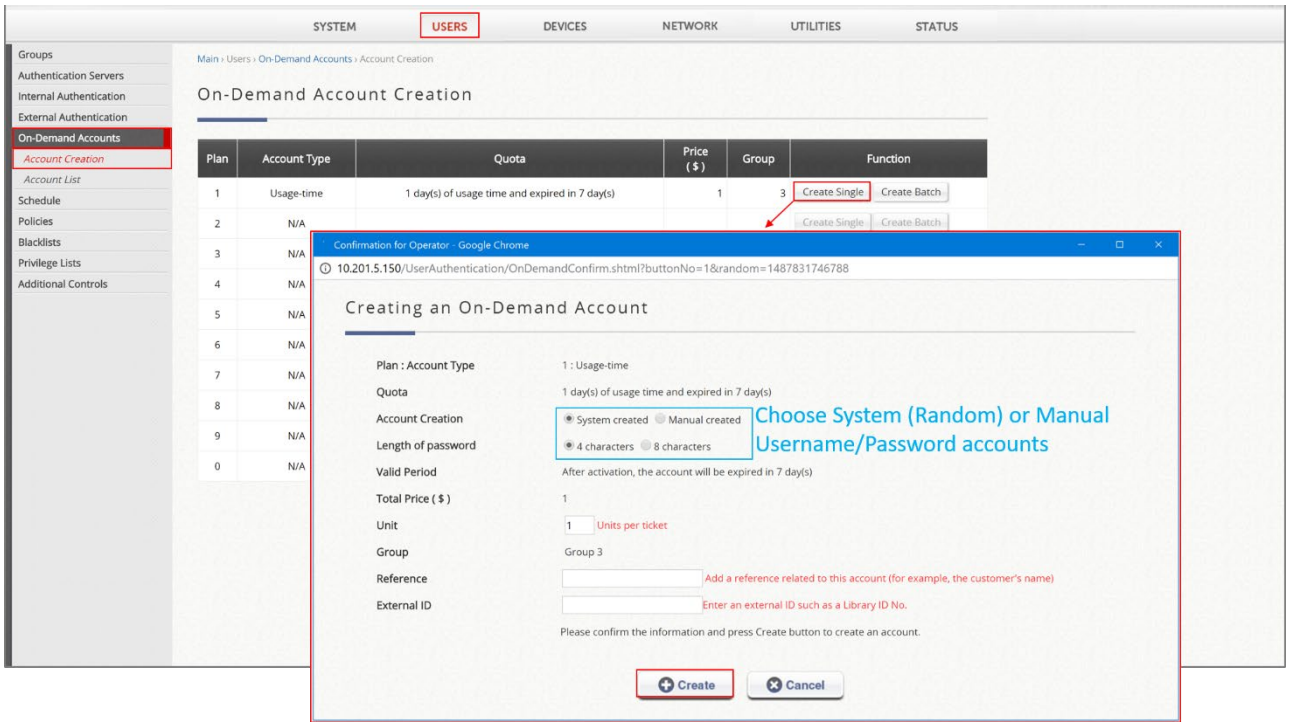


d. Confirm & Activate the Billing Plan.

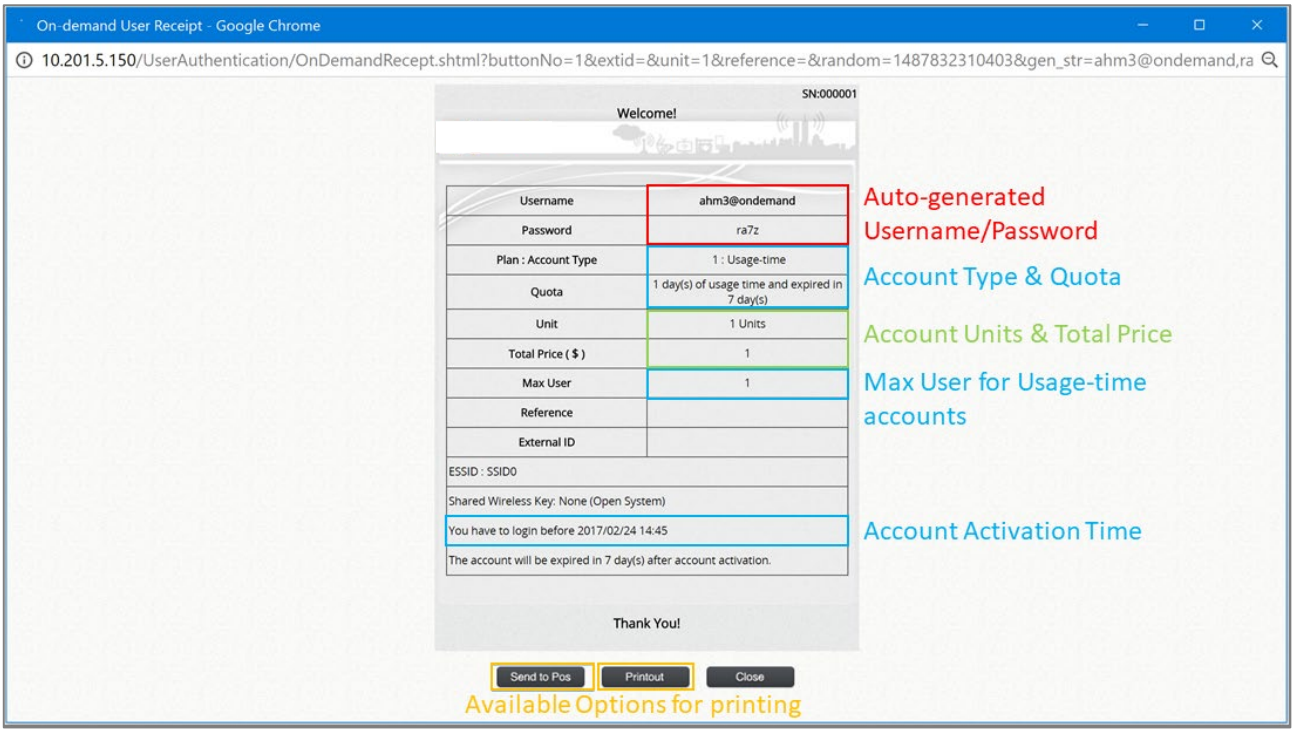


3.4.3 Users - Creating On-Demand Accounts

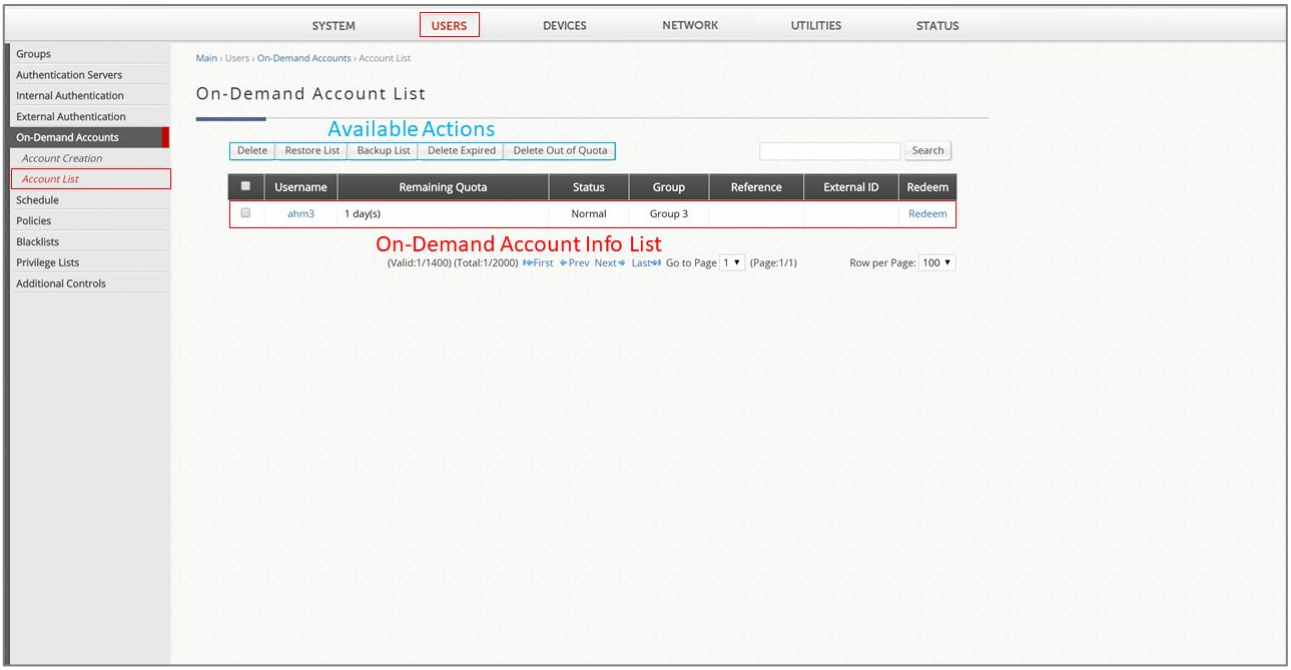
a. Go to Users → Go to Users → On-Demand Accounts → Account Creation to create an On-Demand account using the configured Billing Plan. Click Create Single and Create.



b. The created account will be displayed in a new window.



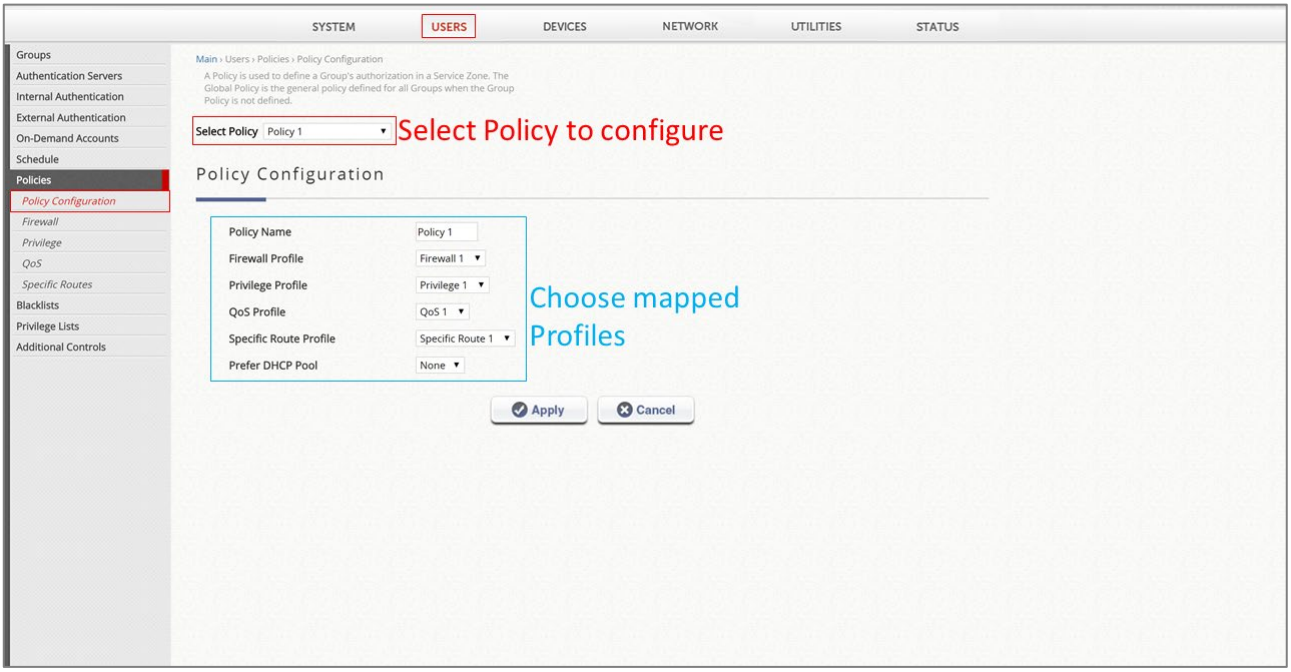
c. Go to Users → On-Demand Accounts → Account List to confirm the created account.



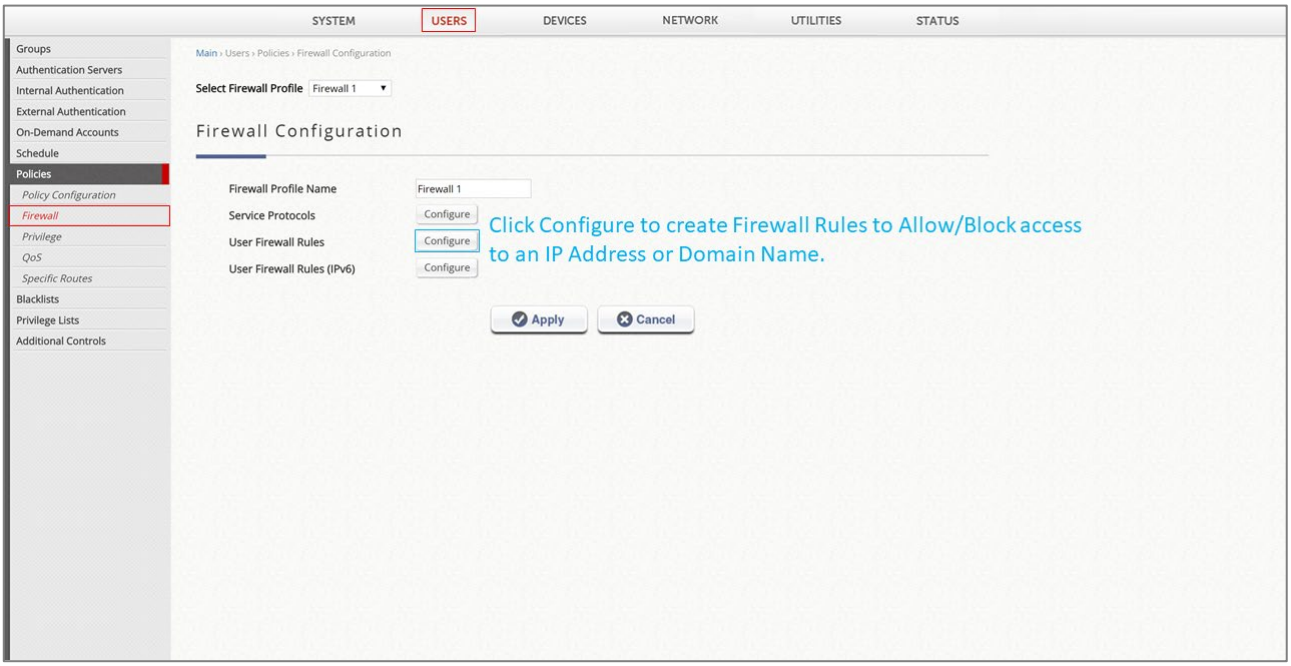
3.5 Users

3.5.1 Users - Policy Configuration

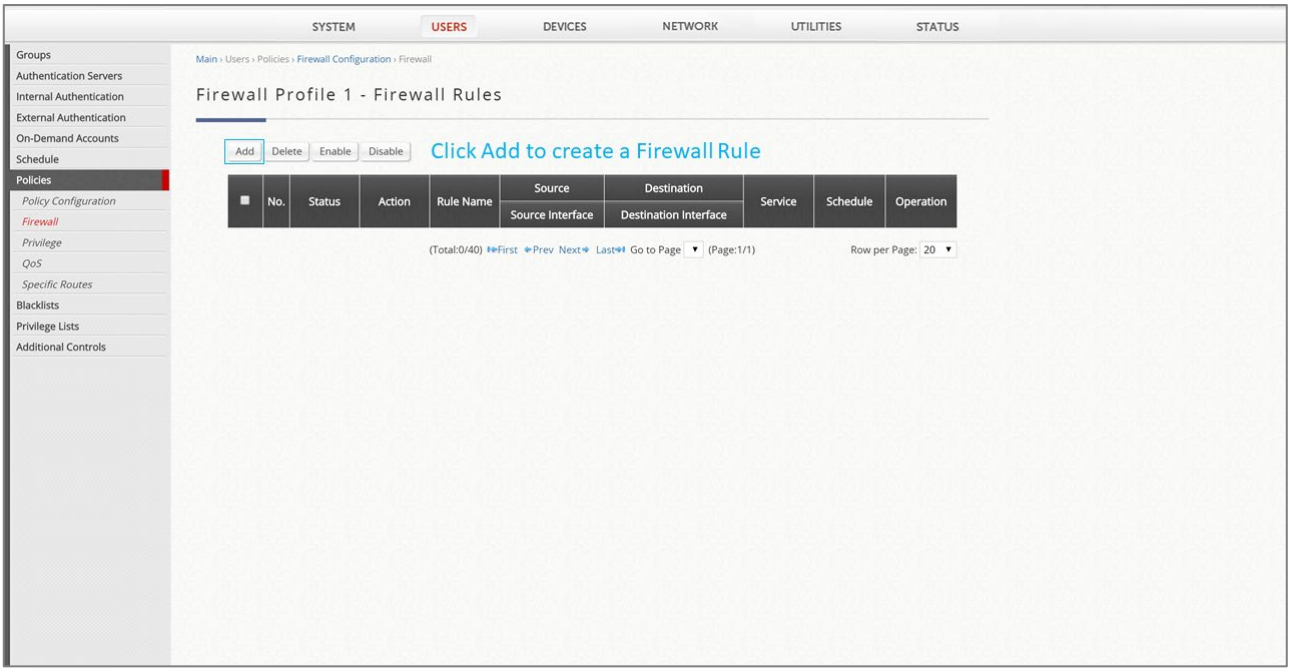
a. Configure and select Firewall Profile, Privilege Profile, QoS Profile and Specific Route Profile to create Policy 1.



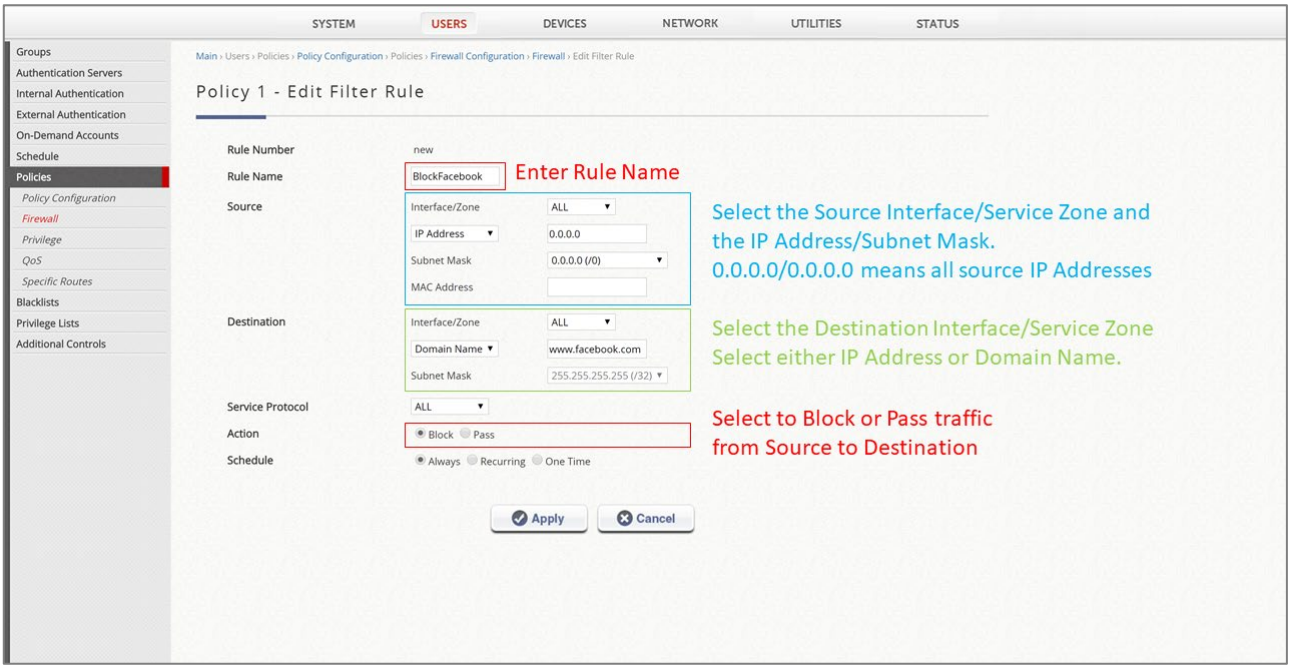
b. Go to Users → Firewall to configure User Firewall Rules to block a user's access to an IP Address or Web Domain.



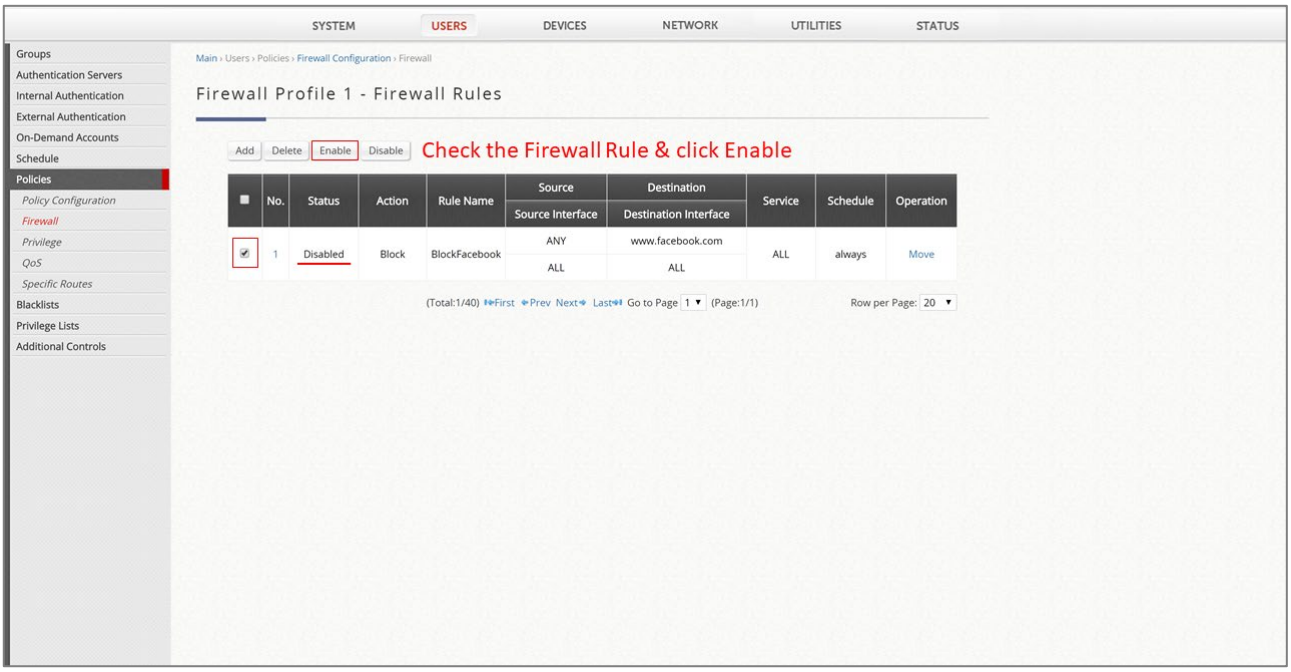
c. Click the Add button to create a new Firewall Rule.



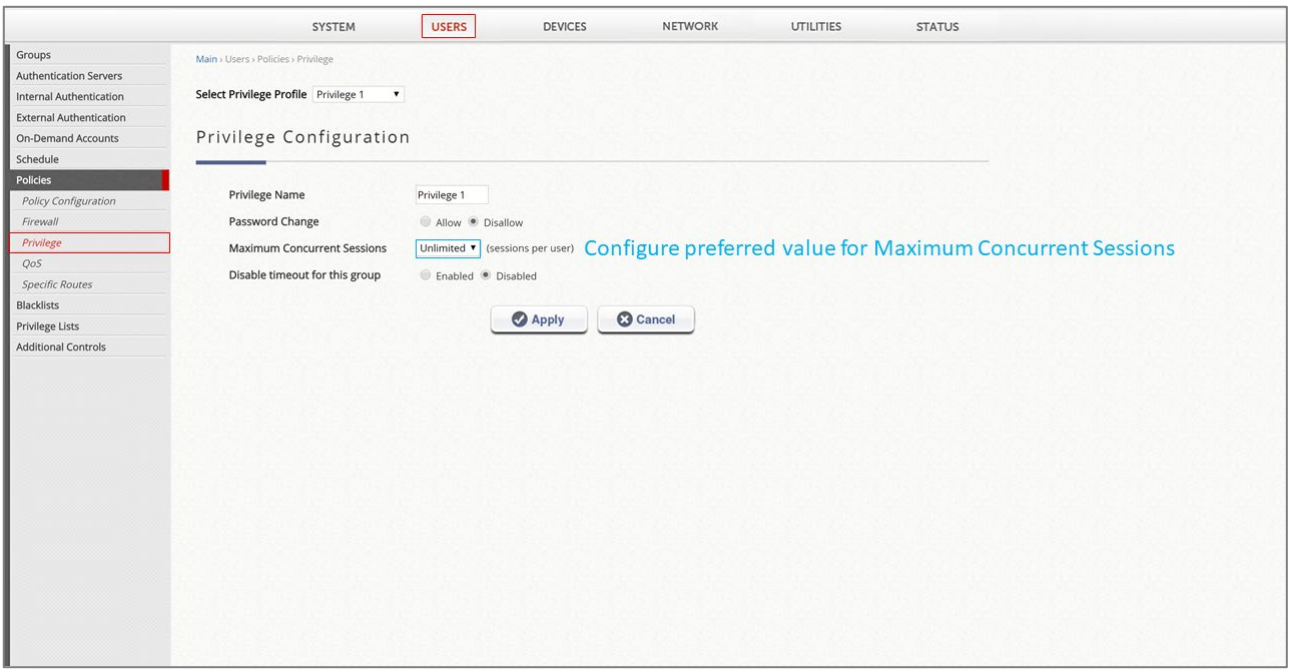
d. Configure a new Firewall Rule (BlockFacebook) with preferred Source/Destination.



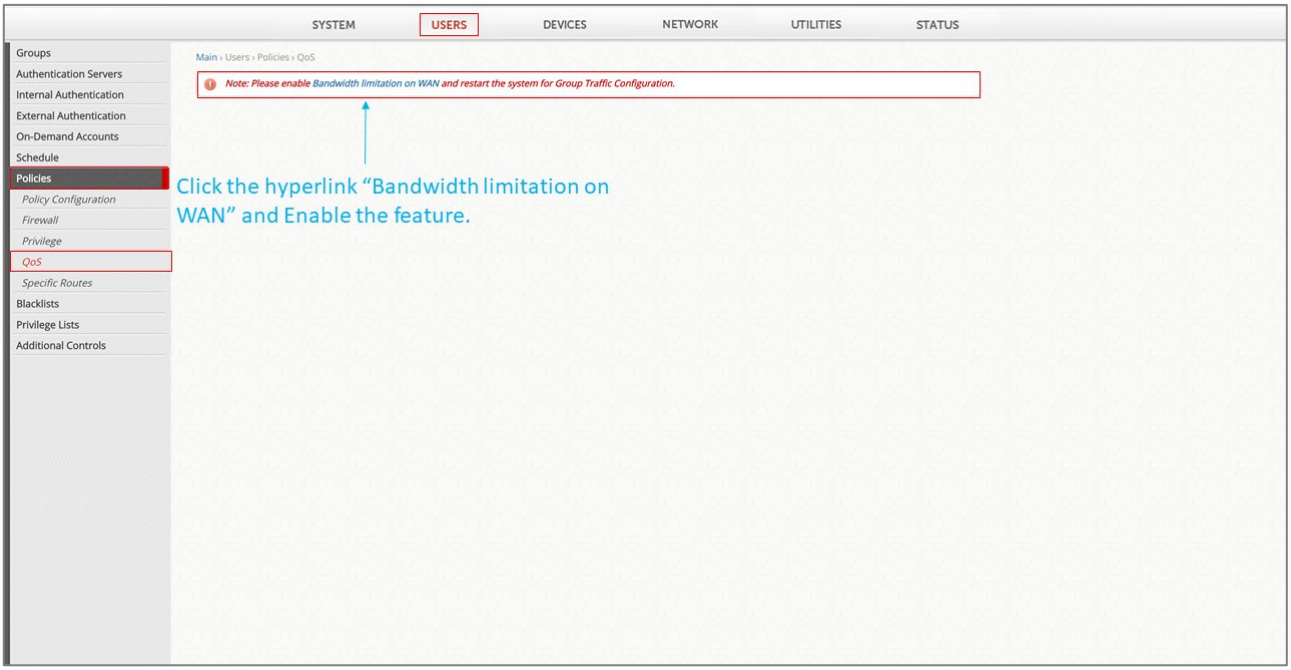
e. Check the checkbox and click the Enable button to Activate & Enable the Firewall Rule.



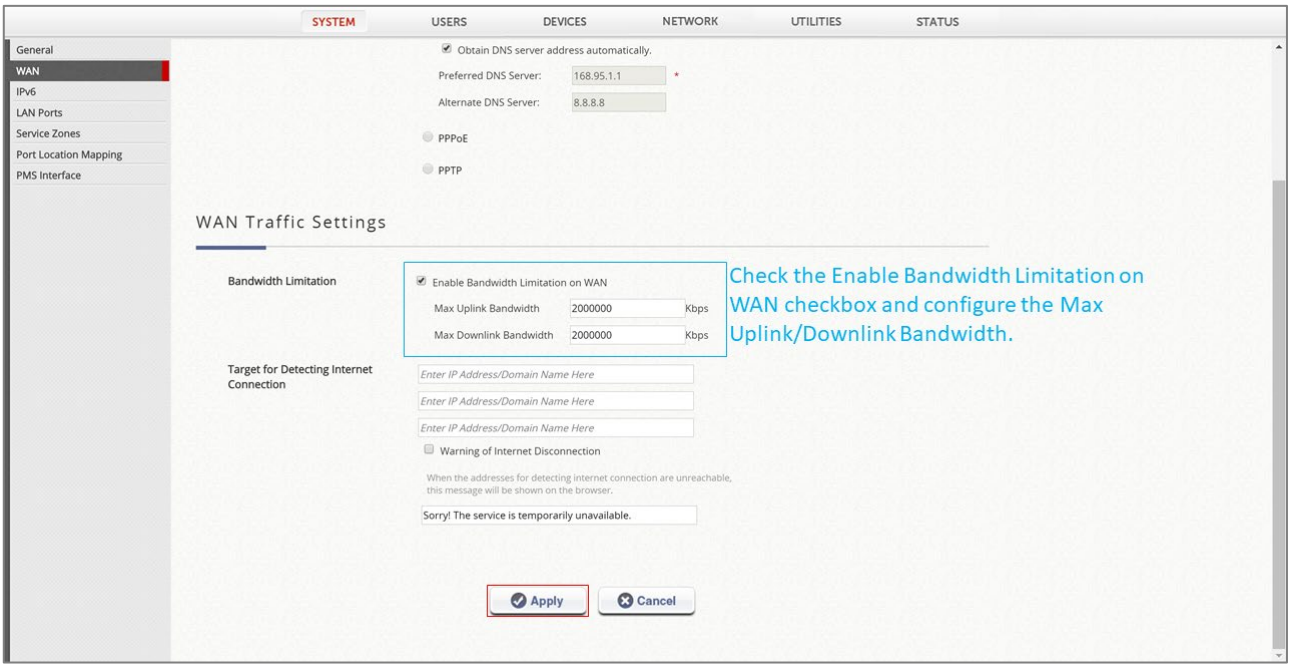
f. Go to Users → Policies → Privilege to configure the Maximum Concurrent Sessions of each user under this Policy. (Default = 500)



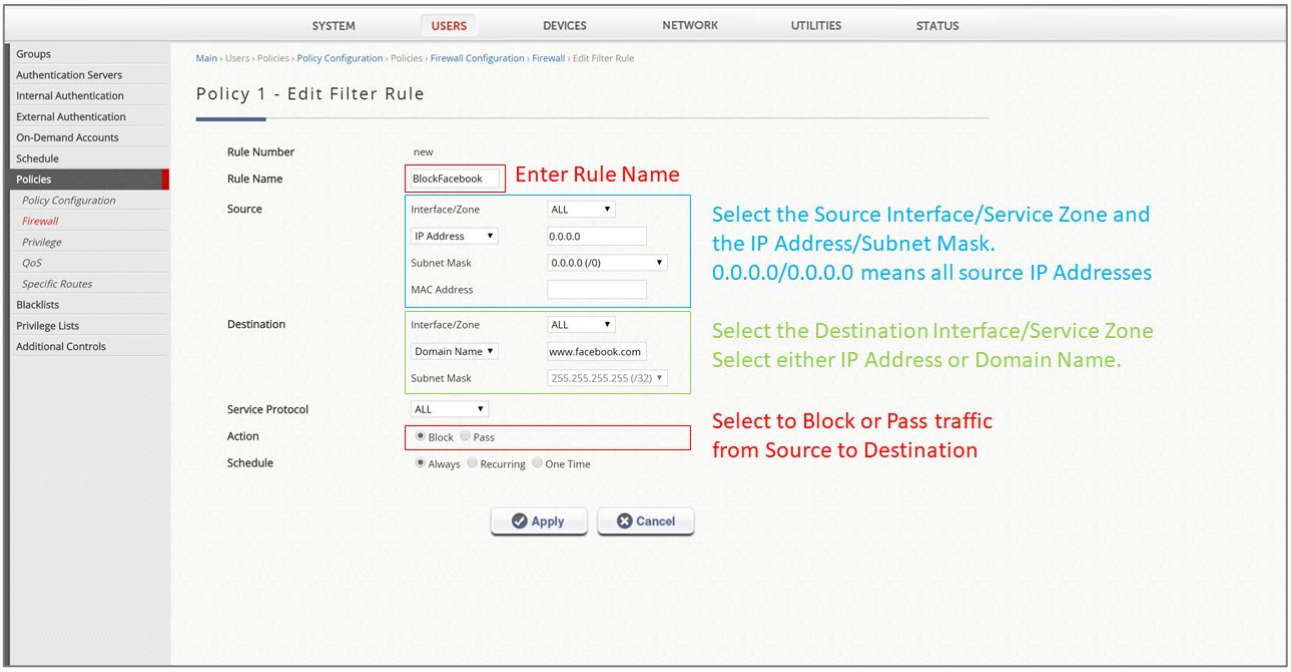
g. Go to Users → Policies → QoS to configure each Group/User's bandwidth.
To configure the QoS Bandwidth Control, Bandwidth Limitation on WAN must be enabled. Click the hyperlink to access the WAN configuration page.



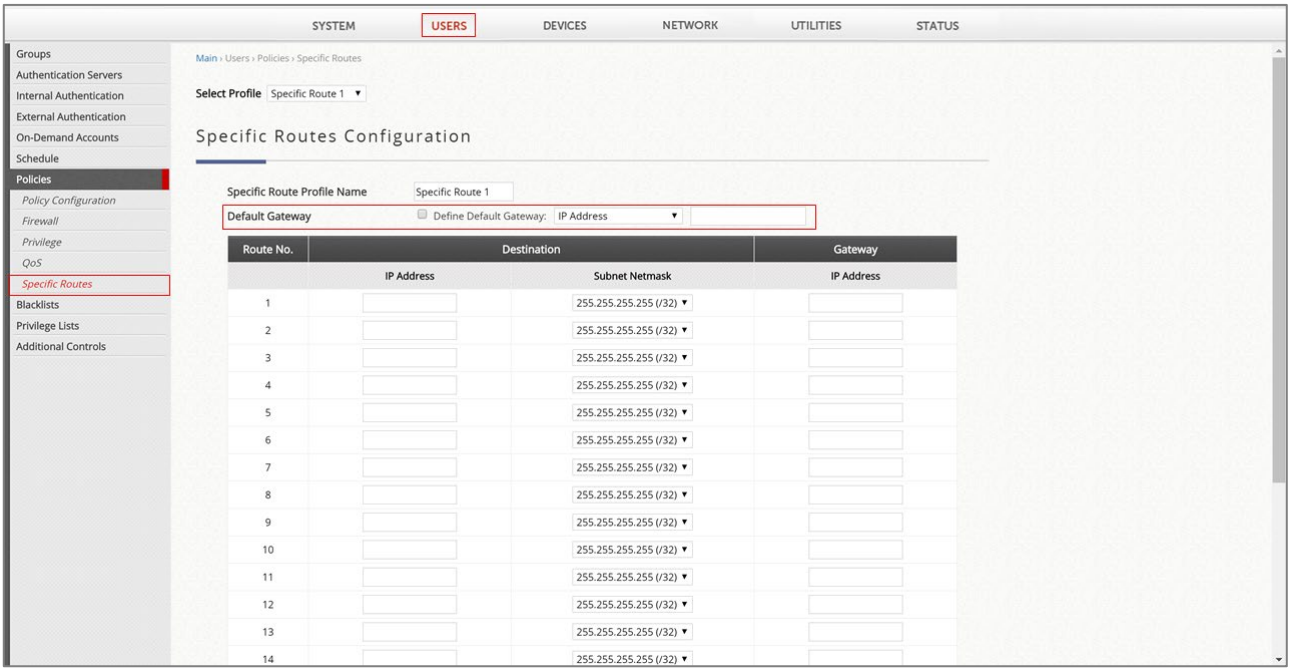
h. Please check the Bandwidth Limitation at WAN checkbox, Apply and restart the EWS to activate the changes.



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



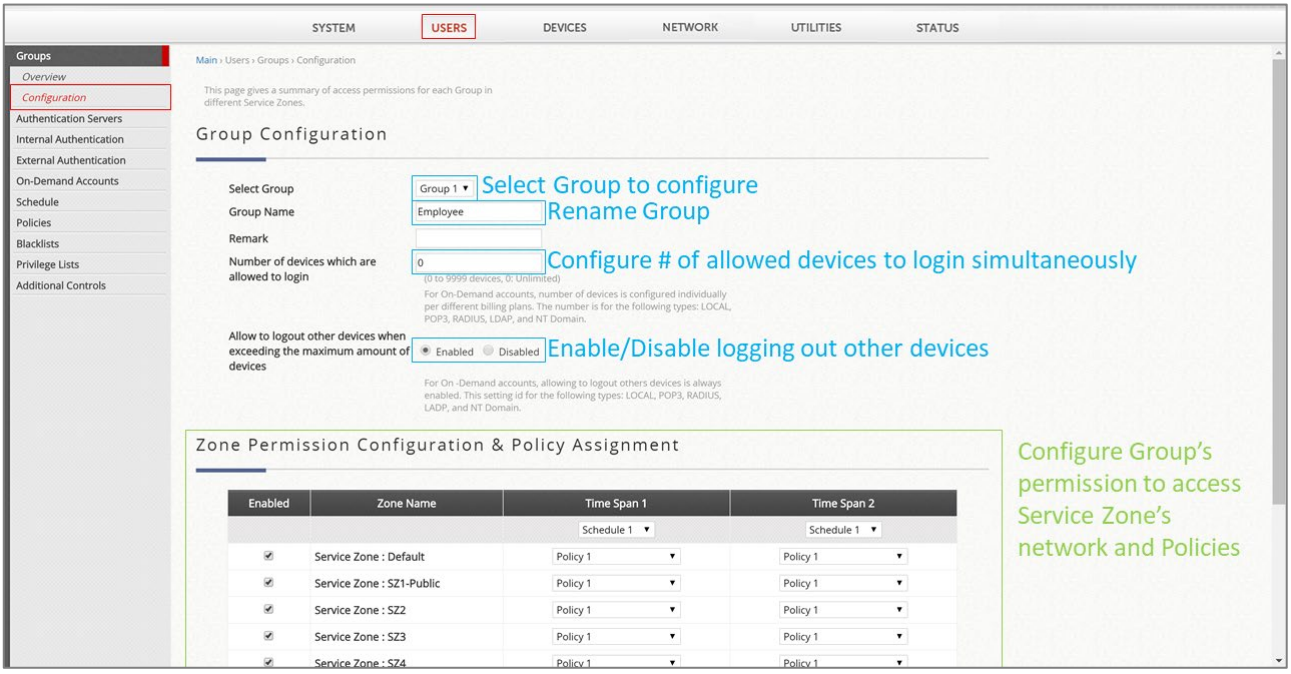
j. Go to Users → Policies → Specific Routes to configure the Specific Route profile to direct user groups to a specified gateway.



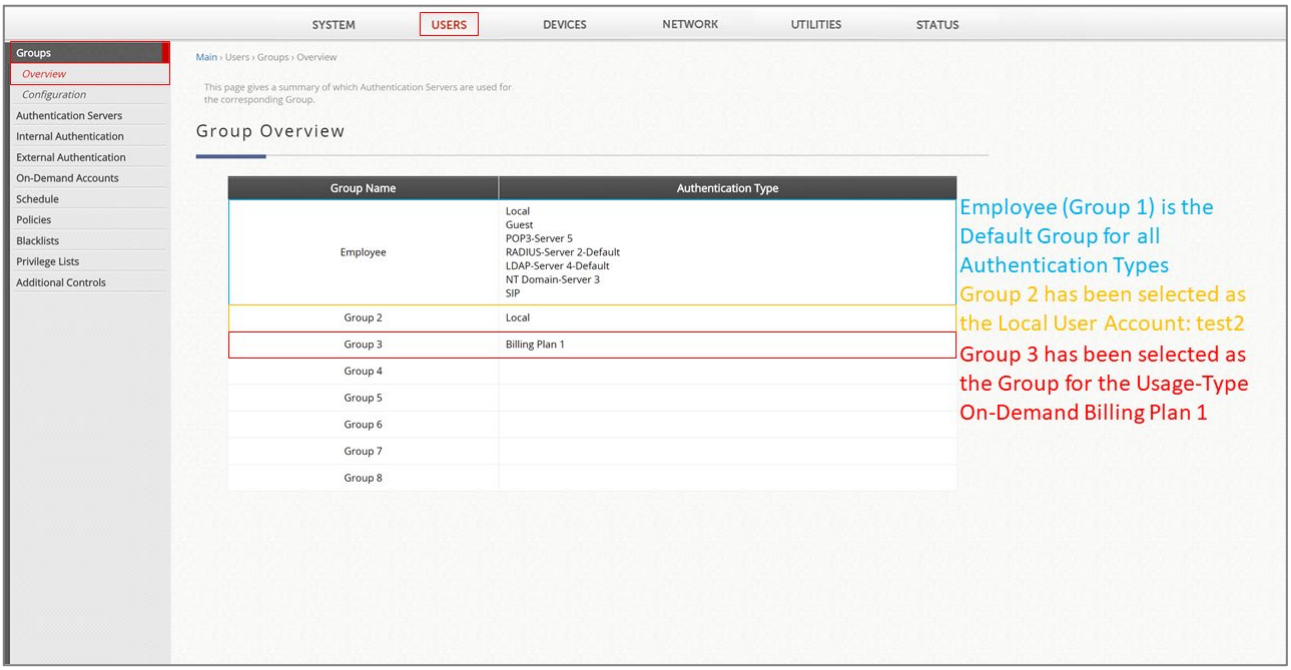
3.6 Users

3.6.1 Users - Group Configuration

a. 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.



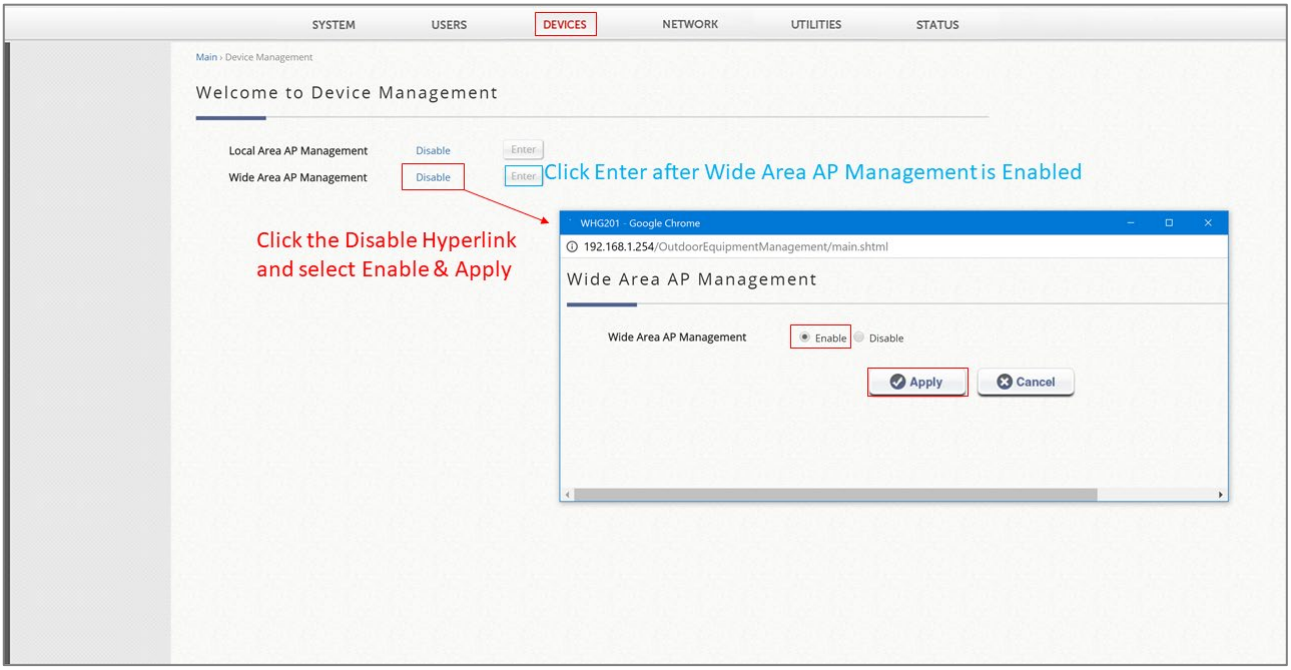
b. Go to Users → Groups → Configuration and select Group 1 to configure the Group parameters, Service Zones Group 1 is allowed access to and the Policy Profile applied when an account in this group connects to the specified Service Zone.



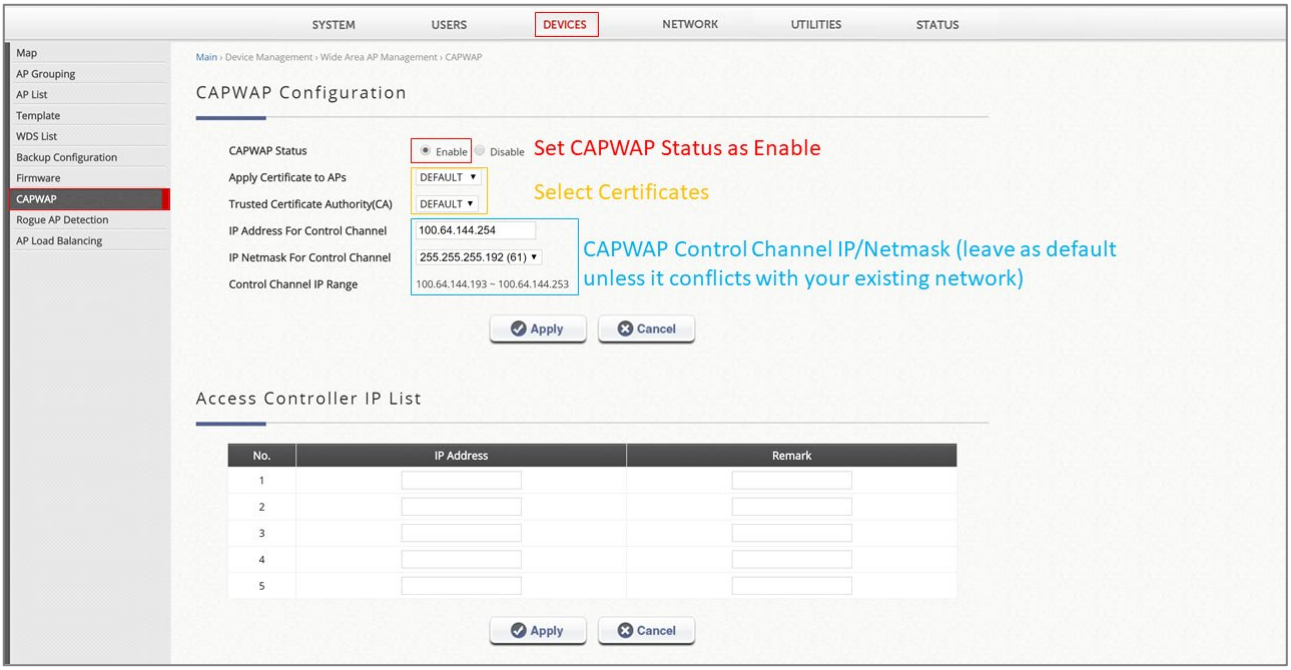
3.7 Devices

3.7.1 Devices - WAPM – CAPWAP Tunnel

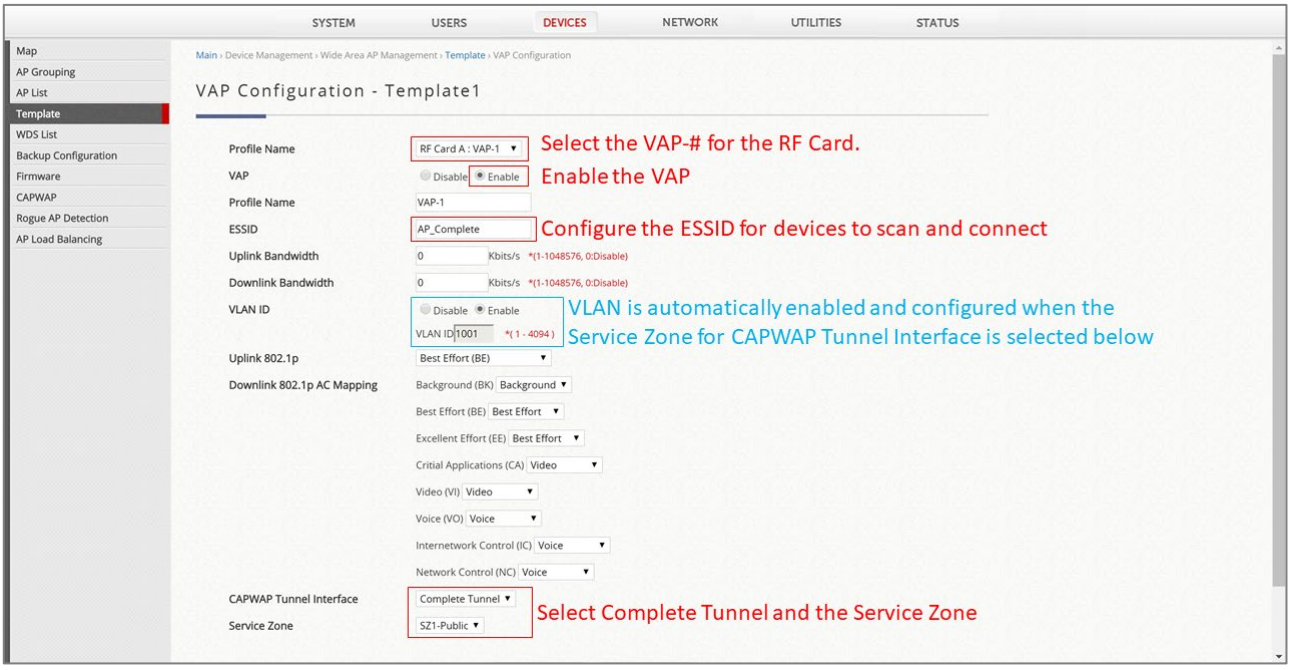
a. Go to Devices, Enable Wide Area AP Management and click Enter to configure WAPM.



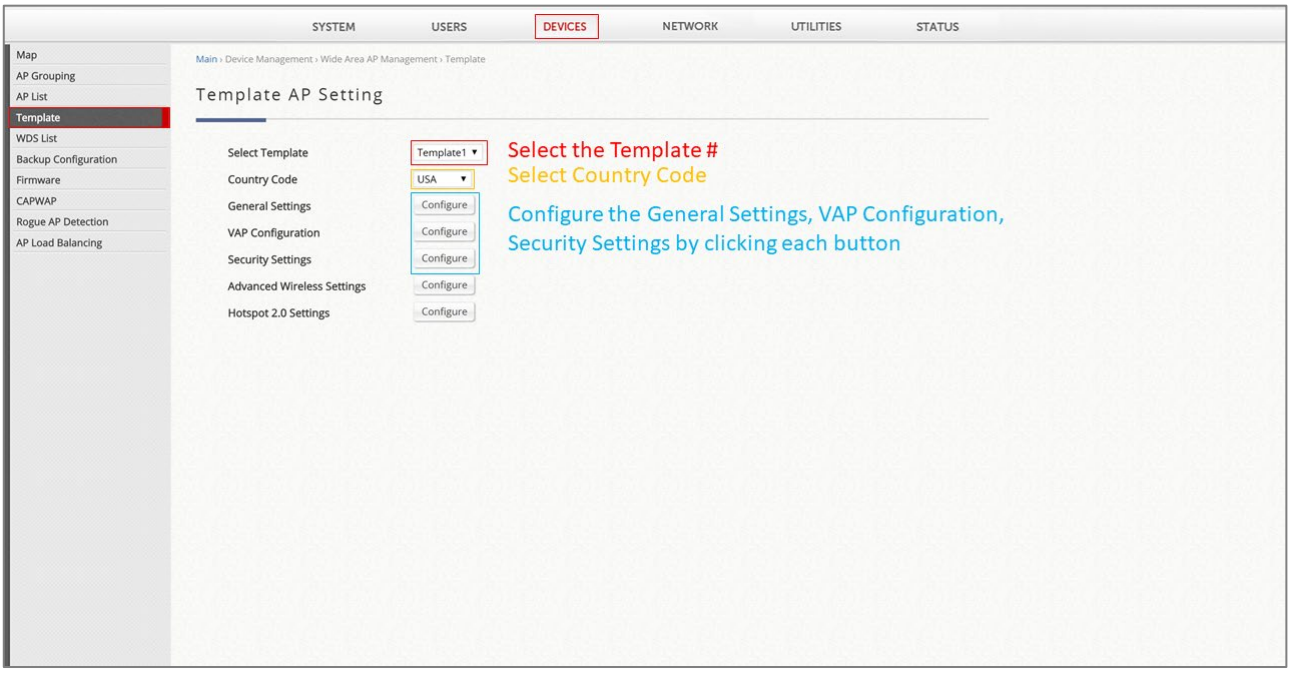
b. Go to CAPWAP to enable CAPWAP on the EWS. Certificates can be uploaded for establishing CAPWAP tunnels between the EWS and AP. The Control Channel IP Address should not be changed unless there is an IP conflict.



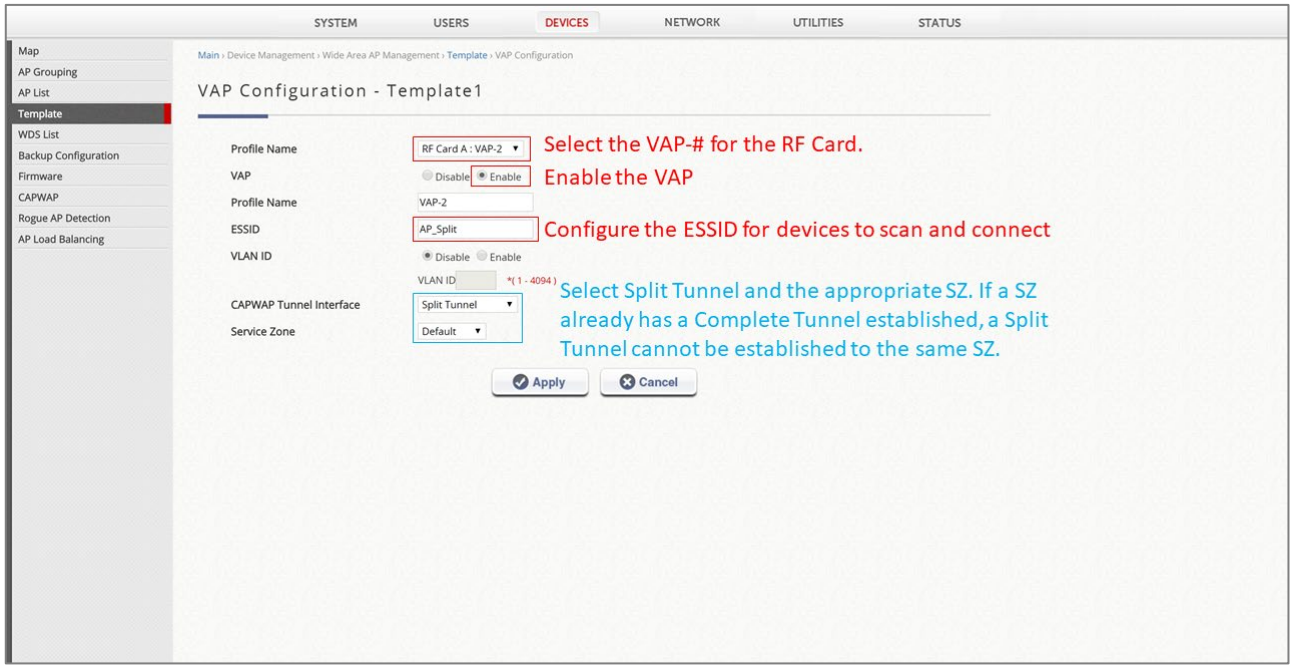
c. Configure the Template to be applied to Edgecore APs prior to adding the APs into WAPM. You may select the Template #, Country Code and begin configuring the General, VAP, Security settings of the AP.



d. Configure VAP Configuration to establish a Complete Tunnel to SZ1-Public in the SSID.
One 1 type of tunnel, Complete/Split, can be established per VAP.
The Service Zone selected will map all user traffic (Authentication and Data) to the selected Service Zone. The fixed VLAN is a private VLAN ID used for communication between the EWS and AP via the Complete Tunnel Interface.

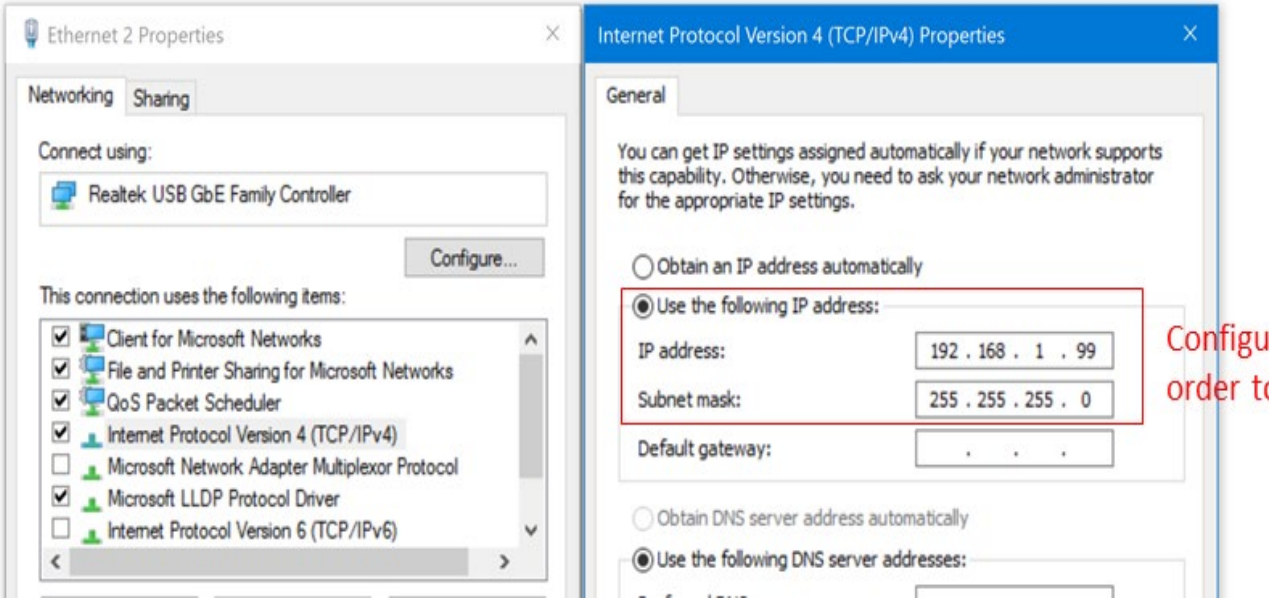


e. Split Tunnel can be configured by selecting Split Tunnel at the CAPWAP Tunnel Interface. If a Complete Tunnel is already established to SZ-Public, a Split Tunnel cannot be established to the same Service Zone. For Split Tunnels, a VLAN is not required.

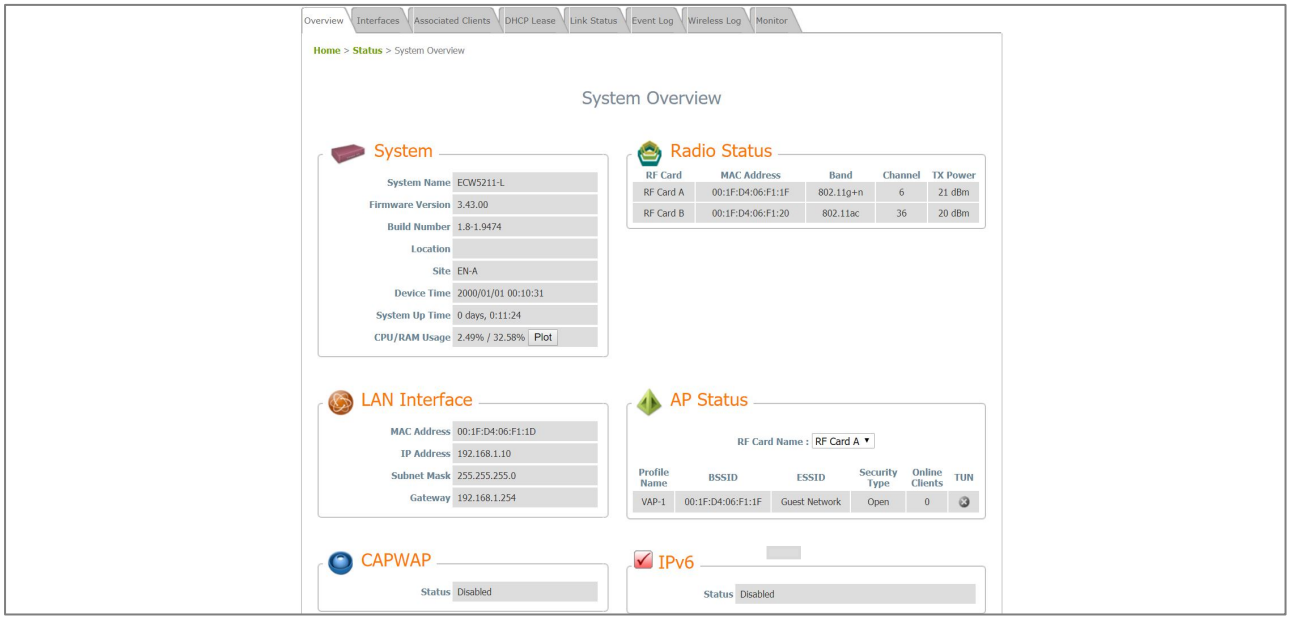


3.7.2 Devices - AP CAPWAP Configuration

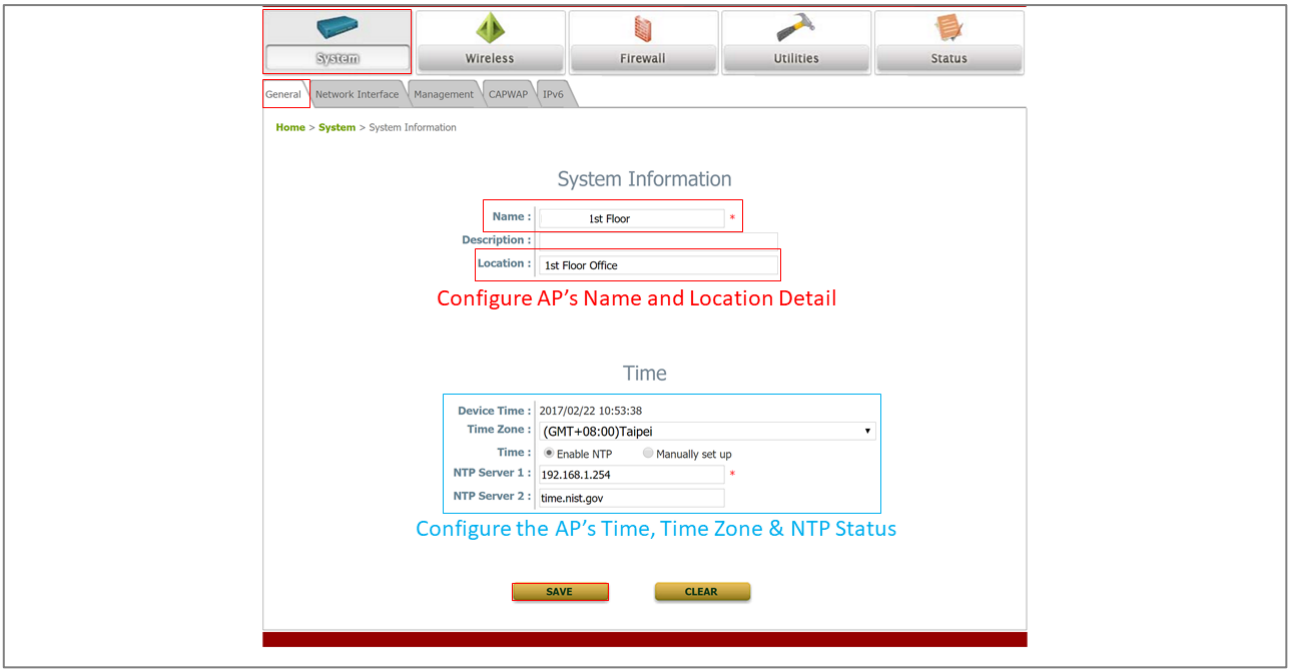
a. Connect to the Edgecore AP on the WAN side either through a switch or directly to the AP's uplink port via an Ethernet cable.



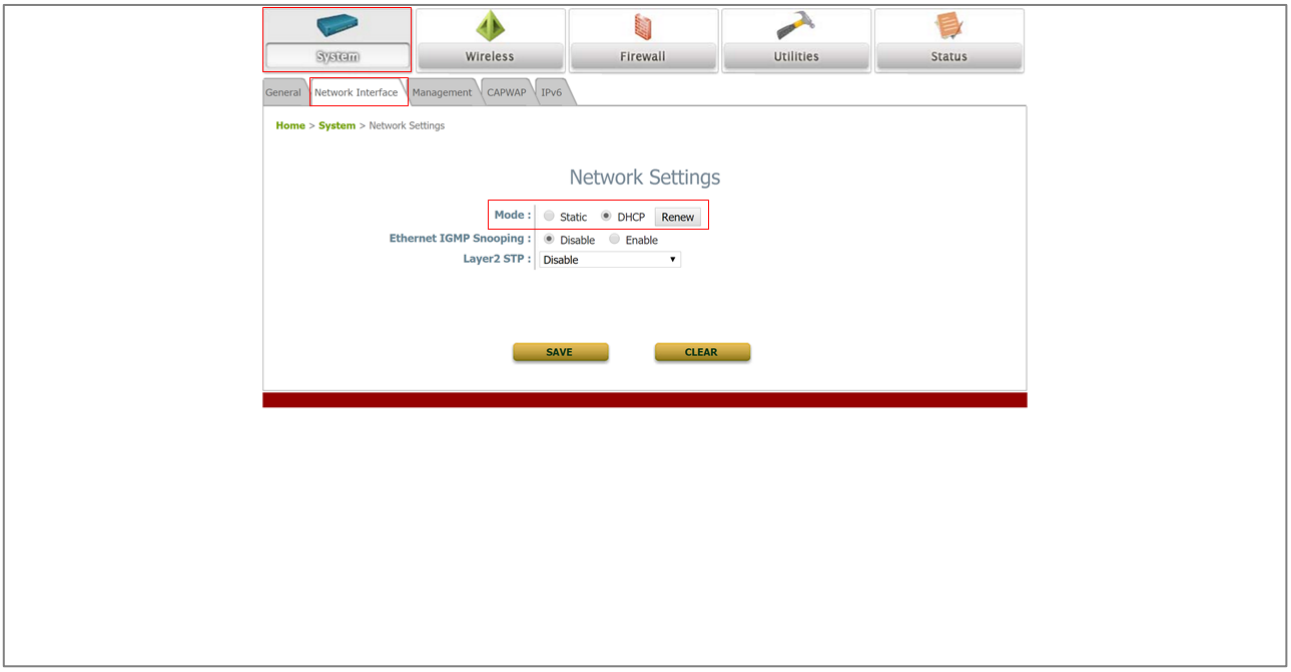
b. Enter the AP's WMI using the AP's Default IP Address: 192.168.1.1
The default AP login username/password is admin/admin. After logging in, you are redirected to the AP's System Overview Page.



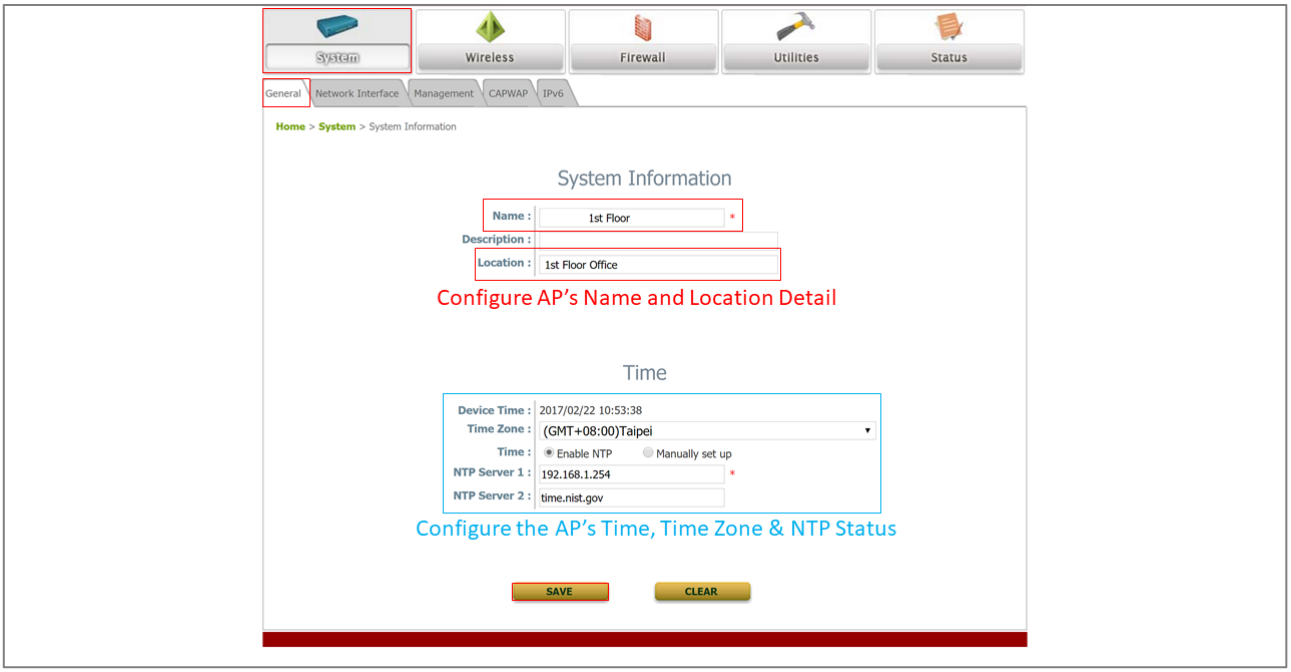
c. Go to System → General to configure the AP's Name and Time Zone.



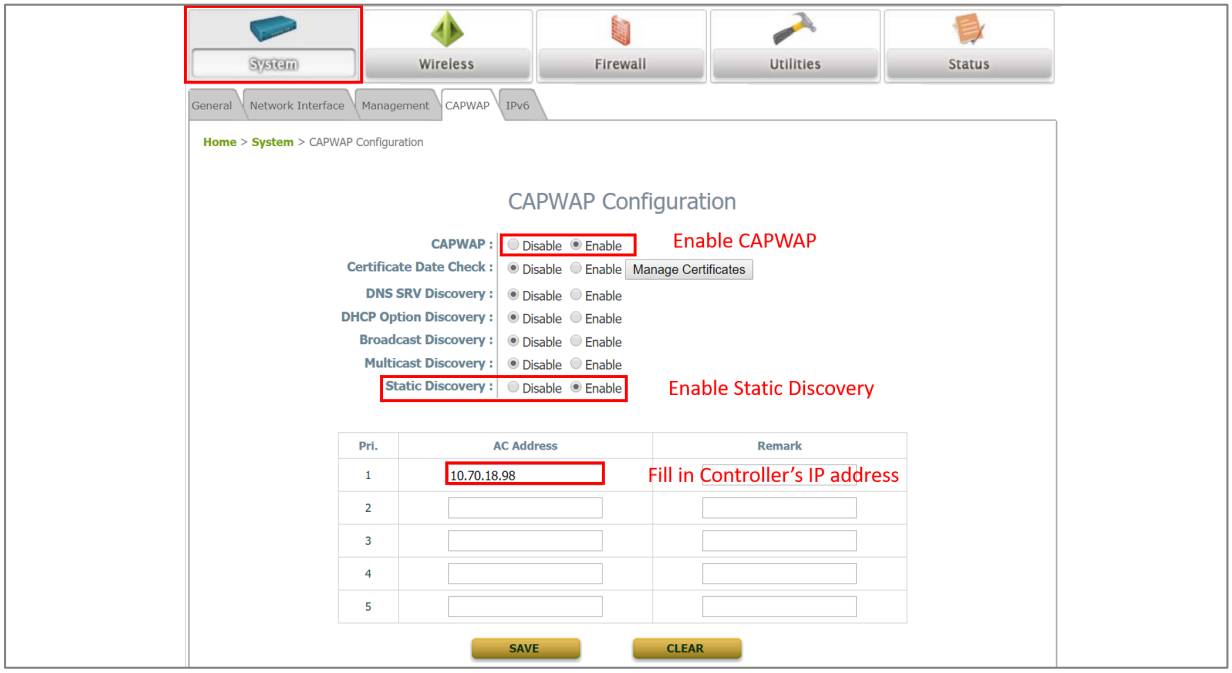
d. Go to System → Network Interface to configure the AP's Static or Dynamic IP Address. After Saving a new Network Setting, a reboot is required.



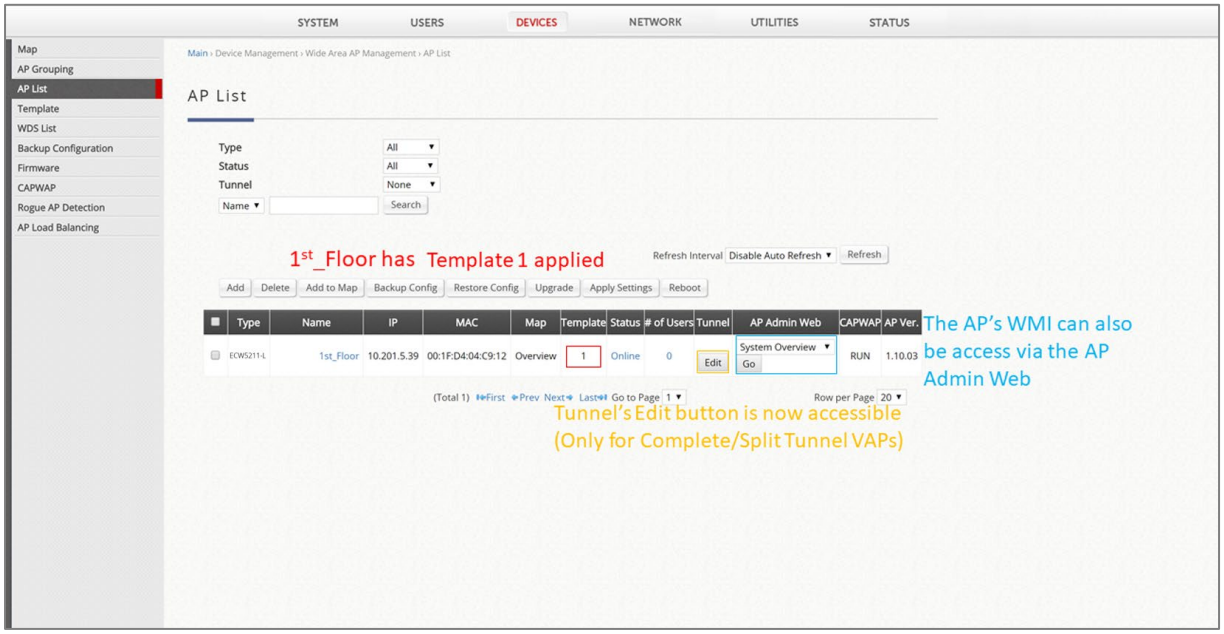
e. Confirm updated System Name, Time and LAN Interface after reboot.



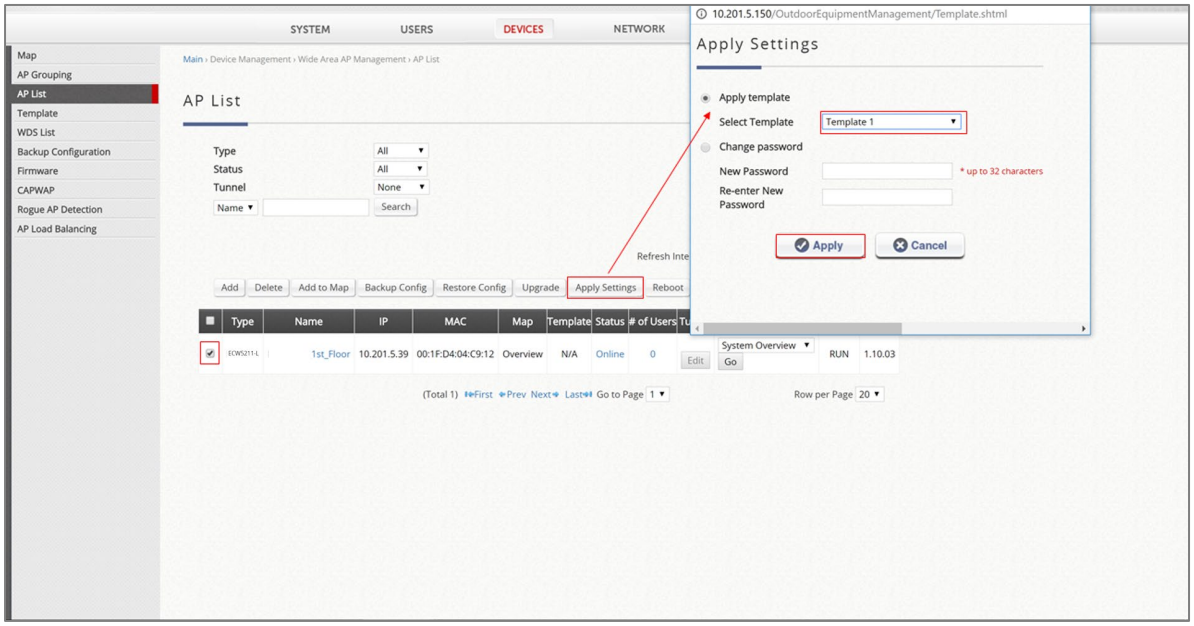
f. Go to System → CAPWAP to enable CAPWAP and select the appropriate Discovery Method. A reboot is required after saving the new CAPWAP configuration.
Note: Select Static Discovery if the EWS's WAN has a Static IP Address.
Select DNS SRV Discovery if the EWS's WAN has a valid Domain Name.
The following example shows using Static Discovery where the EWS's WAN IP is entered under AC Address.



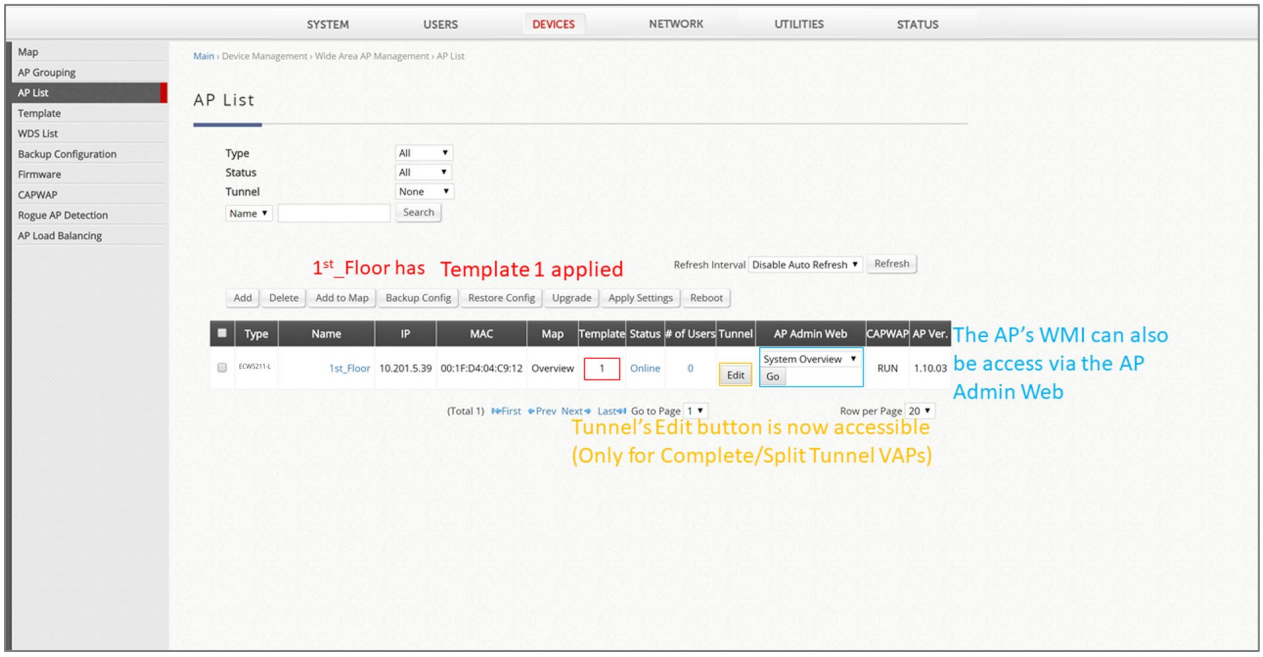
g. Go to Devices → WAPM → AP List to confirm if the AP is automatically added into the AP List. The CAPWAP Status displaying "Run" means the AP can be managed using the EWS and can be applied a Template.



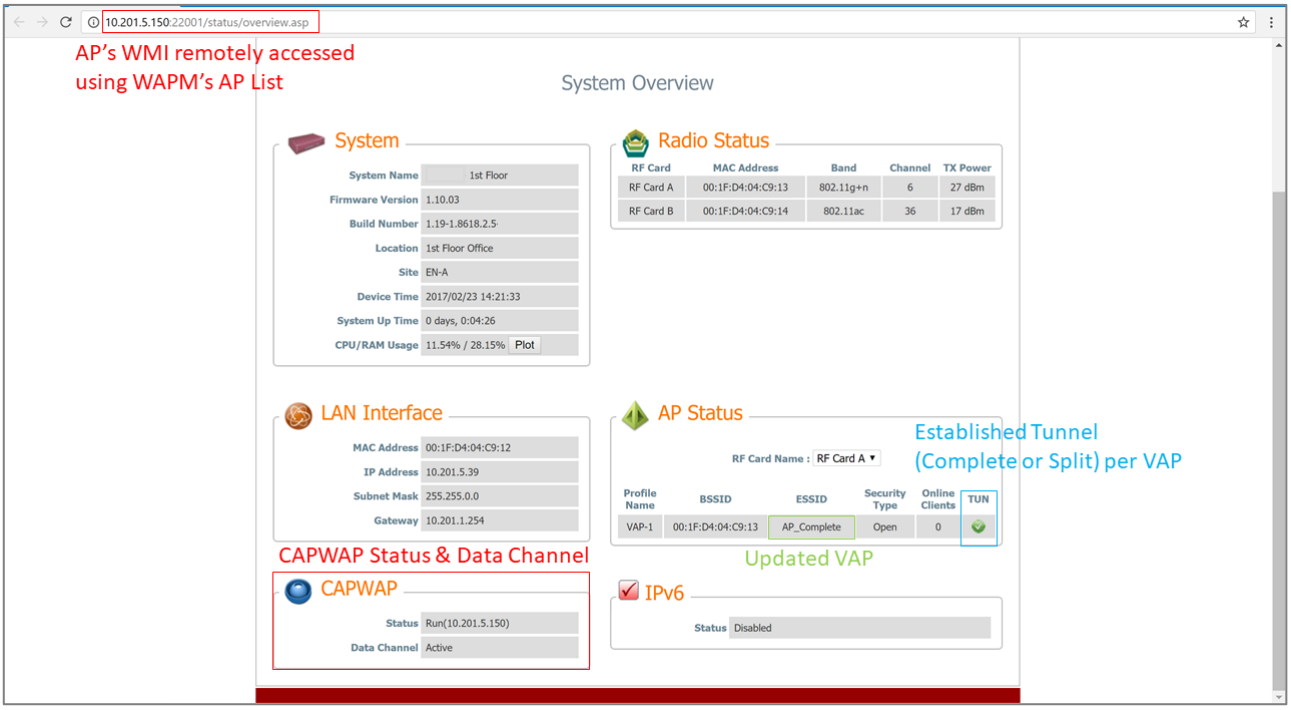
h. Check the AP's checkbox and click Apply Settings. Select the Template and Apply. The Status of the AP will change from Online → Applying.



i. Confirm AP's status after the Template is applied and the AP returns online. The "Go" button can also be used to enter the AP's WMI remotely.



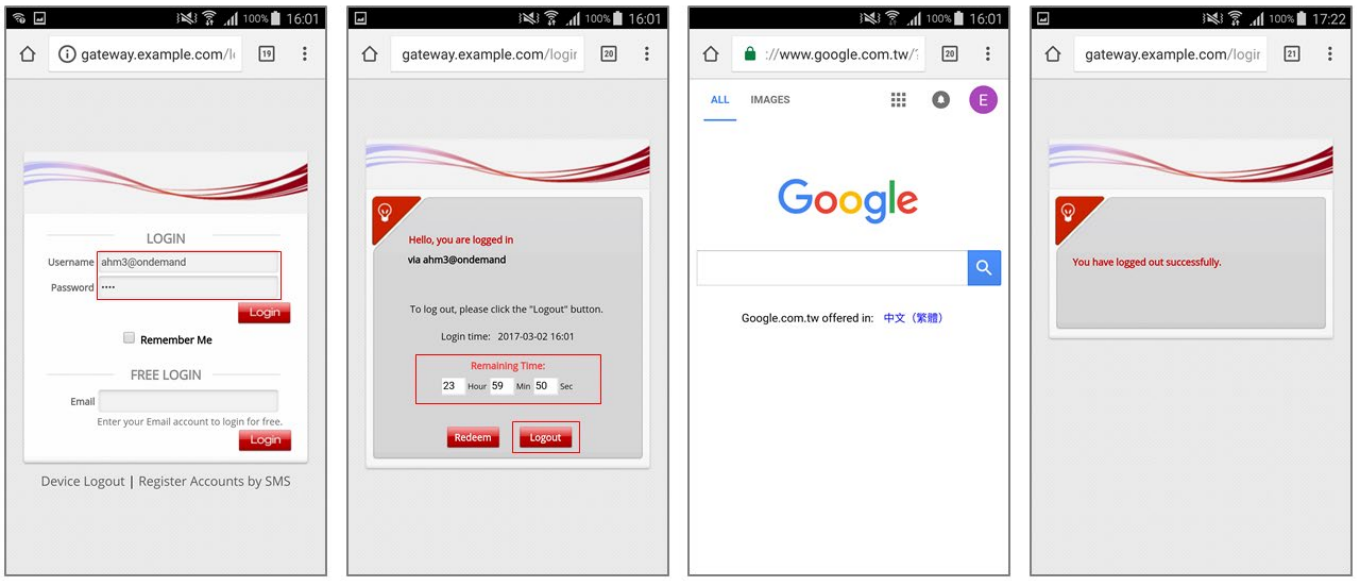
j. Confirm the AP's CAPWAP Tunnel Status by entering the AP's WMI using the AP Admin Web's Go button. The CAPWAP Status should show "Run (EWS IP)" and Data Channel as "Active". The VAP should also display a green checkmark under TUN.



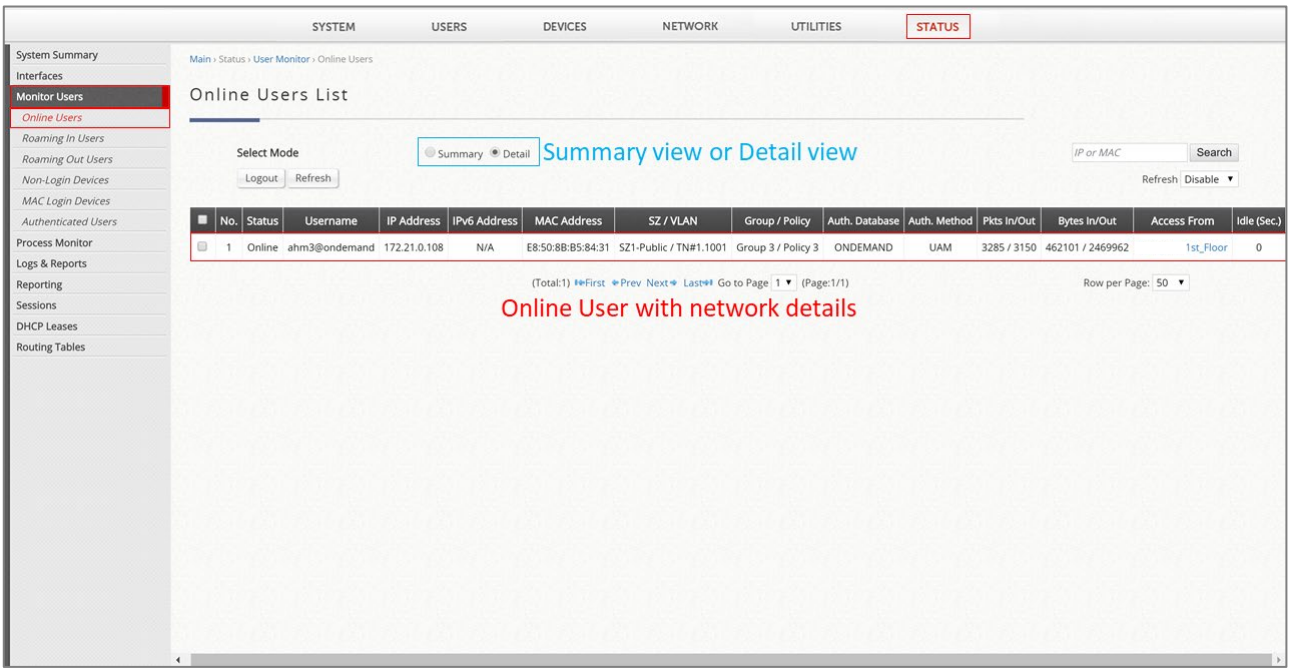
3.8 Client Login

3.8.1 Client Login - User Flow & Monitoring

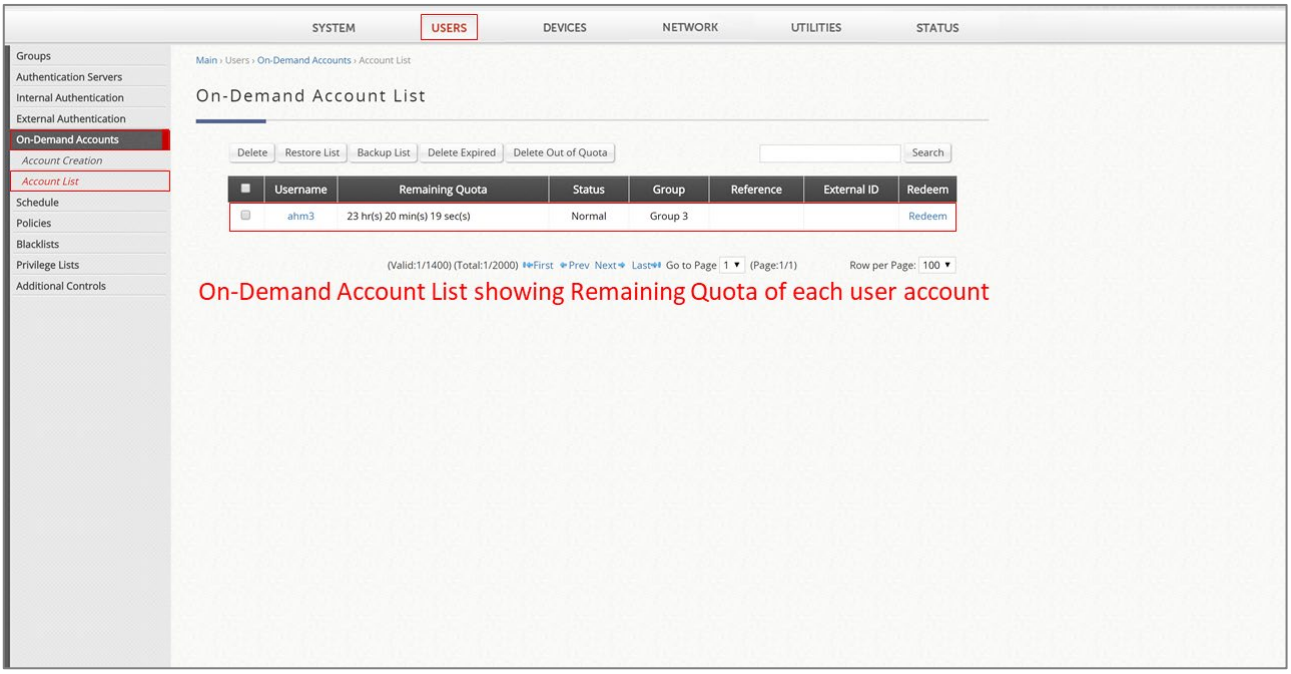
a. Client device associated with the SSID and logged in successfully through the browser. The user may proceed to surf the web or logout using the logout button on the successfully logged in page. If logged in with an On-Demand account, the login successful page will display the remaining quota.



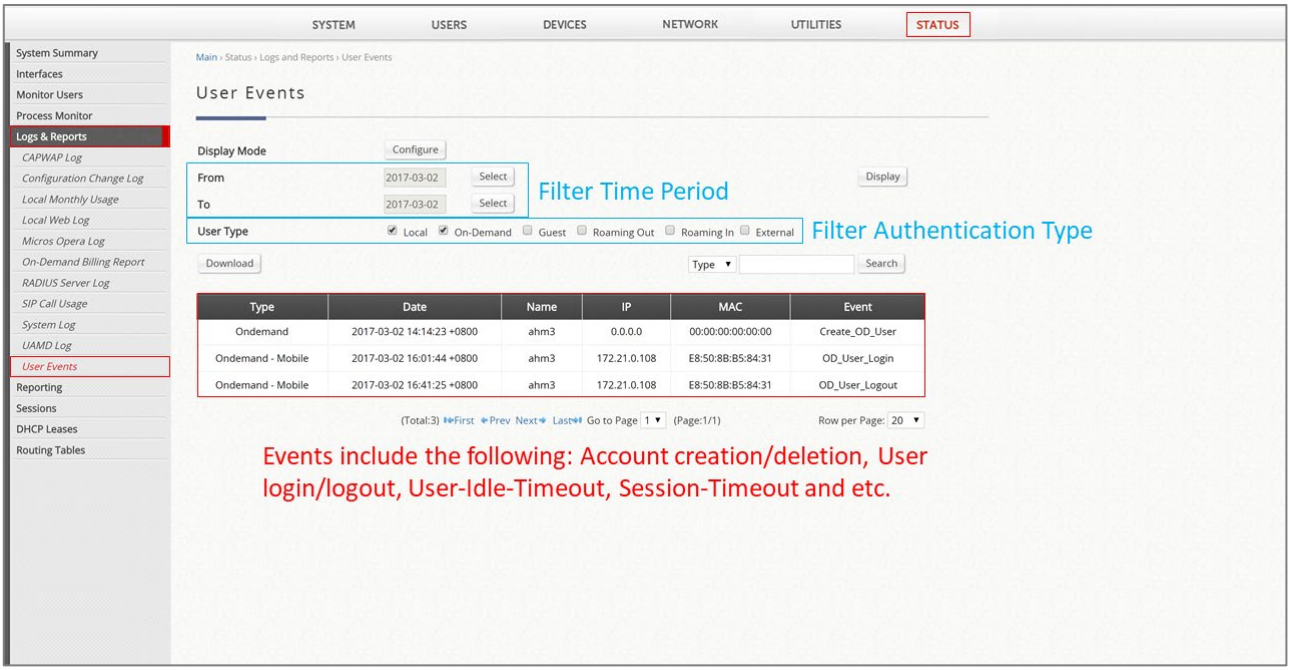
b. Go to Status → Monitor Users → Online Users to monitor online users and view details.



c. Go to Users → On-Demand Accounts → Account List to view On-Demand Accounts and their statuses.



d. Go to Status → Logs & Reports → User Events to monitor user's events.



4 Remarks

Please contact Edgecore's Technical Support Team at ecwifi@edge-core.com for additional inquiries.