



Technical Guide

Basic Configurations

Released: 2018-08-02

Copyright Notification

Edgecore Networks Corporation

© Copyright 2019 Edgecore Networks Corporation.

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

Table of Contents

1	Introduction	2
1.1	Pre-condition	2
1.2	Complete Tunnel Network Topology	2
1.3	Split Tunnel Network Topology	3
2	Configuration Flow Guideline	4
3	Configuration Steps	5
3.0	System - Initial Login	5
3.1	System - WAN & LAN Interface Configuration	5
3.2	Utilities - Admin Password Recovery	8
3.3	System	9
3.3.1	System - Service Zones Configuration	9
3.3.2	System - Service Zone – Captive Portal Customization	11
3.4	Users	13
3.4.1	Users - Local Accounts	13
3.4.2	Users - On-Demand Accounts	15
3.4.3	Users - Creating On-Demand Accounts	17
3.5	Users	19
3.5.1	Users - Policy Configuration	19
3.6	Users	24
3.6.1	Users - Group Configuration	24
3.7	Devices	25
3.7.1	Devices - WAPM – CAPWAP Tunnel	25
3.7.2	Devices - AP CAPWAP Configuration	27
3.8	Client Login	33
3.8.1	Client Login - User Flow & Monitoring	33
4	Remarks	34

1 Introduction

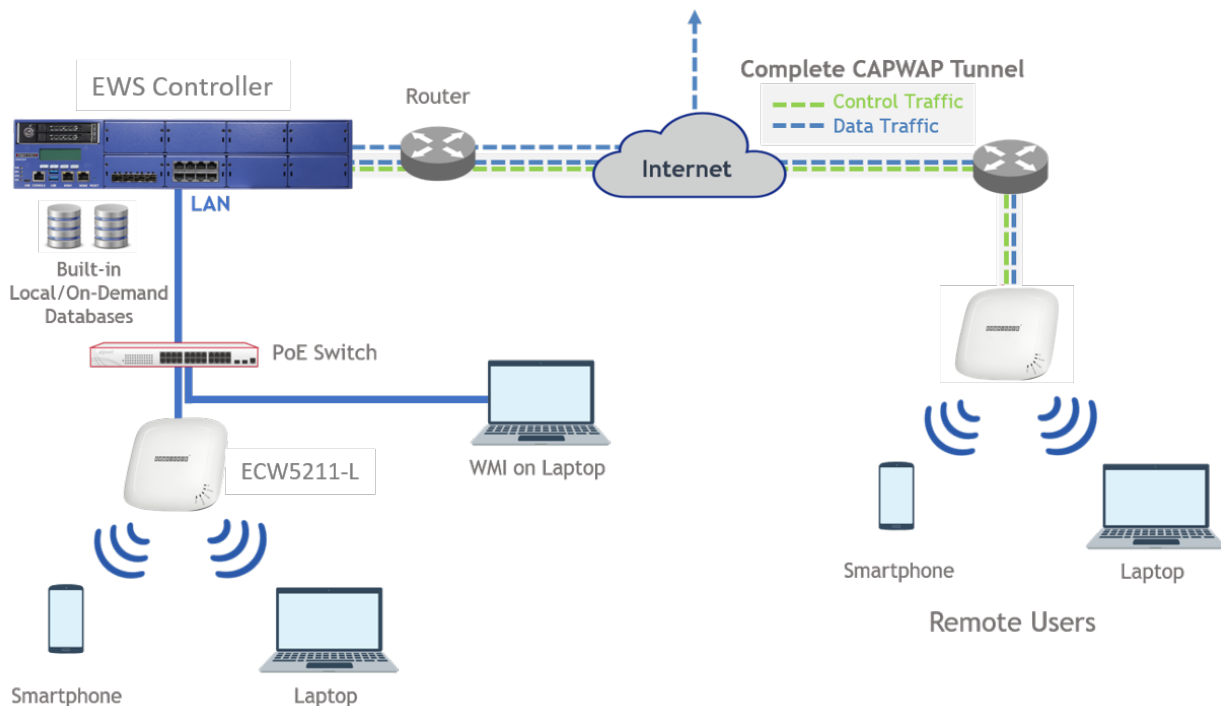
This guide will provide the basic configurations to quickly set up your own managed network. The guide highlights the minimum steps required for a wired or wireless network in each of the EWS controller's features; Service Zones, Authentication, Page Customization and User Policy Management and AP Management.

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

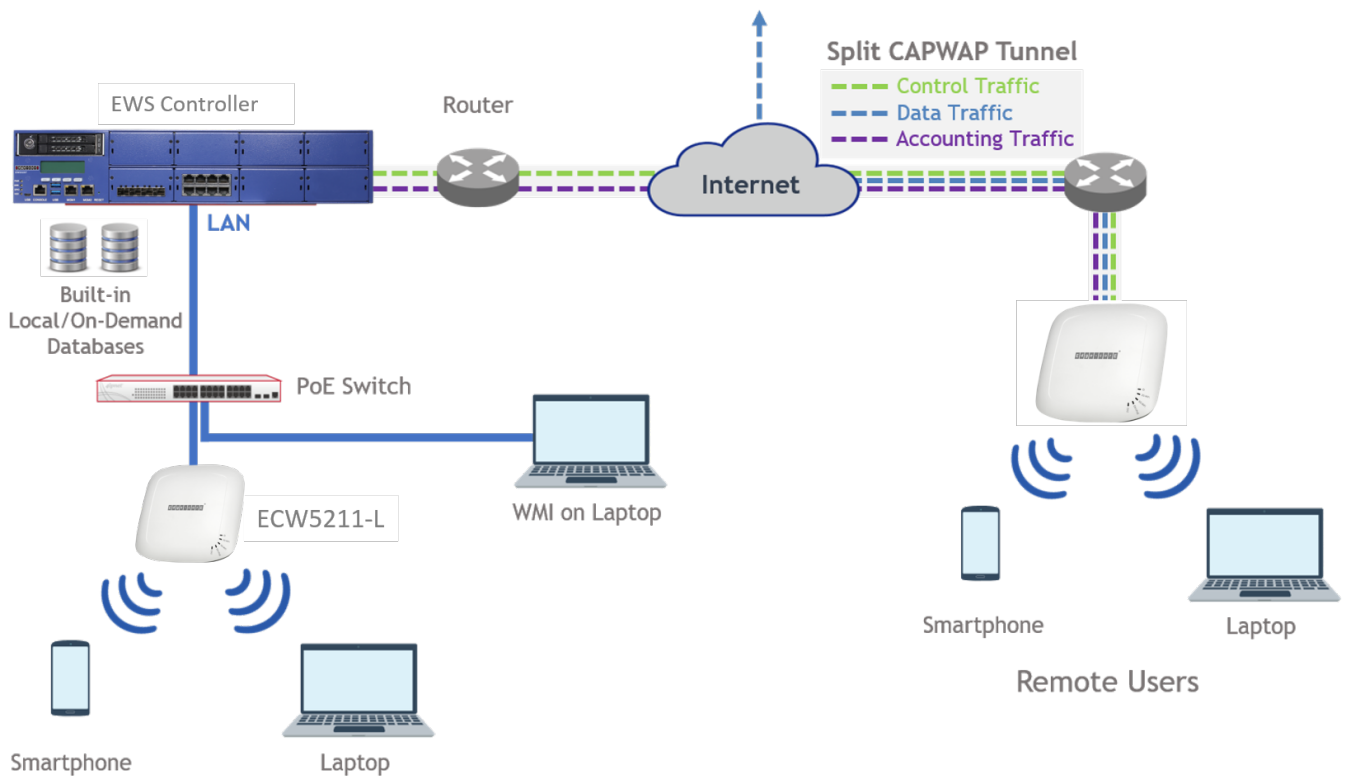
- a. Edgecore EWS controller is installed at the central site with uplink connected to WAN.
 - b. Edgecore AP is deployed locally under the layer 2 network or through the Layer 3 network at a remote site with internet connection at the uplink interface.
 - c. Confirm UDP ports 5246 & 5247 are open for 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

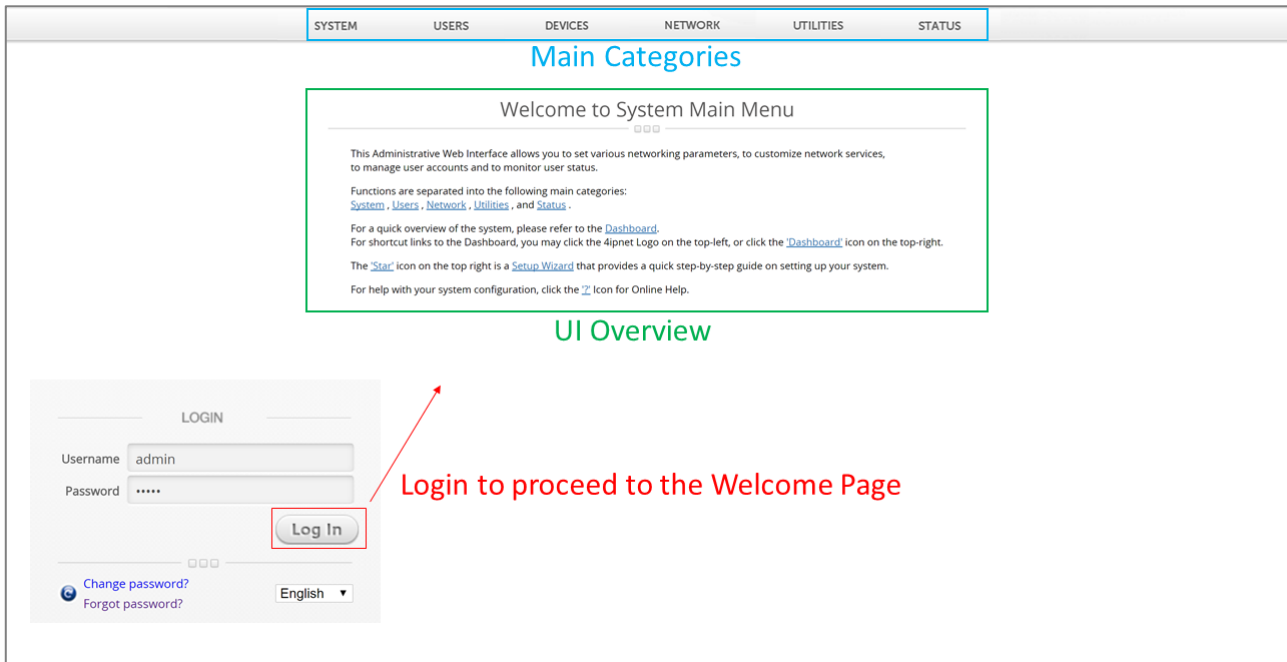
Below is a one-page step by step guideline for first time users in configuring the EWS.

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 Edgcore 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

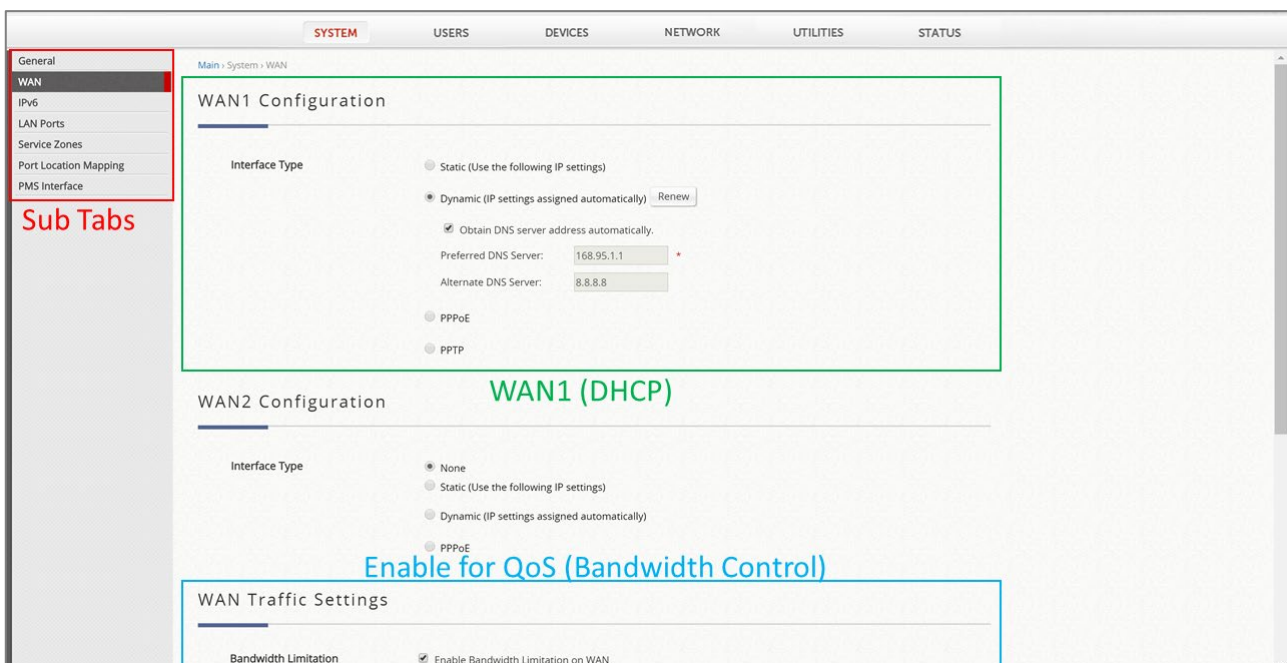
3.0 System - Initial Login

- 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.

The screenshot shows the Mikrotik WinBox interface for the WAN1 configuration page. The breadcrumb trail is Main > Status > Interfaces. A dropdown menu shows 'Select Interface: WAN1'. The main heading is 'WAN1 obtained IP Address'. Below this, a table displays the configuration for the WAN1 network interface:

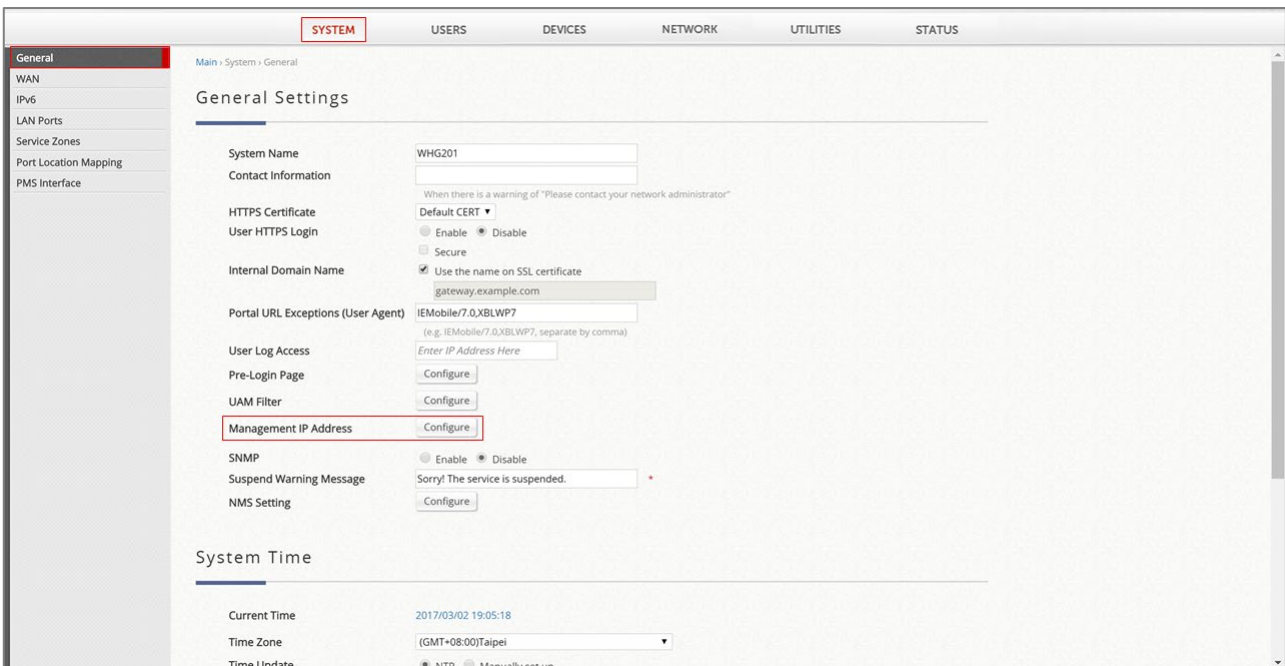
WAN1			
Mode	DHCP	IP Address	10.201.5.150
MAC Address	00:1F:D4:AB:C1:24	Subnet Mask	255.255.0.0
IPv6 Address	N/A	IPv6 Prefix	N/A

Below the configuration table, there is a 'Traffic Summary' section with three circular gauges for 'today', 'yesterday', and 'all time' traffic. To the right is a bar chart showing traffic over the last 30 days. Further down, there are two tables: 'Daily Traffic' and 'Monthly Traffic'. The 'Daily Traffic' table shows data for each day from 01/23/17 to 02/09/17. The 'Monthly Traffic' table shows data for the months of April '13, Jan '17, and Feb '17, along with an estimated total for the current month.

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

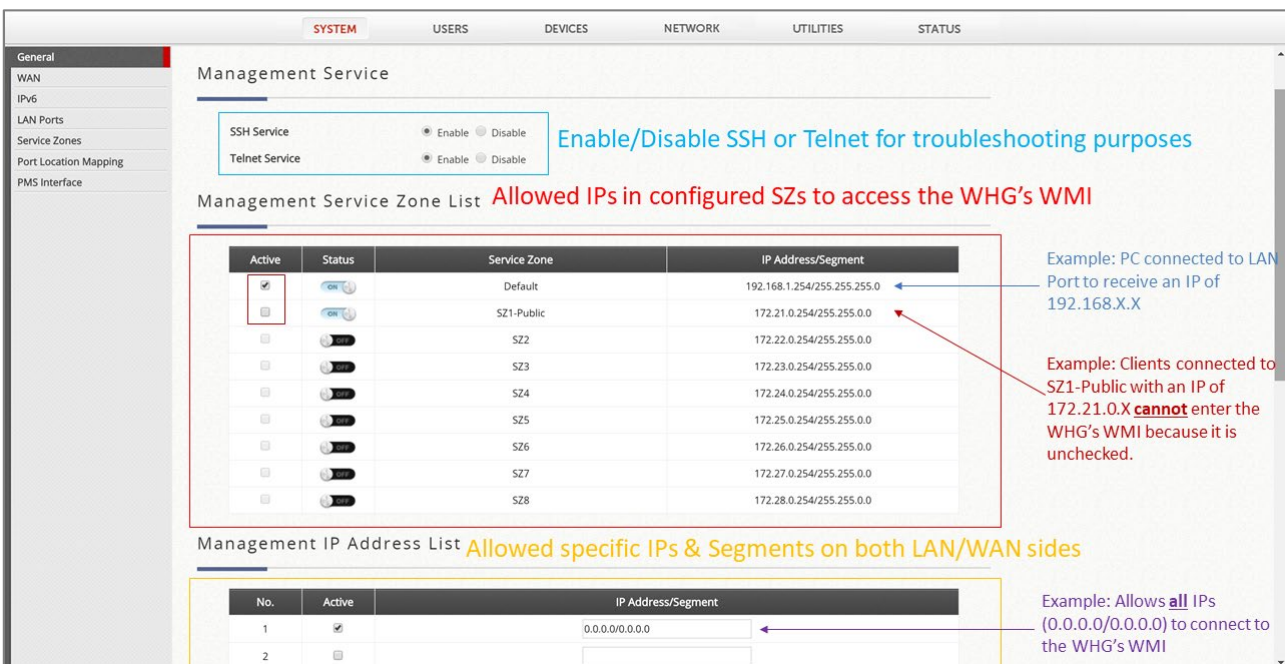
The screenshot shows the Mikrotik WinBox interface for the LAN Ports configuration page. The breadcrumb trail is Main > System > LAN Ports. The page title is 'Port Assignment'. Under 'Port 2 Role', the 'LAN1' radio button is selected. The 'LAN Port Mode' section has 'Tag-Based' selected. Below this, there is a note: 'When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.' The 'Port - Service Zone Mapping' section shows four LAN ports (LAN1, LAN2, LAN3, LAN4) each with a 'Default' dropdown menu. At the bottom, there are 'Apply' and 'Cancel' buttons.

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



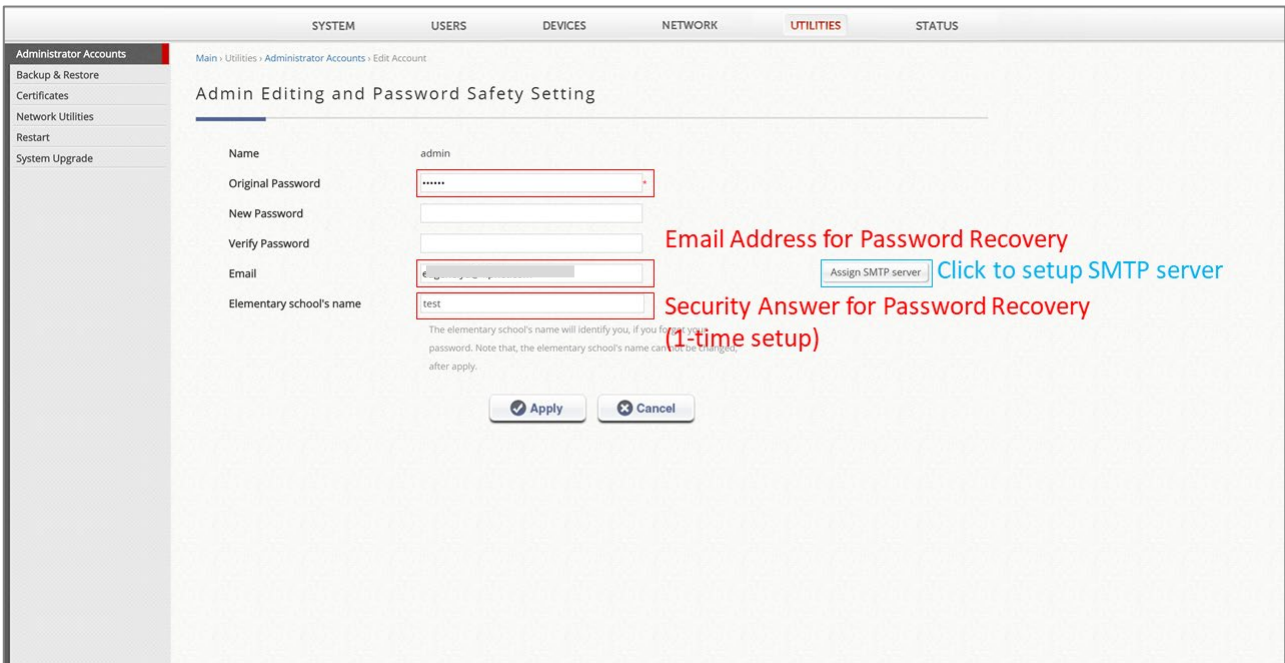
e. Check the appropriate SZs and configure the preferred IP Addresses to allow access to the Web Management Interface.

❖ *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.*

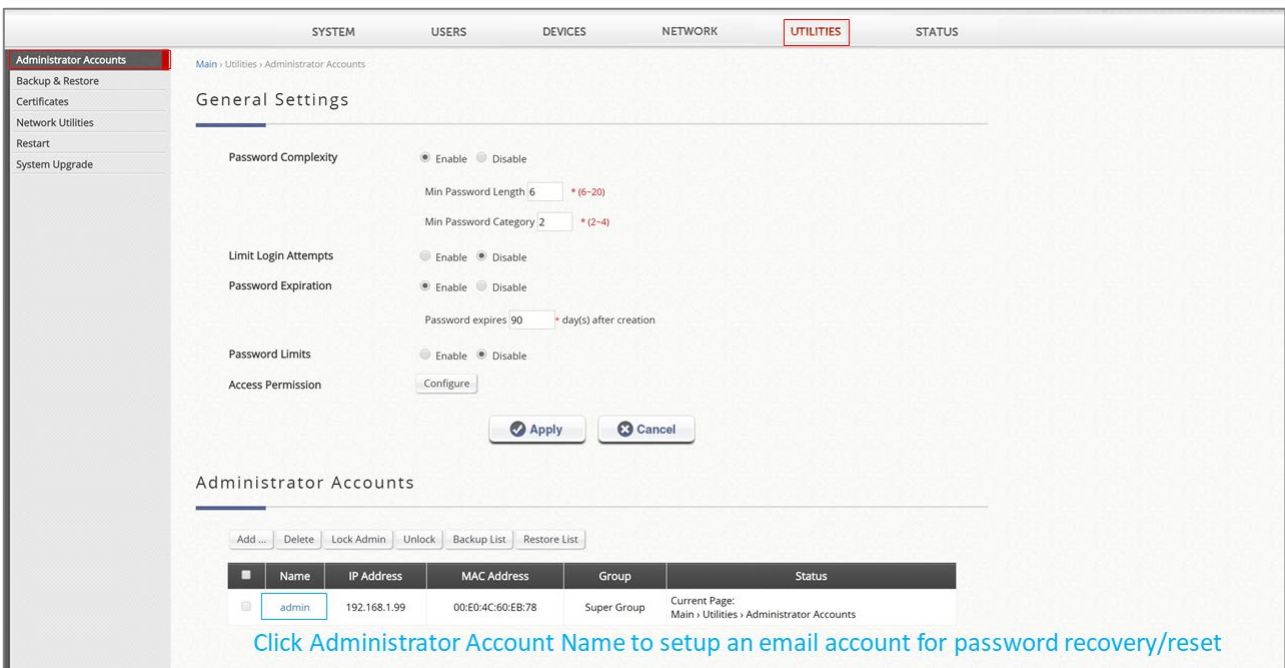


3.2 Utilities - Admin Password Recovery

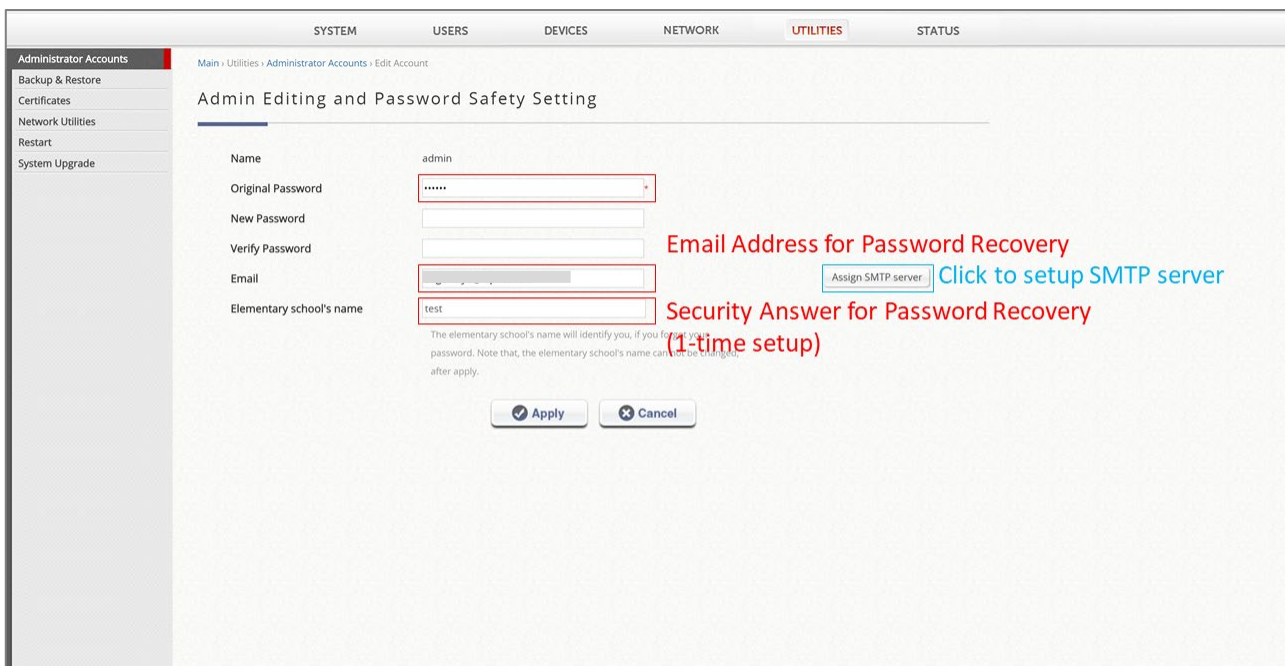
- a. Go to Utilities → Administrator Accounts and click the “admin” Name to configure password recovery.



- 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.

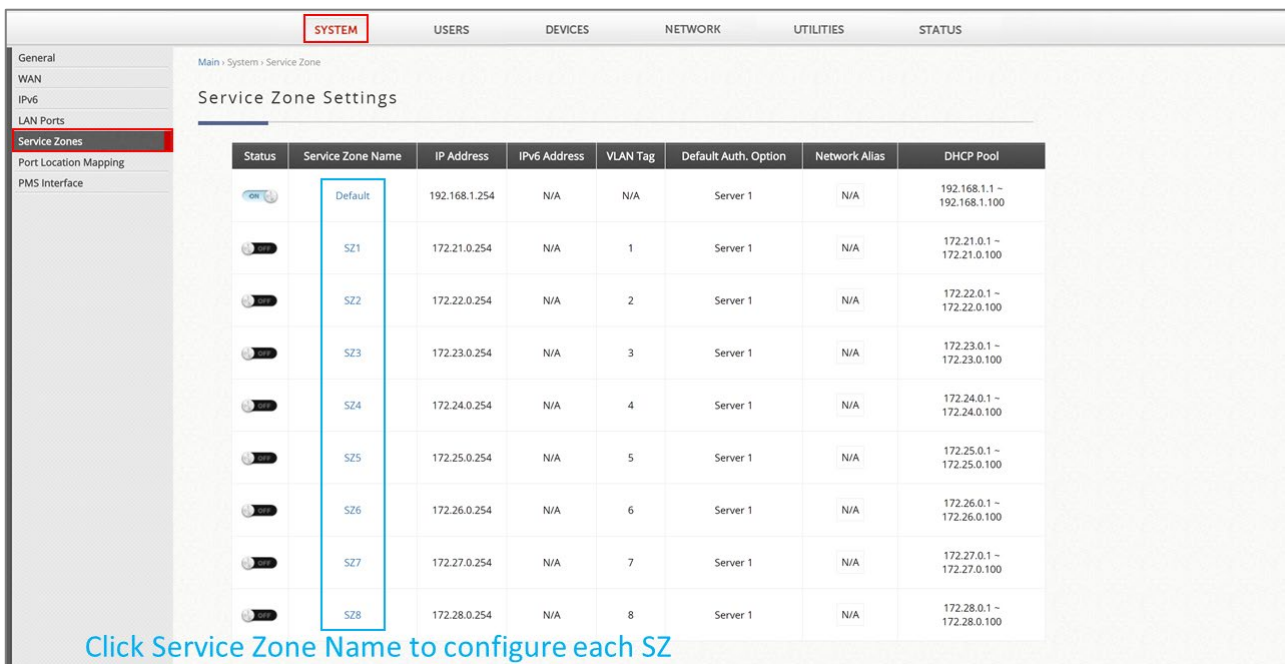


3.3 System

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.

Basic Settings

Service Zone Status: Enabled Disabled

Service Zone Name: **You may rename the SZ Name Change the VLAN Tag**

Network Interface: (Range: 1 - 4094)

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

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

Operation Mode: NAT Router

IP Address: **Configure preferred IP**

Network Alias List:

DHCP: Enabled **Configure DHCP Server**

Assigned IP Address for AP Management

IP Range: Start IP Address End IP Address

Authentication Settings

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

Authentication Settings

Authentication: Enable Disable Suspend **Enable/Disable Authentication on this Service Zone**

Access Permission and Authorization:

Default Policy: Policy 1

Portal URL: Specific Original None **Portal URL opens specified URL after user is authenticated**

MAC Authentication: Enabled Disabled

PPP Authentication: Enabled Disabled

SIP Interface Configuration: Enabled Disabled

WISPr Settings:

Authentication Options:

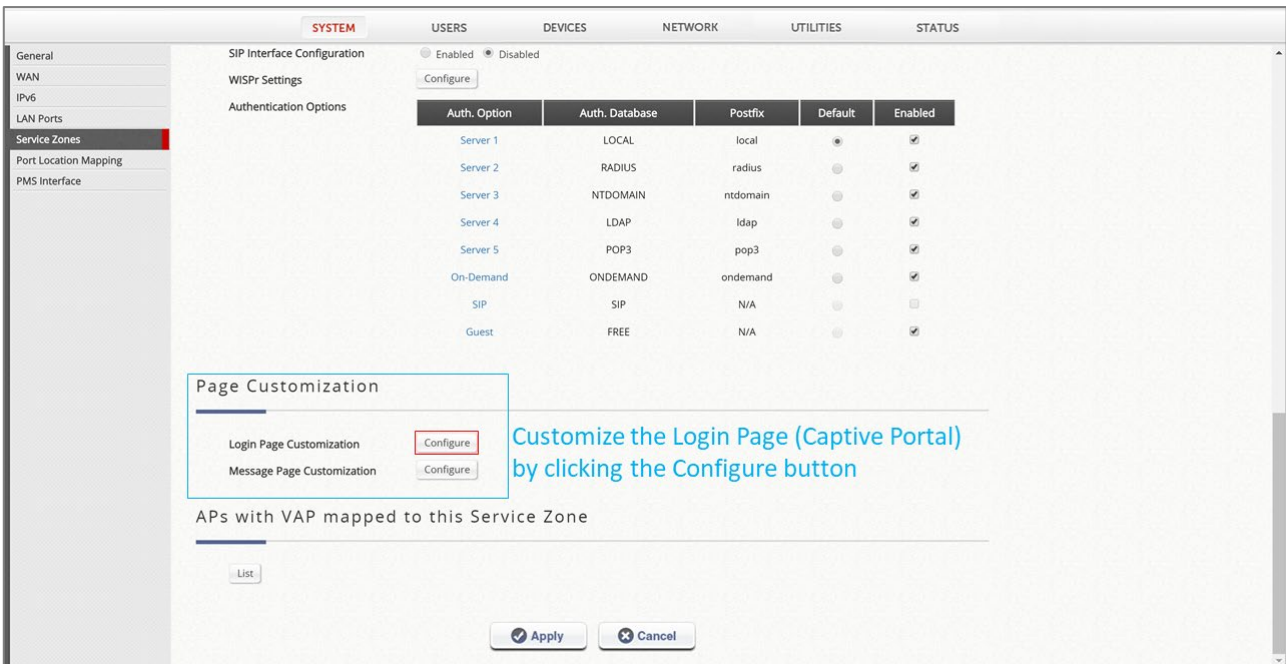
Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>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

Confirm Authentication Databases allowed in this Service Zone

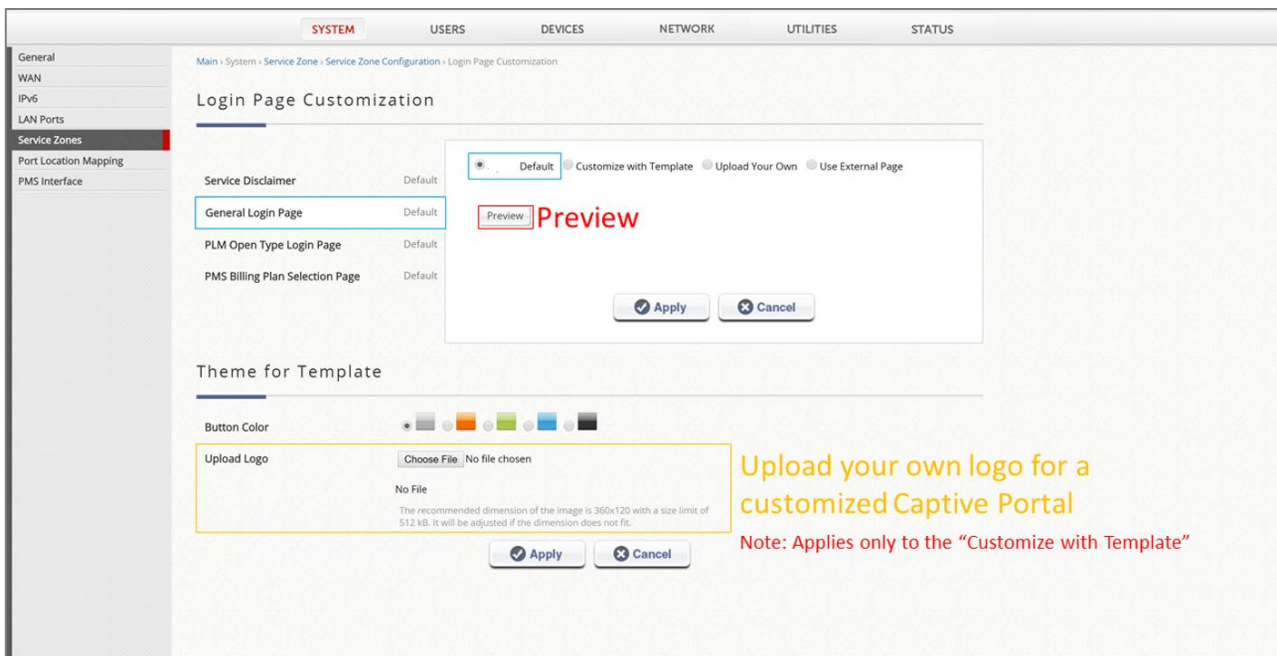
← Enable Guest (Free Access Database)

3.3.2 System - Service Zone – Captive Portal Customization

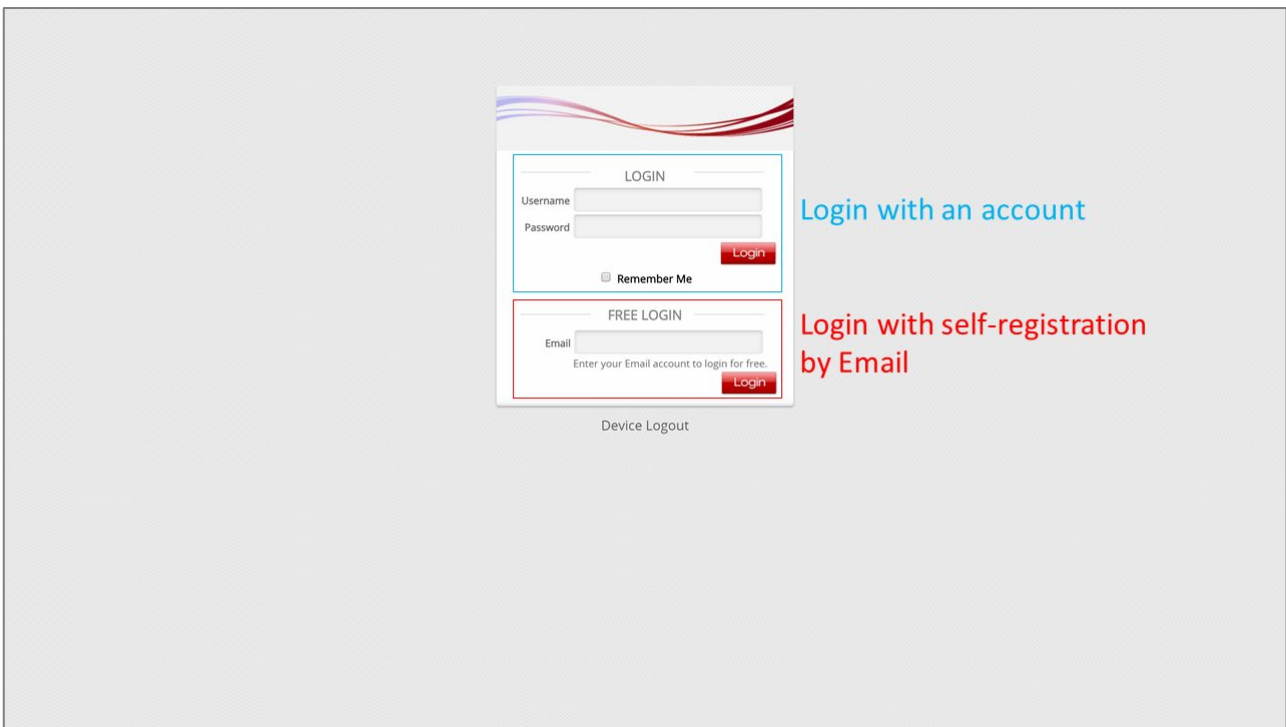
- a. Click configure to customize different Login Page Customization. Message Page Customization will provide customizations to message pages such as the login success page.



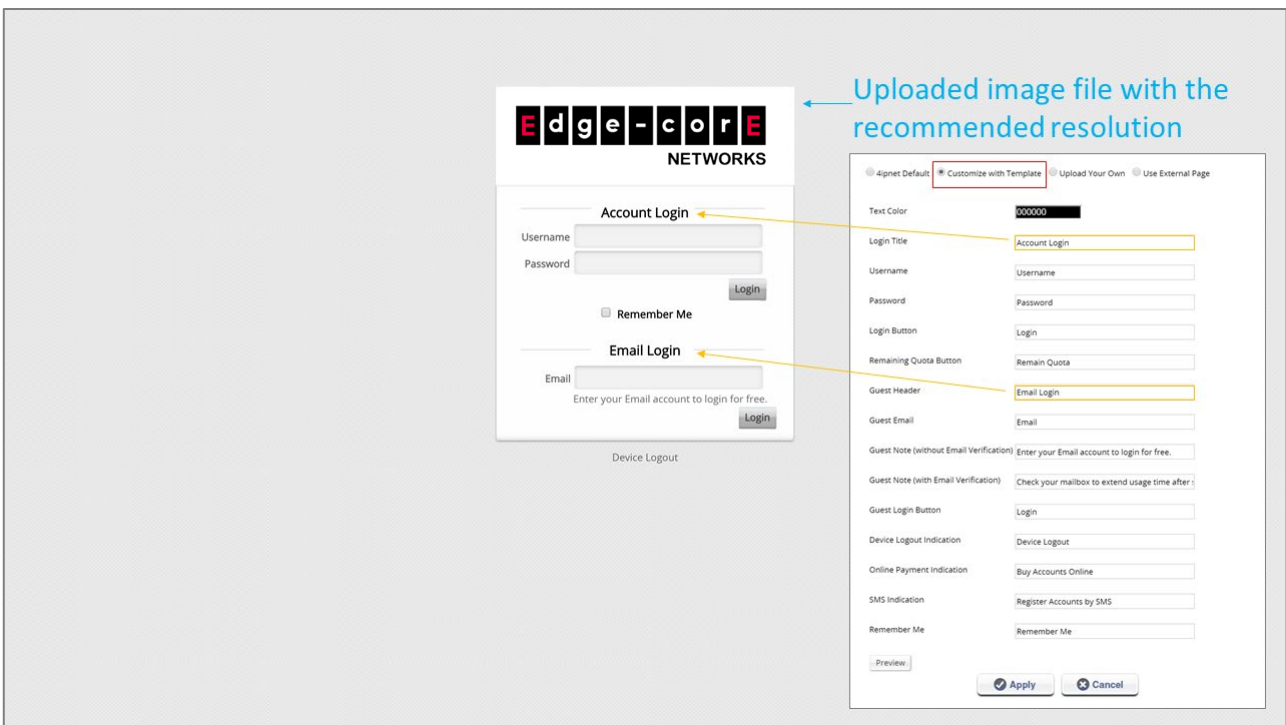
- b. Click configure to customize different Login Page Customization. Message Page Customization will provide customizations to message pages such as the login success page.



c. Preview General Login Page in Default mode.



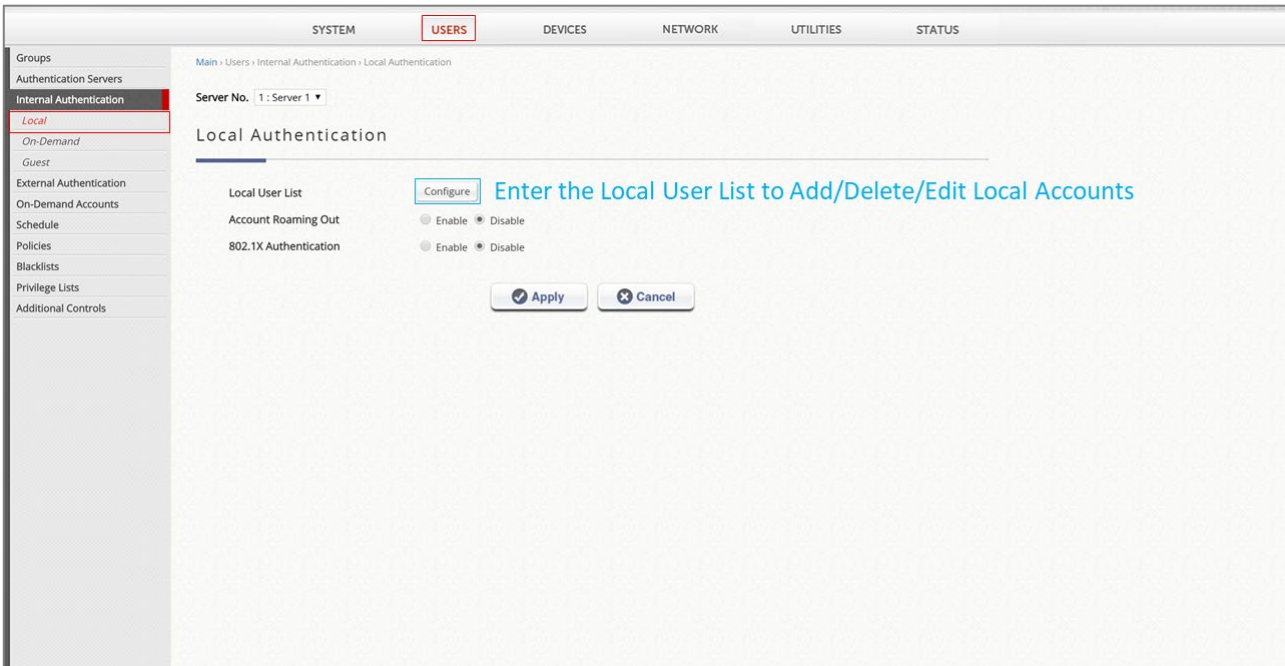
d. Preview General Login Page in Customize with Template selection with an uploaded logo and customized text.



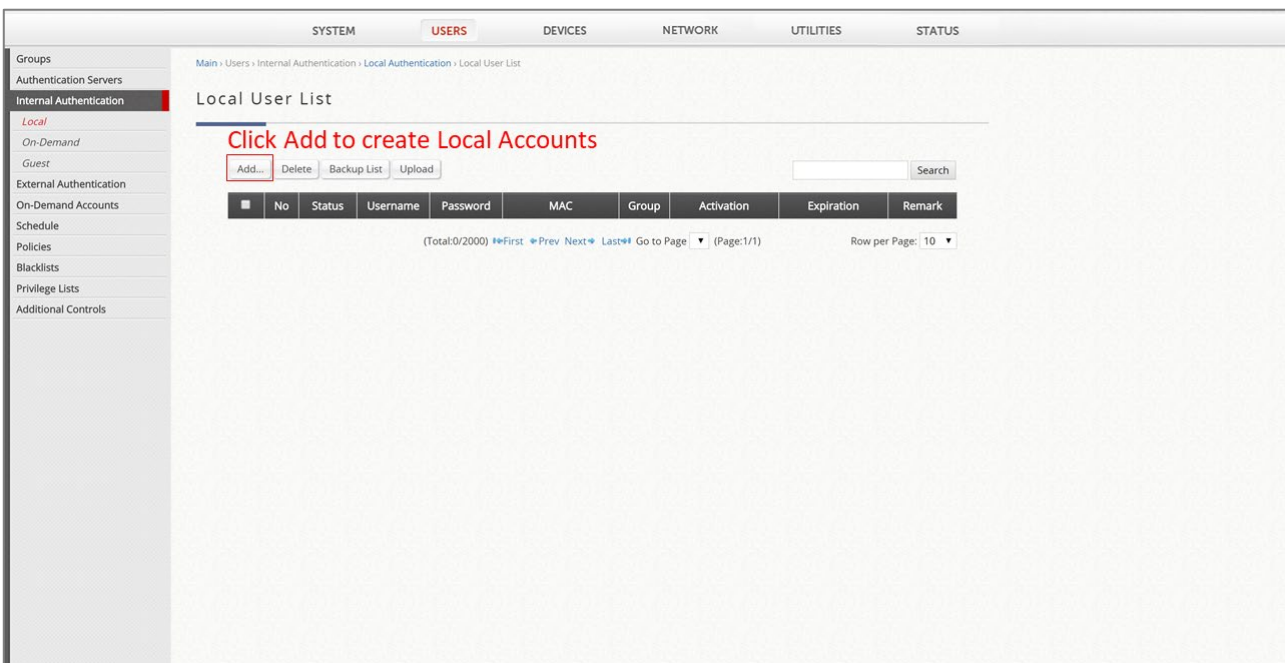
3.4 Users

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)

2000 users can be added to this local user list.

Optionally bind MACs to Local Accounts

Optionally configure Account Span

Optionally add a remark

Fill in Username & Password pairs

Categorize into User Groups

Username	Password	MAC Address	Group	Account Span	Remark
test1		Group 1	<input type="checkbox"/>	
test2		Group 2	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	

Apply Cancel

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

Local User List

Add... Delete Backup List Upload Search

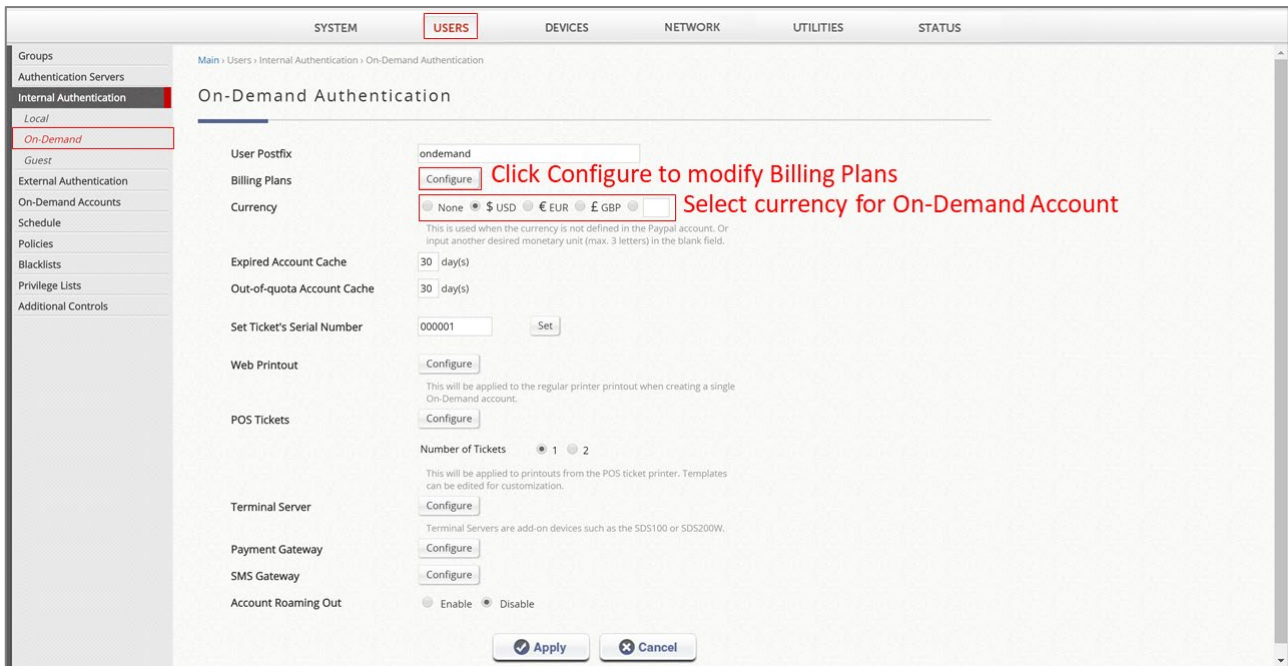
No	Status	Username	Password	MAC	Group	Activation	Expiration	Remark
1	Valid	test1	test1		Group 1			
2	Valid	test2	test2		Group 2			

(Total:2/2000) First Prev Next Last Go to Page: 1 (Page:1/1) Row per Page: 10

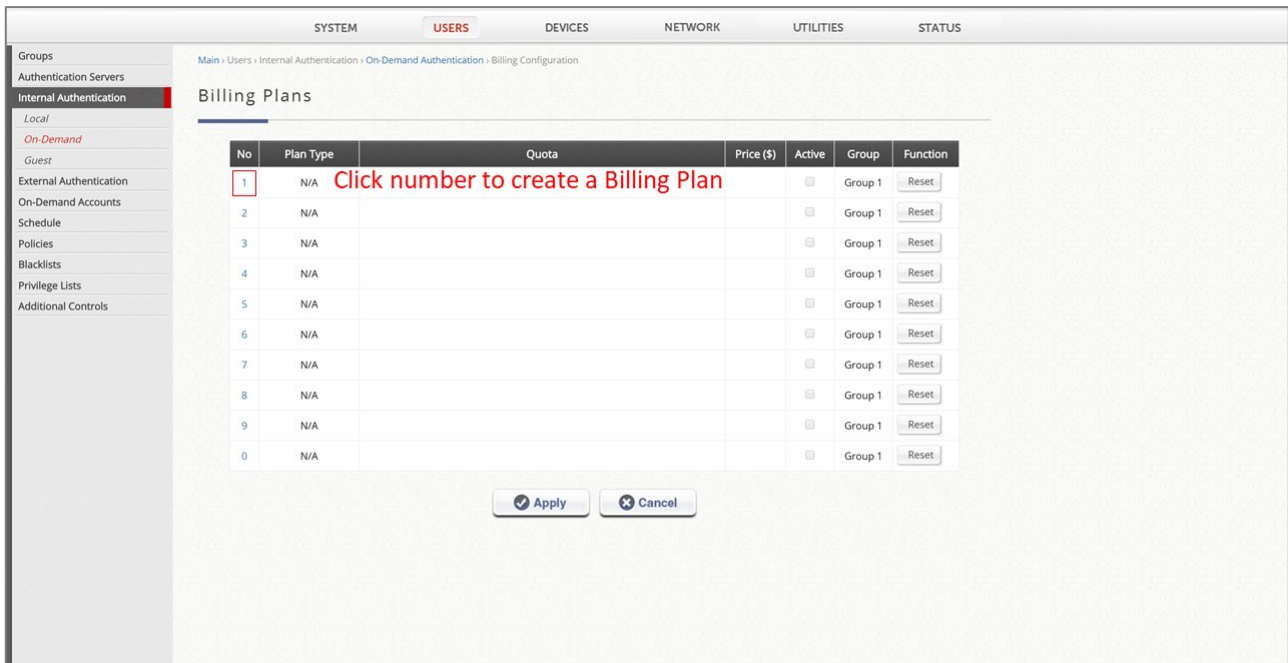
User List available for Add/Delete/Edit/Backup/Restore

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.

No	Plan Type	Quota	Price (\$)	Active	Group	Function
1	Usage-time	1 day(s) of usage time and expired in 7 days)	1	<input checked="" type="checkbox"/>	Group 3	Reset
2	N/A			<input type="checkbox"/>	Group 1	Reset
3	N/A			<input type="checkbox"/>	Group 1	Reset
4	N/A			<input type="checkbox"/>	Group 1	Reset
5	N/A			<input type="checkbox"/>	Group 1	Reset
6	N/A			<input type="checkbox"/>	Group 1	Reset
7	N/A			<input type="checkbox"/>	Group 1	Reset
8	N/A			<input type="checkbox"/>	Group 1	Reset
9	N/A			<input type="checkbox"/>	Group 1	Reset
0	N/A			<input type="checkbox"/>	Group 1	Reset

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.

The screenshot shows the 'On-Demand Account Creation' interface. A table lists various plans, with the first row selected. A modal window is open for creating a new account, showing fields for Plan, Quota, Account Creation (System/Manual), Length of password, Valid Period, Total Price, Unit, Group, Reference, and External ID. A 'Create' button is highlighted at the bottom of the modal.

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

The screenshot shows the 'On-demand User Receipt' window. It displays account details in a table format, including Username (ahm3@ondemand), Password (ra7z), Plan, Quota, Unit, Total Price, Max User, Reference, and External ID. The receipt also includes a welcome message, a thank you message, and printing options (Send to Pos, Printout, Close).

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

The screenshot shows a web-based management console with a navigation menu on the left and a main content area. The navigation menu includes 'Groups', 'Authentication Servers', 'Internal Authentication', 'External Authentication', 'On-Demand Accounts', 'Account Creation', 'Account List', 'Schedule', 'Policies', 'Blacklists', 'Privilege Lists', and 'Additional Controls'. The 'Account List' item is highlighted with a red box. The main content area has a breadcrumb trail: 'Main > Users > On-Demand Accounts > Account List'. Below this, the title 'On-Demand Account List' is displayed. Underneath the title, there is a section for 'Available Actions' with buttons for 'Delete', 'Restore List', 'Backup List', 'Delete Expired', and 'Delete Out of Quota'. A search box is also present. Below the actions, a table lists the account details:

Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
ahm3	1 day(s)	Normal	Group 3			Redeem

Below the table, there is a section for 'On-Demand Account Info List' with pagination controls: '(Valid:1/1400) (Total:1/2000) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 100'.

3.5 Users

3.5.1 Users - Policy Configuration

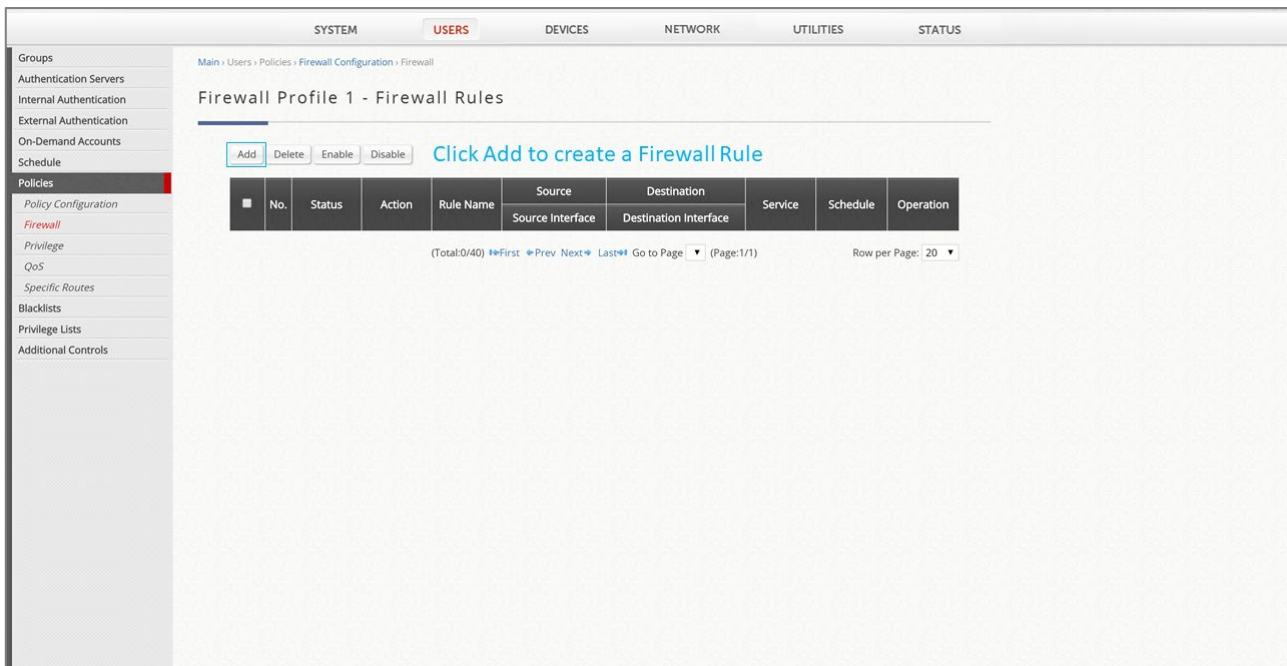
- a. Configure and select Firewall Profile, Privilege Profile, QoS Profile and Specific Route Profile to create Policy 1.

The screenshot shows the 'Policy Configuration' page under the 'USERS' tab. The breadcrumb trail is 'Main > Users > Policies > Policy Configuration'. A dropdown menu for 'Select Policy' is set to 'Policy 1'. A red box highlights this dropdown with the text 'Select Policy to configure'. Below this, a form titled 'Policy Configuration' contains several fields: 'Policy Name' (Policy 1), 'Firewall Profile' (Firewall 1), 'Privilege Profile' (Privilege 1), 'QoS Profile' (QoS 1), 'Specific Route Profile' (Specific Route 1), and 'Prefer DHCP Pool' (None). A blue box highlights the 'Firewall Profile', 'Privilege Profile', and 'QoS Profile' fields with the text 'Choose mapped Profiles'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

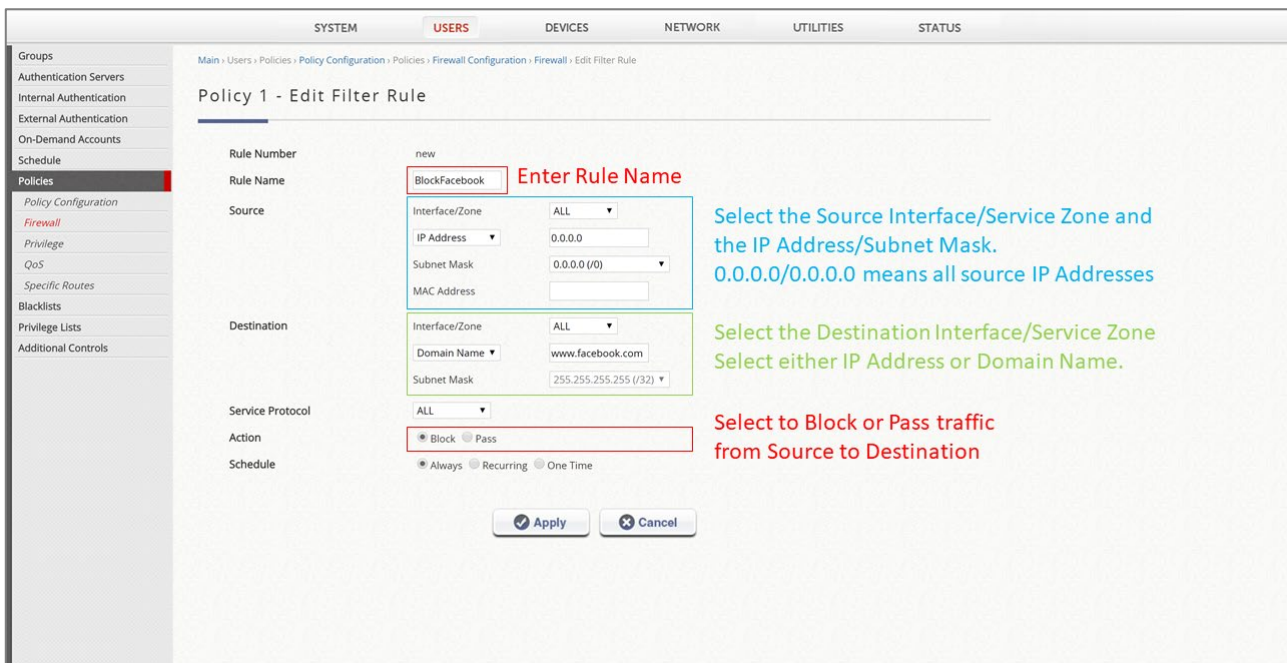
- b. Go to Users → Firewall to configure User Firewall Rules to block a user's access to an IP Address or Web Domain.

The screenshot shows the 'Firewall Configuration' page under the 'USERS' tab. The breadcrumb trail is 'Main > Users > Policies > Firewall Configuration'. A dropdown menu for 'Select Firewall Profile' is set to 'Firewall 1'. Below this, a form titled 'Firewall Configuration' contains several fields: 'Firewall Profile Name' (Firewall 1), 'Service Protocols' (Configure), 'User Firewall Rules' (Configure), and 'User Firewall Rules (IPv6)' (Configure). A blue box highlights the 'Service Protocols', 'User Firewall Rules', and 'User Firewall Rules (IPv6)' fields with the text 'Click Configure to create Firewall Rules to Allow/Block access to an IP Address or Domain Name'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

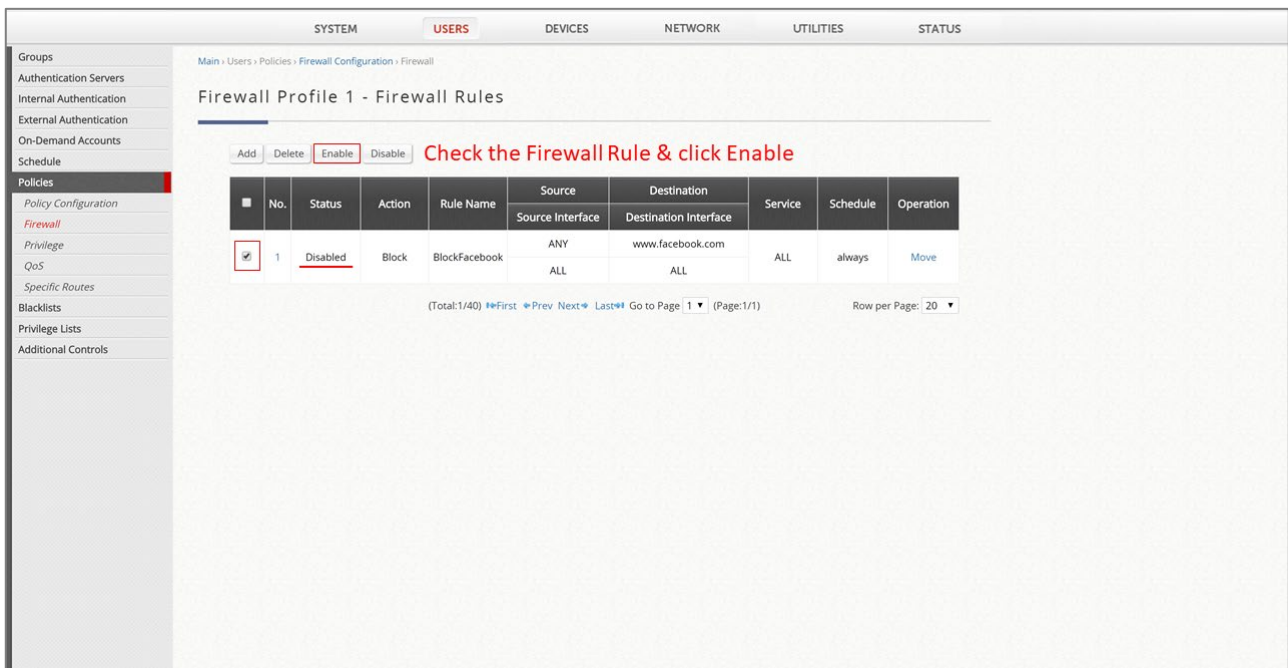
c. Click the Add button to create a new Firewall Rule.



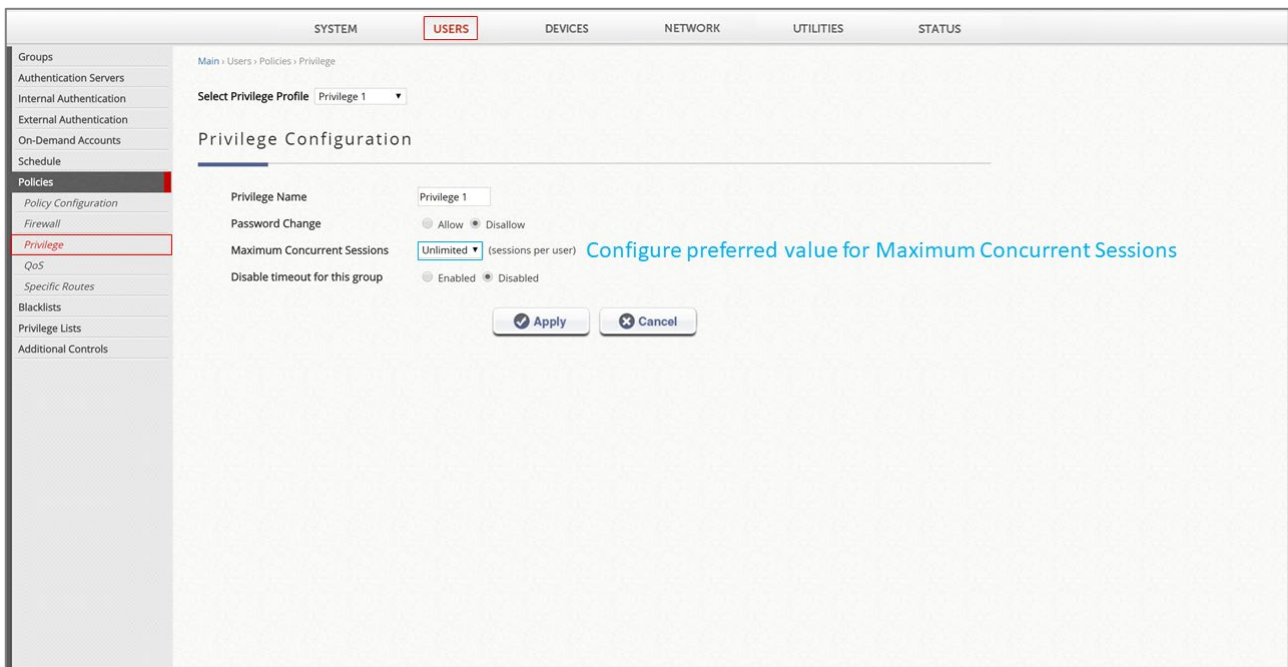
d. Configure a new Firewall Rule (BlockFacebook) with preferred Source/Destination.



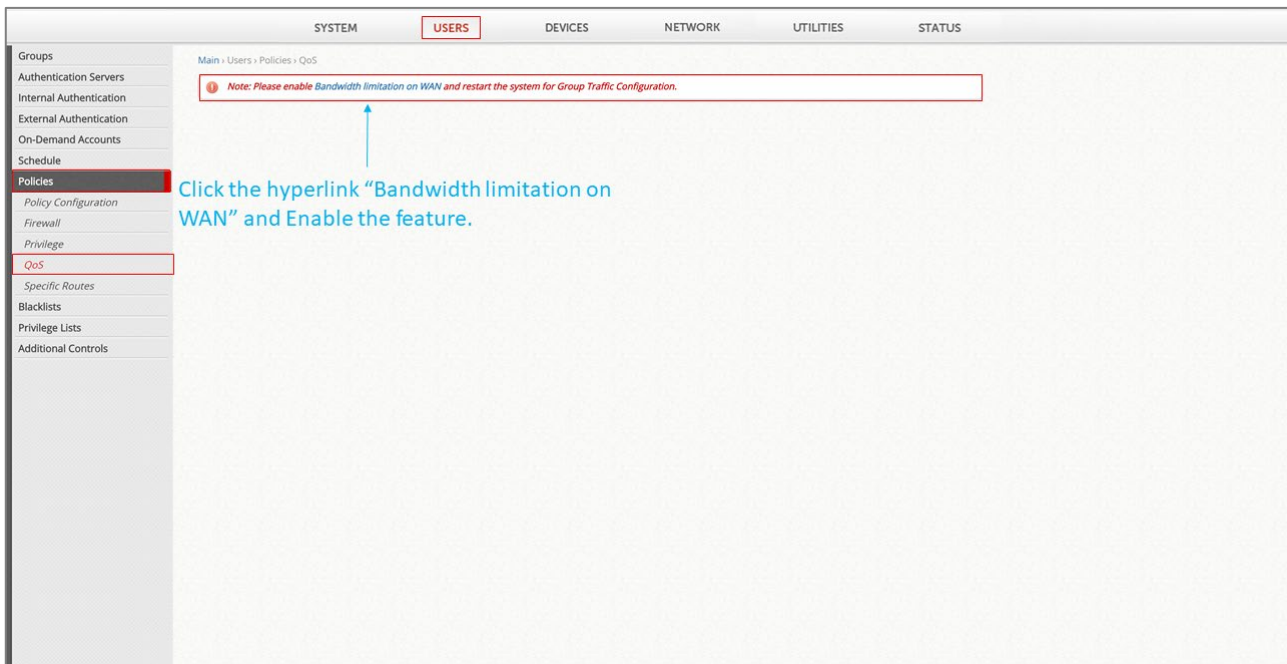
e. Check the checkbox and click the Enable button to Activate & Enable the Firewall Rule.



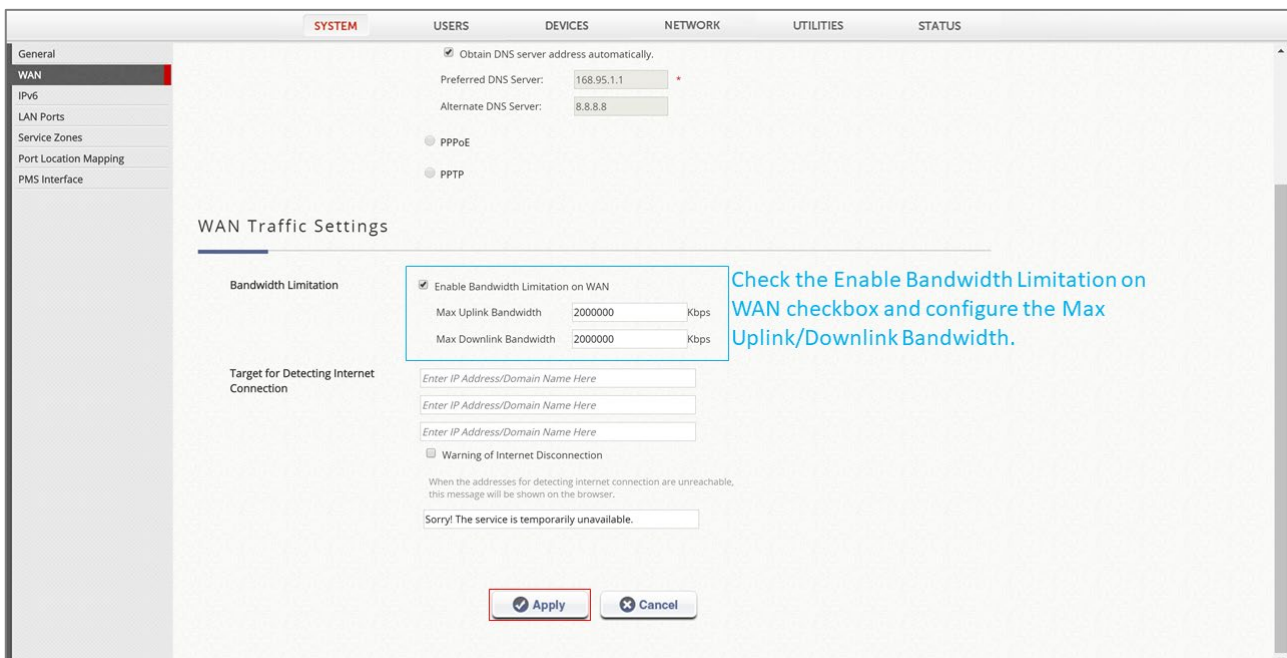
f. Go to Users → Policies → Privilege to configure the Maximum Concurrent Sessions of each user under this Policy. (Default = 500)



- 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.

Policy 1 - Edit Filter Rule

Rule Number: new

Rule Name: BlockFacebook **Enter Rule Name**

Source: Interface/Zone: ALL, IP Address: 0.0.0.0, Subnet Mask: 0.0.0.0 (/0), MAC Address: [empty]

Destination: Interface/Zone: ALL, Domain Name: www.facebook.com, Subnet Mask: 255.255.255.255 (/32)

Service Protocol: ALL

Action: Block Pass

Schedule: Always Recurring One Time

Buttons: Apply, Cancel

Annotations:

- Select the Source Interface/Service Zone and the IP Address/Subnet Mask. 0.0.0.0/0.0.0.0 means all source IP Addresses
- Select the Destination Interface/Service Zone. Select either IP Address or Domain Name.
- Select to Block or Pass traffic from Source to Destination

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

Specific Routes Configuration

Select Profile: Specific Route 1

Specific Route Profile Name: Specific Route 1

Default Gateway: Define Default Gateway: IP Address

Route No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1		255.255.255.255 (/32)	
2		255.255.255.255 (/32)	
3		255.255.255.255 (/32)	
4		255.255.255.255 (/32)	
5		255.255.255.255 (/32)	
6		255.255.255.255 (/32)	
7		255.255.255.255 (/32)	
8		255.255.255.255 (/32)	
9		255.255.255.255 (/32)	
10		255.255.255.255 (/32)	
11		255.255.255.255 (/32)	
12		255.255.255.255 (/32)	
13		255.255.255.255 (/32)	
14		255.255.255.255 (/32)	

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.

Group Configuration

Select Group: **Group 1** *Select Group to configure*
 Group Name: **Employee** *Rename Group*

Remark:

Number of devices which are allowed to login: **0** *Configure # of allowed devices to login simultaneously*
(0 to 9999 devices, 0: Unlimited)

Allow to logout other devices when exceeding the maximum amount of devices: Enabled Disabled *Enable/Disable logging out other devices*

Zone Permission Configuration & Policy Assignment

Enabled	Zone Name	Time Span 1	Time Span 2
		Schedule 1	Schedule 1
<input checked="" type="checkbox"/>	Service Zone : Default	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ1-Public	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

Configure Group's permission to access Service Zone's network and Policies

- b. Go to Users → Groups → Overview 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.

Group Overview

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

Employee (Group 1) is the Default Group for all Authentication Types

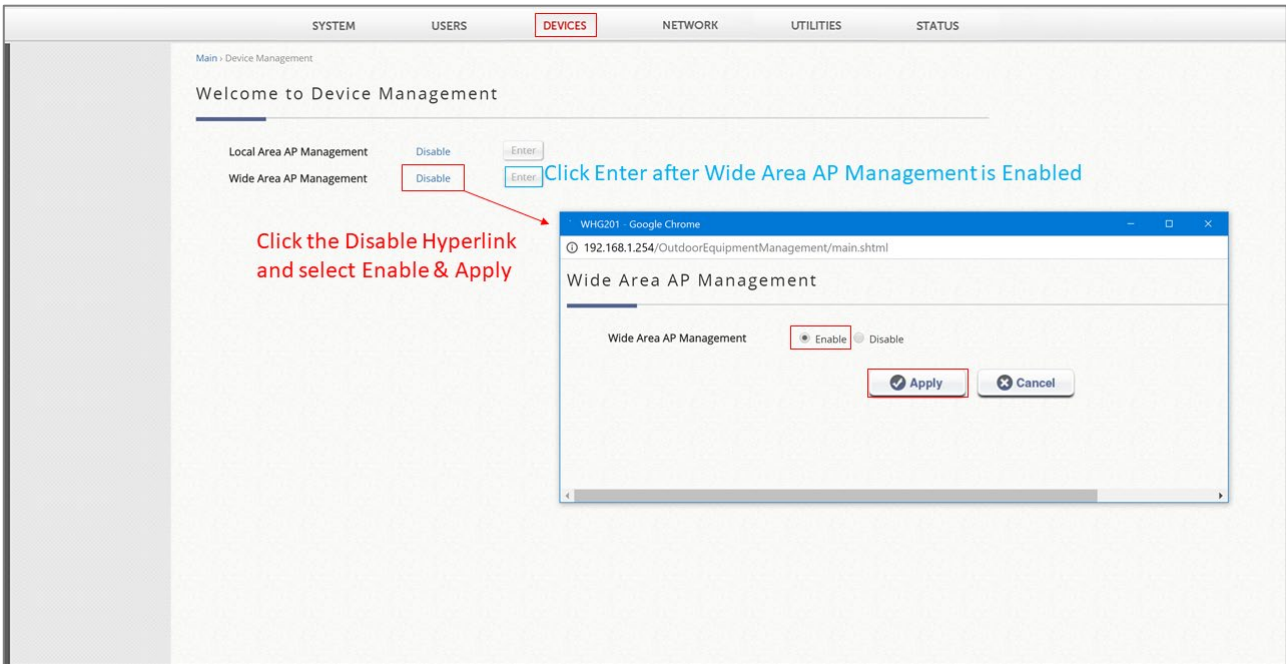
Group 2 has been selected as the Local User Account: test2

Group 3 has been selected as the Group for the Usage-Type On-Demand Billing Plan 1

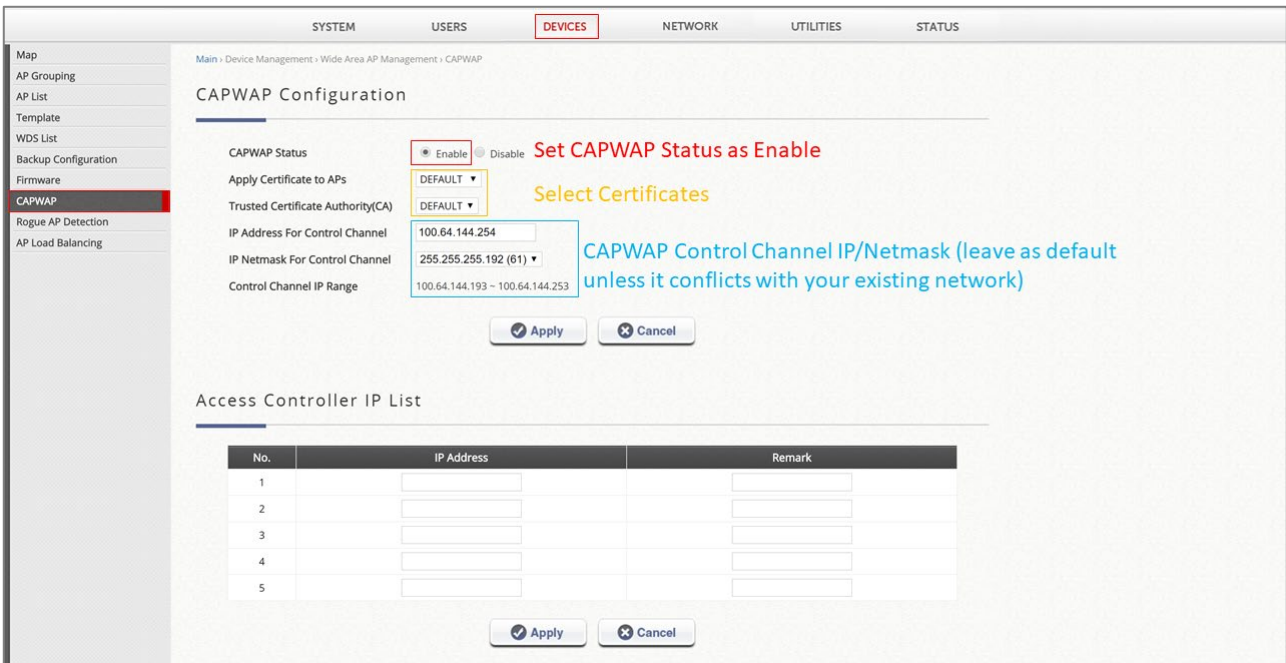
3.7 Devices

3.7.1 Devices - WAPM – CAPWAP Tunnel

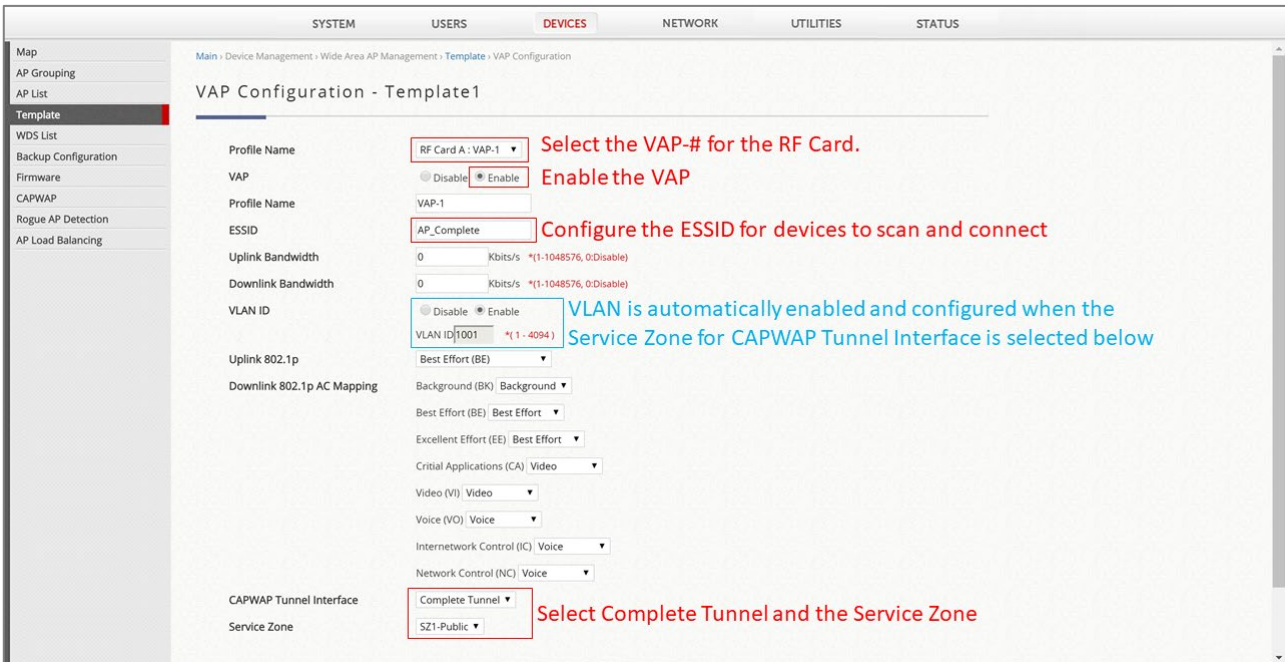
- a. Go to Devices, Enable Wide Area AP Management and click Enter to configure WAPM.



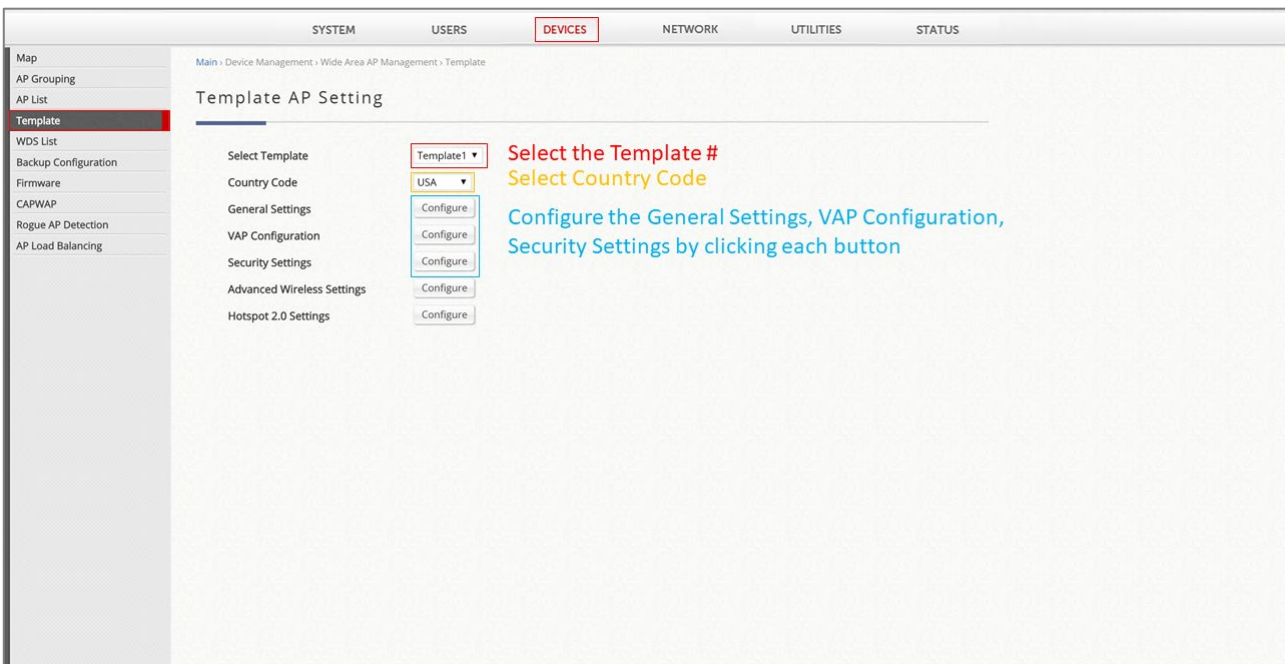
- b. Go to CAPWAP to enable CAPWAP on the EWS. Certificates can be uploaded for establishing CAPWAP tunnels between the EWS and AP. The Control Channel IP Address should not be changed unless there is an IP conflict.



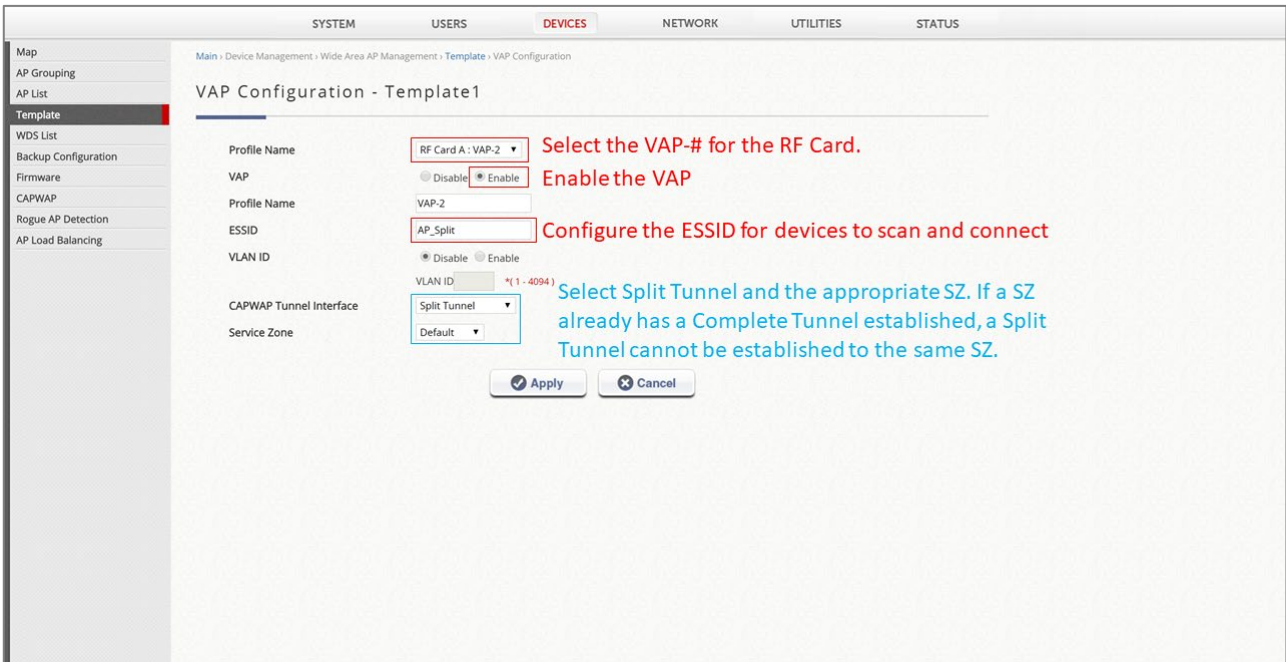
- c. Configure the Template to be applied to Edgecore APs prior to adding the APs into WAPM. You may select the Template #, Country Code and begin configuring the General, VAP, Security settings of the AP.



- 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.

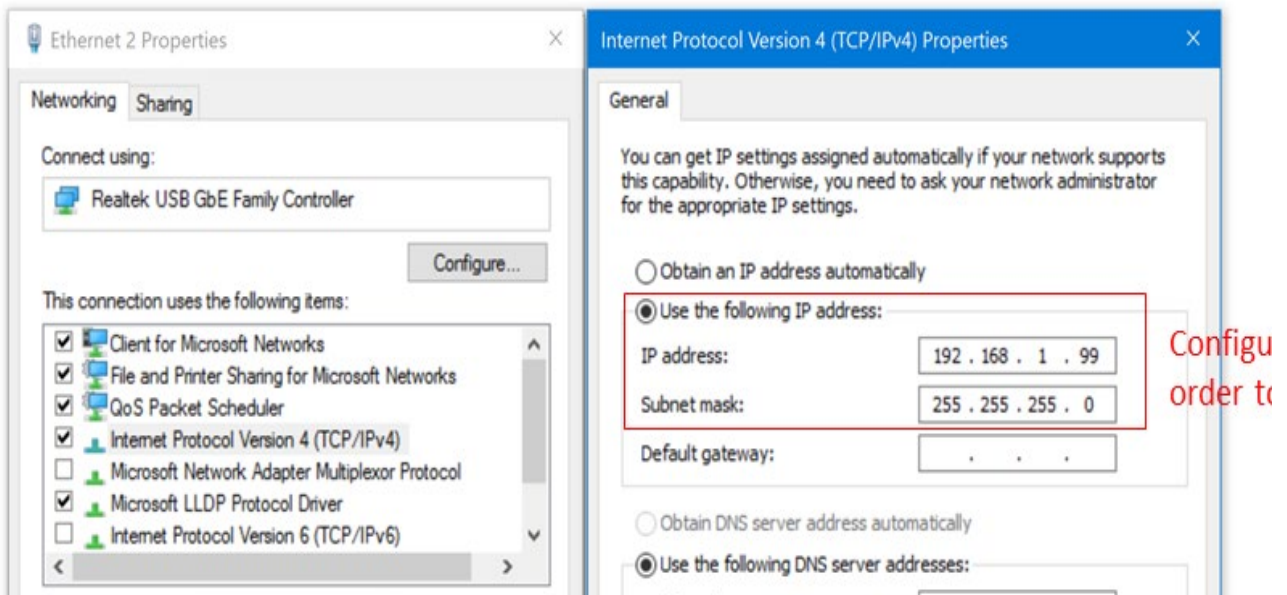


- e. Split Tunnel can be configured by selecting Split Tunnel at the CAPWAP Tunnel Interface. If a Complete Tunnel is already established to SZ-Public, a Split Tunnel cannot be established to the same Service Zone. For Split Tunnels, a VLAN is not required.

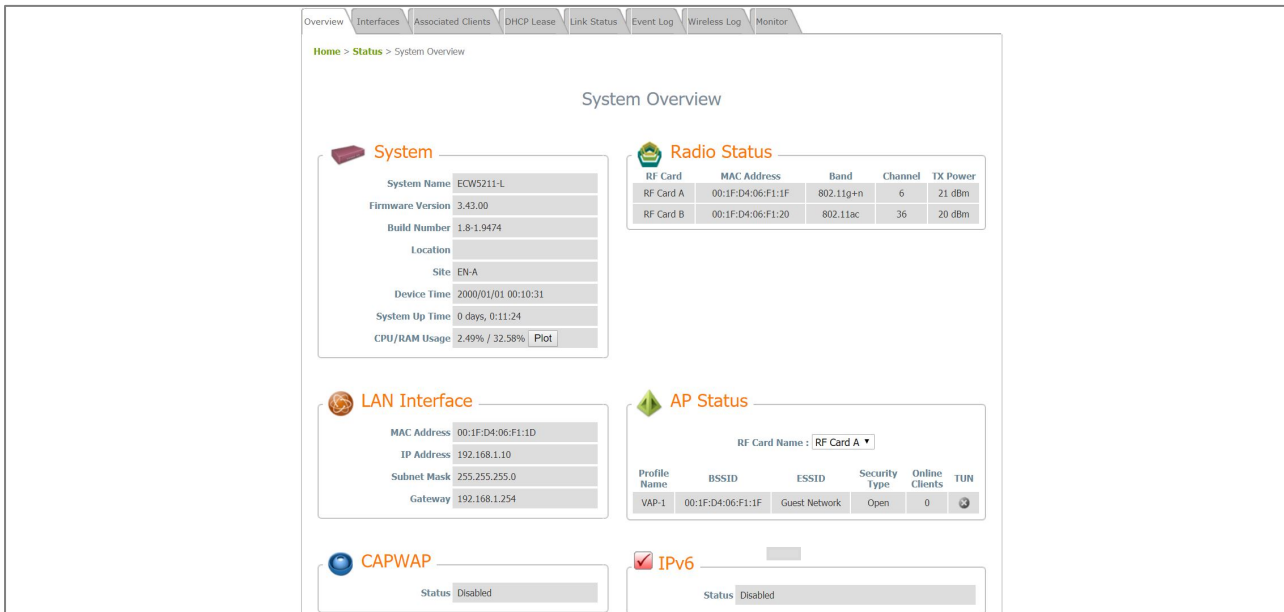


3.7.2 Devices - AP CAPWAP Configuration

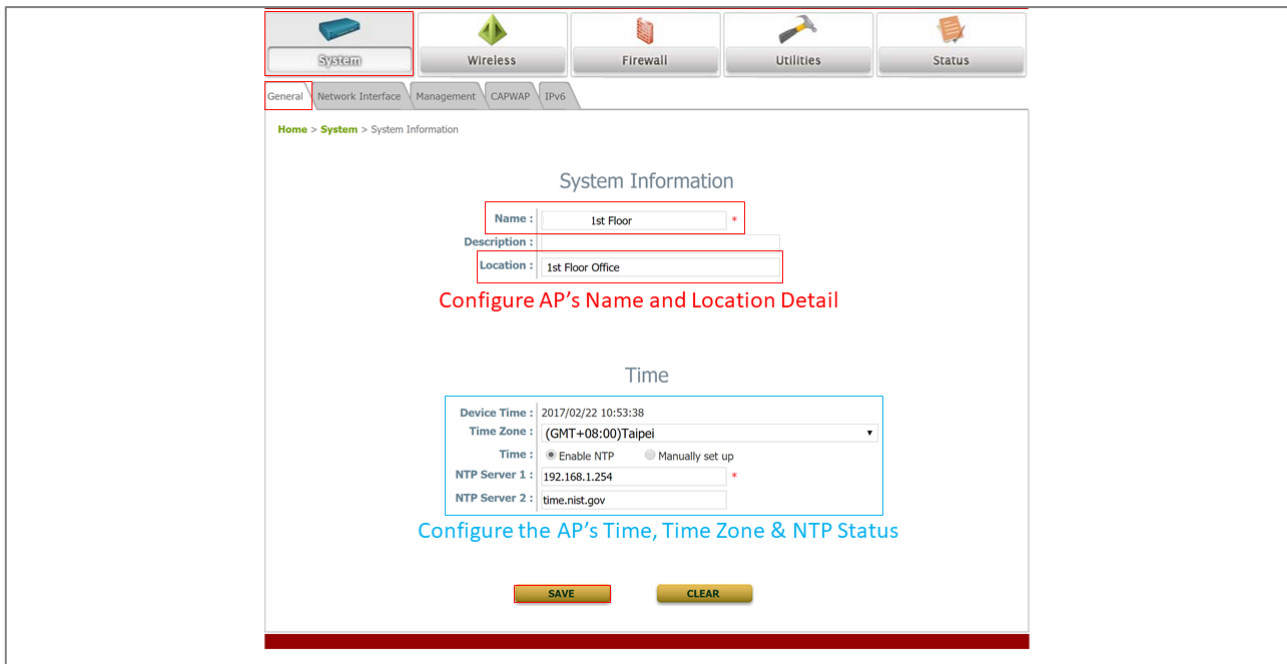
- a. Connect to the Edgecore AP on the WAN side either through a switch or directly to the AP's uplink port via an Ethernet cable.



- 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.



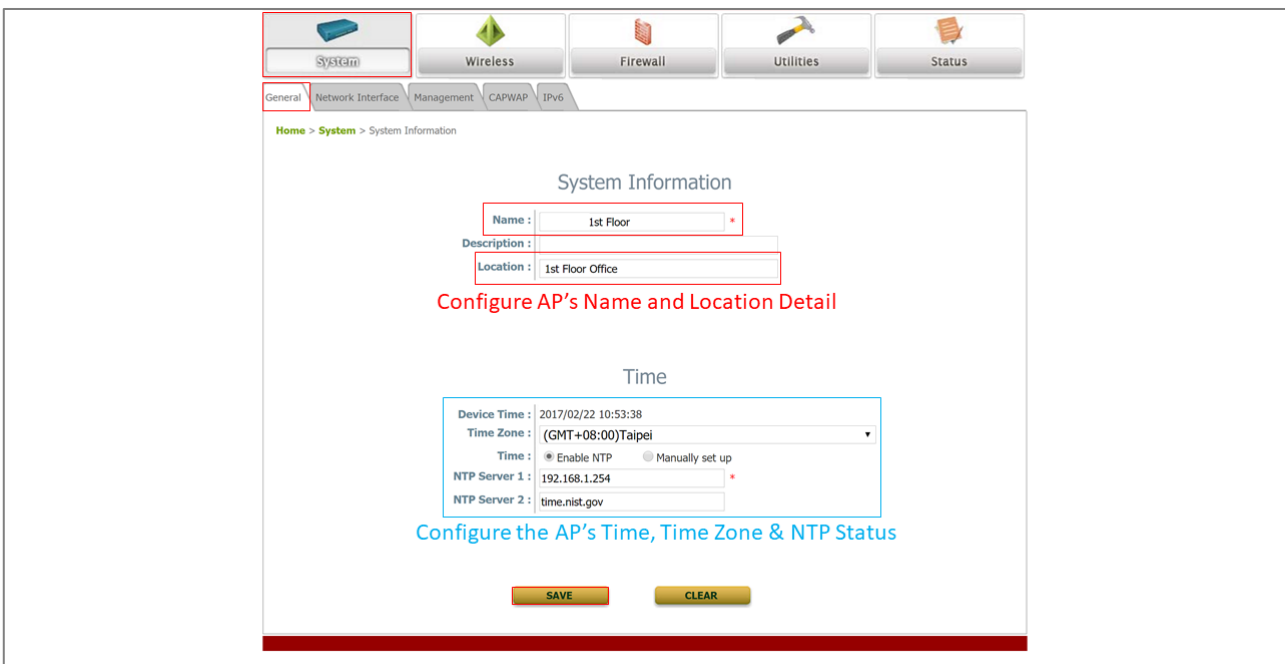
- c. Go to System → General to configure the AP's Name and Time Zone.



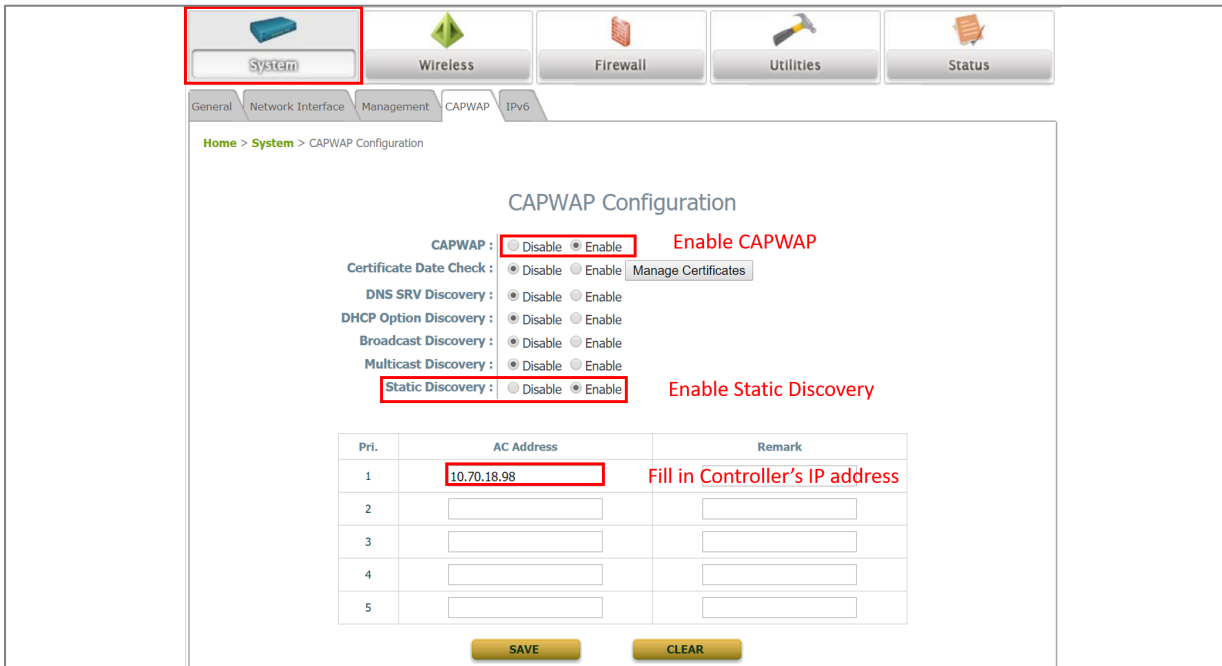
- d. Go to System → Network Interface to configure the AP's Static or Dynamic IP Address. After Saving a new Network Setting, a reboot is required.



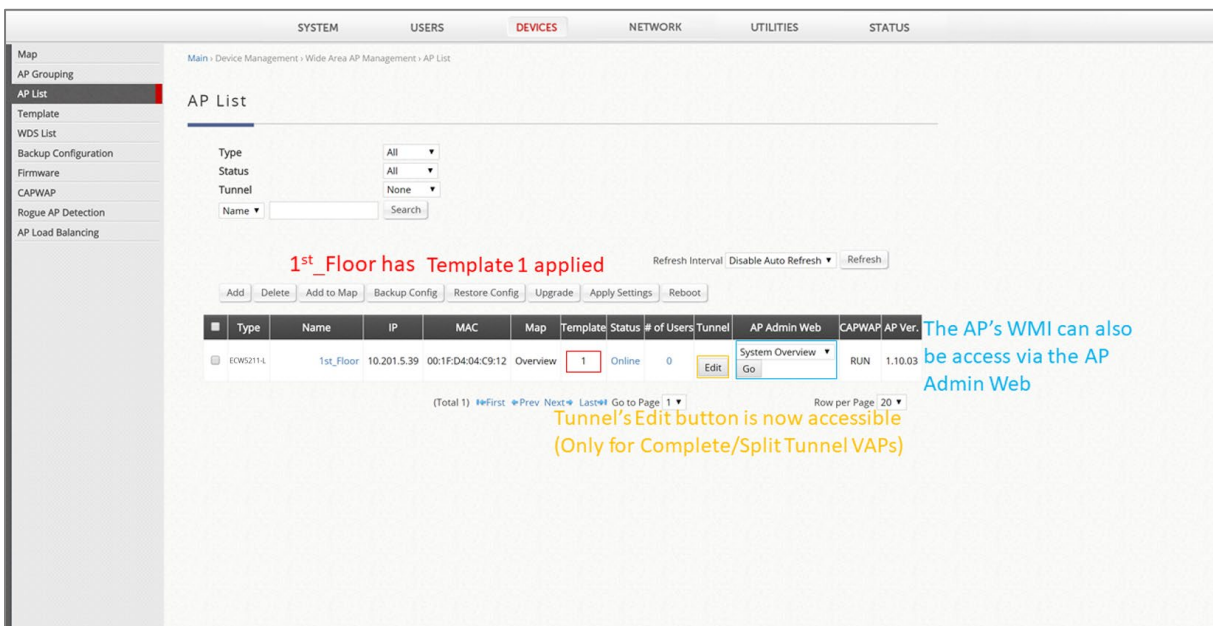
- e. Confirm updated System Name, Time and LAN Interface after reboot.



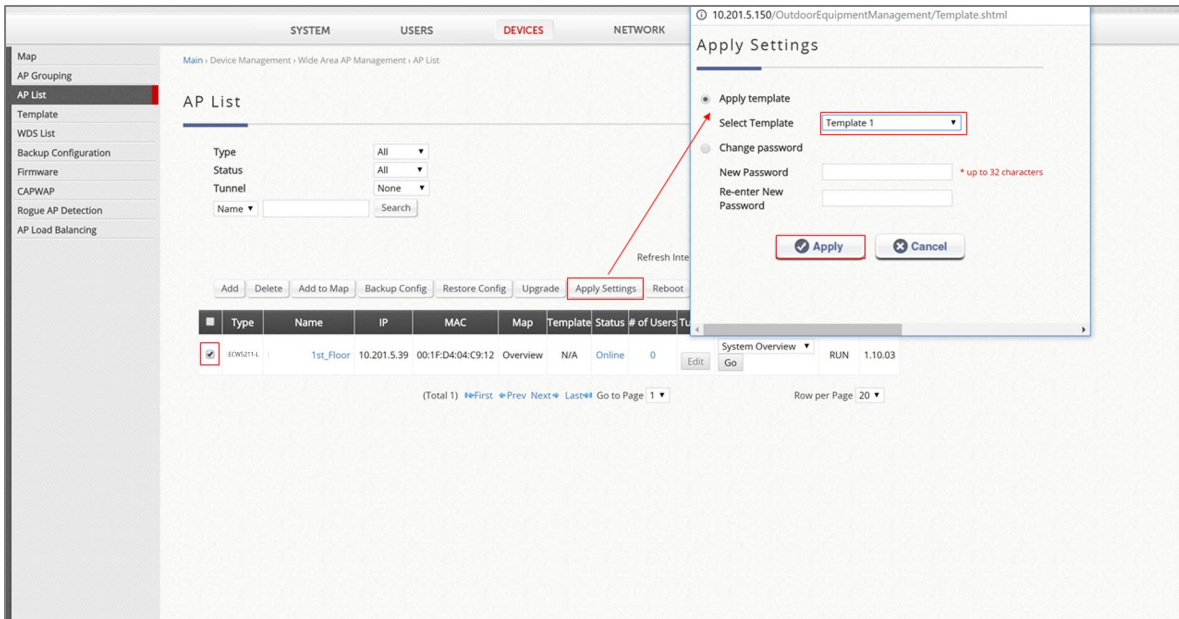
- f. Go to System → CAPWAP to enable CAPWAP and select the appropriate Discovery Method. A reboot is required after saving the new CAPWAP configuration.
 Note: Select Static Discovery if the EWS's WAN has a Static IP Address.
 Select DNS SRV Discovery if the EWS's WAN has a valid Domain Name.
 The following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



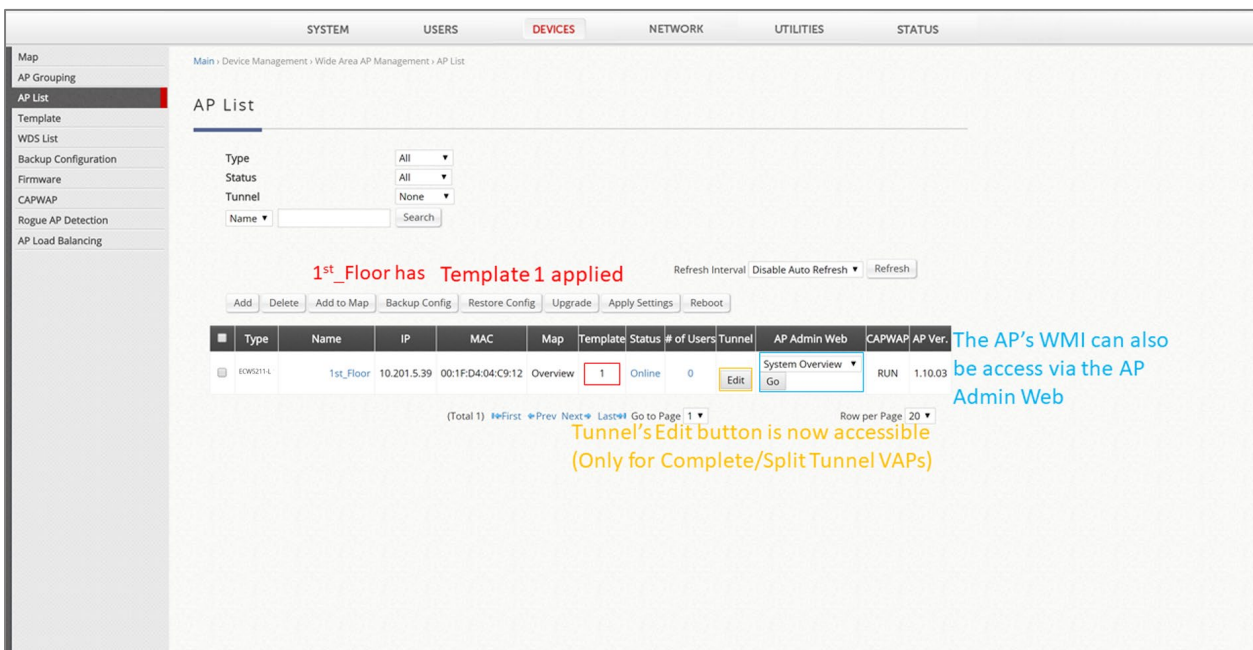
- g. Go to Devices → WAPM → AP List to confirm if the AP is automatically added into the AP List. The CAPWAP Status displaying “Run” means the AP can be managed using the EWS and can be applied a Template.



- 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.

AP's WMI remotely accessed using WAPM's AP List

System Overview

System

System Name: 1st Floor
 Firmware Version: 1.10.03
 Build Number: 1.19-1.8618.2.5
 Location: 1st Floor Office
 Site: EN-A
 Device Time: 2017/02/23 14:21:33
 System Up Time: 0 days, 0:04:26
 CPU/RAM Usage: 11.54% / 28.15% [Plot](#)

Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:1F:D4:04:C9:13	802.11g+n	6	27 dBm
RF Card B	00:1F:D4:04:C9:14	802.11ac	36	17 dBm

LAN Interface

MAC Address: 00:1F:D4:04:C9:12
 IP Address: 10.201.5.39
 Subnet Mask: 255.255.0.0
 Gateway: 10.201.1.254

AP Status

RF Card Name: RF Card A

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	00:1F:D4:04:C9:13	AP_Complete	Open	0	<input checked="" type="checkbox"/>

Established Tunnel (Complete or Split) per VAP

Updated VAP

CAPWAP Status & Data Channel

CAPWAP

Status: Run(10.201.5.150)
 Data Channel: Active

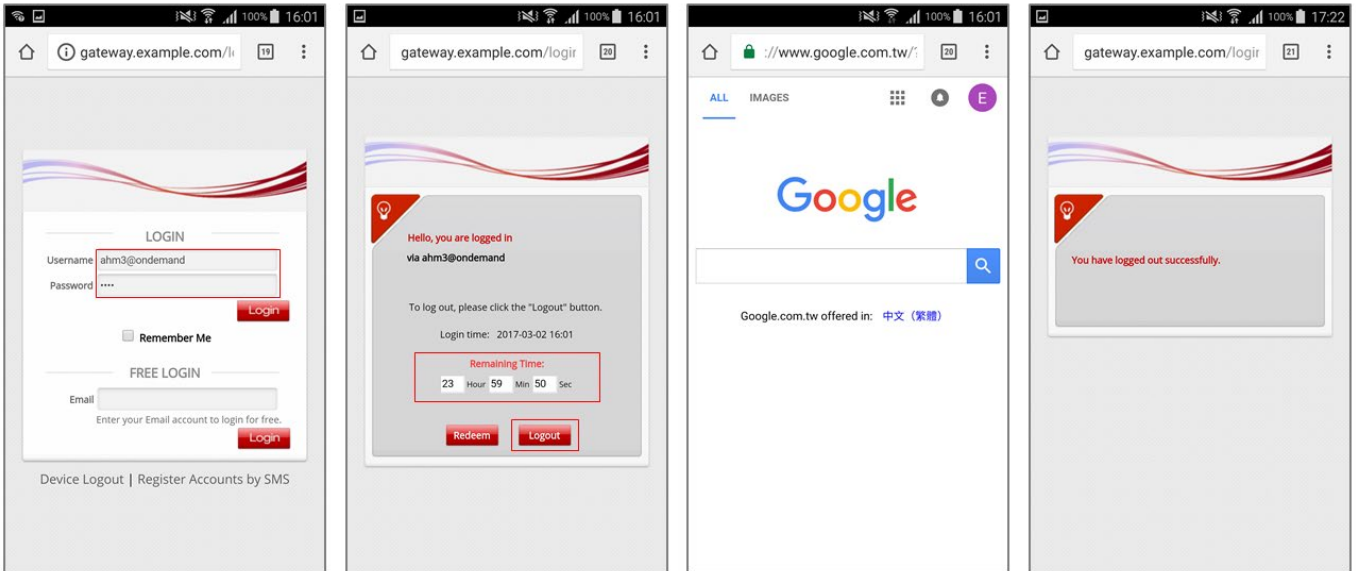
IPv6

Status: Disabled

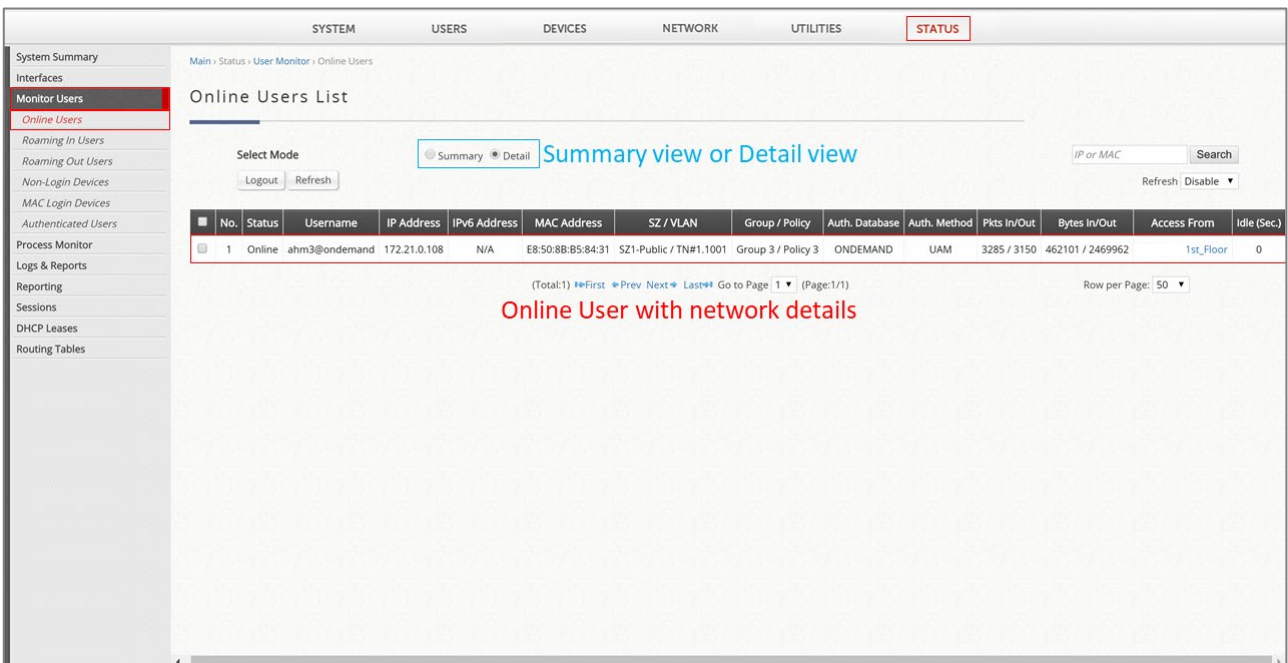
3.8 Client Login

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.

On-Demand Account List

Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
ahm3	23 hr(s) 20 min(s) 19 sec(s)	Normal	Group 3			Redeem

(Valid:1/1400) (Total:1/2000) **First Prev Next Last*# Go to Page: 1 (Page:1/1) Row per Page: 100

On-Demand Account List showing Remaining Quota of each user account

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

User Events

Display Mode: Configure

From: 2017-03-02 Select Filter Time Period

To: 2017-03-02 Select

User Type: Local On-Demand Guest Roaming Out Roaming In External Filter Authentication Type

Type	Date	Name	IP	MAC	Event
Ondemand	2017-03-02 14:14:23 +0800	ahm3	0.0.0.0	00:00:00:00:00:00	Create_OD_User
Ondemand - Mobile	2017-03-02 16:01:44 +0800	ahm3	172.21.0.108	E8:50:88:B5:84:31	OD_User_Login
Ondemand - Mobile	2017-03-02 16:41:25 +0800	ahm3	172.21.0.108	E8:50:88:B5:84:31	OD_User_Logout

(Total:3) **First Prev Next Last*# Go to Page: 1 (Page:1/1) Row per Page: 20

Events include the following: Account creation/deletion, User login/logout, User-Idle-Timeout, Session-Timeout and etc.

4 Remarks

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