



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

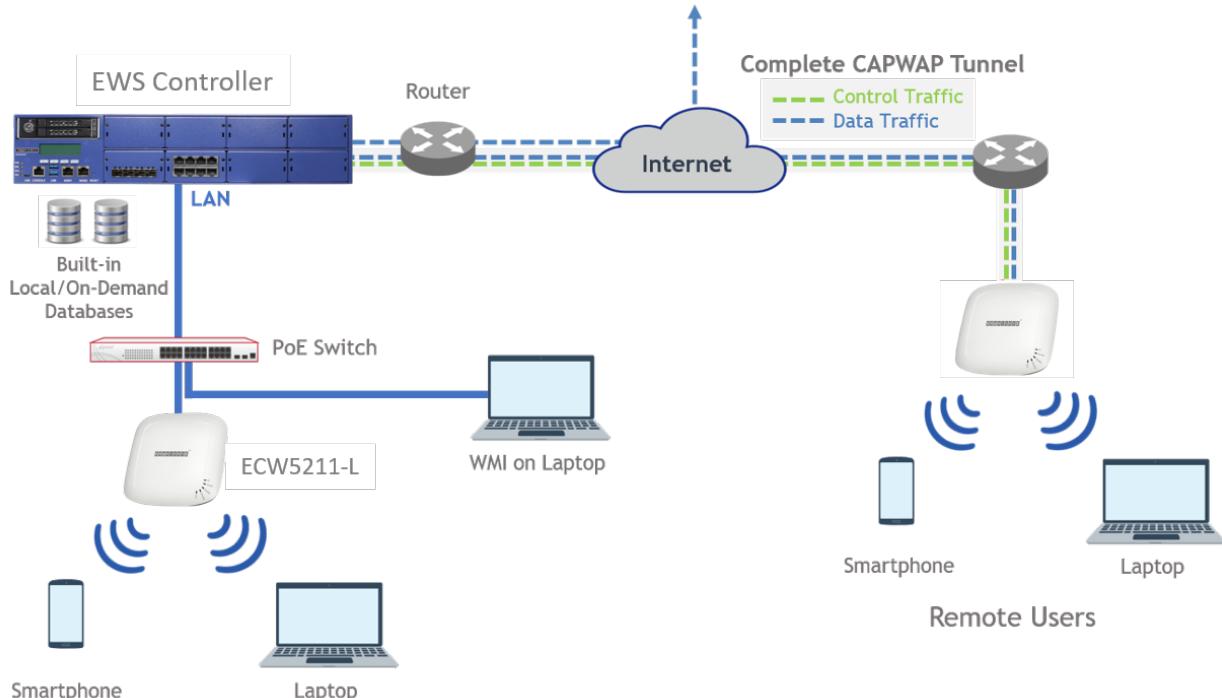
This guide will provide the basic configurations to quickly set up your own managed network. The guide highlights the minimum steps required for a wired or wireless network in each of the EWS controller's features; Service Zones, Authentication, Page Customization and User Policy Management and AP Management.

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

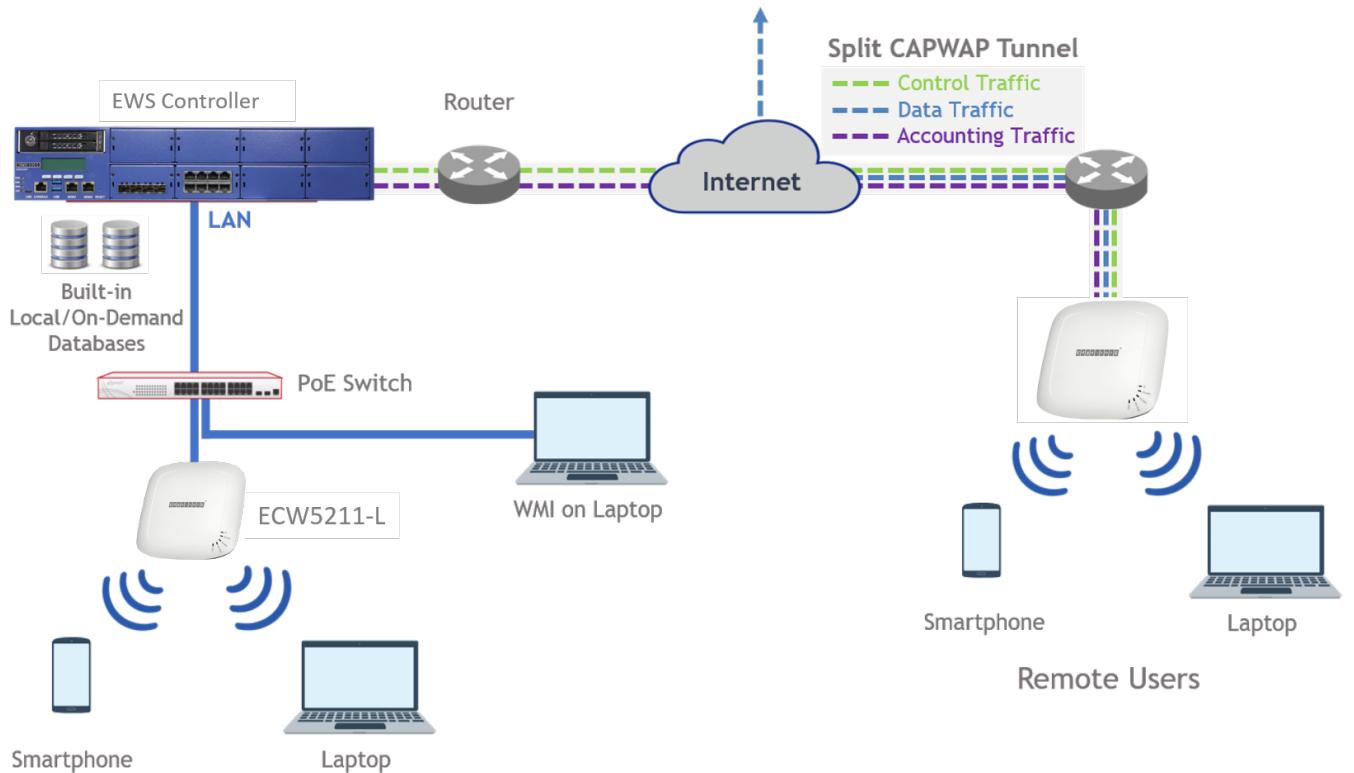
- a. Edgecore EWS controller is installed at the central site with uplink connected to WAN.
 - b. Edgecore AP is deployed locally under the layer 2 network or through the Layer 3 network at a remote site with internet connection at the uplink interface.
 - c. Confirm UDP ports 5246 & 5247 are open for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

The screenshot shows the main navigation bar with tabs: SYSTEM (highlighted in blue), USERS, DEVICES, NETWORK, UTILITIES, and STATUS. Below the navigation bar, the title "Main Categories" is displayed. A large green box highlights the "Welcome to System Main Menu" section. Inside this box, there is a message about the administrative interface, links to System, Users, Network, Utilities, and Status, and information about the Dashboard and Setup Wizard. A red arrow points from the "Log In" button on the left to the "Welcome to System Main Menu" section, with the text "Login to proceed to the Welcome Page".

3.1 System - WAN & LAN Interface Configuration

- a. Go to System → WAN to configure the WAN1 Interface Type as “Dynamic”.

The screenshot shows the "WAN" sub-tab selected in the left sidebar under "General". The main content area is titled "WAN1 Configuration". It shows the "Interface Type" section with "Dynamic (IP settings assigned automatically)" selected. Other options include "Static (Use the following IP settings)", "PPPoE", and "PPTP". Below this is the "WAN2 Configuration" section, which is currently empty. A red arrow points from the "WAN1 Configuration" section to the text "WAN1 (DHCP)". Another red arrow points from the "WAN2 Configuration" section to the text "Enable for QoS (Bandwidth Control)".

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

WAN1 obtained IP Address

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

Traffic Summary

Daily Traffic

day	rx	tx	total	avg. rate
01/23/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
01/24/17	7.05 KiB	781 KiB	788.05 KiB	0.07 kbit/s
01/25/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
01/26/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
01/27/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
01/28/17	0 KiB	782 KiB	782 KiB	0.07 kbit/s
01/29/17	0 KiB	782 KiB	782 KiB	0.07 kbit/s
01/30/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
01/31/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
02/01/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
02/02/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
02/03/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
02/04/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
02/05/17	0 KiB	781 KiB	781 KiB	0.07 kbit/s
02/06/17	4.62 MiB	4.98 MiB	11.90 MiB	1.13 kbit/s
02/07/17	22.44 MiB	20.67 MiB	50.11 MiB	4.75 kbit/s
02/08/17	20.50 MiB	3.38 MiB	23.88 MiB	2.06 kbit/s

Monthly Traffic

month	rx	tx	total	avg. rate
Apr '17	26 KiB	507 KiB	533 KiB	0.00 kbit/s
Jan '17	244.02 MiB	239.05 MiB	583.07 MiB	1.47 kbit/s
Feb '17	968.25 MiB	589.03 MiB	1.52 GiB	7.11 kbit/s
estimated	1.27 GiB	794 MiB	2.05 GiB	

Top 10 Traffic

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

Port Assignment

LAN Ports

LAN Port Mode

Port-Based Tag-Based

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

Port - Service Zone Mapping

LAN1	LAN2	LAN3	LAN4
Default	Default	Default	Default

Buttons:

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

Main > System > General

General Settings

System Name: WHG201

Contact Information: When there is a warning of "Please contact your network administrator"

Default CERT: Default CERT

User HTTPS Login: Enable (radio button selected)

Internal Domain Name: gateway.example.com

Portal URL Exceptions (User Agent): IEMobile/7.0.XBLWP7

User Log Access: Enter IP Address Here

Pre-Login Page: Configure

UAM Filter: Configure

Management IP Address: Configure (highlighted with a red border)

SNMP: Enable (radio button selected)

Suspend Warning Message: Sorry! The service is suspended.

NMS Setting: Configure

System Time

Current Time: 2017/03/02 19:05:18

Time Zone: (GMT+08:00)Taipei

Time Update: NTP (radio button selected)

- 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.

Management Service

SSH Service: Enable (radio button selected)

Telnet Service: Enable (radio button selected)

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

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

Enable/Disable SSH or Telnet for troubleshooting purposes

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

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

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

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

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

3.2 Utilities - Admin Password Recovery

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

Main > Utilities > Administrator Accounts > Edit Account

Admin Editing and Password Safety Setting

Name: admin

Original Password:
New Password:

Verify Password:

Email: [REDACTED]

Elementary school's name: test

Email Address for Password Recovery
Assign SMTP server Click to setup SMTP server

Security Answer for Password Recovery
(1-time setup)

The elementary school's name will identify you, if you forget your password. Note that, the elementary school's name can not be changed after apply.

Apply Cancel

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

Main > Utilities > Administrator Accounts

General Settings

Password Complexity: Enable Disable
Min Password Length: 6 * (6-20)
Min Password Category: 2 * (2-4)

Limit Login Attempts: Enable Disable

Password Expiration: Enable Disable
Password expires: 90 day(s) after creation

Password Limits: Enable Disable

Access Permission: Configure

Administrator Accounts

	Name	IP Address	MAC Address	Group	Status
<input type="checkbox"/>	admin	192.168.1.99	00:E0:4C:60:EB:78	Super Group	Current Page: Main > Utilities > Administrator Accounts

Click Administrator Account Name to setup an email account for password recovery/reset

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

Main > Utilities > Administrator Accounts > Edit Account

Admin Editing and Password Safety Setting

Name	admin
Original Password	[REDACTED]
New Password	[REDACTED]
Verify Password	[REDACTED]
Email	[REDACTED]
Elementary school's name	test

The elementary school's name will identify you, if you forget your password. Note that, the elementary school's name cannot be changed after apply.

Email Address for Password Recovery

Security Answer for Password Recovery (1-time setup)

Assign SMTP server [Click to setup SMTP server](#)

Apply **Cancel**

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

Main > System > Service Zone

Service Zone Settings

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

Click Service Zone Name to configure each SZ

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

The screenshot shows the 'Service Zone Configuration' page under the 'SYSTEM' tab. On the left sidebar, 'Service Zones' is selected. The main area displays 'Basic Settings' for Service Zone SZ1-Public. It includes fields for Service Zone Status (Enabled), Service Zone Name (SZ1-Public), Network Interface (VLAN Tag 1), Operation Mode (NAT), IP Address (172.21.0.254), and Subnet Mask (255.255.0.0). A note about VLAN isolation is present. Below this is a 'DHCP' section with 'Enabled' and 'Configure' buttons. Further down are sections for 'Assigned IP Address for AP Management' (IP Range 172.21.10.1 to 172.21.10.254) and 'Authentication Settings'.

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

The screenshot shows the 'Authentication Settings' page under the 'SYSTEM' tab. The left sidebar lists various authentication-related sections. The main area has sections for 'Authentication' (Enable/Disable), 'Access Permission and Authorization' (Configure), 'Default Policy' (Policy 1), 'Portal URL' (http://www.google.com), 'MAC Authentication' (Enabled), 'PPP Authentication' (Enabled), 'SIP Interface Configuration' (Enabled), 'WISPr Settings' (Configure), and 'Authentication Options'. The 'Authentication Options' section contains a table:

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"/>

Annotations highlight the 'Enable' button in the Authentication section, the 'Portal URL' field, the 'Enabled' checkboxes in the options table, and a note about confirming authentication databases.

3.3.2 System - Service Zone – Captive Portal Customization

- Click configure to customize different Login Page Customization. Message Page

Customization will provide customizations to message pages such as the login success page.

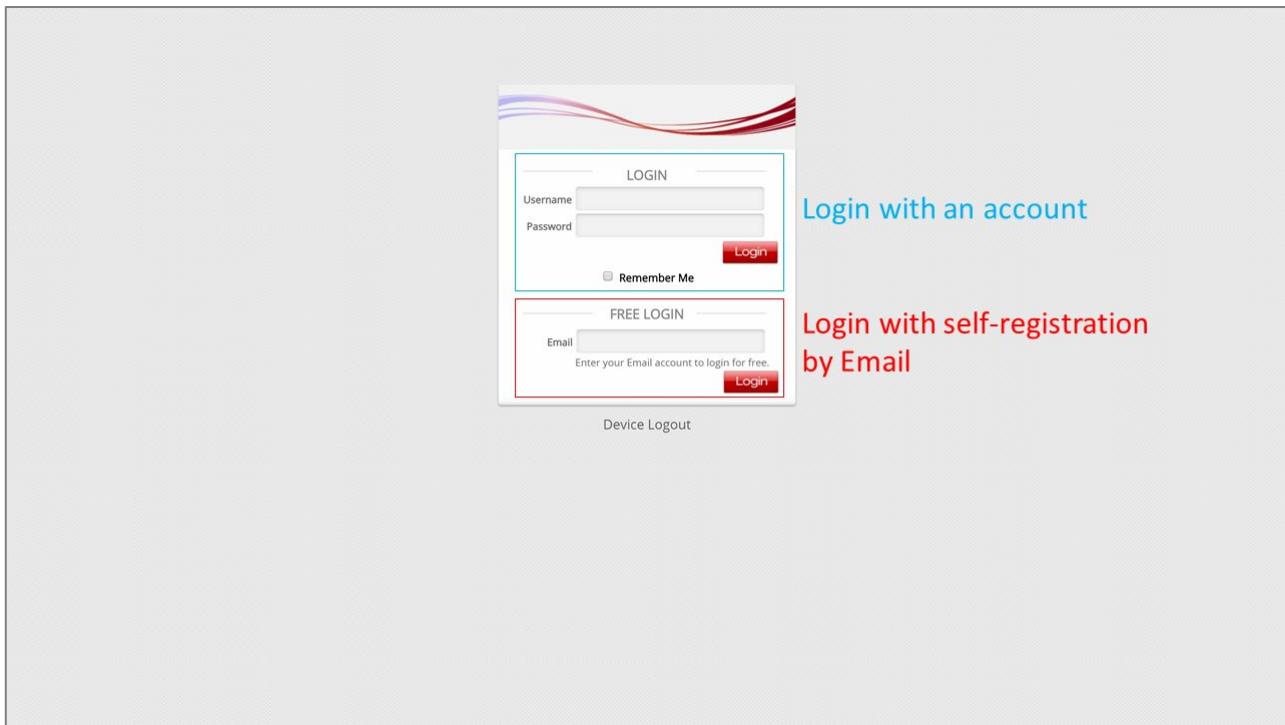
The screenshot shows the 'Service Zones' configuration page under the 'SYSTEM' tab. On the left sidebar, 'Service Zones' is selected. The main area displays 'Authentication Options' with a table showing various authentication methods like LOCAL, RADIUS, and NTDOMAIN. Below this is a 'Page Customization' section with 'Login Page Customization' and 'Message Page Customization' options, each with a 'Configure' button. A blue callout box highlights the 'Configure' button for 'Login Page Customization'. Another blue callout box on the right says 'Customize the Login Page (Captive Portal) by clicking the Configure button'. At the bottom, there's a section for 'APs with VAP mapped to this Service Zone' with a 'List' button, and 'Apply' and 'Cancel' buttons at the very bottom.

- Click configure to customize different Login Page Customization. Message Page

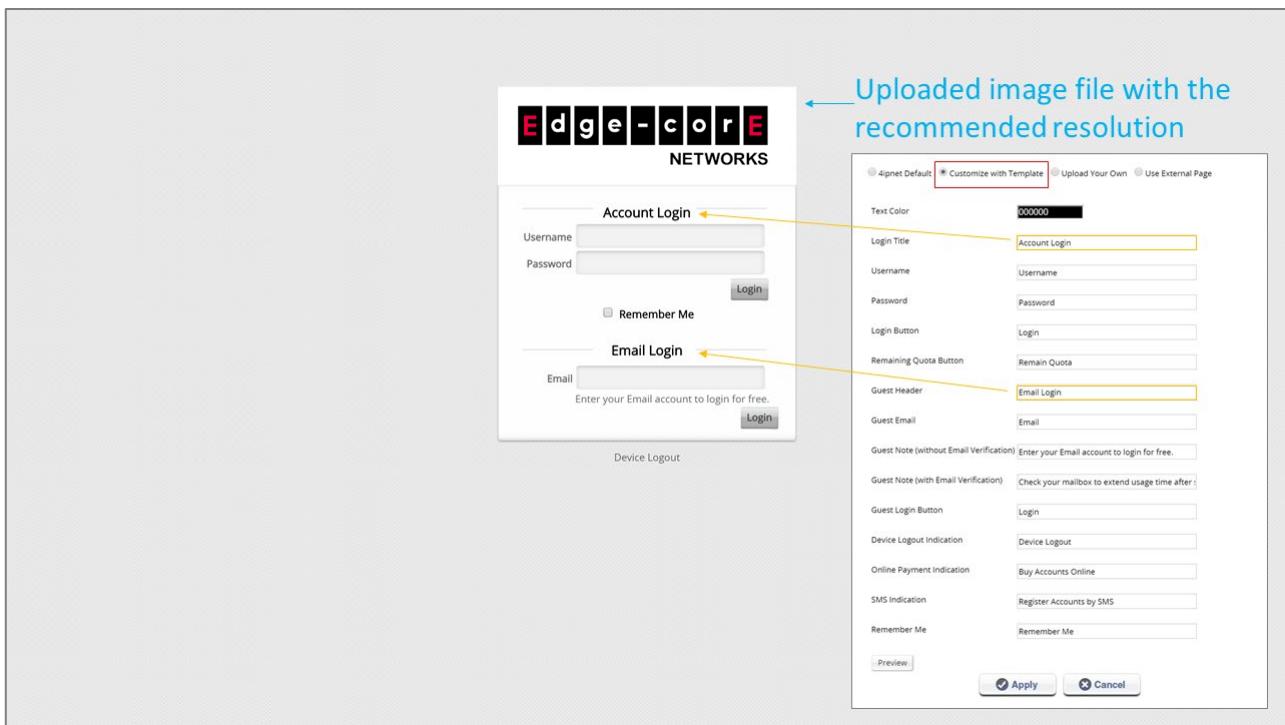
Customization will provide customizations to message pages such as the login success page.

The screenshot shows the 'Login Page Customization' page under the 'SYSTEM' tab. The left sidebar shows 'Service Zones' is selected. The main area has a 'Preview' button highlighted in red. Below it is a 'Theme for Template' section with a 'Button Color' selector and an 'Upload Logo' field with a 'Choose File' button. A yellow callout box highlights the 'Upload Logo' field. To the right, a blue callout box says 'Upload your own logo for a customized Captive Portal' and a red note says 'Note: Applies only to the "Customize with Template"'.

- 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

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

The screenshot shows the 'Local Authentication' configuration page. The left sidebar has a 'Local' section selected under 'Internal Authentication'. The main area shows 'Local User List' settings with options for 'Configure', 'Account Roaming Out' (Enable/Disable), and '802.1X Authentication' (Enable/Disable). Buttons for 'Apply' and 'Cancel' are at the bottom. A blue banner at the top right says 'Enter the Local User List to Add/Delete/Edit Local Accounts'.

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

The screenshot shows the 'Local User List' creation page. The left sidebar has a 'Local' section selected under 'Internal Authentication'. The main area has a red banner at the top saying 'Click Add to create Local Accounts'. Below it is a table header with columns: No, Status, Username, Password, MAC, Group, Activation, Expiration, and Remark. Buttons for 'Add...', 'Delete', 'Backup List', and 'Upload' are above the table. A search bar and a 'Row per Page' dropdown are at the bottom. Navigation links like 'First', 'Prev', 'Next', 'Last', and 'Go to Page' are also present.

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

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

[Main](#) > [Users](#) > [Internal Authentication](#) > [Local Authentication](#) > [Local User List](#)

Local User List

Add...
Delete
Backup List
Upload

Search

<input type="checkbox"/>	No	Status	Username	Password	MAC	Group	Activation	Expiration	Remark
<input type="checkbox"/>	1	Valid	test1	test1		Group 1			
<input type="checkbox"/>	2	Valid	test2	test2		Group 2			

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

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

3.4.2 Users - On-Demand Accounts

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

Main > Users > Internal Authentication > On-Demand Authentication

On-Demand Authentication

User Postfix: ondemand

Billing Plans: **Configure** Click Configure to modify Billing Plans

Currency: None \$ USD € EUR £ GBP Select currency for On-Demand Account

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

Expired Account Cache: 30 day(s)

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

Set Ticket's Serial Number: 000001 **Set**

Web Printout: **Configure**

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

POS Tickets: **Configure**

Number of Tickets: 1 2

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

Terminal Server: **Configure**

Payment Gateway: **Configure**

SMS Gateway: **Configure**

Account Roaming Out: Enable Disable

Apply **Cancel**

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

Main > Users > Internal Authentication > On-Demand Authentication > Billing Configuration

Billing Plans

No	Plan Type	Quota	Price (\$)	Active	Group	Function
1	N/A	Click number to create a Billing Plan			Group 1	Reset
2	N/A				Group 1	Reset
3	N/A				Group 1	Reset
4	N/A				Group 1	Reset
5	N/A				Group 1	Reset
6	N/A				Group 1	Reset
7	N/A				Group 1	Reset
8	N/A				Group 1	Reset
9	N/A				Group 1	Reset
0	N/A				Group 1	Reset

Apply **Cancel**

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

On-demand Billing Plan Configuration Google Chrome
① 192.168.1.254/UserAuthentication/OnDemandCreate.shtml?bpid=1

Billing Plan Configuration

Plan Number	1
Plan Type	Usage-time Usage-time Volume Hotel Cut-off time Duration-time
Activation	must be done within 1 day(s) 0 hour(s) s to be between 0-23; Day(s) and hour(s) cannot
Expiration	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Account will expire in 7 day(s) after activation
Quota	1 day(s) 0 hr(s) 0 min(s) The value for day(s) cannot exceed 364; The value for hr(s) has to be 0-23; The value for min(s) has to be between 0-59.
Unit Price	\$ 1 USD The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 3 ▾
Reference	

Select Plan Type: Usage-time/Volume/Hotel-Cut-off/Duration-Time

Configure Plan parameters:

- Activation/Expiration
- Quota
- Unit Price
- Group

Apply **Cancel**

- d. Confirm & Activate the Billing Plan.

SYSTEM USERS DEVICES NETWORK UTILITIES STATUS

Main > Users > Internal Authentication > On-Demand Authentication > Billing Configuration

Billing Plans

No	Plan Type	Quota	Price (\$)	Active	Group	Function
1	Usage-time	1 day(s) of usage time and expired in 7 day(s)	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

Check and Apply to Activate the configure Billing Plan

Apply **Cancel**

3.4.3 Users - Creating On-Demand Accounts

- 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' page. On the left, there's a sidebar with various options like Groups, Authentication Servers, Internal Authentication, External Authentication, and On-Demand Accounts (which is selected). The main area has tabs for SYSTEM, USERS (selected), DEVICES, NETWORK, UTILITIES, and STATUS. Below the tabs, it says 'Main > Users > On-Demand Accounts > Account Creation'. A table lists accounts with columns for Plan, Account Type, Quota, Price (\$), Group, and Function. Row 3 is highlighted with a red box around 'Create Single' and 'Create Batch'. A modal window titled 'Confirmation for Operator - Google Chrome' is open, showing the URL 10.201.5.150/UserAuthentication/OnDemandConfirm.shtml?buttonNo=1&random=1487831746788. The modal contains fields for Plan, Quota, Account Creation, Length of password, Valid Period, Total Price (\$), Unit, Group, Reference, and External ID. It also includes a note about activation expiration and two buttons: '+ Create' and 'Cancel'. An arrow points from the 'Create Single' button in the table to the 'Create Single' button in the modal.

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

The screenshot shows the 'On-demand User Receipt - Google Chrome' window. The URL is 10.201.5.150/UserAuthentication/OnDemandReceipt.shtml?buttonNo=1&extid=&unit=1&reference=&random=1487832310403&gen_str=ahm3@ondemand,ra. The window displays a receipt with the following information:

Username	ahm3@ondemand
Password	ra7z
Plan : Account Type	1 : Usage-time
Quota	1 day(s) of usage time and expired in 7 day(s)
Unit	1 Units
Total Price (\$)	1
Max User	1
Reference	
External ID	

ESSID : SSID0
Shared Wireless Key: None (Open System)
You have to login before 2017/02/24 14:45
The account will be expired in 7 day(s) after account activation.

Auto-generated Username/Password
Account Type & Quota
Account Units & Total Price
Max User for Usage-time accounts
Account Activation Time
Available Options for printing

At the bottom, there are buttons for 'Send to Pos', 'Printout' (highlighted in yellow), and 'Close'.

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

The screenshot shows a software interface for managing user accounts. At the top, there is a navigation bar with tabs: SYSTEM, USERS (which is highlighted in red), DEVICES, NETWORK, UTILITIES, and STATUS. Below the navigation bar, a left sidebar contains a tree-like menu with categories like Groups, Authentication Servers, Internal Authentication, External Authentication, On-Demand Accounts, Account Creation, Schedule, Policies, Blacklists, Privilege Lists, and Additional Controls. The 'On-Demand Accounts' category is expanded, and 'Account List' is selected, indicated by a red border around the link. The main content area is titled 'On-Demand Account List'. It features a table with the following columns: Username, Remaining Quota, Status, Group, Reference, External ID, and Redeem. A single row is visible in the table, showing 'ahm3' as the Username, '1 day(s)' as the Remaining Quota, 'Normal' as the Status, 'Group 3' as the Group, and a 'Redeem' button. Above the table, there is a section titled 'Available Actions' with buttons for Delete, Restore List, Backup List, Delete Expired, and Delete Out of Quota. There is also a search bar and a 'Search' button. At the bottom of the main content area, there is a footer with pagination information: '(Valid:1/1400) (Total:1/2000) ⏪First ⏪Prev ⏩Next ⏩Last ⏪ Go to Page: 1 (Page:1/1) Row per Page: 100 ⏪'.

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

3.5 Users

3.5.1 Users - Policy Configuration

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

The screenshot shows the 'Policy Configuration' screen under the 'Users' tab. On the left, a sidebar lists various policy categories: Groups, Authentication Servers, Internal Authentication, External Authentication, On-Demand Accounts, Schedule, Policies, Policy Configuration, Firewall, Privilege, QoS, Specific Routes, Blacklists, Privilege Lists, and Additional Controls. The 'Policy Configuration' section is currently selected. In the main area, a message states: 'A Policy is used to define a Group's authorization in a Service Zone. The Global Policy is the general policy defined for all Groups when the Group Policy is not defined.' Below this, a dropdown menu shows 'Select Policy' set to 'Policy 1'. A callout box highlights this dropdown with the text 'Select Policy to configure'. A large blue box encloses the configuration fields for 'Policy Name' (set to 'Policy 1'), 'Firewall Profile' (set to 'Firewall 1'), 'Privilege Profile' (set to 'Privilege 1'), 'QoS Profile' (set to 'QoS 1'), 'Specific Route Profile' (set to 'Specific Route 1'), and 'Prefer DHCP Pool' (set to 'None'). A callout box highlights these fields with the text 'Choose mapped Profiles'. At the bottom are 'Apply' and 'Cancel' buttons.

- 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' screen under the 'Users' tab. The left sidebar is identical to the previous screen, with the 'Policy Configuration' section still selected. In the main area, a message says: 'Main > Users > Policies > Firewall Configuration'. A dropdown menu shows 'Select Firewall Profile' set to 'Firewall 1'. A callout box highlights this dropdown with the text 'Select Firewall Profile'. Below are four configuration buttons: 'Firewall Profile Name' (set to 'Firewall 1'), 'Service Protocols' (with a 'Configure' button), 'User Firewall Rules' (with a 'Configure' button), and 'User Firewall Rules (IPv6)' (with a 'Configure' button). A callout box highlights the 'Configure' button for 'User Firewall Rules' with the text 'Click Configure to create Firewall Rules to Allow/Block access to an IP Address or Domain Name.' At the bottom are 'Apply' and 'Cancel' buttons.

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

Main > Users > Policies > Firewall Configuration > Firewall

Firewall Profile 1 - Firewall Rules

Add Delete Enable Disable Click Add to create a Firewall Rule

No.	Status	Action	Rule Name	Source	Destination	Service	Schedule	Operation
				Source Interface	Destination Interface			
(Total:0/40) First Prev Next Last Go to Page (Page:1/1)								
Row per Page: 20								

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

Main > Users > Policies > Policy Configuration > Policies > Firewall Configuration > Firewall > Edit Filter Rule

Policy 1 - Edit Filter Rule

Rule Number: new

Rule Name: **Enter Rule Name** (highlighted in red)

Source:

Interface/Zone: ALL
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0 (/0)
MAC Address:

Destination:

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

Service Protocol: ALL

Action: **Block** (highlighted in red)

Schedule: Always

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

Apply Cancel

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

Main > Users > Policies > Firewall Configuration > Firewall

Firewall Profile 1 - Firewall Rules

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

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

(Total:1/40) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page: 1 (Page:1/1) Row per Page: 20

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

Main > Users > Policies > Privilege

Select Privilege Profile: Privilege 1

Privilege Configuration

Privilege Name: Privilege 1

Password Change: Allow Disallow

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

Disable timeout for this group: Enabled Disabled

Apply | **Cancel**

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.

Main > Users > Policies > QoS

Note: Please enable Bandwidth limitation on WAN and restart the system for Group Traffic Configuration.

Groups
Authentication Servers
Internal Authentication
External Authentication
On-Demand Accounts
Schedule
Policies
Policy Configuration
Firewall
Privilege
QoS
Specific Routes
Blacklists
Privilege Lists
Additional Controls

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

General
WAN
IPv6
LAN Ports
Service Zones
Port Location Mapping
PMS Interface

WAN Traffic Settings

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

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

Apply **Cancel**

Check the Enable Bandwidth Limitation on WAN checkbox and configure the Max Uplink/Downlink Bandwidth.

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

Main > Users > Policies > Policy Configuration > Policies > Firewall Configuration > Firewall > Edit Filter Rule

Policy 1 - Edit Filter Rule

Rule Number	new
Rule Name	BlockFacebook
Source	Interface/Zone: ALL IP Address: 0.0.0.0 Subnet Mask: 0.0.0.0 (/0) MAC Address:
Destination	Interface/Zone: ALL Domain Name: www.facebook.com Subnet Mask: 255.255.255.255 (/32)
Service Protocol	ALL
Action	<input checked="" type="radio"/> Block <input type="radio"/> Pass <input checked="" type="radio"/> Always <input type="radio"/> Recurring <input type="radio"/> One Time
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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.

Main > Users > Policies > Specific Routes

Specific Routes Configuration

Specific Route Profile Name	Specific Route 1	
Default Gateway <input checked="" type="checkbox"/> Define Default Gateway: IP Address: 255.255.255.255 (/32)		
Route No.	Destination	Gateway
1	255.255.255.255 (/32)	255.255.255.255 (/32)
2	255.255.255.255 (/32)	255.255.255.255 (/32)
3	255.255.255.255 (/32)	255.255.255.255 (/32)
4	255.255.255.255 (/32)	255.255.255.255 (/32)
5	255.255.255.255 (/32)	255.255.255.255 (/32)
6	255.255.255.255 (/32)	255.255.255.255 (/32)
7	255.255.255.255 (/32)	255.255.255.255 (/32)
8	255.255.255.255 (/32)	255.255.255.255 (/32)
9	255.255.255.255 (/32)	255.255.255.255 (/32)
10	255.255.255.255 (/32)	255.255.255.255 (/32)
11	255.255.255.255 (/32)	255.255.255.255 (/32)
12	255.255.255.255 (/32)	255.255.255.255 (/32)
13	255.255.255.255 (/32)	255.255.255.255 (/32)
14	255.255.255.255 (/32)	255.255.255.255 (/32)

3.6 Users

3.6.1 Users - Group 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.

The screenshot shows the 'Group Configuration' page under the 'Configuration' tab for 'Group 1'. The 'Group Name' is set to 'Employee'. A note indicates that the number of devices allowed to log in simultaneously is 0 (0 to 9999 devices, 0; Unlimited). An option to enable/disable logging out other devices is set to 'Enabled'. A green callout box highlights the 'Configure # of allowed devices to login simultaneously' field.

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

- 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.

The screenshot shows the 'Group Overview' page under the 'Overview' tab. It lists groups with their names and authentication types. Group 1 ('Employee') is highlighted in blue and listed under 'Default Group for all Authentication Types'. Group 2 ('Group 2') is highlighted in yellow and listed under 'Group 2 has been selected as the Local User Account: test2'. Group 3 ('Group 3') is highlighted in red and listed under 'Group 3 has been selected as the Group for the Usage-Type On-Demand Billing Plan 1'.

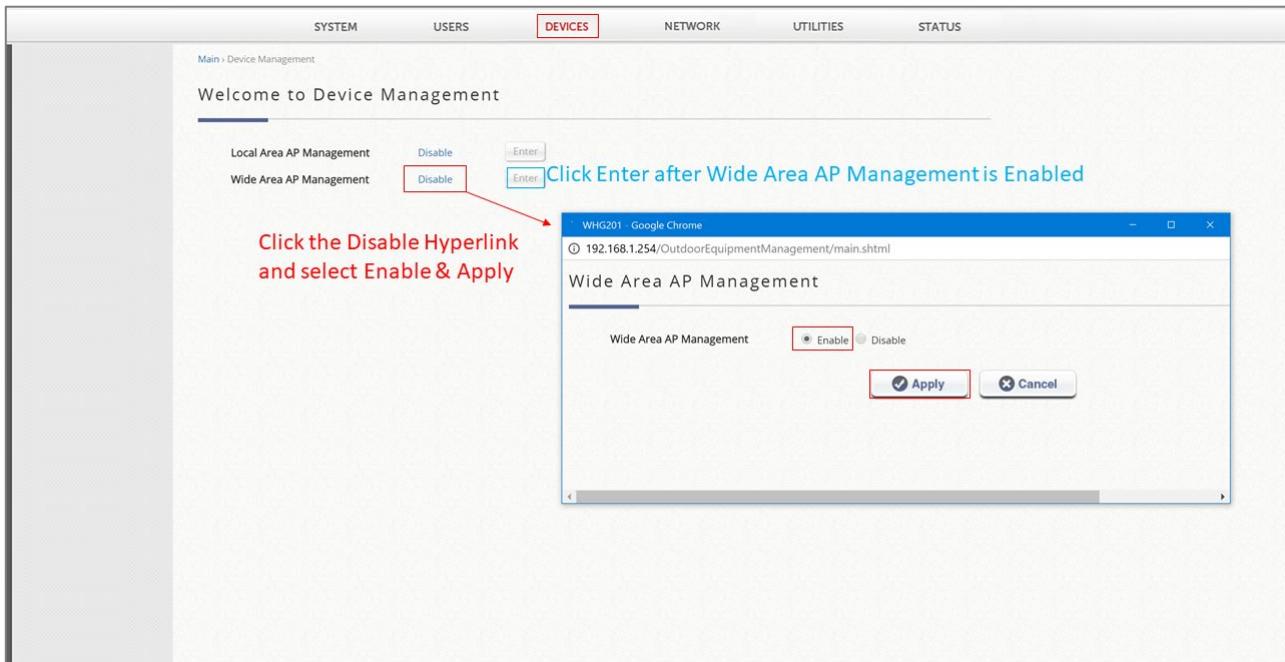
Group Name	Authentication Type
Employee	Local Guest POP3-Server 5 RADUS-Server 2-Default LDAP-Server 4-Default NT Domain-Server 3 SIP
Group 2	Local
Group 3	Billing Plan 1
Group 4	
Group 5	
Group 6	
Group 7	
Group 8	

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

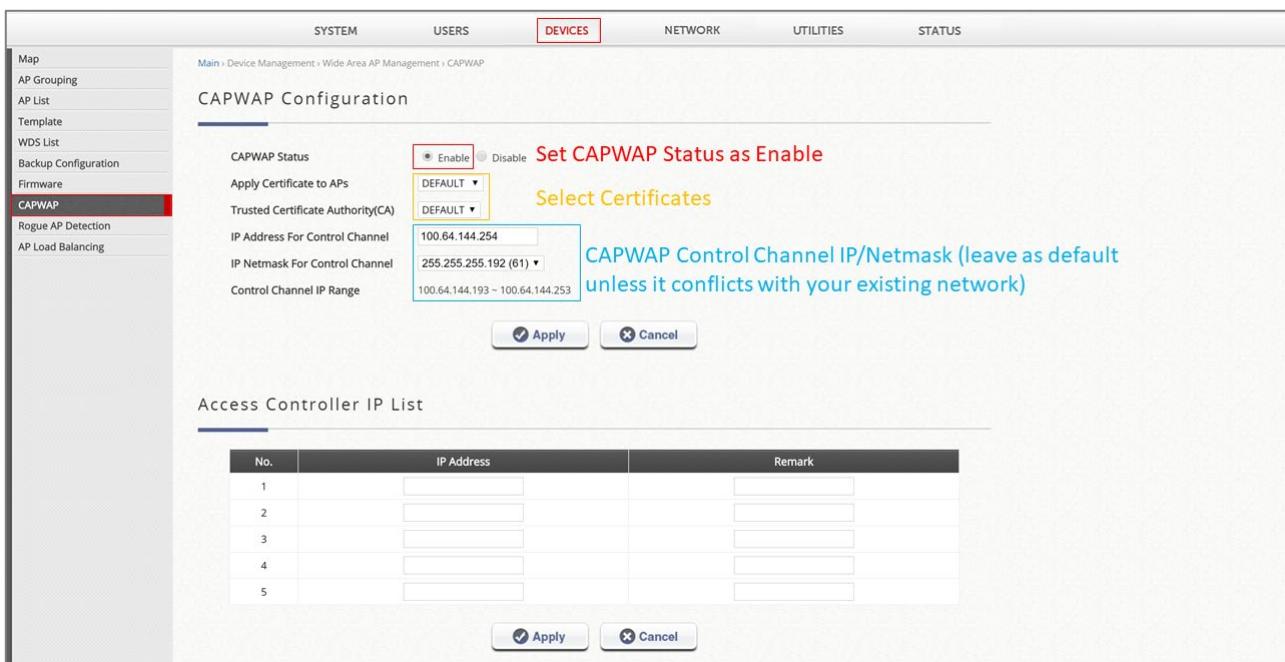
3.7 Devices

3.7.1 Devices - WAPM – CAPWAP Tunnel

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



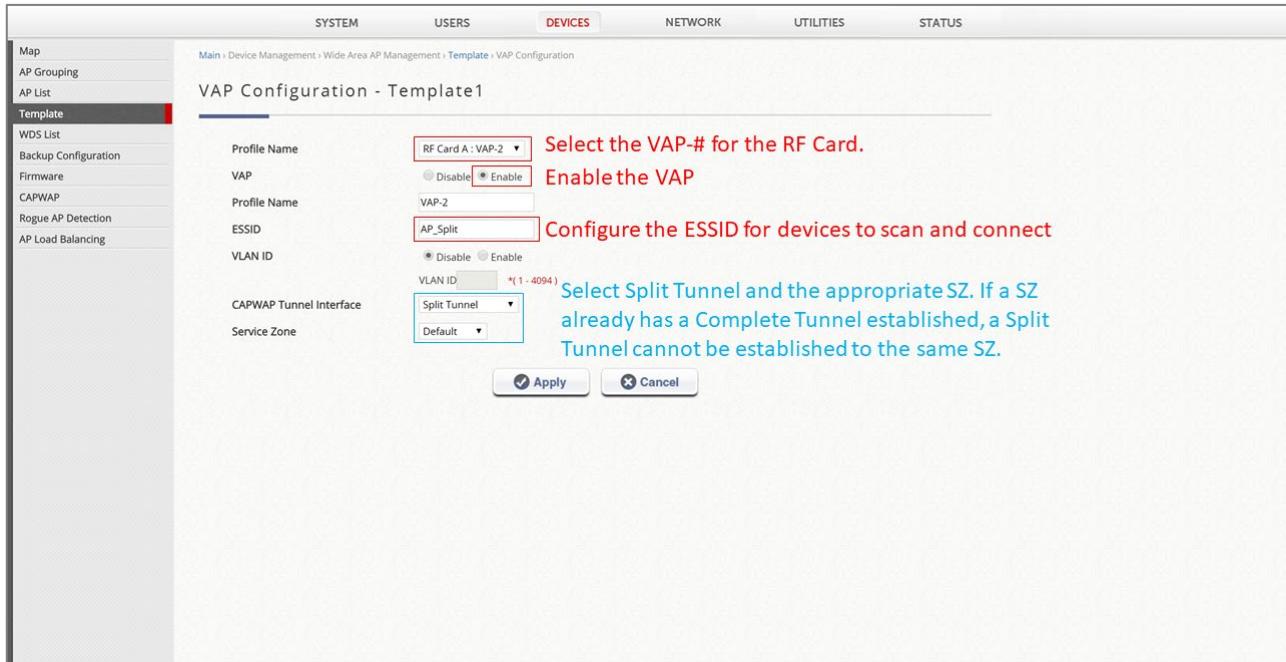
- Go to CAPWAP to enable CAPWAP on the EWS. Certificates can be uploaded for establishing CAPWAP tunnels between the EWS and AP. The Control Channel IP Address should not be changed unless there is an IP conflict.



- 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.

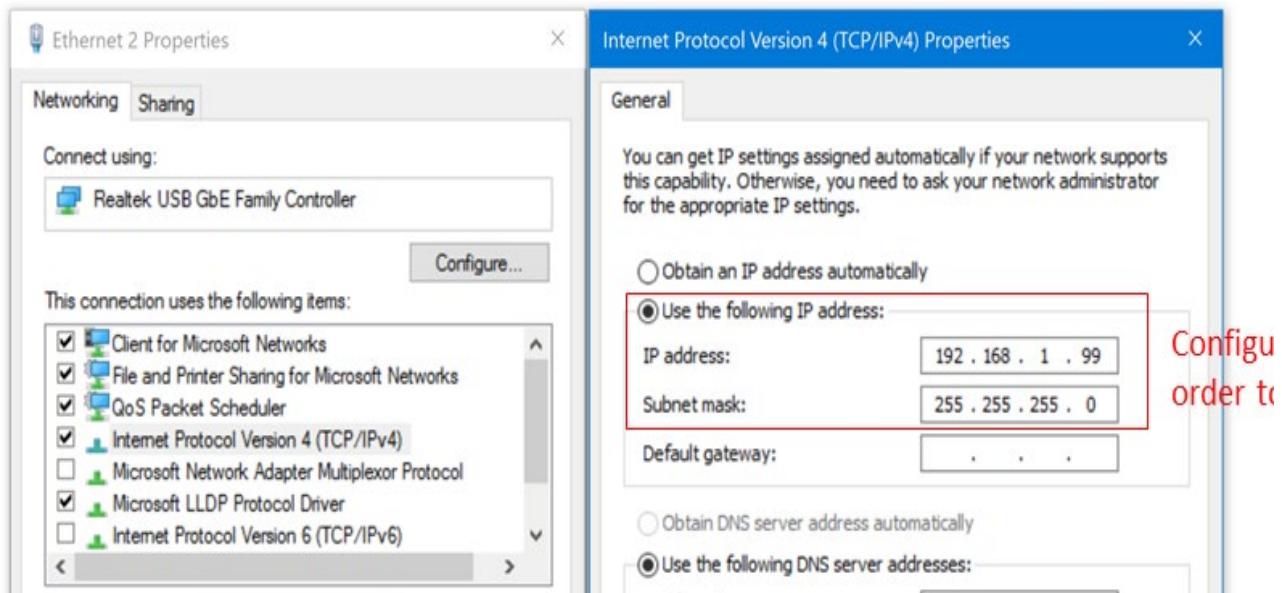
- d. Configure VAP Configuration to establish a Complete Tunnel to SZ1-Public in the SSID. One 1 type of tunnel, Complete/Split, can be established per VAP. The Service Zone selected will map all user traffic (Authentication and Data) to the selected Service Zone. The fixed VLAN is a private VLAN ID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

System Overview

System

System Name	ECW5211-L
Firmware Version	3.43.00
Build Number	1.8-1.9474
Location	EN-A
Site	EN-A
Device Time	2000/01/01 00:10:31
System Up Time	0 days, 0:11:24
CPU/RAM Usage	2.49% / 32.58% Plot

Radio Status

RF Card	MAC Address	Band	Channel	TX Power
RF Card A	00:1F:D4:06:F1:1F	802.11g+n	6	21 dBm
RF Card B	00:1F:D4:06:F1:20	802.11ac	36	20 dBm

LAN Interface

MAC Address	00:1F:D4:06:F1:1D
IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

AP Status

RF Card Name :	RF Card A ▾
Profile Name	VAP-1
BSSID	00:1F:D4:06:F1:1F
ESSID	Guest Network
Security Type	Open
Online Clients	0
TUN	

CAPWAP

Status	Disabled
--------	----------

IPv6

Status	Disabled
--------	----------

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

System

General

System Information

Name :	1st Floor *
Description :	
Location :	1st Floor Office

Configure AP's Name and Location Detail

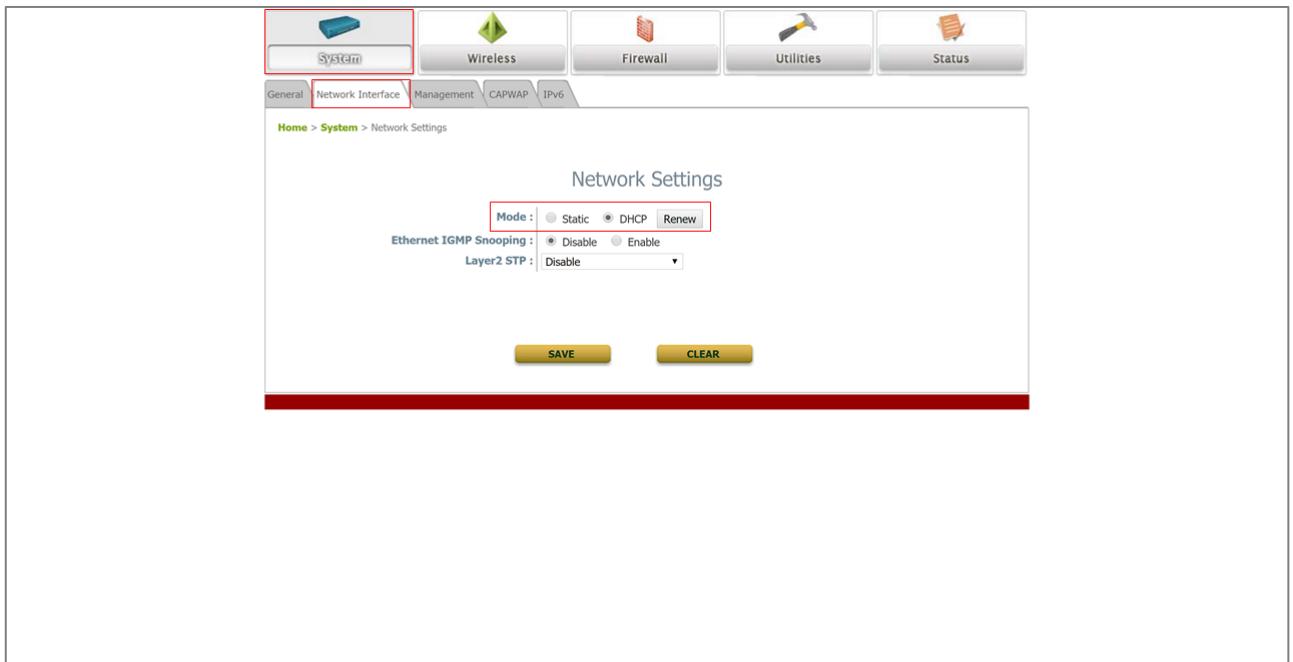
Time

Device Time :	2017/02/22 10:53:38
Time Zone :	(GMT+08:00)Taipei
Time :	<input checked="" type="radio"/> Enable NTP <input type="radio"/> Manually set up
NTP Server 1 :	192.168.1.254 *
NTP Server 2 :	time.nist.gov

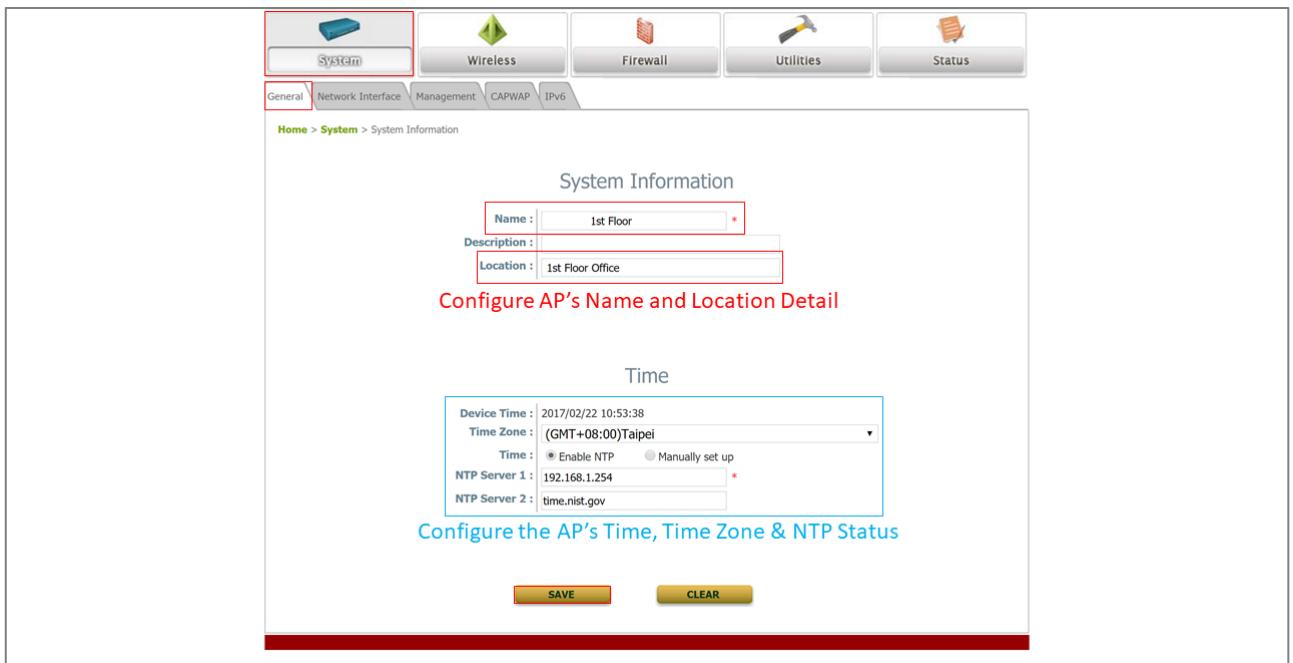
Configure the AP's Time, Time Zone & NTP Status

SAVE **CLEAR**

- 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.

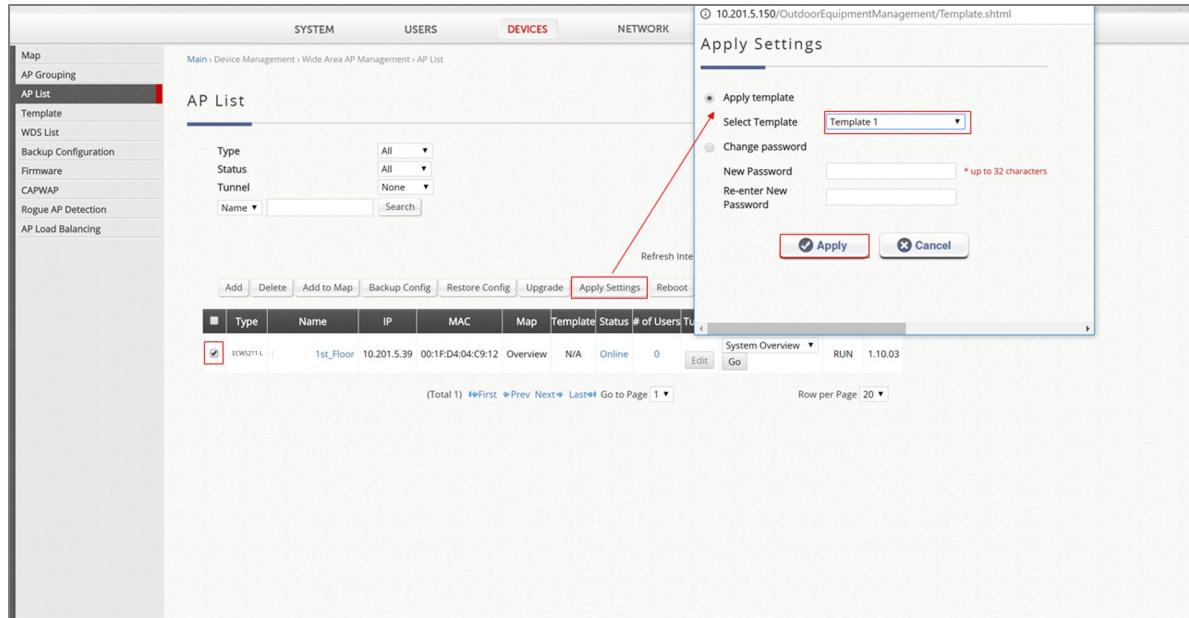
The screenshot shows the CAPWAP Configuration page. The 'System' tab is selected. Under 'CAPWAP', the 'Static Discovery' radio button is selected, highlighted with a red box. To its right, the text 'Enable Static Discovery' is displayed in red. Below this, a table lists 'AC Address' entries. The first entry, '10.70.18.98', is highlighted with a red box and has a red note to its right: 'Fill in Controller's IP address'.

Pri.	AC Address	Remark
1	10.70.18.98	Fill in Controller's IP address
2		
3		
4		
5		

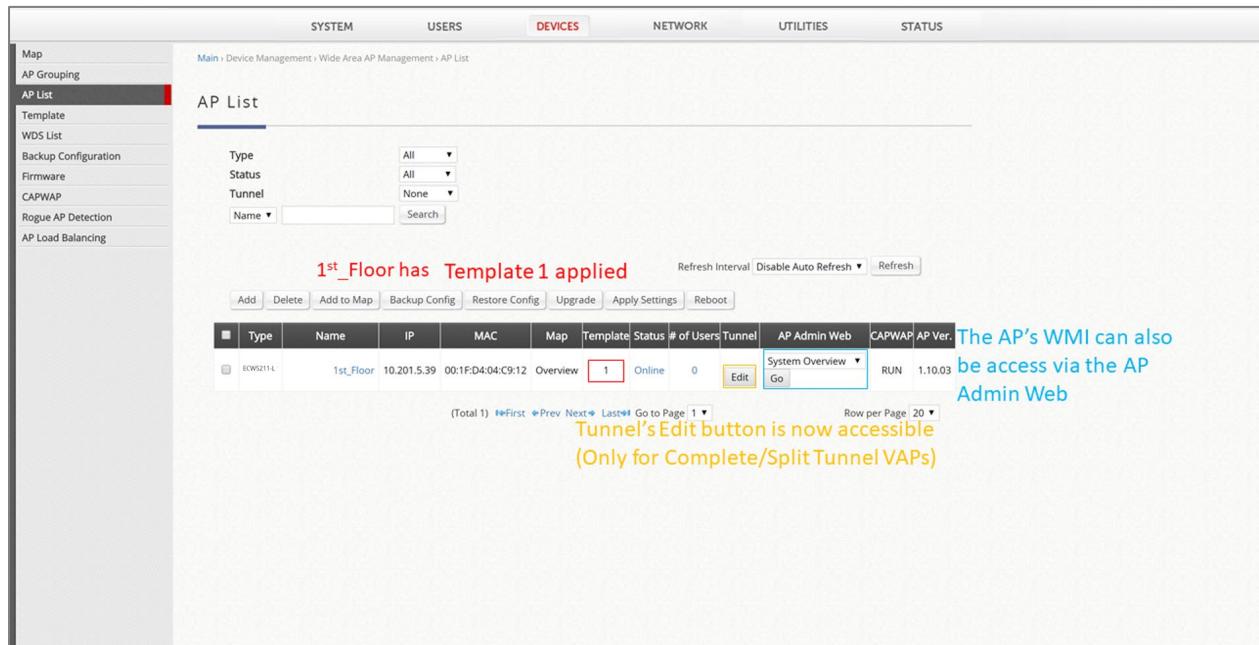
- g. Go to Devices → WAPM → AP List to confirm if the AP is automatically added into the AP List. The CAPWAP Status displaying “Run” means the AP can be managed using the EWS and can be applied a Template.

The screenshot shows the AP List page under the Devices tab. On the left, the 'AP List' option is selected. The main table shows an entry for '1st_Floor'. A red note above the table states '1st_Floor has Template 1 applied'. The 'Edit' button for this entry is highlighted with a yellow box and has a yellow note below it: 'Tunnel's Edit button is now accessible (Only for Complete/Split Tunnel VAPs)'. Another blue note to the right of the table states 'The AP's WMI can also be access via the AP Admin Web'.

- 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

CAPWAP Status & Data Channel

CAPWAP

Status	Run(10.201.5.150)
Data Channel	Active

AP Status

Established Tunnel (Complete or Split) per VAP

Updated VAP

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	00:1F:D4:04:C9:13	AP_Complete	Open	0	

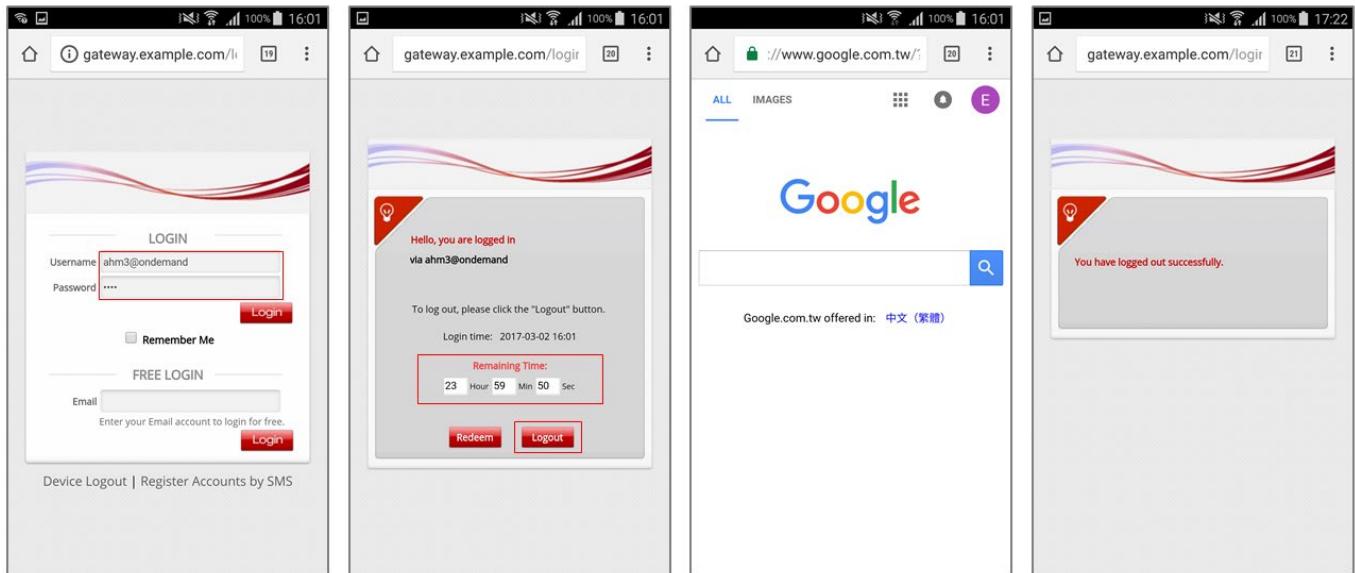
IPv6

Status	Disabled
--------	----------

3.8 Client Login

3.8.1 Client Login - User Flow & Monitoring

- 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.



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

No.	Status	Username	IP Address	IPv6 Address	MAC Address	SZ / VLAN	Group / Policy	Auth. Database	Auth. Method	Pkts In/Out	Bytes In/Out	Access From	Idle (Sec)
1	Online	ahm3@ondemand	172.21.0.108	N/A	E8:50:8B:B5:84:31	SZ1-Public / TN#1.1001	Group 3 / Policy 3	ONDEMAND	UAM	3285 / 3150	462101 / 2469962	1st_Floor	0

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

The screenshot shows the On-Demand Account List page. The left sidebar has a red box around 'On-Demand Accounts' and 'Account List'. The top navigation bar has tabs for SYSTEM, USERS (highlighted in red), DEVICES, NETWORK, UTILITIES, and STATUS. The main content area shows a table with one row for 'ahm3'. The table columns are Username, Remaining Quota, Status, Group, Reference, External ID, and Redeem. The status is 'Normal' and the group is 'Group 3'. Below the table is a pagination bar with '(Valid:1/1400) (Total:1/2000) <First <Prev Next> Last>' and 'Row per Page: 100'.

	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
<input type="checkbox"/>	ahm3	23 hr(s) 20 min(s) 19 sec(s)	Normal	Group 3			Redeem

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

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

The screenshot shows the User Events page. The left sidebar has a red box around 'Logs & Reports' and 'User Events'. The top navigation bar has tabs for SYSTEM, USERS, DEVICES, NETWORK, UTILITIES, and STATUS (highlighted in red). The main content area shows a table with three rows of log entries. The table columns are Type, Date, Name, IP, MAC, and Event. The events listed are 'Create_OD_User', 'OD_User_Login', and 'OD_User_Logout'. Below the table is a pagination bar with '(Total:3) <First <Prev Next> Last>' and 'Row per Page: 20'.

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	E8:50:8B:B5:84:31	OD_User_Login
Ondemand - Mobile	2017-03-02 16:41:25 +0800	ahm3	172.21.0.108	E8:50:8B:B5:84:31	OD_User_Logout

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.