

# **Technical Guide**

# **Basic Configurations**

Released: 2018-08-02

## **Copyright Notification**

## **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.

<sup>©</sup> Copyright 2019 Edgecore Networks Corporation.

# Table of Contents

1	Introduct	tion	2
	1.1	Pre-condition	2
	1.2	Complete Tunnel Network Topology	2
	1.3	Split Tunnel Network Topology	3
2	Configur	ation Flow Guideline	4
3	Configur	ation 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 Flo	w
Steps	User Interface	<b>Configuration Options</b>	Description
<b>1. System</b> 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.
<b>3.1 System</b> 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 CustomizationMessage Page CustomizationDefaultTemplateUploadExternal	Personalize Captive Portal's appearance using built-in customization methods.
<b>4.1 Users</b> Internal Auth. → Local	Local User List	Username Password Group	Create long-term accounts. Ex. Staff, Employees.
<b>4.2.1 Users</b> 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
<b>4.2.2 Users</b> 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	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.

	SYSTEM I	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
			Main C	ategories			
г							1
		We	elcome to S	system Main M	enu		
	This Administrative to manage user ac	ve Web Interface allo accounts and to moni	ws you to set variou: itor user status.	s networking parameters, to c	ustomize network service	\$,	
	Functions are sepa System , Users , N	parated into the follow Network , <u>Utilities</u> , an	wing main categories nd <u>Status</u> .				
	For a quick overvie For shortcut links t	iew of the system, ple to the Dashboard, y	ease refer to the <u>Das</u> ou may click the 4ipr	<u>hboard</u> . et Logo on the top-left, or clie	k the <u>'Dashboard'</u> icon on	the top-right.	
	The <u>'Star'</u> icon on t	the top right is a <u>Set</u>	up Wizard that provi	des a quick step-by-step guid	e on setting up your syste	m.	
	For help with your	ir system configuratio	on, click the 🏆 lcon fo	er Online Help.			
			UI Ov	erview			
LOGIN Username admin Password Configure password? Forgot password? Englise	g In sh v	≁ gin to p	roceed	to the Wel	come Pag	ge	

## 3.1 System - WAN & LAN Interface Configuration

a. Go to System  $\rightarrow$  WAN to configure the WAN1 Interface Type as "Dynamic".

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
General	Main > System > WAN					
IPv6 LAN Ports	WAN1 Configuration					
Port Location Mapping PMS Interface Sub Tabs	Interface Type	<ul> <li>Static (Use the</li> <li>Dynamic (IP si</li> <li>Obtain D)</li> <li>Preferred DNS</li> <li>Alternate DNS</li> <li>PPPoE</li> <li>PPTP</li> </ul>	following IP settings) strings assigned automatic 45 server address automat 5 Server: 168.95.1.1 5 Server: 8.8.8.8	ally Renew		
	WAN2 Configuration	۷	VAN1 (DH	CP)		
	Interface Type	None Static (Use the Dynamic (IP se PPPoE able for	following IP settings) ettings assigned automatic	میں dwidth Co	ntrol)	
	WAN Traffic Settings					
	Bandwidth Limitation	🗷 Enable Bandwi	dth Limitation on WAN			

b. Go to Status  $\rightarrow$  Interfaces  $\rightarrow$  WAN1 to verify WAN1 IP Address.

	SYSTEM	USERS I	DEVICES NETWORK	UTILITIES STATUS
System Summary Interfaces	Main > Status > Interfaces			
Monitor Users Process Monitor Logs & Reports Reporting	Select Interface WAN1 •	WAN1 obta	ained IP Address	
Sessions			WAN1	
Routing Tables	Mode	DHCP	IP Address	10.201.5.150
	MAC Address	00:1F:D4:AB:C1:24	Subnet Mask	255.255.0.0 N/A
L			Traffic Summary	
	Coday tr 9.57 m8 2.7.6 m 8 3.3.3 Mat/s Feb 17 rr 90.55 m8 4.1.5 m 17 rr 90.55 m8 5.1.5 m 10 7.11 Mat/s	yesterday tx 24.14 ms 24.14 ms 2.52 kbit/s Jan '17 tx 20.55 ms tx 20.55 ms 1.67 kbit/s 0 rx	Line 1.75 040 g 0.00 (04) g	
		Daily Traffic	Mor	nthly Traffic
	day         rs         ts           002/2017         0.068         786.05           002/2017         0.688         786.05           002/2017 <td>total         and, rate         er.           0         725 KM         0,07 Mat/r           0         726 KM         0,07 Mat/r           726 KM         0,07 Mat/r         1           726 KM         0,07 Mat/r</td> <td>ta <u>mp 12 34 42 50 10 2000</u> <u>reb 12 34 42 5000</u> <u>reb 12 36000 100 20000</u> <u>reb 12 50000 100 2000</u> <u>ret 12 50000 100 2000</u> <u>ret 12 50000 100 2000</u> <u>ret 1000000000000000000000000000000000000</u></td> <td>104.1         mg, rate         Prr.         % %           110         5.00         10.10         10.00         10.00           14.0         0.00         10.10         10.00         10.00           100         7.11         10.10         10.00         10.00           010         Traffic         10.00         10.00         10.00         10.00</td>	total         and, rate         er.           0         725 KM         0,07 Mat/r           0         726 KM         0,07 Mat/r           726 KM         0,07 Mat/r         1           726 KM         0,07 Mat/r	ta <u>mp 12 34 42 50 10 2000</u> <u>reb 12 34 42 5000</u> <u>reb 12 36000 100 20000</u> <u>reb 12 50000 100 2000</u> <u>ret 12 50000 100 2000</u> <u>ret 12 50000 100 2000</u> <u>ret 1000000000000000000000000000000000000</u>	104.1         mg, rate         Prr.         % %           110         5.00         10.10         10.00         10.00           14.0         0.00         10.10         10.00         10.00           100         7.11         10.10         10.00         10.00           010         Traffic         10.00         10.00         10.00         10.00

c. Go to System  $\rightarrow$  LAN Ports to select "Tag-Based" as the LAN Port Mode and Apply.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
General WAN	Main > System > LAN Ports						
LAN Ports							
Service Zones Port Location Mapping	Port 2 Role	🖲 LAN1 🔍 WAN	2				
PMS Interface	LAN Ports						
	LAN Port Mode	Port-Based When LAN Ports an differentiated by th Based Mode, VLAN Zones. This is need	Tag-Based e set to Port-Based Mode, t e respective LAN ports. Wr s are used to separate traff ed for Port Location Mappi	Service Zones will be ten LAN Ports are set to Tag- fic to different Service ing and Access Point			
	Port - Service Zone Mapping		efault   Default   LAN2 LAN3	LAN4			
			Apply (	Cancel			

d. Go to System  $\rightarrow$  General and click the Configure button beside Management IP Address.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
General	Main > System > General					
WAN						
IPv6	General Settings					
LAN Ports						
Service Zones	Contrary Marrier	1411/2001				
Port Location Mapping	System Name	WHG201				
PMS Interface	Contact Information	When there is a warni	ng of "Please contact your	natwork administrator*		
	HTTPS Certificate	Default CERT V	ing of Thease contact your			
	User HTTPS Login	Enable      Disab	le			
		Secure				
	Internal Domain Name	Use the name on	SSL certificate			
		gateway.example.	.com			
	Portal URL Exceptions (User Agent)	IEMobile/7.0,XBLWP7				
	Station and a state	(e.g. IEMobile/7.0,XBL)	NP7, separate by comma)			
	User Log Access	Enter IP Address Here				
	Pre-Login Page	Configure				
	UAM Filter	Configure				
	Management IP Address	Configure				
	SNMP	Enable Disab	le			
	Suspend Warning Message	Sorry! The service is s	uspended.	*		
	NMS Setting	Configure				
	System Time					
	Current Time	2017/03/02 19:05:18				
	Time Zone	(GMT+08:00)Taipei		•		
	Time Update	NTP Manual	v set up			

- 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.

	SYST	EM USER	S DEVICES	NETWORK	UTILITIES	STATUS							
General WAN IPv6	Management Se	ervice											
LAN Ports Service Zones Port Location Mapping	SSH Service Telnet Service	<ul><li>Enab</li><li>Enab</li></ul>	le Disable Disable Disable	le/Disable SS	H or Telnet fo	r trouble	shooting purposes						
PMS Interface	Management Service Zone List Allowed IPs in configured SZs to access the WHG's WMI												
	Active Sta	tus	Service Zone		IP Address/Segment		Example: PC connected to LAN						
	Defaul		Default	1	92.168.1.254/255.255.255.0		Port to receive an IP of 192,168 X X						
			SZ1-Public		172.21.0.254/255.255.0.0		192.108.7.7						
			SZ2		172.22.0.254/255.255.0.0								
			SZ3		172.23.0.254/255.255.0.0		Example: Clients connected to						
	•		SZ4		172.24.0.254/255.255.0.0		SZ1-Public with an IP of 172.21.0.X <u>cannot</u> enter the WHG's WMI because it is						
	• •		SZ5		172.25.0.254/255.255.0.0								
	• •		SZ6		172.26.0.254/255.255.0.0		unchecked.						
			SZ7		172.27.0.254/255.255.0.0								
			SZ8		172.28.0.254/255.255.0.0								
	Management IP	Address List	Allowed speci	ific IPs & Seg	ments on both	n LAN/W	AN sides						
	No. Act	ive			Example: Allows <b>all</b> IPs								
	1 8	5	0.0.0.0	0/0.0.0.0	4		(0.0.0.0/0.0.0.0) to connect to						
	2 6	1					the WHG's WMI						

## 3.2 Utilities - Admin Password Recovery

a. Go to Utilities  $\rightarrow$  Administrator Accounts and click the "admin" Name to configure password recovery.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Administrator Accounts	Main > Utilities > Administrator Accounts > Edit	Account				
Backup & Restore	Admin Editing and Da	coword Cof	atu Catting			
Network Utilities		3550010 5816	ety setting			
Restart	and the second sec					
System Upgrade	Name	admin				
	Original Password			•		
	New Password					
	New Password			Empil Ac	Idross for D	assword Pacavary
	Verify Password			Email AC	uress for Pa	assword Recovery
	Email	é			Assign SM	TP server Click to setup SMTP server
	Elementary school's name	test		Security	Answer for	Password Recovery
		The elementary :	school's name will identify yo	u, if you for sat you	ratum)	rassword necovery
		password. Note	that, the elementary school's	name can bot be changed,	setup)	
		after apply.				
			@ Anniv	Cancel		
		_	Abbiy	Cancer		
				S. A. S.		

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Administrator Accounts	Main + Utilities + Administrator Accounts						
Backup & Restore Certificates Network Utilities	General Settings						
Restart System Upgrade	Password Complexity	Enable Disat	ble				
		Min Password Leng Min Password Cate	th 6 * (6~20) gory 2 * (2~4)				
	Limit Login Attempts	Enable Inable Inable	ble				
	Password Expiration	Enable Disat	ble				
		Password expires 9	0 • day(s) after crea	ition			
	Password Limits	Enable Initial Enable Initia Enable Initia Enable Initia Enable Initia Enable	ble				
	Access Permission	Configure					
		_	Apply S	Cancel			
	Administrator Accoun	ts					
	Add Delete Lock Admin	Unlock Backup List	Restore List				
	Name IP Addres	s MAC Addre	ess Group		Status		
	admin 192.168.1.5	00:E0:4C:60:E	B:78 Super Gro	up Current Page: Main > Utilities > Admini	istrator Accounts		
	Click Adminis	trator Acco	unt Name	to setup an er	mail acc	ount for pa	ssword recovery/reset

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Administrator Accounts	Main > Utilities > Administrator Accounts > Edit	Account				
Backup & Restore Certificates	Admin Editing and Pa	ssword Safe	ety Setting			
Network Utilities			, ,			
Restart						
System Upgrade	Name	admin				
	Original Password			•		
	New Password					
	Martha Deservered			Email Ad	dress for Pa	assword Recovery
	verity Password					
	Email				Assign SM	TP server CIICK to setup SIVITP server
	Elementary school's name	test		Security	Answer for	Password Recovery
		The elementary s	chool's name will identify y	ou, if you for sat you	otup)	
		password. Note t	hat, the elementary school	s name can hot be changed,	etup)	
		after apply.				
			@ Annly	Cancal		
		_	Abbiy	Calleer		

#### 3.3 System

## 3.3.1 System - Service Zones Configuration

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

Example:

WAN1 IP = Default SZ IP =

10.201.5.150 / Subnet = 255.255.255.0 192.168.1.254 / Subnet = 255.255.0.0

		SYSTEM	USERS	DEVICES		NETWORK	UTILITIES	STATUS
General WAN	Main > System > Servic	e Zone						
IPv6	Service Zo	ne Settings						
Service Zones					NAMES OF A DESCRIPTION OF A DESCRIPTIONO			
Port Location Mapping	Status	Service Zone Name	IP Address	IPv6 Address	VLAN Tag	Default Auth. Option	Network Alias	DHCP Pool
PMS Interface	(ON ())	Default	192.168.1.254	N/A	N/A	Server 1	N/A	192.168.1.1 ~ 192.168.1.100
		SZ1	172.21.0.254	N/A	1	Server 1	N/A	172.21.0.1 ~ 172.21.0.100
		SZ2	172.22.0.254	N/A	2	Server 1	N/A	172.22.0.1 ~ 172.22.0.100
		SZ3	172.23.0.254	N/A	3	Server 1	N/A	172.23.0.1 ~ 172.23.0.100
		SZ4	172.24.0.254	N/A	4	Server 1	N/A	172.24.0.1 ~ 172.24.0.100
		SZ5	172.25.0.254	N/A	5	Server 1	N/A	172.25.0.1 ~ 172.25.0.100
		SZ6	172.26.0.254	N/A	6	Server 1	N/A	172.26.0.1 ~ 172.26.0.100
		527	172.27.0.254	N/A	7	Server 1	N/A	172.27.0.1 ~ 172.27.0.100
		SZ8	172.28.0.254	N/A	8	Server 1	N/A	172.28.0.1 ~ 172.28.0.100
Click S	ervice Zor	ne Name f	to conf	igure ea	ach SZ	Ζ		

- DEVICES NETWORK UTILITIES STATUS SYSTEM USERS General Main -> System -> Service Zone -> Service Zone Configuration WAN IPv6 Basic Settings LAN Ports Enabled
   Disabled
   SZ1-Public
   You may rename the SZ Name
   VLAN Tag
   1 \* (Range: 1 - 4096)
   Change the VLAN Tag
   Tag-based Isolation
   More: When set to "None", the port on a switch connecting to the
   Metwys LAN port "No e Put down if "Loop Protections is enabled on
   the switch and there are 2 VLAN's belonging to this Service Zone.
   Operation Mode
   Nate: When set to "LAN's Belonging to this Service Zone.
   Operation Mode
   Note: When set to "Loop Protections is enabled on
   the switch and there are 2 VLAN's Belonging to this Service Zone.
   Operation Mode
   Note: When set to "Configure
   IP Address 172.21.0.254
   \* Subnet Mask 255.255.0.0
   \*
   Network Alias List
   Configure Service Zones Service Zone Status Port Location Mapping Service Zone Name PMS Interface Network Interface Network Alias List Configure
  This list defines other IP Addresses (range) that are routable in this Service
  Zone. Enabled Configure DHCP Server DHCP Assigned IP Address for AP Management 
   Start IP Address
   172.21.10.1

   End IP Address
   172.21.10.254
   IP Range This defines the range of IP addresses Access Points would use for Local Access Point Management. Authentication Settings
- 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.

	s	YSTEM USERS	DEVICES	NETWORK	ហ	TILITIES	STATUS
Groups Overview	Authentication Settin	gs					<b>^</b>
Configuration							
Authentication Servers	Authentication	Enable      Disable	Suspend Fnak	Disabl	o Auth	onticat	tion on this Service Zone
Internal Authentication		When Authentication is set t	o Suspended, users would see a	suspend	c Auti	critical	tion on this service zone
External Authentication	Access Permission and	message from General Setti	ngs.				
On-Demand Accounts	Authorization	Configure					
Schedule	Default Policy	Policy 1 *					
Blackliste		To set up policies, please go	to Users > Policies.				
Privilege Lists	Portal URL	🖲 Specific 🔘 Original 🛛	None				
Additional Controls		http://www.google.com (e.g. http://www.example.co	• F	Portal URL	opens	specif	fied URL after user is authenticated
	MAC Authentication	Enabled  Disabled RADIUS Authentication using	e MAC address				
	PPP Authentication	Enabled Isabled					
	SIP Interface Configuration	Enabled Disabled					
	WISPr Settings	Configure					
	Authentication Ontions				The second second second	10000104001041	
	Addicidation options	Auth. Option	Auth. Database	Postfix	Default	Enabled	
		Server 1	LOCAL	local	۲	۲	
		Server 2	RADIUS	radius	0	۲	Confirm Authentication Databases
		Server 3	NTDOMAIN	ntdomain			allowed in this Service Zone
		Server 4	LDAP	ldap	0		anowed in this service zone
		Server 5	POP3	pop3			
		On-Demand	ONDEMAND	ondemand			
		SIP	SIP	N/A			
		Guest	FREE	N/A			← Enable Guest (Free Access Database)
	Page Customization						-

#### 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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
General	SIP Interface Configuration	Enabled I Disa	bled			
WAN	WISPr Settings	Configure				
IPv6	Authentication Options	Auth Option	Auth Datab	Poetfix	Default	Enabled
LAN Ports		Addi: Option	Autil: Databa	Positix	Default	Enabled
Service Zones		Server 1	LOCAL	local	٠	8
PMS Interface		Server 2	RADIUS	radius	Θ	
		Server 3	NTDOMAIN	l ntdomain		۲
		Server 4	LDAP	ldap	Θ	
		Server 5	POP3	pop3	0	
		On-Demand	ONDEMAN	D ondeman	d 💿	
		SIP	SIP	N/A		
		Guest	FREE	N/A		
	Page Customization					
	Login Page Customization	Configure	Customize t	he Login Pag	ge (Captiv	ve Portal)
	Message Page Customization	Configure	v clicking t	he Configure	e button	
	0.0		,			
	APs with VAP mapped	to this Servi	ce Zone			
	Lier					
	034					
			Apply 30	ancel		

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

	SYSTEM USERS DEVICES NETWORK UTILITIES STATUS
General WAN IPv6 LAN Ports	Main > System > Service Zone > Service Zone Configuration > Login Page Customization Login Page Customization
Service Zones Port Location Mapping PMS Interface	Service Disclaimer     Default       General Login Page     Default       PLM Open Type Login Page     Default
	PMS Billing Plan Selection Page Default
	Button Color  Upload Logo Choose File No file chosen No File The recommended dimension of the image is 360:120 with a size limit of 512 kB. It will be adjusted if the dimension does not fit.  Apply Cancel Upload your own logo for a customized Captive Portal Note: Applies only to the "Customize with Template"

c. Preview General Login Page in Default mode.

LOGIN Username Password Login	Login with an account
FREE LOGIN Email Enter your Email account to login for free.	Login with self-registration by Email
Device Logout	

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

Edge-corE Networks	Uploaded image file with the recommended resolution
Account Login Username Password Remember Me Email Login Email Login Enter your Email account to login for free. Login Device Logout	Text Culor       Count Login         Login Tole       Account Login         Username       Username         Dogin Button       Login         Remaining Cuota Button       Remain Quota         Guest Header       Email         Guest Mode (who vertification)       Email         Guest Mode (who vertification)       Email account to login for free.         Guest Mode (who vertification)       Check your mailtox to extend usage time after         Guest Login Button       Login         Device Login Undication       Device Logiout         Online Payment Indication       Buy Accounts Online
	SMS indication Register Accounts by SMS Remember Me Remember Me Preview:

## 3.4 Users

#### 3.4.1 Users - Local Accounts

a. Go to Users  $\rightarrow$  Internal Authentication, Local to create accounts using the Local Database.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main > Users > Internal Authentication > Local Aut	thentication				
Authentication Servers						
Internal Authentication	Server No. 1: Server 1 V					
Local						
On-Demand	Local Authentication					
Guest						
External Authentication	Local User List	Configure	Enter the Lo	cal lloor list	to Add/Dele	te/Edit Local Accounts
On-Demand Accounts	Local Oser List	compare		cal Oser List	to Add/Dele	ter Eure Eocal Accounts
Schedule	Account Roaming Out	Enable	Disable			
Policies	802.1X Authentication	Enable	Disable			
Blacklists						
Privilege Lists			Annly	Cancal		
Additional Controls			C Appry	Cancer		

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main > Users > Internal Authentication > Local A	uthentication > Local User	List			
Authentication Servers						
Internal Authentication	Local User List					
Local						
On-Demand	Click Add to cre	ate Local A	Accounts			
Guest	Add Delete Backup List	Upload				Search
External Authentication						
On-Demand Accounts	No Status User	name Password	MAC	Group Activation	Expiration	Remark
Schedule	No. No. Constantion	(T 10/2000) + 1				
Policies		(Tota::0/2000) 🔤	irst • Prev Next• La	Go to Page (Page:1/1)	Row p	er Page: 10 •
Blacklists						
Privilege Lists						
Additional Controls						

	SY	STEM	USERS	DEVICES	NETWOR	K UTILITIES	STATUS
Groups Authentication Servers Internal Authentication	Main > Users > Internal Authen	tication > Local Aut	optionally to Local Ac	bind MAC	Cs Opti Acco	onally configure unt Span	Optionally add a remark
Local On Demand	Username	Password	MAC Address	Group	Ac	ount Span	Remark
Guest	test1			Group 1 🔻	Categorize		
External Authentication	test2			Group 2 🔻	into User		
On-Demand Accounts	Fill in Use	ername		Group 1 V	Groups		
Schedule	& Passwe	ord nairs		Course 1 m	oroups	-	
Policies	Q T d35WC	ora paris		Group 1 V		U.	
Blacklists				Group 1 🔻			
Privilege Lists				Group 1 🔻			
Additional Controls				Group 1 🔻		8	
				Group 1 V			
				Course 1 .		-	
				Group 1 •		U	
				Group 1 🔻			
				Apply	Cancel		

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

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

			SYSTE	м	USERS	DEVICES	NE	TWORK	UTILITIES	STATUS
Groups	Main > Us	ers > Inte	arnal Authentication	on > Local Authent	ication > Local User	List				
Authentication Servers										
Internal Authentication	Loca	Us	er List							
Local		-								
On-Demand										
Guest		Add	Delete Bac	kup List Uploi	ad					Search
External Authentication		outpersonal lite	Statement in case of the local division in t			- 550 petro				
On-Demand Accounts			No Status	Username	Password	MAC	Group	Activation	Expiration	Remark
Schedule			1 Valid	test1	test1		Group 1			
Policies			2 Valid	test2	test2		Group 2			
Blacklists	L									
Privilege Lists				(	Total:2/2000) **Fi	irst +Prev Next+	Last Go to Pag	e 1 • (Page:1/1)	Row	per Page: 10

#### 3.4.2 Users - On-Demand Accounts

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups	Main > Users > Internal Authentication > On-Det	mand Authentication					
Authentication Servers							
Internal Authentication	On-Demand Authenti	cation					
Local							
On-Demand	Licer Postfix	ondemand					
Guest	User Postix	Undernand	lick Config	ure to modify	Rilling Plan	nc .	1.00
External Authentication	Billing Plans	Configure	Chek Coning		y Dining Fiar	13	
On-Demand Accounts	Currency	None • \$	USD ● € EUR ● £ GBI	Select	currency for	On-Demand Account	
Schedule		This is used whe	n the currency is not defined	in the Paypal account. Or			
Policies	Evolved Account Cache	and day(e)	sired monetary unit (max. 5	letters) in the blank held.			
Blacklists	Expired Account Cache	30 day(s)					
Privilege Lists	Out-of-quota Account Cache	30 day(s)					100
Additional Controls	Set Ticket's Serial Number	000001	Set				
	Web Printout	Configure					
		This will be appli On-Demand aco	ed to the regular printer prin ount.	tout when creating a single			
	POS Tickets	Configure					
		Number of Ticke	ets 🖲 1 🗐 2				
		This will be appli can be edited fo	ed to printouts from the PO! r customization.	iticket printer. Templates			
	Terminal Server	Configure					1.1
		Terminal Server	s are add-on devices such as	the SDS100 or SDS200W.			100
	Payment Gateway	Configure					
	SMS Gateway	Configure					
	Account Roaming Out	Enable •	Disable				
		(	Apply	Cancel			

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

		SYSTE	USERS	DEVICES	NETWORK		UTILITIE	ES	STATUS
Groups Authentication Servers	Main⇒Users⇒Int	ternal Authenticati	ion > On-Demand Authentication > Bil	lling Configuration					
Internal Authentication	Billing F	lans							
On-Demand									
Guest	No	Plan Type		Quota		Price (\$)	Active	Group	Function
External Authentication	1	N/A C	lick number to	create a B	illing Plan		0	Group 1	Reset
On-Demand Accounts		NIZA			0			Group 1	Reset
Schedule	2	N/A						Group 1	Reset
Policies	3	N/A						Group 1	Reset
Blacklists	4	N/A						Group 1	Reset
Privilege Lists	5	N/A						Group 1	Reset
Additional Controls	,	N/A						Group i	Reser
	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.

Plan Number	1	
Activation	Usage-time Volume Hotel Cut-off time Duration-time Duration-time	ne/volume/Hotel-Cut-off/Duration-Time
Expiration	Enable Disable  Account will expire in 7 day(s) after activation	Configure Plan parameters: • Activation/Expiration
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.	Quota     Unit Price
Unit Price	\$ USD The unit price cannot exceed 100000, and can take values up to two decimal places.	• Group
Group	Group 3 🔻	
Reference		
	Apply S Cancel	

d. Confirm & Activate the Billing Plan.

		SYSTE	M USERS	DEVICES	NETWORK		UTILITI	ES	STATUS
Groups	Main > Users > In	nternal Authenticati	on > On-Demand Authentication > Bill	ing Configuration					
Authentication Servers									
Internal Authentication	Billing	Plans							
Local									
Guest	No	Plan Type		Quota		Price (\$)	Active	Group	Function
External Authentication	1	Usage-time	1 day(s) of usage time and exp	ired in 7 day(s)		1		Group 3	Reset
On-Demand Accounts		NUA						Cours 1	Pacat
Schedule	4	N/A	Check	k and Appl	y to Activat	te the		Group I	Reser
Policies	3	N/A	confi	gure Billing	Plan			Group 1	Reset
Blacklists	4	N/A						Group 1	Reset
Privilege Lists	5	N/A						Group 1	Reset
Additional controls	-							oroup r	
	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
			E	⊘ Apply	Cancel				

#### 3.4.3 Users - Creating On-Demand Accounts

a. Go to Users  $\rightarrow$  Go to Users  $\rightarrow$  On-Demand Accounts  $\rightarrow$  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.

On-demand User Receipt - Google Chrome			- 🗆 X
① 10.201.5.150/UserAuthentication/OnDemandRecep	t.shtml?buttonNo=1&extic	l=&unit=1&reference=&rand	dom=1487832310403&gen_str=ahm3@ondemand,ra 🔍
	W	elcome!	1
	Username	ahm3@ondemand	Auto-generated
	Password	ra7z	Username/Password
	Plan : Account Type	1 : Usage-time	Assessment Turne & Osseste
	Quota	1 day(s) of usage time and expired in 7 day(s)	Account Type & Quota
	Unit	1 Units	Account Units & Total Price
	Total Price (\$)	1	
	Max User	1	Max User for Usage-time
	Reference		accounts
	External ID		
	ESSID : SSID0		
	Shared Wireless Key: None (Open S	ystem)	
	You have to login before 2017/02/2	4 14:45	Account Activation Time
	The account will be expired in 7 day	(s) after account activation.	
	The	ank You!	
	Send to Pos F Available Optio	rintout Close	

c. Go to Users  $\rightarrow$  On-Demand Accounts  $\rightarrow$  Account List to confirm the created account.

		SYSTEM	USERS	DEVICES	NETWORK	UTI	LITIES	STATUS
Groups	Main > Users > On-Demar	nd Accounts > Acco	unt List					
Authentication Servers								
Internal Authentication	On-Demand	Accoun	t List					
External Authentication								
On-Demand Accounts		Availa	able Actions					
Account Creation	Delete Res	tore List Back	up List Delete Expired	Delete Out of Quota				Search
Account List	E licer	2000	Pempining Queta	Statuc	Group	Poforonco	External ID	Redeem
Schedule	- Osen	laille	Kemaining Quota	Status	Group	Reference	External ID	Kedeelli
Policies	ahr ahr	m3 1 day(s)	)	Normal	Group 3			Redeem
Blacklists		(	On-Demand	Account Info	List			
Privilege Lists			(Valid:1/1400) (Total:1/20	00) **First *Prev Next*	Last Go to Page 1	▼ (Page:1/1)	Row per l	Page: 100 •
Additional Controls								

## 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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups Authentication Servers Internal Authentication External Authentication On-Demand Accounts Schedule Policles Policy Configuration	Main > Users > Policies > Policy Configur A Policy is used to define a Group's a Global Policy is the general policy del Policy is not defined. Select Policy Policy 1 Policy Configurati	ition uthorization in a Service Zone, T ined for all Groups when the Gr Select P on	ne olicy to co	onfigure			
Firewall Privilege QoS Specific Routes Blacklists Privilege Lists Additional Controls	Policy Name Firewall Profile Privilege Profile QoS Profile Specific Route Profile Prefer DHCP Pool	Policy 1 Firewall 1 • Privilege 1 • QoS 1 • Specific Route 1 None •	Choose • Profiles	mapped			
			O Apply	Cancel			

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups	Main > Users > Policies > Firewall Configuration						
Authentication Servers							
Internal Authentication	Select Firewall Profile Firewall 1						
External Authentication							
On-Demand Accounts	Firewall Configuration						
Schedule							
Policies							
Policy Configuration	Firewall Profile Name	Firewall 1					
Firewall	Service Protocols	Configure	Click Configu	e to create Fir	owall Pulos t	Allow/Block access	
Privilege	User Firewall Rules	Configure	Click Conligu	e to creatern	ewan Kules t	O Allow/ Block access	
QoS	Lices Firewall Dules (ID-6)	Configure	to an IP Addr	ess or Domain	Name.		
Specific Routes	User Firewall Rules (IPVO)	comgure					
Blacklists							
Privilege Lists			Apply 1	Cancel			
Additional Controls							

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

		(Contraction)					
	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STAT	US
Groups	Main > Users > Policies > Firewall Configuration >	Firewall					
Authentication Servers							
Internal Authentication	Firewall Profile 1 - Fir	ewall Rules	5				
External Authentication							
On-Demand Accounts		CULA		- Frank II Barla			
Schedule	Add Delete Enable Disable	CIICK A	dd to create a	a Firewall Rule	9		
Policies			Source	Destination			
Policy Configuration	No. Status Activ	on Rule Name	source	bestindton	Service Sch	nedule Operation	n
Firewall			Source Interface	Destination Interface			
Privilege		(Total:0/40) 📭	First +Prev Next+ Last+	Go to Page (Page:1/1)		Row per Page: 20	
QoS							
Specific Routes							
Blacklists							
Privilege Lists							
Additional Controls							

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups Authentication Servers Internal Authentication External Authentication	Main > Users > Policies > Policy Configuratio Policy 1 - Edit Filter	n > Policies > Firewall Config Rule	uration > Firewall > Edit Filter	Rule		
On-Demand Accounts Schedule Policies	Rule Number Rule Name	new BlockFacebook	Enter Rule	Name		
Policy Configuration Firewall Privilege QoS Specific Routes	Source	Interface/Zone IP Address • Subnet Mask MAC Address	ALL •	Sele the I 0.0.0	ct the Source P Address/Su ).0/0.0.0.0 m	e Interface/Service Zone and ubnet Mask. leans all source IP Addresses
Blacklists Privilege Lists Additional Controls	Destination	Interface/Zone Domain Name ▼ Subnet Mask	ALL • www.facebook 255.255.255.2	.com Sele 55 (/32) *	ct the Destin ct either IP A	ation Interface/Service Zone ddress or Domain Name.
	Service Protocol Action Schedule	ALL • • Block • Pass • Always • Rec	curring 🔘 One Time	Sele from	ct to Block or າ Source to D	r Pass traffic estination
		(	Apply	Cancel		

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

		SYSTEM	4	USERS	DEVICES	NETWORK	UTII	LITIES	STATUS
Groups Authentication Servers Internal Authentication External Authentication	Main > Users > Polic	es Firewall Conf Profile 1	figuration - Fire	wall vall Rules					
On-Demand Accounts Schedule	Add	Delete Enable	Disable	Check th	e Firewall	Rule & click Er	nable		
Policies Policy Configuration Firewall	= N	o. Status	Action	Rule Name	Source Source Interface	Destination Destination Interface	Service	Schedule	Operation
Privilege QoS Spacific Pourtes		Disabled	Block	BlockFacebook	ANY	www.facebook.com ALL	ALL	always	Move
Blacklists Privlege Lists Additional Controls				(Total:1/40) teFin	st +Prev Next+ Las	Go to Page 1 💌 (Page: 1	1/1)	Row pr	er Page: 20 •

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups Authentication Servers	Main > Users > Policies > Privilege						
Internal Authentication External Authentication	Select Privilege Profile Privilege 1						
On-Demand Accounts Schedule	Privilege Configuration	1					
Policies Policy Configuration Firewall Privilege QoS Specific Routes Blacklists Privilege Lists Additional Controls	Privilege Name Password Change Maximum Concurrent Sessions Disable timeout for this group	Privilege 1	Disallow (sessions per user) () Disabled () Apply	nfigure preferi	red value for f	Maximum Cc	incurrent Sessions

g. Go to Users  $\rightarrow$  Policies  $\rightarrow$  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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups	Main > Users > Policies > QoS						
Authentication Servers				- Personaliza			
Internal Authentication	Wote: Please enable Bandwidth limitat	ion on waw and restart to	e system for Group Tranic Co	mngurauon.			
External Authentication	1						
On-Demand Accounts							
Schedule							
Policies	Click the hyperlink "B	andwidth li	mitation on				
Policy Configuration	- Click the hyperlink ba	anuwiuum	mation on				
Firewall	WAN" and Enable the	feature.					
Privilege							
Qo5							
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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
General		Obtain DNS serve	address automatically				-
WAN		Preferred DNS Server:	168.95.1.1	*			
IPv6		Alternate DNS Server:	8888				
LAN Ports			0101010				
Service Zones		PPPoE					
Port Location Mapping		PPTP					
PMS Interface							
	WAN Traffic Settings						
	Bandwidth Limitation	C Enable Bandwidth Limit	ation on WAN		Check the Enable	e Bandwidth Limitation on	
		Max Uplink Bandwidth	2000000	Kbps	WAN checkbox a	and configure the Max	
		Max Downlink Bandwid	th 2000000	Kbps	Uplink/Downlink	k Bandwidth.	
	Target for Detecting Internet Connection	Enter IP Address/Domain	Name Here		1		
		Enter IP Address/Domain	<i>Vame Here</i>				
		Enter IP Address/Domain	Name Here				
		Warning of Internet D	sconnection				
		When the addresses for de this message will be shown	tecting internet connecti on the browser.	on are unreachat	ile,		
		Sorry! The service is temp	orarily unavailable.				
		<b>A</b> I	oply 💽 C	ancel			×

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

	SYSTEM	USERS DEVICES NETWORK UTILITIES STATUS
Groups Authentication Servers Internal Authentication External Authentication	Main > Users > Policies > Policy Configuration Policy 1 - Edit Filter	n > Policies > Firewall Configuration > Firewall > Edit Filter Rule Rule
On-Demand Accounts Schedule Policies	Rule Number Rule Name	BlockFacebook Enter Rule Name
Policy Configuration Firewall Privilege QoS Specific Routes Blacklists	Source	Interface/Zone     ALL     Select the Source Interface/Service Zone and the IP Address/Subnet Mask.       Subnet Mask     00.00 (/0)     •       MAC Address     0.0.0/0.0.00 means all source IP Addresses
Privilege Lists Additional Controls	Destination	Interface/Zone     ALL     Select the Destination Interface/Service Zone       Domain Name     www.facebook.com     Select the IP Address or Domain Name.       Subnet Mask     255:255:(32)     Image: Comparison of Compariso
	Service Protocol Action Schedule	ALL       •         • Block       • Pass         • Always       • Recurring         • Always       • Recurring         • One Time

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main > Users > Policies > Specific Routes					
Authentication Servers						
Internal Authentication	Select Profile Specific Route 1 🔻					
External Authentication						
On-Demand Accounts	Specific Routes Con	figuration				
Schedule						
Policies	Specific Poute Profile Name	Specific Doute 1				
Policy Configuration	Specific Route Prome Name Specific Route P					
Firewall	Default Gateway Define Default Gateway: IP Address					
Privilege	Route No.		Destination		Gateway	
Qos	-	IP Address	Subne	t Netmask	IP Address	
Specific Routes			255 255 2	55 255 (/32) ¥		
Blacklists			233.233.2	55.255 (752)		
Additional Controls	2		255.255.2	55.255 (/32) 🔻		
Additional Conditions	3		255.255.2	55.255 (/32) 🔻		
	4		255.255.2	55.255 (/32) 🔻		
	5		255.255.2	55.255 (/32) 🔻		
			255 255 2	5 255 ((22) <b>-</b>		
	0		255.255.2	55.255 (752)		
	7		255.255.2	55.255 (/32) 🔻		
	8		255.255.2	55.255 (/32) 🔻		
	9		255.255.2	55.255 (/32) 🔻		
	10		255.255.2	55.255 (/32) 🔻		
	11		255.255.2	55.255 (/32) 🔻		
	12		255.255.2	55.255 (/32) 🔻		
	13		255.255.2	55.255 (/32) 🔻		
	14		255.255.2	55.255 (/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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups Overview Configuration Authentication Servers Internal Authentication External Authentication On-Demand Accounts Schedule Policies Blacklists Privilege Lists Additional Controls	Main - Users - Groups - Configuration This page gives a summary of access discussion devices Johnson Group Configurat Select Group Group Name Remark Number of devices which allowed to login Allow to logout other devices exceeding the maximum devices	is permissions for each Group in Ei O N Group 1 • Se Employee o are 0 (0 to 9999 devices, For On-Demand a per different billing rices when amount of • Enabled © C For On-Demand a enabled. This setti	Elect Group Rename Configue to Untimited) Counts, number of devices is galars. The number of devices is subted Enable/ Enabled.	to configu e Group re # of allo configured individually following type: LOCAL Disable loo Disable loo Dents devices is always .CCAL POPS, RADIUS,	re owed devices gging out oth	s to login ner device	
	Zone Permission	Configuration &	Policy Assign	iment			Configure Group's
	Enabled	Zone Name	Time Spa	an 1	Time Span 2		Service Zone's
			Schedule	1 🔻	Schedule 1		service zone s
	✓ Service 2	Zone : Default	Policy 1	•	Policy 1	•	network and Policies
	Service 3	Zone : SZ1-Public	Policy 1		Policy 1	•	
	Service 2	Zone : SZ2	Policy 1	•	Policy 1	•	
	Service 2	Zone : SZ3	Policy 1		Policy 1	•	
	Service	Zone : SZ4	Policy 1		Policy 1	•	

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.

		SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups Overview Configuration Authentication Servers Internal Authentication External Authentication	Main > Us This pa the cor Grou	sers > Groups > Overview age gives a summary of which Authen rresponding Group. up Overview	tication Servers are u	sed for			
On-Demand Accounts		Group Name	9		Authentication	Туре	
Schedule				Local			Employee (Group 1) is the
Plackliste				Guest POP3-Server 5			Default Group for all
Privilege Lists	-	Employee		RADIUS-Server 2-Default			Authentiesties Tunes
Additional Controls				NT Domain-Server 3			Authentication Types
Additional Controls				SIP			Group 2 has been selected as
	1215	Group 2		Local			the Local User Account: test2
		Group 3		Billing Plan 1			Group 3 has been selected as
		Group 4					the Crown for the Users Ture
		Group 5					the Group for the Usage-Type
		Group 6					On-Demand Billing Plan 1
		Group 7					
		Group 8					

#### 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.

SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Main > Device Management Welcome to Device Man	agement					
Local Area AP Management Wide Area AP Management	Disable Enter Disable Enter	] Click En	ter after Wide	Area AP Ma	nagement is Enabled	
Click the Disable and select Enabl	Hyperlink e & Apply	♥ WHG20 © 192.16 Wide ₩	I - Google Chrome 8.1.254/OutdoorEquipment Area AP Manage Ide Area AP Management	Aanagement/main.shtr ement	nl sable Sable Cancel	
		٢				

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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Мар	Main > Device Management > Wide Area AP Mana	agement > CAPWAP				
AP Grouping						
AP List	CAPWAP Configuration	1				
Template						
WDS List	CAPWAP Status	🖲 Enable 🔘 Disab	Set CAP	WAP Status as	Enable	
Backup Configuration		OFFAULT -				
Firmware	Apply Certificate to APS	DEFAULT	Select C	ertificates		
Roque AP Detection	Trusted Certificate Authority(CA)	DEFAULT V				
AP Load Balancing	IP Address For Control Channel	100.64.144.254				
	IP Netmask For Control Channel	255.255.255.192 (6	1) • CA	PWAP Control	Channel IP/N	letmask (leave as default
	Control Channel IP Range	100.64.144.193 ~ 100	.64.144.253 <b>un</b>	ess it conflicts	with your ex	isting network)
			Apply	Cancel		
		_				
	Access Controller IP Li	ict				
		151				
	No.	IP Address			Remark	
	1					
	2					
	3					
	4					
	5					
		-				
			Apply	Cancel		

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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Мар	Main > Device Management > Wide Area AP Mar	agement > Template > VAP (	Configuration			
AP Grouping						
AP List	VAP Configuration - T	emplate1				
Template	I					
WDS List	Drofile Name	DE Card A (MAD 1	Select th	e VAP-# for t	he RF Card.	
Backup Configuration	Prome Name	RF Card A : VAP-1			ie in ouron	
Firmware	VAP	Disable 🖲 Enabl	Enablet	he VAP		
CAPWAP	Profile Name	VAP-1				
Rogue AP Detection	ESSID	AP_Complete	Configu	re the ESSID fo	or devices to s	scan and connect
AP Load Balancing	Uplink Bandwidth	0 Kbits/	(1-1048576. 0:Disable	e)		
	Deumlink Randwidth	0 White		-)		
	Downlink Bandwidth	0 KOI(S)	S -(1-1048576, 0.DISADI			
	VLAN ID	Disable     Enabl	e VLAN	is automatica	ally enabled a	ind configured when the
		VLAN ID 1001 *(	1-4094) Servio	ce Zone for CA	APWAP Tunne	el Interface is selected below
	Uplink 802.1p	Best Effort (BE)	•			
	Downlink 802.1p AC Mapping	Background (BK) Bac	ckground 🔻			
		Best Effort (BE) Best	Effort 🔻			
		Excellent Effort (EE)	Best Effort			
		Critial Applications (C	A) Video 🔻			
		Video (VI) Video	•			
		Voice (VO) Voice	•			
		Internetwork Control	(IC) Voice 🔻			
		Network Control (NC)	) Voice 🔻			
	CAPWAP Tunnel Interface	Complete Tunnel 🔻	Colort Co	malata Tuna	al and the Ca	nuise Zono
	Service Zone	SZ1-Public •	Select Co	implete lunn	erand the Ser	TVICe Zone

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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Мар	Main > Device Management > Wide Area AP Mai	nagement > Template					
AP Grouping							
AP List	Template AP Setting						
Template							
WDS List	Select Template	Template1 *	Select the	Template #			
Backup Configuration	Select Template	Templater	Select Cou	ntru Codo			
Firmware	Country Code	USA 🔻	Select Cou	nury code			
CAPWAP	General Settings	Configure	Configure	the General Se	ttings VAP Co	onfiguration	
Rogue AP Detection	VAP Configuration	Configure	Contribute	the deficiency of	terrigo, viti e	onngurution,	
AP Load Balancing	Security Settings	Configure	Security Se	ettings by click	ing each butto	on	
	Secondy Seconds	Configure 1					
	Advanced Wireless Settings	Configure					
	Hotspot 2.0 Settings	Configure					

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.

Map       AP Grouping         AP Grouping       VAP Configuration - Template, VAP Configuration         VAP Configuration - Template - VAP Configuration       VAP Configuration - Template - VAP Configuration         Template       Profile Name       Enable         VAP       Disable       Enable the VAP         Profile Name       VAP -       Enable the VAP         Rogue AP Detection       ESSID       AP-Split         AP Load Balancing       VLAN ID       Image: Configure the ESSID for devices to scan and connect         VLAN ID       Image: Configure the ESSID for devices to scan and connect       VLAN ID         CAPWAP       CAPWAP Tunnel Interface       Select Split Tunnel and the appropriate SZ. If a SZ already has a Complete Tunnel established, a Split Tunnel cannot be established to the same SZ.
Cancer

#### 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.

thernet 2 Properties	×	Internet Protocol Version 4 (TCP/IPv4) Properties	×
working Sharing		General	
onnect using: 🛃 Realtek USB GbE Family Controller		You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	
Configure		Obtain an IP address automatically	
Echine Client for Microsoft Networks	^	Use the following IP address:     IP address:     192, 168, 1, 99	Cont
File and Printer Sharing for Microsoft Networks		Subnet mask: 255 . 255 . 0	orde
<ul> <li>Internet Protocol Version 4 (TCP/IPv4)</li> <li>Microsoft Network Adapter Multiplexor Protocol</li> </ul>		Default gateway:	
Microsoft LLDP Protocol Driver	~	Obtain DNS server address automatically	-
· · · · · · · · · · · · · · · · · · ·		Use the following DNS server addresses:	

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.

Overview Interfaces Associated Clients DHCP Lease Link Stat	us V Event Log V Wireless Log V Monitor
Home > Status > System Overview	
Sys	tem Overview
System	Radio Status
System Name ECW5211-L	RF Card         MAC Address         Band         Channel         TX Power           RF Card A         00:1E:D4:06:E1:1E         802.110±n         6         21.d8m
Firmware Version 3.43.00 Build Number 1 8-1 0474	RF Card B         00:1F:D4:06:F1:20         802.11ac         36         20 dBm
Location	
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	
Interface           MAC Address         00:E94066F1:1D           IP Address         192.168.1.0           Subnet Mask         252.255.255.0           Gateway         192.168.1.254	Profile         BSSID         ESSID         Security Type         Online Clients         TUN           VAP-1         00:1F:D4:06:F1:1F         Guest Network         Open         0         Image: Clients         Image: Clients
CAPWAP	✓ IPv6
Status Disabled	Status Disabled

c. Go to System  $\rightarrow$  General to configure the AP's Name and Time Zone.

	4									
System	Wireless	Firewall	Utilities	Status						
General Network Interface	Management CAPWAP IPv	5								
Home > System > System Information										
		System Informatic	n							
Name : Ist Floor *										
Description :										
	Configure	's Name and Los	ation Detail							
	Comgure Ar	s Name and Loc	ation Detail							
		Time		-						
	Device Time : 201 Time Zone : (G	7/02/22 10:53:38		1						
	Time : ()	Enable NTP Manually set	up							
	NTP Server 1 : 192	.168.1.254								
	NTP Server 2 : time	e.nist.gov	]							
	Configure the <i>i</i>	AP's Time, Time 2	Zone & NTP Stat	us						
	SA	VE								

 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.

				-
System	Wireless	Firewall	Utilities	Status
General Network In	nterface Management CAPWAP	IPv6		
Home > System >	> System Information			
		System Information	on	
	Name :	1st Floor	*	
	Description :	1st Floor Office		
	Configure	AP's Name and Lo	cation Detail	
		Time		
	Device Time : Time Zone :	2017/02/22 10:53:38		
	Time :	Enable NTP     Manually set	up	
	NTP Server 1 :	192.168.1.254	*	
	NTP Server 2 :	time.nist.gov		
	Configure th	e AP's Time, Time	Zone & NTP Stat	us
		SAVE		
				"

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.

	System	Wireless	Firewall	Utilities	Status
General	Network Interface Mana	gement CAPWAP IPv6			
Home	e > <b>System</b> > CAPWAP Config	iration			
	Certific DNS DHCP O Broa Mult	CAPWAP: Di ate Date Check : Di sRV Discovery : Di tion Discovery : Di cast Discovery : Di icast Discovery : Di	PWAP Configurat sable Enable Enable Sable Enable Manage Cer Sable Enable Sable Enable Sable Enable Sable Enable	ion ble CAPWAP ifficates	
	9	itatic Discovery : Discovery :	sable  Enable Enable	ble Static Discovery	
	Pri.	AC Add	ress	Remark	
	1	10.70.18.98	Fill in (	Controller's IP addre	ess
	2				
	3				
	4				
	5				
		SAVI	E CLEAR		

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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Мар	Main > Device Management > Wide A	rea AP Management - AP List					
AP Grouping							
AP List	APlist						
Template	AT LIST						
WDS List							
Backup Configuration	Туре	All 🔻					
Firmware	Status	All 🔻					
CAPWAP	Tunnel	None •					
Rogue AP Detection	Name 🔻	Search					
AP Load Balancing							
	Add Delete Add to Type Name ECW52114 1st	Map Backup Config Rest IP MA Floor 10.201.5.39 00:1F:D4:0	core Config Upgrade A C Map Templa 04:C9:12 Overview 1	e Status # of Users Tunne Online 0 Edit	el AP Admin Web System Overview T Go	CAPWAP AP Ver. RUN 1.10.03	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.

	10.201.5.150/OutdoorEquipmentManagement/Template.shtml
	SYSTEM USERS DEVICES NETWORK
Мар	Main > Device Management > Wide Area AP Management > AP List
AP Grouping	
AP List	A D List   A DD/ template
Template	
WDS List	Select rempiate
Backup Configuration	Type All Change password
Firmware	Status All  Vew Password  * up to 32 characters
CAPWAP	Tunnel None  Re-enter New
Rogue AP Detection	Name  Search Password
AP Load Balancing	
	Apply Cancel
	Refresh Inte
	Add Delete Add to Map Backup Config Restore Config Upgrade Apply Settings Reboot
	Type Name IP MAC Map Template Status # of Users Tu
	System Overview
	Ist_Floor 10.2015.39 00:1F:D4:04:C9:12 Overview N/A Online 0 Edit Go RUN 1.10.03
	(Total 1) #First #Prev Next# Last#I Go to Page 1 * Row per Page 20 *

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.

	SYSTEM USERS DEVICES NETWORK UTILITIES STATUS
Мар	Main - Device Management - Wide Area AP Management - AP List
AP Grouping	
AP List	AD Liet
Template	
WDS List	
Backup Configuration	Туре АІІ •
Firmware	Status All 🔻
CAPWAP	Tunnel None •
Rogue AP Detection	Name  Search
AP Load Balancing	
	1st_Floor has       Template 1 applied       Referesh interval Disable Auto Referesh • Referesh         Add

 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.

<i>?</i> ₀ <b>.</b> .	i 🗱 🛜 📶 100% 💼 16:01	ש אא גע	i 16:01 🕯 🕅 🕅	
00	i) gateway.example.com/lt	☐ gateway.example.com/logir 20 :	☆	gateway.example.com/logir 21 :
			ALL IMAGES III O E	
			Google	
-	LOGIN	Hello, you are logged in		
Pas	ssword ····		<u>م</u>	You have logged out successfully.
	Login	To log out, please click the "Logout" button.	Google.com.tw offered in: 中文 (繁體)	
	FREE LOGIN	Remaining Time:		
	Email	23 Hour 59 Min 50 Sec		
	Enter your Email account to login for free.	Redeem		
Dev	ice Logout   Register Accounts by SMS			

b. Go to Status  $\rightarrow$  Monitor Users  $\rightarrow$  Online Users to monitor online users and view details.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS				
System Summary	Main > Status > User Monitor > Online Users									
Interfaces										
Monitor Users	Online Users List									
Online Users										
Roaming In Users										
Roaming Out Users	Select Mode	Summary 🖲	Detail SUMM	ary view or	Detail viev	V		IP or MAC	Search	
Non-Login Devices	Logout Refresh								Refresh Disable	•
MAC Login Devices							_			
Authenticated Users	No. Status Username	IP Address IPv6 Addr	ess MAC Address	SZ / VLAN	Group / Policy Auth	n. Database Auth. Metho	d Pkts In/Out	Bytes In/Out	Access From	Idle (Sec.)
Process Monitor	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 ON	IDEMAND UAM	3285/3150	462101 / 2469962	1st_Floor	0
Logs & Reports										
Reporting			(Total:1) PFirst	Prev Next + Last+ Go	to Page 1 V (Page:1/1)			Row per P	ige: 50 🔻	
Sessions			Online Use	er with net	work detail	s				
DHCP Leases										
Routing Tables										

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

	SYSTEM	USERS	DEVICES	NETWORK	ហ	TILITIES	STATUS
Groups	Main + Users + On-Demand Accounts + Acco	unt List			1.0.0		
Authentication Servers							
Internal Authentication	On-Demand Account	t List					
External Authentication							
On-Demand Accounts	Delete Restore List Back	up List Delete Expired D	elete Out of Ouota				Search
Account Creation					2	Real Profession	search
Account List	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
chedule	ahm3 23 hr(s	) 20 min(s) 19 sec(s)	Normal	Group 3			Redeem
blicles							
dicklists		04-11-11 (1 (00) (T-+-1-1 (2000)					100 -
ivilege Lists		(valid: 1/1400) (10tal: 1/2000)	WHITST WHITEV Next	Laster Go to Page	(Page: 171)	Row per	Page: 100 •

d. Go to Status  $\rightarrow$  Logs & Reports  $\rightarrow$  User Events to monitor user's events.

Nummary       Nummary         res       Image: Status Lags and Reports User Events         Somator       User Events         War Lag       User Events         Synamic Change Lags       Image: Status Lags and Reports User Events         War Lag       User Events         Somator       Image: Status Lags and Reports User Events         War Lag       User Type         So pera Lag       Image: Status Lags and Reports User Events         War Lag       On-Demand © Guest © Roaming Out © Roaming In © External         So pera Lag       Image: Status Lags and Reports User Events         User Type       Local © On-Demand © Guest © Roaming Out © Roaming In © External         Filter Authentication Type       Image: Status Lags and Reports User Events         User Server Lag       Image: Status Lags and Reports User Events         Indemand 2017-03-02 16:1:14:23 -0600       ahm3       0.0.0.0       Outprotocologic Create: OD, User         Indemand 2017-03-02 16:1:1:25 -0600       ahm3       172:21:0.108       EstosBasEs:43:1       OD, User_Login         Indemand 2017-03-02 16:1:1:25 -0600       ahm3       172:21:0.108       EstosBasEs:43:1       OD, User_Login         Indemand 2017-03-02 16:1:1:25 -0600       ahm3       172:21:0.108       EstosBasEs:43:1       OD, User_Login         <		SYS	TEM USERS	DEVICE	ES N	IETWORK	UTILITIES	STATUS
ces       User Events         s Monitor       Reports         War Log       Usplay Mode         guration (Change Log       Monitor         Work Log       01703.02       Select         You have       01703.02       Select         Filter Time Period       Usplay         You have       0.0.0       Reaming fun External         User Type       0.0.0       0.0.00       Create_OD_User         Outmand       Ondemand       2017-03-02       Select         View Log       Isserver Log       Isserver Log       Isserver Log         Usage       Ondemand       2017-03-02       Local © On-Demand © Guest © Roaming Out © Roaming In © External       Filter Authentication Type         Type       Deta       Type •       Second         Ondemand       2017-03-02       16:11:42:3 +0800       ahm3       0.0.0.0       00:00000000000       Create_OD_User         Ondemand       Mobile       2017-03-02       16:11:42:3 +0800       ahm3       17:22:10.108       E8:50:88:85:84:31       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       Logoin/Logout, User-Idle-Timeout, Session-Timeout	tem Summary	Main > Status > Logs and Report	s > User Events					
viders       User Events         s Monitor       Image: Second Seco	erfaces							
s Monitor Reports WAP Log guration Change Log Monthy Usage Web Log So Opera Log emand Billing Report US Server Log all Usage m Log D Log Events ing ms Leases g Tables Events include the following: Account creation/deletion, User Logen/Logout, User-Idle-Timeout, Session-Timeout and etc.	tor Users	User Events						
Reports       MP Log       Display Mode       Configure         Way Log       guration Change of the Configure       From       Display Mode       Display         Wood Log       So Opera Log       Display Mode       Configure       Filter Time Period       Display         Web Log       So Opera Log       Display Mode       Configure       Filter Time Period       Display         Web Log       So Opera Log       Display Joint Configure       Filter Authentication Type       Search         User Type       Local       On Demand       Guest       Roaming Out       Roaming In       External       Filter Authentication Type         Server Log       Download       Type       Search       S	ss Monitor							
Web tog       Work tog       Usplay         Work tog       Web tog       Select       Filter Time Period         Web tog       Select       Filter Time Period       Select         Web tog       User Type       Local       On-Demand       Guest       Roaming to Letternal       Filter Authentication Type         User rype       User Type       User Type       Search       Search         Usage       Type       Date       Name       P       MAC       Events         Ondemand 2017-03-02 14:14:23 +0800       ahm3       0.0.0.0       00:00000000000       Create_00_User         Ondemand - Mobile       2017-03-02 16:01:44 +0800       ahm3       172.21.0.108       E8:50:88:85:84:31       OD_User_Login         Ondemand - Mobile       2017-03-02 16:01:44 +0800       ahm3       172.21.0.108       E8:50:88:85:84:31       OD_User_Login         Ins       If total:31 ##First #Prev Next # Last# Go to Page 1 • (Page:1/1)       Row per Page: 20 •       Events include the following: Account creation/deletion, User         Iogin/logout, User-Idle-Timeout, Session-Timeout and etc.       Iogin/logout, User-Idle-Timeout, Session-Timeout and etc.	s & Reports	Display Mode	Configure					
And monthy Usage Wonthy Usage Wonthy Usage Wonthy Usage Wonthy Usage Wonthy Usage Wonthy Usage Wonthy Usage Wonthy Usage With To User Type User Type	ofiguration Change Log	From	2017-03-02	Select			Display	
ID       Directory         ID       (D1/L03/2) Select	al Monthly Usage	-		Filte	er Time F	Period		
Sopera Log       User Type       Is Local       On-Demand       Guest       Roaming Out       Roaming U       Roaming In       External       Filter Authentication lype         usserver Log       Isserver Log	I Web Log	10	2017-03-02	Select	<u></u>			
Type       Date       Name       IP       MAC       Events         Server Log       Udsage       nL 0g       Ondemand       2017/03-02 14:14:23 +0800       ahm3       0.0.0       00:00:00:00:000       Create_OD_User         Ondemand       2017/03-02 14:14:23 +0800       ahm3       0.0.0       00:00:00:00:00:00       Create_OD_User         Ondemand       2017/03-02 16:01:44 +0800       ahm3       172.21.0.108       E8:50:88:85:84:31       OD_User_Logout         Searcs       Creates       2017/03-02 16:01:44 +0800       ahm3       172.21.0.108       E8:50:88:85:84:31       OD_User_Logout         Is       Creates       0ndemand - Mobile       2017/03-02 16:01:44 +0800       ahm3       172.21.0.108       E8:50:88:85:84:31       OD_User_Logout         Is       cases       creates       creates       oD       oD       create_OD_User       Create       OD       create       OD       creates	s Opera Log	User Type	🗹 Local 🗹 On-D	emand 🗐 Guest	Roaming Out	Roaming In Extern	nal Filter Au	thentication
US Server Log all Usage m Log D Log Exents aling ns Leases g Tables Leases	Demand Billing Report	Download				Type Y	Search	
Type         Date         Name         IP         MAC         Event           0 Log         Ondemand         2017-03-02 14:14:23 +0800         ahm3         0.0.0.0         0000000000000         Create_OD_User           Ondemand         2017-03-02 14:14:23 +0800         ahm3         172.21.0.108         E8:50:88:85:84:31         OD_User_Login           Ondemand - Mobile         2017-03-02 16:01:44 +0800         ahm3         172.21.0.108         E8:50:88:85:84:31         OD_User_Login           Ing         Ondemand - Mobile         2017-03-02 16:41:25 +0800         ahm3         172.21.0.108         E8:50:88:85:84:31         OD_User_Login           Ing         Croat:33 +PFirst * Prev Next + Last®+ Go to Page 1 •         (Page:1/1)         Row per Page: 20 •            g Tables         Events include the following: Account creation/deletion, User         Login/logout, User-Idle-Timeout, Session-Timeout and etc.	US Server Log							,
Ondemand       2017/03-02 14:14:23:0800       ahm3       0.0.0.0       00:00:00:00:000       Create_OD_User         Ondemand       2017/03-02 14:14:23:0800       ahm3       0.0.0.0       00:00:00:00:000       Create_OD_User         Ondemand-Mobile       2017/03-02 16:01:44:0800       ahm3       172:21:0.108       E8:50:88:85:84:31       OD_User_Login         Is       Indemand-Mobile       2017/03-02 16:41:25:0800       ahm3       172:21:0.108       E8:50:88:85:84:31       OD_User_Login         Is       Indemand-Mobile       2017/03:02 16:41:25:0800       ahm3       172:21:0.108       E8:50:88:85:84:31       OD_User_Login         Is       Intervention       Create_OD_User       Intervention       Row per Page: 20 •       Intervention         Is       Intervention       Create       State       Goto Page 1 • (Page:1/1)       Row per Page: 20 •         Is       Intervention       Intervention       Intervention       Intervention       Intervention         Is       Intervention       Intervention       Intervention       Row per Page: 20 •       Intervention         Is       Intervention       Intervention       Intervention       Intervention       Intervention         Is       Intervention       Interventintex       Intervention       <	III Usage	Туре	Date	Name	IP	MAC	Event	
Log       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 16:01:44 +0800       ahm3       172.21.0.108       E8:50.88:B5.84:31       OD_User_Login         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_Login         seases       (Total:3) H#First ●Prev Next● Last#1 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.	n Log	Ondemand	2017-03-02 14:14:23 +0800	abm3	0.0.0.0	00:00:00:00:00:00	Create OD User	
vents       Ondemand - Mobile       2017/03/02 f6:01:44 -0800       ahm3       172:21.0.108       E8:0388:85:84:31       OD_User_Login         ng       ondemand - Mobile       2017/03/02 f6:01:44 -0800       ahm3       172:21.0.108       E8:0588:85:84:31       OD_User_Login         s       cases       (Total:3) #First @ Prev Next@ Last@f Go to Page 1 v       (Page:1/1)       Row per Page: 20 v         Events include the following: Account creation/deletion, User       Login/logout, User-Idle-Timeout, Session-Timeout and etc.	Log	Chachana	2017 05 02 14.14.25 - 0000	diniis	0.0.0.0		cicule_ob_osci	
ing Ondemand - Mobile 2017-03-02 16:41:25 +0800 ahm3 172.21.0.108 E85088:85:84:31 OD_User_Logout s seases grables Group: Contract: 3) H=First ←Prev Next+ Last+4 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.	Events	Ondemand - Mobile	2017-03-02 16:01:44 +0800	ahm3	172.21.0.108	E8:50:8B:B5:84:31	OD_User_Login	
sees       (Total:3) **First *Prev Next* Last** Go to Page 1 • (Page:1/1)       Row per Page: 20 •         ables       Events include the following: Account creation/deletion, User login/logout, User-Idle-Timeout, Session-Timeout and etc.		Ondemand - Mobile	2017-03-02 16:41:25 +0800	ahm3	172.21.0.108	E8:50:8B:B5:84:31	OD_User_Logout	
bles Events include the following: Account creation/deletion, User login/logout, User-Idle-Timeout, Session-Timeout and etc.			(Total:2) Incirct		Go to Page 1 V	(Page:1/1)	Pow per Page: 20	
Events include the following: Account creation/deletion, User login/logout, User-Idle-Timeout, Session-Timeout and etc.	ases		(Total.5) ****	errev wexter coste	Go to rage 1.	(roge. (r))	Now per rage. 20	
login/logout, User-Idle-Timeout, Session-Timeout and etc.	Tables	Events	include the fo	ollowing:	Account	creation/c	eletion. Us	er
login/logout, User-Idle-Timeout, Session-Timeout and etc.						· -·		
		login/i	ogout, User-Id	ale-Timec	out, Sess	ion-Timeou	ut and etc.	

## **4** Remarks

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