# Application Scenario Guide Enterprise

Release: July 2017 Release Version: R1

#### TABLE OF CONTENT

1	INTRODU	CTION	2
2	PROJECT	REQUIREMENTS	2
	2.1 FEAT		2
3	PROPOSE	ED SOLUTION	3
	3.1 BOM 3.2 NETW 3.3 EXPE 3.3.1 Ca 3.3.2 St	I: VORK TOPOLOGY: CTED RESULTS: aptive Portal with Company Logo taff and Guest connect to the same SSID	3 3 3 3 3
4	CONFIGU	RATION	9
	<ul> <li>4.1 CONF</li> <li>4.2 SYSTI</li> <li>4.3 SYSTI</li> <li>4.4 SYSTI</li> <li>4.5 UTILIT</li> <li>4.6 SYSTI</li> <li>4.7 SYSTI</li> <li>4.8 USER</li> </ul>	FIGURATION CHECKLIST TEM – INITIAL ACCESS BROWSER-BASED GUI TEM – WAN & LAN INTERFACE CONFIGURATION TEM - MANAGEMENT IP ADDRESS LIST TIES - ADMIN PASSWORD RECOVERY TEM - SERVICE ZONES CONFIGURATION TEM - SERVICE ZONE – CAPTIVE PORTAL CUSTOMIZATION RS - LOCAL ACCOUNTS	9 10 12 13 13 14 17 19
	4.9 USER 4.10 USER <i>4.10.1</i>	RS – GUEST AUTHENTICATION RS – USER POLICIES CONFIGURATION Guest Users → Policy 1 profile configuration	21 22 22
	4.9.1 Sta 4.10 USER 4.11 USEV 4.11.1 4.11.2 4.11.3	taff Users $\rightarrow$ Policy 2 profile configuration RS – USER GROUPS CONFIGURATION WAPM ON EWS TO MANAGE ECW Edit WAPM Templates Establish CAPWAP Tunnel from AP to EWS Applying the template	
	4.12 1+1 H 4.12.1 4.12.2 4.12.3 4.13 REPC 4.13.1 4.13.2	HIGH AVAILABILITY Configure EWS#1 HA Configure EWS#2 Confirm HA status of both EWS DRTING Notification FTP Setting	
	4.13.3 4.13.4	SMTP Setting	39 39

# 1 Introduction

In this Application Scenario Guideline we will illustrate an actual Enterprise deployment, including its requirements and the corresponding solution and configurations.

The purpose of this guideline is to provide step-by-step configuration instructions that may also be applied to other enterprise deployments.

# 2 Project Requirements

### 2.1 Deployment Requirements:

	Enterprise Building Wi-Fi										
-	Wall or ceiling mounted										
-	Dual-band 2x2 MIMO Technique										
-	Coverage is the top priority										
-	External antenna										
-	Extra LAN port with PoE downlink capability										
	Network Gateway-Controller										
-	Estimated 3500 concurrent users										
-	Centralized manage 1200 APs										
-	Standby unit for service redundancy										

#### 2.2 Feature Requirements:

### Wi-Fi Features

- Customizable Captive Portal (Login Page) for guest to submit credentials
- User Authentication for granting Wi-Fi access
- SSID with WPA2-Enterprise security (802.1x Transparent Login)
- Multiple concurrent devices login limit via the same account
- Centralized Management for APs at each site
- Built-in DHCP server in solution to allocate IP addresses to all users

#### Administrator Features

- 1+1 High Availability to maintain network service
- Periodic Usage Reports to track
- GUI permission for Staff only
- Websites access limitation for Staff users

# **3 Proposed Solution**

### 3.1 Recommended Edgecore Models:

E	CW		EWS
GE	5088300 <sup>°</sup>		
- 802.11ac wave	e 2 Dual-band	-	5000 recommended concurrent
- 2x2 MIMO			users
- Internal antenr	nas in	-	1200 APs managed
2.4GHz/5GHz	, 2dBi/2dBi, 3 dBi	-	High Availability 1+1
(BLE)		-	Power Redundancy
- Output power	2.4GHz/5GHz,		
18dBm/19 dBr	n		

Location	Area	AP Model	QTY
Factory	500m <sup>2</sup> x 40 sties	ECW	400
Office	300m <sup>2</sup> x 40 floors x 2 buildings	ECW	800

#### 3.2 Network Topology:

#### **3.3 Expected Results:**

#### 3.3.1 Captive Portal with Company Logo

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

	dge-core <sup>®</sup> TRANSFORMING THE WAY THE WORLD CONNECTS
LOGIN Username Password	Login Username Password Login

#### 3.3.2 Staff and Guest connect to the same SSID

#### User Login Flow (UAM) – Staff/Guest account

After connecting to the SSID, a Service Disclaimer page will pop up. The user will need to tick the checkbox and click on the Confirm button move on to the Login Page. Enter staff/staff for the username/password or complete the E-mail field and click Login. The Login Success Page will show up after.

Settings Wi-Fi	< • 905.	Ca	台湾大哥大 En ncel	ter the p	10:51 assword nter Pa	for " <del>dipash</del> ssword	Hotel"	≠ ø 99% ■ Join	 ・ 台湾大哥大 10:51 AM gateway.example.com intigeneticited	Cancel	· ····	◎ 台湾大哥大 >	10:52 AM gateway.example.com	Cancel	• •••• <	○台湾大哥大 ♥	10:52 AM gateway.example.com	→ ♥ 99% ■
WI-FI		Pas	sword	••••	••••													
.seanComplete .SeanSplit .seanSplitNAT *connecting-0019E04048 digmet-Hotes	+ ♥ () + ♥ () + ♥ () 1810 ♥ () ♥ ()								Service Disclaimer Weinen to Agnori Heel Internet access service Before you proceed, please acknowledge hur. 11) There may be interruptions to the service du technical reasons beyond our cortex. 21) There may be interruptions of the information reason with the service. 21) There may be interruption or material appropriateses of the information or material appropriateses and their firewater depending the service.	to ontained the ay be on the		Usernan Passwoi Emi	Account Login	ogin.		Hello staff	you are logged in via out, please cick the "Logout" butto Logon time: 2017-03-17 10-5	и.
		1	2 3	4	5	6 7	8	9 0	I agree with the above terms and control of the second	nditions				Login				
		•	1 :	;	(	)\$	&	@ "										
		#+= A	.BC	•	? spa	! ce	ľ	Join										

#### User Login Flow (WPA2-Enterprise) – Staff account

Client devices associated with the SSID and enter the account username/password to authentication. Once the profile been build and trust, the device could auto transparent connect to the same SSID, simplify the user login flow.

••· 台湾大哥大 4G 4:13 J Settings Wi-I	™ 52% ■_` Fi	****c <u>é</u>	滴大哥大	: 4G Enter th	ne pass	4:13 PM	a or "cip-	802.1)	e"	52% 💶 )	••••• 台湾大哥; Cancel	t 4G 4:15 PM Certificate	52%
Wi-Fi		Car	ncel		Ente	r Pass	word			Join			
HOOSE A NETWORK		Use	rname	Aipe								ateway.example.com ssued by gateway.example.com	n
_Estee Lauder-Guest	<b>२</b> (i)	Pass	word	•••	•							Not Trusted	
171	• 🗢 🕕										Expires '	13/08/2020, 10:36:37 AM	
	<b>〒</b> (i)										More Deta	ils	>
	<b>२</b> (i)												
532421	∎ <del>ຈ</del> (j)												
ASUS	● ╤ ()												
cip-802.1x	<b>≜</b> ╤ (j)												
cip-psk	∎ <del>ຈ</del> (j)												
DIRECT-D7-HP DeskJ	et 5820 s 🔒 후 🚺	q	w	e	r	t y	/ ι	L	i	q q			
hinet	<b>a</b>	а	s	d	f	g	h	j	k	I			
HSG326_TEST_RFA			7	x	c	v	h	n	m				
ITC	<b>▲</b> ╤ (j)		-	Ê	Ľ	Ľ	<u> </u>	<u> </u>	_				
Luxury Free	<del>?</del> (j)	123	۲			space	•		re	turn			

#### Facebook access blocked for Staff accounts

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

●●●○台湾大哥	∃大 令	10:54 AM	7 🛛 99% 🗖
← http	os://www.	facebook.com	2
B.			
This	site ca	n't be reach	ned
www.fa	cebook.co	om took too long to	respond.
Try: Checking	the conne	ection	
ERR_CON	NECTION_T	IMED_OUT	
		RELOAD	
		DETAILS	

#### Real time and daily network usage reports

When the user successfully associates to the SSID, AP's Associated Clients List will display each of their connection details. By clicking Plot button, administrator may check the real-time plotting diagram about user traffics. By clicking Kick button, administrator may manually disconnect this user.



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

	SYSTEM	USERS DE	VICES N	NETWORK L	TILITIES STATUS
System Summary Interfaces	Main - Status - User Monitor - Non-Login Devi	265.			
Monitor Users	Non-Login Devices Li	st			
Online Users					
Roaming In Users	Defresh				Befrech Directio
Roaming Out Users	- Netter				Reiresn Disable
Non-Login Devices	MAC Address	IP Address	VLAN ID	Service Zone	Associated AP
MAC Login Devices	- CONST	IPv4:192.168.1.1			
Authenticated Users	00:1P:D4:D7:A8:28	IPv6:N/A	0	Default	N/A
WiFi Monitor	No. on on one of the other	IPv4:192.168.1.158	0	Default	EAD705-1st Rm1
Process Monitor		IPv6:N/A		Denidit	Cross in Ann
Logs & Reports		(Total:2) seFirst e Prev N	lext + Last++ Go to Pag	ge 1 3 (Page:1/1)	Row per Page: 50
Reporting					
Sessions					
DHCP Leases					
Routing Tables					

	SYS	TEM	USERS	DEVICES	NETV	ORK	UTILITIES	STATU	s			
System Summary	Main - Status - User Monitor - Online	Isers										
nterfaces												
ionitor Users	Online Users List											
Online Users												
Roaming In Users												
loarning Out Users	Select Mode	Sun	nmary Obtail							IP or MAC	Sea	rch
Non-Login Devices	Logout Refresh										Refresh Disable	0
MAC Login Devices			_						_			
Authenticated Users	No. Status Userna	me IP Addre	ss IPv6 Address	MAC Address	SZ / VLAN	Group / Policy	Auth. Database	Auth, Method	Pkts In/Out	Bytes In/Out	Access From	Idle (Sec.
IFI Monitor	1 Online popporterve	192.168.1.1	58 N/A		Default / 0	Guest / Policy 1	FREE	UAM	957/622	801218 / 169168	EAP705-1st Rm1	0
ocess Monitor												
ogs & Reports			(To	tal:1) ##First #Prev I	Next + Last++	Go to Page 1	(Page:1/1)			Row per Pag	ge: 60 🖸	
enorting												

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

		SYSTEM	USERS		DEVICES	NET	WORK		UTILI	TIES	STATUS				
System Summary	Main - Status - Li	ogs and Reports - User Events													
Interfaces															
Monitor Users	User Ev	ents													
WiFi Monitor															
Process Monitor		-		-											
Logs & Reports	Display Mod	Co Co	nfigure	Calar		-	- /1 1								
CAPWAP Log	From	201	7-03-17 Select	Selec	to display Mot	le/ I Im	e/User		_ E	Display					
Configuration Change Log	То	201	7-03-17 Select	Type	to display the	warn	eu inio								
Local Monthly Usage	Hans Turns		acal C On Demand	Cuert O B		ming In (	Externa	1							
Local Web Log	User Type	0.0	ocar _ on-penand	Guest U H		tuning in t	Excerna								
Micros Opera Log	Download				Type		0		1	Search					
On-Demand Billing Report															
RADIUS Server Log	Туре	Date	Name		MAC	Vian IC	Event	Group	Policy	Max Download	Max Upload	Req Download	Req Upload	Packets In	Packets o
SIP Call Usage	Local - Mobile	2017-03-17 10:52:16 +0800	staff@local	192.168.1.158		0	Login	Staff	2	Unlimited	Unlimited	Unlimited	Unlimited	0	0
System Log															
UAMD Log	Local - Mobile	2017-03-17 10:57:10 +0800	starrenocal	192.168.1.158	COLORGIA DI MANA	0	Logout	Staff	2					12789	12193
User Events	Guest - Mobile	2017-03-17 10:58:21 +0800	Support Collipson to the	192.168.1.158	81709D-79-08-84	0	Login	Guest	1	1 mbit	1mbit	512kbit	512kbit	0	0
Reporting	Guest - Mobile	2017-03-17 11:01:12 +0800	support of the second	192.168.1.158		0	Logout	Guest	1					16674	11547
Sessions															-
DHCP Leases		π	otal:4) INFirst Prev	Next + Last++ (	Go to Page 🚺 🔁 🛛	Page:1/1)		Ro	ow per Pa	ge: 20 🖸					
Routing Tables															

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



**GUI permission only for Staff Users** Check the appropriate SZs and the preferred IP Addresses to allow access

#### permission.

	SYSTEM	USERS DEV	/ICES NETWORK	UTILITIES	STATUS	
General WAN IPv6	Management Service					· · · · · ·
LAN Ports Service Zones Port Location Mapping PMS Interface	SSH Service Telnet Service Management Service	Enable Disable     Enable Disable     Disable Zone List Allov	Enable/Disable purposes ved IPs in confi	e SSH or Telno gured SZs to a	et for tro access th	ubleshooting e EWS's WMI
	Active Status	Service Zone		IP Address/Segment		Example: PC connected
	8 (10)	Default		192.168.1.254/255.255.255.0		to LAN Port to receive
	0	SZ1-Public		172.21.0.254/255.255.0.0		an IP of 192.168.X.X
		SZ2		172.22.0.254/255.255.0.0		
	0 ()	SZ3		172.23.0.254/255.255.0.0		Example: Clients
		SZ4		172.24.0.254/255.255.0.0		connected to SZ1-Public
		SZ5		172.25.0.254/255.255.0.0		with an IP of 172.21.0.X
	0 (10)	SZ6		172.26.0.254/255.255.0.0	6.5	cannot enter the EWS's
	0.000	SZ7		172.27.0.254/255.255.0.0		wivil because it is
	· ()	SZ8		172.28.0.254/255.255.0.0		unchecked.
	Management IP Addr	ess List Allowe	d specific IPs &	Segments or	both LA	N/WAN
	No. Arthur	sides	ID Address/Segment			
	No. Active		n Address/Segment			Example: Allows <u>all</u> IPs
	2		0.0.0.0.0.0.0		En l	to the EWS's WMI

# 4 Configuration

## 4.1 Configuration Checklist

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

	- Devices > WAPM > AP List	
	- Establish CAPWAP Tunnel from	
	AP to EWS	
3.13 1+1 High Availability	- System > High Availability	
	- Status > Reporting > Notification	
	<ul> <li>Status &gt; Reporting &gt; FTP Setting</li> </ul>	
3.14 Reporting	<ul> <li>Status &gt; Reporting &gt; SMTP Setting</li> </ul>	
	- Status > Reporting > Syslog	
	Setting	

#### 4.2 System – Initial Access Browser-based GUI

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

Edge-corE <sup>®</sup>						■Dashboard ★Setup Wizard ?Help ⊕Logout
	SYSTEM USER:	DEVICES	NETWORK I	UTILITIES	STATUS	Shorteuts
		Main (	Categories			
		Welcome to S	System Main Menu	I.		
	This Administrative Web to manage user account	Interface allows you to set variou ; and to monitor user status.	s networking parameters, to customiz	ze network services,		
	Functions are separated System, Users, Network	into the following main categorie: , <u>Utilities</u> , and <u>Status</u> .	5:			
	For a quick overview of t For shortcut links to the	ne system, please refer to the <u>Das</u> Dashboard, you may click the 4ipr	i <del>hboard</del> . het Logo on the top-left, or click the <u>'D</u>	Dashboard' icon on the	top-right.	
	The <u>'Star</u> ' icon on the top For help with your system	right is a <u>Setup Wizard</u> that provi n configuration, click the <u>"</u> lcon fo	des a quick step-by-step guide on seti or Online Help.	tting up your system.		
		UI O	verview			
LOGIN Username admin Password	Log In	n to proceec	l to the Welcc	ome Pag	e	

**Note**: first time login will require changing the password.

#### 4.3 System – WAN & LAN Interface Configuration

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

and the second se			DEVICES	NETWORK	UTILITIES	STATUS
General WAN IPv6 LAN Ports	Main-System-WAN WAN1 Configuration	Set WAN1	Interface	e with Sta	atic IP add	dress with other details
High Availability Service Zones	Physical Mode	Auto				
Port Location Mapping	Interface Type	Static (Use the following IP s	ettings)			
PMS Interface		IP Address:	10.201.5.66	<b>.</b>		
Cub Taba		Subnet Mask:	255.255.0.0	<b>□</b> •		
Sub Tabs		Default Gateway:	10.201.1.254			
		Preferred DNS Server:	168.95.1.1			
		Alternate DNS Server:	8.8.8.8			
		O Dynamic (IP settings assigne	d automatically)			
		OPPTP				

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

	SYSTEM	USERS	DEVICES	NETWORK UTI	LITIES STATUS
System Summary	Main - Status - Interfaces				
Interfaces					
Monitor Users	Select Interface WAN1 0				
WiFi Monitor					
Process Monitor	Network Interface				
Logs & Reports					
Reporting					
Sessions	a differentia de la constitución de	A CONTRACTOR OF THE OWNER OW	WAN1		CHILDREN IN CONTRACTOR
DHCP Leases	Mode	STATIC	IP Address	10.	201.5.66
Routing Tables	MAC Address	00:1F:D4:03:9C:35	Subnet Mask	255	.255.0.0
	IPv6 Address	N/A	IPv6 Prefix		N/A
	Auto-Negotiation	On	Speed / Duples	100	Mb/s Full
			Traffic Summary		
	Contrast 10 20 10 10 10 10 20 10	yesterday 12.13.13.00 3.12.14.15.00 3.12.15.00 12.13.00 3.12.10.15.00 12.13.00 12.13.00 12.13.00 12.13.00 12.13.00 12.13.00 12.13.00 12.13.00 12.13.00 13.13.00 13.13.00 14.13.00 14.13.00 14.13.00 15.13.00	L1 time 1.01 018 ± 2.05 018 ± 2.05 018 ± 2.05 018 ± 10 10 10 10 10 10 10 10 10 10 10		13 14 15 16 17 19

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
General WAN	Main - System + LAN Ports						
IPv6 LAN Ports	Port Assignment						
Service zones Port Location Mapping PMS Interface	Port 2 Role	■ LAN1 ○ WAT	N2				
Print Hearing	LAN Ports						
	LAN Port Mode	Port-Based When LAN Ports a differentiated by t Based Mode, VLM Zones, This is need Management.	Tag-Based     reset to Pert-Based Mode,     he respective LAN ports. W     sare used to separate tra     ded for Port Location Mapp	Service Zonies will be sen LINP Ports are set to Tag- fic to different Service ing and Access Point			
	Port - Service Zone Mapping		Default *				
		[	Apply	Cancel			

#### 4.4 System - Management IP Address List

Go to System > General > Management IP Address List 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	System Name	WHG201					
ort Location Mapping	Contact Information						
MS Interface		When there is a w	aming of "Please contact yo	ur network administrator"			
	HTTPS Certificate	Default CERT 🔻					
	User HTTPS Login	Enable 🖲 Di	sable				
	Internal Domain Name	Secure					
	internal Domain Name	<ul> <li>Use the name</li> <li>gateway exam</li> </ul>	on SSL certificate				
	Portal LIPI Exceptions (Liser Agent)	IEMobile/7.0 XBI W	/P7				
	Fortal one Exceptions (oser Agent)	(e.g. IEMobile/7.0,)	KBLWP7, separate by comm	a)			
	User Log Access	Enter IP Address F	lere				
	Pre-Login Page	Configure					
	UAM Filter	Configure					
	Management IP Address	Configure					
	SNMP	🔍 Enable 💌 Di	sable				
	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)Taipe	ei				
	Time Update	NTP Man	ually set up				

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

	S	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS		
General WAN IPv6	Management	Service							
LAN Ports Service Zones Port Location Mapping PMS Interface	SSH Service Telnet Service		<ul> <li>Enable</li> <li>Disal</li> <li>Enable</li> <li>Disal</li> </ul>	ble Enab	le/Disable S	6H or Telnet	for trouble	eshooting purposes	
	Management	Service	Zone List A	llowed IPs	s in configure	ed SZs to acc	ess the EW	/S'S WIVII	
	Active	Status	Servi	ce Zone		IP Address/Segment		Example: PC connected to	
	8	ON ()	Di	efault	1	92.168.1.254/255.255.255.0	•	LAN Port to receive an IP of	
	6	ON (	5Z1	-Public		172.21.0.254/255.255.0.0		192.168.X.X	
	Ð	e orr	10	SZ2		172.22.0.254/255.255.0.0			
	0	() orr	1	SZ3		172.23.0.254/255.255.0.0		Example: Clients connecte	
	0	011	ja -	5Z4		172.24.0.254/255.255.0.0	5.00	to SZ1-Public with an IP of	
	0	e orr	3	SZ5		172.25.0.254/255.255.0.0	E.A.	172.21.0.X cannot enter the	
	0	() orr	ä	SZ6		172.26.0.254/255.255.0.0	100	EWS's WMI because it is	
	0	() or	3	SZ7		172.27.0.254/255.255.0.0	24 F	unchecked.	
	Ð	e orr	3	5Z8		172.28.0.254/255.255.0.0			
	Management	IP Addre	ess List Allo	wed spec	ific IPs & Seg	ments on bo	oth LAN/W	AN sides	
1									
	NO.	Acuve		0000	Address/Segment			Example: Allows <u>all</u> IPs	
				0.0.0.0/	10.0.0			to the EW/S's W/MI	

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

#### 4.5 Utilities - Admin Password Recovery

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

		OBLIG	DETIGED	NETWORK	UTILITIES	STATUS				
Administrator Accounts	Main > Utilities > Administrator Accounts									
Backup & Restore										
Certificates	General Settings									
Network Utilities										
Restart	Password Complexity	Enable Disal	ble							
system opgrade										
		Min Password Leng	th 6 * (6~20)							
		Min Password Cate	gory 2 * (2~4)							
	Limit Login Attempts	🔍 Enable 💌 Disal	ble							
	Research Eveloption									
	Password Expiration	Enable Usal	ble							
		Password expires	• day(s) after cr	eation						
	Password Limits	🔍 Enable 🗶 Disable								
	Access Permission	ermission Configure								
		_	Apply	Cancel						
	Administrator Accou	nts								
	Add Delete Lock Admin	Unlock Backup List	Restore List							
	Name IP Address	ss MAC Addr	ess Group	,	Status					
	admin 192.168	99 00:F0:4C:60:F	B:78 Super Gr	Current Page:						
			and the second s	Main Main . Utilities	dministrator Accounts					

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Administrator Accounts Backup & Restore	Main + Utilities + Administrator Accounts + Edit	Account				
Certificates	Admin Editing and Pa	ssword Safe	ty Setting			
Network Utilities Restart						
System Upgrade	Name	admin				
	Original Password			*		
	New Password					
	Verify Password			Email Add	ress for Pass	word Recovery
	Email	e <del>ng - , 01,</del>			Assign SMT	Pserver Click to setup a SMTP server
	Elementary school's name	test		Security A	nswer for Pa	ssword Recovery (1-time setup)
		The elementary s	chool's name will identify y	ou, if you forgot your		
		password. Note t after apply.	hat, the elementary school'	s name can not be changed,		
			O Apply	S Cancel		

-

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Administrator Accounts Backup & Restore Certificates	Main + Users + Internal Authentication + Gue	t Authentication > SMTP Set	tings				
Network Utilities Restart System Upgrade	SMTP Server	Server Address Port	smtp.gmail.com 465 •	•	Each email do Server Addre	omain uses specific SMTP ss/Port and Encryption.	
	Encryption	Disable      TL:	S 🖲 SSL		This example	uses a Gmail account.	
	Authentication	Plain   Account Name Password		Ma	ain IT Administ	rator Account Credentials	
	Sender E-mail Address	eugene yu@4ipne	Com	- D Back			

#### 4.6 System - Service Zones Configuration

Go to System > Service Zones and confirm WAN Subnet and Default Service

Zone IP Address are in different subnets. Take below as example,

WAN1 = 10.201.5.66 / Subnet = 255.255.0.0

LAN/Default SZ = 192.168.1.254 / Subnet = 255.255.0.0

			SYSTEM	USERS	DEVICES		NETWORK	UTILITIES	STATUS
General WAN IPv6 LAN Ports	Main > System	e Zo	<sup>e Zone</sup> ne Settings						
Service Zones		-							
Port Location Mapping	S	tatus	Service Zone Name	IP Address	IPv6 Address	VLAN Tag	Default Auth. Option	Network Alias	DHCP Pool
PMS Interface	9	SH 🕢	Default	192.168.1.254	N/A	N/A	Server 1	N/A	192.168.1.1 ~ 192.168.1.100
	6	OFF	SZ1	172.21.0.254	N/A	1	Server 1	N/A	172.21.0.1 - 172.21.0.100
	6	OFF	SZ2	172.22.0.254	N/A	2	Server 1	N/A	172.22.0.1 ~ 172.22.0.100
	6	011	SZ3	172.23.0.254	N/A	3	Server 1	N/A	172.23.0.1 ~ 172.23.0.100
	6	OFF	SZ4	172.24.0.254	N/A	4	Server 1	N/A	172.24.0.1 ~ 172.24.0.100
	6		SZ5	172.25.0.254	N/A	5	Server 1	N/A	172.25.0.1 ~ 172.25.0.100
	6	077	SZ6	172.26.0.254	N/A	6	Server 1	N/A	172.26.0.1 ~ 172.26.0.100
	6		SZ7	172.27.0.254	N/A	7	Server 1	N/A	172.27.0.1 ~ 172.27.0.100
	6	OFF	SZ8	172.28.0.254	N/A	8	Server 1	N/A	172.28.0.1 ~ 172.28.0.100
Click S	Service	Zon	e Name to	configu	ire each	n SZ			

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

Main > System > Servi	ce zone > Service zo	ne contiguration			
Basic Setti	nos				
Dasie Setti	1183				
Service Zone	Status	Enabled			
Service Zone	Name	Default			
Network Inte	erface	Tag-based Isolation	Inter-VLAN Isolation	Clients Isolation	None
		gateway's LAN port may b enabled on the switch an Service Zone. Operation Mode	e shut down if 'Loop Prote d there are 2 VLANs belon; NAT	ection' is ging to this	
		IP Address 192.168.1.254	* Subnet Mask 255.2	255.0.0 *	
		Network Alias List	Configure		
		This list defines other IP A Service Zone.	ddresses (range) that are	routable in this	
DHCP		Disabled	Configure		
SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
	Basic Setti Service Zone Service Zone Network Inte DHCP SYSTEM	Basic Settings Service Zone Status Service Zone Name Network Interface DHCP	Service Zone Status Enabled Service Zone Name Default Network Interface Tag-based Isolation Note: When set to "None" gateway's LAN port may b enabled on the switch and Service Zone. Operation Mode IP Address Ip2.168.1.254 Network Alias List This list defines other IP A Service Zone. DHCP Disabled SYSTEM USERS DEVICES	Service Zone Status     Enabled       Service Zone Name     Default       Network Interface     Tag-based Isolation       Network Interface     Tag-based Isolation       Note: When set to "None", the port on a switch com gateway's LAN port may be shut down if 'Loop Prot enabled on the switch and there are 2 VLANs below Service Zone.       Operation Mode     NAT       IP Address     192.168.1.254       Network Alias List     Configure       This list defines other IP Addresses (range) that are Service Zone.       DHCP     Disabled       Configure       System     USERS       DEVICES     NETWORK	Service Zone Status       Enabled         Service Zone Name       Default         Network Interface       Tag-based Isolation       Inter-VLAN Isolation       Clients Isolation         Note: When set to "None", the port on a switch connecting to the gateways LAN port may be shut down if 'Loop Protection is enabled on the switch and there are 2 VLANs belonging to this Service Zone.         Operation Mode       NAT       Router         IP Address       192.168.1.254       * Subnet Mask 255.255.0.0         Network Alias List       Configure         This list defines other IP Addresses (range) that are routable in this Service Zone.         DHCP       Disabled         SYSTEM       USERS       DEVICES       NETWORK

WAN	-								
IPv6	DHCP En	able DHC	P Server 🔻						
LAN Ports	DHCP	Sorv	or Confi	auration fo	r Sa	arvice Zone D	ofault		
High Availability	Drici	Jerv	erconn	guration fo	1 30	ervice zone D	elault		
Service Zones									
Port Location Mapping	No	Active	DHCP Pool	Start IP Address		End IP Address	Preferred DNS Server	Alternate DNS Server	Domain Name
PMS Interface	1		Scope 1	192.168.1.2		192.168.1.200 *	192.168.1.254 *		domain.com
	2		Scope 2		•	*	*		
	3		Scope 3			*	*		
	4		Scope 4		*	×	*		
	5		Scope 5		•	*	*		
	6		Scope 6		*	*	*		
					-				

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

			SYSTEM	USERS	DEVICES	NETWO	RK UTILITIES	STATUS				
General WAN IPv6	Authentication Setting	s										
LAN Ports High Availability Service Zones Port Location Mapping	Authentication	Enable © Disab     When Authenticati     would see a suspe	le OSuspend Ena on is set to Suspended nd message from Geni	able/Disabl , users eral	e Auther	ntication	n on this Servi	ce Zone				
PMS Interface	Access Permission and Authorization	Configure										
	Default Policy	Policy 1 ·										
		To set up policies,	please go to Users > Po	olicies.								
	Portal URL	* Specific O Orig	nal © None									
		http://www.google. (e.g. http://www.e	com cample.com)	• Portal I	URL oper	ns specif	fied URL after	user is authenticated				
	MAC Authentication	tion © Enabled © Disabled RADIUS Authentication using MAC address										
	PPP Authentication	Enabled      Disa	bled									
	SIP Interface Configuration	Enabled  Bisa	bled									
	WISPr Settings	Configure										
	Authentication Options	Auth. Option	Auth. Database	Postfix	Default	Enabled	Confirm Au	thantication				
		Server 1	LOCAL	local		×	Comminia					
		Server 2	RADIUS	radius	0	8	Databases a	llowed in this Service				
		Server 3	NTDOMAIN	ntdomain	0		Zone					
		Server 4	LDAP	Idap	0	0						
		Server 5	POP3	pop3	0							
		On-Demand	ONDEMAND	ondemand	0	0						
		SIP	SIP	N/A								
		Guest	FREE	N/A		* ←	Guest (Free A	ccess Database)				

#### 4.7 System - Service Zone – Captive Portal Customization

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
General	SIP Interface Configuration	Enabled Isab	led			
WAN	WISPr Settings	Configure				
IPv6 LAN Ports	Authentication Options	Auth. Option	Auth. Databas	e Postfix	Default	Enabled
Service Zones		Server 1	LOCAL	local		8
Port Location Mapping		Server 2	RADIUS	radius	0	2
PMS Interface		Server 3	NTDOMAIN	ntdomain	0	ø
		Server 4	LDAP	ldap	0	2
		Server 5	POP3	pop3		2
		On-Demand	ONDEMAND	ondemand		2
		SIP	SIP	N/A		
		Guest	FREE	N/A		8
	Page Customization					
	Login Page Customization Message Page Customization	Configure	Customize the	e Login Page e Configure k	(Captive) outton	Portal)
	APs with VAP mapped	to this Servic	e Zone			
	List					
		0	Apply Ca	ncel		

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

	SYSTEM USERS DEVICES NETWORK UTILITIES STATUS
General WAN IPv6 LAN Ports	Main + System + Service Zone - Service Zone Configuration + Login Page Customization
Service Zones Port Location Mapping PMS Interface	Service Disclaimer Default © Customize with Template © Upload Your Own © Use External Page
	General Login Page     Default       PLM Open Type Login Page     Default   Preview the Default Login Page
	PMS Billing Plan Selection Page Default           Operative         Operative
	Theme for Template
	Button Color 🛛 💼 🔎 💻 🖓 🔜 🖉
	Upload Logo Upload Logo No File No File The recommended dimension of the image is 360x120 with a size limit of St 2 kB it will be adjusted if the dimension does not fit. Upload your own logo for a customized Captive Portal Note: Applies only to the "Customize with Template" selection
	Apply     Cancel

Preview General Login Page in Default mode.

			Username Password	LOGII	N ber Me	Login	Login	with an	accou	nt			
			Email	FREE LO	GIN ccount to log	n for free.	Login	with self	f-regis	tration I	oy Emai	I	
				Device Lo	ogout								

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

					•	Uploaded imag recommended	e file with the resolution (360x120) empire Upload Your Own © Use Esternal Page
				Account Login 🤜		Text Color	000000
				Deemane		Login Title	Account Login
				Password	Login	Username	Username
				Bemember Me	LOBIN	Password	Password
						Login Button	Login
				Email Login 🦂		Remaining Quota Button	Remain Quota
				Email		Guest Header	Email Login
				Enter your Email account to i	Login	Guest Email	Email
			_	Device Logout		Guest Note (without Email Verification	Enter your Email account to login for free.
						Guest Note (with Email Verification)	Check your mailbox to extend usage time after :
						Guest Login Button	Login
						Device Logout Indication	Device Logout
						Online Payment Indication	Buy Accounts Online
						SMS Indication	Register Accounts by SMS
						Remember Me	Remember Me
						Preview	Apply Cancel

#### 4.8 Users - Local Accounts

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

	SYSTEM US	ERS DEVICES	NETWORK	UTILITIES	STATUS	
Groups	Main > Users > Internal Authentica	ition > Local Authentication				
Authentication Servers						
Internal Authentication	Server No. 1 : Server 1 V					
Local						
On-Demand	Local Authentic	ation				
Guest						
External Authentication	Local User List	Configure En	ter the Local User List to Ado	/Delete/Edit Local Acc	ounts	
On-Demand Accounts				, Derete, Eart Lotar, ree	June	
Schedule	Account Roaming Out	Enable 🔍 D	isable Use bulit-in local dat	abase for 802.1X auther	ntication	
Policies	802.1X Authentication	🖲 Enable 🔍 D	isable Enable Account Roan	ning Out and 802.1X Au	uthentication	
Blacklists		RADIUS Client D	evice Settings			
Privilege Lists						
Additional Controls		ĺ	Apply S Ca	ancel		

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main > Users > Internal Authentication > Loc	al Authentication + Local User	List			
Authentication Servers						
Internal Authentication	Local User List					
Local						
On-Demand	Click Add t	o create Loca	I Accounts			
Guest	Add Delete Backup Lis	t Upload				Search
External Authentication						
On-Demand Accounts	No Status Us	ername Password	MAC	Group Activation	Expiration	Remark
Schedule		(T				0
Policies		(10tal:0/2000) 144	-irst • Prev Next• Las	(Hage: 1/1)	Row pe	r Page: 10 V
Blacklists						
Privilege Lists						
Additional Controls						

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

	S	YSTEM USERS	5	DEVICES NETWORK	UTILITIES	STATUS
Groups Authentication Servers Internal Authentication	Main > Users > Internal Authentication > Loca 10000 users can be added to this local user A	l Authentication - Local Use stionally bind M. ddresses to Local	r Lista Add AC I Accor	Optionally conf unts Account Span	gure	
On-Demand	Username Password	MAC Address	Group	Account Span	Remark	Optionally
Guest	staff	St	əff 🔹			add a remark
External Authentication	Fill in Username &	Gu	Jest 🔹	Categorize into		
On-Demand Accounts	Password pairs	Gu	Jest 🔹	User Groups		
Policies		Gu	Jest 🔹	0		
Blacklists		Gu	Jest 🔹	0		
Privilege Lists		Gu	Jest 🔹	0		
Additional Controls		Gu	Jest 🔹	0		
		Gu	vest 🔹	0		
		G	Jest •	0		
		Gu	Jest 🔹	0		
		Apply		Cancel		

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



#### 4.9 Users – Guest Authentication

Administrator expects that Guest users are authenticated by submitting their Email addresses for granting free Wi-Fi Internet access for 24 hours with limited speed and sessions, which can be achieved by Guest Authentication on EWS controller.

This paragraph will illustrate the configuration steps for Guest Authentication.

Go to *Users* > *Internal Authentication* > *Guest Authentication*, select the radio box to make Guest Login Input to be *visible*, which is the column for users to enter their Email address. Select *Limited* radio box to set up limited *Guest Access Time*, and then the further configurations will be visible. Please assign 24 hours 0 minutes as *Quota*; 1 minute for *Access Limit*. Last, assign this Guest Authentication to *Guest Group* for User Policy enforcement.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups Authentication Servers	Main > Users > Internal Au	thentication > G	uest Authentication			
nternal Authentication	Guest Auther	ntication	1			
Local						
Dn-Demand				<u>.</u>		
Guest	Group		Guest	<b>+</b>		
ternal Authentication	Guest Informatio	'n	View			
n-Demand Accounts	Guest Questionn	aire	Configure			
hedule	Guest Access Tim	ne -	🔿 Unlimited 💿 Lim	ited		
olicies	0					
icklists	Quota		24 nour(s) 00 min	ute(s)		
/ilege Lists	Reactivation		After 0 hour(s) 1	minute(s)		
dditional Controls	Access Limit		0 per day *(0:Unlin	nited)		
	Email Verification	ı	<ul> <li>Disable O Enable</li> </ul>	2		
	Guest Quota List		View			
	E-mail Denial List		💿 Disable 🔵 Enable	Configure		
				Apply Ca	Incel	

#### 4.10Users – User Policies Configuration

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

### 4.10.1 Guest Users → Policy 1 profile configuration

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups Authentication Servers Internal Authentication External Authentication On-Demand Accounts Schedule Policies	Main - Users - Policies - Policy Configuration A Policy is used to define a Croup's authors: Clobal Policy is the general policy defined for Policy is not defined. Select Policy Policy 1 • Policy Configuration	ition in a Service 2one. Th r all Groups when the Gro Select Pol	icy to config	ure			
Policy Configuration 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	mapped Profil S Cancol	les		

Go to Users > Policies > Privilege 1 to check if the Maximum Concurrent

Session is 500 as the default value.

		SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STA
Groups	Main > Users > Policies > Privilege						
Authentication Servers		-					
nternal Authentication	Select Privilege Profile Privilege 1	•					
external Authentication							
on-Demand Accounts	Privilege Configuratio	n					
chedule							
olicies							
Policy Configuration	Privilege Name	Privilege 1					
Firewall	Password Change	Allow Isal	low				
Privilege	Maximum Concurrent Sessions	500 × (ses	sions per user)				
Q05	Maximum concurrent sessions	000 000	sions per usery				
Specific Routes	Disable timeout for this group	Enabled O Di	sabled				
lacklists							
rivilege Lists			Apply	Cancel			
Additional Controls		_					

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

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

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups	Main + Users + Policies + Op5						
Authentication Servers							
Internal Authentication	Wote: Please enable Bandwidth limitation	on on waw and restart the	system for Group Traffic Co	onnguration.			
External Authentication	▲ I						
On-Demand Accounts							
Schedule							
Policies	Click the base disk (D						
Policy Configuration	Click the hyperlink "B	andwidth li	mitation				
Firewall	on WAN" and Enable	the feature					
Privilege							
QoS							
Specific Routes							
Blacklists							
Privilege Lists							
Additional Controls							
A CONTRACTOR OF A							

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

SYSTEM	USERS DEVICES	NETWORK	UTILITIES	STATUS	
	🗷 Obtain DNS server address automa	tically.			•
	Preferred DNS Server: 168.95.1.1	•			
	Alternate DNS Server: 8.8.8.8				
	PPPoE				
	🔘 рртр				
WAN Traffic Settings					
Bandwidth Limitation	Enable Bandwidth Limitation on WAN		Check the Ena	able Bandwidth Limitatio	n on
	Max Uplink Bandwidth 2000000	Kbps	WAN checkbo	ox and configure the Max	(
	Max Downlink Bandwidth 2000000	Kbps	Uplink/Down	link Bandwidth.	
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 con this message will be shown on the browser.	nection are unreachabl	e,		
	Sorry! The service is temporarily unavailab	e.			
	Apply	Cancel			
	WAN Traffic Settings Bandwidth Limitation Target for Detecting Internet Connection	SYSTEM     USERS     DEVICES <ul> <li>Obtain DNS server address automat</li> <li>Preferred DNS Server:</li> <li>Taget or Detecting Internet</li> <li>Target for Detecting Internet</li> <li>Target for Detecting Internet</li> <li>Target for Detecting Internet</li> <li>Target for Detecting Internet</li> <li>Enter IP Address/Domain Name Here</li> <li>Enter IP Address/Domain Name Here</li> <li>Target for Detecting Internet</li> <li>Enter IP Address/Domain Name Here</li> <li>Target for Detecting Internet</li> <li>Target for Detecting Internet</li> <li>Enter IP Address/Domain Name Here</li> <li>Enter IP Address/Domain Name Here</li> <li>Torry The service is temporarity unavailable</li> </ul>	SYSTEM       USERS       DEVICES       NETWORK	SYSTEM       USERS       DEVICES       NETWORK       UTILITIES <ul> <li>Obtain DNS server address automatically.</li> <li>Preferred DNS Server:</li> <li>DESS Server:</li> </ul> <ul> <li>PreDE</li> <li>DESS</li> </ul> <ul> <li>DESS Server:</li> <li>DESS Server:</li> <li>DESS Server:</li> <li>DESS Server:</li> <li>DESS Server:</li> </ul> <ul> <li>PreDE</li> <li>DESS Server:</li> </ul> <ul> <li>DESS Server:</li> <li>DESS Server:</li> <li>DESS Server:</li> <li>DESS Server:</li> <li>DESS Server:</li> </ul> <ul> <li>DESS Server:</li> <li>DESS Serv</li></ul>	VIEW       USEN       DEVICE       NEWORK       UTITIES       STATUS <ul> <li>Obain DMS server address automatically.</li> <li>Derect</li> <li>Derect</li> <li>Derect</li> </ul> <ul> <li>DPDE</li> <li>Derect</li> </ul> <ul> <li>Derect</li> <li>Derect</li> </ul> <ul> <li>Derect</li> <li>Derect</li> </ul> <ul> <li>Derect</li> <li>Derect</li> <li>Derect</li> <li>Derect</li> </ul> <ul> <li>Derect</li> <li>Derect</li> <li>Derect</li> <li>Derect</li> </ul> <ul> <li>Derect</li> <li>Derect</li> <li>Derect</li> <li>Derect</li> <li>Derect</li> <li>Derect</li> </ul> <ul> <li>Derect Producted Limitation on VMAL</li> <li>Derect Producted Limitation on VMAL</li> <li>Derect Producted Deremain Name Here</li> <li>Dere</li></ul>

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

	SYSTEM	USERS	DEVICES	NETWO	RK UTILITIES	STATUS
Groups	Main ) Users ) Policies ) QoS					
Authentication Servers						
Internal Authentication	Select QoS Profile QoS 1 •					
External Authentication						
On-Demand Accounts	QoS Configuration					
Schedule						
Policies	OoS Brofile Name	0-51				
Policy Configuration	Qos Prome Name	Qos I				
Firewall	Traffic Class	IPv4 IPv6				
Privilege	Bandwidth Control	🖲 Enable 🔘 Disa	Enab	le Bandwi	dth Control	
QoS		Group Total Dow	mlink	100 Mbps •		
Specific Routes		Group Total Upli	nk	100 Mbps •	Total Group Trat	tic
Blacklists		In all taken Manufa	um Daualish	1 Mhas -		
Additional Controls		Individual Maxin	Ium Downlink	1 mops •	Each User's Max	imum Traffic
Additional Controls		Individual Maxin	num Uplink	1 Mbps •		
		Individual Reque	st Downlink	512 Kbps 🔻	Each Lloor's Mini	imum Traffic
		Individual Reque	st Uplink	512 Kbps 🔻	Lach User S Willin	
		*(Unlimit: 0, Ran	ge: 1-999)			
			Apply	Cancel		

### 4.10.2 Staff Users → Policy 2 profile configuration

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

		SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main & Users & Policies & Policy Confis	ruration				Sen har i ber	biber dieser
Authentication Servers	A Policy is used to define a Group'	s authorization in a Serv	vice				
Internal Authentication	Zone. The Global Policy is the gene	eral policy defined for al	11				
External Authentication	Groups when the Group Policy is r	not defined.					
On-Demand Accounts	Select Policy Policy 2						
Schedule							
Policies	Policy Configuration	1					
Policy Configuration							
Firewall							
Privilege	Policy Name	Policy 2					
Q05	Firewall Profile	Firewall 2 •					
Specific Routes	Drivilago Drofila	Drivilogo 2					
Blacklists	Privilège Profile	Privilege 2 •					
Privilege Lists	QoS Profile	QoS 2 🔻					
Additional Controls	Specific Route Profile	Specific Route 2					
	Prefer DHCP Pool	None 🔻					
			Apply	Cancel			

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



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

			S	YSTEM	USERS	DEVICES	NETWOR	<	UTILITIES
Groups Authentication Servers	Main > Users > Poli	cies > Firewall	Configuratio	on > Firewall					
Internal Authentication	Firewall Pi	rofile 2	- Firew	all Rules					
External Authentication									
On-Demand Accounts	Add De	lete Enable	Disable	Click A	dd to create	e a Firewall Rule	2		
Policies									_
Policy Configuration	No.	Status	Action	Rule Name	Source	Destination	Service	Schedule	Operation
Firewall					Source Interface	Destination Interface			
Privilege				(Total:0) MFirst	t • Prev Next• Las	ter Go to Page 🔹 (Page	:1/1)	Row per	Page: 20 •
QoS Garaifa Davara									
Blacklists									
Privilege Lists									
Additional Controls									

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

		SYSTEM	S DEVICES	NETWORK UTILITIES STATUS
Groups Authentication Servers Internal Authentication	Main > Users > Policies > Policy Cor Policy 2 - Edit Filte	nfiguration > Policies > Firewall Configuration > Policies > Firewall Configuration > Policies > Firewall Configu	ration > Firewall > Edit Filter	Rufe
External Authentication On-Demand Accounts Schedule	Rule Number	new Epto	Pulo Namo	
Policies Policy Configuration Firewall Privilege QoS	Rule Name Source	BlockFacebook All Interface/Zone All IP Address • 0.0 Subnet Mask 0.	L	Select the Souce Interface/Service Zone and the IP Address/Subnet Mask.
Specific Routes Blacklists Privilege Lists Additional Controls	Destination	MAC Address Interface/Zone Al Domain Name  Subnet Mask 2:		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
	Service Protocol Action Schedule	ALL   Block  Pass Always  Recurring  O	ne Time	Select to Block or Pass traffic from Source to Destination
		Apply	Cancel	

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

					SYSTEM	USERS	DEVICES	NETWOR	к	UTILITIES	
Groups	Main , Users ,	Polici	es > Firewall	Configurat	on Firewall						
Authentication Servers											
Internal Authentication	Firewall	Pre	ofile 2	- Firev	vall Rules						
External Authentication											
On-Demand Accounts		0.1			Chock th	Eirowall R	ulo & click Enak	olo			
Schedule	Add	Dele	Enable	Disable	J CHECK III	ernewann	ule & click Linak	Ne			
Policies						Source	Destination				
Policy Configuration		No.	Status	Action	Rule Name	Source Interface	Destination Interface	Service	Schedule	Operation	
Firewall						ANY	water facebook com				
Privilege		1	Disabled	Block	BlockFacebook	000	www.iacebook.com	ALL	always	ways Move	ys Move
QUS Casalifa Davina						ALL	ALL				
Plackliste					(Total-1) te First	Prev Next + Last	Go to Page 1 . (Page	1/1)	Row per	Page 20 .	
Didukiisus Dahillaga Lista											

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



#### 4.11 Users – User Groups Configuration

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

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



Here we select and rename Group 2 as Staff, with unlimited Number of devices which are allowed to login, and assign Policy 2 for Default Service Zone.

		SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	
Groups	Group Configuration	on					
Overview							
Authentication Servers	Select Group	Staff •					
Internal Authentication	Group Name	Staff					
External Authentication	Remark						
On-Demand Accounts	Number of devices which a	re 0					
Schedule	allowed to login	(0 to 9999 dev	ices, 0: Unlimited)	af daviana in anafarana			
Policies		individually pe	nd accounts, number er different billing pla	ns. The number is for th	e		
Blacklists Privilage Lists		following type	s: LOCAL, POP3, RAD	IUS, LDAP, and NT			
Additional Controls	Allow to logout other device	es when					
	Zone Permission C	LOCAL, POP3,	RADIUS, LADP, and M	IT Domain. Ignment			
	Enabled	Zone Name		Time Span 1	Time Sj	oan 2	
				Schedule 2 🔹	Schedul	2 •	
	🗷 Sen	vice Zone : Default		Policy 2 🔹	Policy .	2 •	
	☑ Sen	vice Zone : SZ1		Policy 2 🔹	Policy.	2 🔻	
	🖉 Sen	vice Zone : SZ2		Policy 2 ·	Policy	2 •	
	☑ Sen	vice Zone : SZ3		Policy 2 🔻	Policy.	2 🔹	
	☑ Ser	vice Zone : SZ4		Policy 2 🔹	Policy	2 •	
	☑ Sen	vice Zone : SZ5		Policy 2 ·	Policy.	2 🔻	

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

	SYSTEM	USERS	DEVICES NETWORK	UTILITIES	STATUS
Groups Overview Configuration Authentication Servers Internal Authentication External Authentication	Main + Users + Groups + Overview This page gives a summary of which Aut the corresponding Group. Group Overview	hentication Servers are used fo		Guest Group is the Default Group for all Authentication Types including the Guest Authentication	
On-Demand Accounts	Group	Name	Auth	entication Type	
Schedule Policies Blacklists Privilege Lists Additional Controls	Gue	st	Billing Plan 1 Billing Plan 2 Guest POP3-Server 5 RADIUS-Server 2-Default LDAP-Server 4-Default NT Domain-Server 3 StP		
	Sta	ff	Local		
	Grou	р 3			Staff Group has been
	Grou	p 4			selected as the Staff Local
	Grou	p 5			User Account: staff
	Grou	р б			Oser Account. stan
	Grou	p 7			
	Grou	p 8			

#### 4.12 Use WAPM on EWS to manage ECW

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



#### 4.12.1 Edit WAPM Templates

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

	SYSTEM USE	ERS DEVICES	NETWORK	UTILITIES	STATUS	
AP List	Main > Device Management > Wide /	Area AP Management > Template				
Мар	Tomplato AD Cotti	ng				
AP Grouping	Template AP Setti	ng				
WDS List						
Backup Configuration	Select Template	1: Template 1 🔹				
Firmware	Template Name	HQ-AP	Apply			
CAPWAP	Country Code	USA 🔻				
Rogue AP Detection	General Settings	Configure				
AP LOad Balancing	VAP Configuration	Configure				
	Security Settings	Configure				
	Advanced Wireless Setting	configure				
	Hotspot 2.0 Settings	Configure				
	Firewall Settings	Configure				

#### **General Settings**

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
AP List	Main > Device Managem	ent › Wide Area AP Ma	nagement > Template > Ge	neral Settings		
Мар						
AP Grouping	General Sett	tings - 1: Te	mplate 1			
Template						
WDS List	RE Card Name			and adit DE CARD A (2.4		
Backup Configuration	RF Card Name		RF CARD A - Select	and edit KF CARD A (2.4	0), NF CAND B (30)	
Firmware	Band		802.11g+802.11n 🔻 🗐	Pure 11n		
CAPWAP	Short Preamble		Disable Schable			
Rogue AP Detection	Short Guard Int	erval	Disable Disable			
AP Load Balancing	- Shore Guard Inc		O DISABle O LITABle			
	Channel Width		20 MHz 🔻			
	Channel		6 🔻			
	Max Transmit R	ate	Auto 🔻			
	Transmit Power		Level 1 V		Confirm the setting	are suit for network
	ACK Timeout		0 *(0 - 255, 0:Auto	. Unit:4 micro seconds)		
	Beacon Interval		100 millisecond(s) *(1	00 - 500ms)		
	Airtime Fairness	5	O Disable 🖲 Fair Acces	s 🔘 Preferred Access		
	Packet Delay Th	reshold	1000 millisecond(s) *(1	00 - 5000ms, 0:Disable)		
	Idle Timeout		300 second(s) *(60 - 6	60000)		
	Band Steering		Disable O Enable			
		1925.40.2012	Aggressive			

### **VAP Configuration**

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
AP List	Main > Device Managem	ent > Wide Area AP Ma	nagement > Template > VA	P Configuration			
Мар							
AP Grouping	VAP Configu	ration - 1:	Femplate 1				
Template							
WDS List	Des file Norres		DE Card A - MAD 1				
Backup Configuration	Profile Name		RF Card A : VAP-1 •	Select Profile of VAP			
Firmware	VAP		Disable Inable	Select to enable this V	/AP		
CAPWAP	Profile Name			Assign a Profile Name	9		
Rogue AP Detection	FSSID			Assign a SSID			
AP Load Balancing	Listick Decided			1 1019576 0 Disable)			
	Uplink Bandwid	th	U KDILS/S *(	1-1048576, 0:Disable)			
	Downlink Bandy	vidth	0 Kbits/s *(	1-1048576, 0:Disable)			
	VLAN ID		O Disable   Enable				
			VLAN ID 1000 *(1-4	094)			
	Uplink 802.1p		Best Effort (BE)	•			
	CADWAD Turnel		Complete Tuppel	Select Complete Tun	nel and		
	CAPWAP TUNNEI	Interface	complete funner •	Service Zone and the	VIAN		
	Service Zone		n26 T	ID will auto-change			
				is the date change			
				Apply 🛛 😢 Cance	el		

We can use same procedure to configure other VAP.

### **Security Configuration**

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
AP List	Main > Device Manageme	ent > Wide Area AP Ma	nagement > Template > Se	curity Settings		
Мар						
AP Grouping	Security Sett	tings - 1: Te	emplate 1			
Template						
WDS List						
Backup Configuration	Profile Name		RF Card A : VAP-1 🔻			_
Firmware	Security Type		Open 🔻	Select the Profile an	d choose the Securi	ty Type
CAPWAP						
Rogue AP Detection						
AP Load Balancing					e	

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

### Advanced Wireless Configuration

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
AP List	Main > Device Management >	Wide Area AP Ma	anagement > Template > /	Advanced Wireless Settings			
Мар			0 1				
AP Grouping	Advanced Wire	less Sett	ings - 1: Ter	nplate 1			
Template							
WDS List	Drafile Name		RE Card A . VAD 1				
Backup Configuration			RF Card A : VAP-1 •				
Firmware	RTS Threshold		2346 *(1 - 2346)				
CAPWAP	Fragment Threshold		2346 *(256 - 2346)				
Rogue AP Detection	DTIM period		1 *(1 - 15)				
AP Load Balancing	Consecutive Retries	Threshold	5 *(2 - 50, 0:Disa	ible)			
	Broadcast SSID		Disable    Enable	Select to broadcast t	he SSID or not		
	Wireless Station Isola	ation	🔍 Disable 💿 Enable	If you allow the clien	ts connect to this SSI	D could access each othe	er,
	WMM		🔘 Disable 🖲 Enable	please disable it			
	IAPP		🔘 Disable 🖲 Enable				
	Multicast-to-Unicast	Conversion	Disable				
	TX STBC		🔘 Disable 💿 Enable				
	Multicast/Broadcast	Rate	5.5M ¥				
	Management Frame	Rate	5.5M ¥				
	Receving RSSI Thresh	old	-80 *(-95 ~ 0, 0:dis	able)			
				Apply S Can	cel		

#### 4.12.2 Establish CAPWAP Tunnel from AP to EWS

	SYSTEM USERS	DEVICES	NETWORK	UTILITIES	STATUS
NP List	Main > Device Management > Wide Area AP M	Anagement - CAPWAP			
Иар					
AP Grouping	CAPWAP Configuration	1			
emplate					
VDS List					
Backup Configuration	CAPWAP Status	🖲 Enable 🔘 Disable			
irmware	Apply Certificate to APs	DEFAULT V			
CAPWAP	IP Address For Control Channel	100 64 144 254			
togue AP Detection	in Address for control channel				
P Load Balancing	IP Netmask For Control Channel	255.255.255.128 (125) ▼			
	Control Channel IP Range	100.64.144.1 ~ 100.64.144.253			

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



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

	4				•	1	
System	Wireless	Firewall		Utiliti	es	80	106
Overview Interfaces Associ	ated Clients Link Status	Event Log Monito	r	<u></u>			
Home > Status > System Overv	iew						
		System Ove	erview				
r 🎓 System 🗕		— <u>(</u>	Radio	Status —			
System Name	TS-Joyce	RF Ca	d I	MAC Address	Band	Channel	TX Power
Firmware Version	3.42.10	RF Card	A 00	:1F:D4:04:F8:0A	802.11g+n	11	28 dBm
Build Number	1.36.2.6-1.8992.2.7	RF Card	B 00	:1F:D4:04:F8:0B	802.11ac	36	17 dBm
Location	Tainei Tiawan						
Site	FN-A						
Device Time	2017/07/03 16:33:56						
System Un Time	0 days 12:22:27						
CDII/RAM Usage	48.08% / 30.62% Plot						
Operating Mode	40.0070 / 30.0270 FIOL						
operating rioue	Ar						
	00:1F:D4:04:F8:08		AP Sta	tus			
IP Address	192.168.5.246			RF Card Name	: RF Card A	·	
Subnet Mask	255,255,255,0	Profile	DC	51D 013	Setto Se	ecurity On	line TUN
Gateway	192.168.5.252	VAP-1	00.1E-D4	:04:F8:00 cin	-802 1x WD	Type Clie	ents TON
			30.11.04	io in ologi up			
CAPWAP		IP	v6				
Status	Run(10.201.5.117)		Stat	us Disabled			
Data Channel	Active		otat	21000100			

### 4.12.3 Applying the template

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

Edge-corE	B			10.201.5.117/OutdoorEquipmentManagement/Template.shtml?refer_p;     Mizar     Apply Settings	rd <b>?</b> Help
	SYSTEM	USERS	DEVICES	hppiy seeings	
AP List Map AP Grouping Template	Main, Device Managen	nent 3 Wide Area AP Mar	nagement > AP List	Apply template     Select Template     T:HQ     T     Change password	
WDS List Backup Configuration Firmware CAPWAP Rogue AP Detection	Type Status Tunnel Name ▼	A A N	I T I T one T iearch	New Password vup to 32 characters Re-enter New Password Apply Cancel	
AP Load Balancing	Add Delete	] Add to Map / Floor F	Plan Backup Confi	g Restore Config Upgrade Apply Settings Reboot	
	EAP760	Iame         IP           4F3         10.71.5.130         00:	MAC N 1F:D4:03:10:9C Ove	Iap         Template         Status         # of Users         Tunnel         AP Admin Web         CAPWAP         AP Ver.           rview         5         Online         0         Edit         System Overview ▼         RUN         3.42.10	
			(Total 1) 📭	First  Prev Next Go to Page 1 Row per Page 80	

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
AP List	Main » Device Managem	ent > Wide Area AP N	Management⇒ AP List				
Мар							
AP Grouping	APList						
Template							
WDS List							
Backup Configuration	Туре		EAP760 •				
Firmware	Status		All 🔻				
CAPWAP	Tunnel		None 🔻				
Rogue AP Detection	Name 🔻 4F3		Search				
AP Load Balancing							
					Refresh Interval Disa	ble Auto Refresh	
	Add Delete	Add to Map / Floo	or Plan Backup Config	Restore Config Upgrade	Apply Settings Reboo	ot	
				Tamalata Status H a	fileere Turnel AD A		
			мас мар	o rempiate status # o	r Osers Tunner AP A	amin web CAPWAP AP ver.	
	EAP760	4F3 10.71.5.130 (	00:1F:D4:03:10:9C Overvi	ew 5 Applying	0 Edit Go	RUN 3.42.10	
			(Total 1) 📭	rst ⇔Prev Next⇒ Last <b>⇒i Go</b>	to Page 1 🔻	Row per Page 80 🔻	

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

	STSTEM	USERS	DEVICES	NETWOR	K 01	TILITIES	STATU	US
st	Main > Device Manageme	nt > Wide Area AP Manag	gement - AP List					
rouping	AP List							
late								
List	-							
up Configuration	Туре	EAP	760 •					
ware	Status	All						
AP Detection	Name T	503	e ·					
ad Balancing	Name •	568						
da balancing								
					Refre	sh Interval Disab	le Auto Refres	sh 🔻 Refre
	Add Delete	Add to Map / Floor Pla	n Backup Config	Restore Config	Upgrade Apply Se	ettings Reboot		
	Type National Type	me IP	МАС Мар	Template Statu	s # of Users Tunn	el AP Adn	nin Web	CAPWAP
						System Over	view 🔻	
	EAP760 4F	3 10.71.5.130 00:1F:	D4:03:10:9C Overview	1 Onlin	e 0 Edit	Go		RUN
			(rotari) vernst	errev wexter Lo	Star Of to Page 1			Now per Pag
		4	1	1			E	4
	Line and Lin	• • • • • • • • • • • • • • • • • • •			The second s	°		1
	System	Wireless	Fire	ewall	Utilitie	es	Sie	atus
-								
	Home > Status > System Ove	erview						
	Home > Status > System Ove	erview	System	Overview	1			
	Home > Status > System Ove	erview	System	Overview	Status			
	Home > Status > System Ove	erview	System	Overview	Status —	Pand	Channel	TY Deve
	Home > Status > System Over	arview 4F3	System	Overview Radio RF Card	Status	Band	Channel	TX Power
	Home > Status > System Over System — System Name Firmware Version	4F3 3.42.10	System	Overview Radio	Status MAC Address :1F:D4:03:10:9E	Band 802.11g+n	Channel 6	TX Power 28 dBm
	Home > Status > System Over System — System Name Firmware Version Build Number	4F3 3.42.10 1.36.2.6-1.8992.2.7	System	Overview Radio RF Card JF Card A 00 JF Card B 00	Status           MAC Address           :1F:D4:03:10:9E           :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	<b>TX Power</b> 28 dBm 17 dBm
	Home > Status > System Over System — System Name Firmware Version Build Number	4F3 3.42.10 1.36.2.6-1.8992.2.7	System	Overview Re Card F Card A 00 F Card B 00	Status           MAC Address           :1F:D4:03:10:9E           :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System — System Name Firmware Version Build Number Location	4F3 3.42.10 1.36.2.6-1.8992.2.7	System	Overview Radio RF Card IF Card A 00 IF Card B 00	Status MAC Address :1F:D4:03:10:9E :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System — System Name Firmware Version Build Number Location Site	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A	System	Overview Re Card F Card A 00 F Card B 00	Status           MAC Address           :1F:D4:03:10:9E           :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System — System Name Firmware Version Build Number Location Site Device Time	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32	System	Overview Re Card F Card A 00 F Card B 00	Status           MAC Address           :1F:D4:03:10:9E           :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Mame Firmware Version Build Number Location Site Device Time System Up Time	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41	System	Overview Recard F Card A 00 F Card B 00	Status           MAC Address           :1F:D4:03:10:9E           :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Name Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi	System	Overview Radio F Card F Card A 00 F Card B 00	Status           MAC Address           :1F:D4:03:10:9E           :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Name Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi AP	System	Overview Recard F Card A 00 F Card B 00	Status MAC Address :1F:D4:03:10:9E :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Mame Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi AP	System	Overview Re Card F Card A 00 F Card B 00	Status MAC Address :1F:D4:03:10:9F :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Mame Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi AP	System	Overview Re Card F Card A 00 F Card B 00	Status MAC Address :1F:D4:03:10:9F :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Mame Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi AP	System	Overview Recard F Card A 00 F Card B 00	Status	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Mame Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi AP	System	Overview Recard F Card A 00 F Card B 00	Status MAC Address :1F:D4:03:10:9F :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System — System Name Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi AP CCC 	System	Overview Recard F Card A 00 F Card B 00	Status MAC Address :1F:D4:03:10:9F :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Mame Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi AP CC 00:1F:D4:03:10:9C 192.168.5.247	System	Overview Recard F Card A 00 F Card B 00	Status MAC Address :1F:D4:03:10:9F :1F:D4:03:10:9F	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Name Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi AP CC 00:1F:D4:03:10:9C 192.168.5.247	System	Overview Redio F Card F Card A 00 F Card B 00 AP Sta	Status MAC Address :1F:D4:03:10:9F :1F:D4:03:10:9F RF Card Name	Band 802.11g+n 802.11ac	Channel 6 36	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Name Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	AF3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% Pi AP CC 00:1F:D4:03:10:9C 192.168.5.247 255.255.255.0	System	Overview Redio F Card F Card A 00 F Card B 00 AP Sta	Status MAC Address :1F:D4:03:10:9F :1F:D4:03:10:9F RF Card Name	Band 802.11g+n 802.11ac e : [RF Card A ▼ SSID See T	Channel 6 36 200 200 200 200 200 200 200 200 200 20	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Name Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode	AF3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% [Pi AP CC 00:1F:D4:03:10:9C 192.168.5.247 255.255.255.0 192.168.5.252	System	Overview Redio F Card A 00 F Card B 00 F Card B 00 AP Sta ame BS AP-1 00:1F:D	Status           MAC Address           :1F:D4:03:10:9F           :1F:D4:03:10:9F           RF Card Name           SID         E           :03:10:9E	Band 802.11g+n 802.11ac a : [RF Card A ▼ SSID Set T T	Channel 6 36 curity Onl ype Clie ppen (	TX Power 28 dBm 17 dBm
	Home > Status > System Over System Name Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode With CAU Interfa MAC Address Subnet Mask Gateway	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% PI AP CC 00:1F:D4:03:10:9C 192.168.5.247 255.255.255.0 192.168.5.252	System	Overview Radio F Card A 00 F Card B 00 F Card B 00 AP Sta Standard B 85 AP-1 00:1F:D- If SSID conta	Status MAC Address :1F:D4:03:10:9F :1F:D4:03:10:9F RF Card Name SID E :03:10:9E ,, ain tunnel (It m	Band           802.11g+n           802.11ac             ssin           ssin           ssin           c           c           c           c	Channel 6 36 curity Onl ype Clie pen C	Iine TUN
	Home > Status > System Own System Name Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode With CAU Interfa MAC Address Subnet Mask Gateway	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:32 0 days, 0:13:41 1.96% / 29.15% PI AP CC 00:1F:D4:03:10:9C 192.168.5.247 255.255.255.0 192.168.5.252	System	Overview Radio F Card A 00 F Card B 00 F Card B 00 AP Sta Standard B AP 1 00:1F:D If SSID conta would show	Status MAC Address :1F:D4:03:10:9F :1F:D4:03:10:9F RF Card Name SID E :03:10:9E , , , , , , , , , , , , , , , , , , ,	Band 802.11g+n 802.11ac a : [RF Card A • SSID See T must be confi con	Channel 6 36 curity Onl ype Clie ppen C	TX Power 28 dBm 17 dBm
	Home > Status > System Own System Name Firmware Version Build Number Location Site Device Time System Up Time CPU/RAM Usage Operating Mode WAC Address IP Address Subnet Mask Gateway	4F3 3.42.10 1.36.2.6-1.8992.2.7 EN-A 2017/06/30 01:20:33 0 days, 0:13:41 1.96% / 29.15% [P] AP CC 00:1F:D4:03:10:9C 192.168.5.247 255.255.255.0 192.168.5.252	System	Overview Radio F Card A 00 F Card B 00 F Card B 00 AP Sta AP 1 00:1F:D- If SSID cont. would show IPv6	Atus RF Card Name SID E 103:10:9E 117:D4:03:10:9F Bitus RF Card Name RF Card Na	Band 802.11g+n 802.11ac	Channel 6 36 curity Onl ype Clie ppen ( curity Clie gure with	Ine TUN

Status Disabled

Status Run(10.201.5.117)

Data Channel Active

#### 4.13 1+1 High Availability for Service Redundancy

#### 4.13.1 Configure EWS#1 HA

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
General WAN	System Tim	е					
IPv6							
LAN Ports	Current Time		2017/06/30 10:19:17				
	Time Zone		(GMT+08:00)Taipei		•		
Port Location Mapping	Time Update		NTP Manuall	y set up			
PMS Interface			NTP Server 1: tim	e.nist.gov			
			NTP Server 2: ntp	1.fau.de			
			NTP Server 3: clo	ck.cuhk.edu.hk			
			NTP Server 4: ntp	s1.pads.ufrj.br			
			NTP Server 5: ntp	1.cs.mu.OZ.AU			
			🕑 Use this contr	oller as an NTP server			
				Apply Sc	ancel		

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
General WAN IPv6 LAN Ports High Availability Service Zones Port Location Mapping PMS Interface	Configura Status Number of, Mode HA Port IP A HA Port Sub Peer IP Add Shared Key Action	t i o n Active(s) vddress onet Mask ress	Enabled Disal      Disal      Active Standb      172.31.0.1      255.255.0.0      172.31.0.2        Sync & Swap	Enable the High A Select Number of Select Active/Stat HA Port IP addre other service zon	vailability Active ndby ss, do not duplicate with ne network segment	1	
				Apply Sc	ancel		

#### 4.13.2 Configure EWS#2

Please make sure EWS#1 boot up successfully before configuring EWS#2. Same as EWS#1, go to SYSTEM > High Availability, enable High Availability and select Standby. After click Apply, before reboot, make sure the LAN1 port of both EWS are directly connect.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
General WAN IPv6 LAN Ports	Configuration	I					
High Availability Service Zones Port Location Mapping PMS Interface	Status Number of Active(s Mode HA Port IP Address HA Port Subnet Ma Peer IP Address Shared Key Action	s) s ask	<ul> <li>Enabled Disal</li> <li>Disal</li> <li>Active Standb</li> <li>172.31.0.1</li> <li>255.255.0.0</li> <li>172.31.0.2</li> <li>Sync &amp; Swap</li> </ul>	bled Enable the High Ar Select Number of A Select Active/Star + HA Port IP addre other service zon	vailability Active ndby ss, do not duplicate wit e network segment	h	
				Apply SC.	ancel		

### 4.13.3 Confirm HA status of both EWS

Click "Goto" to access the standby page.

<ul> <li>System ) High Availability Configu</li> </ul>	ration		
rrent Status Act	live	Current Status St	andby
Dedicated Port	LAN1	Dedicated Port	LANI
Status	Peer is detected	Status	Peer is detected
Link to Peer's UI	HA Configuration V Goto	Version	10000
Version	10000		

### 4.14 Reporting

EWS Controller can automatically send various kinds of user and/or system related reports to configured E-mail address, SYSLOG Server, or FTP Server.

#### 4.14.1 Notification

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

	SYSTEM	USERS	DEVICES			Ν	ETWO	DRK	UTILITI	ES	STATUS
System Summary	Main > Stat	us > Reporting > Notification S	ettings								
Interfaces			0								
Monitor Users	Notifi	cation Settings									
WiFi Monitor											
Process Monitor				Dee		F			0/51.00	Defenses (TTD	lator of
Logs & Reports				Rec	elver	E-ma	II Add	ress(es)	STSLUG	Primary FTP	Interval
Reporting			1	2	3	4	5	Detail / Test			
Notification Settings	Mo	nitor IP Report							N/A	N/A	1 Hour
FTP Settings	Loc	al Users Log									1 Hour
SMTP Settings	On	-Demand Users Log						13			1 Hour
Syslog Settings	Gu	est Users Log						15			1 Hour
Sessions	Roa	aming Out Users Log						13			1 Hour
Routing Tables	Roa	aming In Users Log						13			1 Hour
	Ext	ernal Users Log						13			1 Hour
	Soc	ial Media Users Log						13			1 Hour
	Ses	sion Log						13			1 Hour
	Fire	ewall Log						13		N/A	1 Hour
	Hig	h Availability Mode Change						13	N/A	N/A	N/A

### 4.14.2 FTP Setting

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITI	ES STATUS	5
System Summary	Main > Stat	us › Reporting › FTP Setti	ngs				
Interfaces							
Monitor Users		ottings					
WiFi Monitor	FIP 5	ettings					
Process Monitor							
Logs & Reports	Pri	mary FTP Server	IP Address		10.2.103.164	Fill in the IP Add	ress,Port of
Reporting						yor FTP server	
Notification Settings			Port		21		
FTP Settings	Log	çin	Anonym	ous 🖲 Normal			If the FTP server
SMTP Settings							need to login, fill in
Syslog Settings			Username		admin		the username and
Sessions			Password				password
DHCP Leases	- Cor	d Test File	Send	Sand the test file	to confirm the	configuratoin	-
Routing Tables	Ser	id fest file	Send	Send the test me		configuration	
	Sec	ondary FTP Server	IP Address				
			Port				
	Log	<i>i</i> n	Anonym	ous 🔍 Normal			
	Ser	nd Test File	Send				

### 4.14.3 SMTP Setting

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

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
ystem Summary	Main > Stat	us , Reporting , SMTP Set	tings			
rfaces						
onitor Users	SMTP	Settings				
iFi Monitor	_					
ocess Monitor						
ogs & Reports	SM	TP Server	Server Addres	10.2.4.25	*	
Reporting			Port	25	•	
Notification Settings	End	ryption	Disable	TLS SSL		
FTP Settings	Aut	hentication	Login	-		
SMTP Settings			Logar			
Syslog Settings			Account Nam	ne admin	*	
ssions			Password		*	
HCP Leases	Sor	der E-mail Address	controller@ex	ample.com	*	
outing Tables			controller @cx			
	Rec	eiver E-mail Address	Receiver 1	admin@example	e.com	
			Receiver 2	manager@exam	ple.com	
			Receiver 3			
			Receiver 4			
			Receiver 5			

	SYSTEM	ι	JSERS	5		DEVICES	N	IETWORK	UTILITIES	STATUS	
System Summary	Main > Status > Reporting > Notification S	ettings									
Interfaces											
Monitor Users	Notification Settings										
WiFi Monitor		c 1				-		C	1.000 of 11		
Process Monitor		Sele	CT K	ece	iver	C	lick test to	confirm the N	Notification e-mail c	ould receiv	e
Logs & Reports			Rec	eiver	r E-mail	Address(es)	SYSLOG	Primary FTP	Interval		
Reporting		1	2	3	4	5 Detail /	Test			service and	
Notification Settings	Monitor IP Report						N/A	N/A	1 Hour 🔻		alast the conding interval
FTP Settings	Local Users Log								1 Hour 🔻	3	select the senaing interval
SMTP Settings	On-Demand Users Log					10	01		1 Hour ▼		
Syslog Settings	Guest Users Log	0			0	0			1 Hour 🔻		
Sessions	Roaming Out Lisers Log					10	01	01	1 Hour V		
DHCP Leases	Roaming Out Osers Log	-	-	-					Thour	-	
Routing Tables	Roaming In Users Log			-					1 Hour V		
	External Users Log								1 Hour 🔻		
	Social Media Users Log								1 Hour 🔻		
	Session Log					10	0/		1 Hour 🔻	1910	
	Firewall Log					10		N/A	1 Hour 🔻	1.1.1.1	
	High Availability Mode Change					10	N/A	N/A	N/A		
	Local Area AP Status Change						N/A	N/A	2 Mins 🔻		

### 4.14.4 Syslog Setting

	SYSTEM	4 USERS	DEVICES	NETWORK	UTILITIES	STATUS
System Summary	Main > Status > Reporting > SYS	OG Settings				
Interfaces	main / status / neporting / sits	co d settings				
Monitor Users	SYSLOG Settings					
WiFi Monitor						
Process Monitor		-				
Logs & Reports	SYSLOG	Enabled	Disabled Enable SY	SLOG function		
Reporting	SYSLOG Server	Server 1				
Notification Settings			10.4 4444			
FTP Settings			IP Address T0.2.30.3	.0	Fill in IP and port o	of SYSLOG Server
SMTP Settings			Port 514	A CONTRACTOR OF		
Syslog Settings		Server 2	States and Street			
Sessions			IP Address:			
DHCP Leases						
Routing Tables			Port:			
	Severity Level	emergency	<ul> <li>Select Severity L</li> </ul>	evel		
		(	Apply S	Cancel		

	SYSTEM	USERS	DEVICE	s			NETWORK	l.	JTILITIES	STATUS
ystem Summary	Main > Sta	tus > Reporting > Notificatio	n Settings > Lo	ocal U	lsers	Log S	YSLOG Settings			
nterfaces			Ŭ				Ŭ			
Ionitor Users							Local Users Lo	g SYSLOG Se	ettings	
ViFi Monitor	Ta	a			ocal		Dotor	mine the	Tag. Sorverity	and Eacility
rocess Monitor	14	5	<u></u>		infor		Deter	inine the	rag, serverity	and Facility
ogs & Reports	Sev	/enty			mon	natio				
teporting	Fac	lility			local	• •				
Notification Settings										
Notification Settings FTP Settings							Apply	80	ancel	
Notification Settings FTP Settings SMTP Settings							Apply		ancel	
Notification Settings FTP Settings SMTP Settings Syslog Settings							Apply Apply		ancel	
Notification Settings FTP Settings SMTP Settings Syslog Settings essions		Garatian Cattin					Apply Apply		cancel	
Notification Settings FTP Settings SMTP Settings Syslog Settings essions DHCP Leases	Noti	fication Setting	zs				Apply		cancel	
Notification Settings FTP Settings SMTP Settings Syslog Settings essions OHCP Leases touting Tables	Noti	fication Setting	gs				Apply Click pencil t	o edit the	information o	of Local Users Log
Notification Settings FTP Settings SMTP Settings Syslog Settings essions OHCP Leases touting Tables	Noti	fication Setting	gs	Rec	elver	E-ma	Apply     Apply     Click pencil t     Il Address(es)	o edit the sysLog	information c Primary FTP	of Local Users Log Interval
Notification Settings FTP Settings SMTP Settings Syslog Settings eessions OHCP Leases touting Tables	Noti	fication Setting	gs 1	Rec 2	eiver 3	E-ma	Apply     Apply     Click pencil t     Il Address(es)     5 Detail / Te:	o edit the sysLog t	information c Primary FTP	of Local Users Log Interval
Notification Settings FTP Settings SMTP Settings Syslog Settings eessions OHCP Leases touting Tables	Noti	fication Setting Aonitor IP Report	35 1	Rec 2	eiver 3	E-ma 4	Apply     Apply     Click pencil 1     Address(es)     5 Detail / Te:	o edit the sysLog t	information c Primary FTP N/A	of Local Users Log Interval
Notification Settings FTP Settings SMTP Settings Syslog Settings eessions OHCP Leases touting Tables	Noti	fication Setting Aonitor IP Report .ocal Users Log	35 1 0	Rec 2	elver 3	E-ma 4	Click pencil ti Il Address(es) 5 Detail / Ter	o edit the sysLog t	information c Primary FTP N/A	of Local Users Log Interval