

# **Technical Guide**

# Authentication Flow on Controller

Released: 2018-05-03 Doc Rev. No: R1

### **Copyright Notification**

#### **Edgecore Networks Corporation**

© Copyright 2019 Edgecore Networks Corporation.

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

# Table of Contents

1	Introducti	on	.2
2	Authentic	ation Flow on Controller	.3
3	Authentic	ation Methods	.4
	3.1	MAC Access Control List (ACL)	. 4
	3.2	IP Privilege List	4
	3.3	MAC Privilege List	4
	3.4	Walled Garden List	5
	3.5	802.1X Authentication	5
	3.6	MAC Authentication	5
	3.7	WISPr Authentication	5
	3.8	Web-based Authentication	6
4	Configura	tions	.6
	4.1	MAC Access Control List	6
	4.2	IP Privilege List	. 7
	4.3	MAC Privilege List	8
	4.3.1	Example: MAC Address Based Full Group Policy Enforcement (with QoS)	8
	4.4	Walled Garden List	9
	4.5	802.1X Authentication	10
	4.6	MAC Authentication	13
	4.7	WISPr Authentication	14
5	Remarks.	1	12

## 1 Introduction

With support for authentication, authorization, and accounting (AAA), the controller allows network administrators to effectively manage network access, control network usage and monitor user activities.

In this technical guide, the authentication flow on the controller is illustrated using a flowchart. With this flowchart, readers would be able to understand the order in which authentication methods are presented on the controller, so they could better plan the authentication methods they'd like to leverage as well as better understand how they could troubleshoot if necessary.

Furthermore, as will be seen from the flowchart, a variety of authentication methods are available on the controller for network access control, including web-based, 802.1X, WISPr and MAC authentication. How each authentication method works and where to configure its settings are also explained.

## 2 Authentication Flow on Controller

Flowchart below illustrates the authentication flow on the controller.



As can be seen from the flowchart, the authentication flow on the controller goes in the general order of MAC Access Control List > Privilege List > Walled Garden > Non-web Authentication > Web-based Authentication.

For all clients, MAC Access Control List (ACL) is the first "gate". When MAC ACL is enabled, if a client device is not on the Allow List or if it is on the Deny List, it would not be able to obtain a DHCP IP address, and thus would not see the Login Page and be denied network access through the controller.

Clients can be granted network access directly based on their MAC address and/or IP address through the MAC/IP Privilege List. Note that clients authenticated through this method would not appear in "Online Users" but in "Non-Login Devices".

### 3 Authentication Methods

### 3.1 MAC Access Control List (ACL)

MAC Access Control is used to grant or deny permission to access the User Login Page. As mentioned earlier, if a client device is denied access to the network based on this list, it would not even obtain a DHCP IP address and thus would not be able to access the Login Page.

When the List Type is "Allow", the list can be considered as a whitelist because only the MAC addresses on this list can access network. When the list type is "Deny", the list can be considered as a blacklist.

"Allow" type is usually used for closed systems.

### 3.2 IP Privilege List

IPv4 addresses of client devices can be added to the IP Privilege List so that these devices can be granted network access without login. Each device/IP address can be assigned to a Group so that Group Policy can be enforced on the device. For each entry on the list, the client device's MAC address can be optionally added to bind to its IPv4 address.

IP Privilege List can be used with client devices having static IP addresses. Alternatively, it can be used with a DHCP server for assigning DHCP IP addresses to client devices.

### 3.3 MAC Privilege List

MAC addresses of devices can be added to the MAC Privilege List so that these devices can be granted

network access without login. Note that Default Policy (excluding QoS) of the particular Service Zone will be enforced on clients authenticated this way. To configure Default Policy, go to *System > Service Zone > Service Zone Configuration*, and disable Authentication under Authentication Settings to reveal Default Policy. Note that this Default Policy still applies even when Authentication is set to "Enable".

With IP Privilege List, IP address based Group Policy enforcement can be achieved. However, with MAC Privilege List, QoS in Group Policy cannot be applied. Thus, to achieve MAC address based Group Policy enforcement with QoS, one can combine the use of IP Privilege List with DHCP Reserved IP List. An example of this will be provided later in Section 4.3.1.

#### 3.4 Walled Garden List

Client devices can access destinations on the Walled Garden List without login, where the destinations are defined by their domain name, IP address or subnet.

Traffic to Walled Garden List can be blocked by User Firewall Rules under Policy.

#### 3.5 802.1X Authentication

802.1X authentication is to be used in conjunction with back-end authentication server configured on the controller. When enabled, if the connected device has its credentials stored on the back-end server, the controller will automatically authenticate and grant network access to provide transparent login.

For 802.1X authentication, the controller must be the RADIUS server configured on the AP (or switch).

#### 3.6 MAC Authentication

MAC Authentication is to be used in conjunction with a RADIUS server configured on the controller. When enabled, if the connected device has its MAC address stored on the RADIUS Server, the controller will automatically authenticate and grant network access to provide transparent login.

#### 3.7 WISPr Authentication

Similar to WebSheet (Captive Network Assistant) on iOS devices, some devices have built-in Smart Client. The Smart Client will detect if the WLAN is a Captive Network by sending requests to a URL as defined by the manufacturer. When WISPr authentication is configured and the Smart Client on a client device is connected to the WLAN, the controller will automatically authenticate and grant network access to provide transparent login for the device.

Some Android devices do not have built-in Smart Client. For Windows systems, built-in Network

5

Connectivity Status Indicator (msftncsi) is available for Windows 7 and above.

#### 3.8 Web-based Authentication

If client devices cannot be granted network access by all of above methods, a browser or browser-like may pop up, or the user has to open browser to visit a web site then redirect to login page (Captive Portal).

Web-based authentication also called Universal Access Method (UAM).

### 4 Configurations

#### 4.1 MAC Access Control List

a. Go to User > Additional Controls, scroll down to "MAC Access Control List" and click
 "Configure" to enter the configuration page.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups Authentication Servers Internal Authentication External Authentication On-Demand Accounts Schedule Policies Blackling	Session Timeout Idle Timeout Interim Update Certificate Remaining Quota	1 5 C	20 minute(s) *(5-432 0 minute(s) *(1-504 minute(s) *(1-120 Default CERT ▼	00) )0)			
Privilege Lists Additional Controls	Time and Cut-off Remin Volume Reminder	der (	Enable  Disable Lisable Lisable				
	Reminder Refresh Time	( trol List	● 10mins ○ 15mins ○ .	20mins			
	MAC Access Control Lis	t	Configure MAC Access Control is used the User Login Page.	to grant or deny permissior	n to access		

Configure the MAC Access Control List

a. Click "Add MACs" to start adding entries to the list.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main › Users › Additional Cor	ntrol > MAC Address Co	ontrol			
Authentication Servers						
Internal Authentication	List Type O Allow	v 🔍 Denv 🖲 Disab	le Apply			
External Authentication						
On-Demand Accounts	Access Contro	llist				
Schedule	Access contro	I LISC				
Policies						
Blacklists	Add MACs Delet	e Backup List Re	store List			
Privilege Lists						
Additional Controls		No.			MAC Address	
		(т	otal:0/1000) 🍽 First ዽ Pr	ev Next∳ Last∳ Go to Page	• (Page:1/1)	Row per Page: 20 🔻

#### Click "Add MACs" button

c. Enter the MAC address(es) of the client device(s) and click "Apply".

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main > Users > Additional Cont	rol > MAC Address Con	trol - Add MAC			
Authentication Servers						
Internal Authentication	Add MAC Acces	s Control				
External Authentication						
On-Demand Accounts						
Schedule	1000 Remaining MAC					
Policies	No.	MAC	Address	No.	MAC A	ddress
Blacklists						
Privilege Lists	1	00:00:00:	DD:DD:DD	2		
Additional Controls	3			4		

Enter the client device's MAC address

d. Select List Type "Deny" and click Apply. As mentioned earlier, client devices with their MAC addresses on the Deny List would not be able to 1) get a DHCP IP address from the controller, 2) access the Login Page; and 3) have network access through the controller.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main › Users › Additional C	ontrol > MAC Address Co	ntrol			
Authentication Servers			. <u></u>			
nternal Authentication	List Type O Allo	ow 🖲 Denv 🔘 Disabl	Apply			
External Authentication		on a beny a bloos				
On-Demand Accounts	Access Contro	allist				
Schedule	Access contro	JILISU				
Policies						
Blacklists	Add MACs Del	ete Backup List Re	store List			
Privilege Lists						
Additional Controls	•	No.			MAC Address	
		1		00:	00:00:DD:DD:DD	

#### Configure List Type to "Deny"

### 4.2 IP Privilege List

a. Go to Users > Privilege Lists > IP Privilege Lists, click "Add".

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main > Users > Privileg	e List > IP Privilege List				
Authentication Servers						
nternal Authentication	IP Privileg	e List				
External Authentication						
Dn-Demand Accounts						
Schedule	Add D	elete Backup List	Restore List			Search IP
Policies		IP Address		AAC Address	Group	Pemark
lacklists	- 110.	Il Address			Group	Nemark
rivilege Lists			(Total:0/2000) MeFin	st • Prev Next • Last •	Go To Page (Page:1/1)	Row per Page: 10
IP Privilege List						
IPv6 Privilege List						
MAC Privilege List						
Additional Controls						

Click Add button

b. Enter the client device's IP address and click "Apply". The device can access the network without redirection to login page, and be authorized based on its Group Policy. However, only Firewall, Session Limit, QoS and Specific Routes will apply.

Priv	ilege IP	Address			
	Item	IP Address	MAC Address	Group	Remark
	1	192.168.1.2	00:00:00:00:00:02	Group 2 🔻	
	2			Group 1 🔻	
	3			Group 1 🔻	

Enter address to IP Privilege List

#### 4.3 MAC Privilege List

a. Go to *Users > Privilege Lists > MAC Privilege Lists*, click "Add".

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main > Users > Privileg	<b>te List</b> > MAC Privilege Lis	ŧ			
Authentication Servers						
Internal Authentication	MAC Privi	lege List				
External Authentication						
On-Demand Accounts						
Schedule	Add D	Backup List	Restore List			Search MAC
Policies	No.		MAC Address	Statements and statements	Re	mark
Blacklists						
Privilege Lists			(Total:0/2000) PFin	st 🗣 Prev Next 🗣 Last🗣	Go to Page 🔻 (Page:1/1)	Row per Page: 10 🔻
IP Privilege List						
IPv6 Privilege List						
MAC Privilege List						
Additional Controls						

Click "Add" button from MAC Privilege List

b. Add the client device's MAC address to the list and click "Apply". The device with this MAC address can access network without redirect to login page.

Privi	ilege MAC	Address		
	ltem	MAC Address	Remark	
	1	00:00:00:00:03	VIP	
	2			

Enter address to MAC Privilege List

### 4.3.1 Example: MAC Address Based Full Group Policy Enforcement (with QoS)

A client device will be given MAC address based privileged network access in multiple Service Zones with full Group Policy enforcement (with QoS). The client device will have Privilege IP Addresses of

192.168.1.10 in the Default Service Zone, 172.21.0.10 in SZ1 and 172.22.0.10 in SZ2, respectively.

 a. Go to System > Service Zone > Service Zone Configuration > DHCP Configuration > Reserved IP Address List in the Default Service Zone, add an entry with a Reserved IP Address of 192.168.1.10 with a MAC Address of AA:BB:CC:DD:EE:FF.

Reperved in Address List Scrutee Lone Derdalt	Reserved	IP	Address	List -	Service	Zone	Default
---	----------	----	---------	--------	---------	------	---------

No.	Reserved IP Address	MAC Address	Description
1	192.168.1.10	AA:BB:CC:DD:EE:FF	
2			
3			

- b. Go to the Reserved IP Address List in SZ1, add an entry with a Reserved IP Address of 172.21.0.10 with the same MAC Address.
- c. Go to the Reserved IP Address List in SZ2, add an entry with a Reserved IP Address of 172.22.0.10 with the same MAC Address.
- d. Go to *Users > Privilege List > IP Privilege List*, add multiple entries with the same client device's MAC address binding to different Privilege IP Addresses for different Service Zones.

Item	IP Address		MAC Address		Group	Remark
1	192.168.1.10	in Default SZ	AA:BB:CC:DD:EE:F		Privilege 🔻	
2	172.21.0.10	in SZ1	AA:BB:CC:DD:EE:F	Same MAC address	Privilege ▼	
3	172.22.0.10	in SZ2	AA:BB:CC:DD:EE:F		Privilege ▼	
4					Privilege ▼	
5					Privilege 🔻	

#### 4.4 Walled Garden List

Privilege IP Address

a. Go to *Network > Walled Garden*, click "Add".

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
NAT	Main > Network > Wal	lled Garden				
Monitor List						
Walled Garden	Walled Ga	arden List				
VPN						
Proxy Server						
Local DNS Records	480 entries 80 advertise	can be added to the Wall ement entries can be disp	led Garden List. blayed on the user login	page.		
Dynamic Routing	Add De	elete Backup Walled G	arden List Restore W	alled Garden List		
DDNS						
Client Mobility	No.	Domain Name/IP A	Address/URL		Walled Garden / Advertise	ment
			(Total:0/480) MeFi	rst •Prev Next• Last• G	to Page 🔻 (Page:1/1)	Row per Page: 20

Click "Add" button from Walled Garden List

b. Add the domain name, IP address or subnet of the desired destination to the list and click"Apply". Client devices can go to these destinations without redirection to the Login Page.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
NAT	Main > Network > Wal	led Garden › Add Walled G	arden List				
Monitor List							
Walled Garden	Add Walle	d Garden Lis	st				
VPN							
Proxy Server			Non				
Local DNS Records	Domain Nar	me/IP Address/URL 8.8.8	3.8				
Dynamic Routing	Walled Gard	len		Advertisem	ent		
DDNS		Active: 🗹			Display:		
Client Mobility	Se	ervice Zone: All			Protocol: http 🔻		
		Remark: Google DNS			Topic:	*	
					Description		

Add destinations to Walled Garden List

c. Go to System > Service Zone > Service Zone Configuration, scroll down to "MAC Authentication" of Service Zone and Enable this option. By default, the back-end RADIUS server is "Server 2" (Configured in the Auth. Option for RADIUS).

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATU
General	Authentic	ation Settin	gs			
WAN			.0-			
IPv6						
LAN Ports	Authenticat	ion	🖲 Enable 🔘 Disat	ole 🔍 Suspend		
High Availability			When Authentication	is set to Suspended, users wo	uld see a suspend	
Service Zones			message from Genera	al Settings.		
Port Location Mapping	Access Pern Authorizatio	nission and	Configure			
PMS Interface	, action 2000					
	Portal URL		🖲 Specific 🔘 Orig	ginal 🔍 None		
			http://www.google.c	om *		
			(e.g. http://www.exa	mple.com)		
	MAC Authe	entication	Enabled Dis	abled		
			MAC Auth. Serve	r Server 2(radius) 🔻		
			RADIUS Authenticatio	on using MAC address		
	PPP Auther	ntication	Enabled I Dis	abled		

MAC Authentication

#### 4.5 802.1X Authentication

a. Go to *Users > Authentication Servers*, click Server Name "Server 2" in this case.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups	Main > Users > Authent	ication Servers					
Authentication Servers							
Internal Authentication	Authentica	ation Servers					
External Authentication							
On-Demand Accounts				100 C 100		AND MARKED	100
Schedule	No.	Server Name	Authe	entication	Postfix	BlackList	Remark
Policies	1	Server 1	L	OCAL	e	None	
Blacklists	2	Server 2	R	ADIUS	radius	None	
Privilege Lists	2	Comune 2	NIT	COMMIN	otdomain	Nana	
Additional Controls	3	Server 3	NIL	JOMAIN	ntdomain	None	
	4	Server 4	1	LDAP	Idap	None	
	5	Server 5	f	POP3	pop3	None	

#### Authentication Servers

b. Configure Authentication Option. The postfix is "example.com" in this case.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main > Users > Auther	itication Servers > Authen	itication Option			
Authentication Servers						
Internal Authentication	Authentic	ation Optio	n - Server 2			
External Authentication						
On-Demand Accounts						
Schedule	Server No	0.2				
Policies	Name		Server 2	*		
Blacklists	User Postfix	¢	example.com	*		
Privilege Lists	Demande					
Additional Controls	Remark					
	Blacklist		None 🔻			
	Authenticat	ion	RADIUS •			

Configure Authentication Option

c. Go to *Users > Internal Authentication > RADIUS*, configure RADIUS Server settings.

	SYSTEM	USERS	DEVICES	NETWORK	UTILIT	IES STATUS
Groups	Primary RADI	US Server	Authoritication Sonior			*(Domain Name/IR Address)
Authentication Servers			Authentication Server			(Domain Namerie Address)
Internal Authentication			Authentication Port		*(Default: 1812)	
External Authentication			Authentication Secret Key		*	
POP3			Authentication Protocol	CHAP V		
LDAP						
RADIUS			Accounting Service	Enable	Disable	
NT Domain			Accounting Server			*(Domain Name/IP Address)
SIP			Accounting Port		*(Default: 1813)	
Social Media			Accounting Secret Key		*	
On-Demand Accounts			Accounting Secret Key			
Schedule	Secondary RA	DIUS Server				
Policies			Authentication Server			(Domain Name/IP Address)
Blacklists			Authentication Port			
Privilege Lists			Authentication Secret Key			
Additional Controls			Authentication Protocol	CHAP V		

Configure RADIUS Server settings

d. Enable "802.1X Authentication" and click "Apply". Then, go to "802.1X Settings".

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main > Users > External Authentic	cation > RADIUS	5			
Authentication Servers						
Internal Authentication	Server No. 2: Server 2 🔻					
External Authentication						
POP3	External RADIUS	Server	Settings			
LDAP						
RADIUS	Froun		Croup 2 .			
NT Domain	Group		Gloup 2 •			
SIP	802.1X Authentication		Enable Disable 802.1	(Settings		
Social Media	Username Format		Leave Unmodified O Com	plete (e.g. user1@postfix	) Only ID (e.g. user1)	
On-Demand Accounts	NAS Identifier					
Schedule						
Policies	NAS PORT Type		19 *(Derault 19, Range: 043	33)		
Blacklists	Accounting Delay Time		0 *(Deafult: 0)			
Privilege Lists	Service Type		1 *(Default: 1, Range: 1~1	1)		
Additional Controls	Class					

Enable 802.1X Authentication

e. Add the subnet or IP address of the 802.1X authenticator (AP or switch) to the RADIUS Client Device List, and select default RADIUS server for the client credential only with ID (without the email-like postfix "@example.com").

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS						
Groups	Main > Users > External Aut	hentication > RADIUS > R	oaming Out & 802.1X									
Authentication Servers												
Internal Authentication	802.1X Auth S	802.1X Auth Setting										
External Authentication												
POP3			0.0									
LDAP	Default Auth Serve	er Se	rver 21 Postfix: exampl	e.com) • (The Auth server is	tor username only with ID, i	.g. useri.)						
RADIUS												
NT Domain	RADIUS Clien	t Device Set	tings									
SIP		e bernee bet										
Social Media												
On-Demand Accounts	No. Type	e IP Ad	ldress	Subnet Mask	Secret Key	SNMP Community						
Schedule	1 802.1X	▼ 192.168	1.0	55.255.255.0 (/24)								
Policies												
Blacklists	2 Disable	• L		55.255.255.255 (/32) 🔻								
Privilege Lists	3 Disable	<b>v</b>		55.255.255.255 (/32) 🔻								
Additional Controls	4 Disable	•		55.255.255.255 (/32) 🔻								

Configure RADIUS client device list

f. Configure control as RADIUS server in AP, and security should be WPA2-Enterprise.



g. When client device connected to the WLAN, the controller will automatically authenticate and grant network access to provide transparent login.

### 4.6 MAC Authentication

a. Go to *System > Service Zones*. In this example, "Default" Service Zone is selected.

	SYSTEM	USERS	NETWO	ORK	UTILITIES	STATUS				
General	Main > System > Servi	ce Zone								
WAN										
IPv6	Service Zone Settings									
LAN Ports										
Service Zones										
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		
	011	SZ1	172.21.0.254	N/A	1	Server 1	N/A	172.21.0.1 ~ 172.21.0.100		
	C OFF	SZ2	172.22.0.254	N/A	2	Server 1	N/A	172.22.0.1 ~ 172.22.0.100		

To configure Default Service Zone

b. Scroll down to "MAC Authentication" of Service Zone and Enable this this option. By default, the back-end RADIUS server is "Server 2" (Configured in the Auth. Option for RADIUS).

	SYSTEM	USERS	DEVICES	5 N	etwork		UTILIT	TIES STATUS
General	MAC Authent	ication	Enabled O Dis	sabled				
WAN			MAC Auth. Serve	er Server 2(radius)	•			
IPv6			RADIUS Authenticati	ion using Maraddre				
LAN Ports	PPP Authenti	cation		cabled	-			
Service Zones	FFF Autient	cauon	<ul> <li>Enabled</li> <li>Dis</li> </ul>	sabled				
Port Location Mapping	SIP Interface	Configuration	Enabled I Dis	sabled				
PMS Interface	WISPr Setting	s	Configure					
	Authentication Options		Auth. Option	Auth. Database	Postfix	Default E	nabled	
			Server 1	LOCAL	local	۲		
			Server 2	RADIUS	radius	0		
			Server 3	NTDOMAIN	ntdomain	0		
			Server 4	LDAP	ldap	•		
			Server 5	POP3	рор3	•		
			On Domand	ONDEMAND	ondomand	0		



c. Go to *Users > External Authentication > RADIUS*, enter settings of RADIUS server.

	SYSTEM	USERS	DEVICES	NETWORK	UTILIT	IES STATUS
Groups	Primary RAD	OIUS Server	Authoritication Comm			t(Domein Nome (ID Address)
Authentication Servers			Authentication Server			"(Domain Name/IP Address)
Internal Authentication			Authentication Port		*(Default: 1812)	
External Authentication			Authentication Secret Key		*	
POP3			Authentication Protocol	CHAP <b>T</b>		
LDAP						
RADIUS			Accounting Service	Enable	Disable	
NT Domain			Accounting Server			*(Domain Name/IP Address)
SIP			Accounting Port		*(Default: 1813)	
Social Media			Accounting Secret Key		*	
On-Demand Accounts			Accounting Secret Key			
Schedule	Secondary R	ADIUS Server				
Policies	,		Authentication Server			(Domain Name/IP Address)
Blacklists			Authentication Port			
Privilege Lists			Authentication Secret Key			
Additional Controls			Authentication Protocol	CHAP <b>T</b>		



d. When the connected device has its MAC address stored on the RADIUS Server, the controller will automatically authenticate and grant network access to provide transparent login.

#### 4.7 WISPr Authentication

a. Go to *System > Service Zones > Service Zone Configuration*, configure WISPr Settings.

	SYSTEM	ERS	DEVICES	NETWORK	UTILITIES	STATUS
General	Authentication Setti	ings				
WAN						
IPv6						
LAN Ports	Authentication	• E	nable 🔍 Disable 🔍	Suspend		
High Availability		Wh	en Authentication is set pend message from Ge	t to Suspended, users would si eneral Settings.	ee a	
Service Zones	Access Permission and Author	rization Cor	nfigure			
Port Location Mapping						
PMS Interface	Portal URL	۲	Specific 🔍 Original 🕛	None		
		http: (e	<b>://www.google.com</b> .g. http://www.example.	.com)		
	MAC Authentication	•	Enabled 💿 Disabled			
		RA	DIUS Authentication us	ing MAC address		
	PPP Authentication	•	Enabled 💿 Disabled			
	SIP Interface Configuration	0	Enabled 💿 Disabled			
	WISPr Settings	Co	nfigure			
	Authentication Options	1	Auth. Option Auth.	Database Postfix Def	ault Enabled	

Configure "WISPr Settings"

b. Enable WISPr Smart Client and enter related parameters.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
General	Main > System > Service Zone	> Service Zone Co	nfiguration - WISPr Configuration	n		
WAN						
IPv6	WISPr Configu	ration				
LAN Ports						
High Availability			a a			
Service Zones	WISPr Smart Client		Enabled U Disabled			
Port Location Mapping	Smart Client Black Li	st	Enabled I Disabled			
PMS Interface						(Separate by comma)
	WISPr Location ID		ISO Country Code E.164 Country Code E.164 Area Code Network (SSID/ZONE)	[[] [] [] [] [] [] [] [] [] [] [] [] []	g. US) g. 1) g. 408) g. MYWIFI)	
	WISPr Location Nan	ie	Hotspot Operator Location		(e.g. (e.g.	MYISP) Lobby_of_Airport)
	WISPr Billing Time		0 • : 0 • (HH:MM)			

Enter WISPr Parameters

c. When Smart Client on a client device is connected to the WLAN, the controller will automatically authenticate the device and grant network access to provide transparent login.

## 5 Remarks

Please contact Technical Support Team for additional inquiries.