Technical Guide

How to setup 802.1x Transparent Login with a CAPWAP-tunneled AP

Released: 2020-05-27

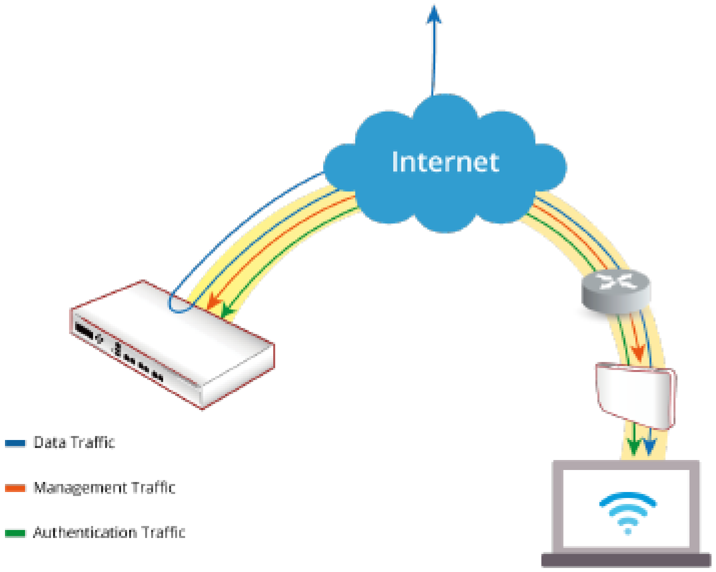
Copyright Notification

Edgecore Networks Corporation

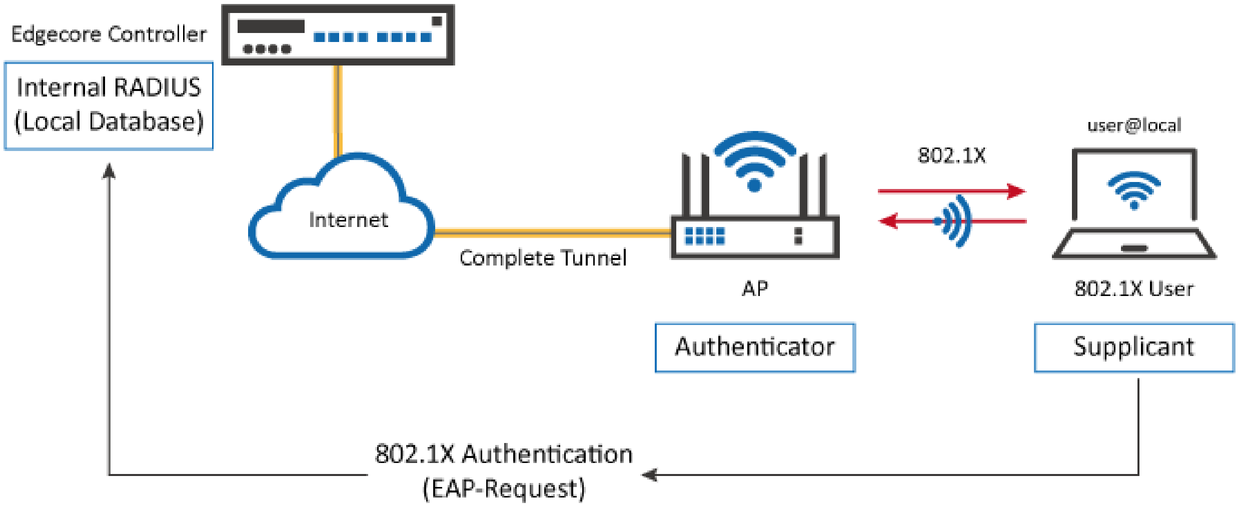
Table of Contents

Pre-requisite

Refer to the technical guide “CAPWAP Tunnel Configuration.” Complete Tunnel uses the CAPWAP protocol to communicate with an Access Point so that all management traffic, authentication traffic, and data traffic from the service area Access Point provided area transmitted back to the Controller before forwarding data traffic to the internet.



1. Introduction



This technical guide provides the administrator with instructions on how to set up the scenarios above.

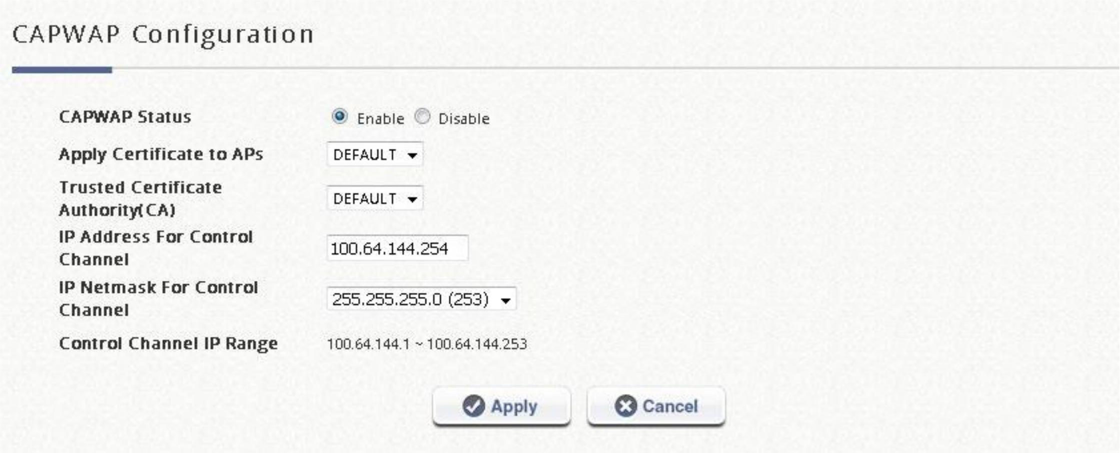
The Controller can implement role-based policies over Layer 3 networks, with user access control available in the remote sites. This feature allows the Controller to support centralized

Access Point management and user management, including authenticated with a RADIUS server in 802.1x Authentication (transparent login).
User can deploy this scenario if there RADIUS server is in a intranet, but they could have a Controller deployed with a public IP, so that their network could extend across the Internet, penetrating NATs, and deploy the local network to a remote site, such as penetrating the Great Fire Wall.

2. Configuring CAPWAP and WAPM

2.1. Configure CAPWAP Settings on the Controller with complete-tunnel

Step 1. Enable CAPWAP Status under CAPWAP Tab in WAPM



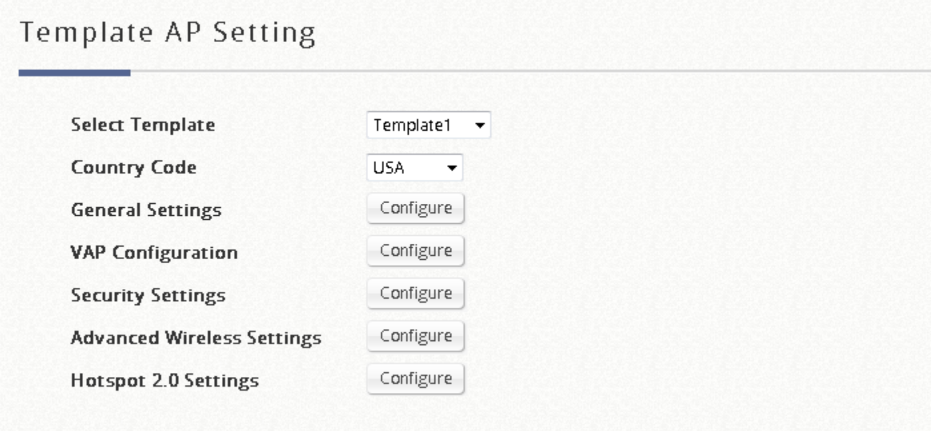
CAPWAP Configuration

CAPWAP Status	● Enable ○ Disable
Apply Certificate to APs	DEFAULT
Trusted Certificate Authority(CA)	DEFAULT
IP Address For Control Channel	100.64.144.254
IP Netmask For Control Channel	255.255.255.0 (253)
Control Channel IP Range	100.64.144.1 ~ 100.64.144.253

Main › Device Management › Wide Area AP Management › CAPWAP

Note: Certificate field can be modified with an uploaded certificate if required.
Note: Not recommended to modify IP Address and Netmask for Control Channel.

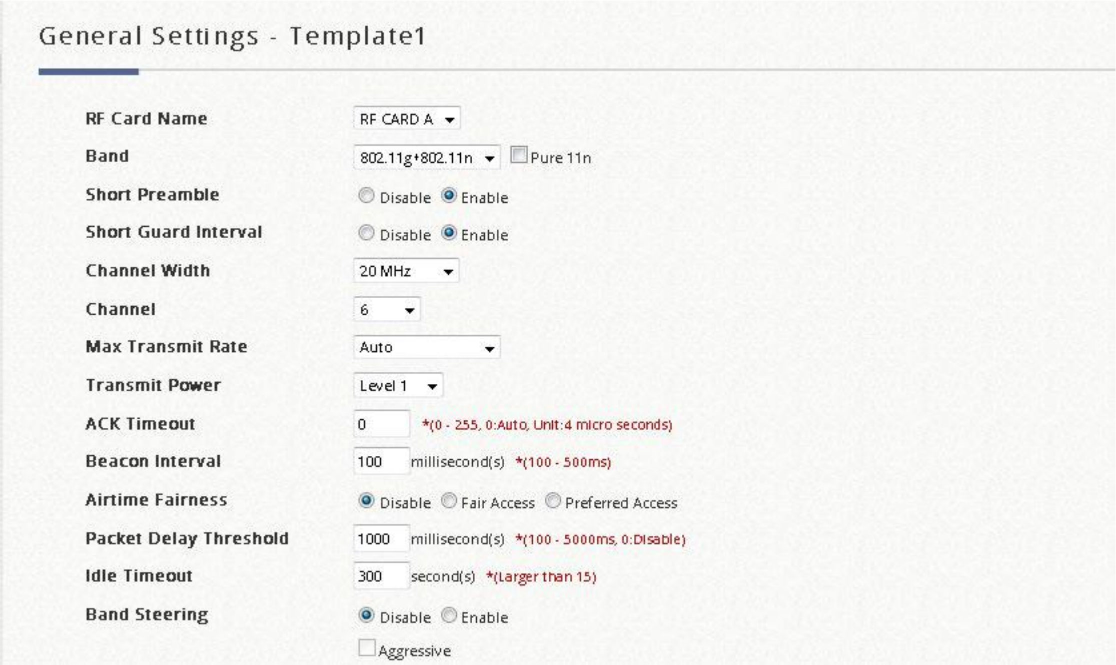
2.2. Configure Template for Remote AP Configuration



Template AP Setting

Select Template	Template1
Country Code	USA
General Settings	Configure
VAP Configuration	Configure
Security Settings	Configure
Advanced Wireless Settings	Configure
Hotspot 2.0 Settings	Configure

Step 1. Confirm the specifications of the AP before configuring the Template.
Step 2. Configure Template.
Step 3. Configure General Settings.
Step 4. Confirm RF Card A & B support selected Bands.
Step 5. Step 5. Click Apply and return to the Template page.



General Settings - Template1

RF Card Name	RF CARD A
Band	802.11g+802.11n □ Pure 11n
Short Preamble	○ Disable ● Enable
Short Guard Interval	○ Disable ● Enable
Channel Width	20 MHz
Channel	6
Max Transmit Rate	Auto
Transmit Power	Level 1
ACK Timeout	0 *(0 - 255, 0:Auto, Unit:4 micro seconds)
Beacon Interval	100 millisecond(s) *(100 - 500ms)
Airtime Fairness	● Disable ○ Fair Access ○ Preferred Access
Packet Delay Threshold	1000 millisecond(s) *(100 - 5000ms, 0:Disable)
Idle Timeout	300 second(s) *(Larger than 15)
Band Steering	● Disable ○ Enable □ Aggressive

Step 6. Configure VAP Configuration.

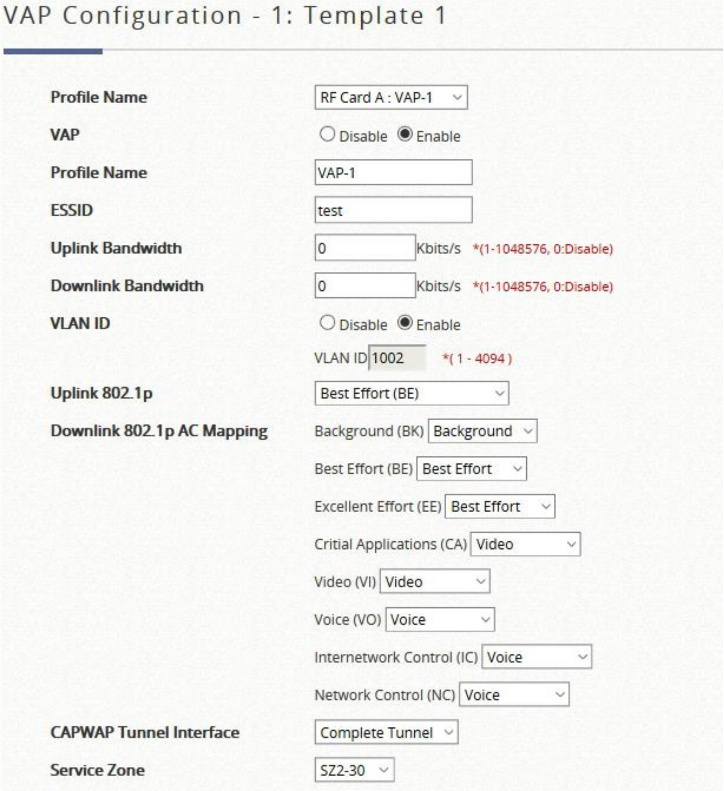
Step 7. Enable VAP.

Step 8. Fill in a Profile Name and ESSID.

Step 9. Configure VAPs with Complete Tunnel.

Select Complete Tunnel under CAPWAP Tunnel Interface.

Select Service Zone for AP to be managed and Apply.

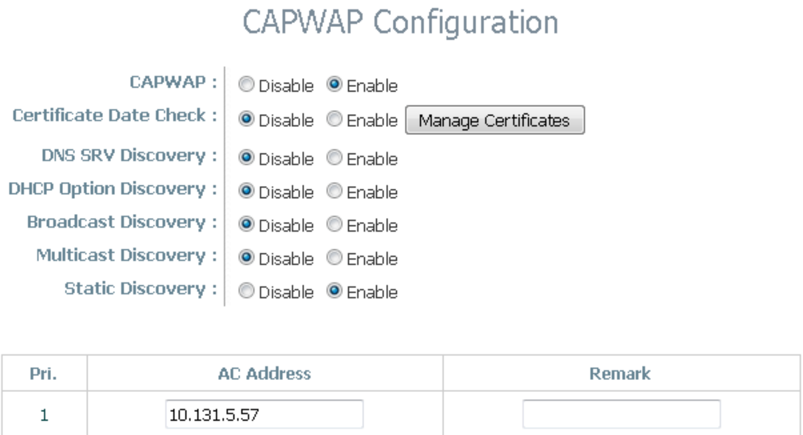


VAP Configuration - 1: Template 1

Profile Name	RF Card A : VAP-1
VAP	○ Disable ● Enable
Profile Name	VAP-1
ESSID	test
Uplink Bandwidth	0 Kbits/s *(1-1048576, 0:Disable)
Downlink Bandwidth	0 Kbits/s *(1-1048576, 0:Disable)
VLAN ID	○ Disable ● Enable VLAN ID 1002 *(1 - 4094)
Uplink 802.1p	Best Effort (BE)
Downlink 802.1p AC Mapping	Background (BK) Background Best Effort (BE) Best Effort Excellent Effort (EE) Best Effort Critial Applications (CA) Video Video (VI) Video Voice (VO) Voice Internetwork Control (IC) Voice Network Control (NC) Voice
CAPWAP Tunnel Interface	Complete Tunnel
Service Zone	SZ2-30

3. Pre-deployment or On-site Configuration

Step 1. Enable CAPWAP on AP’s WMI.
Step 2. Enable only Static Discovery.
Step 3. Enter and Apply AC’s WAN IP Address into field.
Step 4. Reboot as required.



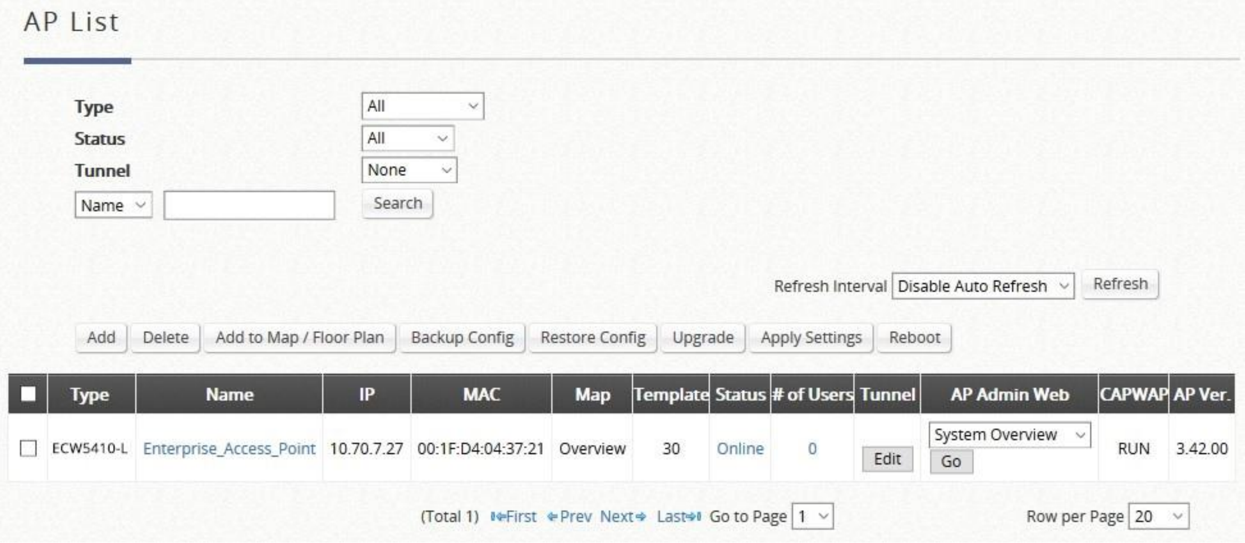
CAPWAP Configuration

CAPWAP :	○ Disable ● Enable
Certificate Date Check :	● Disable ○ Enable [Manage Certificates]
DNS SRV Discovery :	● Disable ○ Enable
DHCP Option Discovery :	● Disable ○ Enable
Broadcast Discovery :	● Disable ○ Enable
Multicast Discovery :	● Disable ○ Enable
Static Discovery :	○ Disable ● Enable

Pri.	AC Address	Remark
1	10.131.5.57	

Note: Static discovery is the most recommended discovery method since it is intuitive to implement without any pre-settings to complete in advance. Enable the function and type in the IP address of the Controller that will manage this AP.

Successful CAPWAP joining will lead to the Access Point being listed in the managed AP list, as illustrated below:
CAPWAP column will display a ‘RUN’ status, and the tunnel status will show a clickable ‘Edit’ button in black if configure a VAP tunneled back to the Controller.



AP List

Type	All
Status	All
Tunnel	None
Name	[Search]

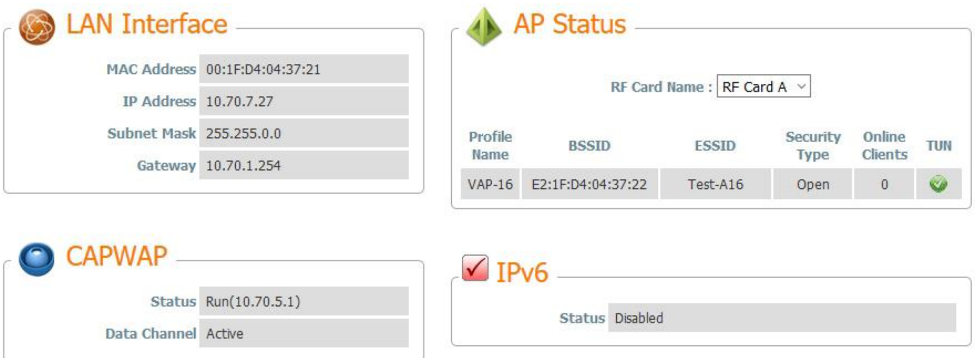
Refresh Interval: Disable Auto Refresh [Refresh]

■	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.
☐	ECW5410-L	Enterprise_Access_Point	10.70.7.27	00:1F:D4:04:37:21	Overview	30	Online	0	Edit	System Overview Go	RUN	3.42.00

(Total 1) First Prev Next Last Go to Page 1 Row per Page 20

Note: Remember the Public IP shown on the Controller, for example, 10.70.7.27. We will need it when editing the 802.1x settings. This will be mentioned in the later chapter.

The Access Point’s WMI will show the VAP enabled, the VAP’s tunnel status with a green checkmark and the CAPWAP status on the System Overview page:



LAN Interface

MAC Address	00:1F:D4:04:37:21
IP Address	10.70.7.27
Subnet Mask	255.255.0.0
Gateway	10.70.1.254

AP Status

RF Card Name : RF Card A

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-16	E2:1F:D4:04:37:22	Test-A16	Open	0	✓

CAPWAP

Status	Run(10.70.5.1)
Data Channel	Active

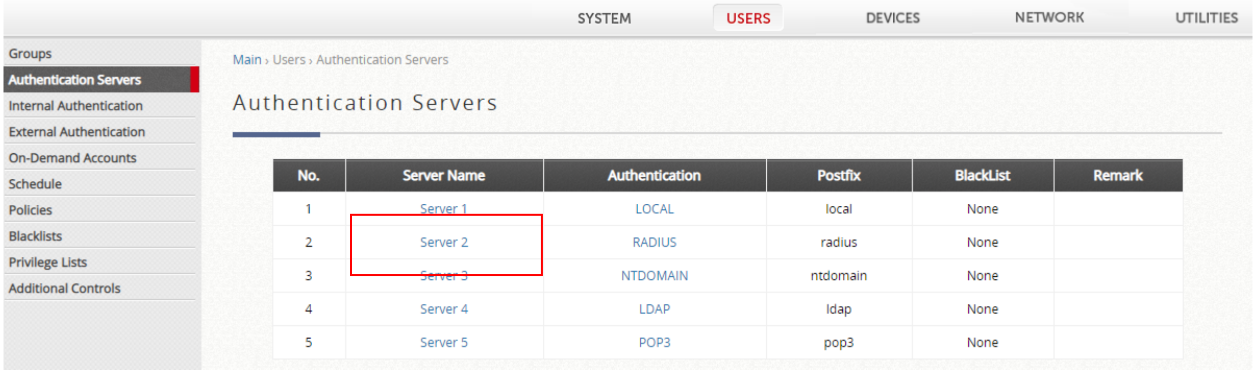
IPv6

Status	Disabled

On the Access Point side, a successful CAPWAP will display the Status as Run and followed by the AC's IP Address.

The Data Channel as Active indicates both Control and Data Channels are successfully established.

Go to USERS→Authentication Servers, select "Server 2."

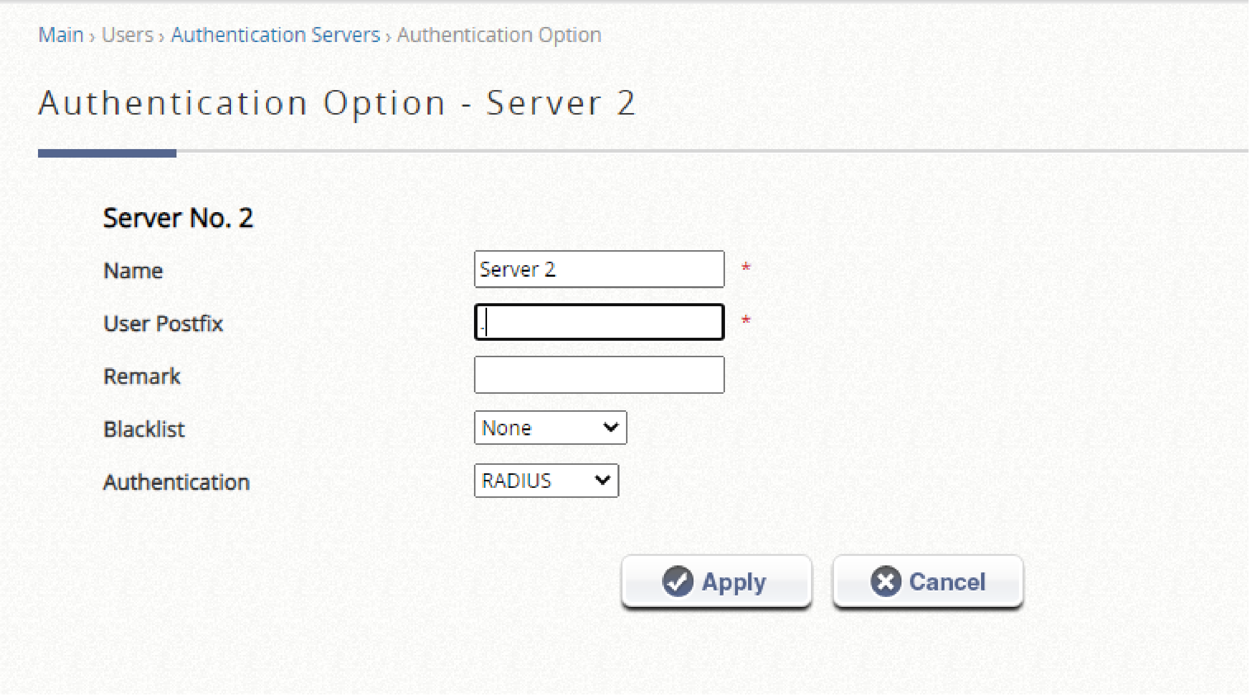


Main › Users › Authentication Servers

Authentication Servers

No.	Server Name	Authentication	Postfix	BlackList	Remark
1	Server 1	LOCAL	local	None	
2	Server 2	RADIUS	radius	None	
3	Server 3	NTDOMAIN	ntdomain	None	
4	Server 4	LDAP	ldap	None	
5	Server 5	POP3	pop3	None	

And edit the User Postfix="." Then Apply.



Main › Users › Authentication Servers › Authentication Option

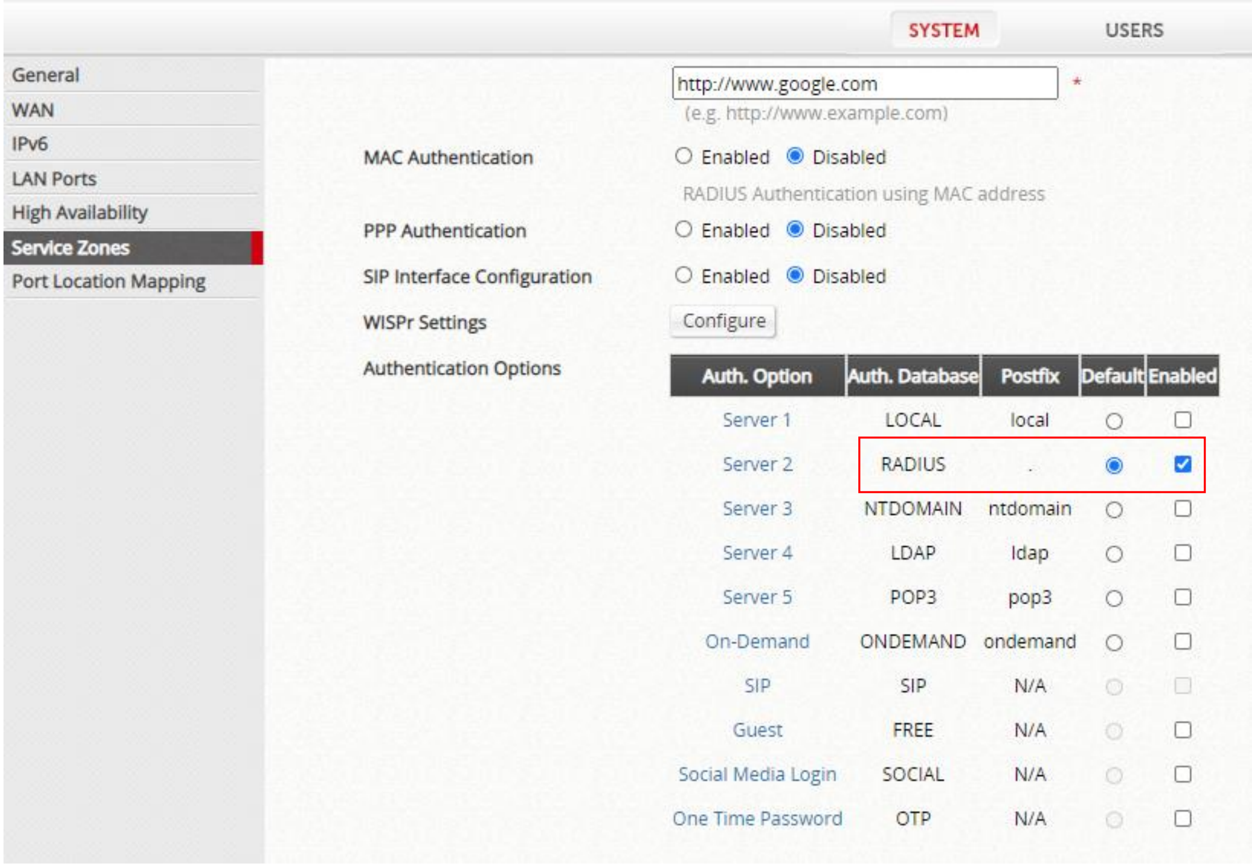
Authentication Option - Server 2

Server No. 2

Name	Server 2 *
User Postfix	. *
Remark	
Blacklist	None
Authentication	RADIUS

4. Configuring the desired Service Zone and RADIUS 802.1x authentication

Step 1. Go to SYSTEM→Service Zones→Authentication Options
Enable RADIUS.



http://www.google.com *
(e.g. http://www.example.com)

MAC Authentication ○ Enabled ● Disabled
RADIUS Authentication using MAC address

PPP Authentication ○ Enabled ● Disabled

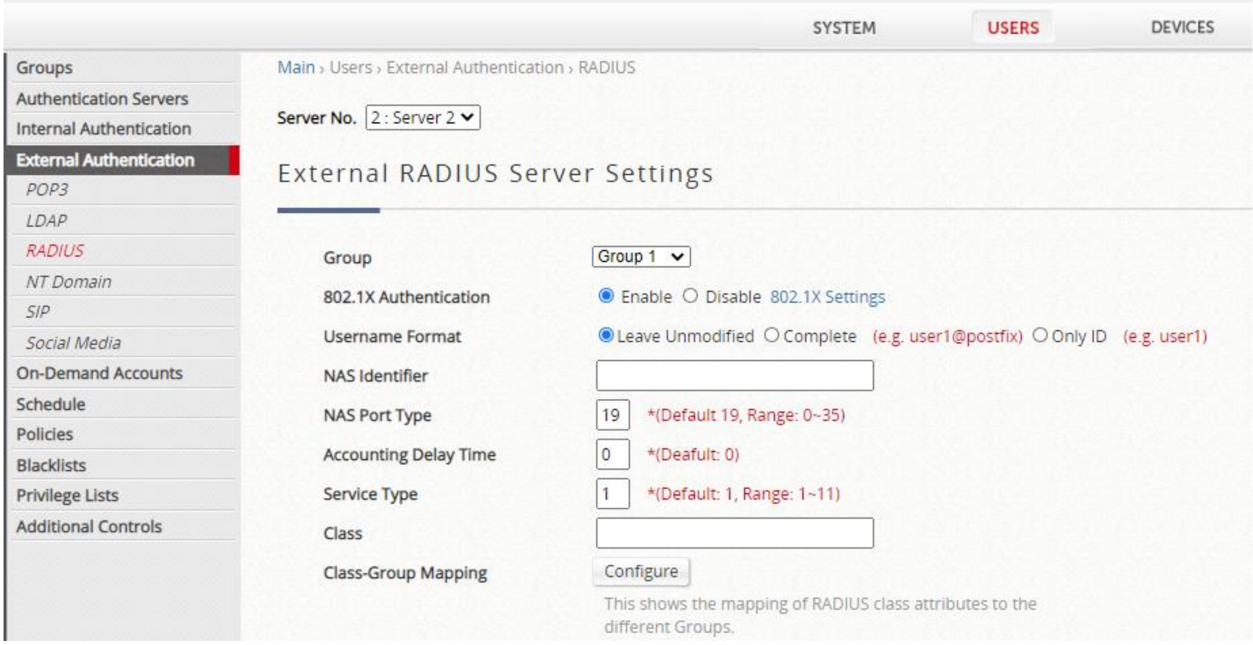
SIP Interface Configuration ○ Enabled ● Disabled

WISPr Settings

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	○	□
Server 2	RADIUS	.	●	☑
Server 3	NTDOMAIN	ntdomain	○	□
Server 4	LDAP	ldap	○	□
Server 5	POP3	pop3	○	□
On-Demand	ONDEMAND	ondemand	○	□
SIP	SIP	N/A	○	□
Guest	FREE	N/A	○	□
Social Media Login	SOCIAL	N/A	○	□
One Time Password	OTP	N/A	○	□

Step 2. Go the USERS→External Authentication
Enable 802.1x Authentication, then select “802.1X Settings.”



Main › Users › External Authentication › RADIUS

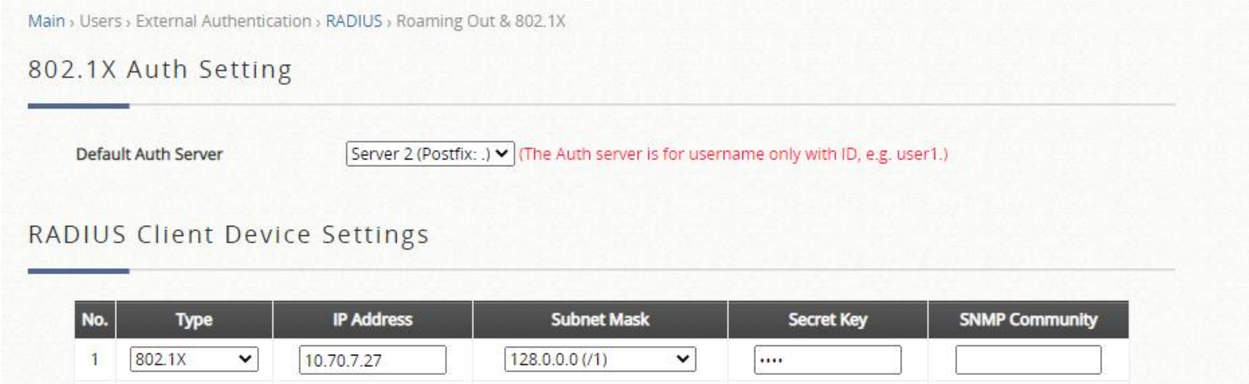
Server No. 2 : Server 2

External RADIUS Server Settings

Group	Group 1
802.1X Authentication	● Enable ○ Disable 802.1X Settings
Username Format	● Leave Unmodified ○ Complete (e.g. user1@postfix) ○ Only ID (e.g. user1)
NAS Identifier	
NAS Port Type	19 *(Default 19, Range: 0~35)
Accounting Delay Time	0 *(Deafult: 0)
Service Type	1 *(Default: 1, Range: 1~11)
Class	
Class-Group Mapping	Configure This shows the mapping of RADIUS class attributes to the different Groups.

Step 3. 802.1X Settings

- In the 802.1X Auth Setting, select Default Auth Server as “Server 2 (Postfix:.)”.
- In the 802.1x Auth Setting, write the public IP of the AP to the list.
  Note: Secret Key is RVHS. It is the secret key between the Controller and the complete-tunneled AP, regardless of the authentication RADIUS server.
- →Apply



Main › Users › External Authentication › RADIUS › Roaming Out & 802.1X

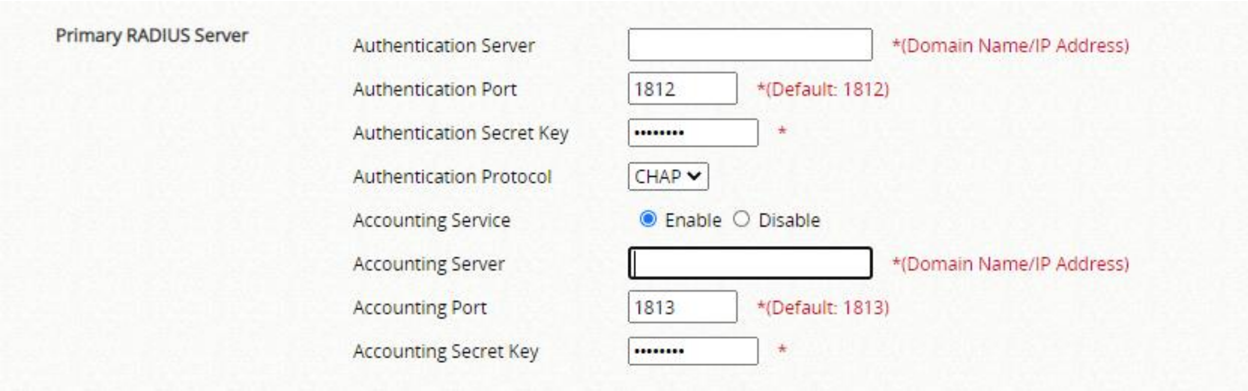
802.1X Auth Setting

Default Auth Server: Server 2 (Postfix: .) (The Auth server is for username only with ID, e.g. user1.)

RADIUS Client Device Settings

No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	802.1X	10.70.7.27	128.0.0.0 (/1)	••••	

Step 4. Back to the USERs→External Authentication→RADIUS
Edit your own Primary RADIUS Server information.



Primary RADIUS Server

Authentication Server: *(Domain Name/IP Address)

Authentication Port: 1812 *(Default: 1812)

Authentication Secret Key: •••••••• *

Authentication Protocol: CHAP

Accounting Service: ● Enable ○ Disable

Accounting Server: *(Domain Name/IP Address)

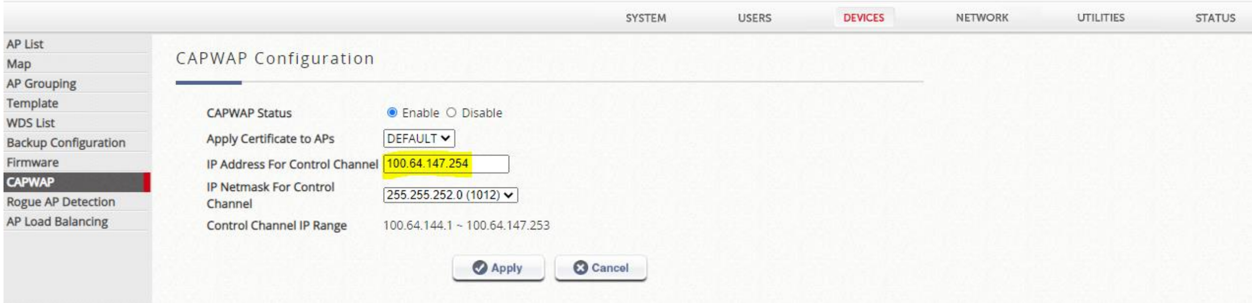
Accounting Port: 1813 *(Default: 1813)

Accounting Secret Key: •••••••• *

5. Apply Template to the complete-tunneled AP with 802.1x SSID

Now we have a complete-tunneled AP and the RADIUS 802.1x settings, we need to apply the 802.1x SSID to the AP.

Step 0. Go to Go to DEVICE→Wide Area AP Management→CAPWAP, and check your IP Address for Control Channel



CAPWAP Configuration

CAPWAP Status: ● Enable ○ Disable

Apply Certificate to APs: DEFAULT

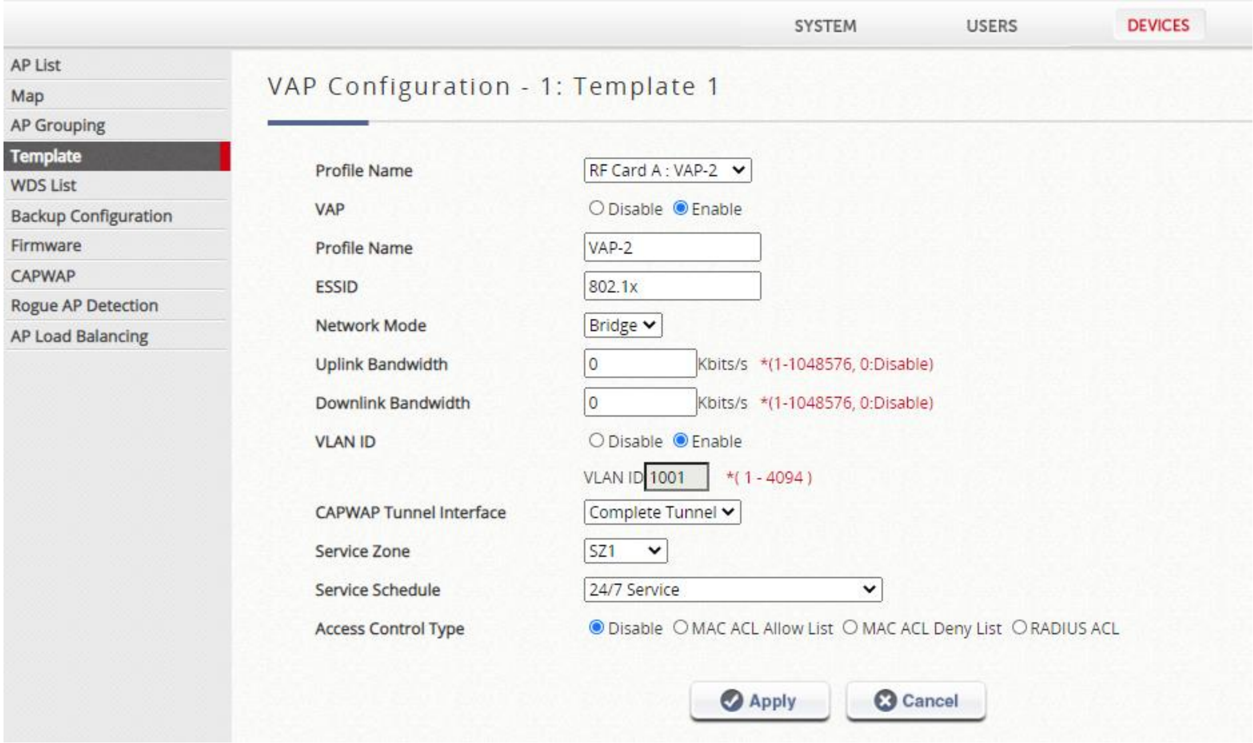
IP Address For Control Channel: 100.64.147.254

IP Netmask For Control Channel: 255.255.252.0 (1012)

Control Channel IP Range: 100.64.144.1 ~ 100.64.147.253

Step 1. Go to DEVICE→Wide Area AP Management→Template

Select a template and configure an SSID, for example, 802.1x, and be sure to set the CAPWAP Tunnel Interface=Complete Tunnel, with the corresponding Service Zone. Then Apply.

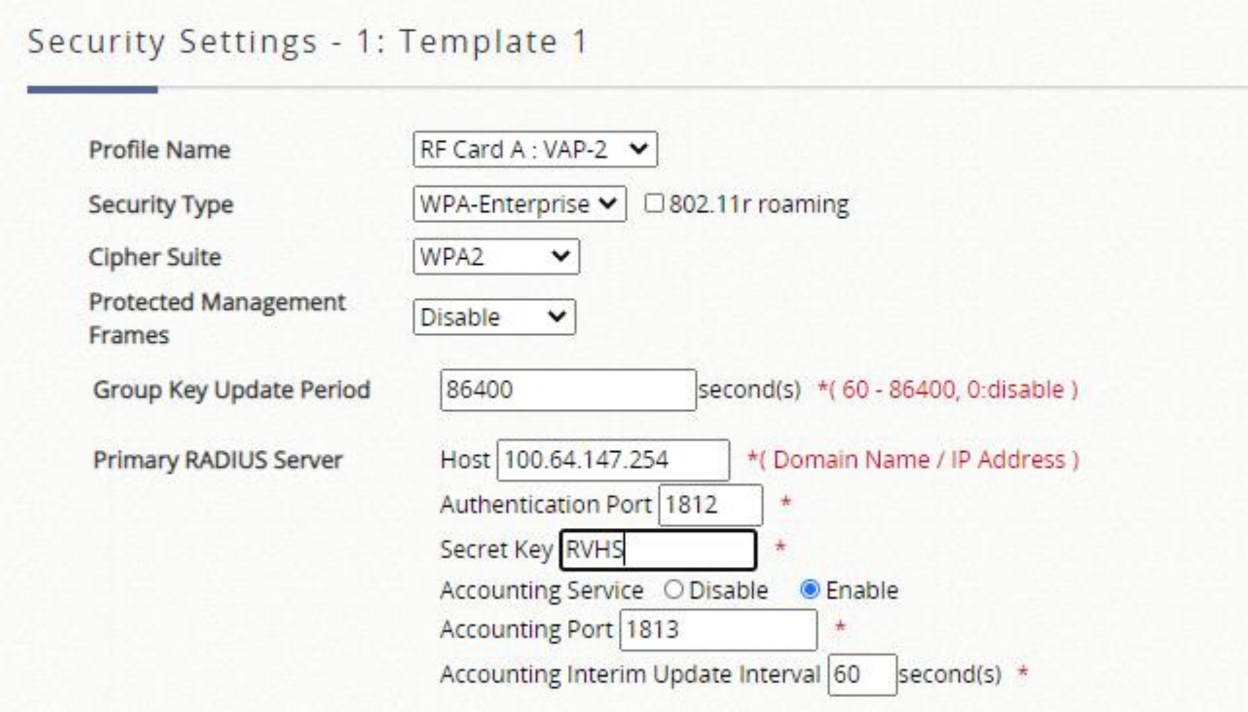


VAP Configuration - 1: Template 1

Profile Name	RF Card A : VAP-2
VAP	○ Disable ● Enable
Profile Name	VAP-2
ESSID	802.1x
Network Mode	Bridge
Uplink Bandwidth	0 Kbits/s *(1-1048576, 0:Disable)
Downlink Bandwidth	0 Kbits/s *(1-1048576, 0:Disable)
VLAN ID	○ Disable ● Enable VLAN ID 1001 *(1 - 4094)
CAPWAP Tunnel Interface	Complete Tunnel
Service Zone	SZ1
Service Schedule	24/7 Service
Access Control Type	● Disable ○ MAC ACL Allow List ○ MAC ACL Deny List ○ RADIUS ACL

Step 2. Back to the Template, continue to edit the Security Settings of that SSID.

- Security Type=WPA-Enterprise
- Cipher Suite=WPA2
- Protected Management Frames=Disable
- Group Key Update Period=86400
- Primary RADIUS Server
  Host= IP Address for Control Channel
  Authentication Port=1812
  Secret Key=RVHS

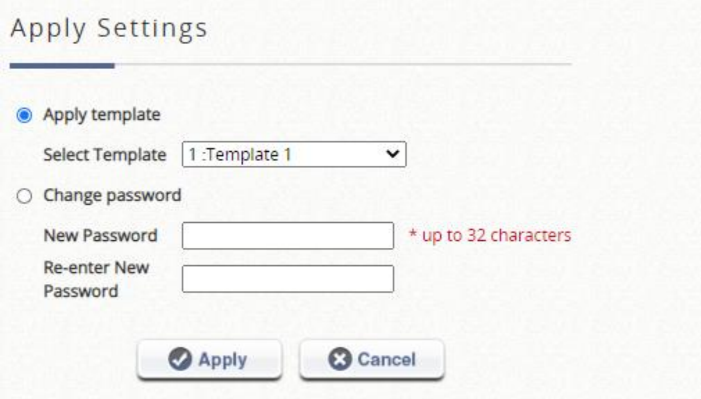


Security Settings - 1: Template 1

Profile Name	RF Card A : VAP-2
Security Type	WPA-Enterprise □ 802.11r roaming
Cipher Suite	WPA2
Protected Management Frames	Disable
Group Key Update Period	86400 second(s) *(60 - 86400, 0:disable)
Primary RADIUS Server	Host 100.64.147.254 *(Domain Name / IP Address)
	Authentication Port 1812 *
	Secret Key RVHS *
	Accounting Service ○ Disable ● Enable
	Accounting Port 1813 *
	Accounting Interim Update Interval 60 second(s) *

- Then Apply

Step 3. Go to DEVICES→Wide Area AP Management→Select the AP and apply the Template.



Apply Settings

● Apply template

Select Template 1 :Template 1

○ Change password

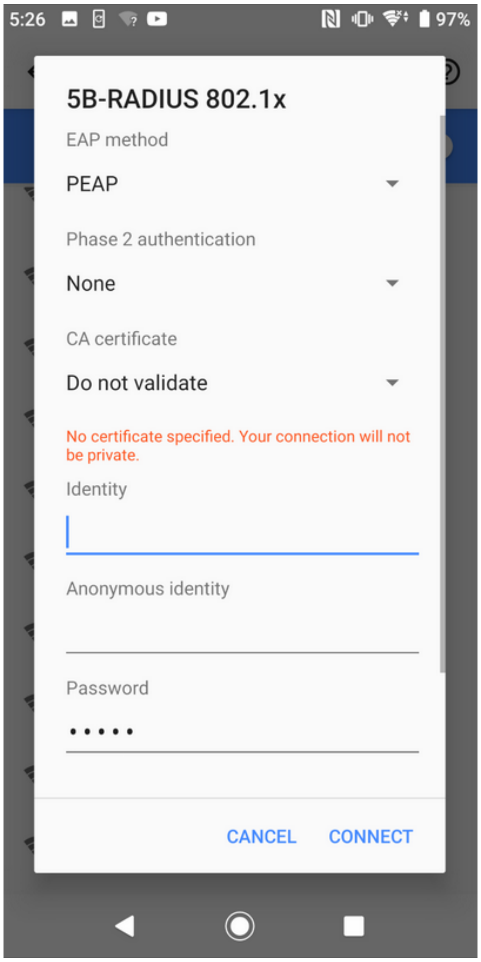
New Password * up to 32 characters

Re-enter New Password

6. Client Side Verification

Step 1. Connect to the 802.1x SSID, with the folloing settings.

- EAP method=PEAP
- CA certificate=Do not validate
- Enter Identify and Passwrod


5:26 97%

5B-RADIUS 802.1x

EAP method: PEAP

Phase 2 authentication: None

CA certificate: Do not validate

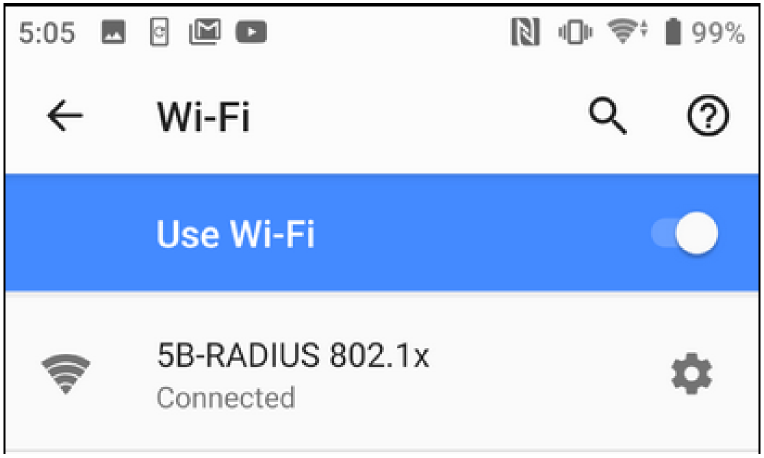
No certificate specified. Your connection will not be private.

Identity

Anonymous identity

Password: ••••••

Step 2. Connected.


5:05 99%

Wi-Fi

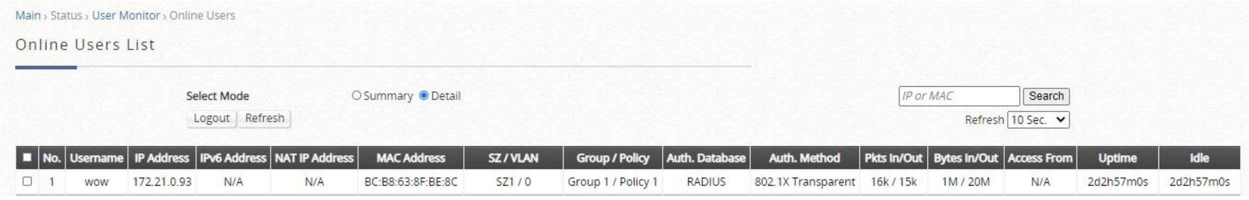
Use Wi-Fi

5B-RADIUS 802.1x

Connected

※Note: Verified with Android 9 & 10.

Step 3. Go to the Controller, and you could see the 802.1x user on the Monitor Users.



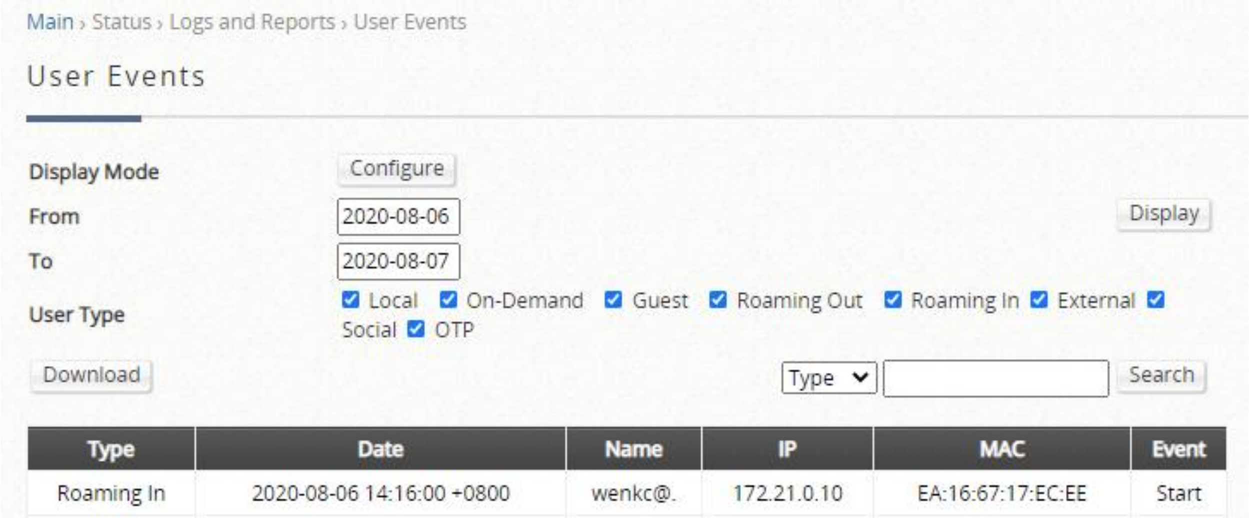
Main › Status › User Monitor › Online Users

Online Users List

Select Mode ○ Summary ● Detail

■	No.	Username	IP Address	IPv6 Address	NAT IP Address	MAC Address	SZ / VLAN	Group / Policy	Auth. Database	Auth. Method	Pkts In/Out	Bytes In/Out	Access From	Uptime	Idle
□	1	wow	172.21.0.93	N/A	N/A	BC:B8:63:8F:BE:8C	SZ1 / 0	Group 1 / Policy 1	RADIUS	802.1X Transparent	16k / 15k	1M / 20M	N/A	2d2h57m0s	2d2h57m0s

Step 4. You could also get detailed information on the User Event Log.



Main › Status › Logs and Reports › User Events

User Events

Display Mode: Configure

From: 2020-08-06

To: 2020-08-07

User Type: ☑ Local ☑ On-Demand ☑ Guest ☑ Roaming Out ☑ Roaming In ☑ External ☑ Social ☑ OTP

Type	Date	Name	IP	MAC	Event
Roaming In	2020-08-06 14:16:00 +0800	wenkc@.	172.21.0.10	EA:16:67:17:EC:EE	Start

7. Conclusion

Now the configuration is ready, and you can test the SSID with 802.1x Transparent Authentication from a remote AP, via the Controller, to the RADIUS of the main office. The Complete Tunnel makes the remote network and the central office network as the same segment and allows the RADIUS account to authenticate from the remote location.
You can implement the deployment when there is NATs between main office and remote site.

8. Remarks