Technical Guide

EWS Controller as RADIUS Server

Released: 2018-06-14

Doc Rev No: R4

Copyright Notification

Edgecore Networks Corporation

Table of Contents

1. Introduction

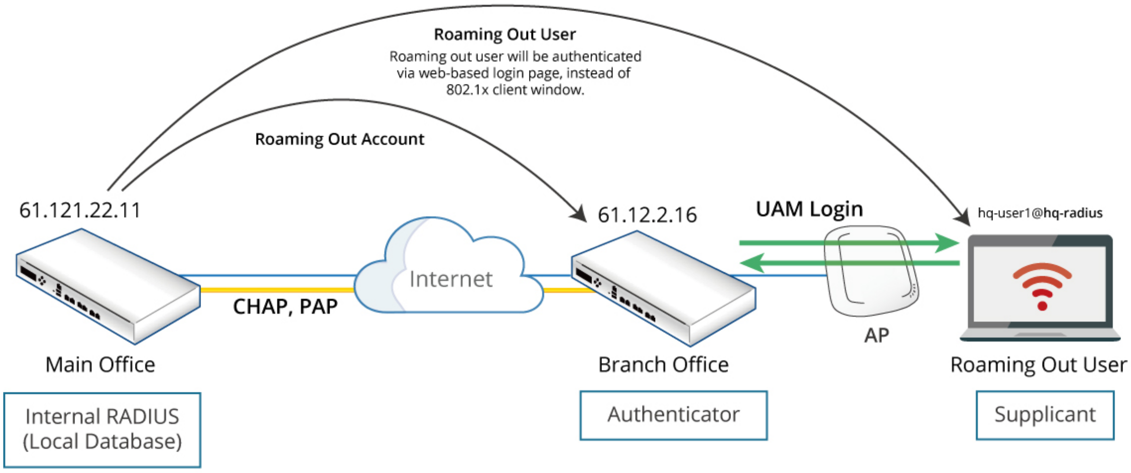
The article is aimed at explaining the setup of a powerful feature of the EWS Controller – its ability to act as a RADIUS server for different applications. In this article, two scenarios will be illustrated: **using the EWS Controller as an external RADIUS server (Local and/or On-Demand databases) for a remote gateway** and **using the EWS Controller as a RADIUS server in 802.1X authentication (transparent login).** Note that for the first scenario, the remote gateway can be a EWS Controller or a third-party controller, and multiple remote gateways can be setup. Detailed configuration are shown in the following chapters.

This technical guide provides the administrator with instructions on how to setup the scenarios above for different applications. Verification from the client side is also shown in the end of the document.

2. EWS Controller as External RADIUS Server for Remote Gateway

2.1 Network Architecture

The Local and On-Demand Databases of the EWS Controller act as an external RADIUS server for remote gateway to service “Roaming Out” users. Note that in this scenario, the EWS Controller to be used as the external RADIUS server is typically deployed on the WAN side of the remote gateway.

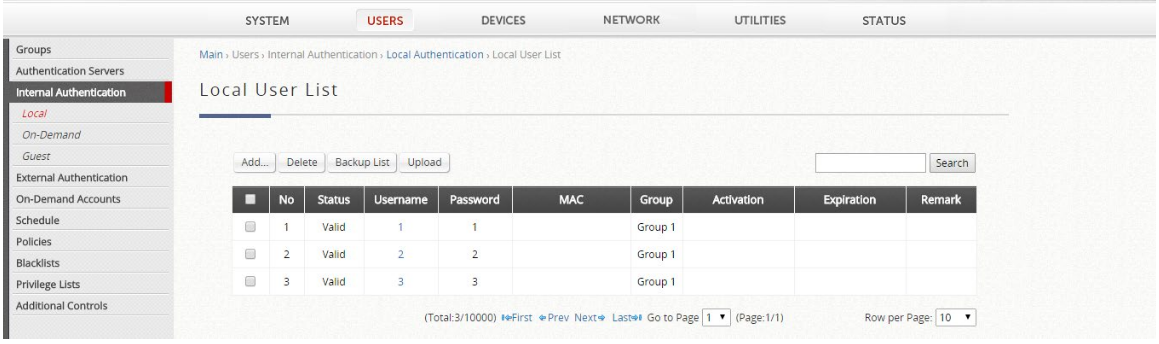


2.2 Device Preparation

- Main Office Gateway: EWS Controller
- Branch Office Gateway: EWS Controller
- Access Point: ECW/ECWO Access Point
- Supplicant: notebooks or moblie devices

2.3 Main Office Gateway Configuration

1. Create Local accounts in Local database



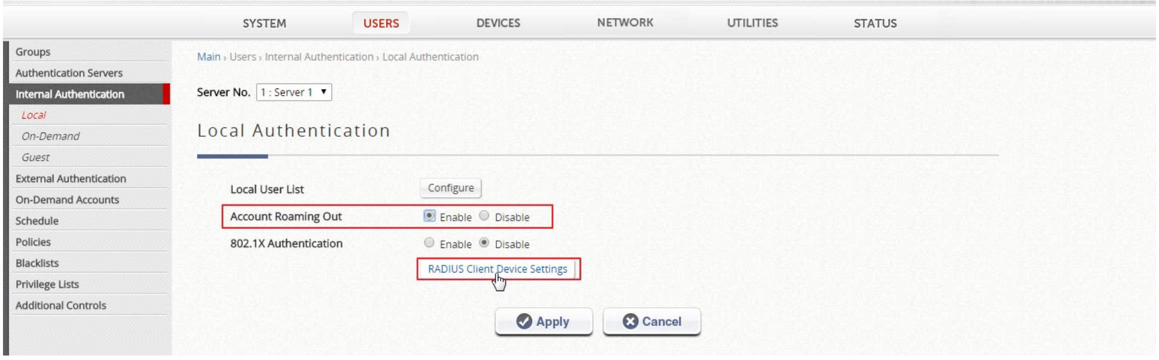
Main › Users › Internal Authentication › Local Authentication › Local User List

Local User List

□	No	Status	Username	Password	MAC	Group	Activation	Expiration	Remark
□	1	Valid	1	1		Group 1			
□	2	Valid	2	2		Group 1			
□	3	Valid	3	3		Group 1			

(Total:3/10000) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 10

2. Enable Account Roaming Out feature and click on RADIUS Client Device Settings button



Main › Users › Internal Authentication › Local Authentication

Server No. 1 : Server 1

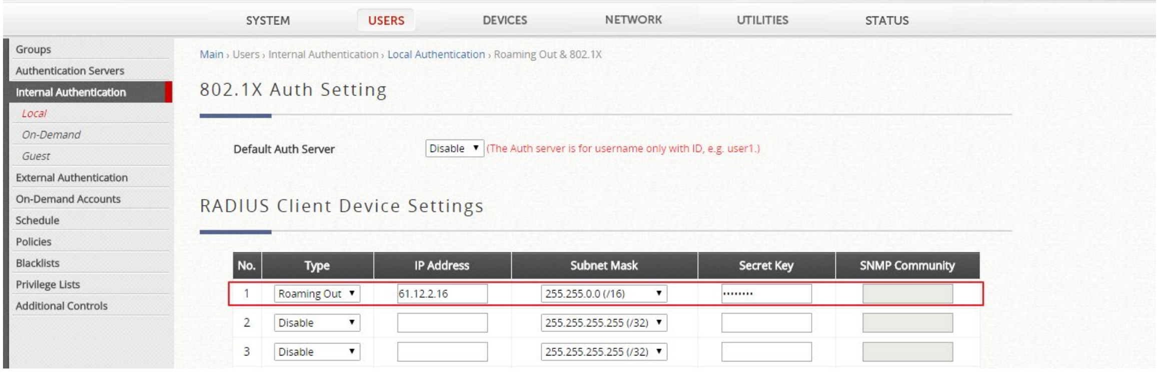
Local Authentication

Local User List

Account Roaming Out ● Enable ○ Disable

802.1X Authentication ○ Enable ● Disable

3. Select Type as Roaming out, type in the WAN IP address of the Remote Gateway, and select the appropriate subnet mask and type in a secret key. (e.g., 12345678)



Main › Users › Internal Authentication › Local Authentication › Roaming Out & 802.1X

802.1X Auth Setting

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

RADIUS Client Device Settings

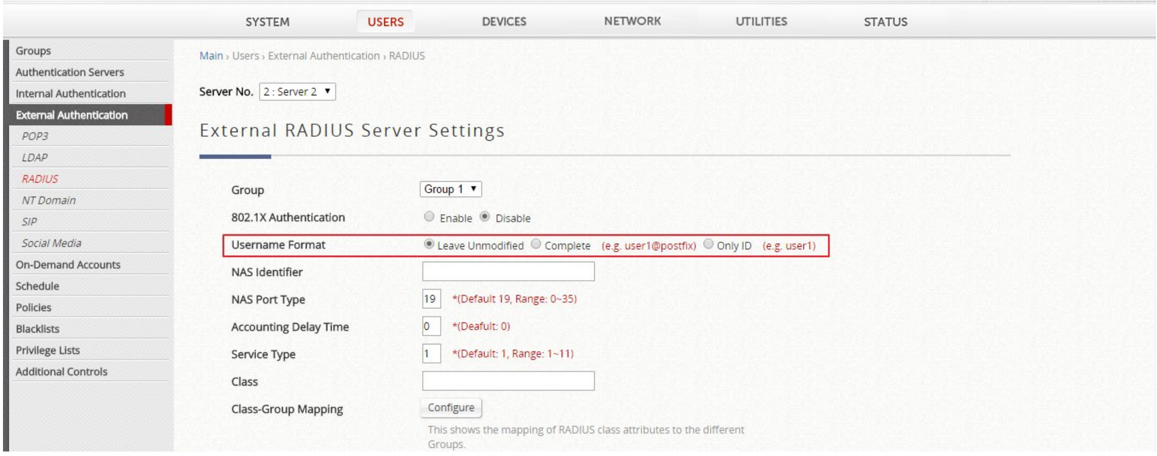
No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	Roaming Out	61.12.2.16	255.255.0.0 (/16)	••••••••	
2	Disable		255.255.255.255 (/32)		
3	Disable		255.255.255.255 (/32)		

2.4 Branch Office Gateway Configuration

1. It is recommended to select "Leave Unmodified" for Username Format

- Leave Unmodified: EWS will directly transfer what client types in Username

- Complete: both the username and postfix will be transferred to the RADIUS server for authentication
- Only ID: only the username will be transferred to the external RADIUS server for authentication



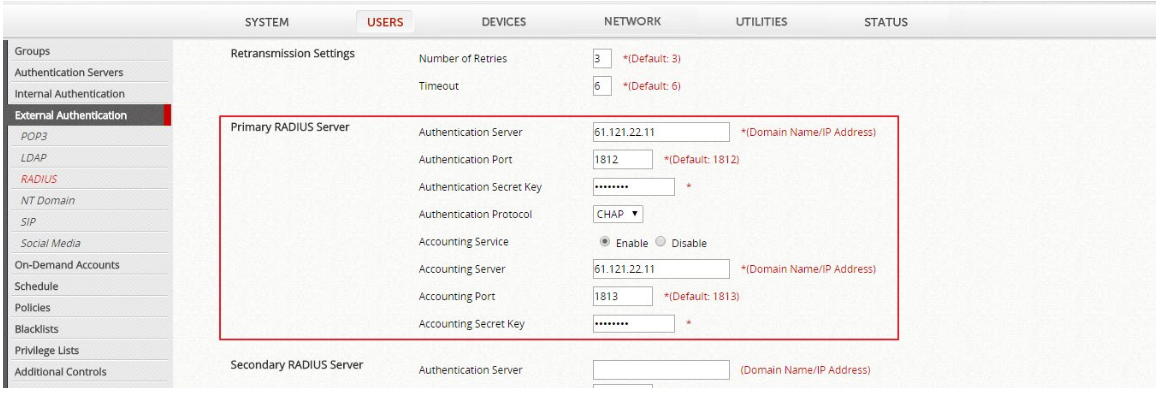
Server No. 2 : Server 2

External RADIUS Server Settings

Group	Group 1
802.1X Authentication	○ Enable ● Disable
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.

s

2. The Main Office Gateway acts as Primary RADIUS Server. The related configuration follows the network environment of main office gateway.



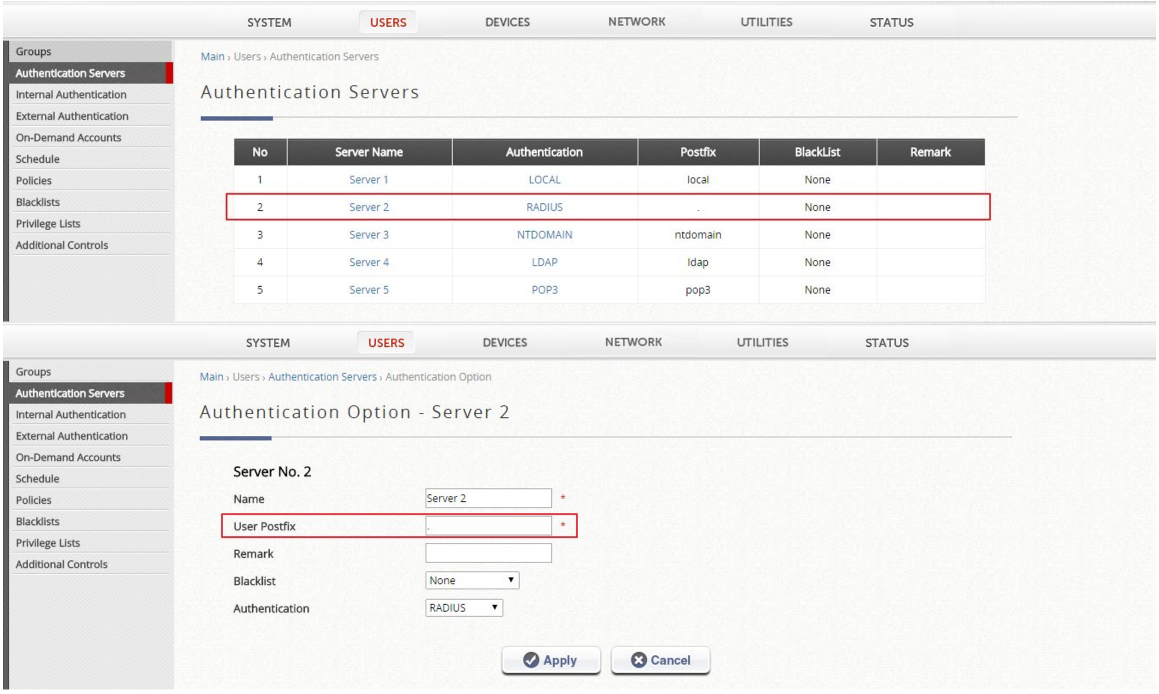
Retransmission Settings	Number of Retries	3 *(Default: 3)
	Timeout	6 *(Default: 6)
Primary RADIUS Server	Authentication Server	61.121.22.11 *(Domain Name/IP Address)
	Authentication Port	1812 *(Default: 1812)
	Authentication Secret Key	•••••••• *
	Authentication Protocol	CHAP
	Accounting Service	● Enable ○ Disable
	Accounting Server	61.121.22.11 *(Domain Name/IP Address)
	Accounting Port	1813 *(Default: 1813)
	Accounting Secret Key	•••••••• *
Secondary RADIUS Server	Authentication Server	(Domain Name/IP Address)

3. Administrators should confirm the postfix of RADIUS authentication method on the Authentication Servers page.

- **Note1**: Make sure that the Local/On-demand postfix at main gateway is not duplicated in any postfix on the remote gateway

Main Office Gateway		**Remote Office Gateway**	
Local	@domain.com	Local	local
Ondemand	od	Ondemand	ondemand
RADIUS	radius	RADIUS	.
NTDomain	ntdomain	NTDomain	ntdomain
LDAP	ldap	LDAP	ldap
POP3	pop3	POP3	pop3

- **Note2:** If both the Local and On-Demand databases are configured as roaming out server, please set the Postfix in the remote controller as "." (dot).



Main › Users › Authentication Servers

Authentication Servers

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

Main › Users › Authentication Servers › Authentication Option

Authentication Option - Server 2

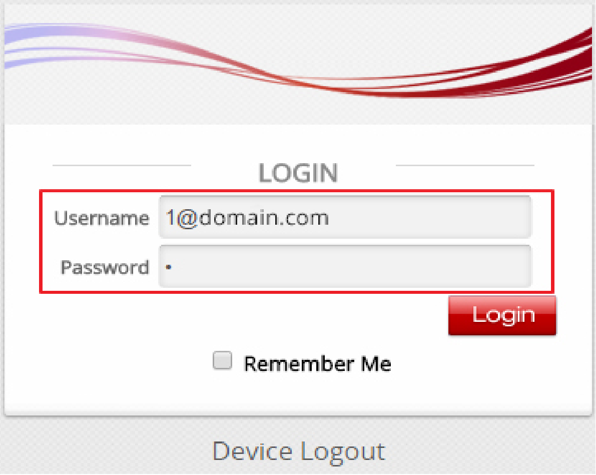
Server No. 2

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

4. For instructions on other configuration on the EWS Controller, such as Service Zone, AP Management, and Customized Login Page, please refer to the EWS User Manual.

2.5 Client Side Verification

After a client connects to the SSID with RADIUS authentication service, a web-based login page will pop up. For verification, the client enters “1@domain.com/1” as his or her username and password for external RADIUS authentication. Since “1@domain.com/1” is the credential stored in the main office gateway’s Local database, the client is authenticated successfully.


LOGIN

Username 1@domain.com

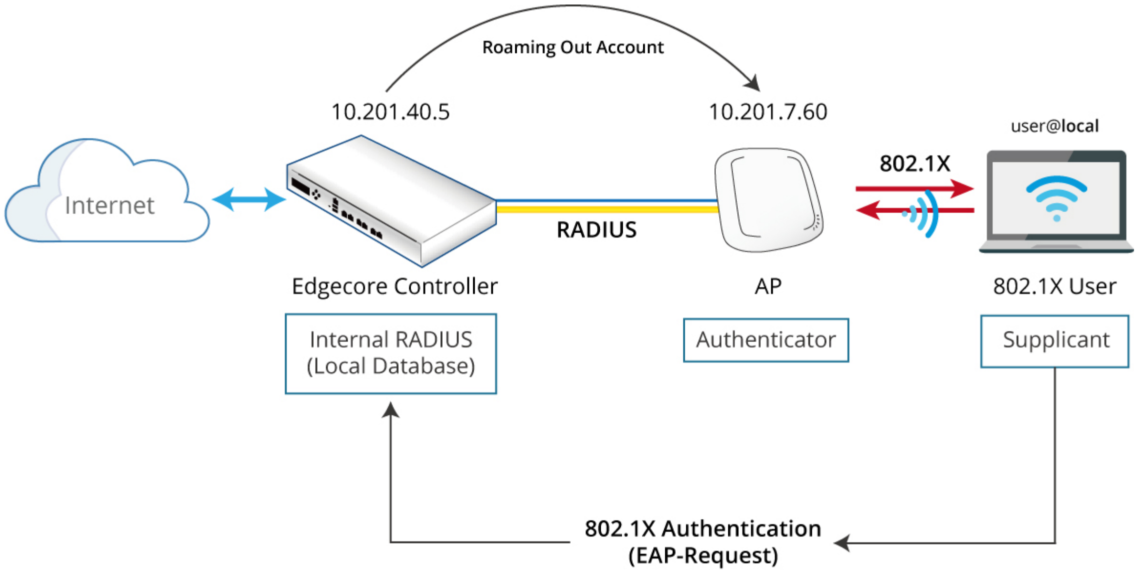
Password •

3. EWS Controller as RADIUS Server in 802.1X Authentication (Transparent Login)

3.1 Network Architecture

In this scenario, a client associates to the Wi-Fi network provided by the Access Point and logs in using a local account and 802.1X authentication. As can be seen from the diagram, the Access Point acts as the authenticator for the supplicant, which is the client, and the EWS Controller acts as the authentication server.

Note that the Access Point is deployed on the LAN side of the EWS Controller, and the supplicant associated to the Access Point is also on the LAN side. In this case, the EWS Controller grants network access through itself to the supplicant after authentication. In other cases where the supplicant is on the WAN side of the EWS Controller, the EWS Controller simply “roams out” accounts for authentication but does not grant network access through itself after authentication. In these cases, please enable and configure for “Account Roaming Out” rather than “802.1X Authentication” even though the supplicant is using 802.1X authentication to be granted network access.

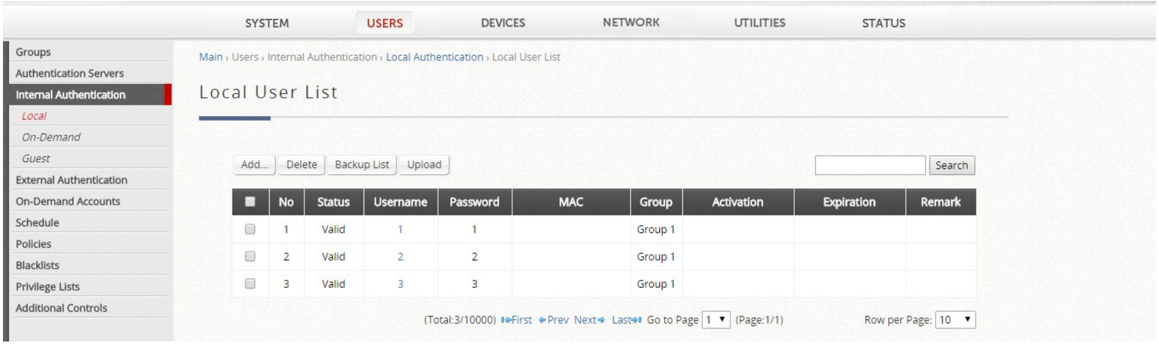


3.2 Device Preparation

- Gateway: EWS Controller to act as a RADIUS server in 802.1X authentication
- Access Point: ECW/ECWO Access Point to act as authenticator
- Supplicant: notebooks or moblie devices

3.3 Gateway Configuration

1. Create Local accounts in the Local database



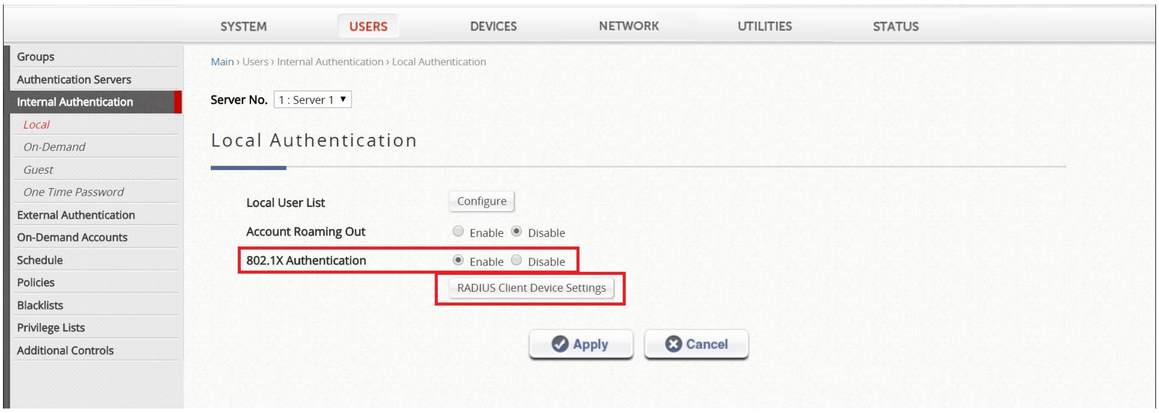
Main › Users › Internal Authentication › Local Authentication › Local User List

Local User List

□	No	Status	Username	Password	MAC	Group	Activation	Expiration	Remark
□	1	Valid	1	1		Group 1			
□	2	Valid	2	2		Group 1			
□	3	Valid	3	3		Group 1			

(Total:3/10000) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 10

2. Enable 802.1X Authentication, and click on RADIUS Client Device Settings button



Main › Users › Internal Authentication › Local Authentication

Server No. 1 : Server 1

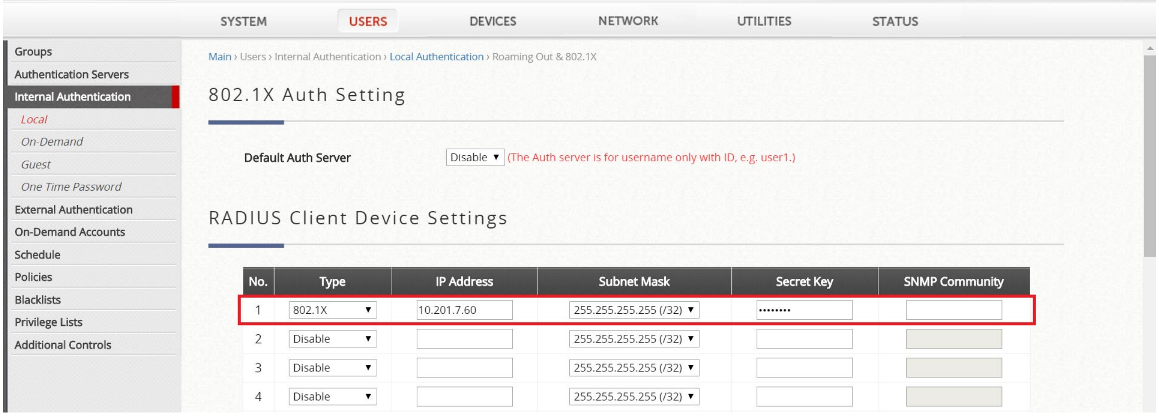
Local Authentication

Local User List Configure

Account Roaming Out ○ Enable ● Disable

802.1X Authentication ● Enable ○ Disable

3. Select "802.1X" under Type, enter the WAN IP address of the **Access Point** (Access point acts as a RADIUS authenticator), and select the appropriate subnet mask and enter a secret key. (e.g., 12345678)



Main › Users › Internal Authentication › Local Authentication › Roaming Out & 802.1X

802.1X Auth Setting

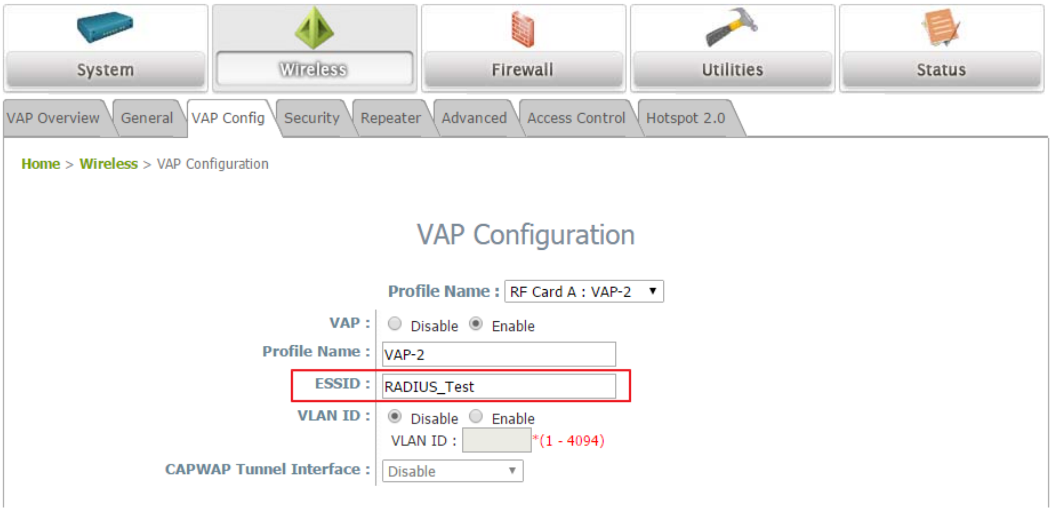
Default Auth Server Disable (The Auth server is for username only with ID, e.g. user1.)

RADIUS Client Device Settings

No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	802.1X	10.201.7.60	255.255.255.255 (/32)	••••••••	
2	Disable		255.255.255.255 (/32)		
3	Disable		255.255.255.255 (/32)		
4	Disable		255.255.255.255 (/32)		

3.4 AP Configuration

1. Enable a VAP and give it an appropriate SSID, e.g., RADIUS_Test



Home > Wireless > VAP Configuration

VAP Configuration

Profile Name : RF Card A : VAP-2

VAP : ○ Disable ● Enable

Profile Name : VAP-2

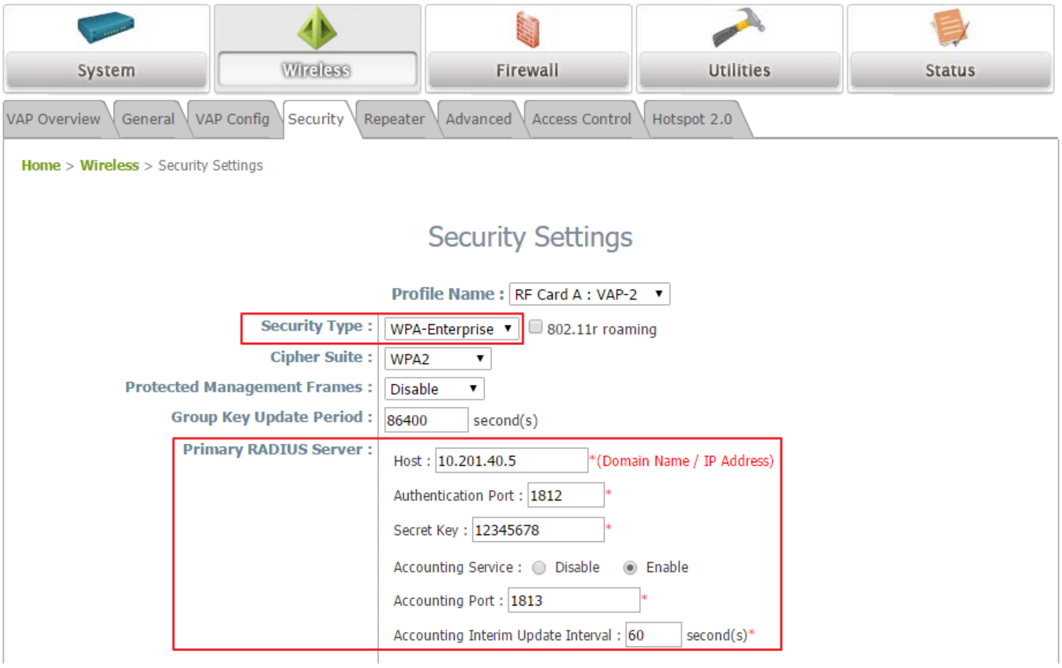
ESSID : RADIUS_Test

VLAN ID : ● Disable ○ Enable

VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface : Disable

2. Go to Security Settings within the same VAP and select **WPA-Enterprise** as the security type, which supports 802.1x RADIUS authentication. Then, administrators type in the Gateway’s IP address as primary RADIUS Server. In this case, enabling accounting service is not mandatory.



Home > Wireless > Security Settings

Security Settings

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)

Primary RADIUS Server :

Host : 10.201.40.5 *(Domain Name / IP Address)

Authentication Port : 1812 *

Secret Key : 12345678 *

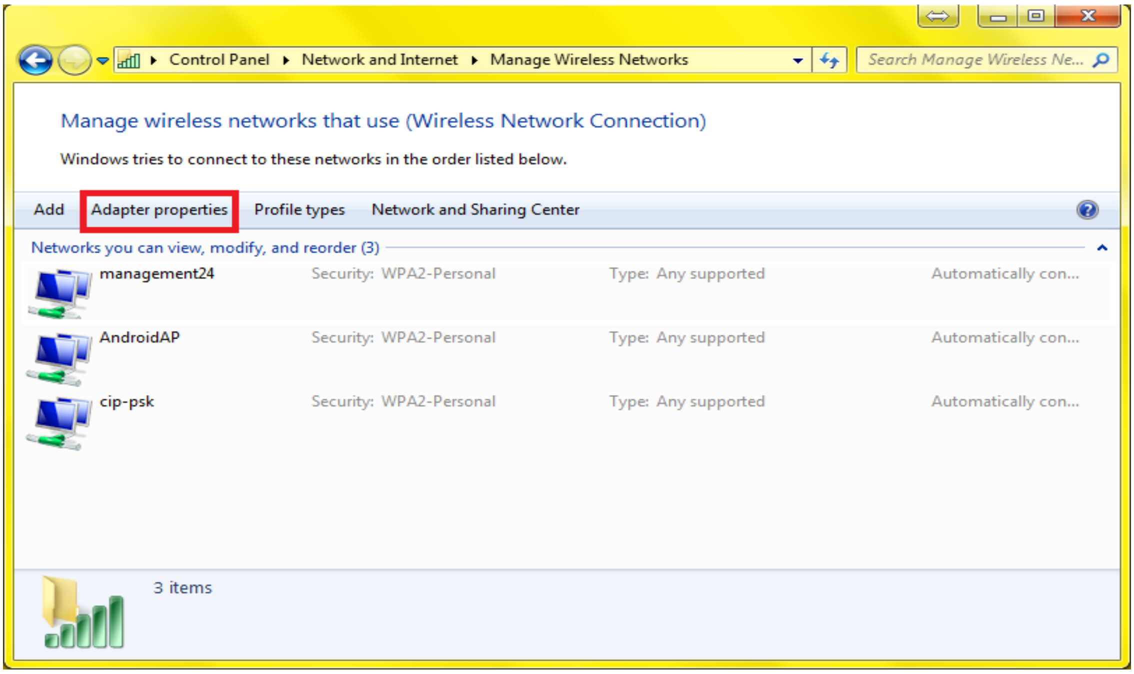
Accounting Service : ○ Disable ● Enable

Accounting Port : 1813 *

Accounting Interim Update Interval : 60 second(s)*

3.5 Client Side Verification

1. Add Adapter properties under “Manage Wireless Networks”



Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Ne...

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

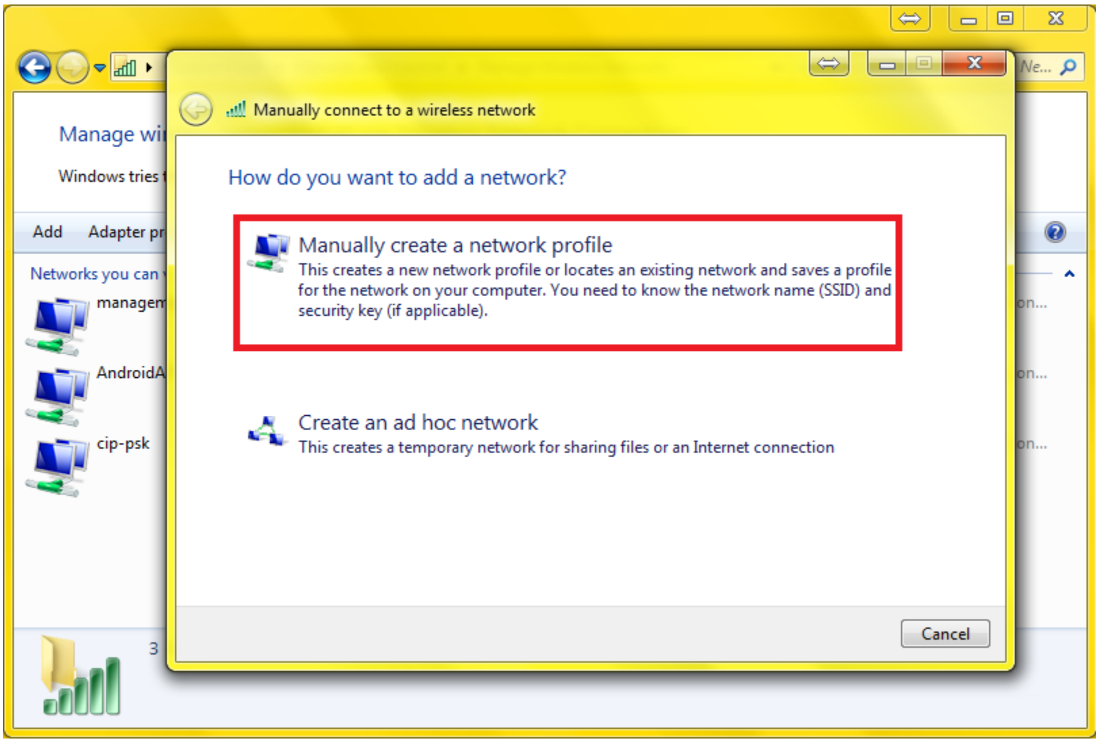
Add
Adapter properties
Profile types
Network and Sharing Center

Networks you can view, modify, and reorder (3)

management24	Security: WPA2-Personal	Type: Any supported	Automatically con...
AndroidAP	Security: WPA2-Personal	Type: Any supported	Automatically con...
cip-psk	Security: WPA2-Personal	Type: Any supported	Automatically con...

3 items

2. Select “Manually Create a Network Profile”

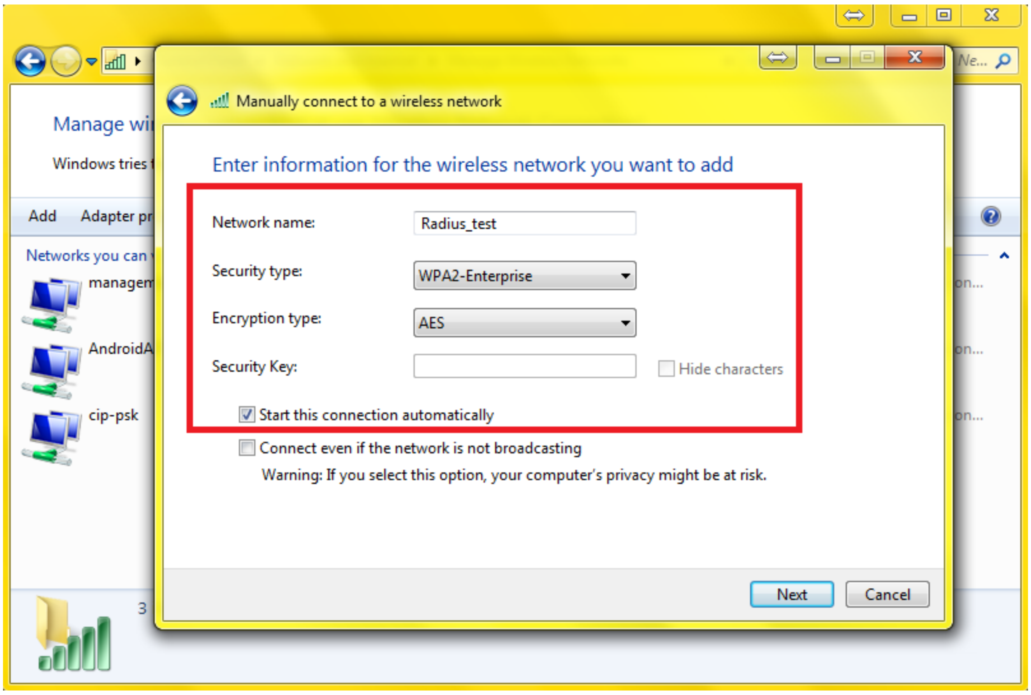


How do you want to add a network?

Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

3. Enter the information for the wireless network
    - Network name: RADIUS_Test
    - Security type: WPA2-Enterprise
    - Encryption type: AES
    - Checkmark Start this connection automatically



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: Radius_test

Security type: WPA2-Enterprise

Encryption type: AES

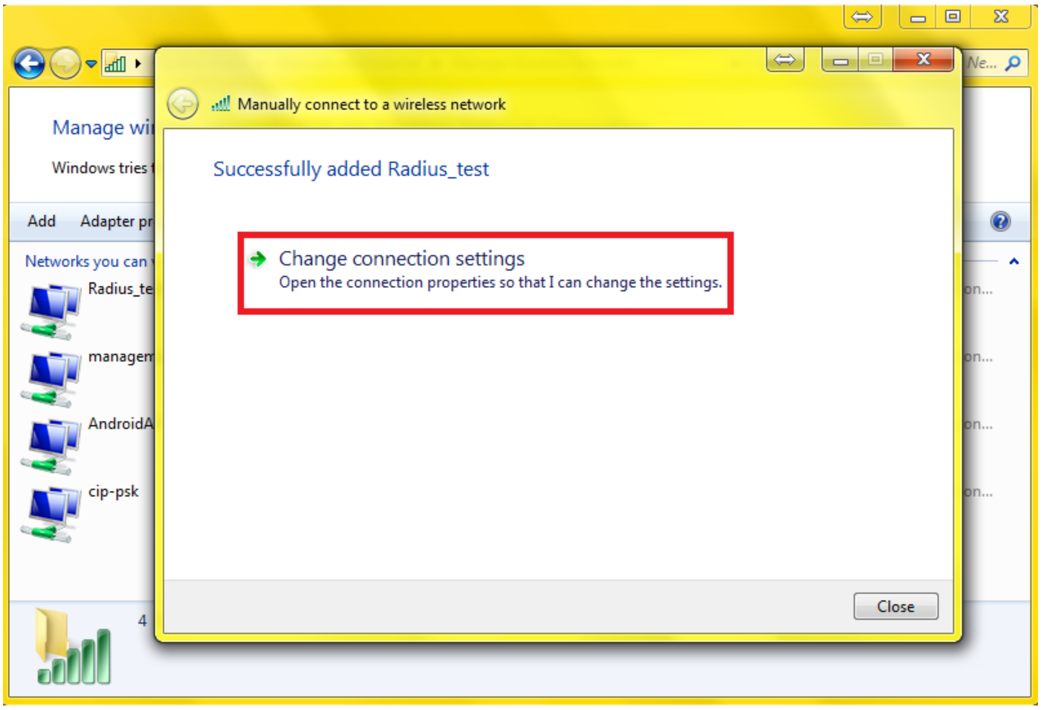
Security Key: ☐ Hide characters

☑ Start this connection automatically

☐ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

4. Select Change connection Settings



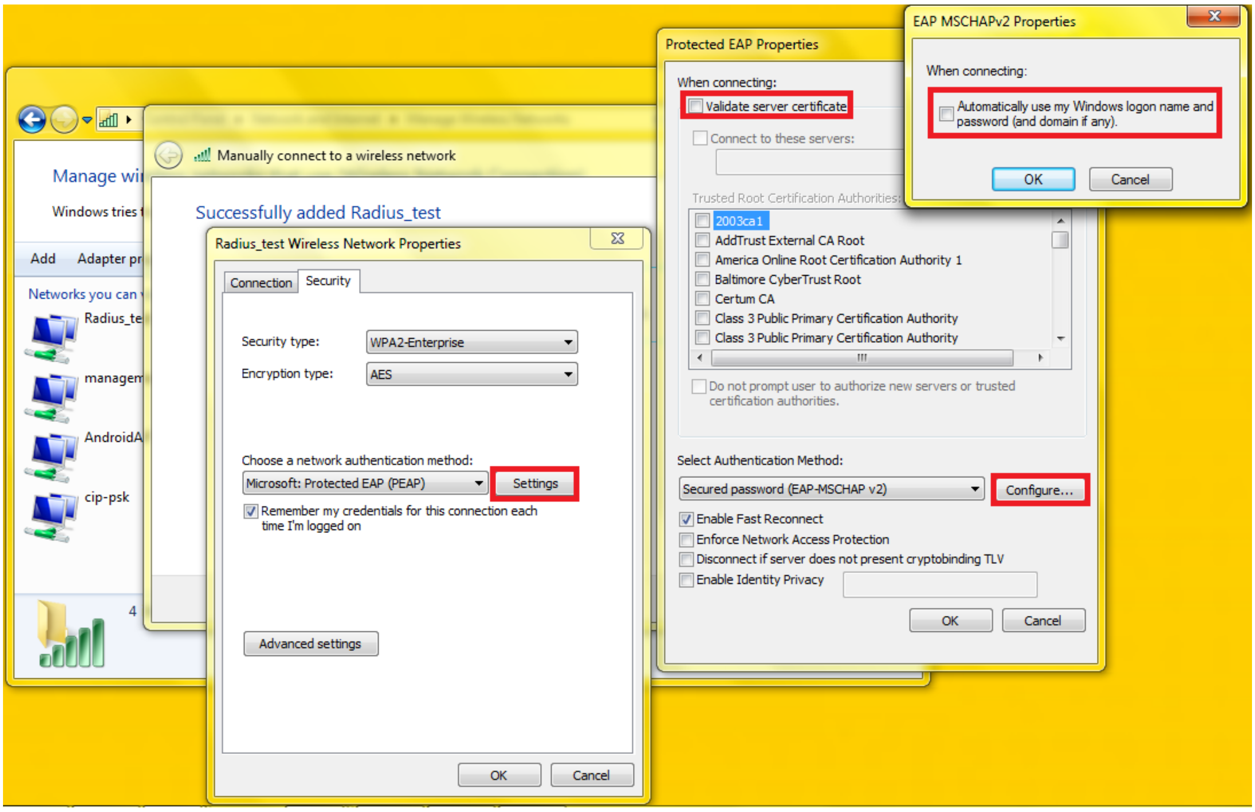
Manually connect to a wireless network

Successfully added Radius_test

Change connection settings
Open the connection properties so that I can change the settings.

5. Change the Security type to WPA2-Enterprise and Encryption type to AES while further selecting the Settings button of the network authentication method as Microsoft PEAP.

- Ensure to deselect the “Validate server certificate” and the “Automatically use my Windows logon name and password (and domain if any)”.
- When done, Click OK, OK, and OK again.



Manually connect to a wireless network

Successfully added Radius_test

Radius_test Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) | Settings

☑ Remember my credentials for this connection each time I'm logged on

Advanced settings

OK | Cancel

Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ 2003ca1
□ AddTrust External CA Root
□ America Online Root Certification Authority 1
□ Baltimore CyberTrust Root
□ Certum CA
□ Class 3 Public Primary Certification Authority
□ Class 3 Public Primary Certification Authority

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2) | Configure...

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

OK | Cancel

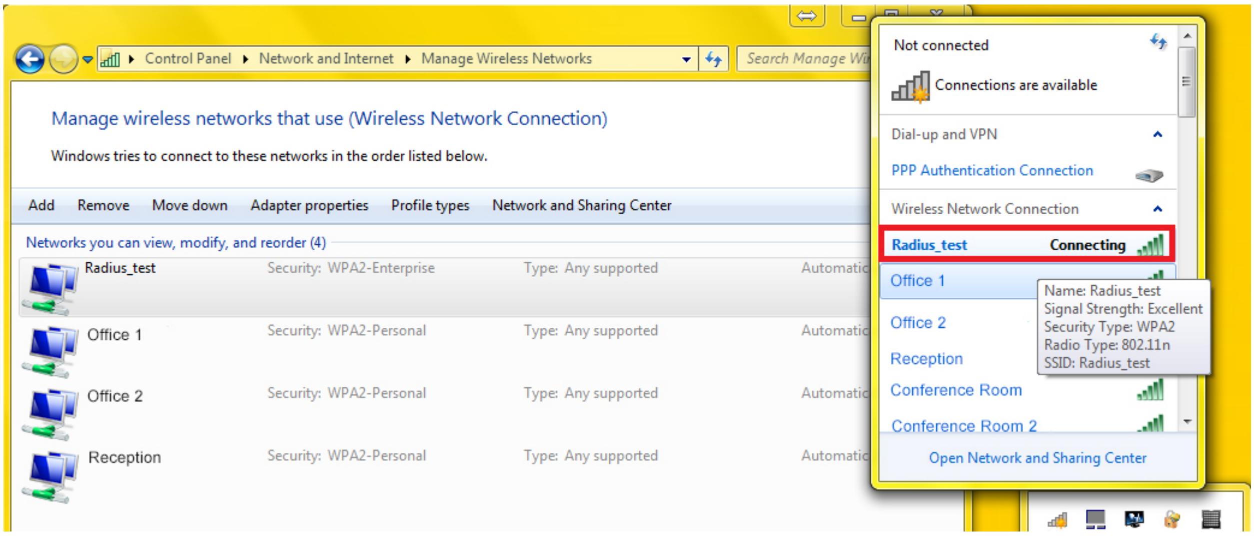
EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

OK | Cancel

6. Connect to the created SSID “RADIUS_Test”



Control Panel ▸ Network and Internet ▸ Manage Wireless Networks

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

Add | Remove | Move down | Adapter properties | Profile types | Network and Sharing Center

Networks you can view, modify, and reorder (4)

Radius_test	Security: WPA2-Enterprise	Type: Any supported	Automatic
Office 1	Security: WPA2-Personal	Type: Any supported	Automatic
Office 2	Security: WPA2-Personal	Type: Any supported	Automatic
Reception	Security: WPA2-Personal	Type: Any supported	Automatic

Not connected

Connections are available

Dial-up and VPN

PPP Authentication Connection

Wireless Network Connection

Radius_test Connecting

Office 1

Office 2

Reception

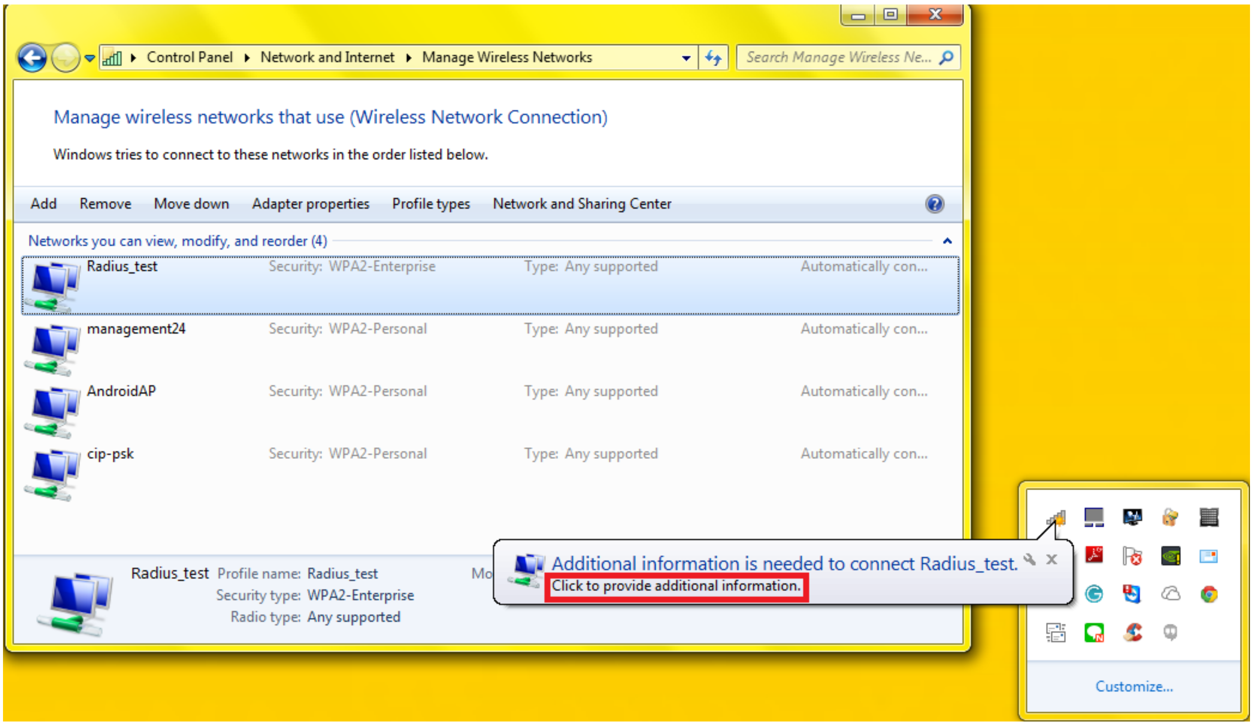
Conference Room

Conference Room 2

Open Network and Sharing Center

Name: Radius_test
Signal Strength: Excellent
Security Type: WPA2
Radio Type: 802.11n
SSID: Radius_test

7. Click on the message that says “Additional information is needed to connect RADIUS_Test”.


Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Ne...
Add
Remove
Move down
Adapter properties
Profile types
Network and Sharing Center
Customize...

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

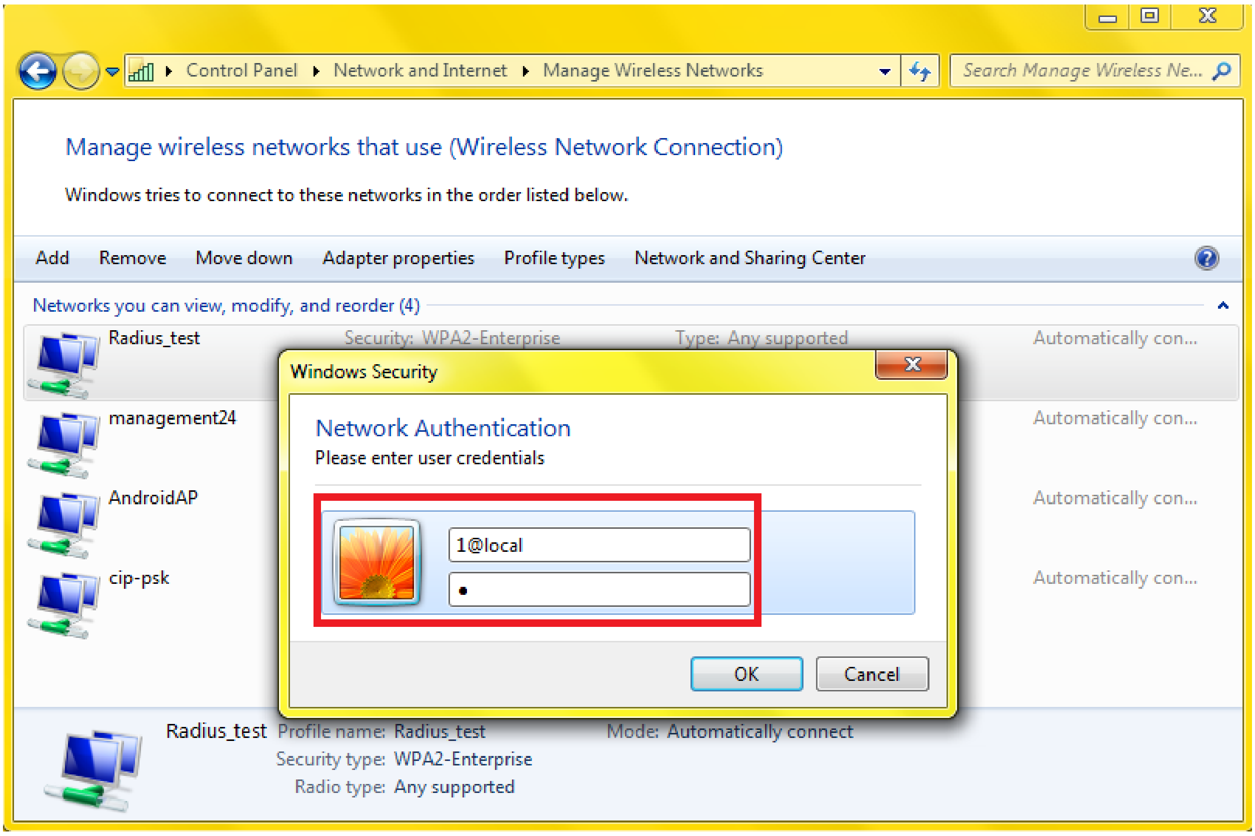
Networks you can view, modify, and reorder (4)

Radius_test	Security: WPA2-Enterprise	Type: Any supported	Automatically con...
management24	Security: WPA2-Personal	Type: Any supported	Automatically con...
AndroidAP	Security: WPA2-Personal	Type: Any supported	Automatically con...
cip-psk	Security: WPA2-Personal	Type: Any supported	Automatically con...

Radius_test Profile name: Radius_test
Security type: WPA2-Enterprise
Radio type: Any supported

Additional information is needed to connect Radius_test.
Click to provide additional information.

8. Enter the user credentials at the Network Authentication box with username “1@local” and password “1”.


Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Ne...
Add
Remove
Move down
Adapter properties
Profile types
Network and Sharing Center
OK
Cancel

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

Networks you can view, modify, and reorder (4)

Radius_test	Security: WPA2-Enterprise	Type: Any supported	Automatically con...
management24			Automatically con...
AndroidAP			Automatically con...
cip-psk			Automatically con...

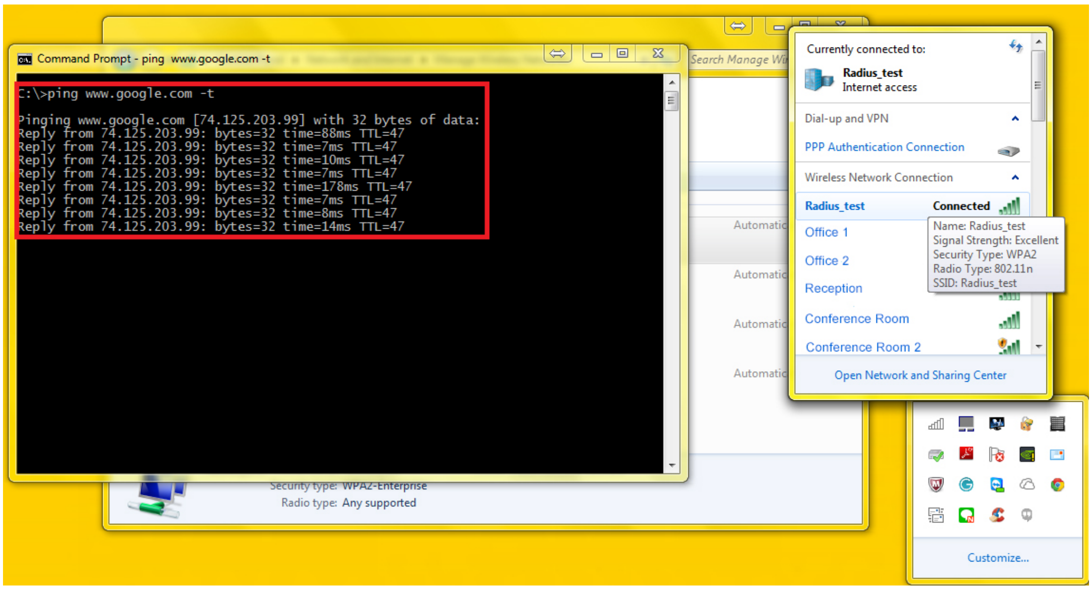
Windows Security

Network Authentication
Please enter user credentials

1@local
•

Radius_test Profile name: Radius_test Mode: Automatically connect
Security type: WPA2-Enterprise
Radio type: Any supported

9. Check that the connected SSID connection can reach outbound via the URL of www.google.com



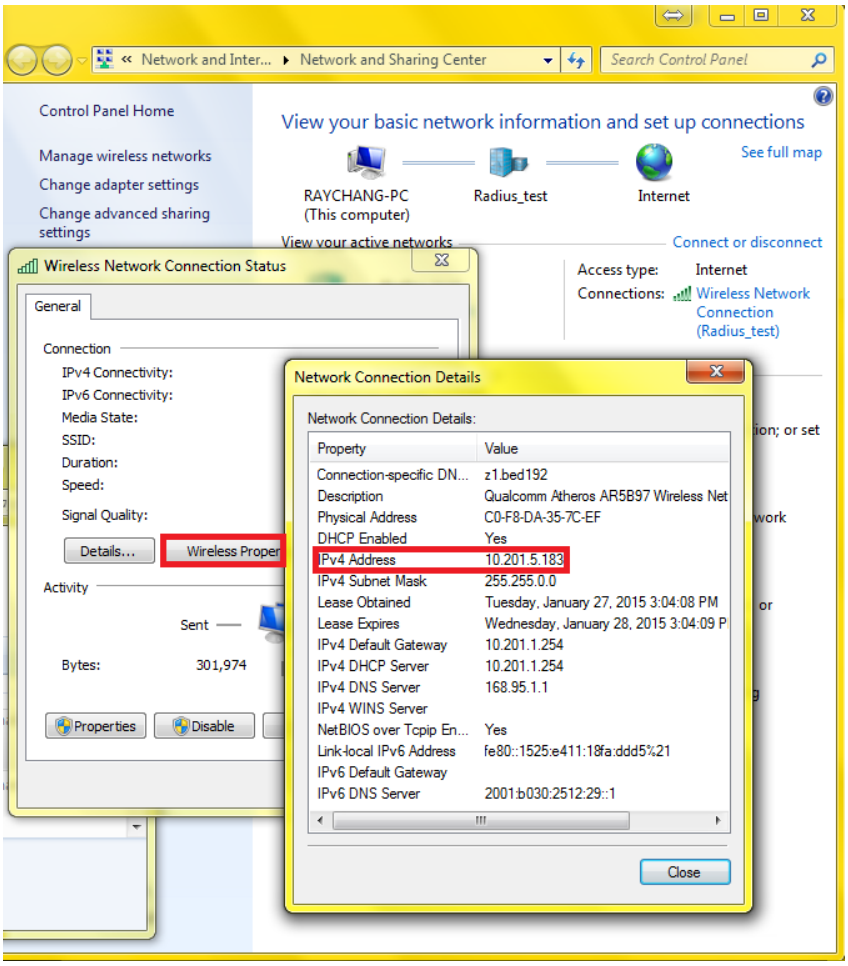
Command Prompt - ping www.google.com -t
Search Manage Wi
Currently connected to:
Radius_test
Internet access
Dial-up and VPN
PPP Authentication Connection
Wireless Network Connection
Radius_test Connected
Office 1
Office 2
Reception
Conference Room
Conference Room 2
Open Network and Sharing Center
Customize...
Automatic
Security type: WPA2-Enterprise
Radio type: Any supported

```
C:\>ping www.google.com -t

Pinging www.google.com [74.125.203.99] with 32 bytes of data:
Reply from 74.125.203.99: bytes=32 time=88ms TTL=47
Reply from 74.125.203.99: bytes=32 time=7ms TTL=47
Reply from 74.125.203.99: bytes=32 time=10ms TTL=47
Reply from 74.125.203.99: bytes=32 time=7ms TTL=47
Reply from 74.125.203.99: bytes=32 time=178ms TTL=47
Reply from 74.125.203.99: bytes=32 time=7ms TTL=47
Reply from 74.125.203.99: bytes=32 time=8ms TTL=47
Reply from 74.125.203.99: bytes=32 time=14ms TTL=47
```

Name: Radius_test
Signal Strength: Excellent
Security Type: WPA2
Radio Type: 802.11n
SSID: Radius_test

10. Also, check the received client IP address at its Wireless Connection Details.



Access type: Internet
Connections: Wireless Network Connection (Radius_test)

IPv4 Connectivity:
IPv6 Connectivity:
Media State:
SSID:
Duration:
Speed:
Signal Quality:
Bytes: 301,974

Network Connection Details:

Property	Value
Connection-specific DN...	z1.bed192
Description	Qualcomm Atheros AR5B97 Wireless Net
Physical Address	C0-F8-DA-35-7C-EF
DHCP Enabled	Yes
IPv4 Address	10.201.5.183
IPv4 Subnet Mask	255.255.0.0
Lease Obtained	Tuesday, January 27, 2015 3:04:08 PM
Lease Expires	Wednesday, January 28, 2015 3:04:09 P
IPv4 Default Gateway	10.201.1.254
IPv4 DHCP Server	10.201.1.254
IPv4 DNS Server	168.95.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::1525:e411:18fa:ddd5%21
IPv6 Default Gateway	
IPv6 DNS Server	2001:b030:2512:29::1

4. Conclusion

EWS Controller can be deployed as a RADIUS Server under two different scenarios, **Local/ On-Demand**

Databases for Remote Gateway and **using the EWS Controller as Internal RADIUS Server**. Set up configuration flow for both scenarios are demonstrated; RADIUS authentication with web-based login page and 802.1X authentication with AP as an authenticator. Upon successful client login, other EWS powerful features such as bandwidth control, logs and report for the user events, and other existing function all contribute to creating a robust and easily managed network.

5. Remarks

Please contact Technical Support Team for additional inquiries.