



Technical Guide

EWS Controller as RADIUS Server

Released: 2018-06-14

Doc Rev No: R4

Copyright Notification

Edgecore Networks Corporation

© Copyright 2018 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. Introduction 2**
- 2. EWS Controller as External RADIUS Server for Remote Gateway 3**
 - 2.1 Network Architecture 3
 - 2.2 Device Preparation 3
 - 2.3 Main Office Gateway Configuration 4
 - 2.4 Branch Office Gateway Configuration 4
 - 2.5 Client Side Verification..... 7
- 3. EWS Controller as RADIUS Server in 802.1X Authentication (Transparent Login) 8**
 - 3.1 Network Architecture 8
 - 3.2 Device Preparation 8
 - 3.3 Gateway Configuration 9
 - 3.4 AP Configuration 9
 - 3.5 Client Side Verification..... 10
- 4. Conclusion..... 15**
- 5. Remarks 16**

1. Introduction

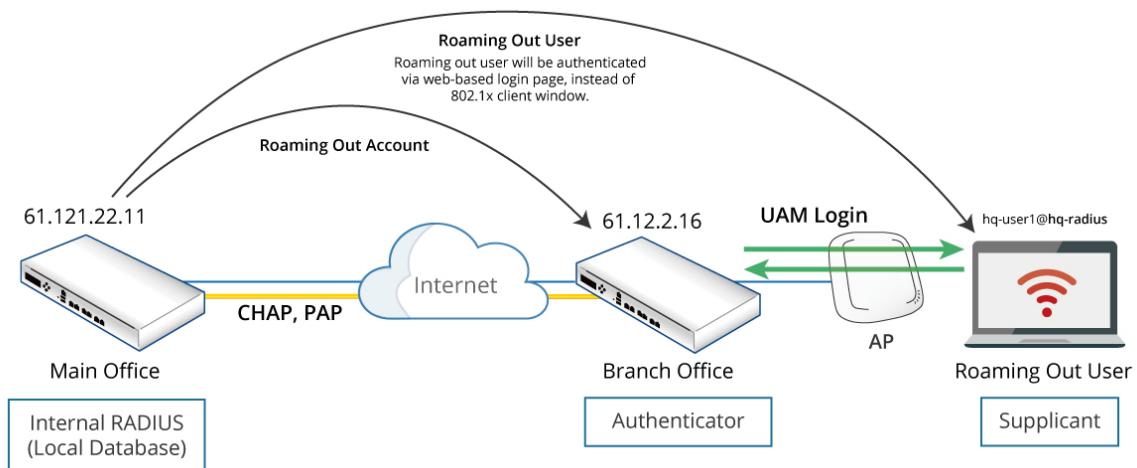
The article is aimed at explaining the setup of a powerful feature of the EWS Controller – its ability to act as a RADIUS server for different applications. In this article, two scenarios will be illustrated: **using the EWS Controller as an external RADIUS server (Local and/or On-Demand databases) for 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.

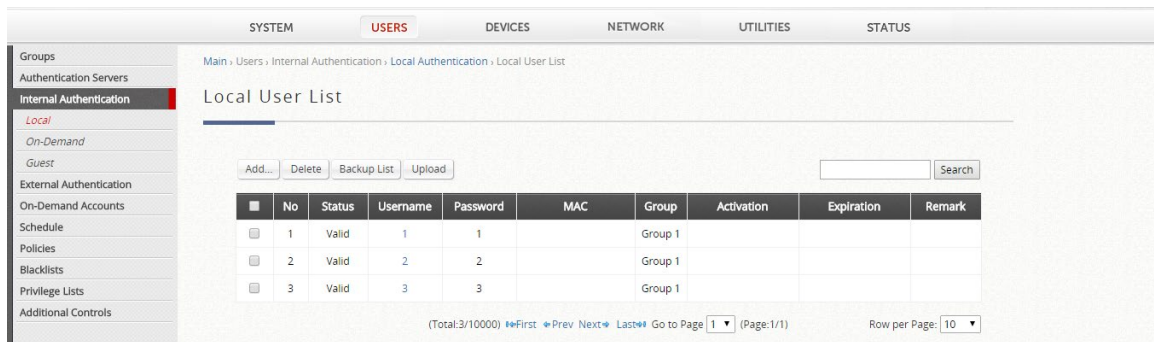


2.2 Device Preparation

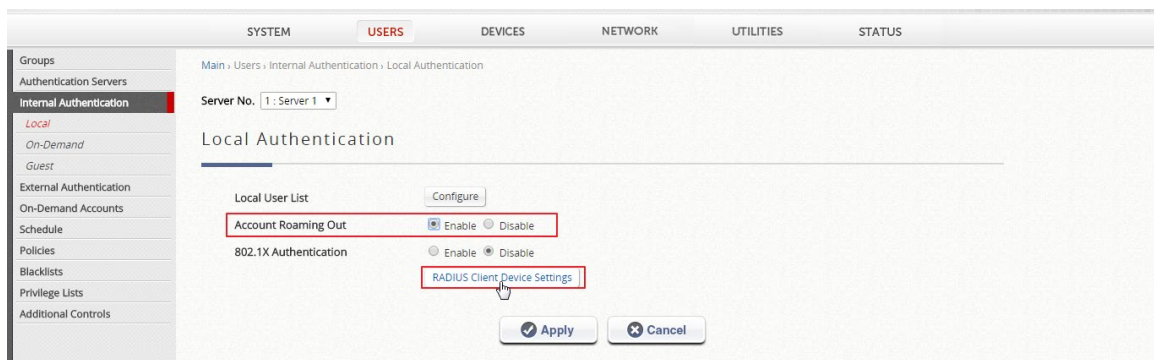
- Main Office Gateway: EWS Controller
- Branch Office Gateway: EWS Controller
- Access Point: ECW/ECWO Access Point
- Supplicant: notebooks or mobile devices

2.3 Main Office Gateway Configuration

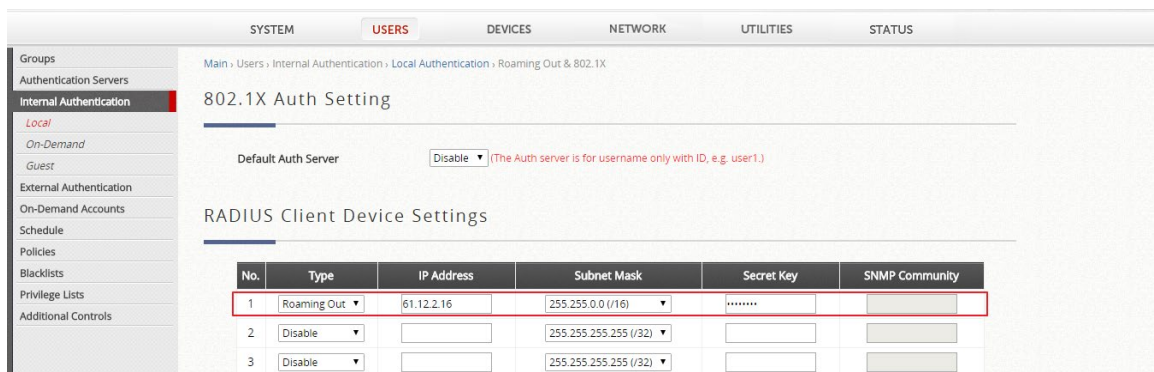
1. Create Local accounts in Local database



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



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)

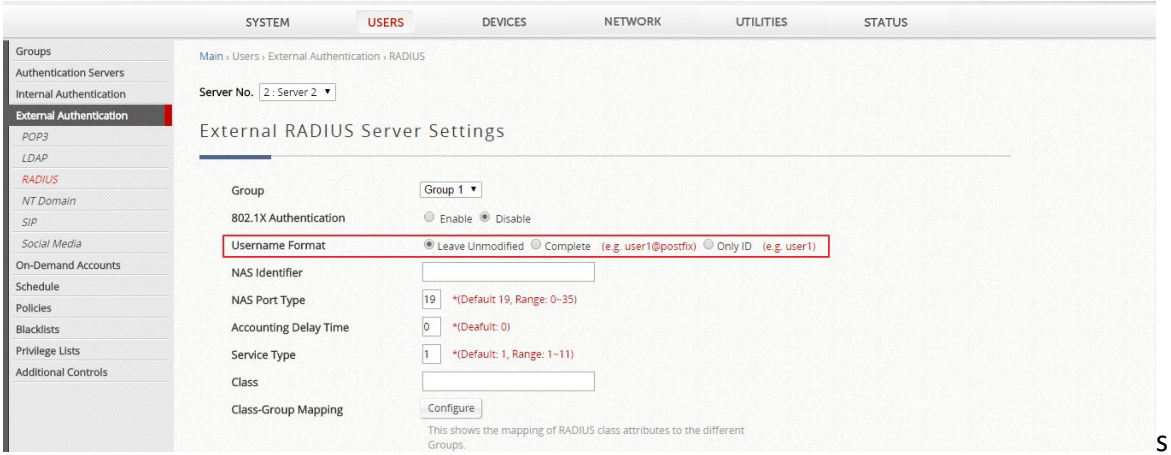


2.4 Branch Office Gateway Configuration

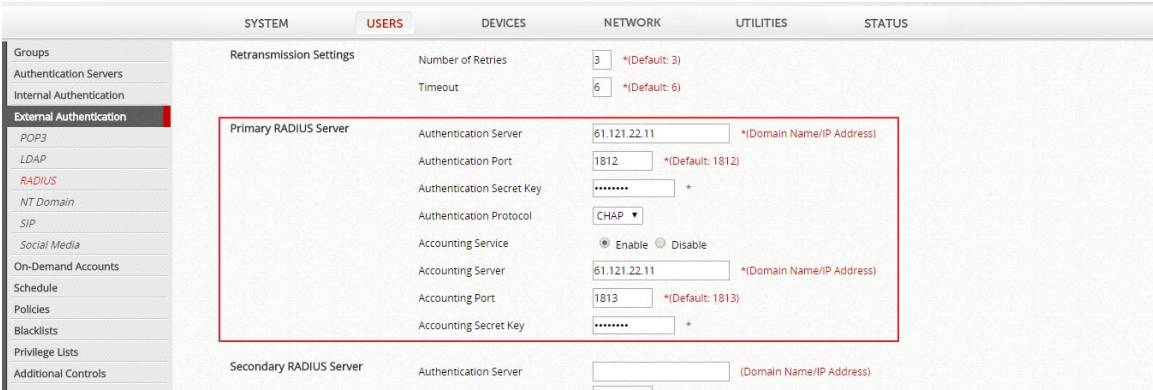
1. It is recommended to select "Leave Unmodified" for Username Format

- 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



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



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).

The screenshot shows the EWS Controller interface. The top navigation bar includes SYSTEM, USERS (selected), DEVICES, NETWORK, UTILITIES, and STATUS. The left sidebar lists various configuration options, with Authentication Servers selected. The main content area displays the 'Authentication Servers' table:

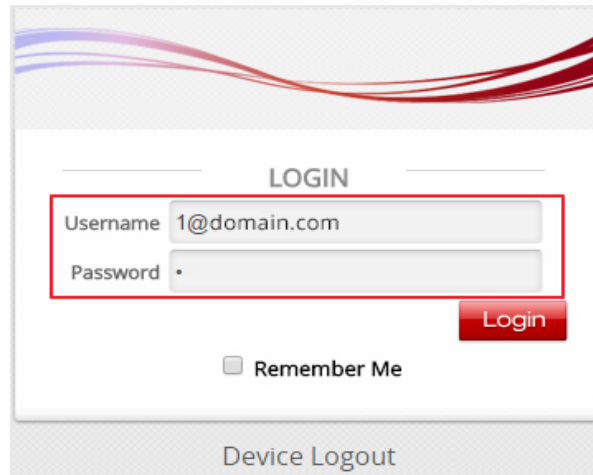
No	Server Name	Authentication	Postfix	BlackList	Remark
1	Server 1	LOCAL	local	None	
2	Server 2	RADIUS	.	None	
3	Server 3	NTDOMAIN	ntdomain	None	
4	Server 4	LDAP	ldap	None	
5	Server 5	POP3	pop3	None	

Below the table, the 'Authentication Option - Server 2' configuration form is shown. The 'User Postfix' field is highlighted with a red box and contains a dot (.). Other fields include Name (Server 2), Remark, Blacklist (None), and Authentication (RADIUS). Buttons for 'Apply' and 'Cancel' are at the bottom.

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 •

Remember Me

Login

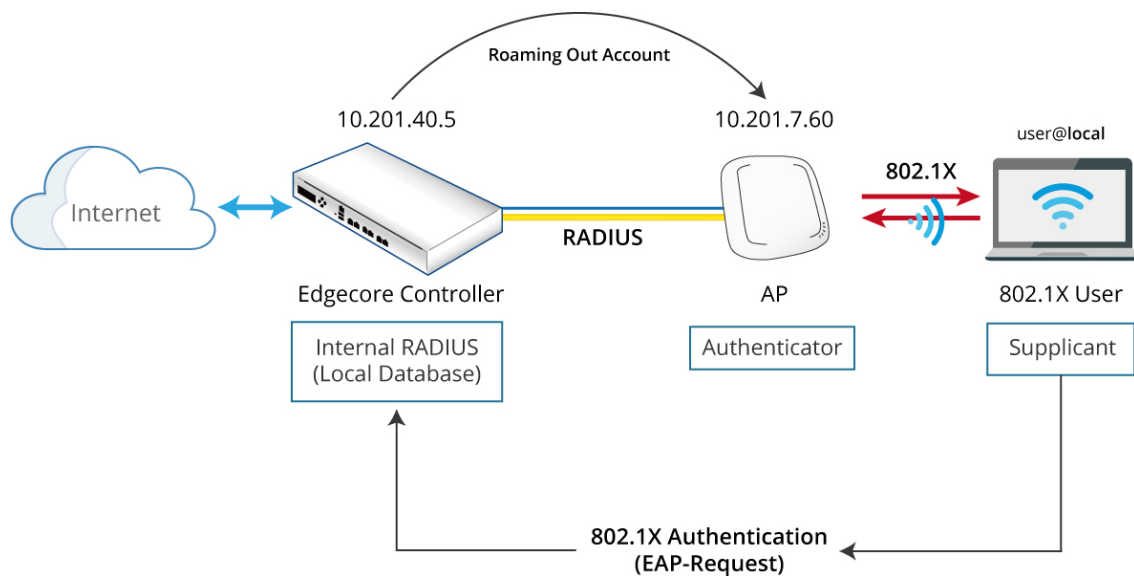
Device Logout

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.

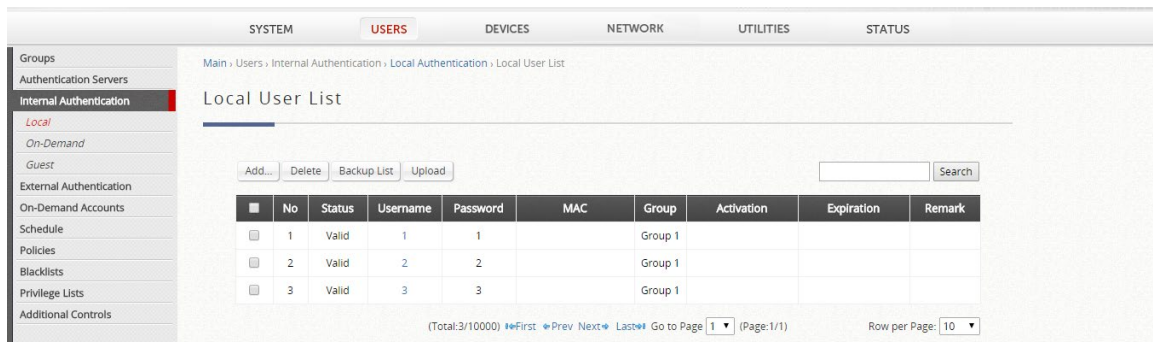


3.2 Device Preparation

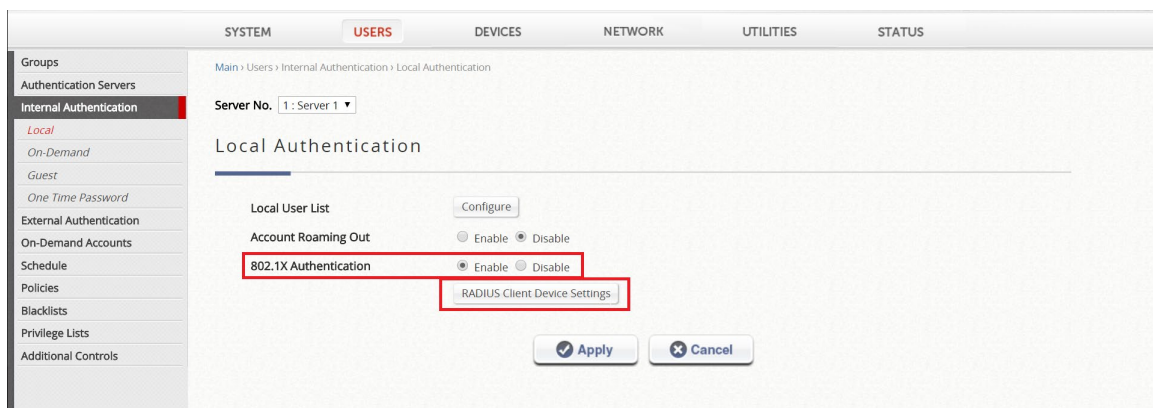
- Gateway: EWS Controller to act as a RADIUS server in 802.1X authentication
- Access Point: ECW/ECWO Access Point to act as authenticator
- Supplicant: notebooks or mobile devices

3.3 Gateway Configuration

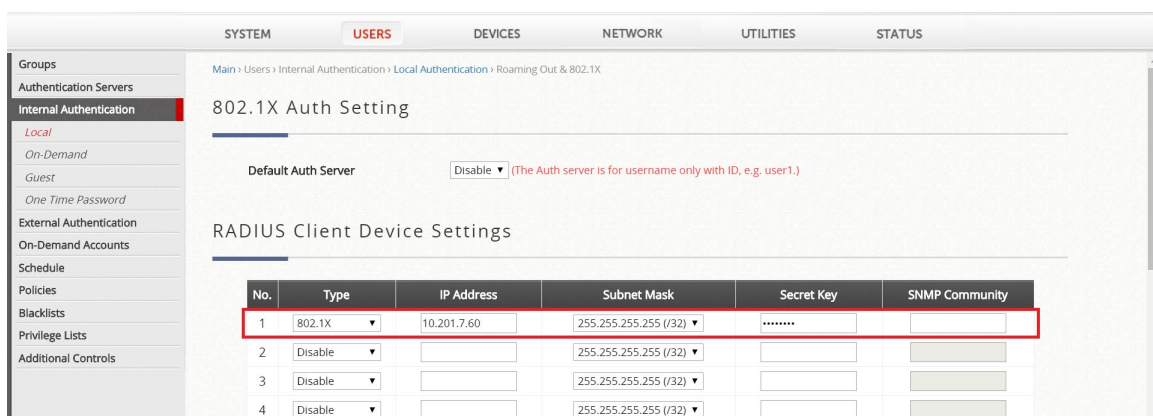
1. Create Local accounts in the Local database



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

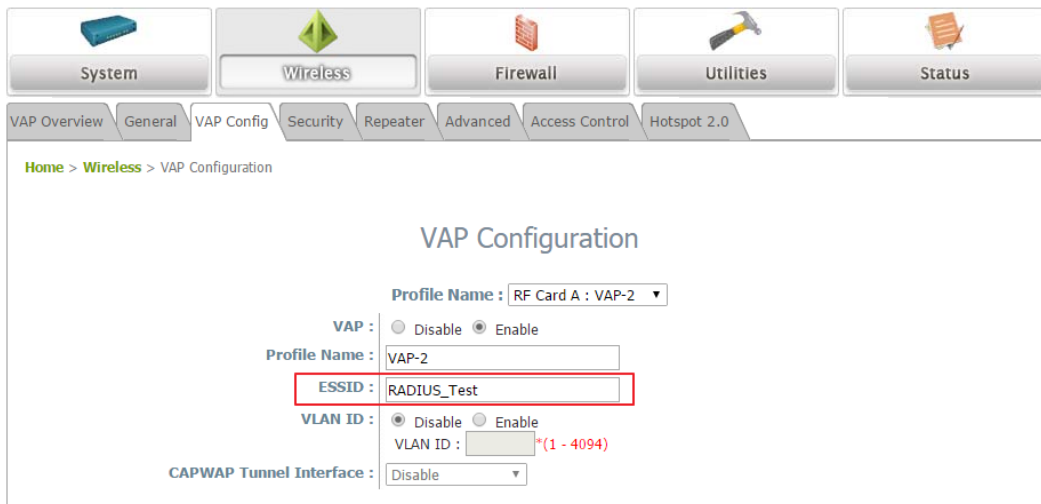


3. Select "802.1X" under Type, enter the WAN IP address of the **Access Point** (Access point acts as a RADIUS authenticator), and select the appropriate subnet mask and enter a secret key. (e.g., 12345678)

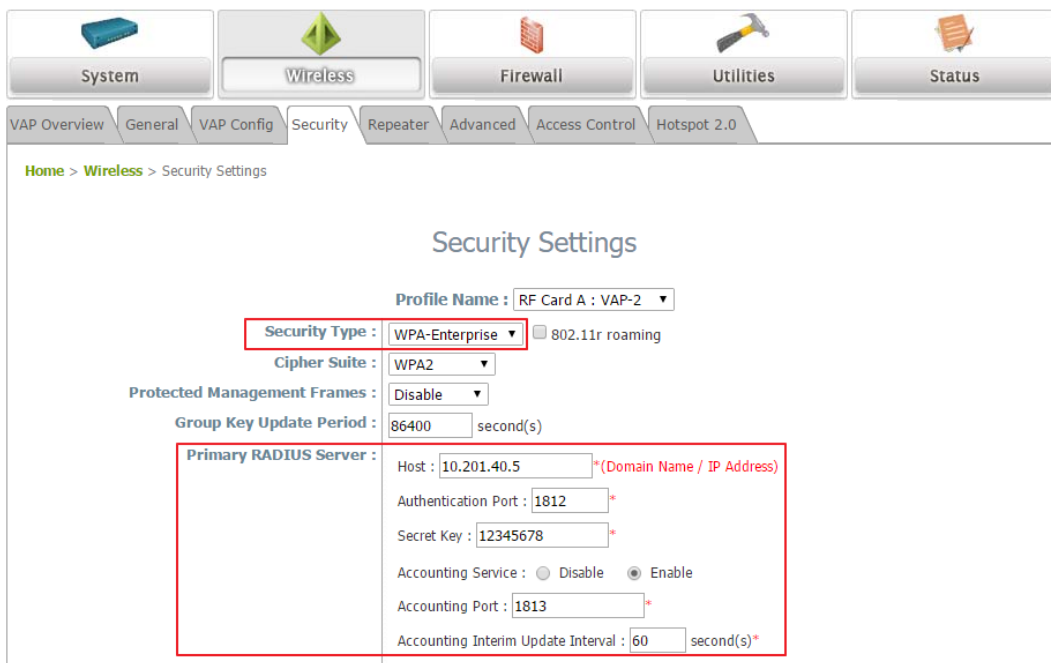


3.4 AP Configuration

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

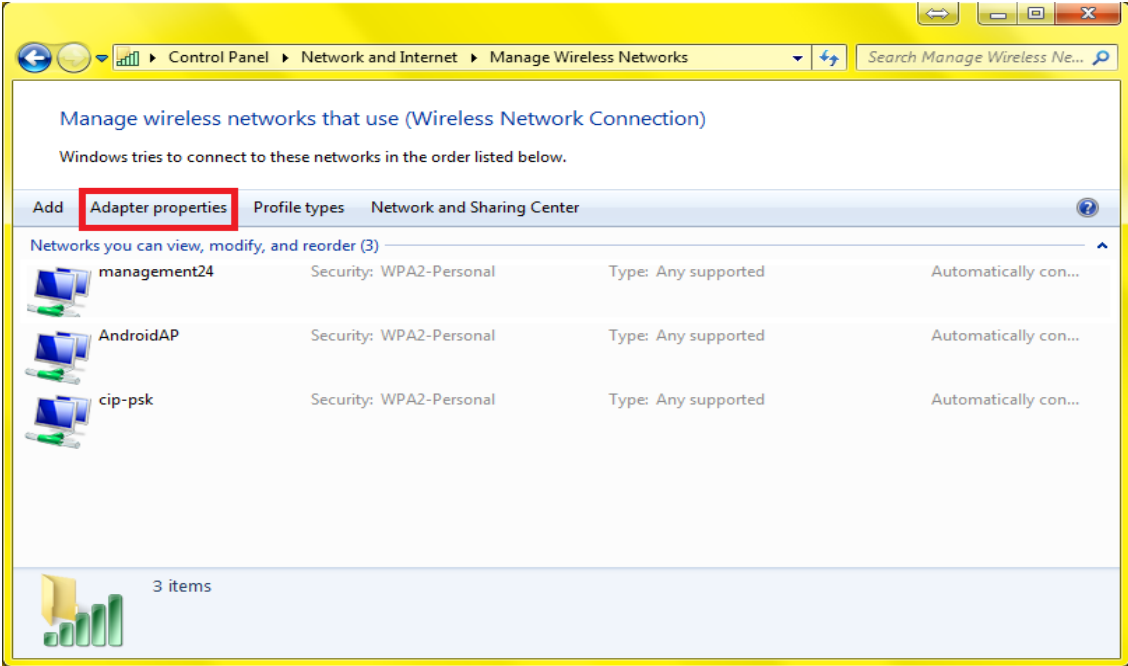


- Go to Security Settings within the same VAP and select **WPA-Enterprise** as the security type, which supports 802.1x RADIUS authentication. Then, administrators type in the Gateway's IP address as primary RADIUS Server. In this case, enabling accounting service is not mandatory.

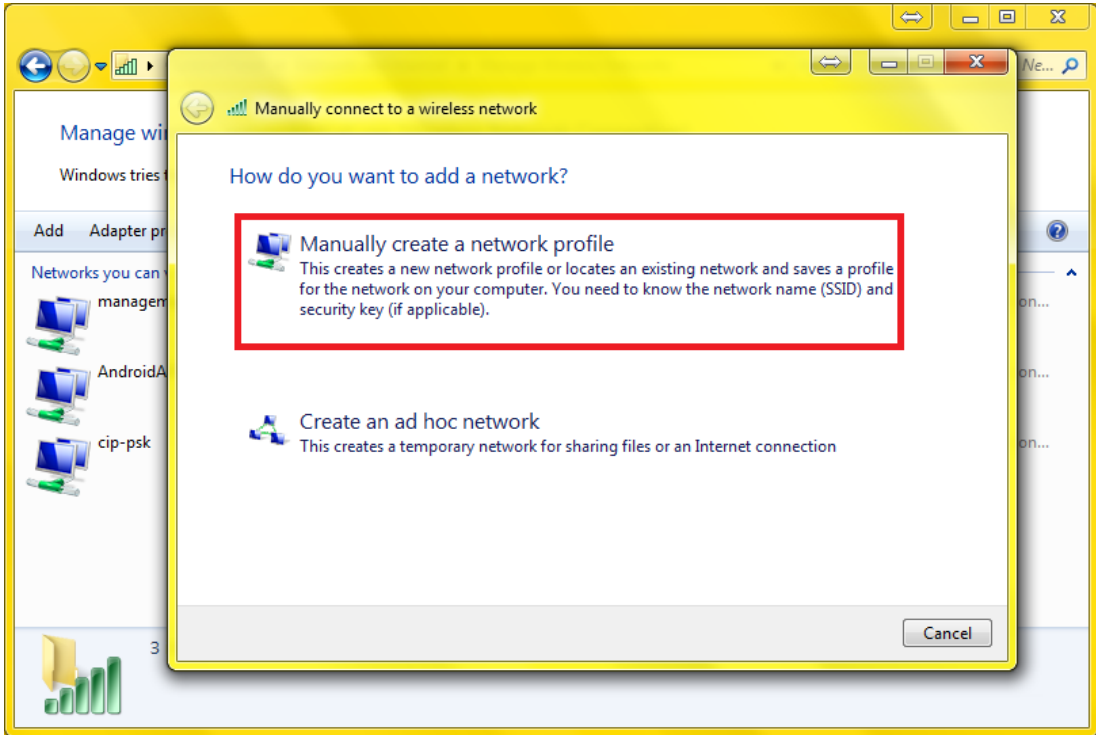


3.5 Client Side Verification

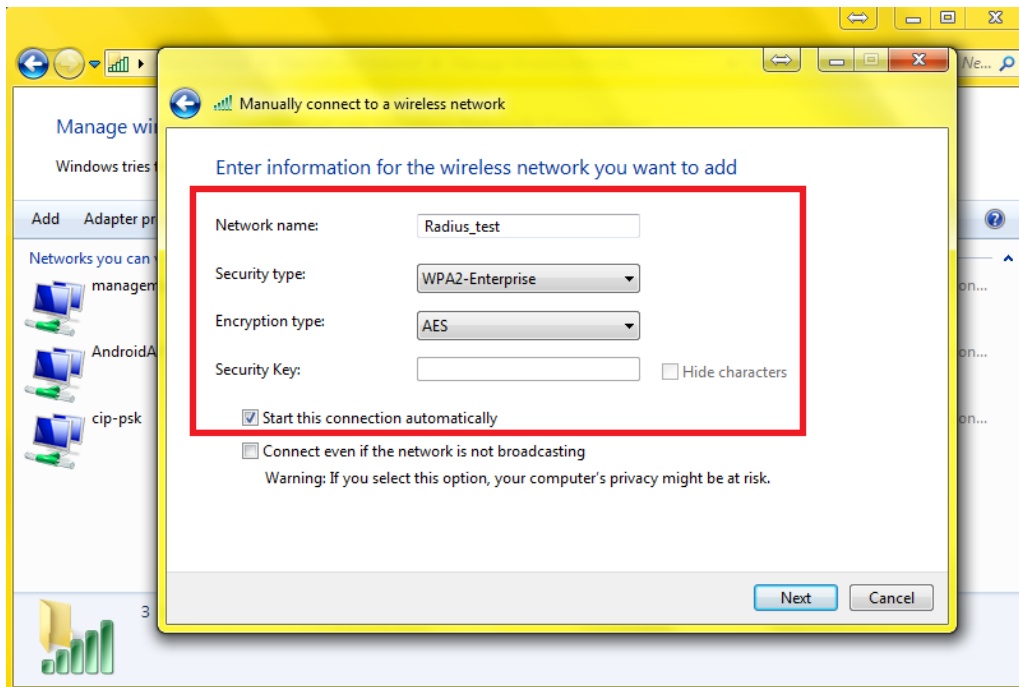
- Add Adapter properties under "Manage Wireless Networks"



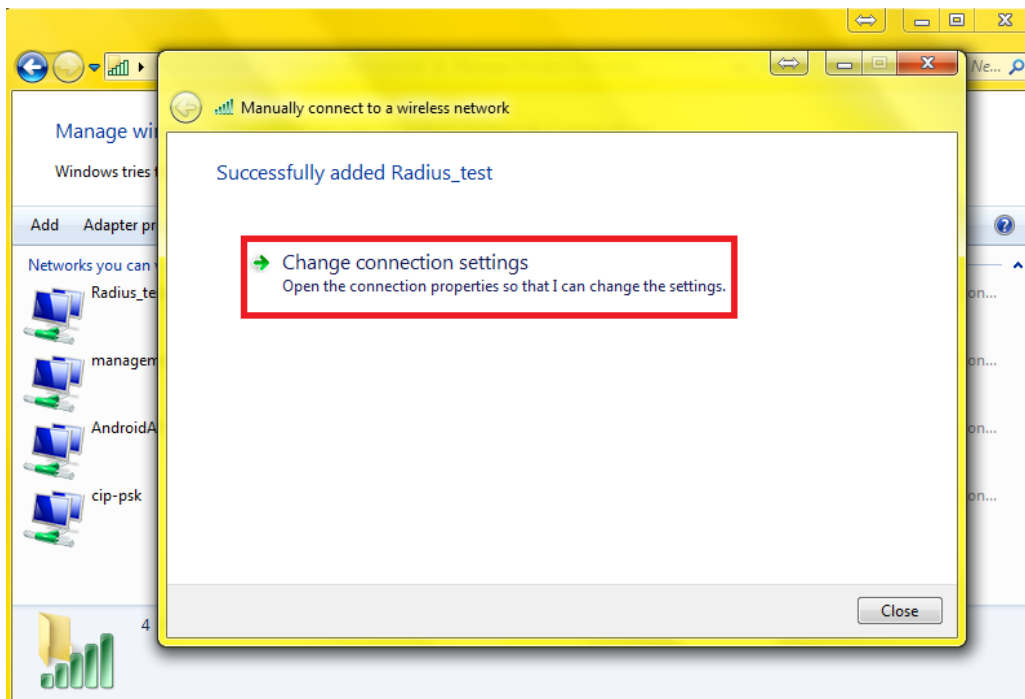
2. Select "Manually Create a Network Profile"



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

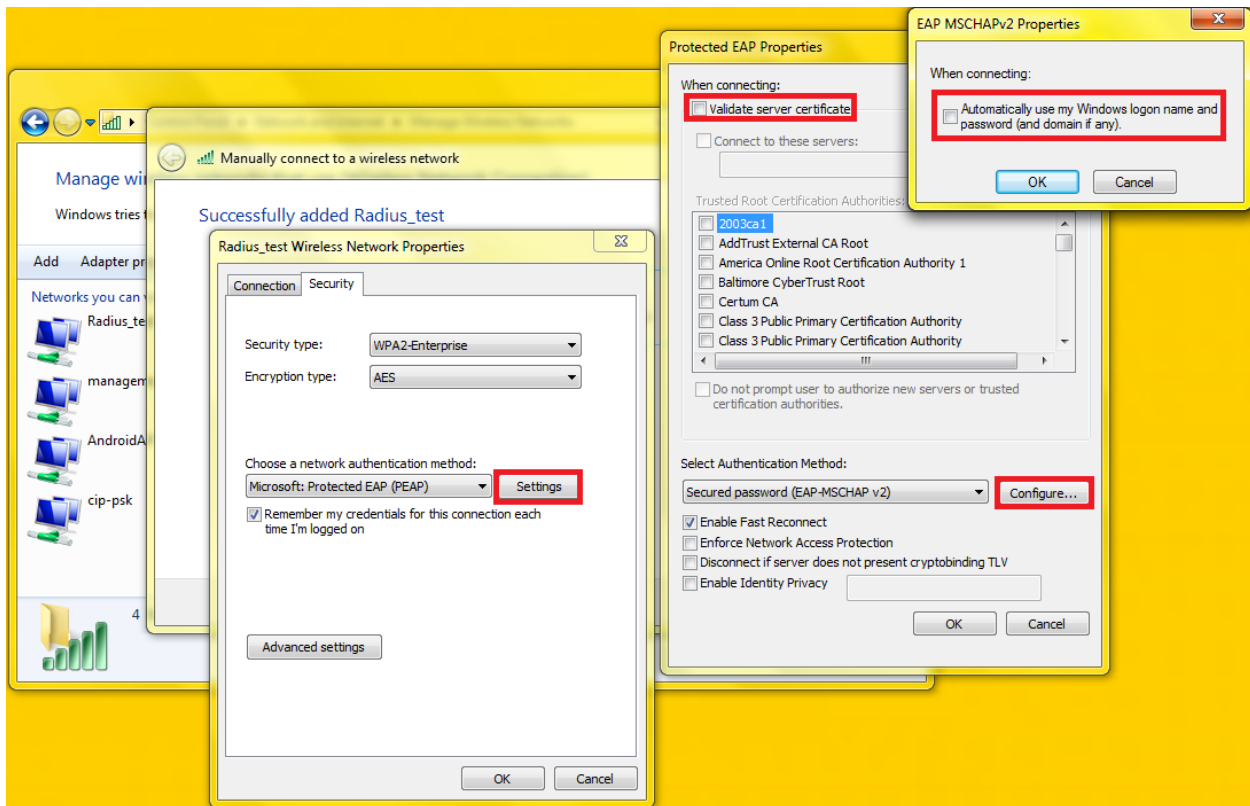


4. Select Change connection Settings

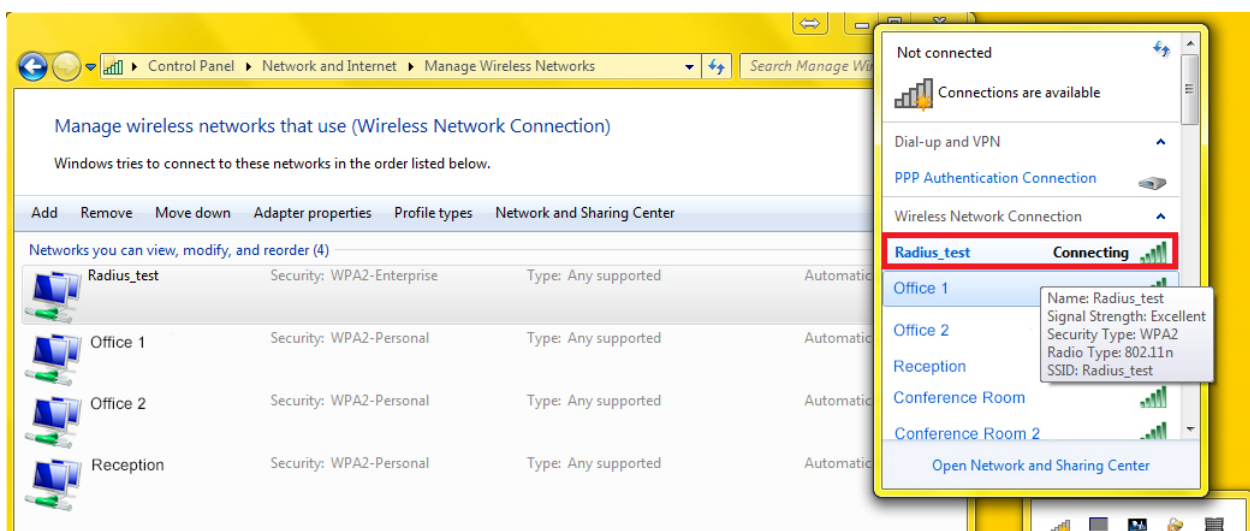


5. Change the Security type to WPA2-Enterprise and Encryption type to AES while further selecting the Settings button of the network authentication method as Microsoft PEAP.

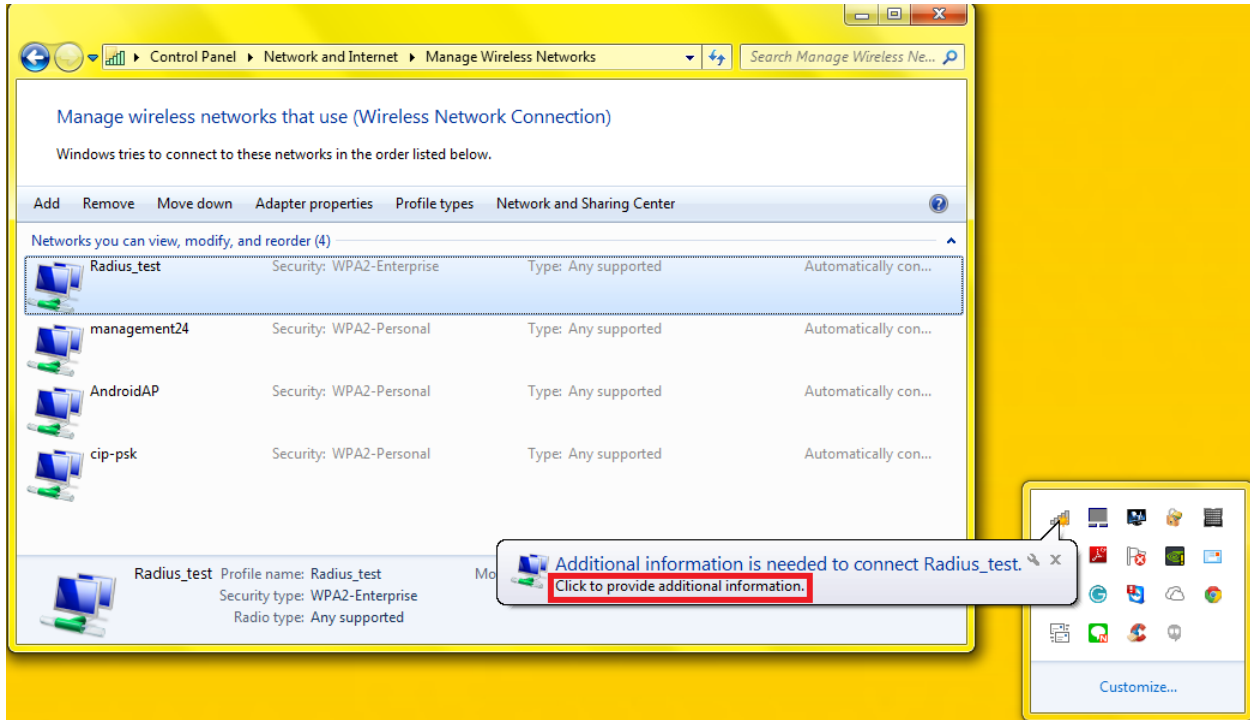
- Ensure to deselect the “Validate server certificate” and the “Automatically use my Windows logon name and password (and domain if any)”.
- When done, Click OK, OK, and OK again.



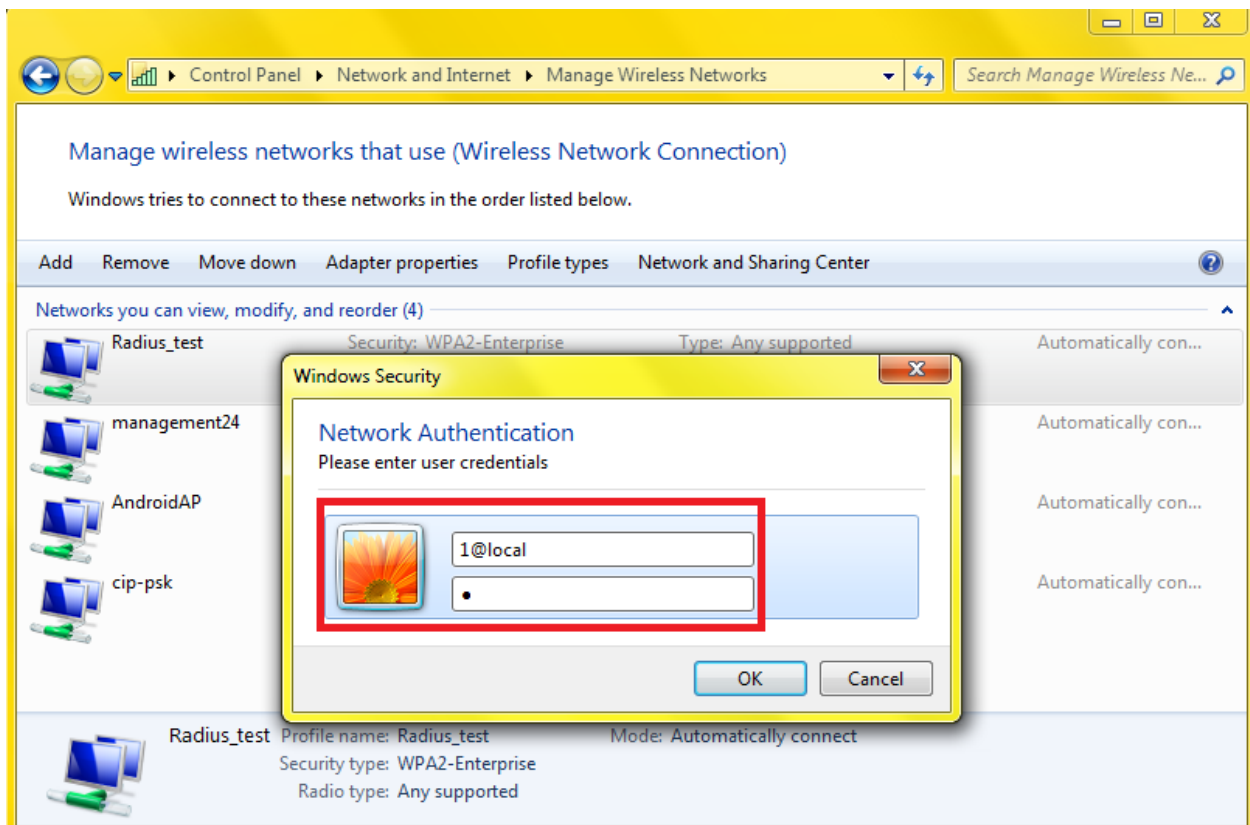
6. Connect to the created SSID “RADIUS_Test”



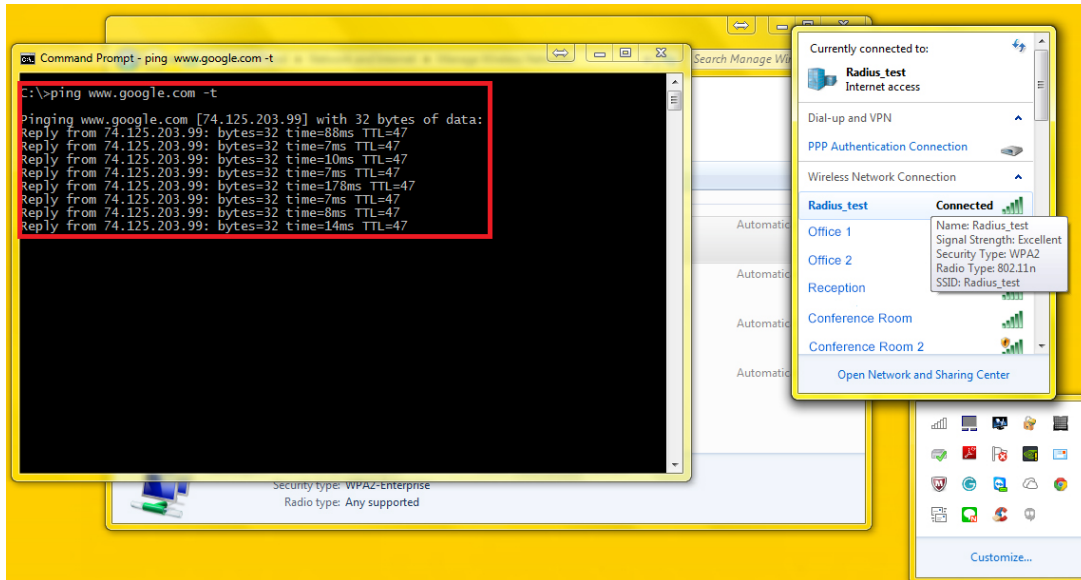
7. Click on the message that says “Additional information is needed to connect RADIUS_Test”.



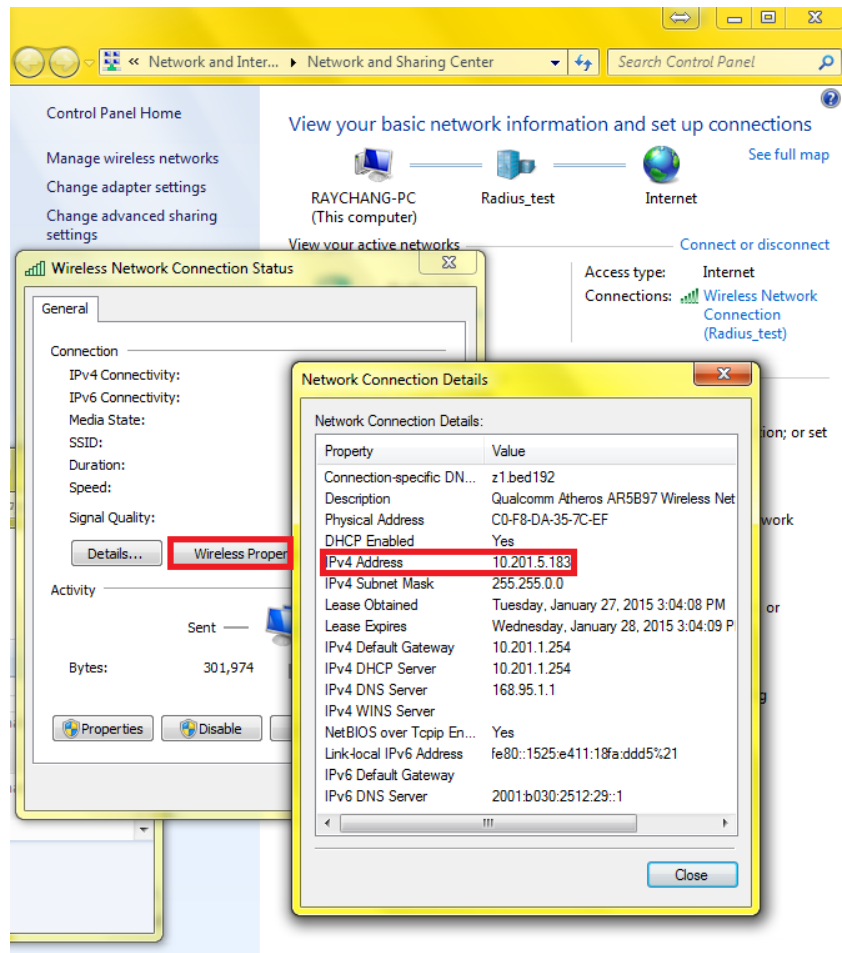
8. Enter the user credentials at the Network Authentication box with username "1@local" and password "1".



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



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



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.