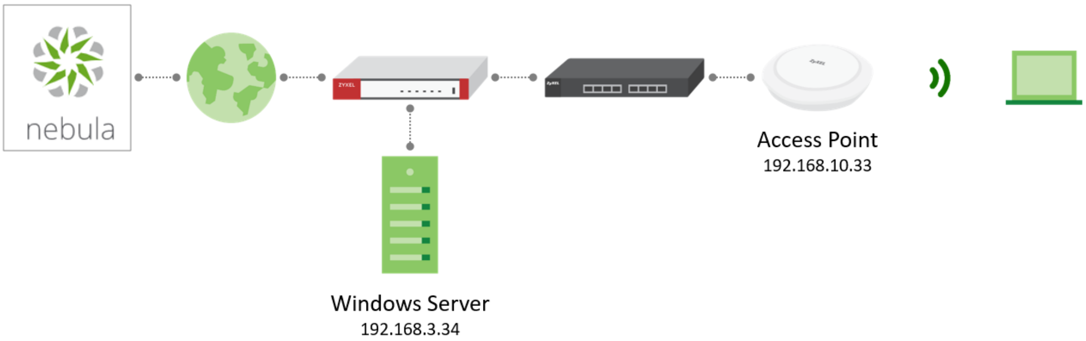
Implement EAP-TLS and EAP-TTLS on Nebula Managed AP

Background

Windows Active Directory Server are widely used to maintain enterprise inventory and employee information. Furthermore, we can utilize the information inside server for wireless authentication to raise the network security. Over several authentication credentials, the certificate is much securer than username/password, and In the wireless network, there're two popular approaches using certificate: **EAP-TTLS and EAP-TLS**. The former approach uses certificate to protect authentication traffic and verify server's identity (make sure the client is connecting to a trusted server), and uses **username and password** for client authentication. Meanwhile, the latter one uses **certificate** for both server and client authentication.
This document includes the process for constructing an environment using EAP-TTLS and EAP-TLS when APs are managed in Nebula Control Center, which covers configurations on client device and Nebula Control Center. Help user to deploy their network easily and efficiently.

Topology



Outline of this Document

Prerequisite

1. Windows Server should be already added roles below:
   - Active Directory Domain Services
   - Active Directory Certificate Services
     - Certificate Authority
     - Certificate Authority Web Enrollment
   - Network Policy and Access Services (RADIUS)
   - Web Server (IIS)
2. All the certificates on RADIUS's certification path have been exported from server
3. Client's Personal Certificate has been exported from server
4. A domain user has been created in Active Directory
5. Access Point has been added in the RADIUS Server's trusted client
6. Traffic between [AP,Server] and [PC,Server] shouldn't be blocked
7. AP is already managed in a specific site in Nebula Control Center

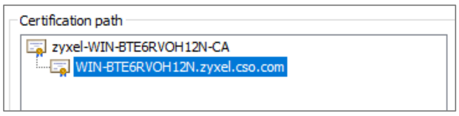
Configuration on Client PC

Three steps are required on Windows PC before they use EAP-TLS or EAP-TTLS to access the network. These initial configuration requires user to connect their PCs into Ethernet first, listed below:

1. Import server's certificates into PC's "Trusted Root CA List"
2. Import a personal certificate to PC's "Personal Certificate"
3. Establish a Wi-Fi profile

Import Server's Certificates into PC's "Trusted Root CA List"

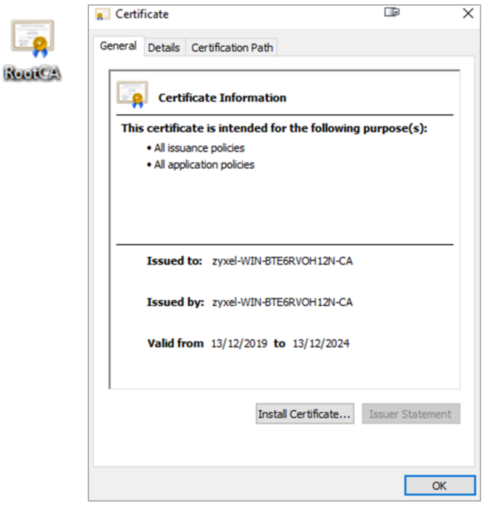
First, we need to import required certificates to the client PC. Remember that **all certificates in the certification path** should be imported.


Certification path

zyxel-WIN-BTE6RVOH12N-CA
WIN-BTE6RVOH12N.zyxel.cso.com

(Certificate Path of RADIUS Server's Certificate, two certificates need to be imported)

Simply open the certificates' icon, and click "Install Certificate" in the certificate General page.



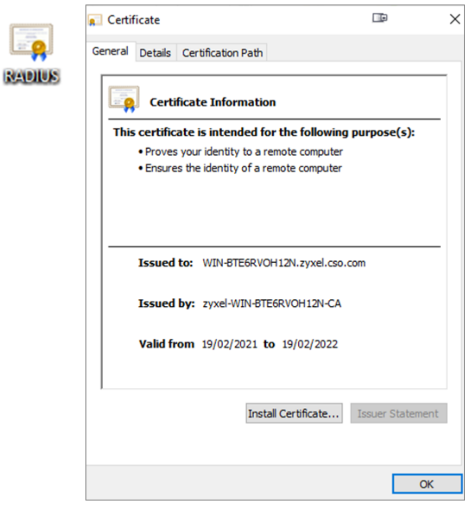
This certificate is intended for the following purpose(s):
- All issuance policies
- All application policies

Issued to: zyxel-WIN-BTE6RVOH12N-CA

Issued by: zyxel-WIN-BTE6RVOH12N-CA

Valid from 13/12/2019 to 13/12/2024

Root CA's Certificate



This certificate is intended for the following purpose(s):
- Proves your identity to a remote computer
- Ensures the identity of a remote computer

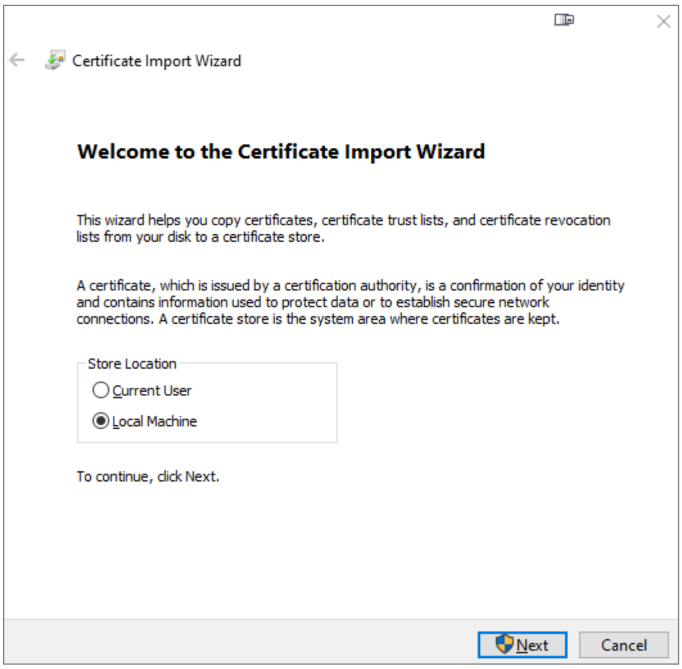
Issued to: WIN-BTE6RVOH12N.zyxel.cso.com

Issued by: zyxel-WIN-BTE6RVOH12N-CA

Valid from 19/02/2021 to 19/02/2022

RADIUS Certificate

In the pop-out window, select “Local Machine” and press next.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

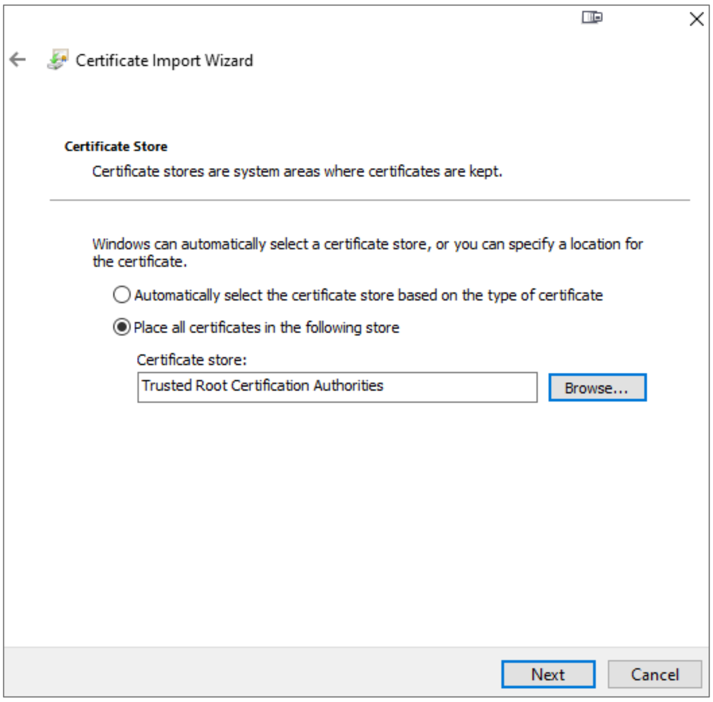
Store Location

○ Current User

● Local Machine

To continue, click Next.

In the next page, click **Browse** and place the certificate in “Trusted Root Certification Authorities”. Then click Next



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

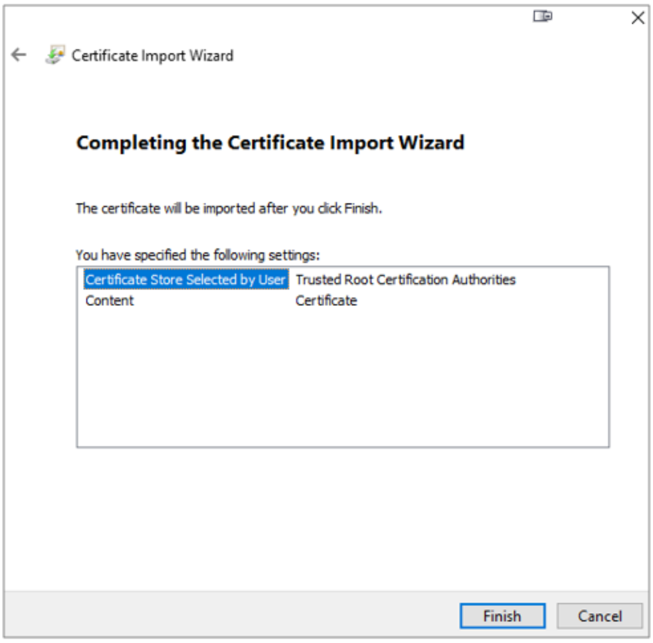
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Click "Finish" in the next page, and then the system will inform the import was successful.

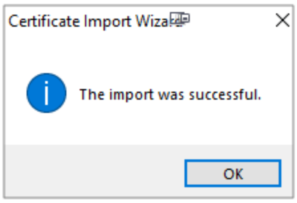


Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

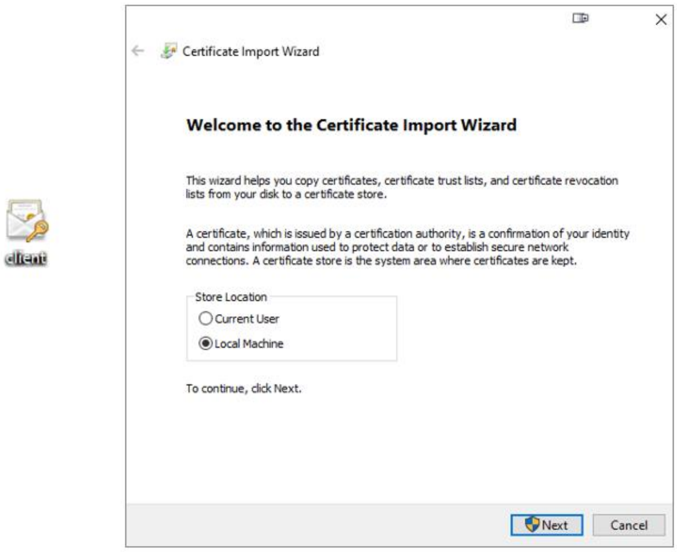
Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate



The import was successful.

Import a Personal Certificate to PC's "Personal Certificate"

After export the client certificate from server, we can put the file into testing device through cloud drive or USB Storage.
Double click the Certificate icon, and select "Local Machine" and then press "Next".



Welcome to the Certificate Import Wizard

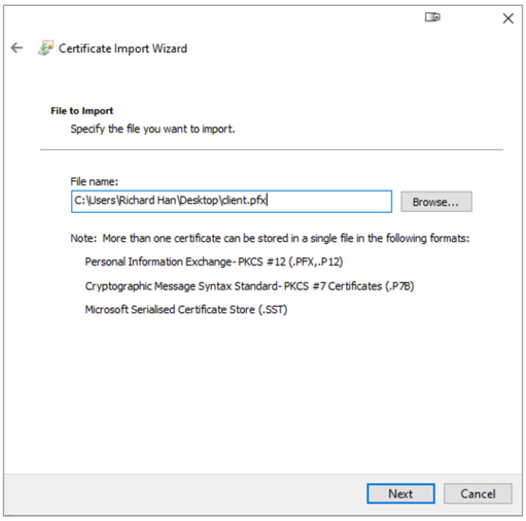
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

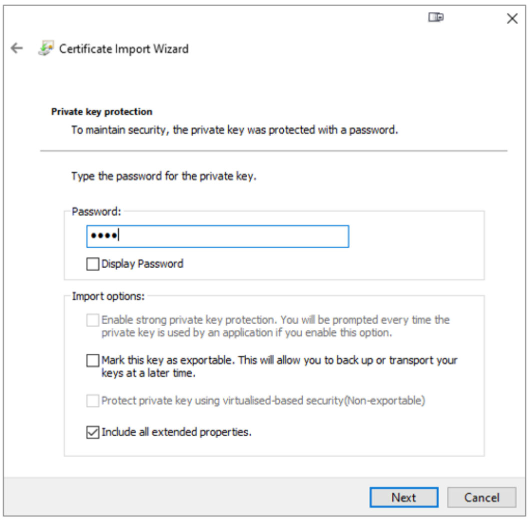
Confirm the selected file, and then press "Next". In the next page, type the password to extract the file, and then press "Next"



File to Import
Specify the file you want to import.

File name:
C:\Users\Richard Han\Desktop\client.pfx

Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialised Certificate Store (.SST)



Private key protection
To maintain security, the private key was protected with a password.

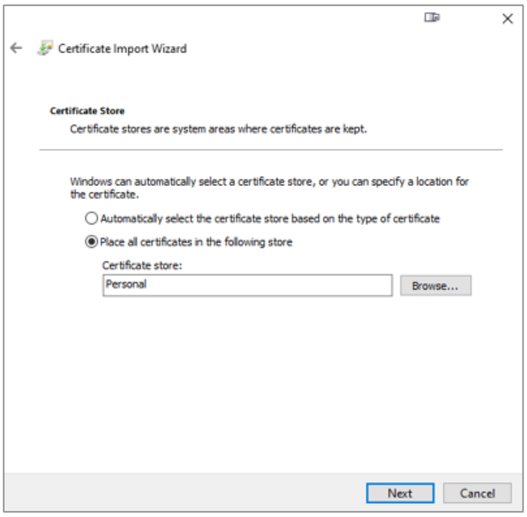
Type the password for the private key.

Password:
••••

□ Display Password

Import options:
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
□ Protect private key using virtualised-based security(Non-exportable)
☑ Include all extended properties.

Import the certificate in the "Personal" folder, and then click "Next". In the next page, confirm the information, and click "Finish".



Certificate Store

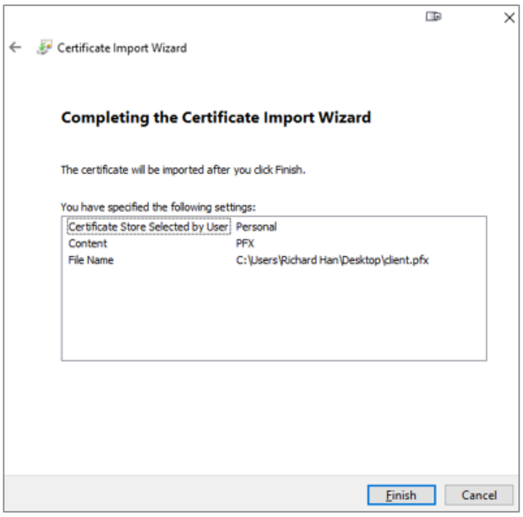
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Personal



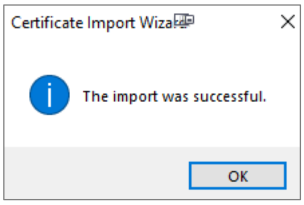
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Users\Richard Han\Desktop\client.pfx

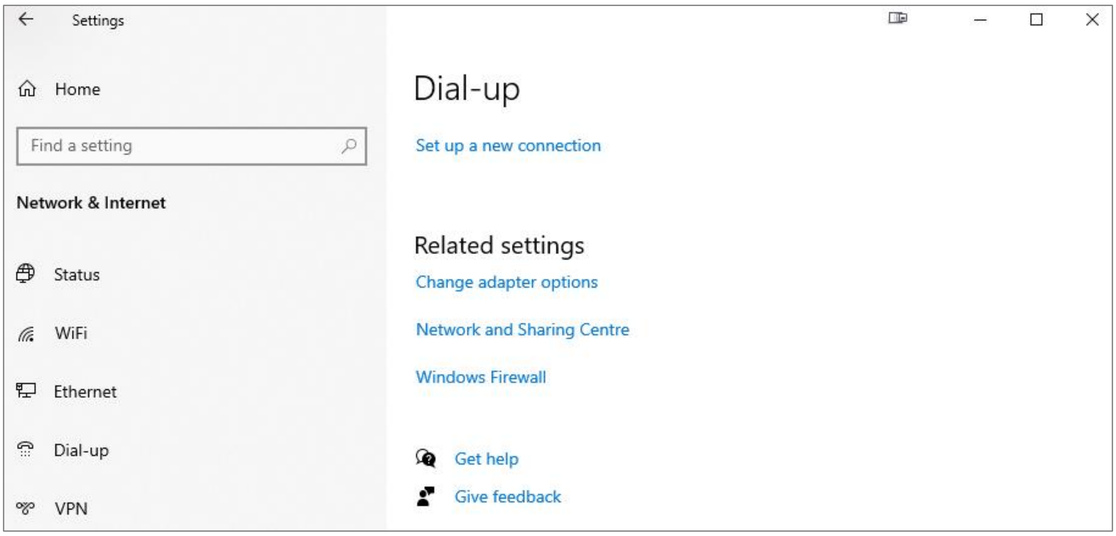
After that, we'll see the success page pops-out.



The import was successful.

Establish a Wi-Fi profile

We need to manually create Wi-Fi profile to let station connects to network using EAP-TTLS or EAP-TLS. In Windows 10 system, press "Set up a new connection" under the directory **Settings > Network & Internet > Dial-up.**


Settings

Home

Find a setting

Network & Internet

Status

WiFi

Ethernet

Dial-up

VPN

Dial-up

Set up a new connection

Related settings

Change adapter options

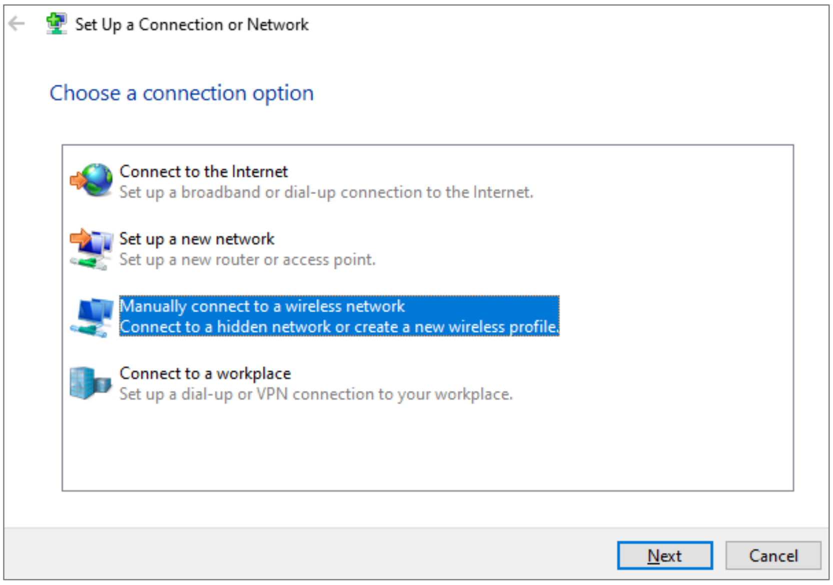
Network and Sharing Centre

Windows Firewall

Get help

Give feedback

Select "Manually connect to a wireless network", and then press "Next"


Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

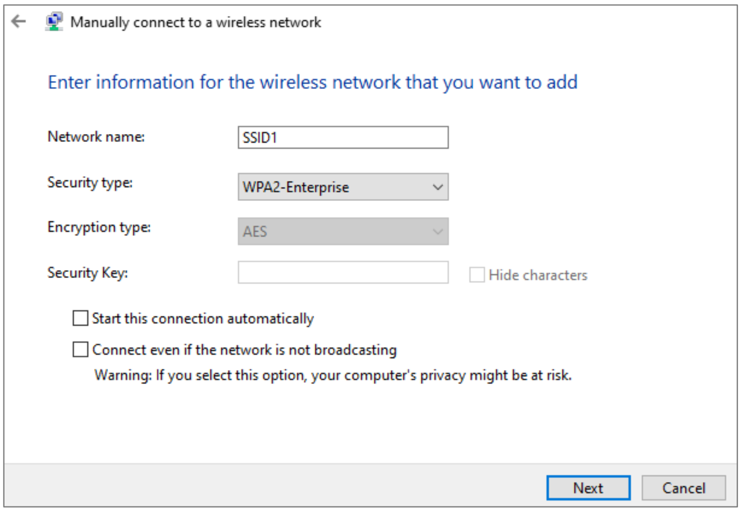
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Next

Cancel

Fill in the information as below, and then press "Next" (Make sure the Network name is the same as the SSID name AP uses)



Manually connect to a wireless network

Enter information for the wireless network that you want to add

Network name: SSID1

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

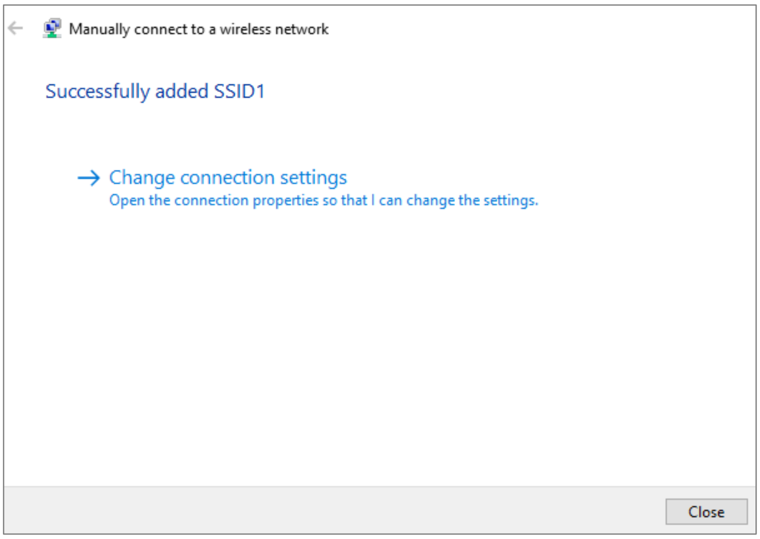
□ Hide characters

□ 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.

After the result page shows up, click "Change connection settings".



Manually connect to a wireless network

Successfully added SSID1

→ Change connection settings

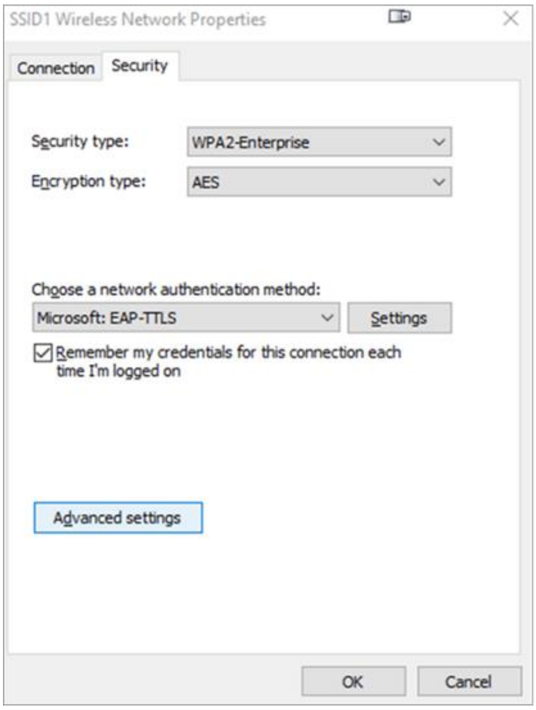
Open the connection properties so that I can change the settings.

Moving to the Security Tab, and do following settings depends on which authentication method you'd like to use.

EAP-TTLS

Select "Microsoft: EAP-TTLS" in the authentication method column, and then press the "Settings" button beside it. Fill in the table as the screenshot below.

*Make sure the server's IP is filled in the "Connect to these servers" column.
**Make sure all certificates in the Certificate Path are selected



SSID1 Wireless Network Properties

Connection | Security

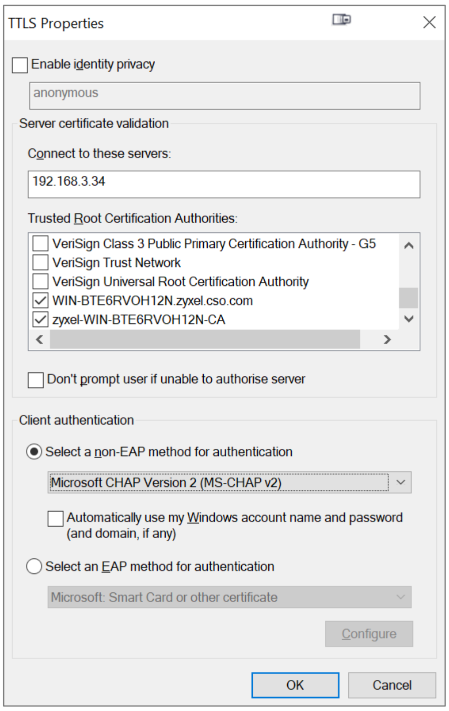
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: EAP-TTLS

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



TTLS Properties

□ Enable identity privacy

anonymous

Server certificate validation

Connect to these servers:

192.168.3.34

Trusted Root Certification Authorities:

□ VeriSign Class 3 Public Primary Certification Authority - G5
□ VeriSign Trust Network
□ VeriSign Universal Root Certification Authority
☑ WIN-BTE6RVOH12N.zyxel.cso.com
☑ zyxel-WIN-BTE6RVOH12N-CA

□ Don't prompt user if unable to authorise server

Client authentication

● Select a non-EAP method for authentication

Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows account name and password (and domain, if any)

○ Select an EAP method for authentication

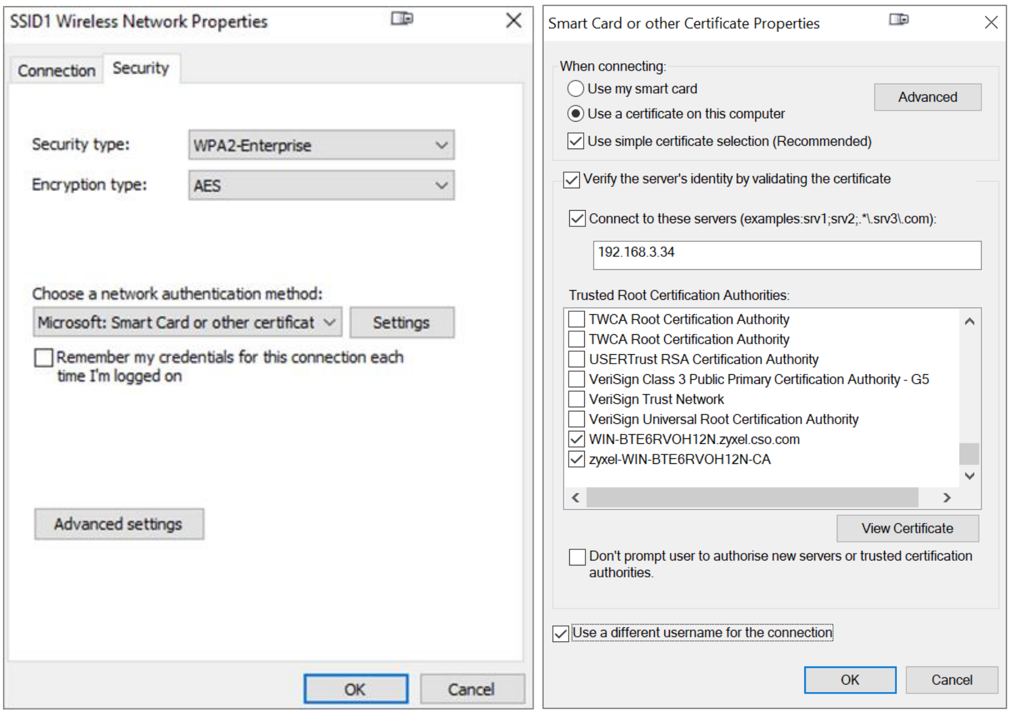
Microsoft: Smart Card or other certificate

After completing above configurations, press "OK" in both **TTLS Properties** and **Wireless Network Properties** page, and then press "Close" in SSID Profile creating page.

EAP-TLS

Select “Microsoft: Smart Card or other certificate” in the authentication method column, and then press the “Settings” button beside it. Fill in the table as the screenshot below.

*Make sure the server’s IP is filled in the “Connect to these servers” column.
**Make sure all certificates in the Certificate Path are selected



SSID1 Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:
Microsoft: Smart Card or other certificat | Settings

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

Advanced settings

OK | Cancel

Smart Card or other Certificate Properties

When connecting:
○ Use my smart card | Advanced
● Use a certificate on this computer
☑ Use simple certificate selection (Recommended)

☑ Verify the server's identity by validating the certificate

☑ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
192.168.3.34

Trusted Root Certification Authorities:
□ TWCA Root Certification Authority
□ TWCA Root Certification Authority
□ USERTrust RSA Certification Authority
□ VeriSign Class 3 Public Primary Certification Authority - G5
□ VeriSign Trust Network
□ VeriSign Universal Root Certification Authority
☑ WIN-BTE6RVOH12N.zyxel.cso.com
☑ zyxel-WIN-BTE6RVOH12N-CA

View Certificate

□ Don't prompt user to authorise new servers or trusted certification authorities.

☑ Use a different username for the connection

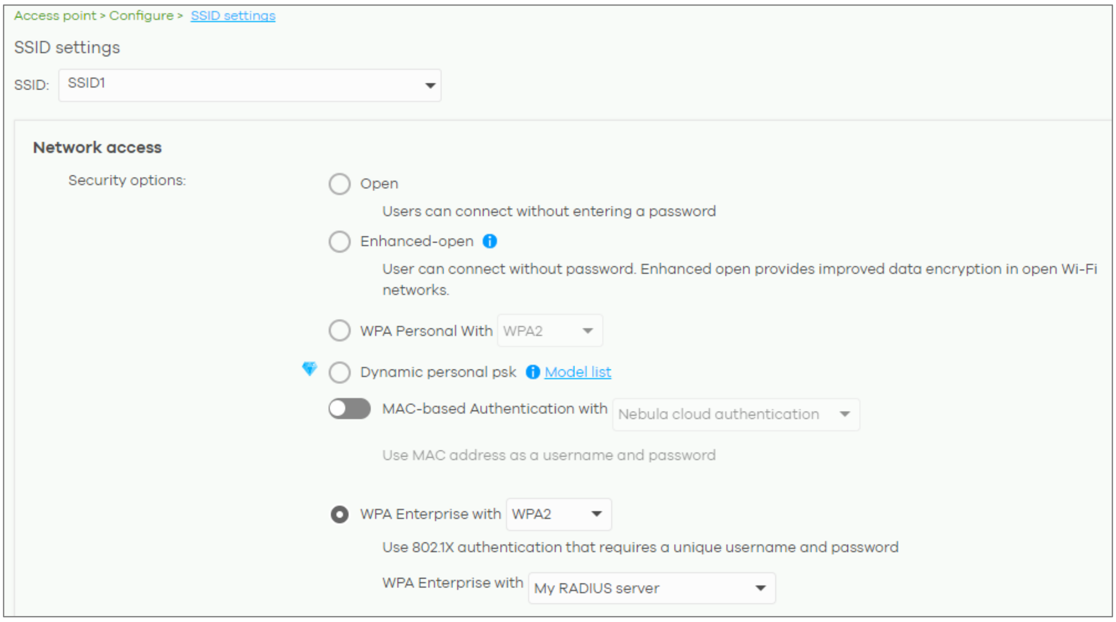
OK | Cancel

After completing above configurations, press “OK” in both **Smart and other Certificates Properties** and **Wireless Network Properties** page, and then press “Close” in SSID Profile creating page.

Configuration on Nebula Control Center

Only one setting is required to be configured on NCC, which is about SSID Profile. We need to create an SSID using WPA2-Enterprise with external server, so that AP can access Widows Server for wireless authentication when a client associating to the SSID.

So after login to the NCC and select the specific site, simply access the SSID page under directory **Access Point > Configure > SSID Settings**, and select the SSID that we'd like to use. In the **Security Options**, select "WPA Enterprise with WPA2", and using "My RADIUS server".



Access point > Configure > SSID settings

SSID settings

SSID: SSID1

Network access

Security options:

○ Open
Users can connect without entering a password

○ Enhanced-open
User can connect without password. Enhanced open provides improved data encryption in open Wi-Fi networks.

○ WPA Personal With WPA2

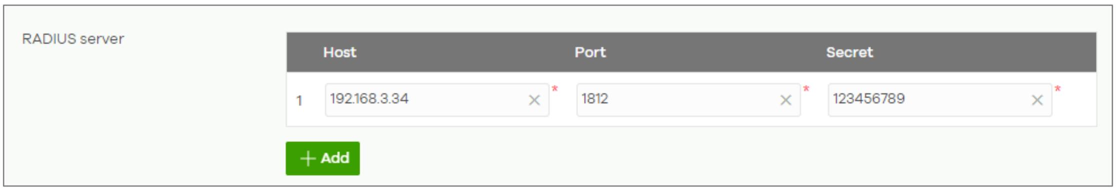
○ Dynamic personal psk Model list

MAC-based Authentication with Nebula cloud authentication
Use MAC address as a username and password

● WPA Enterprise with WPA2
Use 802.1X authentication that requires a unique username and password

WPA Enterprise with My RADIUS server

After that, scrolling down the page and finding **RADIUS Server** column, entering server's "IP address", "used port" and "secret number". Remember the number should be the same as the one configured in the trusted client page of RADIUS Server.



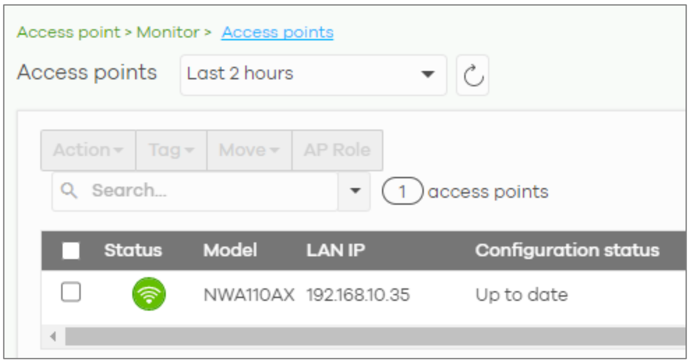
RADIUS server

	Host	Port	Secret
1	192.168.3.34	1812	123456789

+ Add

After finishing above settings, remember to press "SAVE" in the webpage.

After finishing above step, go back to the Access Point page to make sure the AP is online with updated configurations. Follow the directory **Access Point > Monitor > Access Points**, and check if the **Configuration Status** is "Up to date".



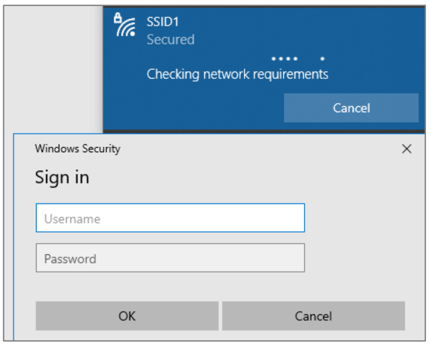
	Status	Model	LAN IP	Configuration status
□	●	NWA110AX	192.168.10.35	Up to date

Test the Result

Open the Wi-Fi list on the PC, and then select the created SSID name.

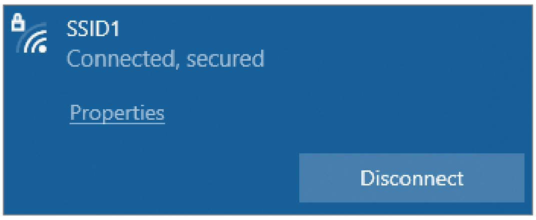
EAP-TTLS

Click SSID1 in the Wi-Fi list, and then type in the username and password.



SSID1
Secured
Checking network requirements

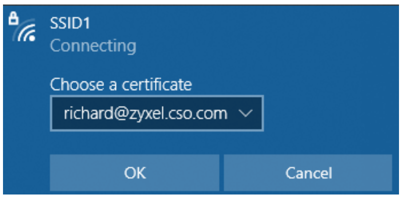
Windows Security
Sign in



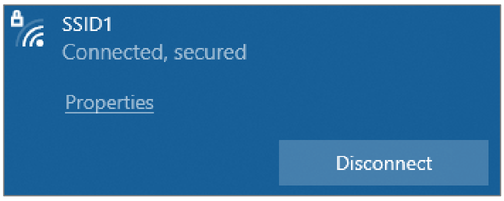
SSID1
Connected, secured

EAP-TLS

Click SSID1 in the Wi-Fi list, and then select the imported certificates.



SSID1
Connecting
Choose a certificate
richard@zyxel.cso.com

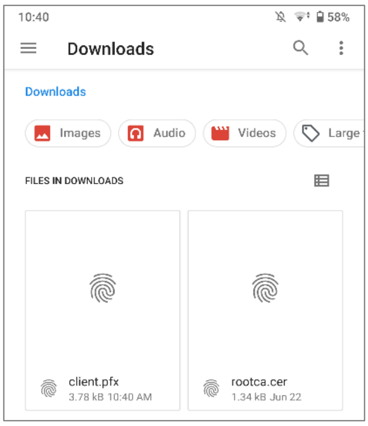


SSID1
Connected, secured

Appendix 1: Configurations on Android Smartphone

Configurations on smartphone are different from those in PC. Such as only root certificate is needed to be imported, and Android user needs to configure some settings when connecting to the SSID. This appendix includes the screenshot of each procedure to let user connect their Android smartphone to wireless network using EAP-TLS or EAP-TTLS.

Just like what we did in configuring the PC, we can also put all the required files into client device through cloud drive.

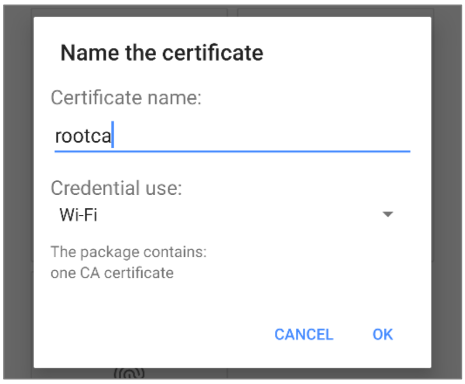


client.pfx 3.78 kB 10:40 AM

rootca.cer 1.34 kB Jun 22

Import Server's Root CA Certificates on Android Phone

Click the certificate file of Root CA, and select "Wi-Fi" in the **Credential use** column, and click OK



Name the certificate

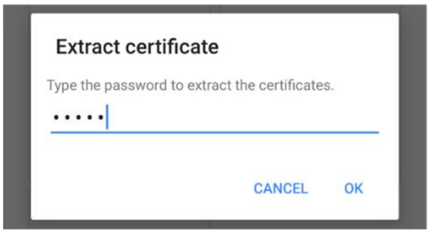
Certificate name: rootca

Credential use: Wi-Fi

The package contains: one CA certificate

Import Client Certificate on Android Phone

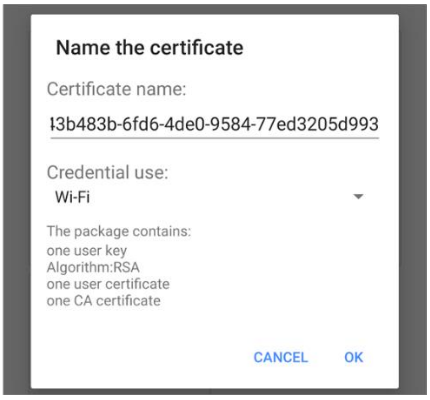
Click the file of client's certificate, and type the correct password to extract the certificate file. In the next page, also select "Wi-Fi" in the **Credential use** column, and click OK.



Extract certificate

Type the password to extract the certificates.

•••••



Name the certificate

Certificate name:

13b483b-6fd6-4de0-9584-77ed3205d993

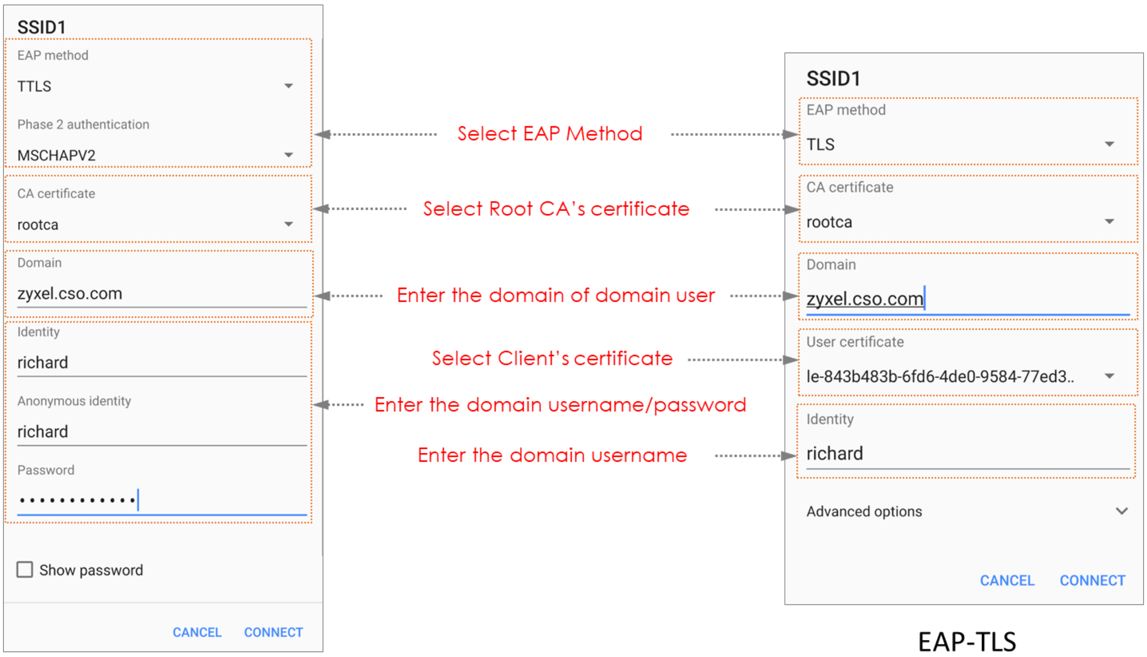
Credential use:

Wi-Fi

The package contains:
one user key
Algorithm:RSA
one user certificate
one CA certificate

Configure SSID Profile

Moving to the Wi-Fi list page, and click the SSID that we're going to connect. Configure the settings for the policy you'd like to use as the page below, and press "Connect".



SSID1

EAP method: TTLS

Phase 2 authentication: MSCHAPV2

CA certificate: rootca

Domain: zyxel.cso.com

Identity: richard

Anonymous identity: richard

Password: ••••••••••••

□ Show password

SSID1

EAP method: TLS

CA certificate: rootca

Domain: zyxel.cso.com

User certificate: le-843b483b-6fd6-4de0-9584-77ed3..

Identity: richard

Advanced options
CANCEL
CONNECT

Select EAP Method
Select Root CA's certificate
Enter the domain of domain user
Select Client's certificate
Enter the domain username/password
Enter the domain username

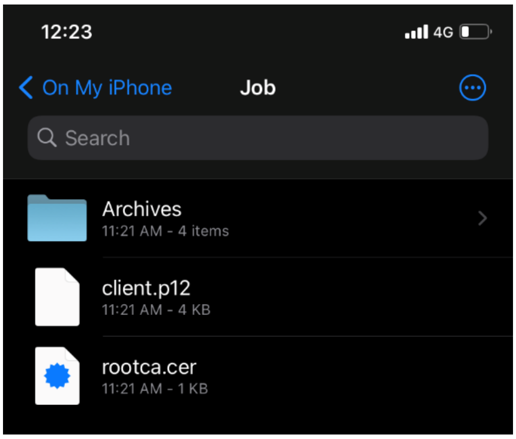
EAP-TLS

EAP-TTLS

Appendix 2: Configurations on iPhone

Configurations on smartphone are different from those in PC. Such as only root certificate is needed to be imported. Comparing to Android phone, less configuration needs to be configured on iPhone, although some settings are still required to be configured under specific directory. This appendix includes the screenshot of each procedure to let user connect their iPhone to wireless network using EAP-TLS.

Just like what we did in configuring the PC, we can also put all the required files into client device through cloud drive.



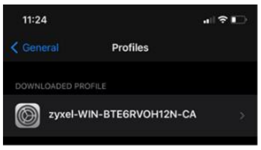
Archives
11:21 AM - 4 items

client.p12
11:21 AM - 4 KB

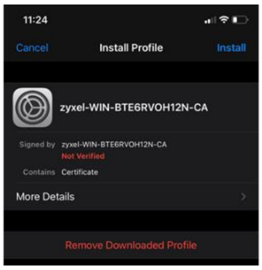
rootca.cer
11:21 AM - 1 KB

Import Server's Root CA Certificate on iPhone

Access the directory **General > Profiles**, where one configuration file will be displayed. Click the file, and then click "Install" button in the pages afterwards. Finally, we can see the Profile Installed page, click "Done" on the upper-right corner.



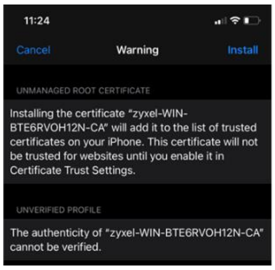
zyxel-WIN-BTE6RVOH12N-CA



zyxel-WIN-BTE6RVOH12N-CA

Signed by zyxel-WIN-BTE6RVOH12N-CA
Not Verified

Contains Certificate

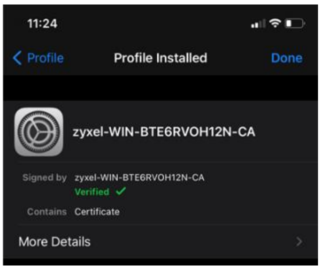


UNMANAGED ROOT CERTIFICATE

Installing the certificate "zyxel-WIN-BTE6RVOH12N-CA" will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.

UNVERIFIED PROFILE

The authenticity of "zyxel-WIN-BTE6RVOH12N-CA" cannot be verified.



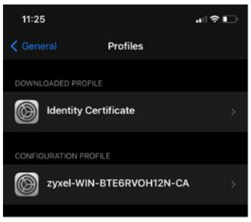
zyxel-WIN-BTE6RVOH12N-CA

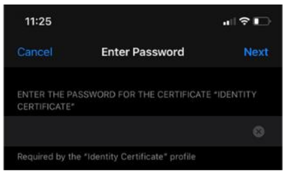
Signed by zyxel-WIN-BTE6RVOH12N-CA
Verified ✓

Contains Certificate

Import Client Certificate on iPhone

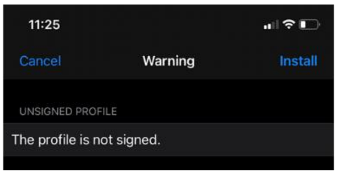
After the Root CA's certificate is installed, we can find another item displayed in the original directory **General > Profiles**. Click the Identity Certification, and enter the password in the next page to let iPhone extract the file. In the third page, click the Install on the upper-right corner, and click "Done" to complete the profile installation process.



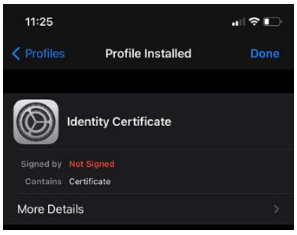


ENTER THE PASSWORD FOR THE CERTIFICATE "IDENTITY CERTIFICATE"

Required by the "Identity Certificate" profile



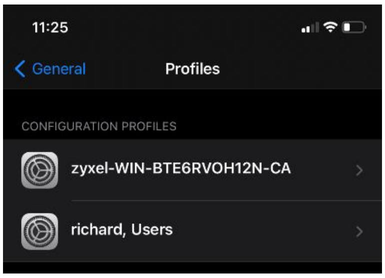
The profile is not signed.



Signed by Not Signed

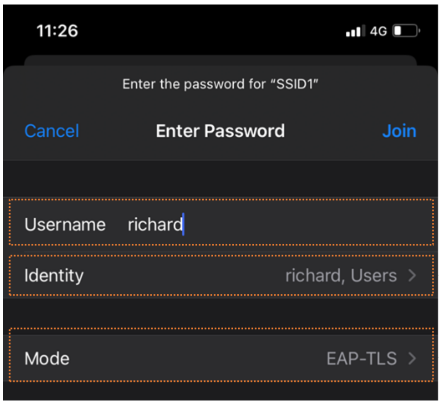
Contains Certificate

After above process complete, we can see both certificates are put in the "Configuration Profile" list.



Configure SSID Profile

Moving to the Wi-Fi list page, and click the SSID that we're going to connect. Configure the settings for the policy you'd like to use as the page below, and press "Join".



Enter the password for "SSID1"

Username richard

Identity richard, Users

Mode EAP-TLS

Enter the domain username

Select Client's certificate

Enter the domain username/password