

Understand and Configure EAP-TLS with Mobility Express and ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[EAP-TLS Flow](#)

[Steps in EAP-TLS Flow](#)

[Configure](#)

[Cisco Mobility Express](#)

[ISE with Cisco Mobility Express](#)

[EAP-TLS Settings](#)

[Mobility Express Settings on ISE](#)

[Trust Certificate on ISE](#)

[Client for EAP-TLS](#)

[Download User Certificate on Client Machine \(Windows Desktop\)](#)

[Wireless Profile for EAP-TLS](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to set up a Wireless Local Area Network (WLAN) with 802.1x security in a Mobility Express Controller. This document also explains the use of Extensible Authentication Protocol (EAP) -Transport Layer Security (TLS) specifically.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Mobility Express initial setup
- 802.1x authentication process
- Certificates

Components Used

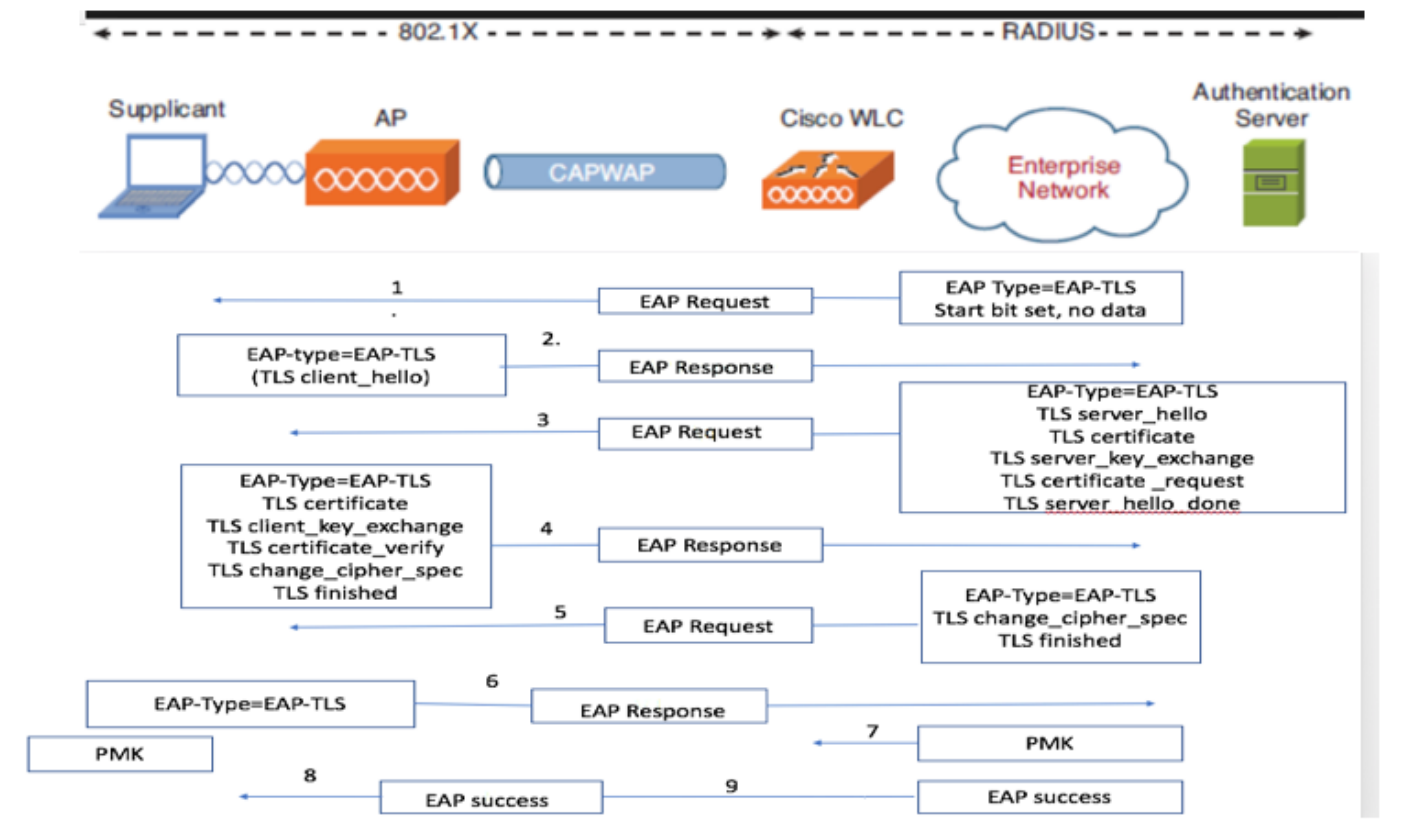
The information in this document is based on these software and hardware versions:

- WLC 5508 version 8.5
- Identity Services Engine (ISE) version 2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

EAP-TLS Flow



Steps in EAP-TLS Flow

1. Wireless Client gets associated with the Access Point (AP).
2. AP does not permit the client to send any data at this point and sends an authentication request.
3. The supplicant then responds with an EAP-Response Identity. The WLC then communicates the user-id information to the Authentication Server.
4. RADIUS server responds back to the client with an EAP-TLS Start Packet. The EAP-TLS conversation starts at this point.
5. The peer sends an EAP-Response back to the authentication server which contains a "client_hello" handshake message, a cipher that is set for NULL.
6. The authentication server responds with an Access-challenge packet that contains:

TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.

7. Client responds with a EAP-Response message that contains:

Certificate → Server can validate to verify that it is trusted.

client_key_exchange

certificate_verify → Verifies the server is trusted

change_cipher_spec

TLS finished

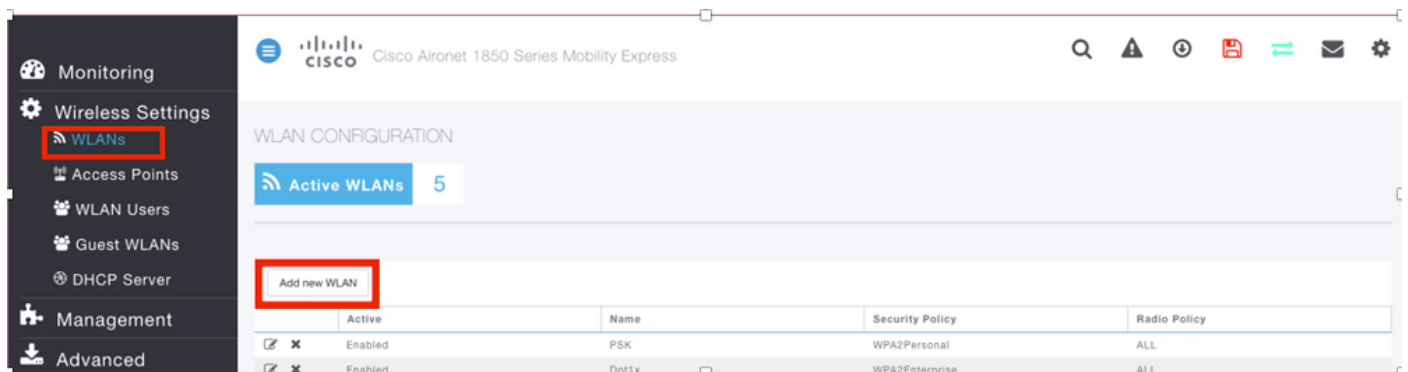
8. After the client authenticates successfully, the RADIUS server responds with an Access-challenge, which contains the "change_cipher_spec" and handshake finished message. Upon receiving this, the client verifies the hash in order to authenticate the RADIUS server. A new encryption key is dynamically derived from the secret during the TLS handshake.

9. At this point, the EAP-TLS enabled wireless client can access the wireless network.

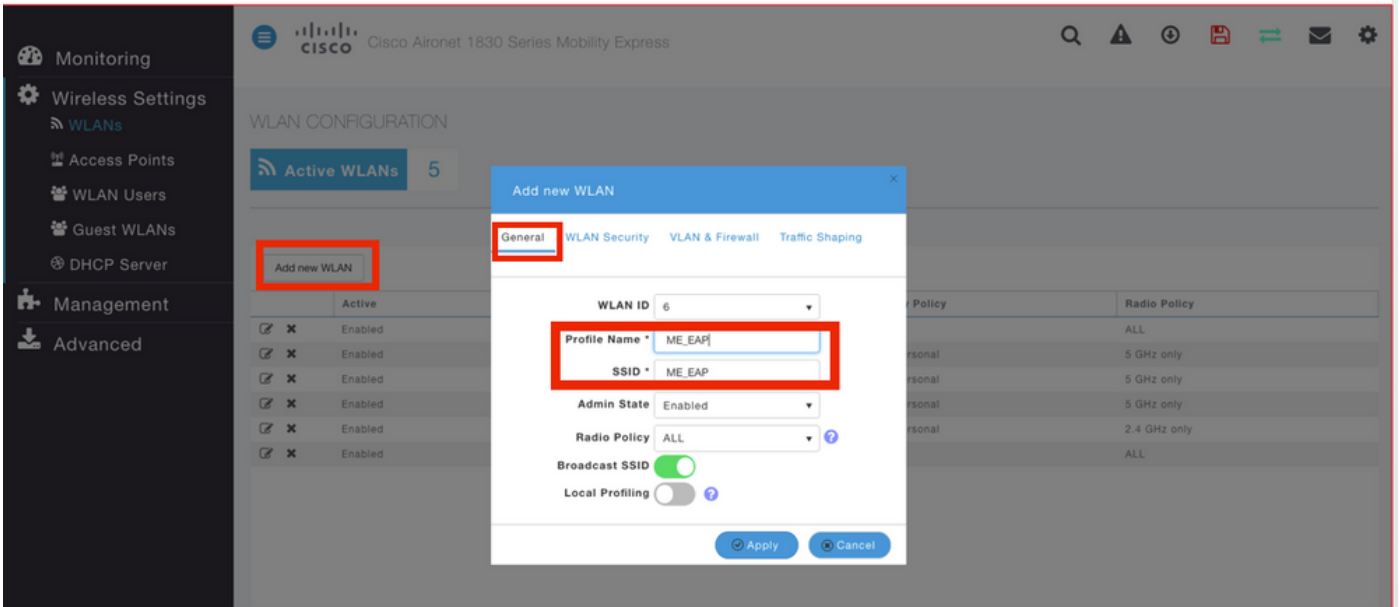
Configure

Cisco Mobility Express

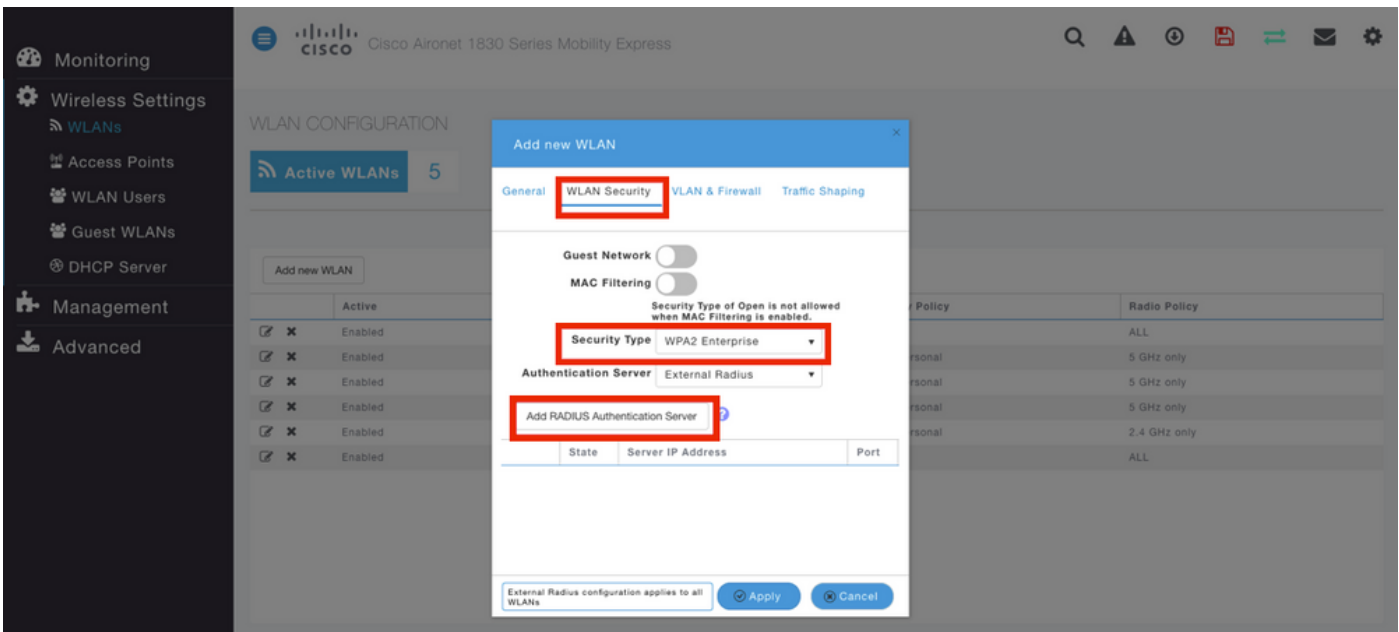
Step 1. The first step is to create a WLAN on Mobility Express. In order to create a WLAN, navigate to **WLAN > Add new WLAN** as shown in the image.



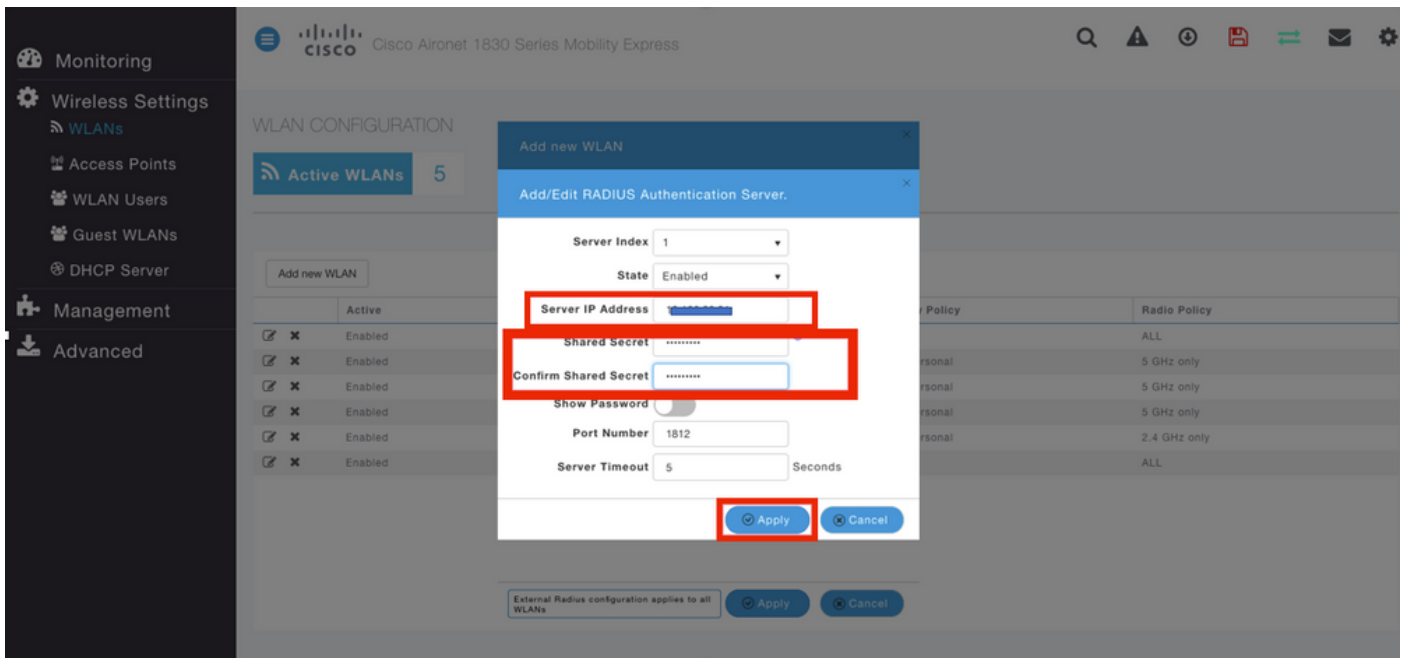
Step 2. A new popup window will appear once you click **Add new WLAN**. In order to create a Profile name, navigate to **Add new WLAN > General** as shown in the image.



Step 3. Configure the authentication type as WPA Enterprise for 802.1x and configure RADIUS Server under **Add new WLAN > WLAN Security** as shown in the image.



Step 4. Click **Add RADIUS Authentication Server** and provide the IP address of the RADIUS server and Shared Secret which must match exactly what has been configured on ISE and then click **Apply** as shown in the image.



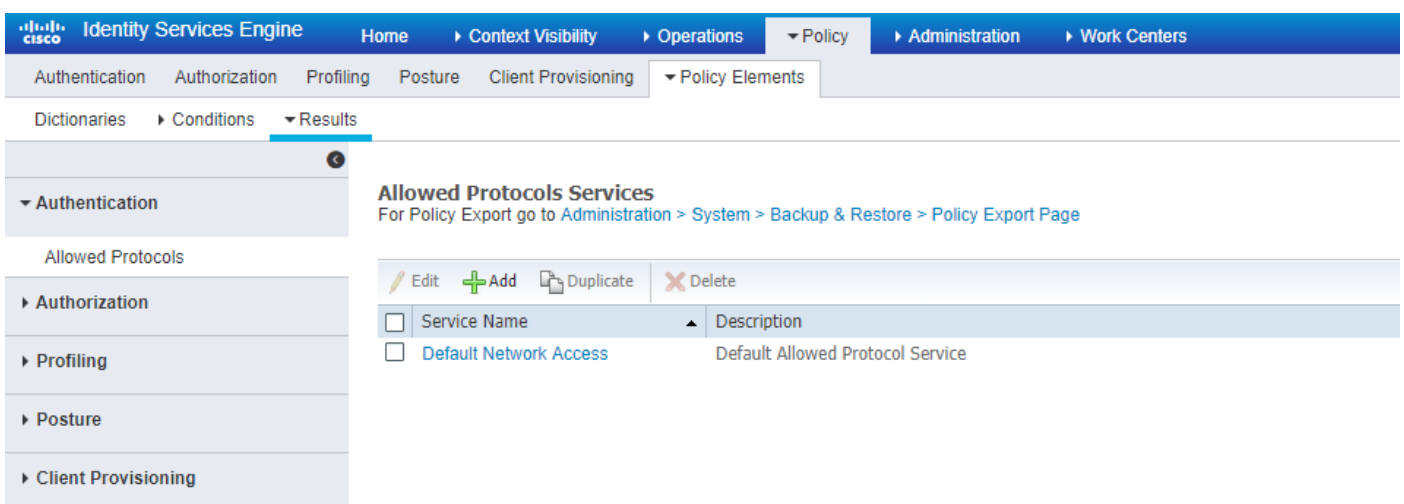
ISE with Cisco Mobility Express

EAP-TLS Settings

In order to build the policy, you need to create the allowed protocol list to use in your policy. Since a dot1x policy is written, specify the allowed EAP type based on how the policy is configured.

If you use the default, you allow most EAP types for authentication which might not be preferred if you need to lock down access to a specific EAP type.

Step 1. Navigate to **Policy > Policy Elements > Results > Authentication > Allowed Protocols** and click **Add** as shown in the image.



Step 2. On this Allowed Protocol list, you can enter the name for the list. In this case, **Allow EAP-TLS** box is checked and other boxes are unchecked as shown in the image.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionaries > Conditions > Results

Allowed Protocols Services List > **New Allowed Protocols Service**

Allowed Protocols

Name

Description

Allowed Protocols

- Authentication Bypass
 - Process Host Lookup *(?)*
- Authentication Protocols
 - Allow PAP/ASCII
 - Allow CHAP
 - Allow MS-CHAPv1
 - Allow MS-CHAPv2
 - Allow EAP-MD5
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy *(?)*
 - Enable Stateless Session Resume
 - Session ticket time to live
 - Proactive session ticket update will occur after % of Time To Live has expired
 - Allow LEAP
 - Allow PEAP
 - PEAP Inner Methods
 - Allow EAP-MS-CHAPv2
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-GTC
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy *(?)*
 - Require cryptobinding TLV *(?)*

Mobility Express Settings on ISE

Step 1. Open ISE console and navigate to **Administration > Network Resources > Network Devices > Add** as shown in the image.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Threat Centric NAC

Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services

Network devices

Default Device

Network Devices

Selected 0 | Total 1

Name	IP/Mask	Profile Name	Location	Type	Description

Step 2. Enter the information as shown in the image.

The screenshot shows the 'New Network Device' configuration page in Cisco ISE. The 'RADIUS Authentication Settings' section is expanded, and the 'Shared Secret' field is highlighted with a red box. Below the main form, there are three expandable sections: 'TACACS Authentication Settings', 'SNMP Settings', and 'Advanced TrustSec Settings'. At the bottom, the 'Submit' button is highlighted with a red box.

Trust Certificate on ISE

Step 1. Navigate to **Administration > System > Certificates > Certificate Management > Trusted certificates**.

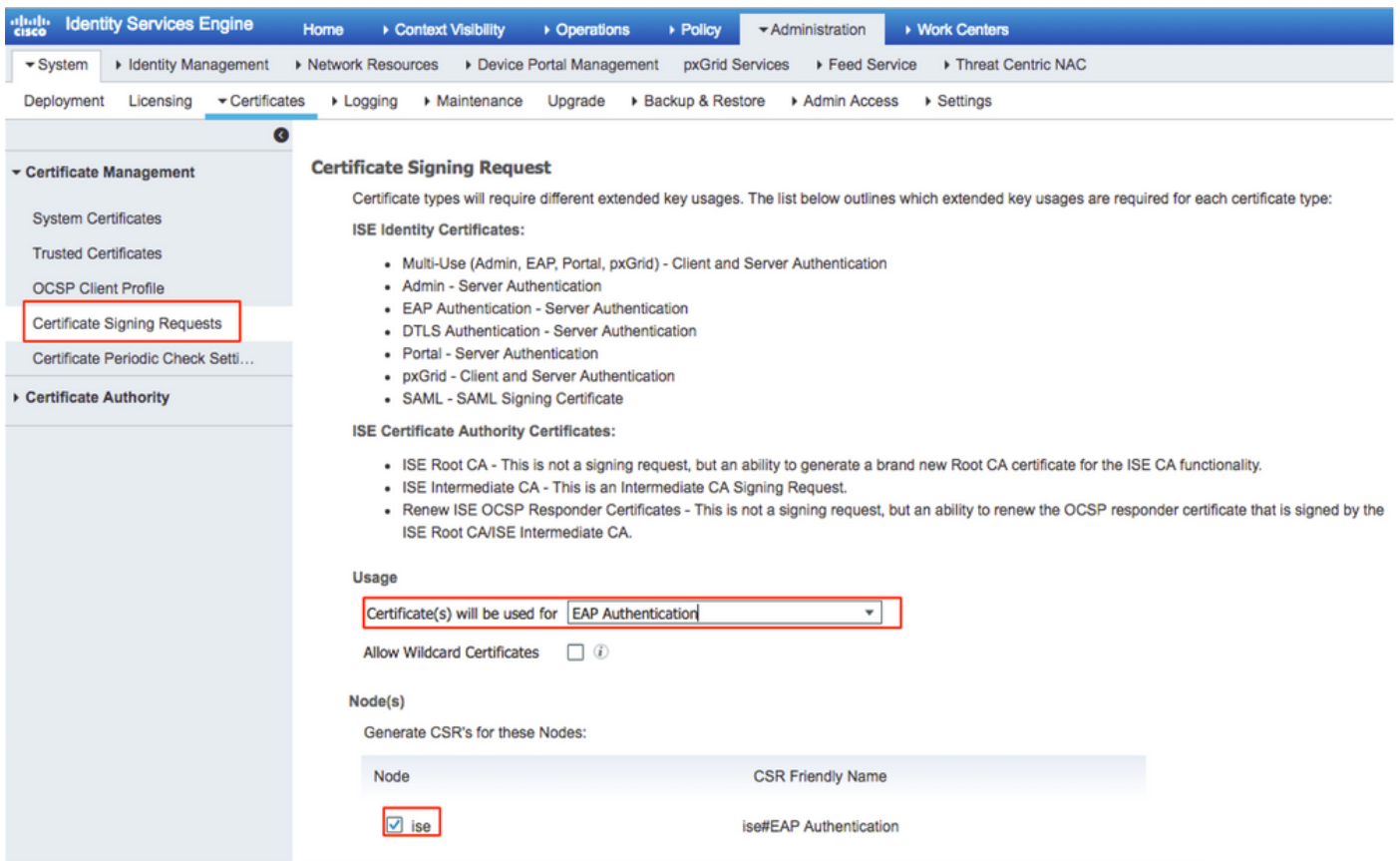
Click **Import** in order to import a certificate to ISE. Once you add a WLC and create a user on ISE, you need to do the most important part of EAP-TLS that is to trust the certificate on ISE. For that, you need to generate CSR.

Step 2. Navigate to **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR)** as shown in the image.

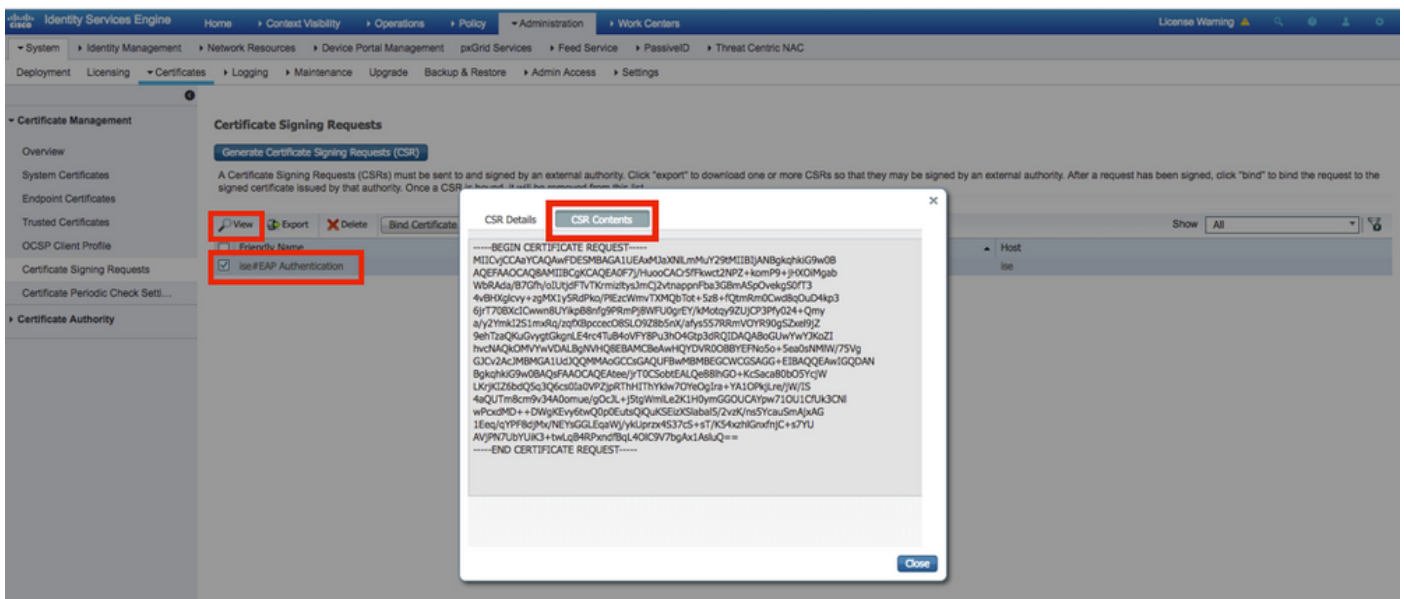
The screenshot shows the 'Generate Certificate Signing Requests (CSR)' page in Cisco ISE. The page has a table with the following data:

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input type="checkbox"/>	ise#EAP Authentication	CN=ise.c.com	2048	ise	Wed, 11 Jul 2018

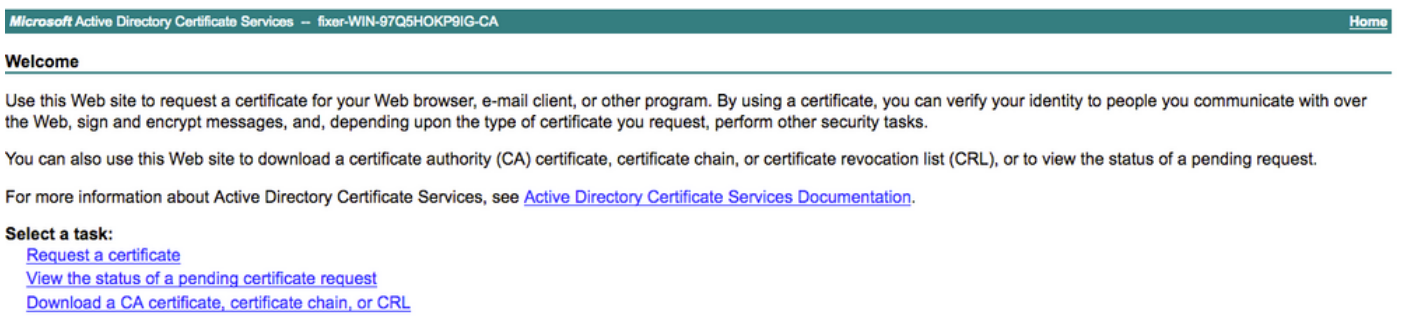
Step 3. In order to generate CSR, navigate to **Usage** and from the **Certificate(s) will be used for** drop down options select **EAP Authentication** as shown in the image.



Step 4. The CSR generated on ISE can be viewed. Click **View** as shown in the image.



Step 5. Once CSR is generated, browse for CA server and click **Request a certificate** as shown in the image:



Step 6. Once you request a certificate, you get options for **User Certificate** and **advanced certificate request**, click **advanced certificate request** as shown in the image.

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#)

Step 7. Paste the CSR generated in **Base-64 encoded certificate request**. From the **Certificate Template**: drop down option, choose **Web Server** and click **Submit** as shown in the image.

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

Additional Attributes:
Attributes:

Step 8. Once you click **Submit**, you get the option to select the type of certificate, select **Base-64 encoded** and click **Download certificate chain** as shown in the image.

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Certificate Issued

The certificate you requested was issued to you.

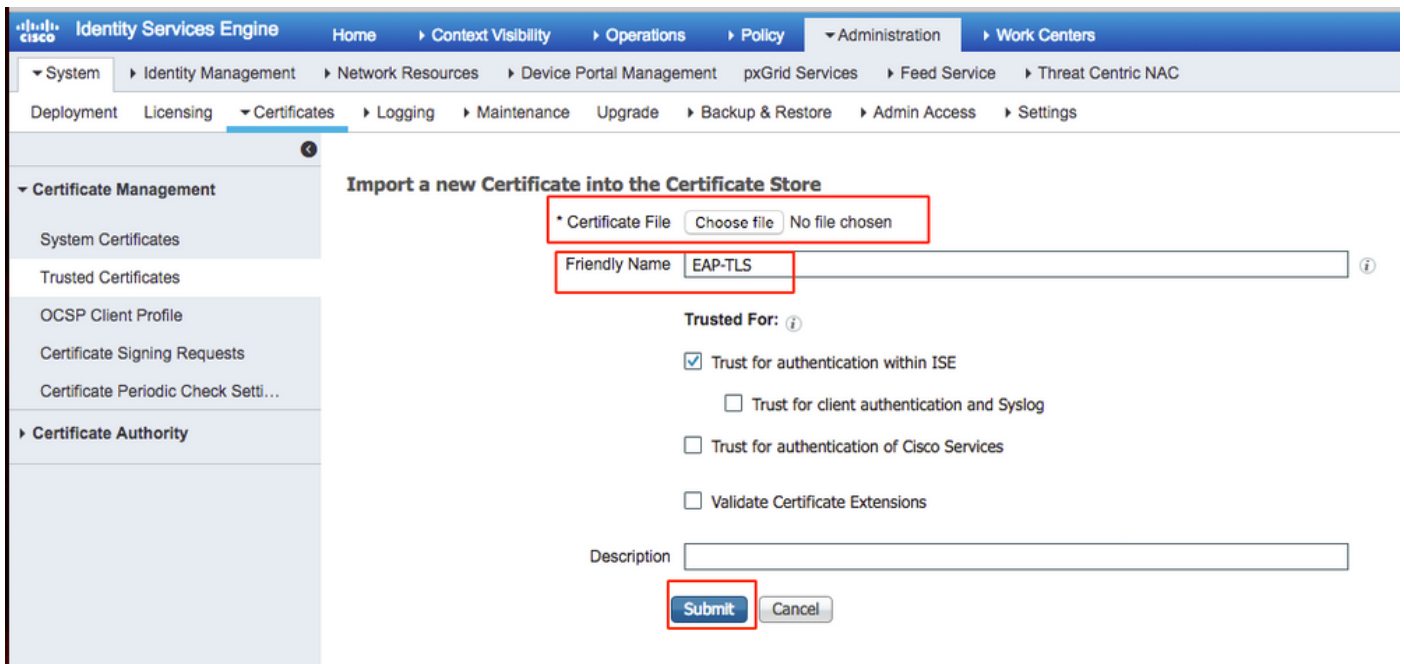
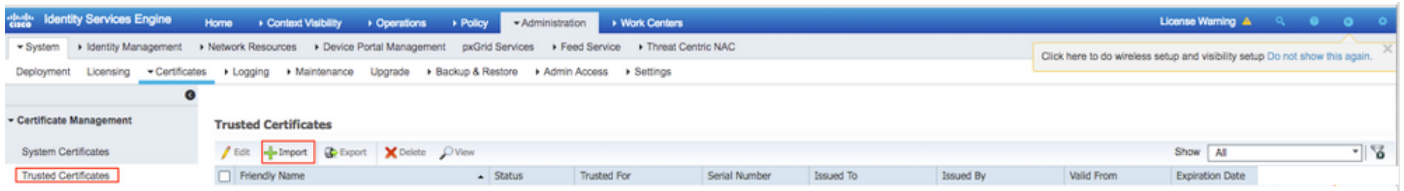
DER encoded or Base 64 encoded



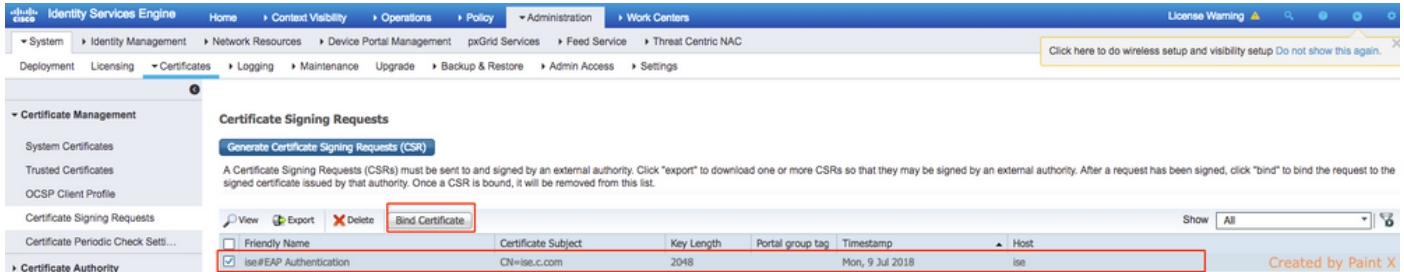
[Download certificate](#)

[Download certificate chain](#)

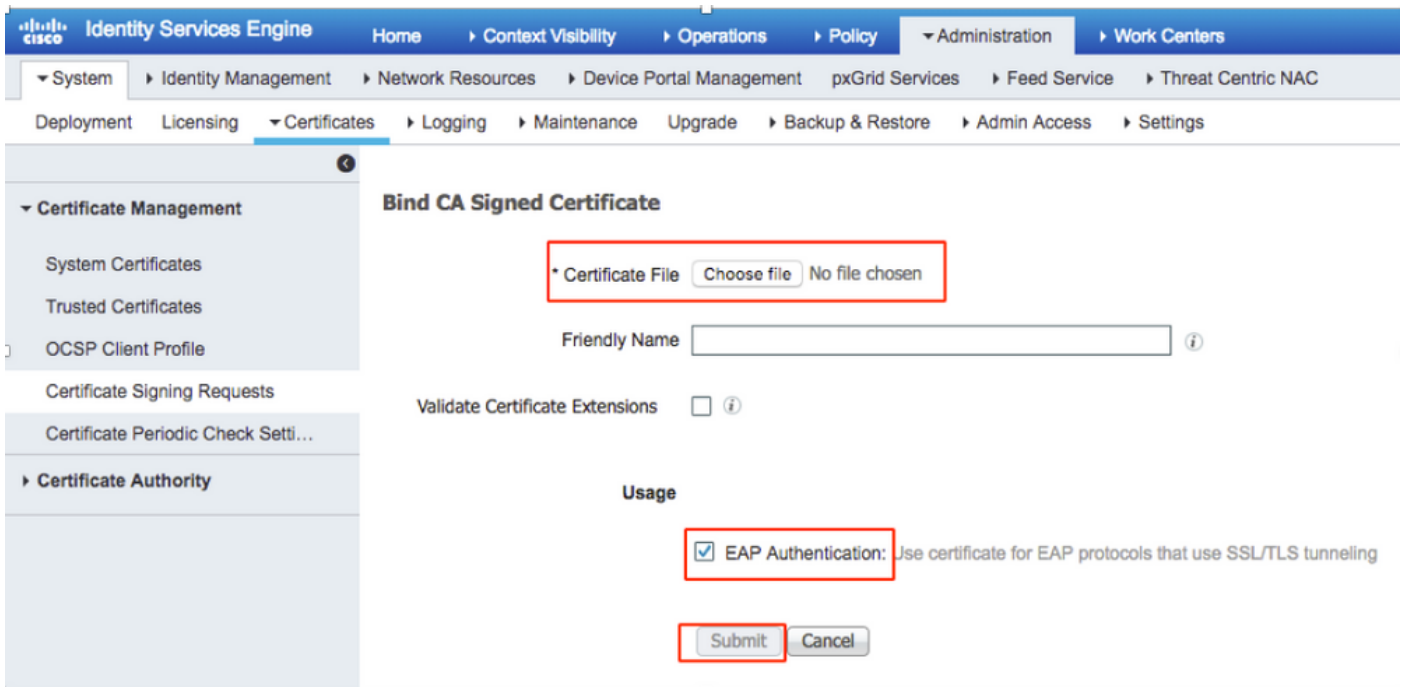
Step 9. The certificate download is completed for the ISE server. You can extract the certificate, the certificate will contain two certificates, one root certificate and other intermediate. The root certificate can be imported under **Administration > Certificates > Trusted certificates > Import** as shown in the images.



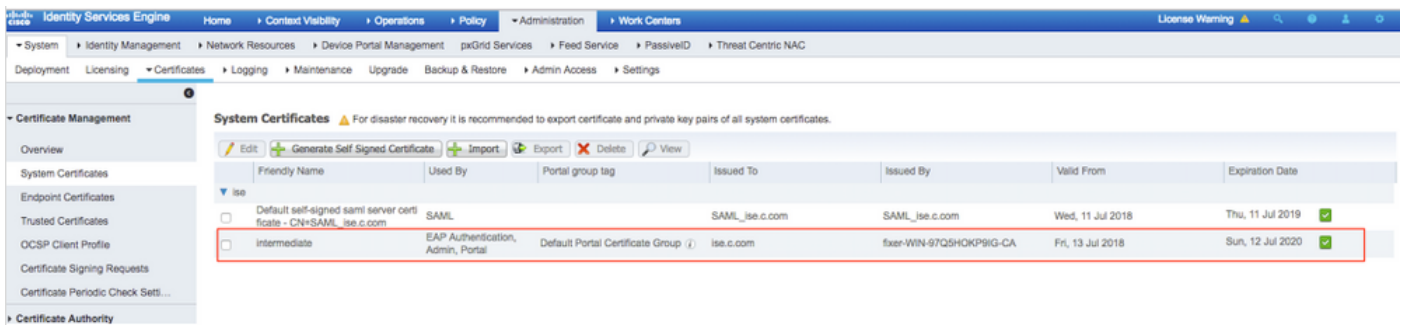
Step 10. Once you click **Submit**, the certificate is added to the trusted certificate list. Also, the intermediate certificate is needed in order to bind with CSR as shown in the image.



Step 11. Once you click on **Bind certificate**, there is an option to choose the certificate file saved in your desktop. Browse to the intermediate certificate and click **Submit** as shown in the image.



Step 12. In order to view the certificate, navigate to **Administration > Certificates > System Certificates** as shown in the image.



Client for EAP-TLS

Download User Certificate on Client Machine (Windows Desktop)

Step 1. In order to authenticate a wireless user through EAP-TLS, you have to generate a client certificate. Connect your Windows computer to the network so that you can access the server. Open a web browser and enter this address: <https://server ip addr/certsrv--->

Step 2. Note that the CA must be the same with which the certificate was downloaded for ISE.

For this, you need to browse for the same CA server that you used to download the certificate for server. On the same CA, click **Request a certificate** as previously done, however this time you need to select **User** as the Certificate Template as shown in the image.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIspJry  
aF412aLpmDFp1PfVZ3VaP6Oa/mej3IXh0RFxBUII  
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxF1j3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

Attributes:

Submit >

Step 3. Then, click **download certificate chain** as was done previously for server.

Once you get the certificates, follow these steps in order to import the certificate on windows laptop.

Step 4. In order to import the certificate, you need to access it from the Microsoft Management Console (MMC).

1. In order to open the MMC navigate to **Start > Run > MMC**.
2. Navigate to **File > Add / Remove Snap In**
3. Double Click **Certificates**.
4. Select **Computer Account**.
5. Select **Local Computer > Finish**
6. Click **OK** in order to exit the Snap-In window.
7. Click **[+]** next to **Certificates > Personal > Certificates**.
8. Right click on **Certificates** and select **All Tasks > Import**.
9. Click **Next**.
10. Click **Browse**.
11. Select the **.cer, .crt, or .pfx** you would like to import.

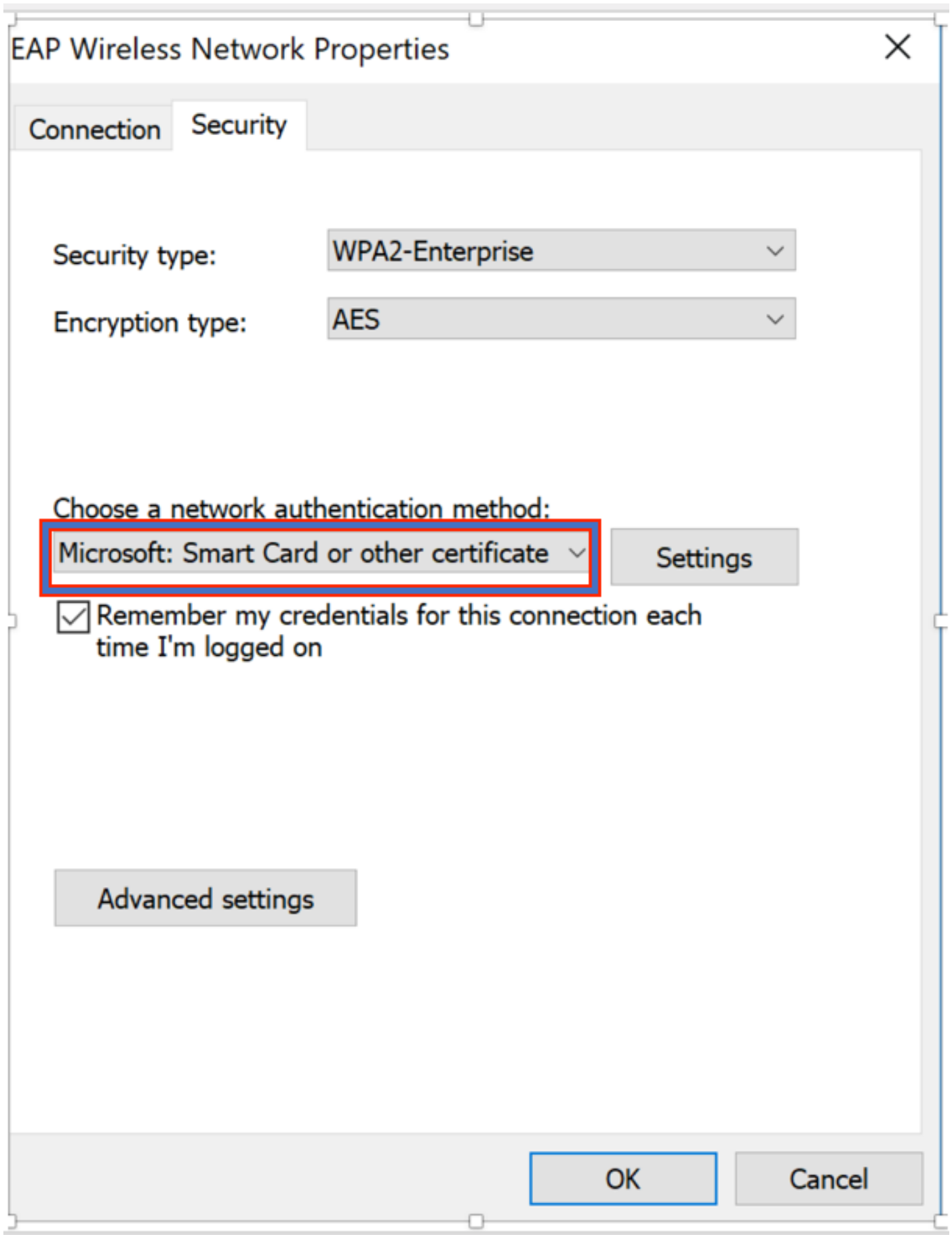
12. Click **Open**.
13. Click **Next**.
14. Select **Automatically select the certificate store based on the type of certificate**.
15. Click **Finish & OK**

Once import of certificate is done, you need to configure your wireless client (windows desktop in this example) for EAP-TLS.

Wireless Profile for EAP-TLS

Step 1. Change the wireless profile that was created earlier for Protected Extensible Authentication Protocol (PEAP) in order to use EAP-TLS instead. Click **EAP Wireless Profile**.

Step 2. Select **Microsoft: Smart Card or other certificate** and click **OK** as shown in the image.



Step 3. Click **Settings** and select the root certificate issued from CA server as shown in the image.

Smart Card or other Certificate Properties

When connecting:

Use my smart card

Use a certificate on this computer

Advanced

Use simple certificate selection (Recommended)

Verify the server's identity by validating the certificate

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

Trusted Root Certification Authorities:

Entrust.net Certification Authority (2048)

Equifax Secure Certificate Authority

fixer-WIN-97Q5HOKP9IG-CA

GeoTrust Global CA

GeoTrust Primary Certification Authority

GeoTrust Primary Certification Authority - G3

GlobalSign

GlobalSign

GlobalSign Root CA



View Certificate

Step 4. Click **Advanced Settings** and select **User or computer authentication** from the 802.1x settings tab as shown in the image.

Advanced settings

802.1X settings

802.11 settings

Specify authentication mode:

User or computer authentication

Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

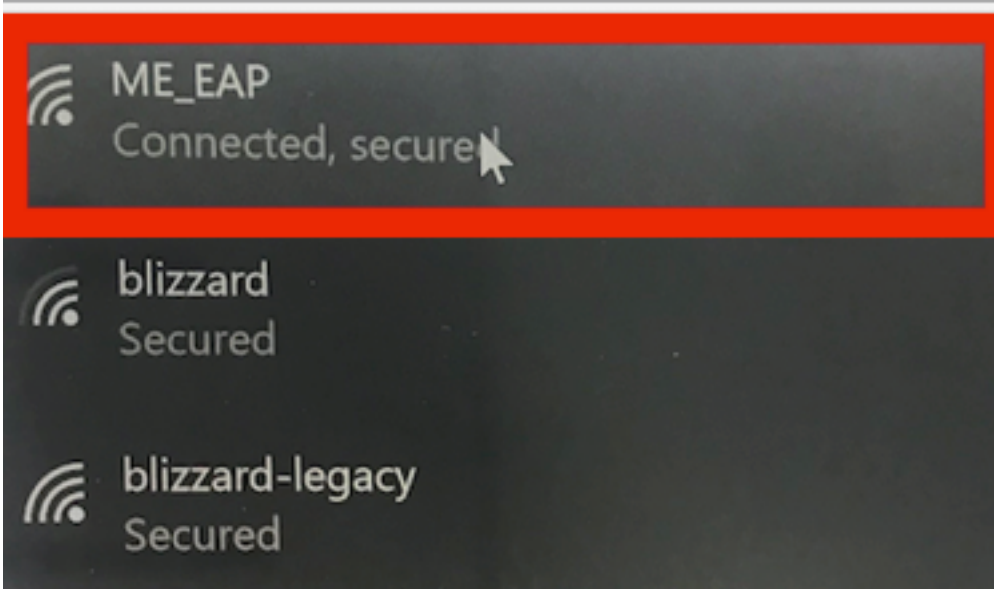
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

Step 5. Now, try to connect again to the wireless network, select the correct profile (EAP in this example) and **Connect**. You are connected to the wireless network as shown in the image.

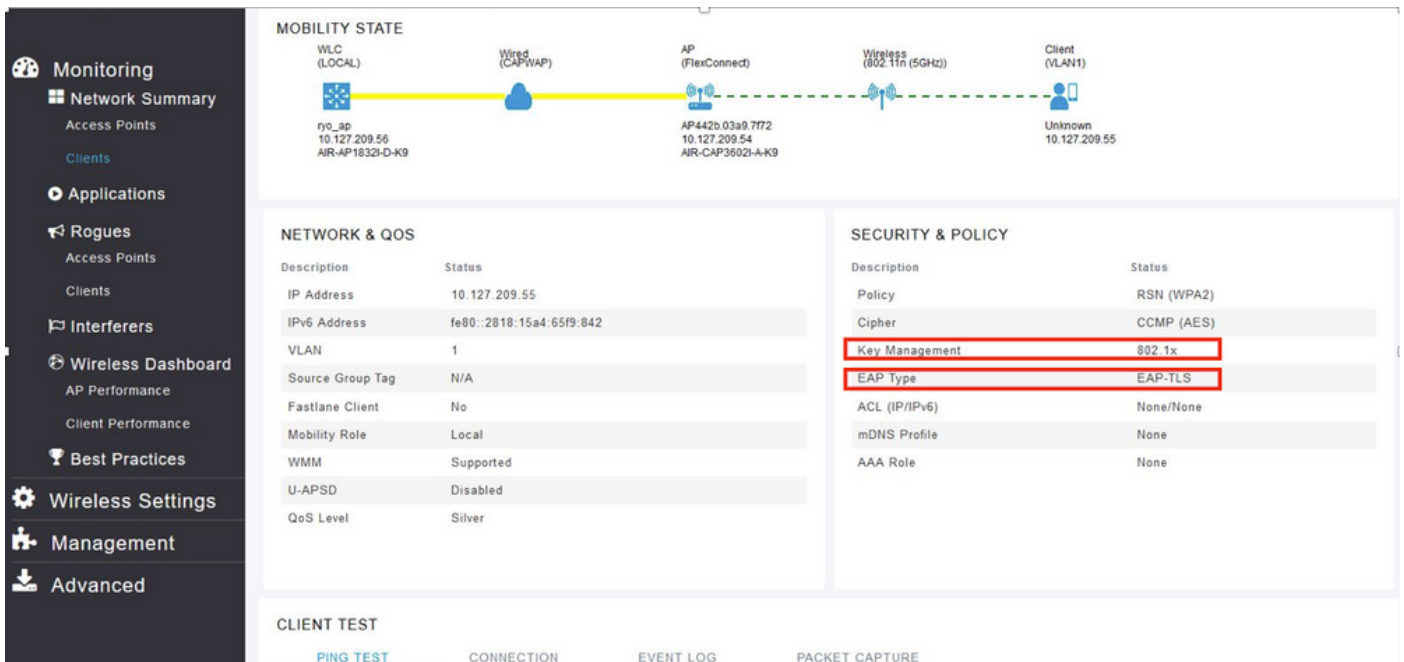


Verify

Use this section in order to confirm that your configuration works properly.

Step 1. The client EAP-Type must be EAP-TLS. This means that the client has completed authentication, with the use of EAP-TLS, obtained IP address and is ready to pass the traffic as shown in the images.

The screenshot shows a network management interface with a sidebar on the left and a main content area. The sidebar includes sections for Monitoring, Applications, Rogues, Interferers, Wireless Dashboard, Best Practices, Wireless Settings, Management, and Advanced. The main content area is titled 'CLIENT VIEW' and displays details for a client named 'ME_EAP'. The 'GENERAL' section shows the User Name as 'Administrator', Host Name as 'Unknown', MAC Address as '34:02:86:96:2f:b7', Uptime as 'Associated since 37 Seconds', and SSID as 'ME_EAP' (highlighted with a red box). The AP Name is 'AP442b.03a9.7f72 (Ch 56)'. The 'CONNECTIVITY' section shows a flowchart with five steps: Start, Association, Authentication, DHCP, and Online, all marked as successful. The 'TOP APPLICATIONS' section shows 'No Data Available!'. The 'MOBILITY STATE' section shows a diagram of the network path: WLC (LOCAL) -> Wired (CAP-WAP) -> AP (FlexConnect) -> Wireless (802.11n (5GHz)) -> Client (VLAN1).






Step 2. Here are the client detail from CLI of the controller (output clipped):

```
(Cisco Controller) >show client detail 34:02:86:96:2f:b7
Client MAC Address..... 34:02:86:96:2f:b7
Client Username ..... Administrator
AP MAC Address..... c8:f9:f9:83:47:b0
AP Name..... AP442b.03a9.7f72
AP radio slot Id..... 1
Client State..... Associated
Client User Group..... Administrator
Client NAC OOB State..... Access
Wireless LAN Id..... 6
Wireless LAN Network Name (SSID)..... ME_EAP
Wireless LAN Profile Name..... ME_EAP
Hotspot (802.11u)..... Not Supported
BSSID..... c8:f9:f9:83:47:ba
Connected For ..... 18 secs
Channel..... 56
IP Address..... 10.127.209.55
Gateway Address..... 10.127.209.49
Netmask..... 255.255.255.240
IPv6 Address..... fe80::2818:15a4:65f9:842
--More-- or (q)uit
Security Policy Completed..... Yes
Policy Manager State..... RUN
Policy Type..... WPA2
Authentication Key Management..... 802.1x
Encryption Cipher..... CCMP-128 (AES)
Protected Management Frame ..... No
Management Frame Protection..... No
EAP Type..... EAP-TLS
```

Step 3. On ISE, navigate to **Context Visibility > End Points > Attributes** as shown in the images.

Endpoints > 34:02:86:96:2F:B7

34:02:86:96:2F:B7   



MAC Address: 34:02:86:96:2F:B7
 Username: Administrator@fixer.com
 Endpoint Profile: Intel-Device
 Current IP Address:
 Location:

Attributes Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment	false
Endpoint Policy	Intel-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

Custom Attributes

Filter 

Attribute Name	Attribute Value
<input type="text" value="Attribute Name"/>	<input type="text" value="Attribute Value"/>

No data found. Add custom attributes here.

Other Attributes

AAA-Server	ise
AKI	88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd
Airespace-Wlan-Id	6
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509_PKI
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access

BYODRegistration	Unknown
Called-Station-ID	c8-f9-f9-83-47-b0:ME_EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	344
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.127.209.56
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	21
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.11
FailureReason	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA,DC=fixer,DC=cc
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com
Key Usage	0, 2
Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7

MatchedPolicy	Intel-Device
MessageCode	5411
NAS-IP-Address	10.127.209.56
NAS-Identifier	ryo_ap
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	ryo_ap
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	Drop
SSID	c8-f9-f9-83-47-b0:ME_EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.