

Understand and Configure EAP-TLS with a WLC and ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[EAP-TLS Flow](#)

[Steps in EAP-TLS Flow](#)

[Configure](#)

[Cisco Wireless LAN Controller](#)

[ISE with Cisco WLC](#)

[EAP-TLS Settings](#)

[WLC Settings on ISE](#)

[Create New User 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 and Extensible Authentication Protocol EAP-TLS.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 802.1X authentication process
- Certificates

Components Used

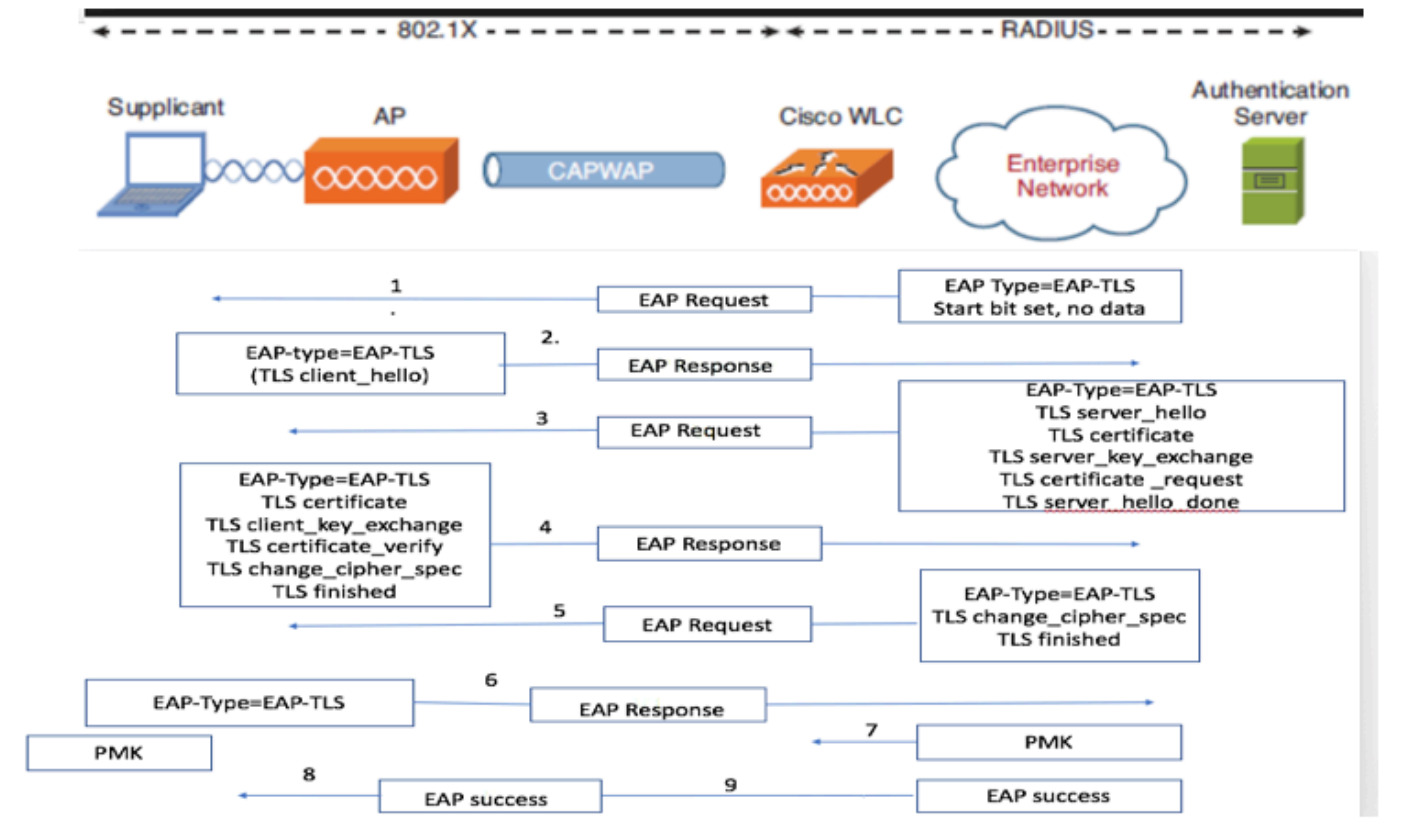
The information in this document is based on these software and hardware versions:

- WLC 3504 version 8.10
- Identity Services Engine (ISE) version 2.7

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). AP does not permit the client to send any data at this point and sends an authentication request. The supplicant then responds with an EAP-Response Identity. The WLC then communicates the user-id information to the Authentication Server. RADIUS server responds back to the client with an EAP-TLS Start Packet. The EAP-TLS conversation starts at this point.
2. 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
3. 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.

4. 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

5. After the client authenticates successfully, the RADIUS server responds with an Access-challenge, which contains the change_cipher_spec and handshake finished message.

6. When it receives this, the client verifies the hash in order to authenticate the radius server.

7. A new encryption key is dynamically derived from the secret during the TLS handshake.

8/9. EAP-Success is finally sent from server to authenticator which then is passed to the supplicant.

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

Configure

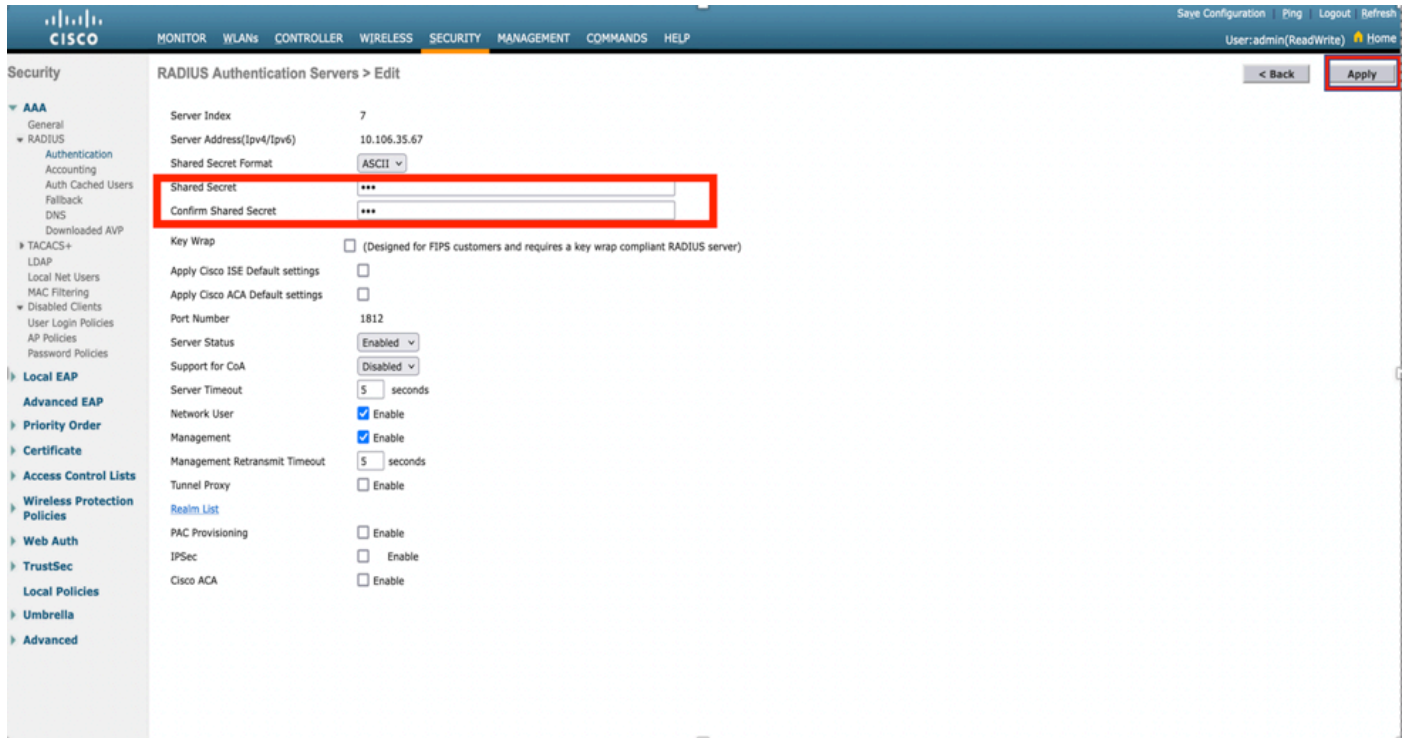
Cisco Wireless LAN Controller

Step 1. The first step is to configure the RADIUS server on the Cisco WLC. In order to add a RADIUS server, navigate to **Security > RADIUS > Authentication**. Click **New** as shown in the image.

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The 'Security' tab is selected, and the 'RADIUS Authentication Servers' page is displayed. The 'Authentication' sub-tab is active. The 'New...' button is highlighted in red. The table below shows the configuration for six RADIUS servers.

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	138.77.0.84	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	138.77.0.83	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3	138.77.97.20	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4	138.77.97.21	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5	* 172.27.1.71	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	6	* 10.100.120.41	1812	Disabled	Enabled

Step 2. Here, you need to enter the IP address and the shared secret <password> that is used in order to validate the WLC on the ISE. Click **Apply** in order to continue as shown in the image.



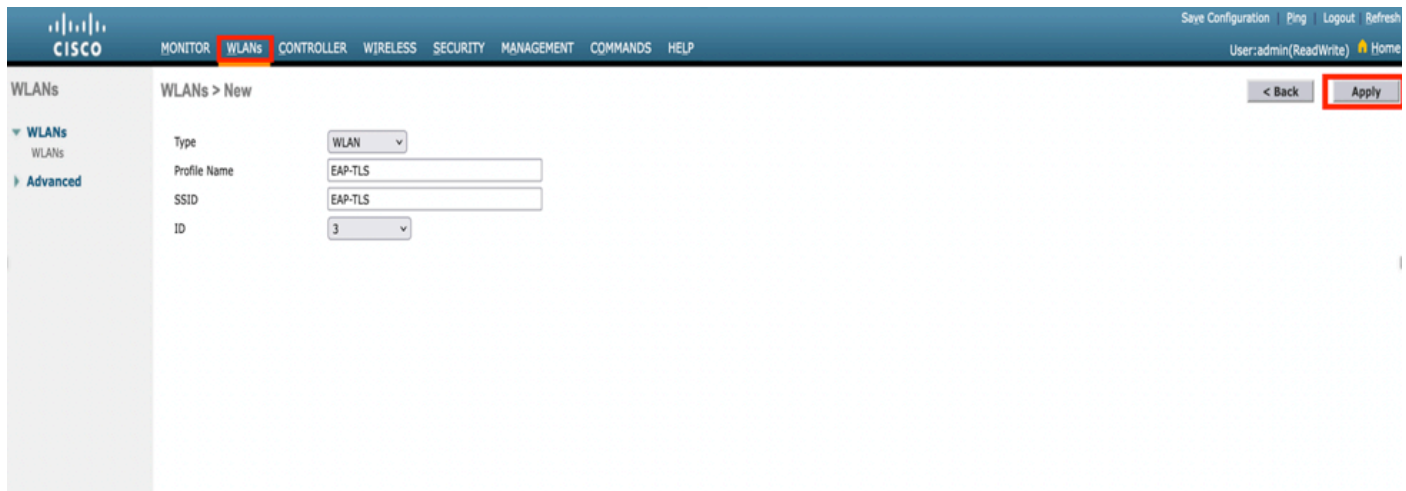
Step 3. Create WLAN for RADIUS Authentication.

Now, you can create a new WLAN and configure it to use WPA-enterprise mode, so it can use RADIUS for authentication.

Step 4. Select **WLANs** from the main menu, choose **Create New** and click **Go** as shown in the image.

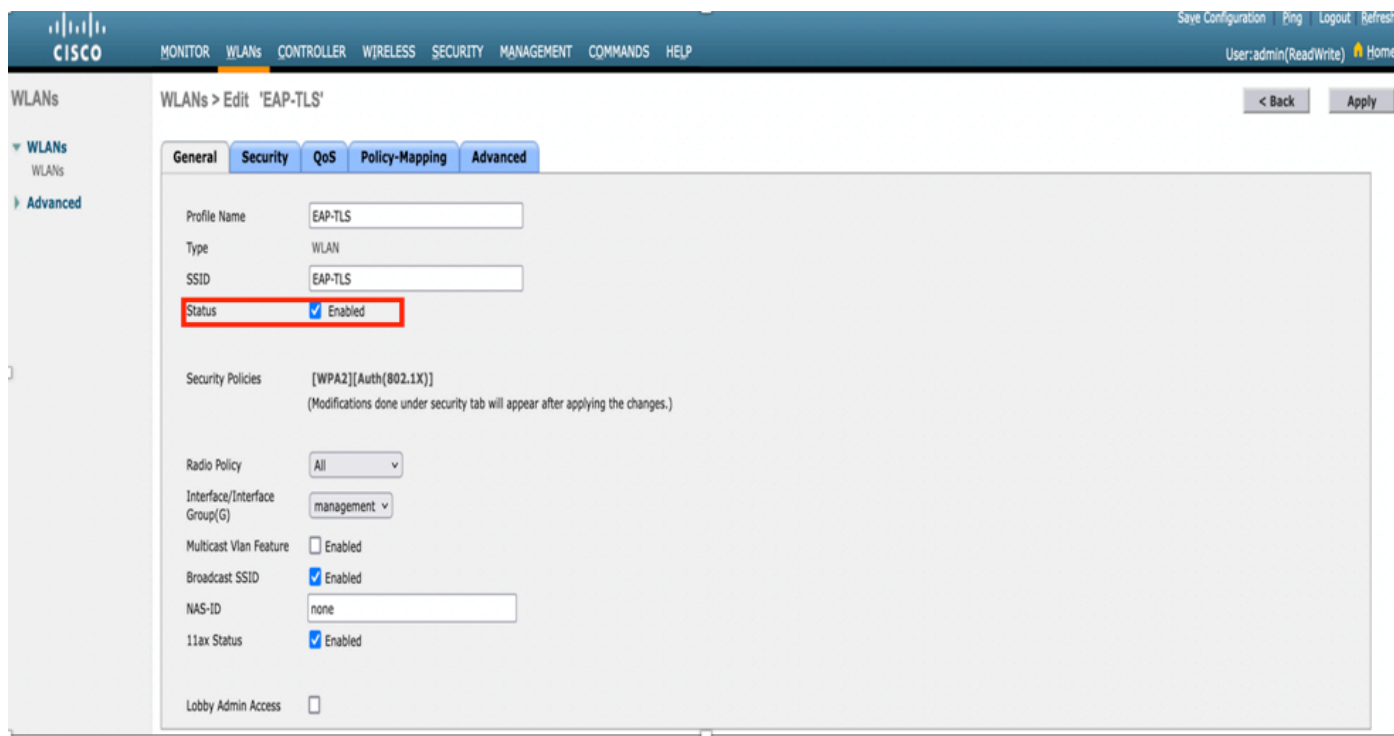


Step 5. Name the new WLAN **EAP-TLS**. Click **Apply** in order to continue as shown in the image.

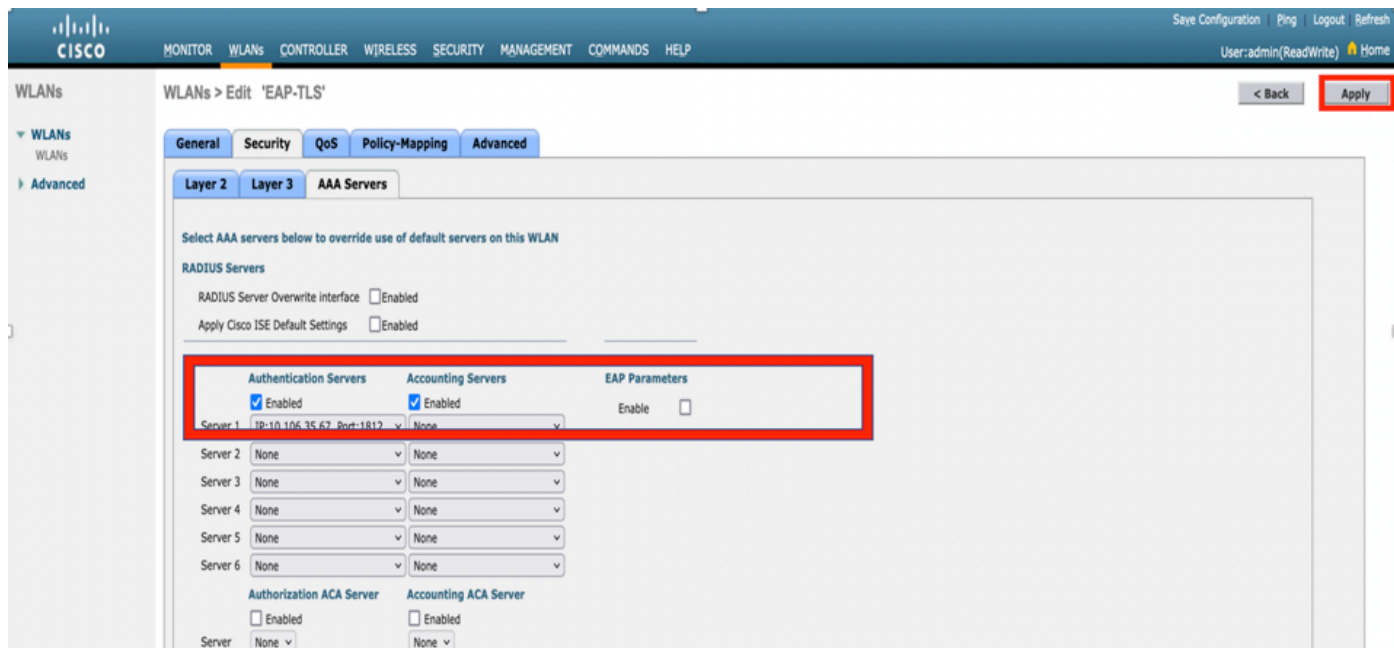


Step 6. Click **General** and ensure that the Status is **Enabled**. The default Security Policies is 802.1X

authentication and WPA2 as shown in the image.



Step 7. Now, navigate to **Security > AAA Servers** tab, select the RADIUS server that you just configured as shown in the image.





Note: It is a good idea to verify that you can reach the RADIUS server from the WLC before you continue. RADIUS uses UDP port 1812 (for authentication), so you need to ensure that this traffic does not get blocked anywhere in the network.

ISE with Cisco WLC

EAP-TLS Settings

In order to build the policy, you need to create the allowed protocol list to use in our 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 are not 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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit Add Duplicate Delete

<input type="checkbox"/>	Service Name	Description
<input type="checkbox"/>	Default Network Access	Default Allowed Protocol Service

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 *(?)*

WLC 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 > jpf@ed Services > Feed Service > Threat Center NAC

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

Click here to do wireless setup and visibility setup. Do not show this again.

Network devices

Default Device

Device Security Settings

Network Devices

ADD Duplicate Import Export Generate PAK Delete

Name	IP Mask	Profile Name	Location	Type	Description

Show: All

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

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for a new network device. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC. The left sidebar shows 'Network Devices' with sub-items: Default Device and Device Security Settings. The main content area is titled 'Network Devices List > New Network Device'. The configuration fields are as follows:

- Name: Bharti-WLC
- Description: (empty)
- IP Address: 10.106.35.67 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (Set To Default)
- IPSEC: Is IPSEC Device (Set To Default)
- Device Type: All Device Types (Set To Default)
- RADIUS Authentication Settings (checked):
 - RADIUS UDP Settings:
 - Protocol: RADIUS
 - Shared Secret: (masked with asterisks, highlighted with a red box) (Show)
 - Use Second Shared Secret: (unchecked)
 - CoA Port: (empty) (Set To Default)
 - RADIUS DTLS Settings: (empty)

Create New User on ISE

Step 1. Navigate to **Administration > Identity Management > Identities > Users > Add** as shown in the image.

The screenshot shows the Cisco Identity Services Engine (ISE) 'Add User' page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Identity Management > Identities > Users > Add. The left sidebar shows 'Users' with sub-items: Latest Manual Network Scan Results and Network Access Users. The main content area is titled 'Add User'. The page shows a table with columns for Status, Name, Description, First Name, Last Name, Email Address, and User Identity Groups. The 'Add' button is highlighted.

Step 2. Enter the information 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 | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name:

Status: Enabled

Email:

Passwords

Password Type:

Password:
 Re-Enter Password:
 ⓘ

* Login Password:
 ⓘ

Enable Password:
 ⓘ

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login:

Account Disable Policy

Disable account if date exceeds: (yyyy-mm-dd)

User Groups

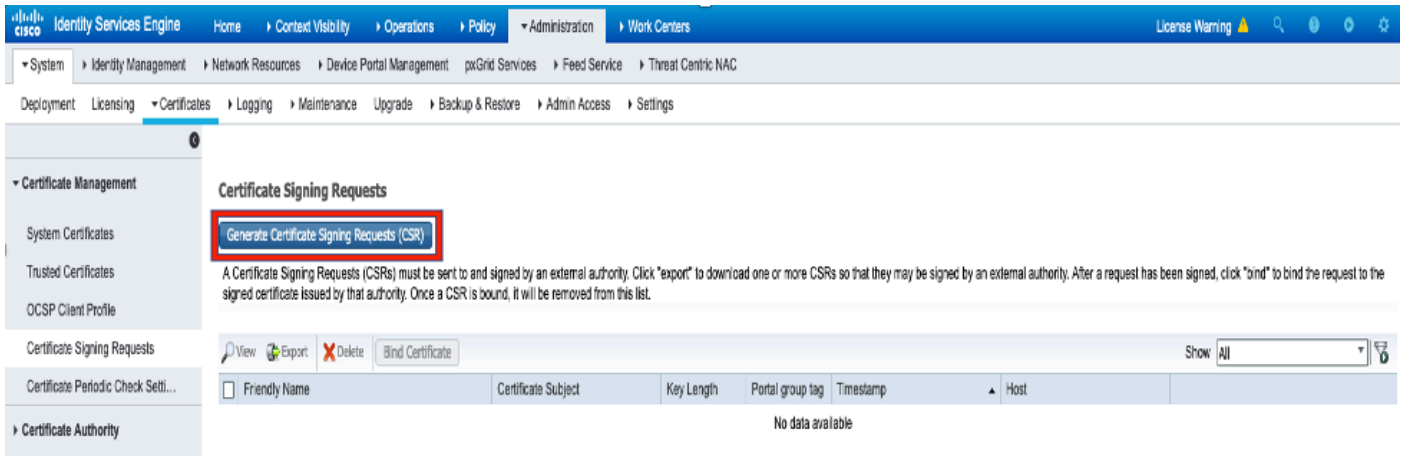
Select an item

Trust Certificate on ISE

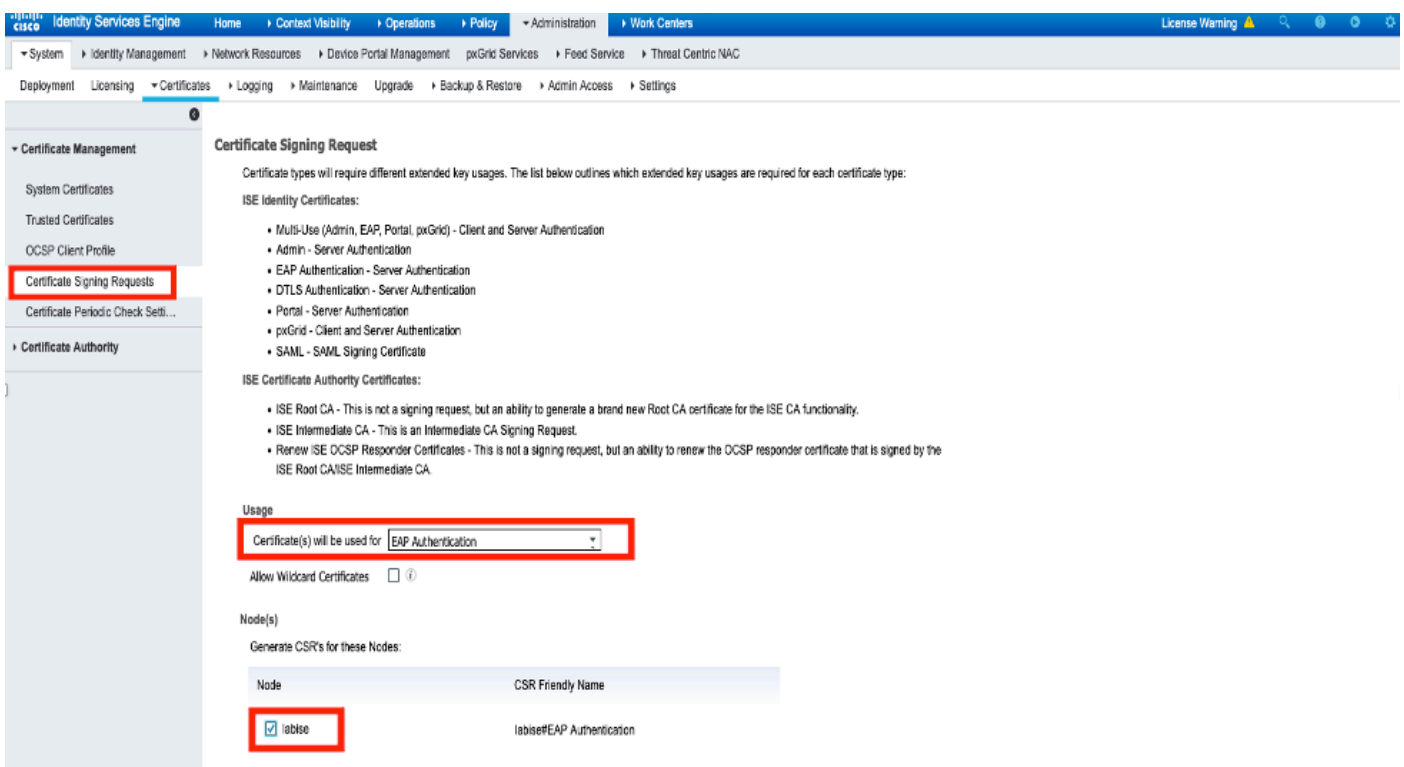
Step 1. Navigate to **Administration > System > Certificates > Certificate Management > Trusted certificates**.

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 we need to generate CSR.

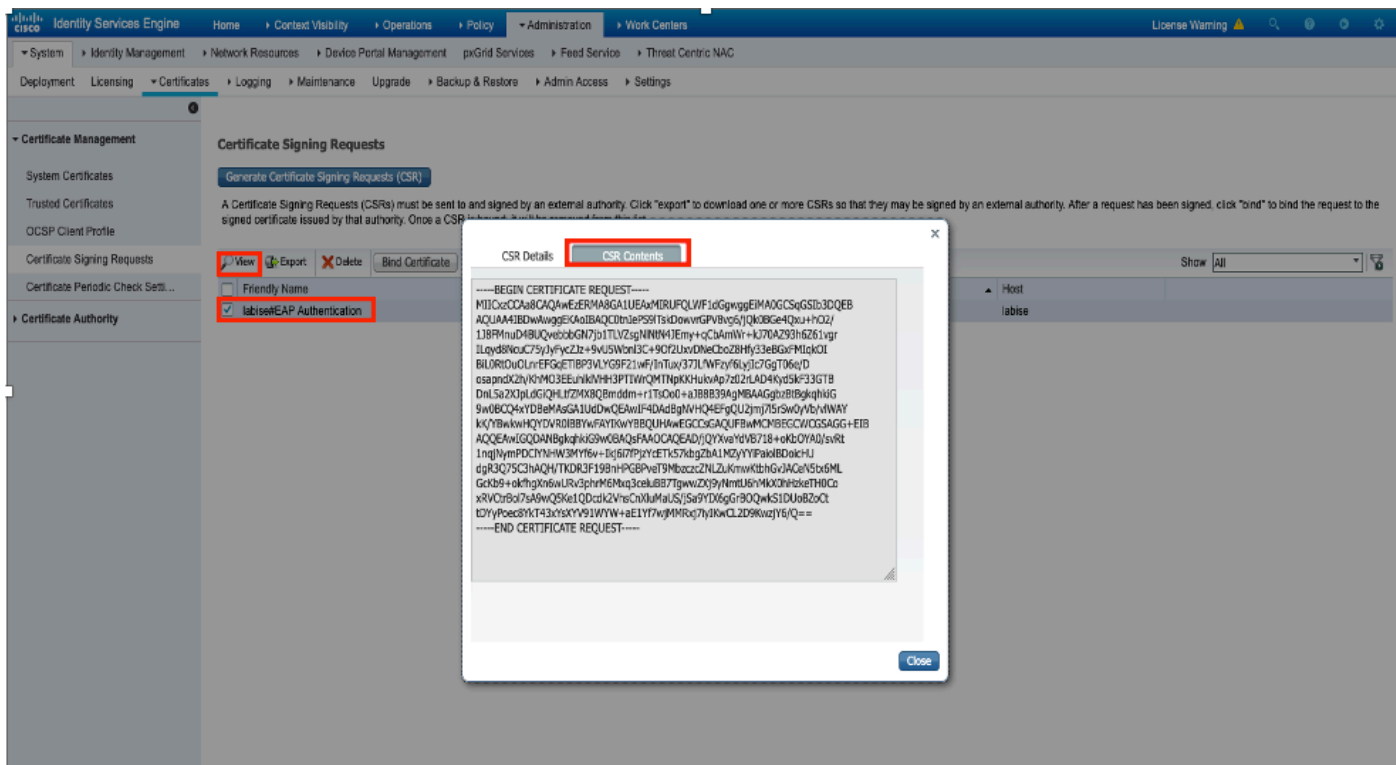
Step 2. Navigate to **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR)** as shown in the image.



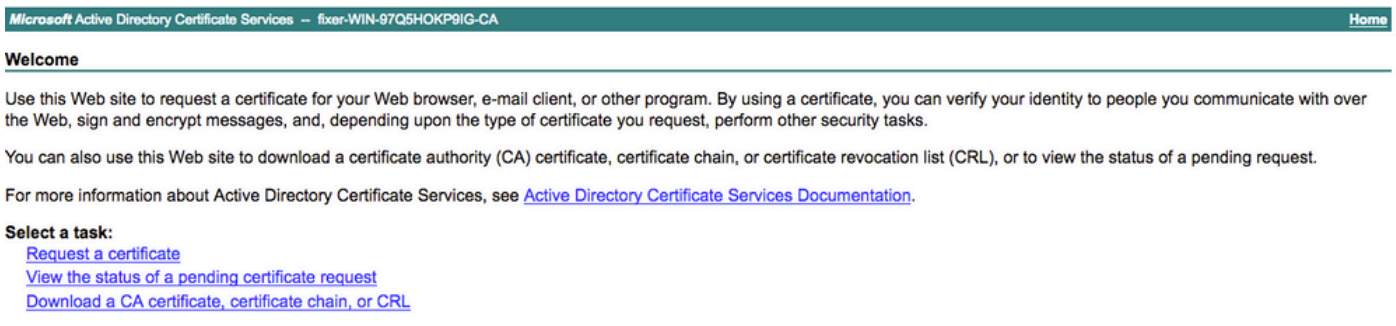
Step 3. In order to generate CSR, navigate to **Usage** and from the **Certificate(s) are used for** drop down options select **EAP Authentication** as shown in the image.



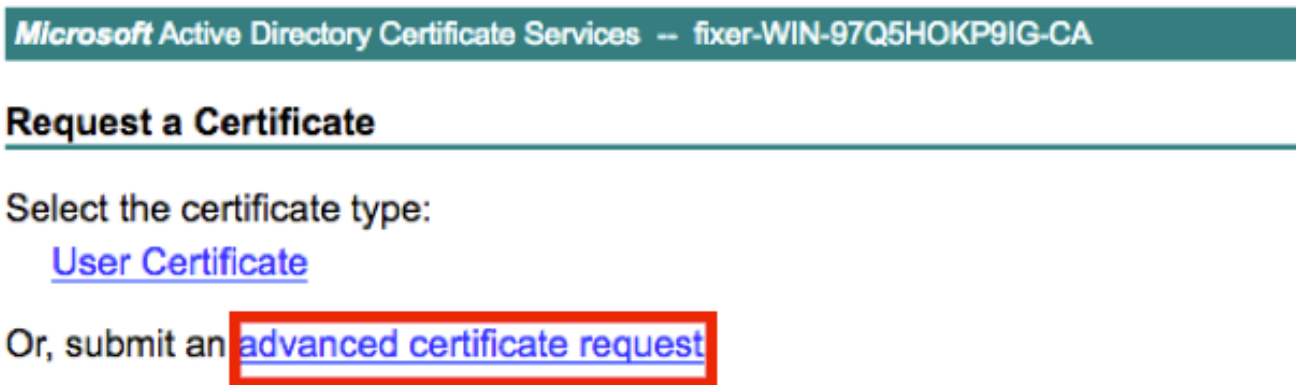
Step 4. The CSR generated on ISE can be viewed. Click **View** as shown in the image.



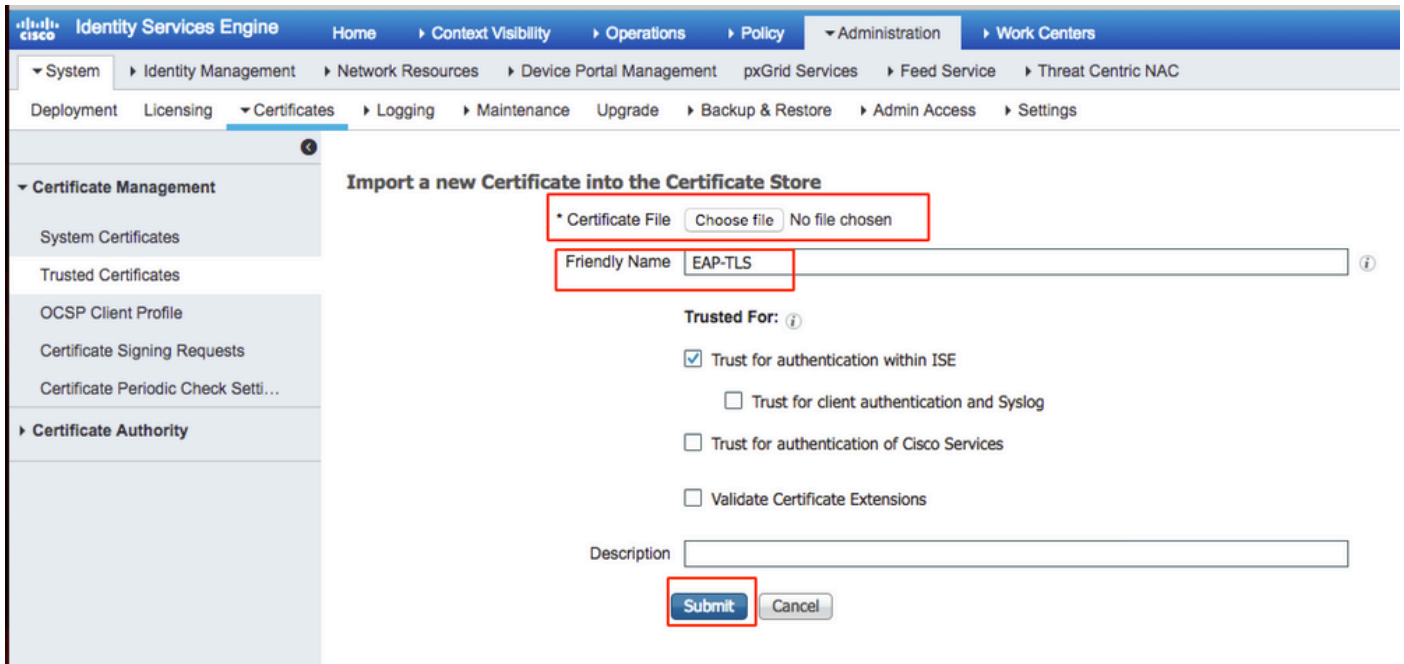
Step 5. Once CSR is generated, browse for CA server and click **Request a certificate** as shown in the image:



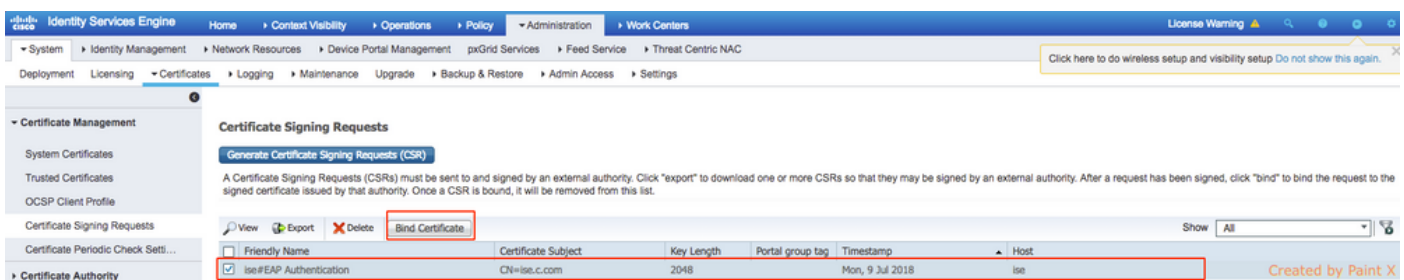
Step 6. Once you request a certificate, you get options for **User Certificate** and **advanced certificate request**, click **advanced certificate request** as shown in the image.



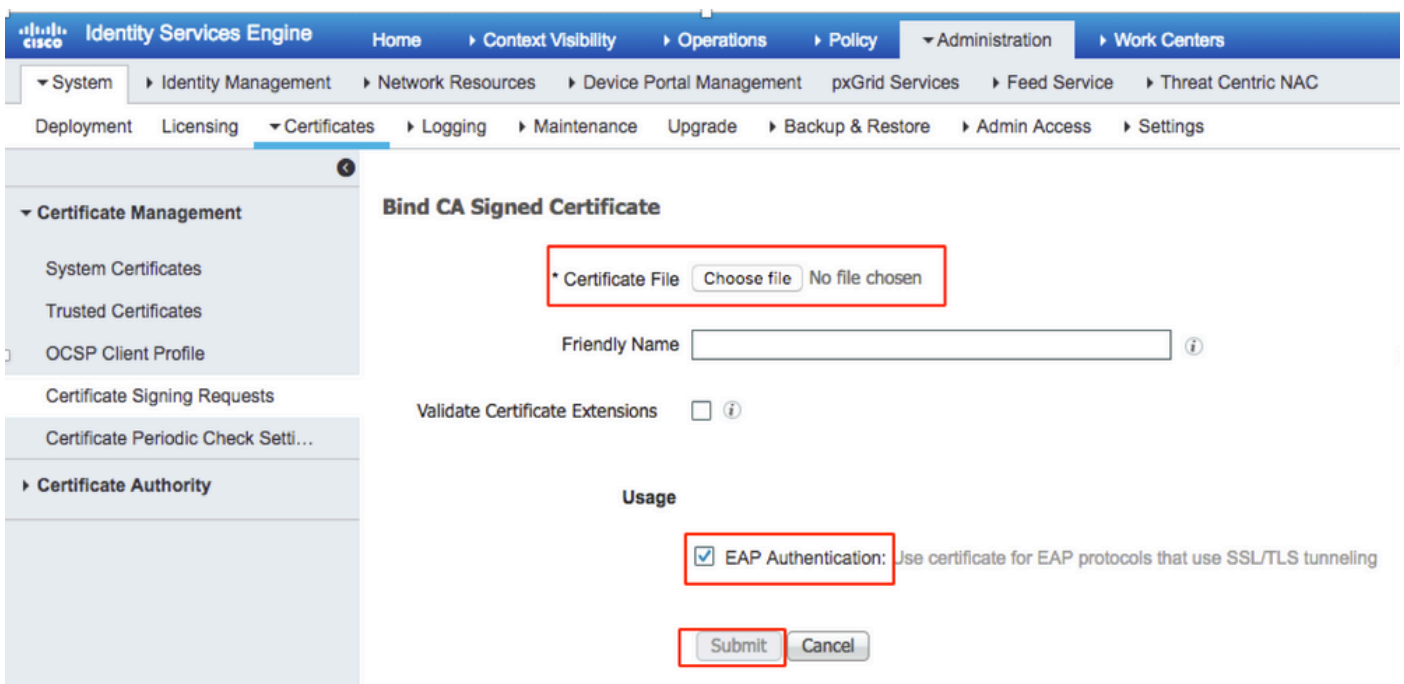
Step 7. Paste the CSR generated in **Base-64 encoded certificate request**. From the **Certificate Template:** drop down option, choose **Web Server** and click **Submit** as shown in the image.



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.

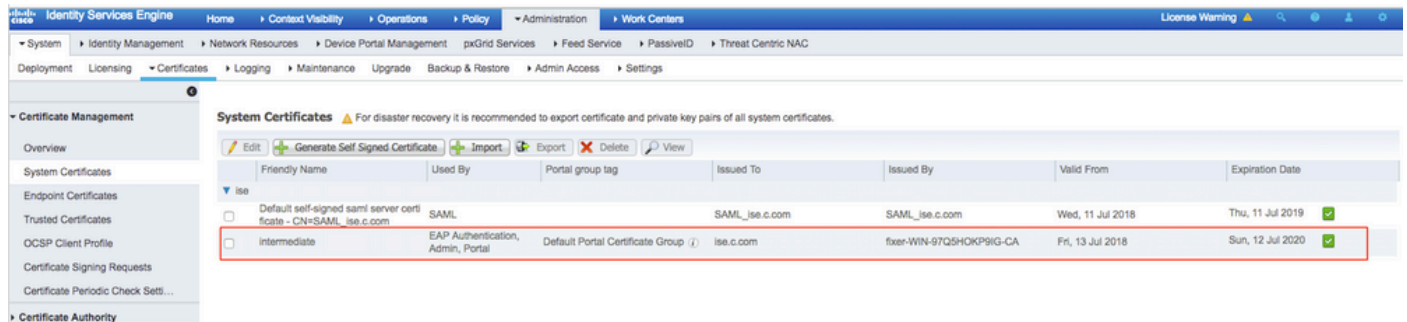


Step 11. Once you click **Bind certificate**, there is an option to choose the certificate file saved in your desktop. Browse to the intermediate certificate and click **Submit** as shown in the image.



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://sever 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  
aF4l2aLpmDFp1PfvZ3VaP6Oa/mej3IXh0RFxBUII  
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxFlj3SwvLTKLDJq+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, use 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.**

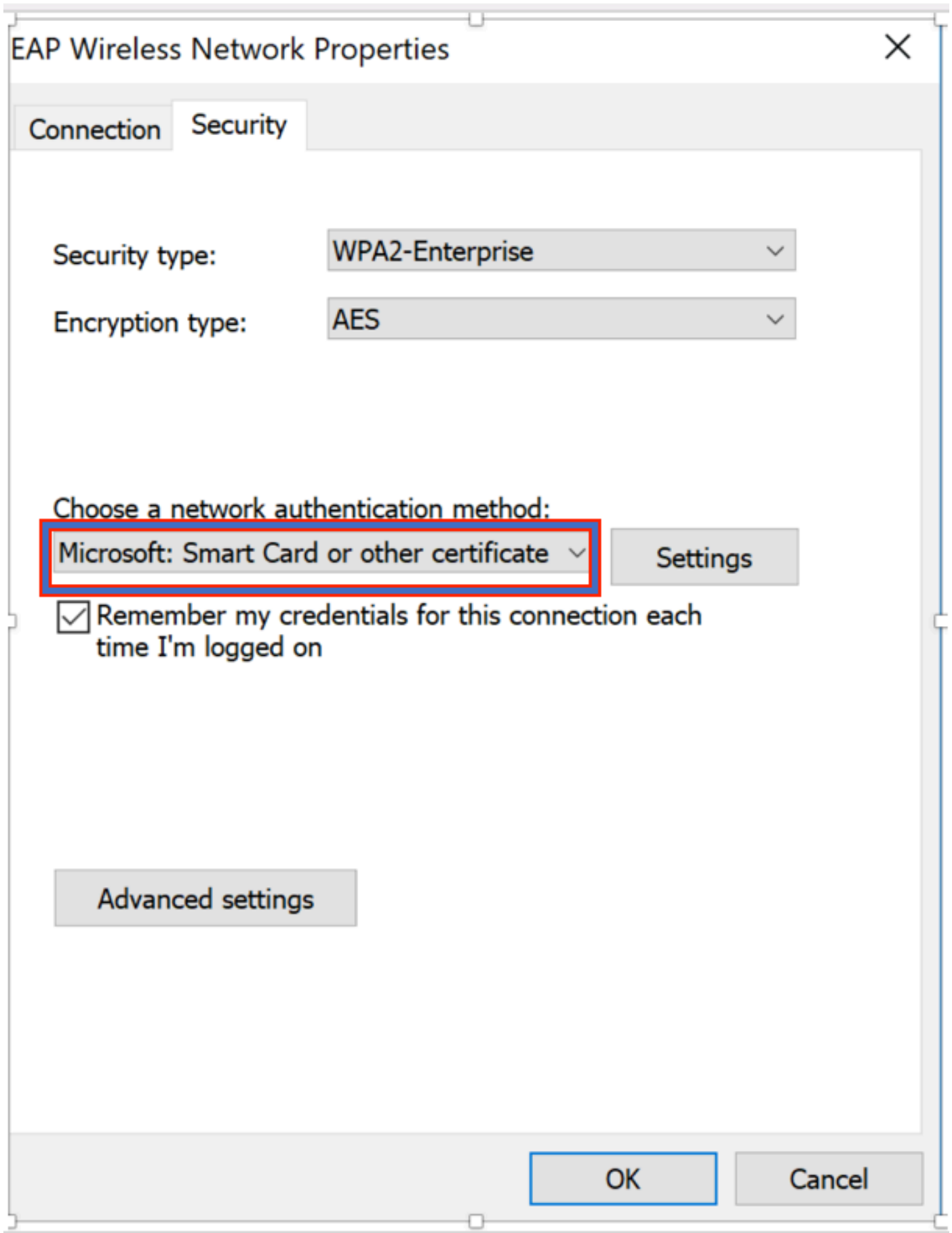
15. Click **Finish & OK**

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 the EAP-TLS instead. Click **EAP wireless profile.**

Step 2. Select **Microsoft: Smart Card or other certificate** and click **OK** 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.



EAP

Connected, secured



blizzard-legacy

Secured



blizzard

Secured



internet

Open



dot1x_test

Secured



JioPrivateNet

Secured, Hotspot 2.0



mac_filter

Secured

. This means that the client has completed authentication, obtained IP address and is ready to pass the traffic shown in the image.

The screenshot displays the 'Clients > Detail' page in a Cisco WLC interface. The left sidebar contains navigation options like 'Summary', 'Access Points', 'Statistics', 'CDP', 'Rogues', 'Redundancy', 'Clients', 'Sleeping Clients', 'Multicast', 'Applications', 'Lync', and 'Local Profiling'. The main content area is divided into 'General' and 'AVC Statistics' tabs. The 'AVC Statistics' tab is active, showing 'Client Properties' and 'AP Properties'.

Client Properties

MAC Address	34:02:86:96:2f:b7
IPv4 Address	10.106.32.239
IPv6 Address	fe80::2818:15a4:65f9:842,
Client Type	Simple IP
User Name	Administrator
Port Number	1
Interface	management
VLAN ID	32
Quarantine VLAN ID	0
CCX Version	CCXv1
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Mobility Move Count	0
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	146

AP Properties

AP Address	00:d7:8f:52:db:a0
AP Name	Alpha2802_3rdfloor
AP Type	802.11bn
AP radio slot Id	0
WLAN Profile	EAP
WLAN SSID	EAP
Data Switching	Central
Authentication	Central
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	1682
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Lync Properties

Lync State	Disabled
Audio Qos Policy	Silver

Step 2. Also verify the correct EAP method on WLC in the client details page as shown in the image.

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Auth Key Mgmt	802.1x
Encryption Cipher	CCMP (AES)
EAP Type	EAP-TLS
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	none
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied	Unavailable

Step 3. Here are the client details from CLI of the controller (output clipped):

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address..... 34:02:86:96:2f:b7
Client Username ..... Administrator
AP MAC Address..... 00:d7:8f:52:db:a0
AP Name..... Alpha2802_3rdfloor
AP radio slot Id..... 0
Client State..... Associated
Wireless LAN Id..... 5
Wireless LAN Network Name (SSID)..... EAP
Wireless LAN Profile Name..... EAP
Hotspot (802.11u)..... Not Supported
BSSID..... 00:d7:8f:52:db:a4
Connected For ..... 48 secs
Channel..... 1
IP Address..... 10.106.32.239
Gateway Address..... 10.106.32.1
Netmask..... 255.255.255.0
```

```

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

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is **Context Visibility > End Points > Attributes**. The endpoint details for MAC address **34:02:86:96:2F:B7** are shown, including the username **Administrator@fixer.com** and endpoint profile **Intel-Device**. The **Attributes** tab is active, showing a table of attributes. The **AllowedProtocolMatchedRule** attribute is highlighted with a red box.

General Attributes	
Description	
Static Assignment	false
Endpoint Policy	Intel-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

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	5
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509 PKI

Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7
MatchedPolicy	Intel-Device
MessageCode	5200
NAS-IP-Address	10.106.32.223
NAS-Identifier	HA_Pri
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	HA_Pri
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"
OpenSSLErrorStack	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	AccessRequest
SSID	00-d7-8f-52-db-a0:EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 11...

Troubleshoot

There is currently no specific information available to troubleshoot for this configuration.