

Comprender y configurar EAP-TLS con Mobility Express e ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo EAP-TLS](#)

[Pasos en el Flujo EAP-TLS](#)

[Configurar](#)

[Cisco Mobility Express](#)

[ISE con Cisco Mobility Express](#)

[Configuración EAP-TLS](#)

[Configuración de Mobility Express en ISE](#)

[Certificado de confianza en ISE](#)

[Cliente para EAP-TLS](#)

[Descargar certificado de usuario en equipo cliente \(escritorio de Windows\)](#)

[Perfil inalámbrico para EAP-TLS](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar una red de área local inalámbrica (WLAN) con seguridad 802.1x en un controlador Mobility Express. Este documento también explica el uso específico del protocolo de autenticación extensible (EAP): seguridad de la capa de transporte (TLS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración inicial de Mobility Express
- Proceso de autenticación 802.1x
- Certificados

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

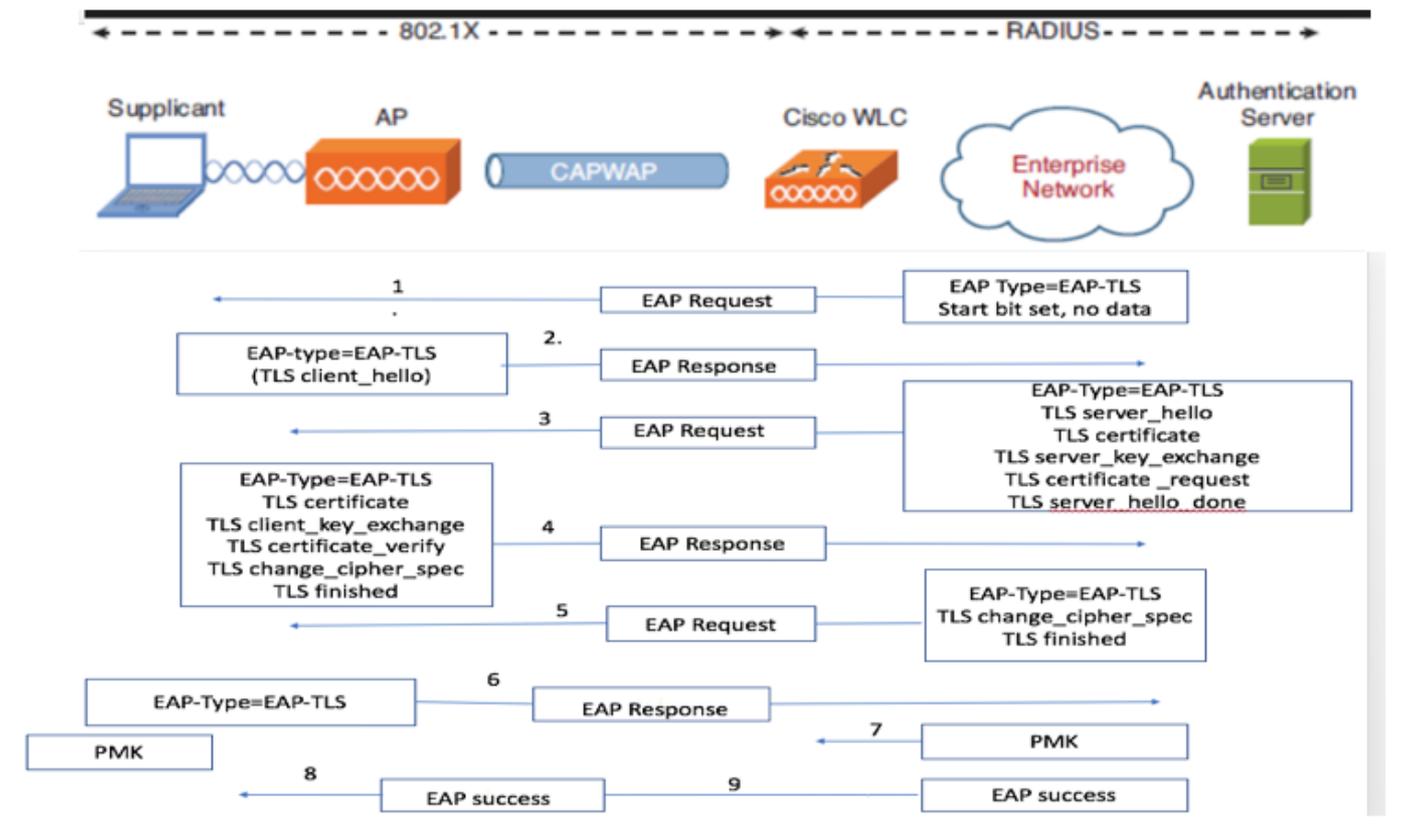
hardware.

- WLC 5508 versión 8.5
- Identity Services Engine (ISE) versión 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Flujo EAP-TLS



Pasos en el Flujo EAP-TLS

1. El cliente inalámbrico se asocia con el punto de acceso (AP).
2. AP no permite que el cliente envíe ningún dato en este punto y envía una solicitud de autenticación.
3. A continuación, el suplicante responde con una identidad de respuesta EAP. A continuación, el WLC comunica la información de ID de usuario al servidor de autenticación.
4. El servidor RADIUS responde al cliente con un paquete de inicio EAP-TLS. La conversación EAP-TLS comienza en este punto.
5. El par envía un EAP-Response de vuelta al servidor de autenticación que contiene un mensaje de entrada en contacto "client_hello", un dígito que está configurado como NULL.

6. El servidor de autenticación responde con un paquete de desafío de acceso que contiene:

```
TLS server_hello  
handshake message  
certificate  
server_key_exchange  
certificate request  
server_hello_done.
```

7. El cliente responde con un mensaje EAP-Response que contiene:

```
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
```

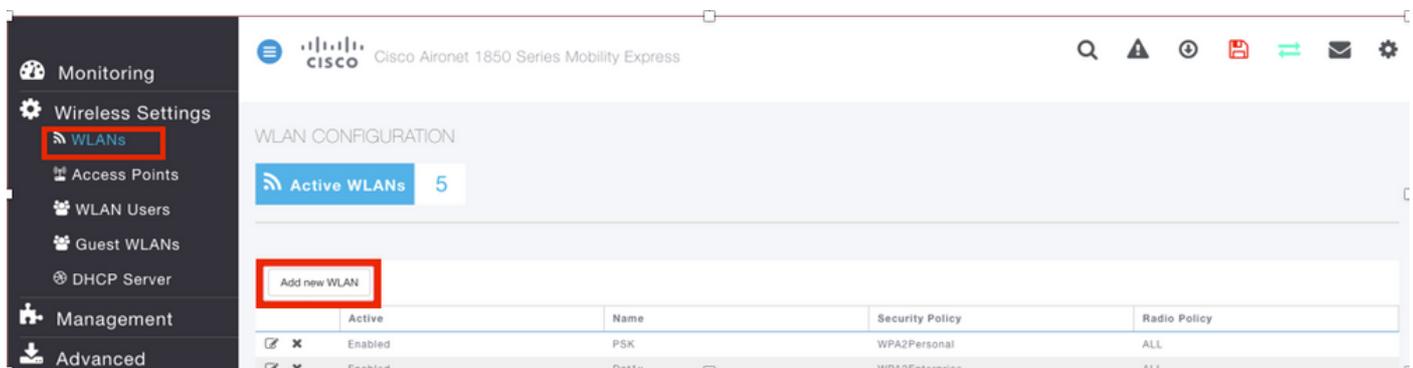
8. Después de que el cliente se autentica correctamente, el servidor RADIUS responde con un desafío de acceso, que contiene el mensaje "change_cipher_spec" y entrada en contacto. Al recibir esto, el cliente verifica el hash para autenticar el servidor RADIUS. Una nueva clave de cifrado se deriva dinámicamente del secreto durante el intercambio de señales TLS.

9. En este momento, el cliente inalámbrico habilitado para EAP-TLS puede acceder a la red inalámbrica.

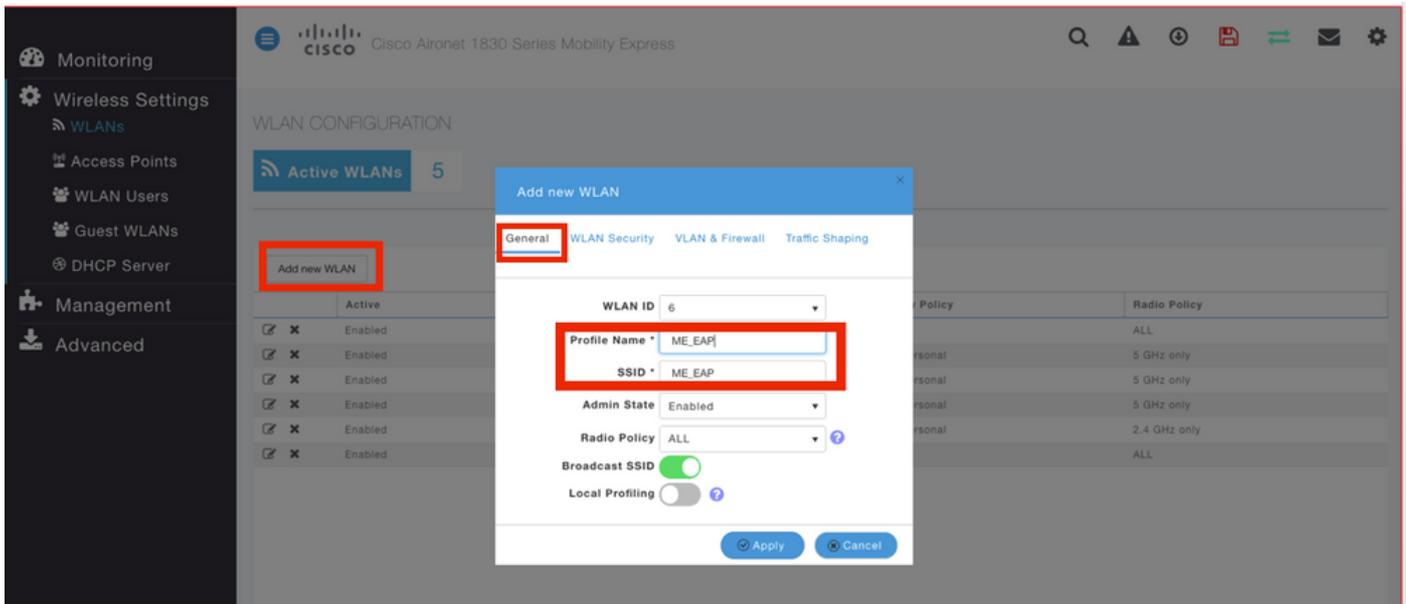
Configurar

Cisco Mobility Express

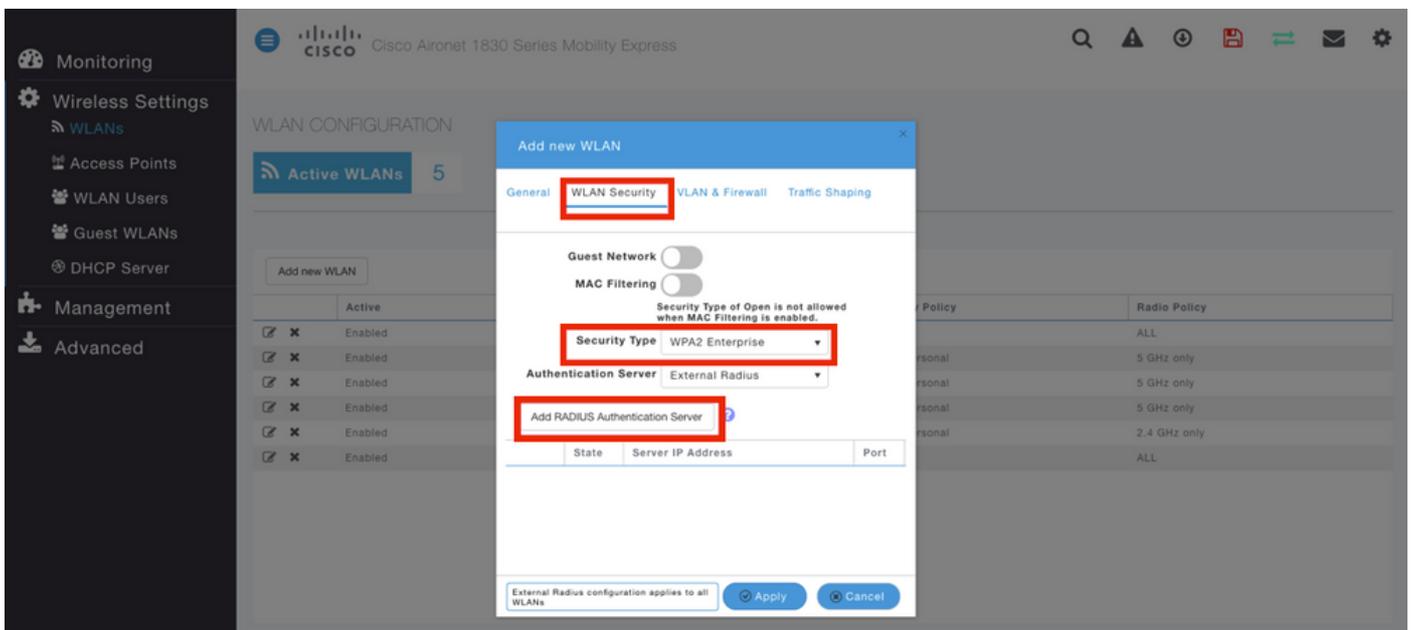
Paso 1. El primer paso es crear una WLAN en Mobility Express. Para crear una WLAN, navegue hasta **WLAN > Add new WLAN** como se muestra en la imagen.



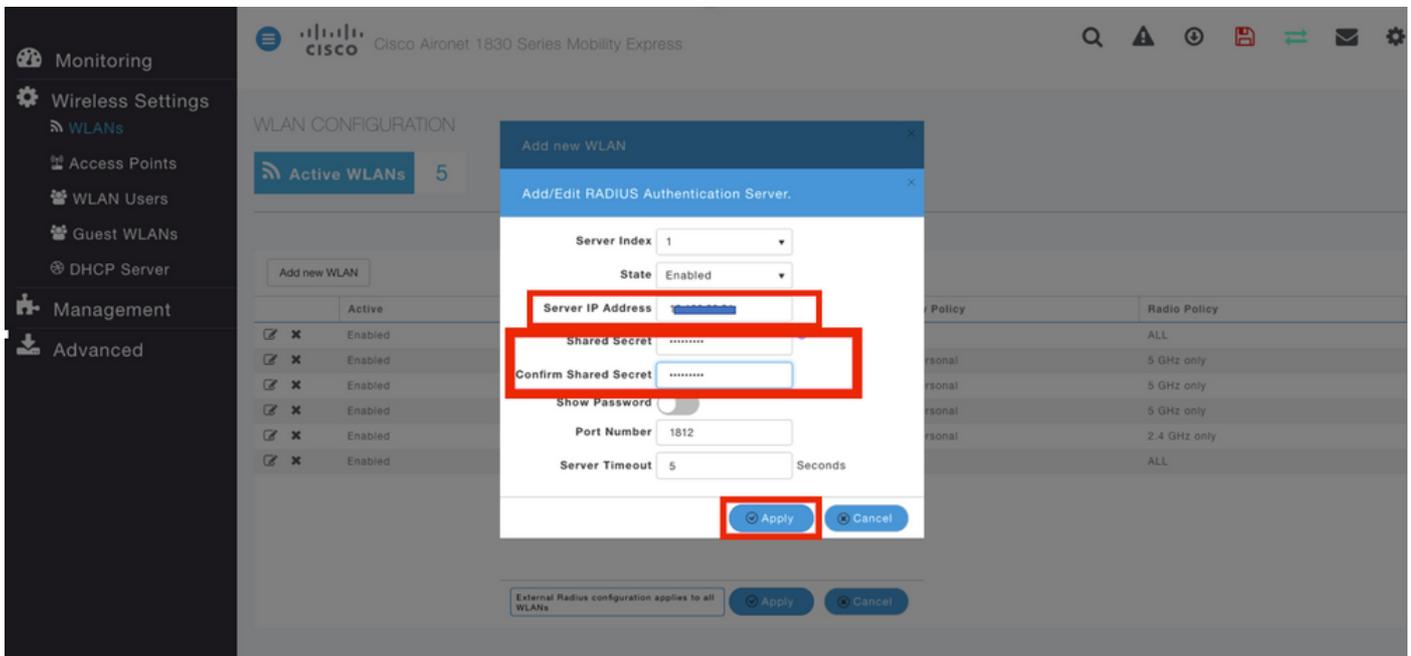
Paso 2. Aparecerá una nueva ventana emergente cuando haga clic en **Agregar nueva WLAN**. Para crear un nombre de perfil, navegue hasta **Add new WLAN > General** como se muestra en la imagen.



Paso 3. Configure el tipo de autenticación como WPA Enterprise para 802.1x y configure el servidor RADIUS bajo **Agregar nueva WLAN > Seguridad WLAN** como se muestra en la imagen.



Paso 4. Haga clic en **Add RADIUS Authentication Server** y proporcione la dirección IP del servidor RADIUS y Shared Secret que debe coincidir exactamente con lo que se ha configurado en ISE y luego haga clic en **Apply** como se muestra en la imagen.



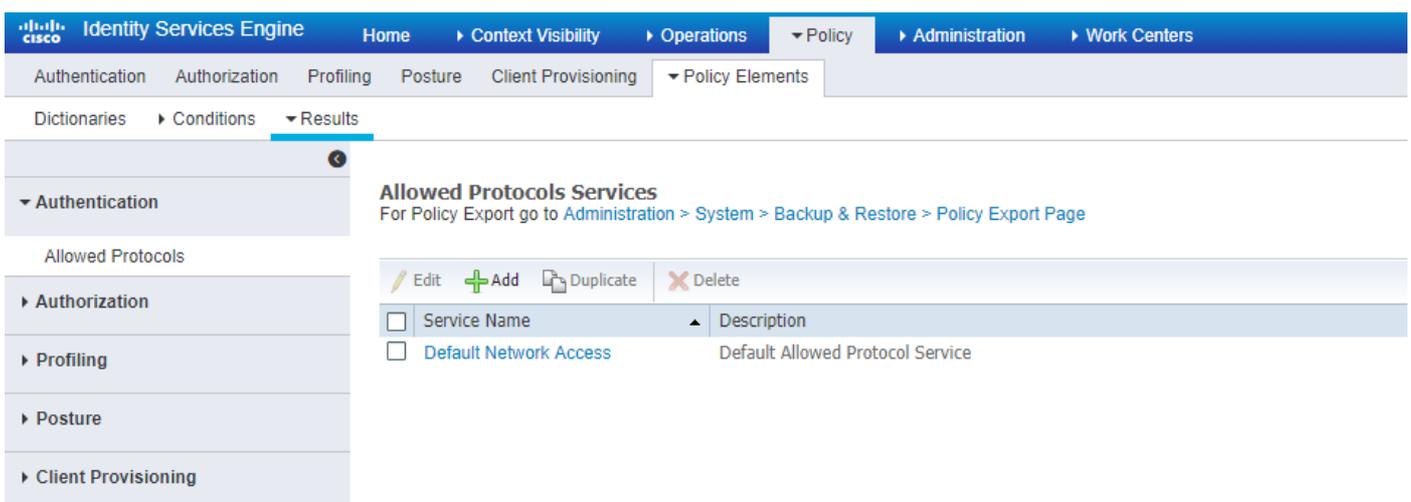
ISE con Cisco Mobility Express

Configuración EAP-TLS

Para generar la política, debe crear la lista de protocolos permitidos para utilizarla en la política. Dado que se escribe una política dot1x, especifique el tipo EAP permitido en función de cómo se configura la política.

Si utiliza el valor predeterminado, permite la mayoría de los tipos de EAP para la autenticación, que puede no ser preferible si necesita bloquear el acceso a un tipo de EAP específico.

Paso 1. Vaya a **Policy > Policy Elements > Results > Authentication > Allowed Protocols** y haga clic en **Add** como se muestra en la imagen.



Paso 2. En esta lista de protocolo permitido, puede introducir el nombre de la lista. En este caso, la casilla **Allow EAP-TLS** está marcada y otras casillas están desmarcadas como se muestra en la imagen.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services List > New Allowed Protocols Service

Allowed Protocols

Name

Description

Allowed Protocols

Authentication Bypass

Process Host Lookup (i)

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 (i)

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 (i)

Require cryptobinding TLV (i)

Configuración de Mobility Express en ISE

Paso 1. Abra la consola ISE y navegue hasta **Administration > Network Resources > Network Devices > Add** como se muestra en la imagen.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

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
------	---------	--------------	----------	------	-------------

Paso 2. Introduzca la información como se muestra en la imagen.

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.

Certificado de confianza en ISE

Paso 1. Vaya a **Administration > System > Certificates > Certificate Management > Trusted certificates**.

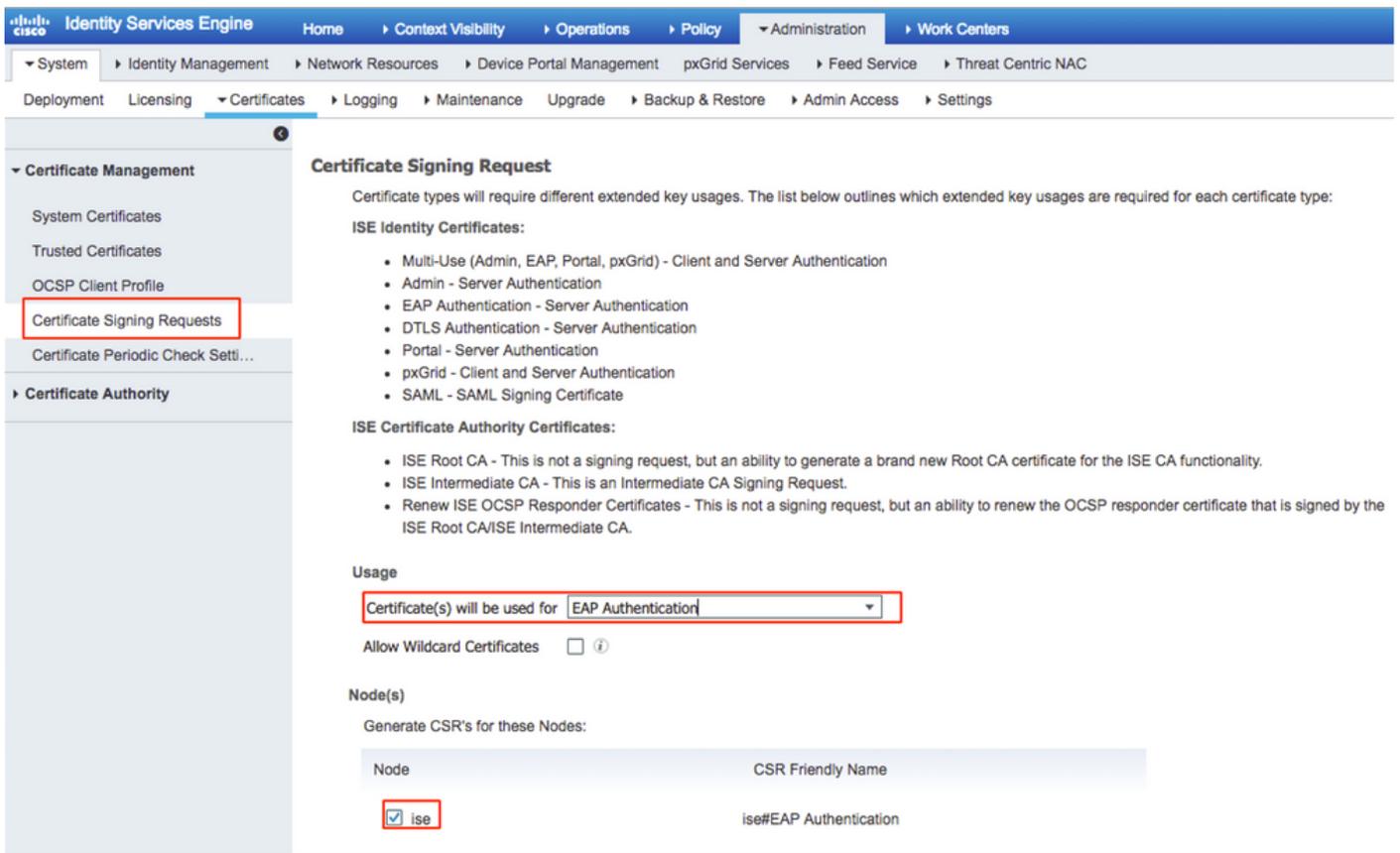
Haga clic en **Importar** para importar un certificado a ISE. Una vez que agrega un WLC y crea un usuario en ISE, debe hacer la parte más importante de EAP-TLS que es confiar en el certificado en ISE. Para ello, debe generar CSR.

Paso 2. Vaya a **Administración > Certificados > Solicitudes de firma de certificados > Generar solicitudes de firma de certificados (CSR)** como se muestra en la imagen.

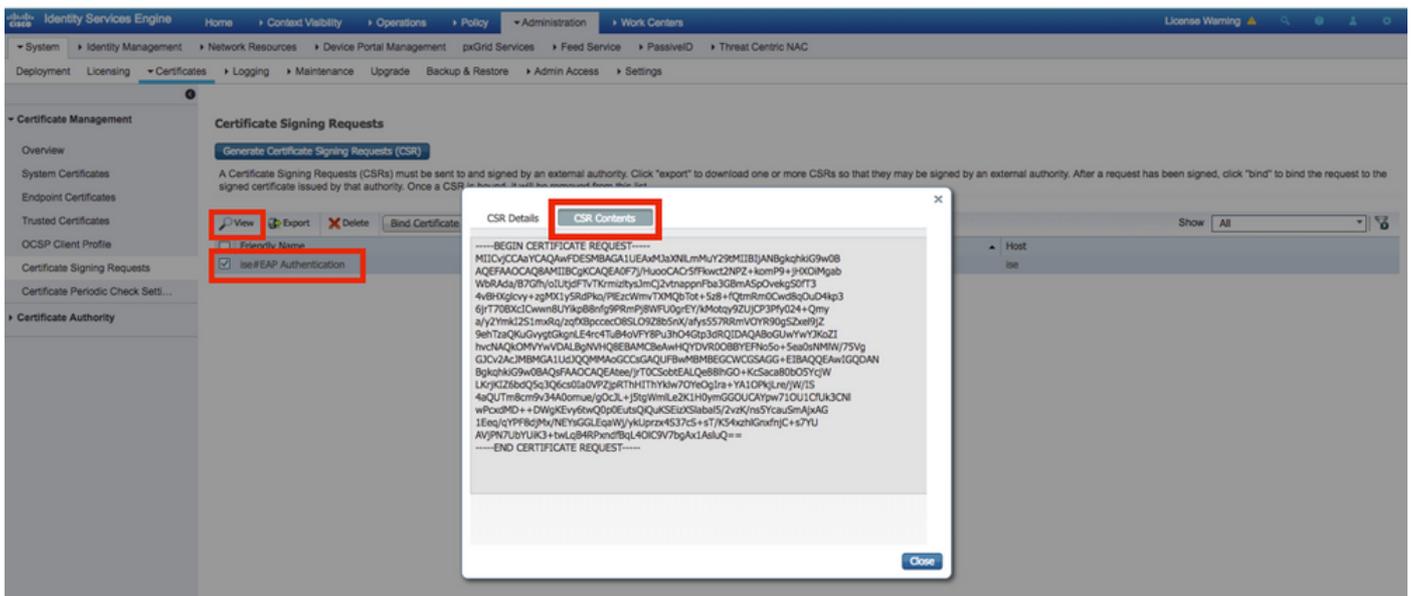
The screenshot shows the 'Certificate Signing Requests' page in Cisco ISE. The table below contains the following data:

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

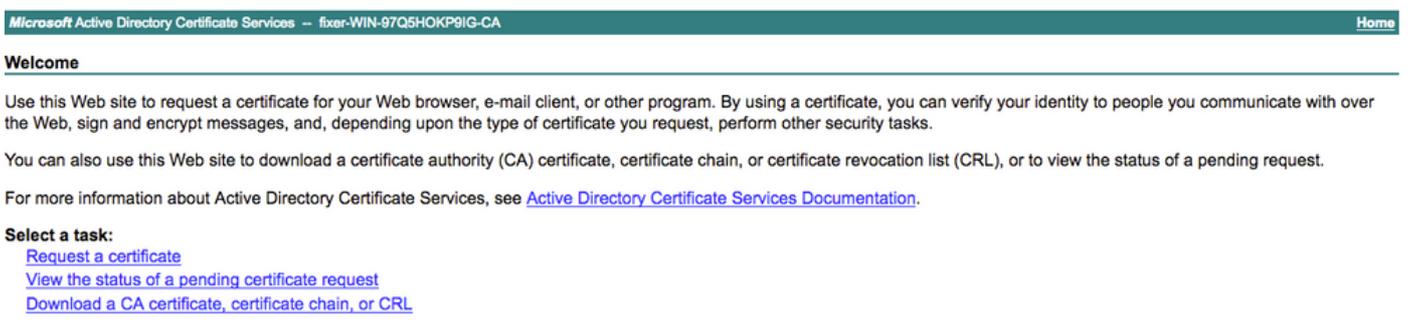
Paso 3. Para generar CSR, navegue hasta **Uso** y desde **Los certificados se utilizarán para** opciones desplegadas seleccione **Autenticación EAP** como se muestra en la imagen.



Paso 4. Se puede ver la CSR generada en ISE. Haga clic en **Ver** como se muestra en la imagen.



Paso 5. Una vez que se genera CSR, busque el servidor de la CA y haga clic en **Solicitar un certificado** como se muestra en la imagen:



Paso 6. Una vez que solicita un certificado, obtiene opciones para **Certificado de usuario** y **solicitud de certificado avanzado**, haga clic en **solicitud de certificado avanzado** como se muestra en la imagen.

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

Request a Certificate

Select the certificate type:

[User Certificate](#)

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

Paso 7. Pegue la CSR generada en la **solicitud de certificado codificado Base-64**. En la opción **Certificate Template**: desplegable, elija **Web Server** y haga clic en **Submit** como se muestra en la imagen.

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:

Web Server

Additional Attributes:

Attributes:

Paso 8. Una vez que haga clic en **Enviar**, tendrá la opción de seleccionar el tipo de certificado, seleccione **Base-64 codificado** y haga clic en **Descargar cadena de certificado** como se muestra en la imagen.

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

Certificate Issued

The certificate you requested was issued to you.

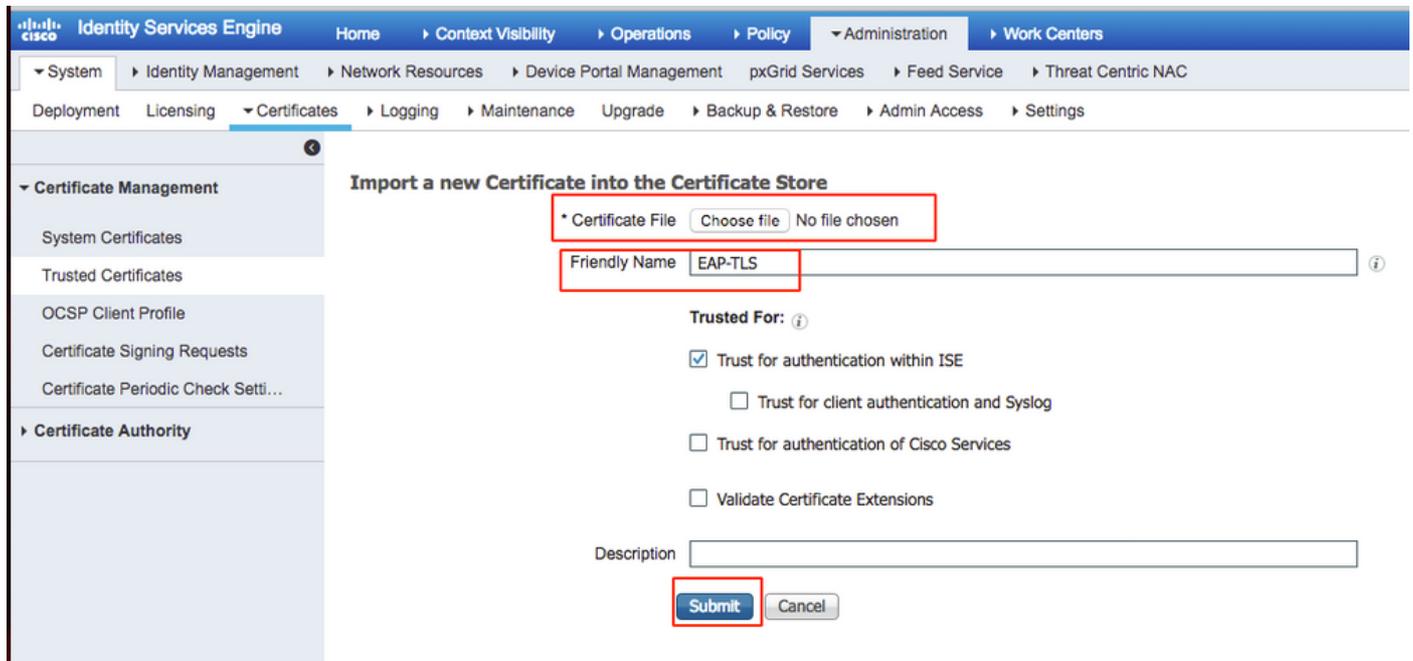
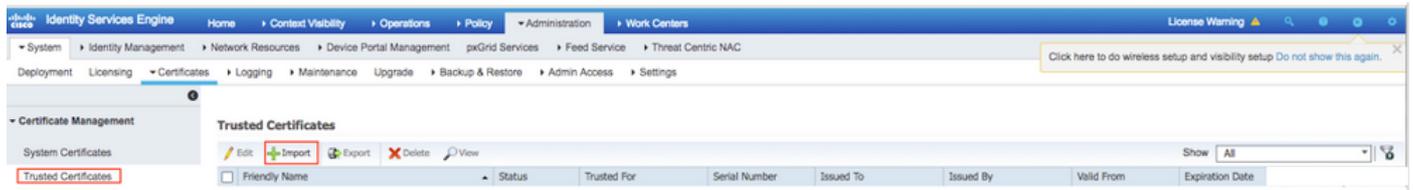
DER encoded or Base 64 encoded

 [Download certificate](#)

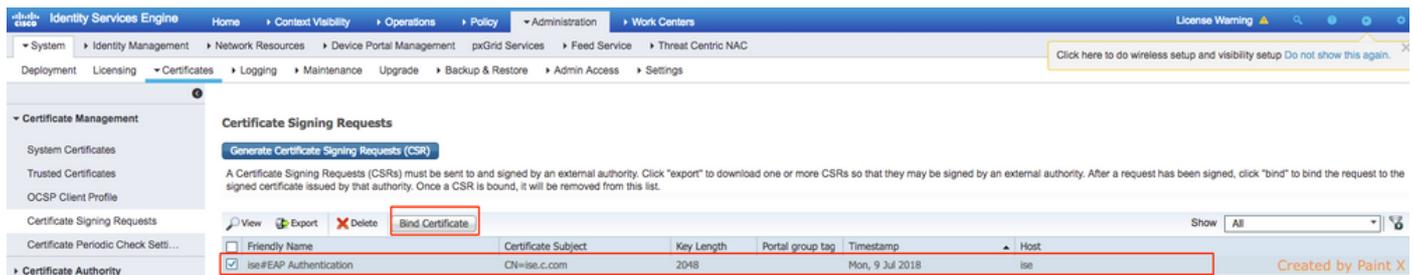
[Download certificate chain](#)

Paso 9. La descarga del certificado se ha completado para el servidor ISE. Puede extraer el

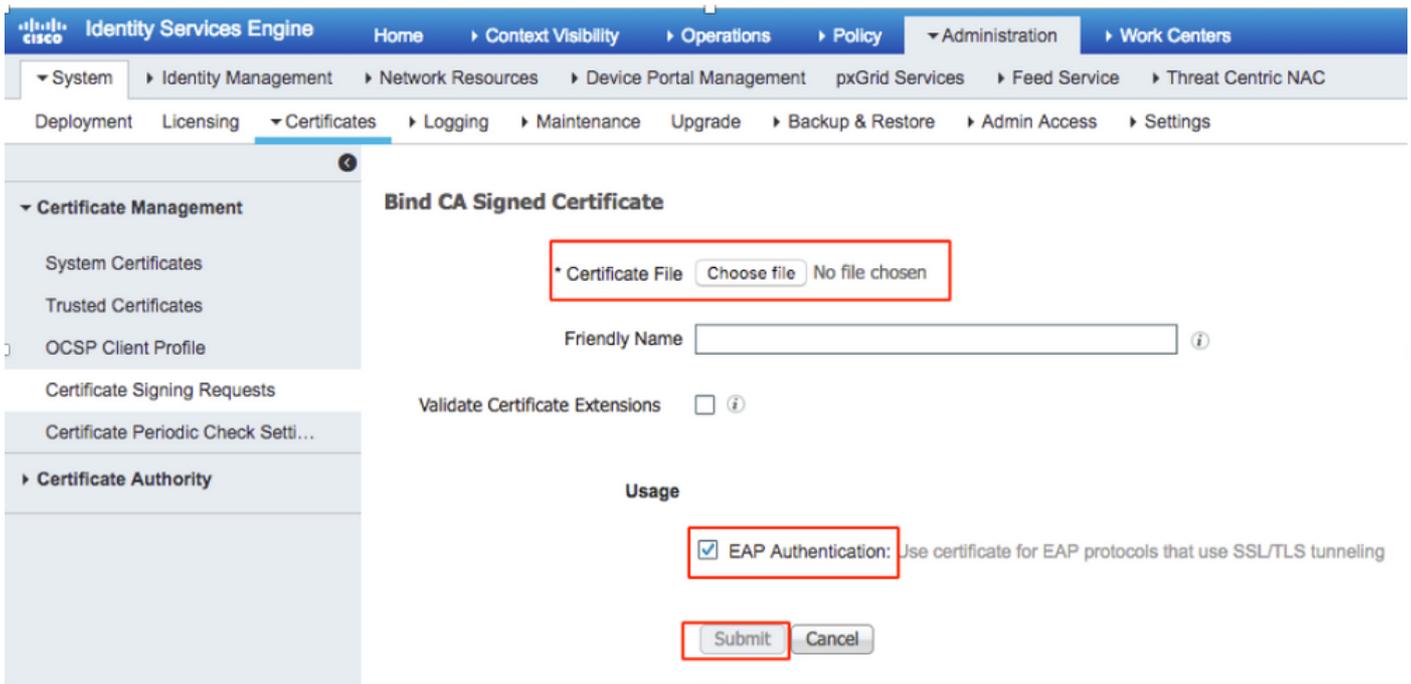
certificado, el certificado contendrá dos certificados, un certificado raíz y otro intermedio. El certificado raíz se puede importar bajo **Administración > Certificados > Certificados de confianza > Importar** como se muestra en las imágenes.



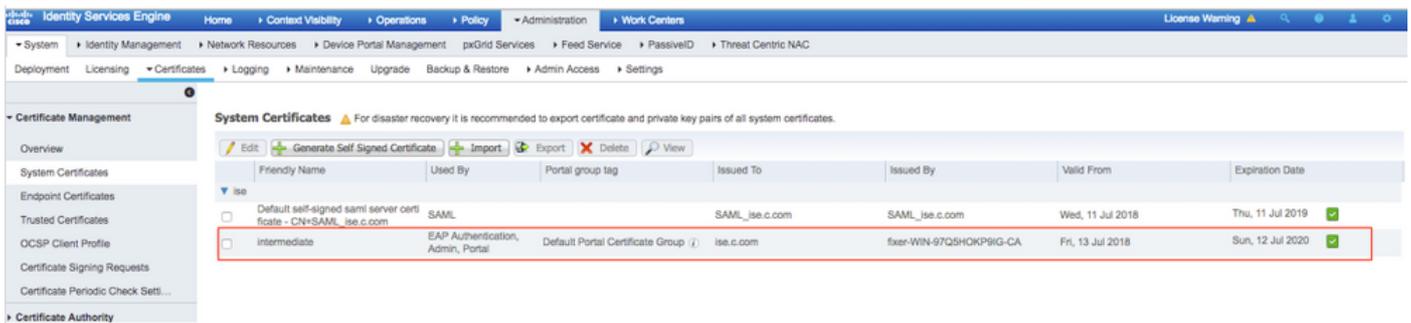
Paso 10. Una vez que haga clic en **Enviar**, el certificado se agrega a la lista de certificados de confianza. Además, el certificado intermedio es necesario para enlazar con CSR como se muestra en la imagen.



Paso 11. Una vez que haga clic en **Bind certificate**, hay una opción para elegir el archivo de certificado guardado en su escritorio. Busque el certificado intermedio y haga clic en **Enviar** como se muestra en la imagen.



Paso 12. Para ver el certificado, navegue hasta **Administración > Certificados > Certificados del sistema** como se muestra en la imagen.



Cliente para EAP-TLS

Descargar certificado de usuario en equipo cliente (escritorio de Windows)

Paso 1. Para autenticar un usuario inalámbrico a través de EAP-TLS, debe generar un certificado de cliente. Conecte el ordenador con Windows a la red para poder acceder al servidor. Abra un navegador web e introduzca esta dirección: <https://sever ip addr/certsrv/>

Paso 2. Tenga en cuenta que la CA debe ser la misma con la que se descargó el certificado para ISE.

Para ello, debe buscar el mismo servidor de la CA que utilizó para descargar el certificado para el servidor. En la misma CA, haga clic en **Solicitar un certificado** como se hizo anteriormente, sin embargo, esta vez debe seleccionar **Usuario** como Plantilla de Certificado como se muestra en la imagen.

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 >

Paso 3. A continuación, haga clic en **descargar cadena de certificados** como se hizo anteriormente para el servidor.

Una vez que obtenga los certificados, siga estos pasos para importar el certificado en el portátil de windows.

Paso 4. Para importar el certificado, debe tener acceso desde Microsoft Management Console (MMC).

1. Para abrir MMC, navegue hasta **Inicio > Ejecutar > MMC**.
2. Vaya a **Archivo > Agregar o quitar complemento**
3. Haga doble clic en **Certificados**.
4. Seleccione **Cuenta de computadora**.
5. Seleccione **Equipo local > Finalizar**
6. Haga clic en **Aceptar** para salir de la ventana Complemento.
7. Haga clic en **[+]** junto a **Certificados > Personal > Certificados**.
8. Haga clic con el botón derecho en **Certificados** y seleccione **Todas las tareas > Importar**.
9. Haga clic en **Next (Siguiente)**.
10. Haga clic en **Examinar**.

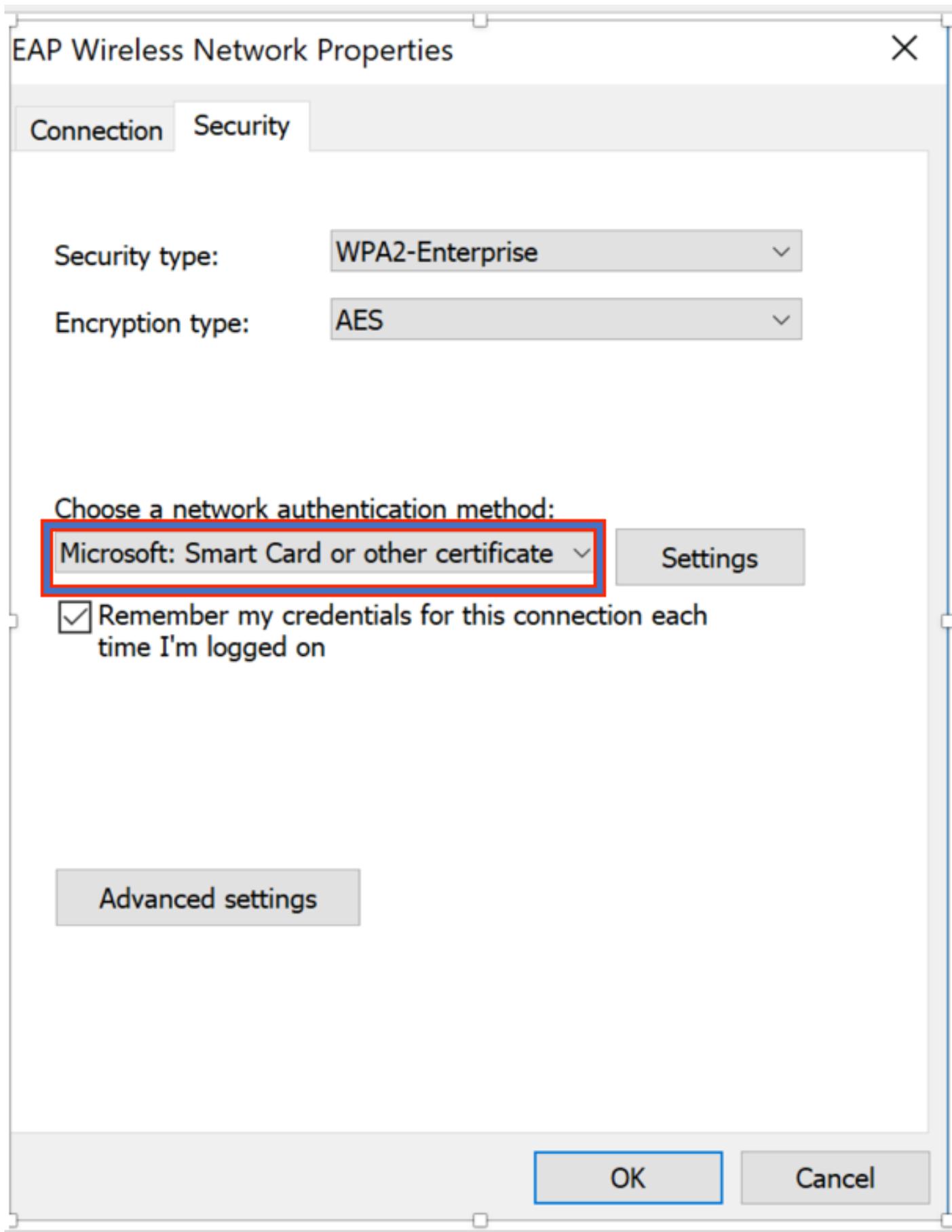
11. Seleccione **.cer, .crt o .pfx** que desea importar.
12. Haga clic en **Abrir**.
13. Haga clic en **Next (Siguiente)**.
14. Seleccione **Automatically select the certificate store basado en el tipo de certificado**.
15. Haga clic en **Finalizar y Aceptar**

Una vez realizada la importación del certificado, debe configurar su cliente inalámbrico (windows desktop en este ejemplo) para EAP-TLS.

Perfil inalámbrico para EAP-TLS

Paso 1. Cambie el perfil inalámbrico que se creó anteriormente para el protocolo de autenticación extensible protegido (PEAP) para utilizar en su lugar EAP-TLS. Haga clic en **EAP Wireless Profile**.

Paso 2. Seleccione **Microsoft: Tarjeta inteligente u otro certificado** y haga clic en **Aceptar** como se muestra en la imagen.



Paso 3. Haga clic en **Settings** y seleccione el certificado raíz emitido desde el servidor de la CA como se muestra en la imagen.

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

Paso 4. Haga clic en **Advanced Settings** y seleccione **User or computer authentication** en la pestaña 802.1x settings como se muestra en la imagen.

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

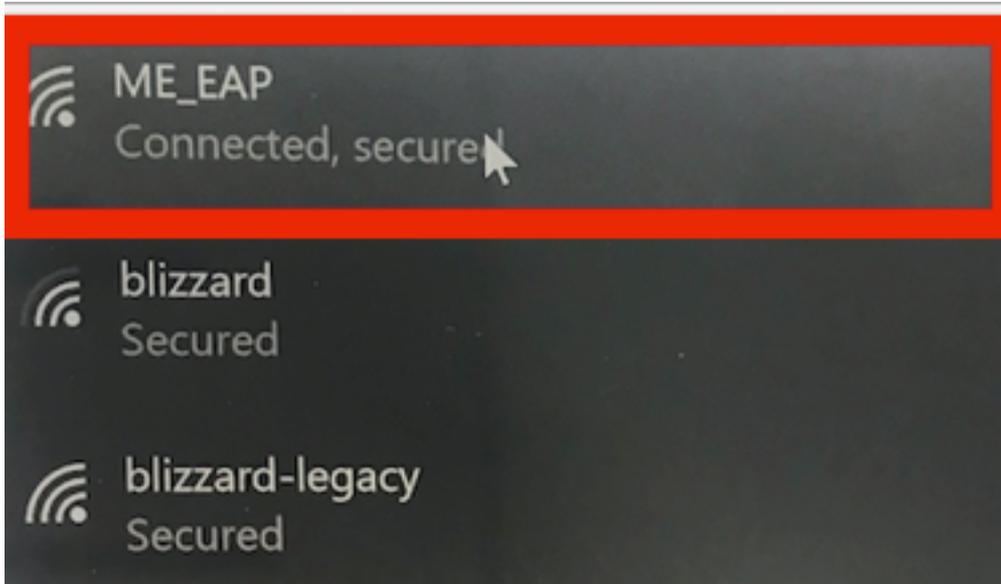
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

Paso 5. Ahora, intente conectarse de nuevo a la red inalámbrica, seleccione el perfil correcto (EAP en este ejemplo) y **Conectar**. Está conectado a la red inalámbrica como se muestra en la imagen.



Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Paso 1. El tipo EAP del cliente debe ser EAP-TLS. Esto significa que el cliente ha completado la autenticación, con el uso de EAP-TLS, ha obtenido la dirección IP y está listo para pasar el tráfico como se muestra en las imágenes.

The screenshot shows a network management interface with a sidebar on the left and a main content area. The sidebar includes sections for Monitoring, Wireless Settings, Management, and Advanced. The main content area is titled 'CLIENT VIEW' and displays details for a client with SSID 'ME_EAP'. The 'GENERAL' section shows the user name as 'Administrator' and host name as 'Unknown'. The 'CONNECTIVITY' section shows a flowchart with steps: Start, Association, Authentication, DHCP, and Online. The 'TOP APPLICATIONS' section is empty. The 'MOBILITY STATE' section shows a diagram of the network path: WLC (LOCAL) -> Wired (CAP-WAP) -> AP (FlexConnect) -> Wireless (802.11n (5GHz)) -> Client (VLAN1).

CLIENT VIEW

GENERAL

User Name: Administrator
Host Name: Unknown

MAC Address: 34:02:86:96:2f:b7
Uptime: Associated since 37 Seconds
SSID: ME_EAP
AP Name: AP442b.03a9.7f72 (Ch 56)

Nearest APs

Device Type

Performance: Signal Strength: 0 dBm Signal Quality: 0 dB Connection Speed: 0 Channel Width: 40 MHz

Capabilities: 802.11n (5GHz) Spatial Stream: 0

Cisco Compatible: Supported (CCX v 4)

Connection Score: 0%

CONNECTIVITY

Start Association Authentication DHCP Online

TOP APPLICATIONS

Name	Usage	% Usage
No Data Available!		

MOBILITY STATE

WLC (LOCAL) -> Wired (CAP-WAP) -> AP (FlexConnect) -> Wireless (802.11n (5GHz)) -> Client (VLAN1)

Paso 2. A continuación se muestra el detalle del cliente de la CLI del controlador (salida recortada):

```
(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
```

Paso 3. En ISE, navegue hasta **Visibilidad de contexto > Terminales > Atributos** como se muestra en las imágenes.

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-97Q5HOKP9\G-CA,DC=fixer,DC=cc
Issuer - Common Name	fixer-WIN-97Q5HOKP9\G-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

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.