

Comprensión y configuración de EAP-TLS con un WLC e ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo EAP-TLS](#)

[Pasos del flujo EAP-TLS](#)

[Configurar](#)

[Controlador de LAN inalámbrica de Cisco](#)

[ISE con Cisco WLC](#)

[Configuración de EAP-TLS](#)

[Configuración de WLC en ISE](#)

[Creación de un usuario nuevo en ISE](#)

[Certificado de confianza en ISE](#)

[Cliente para EAP-TLS](#)

[Descargar certificado de usuario en el 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 802.1X y protocolo de autenticación extensible EAP-TLS

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Proceso de autenticación 802.1X
- Certificados

Componentes Utilizados

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

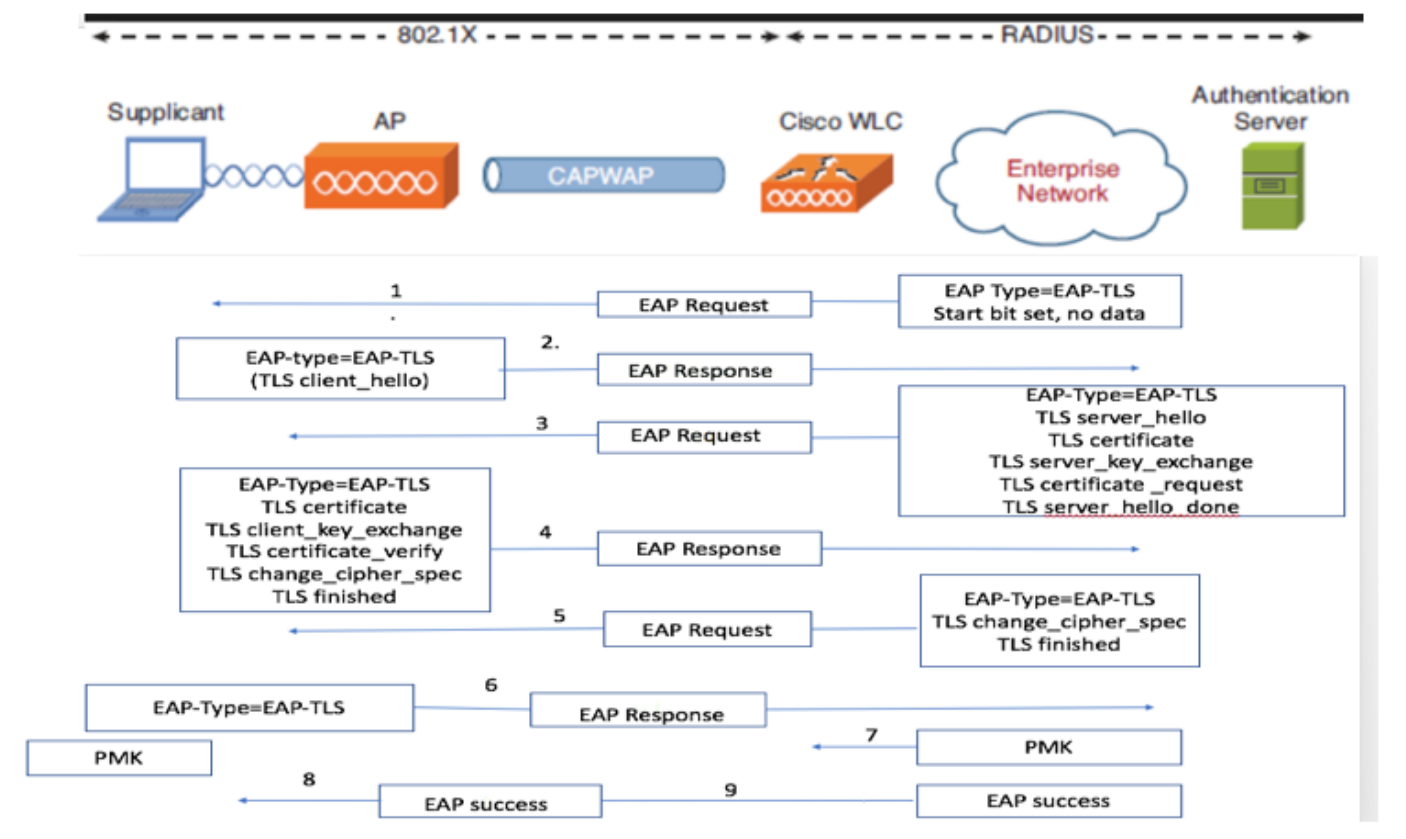
hardware.

- WLC 3504 versión 8.10
- Identity Services Engine (ISE) versión 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Flujo EAP-TLS



Pasos del flujo EAP-TLS

1. El cliente inalámbrico se asocia al punto de acceso (AP). El AP no permite que el cliente envíe ningún dato en este punto y envía una solicitud de autenticación. El solicitante responde entonces con una identidad de respuesta EAP. El WLC luego comunica la información de la ID de usuario al servidor de autenticación. El servidor RADIUS responde al cliente con un paquete de inicio EAP-TLS. La conversación EAP-TLS comienza en este punto.
2. El par envía una respuesta EAP al servidor de autenticación que contiene un mensaje de intercambio de señales "client_hello", un cifrado que se establece en NULL
3. 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.

4. 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

5. Después de que el cliente se autentique con éxito, el servidor RADIUS responde con un desafío de acceso, que contiene el mensaje "change_cipher_spec" y entrada en contacto finalizado.

6. Cuando recibe esto, el cliente verifica el hash para autenticar el servidor RADIUS.

7. Una nueva clave de cifrado se deriva dinámicamente del secreto durante el intercambio de señales TLS

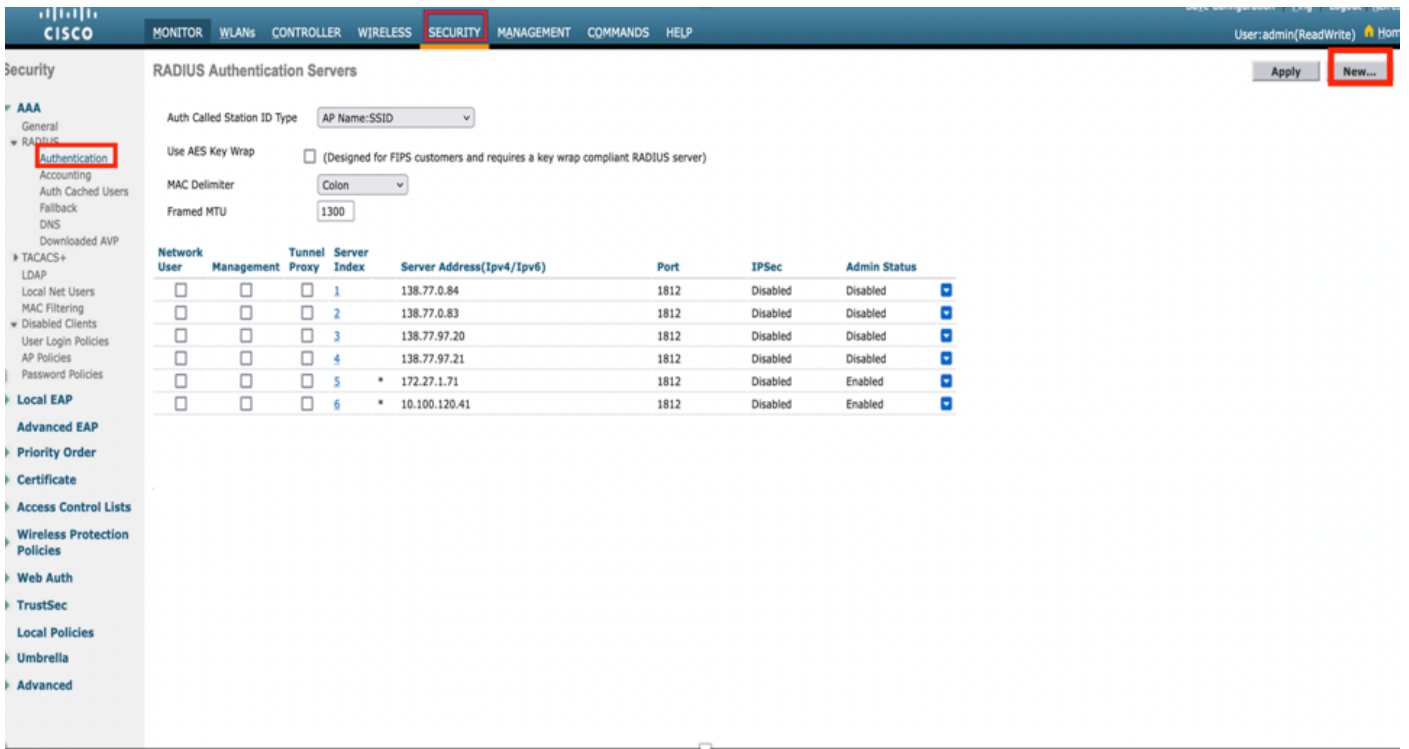
8/9. EAP-El éxito finalmente se envía del servidor al autenticador que luego se pasa al solicitante.

En este momento, el cliente inalámbrico con EAP-TLS activado puede acceder a la red inalámbrica.

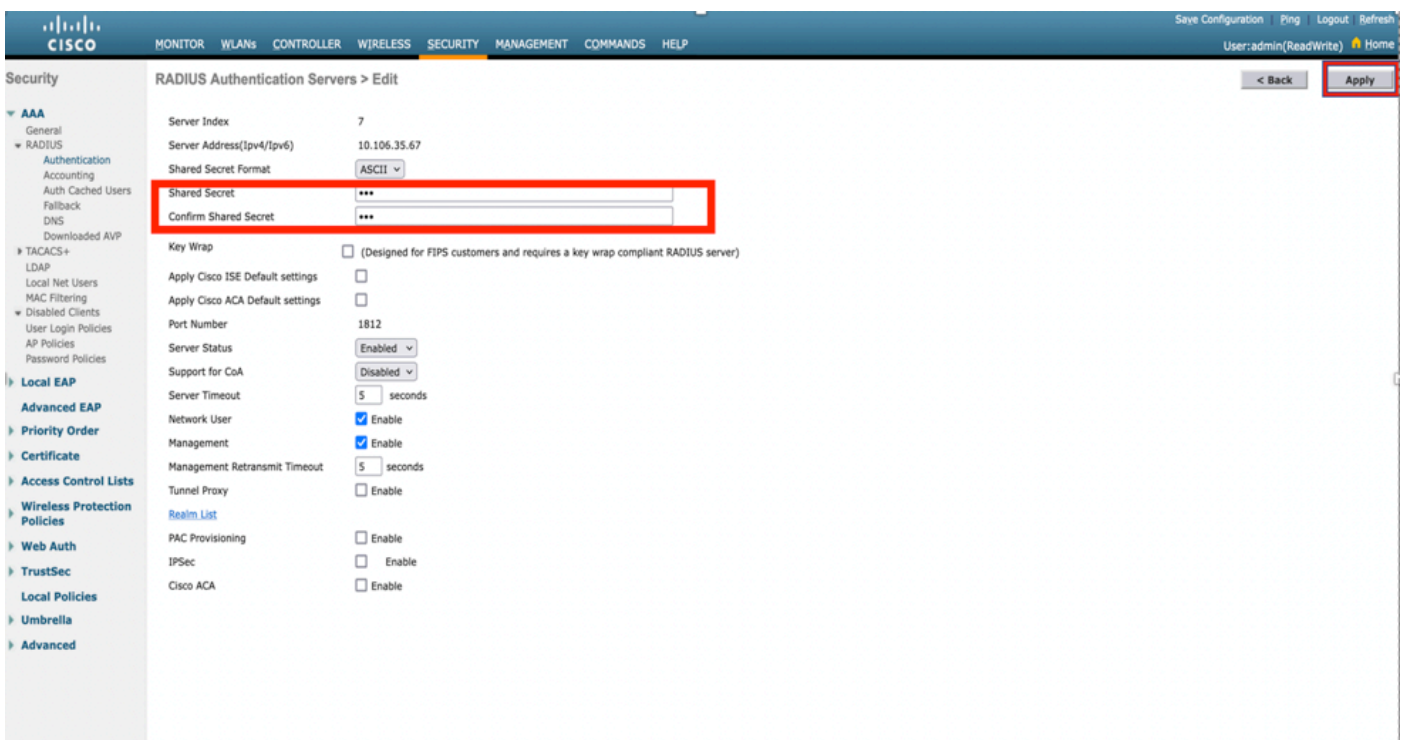
Configurar

Controlador de LAN inalámbrica de Cisco

Paso 1. El primer paso es configurar el servidor RADIUS en el WLC de Cisco. Para agregar un servidor RADIUS, navegue hasta **Seguridad > RADIUS > Autenticación**. Haga clic en **Nuevo** como se muestra en la imagen.



Paso 2. Aquí, debe ingresar la dirección IP y el secreto compartido <contraseña> que se utiliza para validar el WLC en ISE. Haga clic en **Aplicar** para continuar como se muestra en la imagen.



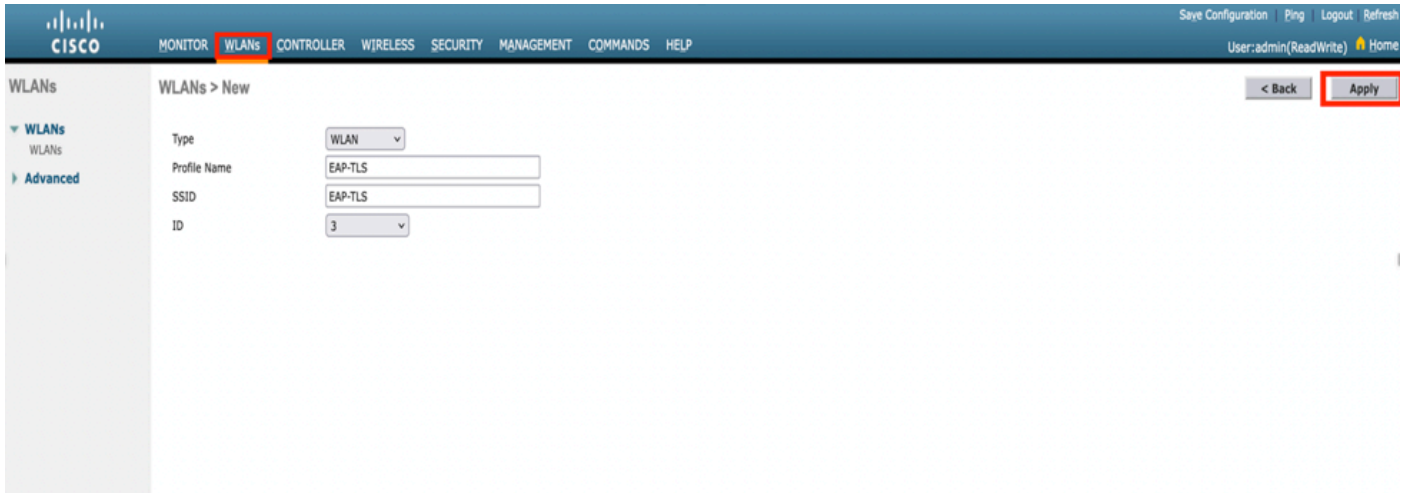
Paso 3. Crear WLAN para la autenticación RADIUS.

Ahora puede crear una nueva WLAN y configurarla para utilizar el modo WPA-Enterprise, de modo que pueda utilizar RADIUS para la autenticación.

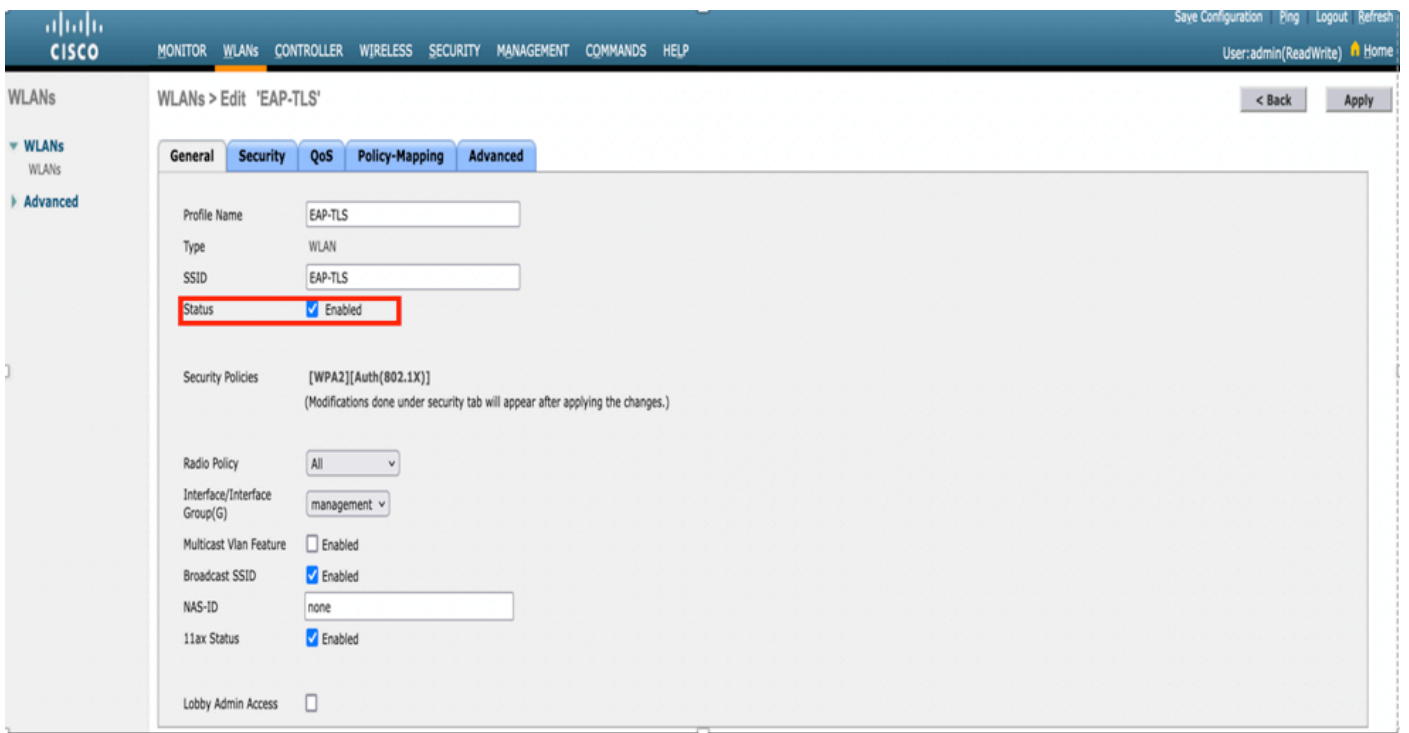
Paso 4. Seleccione **WLANs** en el menú principal, elija **Create New** y haga clic en **Go** como se muestra en la imagen.



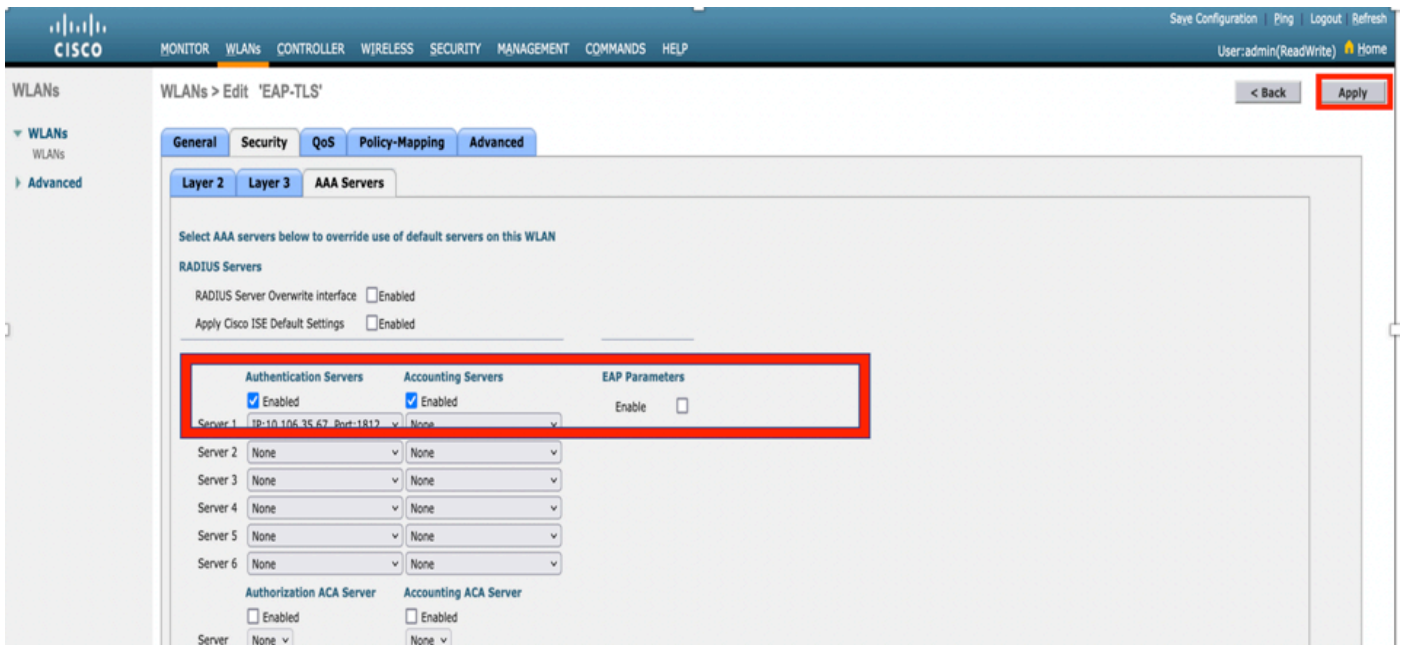
Paso 5. Asigne el nombre **EAP-TLS** a la nueva WLAN. Haga clic en **Aplicar** para continuar como se muestra en la imagen.



Paso 6. Haga clic en **General** y asegúrese de que el estado es **Activado**. Las políticas de seguridad predeterminadas son autenticación 802.1X y WPA2, como se muestra en la imagen.



Paso 7. Ahora, navegue hasta **Seguridad > Servidores AAA**, seleccione el servidor RADIUS que acaba de configurar y como se muestra en la imagen.



Nota: Es una buena idea verificar que puede alcanzar el servidor RADIUS del WLC antes de continuar. RADIUS utiliza el puerto UDP 1812 (para la autenticación), por lo que debe asegurarse de que este tráfico no se bloquea en ninguna parte de la red.

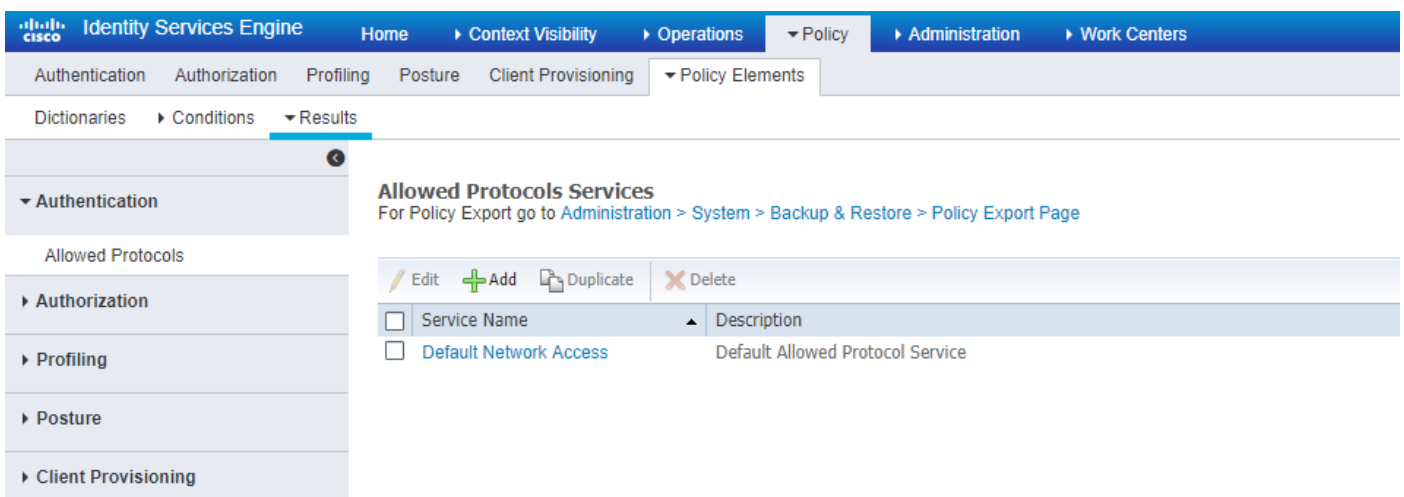
ISE con Cisco WLC

Configuración de EAP-TLS

Para crear la política, debe crear la lista de protocolos permitidos para utilizar en nuestra política. Dado que se escribe una política dot1x, especifique el tipo de EAP permitido en función de la configuración de la política.

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

Paso 1. Navegue hasta **Política > Elementos de Política > Resultados > Autenticación > Protocolos Permitidos** y haga clic en **Agregar** como se muestra en la imagen.



Paso 2. En esta lista de protocolos permitidos, puede introducir el nombre de la lista. En este caso, la casilla **Allow EAP-TLS** está marcada y las demás 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

Dictionaryes 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)

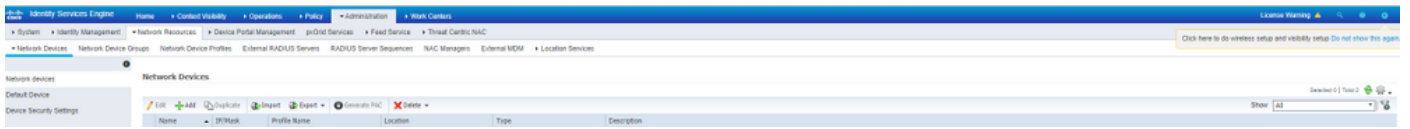
Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)

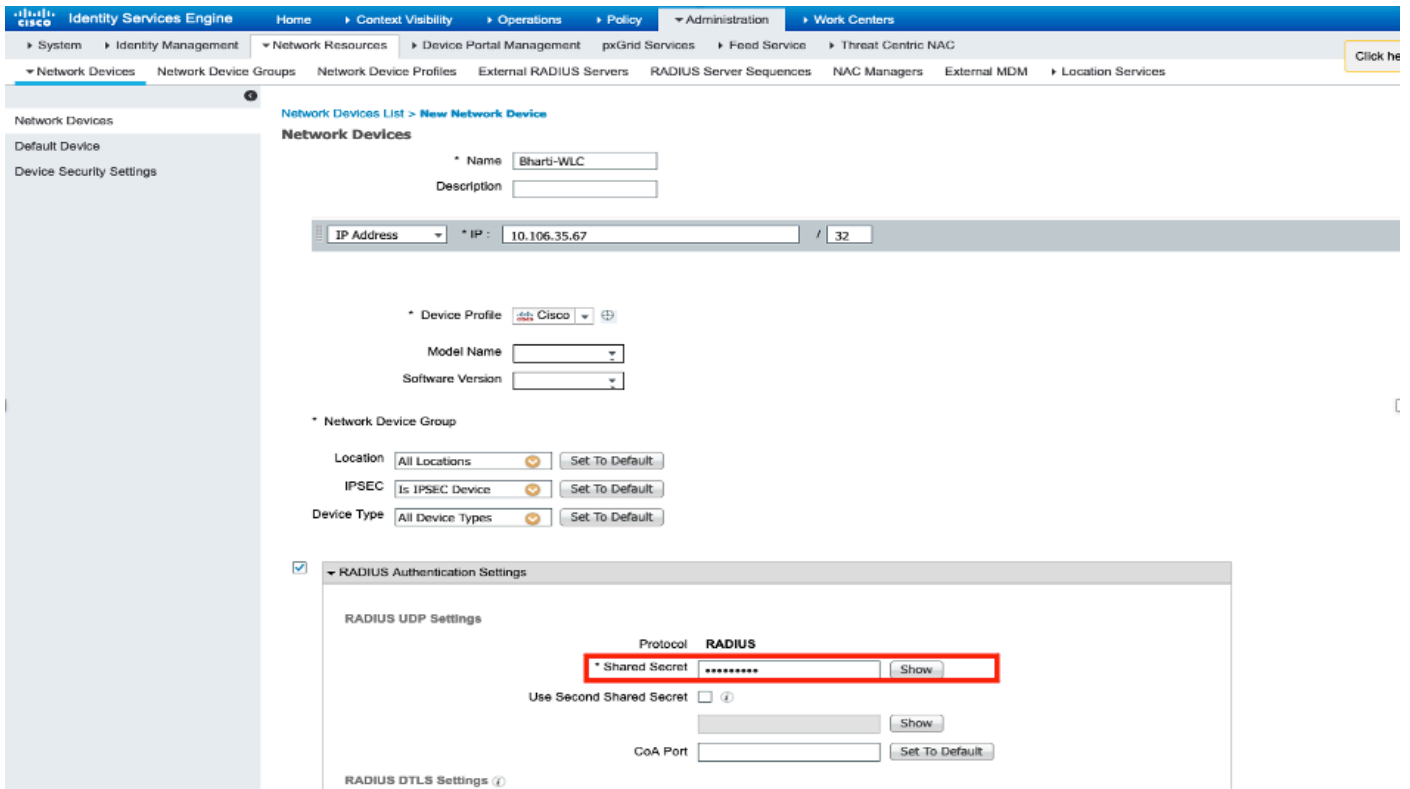
Require cryptobinding TLV (i)

Configuración de WLC en ISE

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

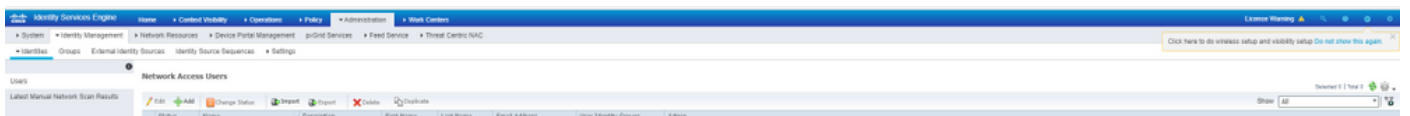


Paso 2. Introduzca los valores como se muestra en la imagen.

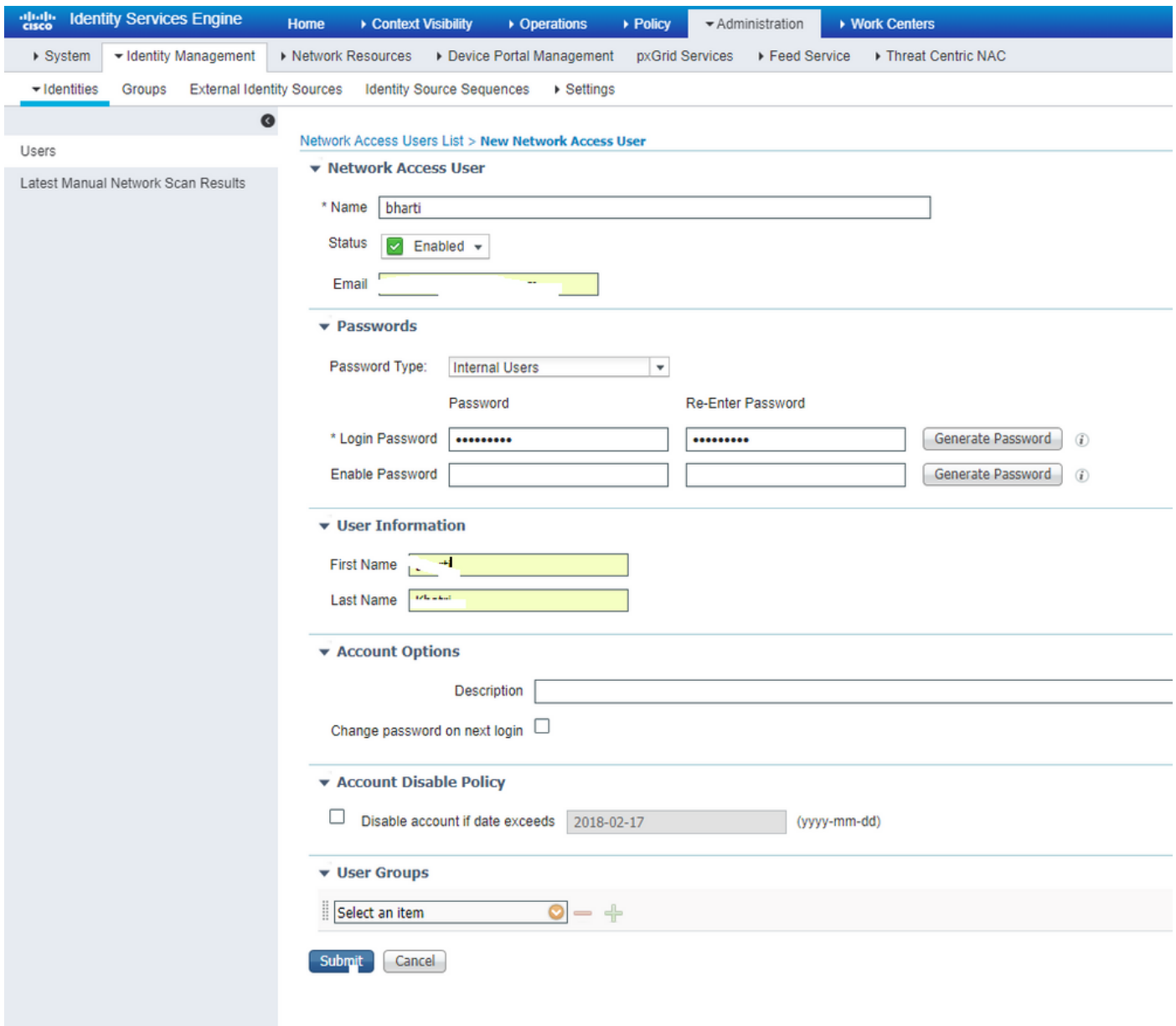


Creación de un usuario nuevo en ISE

Paso 1. Navegue hasta **Administration > Identity Management > Identities > Users > Add** como se muestra en la imagen.



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

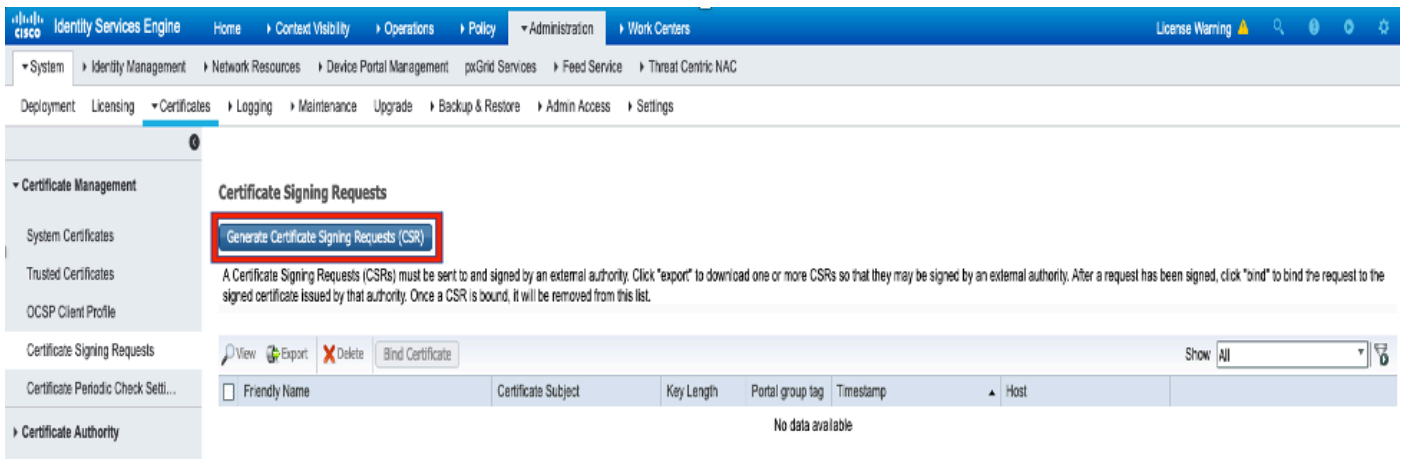


Certificado de confianza en ISE

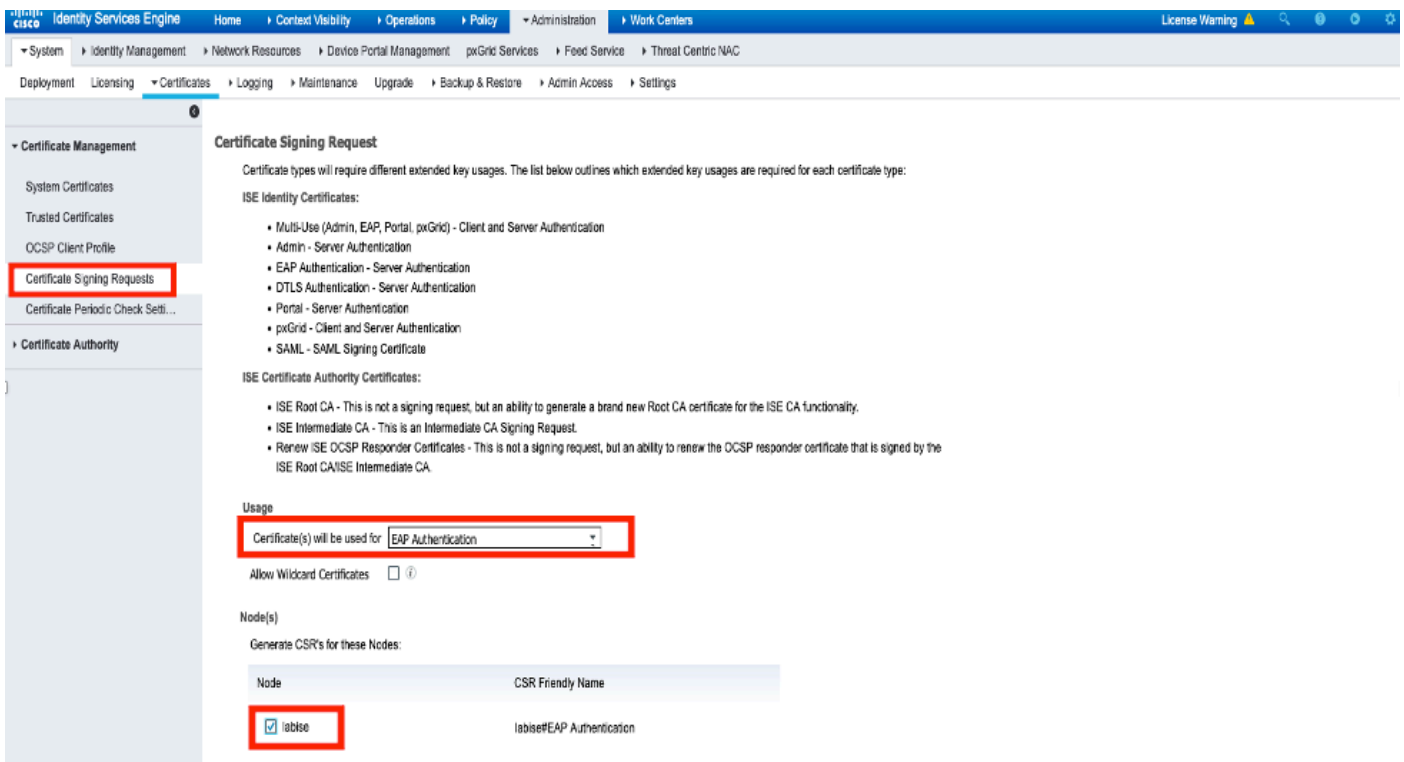
Paso 1. Navegue hasta **Administración > Sistema > Certificados > Administración de certificados > Certificados de confianza**.

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

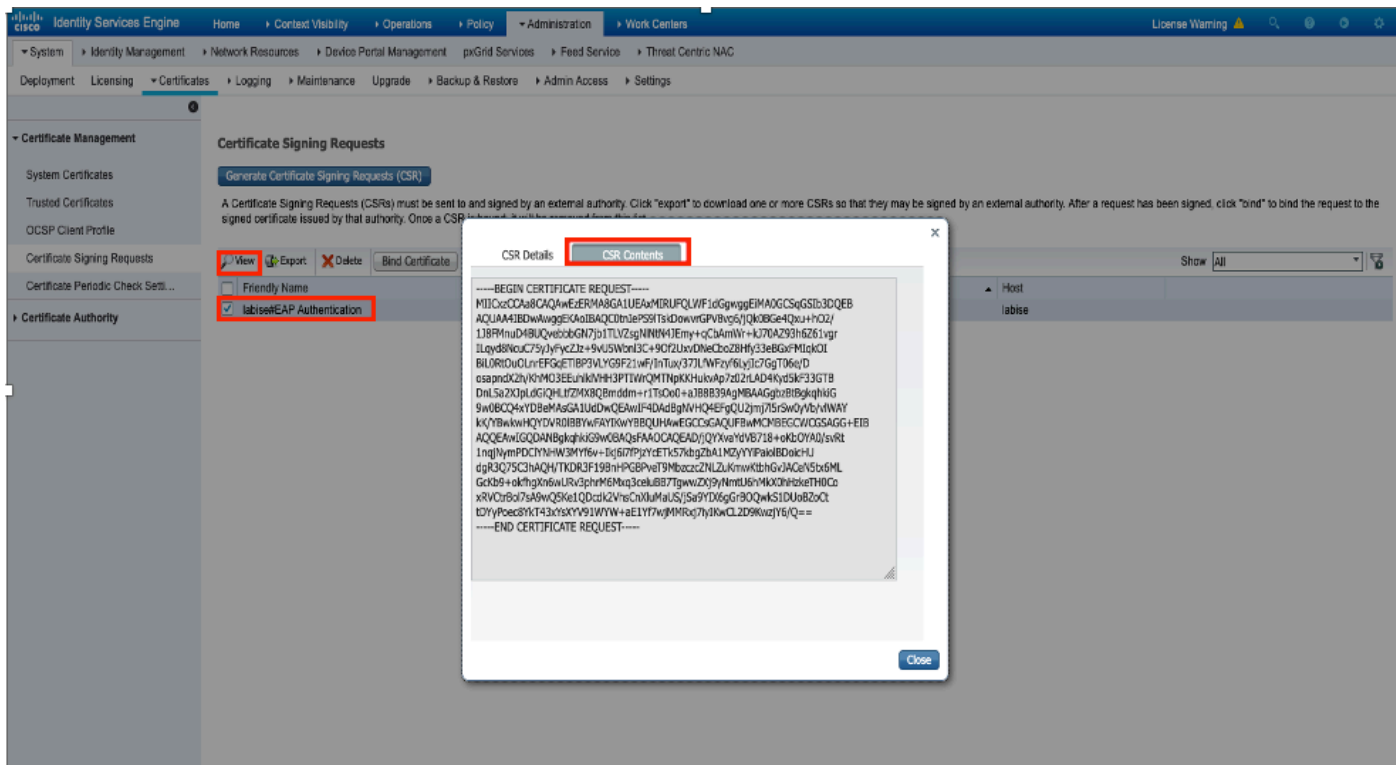
Paso 2. Vaya a **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR)** como se muestra en la imagen.



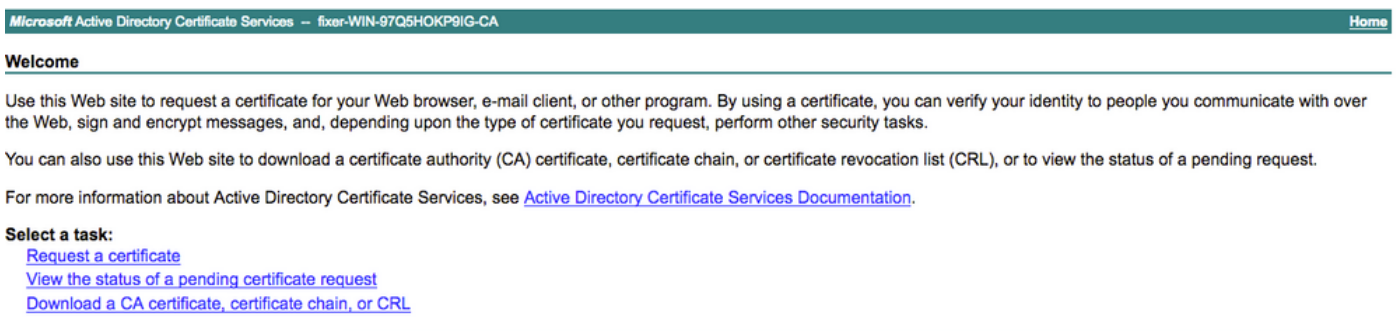
Paso 3. Para generar CSR, navegue hasta **Uso** y desde **Se utilizan los certificados para las opciones desplegables** seleccione **Autenticación EAP** como se muestra en la imagen.



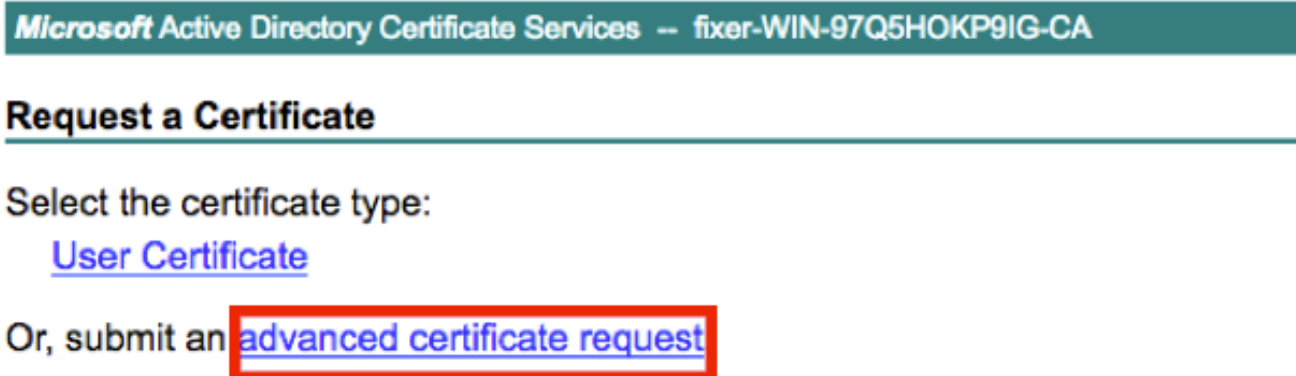
Paso 4. Se puede ver la CSR generada en ISE. Haga clic en **View** como se muestra en la imagen.



Paso 5. Una vez generado 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 solicite un certificado, obtendrá las opciones **Certificado de usuario** y **solicitud de certificado avanzado**, haga clic en **Solicitud de certificado avanzado** como se muestra en la imagen.



Paso 7. Pegue el CSR generado en la **solicitud de certificado codificado en Base-64**. En la **plantilla de certificado**: seleccione **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:

Additional Attributes:

Attributes:


Paso 8. Una vez que haga clic en **Submit**, tendrá la opción de seleccionar el tipo de certificado, seleccione **Base-64 codificado** y haga clic en **Download certificate chain** 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 completa para el servidor ISE. Puede extraer el certificado, el certificado contiene dos certificados, un certificado raíz y otro intermedio. El certificado raíz se puede importar en **Administration > Certificates > Trusted certificates > Import** como se muestra en las imágenes.

Identity Services Engine License Warning

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

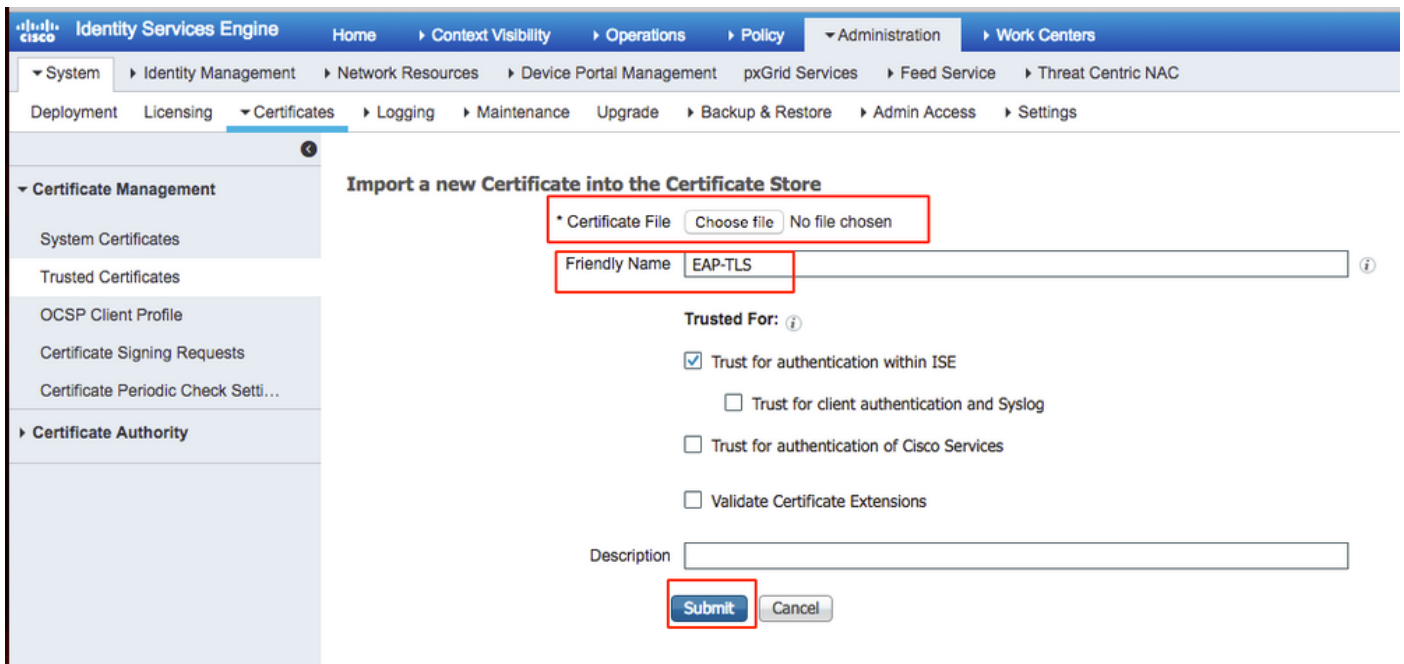
Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings

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

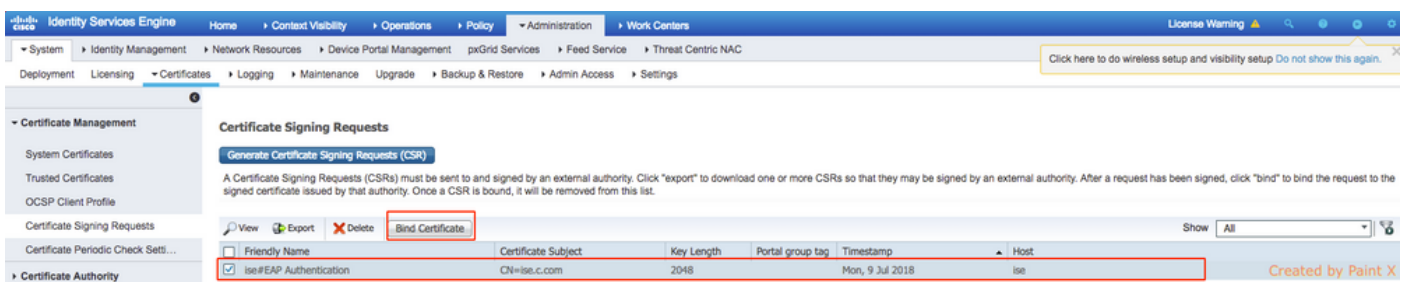
Trusted Certificates

Show All

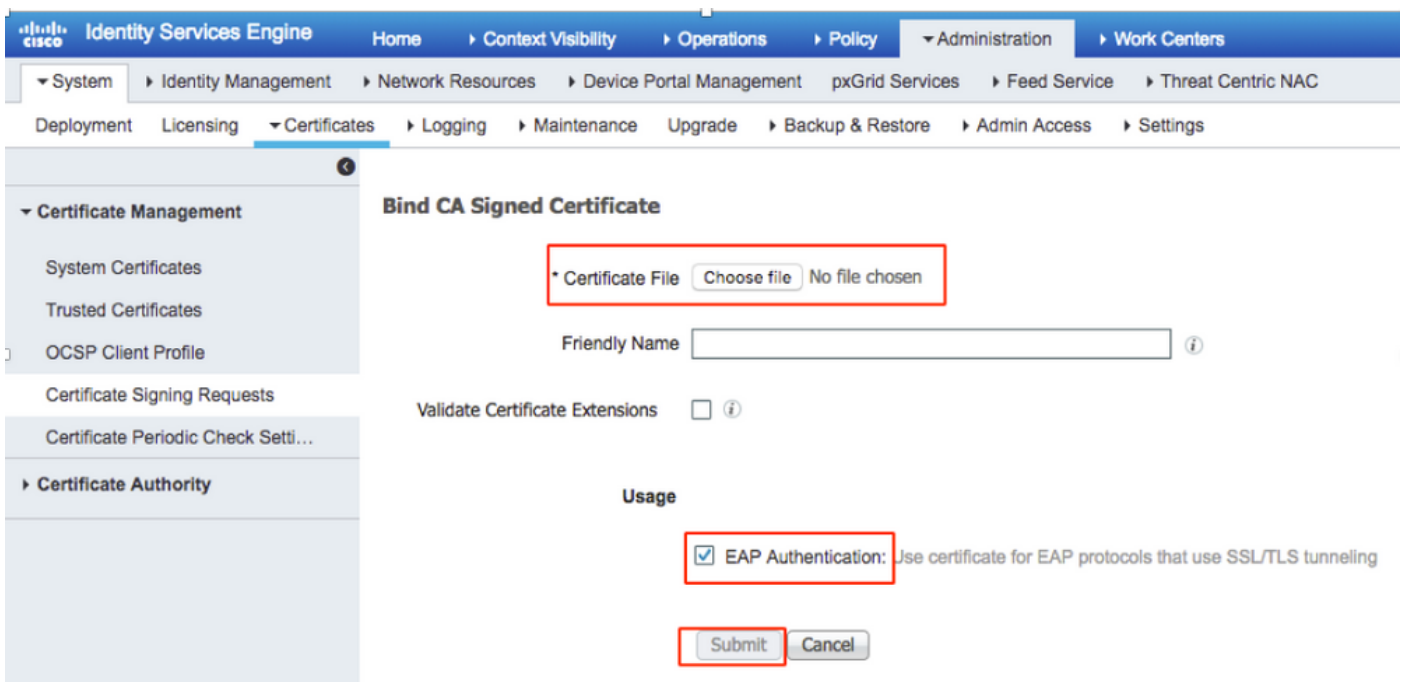
Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
---------------	--------	-------------	---------------	-----------	-----------	------------	-----------------



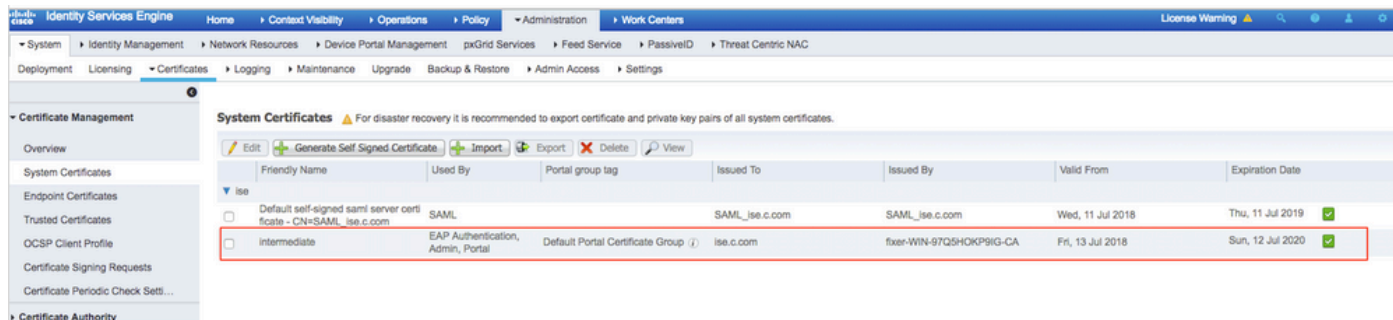
Paso 10. Una vez que haga clic en **Enviar**, el certificado se agrega a la lista de certificados de confianza. Además, el certificado intermedio es necesario para enlazar con CSR como se muestra en la imagen.



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 **Submit** como se muestra en la imagen.



Paso 12. Para ver el certificado, navegue hasta **Administration > Certificates > System Certificates** como se muestra en la imagen.



Cliente para EAP-TLS

Descargar certificado de usuario en el 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 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 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. Luego, 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 equipo portátil con Windows:

Paso 4. Para importar el certificado, debe tener acceso a él 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 **Certificates**.
4. **Seleccione Cuenta de equipo**.
5. Seleccione **Equipo local > Finalizar**
6. Haga clic en **Aceptar** para salir de la ventana Snap-In.
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 (Siguiete)**.
10. Haga clic en **Browse**.

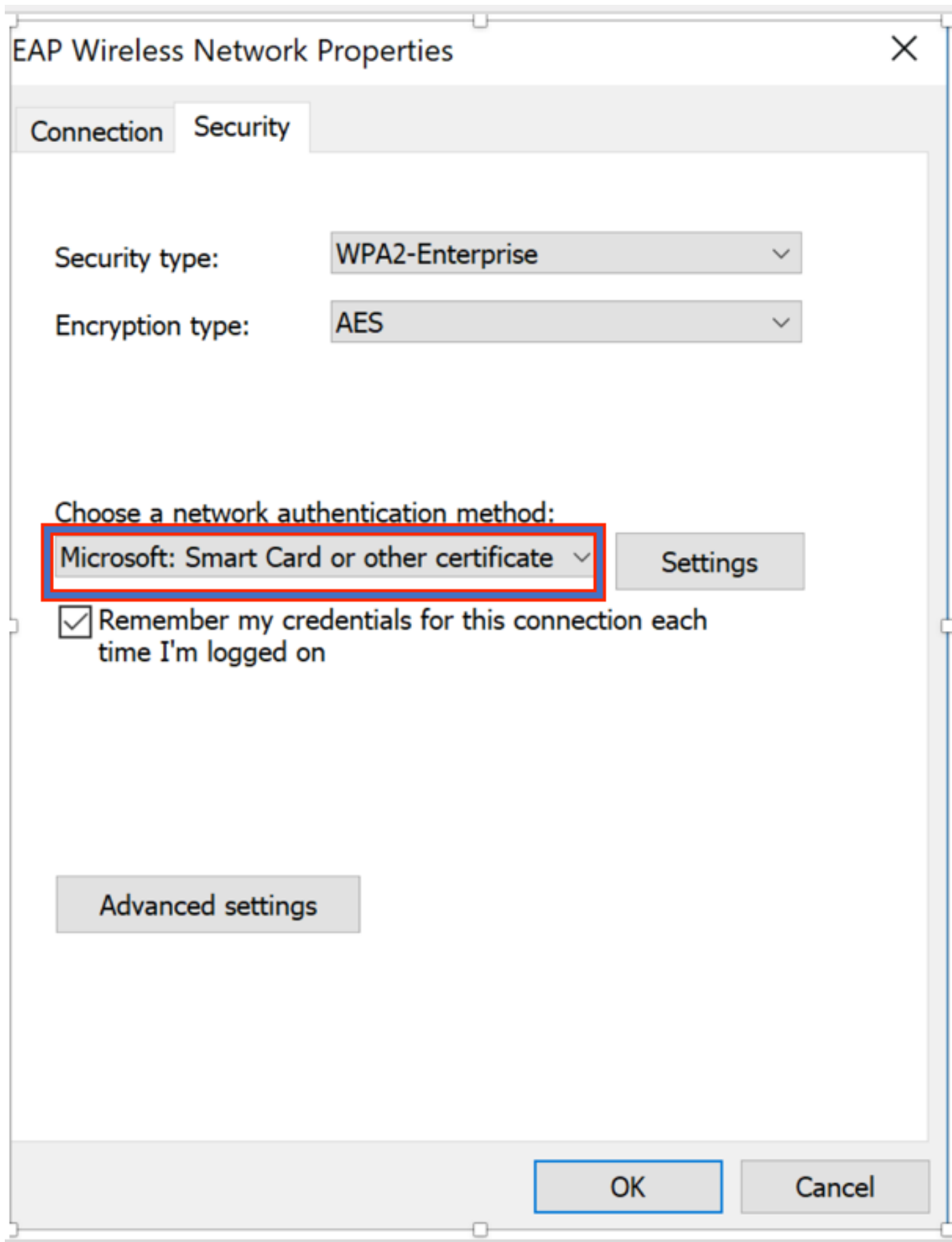
11. Seleccione el archivo **.cer, .crt o .pfx** que desee importar.
12. Haga clic en **Abrir**.
13. Haga clic en Next (Siguiente).
14. Seleccione **Seleccionar automáticamente el almacén de certificados según el tipo de certificado**.
15. Haga clic en **Finalizar y aceptar**

Una vez que haya terminado la importación del certificado, debe configurar el cliente inalámbrico (escritorio de Windows 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 el EAP-TLS en su lugar. Haga clic en **Perfil inalámbrico EAP**.

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



Paso 3. Haga clic en **configuración** 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 (Configuración 802.1x), 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

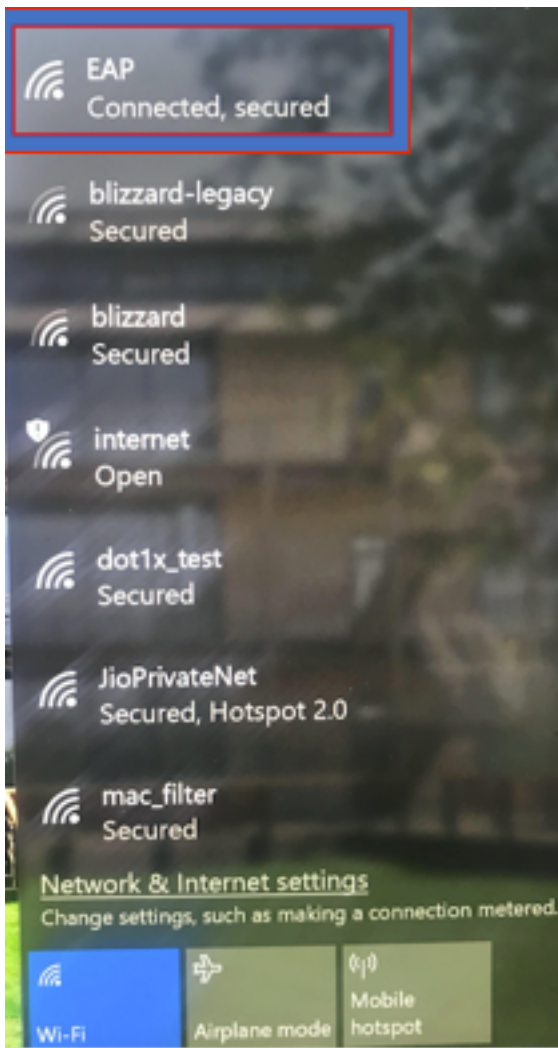
Maximum delay (seconds):

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 **Connect**. 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 estado del administrador de políticas de cliente debe mostrarse como **RUN**. Esto significa que el cliente ha completado la autenticación, obtenido la dirección IP y está listo para pasar el tráfico que se muestra en la imagen.

Monitor

Clients > Detail

Max Number of Records Clear AVC Stats

General **AVC Statistics**

Client Properties		AP Properties	
MAC Address	34:02:86:96:2f:b7	AP Address	00:d7:8f:52:db:a0
IPv4 Address	10.106.32.239	AP Name	Alpha2802_3rdfloor
IPv6 Address	fe80::2818:15a4:65f9:842,	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
Client Type	Simple IP	Reason Code	1
User Name	Administrator	Status Code	0
Port Number	1	CF Pollable	Not Implemented
Interface	management	CF Poll Request	Not Implemented
VLAN ID	32	Short Preamble	Not Implemented
Quarantine VLAN ID	0	PBCC	Not Implemented
CCX Version	CCXv1	Channel Agility	Not Implemented
E2E Version	Not Supported	Re-authentication timeout	1682
Mobility Role	Local	Remaining Re-authentication timeout	0
Mobility Peer IP Address	N/A	WEP State	WEP Enable
Mobility Move Count	0		
Policy Manager State	RUN		
Management Frame Protection	No		
UpTime (Sec)	146		

Lync Properties	
Lync State	Disabled
Audio Qos Policy	Silver

Paso 2. Verifique también el método EAP correcto en el WLC en la página de detalles del cliente como se muestra en la imagen.

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

Paso 3. Aquí están los detalles del cliente de CLI del controlador (salida recortada):

```
(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

Paso 4. En ISE, navegue hasta **Visibilidad del contexto > Terminales > Atributos** como se muestra en las imágenes.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below this, there are tabs for 'Endpoints' and 'Network Devices'. The main content area shows the MAC address '34:02:86:96:2F:B7' and its details: 'MAC Address: 34:02:86:96:2F:B7', 'Username: Administrator@flxer.com', 'Endpoint Profile: Intel-Device', 'Current IP Address:', and 'Location:'. Below this, there are tabs for 'Attributes', 'Authentication', 'Threats', and 'Vulnerabilities'. The 'Attributes' tab is selected, showing 'General Attributes' and 'Custom Attributes' sections. The 'General Attributes' section lists: 'Static Assignment: false', 'Endpoint Policy: Intel-Device', 'Static Group Assignment: false', and 'Identity Group Assignment: Profiled'. The 'Custom Attributes' section is empty, with a message 'No data found. Add custom attributes here.' and a 'Filter' button. Below this, there is a table for 'Other Attributes' with the following data:

Attribute Name	Attribute Value
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

BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
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, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

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

Actualmente no hay información específica disponible para resolver problemas de esta configuración.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).