# Entender e configurar EAP-TLS com Mobility Express e ISE

## Contents



## Introduction

Este documento descreve como configurar uma rede local sem fio (WLAN) com segurança 802.1x em um controlador Mobility Express. Este documento também explica especificamente o uso do Extensible Authentication Protocol (EAP) - Transport Layer Security (TLS).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração inicial do Mobility Express
- processo de autenticação 802.1x
- Certificados

### Componentes Utilizados

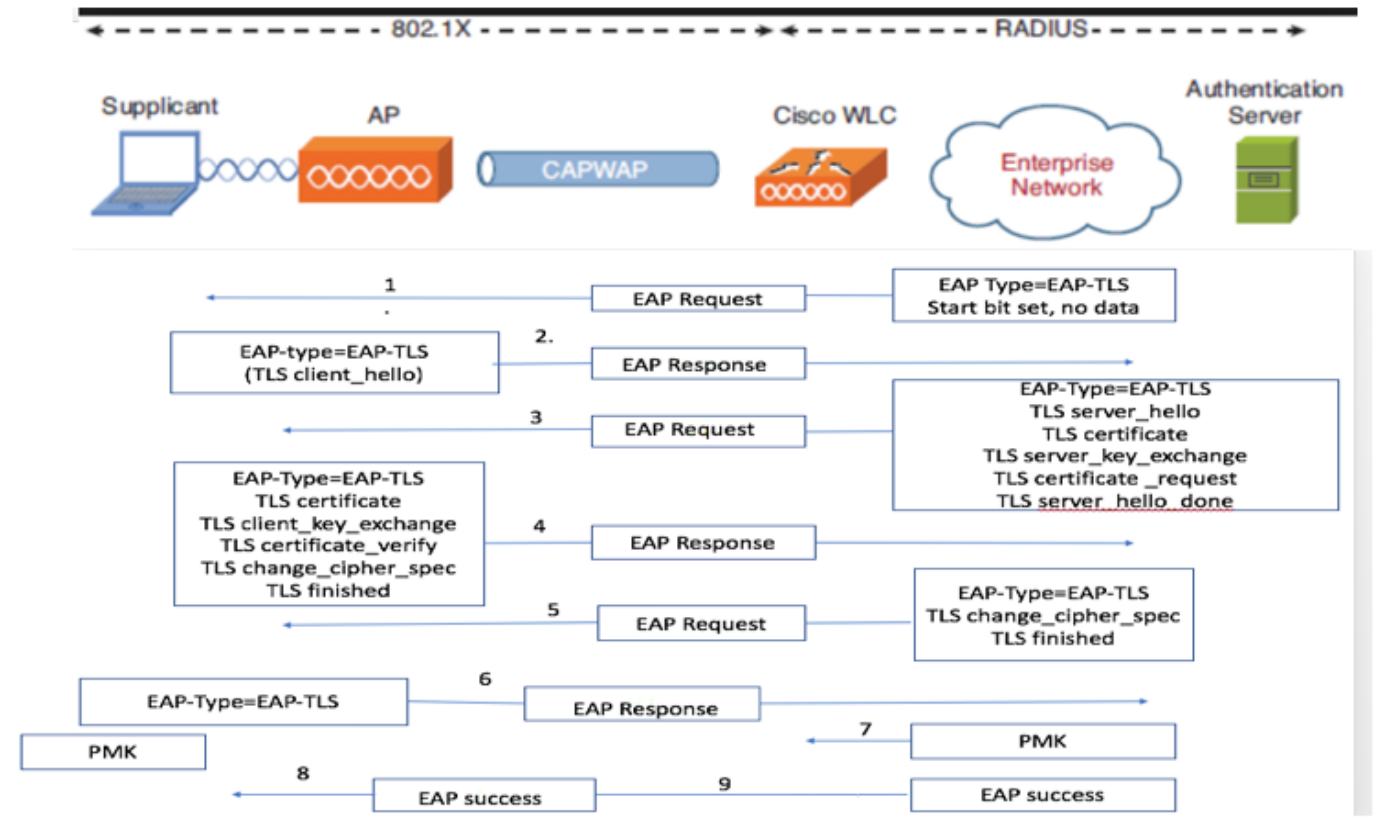
As informações neste documento são baseadas nestas versões de software e hardware:

- WLC 5508 versão 8.5
- Identity Services Engine (ISE) versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

## Fluxo EAP-TLS




### Etapas do fluxo EAP-TLS

1. O cliente sem fio é associado ao ponto de acesso (AP).
2. O AP não permite que o cliente envie dados neste momento e envia uma solicitação de autenticação.
3. Em seguida, o requerente responde com uma identidade EAP-Response. Em seguida, a WLC comunica as informações de ID de usuário ao Servidor de autenticação.
4. O servidor RADIUS responde de volta ao cliente com um pacote de início EAP-TLS. A conversação EAP-TLS começa neste ponto.
5. O peer envia uma Resposta EAP de volta ao servidor de autenticação que contém uma mensagem de handshake "client_hello", uma cifra definida para NULL.
6. O servidor de autenticação responde com um pacote de desafio de acesso que contém:

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

7. O cliente responde com uma mensagem EAP-Response que contém:

```
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
```

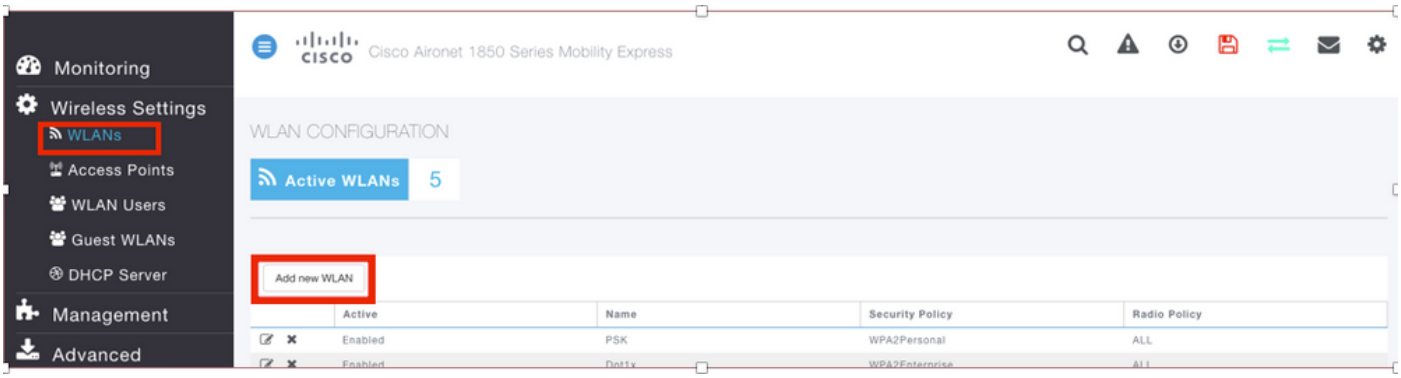
8. Depois que o cliente se autentica com êxito, o servidor RADIUS responde com um desafio de acesso, que contém a mensagem "change_cipher_spec" e handshake concluído. Ao receber isso, o cliente verifica o hash para autenticar o servidor RADIUS. Uma nova chave de criptografia é derivada dinamicamente do segredo durante o handshake TLS.

9. Neste ponto, o cliente sem fio EAP-TLS ativado pode acessar a rede sem fio.

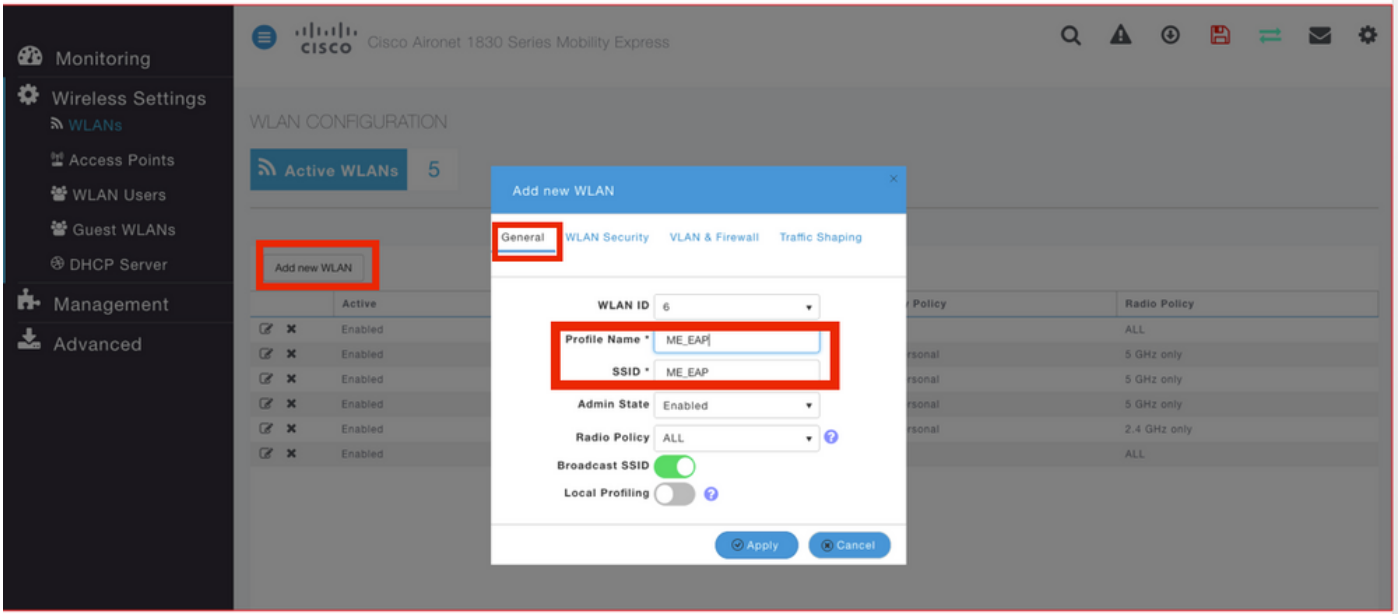
# Configurar

## Cisco Mobility Express

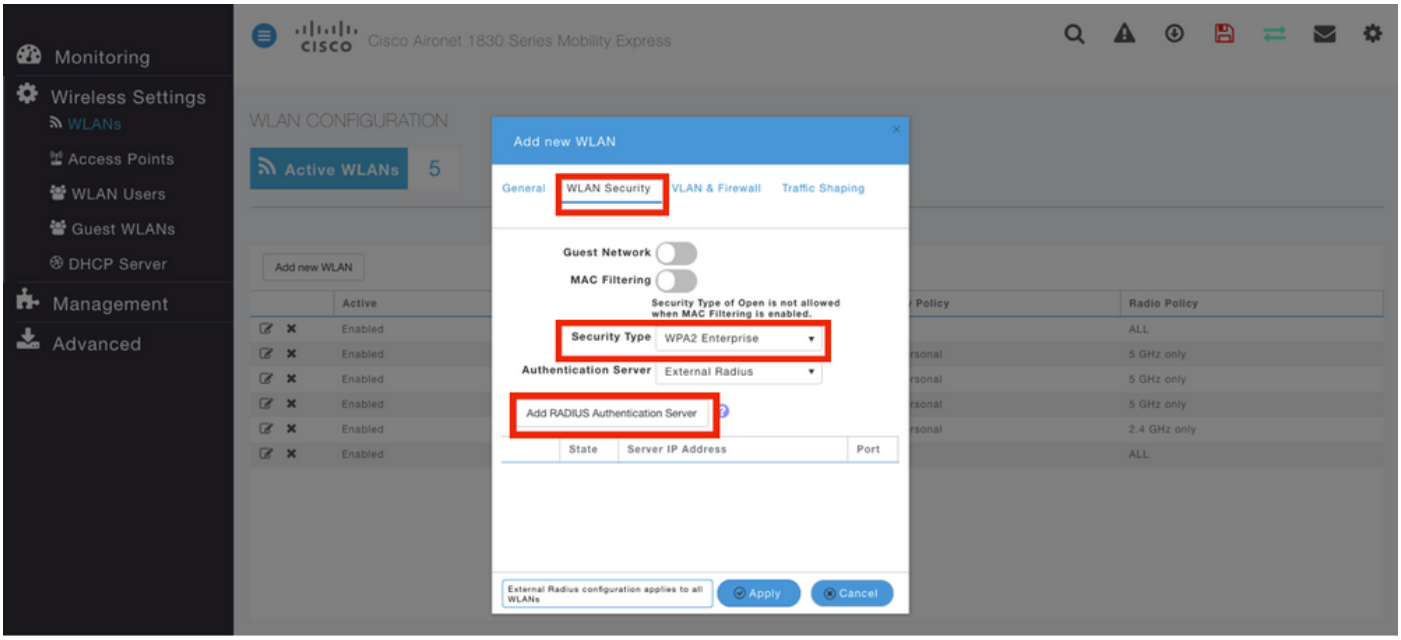
Etapa 1. A primeira etapa é criar uma WLAN no Mobility Express. Para criar uma WLAN, navegue até **WLAN > Add new WLAN** como mostrado na imagem.



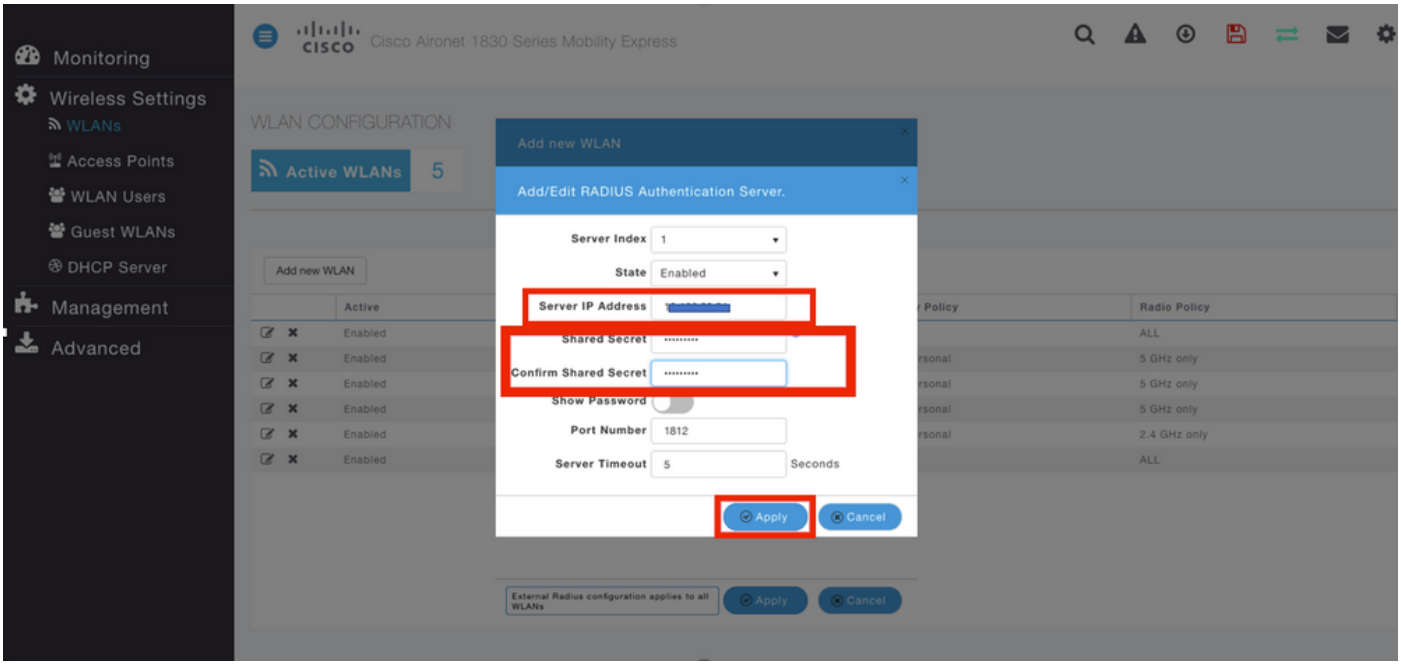

Etapa 2. Uma nova janela pop-up será exibida quando você clicar em **Adicionar nova WLAN**. Para criar um nome de perfil, navegue até **Add new WLAN > General**, como mostrado na imagem.




Etapa 3. Configure o tipo de autenticação como WPA Enterprise para 802.1x e configure o servidor RADIUS em **Adicionar nova WLAN > Segurança WLAN**, como mostrado na imagem.




Etapa 4. Clique em **Add RADIUS Authentication Server** e forneça o endereço IP do servidor RADIUS e do segredo compartilhado que devem corresponder exatamente ao que foi configurado no ISE e clique em **Apply** conforme mostrado na imagem.



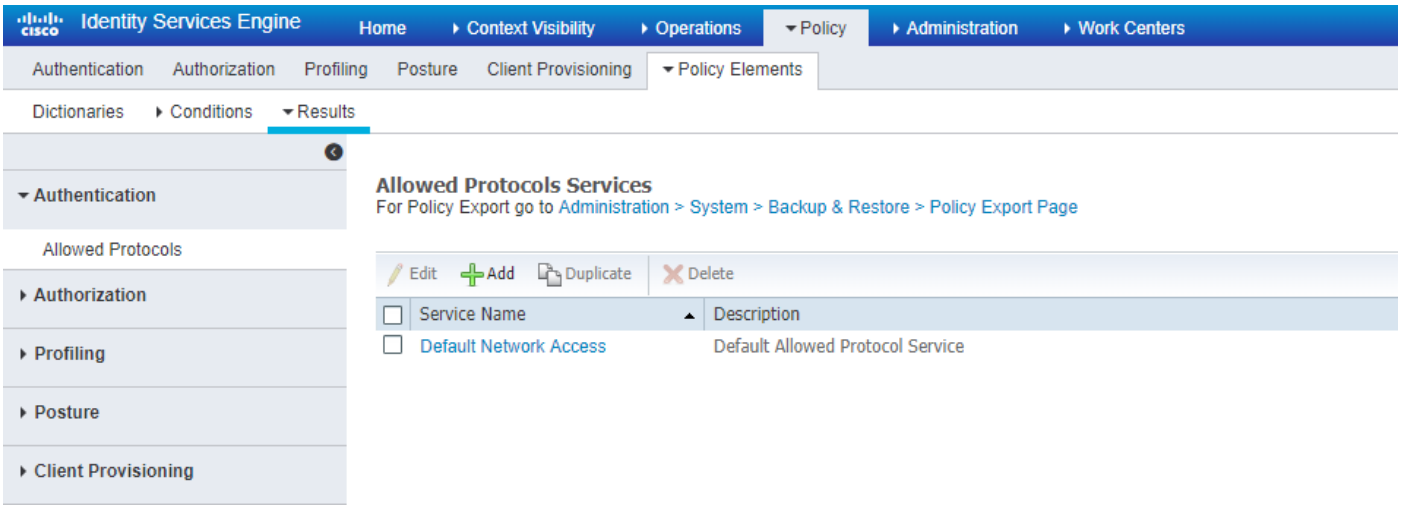

## ISE com Cisco Mobility Express

### Configurações EAP-TLS

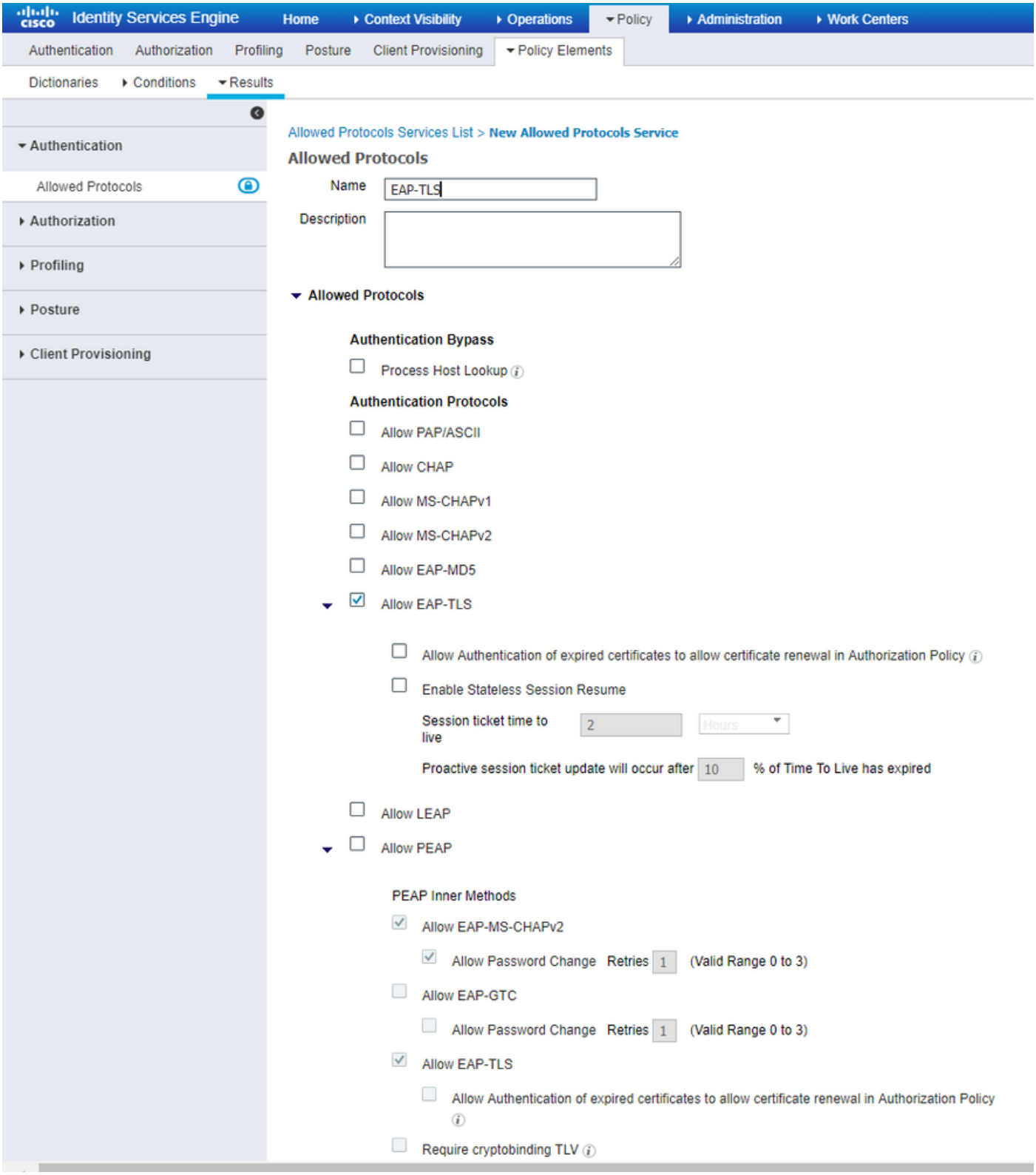
Para criar a política, você precisa criar a lista de protocolos permitidos para usar em sua política. Como uma política dot1x é gravada, especifique o tipo de EAP permitido com base em como a política é configurada.

Se você usar o padrão, você permitirá a maioria dos tipos de EAP para autenticação que talvez não seja preferível se precisar bloquear o acesso a um tipo específico de EAP.

Etapa 1. Navegue até **Política > Elementos de política > Resultados > Autenticação > Protocolos permitidos** e clique em **Adicionar** conforme mostrado na imagem.

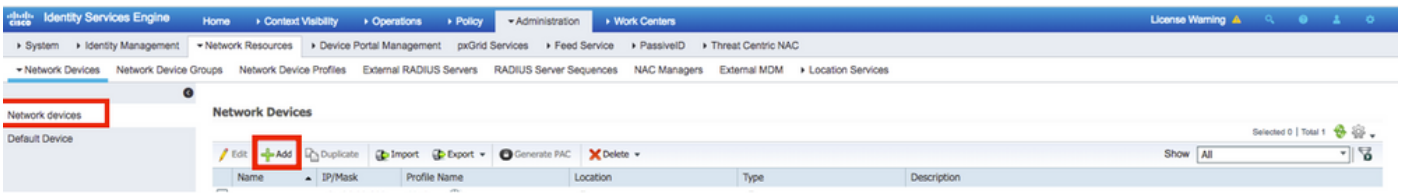



Etapa 2. Nessa lista de Protocolos Permitidos, você pode digitar o nome da lista. Nesse caso, a caixa **Permitir EAP-TLS** está marcada e outras caixas estão desmarcadas, como mostrado na imagem.

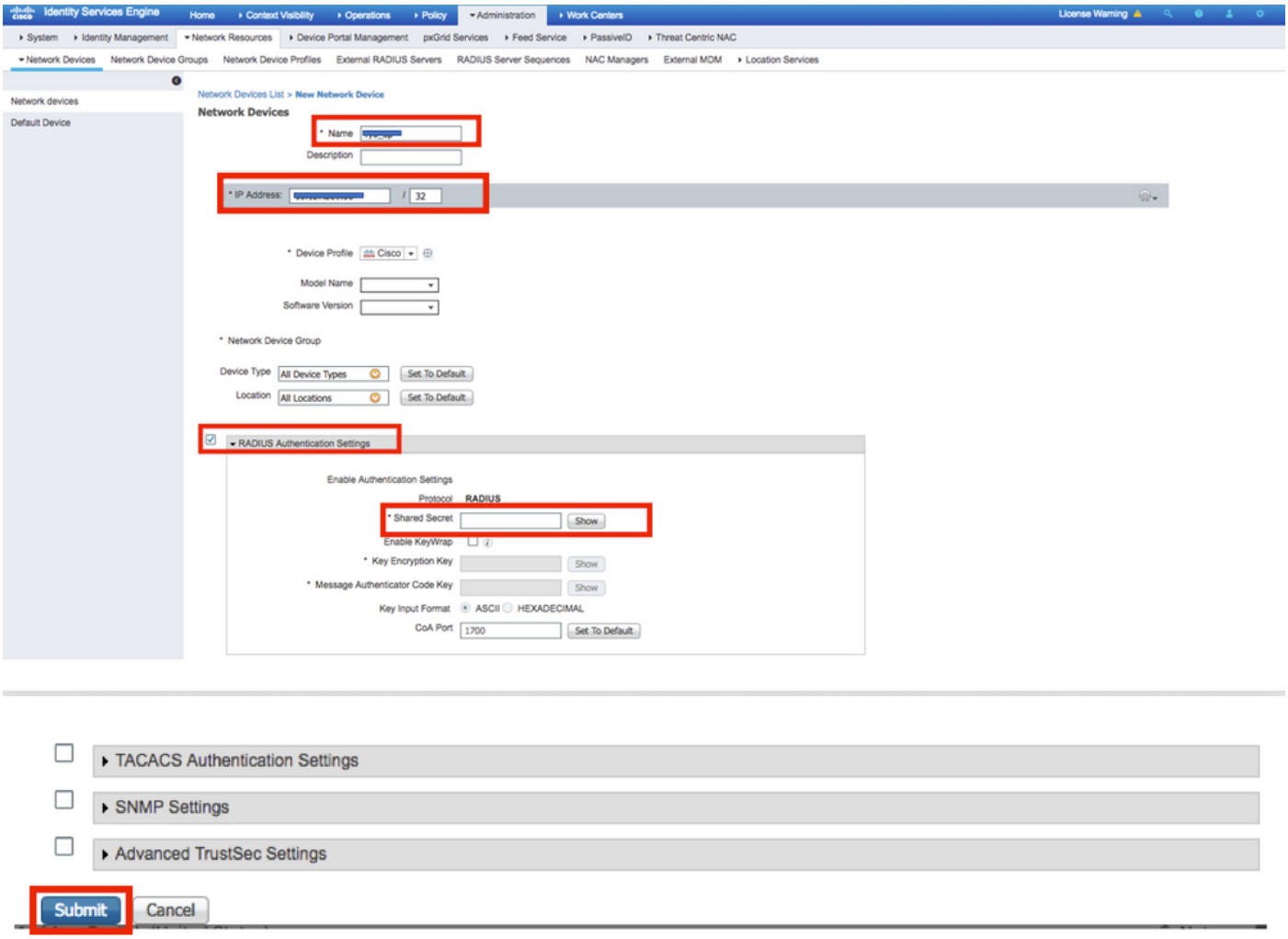



## Configurações do Mobility Express no ISE

Etapa 1. Abra o console do ISE e navegue até **Administration > Network Resources > Network Devices > Add**, como mostrado na imagem.



Etapa 2. Insira as informações conforme mostrado na imagem.





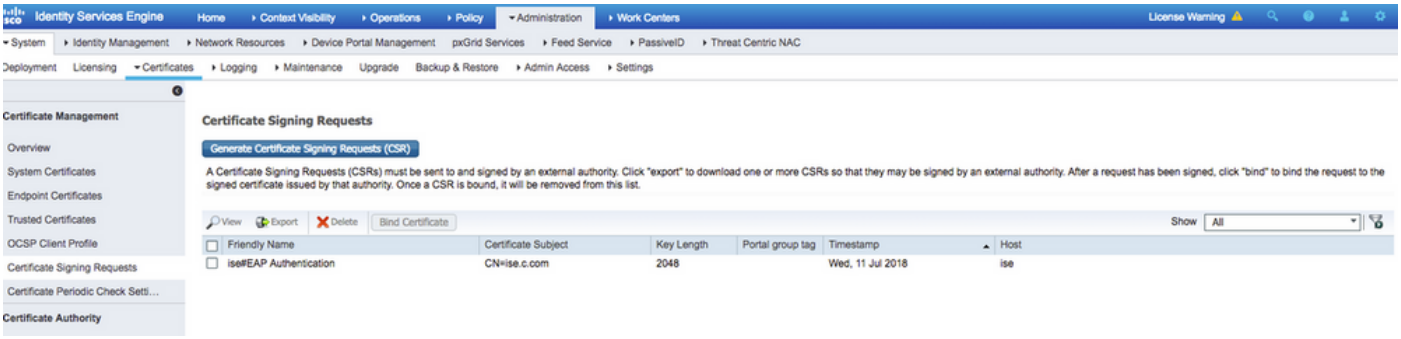


## Certificado de Confiança no ISE

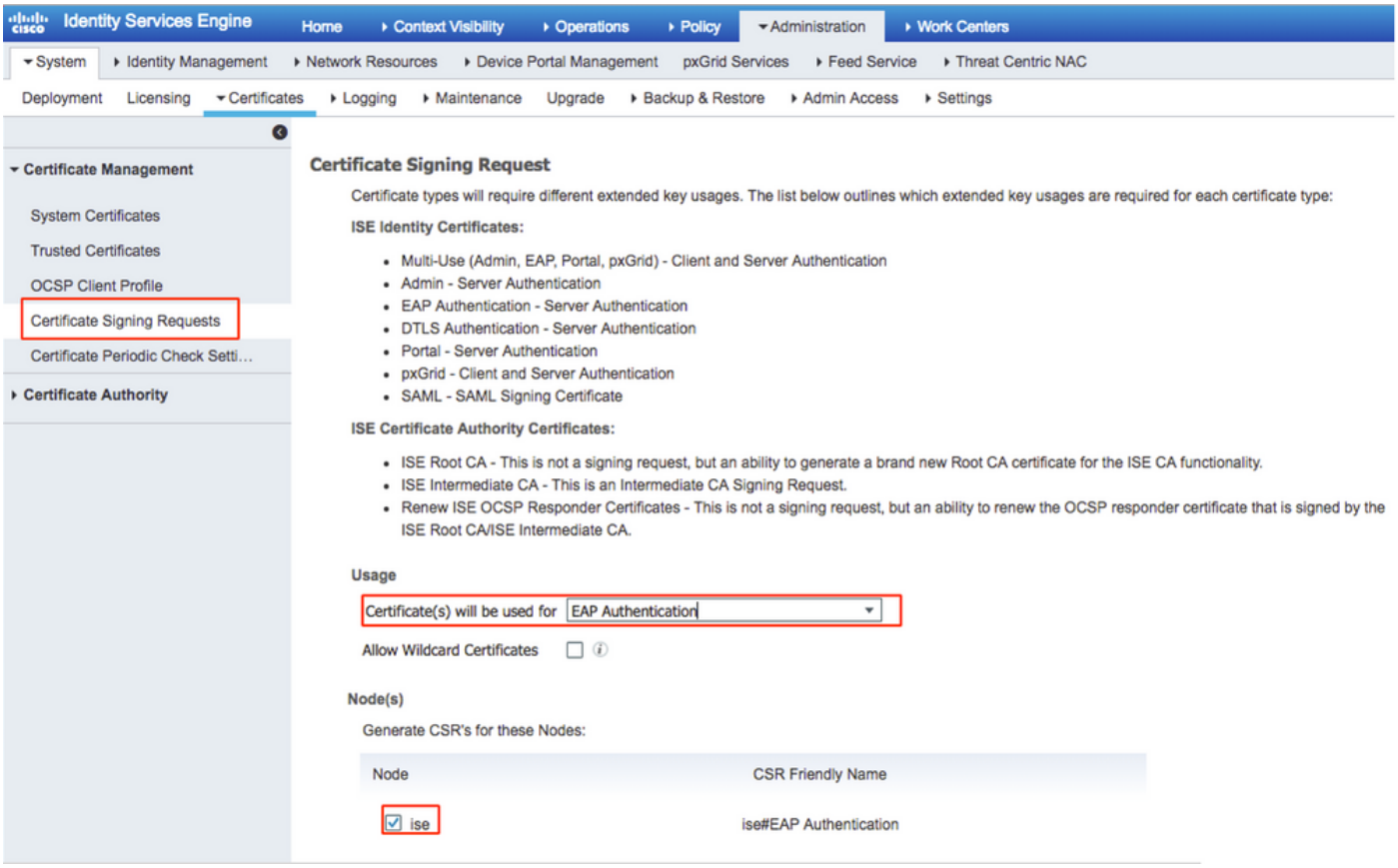
Etapa 1. Navegue até **Administração > Sistema > Certificados > Gerenciamento de Certificados > Certificados Confiáveis**.

Clique em **Importar** para importar um certificado para o ISE. Depois de adicionar uma WLC e criar um usuário no ISE, você precisa fazer a parte mais importante do EAP-TLS que é confiar no certificado no ISE. Para isso, você precisa gerar CSR.

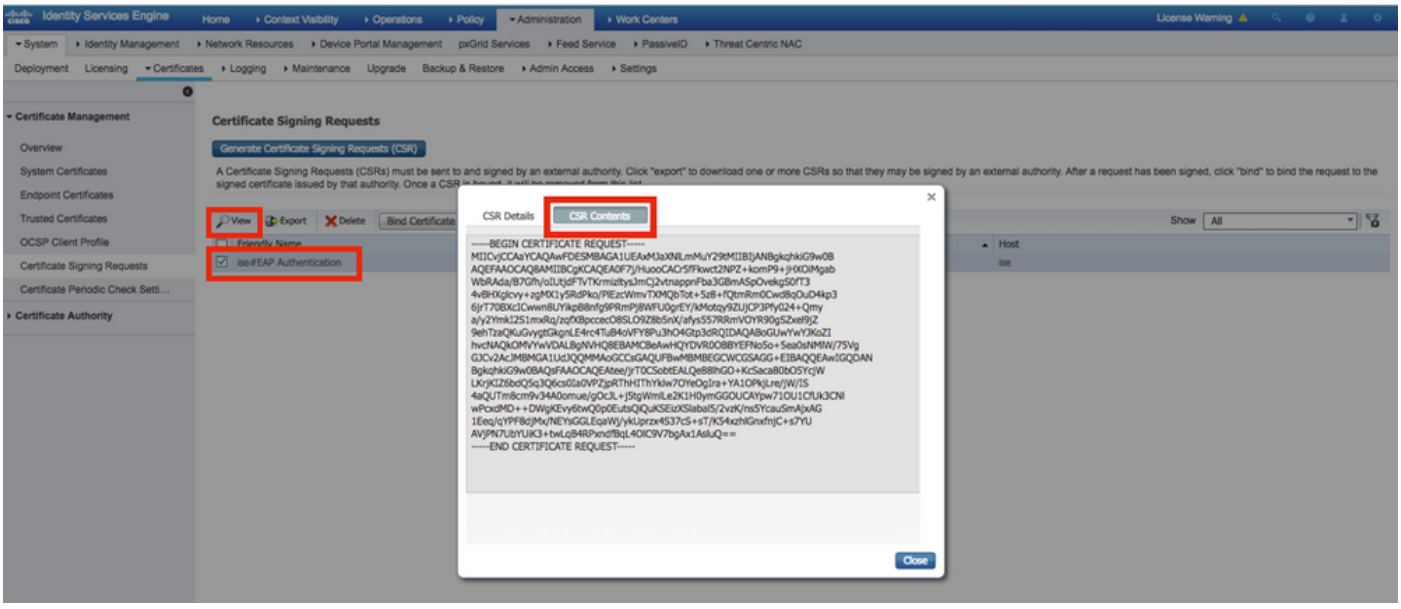
Etapa 2. Navegue até **Administrador > Certificados > Solicitações de Assinatura de Certificado > Gerar Solicitações de Assinatura de Certificado (CSR)** conforme mostrado na imagem.



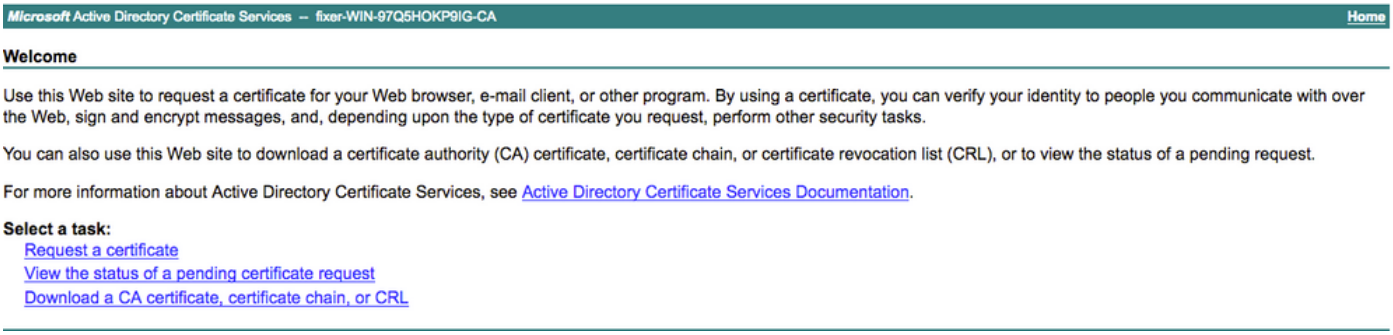

Etapa 3. Para gerar CSR, navegue até **Usage** e, a partir dos **certificados, os certificados serão usados para** as opções suspensas, selecione **EAP Authentication** como mostrado na imagem.



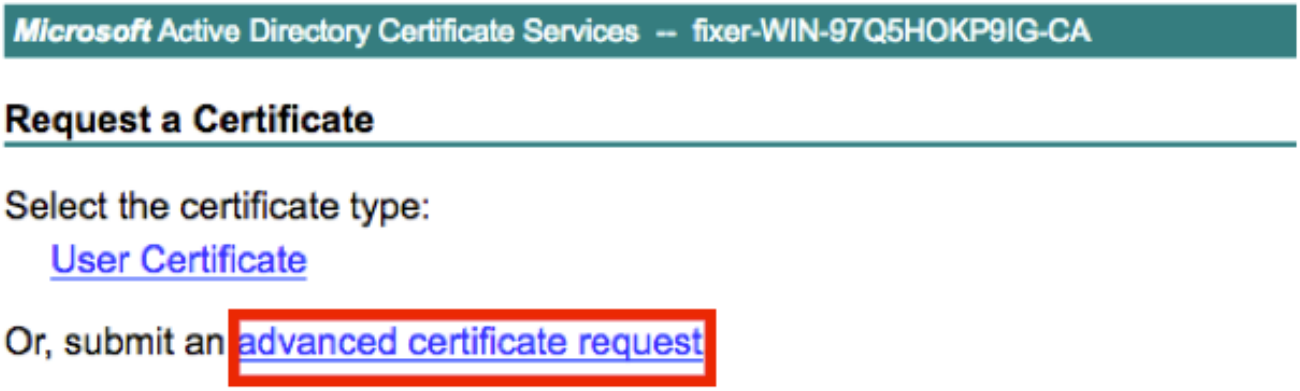

Etapa 4. O CSR gerado no ISE pode ser visualizado. Clique em **Exibir** conforme mostrado na imagem.



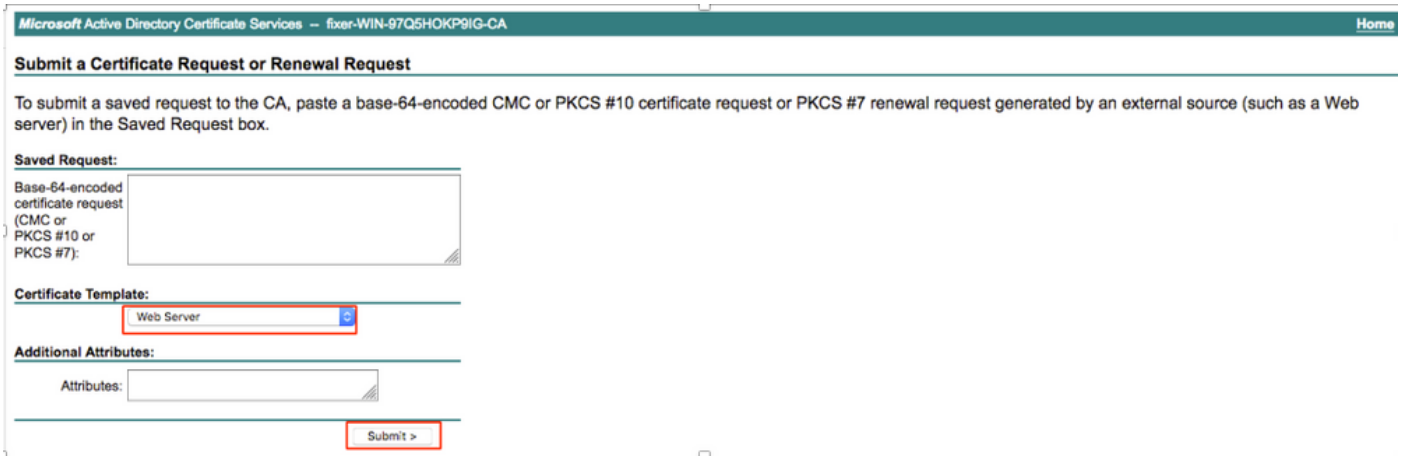

Etapa 5. Depois que o CSR for gerado, procure o servidor CA e clique em **Solicitar um certificado** conforme mostrado na imagem:



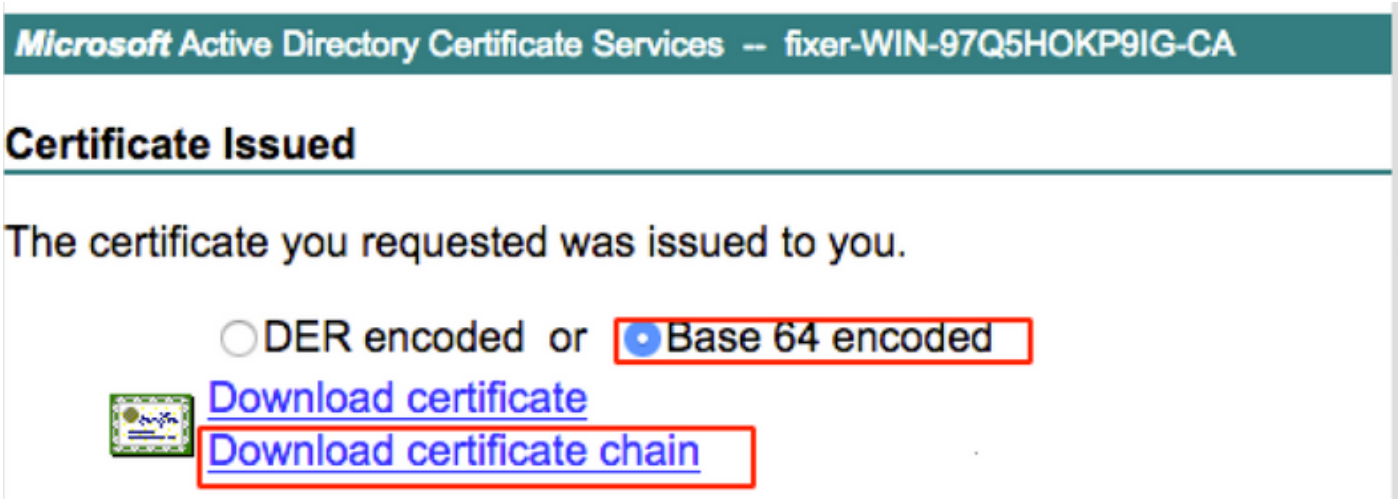

Etapa 6. Depois de solicitar um certificado, você obtém opções para **Certificado do usuário** e **solicitação de certificado avançado**, clique em **solicitação de certificado avançado** como mostrado na imagem.



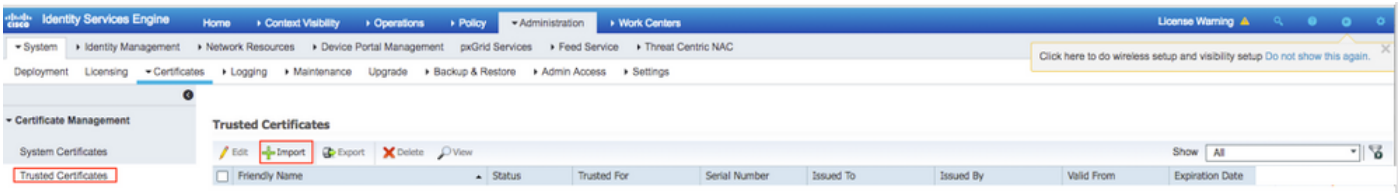

Passo 7. Cole o CSR gerado na **solicitação de certificado codificada em Base 64**. Na opção suspensa **Modelo de certificado:**, escolha **Servidor Web** e clique em **Enviar** conforme mostrado na imagem.

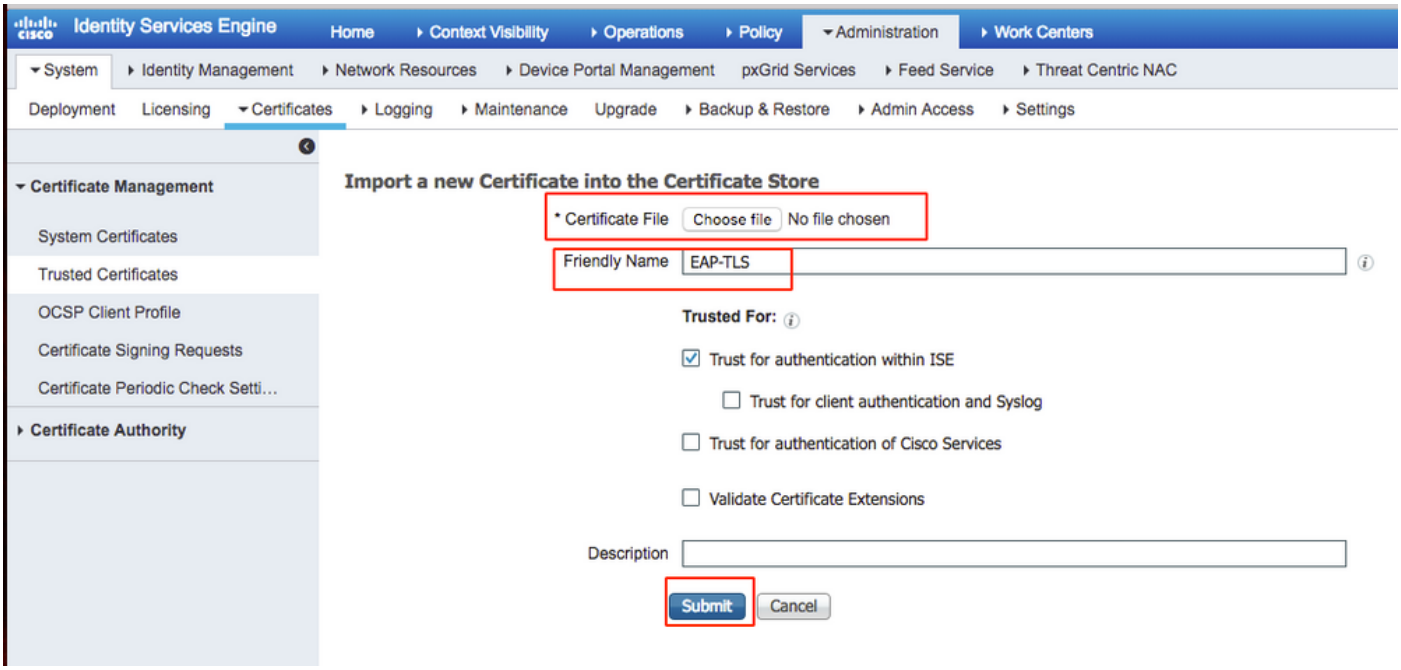



Etapa 8. Depois de clicar em **Enviar**, você terá a opção de selecionar o tipo de certificado, selecionar **Base 64 codificado** e clicar em **Baixar cadeia de certificados** como mostrado na imagem.

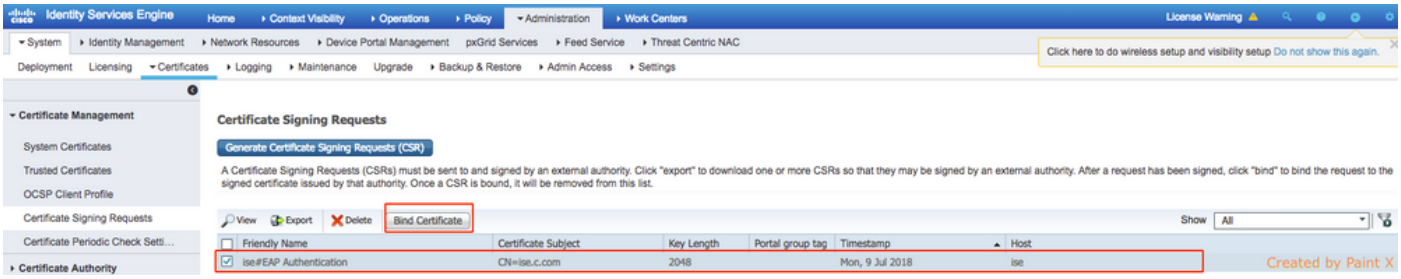



Etapa 9. O download do certificado foi concluído para o servidor ISE. Você pode extrair o certificado, o certificado conterá dois certificados, um certificado raiz e outro intermediário. O certificado raiz pode ser importado em **Administração > Certificados > Certificados Confiáveis > Importar** como mostrado nas imagens.

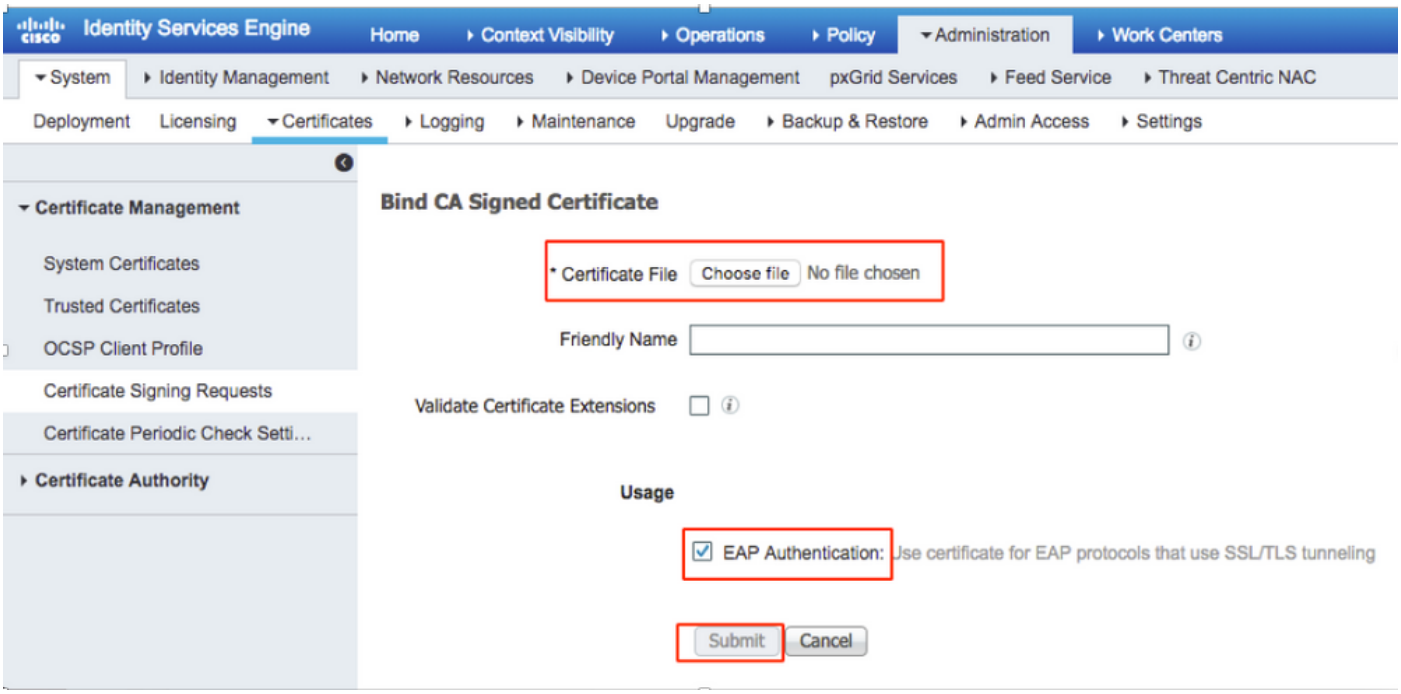


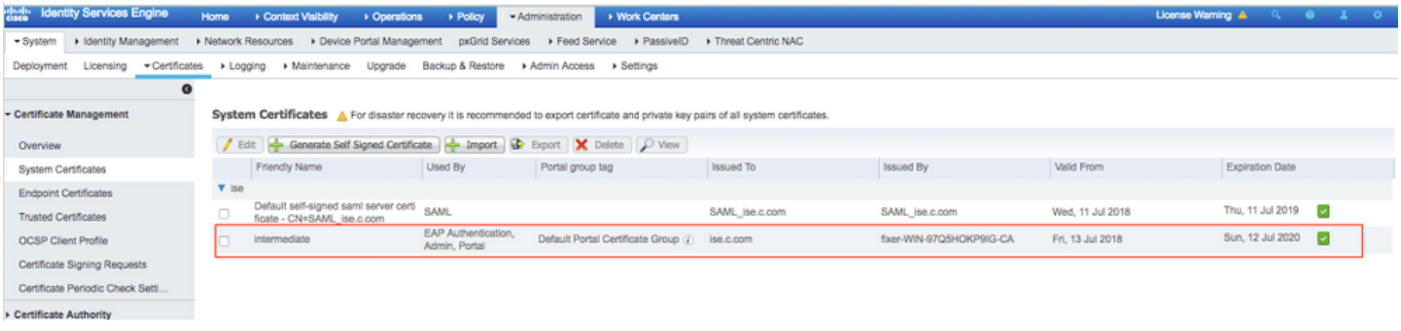

Etapa 10. Depois de clicar em **Enviar**, o certificado é adicionado à lista de certificados fidedignos. Além disso, o certificado intermediário é necessário para se vincular ao CSR, como mostrado na imagem.




Etapa 11. Depois de clicar em **Vincular certificado**, há uma opção para escolher o arquivo de certificado salvo em sua área de trabalho. Navegue até o certificado intermediário e clique em **Enviar** conforme mostrado na imagem.




Etapa 12. Para visualizar o certificado, navegue para **Administração > Certificados > Certificados do Sistema**, conforme mostrado na imagem.



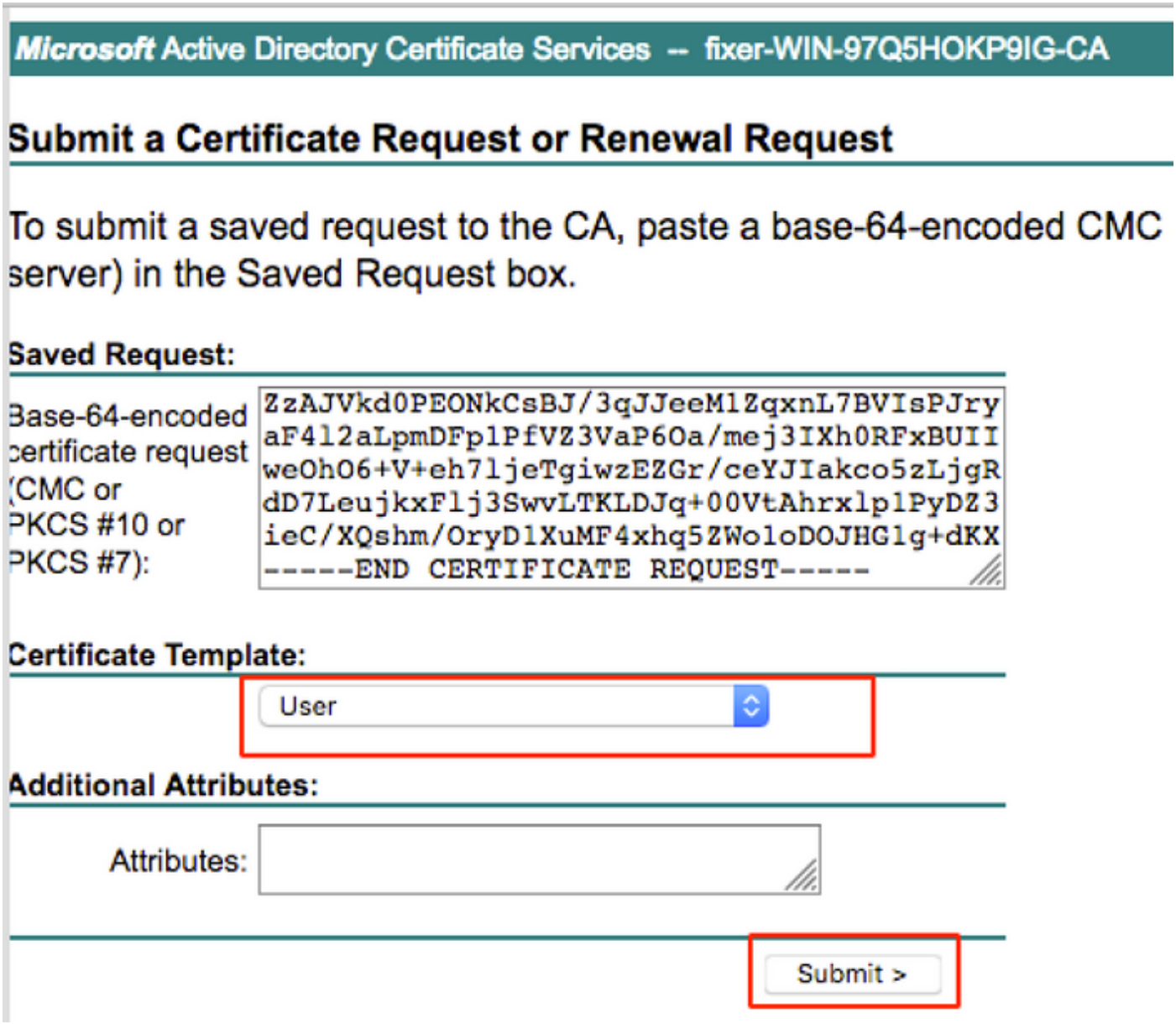

## Cliente para EAP-TLS

### Fazer download do certificado do usuário na máquina cliente (Windows Desktop)

Etapa 1. Para autenticar um usuário sem fio por meio do EAP-TLS, você precisa gerar um certificado de cliente. Conecte seu computador Windows à rede para que você possa acessar o servidor. Abra um navegador da Web e digite este endereço: [https://sever ip addr/certsrv—](https://sever ip addr/certsrv—)

Etapa 2. Observe que a CA deve ser a mesma com a qual o certificado foi baixado para o ISE.

Para isso, você precisa procurar o mesmo servidor CA que você usou para baixar o certificado para o servidor. Na mesma CA, clique em **Solicitar um certificado** como feito anteriormente, mas desta vez você precisa selecionar **Usuário** como o Modelo de certificado como mostrado na imagem.




Etapa 3. Em seguida, clique em **baixar a cadeia de certificados** como foi feito anteriormente para o servidor.

Depois de obter os certificados, siga estas etapas para importar o certificado no windows laptop.

Etapa 4. Para importar o certificado, você precisa acessá-lo do Console de Gerenciamento da Microsoft (MMC).

1. Para abrir o MMC, navegue até **Start > Run > MMC**.
2. Navegue até **Arquivo > Adicionar/remover snap-in**
3. Clique Duas Vezes Em **Certificados**.
4. Selecione **Conta do computador**.
5. Selecione **Computador local > Concluir**
6. Clique em **OK** para sair da janela Snap-In.
7. Clique em **[+]** ao lado de **Certificados > Pessoal > Certificados**.

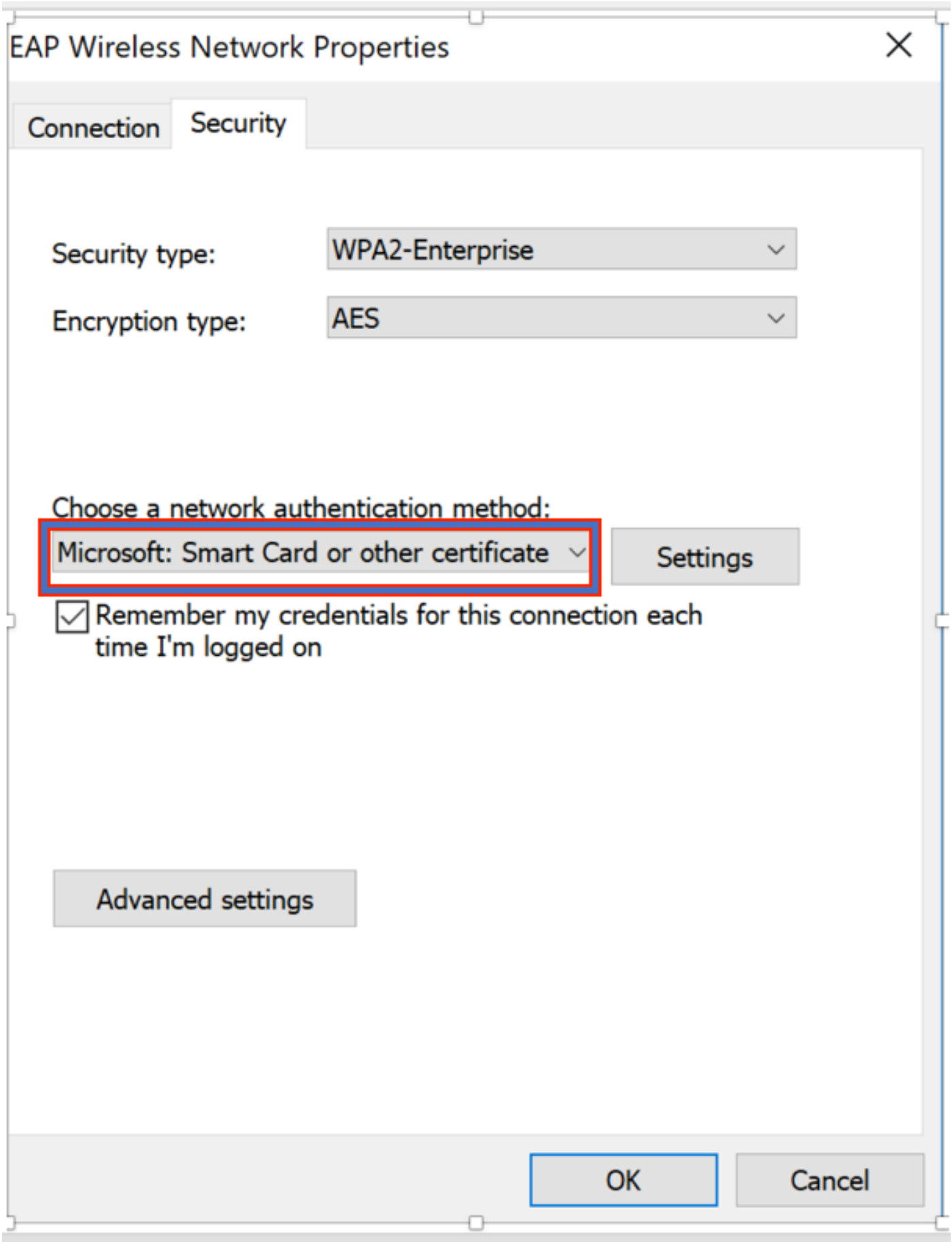
8. Clique com o botão direito em **Certificados** e selecione **Todas as Tarefas > Importar**.
9. Clique em Next.
10. Clique em **Procurar**.
11. Selecione o **.cer, .crt ou .pfx** que deseja importar.
12. Clique em **Abrir**.
13. Clique em Next.
14. Selecione **Selecionar automaticamente o arquivo de certificados com base no tipo de certificado**.
15. Clique em **Concluir e OK**

Quando a importação do certificado estiver concluída, você precisará configurar seu cliente sem fio (desktop do windows neste exemplo) para EAP-TLS.

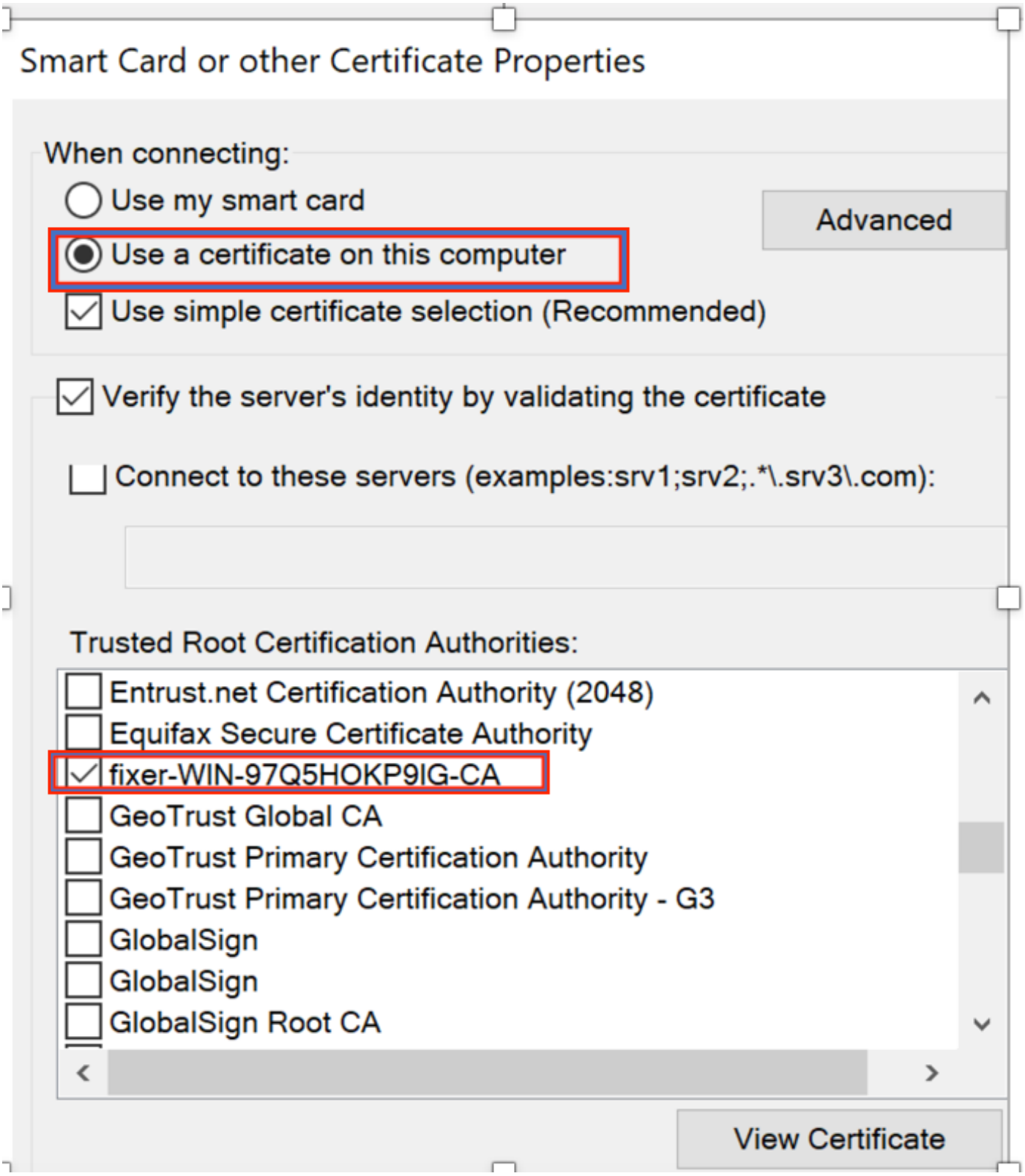
## Perfil sem fio para EAP-TLS

Etapa 1. Altere o perfil sem fio criado anteriormente para o PEAP (Protected Extensible Authentication Protocol) para usar EAP-TLS. Clique em **EAP Wireless Profile**.

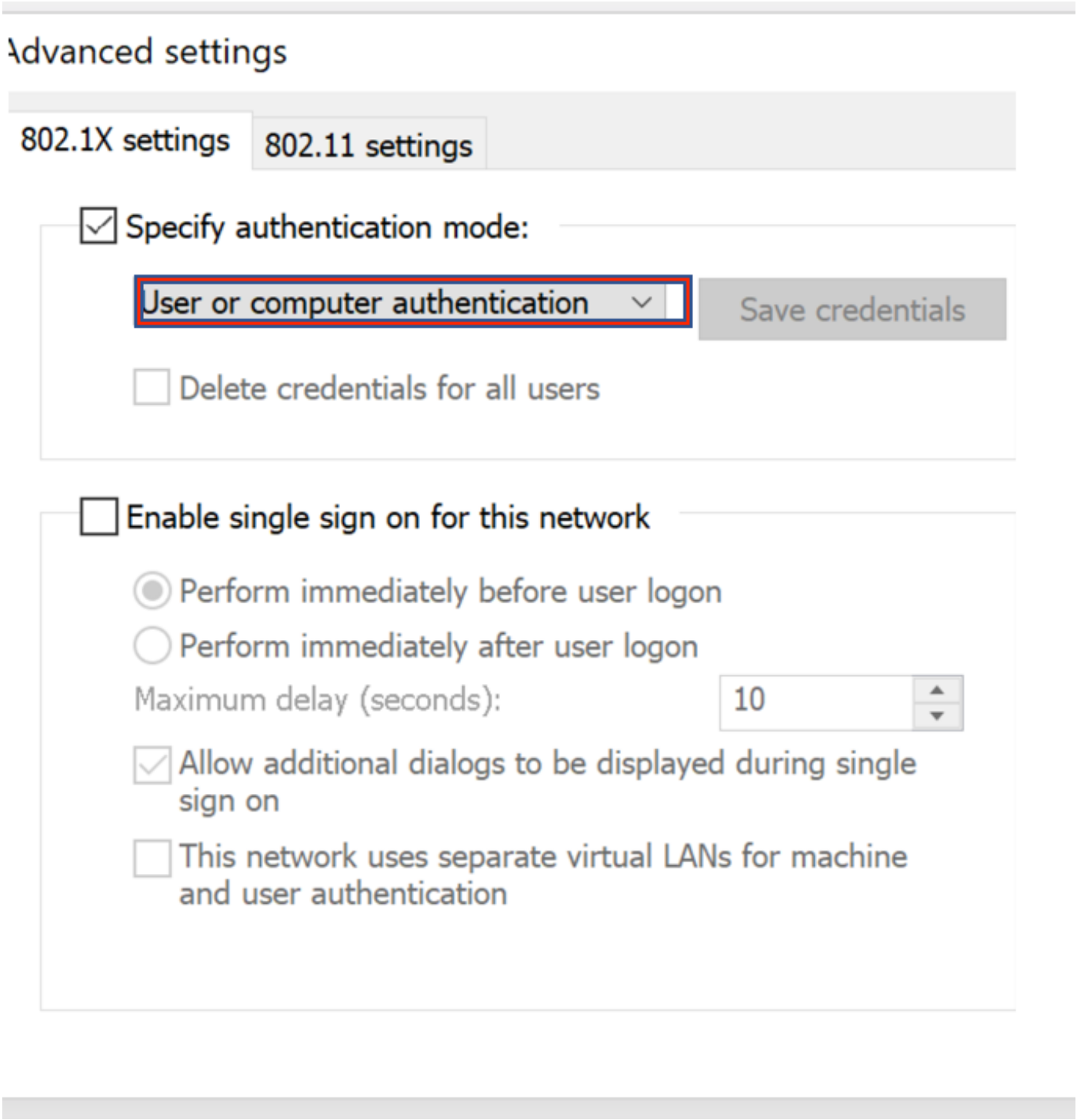
Etapa 2. Selecione **Microsoft: Smart Card ou outro certificado** e clique em **OK** conforme mostrado na imagem.



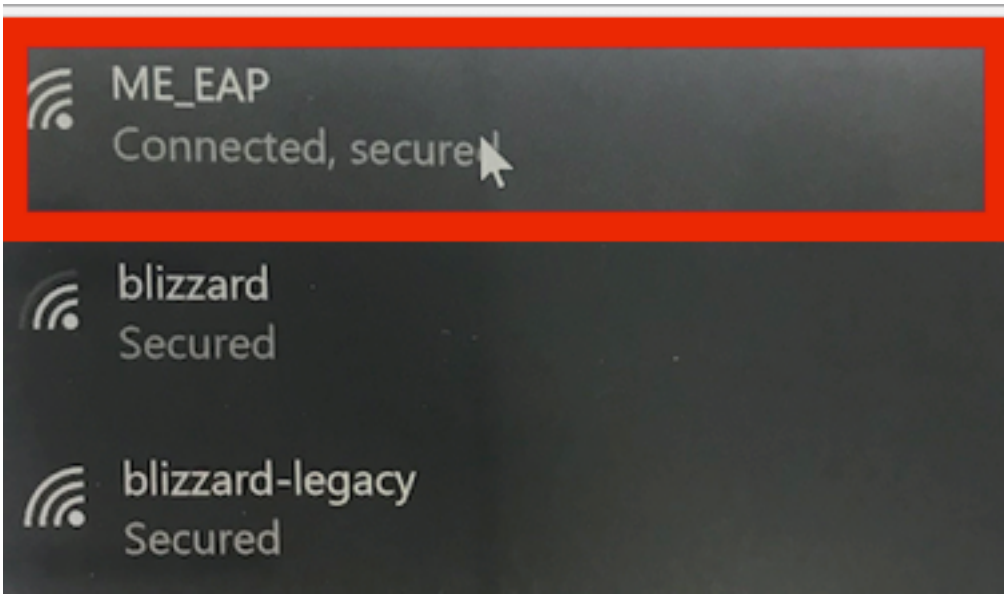

Etapa 3. Clique em **Configurações** e selecione o certificado raiz emitido do servidor CA como mostrado na imagem.




Etapa 4. Clique em **Configurações avançadas** e selecione **Autenticação de usuário ou computador** na guia Configurações 802.1x, conforme mostrado na imagem.



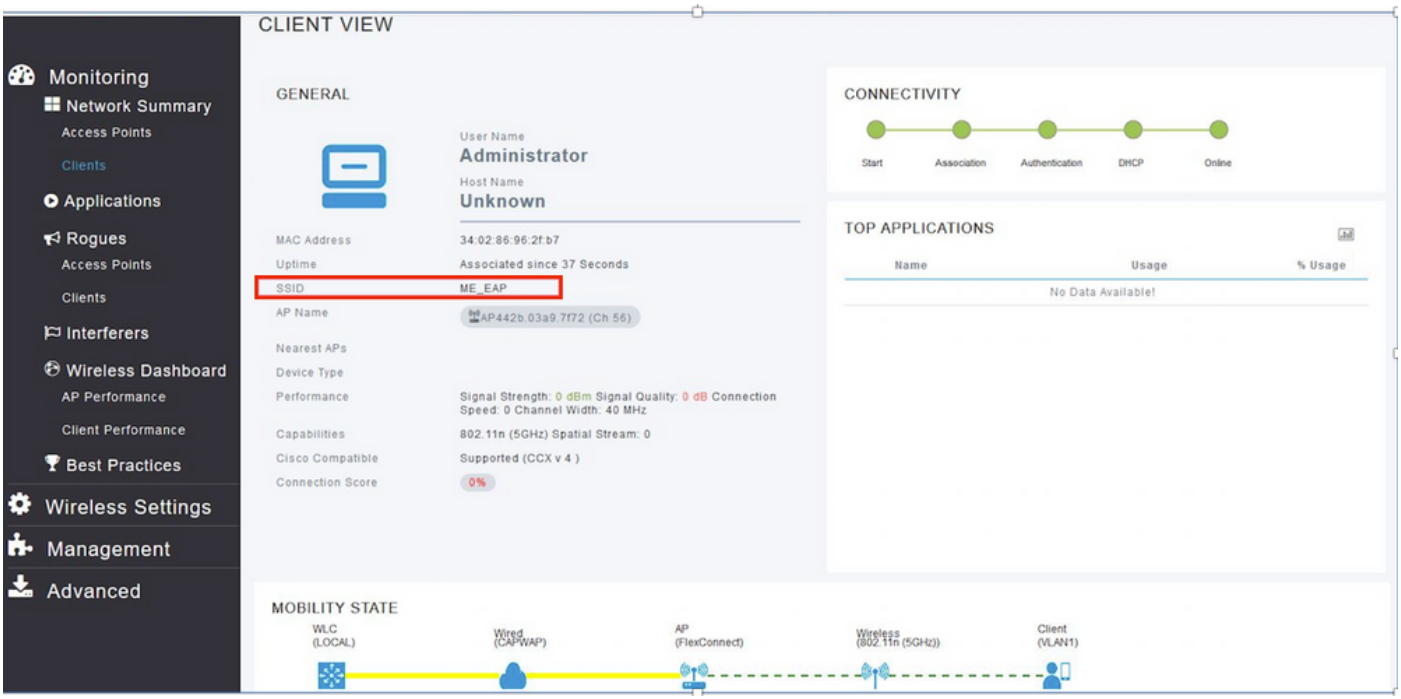

Etapa 5. Agora, tente se conectar novamente à rede sem fio, selecione o perfil correto (EAP neste exemplo) e **Conecte**. Você está conectado à rede sem fio conforme mostrado na imagem.

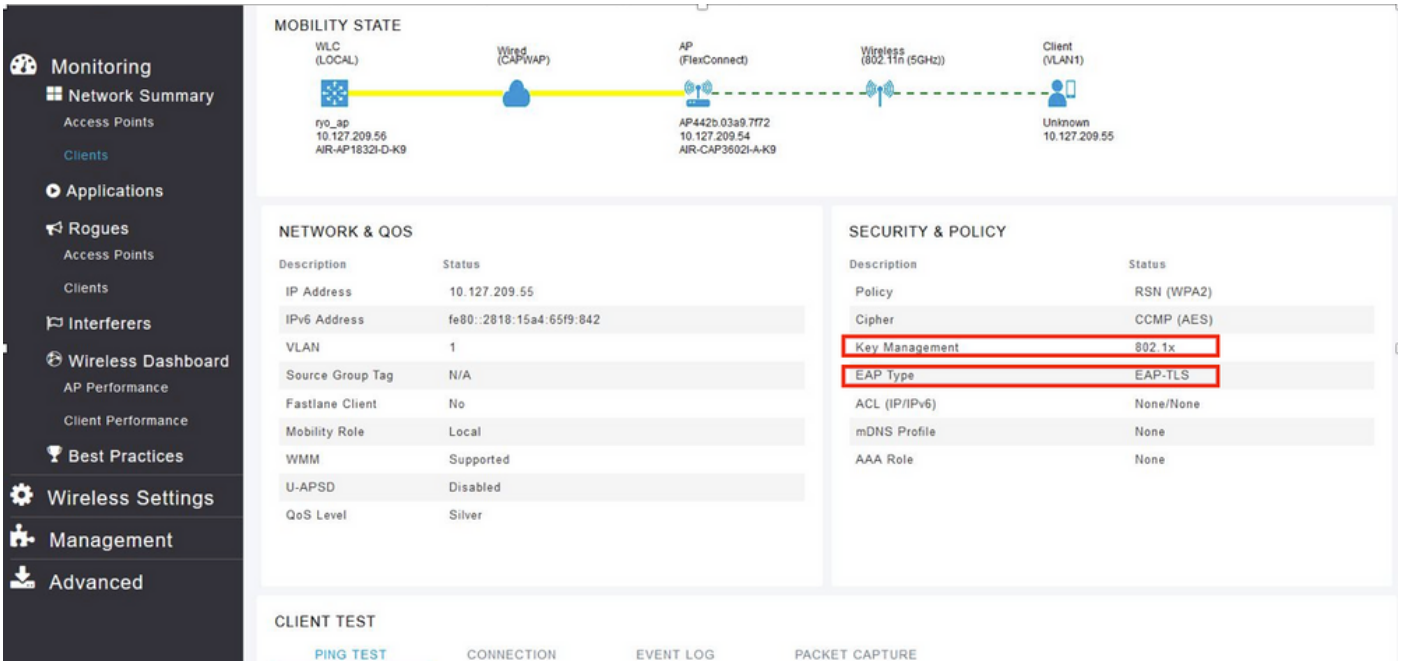



# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. O cliente EAP-Type deve ser EAP-TLS. Isso significa que o cliente concluiu a autenticação, com o uso de EAP-TLS, obteve o endereço IP e está pronto para passar o tráfego, como mostrado nas imagens.

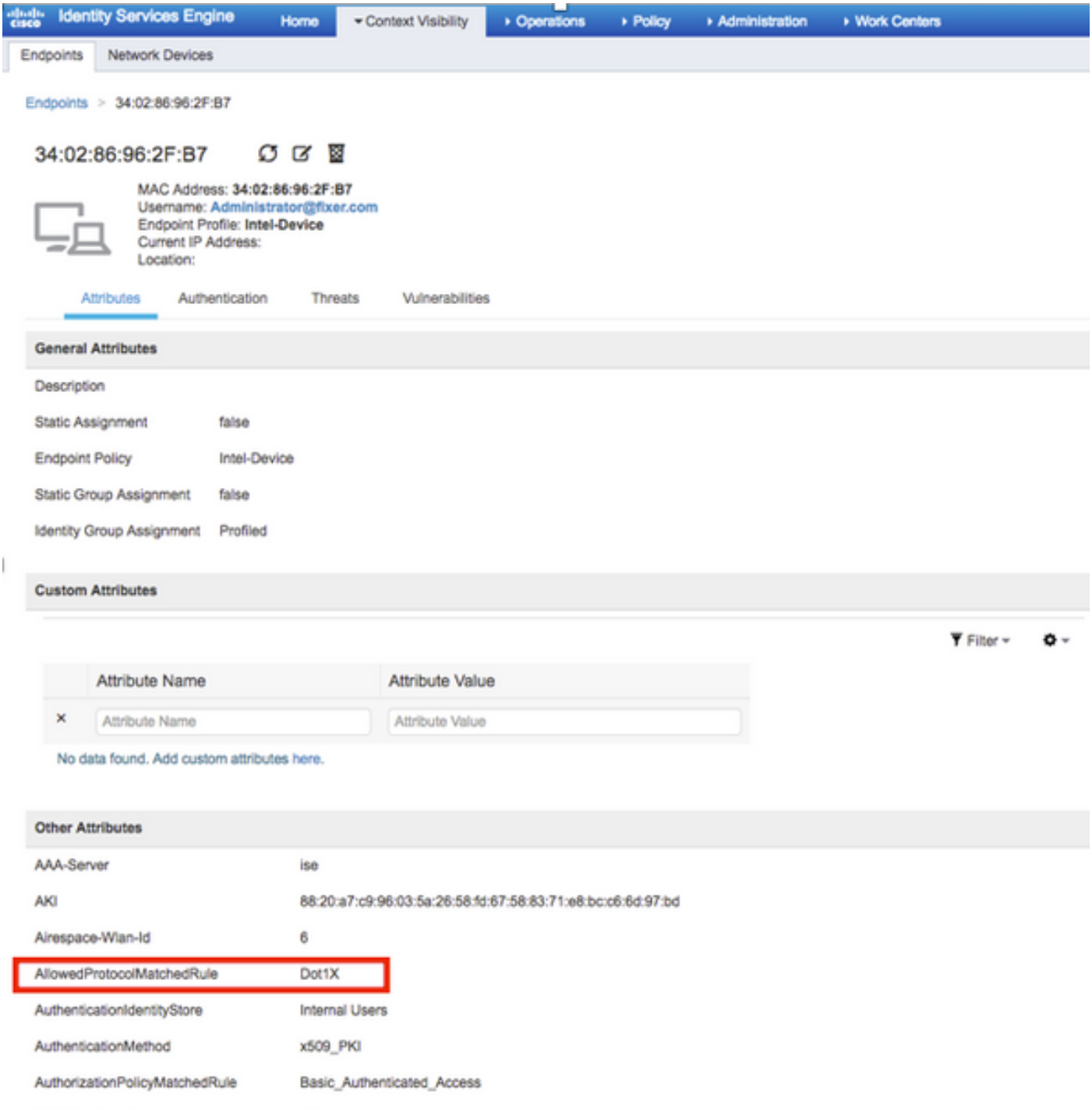





Etapa 2. Aqui estão os detalhes do cliente da CLI da controladora (saída recortada):

```
(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
```

Etapa 3. No ISE, navegue até **Context Visbility > End Points > Attributes**, como mostrado nas imagens.


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Endpoints
Network Devices
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
Attribute Name
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, 1.3.6.1.4.1.311.1 |
| FailureReason | 12935 Supplicant stopped responding to ISE during |
| IdentityGroup | Profiled |
| InactiveDays | 0 |
| IsThirdPartyDeviceFlow | false |
| Issuer | CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=co |
| 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" |
| 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 | 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 00 11 |
| Service-Type | Framed |
| StaticAssignment | false |
| StaticGroupAssignment | false |
| StepData | 4=Dot1X |

# Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.