

Entender e configurar o EAP-TLS com uma WLC e um ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Fluxo de EAP-TLS](#)

[Etapas do fluxo EAP-TLS](#)

[Configurar](#)

[Controlador de LAN sem fio Cisco](#)

[ISE com Cisco WLC](#)

[Configurações de EAP-TLS](#)

[Configurações de WLC no ISE](#)

[Criar novo usuário no ISE](#)

[Certificado de Confiança no ISE](#)

[Cliente para EAP-TLS](#)

[Baixar Certificado do Usuário na Máquina Cliente \(Windows Desktop\)](#)

[Perfil sem fio para EAP-TLS](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar uma rede local sem fio (WLAN) com 802.1X e protocolo de autenticação extensível EAP-TLS

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Processo de autenticação 802.1X
- Certificados

Componentes Utilizados

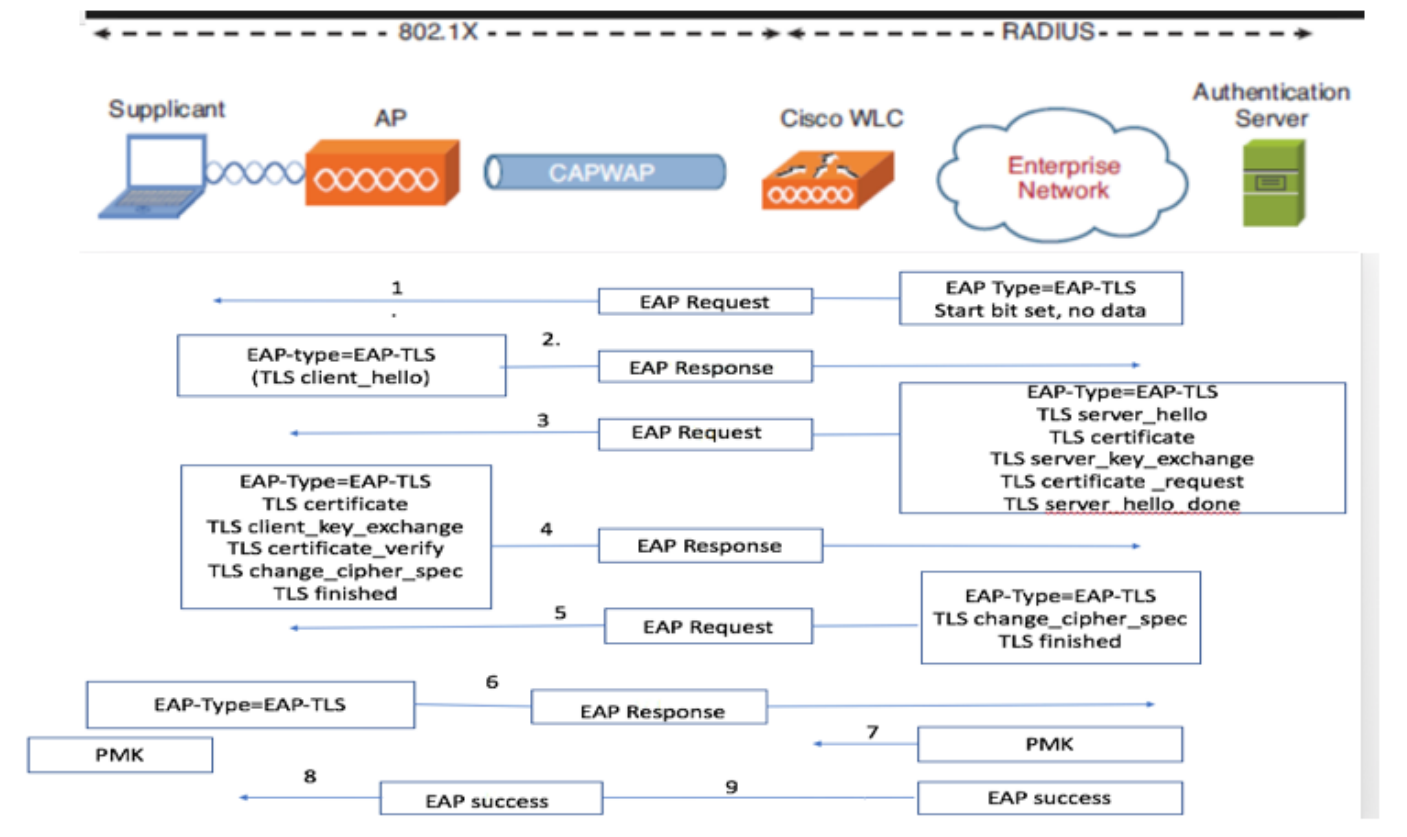
As informações neste documento são baseadas nestas versões de software e hardware:

- WLC 3504 versão 8.10
- Identity Services Engine (ISE) versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Fluxo de EAP-TLS



Etapas do fluxo EAP-TLS

1. O cliente sem fio é associado ao ponto de acesso (PA). O AP não permite que o cliente envie nenhum dado neste ponto e envia uma solicitação de autenticação. O solicitante responde com uma Identidade de Resposta EAP. A WLC comunica as informações de id de usuário ao Servidor de autenticação. O servidor RADIUS responde de volta ao cliente com um pacote inicial EAP-TLS. A conversa EAP-TLS começa neste ponto.
2. O peer envia uma EAP-Response de volta ao servidor de autenticação que contém uma mensagem de handshake "client_hello", uma cifra definida como NULL
3. 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.
```

4. 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

5. 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.

6. Quando recebe isso, o cliente verifica o hash para autenticar o servidor radius.

7. Uma nova chave de criptografia é derivada dinamicamente do segredo durante o handshake TLS

8/9. EAP-Success é finalmente enviado do servidor para o autenticador, que é então passado para o requerente.

Nesse ponto, o cliente sem fio habilitado para EAP-TLS pode acessar a rede sem fio.

Configurar

Controlador de LAN sem fio Cisco

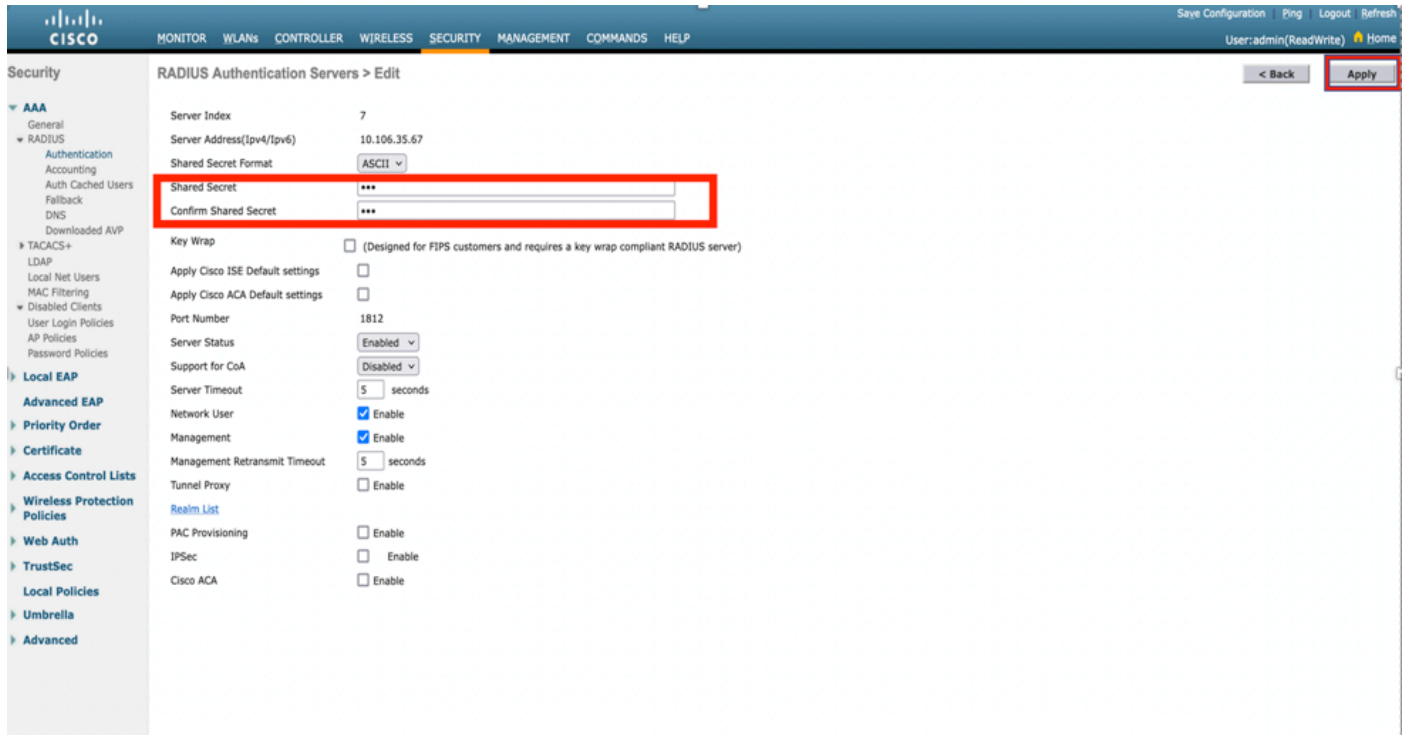
Etapa 1. A primeira etapa é configurar o servidor RADIUS no Cisco WLC. Para adicionar um servidor RADIUS, navegue para **Segurança > RADIUS > Autenticação**. Clique em **New** conforme mostrado na imagem.

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'SECURITY' tab is selected. On the left sidebar, the navigation tree is expanded to 'RADIUS > Authentication'. The main content area is titled 'RADIUS Authentication Servers' and contains several configuration fields: 'Auth Called Station ID Type' (set to 'AP Name:SSID'), 'Use AES Key Wrap' (unchecked), 'MAC Delimiter' (set to 'Colon'), and 'Framed MTU' (set to '1300'). Below these fields is a table of existing 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

At the bottom right of the configuration area, there are 'Apply' and 'New...' buttons. The 'New...' button is highlighted with a red box.

Etapa 2. Aqui, você precisa digitar o endereço IP e o segredo compartilhado <senha> que é usado para validar a WLC no ISE. Clique em **Apply** para continuar como mostrado na imagem.



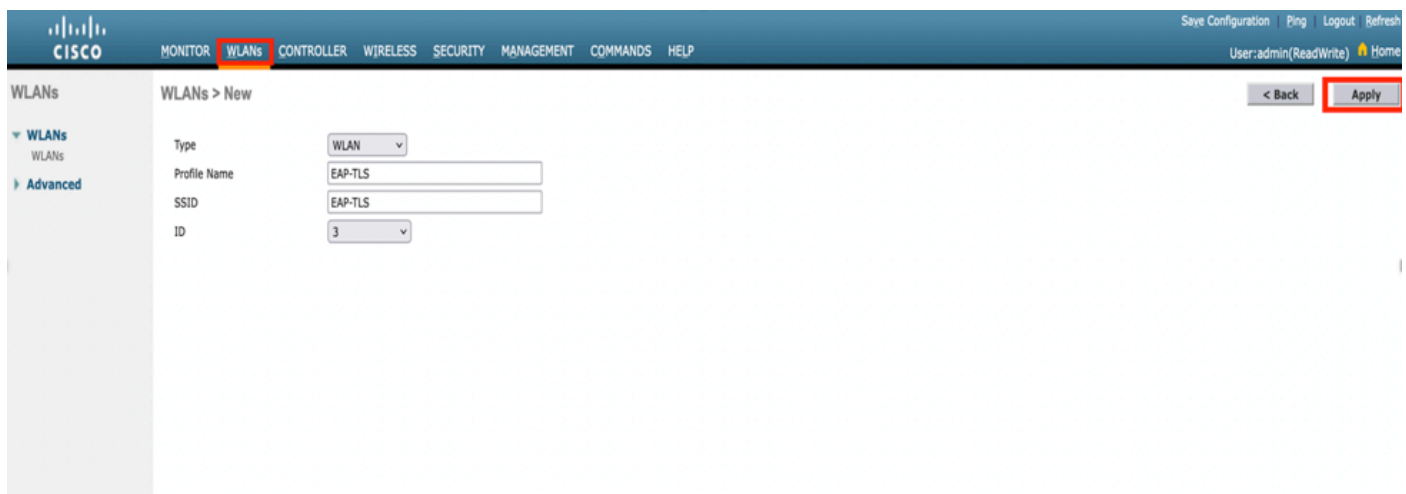
Etapa 3. Criar WLAN para Autenticação RADIUS.

Agora, você pode criar uma nova WLAN e configurá-la para usar o modo WPA-empresa, de modo que ela possa usar o RADIUS para autenticação.

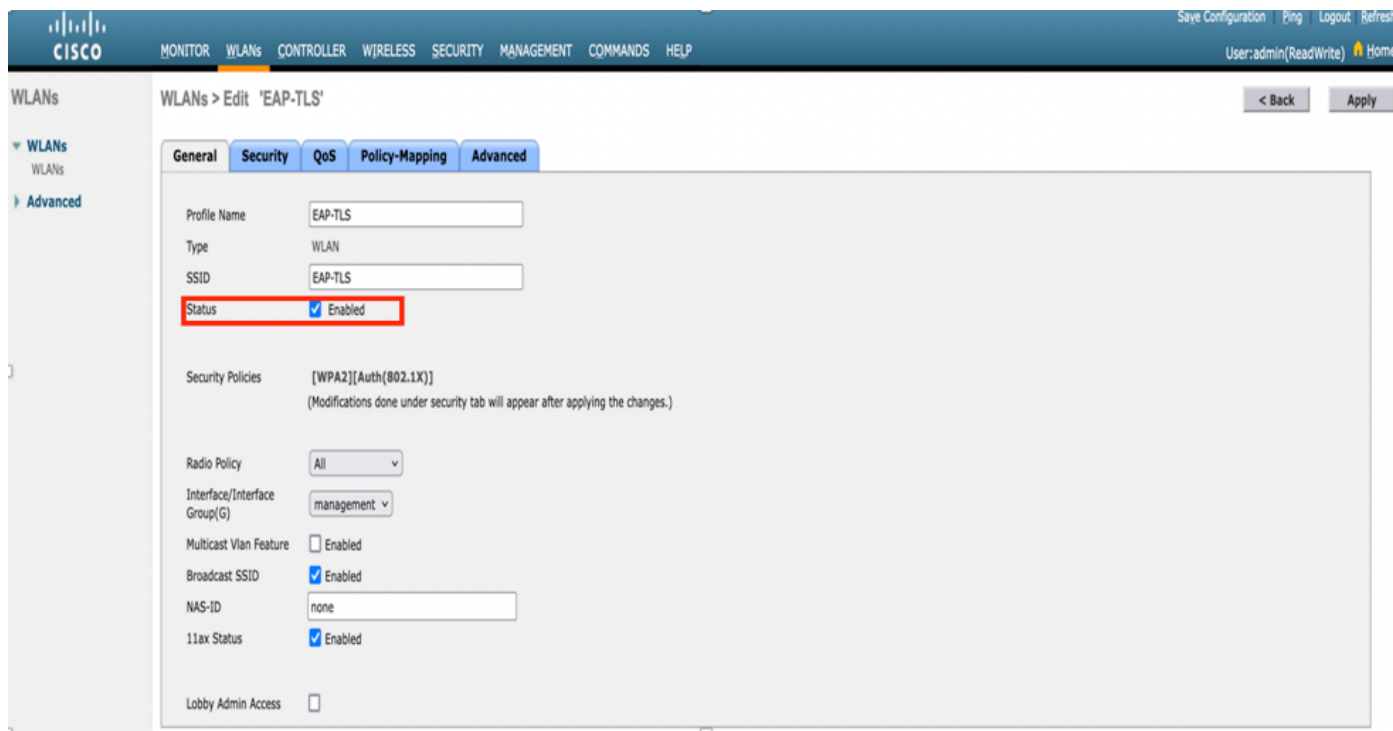
Etapa 4. Selecione **WLANs** no menu principal, escolha **Create New** e clique em **Go** como mostrado na imagem.



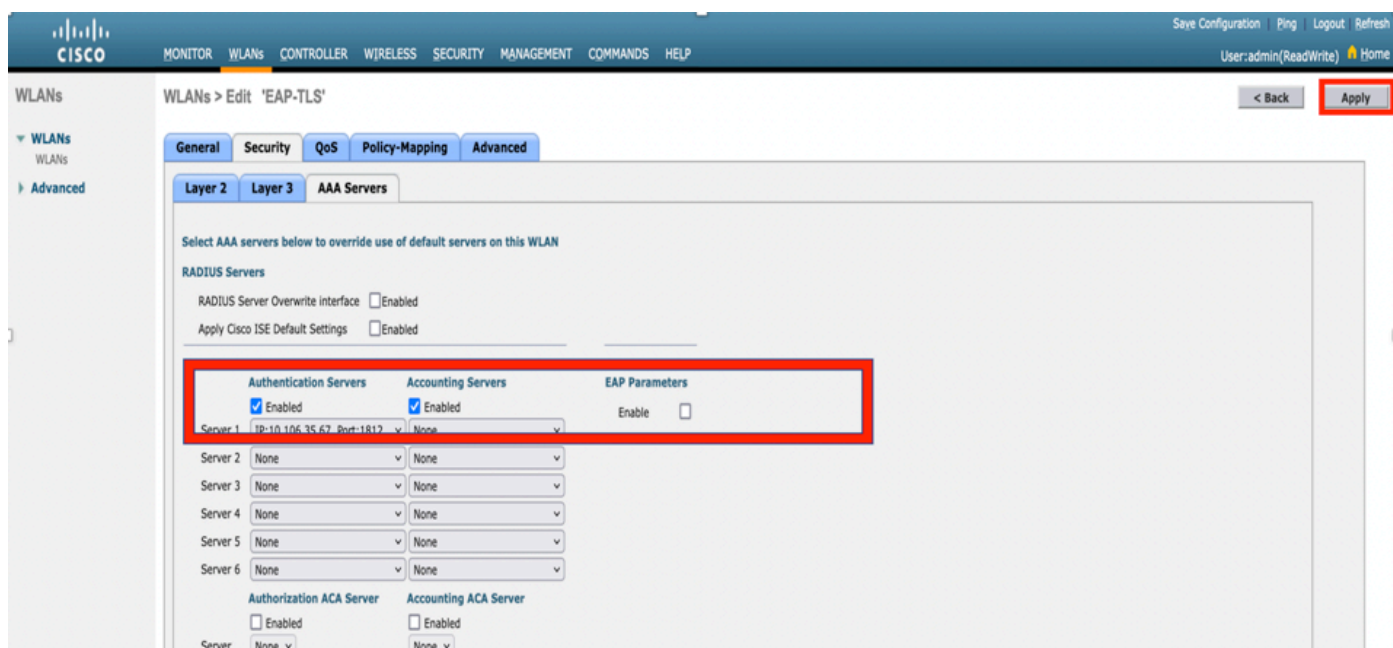
Etapa 5. Nomeie a nova WLAN **EAP-TLS**. Clique em **Apply** para continuar como mostrado na imagem.



Etapa 6. Clique em **Geral** e verifique se o Status está **Habilitado**. As Políticas de segurança padrão são a autenticação 802.1X e WPA2, como mostrado na imagem.



Etapa 7. Agora, navegue até a guia **Security > AAA Servers**, selecione o servidor RADIUS que você acabou de configurar e como mostrado na imagem.



Note: É uma boa ideia verificar se você pode acessar o servidor RADIUS a partir da WLC antes de continuar. O RADIUS usa a porta UDP 1812 (para autenticação), portanto, você precisa garantir que esse tráfego não seja bloqueado em nenhum lugar da rede.

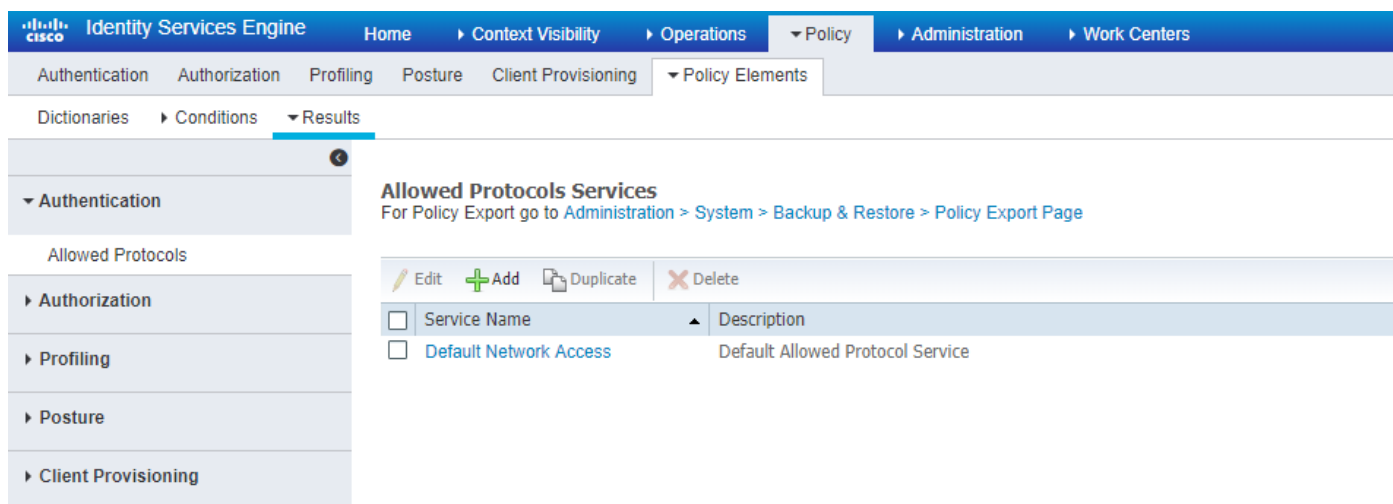
ISE com Cisco WLC

Configurações de EAP-TLS

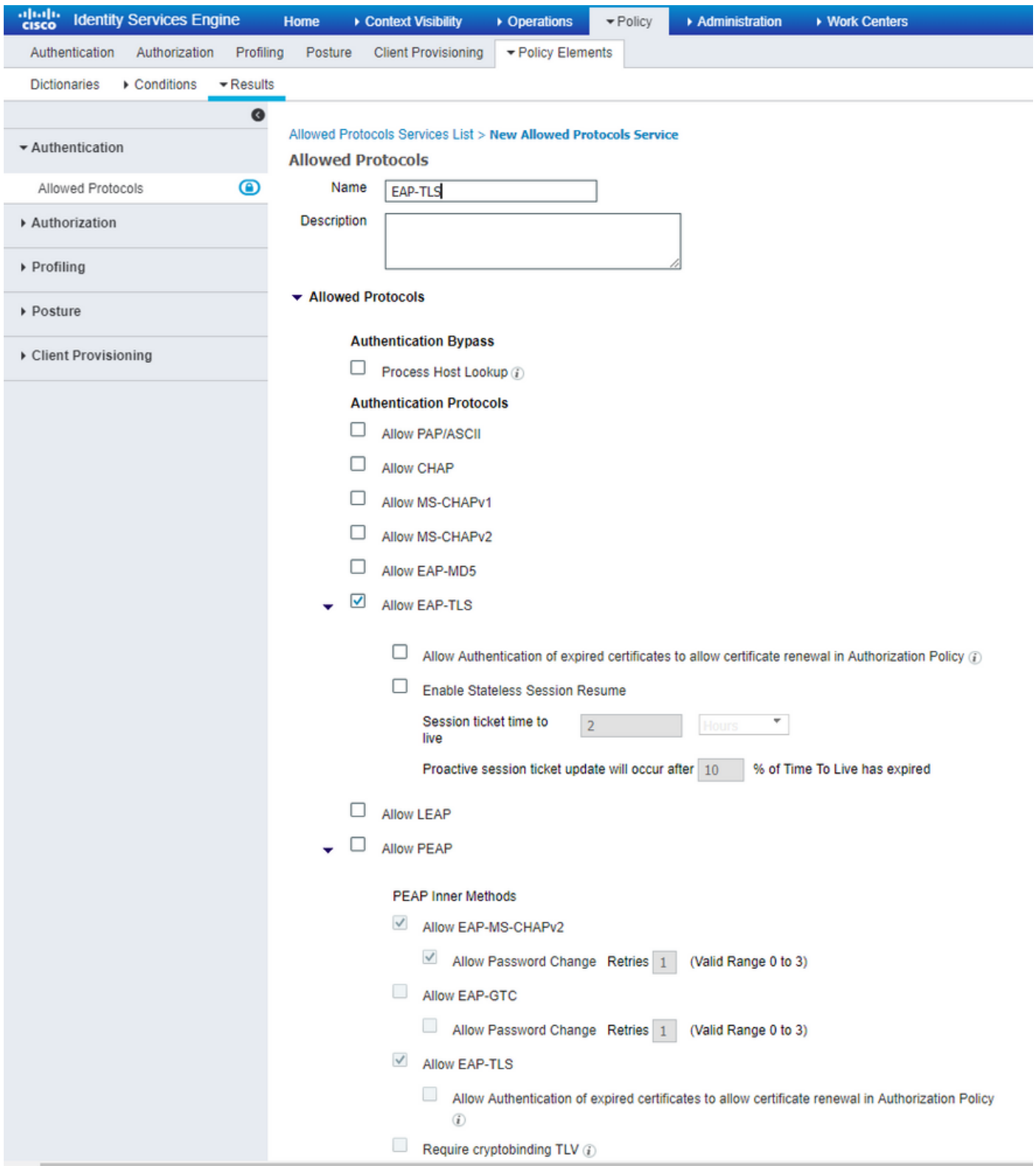
Para criar a política, você precisa criar a lista de protocolos permitidos para usar em nossa política. Como uma política dot1x é escrita, especifique o tipo de EAP permitido com base em como a política é configurada.

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

Etapa 1. Navegue até **Policy > Policy Elements > Results > Authentication > Allowed Protocols** e clique em **Add** conforme mostrado na imagem.

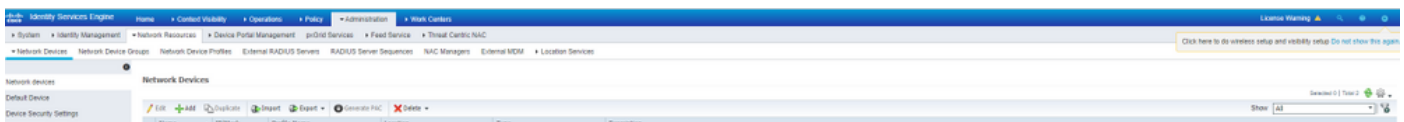


Etapa 2. Nessa lista de protocolos permitidos, você pode digitar o nome da lista. Nesse caso, a caixa **Allow EAP-TLS** (Permitir EAP-TLS) é marcada e outras caixas são desmarcadas, como mostrado na imagem.

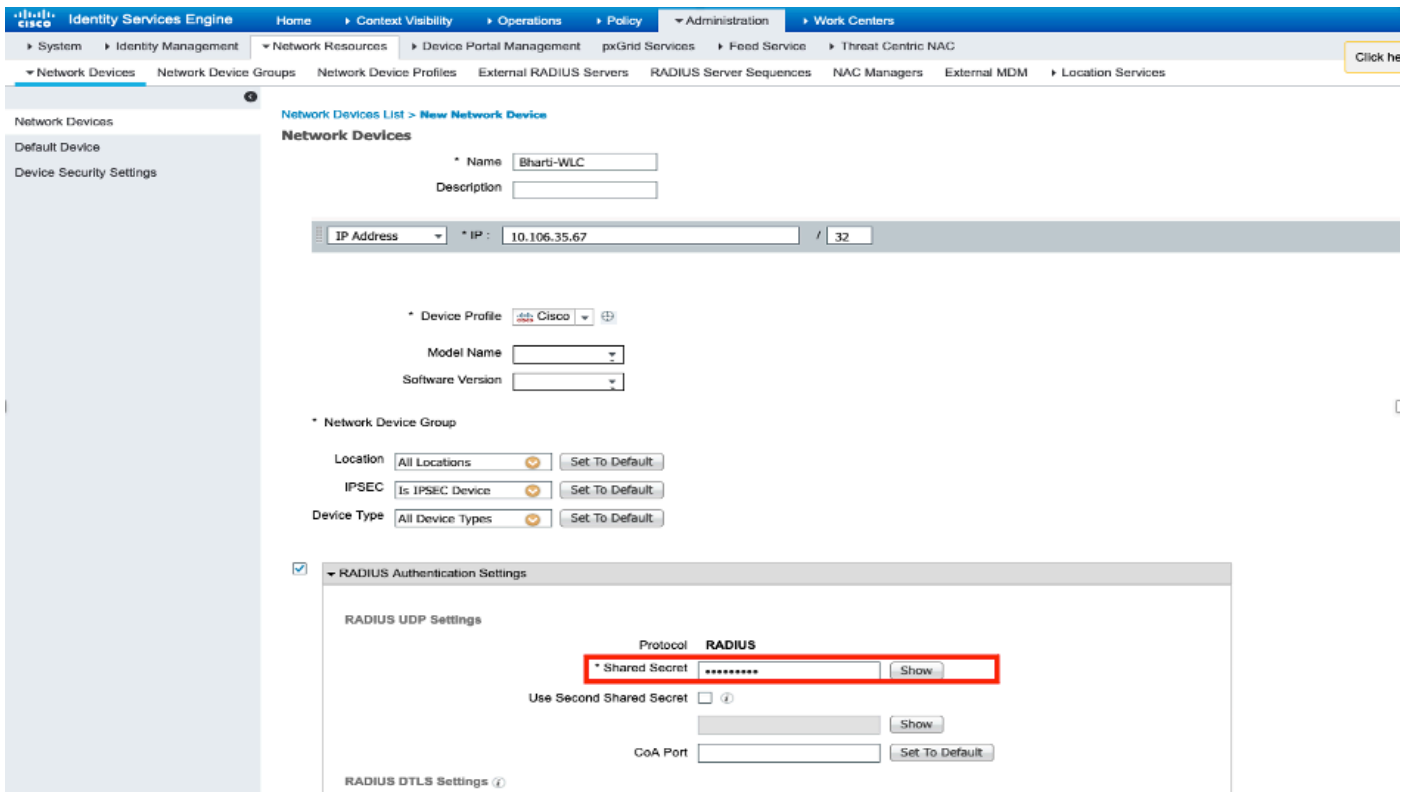


Configurações de WLC no ISE

Etapa 1. Abra o console do ISE e navegue até **Administração > Recursos de rede > Dispositivos de rede > Adicionar** conforme mostrado na imagem.

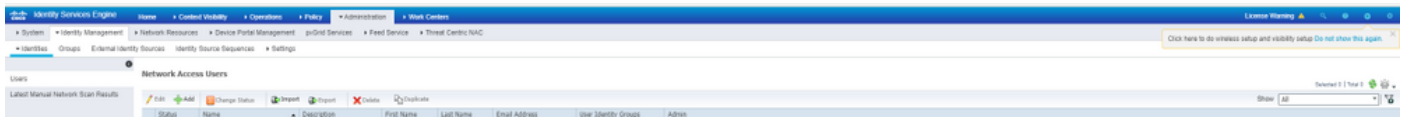


Etapa 2. Digite os valores conforme mostrado na imagem.

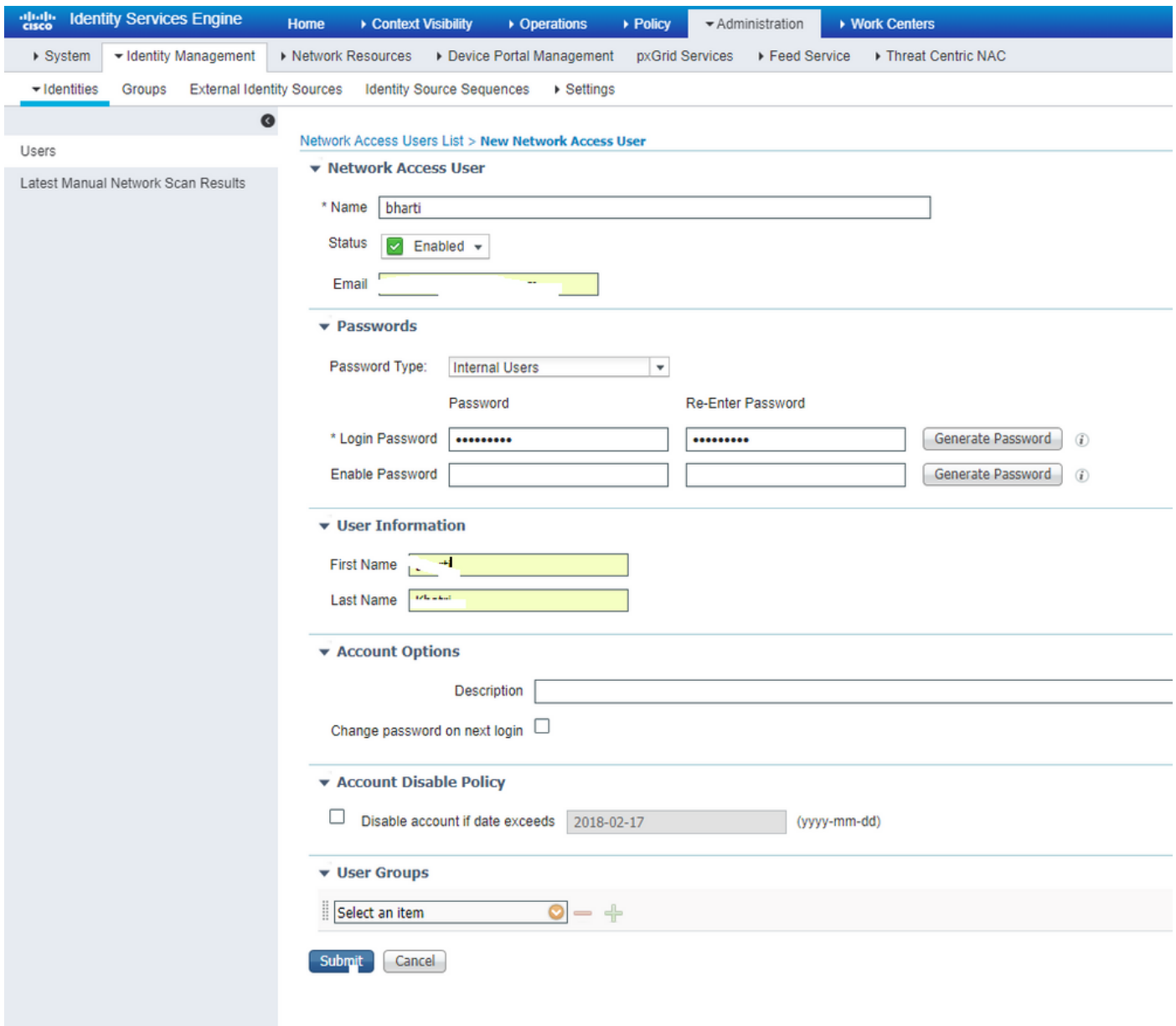


Criar novo usuário no ISE

Etapa 1. Navegue até **Administração > Gerenciamento de identidades > Identidades > Usuários > Adicionar** conforme mostrado na imagem.



Etapa 2. Insira as informações conforme mostrado na imagem.

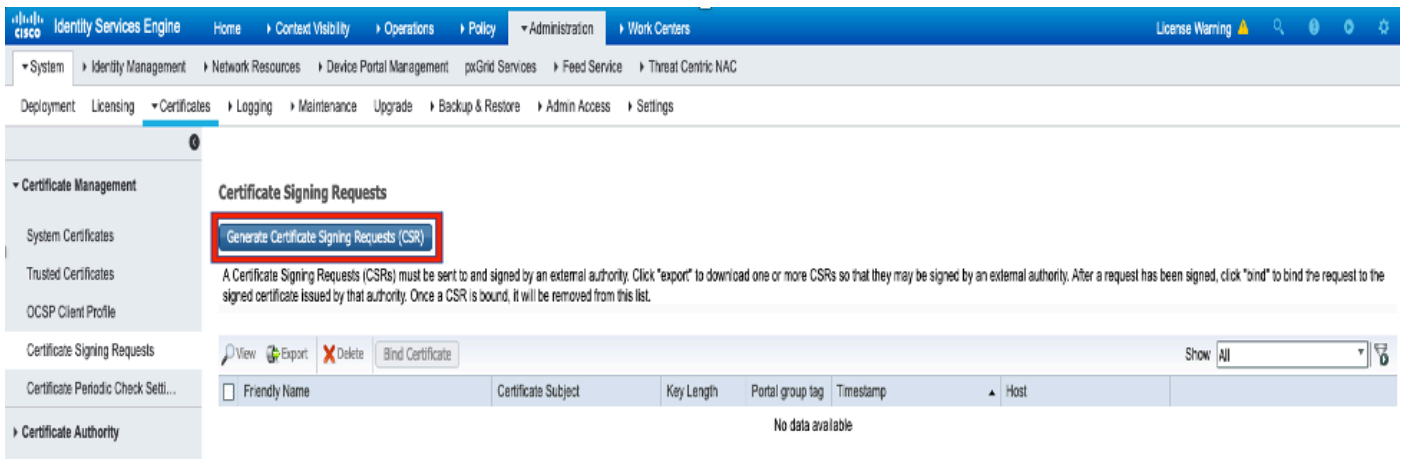


Certificado de Confiança no ISE

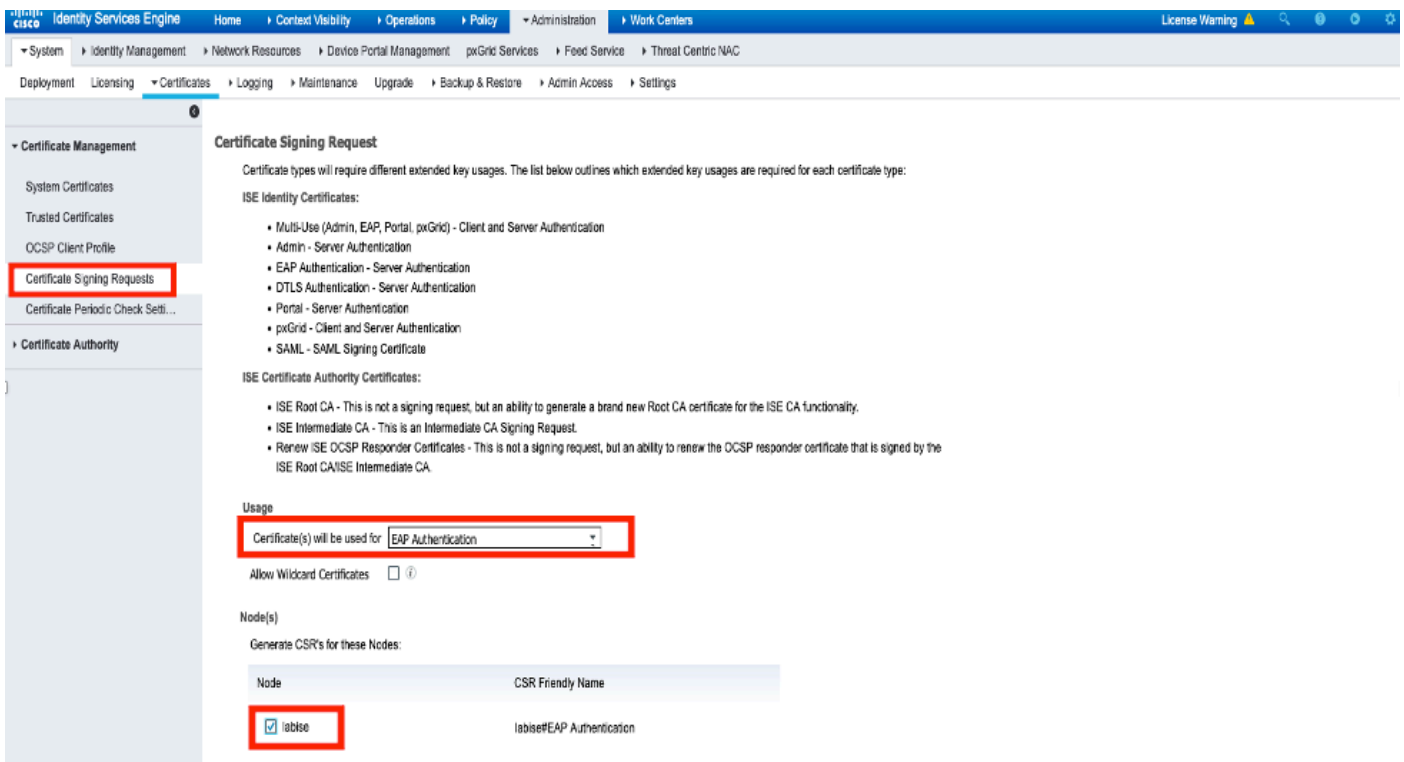
Etapa 1. Navegue até **Administration > System > Certificates > Certificate Management > Trusted certificates**.

Clique em **Import** 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, precisamos gerar CSR.

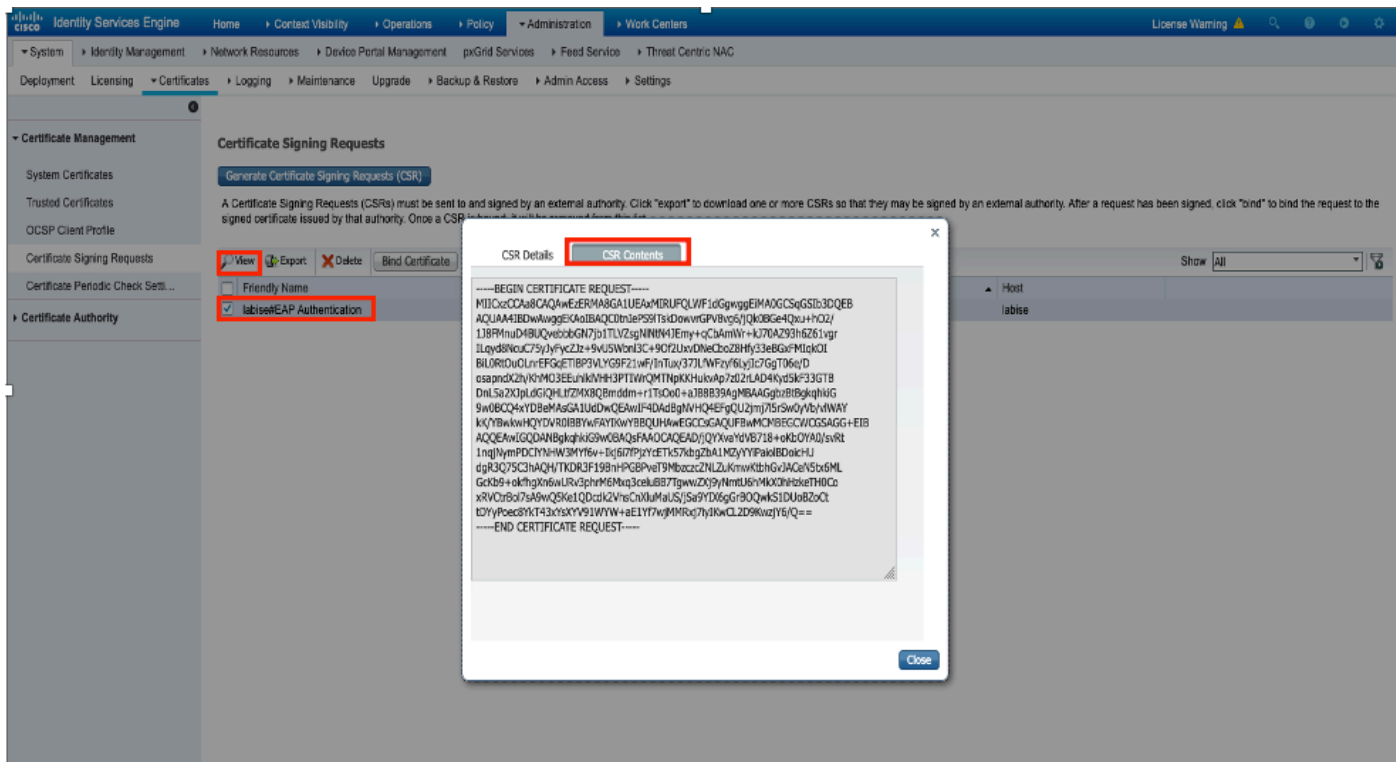
Etapa 2. Navegue até **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR)** conforme mostrado na imagem.



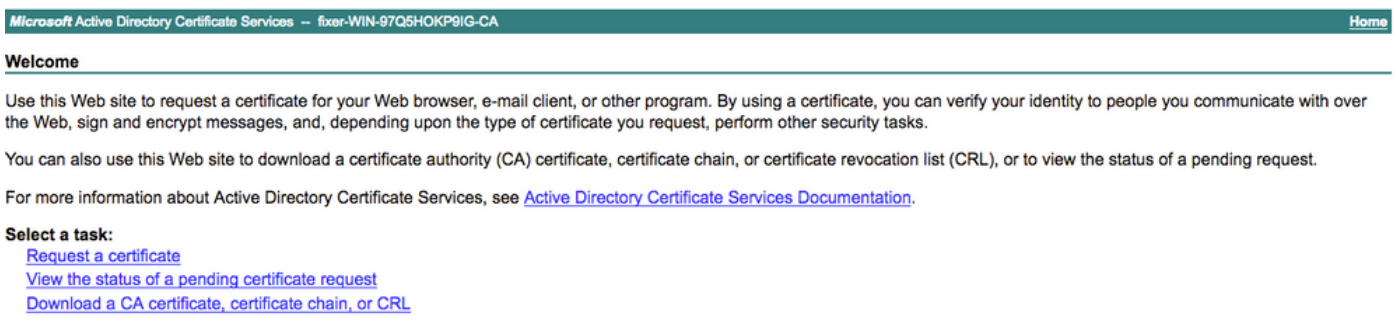
Etapa 3. Para gerar o CSR, navegue até **Usage** e, nas opções suspensas **Certificate(s) are used for**, selecione **EAP Authentication** conforme mostrado na imagem.



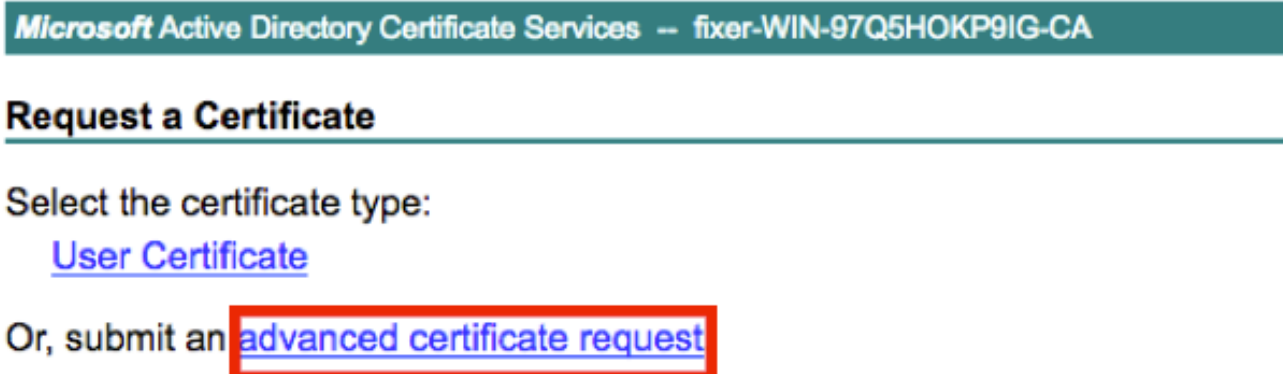
Etapa 4. O CSR gerado no ISE pode ser visualizado. Clique em **View** conforme mostrado na imagem.



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 obterá opções para **Certificado do usuário** e **solicitação de certificado avançada**, clique em **solicitação de certificado avançada**, conforme mostrado na imagem.



Etapa 7. Cole o CSR gerado na **solicitação de certificado codificada na Base 64**. No campo **Modelo de certificado**: selecione **Web Server** e clique em **Submit** conforme mostrado na imagem.

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:


Etapa 8. Depois de clicar em **Submit**, você terá a opção de selecionar o tipo de certificado, selecionar a **codificação Base-64** e clicar em **Fazer download da cadeia de certificados**, como mostrado na imagem.

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](#)

Etapa 9. O download do certificado está concluído para o servidor ISE. Você pode extrair o certificado, o certificado contém dois certificados, um certificado raiz e outro intermediário. O certificado raiz pode ser importado em **Administration > Certificates > Trusted certificates > Import**, conforme mostrado nas imagens.

Identity Services Engine License Warning

Home > Context Visibility > Operations > Policy > Administration > Work Centers

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

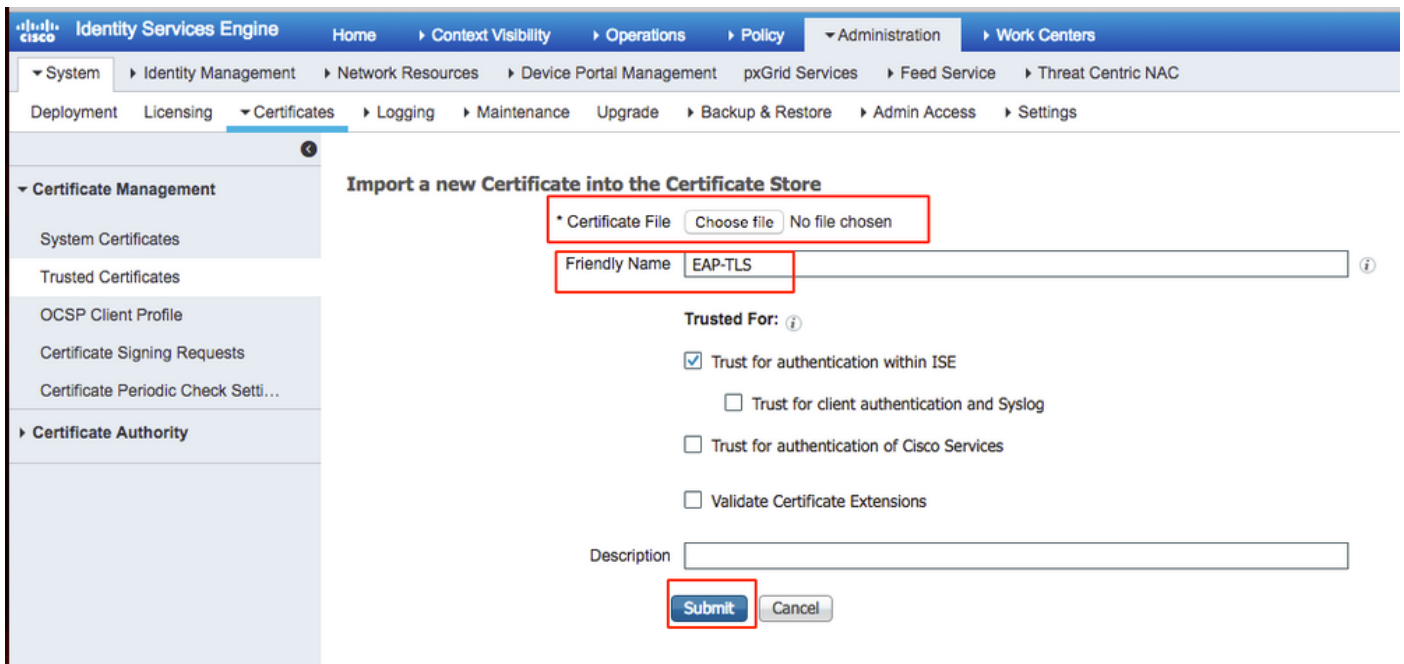
Click here to do wireless setup and visibility setup Do not show this again.

Trusted Certificates

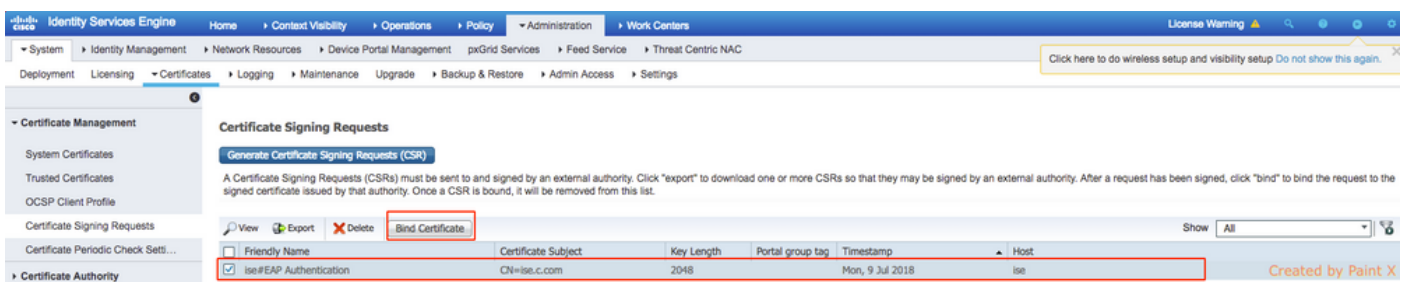
System Certificates

Trusted Certificates

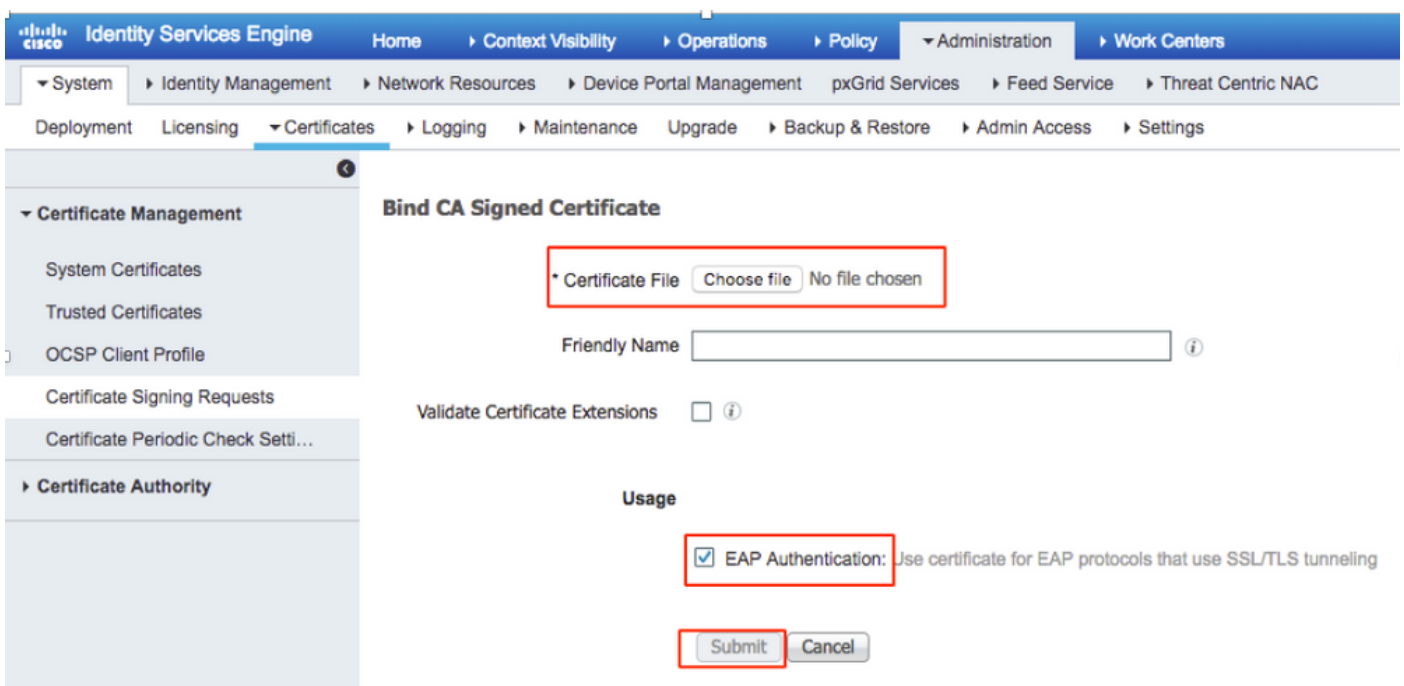
Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
---------------	--------	-------------	---------------	-----------	-----------	------------	-----------------



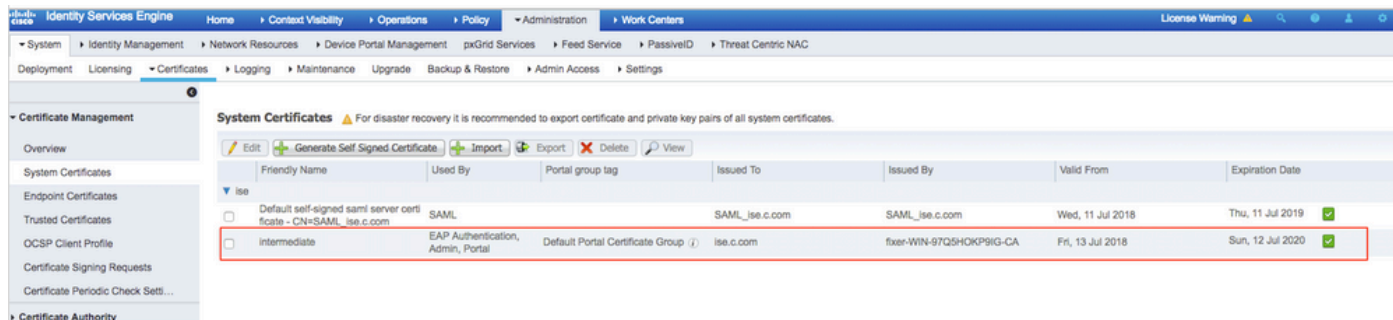
Etapa 10. Quando você clicar em **Submit**, o certificado será adicionado à lista de certificados confiáveis. Além disso, o certificado intermediário é necessário para vincular com o CSR, como mostrado na imagem.



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 **Submit** conforme mostrado na imagem.



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



Cliente para EAP-TLS

Baixar Certificado do Usuário na Máquina Cliente (Windows Desktop)

Etapa 1. Para autenticar um usuário sem fio por meio de EAP-TLS, é necessário gerar um certificado de cliente. Conecte o computador Windows à rede para poder acessar o servidor. Abra um navegador da Web e insira este endereço: <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 de CA que usou para baixar o certificado do servidor. Na mesma CA, clique em **Solicitar um certificado** como feito anteriormente; no entanto, desta vez você precisará selecionar **Usuário** como o Modelo de certificado mostrado na imagem.

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  
dD7LeujkxF1j3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

Attributes:

Submit >

Etapa 3. Em seguida, clique em **baixar 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 Microsoft (MMC).

1. Para abrir o MMC, navegue para **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 do mouse em **Certificados** e selecione **Todas as Tarefas > Importar**.
9. Clique em **Next**.
10. Clique em **Procurar**.

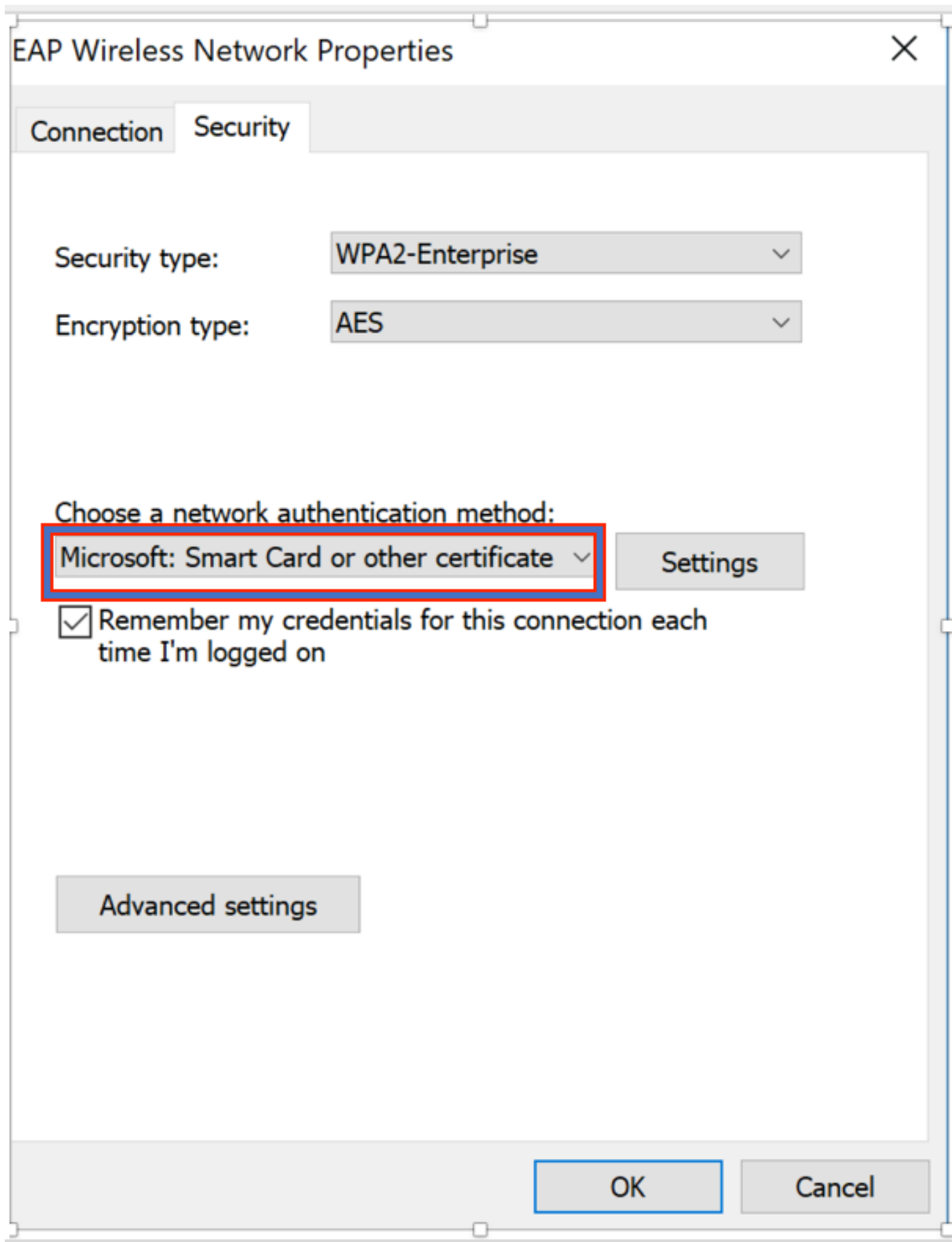
11. Selecione o **.cer**, **.crt** ou **.pfx** que deseja importar.
12. Clique em **Abrir**.
13. Clique em **Next**.
14. Selecione **Selecionar automaticamente o armazenamento de certificados com base no tipo de certificado**.
15. Clique em **Concluir e OK**

Após a importação do certificado, você precisa configurar seu cliente sem fio (área de trabalho do Windows, neste exemplo) para EAP-TLS.

Perfil sem fio para EAP-TLS

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

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



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

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

Etapa 4. Clique em **Advanced Settings** e selecione **User or computer authentication** na guia 802.1x settings, como mostrado na imagem.

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

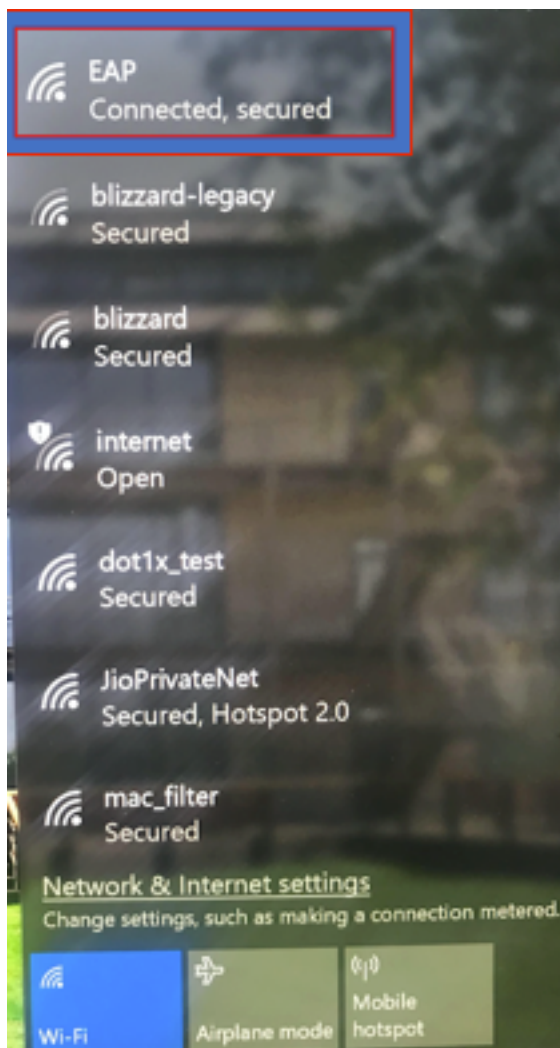
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

Etapa 5. Agora, tente se conectar novamente à rede sem fio, selecione o perfil correto (EAP neste exemplo) e **Connect**. 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 estado do gerenciador de políticas do cliente deve ser exibido como **RUN**. Isso significa que o cliente concluiu a autenticação, obteve o endereço IP e está pronto para passar o tráfego mostrado na imagem.

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Redundancy
- Clients
 - Sleeping Clients
 - Multicast
 - Applications
 - Lync
 - Local Profiling

Clients > Detail

Max Number of Records

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
Client Type	Simple IP	AP radio slot Id	0
User Name	Administrator	WLAN Profile	EAP
Port Number	1	WLAN SSID	EAP
Interface	management	Data Switching	Central
VLAN ID	32	Authentication	Central
Quarantine VLAN ID	0	Status	Associated
CCX Version	CCXv1	Association ID	1
E2E Version	Not Supported	802.11 Authentication	Open System
Mobility Role	Local	Reason Code	1
Mobility Peer IP Address	N/A	Status Code	0
Mobility Move Count	0	CF Pollable	Not Implemented
Policy Manager State	RUN	CF Poll Request	Not Implemented
Management Frame Protection	No	Short Preamble	Not Implemented
UpTime (Sec)	146	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

Etapa 2. Verifique também o método EAP correto no WLC na página de detalhes do cliente, conforme mostrado na imagem.

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

Etapa 3. Aqui estão os detalhes do cliente do CLI da controladora (saída cortada):

```
(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

Etapa 4. No ISE, navegue até **Visualização de contexto > Pontos finais > Atributos** conforme mostrado nas imagens.

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 endpoint details for MAC address 34:02:86:96:2F:B7. The 'Attributes' tab is selected, showing a list of attributes. The 'General Attributes' section includes fields for Static Assignment, Endpoint Policy, Static Group Assignment, and Identity Group Assignment. The 'Custom Attributes' section is currently empty. The 'Other Attributes' section lists various system attributes, with 'AllowedProtocolMatchedRule' set to 'Dot1X' and highlighted by a red box.

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

General Attributes

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

Custom Attributes

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	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

No momento, não há informações específicas disponíveis para solucionar problemas dessa configuração.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.