

Configurar 802.1X em APs para PEAP ou EAP-TLS com LSC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurar](#)

[CA SCEP do Windows Server 2016](#)

[Configurar o modelo de certificado e o registro](#)

[Configurar o LSC no 9800](#)

[Etapas de configuração da GUI do AP LSC](#)

[Etapas de configuração do AP LSC CLI](#)

[Verificação LSC do AP](#)

[Solucionar problemas de provisionamento de LSC](#)

[Autenticação 802.1X com fio AP usando LSC](#)

[Etapas de Configuração da Autenticação 802.1x com Fio AP](#)

[Configuração da GUI de autenticação do AP Wired 802.1x](#)

[Configuração CLI de autenticação 802.1x com fio do AP](#)

[Configuração do switch de autenticação 802.1x com fio AP](#)

[Instalação do Certificado de Servidor RADIUS](#)

[Verificação de autenticação AP Wired 802.1x](#)

[Solucionar problemas da autenticação 802.1X](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como autenticar pontos de acesso Cisco em suas portas de switch usando métodos 802.1X PEAP ou EAP-TLS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controlador sem fio

- Ponto de acesso
- Switch
- servidor ISE
- Autoridade de certificado.

Componentes Utilizados

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

- Controlador sem fio: C9800-40-K9 executando 17.09.02
- Ponto de acesso: C9117AXI-D
- Switch: C9200L-24P-4G executando 17.06.04
- Servidor AAA: ISE-VM-K9 executando 3.1.0.518
- Autoridade de Certificação: Windows Server 2016

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Se você quiser que seus pontos de acesso (APs) se autenticem com suas portas de switch usando 802.1X, por padrão eles usam o protocolo de autenticação EAP-FAST, que não exige certificados. Se você quiser que os APs usem o método PEAP-mschapv2 (que usa credenciais no lado do AP, mas um certificado no lado do RADIUS) ou o método EAP-TLS (que usa certificados nos dois lados), é preciso configurar o LSC primeiro. É a única maneira de provisionar um certificado confiável/raiz em um ponto de acesso (e também um certificado de dispositivo no caso de EAP-TLS). Não é possível para o AP fazer PEAP e ignorar a validação do lado do servidor. Este documento aborda primeiro a configuração do LSC e, em seguida, o lado da configuração do 802.1X.

Use um LSC se desejar que sua PKI ofereça melhor segurança, tenha o controle de sua CA (Certificate Authority, autoridade de certificação) e defina políticas, restrições e usos nos certificados gerados.

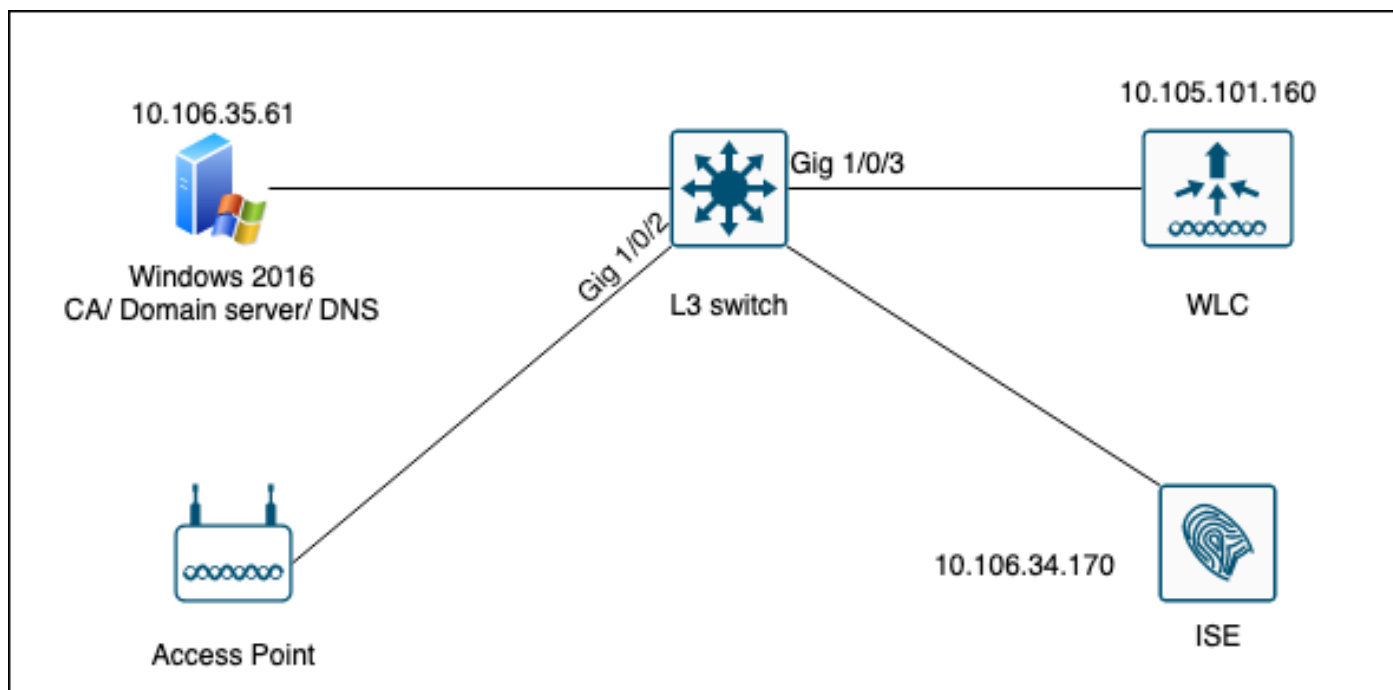
Com o LSC, o controlador obtém um certificado emitido pela CA. Um AP não se comunica diretamente com o servidor de CA, mas a WLC solicita certificados em nome dos APs de junção. Os detalhes do servidor de autoridade de certificação devem ser configurados no controlador e devem estar acessíveis.

O controlador usa o protocolo SCEP para encaminhar certReqs gerados nos dispositivos para a CA e usa o SCEP novamente para obter os certificados assinados da CA.

O SCEP é um protocolo de gerenciamento de certificados que os clientes PKI e os servidores CA usam para oferecer suporte à inscrição e revogação de certificados. Ele é amplamente usado na Cisco e é suportado por muitos servidores CA. No SCEP, o HTTP é usado como o protocolo de

transporte para as mensagens PKI. O objetivo principal do SCEP é a emissão segura de certificados para dispositivos de rede.

Diagrama de Rede



Configurar

Há duas coisas para configurar principalmente: a CA SCEP e a WLC 9800.

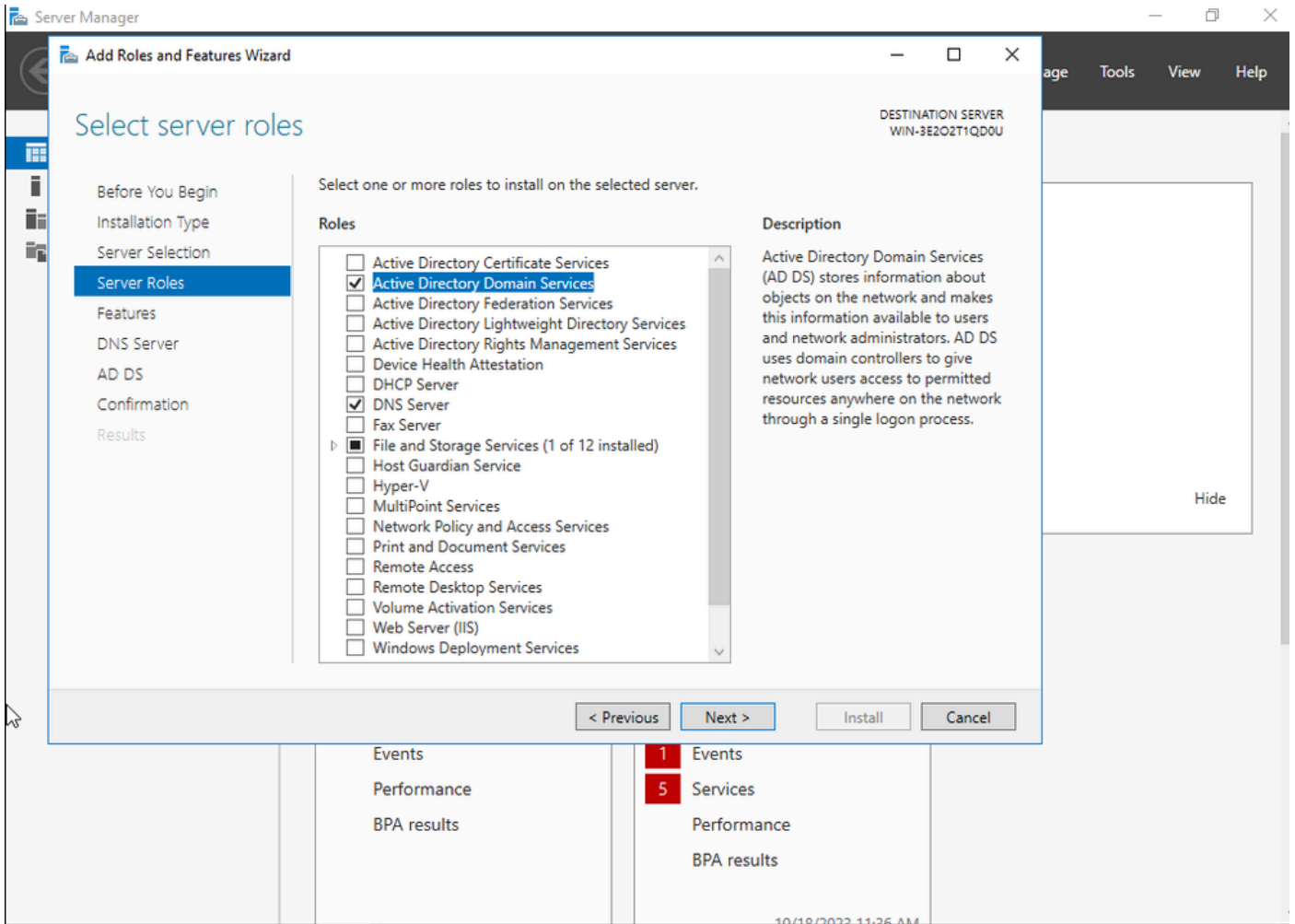
CA SCEP do Windows Server 2016

Este documento aborda uma instalação básica de uma CA SCEP do Windows Server para fins de laboratório. Uma CA do Windows de nível de produção real deve ser configurada de forma segura e apropriada para operações corporativas. Esta seção tem o objetivo de ajudá-lo a testá-la no laboratório, bem como inspirar-se nas configurações necessárias para fazer essa configuração funcionar. Aqui estão as etapas:

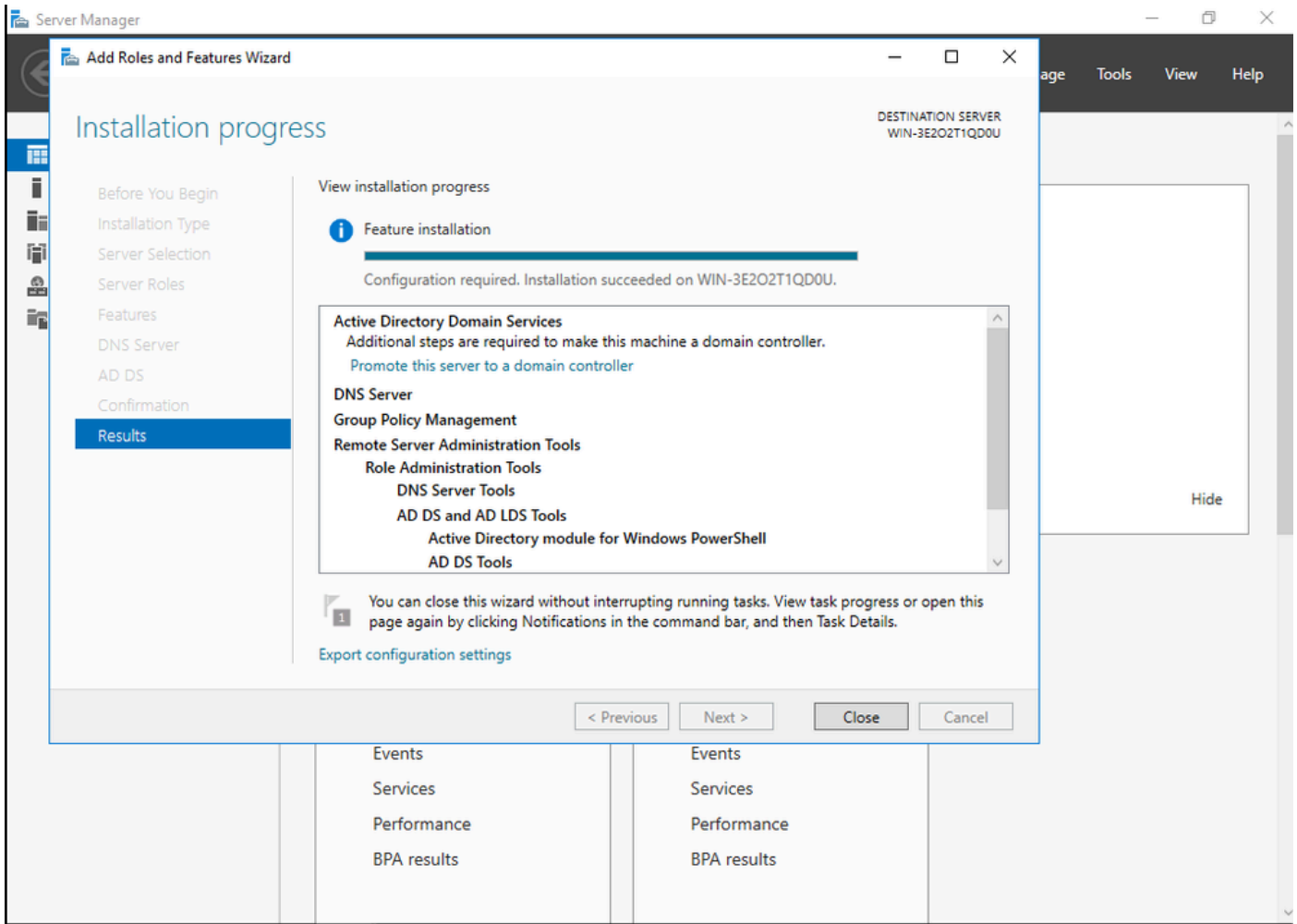
Etapa 1. Instale uma nova experiência de desktop do Windows Server 2016.

Etapa 2. Verifique se o servidor está configurado com um endereço IP estático.

Etapa 3. Instale uma nova função e um novo serviço, inicie com os serviços de domínio do Active Directory e o servidor DNS.

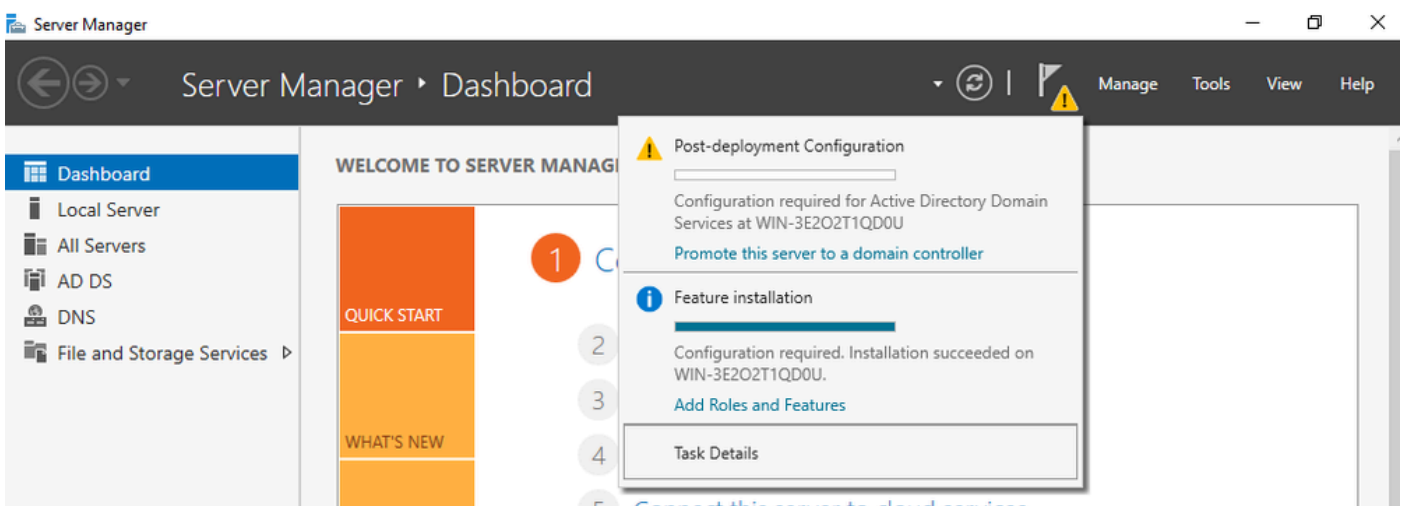


Instalação do Ative Diretory



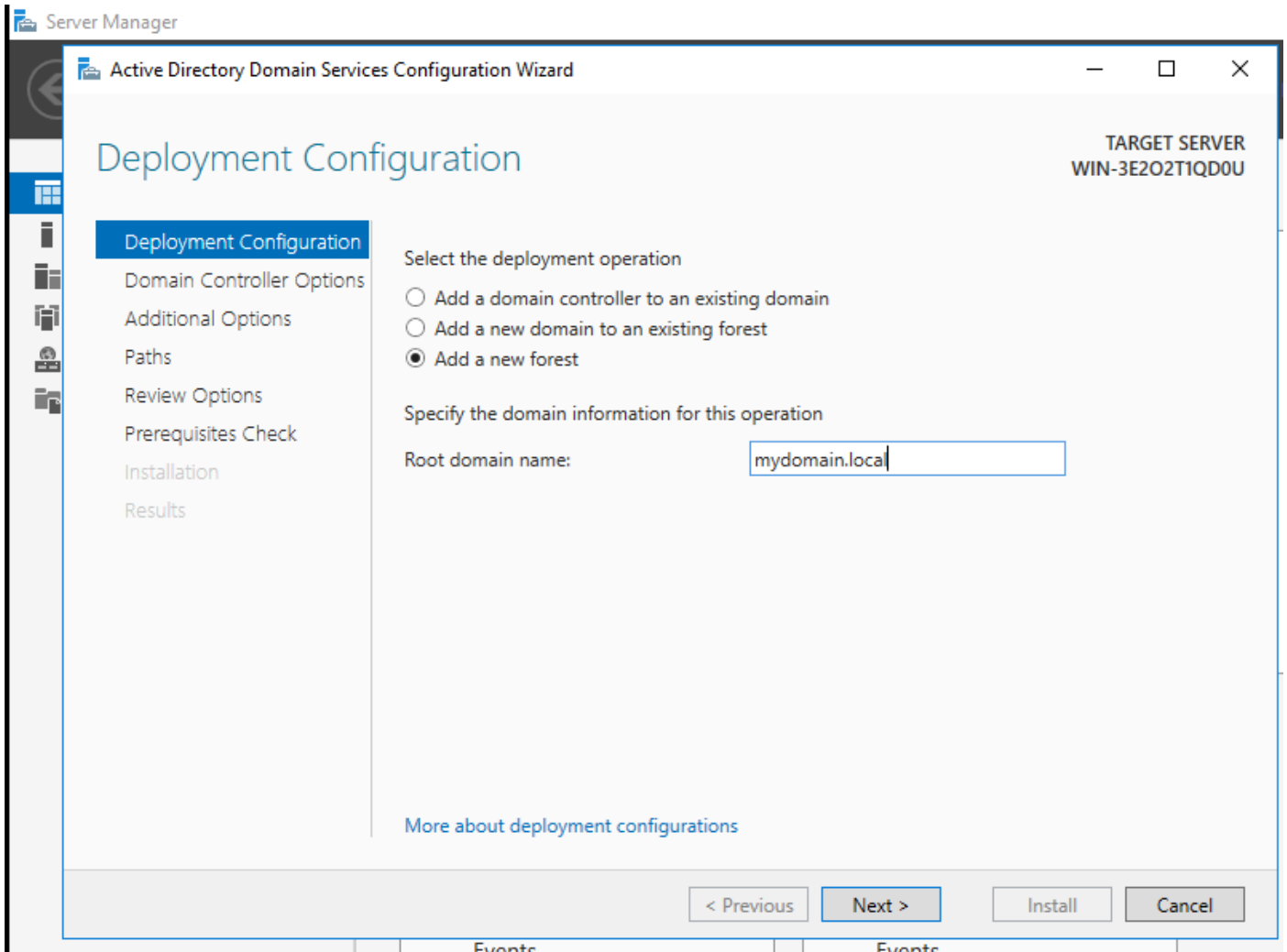
Fim da instalação do AD

Etapa 4. Depois de concluir, clique em no painel em Promover este servidor a um controlador de domínio.



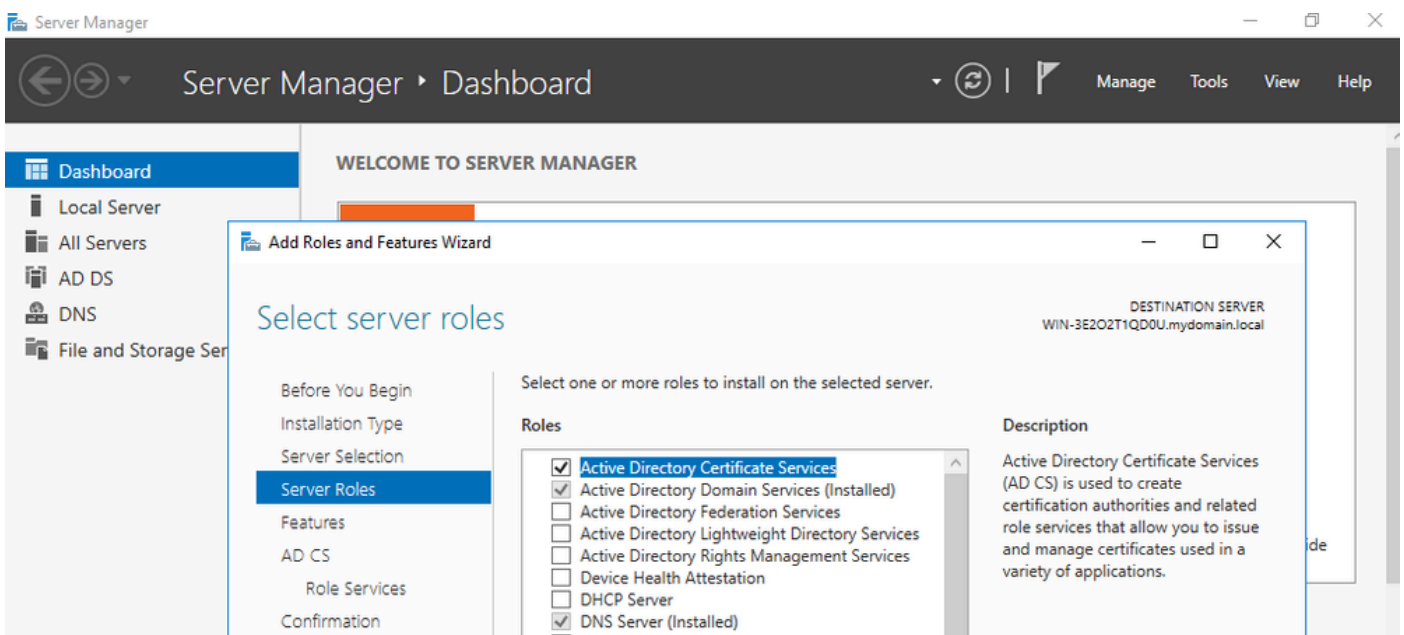
Configurar os serviços do AD

Etapa 5. Crie uma nova floresta e escolha um nome de domínio.

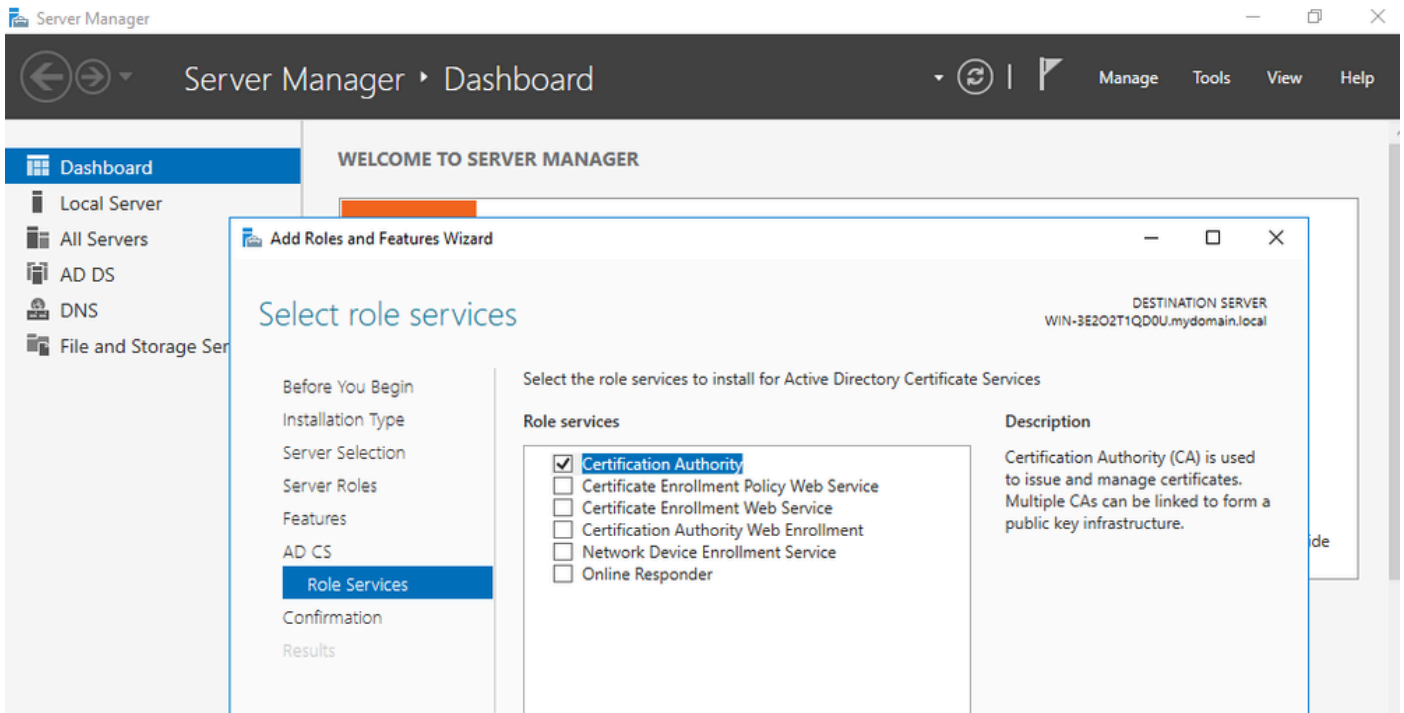


Escolher um nome de floresta

Etapa 6. Adicione a função Serviços de certificado ao servidor:

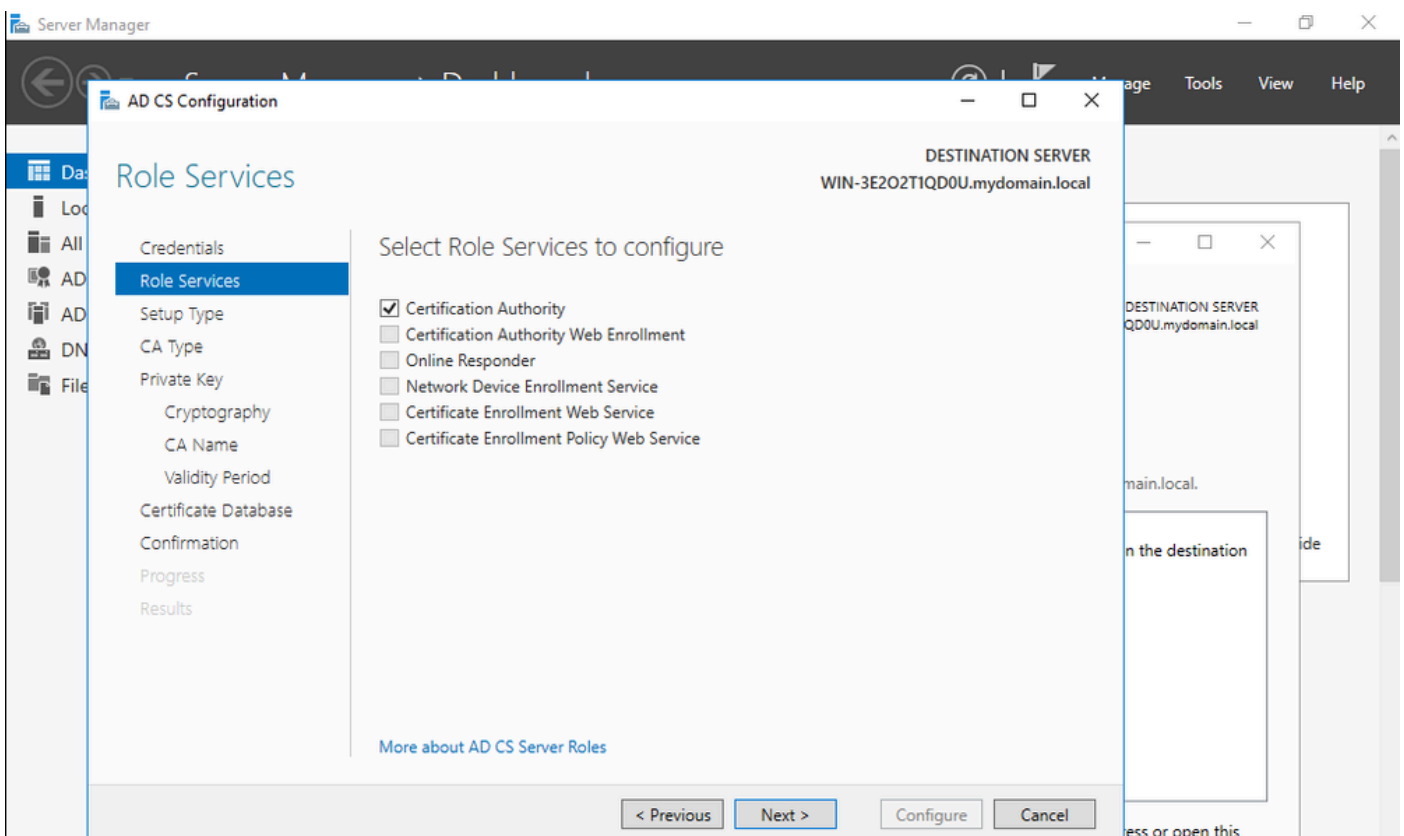


Adicionar serviços de certificado

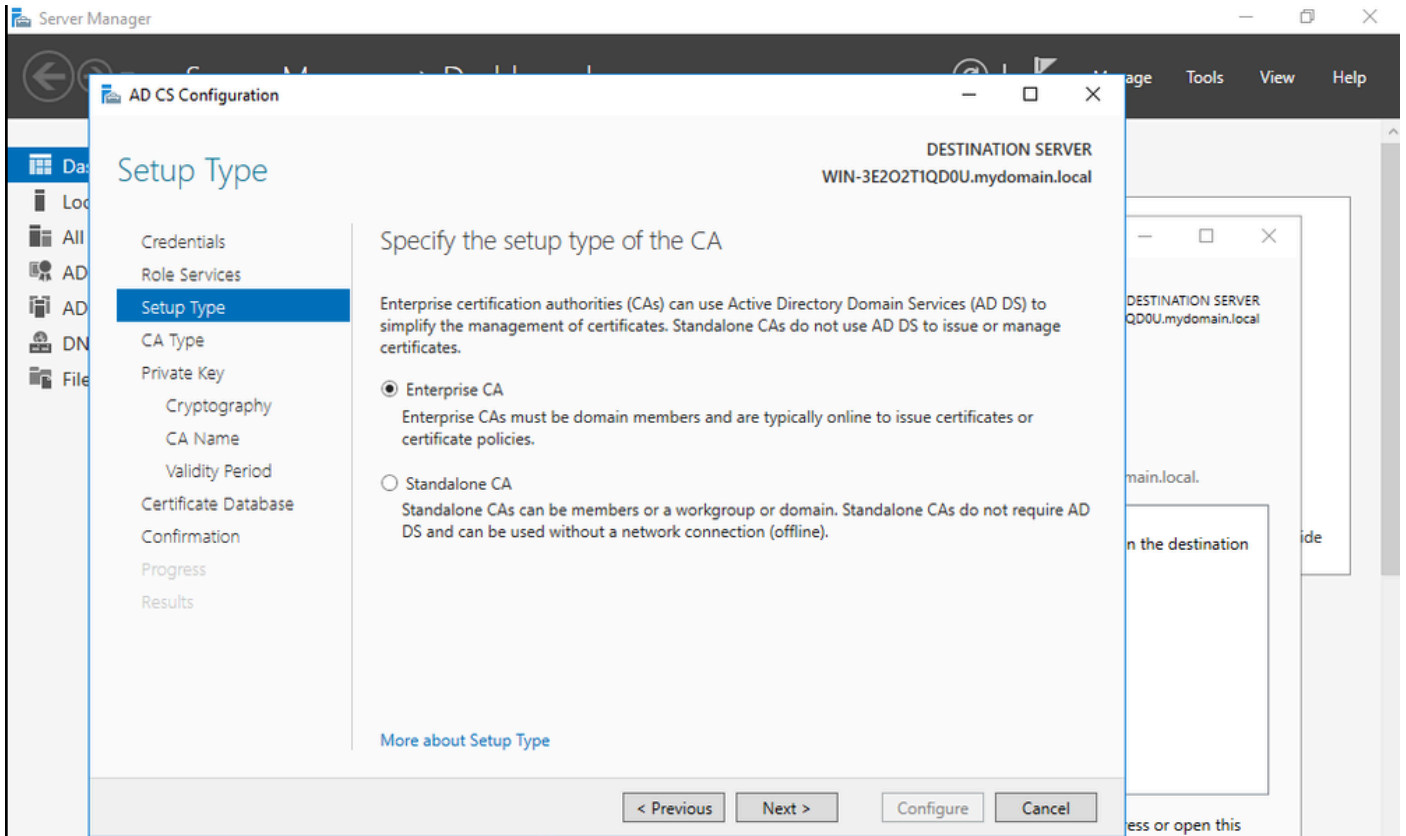


Adicionar apenas a autoridade de certificação

Etapa 7. Depois de concluir, configure sua autoridade de certificação.

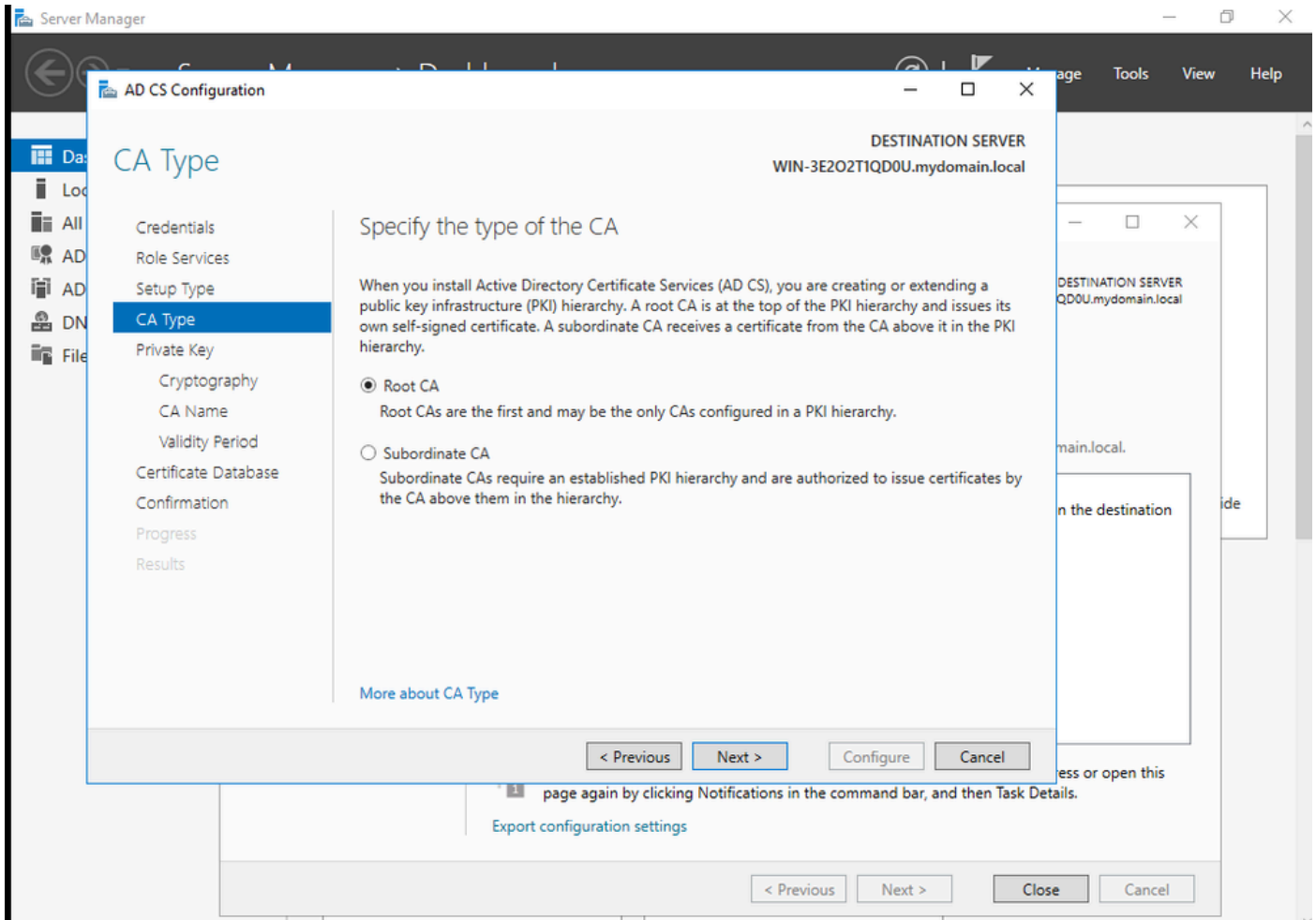


Etapa 8. Escolha CA Corporativa.



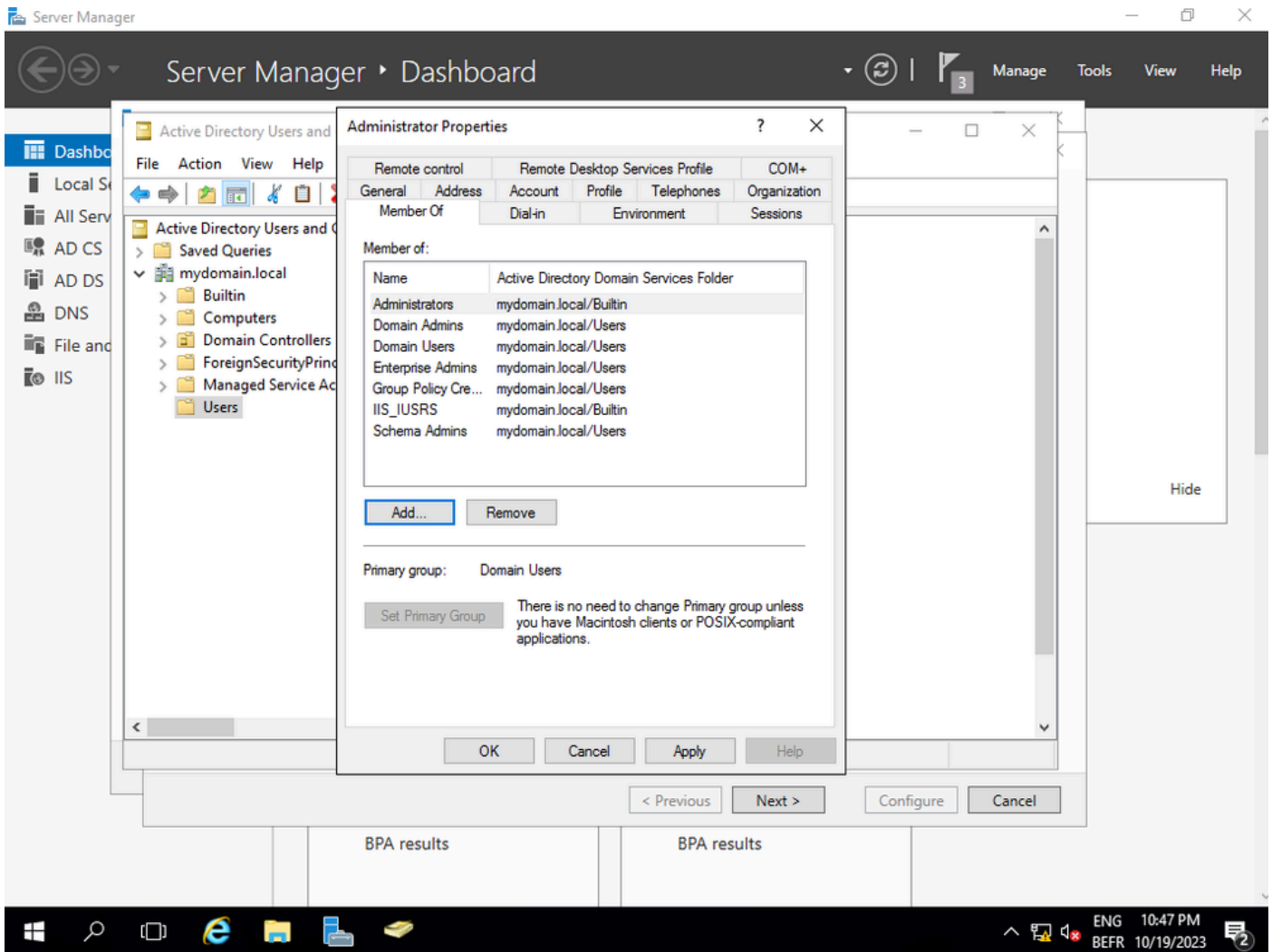
CA Corporativa

Etapa 9. Torne-a uma CA raiz. Desde o Cisco IOS XE 17.6, CAs subordinadas são suportadas para LSC.



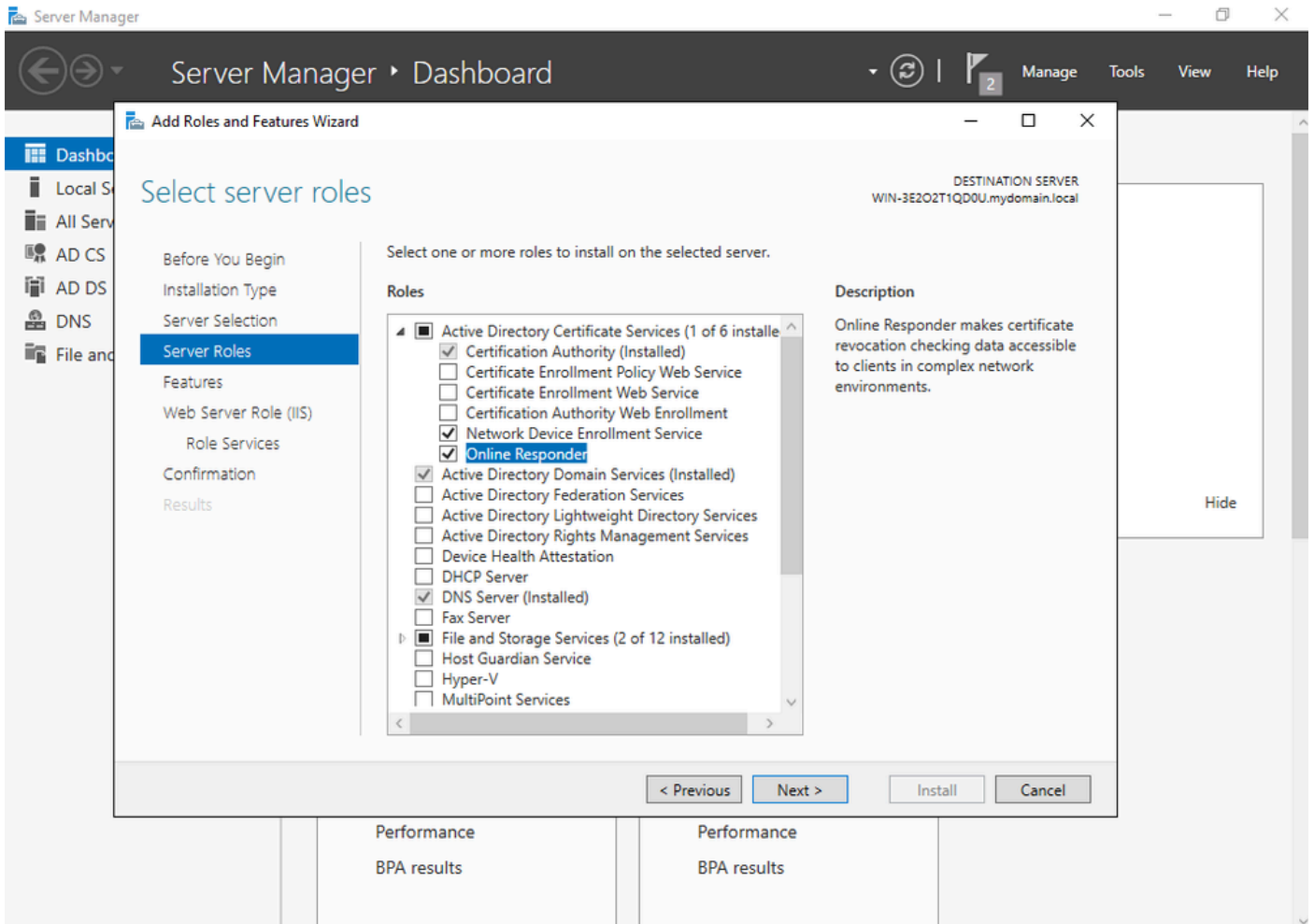
Escolher uma CA Raiz

É importante que a conta que você usa para sua autoridade de certificação faça parte do grupo IIS_IUSRS. Neste exemplo, você usa a conta Administrador e vai para o menu Usuários e Computadores do Ative Diretory para adicionar os usuários Administrador ao grupo IIS_IUSRS.



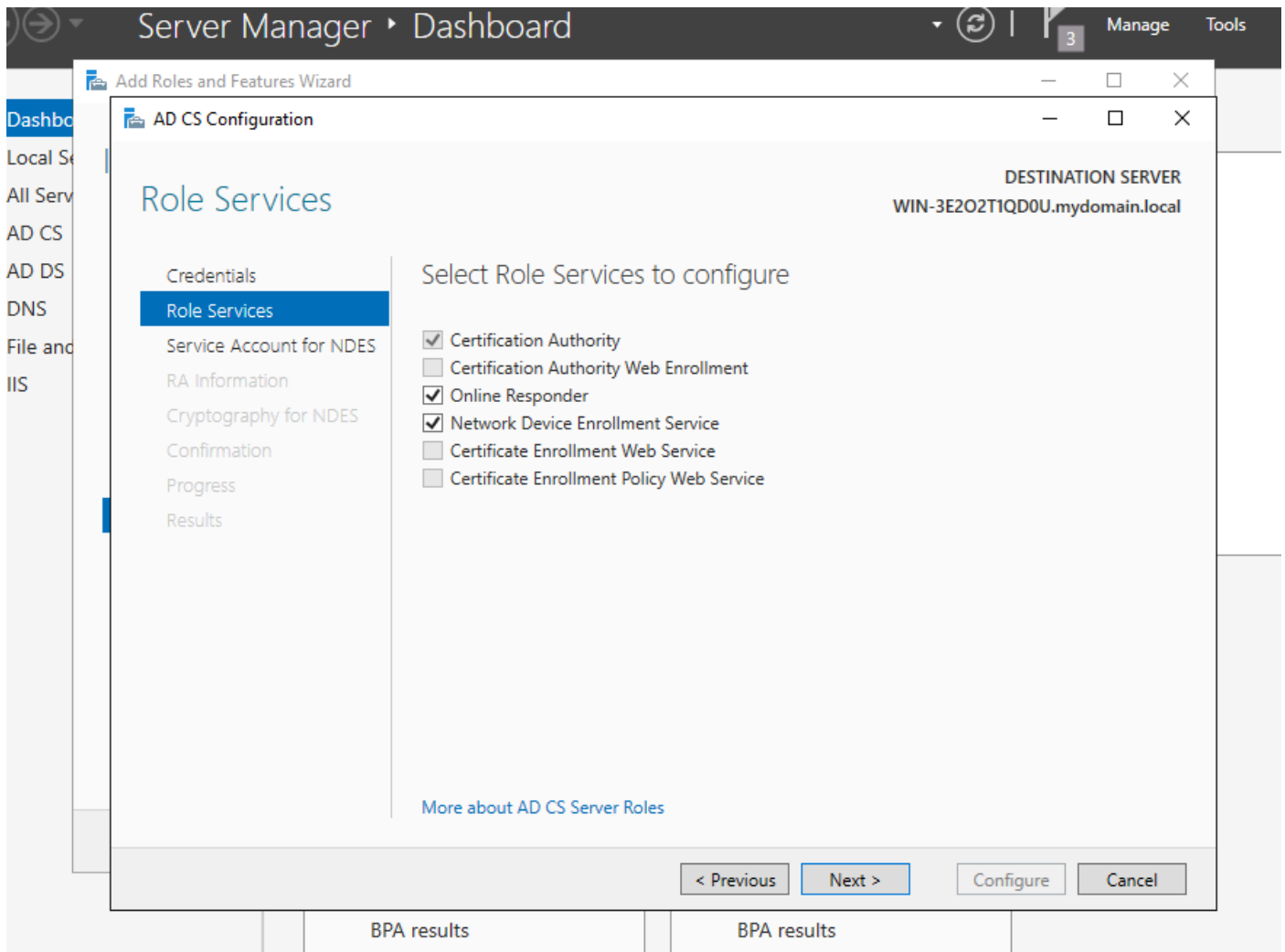
Adicione sua conta de administrador ao grupo IIS_USER

Etapa 10. Depois que você tiver um usuário no grupo do IIS correto, adicione funções e serviços. Em seguida, adicione o Respondente Online e os serviços NDES à sua Autoridade de Certificação.



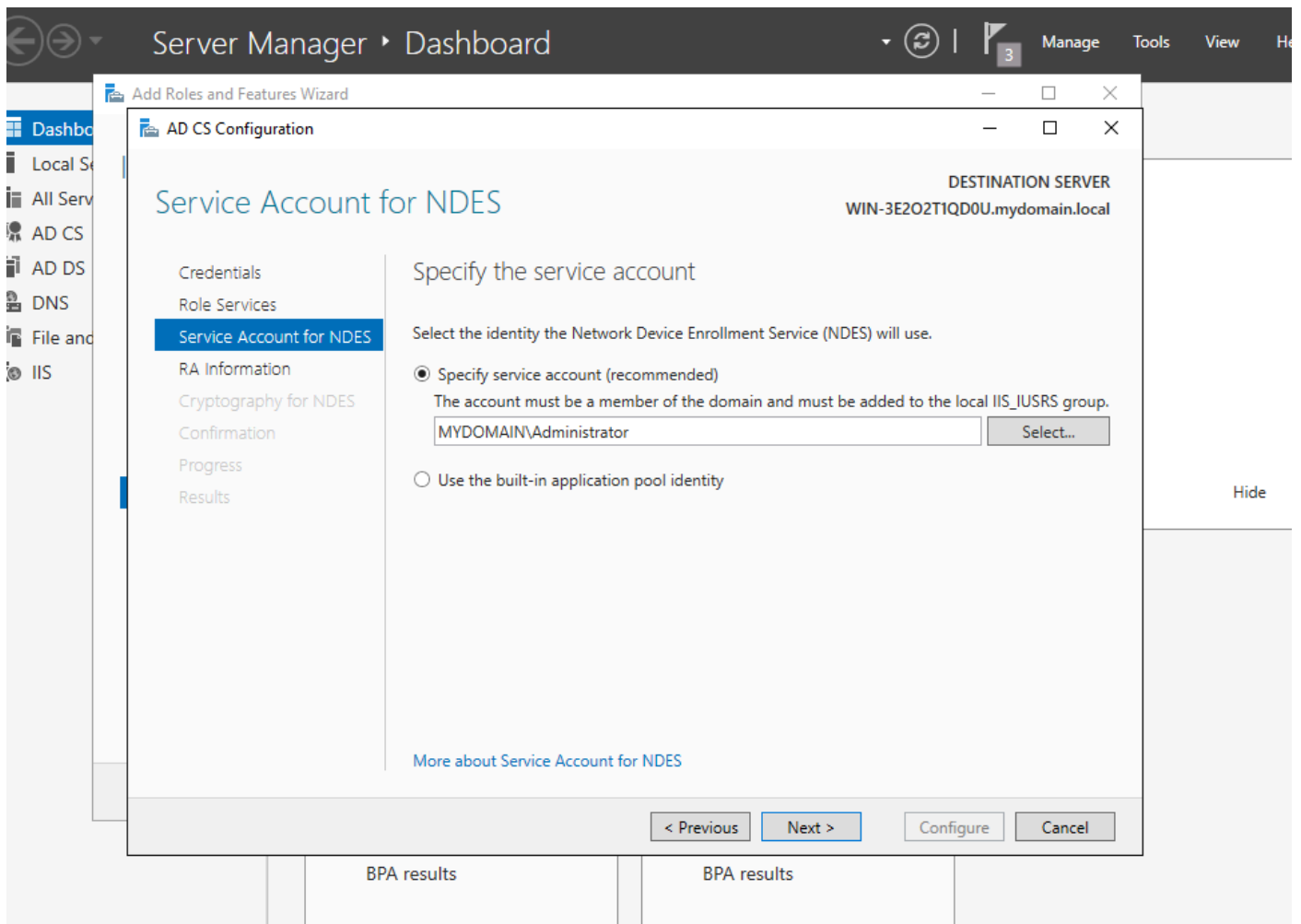
Instalar o NDES e os serviços de respondente online

Etapa 11. Depois de concluído, configure esses serviços.



Instalar o Respondente Online e o serviço NDES

Etapa 12. Você será solicitado a escolher uma conta de serviço. Esta é a conta que você adicionou anteriormente ao grupo IIS_IUSRS.



Selecione o usuário que você adicionou ao grupo IIS

Etapa 13. Isso é suficiente para operações SCEP, mas para obter a autenticação 802.1X, você também precisa instalar um certificado no servidor RADIUS. Portanto, para facilitar, instale e configure o serviço de inscrição na Web para poder copiar e colar facilmente a solicitação de certificado ISE em nosso Windows Server.

Select server roles

DESTINATION SERVER
WIN-3E202T1QD0U.mydomain.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

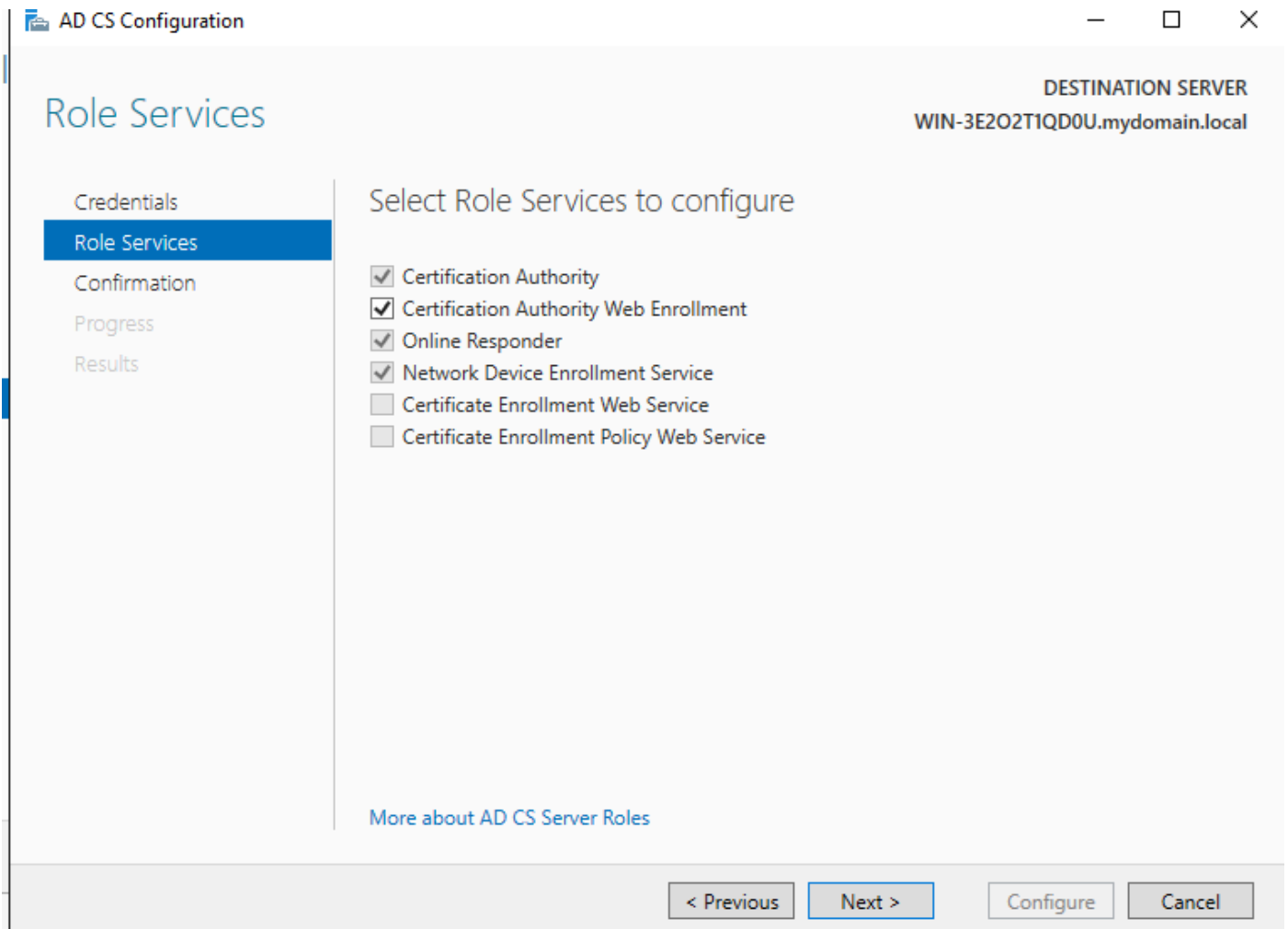
- Active Directory Certificate Services (3 of 6 installed)
 - Certification Authority (Installed)
 - Certificate Enrollment Policy Web Service
 - Certificate Enrollment Web Service
 - Certification Authority Web Enrollment**
 - Network Device Enrollment Service (Installed)
 - Online Responder (Installed)
- Active Directory Domain Services (Installed)
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server (Installed)
- Fax Server
- File and Storage Services (2 of 12 installed)
 - Host Guardian Service
 - Hyper-V
 - MultiPoint Services

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

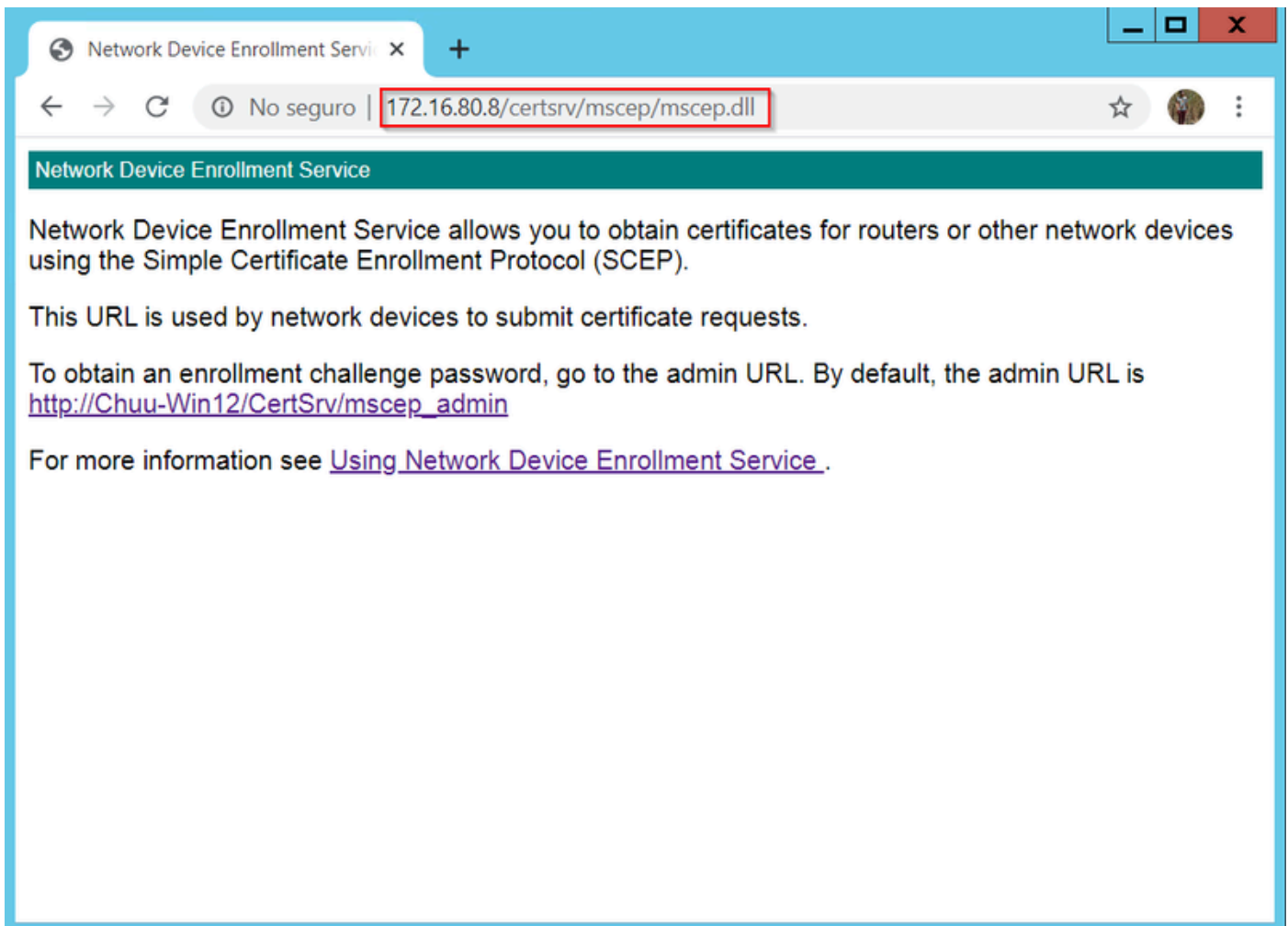
< Previous Next > Install Cancel

Instalar o serviço de registro na Web



configurar o serviço de registro na web

Etapa 14. Você pode verificar se o serviço SCEP está operando corretamente visitando <http://<serverip>/certsrv/mscep/mscep.dll>:



Verificação do portal SCEP

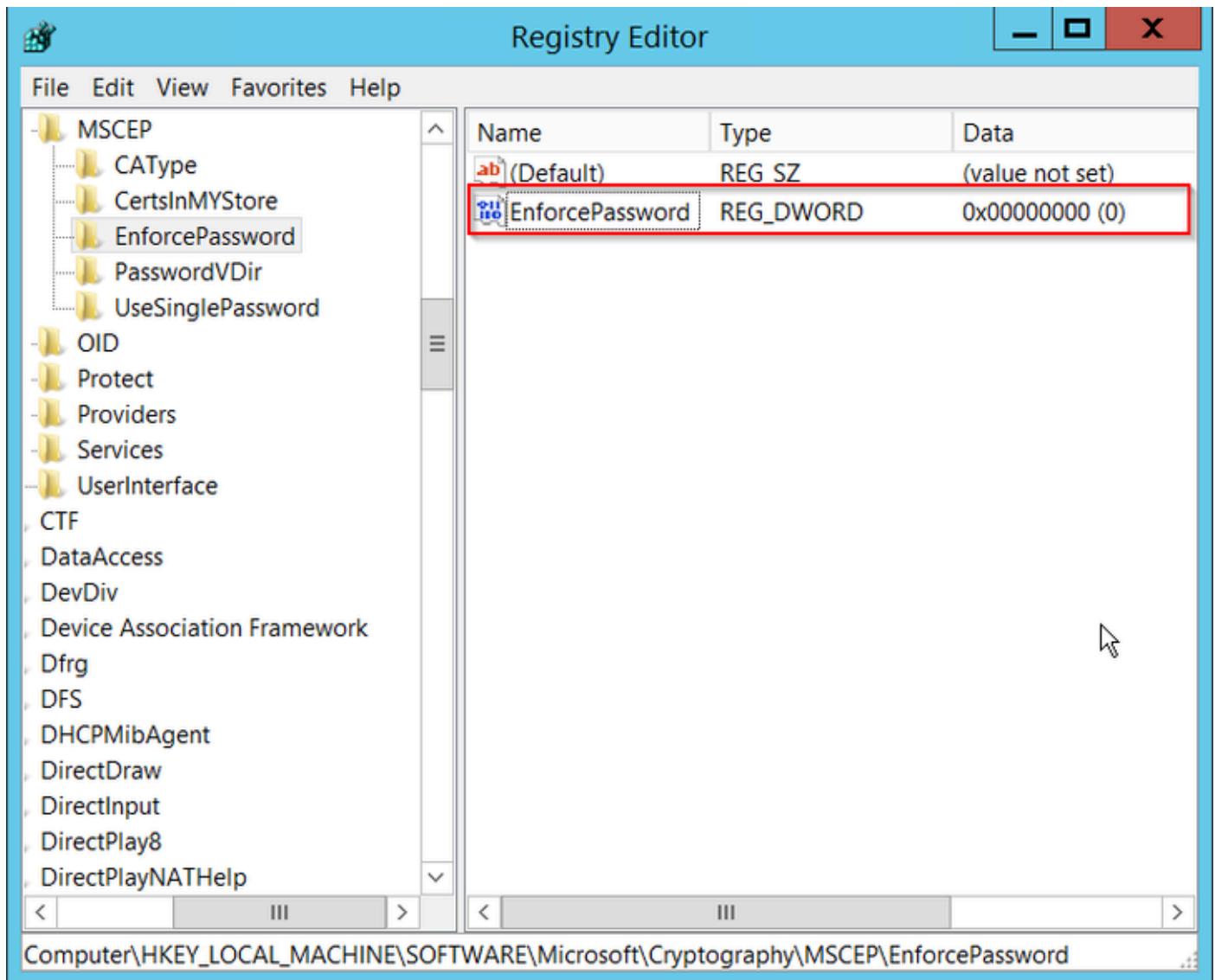
Etapa 15.

Por padrão, o Windows Server usava uma senha de desafio dinâmico para autenticar solicitações de cliente e de endpoint antes da inscrição no Microsoft SCEP (MSCEP). Isso exige que uma conta de administrador navegue até a GUI da Web para gerar uma senha sob demanda para cada solicitação (a senha deve ser incluída na solicitação). O controlador não é capaz de incluir essa senha nas solicitações que ele envia ao servidor. Para remover este recurso, a chave do Registro no servidor NDES precisa ser modificada:

Abra o Editor do Registro, procure Regedit no menu Iniciar.

Navegue até Computador > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografia > MSCEP > Aplicar senha

Altere o valor de EnforcePassword para 0. Se já for 0, deixe-o como está.



Defina o valor de Enforcepassword

Configurar o modelo de certificado e o registro

Os certificados e suas chaves associadas podem ser usados em vários cenários para diferentes finalidades definidas pelas políticas de aplicativo no servidor CA. A política de aplicativo é armazenada no campo Uso Estendido de Chave (EKU) do certificado. Esse campo é analisado pelo autenticador para verificar se é usado pelo cliente para a finalidade pretendida. Para certificar-se de que a política de aplicativo apropriada esteja integrada aos certificados WLC e AP, crie o modelo de certificado apropriado e mapeie-o para o registro NDES:


Etapa 1. Navegue até Start > Administrative Tools > Certification Authority.

Etapa 2. Expanda a árvore de pastas do servidor CA, clique com o botão direito do mouse nas pastas Modelos de certificado e selecione Gerenciar.

Etapa 3. Clique com o botão direito do mouse no modelo de certificado Users e selecione Duplicate Template no menu de contexto.

Etapa 4. Navegue até a guia Geral, altere o nome do modelo e o período de validade conforme

desejado e deixe todas as outras opções desmarcadas.

 Cuidado: quando o período de Validade for modificado, verifique se ele não é maior que a validade do certificado raiz da Autoridade de Certificação.

Properties of New Template



Subject Name		Server		Issuance Requirements	
Superseded Templates			Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation	

Template display name:

Template name:

Validity period:

Renewal period:

Publish certificate in Active Directory

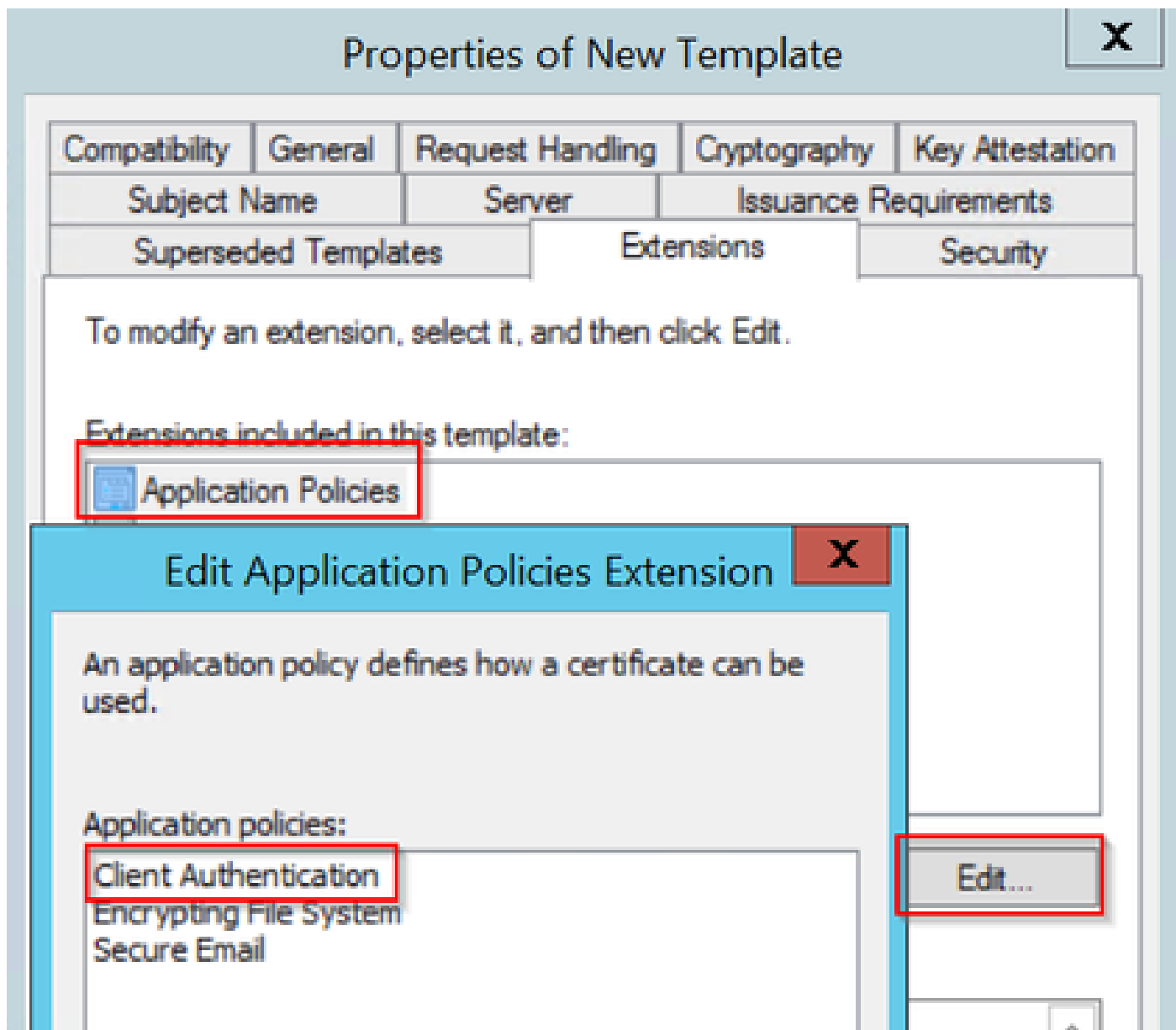
Do not automatically reenroll if a duplicate certificate exists in Active Directory

Etapa 5. Navegue até a guia Nome do assunto, certifique-se de que Suprimento na solicitação esteja selecionado. Um pop-up aparece para indicar que os usuários não precisam de aprovação do administrador para obter seu certificado assinado. Selecione OK.



Fornecimento na Solicitação

Etapa 6. Navegue até a guia Extensions, selecione a opção Application Policies e selecione o botão Edit.... Certifique-se de que Client Authentication esteja na janela Application Policies; caso contrário, selecione Add e adicione-a.



Verificar extensões

Passo 7. Navegue até a guia Segurança, certifique-se de que a conta de serviço definida na Etapa 6 de Ativar serviços SCEP no Windows Server tenha permissões de Controle Total do modelo e selecione Aplicar e OK.

Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
Superseded Templates		Extensions		Security

Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (CHUU-DOMAIN\Domain Admins)
- Domain Users (CHUU-DOMAIN\Domain Users)
- Enterprise Admins (CHUU-DOMAIN\Enterprise Admins)

Permissions for Administrator

Allow


Deny

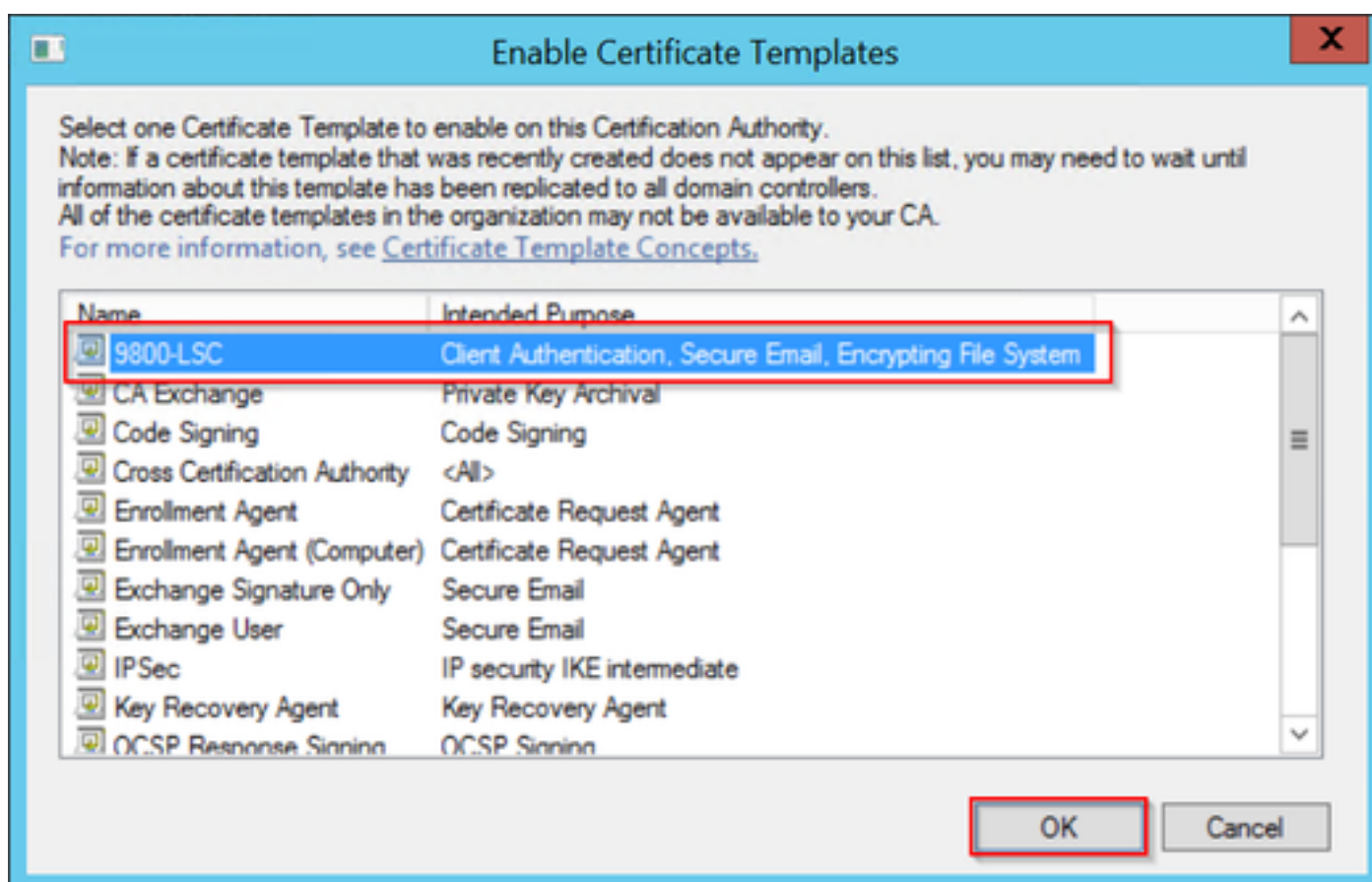
	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Etapa 8. Retorne à janela Autoridade de certificação, clique com o botão direito do mouse na pasta Modelos de certificado e selecione Novo > Modelo de certificado a ser emitido.

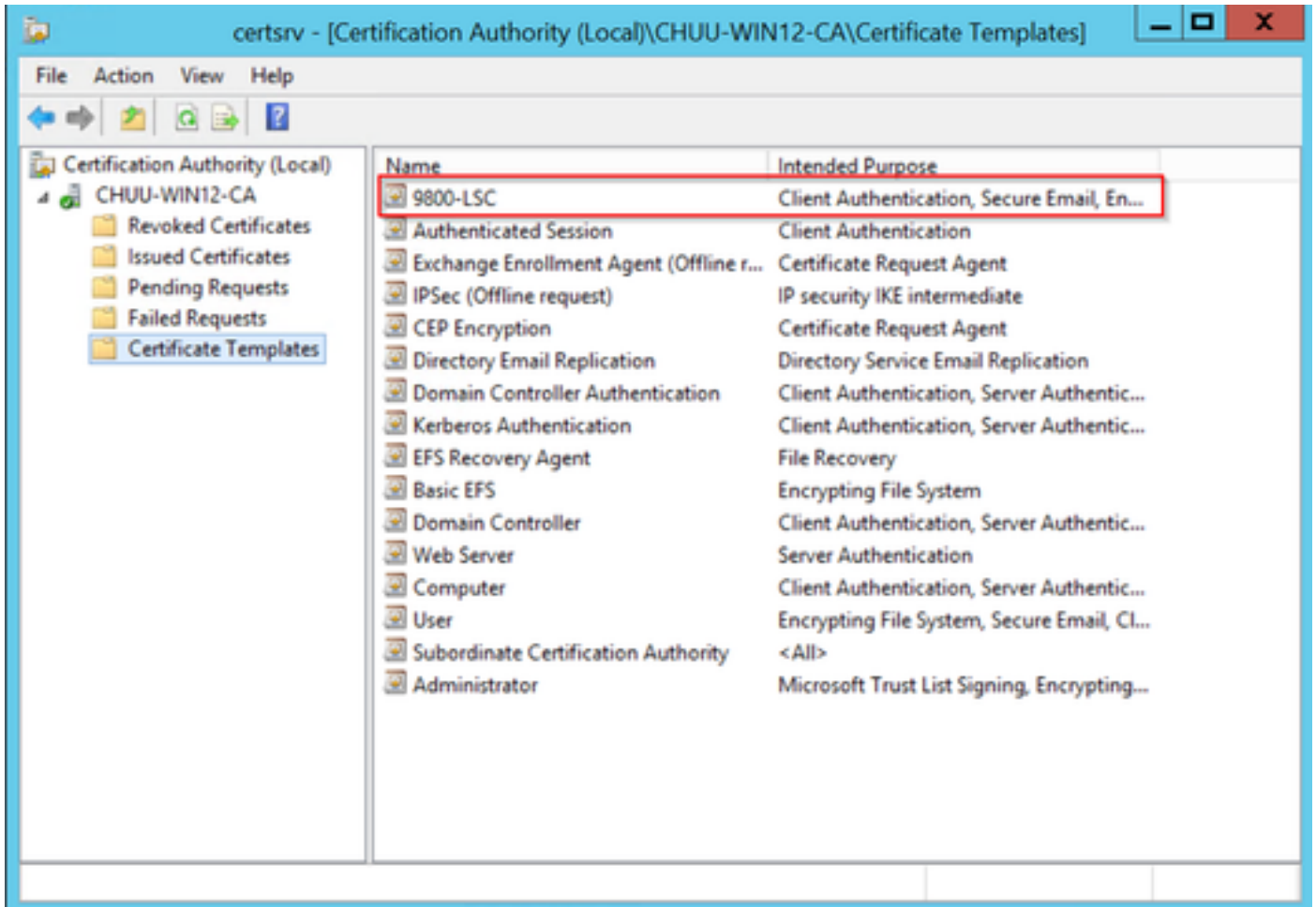
Etapa 9. Selecione o modelo de certificado criado anteriormente, neste exemplo é 9800-LSC, e selecione OK.

 Observação: o modelo de certificado recém-criado pode demorar mais para ser listado em várias implantações de servidor, pois precisa ser replicado em todos os servidores.



Escolha o modelo

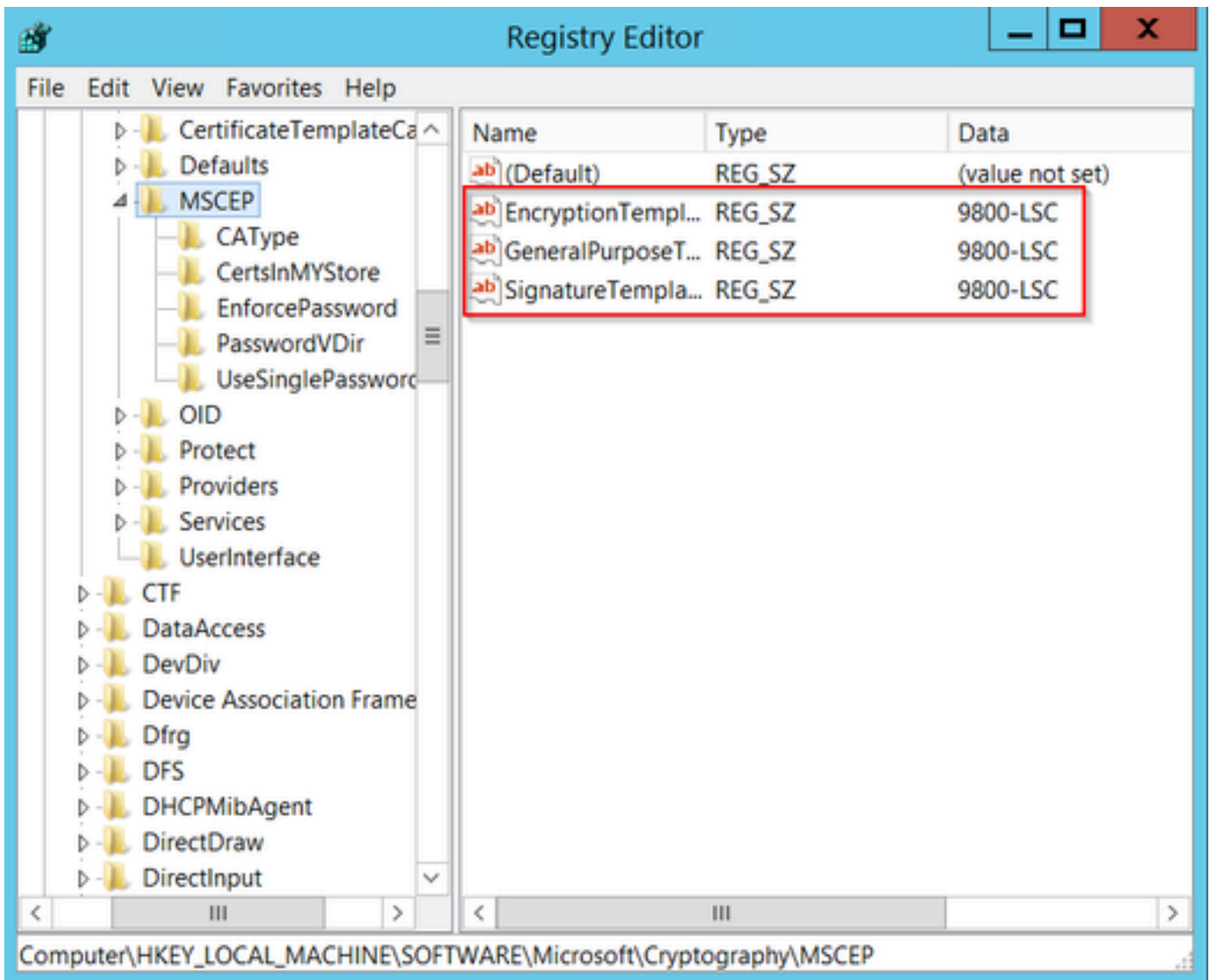
O novo modelo de certificado está listado agora no conteúdo da pasta Modelos de certificado.



Seleção o LSC

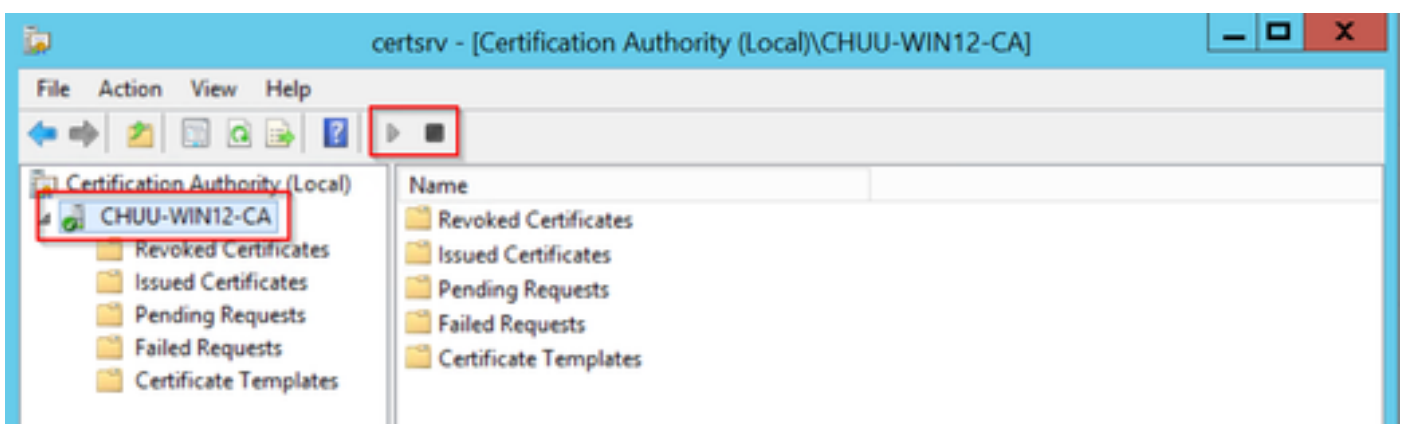
Etapa 10. Retorne à janela Editor do Registro e navegue para Computador > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografia > MSCEP.

Etapa 11. Edite os registros EncryptionTemplate, GeneralPurposeTemplate e SignatureTemplate para que eles apontem para o modelo de certificado recém-criado.



Alterar o Modelo no Registro

Etapa 12. Reinicialize o servidor NDES, então retorne à janela Certification Authority , selecione o nome do servidor e selecione o botão Stop e Play sucessivamente.



Configurar o LSC no 9800

Aqui estão as etapas na sequência para configurar o LSC para AP no WLC.

1. Criar chave RSA. Essa chave é usada posteriormente para o ponto de confiança PKI.
2. Crie um ponto confiável e mapeie a chave RSA criada.
3. Habilite o provisionamento LSC para APs e mapeie o ponto de confiança.
 1. Habilite o LSC para todos os APs associados.
 2. Habilitar LSC para APs selecionados através da lista de provisionamento.
4. Altere o ponto confiável de gerenciamento sem fio e aponte para o ponto confiável LSC.

Etapas de configuração da GUI do AP LSC

Etapa 1. Navegue até Configuration > Security > PKI Management > Key Pair Generation.

1. Clique em adicionar e atribua a ele um nome relevante.
2. Adicione o tamanho da chave RSA.
3. A opção de chave exportável é opcional. Isso só é necessário se você quiser exportar a chave fora da caixa.
4. Selecione Gerar

The screenshot shows the 'Key Pair Generation' configuration page in the Cisco ISE GUI. The breadcrumb navigation is 'Configuration > Security > PKI Management'. The page has tabs for 'Trustpoints', 'CA Server', 'Key Pair Generation', 'Add Certificate', and 'Trustpool'. A '+ Add' button is visible. Below it is a table of existing key pairs:

Key Name	Key Type	Key Exportable	Zeroize
TP-self-signed-2147029136	RSA	No	Zeroize
9800-40.cisco.com	RSA	No	Zeroize
TP-self-signed-2147029136.server	RSA	No	Zeroize
CISCO_IDEVID_SUDI	RSA	No	Zeroize
CISCO_IDEVID_SUDI_LEGACY	RSA	No	Zeroize

Below the table is a form to create a new key pair. The fields are:

- Key Name***: AP-SCEP
- Key Type***: RSA Key (selected), EC Key
- Modulus Size***: 2048
- Key Exportable***:

Buttons for 'Cancel' and 'Generate' are at the bottom right of the form.

Etapa 2. Navegue até Configuration > Security > PKI Management > Trustpoints

1. Clique em adicionar e atribua a ele um nome relevante.
2. Insira o URL de inscrição (aqui o URL é <http://10.106.35.61:80/certsrv/mscep/mscep.dll>) e o restante dos detalhes.
3. Selecione os pares de chaves RSA criados na etapa 1.
4. Clique em Authenticate.
5. Clique em registrar ponto confiável e insira uma senha.
6. Clique em Aplicar ao dispositivo.

Configuration > Security > PKI Management

Add Trustpoint

Label* Enrollment Type SCEP Terminal

Subject Name

Country Code State

Location Domain Name

Organization Email Address

Enrollment URL Authenticate

Key Generated Available RSA Keypairs

Enroll Trustpoint

Password*

Re-Enter Password*

Etapa 3. Navegue até Configuration > Wireless > Access Points. Role para baixo e selecione Provisionamento LSC.

1. Selecione o status como habilitado. Isso ativa o LSC para todos os APs que estão conectados a esta WLC.
2. Selecione o nome do ponto confiável que criamos na Etapa 2.

Preencha o restante dos detalhes de acordo com suas necessidades.

Configuration > Wireless > Access Points

All Access Points

Total APs: 1

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Config Status
AP000-F89A-46E0	C9117AXI-D	2	Enabled	0 days 0 hrs 26 mins 42 secs	10.105.101.158	80ec.3579.0300	0cd0.f99a.46e0	Local	Yes	Registered	Healthy

6 GHz Radios

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

Status

Trustpoint Name

Number of Join Attempts

Key Size

Certificate chain status

Subject Name Parameters

Country

State

City

Organization

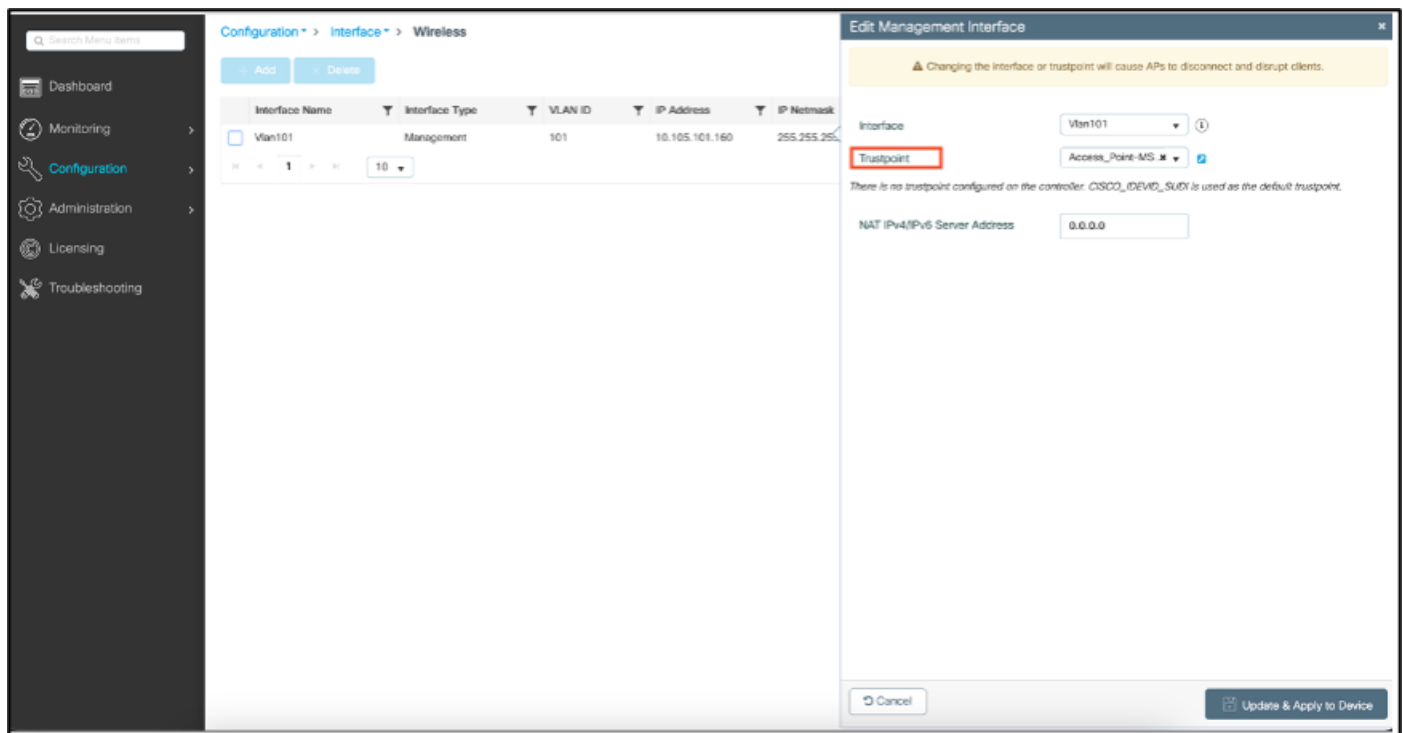
Depois de habilitar o LSC, os APs baixam o certificado via WLC e reinicializam. Na sessão de console do AP, você verá algo como esse snippet.

```
[*09/25/2023 10:03:28.0993] .....
[*09/25/2023 10:03:28.7016] .....+++++
[*09/25/2023 10:03:28.7663] writing new private key to '/tmp/lsc/priv_key'
[*09/25/2023 10:03:28.7666] -----
[*09/25/2023 10:03:28.9212] LSC_ENABLE: saving ROOT_CERT
[*09/25/2023 10:03:28.9212]
[*09/25/2023 10:03:28.9293] LSC_ENABLE: saving DEVICE_CERT
[*09/25/2023 10:03:28.9293]
[*09/25/2023 10:03:28.9635] LSC certs and private key verified
[*09/25/2023 10:03:28.9635]
[*09/25/2023 10:03:29.4997] LSC private key written to hardware TAM
[*09/25/2023 10:03:29.4997]
[*09/25/2023 10:03:29.5526] A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed
```

Etapa 4. Quando o LSC estiver habilitado, você poderá alterar o certificado de Gerenciamento sem fio para corresponder ao ponto confiável do LSC. Isso faz com que os APs se unam com seus certificados LSC e a WLC use seu certificado LSC para junção de AP. Esta é uma etapa opcional se seu único interessado for fazer a autenticação 802.1X de seus APs.

1. Vá para Configuration > Interface > Wireless e clique em Management Interface.
2. Altere o ponto confiável para corresponder ao ponto confiável criado na etapa 2.

Isso conclui a parte de configuração da GUI do LSC. Os APs devem poder se unir à WLC usando o certificado LSC agora.



Etapas de configuração do AP LSC CLI

1. Crie uma chave RSA usando este comando.

```
9800-40(config)#crypto key generate rsa general-keys modulus 2048 label AP-SCEP
```

```
% You already have RSA keys defined named AP-SCEP.
% They will be replaced
```

```
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Sep 27 05:08:13.144: %CRYPTO_ENGINE-5-KEY_DELETED: A key named AP-SCEP has been removed from key storage
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. Crie um ponto de confiança PKI e mapeie o par de chaves RSA. Insira o URL de inscrição e o restante dos detalhes.

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
9800-40(ca-trustpoint)#rsaakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. Autentique e registre o ponto de confiança PKI com o servidor de CA usando o comando `crypto pki authenticate <trustpoint>`. Digite uma senha no prompt de senha.

```
9800-40(config)#crypto pki authenticate Access_Point-MS-CA
Certificate has the following attributes:
Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B
Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-40(config)#crypto pki enroll Access_Point-MS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Sep 26 01:25:00.880: %PKI-6-CERT_ENROLL_MANUAL: Manual enrollment for trustpoint Access_Point-MS-CA
Re-enter password:
% The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local
% The subject name in the certificate will include: 9800-40.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: TTM244909MX
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose Access_Point-MS-CA' command will show the fingerprint.
Sep 26 01:25:15.062: %PKI-6-CSR_FINGERPRINT:
CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667
CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005
CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9
Sep 26 01:25:15.063: CRYPTO_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27
Sep 26 01:25:30.239: %PKI-6-CERT_INSTALL: An ID certificate has been installed under
Trustpoint : Access_Point-MS-CA
```

```
Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4
Serial-number: 5C0000001400DD405D77E6FE7F000000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#
```

4. Configure a junção de AP com o certificado LSC.

```
9800-40(config)#ap lsc-provision join-attempt 10
9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-L
9800-40(config)#ap lsc-provision key-size 2048
9800-40(config)#ap lsc-provision trustpoint Access_Point-MS-CA
9800-40(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration
Are you sure you want to continue? (y/n): y
```

5. Altere Wireless Management Trustpoint (Ponto confiável de gerenciamento sem fio) para corresponder ao ponto confiável criado acima.

```
9800-40(config)#wireless management trustpoint Access_Point-MS-CA
```

Verificação LSC do AP

Execute esses comandos no WLC para verificar o LSC.

```
#show wireless management trustpoint
#show ap lsc-provision summary
#show ap name < AP NAME > config general | be Certificate
```

```

9800-40#sho ap lsc-provision summ
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : Access_Point-MS-CA
Certificate chain status : Available
Number of certs on chain : 2
Certificate hash      : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : Bengaluru
Orgn : TAC
Dept : TAC-LAB.cisco.local
Email : mail@tac-lab.local
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 0

Mac Addresses :
-----

9800-40#sho wire
9800-40#sho wireless man
9800-40#sho wireless management tru
9800-40#sho wireless management trustpoint
Trustpoint Name : Access_Point-MS-CA
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
Private key Info : Available
FIPS suitability : Not Applicable

9800-40#

```

```

9800-40#sho ap name AP@CD0.F89A.46E0 config general | begin Certificate
AP Certificate type : Locally Significant Certificate
AP Certificate expiry-time : 09/25/2024 06:48:23
AP Certificate issuer common-name : sumans-lab-ca
AP Certificate Policy : Default
AP CAPWAP-OTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP 002.lx LSC Status
Certificate status : Not Available
AP LSC authentication state : CAPWAP-OTLS

```

Depois que os APs forem recarregados, faça login na CLI do AP e execute esses comandos para verificar a configuração do LSC.

```

#show crypto | be LSC
#show capwap cli config | in lsc
#show dtls connection

```

```

AP@CD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
----- Device Certificate -----
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:18
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
  Validity
    Not Before: Sep 28 04:15:28 2023 GMT
    Not After : Sep 27 04:15:28 2024 GMT
  Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0 emailAddress = mail@tac-lab.local
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:

```

```
AP0CD0.F89A.46E0#sho crypto | in LSC
LSC: Enabled
AP0CD0.F89A.46E0#sho capwap cli config | in lsc
AP lsc enable : 1
AP lsc reboot cnt : 0
AP lsc max num of retry : 10
AP lsc mode : 0x1
AP lsc dtls fallback state : 0
AP0CD0.F89A.46E0#
Read timed out
```

```
AP0CD0.F89A.46E0#sho dtls connections
```

```
Number of DTLS connection = 1
```

```
[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version
```

```
[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2
```

```
Current connection certificate issuer name: sumans-lab-ca
```

Solucionar problemas de provisionamento de LSC

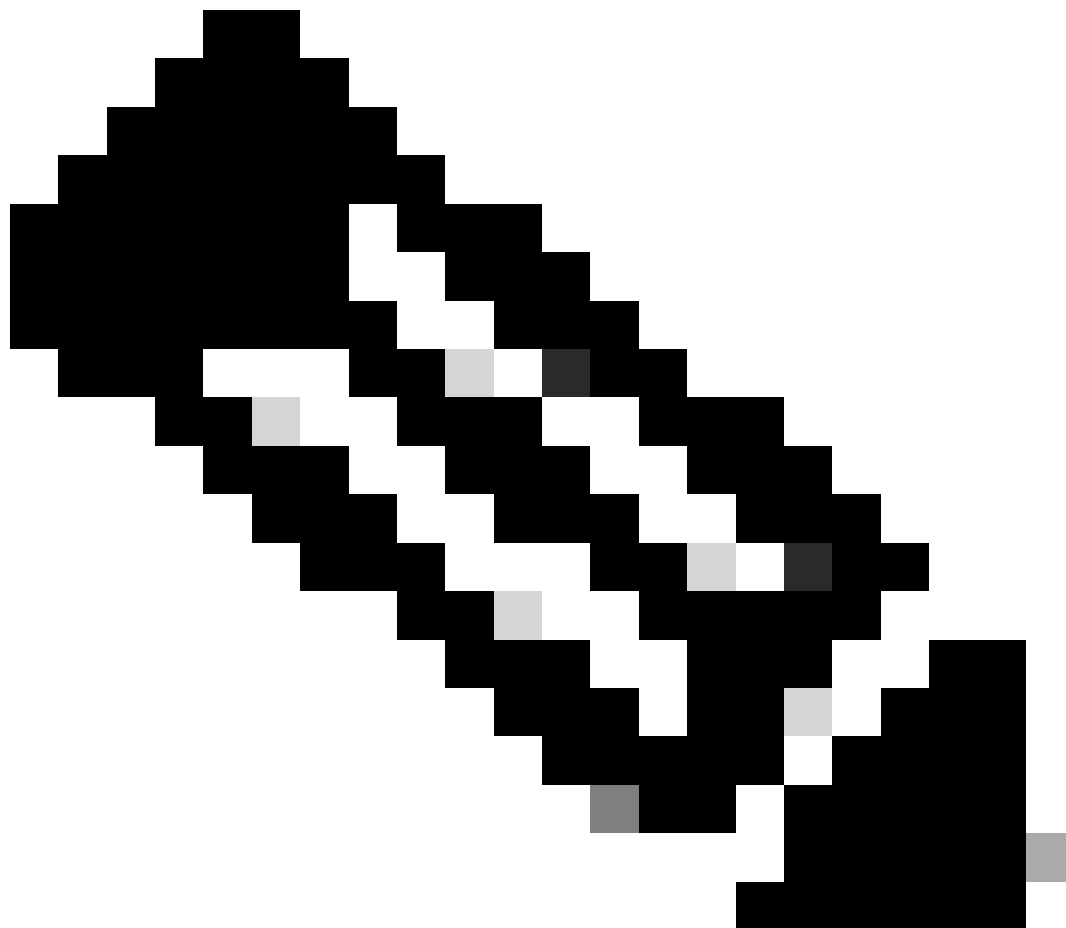
Você pode fazer uma captura EPC da porta do switch de uplink da WLC ou do AP para verificar o certificado que o AP está usando para formar o túnel CAPWAP. Verifique a partir do PCAP se o túnel DTLS foi criado com êxito.

```
▼ Datagram Transport Layer Security
  ▼ DTLSv1.2 Record Layer: Handshake Protocol: Certificate (Reassembled)
    Content Type: Handshake (22)
    Version: DTLS 1.2 (0xfefd)
    Epoch: 0
    Sequence Number: 5
    Length: 82
  ▼ Handshake Protocol: Certificate (Reassembled)
    Handshake Type: Certificate (11)
    Length: 1627
    Message Sequence: 2
    Fragment Offset: 1557
    Fragment Length: 70
    Certificates Length: 1624
  ▼ Certificates (1624 bytes)
    Certificate Length: 1621
  ▼ Certificate: 3082065130820539a00302010202135c000000181814edda85f9bfd100000000018300d. (pkcs-9-at-emailAddress@mail@tac-lab.local,id-at-commonName=
  ▼ signedCertificate
    version: v3 (2)
    serialNumber: 0x5c000000181814edda85f9bfd1000000000018
  ▼ signature (sha256WithRSAEncryption)
    Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
  ▼ issuer: rdnSequence (0)
  ▼ rdnSequence: 4 items (id-at-commonName=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com)
  ▼ RDNSSequence item: 1 item (dc=com)
  ▼ RelativeDistinguishedName item (dc=com)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: com
  ▼ RDNSSequence item: 1 item (dc=tac-lab)
  ▼ RelativeDistinguishedName item (dc=tac-lab)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: tac-lab
  ▼ RDNSSequence item: 1 item (dc=sumans)
  ▼ RelativeDistinguishedName item (dc=sumans)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: sumans
  ▼ RDNSSequence item: 1 item (id-at-commonName=sumans-lab-ca)
  ▼ RelativeDistinguishedName item (id-at-commonName=sumans-lab-ca)
    Object Id: 2.5.4.3 (id-at-commonName)
  ▼ DirectoryString: printableString (1)
    printableString: sumans-lab-ca
  ▼ validity
  ▼ notBefore: utcTime (0)
    utcTime: 2023-09-28 04:15:28 (UTC)
  ▼ notAfter: utcTime (0)
    utcTime: 2024-09-27 04:15:28 (UTC)
  ▼ subject: rdnSequence (0)
```

As depurações de DTLS podem ser executadas no AP e no WLC para entender o problema do certificado.

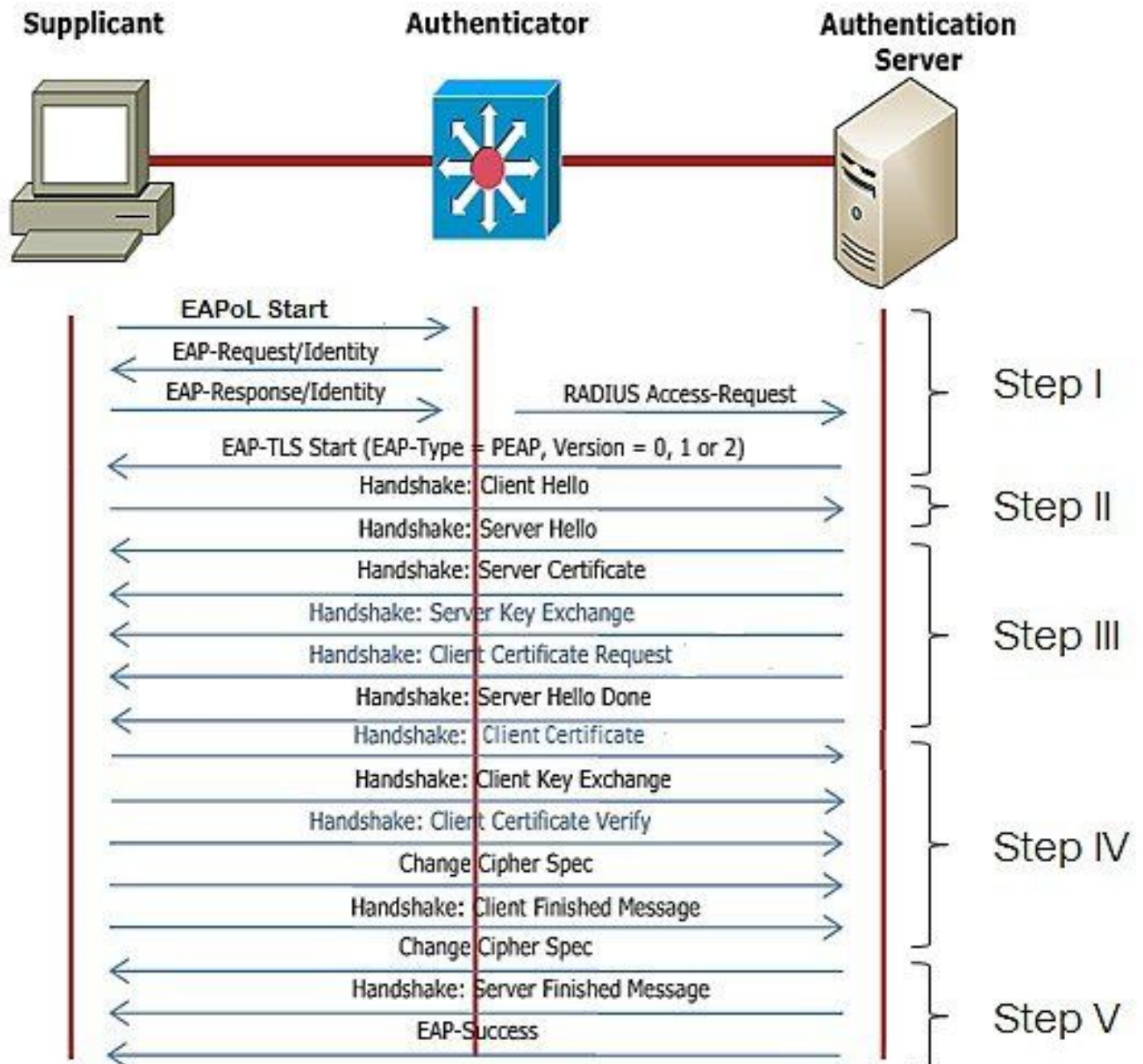
Autenticação 802.1X com fio AP usando LSC

O AP é configurado para usar o mesmo certificado LSC para se autenticar. O AP atua como solicitante 802.1X e é autenticado pelo switch no servidor ISE. O servidor ISE conversa com o AD no back-end.



Observação: depois que a autenticação dot1x é habilitada na porta do switch de uplink do AP, os APs não podem encaminhar ou receber nenhum tráfego até que a autenticação seja passada. Para recuperar APs com autenticação malsucedida e obter acesso ao AP, desabilite a autenticação dot1x na porta do switch com fio do AP.

Fluxo de trabalho de autenticação e troca de mensagens EAP-TLS

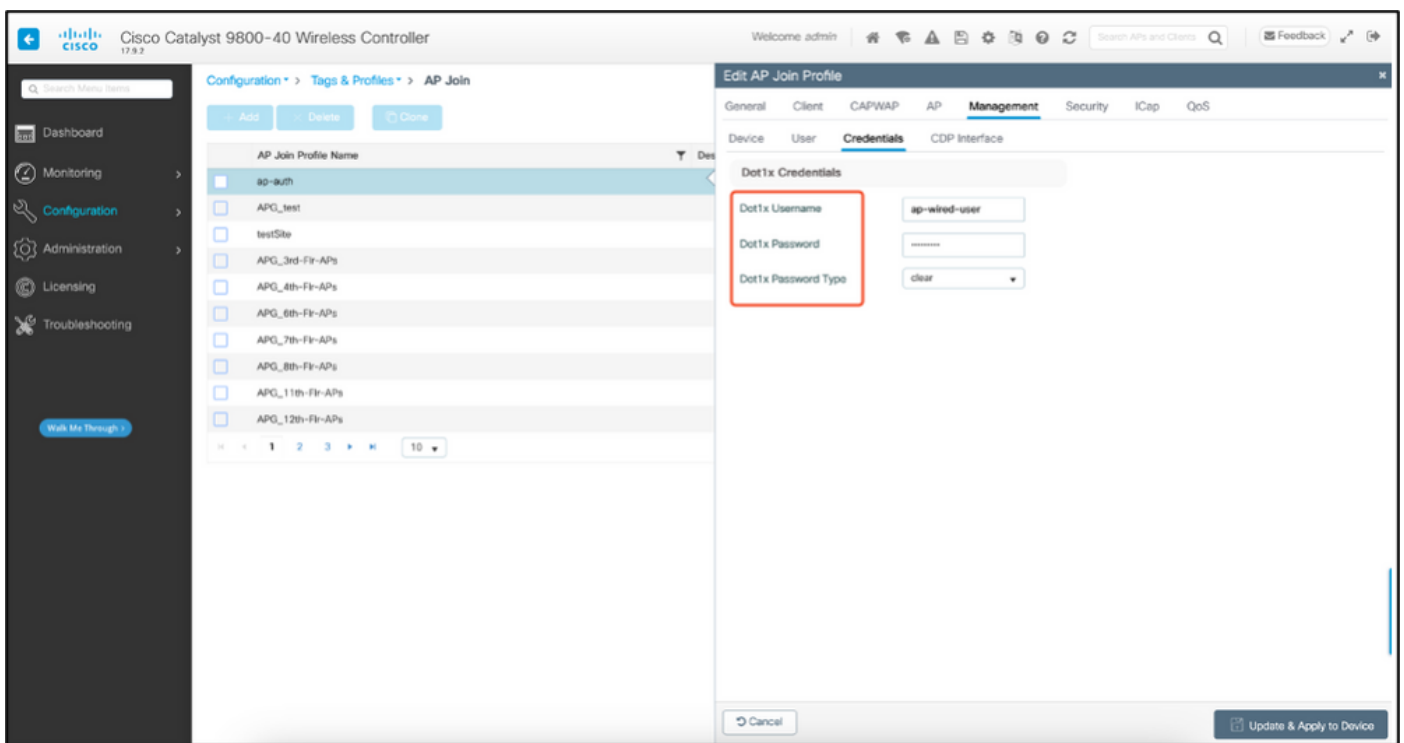
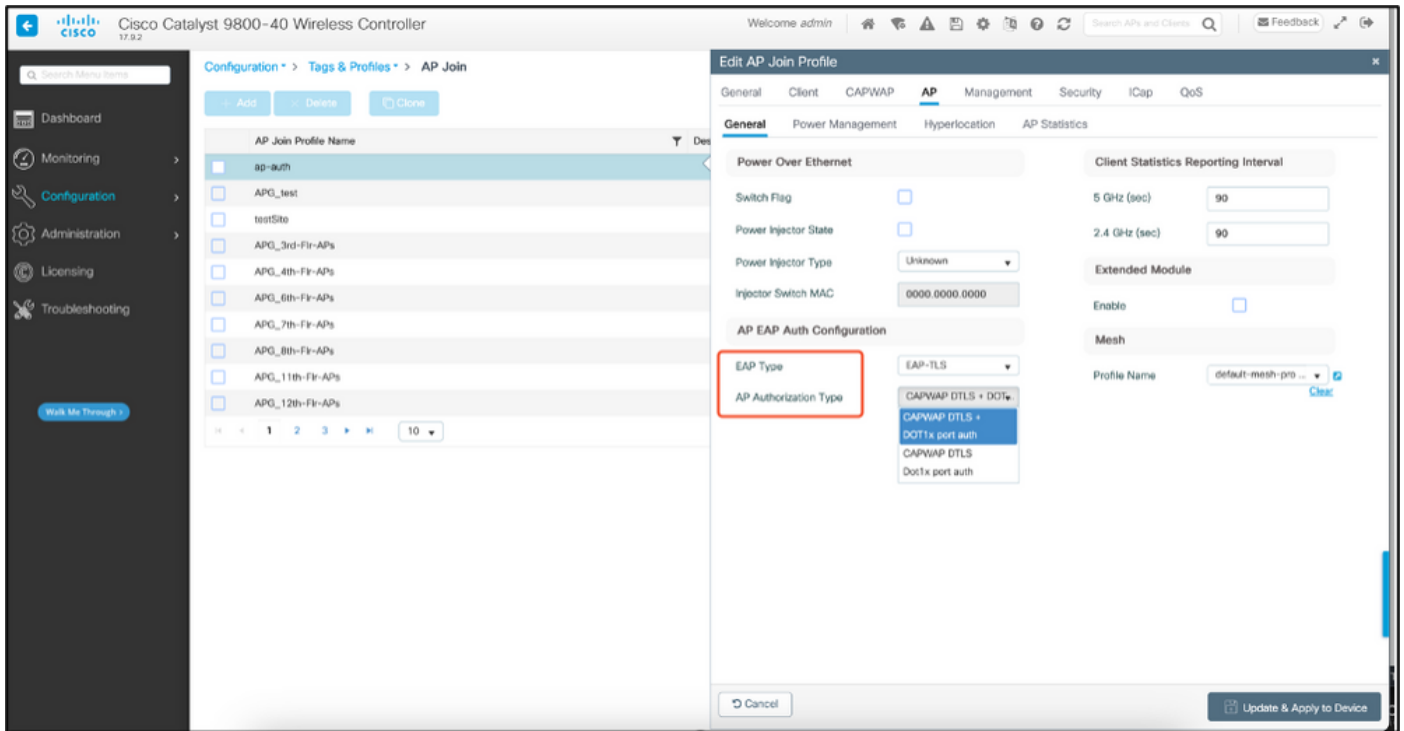


Etapas de Configuração da Autenticação 802.1x com Fio AP

1. Ative a autenticação de porta dot1x junto com CAPWAP DTLS e selecione o tipo de EAP.
2. Crie credenciais dot1x para APs.
3. Ative dot1x na porta do switch.
4. Instale um certificado confiável no servidor RADIUS.

Configuração da GUI de autenticação do AP Wired 802.1x

1. Navegue até o perfil de junção AP e clique no perfil.
 1. Clique em AP > Geral. Selecione o tipo de EAP e o tipo de autorização de AP como "CAPWAP DTLS + dot1x port auth".
 2. Navegue para Gerenciamento > Credenciais e crie um nome de usuário e uma senha para a autenticação dot1x do AP.



Configuração CLI de autenticação 802.1x com fio do AP

Use estes comandos para ativar o dot1x para APs a partir da CLI. Isso só permite a autenticação com fio para APs que estão usando o perfil de junção específico.

```
#ap profile ap-auth
#dot1x eap-type eap-tls
#dot1x lsc-ap-auth-state both
#dot1x username ap-wired-user password 0 cisco!123
```

```
9808-40(config)#ap profile ap-auth
9808-40(config-ap-profile)#dot1x cap-type cap-tls
9808-40(config-ap-profile)#dot1x lsc-ap-auth-state both
9808-40(config-ap-profile)#
```

Configuração do switch de autenticação 802.1x com fio AP

Essas configurações de switch são usadas no LAB para ativar a autenticação com fio do AP. Você pode ter configurações diferentes com base no design.

```
aaa new-model
dot1x system-auth-control
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius server ISE
address ipv4 10.106.34.170 auth-port 1812 acct-port 1813
key cisco!123
!
interface GigabitEthernet1/0/2
description "AP-UPLINK-PORT-AUTH-ENABLED"
switchport access vlan 101
switchport mode access
authentication host-mode multi-host
authentication order dot1x
authentication priority dot1x
authentication port-control auto
dot1x pae authenticator
end
```

Instalação do Certificado de Servidor RADIUS

A autenticação ocorre entre o AP (que está atuando como o solicitante) e o servidor RADIUS. Ambos devem confiar um no outro certificado. A única maneira de fazer com que o AP confie no certificado do servidor RADIUS é fazer com que o servidor RADIUS use uma taxa de certificação emitida pela CA SCEP que também emitiu o certificado do AP.

No ISE, vá para Administração > Certificados > Gerar solicitações de assinatura de certificado

Gere um CSR e preencha os campos com as informações do nó do ISE.

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority

Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - Generate a Signing Certificate or generate a brand new Messaging Certificate.
- Data Connect Certificate - Connect to Oracle Database

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for EAP Authentication

Allow Wildcard Certificates ⊙

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ISE99	ISE99#EAP Authentication

Subject

Common Name (CN) ⊙

Organizational Unit (OU) ⊙

Organization (O) ⊙

City (L)

State (ST)

Depois de gerada, você também pode exportá-la e copiá-la e colá-la como texto.

Navegue até o endereço IP da CA do Windows e adicione /certsrv/ à URL

Clique em Solicitar um certificado

← → ↻ Non sécurisé | 192.168.1.98/certsrv/

Microsoft Active Directory Certificate Services — mydomain-WIN-3E202T1QD0U-CA

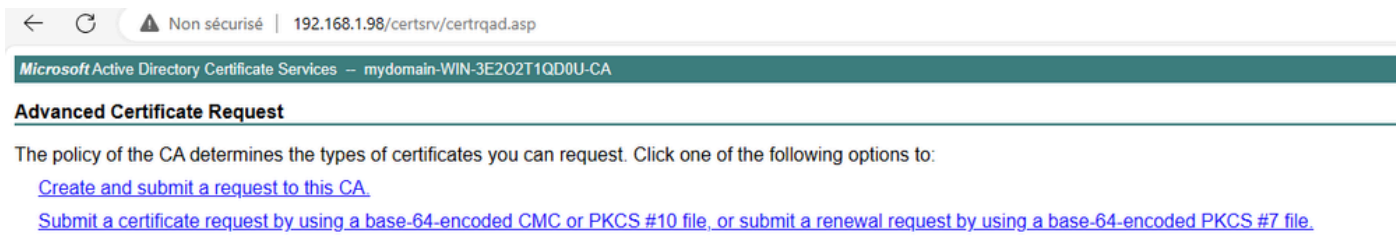
Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

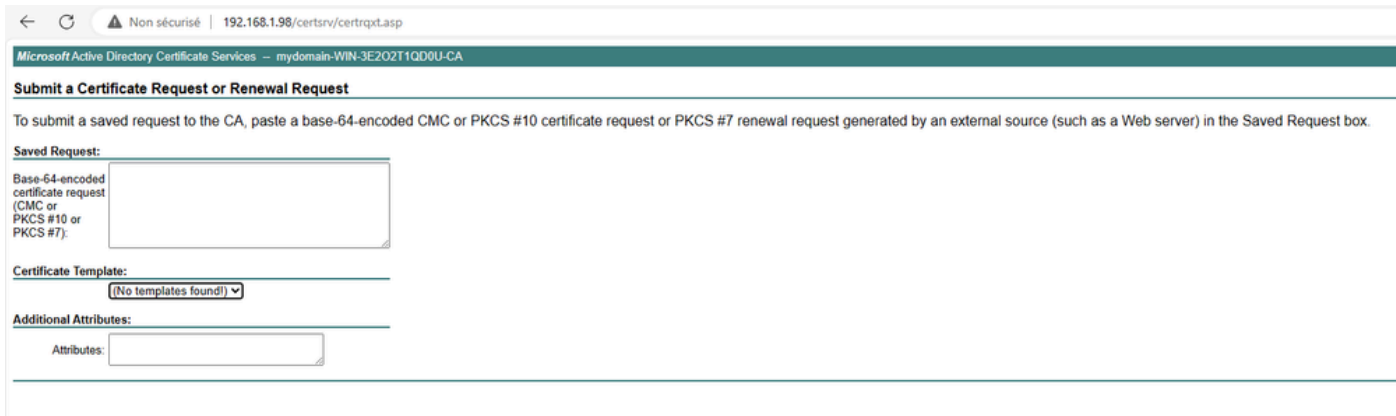
Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

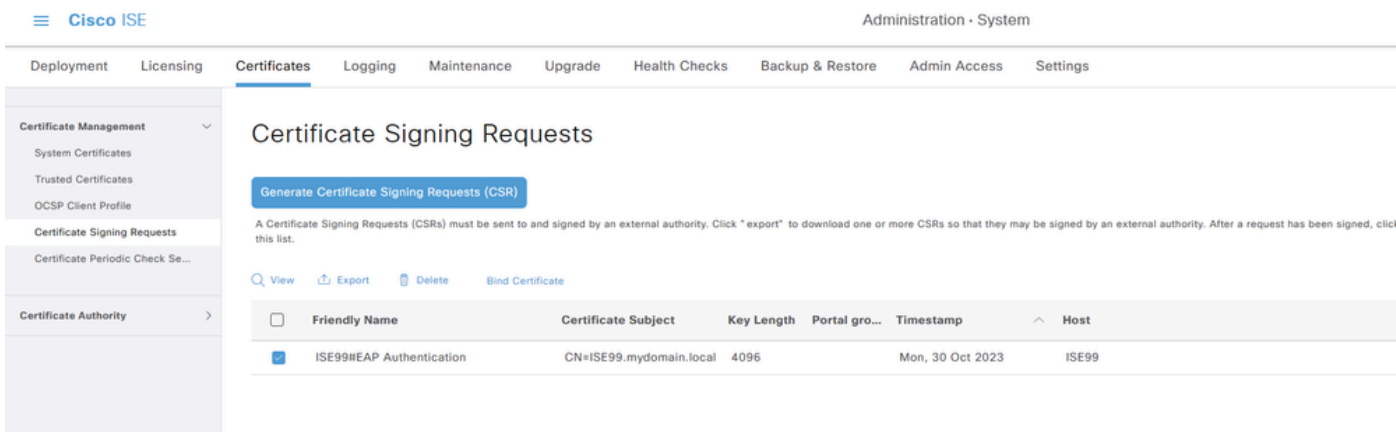
Clique em Submit a certificate request by using a base-64



Cole o texto CSR na caixa de texto. Escolha o modelo de certificado do servidor Web.



Você pode instalar este certificado no ISE voltando ao menu Certificate Signing Request e clicando em Bind certificate. Em seguida, você pode carregar o certificado obtido do Windows C.



Verificação de autenticação AP Wired 802.1x

Aceite o acesso do console ao AP e execute o comando:

```
#show ap authentication status
```

A autenticação do aplicativo não está habilitada:

```
AP0C0B.F89A.46E8#sho ap authentication status
AP dot1x feature is disabled.
AP0C0B.F89A.46E8#
```

Registros de console do AP após ativar a autenticação do AP:

```
AP0CD0.F89A.46E0#[*09/26/2023 08:57:40.9154]
[*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode
[*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL
```

AP autenticado com êxito:

```
AP0CD0.F89A.46E0#sho ap authentication status
ap_name=IEEE_802.1X (no WPA)
ap_state=COMPLETED
address=c1:08:f8:9a:46:e0
supplicant_PAE_state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
wap_tls_version=TLSv1.2
EAP TLS cipher=ECDHE-RSA-AES256-GCM-SHA384
tls_session_reused=0
wap_session_id=07b91a744885afe8e460d49fee7d2d5604ea2bdd11f40494a4325c98d1919af48b9fb33ee526f18eda11effcb2ea0238cf95244aaf5f17decf336ad1e88121
AP0CD0.F89A.46E0#
```

Verificação de WLC:

```
9800-48#sho ap name AP0CD0.F89A.46E0 config general | begin Certificate
AP Certificate type : Locally Significant Certificate
AP Certificate Expiry-time : 09/25/2024 06:48:23
AP Certificate issuer common-name : sumans-lab-ca
AP Certificate Policy : Default
AP CAPWAP-DTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP 802.1x LSC Status
Certificate status : Available
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP LSC authentication state : CAPWAP-DTLS and 802.1x authentication
```

Pós-autenticação bem-sucedida do status da interface da porta do switch:

```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface MAC Address Method Domain Status Fg Session ID
-----
G11/0/2 0cd0.f89a.46e0 dot1x DATA Auth 9765690A000005CCEED8FBF
```

Este é um exemplo de registros de console de AP indicando uma autenticação bem-sucedida:

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 compl
```


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.