Configuración de 802.1X en AP para PEAP o EAP-TLS con LSC

Contenido

Introducción

Este documento describe cómo autenticar los puntos de acceso de Cisco en su puerto de switch mediante los métodos 802.1X PEAP o EAP-TLS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controlador inalámbrico

- Punto de Acceso
- Switch
- servidor ISE
- Autoridad de certificados.

Componentes Utilizados

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

- Controlador inalámbrico: C9800-40-K9 que ejecuta 17.09.02
- Punto de acceso: C9117AXI-D
- Switch: C9200L-24P-4G que ejecuta 17.06.04
- Servidor AAA: ISE-VM-K9 con 3.1.0.518
- Autoridad de certificación: Windows Server 2016

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Si desea que sus puntos de acceso (AP) se autentiquen con su puerto de switch usando 802.1X, de forma predeterminada utilizan el protocolo de autenticación EAP-FAST que no requiere certificados. Si desea que los AP utilicen el método PEAP-mschapv2 (que utiliza credenciales en el lado AP pero un certificado en el lado RADIUS) o el método EAP-TLS (que utiliza certificados en ambos lados), primero debe configurar LSC. Es la única manera de aprovisionar un certificado raíz/de confianza en un punto de acceso (y también un certificado de dispositivo en el caso de EAP-TLS). No es posible que el AP haga PEAP e ignore la validación del lado del servidor. En este documento se trata primero la configuración de LSC y, a continuación, el lado de la configuración de 802.1X.

Utilice un LSC si desea que su PKI proporcione una mayor seguridad, tenga el control de su autoridad de certificación (CA) y defina políticas, restricciones y usos en los certificados generados.

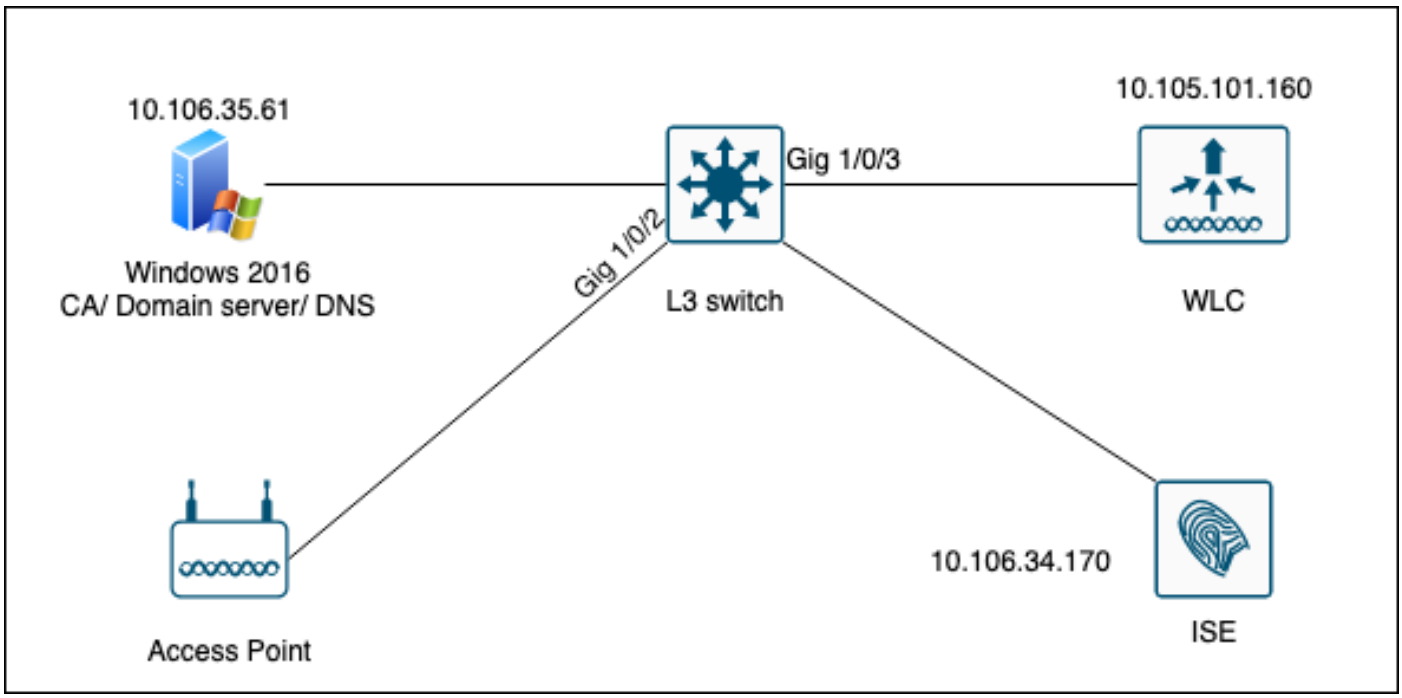
Con LSC, el controlador obtiene un certificado emitido por la CA. Un AP no se comunica directamente con el servidor CA pero el WLC solicita certificados en nombre de los AP que se unen. Los detalles del servidor de la CA deben configurarse en el controlador y deben ser accesibles.

El controlador utiliza el Protocolo simple de inscripción de certificados (SCEP) para reenviar las solicitudes de certificado generadas en los dispositivos a la CA y vuelve a utilizar SCEP para obtener los certificados firmados de la CA.

SCEP es un protocolo de administración de certificados que los clientes PKI y los servidores CA

utilizan para admitir la inscripción y revocación de certificados. Se utiliza ampliamente en Cisco y es compatible con muchos servidores de CA. En SCEP, HTTP se utiliza como protocolo de transporte para los mensajes PKI. El principal objetivo de SCEP es la emisión segura de certificados para los dispositivos de red.

Diagrama de la red



Configurar

Hay dos cosas que configurar principalmente: la CA SCEP y el WLC 9800.

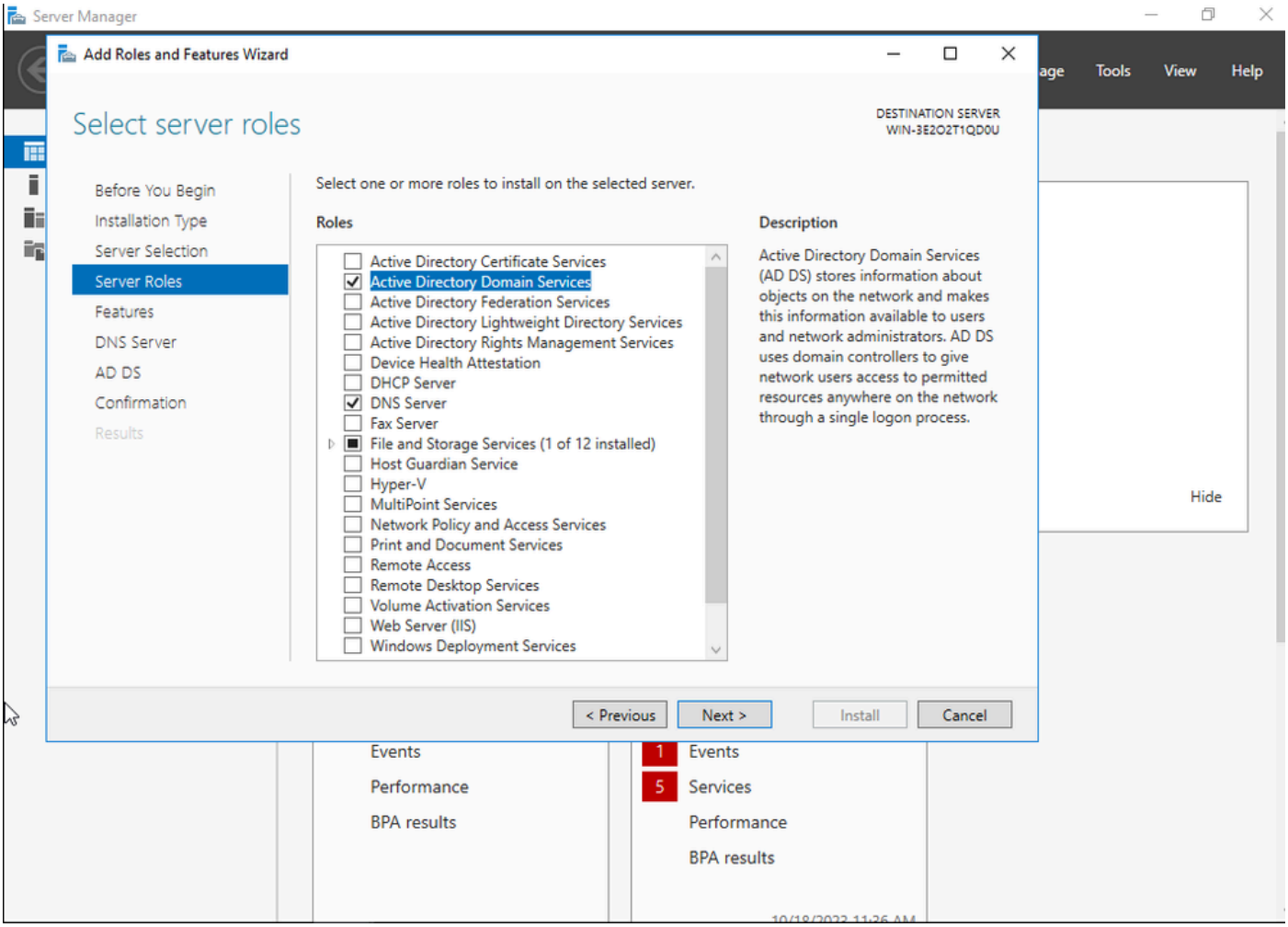
CA SCEP de Windows Server 2016

Este documento cubre una instalación básica de una CA SCEP de Windows Server para fines de laboratorio. Una CA de Windows real de nivel de producción debe configurarse de forma segura y adecuada para las operaciones empresariales. Esta sección está pensada para ayudarle a probarlo en el laboratorio, así como inspirarse en los ajustes requeridos para hacer que esta configuración funcione. Éstos son los pasos:

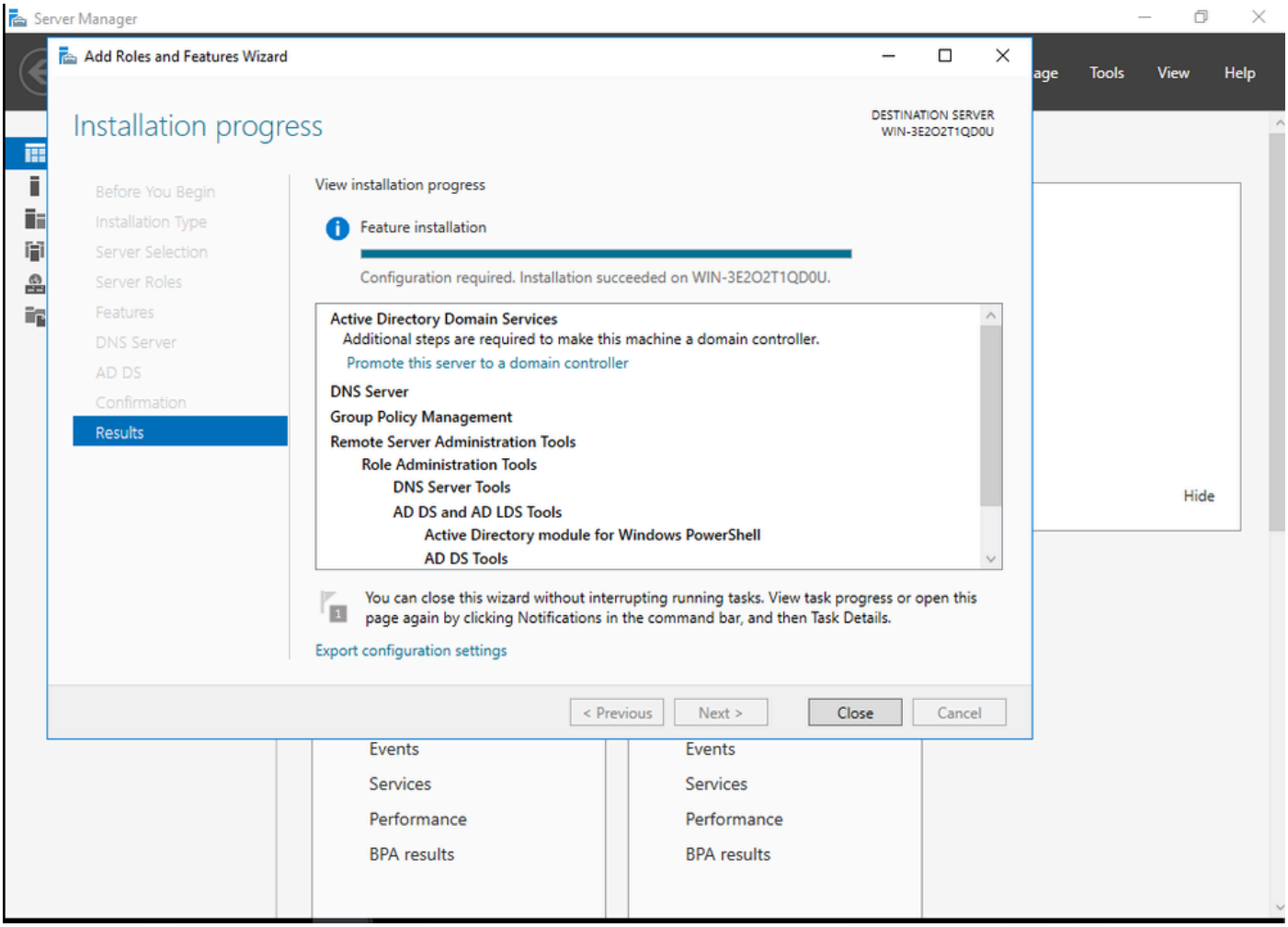
Paso 1.Instalar una experiencia de escritorio de Windows Server 2016 nueva.

Paso 2.Asegúrese de que el servidor está configurado con una dirección IP estática.

Paso 3.Instale un nuevo rol y servicio, comience con los servicios de dominio de Active Directory y el servidor DNS.

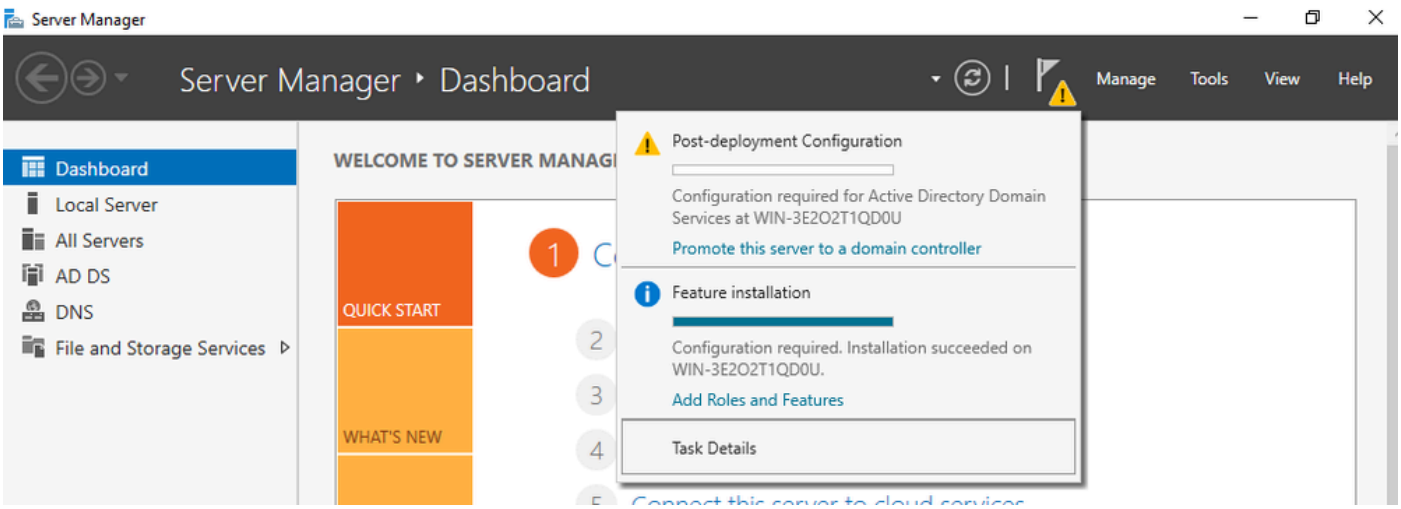


instalación de Active Directory



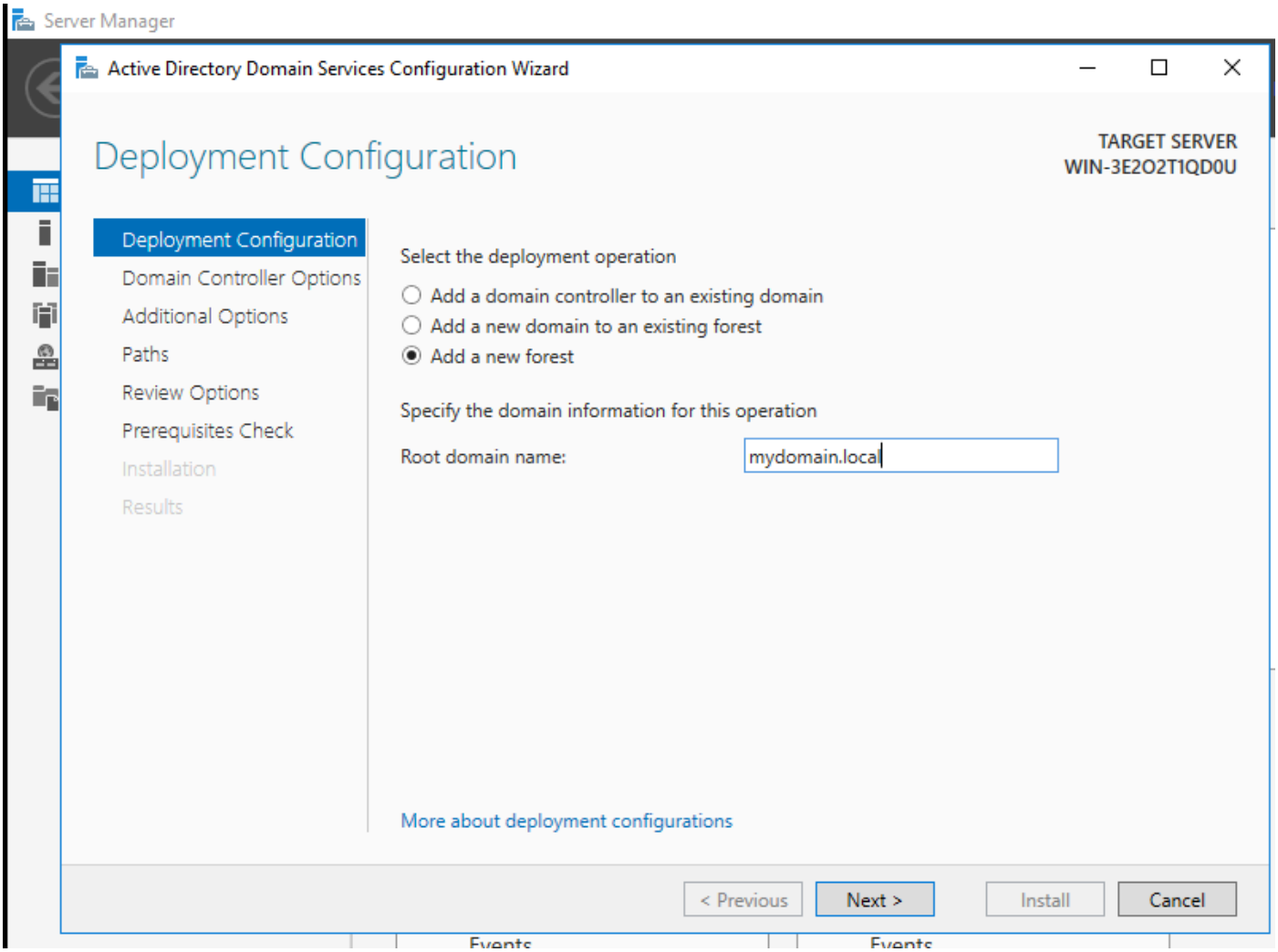
Fin de la instalación de AD

Paso 4.Una vez hecho, haga clic en el panel de Promover este servidor a un controlador de dominio.



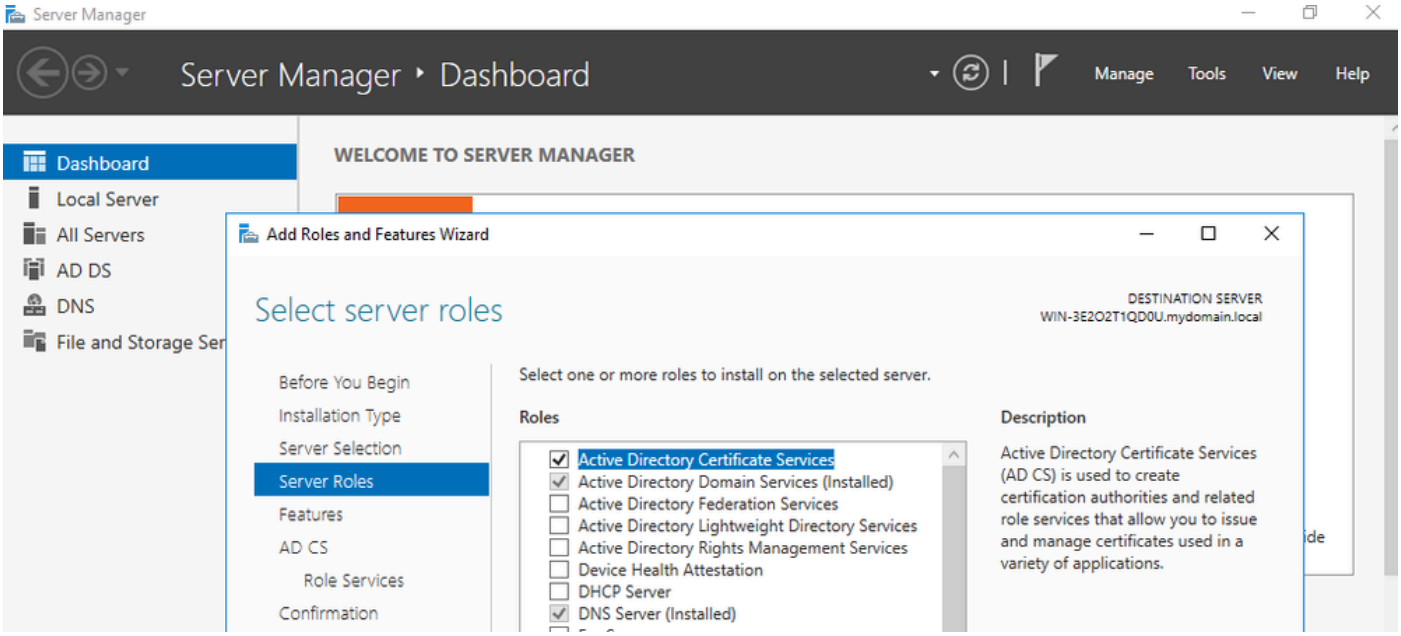
Configurar los servicios de AD

Paso 5.Cree un nuevo bosque y elija un nombre de dominio.

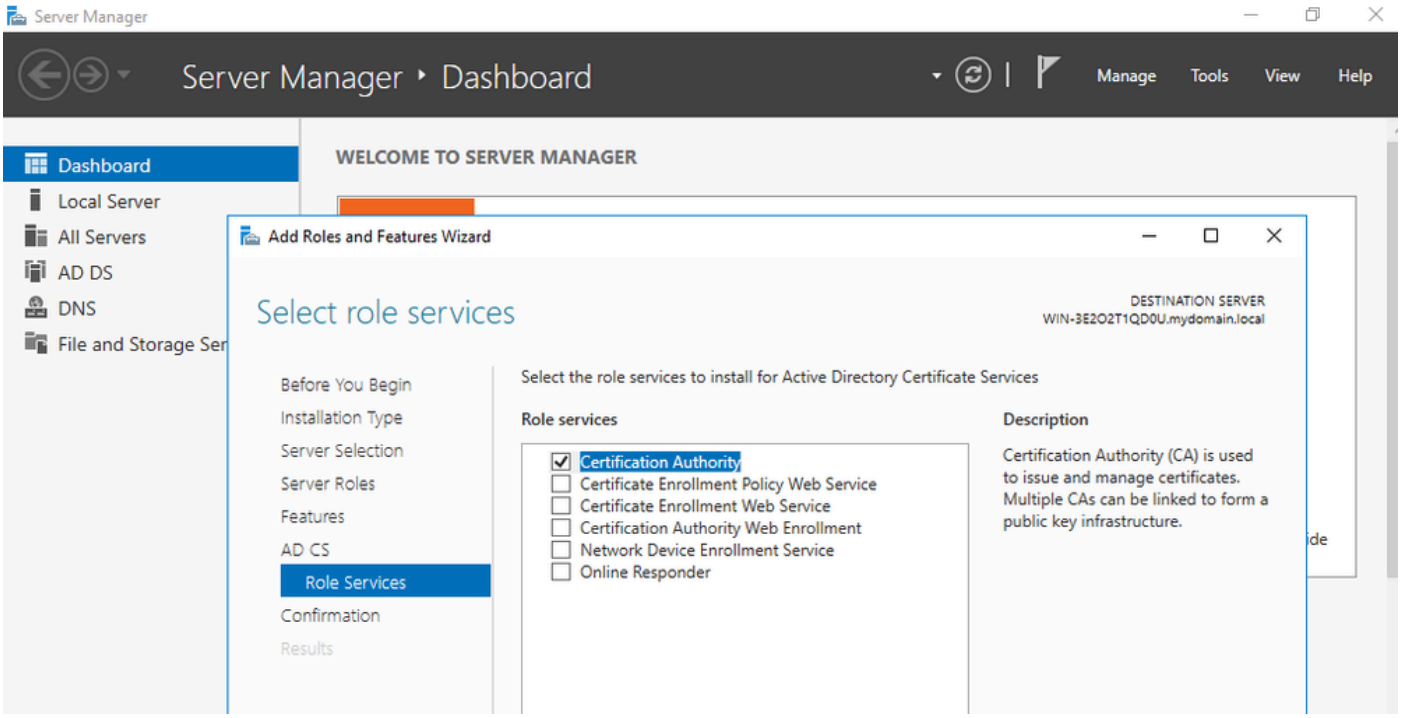


Elija un nombre de bosque

Paso 6.Agregue el rol Servicios de Certificate Server:

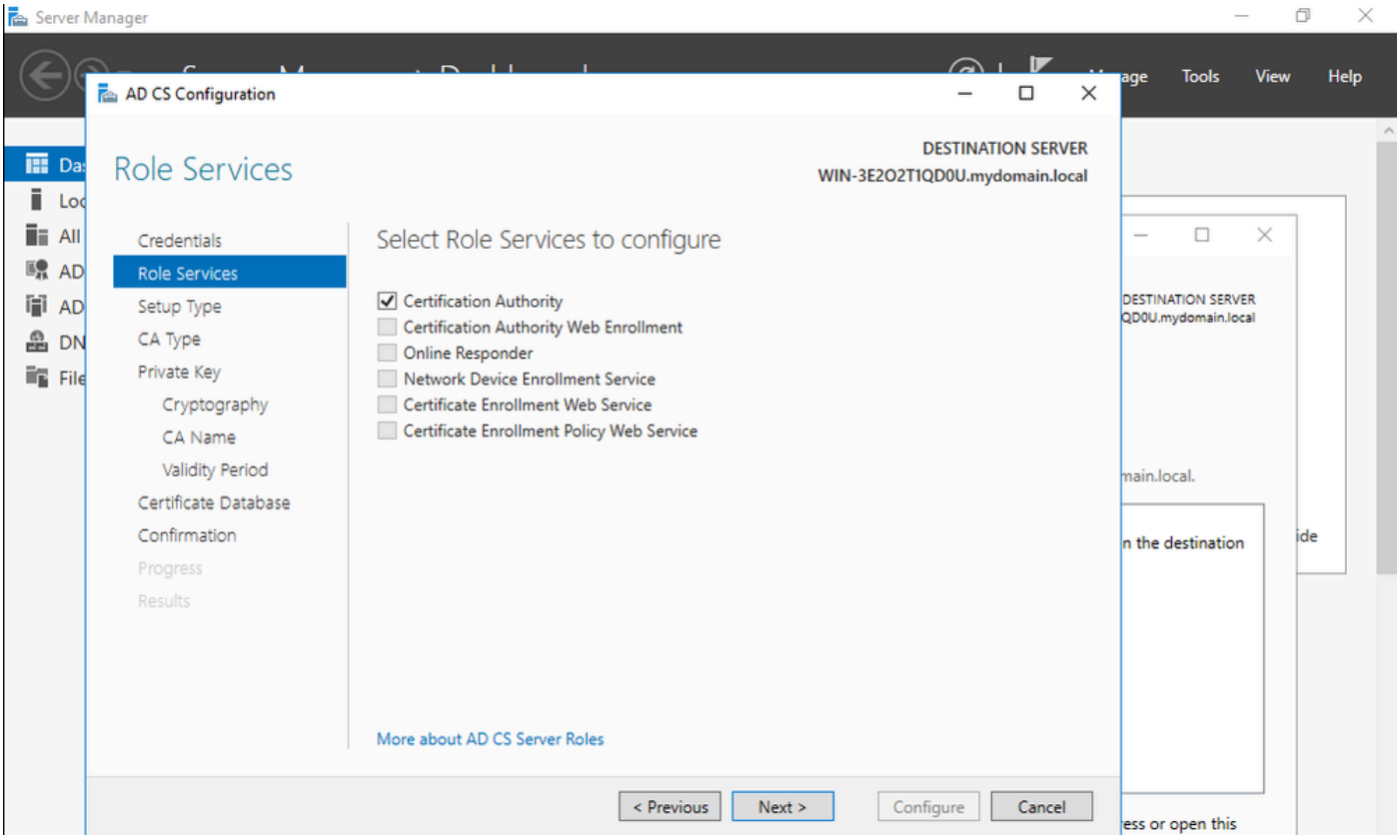


Agregar servicios de certificados

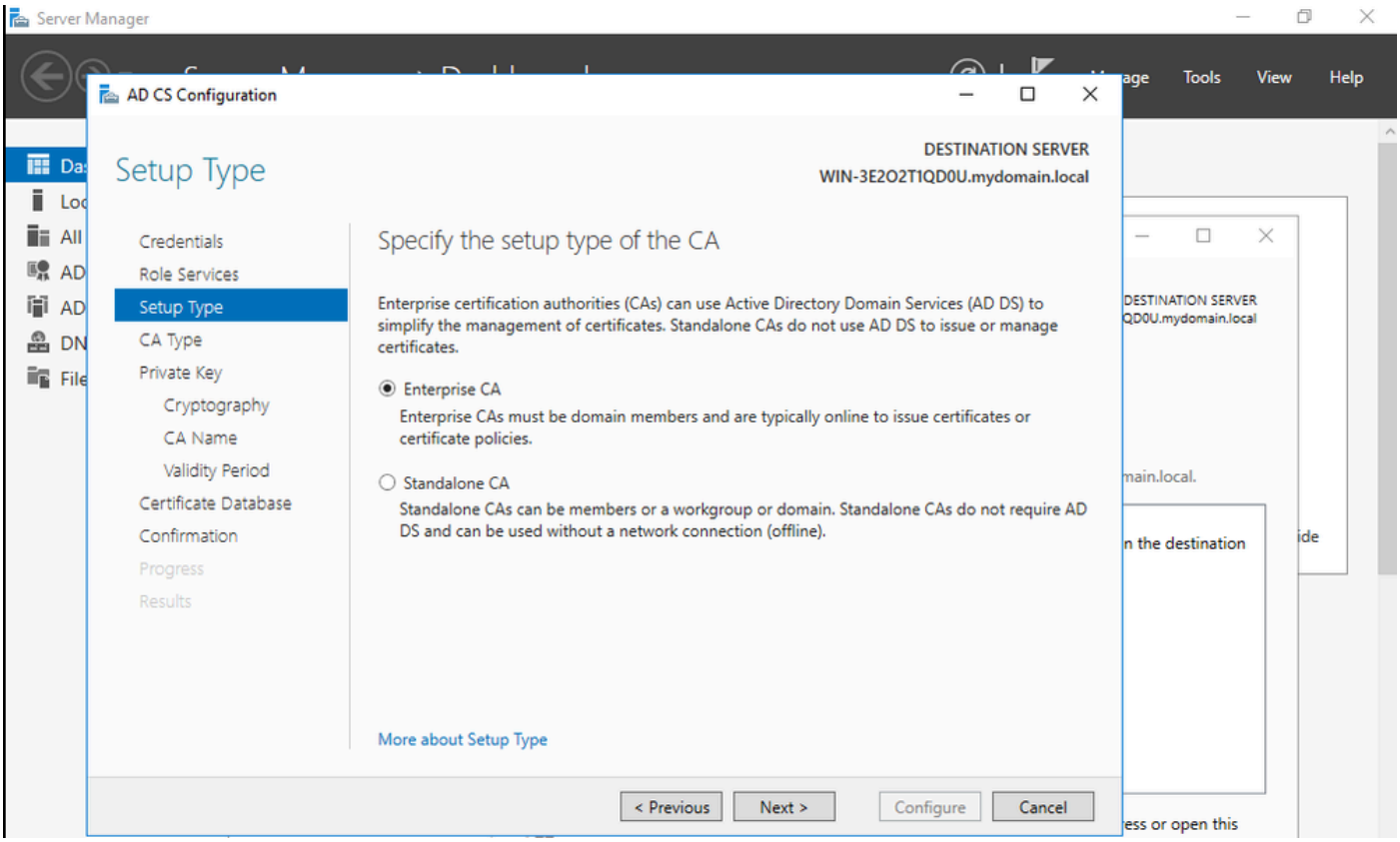


Agregue sólo la entidad emisora de certificados

Paso 7.Una vez hecho esto, configure su entidad emisora de certificados.

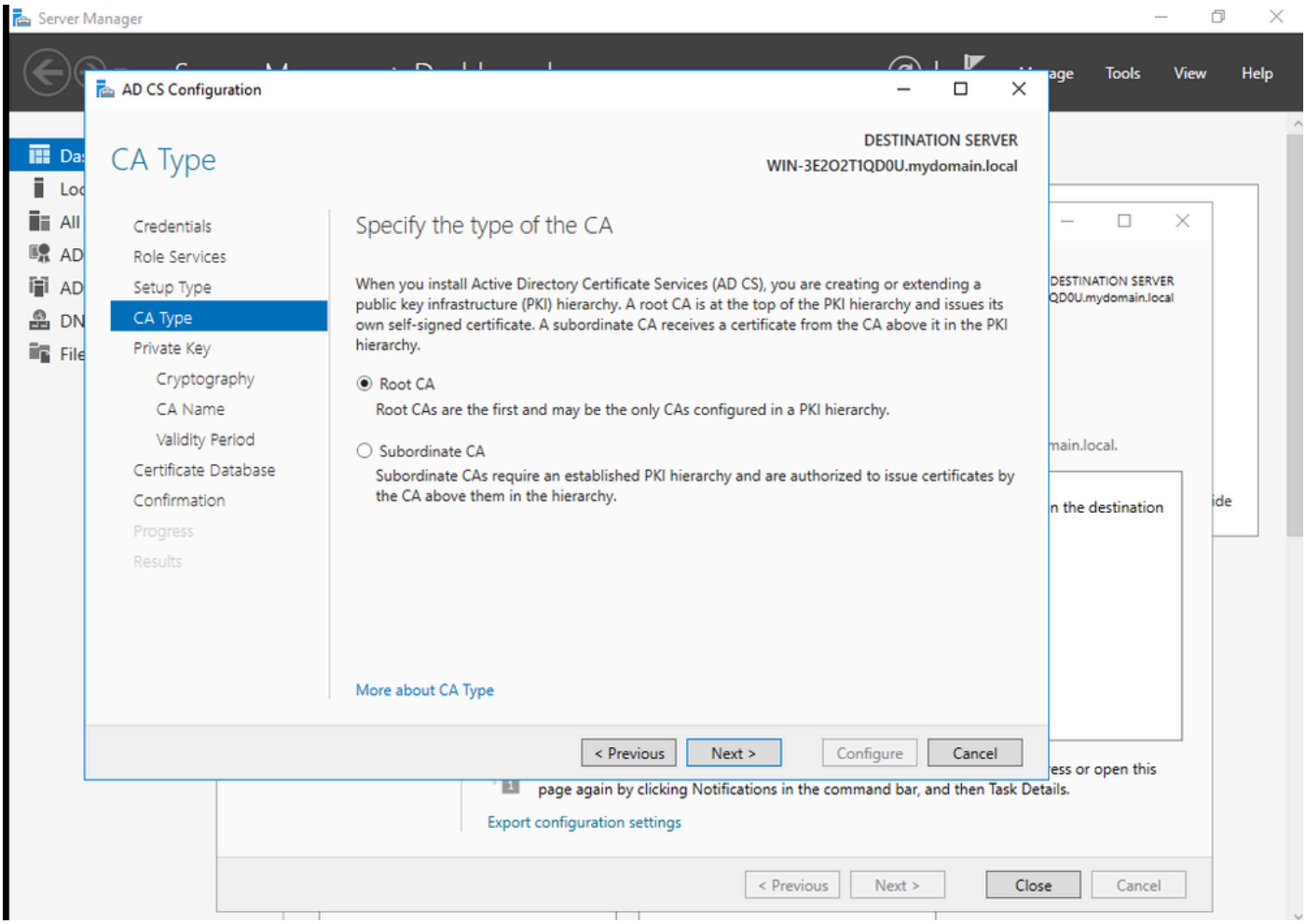


Paso 8.Seleccione Enterprise CA.



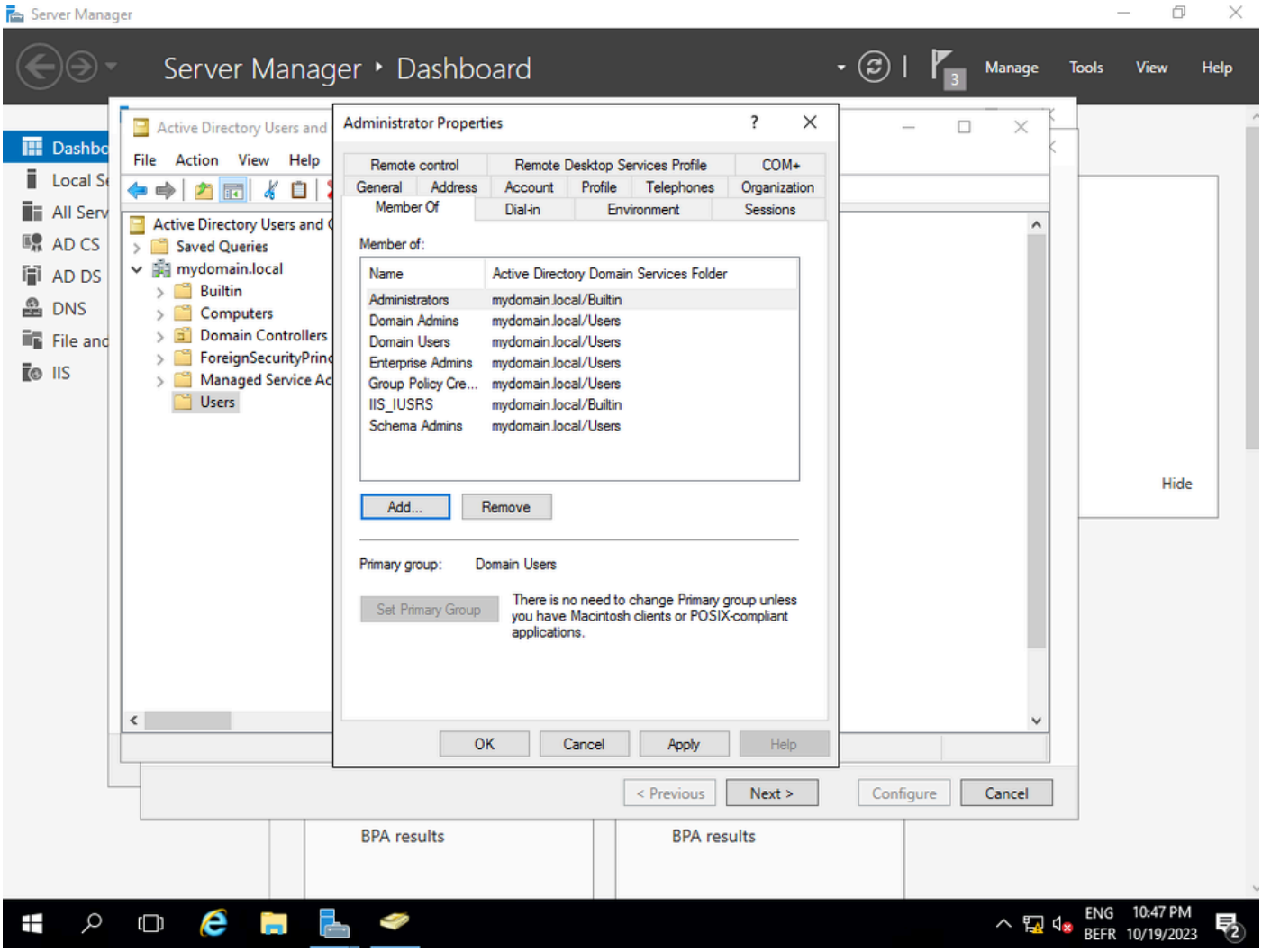
CA empresarial

Paso 9.Conviértalo en una CA raíz. Desde Cisco IOS XE 17.6, las CA subordinadas son compatibles con LSC.



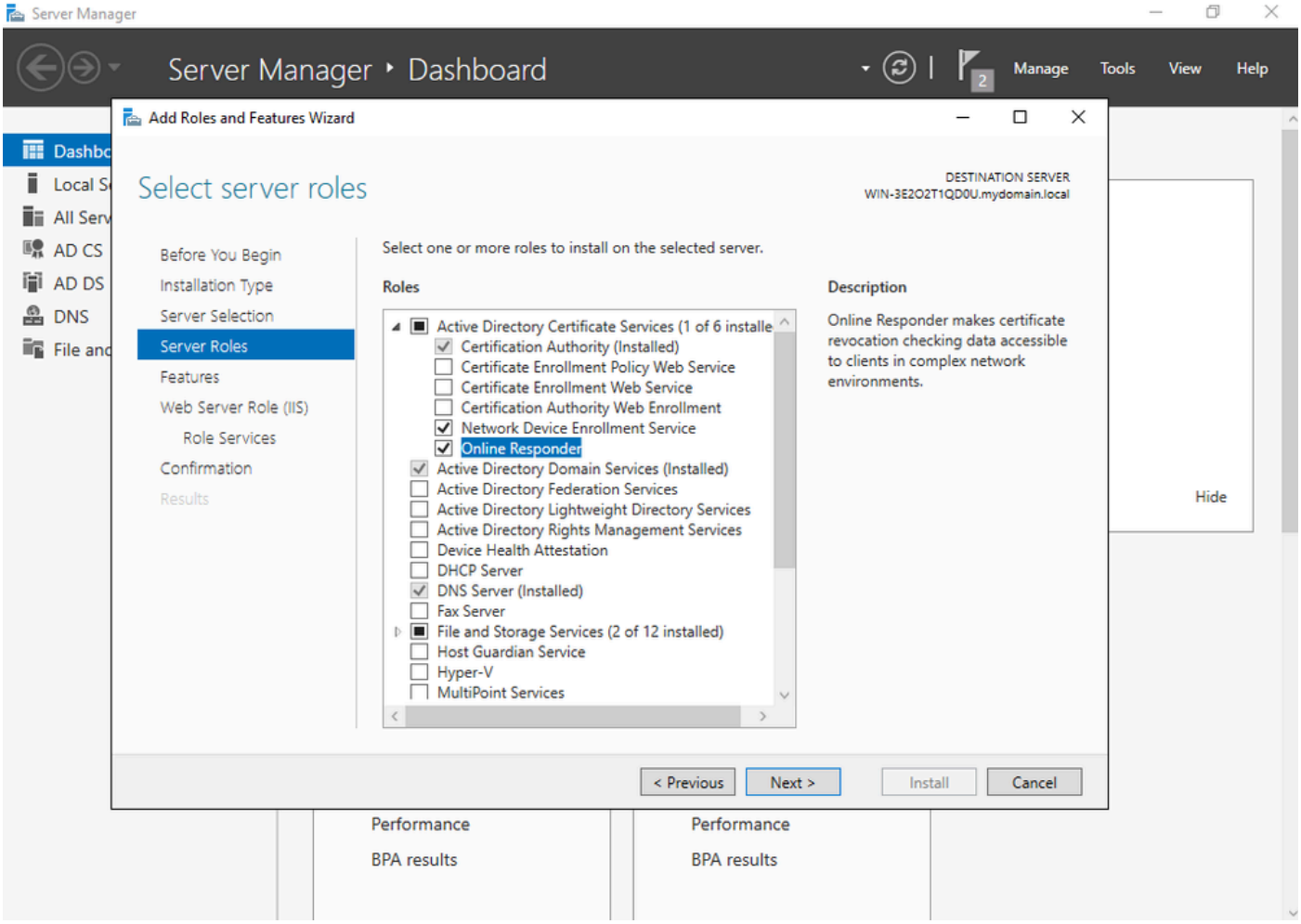
Elija una CA raíz

Es importante tener la cuenta que utiliza para que la CA forme parte del grupo IIS_IUSRS. En este ejemplo, se utiliza la cuenta Administrador y se va al menú Usuarios y equipos de Active Directory para agregar los usuarios Administrador al grupo IIS_IUSRS.



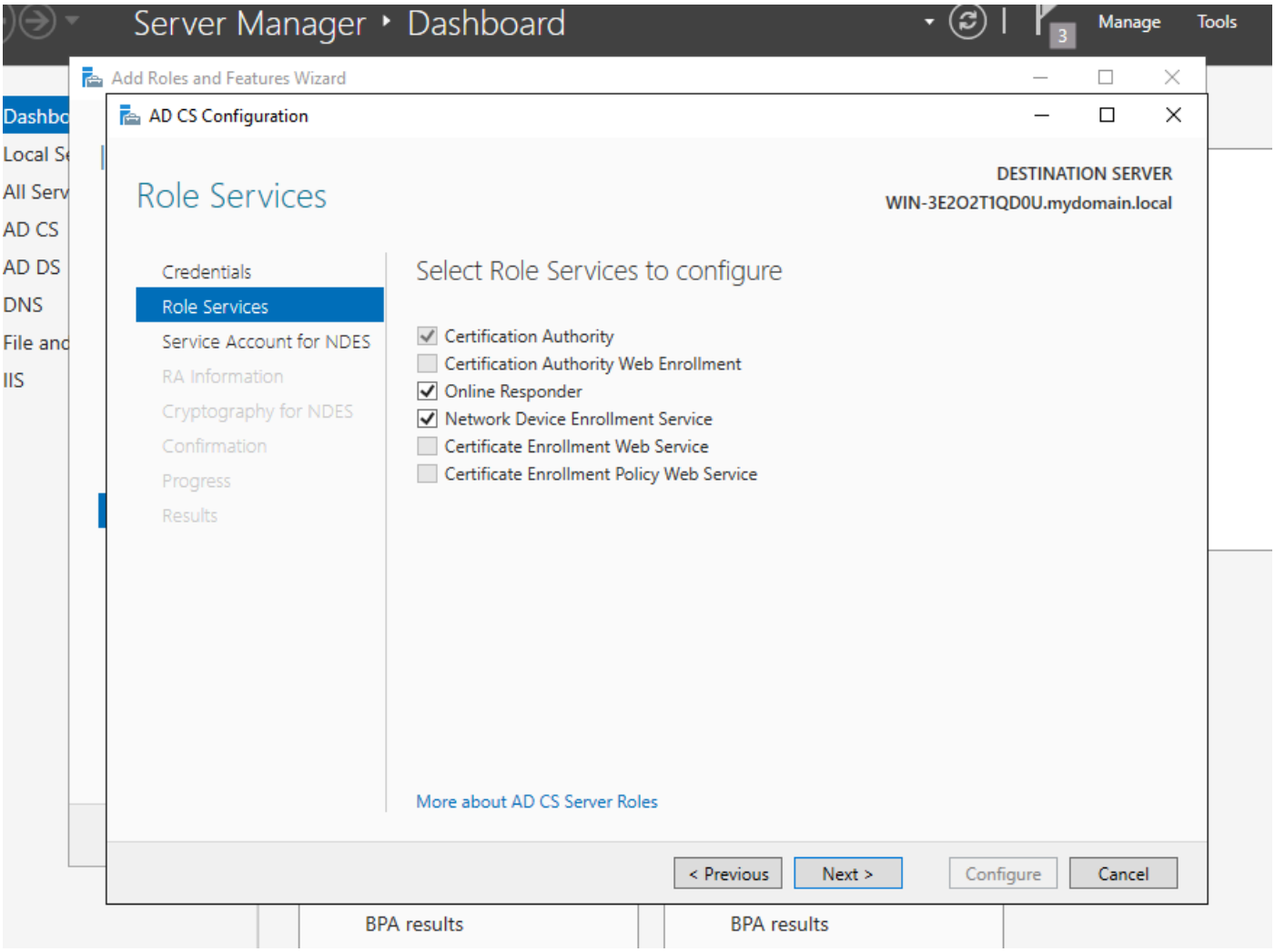
Agregue su cuenta de administrador al grupo IIS_USER

Paso 10.Una vez que tenga un usuario en el grupo de IIS adecuado, agregue funciones y servicios. A continuación, agregue los servicios Respondedor en línea y NDES a la entidad emisora de certificados.



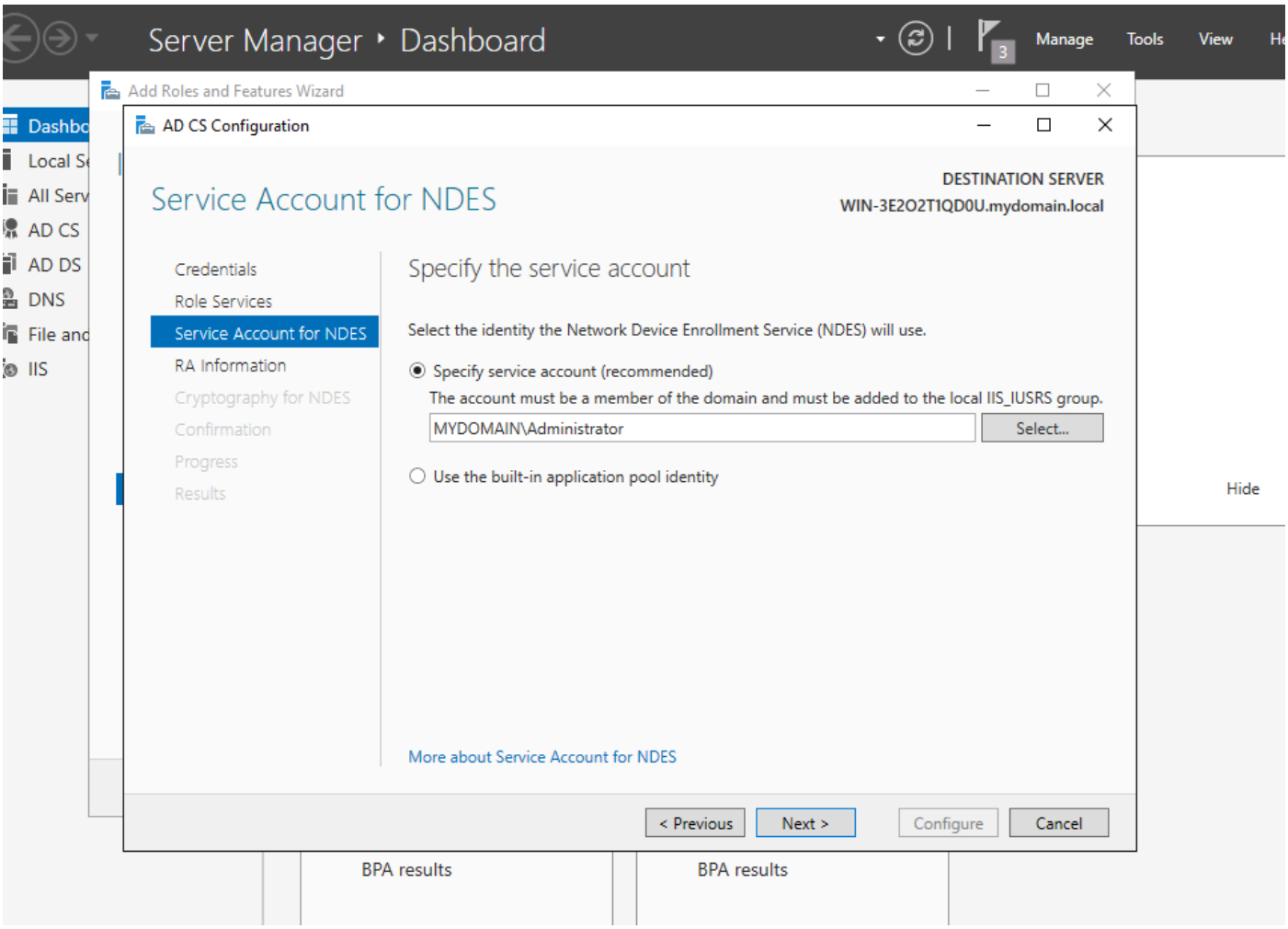
Instalar los servicios NDES y Respondedor en línea

Paso 11.Una vez hecho esto, configure esos servicios.



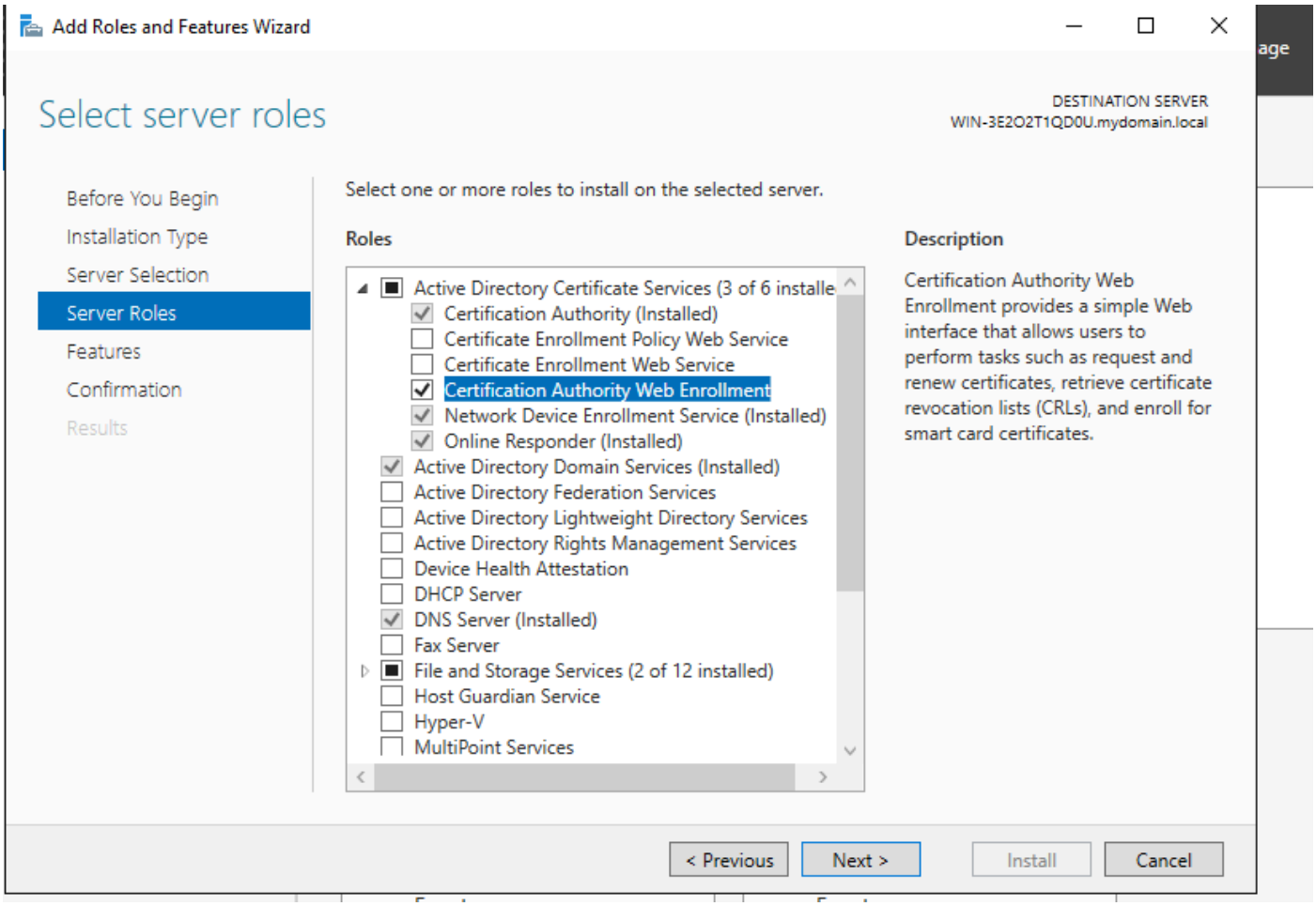
Instalar el Respondedor en línea y el servicio NDES

Paso 12.Se le solicita que elija una cuenta de servicio. Ésta es la cuenta que agregó previamente al grupo IIS_IUSRS.

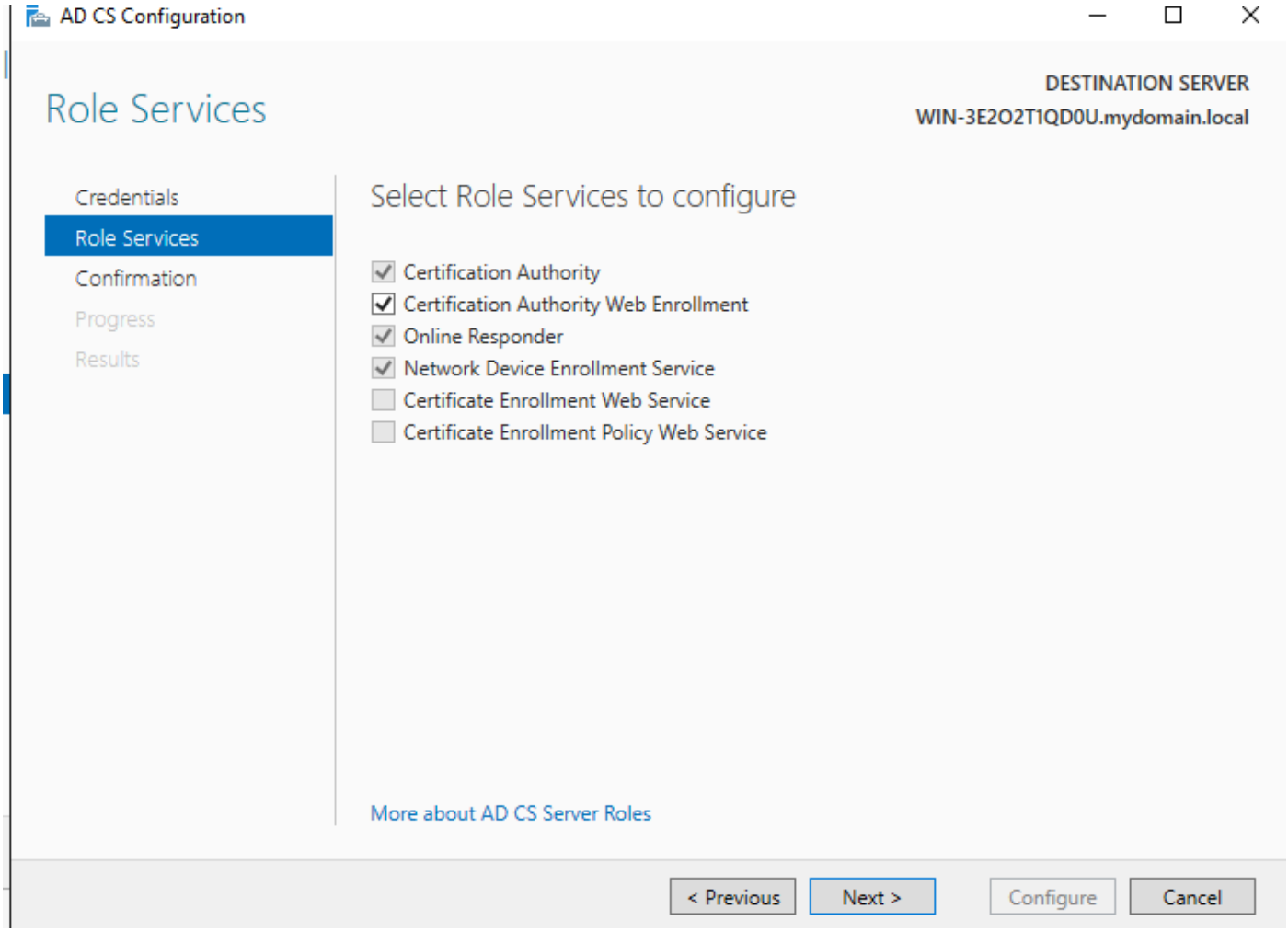


Seleccione el usuario que agregó al grupo IIS

Paso 13. Esto es suficiente para las operaciones SCEP, pero para lograr la autenticación 802.1X, también necesita instalar un certificado en el servidor RADIUS. Por lo tanto, para mayor facilidad, instale y configure el servicio de inscripción web para poder copiar y pegar fácilmente la solicitud de certificado de ISE en nuestro servidor Windows.

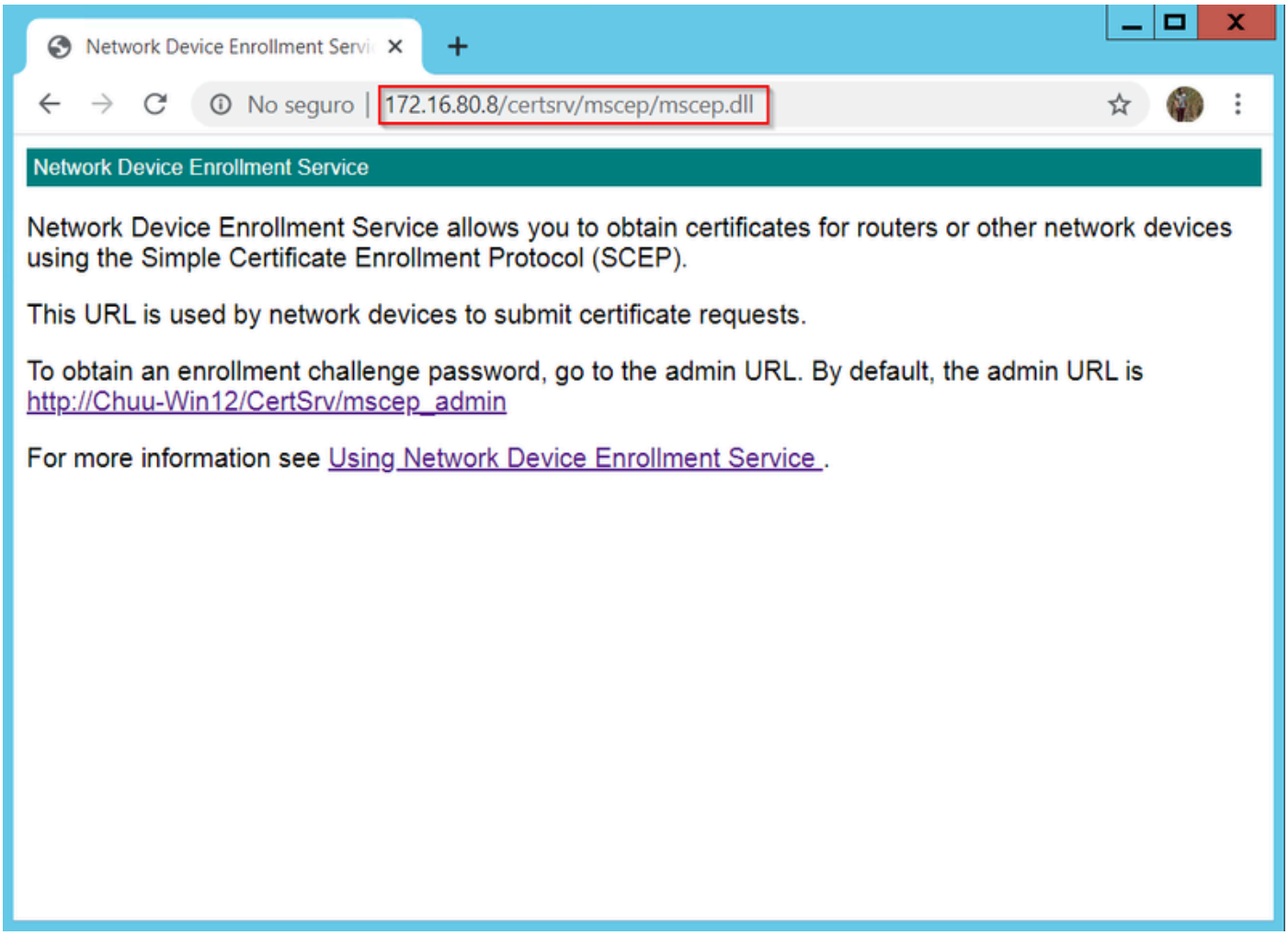


Instalar el servicio de inscripción en la Web



configurar el servicio de inscripción web

Paso 14. Puede verificar que el servicio SCEP funciona correctamente visitando http://<serverip>/certsrv/mscep/mscep.dll:



Verificación del portal SCEP

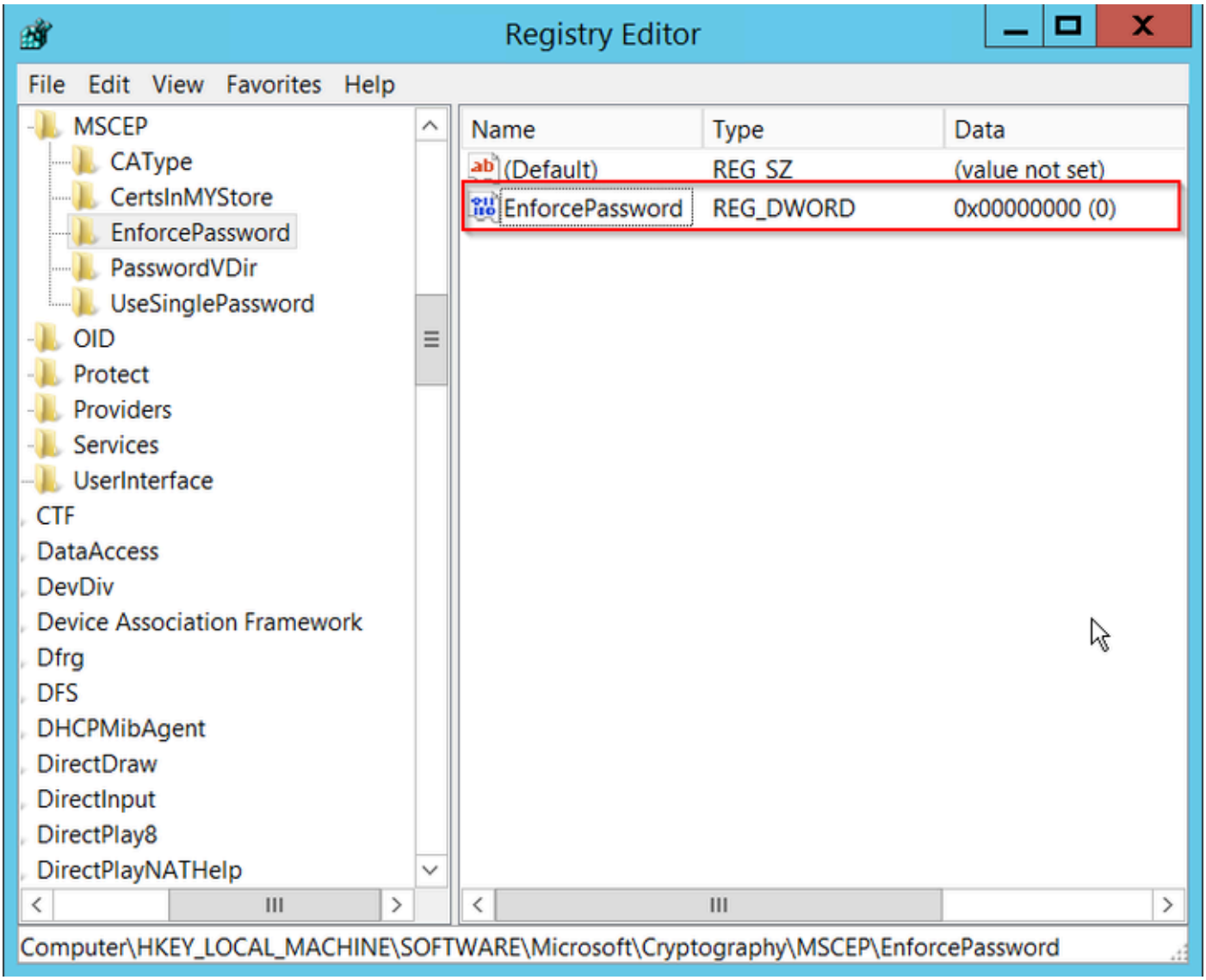
Paso 15.

De forma predeterminada, Windows Server utilizó una contraseña de desafío dinámico para autenticar las solicitudes de cliente y de extremo antes de la inscripción en Microsoft SCEP (MSCEP). Esto requiere una cuenta de administrador para navegar a la GUI web y generar una contraseña a pedido para cada solicitud (la contraseña debe incluirse en la solicitud). El controlador no puede incluir esta contraseña en las solicitudes que envía al servidor. Para quitar esta característica, es necesario modificar la clave del Registro en el servidor NDES:

Abra el Editor del Registro y busque Regedit en el menú Inicio.

Vaya a Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword

Cambie el valor de EnforcePassword a 0. Si ya es 0, déjelo tal cual.



Establecer el valor de EnforcePassword

Configurar la plantilla de certificado y el Registro

Los certificados y sus claves asociadas se pueden utilizar en varios escenarios para diferentes propósitos definidos por las directivas de la aplicación dentro del servidor de la CA. La directiva de aplicación se almacena en el campo Uso extendido de claves (EKU) del certificado. El autenticador analiza este campo para comprobar que el cliente lo utiliza para el fin previsto. Para asegurarse de que la política de aplicación adecuada esté integrada en los certificados WLC y AP, cree la plantilla de certificado adecuada y asígnela al registro NDES:

Paso 1. Vaya a Inicio > Herramientas administrativas > Entidad emisora de certificados.

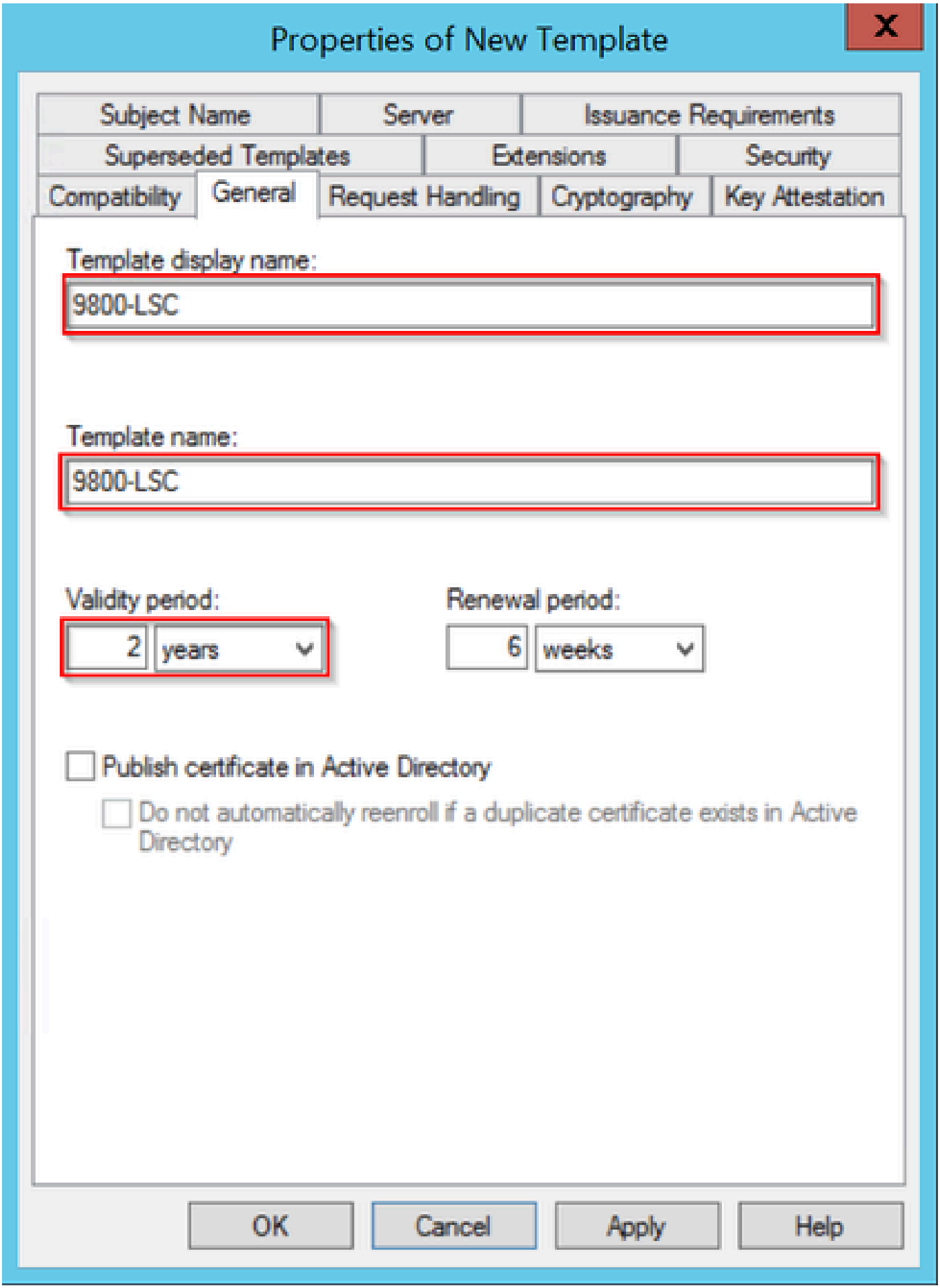
Paso 2. Expanda el árbol de carpetas Servidor de la CA, haga clic con el botón derecho en las carpetas Plantillas de certificado y seleccione Administrar.

Paso 3. Haga clic con el botón derecho en la plantilla de certificado Users y, a continuación, seleccione Duplicate Template en el menú contextual.

Paso 4. Vaya a la pestaña General, cambie el nombre de la plantilla y el período de validez según

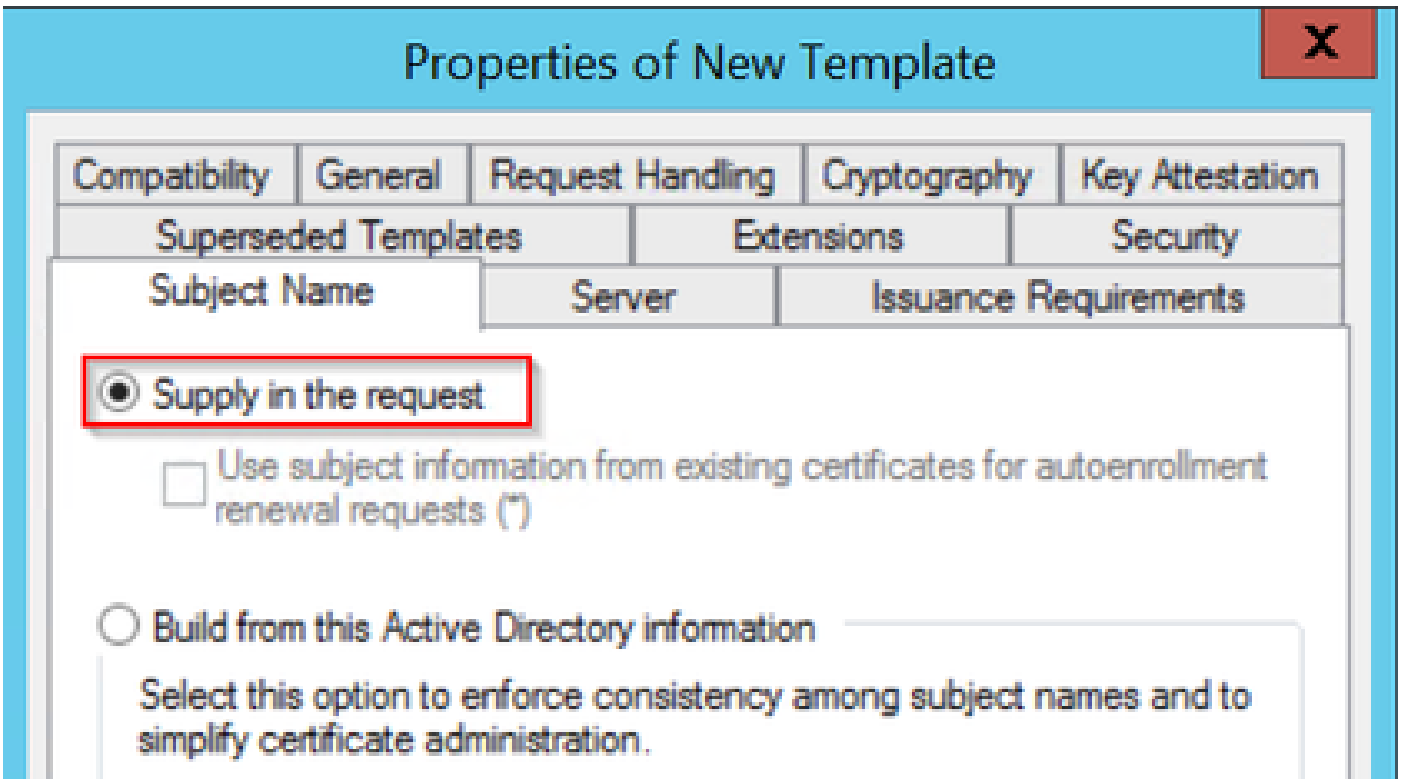
desee y deje todas las demás opciones sin marcar.

⚠ Precaución: cuando se modifique el período de validez, asegúrese de que no sea mayor que la validez del certificado raíz de la entidad emisora de certificados.



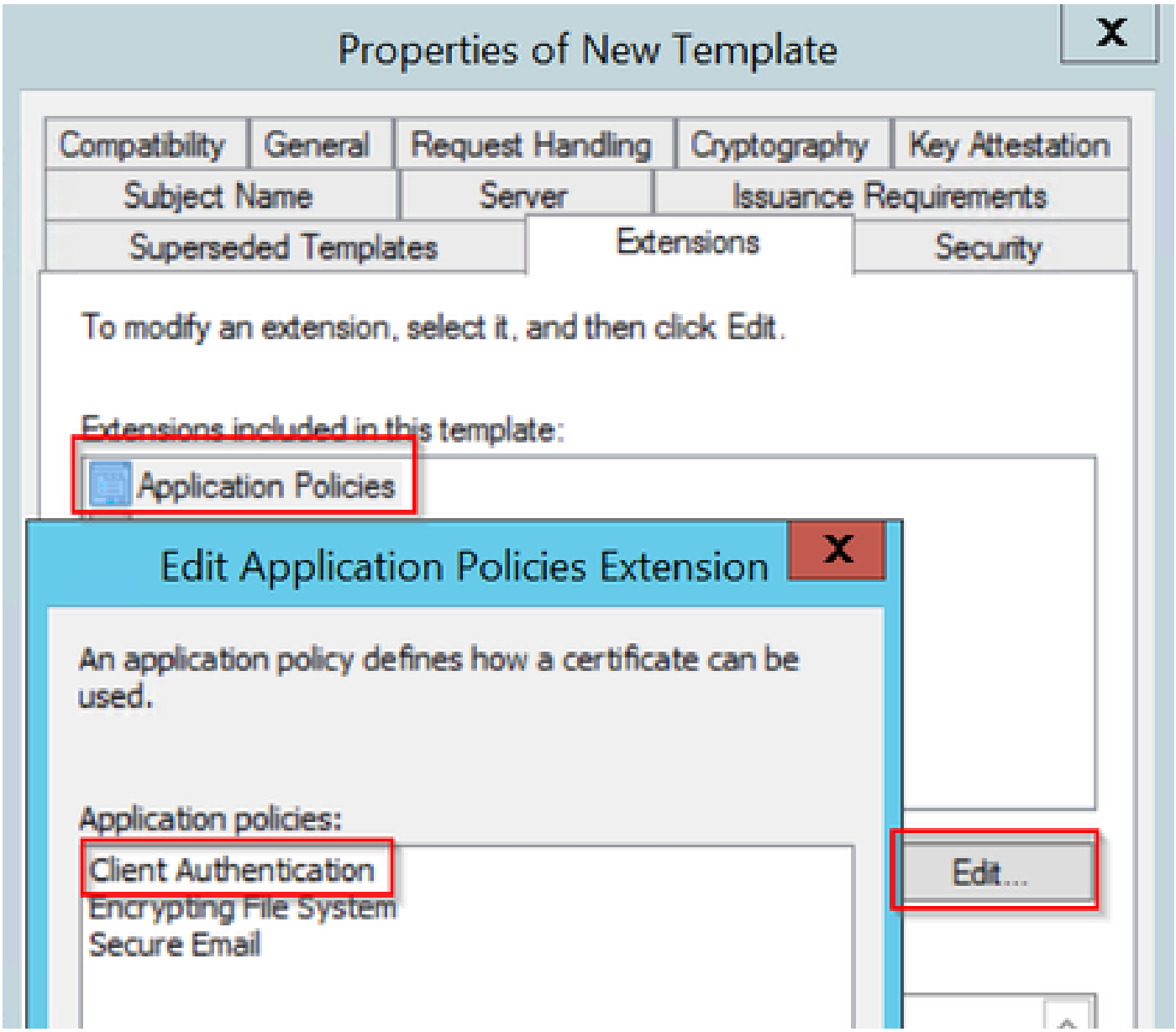
Configuración de la plantilla de certificado

Paso 5. Vaya a la pestaña Nombre del Asunto, asegúrese de que Aprovisionar en la solicitud está seleccionado. Aparecerá una ventana emergente para indicar que los usuarios no necesitan la aprobación del administrador para firmar su certificado. Seleccione Aceptar.



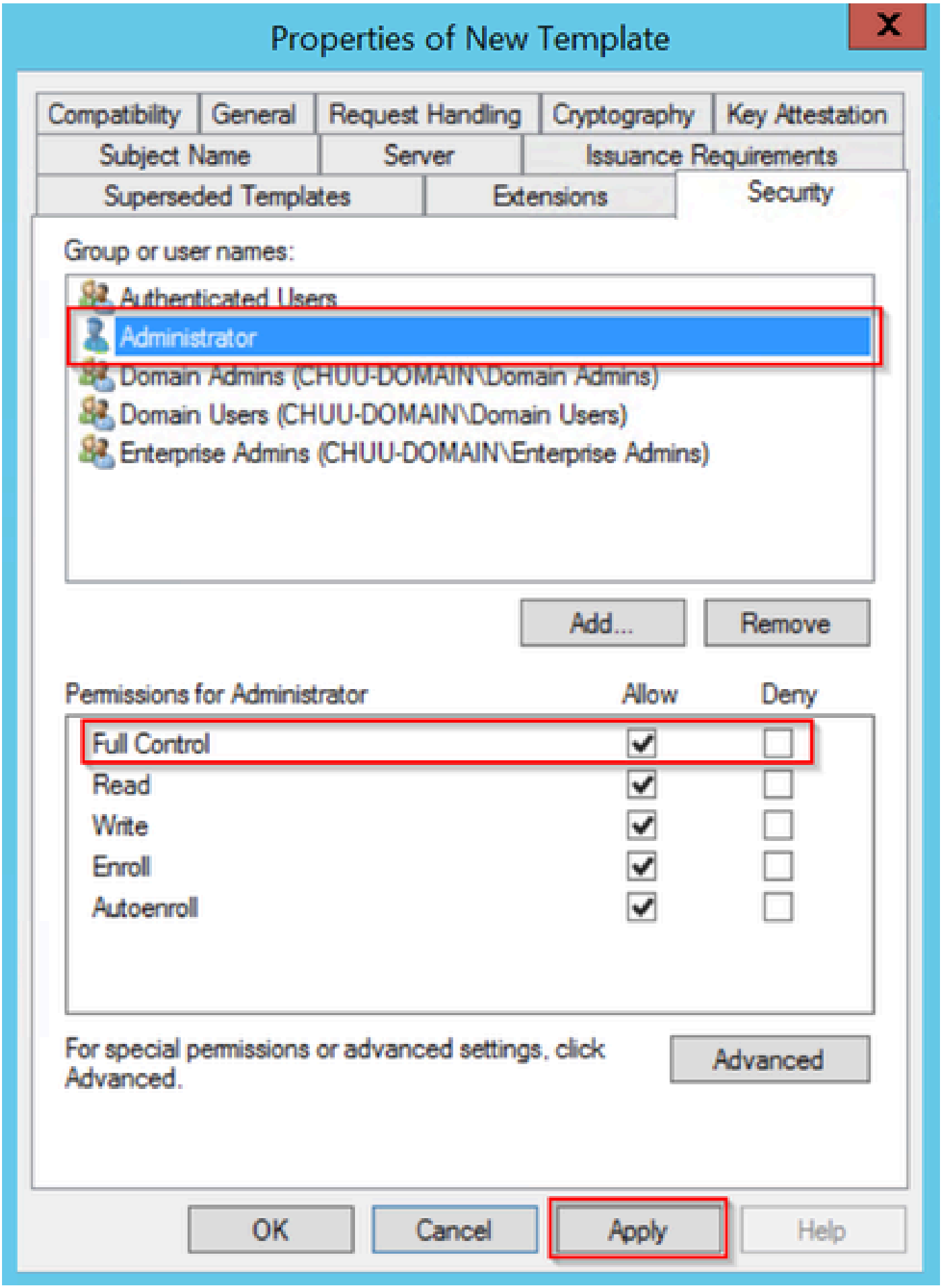
Aprovisionamiento en la solicitud

Paso 6. Vaya a la pestaña Extensions, seleccione la opción Application Policies y seleccione el botón Edit.... Asegúrese de que Client Authentication esté en la ventana Application Policies; de lo contrario, seleccione Add y agréguelo.



Verificar extensiones

Paso 7. Vaya a la ficha Seguridad, asegúrese de que la cuenta de servicio definida en el paso 6 de Habilitar servicios SCEP en el servidor de Windows tiene los permisos de Control total de la plantilla y, a continuación, seleccione Aplicar y Aceptar.

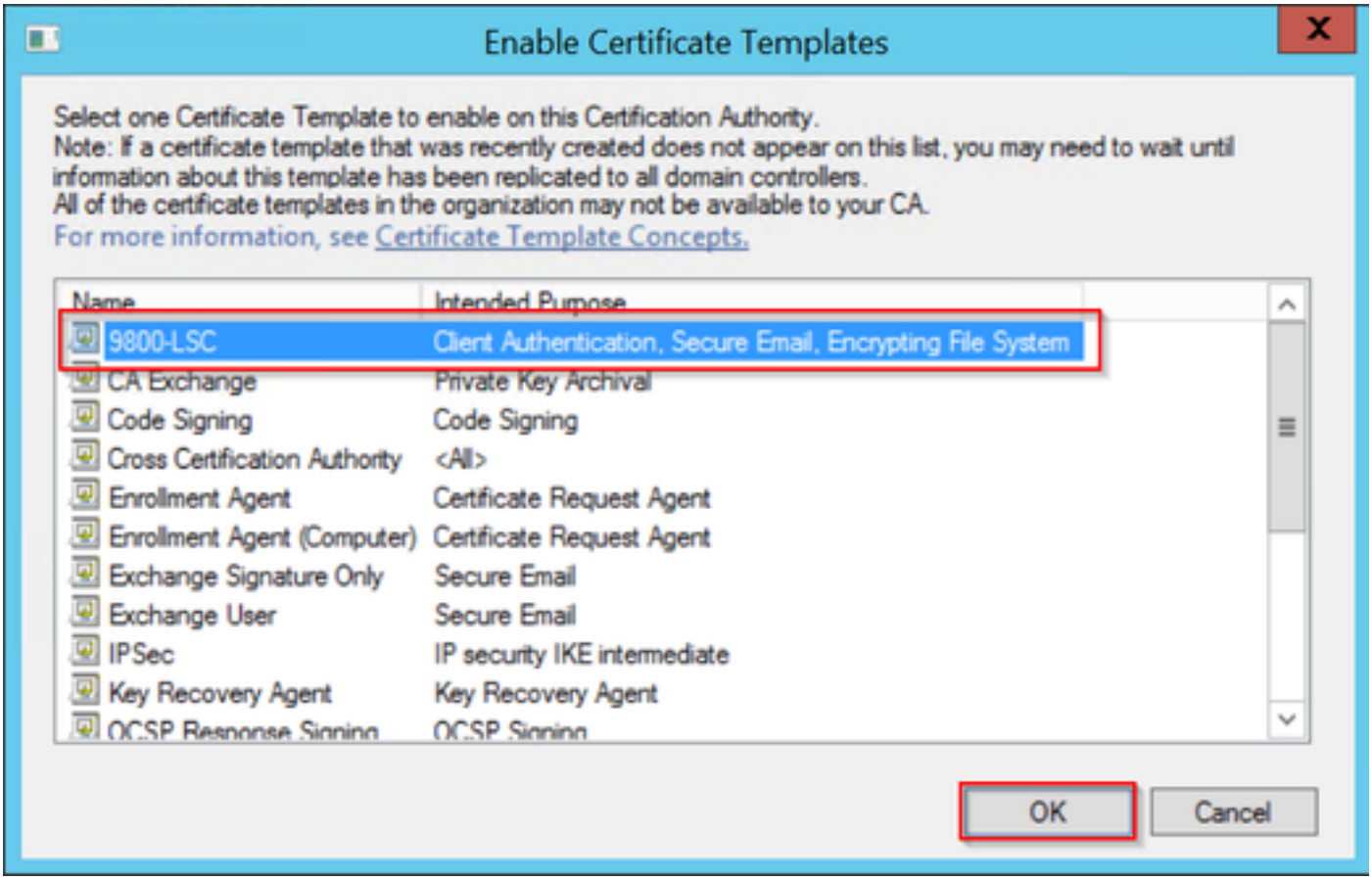


Proporcionar control total

Paso 8. Vuelva a la ventana Entidad de certificación, haga clic con el botón derecho en la carpeta Plantillas de certificado y seleccione Nuevo > Plantilla de certificado para emitir.

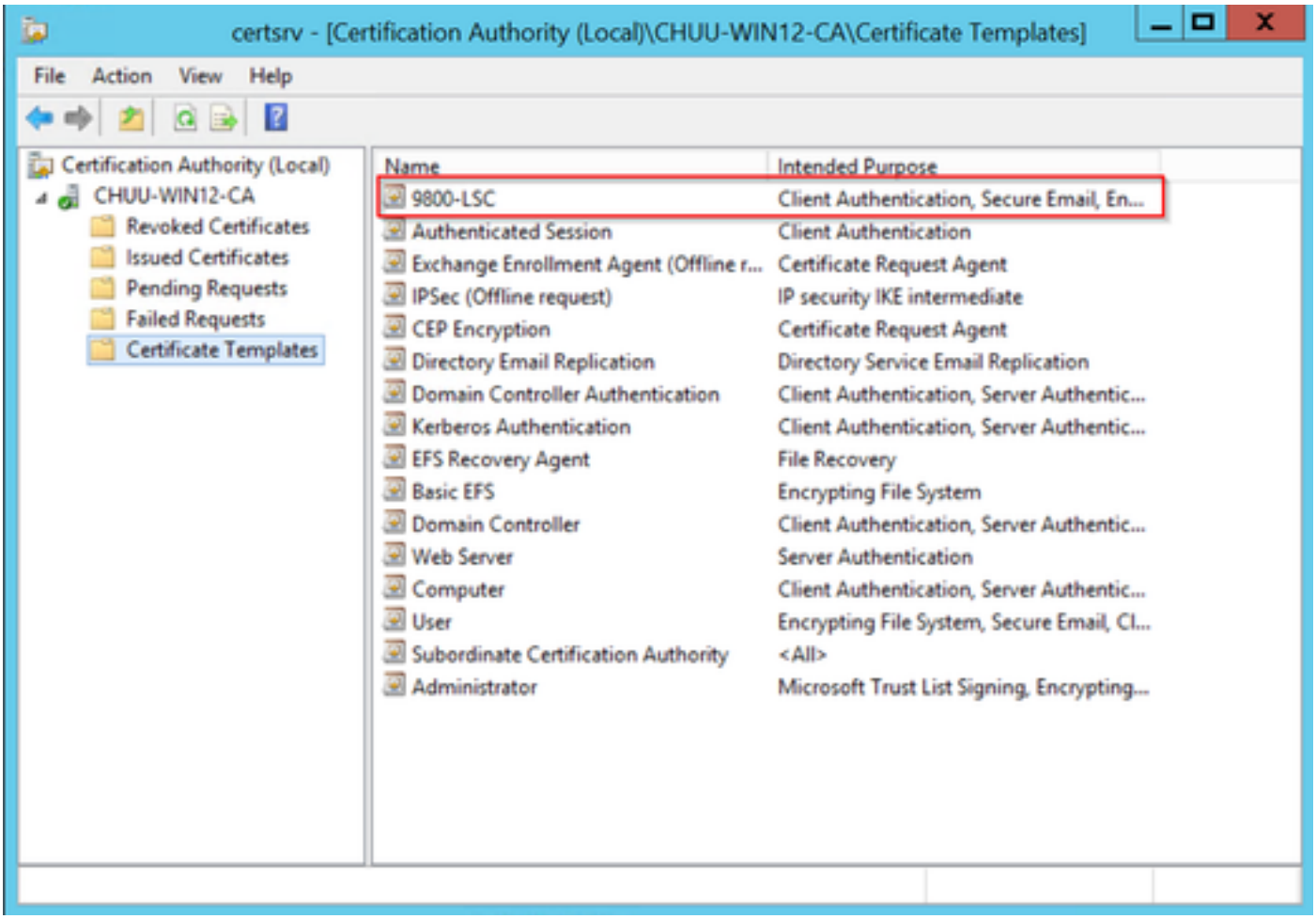
Paso 9. Seleccione la plantilla de certificado creada anteriormente, en este ejemplo es 9800-LSC, y seleccione Aceptar.

Nota: la plantilla de certificado recién creada puede tardar más en aparecer en varias implementaciones de servidores, ya que debe replicarse en todos los servidores.



Elija la plantilla

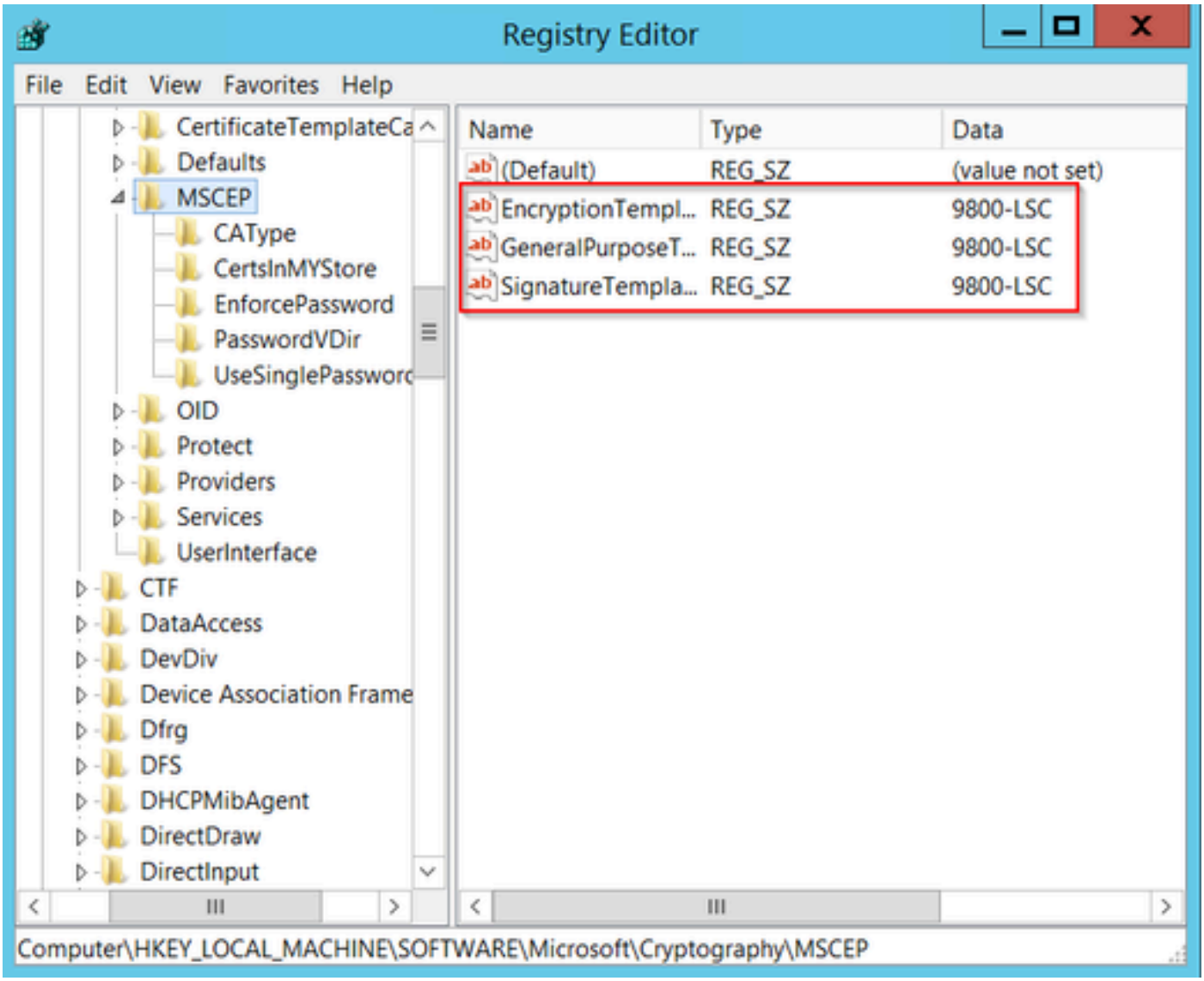
La nueva plantilla de certificado aparece ahora en el contenido de la carpeta Plantillas de certificado.



Seleccione el LSC

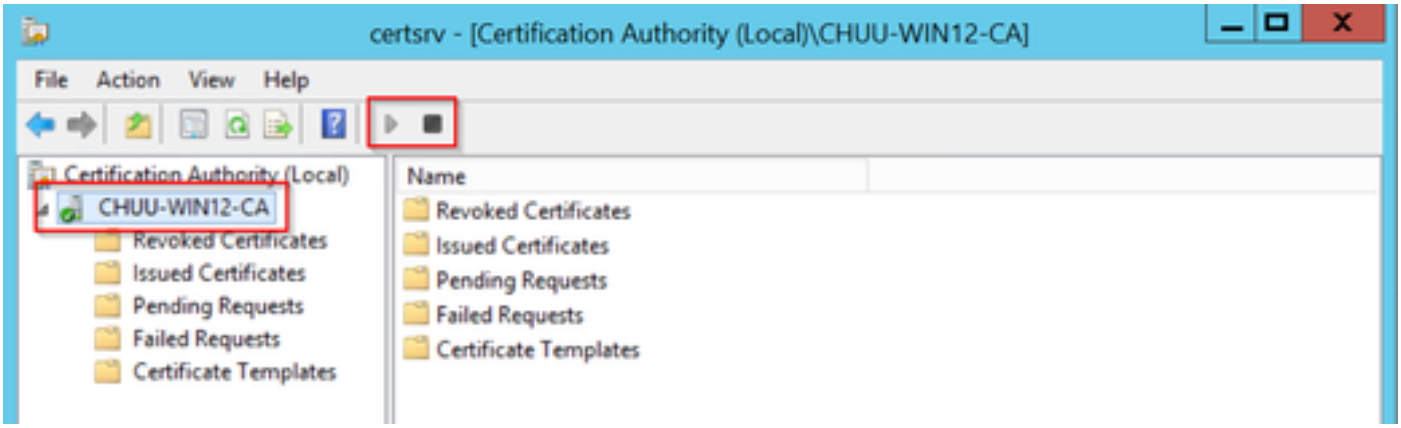
Paso 10. Vuelva a la ventana Registry Editor y navegue hasta Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP.

Paso 11. Edite los registros EncryptionTemplate, GeneralPurposeTemplate y SignatureTemplate para que señalen a la plantilla de certificado recién creada.



Cambiar la plantilla en el Registro

Paso 12. Reinicie el servidor NDES, de modo que vuelva a la ventana Certification Authority, seleccione el nombre del servidor y seleccione el botón Stop y Play sucesivamente.



Configuración de LSC en el 9800

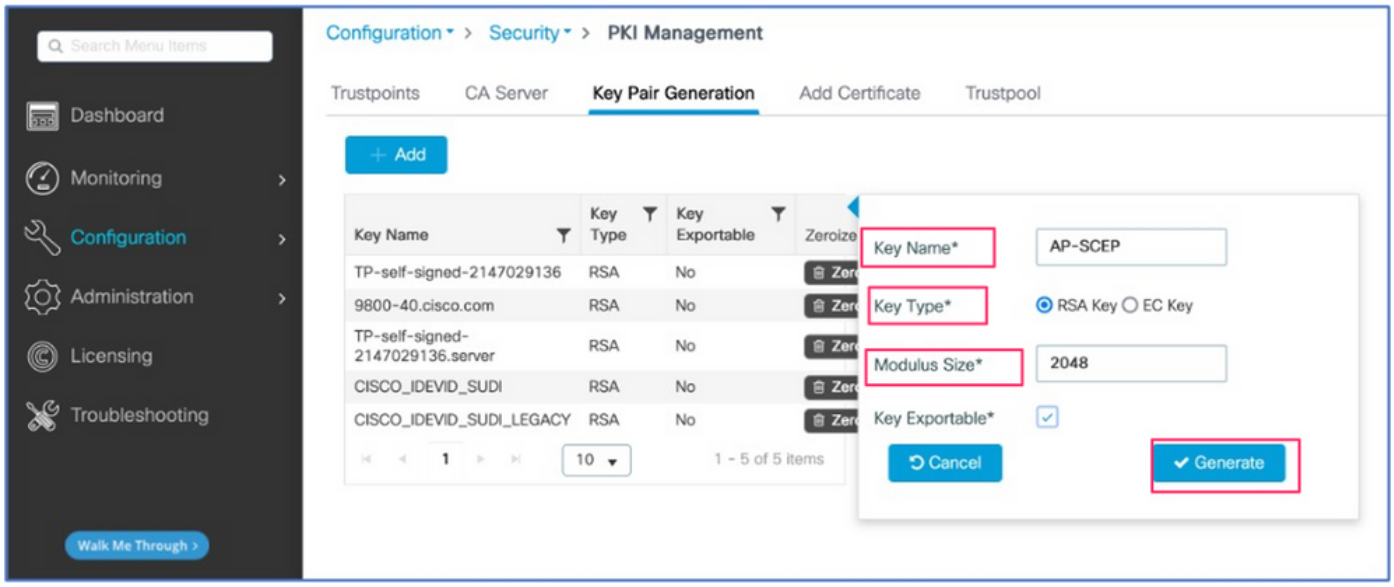
Estos son los pasos en secuencia para configurar LSC para AP en WLC.

1. Crear clave RSA. Esta clave se utiliza más adelante para el punto de confianza PKI.
2. Cree un punto de confianza y asigne la clave RSA creada.
3. Habilite el aprovisionamiento de LSC para los AP y asigne el punto de confianza.
    1. Habilite LSC para todos los AP unidos.
    2. Habilite el LSC para los AP seleccionados a través de la lista de aprovisionamiento.
4. Cambie el punto de confianza de administración inalámbrica y señale al punto de confianza LSC.

Pasos de Configuración de GUI de AP LSC

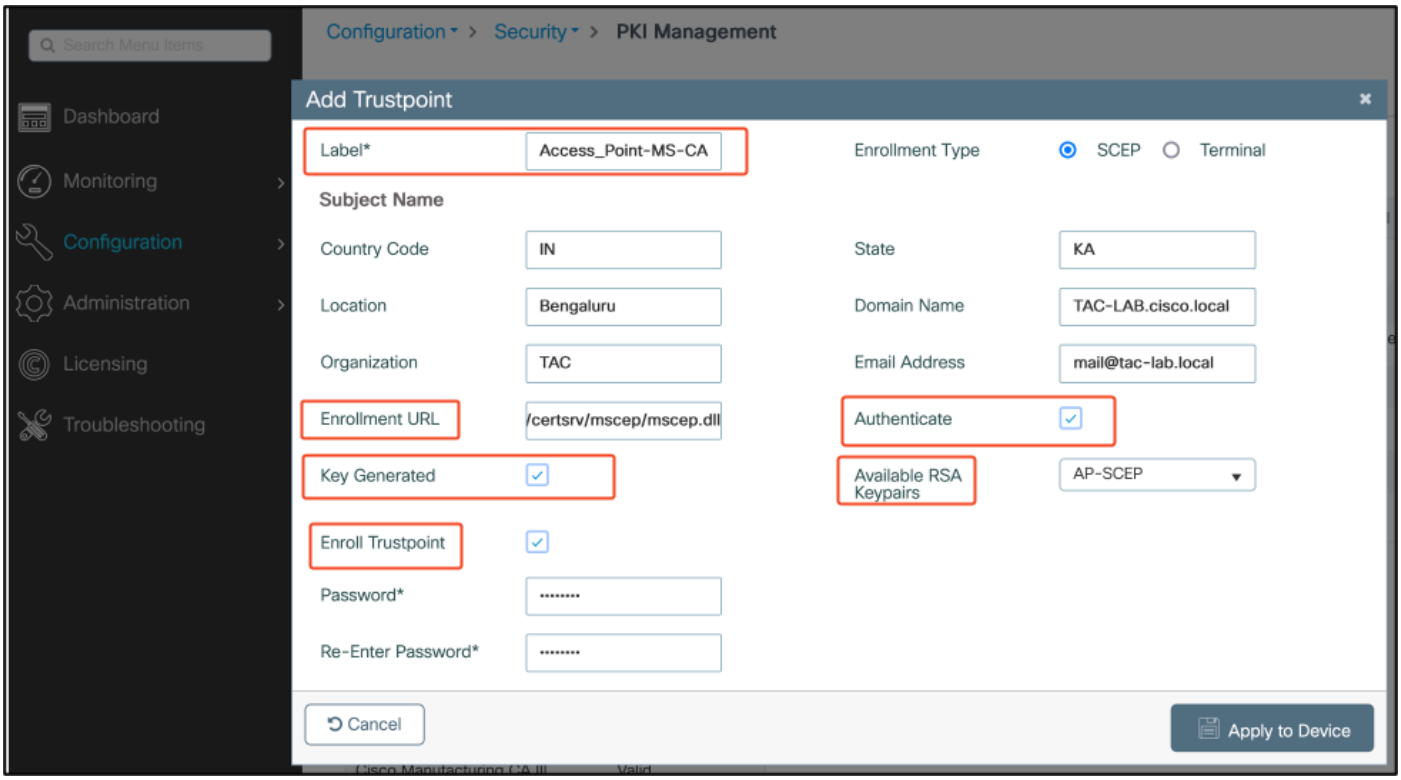
Paso 1.Vaya a Configuration > Security > PKI Management > Key Pair Generation .

1. Haga clic en Agregar y asígnele un nombre relevante.
2. Agregue el tamaño de la clave RSA.
3. La opción de clave exportable es opcional. Esto sólo es necesario si desea exportar la clave fuera de la caja.
4. Seleccione Generar



Paso 2. Vaya a Configuration > Security > PKI Management > Trustpoints

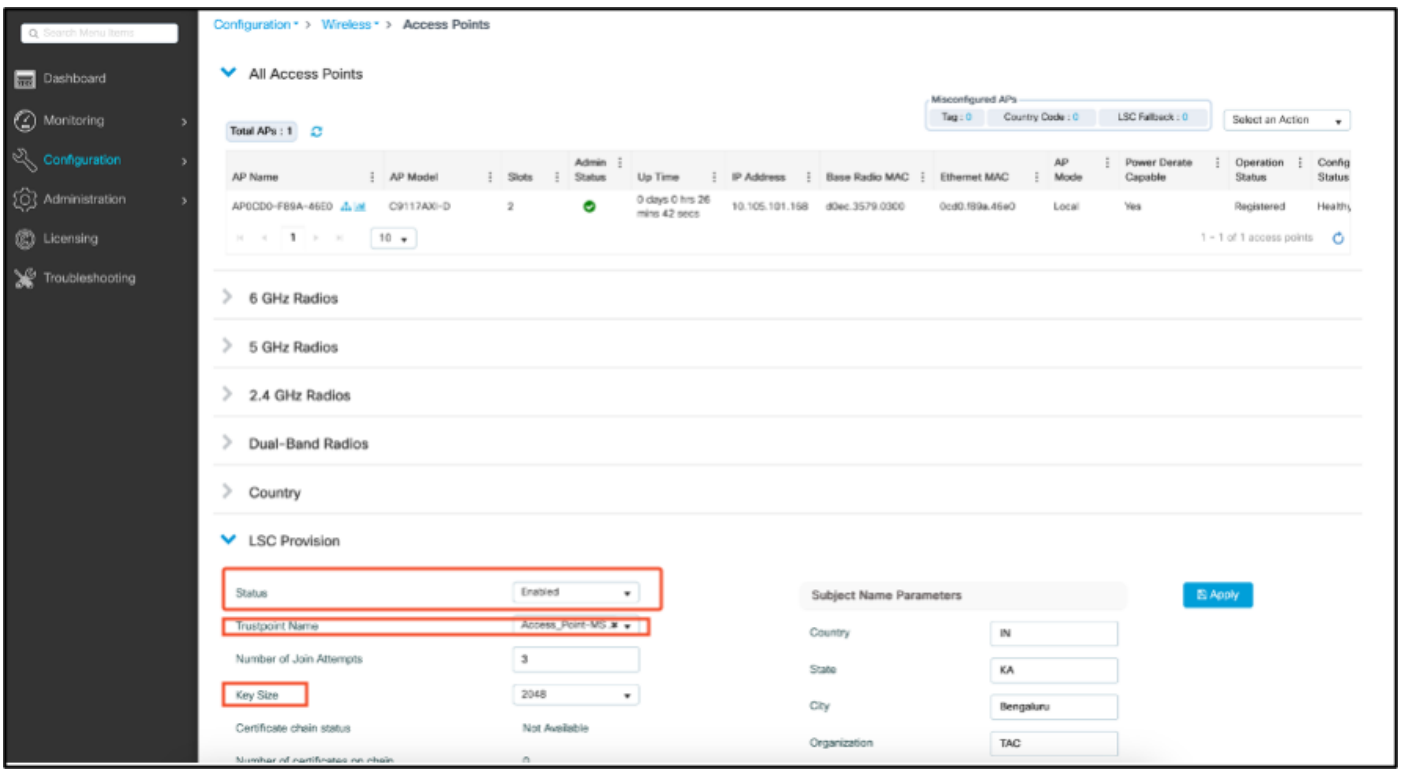
1. Haga clic en Agregar y asígnele un nombre relevante.
2. Introduzca la URL de inscripción (donde la URL es http://10.106.35.61:80/certsrv/mscep/mscep.dll) y el resto de los detalles.
3. Seleccione los pares de claves RSA creados en el paso 1.
4. Haga clic en Authenticate.
5. Haga clic en Inscribir punto de confianza e introduzca una contraseña.
6. Haga clic en Aplicar al dispositivo.



Paso 3.Vaya a Configuración > Inalámbrico > Puntos de acceso. Desplácese hacia abajo y seleccione LSC Provisioning.

1. Seleccione el estado como activado. Esto habilita el LSC para todos los AP que están conectados a este WLC.
2. Seleccione el nombre de punto de confianza que creamos en el paso 2.

Rellene el resto de los datos según sus necesidades.



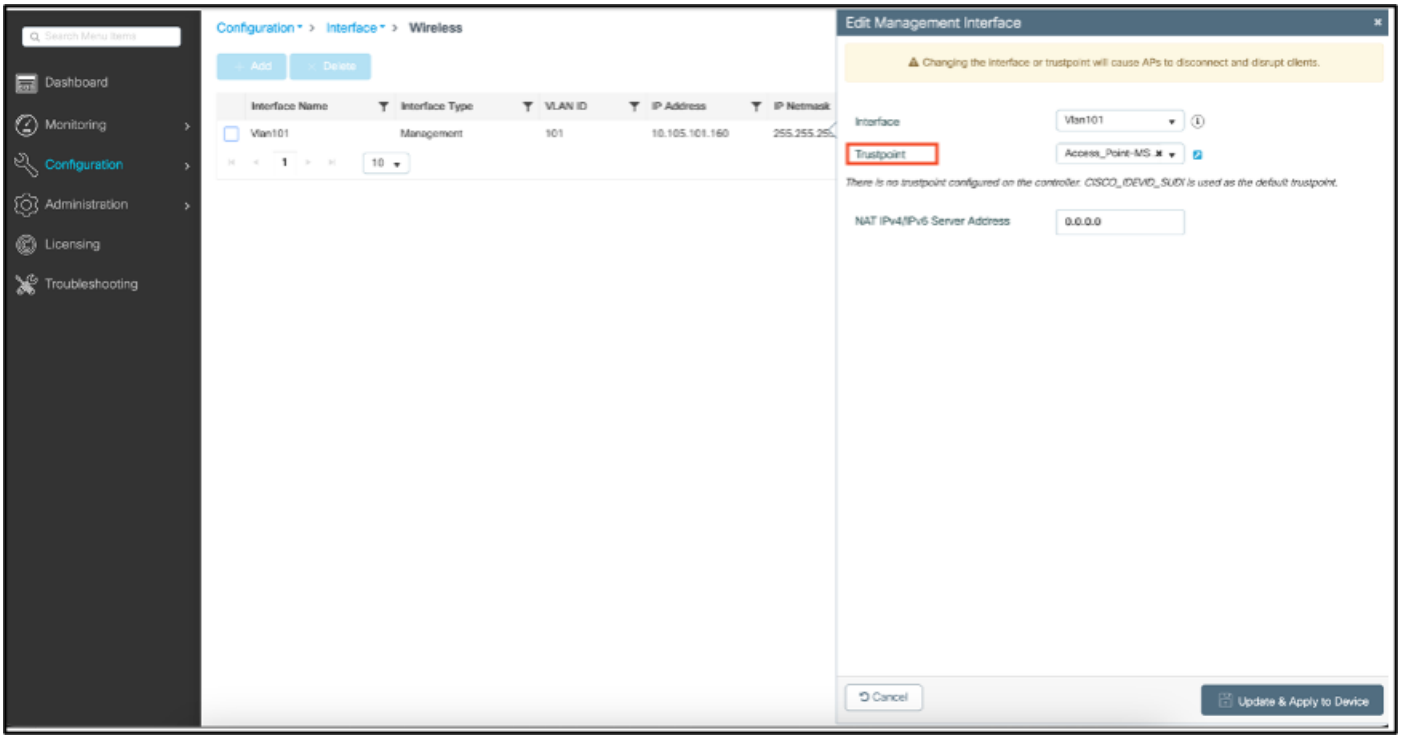
Una vez que habilita el LSC, los AP descargan el certificado vía el WLC y reinician. En la sesión de la consola AP, verá algo como este fragmento de código.

```
[*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
```

Paso 4.Una vez habilitado LSC, puede cambiar el certificado de administración inalámbrica para que coincida con el punto de confianza de LSC. Esto hace que los AP se unan con sus certificados LSC y que el WLC utilice su certificado LSC para la unión AP. Este es un paso opcional si su único interesado es hacer la autenticación 802.1X de sus AP.

1. Vaya a Configuration > Interface > Wireless y haga clic en Management Interface.
2. Cambie el Trustpoint para que coincida con el trustpoint que creamos en el paso 2.

Esto concluye la parte de configuración de la GUI de LSC. Los AP deben poder unirse al WLC usando el certificado LSC ahora.



Pasos de Configuración de LSC CLI de AP

1. Cree una clave RSA con 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 storag
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. Cree el punto de confianza PKI y asigne el par de claves RSA. Introduzca la URL de inscripción y el resto de los detalles.

```
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)#rsakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. Autentique e inscriba el punto de confianza PKI con el servidor CA mediante el comando crypto pki authenticate <trustpoint>. Introduzca una contraseña en la solicitud de contraseña.

```
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' commandwill 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 la unión de AP con el 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-LA
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. Cambie el punto de confianza de gestión inalámbrica para que coincida con el punto de confianza creado anteriormente.

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

Verificación de LSC de AP

Ejecute estos comandos en el WLC para verificar el 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 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       : Not Available
AP LSC authentication state                  : CAPWAP-DTLS
```

Una vez que se recargan los AP, inicie sesión en la CLI del AP y ejecute estos comandos para verificar la configuración de LSC.

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

```
AP0CD0.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
```

Resolución de Problemas del Aprovisionamiento de LSC

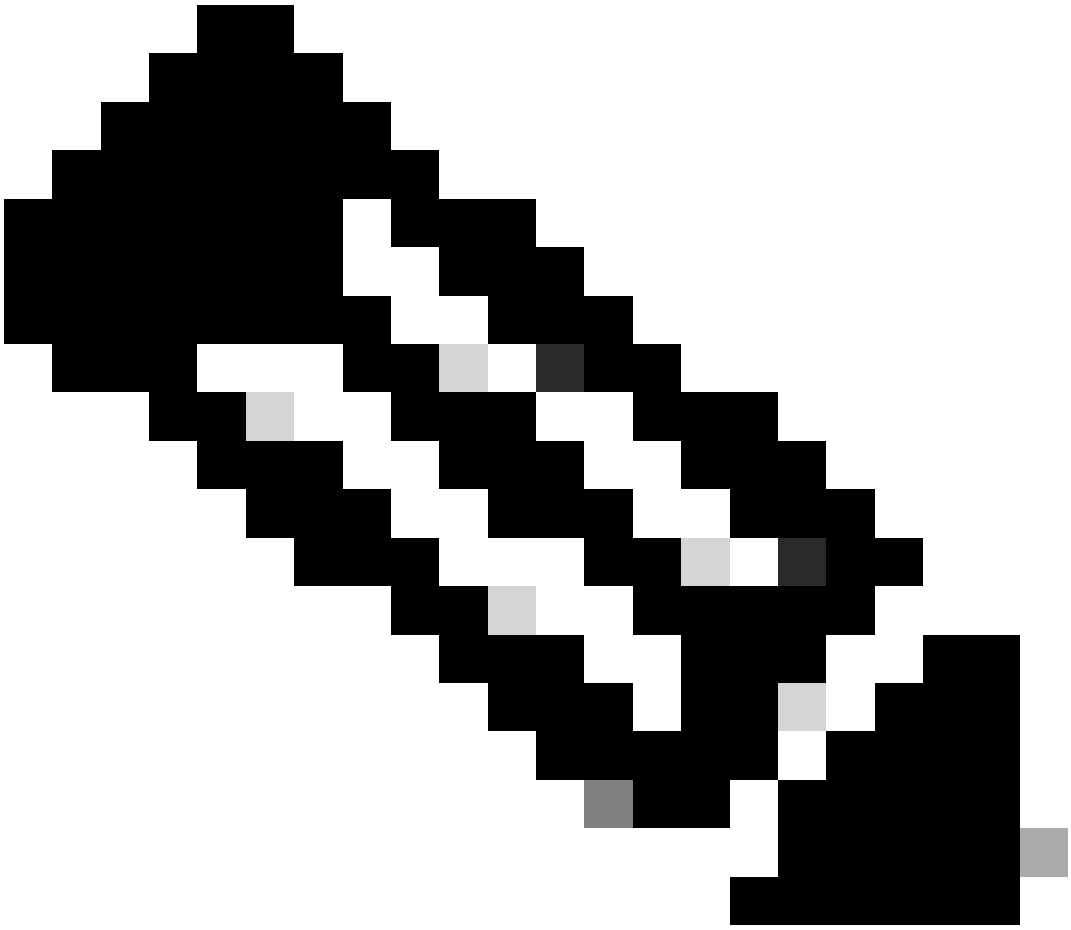
Puede tomar una captura EPC del puerto del switch de link ascendente WLC o AP para verificar el certificado que AP está utilizando para formar el túnel CAPWAP. Verifique desde el PCAP si el túnel DTLS se ha construido correctamente.

```
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: 3082065130820539a00302010202135c000000181814edda85f9bfd1000000000018300d… (pkcs-9-at-emailAddress=mail@tac-lab.local,id-at-commonNa
          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)
                RDNSequence item: 1 item (dc=com)
                  RelativeDistinguishedName item (dc=com)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: com
                RDNSequence item: 1 item (dc=tac-lab)
                  RelativeDistinguishedName item (dc=tac-lab)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: tac-lab
                RDNSequence item: 1 item (dc=sumans)
                  RelativeDistinguishedName item (dc=sumans)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: sumans
                RDNSequence 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)
```

Los debugs DTLS se pueden ejecutar en AP y WLC para comprender el problema del certificado.

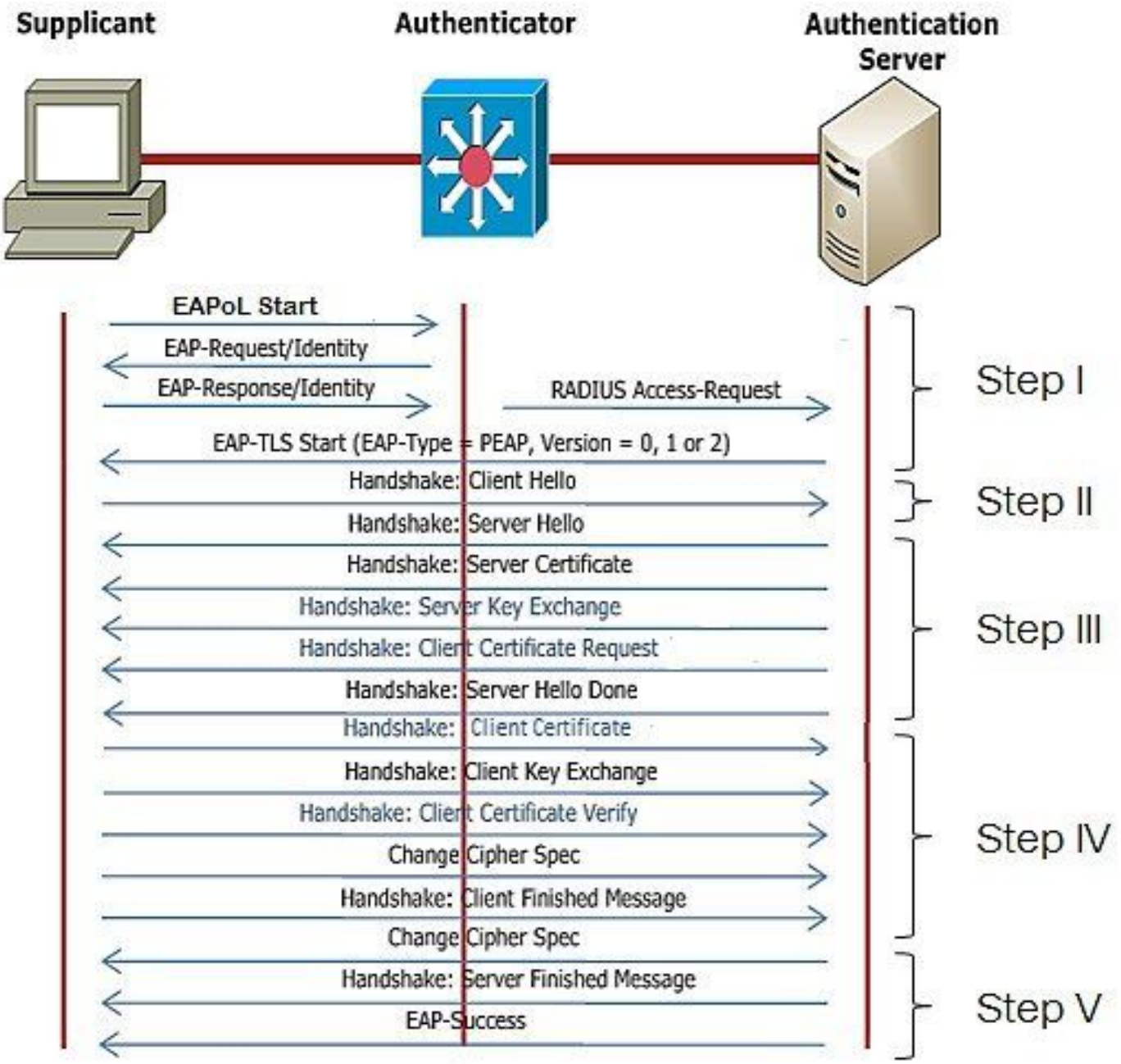
Autenticación 802.1X por cable AP mediante LSC

El AP está configurado para utilizar el mismo certificado LSC para autenticarse. El AP actúa como suplicante de 802.1X y es autenticado por el switch contra el servidor ISE. El servidor ISE se dirige al AD en el back-end.



> Nota: Una vez que se habilita la autenticación dot1x en el puerto del switch de link ascendente AP, los AP no pueden reenviar ni recibir tráfico hasta que se pasa la autenticación. Para recuperar los AP con autenticación fallida y obtener acceso al AP, inhabilite la autenticación dot1x en el puerto del switch cableado AP.

Flujo de trabajo de autenticación EAP-TLS e intercambio de mensajes

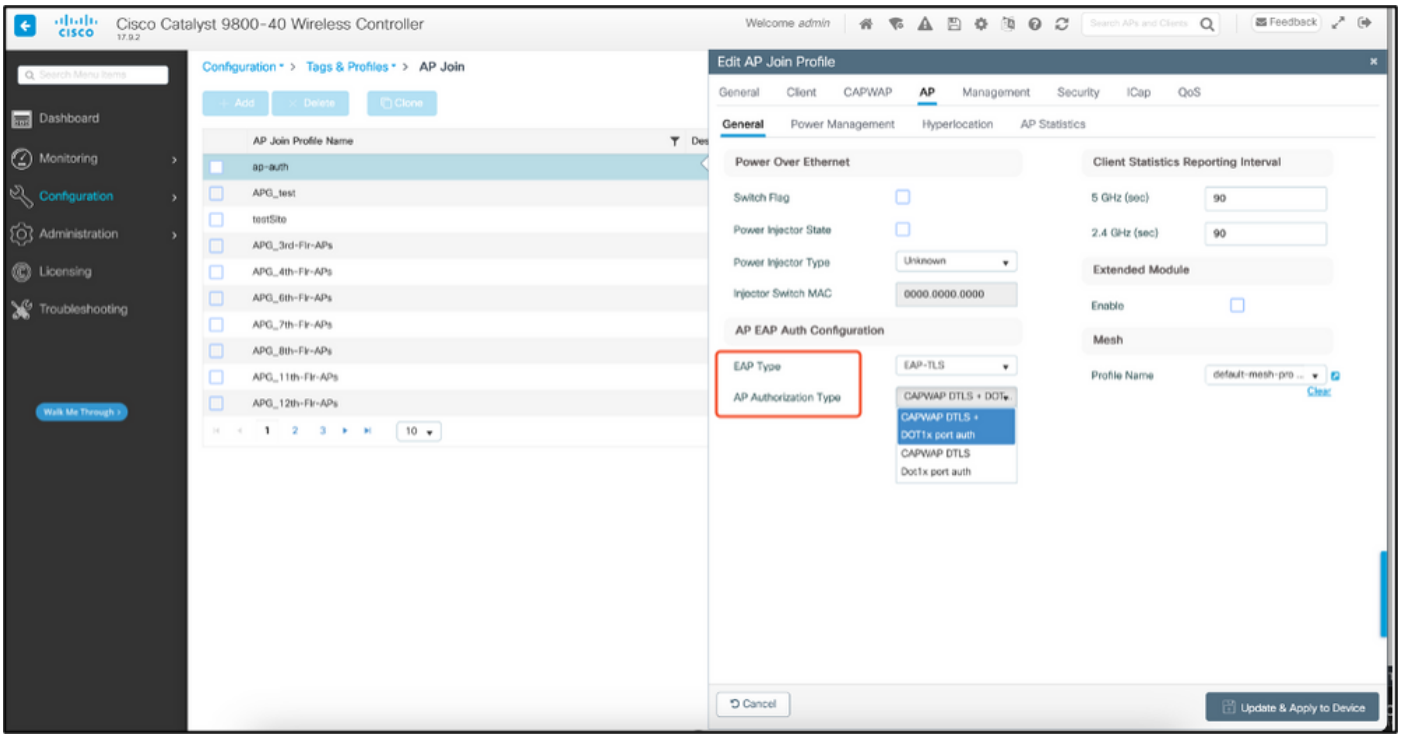


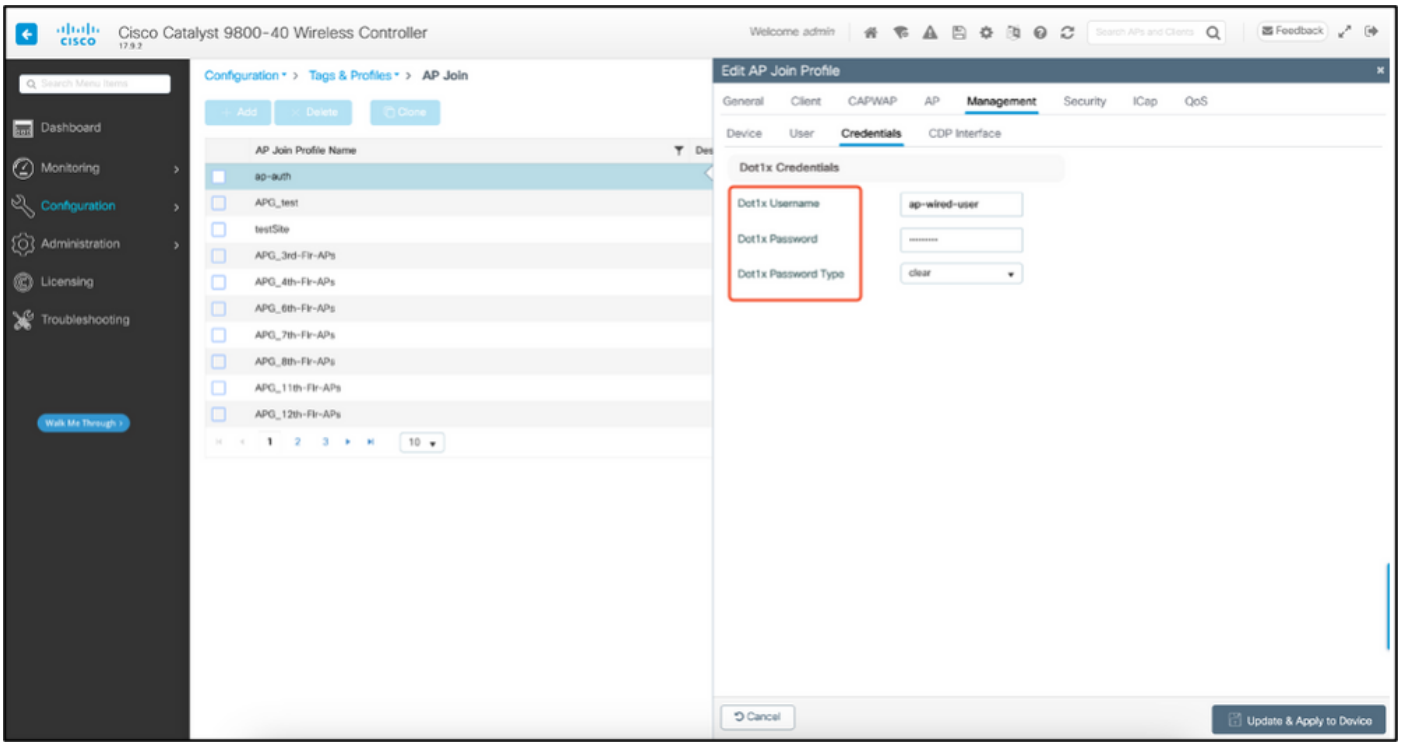
Pasos de Configuración de Autenticación 802.1x por Cable AP

1. Active la autenticación de puerto dot1x junto con CAPWAP DTLS y seleccione el tipo de EAP.
2. Cree credenciales dot1x para AP.
3. Habilite dot1x en el puerto del switch.
4. Instale un certificado de confianza en el servidor RADIUS.

Configuración GUI de autenticación 802.1x con cable AP

1. Navegue hasta el perfil de unión a AP y haga clic en el perfil.
    1. Haga clic en AP > General. Seleccione el tipo de EAP y el tipo de autorización de AP como "CAPWAP DTLS + autenticación de puerto dot1x".
    2. Navegue hasta Administración > Credenciales y cree un nombre de usuario y una contraseña para AP dot1x auth.





Configuración CLI de autenticación 802.1x por cable de PA

Utilice estos comandos para habilitar dot1x para AP desde la CLI. Esto solo habilita la autenticación por cable para los AP que están usando el perfil de unión 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
```

```
9800-40(config)#ap profile ap-auth
9800-40(config-ap-profile)#dot1x eap-type eap-tls
9800-40(config-ap-profile)#dot1x lsc-ap-auth-state both
9800-40(config-ap-profile)#
```

Configuración del switch de autenticación 802.1x por cable AP

Esta configuración del switch se utiliza en LAB para habilitar la autenticación por cable AP. Puede tener diferentes configuraciones basadas en el diseño.

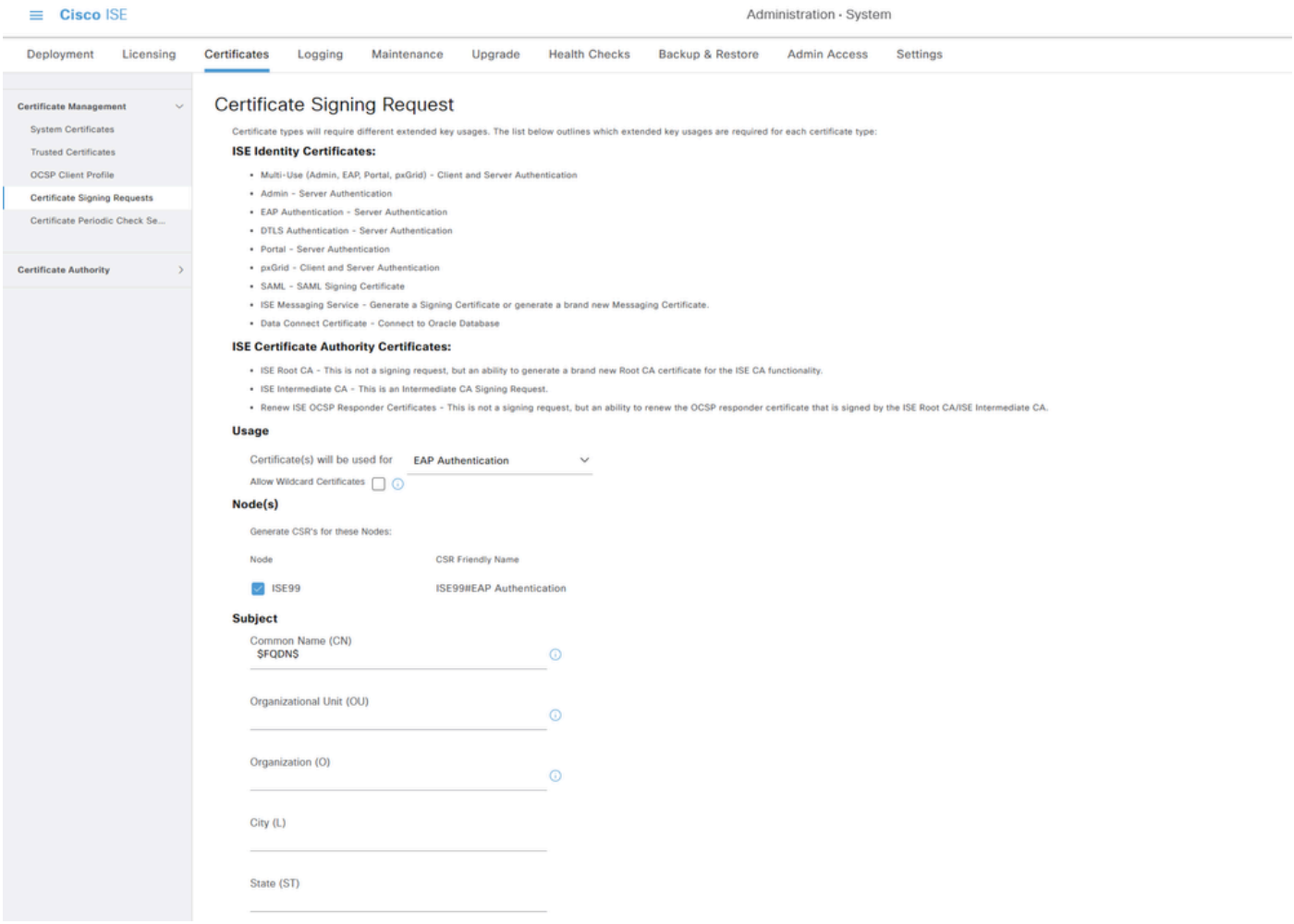
```
aaa new-model
dot1x system-auth-control
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius server ISE
address ipv4 10.106.34.170 auth-port 1812 acct-port 1813
key cisco!123
!
interface GigabitEthernet1/0/2
description "AP-UPLINK-PORT-AUTH-ENABLED"
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
```

Instalación del certificado del servidor RADIUS

La autenticación se produce entre el AP (que actúa como el solicitante) y el servidor RADIUS. Ambos deben confiar en el otro certificado. La única manera de que el AP confíe en el certificado del servidor RADIUS es hacer que el servidor RADIUS utilice una velocidad certici emitida por la CA SCEP que también emitió el certificado AP.

En ISE, vaya a Administration > Certificates > Generate Certificate Signing Requests.

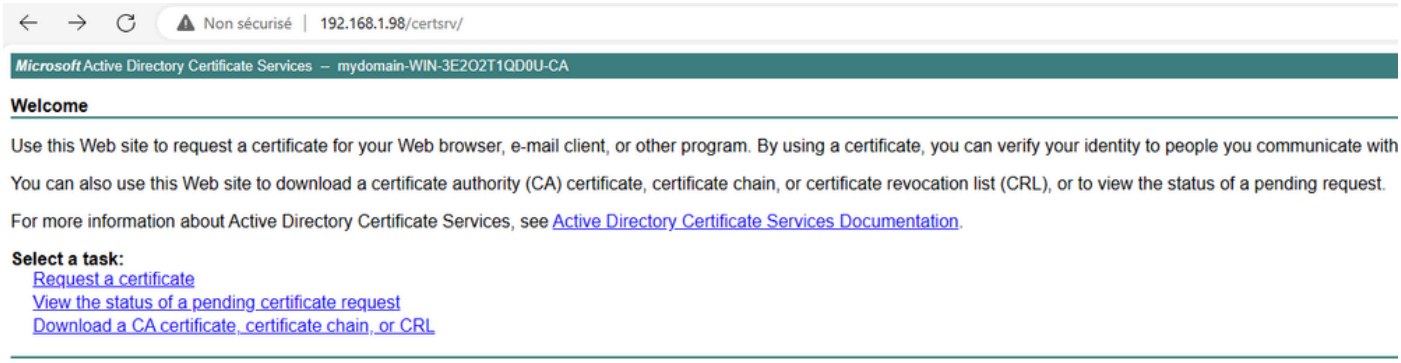
Genere una CSR y rellene los campos con la información de su nodo de ISE.



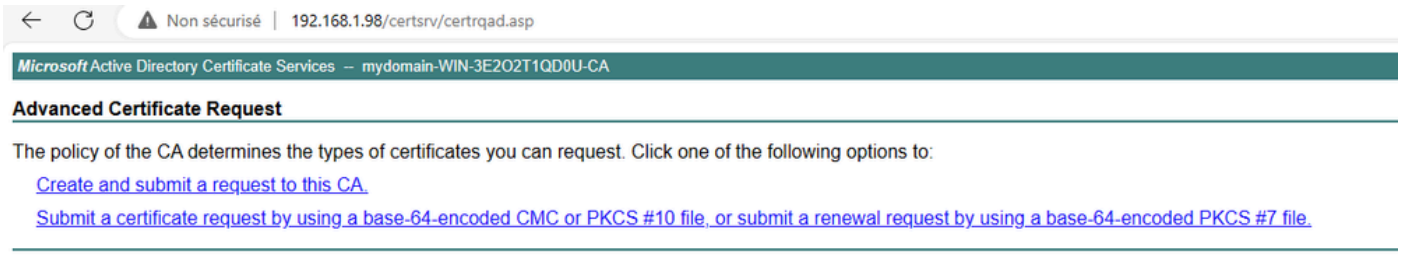
Una vez generado, puede exportarlo y copiarlo y pegarlo como texto también.

Navegue hasta la dirección IP de la CA de Windows y agregue /certsrv/ a la URL

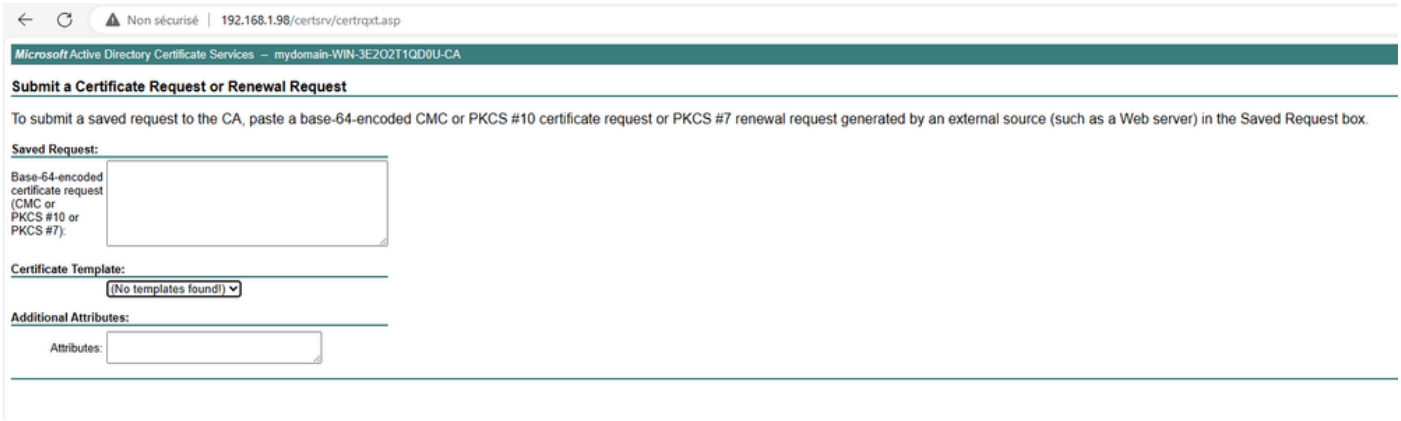
Haga clic en Solicitar un certificado



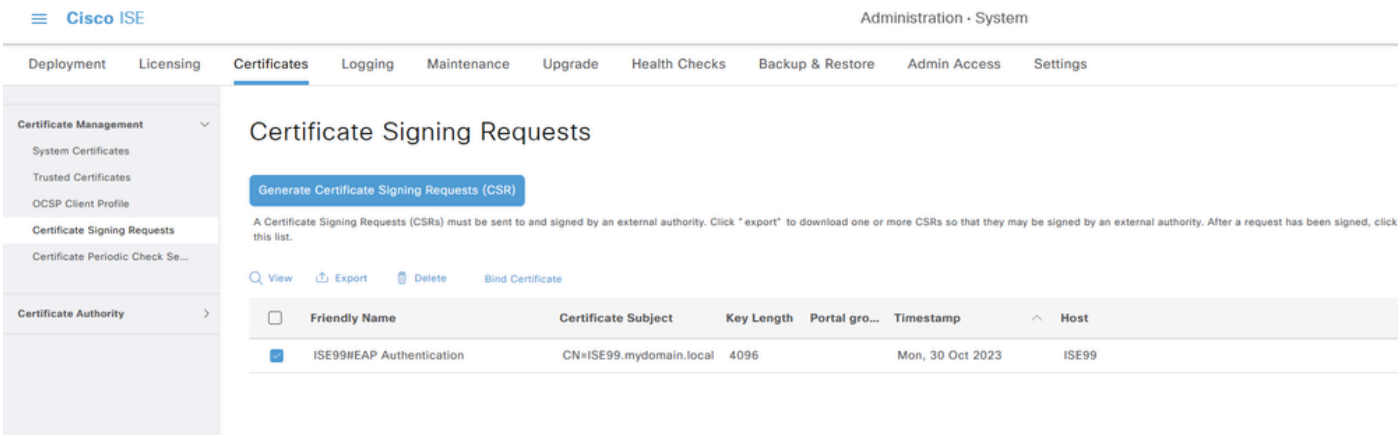
Haga clic en Enviar una solicitud de certificado con un certificado base-64 ....



Pegue el texto CSR en el cuadro de texto. Elija la plantilla de certificado del servidor Web.



A continuación, puede instalar este certificado en ISE volviendo al menú Solicitud de firma de certificado y haciendo clic en Enlazar certificado. A continuación, puede cargar el certificado obtenido desde Windows C.



Verificación de autenticación 802.1x por cable del PA

Tome el acceso de la consola al AP y ejecute el comando:

```
#show ap authentication status
```

La autenticación de AP no está habilitada:

```
AP0CD0.F89A.46E0#sho ap authentication status
AP dot1x feature is disabled.
AP0CD0.F89A.46E0#
```

Registros de la consola desde el AP después de habilitar la autenticación de 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 correctamente:

```
AP0CD0.F89A.46E0#sho ap authentication status
key_mgmt=IEEE 802.1X (no WPA)
wpa_state=COMPLETED
address=0c:d0:f8:9a:46:e0
supplicant_PAE_state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
eap_tls_version=TLSv1.2
EAP TLS cipher=ECDHE-RSA-AES256-GCM-SHA384
tls_session_reused=0
eap_session_id=0d7b91a744885a6e8e460d49fee7d2d5604ea2bdd11f40494a4325dc98d1919af48b9fb33ee526f18eda11effcb2ea0238cf95244aafb5f17decf336ad11e88121
AP0CD0.F89A.46E0#
```

Verificación del WLC:

```
9800-40#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
```

Estado de la interfaz de puerto de switch tras autenticación satisfactoria:

```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface              MAC Address    Method  Domain  Status Fg  Session ID
---------------------------------------------------------------------------
Gi1/0/2                0cd0.f89a.46e0 dot1x   DATA    Auth       9765690A0000005CCEED0FBF
```

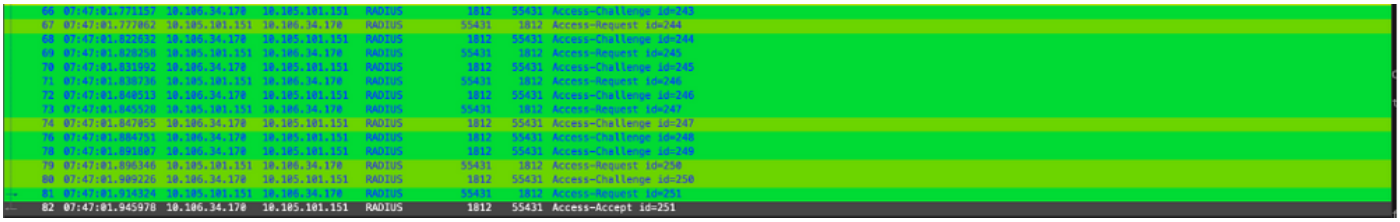
Este es un ejemplo de los registros de la consola AP que indican una autenticación exitosa:

```
[*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
```

Solucionar problemas de autenticación 802.1X

Tome PCAP en el link ascendente del AP y verifique la autenticación del radio. Este es un fragmento de la autenticación exitosa.

TCPdump collect de ISE que captura la autenticación.



Si se observa un problema durante la autenticación, se necesitaría la captura simultánea de paquetes desde el enlace ascendente por cable AP y el lado ISE.

Comando de depuración para AP:

```
#debug ap authentication packet
```

Información Relacionada

- Soporte técnico y descargas de Cisco
- Configuración de 802.1X en AP con AireOS
- Guía de configuración de 9800 para LSC
- Ejemplo de configuración de LSC para 9800
- Configuración de 802.1X para AP en 9800

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

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

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