

Configuración de SCEP para el Aprovisionamiento de Certificados de Significación Local en el WLC 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Habilitar servicios SCEP en Windows Server](#)

[Desactivar el requisito de contraseña de desafío de inscripción SCEP](#)

[Configuración de la plantilla de certificados y del registro](#)

[Configuración del punto de confianza del dispositivo 9800](#)

[Definir los Parámetros de Inscripción AP y Update Management Trustpoint](#)

[Verificación](#)

[Verificar la instalación del certificado del controlador](#)

[Verificación de la Configuración de 9800 WLC LSC](#)

[Verificar la instalación del certificado del punto de acceso](#)

[Troubleshoot](#)

[Problemas comunes](#)

[Comandos Debug y Log](#)

[Ejemplo de un Intento de Inscripción Satisfactorio](#)

Introducción

Este documento describe cómo configurar el controlador de LAN inalámbrica 9800 (WLC) para la inscripción de certificado de significación local (LSC) para los fines de unión de punto de acceso (AP) a través de las funciones Microsoft Network Device Enrollment Service (NDES) y Simple Certificate Enrollment Protocol (SCEP) dentro del estándar Windows Server 2012 R2.

Prerequisites

Para realizar correctamente SCEP con Windows Server, el WLC 9800 debe cumplir estos requisitos:

- Debe haber disponibilidad entre el controlador y el servidor.
- El controlador y el servidor se sincronizan con el mismo servidor NTP, o comparten la misma fecha y zona horaria (si la hora es diferente entre el servidor de la CA y la hora del AP, el AP tiene problemas con la validación del certificado y la instalación).

Windows Server debe tener los Servicios de Internet Information Server (IIS) habilitados anteriormente.

Requirements

Cisco recomienda que conozca estas tecnologías:

- 9800 Wireless LAN Controller versión 16.10.1 o superior.
- Estándar de Microsoft Windows Server 2012.
- Infraestructura de clave privada (PKI) y certificados.

Componentes Utilizados

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

- 9800-L Software WLC versión 17.2.1.
- Windows Server 2012 Standard R2.
- Puntos de acceso 3802.

Nota: La configuración del lado del servidor en este documento es específicamente WLC SCEP, para configuraciones adicionales fortalecidas, de seguridad y del servidor de certificados, consulte Microsoft TechNet.

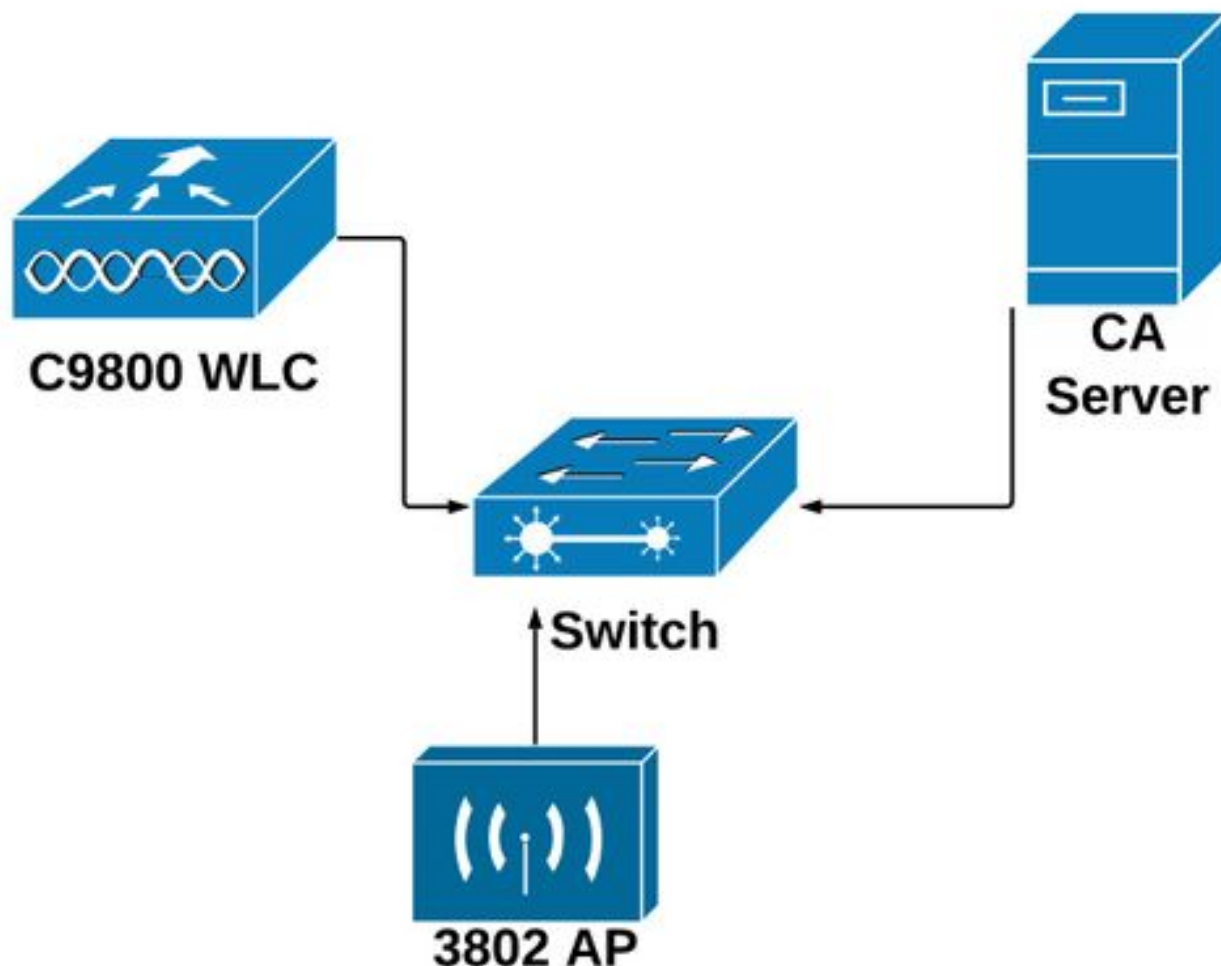
Antecedentes

Los nuevos certificados LSC, tanto el certificado raíz de la Autoridad de Certificación (CA) como el certificado de dispositivo, deben estar instalados en el controlador para descargarlos eventualmente en los AP. Con SCEP, los certificados de CA y de dispositivo se reciben del servidor de la CA y se instalan posteriormente automáticamente en el controlador.

El mismo proceso de certificación ocurre cuando los AP se aprovisionan con LSC; para hacerlo, el controlador actúa como proxy de CA y ayuda a obtener la solicitud de certificado (autogenerado) firmada por la CA para el AP.

Configurar

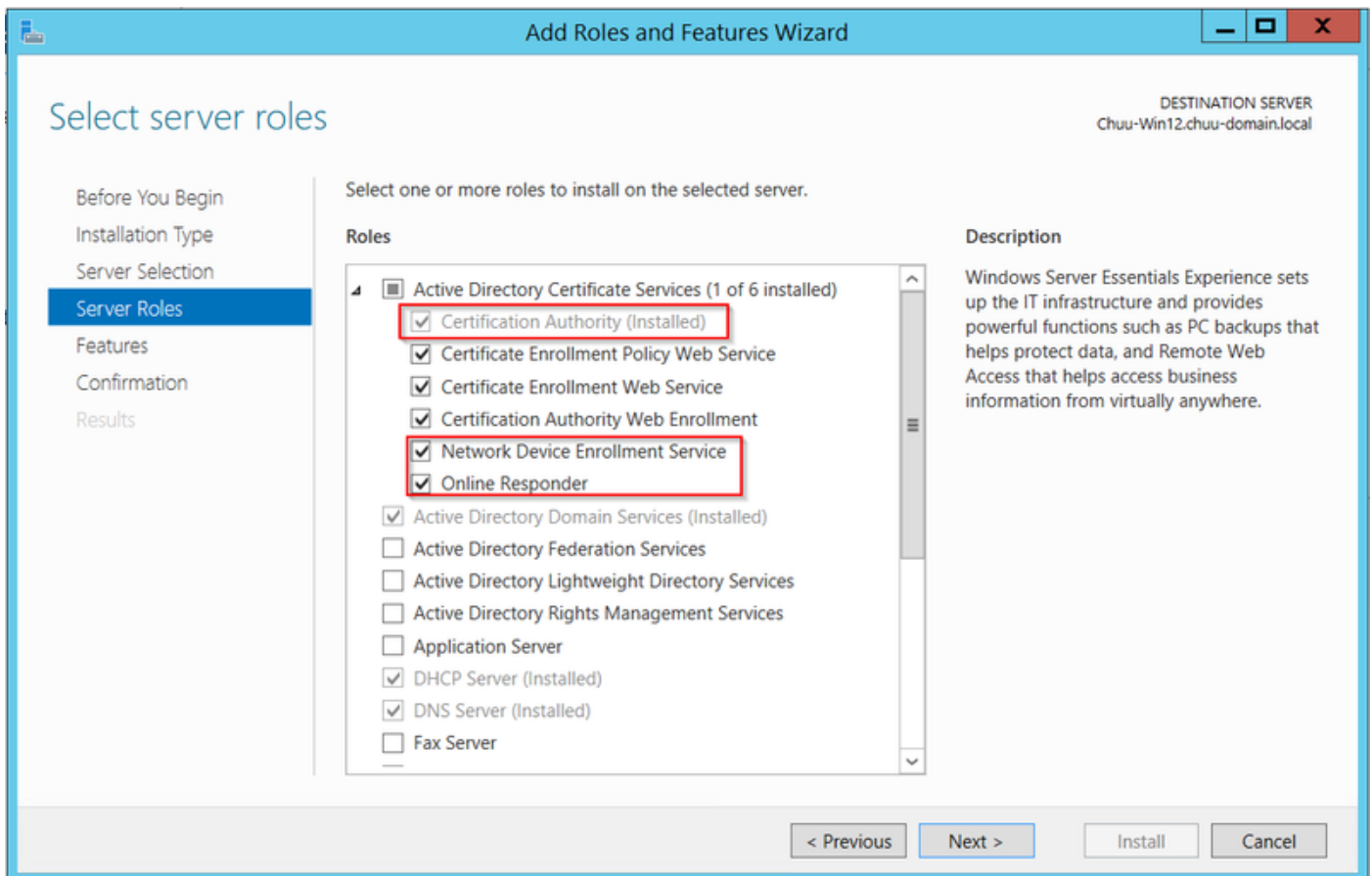
Diagrama de la red



Habilitar servicios SCEP en Windows Server

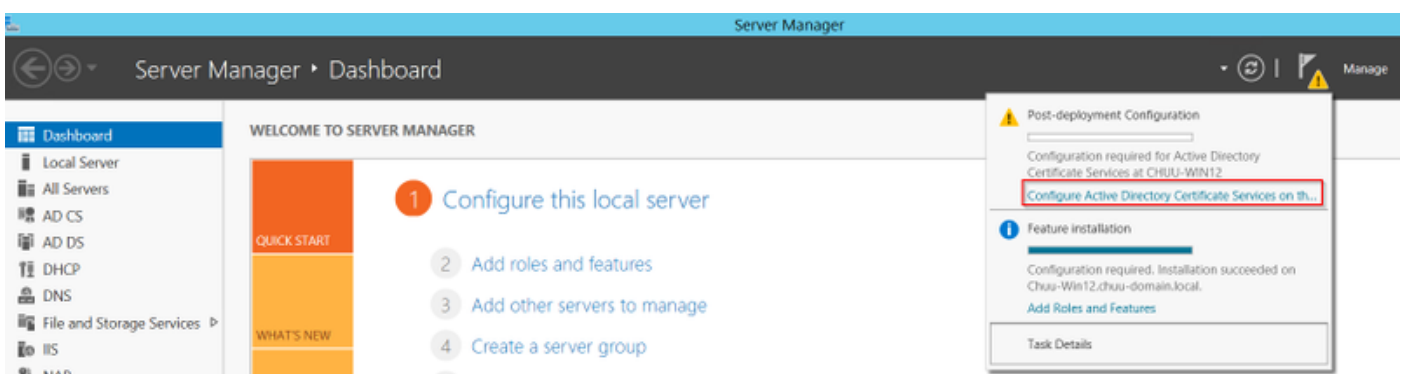
Paso 1. En la aplicación **Administrador de servidores**, seleccione el menú **Administrar** y, a continuación, seleccione la opción **Agregar funciones y características** para abrir la función Asistente para agregar funciones y funciones. Desde allí, seleccione la instancia del servidor que se utiliza para la inscripción del servidor SCEP.

Paso 2. Verifique que las funciones **Certification Authority**, **Network Device Enrollment Service** y **Online Responder** estén seleccionadas y luego seleccione **Next**:



Paso 3. Seleccione **Next** dos veces y **Finish** para finalizar el asistente de configuración. Espere a que el servidor complete el proceso de instalación de la función y, a continuación, seleccione **Cerrar** para cerrar el asistente.

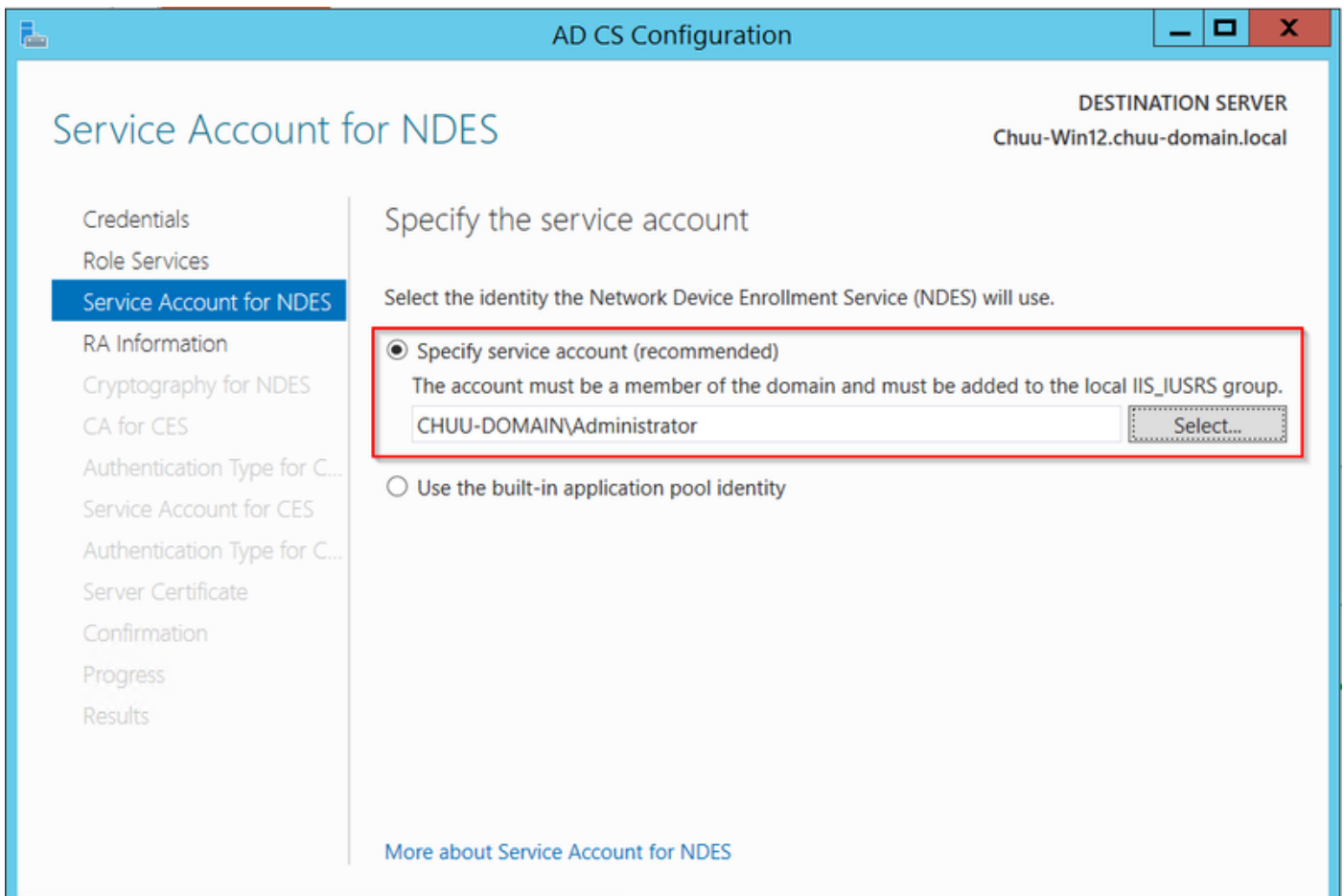
Paso 4. Una vez finalizada la instalación, aparece un icono de advertencia en el icono Notificación del administrador de servidores. Selecciónelo y seleccione el enlace **Configurar servicios de Active Directory** en la opción del **servidor de destino** para iniciar el menú **Asistente de configuración de AD CS**.



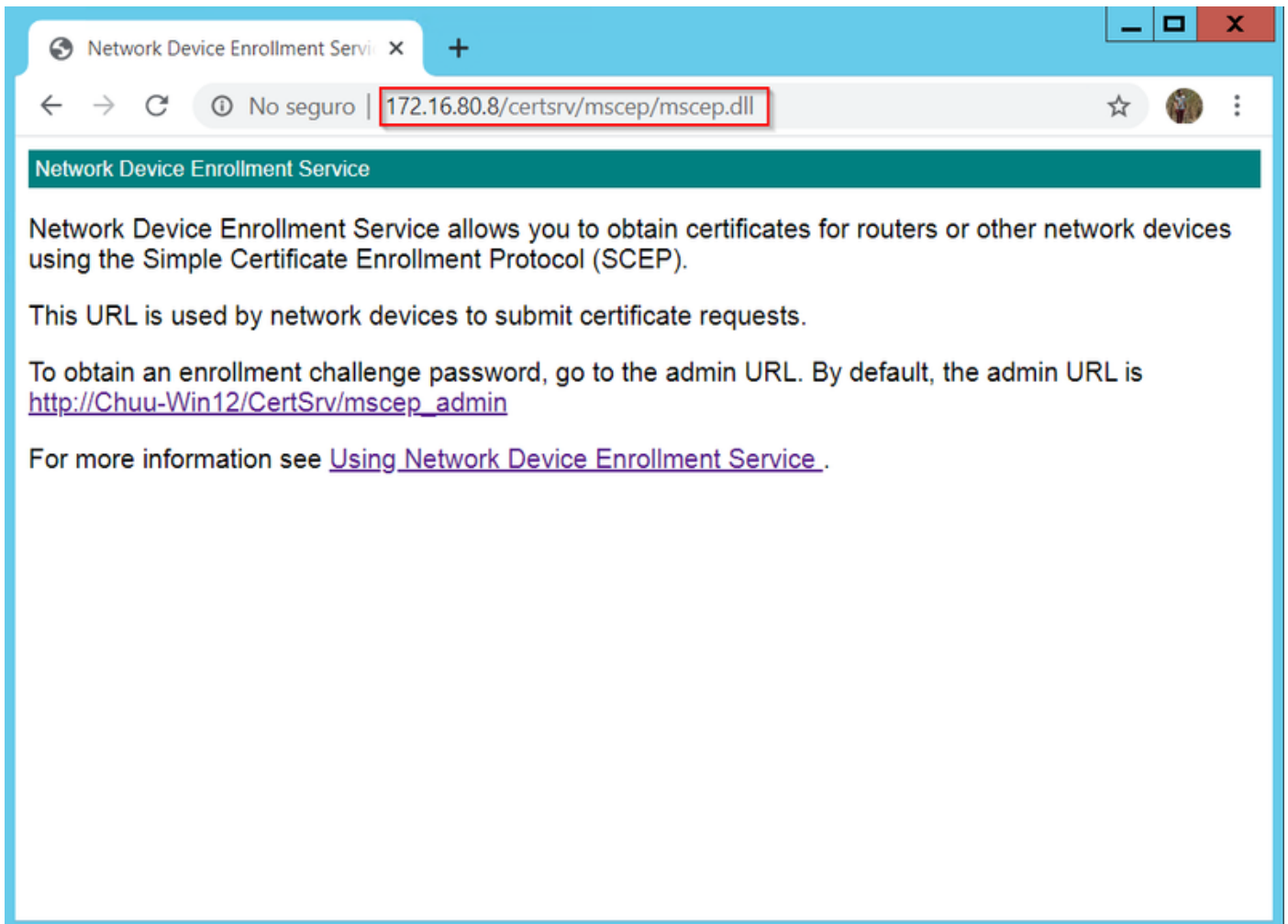
Paso 5. Seleccione los servicios de función **Network Device Enrollment Service** y **Online Responder** que se configurarán en el menú y, a continuación, seleccione **Next**.

Paso 6. En la **Cuenta de servicio para NDES** seleccione una opción entre el conjunto de aplicaciones integrado o la cuenta de servicio y, a continuación, seleccione **Siguiente**.

Nota: Si cuenta de servicio, asegúrese de que la cuenta forma parte del grupo **IIS_IUSRS**.



Paso 7. Seleccione **Next** para las pantallas siguientes y deje que finalice el proceso de instalación. Después de la instalación, la url SCEP está disponible con cualquier navegador web. Navegue hasta la URL <http://<server ip>/certsrv/mscep/mscep.dll> para verificar que el servicio esté disponible.



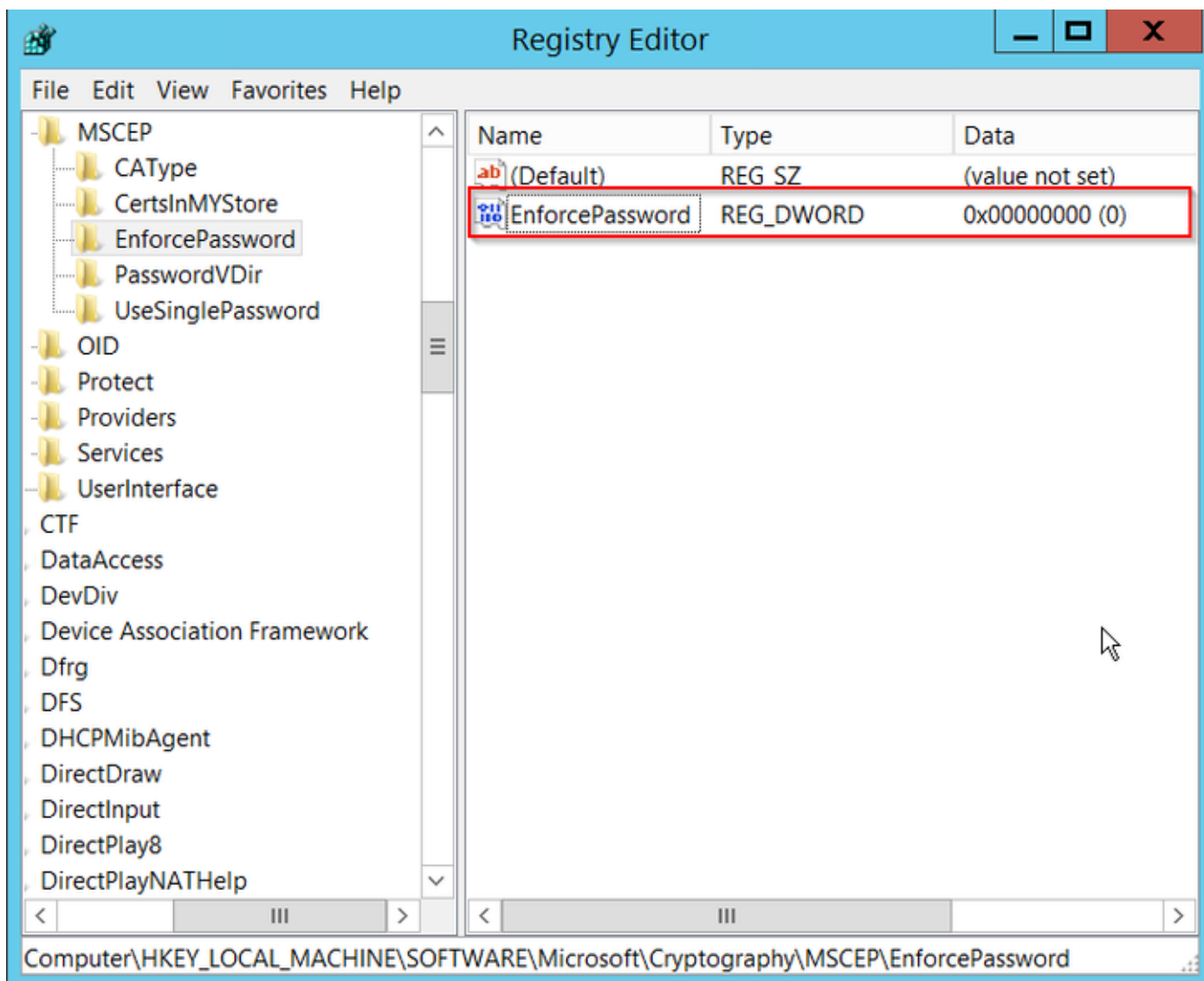
Desactivar el requisito de contraseña de desafío de inscripción SCEP

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

Paso 1. Abra el Editor del Registro, busque **Regedit** en el **menú Inicio**.

Paso 2. Vaya a **Equipo > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografía > MSCEP > AplicarContraseña**

Paso 3. Cambie el valor **EnforcePassword** a 0. Si ya es 0, déjelo como está.



Configuración de la plantilla de certificados y del registro

Los certificados y sus claves asociadas se pueden utilizar en varios escenarios para diferentes propósitos definidos por las políticas de aplicación dentro del servidor de la CA. La política de la aplicación se almacena en el campo Uso de clave extendida (EKU) del certificado. El autenticador analiza este campo para verificar que el cliente lo utiliza para el propósito deseado. Para asegurarse de que la política de aplicación adecuada esté integrada con los certificados WLC y AP, cree la plantilla de certificado adecuada y asígnele al registro NDES:

Paso 1. Vaya a Inicio > Herramientas administrativas > Autoridad de certificación.

Paso 2. Expanda el árbol de carpetas del 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 del ratón en la plantilla de certificado **Users** y, a continuación, seleccione **Duplicate Template** en el menú contextual.

Paso 4. Navegue hasta la pestaña **General**, cambie el nombre de la plantilla y el período de validez como desee y deje el resto de opciones sin marcar.

Precaución: Cuando se modifique el período de validez, asegúrese de que no sea superior a la validez del certificado raíz de la Autoridad de certificación.

Properties of New Template

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

Template display name:
9800-LSC

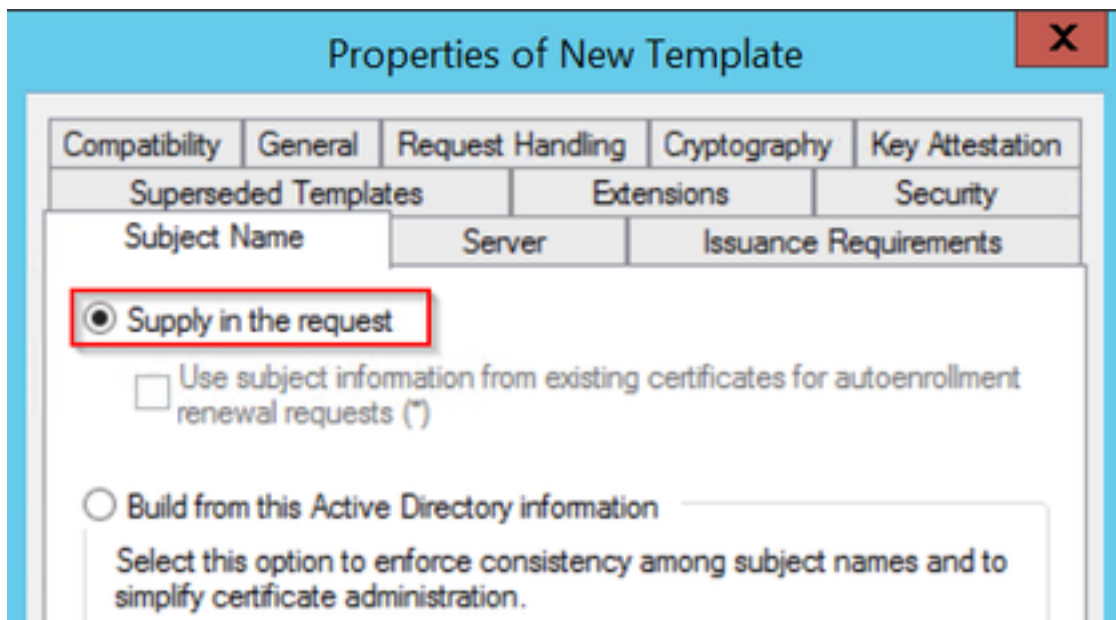
Template name:
9800-LSC

Validity period: 2 years
Renewal period: 6 weeks

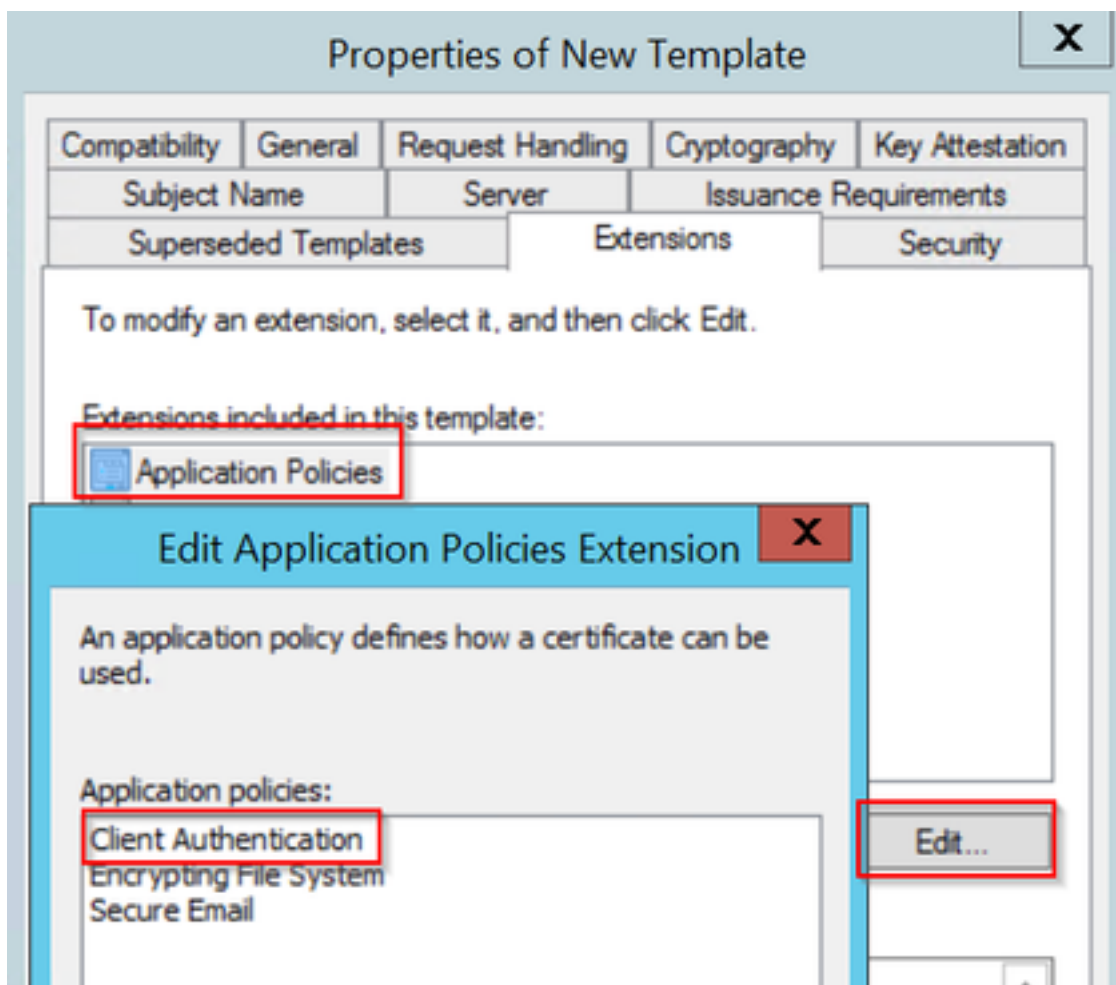
Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

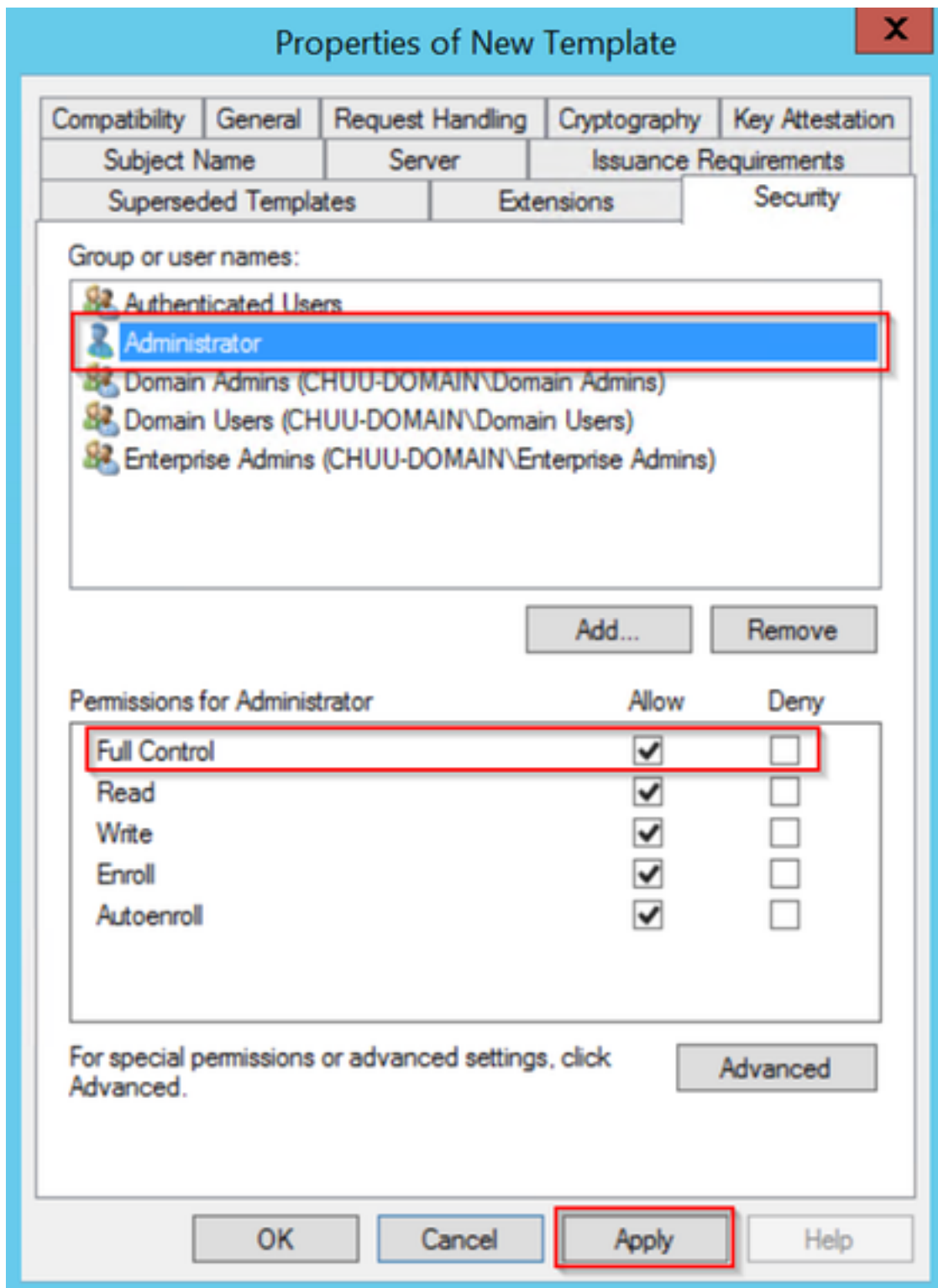
Paso 5. Vaya a la pestaña **Nombre del asunto**, asegúrese de que se haya seleccionado **Abastecimiento en la solicitud**. Aparece una ventana emergente para indicar que los usuarios no necesitan aprobación de administrador para que se firme su certificado, seleccione **Aceptar**.



Paso 6. Navegue hasta la pestaña **Extensiones**, luego seleccione la opción **Políticas de Aplicación** y seleccione la opción **Editar...** para abrir el Navegador. Asegúrese de que la **Autenticación de Cliente** esté en la **ventana Políticas de Aplicación**; de lo contrario, seleccione **Add** y agréguelo.



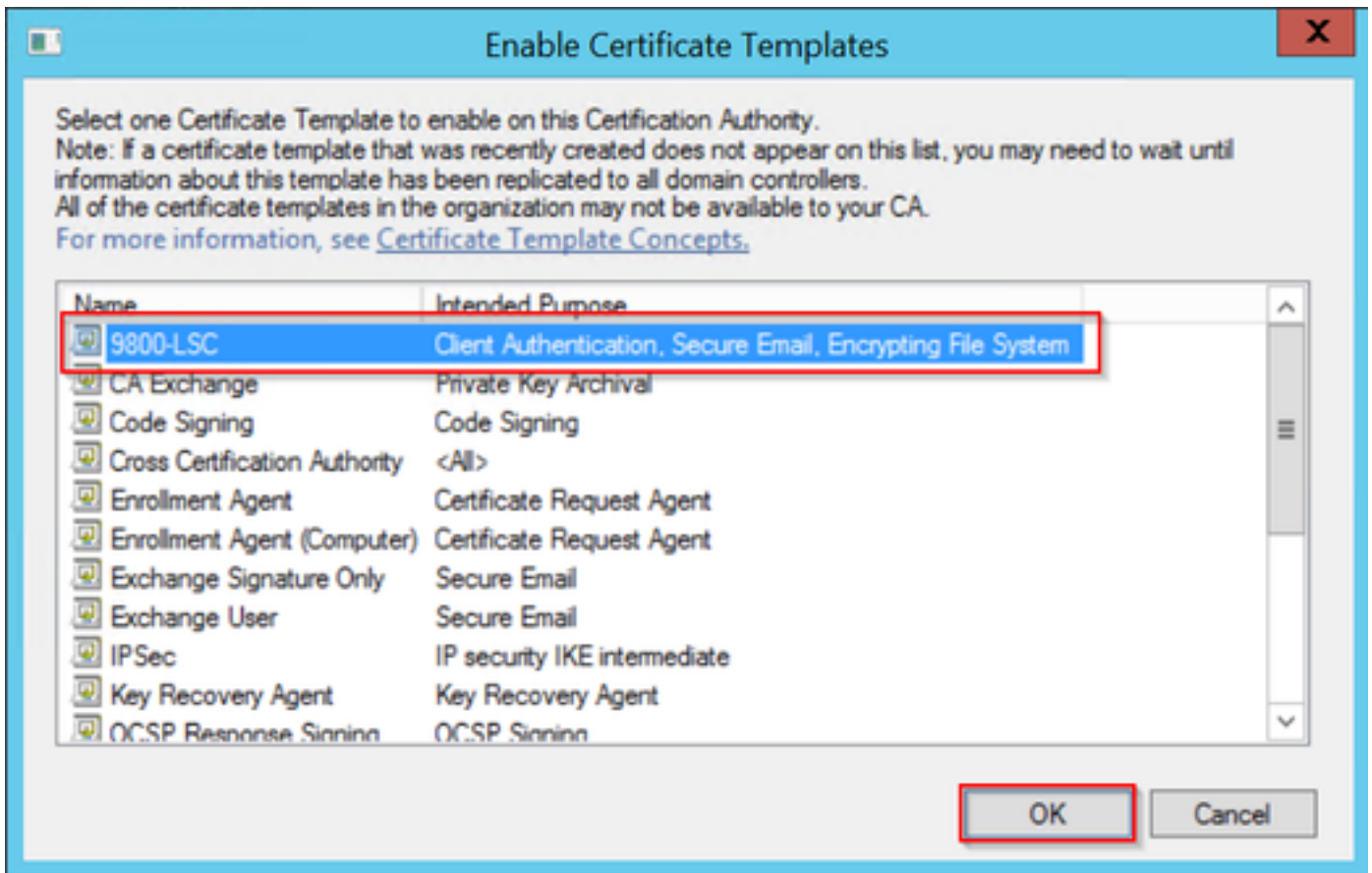
Paso 7. Navegue hasta la ficha Seguridad, asegúrese de que la cuenta de servicio definida en el Paso 6 de Habilitar servicios SCEP en el **servidor** de Windows tenga **permisos de control completo** de la plantilla y, a continuación, seleccione **Aplicar** y **Aceptar**.



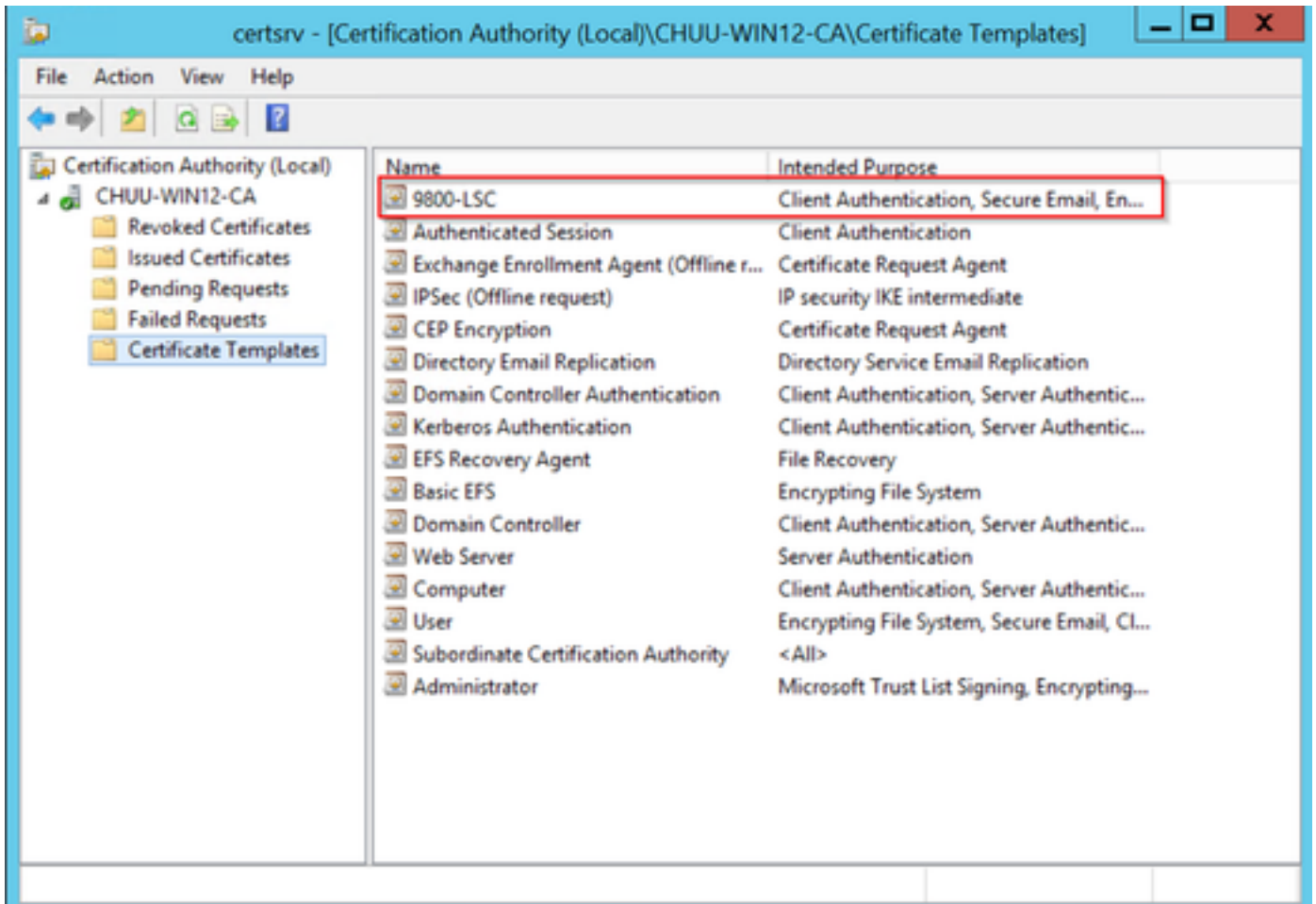
Paso 8. Vuelva a la ventana **Certification Authority**, haga clic con el botón derecho en la carpeta **Certificate Templates** y seleccione **New > Certificate Template to Issue**.

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

Nota: La plantilla de certificados creada recientemente puede tardar más en aparecer en varias implementaciones de servidores, ya que debe replicarse en todos los servidores.

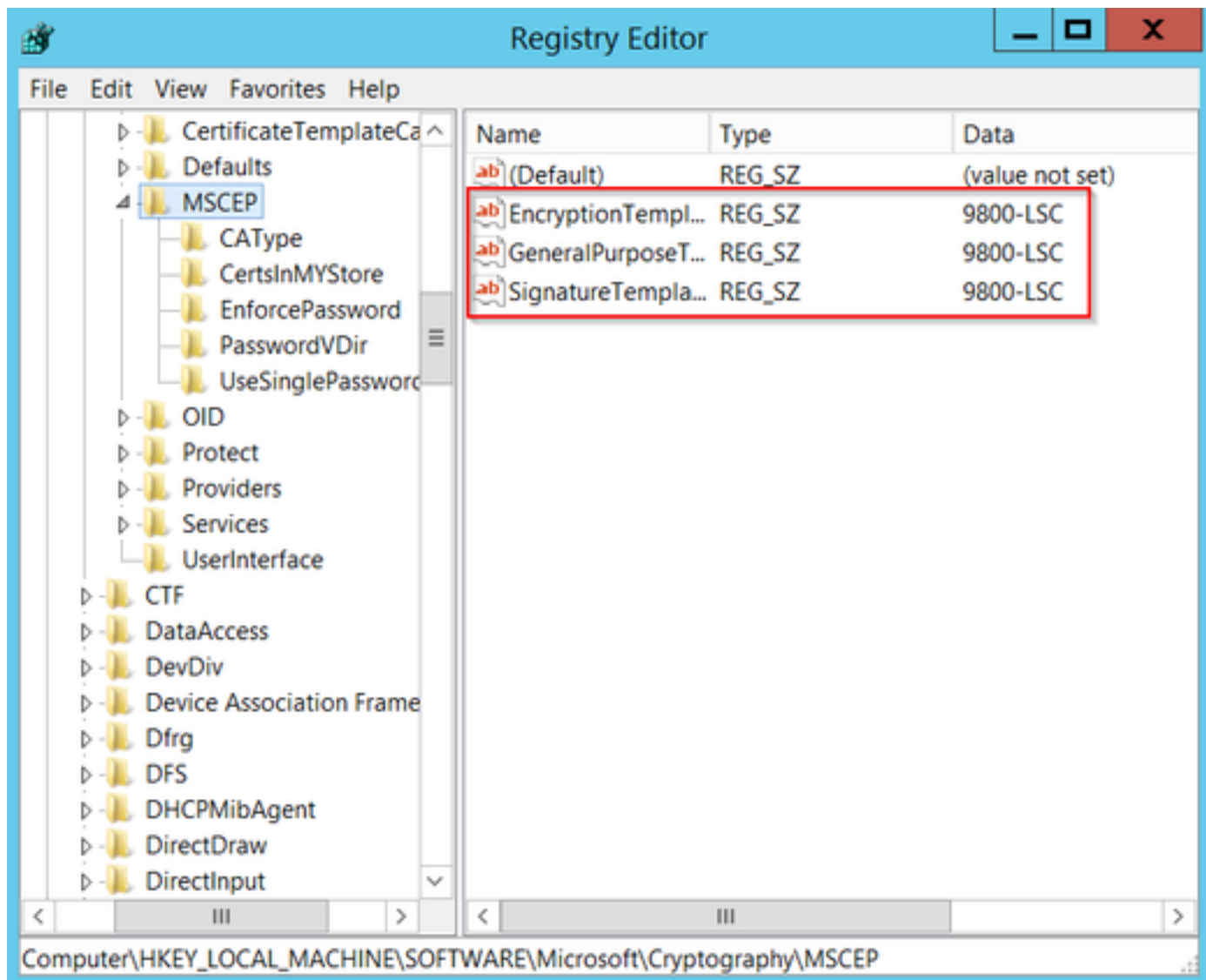


La nueva plantilla de certificado aparece ahora en el contenido de la carpeta **Plantillas de certificado**.

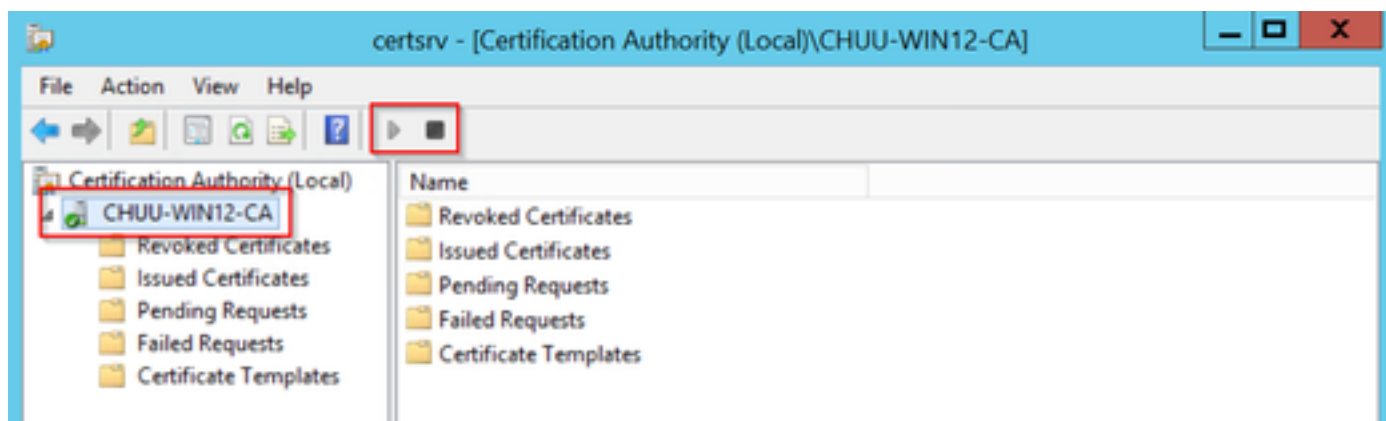


Paso 10. Vuelva a la ventana **Editor del Registro** y navegue hasta **Equipo > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografía > MSCEP**.

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



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



Configuración del punto de confianza del dispositivo 9800

El controlador necesita tener un punto de confianza definido para autenticar APs una vez que hayan sido aprovisionados. El punto de confianza incluye el certificado de dispositivo 9800, junto con el certificado raíz de CA ambos obtenidos del mismo servidor de CA (Microsoft CA en este ejemplo). Para que un certificado se instale en el punto de confianza, debe contener los atributos del sujeto junto con un par de claves RSA asociadas a él. La configuración se realiza a través de la interfaz web o de la línea de comandos.

Paso 1. Navegue hasta **Configuration > Security > PKI Management** y seleccione la pestaña **Generación de par de llaves RSA**. Seleccione el botón **+ Add**.

Paso 2. Defina una etiqueta asociada al par de claves y asegúrese de que la casilla **Exportable** esté seleccionada.

Key Label	Key Exportable	Zeroize RSA Key
TP-self-signed-1997188793	No	Zeroize
AP-KEY	Yes	Zeroize
chaincert.pfx	No	Zeroize
TP-self-signed-1997188793.server	No	Zeroize
CISCO_IDEVID_SUDI_LEGACY	No	Zeroize
CISCO_IDEVID_SUDI	No	Zeroize
SLA-KeyPair	Yes	Zeroize
SLA-KeyPair2	Yes	Zeroize

Configuración CLI para los pasos uno y dos, en este ejemplo de configuración el par de llaves se genera con la etiqueta AP-LSC y el tamaño del módulo de 2048 bits:

```
9800-L(config)#crypto key generate rsa exportable general-keys modulus
```

```
The name for the keys will be: AP-LSC
```

```
% The key modulus size is 2048 bits  
% Generating 2048 bit RSA keys, keys will be exportable...  
[OK] (elapsed time was 1 seconds)
```

Paso 3. Dentro de la misma sección, seleccione la ficha **Trustpoint** y seleccione el **+ botón Agregar**.

Paso 4. Rellene los detalles del punto de confianza con la información del dispositivo y, a continuación, seleccione **Aplicar al dispositivo**:

- El campo **Etiqueta** es el nombre asociado al punto de confianza
- Para la **URL de inscripción** utilice la definida en el Paso 7 de la sección **Habilitar servicios SCEP en Windows Server**.

- Marque la casilla de verificación **Authenticate** para que se descargue el certificado CA
- El campo **Domain Name** se coloca como el atributo de nombre común de la solicitud de certificado
- Marque la casilla **Key Generated**, aparecerá un menú desplegable, seleccione el par de claves generado en el Paso 2
- Marque la casilla de verificación **Inscribir punto de confianza**, aparecen dos campos de contraseña; escriba una contraseña. Esto se utiliza para encadenar las claves de certificado con el certificado del dispositivo y el certificado de CA

Advertencia: El controlador 9800 no soporta cadenas de servidores de varios niveles para la instalación de LSC, así que la CA raíz debe ser la que firme las solicitudes de certificado del controlador y los AP.

Configuración CLI para los pasos tres y cuatro:

Precaución: La línea de configuración subject-name debe tener el formato de sintaxis LDAP; de lo contrario, el controlador no la acepta.

```
9800-L(config)#crypto pki trustpoint
```

```
9800-L(ca-trustpoint)#enrollment url http://
```

```
9800-L(ca-trustpoint)#subject-name C=
```

```
9800-L(ca-trustpoint)#rsakeypair
```

```
9800-L(ca-trustpoint)#revocation-check none
```

```
9800-L(ca-trustpoint)#exit
```

```
9800-L(config)#crypto pki authenticate
```

Certificate has the following attributes:

Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224

Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B

```
% Do you accept this certificate? [yes/no]: yes
```

Trustpoint CA certificate accepted.

```
9800-L(config)#crypto pki enroll <trustpoint name>
```

```
%
```

```
% 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:
```

```
Re-enter password:
```

```
% The subject name in the certificate will include: C=MX, ST=CDMX, L=Juarez, O=Wireless TAC,  
CN=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
```

```
% The subject name in the certificate will include: 9800-L.alzavala.local
```

```
% Include the router serial number in the subject name? [yes/no]: no
```

```
% 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 AP-LSC' command will show the fingerprint.
```

Definir los Parámetros de Inscripción AP y Update Management Trustpoint

La inscripción AP utiliza los detalles del punto de confianza previamente definidos para determinar los detalles del servidor a los que el controlador reenvía la solicitud de certificado. Dado que el controlador se utiliza como proxy para la inscripción de certificados, debe ser consciente de los parámetros de asunto incluidos en la solicitud de certificado. La configuración se realiza a través de la interfaz web o de la línea de comandos.

Paso 1. Navegue hasta **Configuración > Inalámbrico > Puntos de Acceso** y expanda el menú **Provisión LSC**.

Paso 2. Rellene los **Parámetros del Nombre del Asunto** con los atributos que se rellenan en las solicitudes de certificado AP y, a continuación, seleccione **Aplicar**.

Subject Name Parameters	
Country	MX
State	CDMX
City	Juarez
Organisation	Cisco TAC
Department	Wireless TAC
Email Address	jesuherr@cisco.com

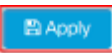
Configuración CLI para los pasos uno y dos:

```
9800-L(config)#ap lsc-provision subject-name-parameter country
```

Nota: Los parámetros de nombre de asunto restringidos a 2 caracteres como código de país deben respetarse estrictamente, ya que el WLC 9800 no valida esos atributos.

Para obtener más información, consulte el defecto [CSCvo72999](#) como referencia.

Paso 3. Dentro del mismo menú, seleccione el punto de confianza definido previamente en la lista desplegable, especifique un número de intentos de unión AP (esto define el número de intentos de unión antes de que vuelva a utilizar el MIC) y establezca el tamaño de la clave de certificado. A continuación, haga clic en **Aplicar**.

Status	Disabled	
Trustpoint Name	AP-LSC	
Number of Join Attempts	10	
Key Size	2048	
Add APs to LSC Provision List		
Subject Name Parameters		
Country	MX	
State	CDMX	
City	Juarez	
Organisation	Cisco TAC	

Configuración CLI para el paso tres:

```
9800-L(config)#ap lsc-provision join-attempt
```

```
9800-L(config)#ap lsc-provision trustpoint
```

```
9800-L(config)#ap lsc-provision key-size
```

Paso 4. (Opcional) El aprovisionamiento de LSC de AP se puede activar para todos los APs unidos al controlador, o para APs específicos definidos en una lista de direcciones MAC. Dentro del mismo menú, ingrese la dirección MAC Ethernet AP en el formato xxxx.xxxx.xxxx en el campo de texto y haga clic en el signo +. Alternativamente, cargue un archivo csv que contenga las direcciones MAC AP, seleccione el archivo y luego seleccione **Cargar archivo**.

Nota: El controlador omite cualquier dirección mac en el archivo csv que no reconoce de su lista de AP unida.

Add APs to LSC Provision List

Select File

Select CSV File

Upload File

AP MAC Address

Enter MAC/Sear

+

APs in Provision List : 1

286f.7fcf.53ac	
----------------	--

286f.7fcf.53ac

< >

Configuración CLI para el paso cuatro:

```
9800-L(config)#ap lsc-provision mac-address
```

Paso 5. Seleccione **Enabled** o **Provisioning List** en el menú desplegable junto a la etiqueta **Status** y luego haga clic en **Apply** para activar la inscripción LSC AP.

Nota: Los AP comienzan la solicitud, descarga e instalación del certificado. Una vez que el certificado está completamente instalado, el AP se reinicia e inicia el proceso de unión con el nuevo certificado.

Consejo: Si el aprovisionamiento de LSC de AP se realiza a través de un controlador de pre-producción se utiliza junto con la lista de aprovisionamiento, no elimine las entradas de AP una vez que se aprovisiona el certificado. Si esto se hace, y los AP se devuelven a MIC y se unen al mismo controlador previo a la producción, sus certificados LSC se borran.



Configuración CLI para el paso cinco:

```
9800-L(config)#ap lsc-provision
```

In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration. In WLANCC mode APs will be provisioning with EC certificates with a 384 bit key by-default or 256 bit key if configured.

Are you sure you want to continue? (y/n): y If specific AP list provisioning is preferred then use: 9800-L(config)#ap lsc-provision provision-list

Paso 6. Navegue hasta **Configuration > Interface > Wireless** y seleccione la interfaz de administración. En el campo **Trustpoint**, seleccione el nuevo punto de confianza en el menú desplegable y haga clic en **Update & Apply to Device**.

Precaución: Si LSC está habilitado pero el punto de confianza del WLC 9800 se refiere al MIC o a un SSC, los AP intentan unirse al LSC para el número configurado de intentos de unión. Una vez que se alcanza el límite máximo de intentos, los AP retornan a MIC y se unen nuevamente, pero dado que el aprovisionamiento de LSC está habilitado, los AP solicitan un nuevo LSC. Esto lleva a un loop donde el servidor de la CA firma constantemente los certificados para los mismos AP y los AP atascados en un loop de solicitud-reinicio de unión.

Nota: Una vez que el trustpoint de administración se actualiza para utilizar el certificado LSC, los nuevos AP no pueden unirse al controlador con el MIC. Actualmente no hay soporte para abrir una ventana de provisión. Si necesita instalar nuevos APs, deben ser aprovisionados previamente con un LSC firmado por la misma CA que el del punto de confianza de administración.

Edit Management Interface ✕

Interface Vlan2622 ▼

Trustpoint AP-LSC ✕ ▼

NAT Status DISABLED

↶ Cancel 📄 Update & Apply to Device

Configuración CLI para el paso seis:

```
9800-L(config)#wireless management trustpoint
```

Verificación

Verificar la instalación del certificado del controlador

Para verificar que la información de LSC está presente en el punto de confianza del WLC 9800 ejecute el comando **show crypto pki certificates verbose <nombre del punto de confianza>**, dos certificados están asociados al punto de confianza creado para el aprovisionamiento y la

inscripción de LSC. En este ejemplo, el nombre del punto de confianza es "microsoft-ca" (sólo se muestra el resultado relevante):

```
9800-L#show crypto pki certificates verbose microsoft-ca
```

Certificate

Status: Available

Version: 3

Certificate Usage: General Purpose

Issuer:

cn=CHUU-WIN12-CA

dc=chuu-domain

dc=local

Subject:

Name: 9800-L.alzavala.local

cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com

o=Wireless TAC

l=Juarez

st=CDMX

c=MX

hostname=9800-L.alzavala.local

CRL Distribution Points:

ldap:///CN=CHUU-WIN12-CA,CN=Chuu-

Win12,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Coint

Validity Date:

start date: 04:25:59 Central May 11 2020

end date: 04:25:59 Central May 11 2022 Subject Key Info: Public Key Algorithm: rsaEncryption RSA

Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption [...] Authority Info

Access: CA ISSUERS: ldap:///CN=CHUU-WIN12-

CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=chuu-

domain,DC=local?cACertificate?base?objectClass=certificationAuthority [...] **CA Certificate**

Status: Available

Version: 3

Certificate Serial Number (hex): 37268ED56080CB974EF3806CCACC77EC

Certificate Usage: Signature

Issuer:

cn=CHUU-WIN12-CA

dc=chuu-domain

dc=local

Subject:

cn=CHUU-WIN12-CA

dc=chuu-domain

dc=local

Validity Date:

start date: 05:58:01 Central May 10 2019

end date: 06:08:01 Central May 10 2024 Subject Key Info: Public Key Algorithm: rsaEncryption RSA

Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption

Verificación de la Configuración de 9800 WLC LSC

Para verificar los detalles sobre el trustpoint de administración inalámbrica ejecute el comando **show wireless management trustpoint**, asegúrese de que el trustpoint correcto (el que contiene los detalles de LSC, AP-LSC en este ejemplo) esté en uso y marcado como Disponible:

```
9800-L#show wireless management trustpoint
```

Trustpoint Name : AP-LSC

Certificate Info : Available

Certificate Type : LSC

Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb

Private key Info : Available

Para verificar los detalles sobre la configuración de aprovisionamiento de LSC de AP, junto con la lista de AP agregados a la lista de aprovisionamiento, ejecute el comando **show ap lsc-provision summary**. Asegúrese de que se muestra el estado de disposición correcto:

```
9800-L#show ap lsc-provision summary
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : AP-LSC
LSC Revert Count in AP reboots : 10
```

AP LSC Parameters :

```
Country : MX
State : CDMX
City : Juarez
Orgn : Cisco TAC
Dept : Wireless TAC
Email : josuvill@cisco.com
Key Size : 2048
EC Key Size : 384 bit
```

AP LSC-provision List :

```
Total number of APs in provision list: 2
```

Mac Addresses :

```
-----
xxxx.xxxx.xxxx
xxxx.xxxx.xxxx
```

Verificar la instalación del certificado del punto de acceso

Para verificar los certificados instalados en el AP ejecute el comando **show crypto** desde la CLI del AP, asegúrese de que tanto el certificado raíz de la CA como el certificado del dispositivo estén presentes (el resultado muestra sólo los datos relevantes):

```
AP3802#show crypto
```

```
[...]
```

```
----- LSC: Enabled
----- Device Certificate -----
```

Certificate:

Data:

```
Version: 3 (0x2)
Serial Number:
73:00:00:00:0b:9e:c4:2e:6c:e1:54:84:96:00:00:00:00:00:0b
```

Signature Algorithm: sha256WithRSAEncryption

Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA

Validity

Not Before: May 13 01:22:13 2020 GMT

Not After : May 13 01:22:13 2022 GMT

Subject: C=MX, ST=CDMX, L=Juarez, O=Cisco TAC, CN=ap3g3-286F7FCF53AC/emailAddress=josuvill@cisco.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

```
----- Root Certificate -----
```

Certificate:

Data:

```
Version: 3 (0x2)
```

```
Serial Number:
```

```
32:61:fb:93:a8:0a:4a:97:42:5b:5e:32:28:29:0d:32
Signature Algorithm: sha256WithRSAEncryption
Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
Validity
  Not Before: May 10 05:58:01 2019 GMT
  Not After : May 10 05:58:01 2024 GMT
Subject: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (2048 bit)
```

Si se utiliza LSC para la autenticación dot1x del puerto del switch, desde el AP puede verificar si la autenticación del puerto está habilitada.

```
AP3802#show ap authentication status
AP dot1x feature is disabled.
```

Nota: Para habilitar el puerto dot1x para los AP, es necesario definir las credenciales dot1x para los APs en el perfil AP o en la propia configuración AP con valores ficticios.

Troubleshoot

Problemas comunes

1. Si las plantillas no se asignan correctamente en el registro del servidor o si el servidor requiere desafío de contraseña, se rechaza la solicitud de certificado para el WLC 9800 o los AP.
2. Si los sitios predeterminados de IIS están inhabilitados, el servicio SCEP también está inhabilitado, por lo tanto la URL definida en el punto de confianza no es accesible y el WLC 9800 no envía ninguna solicitud de certificado.
3. Si el tiempo no se sincroniza entre el servidor y el WLC 9800, los certificados no se instalan porque falla la verificación de validez de tiempo.

Comandos Debug y Log

Utilice estos comandos para resolver problemas de inscripción de certificados del controlador 9800:

```
9800-L#debug crypto pki transactions
9800-L#debug crypto pki validation
9800-L#debug crypto pki scep
```

Para resolver problemas y monitorear la inscripción de AP utilice estos comandos:

```
AP3802#debug capwap client payload
AP3802#debug capwap client events
```

Desde la línea de comandos AP, **show logging** muestra si el AP tuvo problemas con la instalación del certificado y proporciona detalles sobre el motivo por el cual el certificado no fue instalado:

[...]

```
Mar 19 19:39:13 kernel: *03/19/2020 19:39:13.3429] AP has joined controller 9800-L Mar 19
```

```
19:39:13 kernel: 03/19/2020 19:39:13.3500] SELinux: initialized (dev mtd_inodefs, type
mtd_inodefs), not configured for labeling Mar 19 19:39:13 kernel: *03/19/2020 19:39:13.5982]
Generating a RSA private key Mar 19 19:39:14 kernel: *03/19/2020 19:39:13.5989]
..... Mar 19 19:39:15 kernel: *03/19/2020 19:39:14.4179] .. Mar 19 19:39:15
kernel: *03/19/2020 19:39:15.2952] writing new private key to '/tmp/lsc/priv_key' Mar 19
19:39:15 kernel: *03/19/2020 19:39:15.2955] ----- Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5421] cen_validate_lsc: Verification failed for certificate: Mar 19 19:39:15 kernel:
*03/19/2020 19:39:15.5421] countryName = MX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421]
stateOrProvinceName = CDMX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] localityName =
Juarez Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] organizationName = cisco-tac Mar 19
19:39:15 kernel: *03/19/2020 19:39:15.5421] commonName = ap3g3- Mar 19 19:39:15 kernel:
*03/19/2020 19:39:15.5421] emailAddress = jesuherr@cisco.com Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5427] LSC certificates/key failed validation! Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5427]
```

Ejemplo de un Intento de Inscripción Satisfactorio

Este es el resultado de los debugs antes mencionados para una inscripción exitosa tanto para el controlador como para sus AP asociados.

Importación de certificado raíz de CA al WLC 9800:

[...]

```
Certificate has the following attributes: Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224
Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B % Do you accept this certificate?
[yes/no]: yes CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA
Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-
LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8
CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened
CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0
(compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC,
refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length
received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length :
(3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0
CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert
Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:47:34 GMT Connection:
close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates.
CRYPTO_PKI_SCEP: Client received CA and RA certificate
CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3
certificates. CRYPTO_PKI:crypto_pkcs7_extract_ca_cert found cert CRYPTO_PKI: Bypassing SCEP
capabilities request 0 CRYPTO_PKI: transaction CRYPTO_REQ_CA_CERT completed CRYPTO_PKI: CA
certificate received. CRYPTO_PKI: CA certificate received. CRYPTO_PKI:
crypto_pki_get_cert_record_by_cert() CRYPTO_PKI: crypto_pki_authenticate_tp_cert() CRYPTO_PKI:
trustpoint AP-LSC authentication status = 0 Trustpoint CA certificate accepted.
```

Inscripción de dispositivo WLC 9800:

[...]

```
CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI_SCEP: Client sending GetCACert
request CRYPTO_PKI: Sending CA Certificate Request: GET
/certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent:
Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint
AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message
CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco
PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked
trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse
content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data
arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-
By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 3638 Content-
Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and
```

RA certificate CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI_SCEP: Client Sending GetCACaps request with msg = GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACaps&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 171 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (34) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: text/plain Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 34 CRYPTO_PKI: HTTP header content length is 34 bytes CRYPTO_PKI_SCEP: Server returned capabilities: 92 CA_CAP_RENEWAL CA_CAP_S alz_9800(config)#HA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: %PKI-6-CSR_FINGERPRINT: CSR Fingerprint MD5 : 9BFBA438303487562E888087168F05D4 CSR Fingerprint SHA1: 58DC7DB84C632A7307631A97A6ABCF65A3DEFEEF CRYPTO_PKI: Certificate Request Fingerprint MD5: 9BFBA438 30348756 2E888087 168F05D4 CRYPTO_PKI: Certificate Request Fingerprint SHA1: 58DC7DB8 4C632A73 07631A97 A6ABCF65 A3DEFEEF PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 0F 0E 00 00 00 00 38 CRYPTO_PKI: Deleting cached key having key id 65 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 66 CRYPTO_PKI: Expiring peer's cached key with key id 66 PKI: Trustpoint AP-LSC has no router cert PKI: Signing pkcs7 with AP-LSC trustpoint temp self-signed cert CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (2807) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: received msg of 2995 bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 2807 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI: Deleting cached key having key id 66 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 67 CRYPTO_PKI: Expiring peer's cached key with key id 67 CRYPTO_PKI: Remove global revocation service providers The PKCS #7 message has 1 verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO_PKI_SCEP: Client received CertRep - GRANTED (AF58BA9313638026C5DC151AF474723F) CRYPTO_PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Newly-issued Router Cert: issuer=cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial=1800043245DC93E1D943CA70000043 start date: 21:38:34 Central May 19 2020 end date: 21:38:34 Central May 19 2022 Router date: 21:48:35 Central May 19 2020 %PKI-6-CERT_INSTALL: An ID certificate has been installed under Trustpoint : AP-LSC Issuer-name : cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local Subject-name : cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com,o=Wireless TAC,l=Juarez,st=CDMX,c=MX,hostname=alz_9800.alzavala.local Serial-number: 1800000043245DC93E1D943CA7000000000043 End-date : 2022-05-19T21:38:34Z Received router cert from CA CRYPTO_PKI: Not adding alz_9800.alzavala.local to subject-alt-name field because : Character allowed in the domain name. Calling pkiSendCertInstallTrap to send alert CRYPTO_PKI: All enrollment requests completed for trustpoint AP-LSC

Salida de depuración de inscripción AP desde el lado del controlador, esta salida se repite varias veces para cada AP que se une al 9800 WLC:

[...]

CRYPTO_PKI: (A6964) Session started - identity selected (AP-LSC) CRYPTO_PKI: Doing re-auth to fetch RA certificate. CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC,

refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and RA certificate CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI: Capabilities already obtained CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 PKCS10 request is compulsory CRYPTO_PKI: byte 2 in key usage in PKCS#10 is 0x5 May 19 21: alz_9800(config)#51:04.985: CRYPTO_PKI: all usage CRYPTO_PKI: key_usage is 4 CRYPTO_PKI: creating trustpoint clone Proxy-AP-LSC8 CRYPTO_PKI: Creating proxy trustpoint Proxy-AP-LSC8 CRYPTO_PKI: Proxy enrollment request trans id = 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: Proxy forwarding an enrollment request CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI: Proxy send CA enrollment request with trans id: 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: No need to re-auth as we have RA in place CRYPTO_PKI: Capabilities already obtained CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 0F 0E 00 00 00 00 00 38 CRYPTO_PKI: Deleting cached key having key id 67 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 68 CRYPTO_PKI: Expiring peer's cached key with key id 68 PKI: Trustpoint Proxy-AP-LSC8 has no router cert and loaded PKI: Signing pkcs7 with Proxy-AP-LSC8 trustpoint temp self-signed cert CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 3 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (2727) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: received msg of 2915 bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 2727 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI: Deleting cached key having key id 68 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 69 CRYPTO_PKI: Expiring peer's cached key with key id 69 CRYPTO_PKI: Remove global revocation service providers The PKCS #7 message has 1 alz_9800(config)# verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO_PKI_SCEP: Client received CertRep - GRANTED (7CBB299A2D9BC77DBB1A8716E6474C0C) CRYPTO_PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Received router cert from CA CRYPTO_PKI: Enrollment poroxy callback status: CERT_REQ_GRANTED CRYPTO_PKI: Proxy received router cert from CA CRYPTO_PKI: Rcvd request to end PKI session A6964. CRYPTO_PKI: PKI session A6964 has ended. Freeing all resources. CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Cleaning RA certificate for TP : AP-LSC CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_CS: removing trustpoint clone Proxy-AP-LSC8

Salida de depuración de inscripción AP del lado AP:

```
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 40 len 407
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: CERTIFICATE_PARAMETER_PAYLOAD(63) vendId 409600
LSC set retry number from WLC: 1
```

```
Generating a RSA private key
...
.....
writing new private key to '/tmp/lsc/priv_key'
```

```
-----
[ENC] CAPWAP_WTP_EVENT_REQUEST(9)
```

```
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) Len 1135 Total 1135
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 41 len 20
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_CERT_ENROLL_PENDING from WLC
```

```
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
Received Capwap watchdog update msg.
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 42 len 1277
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_ENABLE: saving ROOT_CERT
```

```
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 43 len 2233
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_ENABLE: saving DEVICE_CERT
```

SC private key written to hardware TAM

root: 2: LSC enabled

AP Rebooting: Reset Reason - LSC enabled

Esto concluye el ejemplo de configuración para la inscripción LSC a través de SCEP.