Localmente - Certificados significativos en el ejemplo inalámbrico de la configuración de los reguladores LAN

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Localmente - Certificados significativos
Aprovisionamiento del certificado en los reguladores inalámbricos LAN (WLCs)
Aprovisionamiento del certificado en LWAPP AP
Ayuda LSC en los reguladores inalámbricos LAN (WLCs) y los Puntos de acceso ligeros (revestimientos)
Configurar
Configuración de la red
Proceso de configuración CA y SCEP
Configure el regulador LAN de la Tecnología inalámbrica a través del GUI
Configure el regulador LAN de la Tecnología inalámbrica con el CLI
Verificación
Troubleshooting
Información Relacionada

Introducción

Este documento explica cómo configurar el regulador LAN de la Tecnología inalámbrica (WLC) y los Puntos de acceso ligeros (revestimientos) para utilizar localmente - la característica significativa del certificado. Esta función se introduce con la versión 5.2 del Controlador de LAN Inalámbrico. Con esta característica, si usted elige controlar el Public Key Infrastructure (PKI), usted puede generar localmente - los Certificados significativos (LSC) en los Puntos de acceso y los reguladores. Estos Certificados se pueden entonces utilizar para autenticar mutuamente el WLC y PARA TRASLAPAR.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el WLC, el REVESTIMIENTO, y el indicador luminoso LED amarillo de la placa muestra gravedad menor del cliente de red inalámbrica para la operación básica
- Conocimiento de cómo configurar y utilizar el servidor de Microsoft Windows 2003 CA
- Conocimiento de la infraestructura y de los Certificados digitales de la clave pública

Componentes Utilizados

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

- Cisco 4400 Series WLC que funciona con los firmwares 5.2
- Punto de acceso ligero del Cisco Aironet de la serie 1130 AG (REVESTIMIENTO)
- Servidor de Microsoft Windows 2003 configurado como regulador del dominio, y como servidor de la autoridad de certificación.
- Adaptador del cliente del 802.11 a/b/g de Cisco Aironet que funciona con la versión 4.2 de los firmwares
- Cisco utilidad Aironet Desktop (ADU) esa versión de firmware 4.2 de los funcionamientos

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Localmente - Certificados significativos

En las versiones de software del regulador anterior que 5.2.157.0, el regulador puede utilizar los certificados autofirmados (SSCs) para autenticar los Puntos de acceso o para enviar la información de autorización a un servidor de RADIUS, si los Puntos de acceso fabricación-han instalado los Certificados (MICs). En la versión de software 5.2.157.0 del regulador, usted puede configurar el regulador para utilizar un certificado significativo local (LSC). Usted puede utilizar un LSC si usted quisiera que su propio Public Key Infrastructure (PKI) proporcionara a una mejor Seguridad; para tener control de su Certificate Authority (CA), y definir las directivas, las restricciones, y los usos en los Certificados generados.

El nuevo LSC certifica las necesidades primero y después de provisioned en el regulador el REVESTIMIENTO del servidor del Certificate Authority (CA).

El REVESTIMIENTO comunica con el regulador (WLC) con el protocolo CAPWAP. Cualquier petición de firmar el certificado y de publicar los Certificados CA para el REVESTIMIENTO y para el WLC sí mismo, se debe iniciar del WLC. El REVESTIMIENTO no comunica directamente con el servidor CA. El WLC se comporta como Ca-proxy al AP del LWAPP. Los detalles del servidor CA se deben configurar en el WLC, y debe ser accesible.

El regulador hace uso del protocolo simple certificate enrollment (SCEP) para remitir los certReqs

generados en los dispositivos al CA y hace uso de SCEP otra vez para conseguir los certificados firmados del CA.

SCEP es un protocolo de la Administración de certificado que los clientes del Public Key Infrastructure (PKI) y los servidores de la autoridad de certificación utilizan para utilizar la inscripción del certificado y la revocación. Es ampliamente utilizado en Cisco y es utilizado por muchos Ca-servidores. En el protocolo SCEP, el HTTP se utiliza como el Transport Protocol para los mensajes PKI. El objetivo principal de SCEP es la emisión segura de los Certificados a los dispositivos de red. SCEP es capaz de muchas operaciones, pero para este proyecto y versión, SCEP se utiliza para estas operaciones.

- Distribución de la clave pública CA y del RA
- Inscripción del certificado

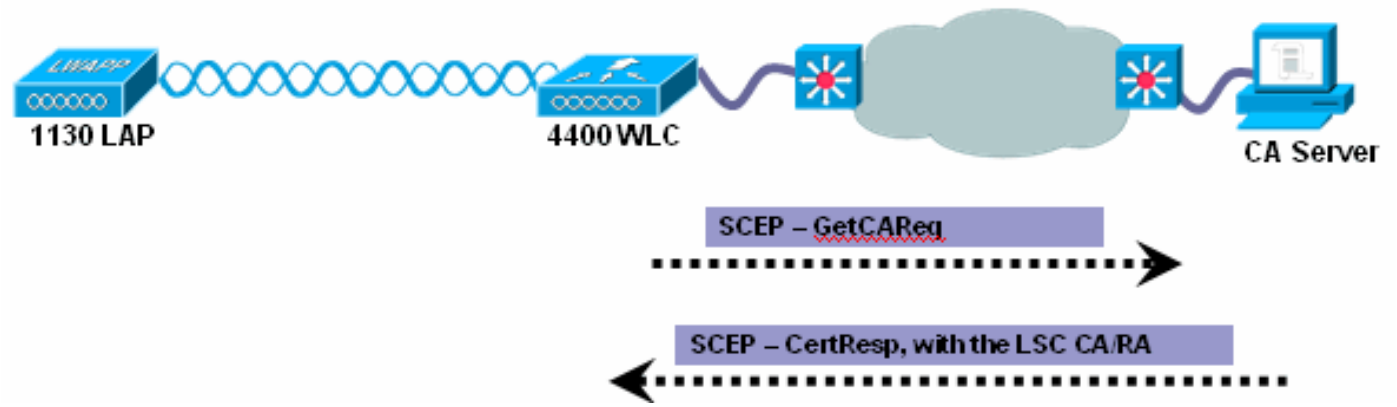
Todas las transacciones SCEP suceden en el Modo automático. La revocación de certificado no se utiliza.

Nota: Los LSC no se utilizan en los Puntos de acceso que se configuran para el modo del puente.

Aprovisionamiento del certificado en los reguladores inalámbricos LAN (WLCs)

Los nuevos Certificados LSC, el CA y los Certificados del dispositivo se deben instalar en el regulador.

Con el protocolo SCEP, los Certificados CA se reciben del servidor CA. Desde a este punto, no hay Certificados presentes en el regulador, esta operación está un claro consigue la operación. Éstos están instalados en el regulador. Estos mismos Certificados CA también se empujan a los APs cuando los APs provisioned con los LSC.



Operación de la inscripción del certificado del dispositivo

Para el REVESTIMIENTO y el regulador que pide un certificado firmado CA, el más certRequest se envía como mensaje PKCS#10. El más certRequest contiene el asunto, PublicKey y otros atributos que se incluirán en el certificado X.509, y firmados digitalmente por el PrivateKey del solicitante. Éstos se deben enviar al CA, que transforma el más certRequest en un certificado X.509.

El CA que recibe un PKCS#10 más certRequest requiere la información adicional autenticar la identidad del solicitante y verificar que la petición es inalterada. Muchas veces PKCS#10 combinadas con otros acercamientos, tales como PKCS-7, para enviar y para recibir el CERT Reqs/Resps.

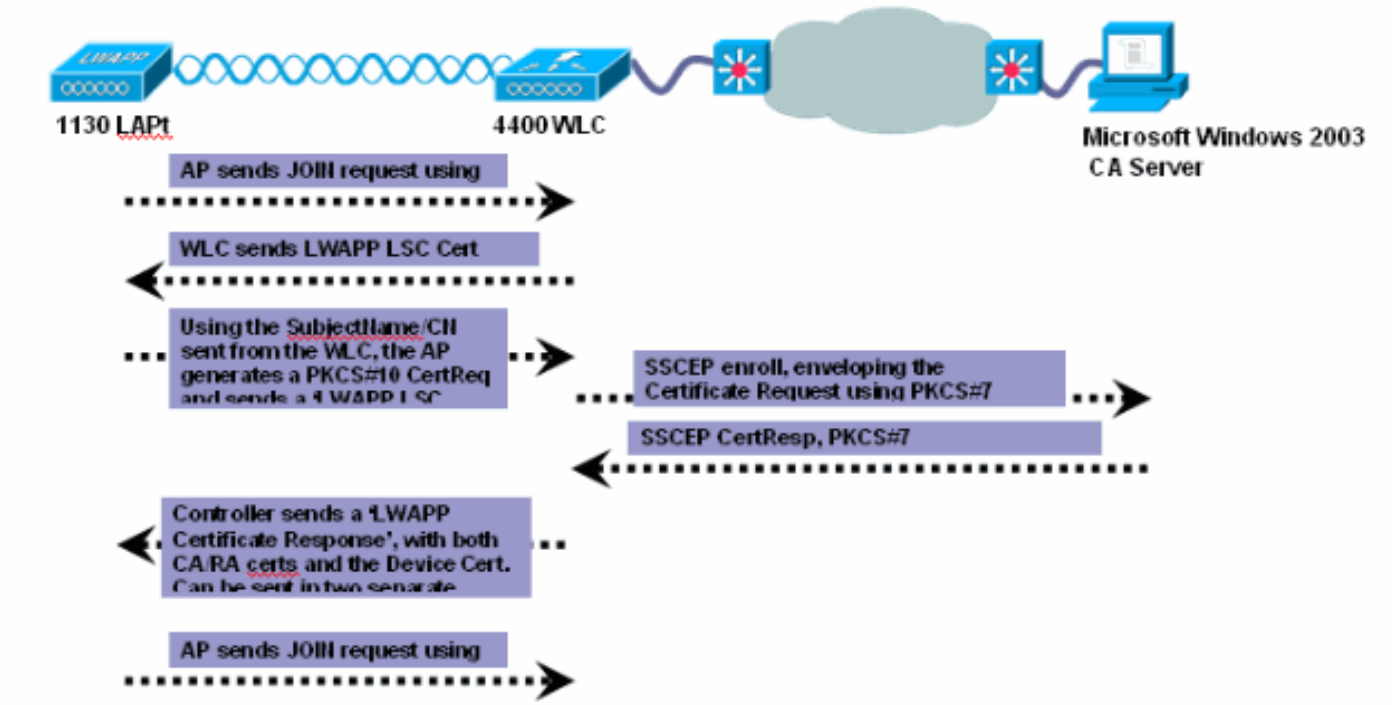
Aquí, el PKCS#10 se envuelve en PKCS-7 un Tipo de mensaje de SignedData. Esto se utiliza como parte de la funcionalidad del cliente SCEP, mientras que el mensaje de PKCSReq se envía al regulador.

Sobre la operación acertada de la inscripción, el CA y el certificado del dispositivo están presentes ahora en el regulador.

Aprovisionamiento del certificado en LWAPP AP

Para que un nuevo certificado provisioned en el REVESTIMIENTO, mientras que en el modo CAPWAP el REVESTIMIENTO debe poder conseguir el nuevo certificado firmado X.509. Para hacer esto, envía un la más certRequest al regulador, que actúa como Ca-proxy y las ayudas obtienen el más certRequest firmada por el CA para el REVESTIMIENTO.

El certReq y los certResponses se envían al REVESTIMIENTO con las cargas útiles LWAPP. Este diagrama muestra el flujo para que el REVESTIMIENTO provision un LSC.



Aquí están los pasos detalladamente:

1. El aprovisionamiento del REVESTIMIENTO con LSC más nuevos sucede una vez que el REVESTIMIENTO está en el estado ASCENDENTE, después de que SE HAYA UNIDO Al WLC con su MIC/SSC actual. En la fase del aprovisionamiento LSC, aunque el AP está en el estado ASCENDENTE, las radios se cierran fuertemente.
2. El uso y la disposición del LSC se deben activar en el WLC. Este proceso incluye para activar el LSC, para agregar el servidor CA, y para configurar otros parámetros. Los parámetros de un certificado LSC ordenan la petición se envían del regulador PARA TRASLAPAR, con el tema-nombre, el tiempo de la validez y Keysize fijado en el payload. Estos campos son utilizados por el REVESTIMIENTO cuando se crea el más certRequest. El payload también indica que el REVESTIMIENTO debe crear un la más certRequest y enviarlo de nuevo al regulador.
3. El REVESTIMIENTO genera configurado keysize el par clave público/privado RSA. Después de la generación del keypair, se configura un la más certRequest se genera después del

SubjectName recibido del regulador. El NC autogenerated con el formato existente SSC/MIC, “Cxxxx-EtherMacAddr”. El REVESTIMIENTO genera un PKCS#10 CertReq y lo envía como payload, solicitud de certificado LSC, al regulador.

4. El regulador entonces crea un mensaje SSCEP PKCSReq, PKCS-7 un mensaje formateado, y lo envía al CA en nombre del: TRASLAPE, para conseguir la solicitud de certificado firmada por el CA configurado. Los certs instalados CA/RA se utilizan para cifrar el certReq.
5. Si el CA puede aprobar la solicitud de certificado, un mensaje de CertRep con Status=SUCCESS se devuelve al cliente SSCEP (regulador) en PKCS-7 un formato. La respuesta CERT se escribe localmente en un fichero como certificado del formato PEM.
6. Puesto que este CertResp está para el REVESTIMIENTO, WLC envía el certificado al REVESTIMIENTO con un payload “respuesta del certificado”. El CERT CA se envía primero con el mismo payload, después el certificado del dispositivo se envía en un payload separado.

El LSC CA y los Certificados del dispositivo del REVESTIMIENTO están instalados en el REVESTIMIENTO, y las uno mismo-reinicializaciones del sistema. La próxima vez que sube, puesto que se configura para utilizar los LSC, el AP envía el certificado del dispositivo LSC al regulador como parte de la petición del UNIDO. Como parte de la respuesta del UNIDO, el regulador envía su nuevo certificado del dispositivo y también valida el certificado entrante del REVESTIMIENTO con el nuevo certificado raíz CA.

Nota: Los LSC no se utilizan en los Puntos de acceso que se configuran para el modo del puente.

Ayuda LSC en los reguladores inalámbricos LAN (WLCs) y los Puntos de acceso ligeros (revestimientos)

El LSC se utiliza en estas Plataformas WLC:

- Cisco Wireless LAN Controllers de la serie 4400
- Cisco 2100 Series Wireless LAN Controllers
- Módulo de Servicios inalámbricos de las Cisco Catalyst 6500 Series (WiSM)
- Regulador integrado LAN de la Tecnología inalámbrica del Cisco Catalyst 3750G
- Cisco Wireless LAN Controller Module

El LSC se utiliza en Cisco los Puntos de acceso C1130, C1140, C1240, C1252 de Aironet y cualquier nuevo Punto de acceso.

El LSC no se utiliza en la MALLA AP (1510, 1522), el modo AP del puente.

Este documento explica con un ejemplo de la configuración, cómo activar y autenticar los revestimientos con localmente - los Certificados significativos.

Configurar

Nota: Localmente - la característica significativa del certificado se puede activar con el GUI o el CLI en el regulador.

Nota: La característica LSC en un regulador no toma el desafío de la contraseña. Por lo tanto, para que el LSC trabaje, usted debe inhabilitar el desafío de la contraseña en el servidor CA. También, usted no puede utilizar el servidor 2008 de Microsoft Windows como servidor CA porque no es posible inhabilitar el desafío de la contraseña en él.

Configuración de la red

En este ejemplo, usted configura un regulador LAN de 4400 Tecnologías inalámbricas y un Punto de acceso ligero de las 1130 Series para utilizar localmente - los Certificados significativos (LSC). Para lograr esto, usted debe provision el regulador LAN de la Tecnología inalámbrica y el REVESTIMIENTO con los LSC del servidor del Certificate Authority (CA).

Este documento utiliza el servidor de Microsoft Windows 2003 como el servidor CA.

Proceso de configuración CA y SCEP

El documento asume que la Configuración del servidor CA en el servidor de Microsoft Windows 2003 existe. Aquí está el resumen de los pasos para el proceso de configuración CA y SCEP:

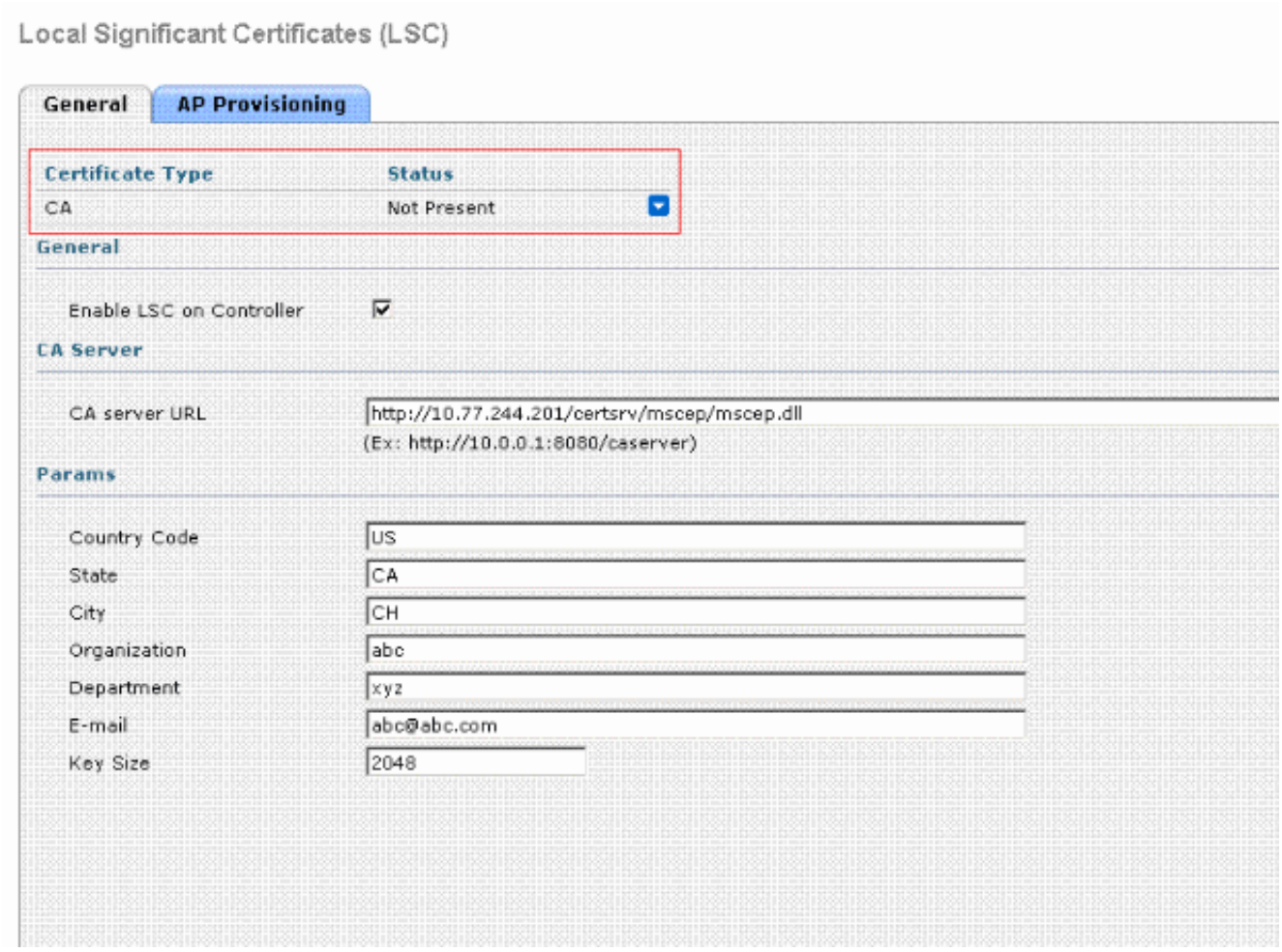
1. La disposición Windows 2003 y el servidor CA, se aseguran del trabajo de *http://ca-server/certsrv*
2. Transferencia directa *cepsetup.exe del* sitio Web de Microsoft
3. Instale cepsetup.exe, uncheck “la *frase del desafío de* RequireSCEP*”,* puesto que WLC no podría utilizar el desafío ahora alista el modo.
4. Proporcione al nombre, al correo electrónico, al país, a la ciudad y a los otros detalles.
5. Asegure los trabajos de *http://ca-server/certsrv/mscep/mscep.dll* como se esperaba.

Nota: Usted necesitará crear una cuenta de usuario, asignarla lea y aliste los permisos para la plantilla de IPSec (petición offline), y hágale a un miembro del grupo IIS_WPG. Para los detalles completos refiera al sitio Web de Microsoft para instalar y configurar SCEP

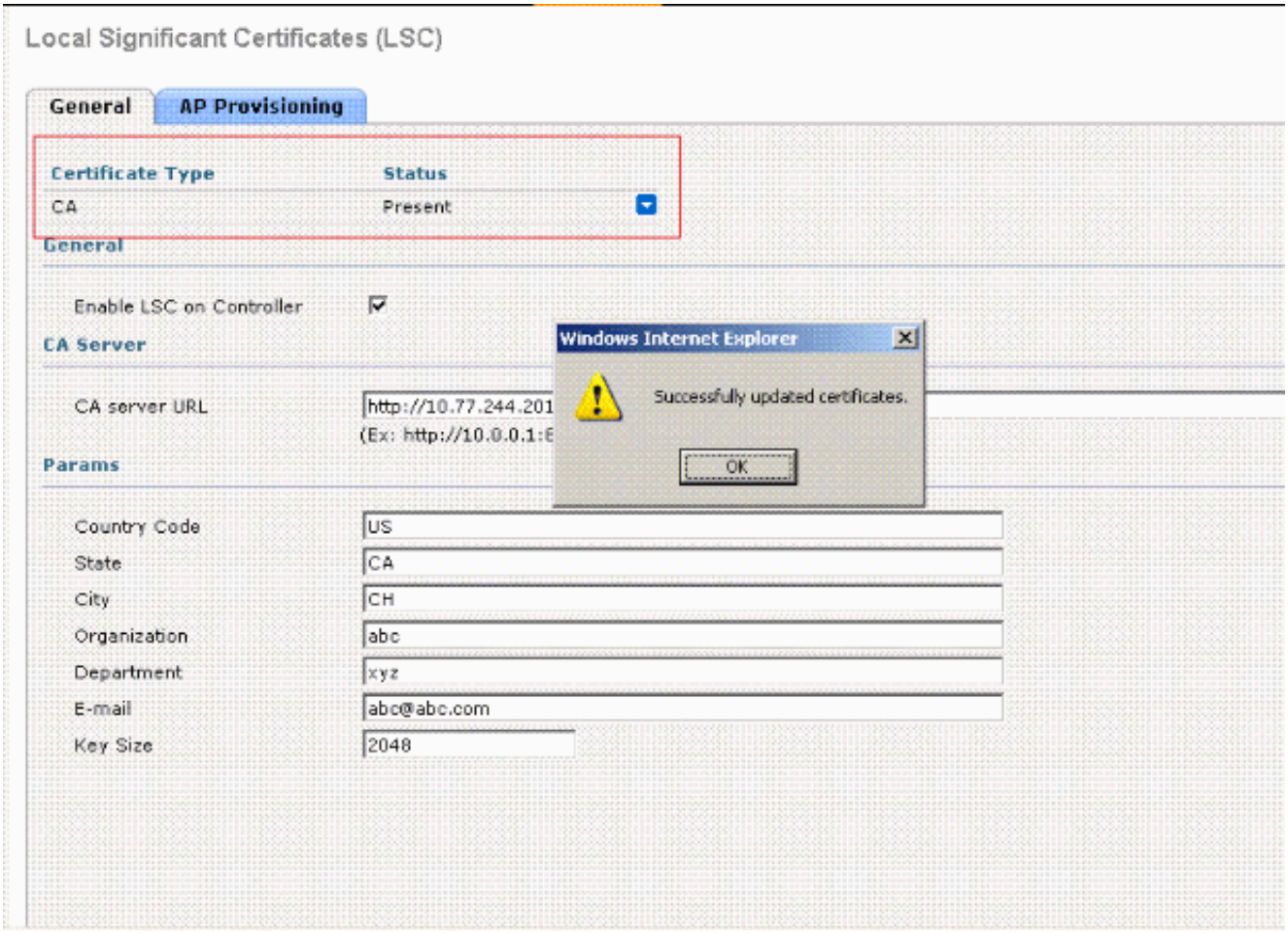
Configure el regulador LAN de la Tecnología inalámbrica a través del GUI

Complete estos pasos:

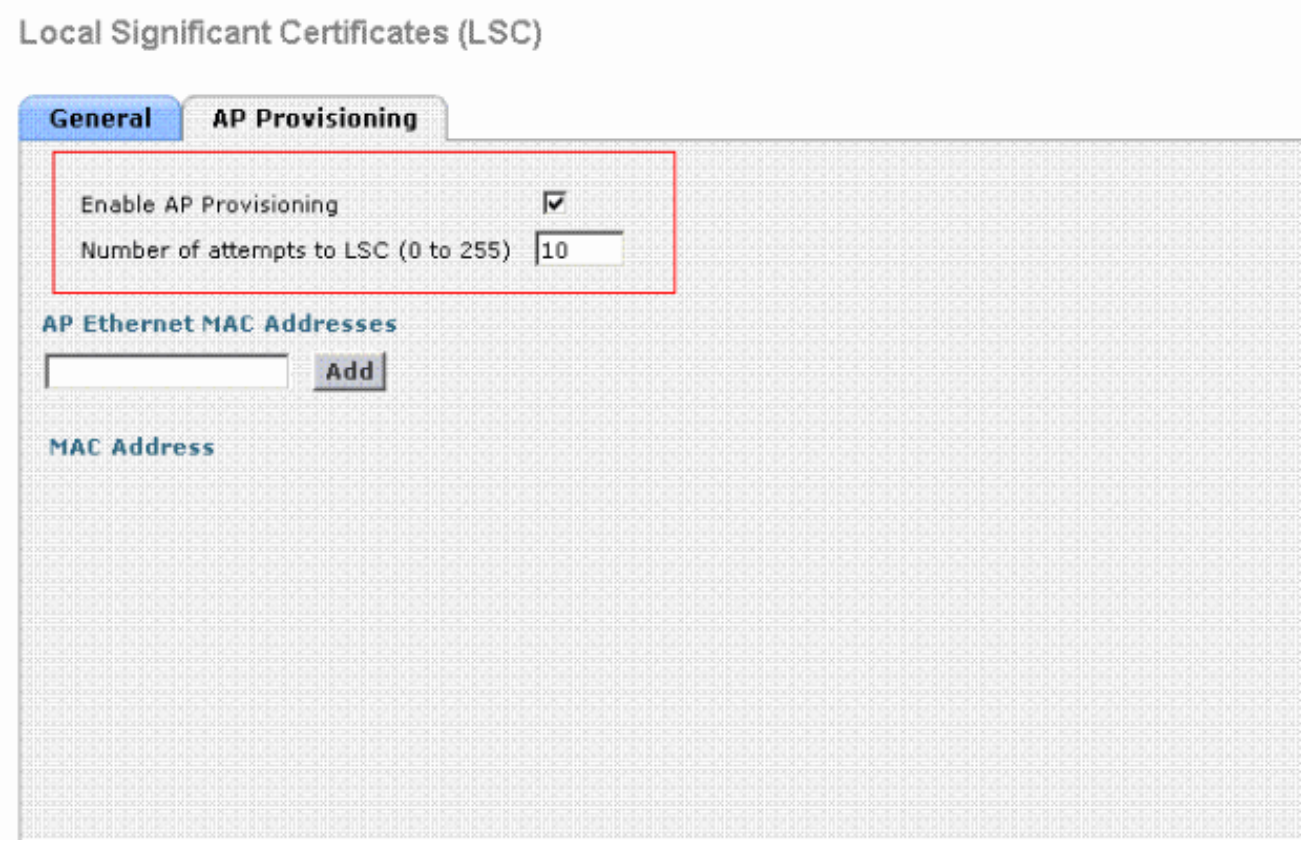
1. Del GUI del regulador LAN de la Tecnología inalámbrica, haga clic la **Seguridad > el certificado > el LSC** para abrir la página significativa local de los Certificados (LSC).
2. Haga clic la **ficha general**.
3. Para activar el LSC en el sistema, controle el **permiso LSC en la** casilla de verificación del **regulador**.
4. En el campo URL del servidor CA, ingrese el URL al servidor CA. Usted puede ingresar un Domain Name o un IP address.
5. En los campos de los Params, ingrese los parámetros para el certificado del dispositivo. El tamaño de clave es un valor a partir del 384 a 2048 (en los bits), y el valor predeterminado es 2048.
6. Haga clic en Apply para aplicar sus cambios.



7. Para agregar el certificado CA en la base de datos del certificado CA del regulador, asomar su cursor sobre la flecha desplegable azul para el tipo de certificado, y elegir **agregue**. Aquí está un
ejemplo.



8. Para provision el LSC en el Punto de acceso, hacer clic la tabulación del **aprovisionamiento AP**, y controlar la casilla de verificación del **aprovisionamiento del permiso AP**.
9. Para agregar los Puntos de acceso a la lista de la disposición, ingresar el MAC address del Punto de acceso en el campo y el tecleo de direccionamientos del MAC Ethernet AP **agregue**. Para quitar un Punto de acceso de la lista de la disposición, asomar su cursor sobre la flecha desplegable azul para el Punto de acceso, y elegir **quita**.Si usted configura una lista de la disposición del Punto de acceso, sólo los Puntos de acceso en la lista de la disposición provisioned cuando usted activa el aprovisionamiento AP. Si usted no configura una lista de la disposición del Punto de acceso, todos los Puntos de acceso con un certificado MIC o de SSC que se unen al regulador son LSC provisioned.
10. Haga clic en Apply para aplicar sus cambios.



Configure el regulador LAN de la Tecnología inalámbrica con el CLI

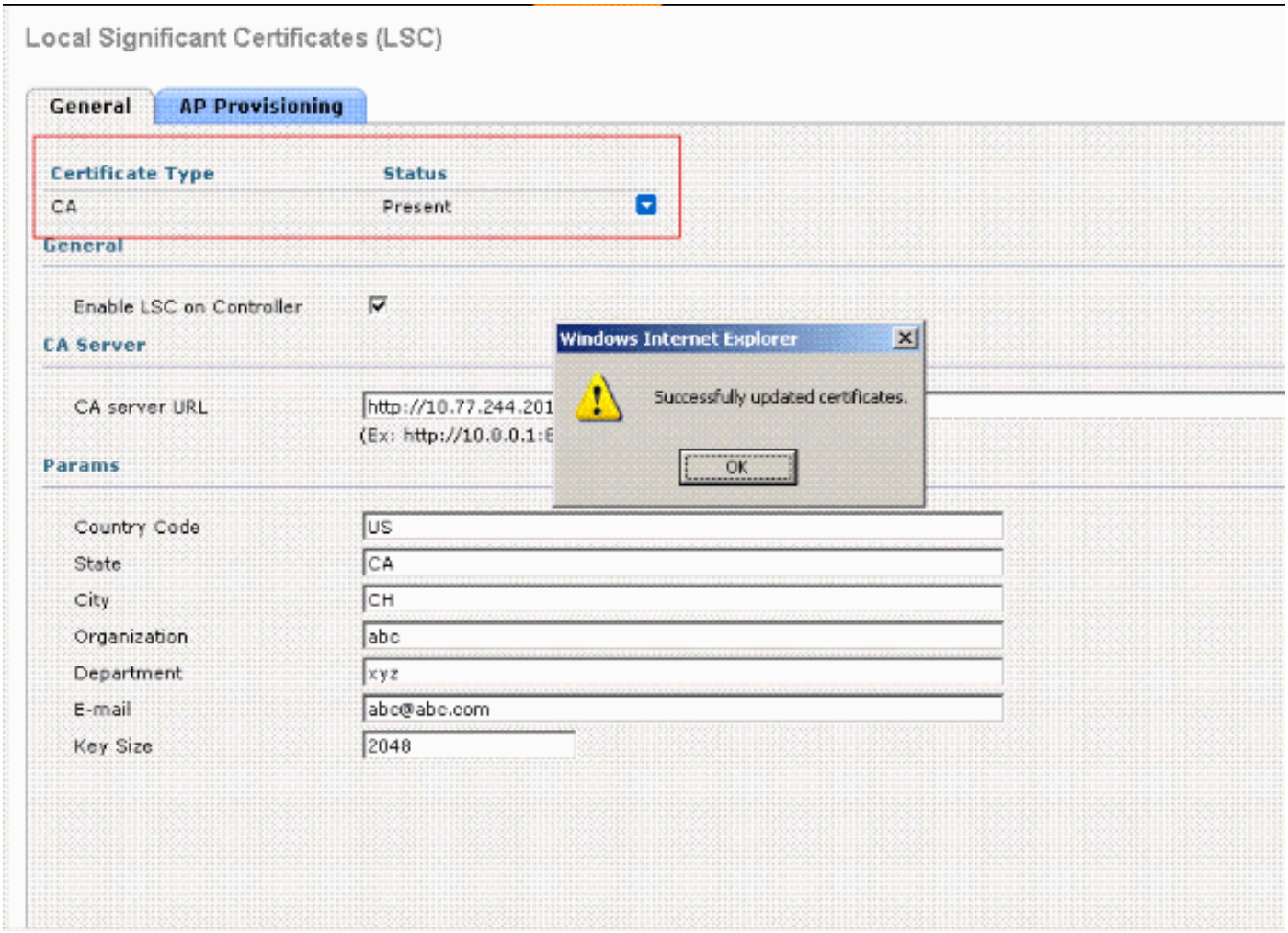
Refiera a **usar el CLI para configurar la** sección **LSC de la** guía de configuración inalámbrica del regulador LAN de Cisco, publique 5.2 para la información sobre el procedimiento para activar localmente - la característica significativa del certificado (LSC) del CLI en el regulador.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice el OIT para ver un análisis de la **salida del comando show**.

Una vez que se configura el regulador LAN de la Tecnología inalámbrica y el servidor CA existe, el regulador LAN de la Tecnología inalámbrica utiliza el protocolo SCEP para comunicar con el servidor CA y adquirir el certificado LSC. Aquí está un tiro de pantalla del WLC una vez que el certificado está instalado.



Cuando sube el REVESTIMIENTO, el REVESTIMIENTO descubre el WLC con la capa los mecanismos del descubrimiento de 2 capas 3 y envía las peticiones de un unido al regulador con el certificado MIC.

El regulador LAN de la Tecnología inalámbrica entonces envía el pedido del parámetro del certificado LSC al REVESTIMIENTO.

Con el SubjectName/CN enviado del WLC, el AP genera PKCS #10 CertReq y envía una “solicitud de certificado LWAPP LSC” al WLC.

Esta petición a su vez es remitida por el WLC al servidor CA. El servidor CA envía el certificado del REVESTIMIENTO LSC al regulador. El regulador entonces envía el LSC al REVESTIMIENTO.

Este mensaje aparece en el AP CLI.

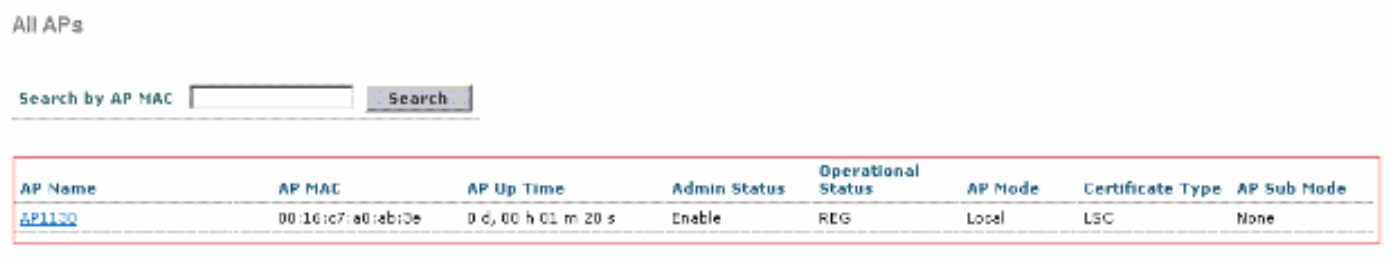
```
The name for the keys will be: Cisco_IOS_LSC_Keys

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
LSC CA cert successfully imported
LSC device cert successfully imported
```

Finalmente, el REVESTIMIENTO envía una petición del unido con el LSC.

Publique el **comando enable de los eventos del capwap de la depuración** para ver esta Secuencia de eventos.

El REVESTIMIENTO se registra una vez con el WLC con el LSC, usted puede confirmar esto en el GUI WLC.



Usted puede también utilizar estos comandos del WLC CLI para verificar esto. Aquí tiene un ejemplo:

```
show certificate lsc summary
Information similar to the following appears:
LSC Enabled..................................... Yes
LSC CA-Server..................................... http://10.77.244.201:8080/caserver

LSC AP-Provisioning............................... Yes
Provision-List.................................. Not Configured
LSC Revert Count in AP reboots.................. 3

LSC Params:
Country..................................... 4
State....................................... ca
City........................................ ch
Orgn........................................ abc
Dept........................................ xyz
Email....................................... abc@abc.com
KeySize..................................... 2048

LSC Certs:
CA Cert..................................... Not Configured
RA Cert..................................... Not Configured
```

Para ver los detalles sobre los Puntos de acceso que provisioned con el LSC, ingrese este comando:

```
show certificate lsc ap-provision
Information similar to the following appears:
LSC AP-Provisioning.......................... Yes
Provision-List............................... Present

IdxMac Address
---------------
100:18:74:c7:c0:90
```

Troubleshooting

Esta sección explica cómo resolver problemas su configuración. Usted puede utilizar el **comando enable del scep del pki de la depuración P.M.** para ver la Secuencia de eventos.

Aquí está un ejemplo de un registro acertado de la depuración:

Success log:

WLC

(Cisco Controller) >

scep: waiting for 10 secsmLscScepTask: Nov 23 06:52:21.455:
scep: : Nov 23 06:52:27.519:

===== SCEP_OPERATION_GETCAPS =====
scep: Failed to get SCEP Capabilities from CA. Some CA's do not support this.
scep: Getting CA Certificate(s).
scep: : Nov 23 06:52:27.519:

===== SCEP_OPERATION_GETCA =====
scep: requesting CA certificate

scep: Sent 82 byteseded: Operation now in progress*emWeb: Nov 23 06:52:27.526:
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.
scep: header info: <Connection: close>
scep: header info: <Date: Wed, 23 Nov 2011 06:52:30 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 3795>
scep: header info: <Content-Type: application/x-x509-ca-ra-cert>
scep: MIME header: application/x-x509-ca-ra-cert
scep: found certificate:
  subject: /DC=com/DC=ccie/CN=AD
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature, Certificate Sign, CRL Sign
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Key Encipherment
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature
scep: CA cert retrieved with fingerprint 639993FF7FF8FB12EF2FB09DEC7C5BED

scep: waiting for 10 secs 06:52:34.463:

AP
(Cisco Controller) >
scep: waiting for 10 secsmLscScepTask: Nov 23 06:52:47.471:
scep: waiting for 10 secs 06:53:00.479:
scep: AP MAC: 58:bc:27:13:4a:d0 Starting new enrollment request.
scep: creating inner PKCS#7:01.542:
scep: data payload size: 797 bytes:
scep: successfully encrypted payload
scep: envelope size: 1094 bytes545:
scep: Sender Nonce before send: 089AC8C4604FCEB10C1F30E045073B10
scep: creating outer PKCS#7:01.545:
scep: signature added successfully:
scep: adding signed attributes.545:
scep: adding string attribute transId
scep: adding string attribute messageType
scep: adding octet attribute senderNonce
scep: PKCS#7 data written successfully
scep: applying base64 encoding.565:
scep: base64 encoded payload size: 3401 bytes

```
scep: Sent 3646 bytesed: Operation now in progress*sshpmLscTask: Nov 23 06:53:01.613:
scep: SenderNonce in reply: BF4EE64D4169584D90B2502ECCC0C133
scep: recipientNonce in reply: 089AC8C4604FCEB10C1F30E045073B10
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.:
scep: header info: <Connection: close>:
scep: header info: <Date: Wed, 23 Nov 2011 06:53:02 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 2549>
scep: header info: <Content-Type: application/x-pki-message>
scep: MIME header: application/x-pki-message

scep: reading outer PKCS#706:53:13.488:
scep: PKCS#7 payload size: 2549 bytes8:
scep: PKCS#7 contains 2023 bytes of enveloped data
scep: verifying signature 06:53:13.489:
scep: signature ok Nov 23 06:53:13.490:
scep: finding signed attributes:13.490:
scep: finding attribute transId:13.490:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: A984A2DFE20DA7E0FE702DC8EC307F33
scep: finding attribute messageType490:
scep: allocating 1 bytes for attribute.
scep: reply message type is good13.490:
scep: finding attribute senderNonce490:
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus3.491:
scep: allocating 1 bytes for attribute.
scep: pkistatus: SUCCESS3 06:53:13.491:
scep: reading inner PKCS#706:53:13.491:
scep: decrypting inner PKCS#753:13.492:
scep: found certificate:
  subject: /serialNumber= PID:AIR-LAP1262N-A-K9
    SN:FTX1433K60R/C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=AP3G1-f866f267577e/emailAddress=
tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
scep: PKCS#7 payload size: 1580 bytes:53:13.518:

Digital Signature, Key Encipherment
scep: waiting for 10 secs 06:53:13.520:
```

Éste es un ejemplo de un caso donde falla:

```
Fail log
WLC
(Cisco Controller) >debug pm pki scep detail enable
scep: waiting for 10 secsmLscScepTask: Nov 23 00:57:52.407:
scep: waiting for 10 secs 00:58:05.415:
scep: waiting for 10 secs 00:58:18.423:
scep: waiting for 10 secs 00:58:31.431:
scep: waiting for 10 secs 00:58:44.439:
scep: waiting for 10 secs 00:58:57.447:
scep: waiting for 10 secs 00:59:10.455:
scep: : Nov 23 00:59:22.479:
===== SCEP_OPERATION_GETCAPS =====
scep: Failed to get SCEP Capabilities from CA. Some CA's do not support this.
scep: Getting CA Certificate(s).
scep: : Nov 23 00:59:22.479:
===== SCEP_OPERATION_GETCA =====
scep: requesting CA certificate
```

```
scep: Sent 82 byteseded: Operation now in progress*emWeb: Nov 23 00:59:22.486:
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.
scep: header info: <Connection: close>
scep: header info: <Date: Wed, 23 Nov 2011 00:59:22 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 3795>
scep: header info: <Content-Type: application/x-x509-ca-ra-cert>
scep: MIME header: application/x-x509-ca-ra-cert
scep: found certificate:
  subject: /DC=com/DC=ccie/CN=AD
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature, Certificate Sign, CRL Sign
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Key Encipherment
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature
scep: CA cert retrieved with fingerprint 639993FF7FF8FB12EF2FB09DEC7C5BED

scep: waiting for 10 secs 00:59:23.463:

AP:
(Cisco Controller) >debug pm pki scep detail enable
scep: waiting for 10 secsmLscScepTask: Nov 22 18:06:22.100:
scep: waiting for 10 secs 18:06:35.108:
scep: waiting for 10 secs 18:06:48.116:
scep: waiting for 10 secs 18:07:01.124:
scep: AP MAC: 58:bc:27:13:4a:d0 Starting new enrollment request.
scep: creating inner PKCS#7:04.631:
scep: data payload size: 536 bytes:
scep: successfully encrypted payload
scep: envelope size: 838 bytes.633:
scep: Sender Nonce before send: F8BBA9EB06579188A62635A1DFA6510A
scep: creating outer PKCS#7:04.634:
scep: signature added successfully:
scep: adding signed attributes.634:
scep: adding string attribute transId
scep: adding string attribute messageType
scep: adding octet attribute senderNonce
scep: PKCS#7 data written successfully
scep: applying base64 encoding.655:
scep: base64 encoded payload size: 3055 bytes

scep: Sent 3280 bytesed: Operation now in progress*sshpmLscTask: Nov 22 18:07:04.690:
scep: SenderNonce in reply: 69A4BF610ED41746B1066B5BEC4427F0
scep: recipientNonce in reply: F8BBA9EB06579188A62635A1DFA6510A
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.:
scep: header info: <Connection: close>:
scep: header info: <Date: Tue, 22 Nov 2011 18:07:04 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 540>
scep: header info: <Content-Type: application/x-pki-message>
scep: MIME header: application/x-pki-message

scep: reading outer PKCS#718:07:14.133:
scep: PKCS#7 payload size: 540 bytes33:
scep: PKCS#7 contains 1 bytes of enveloped data
scep: verifying signature 18:07:14.134:
scep: signature ok Nov 22 18:07:14.135:
```

```
scep: finding signed attributes:14.135:
scep: finding attribute transId:14.135:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: 3DA1646840CD4FFEB1534EA8F1D45F76
scep: finding attribute messageType135:
scep: allocating 1 bytes for attribute.
scep: reply message type is good14.135:
scep: finding attribute senderNonce135:
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus4.136:
scep: allocating 1 bytes for attribute.
scep: pkistatus: FAILURE2 18:07:14.136:
scep: finding attribute failInfo14.136:
scep: allocating 1 bytes for attribute.
scep: reason: Transaction not permitted or supported
scep: waiting for 10 secs 18:07:14.136:
scep: waiting for 10 secs 18:07:27.144:
scep: waiting for 10 secs 18:07:40.152:
scep: waiting for 10 secs 18:07:53.160:
scep: waiting for 10 secs 18:08:06.168:
scep: waiting for 10 secs 18:08:19.176:
scep: waiting for 10 secs 18:08:32.184:
scep: waiting for 10 secs 18:08:45.192:
scep: waiting for 10 secs 18:08:58.200:
scep: waiting for 10 secs 18:09:11.208:
```

Información Relacionada

- Guía de configuración inalámbrica del regulador LAN de Cisco, versión 5.2
- Generación del pedido de firma de certificado (CSR) para un certificado de tercera persona en un regulador de la red inalámbrica (WLAN) (WLC)
- Generación del pedido de firma de certificado para un certificado y un procedimiento de tercera persona para cargar por teletratamiento los Certificados encadenados al WLC
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems