Localmente - Certificados significativos no exemplo de configuração dos controladores do Wireless LAN

Índice

Introdução

Este documento explica como configurar o controlador do Wireless LAN (WLC) e o Lightweight Access Points (regaços) para usar localmente - a característica significativa do certificado. Este recurso foi incorporado na versão 5.2 do Controlador de LAN Wireless. Com esta característica, se você escolhe controlar o Public Key Infrastructure (PKI), você pode gerar localmente - os Certificados significativos (LSC) nos Access point e nos controladores. Estes Certificados podem então ser usados para autenticar mutuamente o WLC e PARA DOBRÁ-LO.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar o WLC, o REGAÇO, e o cartão do cliente Wireless para a

operação básica
- Conhecimento de como configurar e usar o server de Microsoft Windows 2003 CA
- Conhecimento da infraestrutura de chave pública e dos Certificados digitais

Componentes Utilizados

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

- Cisco 4400 Series WLC que executa o firmware 5.2
- Access point de pouco peso do Cisco Aironet série 1130 AG (REGAÇO)
- Server de Microsoft Windows 2003 configurado como o controlador de domínio, e como um server do Certificate Authority.
- Adaptador cliente do a/b/g do 802.11 do Cisco Aironet que executa a versão de firmware 4.2
- Utilitário de desktop do Cisco Aironet (ADU) essa versão de firmware 4.2 das corridas

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

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Localmente - Certificados significativos

Em software release do controlador mais cedo do que 5.2.157.0, o controlador pode usar certificados auto-assinados (SSCs) para autenticar Access point ou enviar a informação de autorização a um servidor Radius, se os Access point fabricação-instalaram os Certificados (MIC). No software release 5.2.157.0 do controlador, você pode configurar o controlador para usar um certificado significativo local (LSC). Você pode usar um LSC se você quer seu próprio Public Key Infrastructure (PKI) fornecer a melhor Segurança; para ter o controle de seu Certificate Authority (CA), e definir políticas, limitações, e usos nos Certificados gerados.

Os Certificados novos LSC precisam de ser fornecida no controlador primeiramente e então o REGAÇO do server do Certificate Authority (CA).

O REGAÇO comunica-se com o controlador (WLC) com o protocolo CAPWAP. Todos os pedidos assinar o certificado e emitir os certificados de CA para o REGAÇO e para o WLC próprio, devem ser iniciados do WLC. O REGAÇO não se comunica diretamente com o server de CA. O WLC comporta-se como um CA-proxy ao AP do LWAPP. Os detalhes do server de CA devem ser configurados no WLC, e deve ser alcançável.

O controlador utiliza o protocolo simple certificate enrollment (SCEP) para enviar os certReqs gerados nos dispositivos a CA e utiliza o SCEP outra vez para obter os certificados assinados de CA.

O SCEP é um protocolo do gerenciamento certificado que os clientes do Public Key Infrastructure (PKI) e os server do Certificate Authority se usem para apoiar o certificado de registro e a revogação. É amplamente utilizado em Cisco e é apoiado por muitos CA-server. No protocolo

scep, o HTTP é usado como o protocolo de transporte para as mensagens PKI. O objetivo principal do SCEP é a emissão segura dos Certificados aos dispositivos de rede. O SCEP é capaz de muitas operações, mas para estes projeto e liberação, o SCEP é utilizado para estas operações.

- Distribuição da chave pública de CA e RA
- Certificado de registro

Todas as transações SCEP acontecem no modo automático. A revogação de certificado não é apoiada.

Note: Os LSC não são apoiados nos Access point que são configurados para o modo de Bridge.

Abastecimento do certificado nos controladores do Wireless LAN (WLC)

Os Certificados novos LSC, CA e os Certificados do dispositivo devem ser instalados no controlador.

Com o protocolo scep, os certificados de CA são recebidos do server de CA. Desde neste momento, não há nenhum Certificados atual no controlador, esta operação está um claro obtém a operação. Estes são instalados no controlador. Estes mesmos certificados de CA estão empurrados igualmente para os AP quando os AP são fornecida com LSC.

Operação do certificado de registro do dispositivo

Para o REGAÇO e o controlador que pede um certificado assinado de CA, o mais certRequest é enviado como uma mensagem PKCS#10. O mais certRequest contém o nome do sujeito, PublicKey e outros atributos a ser incluídos no certificado X.509, e assinados digitalmente pelo PrivateKey do solicitador. Estes devem ser enviados a CA, que transforma o mais certRequest em um certificado X.509.

CA que recebe um PKCS#10 o mais certRequest exige a informação adicional autenticar a identidade do solicitador e verificar que o pedido é inalterado. Muitas vezes PKCS#10 combinadas com outras aproximações, tais como PKCS#7, para enviar e receber o CERT Reqs/Resps.

Aqui, o o PKCS#10 é envolvido em um tipo de mensagem PKCS#7 SignedData. Isto está apoiado como parte da funcionalidade de cliente SCEP, quando a mensagem de PKCSReq for enviada ao controlador.

Em cima da operação bem sucedida do registro, CA e o certificado do dispositivo estão agora atuais no controlador.

Abastecimento do certificado em LWAPP AP

Para que um certificado novo seja fornecida no REGAÇO, quando do modo CAPWAP o REGAÇO dever reagir capaz de obter o certificado X.509 assinado novo. A fim fazer isto, envia um o mais certRequest ao controlador, que atua como um CA-proxy e as ajudas obtêm o mais certRequest assinado por CA para o REGAÇO.

O certReq e os certResponses são enviados ao REGAÇO com as cargas úteis LWAPP. Este diagrama mostra o fluxo para que o REGAÇO provision um LSC.

São aqui as etapas em detalhe:

1. O abastecimento do REGAÇO com LSC mais novos acontece uma vez que o REGAÇO está no estado ASCENDENTE, depois que SE JUNTOU ao WLC com seu MIC/SSC atual. Na fase do abastecimento LSC, mesmo que o AP esteja no estado ASCENDENTE, os rádios são fechados forçosamente.
2. O uso e a disposição do LSC devem ser permitidos no WLC. Este processo inclui para permitir o LSC, adicionar o server de CA, e para configurar outros parâmetros. Os parâmetros de um certificado LSC comandam o pedido são enviados do controlador PARA DOBRAR, com o assunto-nome, o tempo da validez e Keysize ajustado no payload. Estes campos estão usados pelo REGAÇO quando o mais certRequest é criado. O payload igualmente indica que o REGAÇO deve criar um o mais certRequest e o enviar de volta ao controlador.
3. O REGAÇO gerencie configurado keysize par de chaves público/privado RSA. Após a geração do keypair, um o mais certRequest é gerado após o SubjectName recebido do controlador é configurado. O CN é gerado automaticamente com o formato existente SSC/MIC, “Cxxxx-EtherMacAddr”. O REGAÇO gerencie um PKCS#10 CertReq e envia-o como um payload, pedido do certificado LSC, ao controlador.
4. O controlador cria então uma mensagem SSCEP PKCSReq, um mensagem formatada PKCS#7, e envia-à CA em nome do: DOBRE, a fim obter o pedido do certificado assinado por CA configurado. Os certs instalados CA/RA são usados para cifrar o certReq.
5. Se CA pode aprovar o pedido do certificado, uma mensagem de CertRep com Status=SUCCESS está enviada para trás ao cliente SSCEP (controlador) em um formato PKCS#7. A resposta CERT é escrita localmente em um arquivo como um certificado do formato PEM.
6. Desde que este CertResp é para o REGAÇO, o WLC envia o certificado ao REGAÇO com um payload do “resposta certificado”. O CERT de CA é enviado primeiramente com o mesmo payload, a seguir o certificado do dispositivo é enviado em um payload separado.

o LSC CA e os Certificados do dispositivo do REGAÇO são instalados no REGAÇO, e nas auto-repartições do sistema. A próxima vez que vem acima, desde que está configurado para usar LSC, o AP envia o certificado do dispositivo LSC ao controlador como parte do pedido da JUNTA. Como parte da resposta da JUNTA, o controlador envia seu certificado novo do dispositivo e igualmente valida o certificado de entrada do REGAÇO com o certificado de raiz de CA novo.

Note: Os LSC não são apoiados nos Access point que são configurados para o modo de Bridge.

O LSC apoia nos controladores do Wireless LAN (WLC) e no Lightweight Access Points (os regaços)

O LSC é apoiado nestas Plataformas WLC:

- Cisco 4400 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Módulo de Serviços sem fio do Cisco Catalyst 6500 Series (WiSM)
- Controlador integrado 3750G do Wireless LAN do Cisco catalyst
- Cisco Wireless LAN Controller Module

O LSC é apoiado nos Access point C1130, C1140, C1240, C1252 do Cisco Aironet e em todos os Access point novos.

O LSC não é apoiado na MALHA AP (1510, 1522), o modo de Bridge AP.

Este documento explica com um exemplo de configuração, como permitir localmente e autenticar regaços com - os Certificados significativos.

Configurar

Note: Localmente - a característica significativa do certificado pode ser permitida com o GUI ou o CLI no controlador.

Note: A característica LSC em um controlador não toma o desafio da senha. Consequentemente, para que o LSC trabalhe, você deve desabilitar o desafio da senha no server de CA. Também, você não pode usar o Microsoft Windows server 2008 como um server de CA porque não é possível desabilitar o desafio da senha nele.

Instalação de rede

Neste exemplo, você configura um controlador do Wireless LAN 4400 e um Access point de pouco peso do 1130 Series para usar localmente - os Certificados significativos (LSC). A fim realizar isto, você deve provision o controlador do Wireless LAN e o REGAÇO com os LSC do server do Certificate Authority (CA).

Este documento usa o server de Microsoft Windows 2003 como o server de CA.

Processo de instalação de CA e SCEP

O documento supõe que a configuração do servidor de CA no server de Microsoft Windows 2003 é no lugar. Está aqui o sumário das etapas para o processo de instalação de CA e SCEP:

1. A instalação Windows 2003 e o server de CA, certificam-se do trabalho de *http://ca-server/certsrv*
2. Transferência *cepsetup.exe da* site do microsoft
3. Instale cepsetup.exe, desmarcar de “a *frase do desafio* RequireSCEP*”,* desde que o WLC não poderia apoiar o desafio registra o modo agora.
4. Forneça o nome, o email, o país, a cidade e os outros detalhes.
5. Assegure trabalhos de *http://ca-server/certsrv/mscep/mscep.dll* como esperado.

Note: Você precisará de criar uma conta de usuário, para atribui-la leia e registre permissões para o molde do IPsec (pedido autônomo), e faça-lhe um membro do grupo IIS_WPG. Para detalhes completos refira a site do microsoft instalando e configurando o SCEP

Configurar o controlador do Wireless LAN com o GUI

Conclua estes passos:

1. Do controlador GUI do Wireless LAN, clique a **Segurança > o certificado > o LSC** a fim abrir a página significativa local dos Certificados (LSC).
2. Clique o **tab geral**.
3. A fim permitir o LSC no sistema, verifique a **possibilidade LSC na** caixa de verificação do **controlador**.

4. No campo URL do server de CA, incorpore a URL ao server de CA. Você pode incorporar um Domain Name ou um endereço IP de Um ou Mais Servidores Cisco ICM NT.
5. Nos campos dos Params, incorpore os parâmetros para o certificado do dispositivo. O tamanho chave é um valor de 384 a 2048 (nos bit), e o valor padrão é 2048.
6. O clique **aplica-se** para comprometer suas mudanças.
7. A fim adicionar o certificado de CA no base de dados do certificado de CA do controlador, para pairar seu cursor sobre a seta azul da gota-para baixo para o tipo do certificado, e para escolher **adicionar**. Exemplo:
8. A fim provision o LSC no Access point, clicar a **ABA de provisionamento AP**, e verificar a caixa de verificação do **abastecimento da possibilidade AP**.
9. A fim adicionar Access point à lista da disposição, para incorporar o MAC address do Access point ao campo e ao clique de endereços MAC de Ethernet AP **adicionar**. A fim remover um Access point da lista da disposição, para pairar seu cursor sobre a seta azul da gota-para baixo para o Access point, e para escolher **remove**.Se você configura uma lista da disposição do Access point, simplesmente os Access point na lista da disposição são fornecida quando você permitir o abastecimento AP. Se você não configura lista da disposição do Access point, todos os Access point com um certificado MIC ou de SSC que se juntam ao controlador são LSC fornecida.
10. O clique **aplica-se** para comprometer suas mudanças.

Configurar o controlador do Wireless LAN com o CLI

Refira a **utilização do CLI para configurar a** seção **LSC do** manual de configuração do controlador de LAN do Cisco Wireless, libere 5.2 para obter informações sobre do procedimento para permitir localmente - a característica significativa do certificado (LSC) do CLI no controlador.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Uma vez que o controlador do Wireless LAN é configurado e o server de CA é no lugar, o controlador do Wireless LAN usa o protocolo scep a fim comunicar-se com o server de CA e adquirir o certificado LSC. Está aqui um tiro de tela do WLC uma vez que o certificado é instalado.

Quando o REGAÇO vem acima, o REGAÇO descobre o WLC com a camada mecanismos de descoberta de 2 camadas 3 e envia pedidos de uma junta ao controlador com o certificado MIC.

O controlador do Wireless LAN envia então a requisição de parâmetro do certificado LSC ao REGAÇO.

Com o SubjectName/CN enviado do WLC, o AP gerencie PKCS #10 CertReq e envia “um pedido do certificado LWAPP LSC” ao WLC.

Este pedido por sua vez é enviado pelo WLC ao server de CA. O server de CA envia o certificado do REGAÇO LSC ao controlador. O controlador envia então o LSC ao REGAÇO.

Esta mensagem aparece no 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, o REGAÇO envia um pedido da junta com o LSC.

Emita o **comando enable dos eventos do capwap debugar** a fim ver esta sequência de evento.

Uma vez o REGAÇO registra-se com o WLC com o LSC, você pode confirmar isto no WLC GUI.

Você pode igualmente usar estes comandos do WLC CLI a fim verificar este. Aqui está um exemplo:

```
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
```

A fim ver detalhes sobre os Access point que são fornecida com LSC, incorpore 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 seção explica como pesquisar defeitos sua configuração. Você pode usar o **comando enable do scep do pki pm debugar** a fim ver a sequência de evento.

Está aqui um exemplo de um bem sucedido debuga o log:

```
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:
```

Este é um exemplo de um caso onde falhe:

```
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:
```

Informações Relacionadas

- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 5.2
- Geração da solicitação de assinatura de certificado (CSR) para um certificado da terceira em um controlador de WLAN (WLC)
- Geração da solicitação de assinatura de certificado para um certificado e um procedimento da terceira para transferir arquivos pela rede Certificados acorrentados ao WLC
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems